Pierre COLMEZ

ÉLÉMENTS D'ANALYSE ET D'ALGÈBRE

Pierre COLMEZ
C.M.L.S., École Polytechnique, 91128 Palaiseau Cedex, France.

ÉLÉMENTS D'ANALYSE ET D'ALGÈBRE

Pierre COLMEZ

SYNOPSIS

TABLE DES MATIÈRES

TABLE DES MATIÈRES DÉTAILLÉE

INTRODUCTION

Les mathématiques sont à la fois un outil d'une puissance surprenante, utilisé à des degrés divers par les autres sciences, et une des plus incroyables constructions collectives de l'humanité, s'appuyant sur des bases consolidées génération après génération pour permettre à l'édifice de monter toujours plus haut.

Ce cours est une introduction à trois des théories qui servent de socle aux mathématiques. La première (chap. I) est la théorie des représentations des groupes finis et de leurs caractères, développée dans les années 1895-1905 par F. Frobenius, W. Burnside et I. Schur. Cette théorie est une extension de l'algèbre linéaire (il s'agit de comprendre l'action simultanée de plusieurs isomorphismes sur un espace vectoriel de dimension fini, et donc l'action du groupe qu'ils engendrent), mais la théorie des caractères est aussi une première approche de la transformée de Fourier dans un cadre fini où les difficultés analytiques sont absentes. La théorie des représentations des groupes joue un rôle central en mathématiques, dans certaines branches de la physique (par exemple en physique des particules) ou encore dans une petite partie de la chimie classique (cristallographie) ; le cas des groupes finis sert souvent de guide pour deviner ce que l'on est en droit d'espérer dans des cas plus compliqués.

La seconde (chap. II, III et IV) est l'analyse fonctionnelle des années 1900-1930 (espaces de Banach, intégration de Lebesgue, transformée de Fourier), dans laquelle se sont illustrés R. Baire, S. Banach, M. Fréchet, H. Hahn, D. Hilbert, H. Lebesgue, M. Plancherel, F. Riesz, H. Steinhaus... Cette théorie, née des préoccupations du siècle précédent concernant les équations différentielles, les équations aux dérivées partielles..., forme la base de l'analyse réelle moderne. Ses applications à l'étude des équations aux dérivées partielles provenant de la physique (équations de la chaleur, des ondes, de Schrödinger...) sont innombrables.

La dernière partie du cours (chap V, VI et VII) est consacrée à la théorie des fonctions analytiques d'une variable complexe, qui s'est développée entre les mains de A. Cauchy dans les années 1820-1840, mais a été revisitée régulièrement depuis ; la présentation suivie dans ce cours doit beaucoup aux apports de K. Weierstrass et de H. Poincaré datant de

la seconde moitié du XIX$^{\text{e}}$ siècle. Cette théorie est probablement, avec la théorie générale des groupes, celle qui est utilisée dans le plus grand nombre des autres branches des mathématiques ou de la physique théorique. Par exemple, la représentation conforme des ouverts du plan, à laquelle nous ne ferons qu'une brève allusion (note 1 du chap. VI), a des applications à l'étude de l'équation de la chaleur avec conditions au bord dans un domaine plan, à l'aérodynamique (transformation de Joukovski), à l'étude du mouvement brownien ou celle des polymères, etc.

Le problème majeur d'un cours de ce type est que l'on est conduit à privilégier les résultats qui ont le plus d'applications futures et à reléguer en exercice tout ce qui fait le sel des mathématiques, ce qui revient un peu à visiter une cathédrale en ne s'intéressant qu'aux consolidations successives de la base de ses piliers. Pour essayer de lutter contre cette tendance, nous avons privilégié des objets analytiques, issus de la théorie des nombres, ayant la faculté étonnante d'interagir avec quasiment tous les domaines des mathématiques (voire de la physique théorique) et, ce faisant, de contribuer fortement au développement de ces domaines. Il s'agit des fonctions L, dont la fonction zêta de Riemann (définie par $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$ pour $\mathrm{Re}(s) > 1$) est le prototype. L'un des premiers résultats remarquables concernant ces objets est probablement la célèbre formule $\zeta(2) = \frac{\pi^2}{6}$ de L. Euler (1734), répondant à une question posée en 1644 et connue sous le nom de « problème de Bâle ». Le même Euler a mis au jour un lien heuristique entre la fonction ζ et la répartition des nombres premiers qui ne fut rigoureusement établi qu'en 1896 par J. Hadamard et C. de la Vallée Poussin en suivant une stratégie suggérée par B. Riemann en 1858. Entre-temps, G. Dirichlet avait introduit en 1837 les premières fonctions L pour démontrer l'existence d'une infinité de nombres premiers dans les progressions arithmétiques. L'annexe A, consacrée à ces résultats, fournit une illustration frappante de l'utilité des fonctions holomorphes pour attaquer des problèmes qui en semblent fort éloignés. Depuis, le monde des fonctions L s'est enrichi au point de former un édifice imposant dont l'annexe G essaie de donner une idée en partant de la constatation que, pour apprécier l'élégance et la majesté de la voûte de Notre-Dame, il n'est nul besoin de comprendre pourquoi elle ne s'écroule pas ni, a fortiori, comment on a fait pour la construire sans que tout tombe au fur et à mesure. Nous nous sommes restreint à l'aspect analytique des fonctions L ; celui-ci fait intervenir d'autres objets mathématiques ayant un don d'ubiquité assez époustouflant, à savoir les formes modulaires que nous avons reléguées dans une série d'exercices en vertu du principe énoncé plus haut. Nous avons (presque) résisté à la tentation d'explorer les propriétés arithmétiques de ces fonctions L : leurs valeurs aux entiers cachent des trésors qui font l'objet de conjectures générales de P. Deligne (1977, dont la conjecture met en perspective le π^2 de la formule d'Euler, et la non apparition de π^3 pour $\zeta(3)$), de A. Beilinson (1985, qui vise, en particulier, à expliquer quels objets interviennent dans $\zeta(3)$) et de S. Bloch et K. Kato (1989, dont la conjecture donne une formule totalement générale fournissant, par exemple, une signification à l'apparition de 691 dans la formule $\zeta(12) = \frac{691\,\pi^{12}}{3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13}$). Un exemple de ces trésors cachés est la conjecture

de Birch et Swinnerton-Dyer, qui date du début des années 1960, et à laquelle l'annexe F est consacrée.

Bibliographie sommaire

Le lecteur désirant approfondir [1] certains des thèmes développés dans ce cours est invité à consulter les ouvrages ci-dessous. Ces ouvrages partent à peu près au même niveau que le présent cours, mais sont plus spécialisés, ce qui leur permet d'aller plus loin.

P. Biane, J-B. Bost et P. Colmez, *La fonction zêta*, Presses de l'École Polytechnique.

Le lecteur y trouvera divers aspects de la fonction zêta en lien avec l'arithmétique ou les probabilités.

J-B. Bost, *Fonctions analytiques d'une variable complexe*, École Polytechnique.

Couvre les chapitres V à VII, et une partie de l'annexe A.

D. Bump, *Automorphic forms and representations*, Cambridge University Press.

Version développée de l'annexe G ; sa lecture demande un investissement non négligeable.

H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann.

Couvre les chapitres V et VI, et poursuit en direction de la géométrie (surfaces de Riemann, et fonctions de plusieurs variables).

W. Ellison, *Les nombres premiers*, Hermann.

Couvre l'annexe A, et bien plus.

W. Fulton et J. Harris, *Representation theory. A first course*, GTM 129, Springer-Verlag.

Débute par le chapitre I et l'annexe C, et poursuit en direction des représentations des groupes de Lie.

R. Godement, *Analyse mathématique II, III et IV*, Springer-Verlag.

Couvre l'essentiel du cours, et de ce que j'aurais voulu y mettre, en prenant son temps, ce que son nombre de pages permet. Les formes modulaires y sont traitées avec le respect qu'elles méritent.

N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer-Verlag.

Offre un voyage à travers la théorie des nombres en prenant comme fil conducteur le problème des nombres congruents (annexe F).

S. Patterson, *An introduction to the theory of the Riemann Zeta-function*, Cambridge University Press.

Couvre l'annexe A, et poursuit en direction des hypothèses de Riemann et Lindelöf.

W. Rudin, *Real and complex Analysis*, Mc Graw-Hill

Un cours d'analyse qui couvre en particulier la partie analyse du cours (chapitres II à VI), mais ne s'arrête pas là, loin s'en faut.

J-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France.

1. La manière standard pour fabriquer des exercices est de prendre des résultats démontrés dans des ouvrages plus spécialisés et de les découper en questions. Le lecteur trouvera donc dans ces ouvrages la solution de la plupart des exercices de ce cours...

Un fort joli livre pour en apprendre davantage sur les formes quadratiques à coefficients rationnels et les formes modulaires.

J-P. Serre, *Représentations linéaires des groupes finis*, Hermann.

Couvre le chapitre I et une partie de l'annexe C, et continue sur des sujets plus pointus concernant les représentations des groupes finis.

A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Springer-Verlag.

Un livre semi-historique très agréable à lire, illustrant à un niveau élémentaire les liens entre les fonctions holomorphes et la théorie des nombres.

Enfin, voici deux livres portant sur l'histoire des idées mathématiques dont beaucoup de notes de bas de page du présent texte sont issues. Les périodes couvertes par ces deux ouvrages ne sont pas identiques bien qu'il y ait une intersection non vide ; celle du second est plus récente et demande un bagage mathématique un peu plus solide.

A. Dahan-Dalmedico et J. Peiffer, *Une histoire des mathématiques, routes et dédales*, Points Sciences, Éditions du Seuil.

J. Dieudonné, *Abrégé d'histoire des mathématiques*, Hermann.

Préface de la seconde édition

Le cours dont est issu ce livre a pris fin, et j'en ai profité pour inclure le matériel pédagogique de la dernière année, et divers compléments (près de 200 pages au total).

Le Vocabulaire Mathématique a vu sa taille doubler par rapport à la première édition, et offre maintenant (si on lui adjoint un peu de l'analyse réelle des chapitres II, III et IV) un survol assez complet d'un cours correspondant aux deux années de classe préparatoire dans un lycée ambitieux [2], avec plus d'une centaine d'exercices corrigés dont beaucoup sont des classiques faisant partie de la culture de ces classes. Il ne s'agit pas d'un cours organisé, et je ne pense pas que ce soit l'endroit parfait pour un premier contact avec les sujets qu'il regroupe (les cours sont faits pour cela) ; son but est plutôt de rassembler et de préciser, sous une forme compacte, les résultats d'usage constant [3].

Le chapitre « Problèmes corrigés » a été enrichi d'exercices posés lors des examens finaux, et de quatre problèmes : l'un (prob. H.12) propose une démonstration de l'irrationalité de $\zeta(3)$ qui utilise la fonction Γ dans le plan complexe, un autre (prob. H.11) vise à démontrer l'identité $q^{1/24}\prod_{n\geqslant 1}(1-q^n) = \sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$ due à Euler et en profite pour passer en revue la plupart des techniques de transformée de Fourier et de fonctions holomorphes, le troisième (prob. H.13) présente un résultat très frappant de Borel concernant la rationalité d'une série $\sum a_n z^n$ à coefficients entiers, et le dernier (prob. H.4) établit la table des caractères du plus petit groupe simple après A_5. Les problèmes de ce genre sont une spécialité bien française, et je pense qu'ils expliquent en grande partie les succès de l'École Française de mathématiques : ils permettent d'illustrer l'unité des mathématiques en montrant, à un niveau relativement élémentaire, l'intérêt de combiner des techniques différentes. Ils offrent une aide irremplaçable pour assimiler les énoncés du cours et apprécier leur puissance, et mon conseil serait de chercher à les résoudre (et d'aller voir [4] la solution en cas d'échec), avant d'essayer de maîtriser les démonstrations des théorèmes fondamentaux (lire lesdites démonstrations peut toutefois être utile pour

2. Cela correspond à peu près à ce que j'ai eu la chance de recevoir comme cours en math. sup. (la pénurie de professeurs de mathématiques n'avait pas encore été résolue par une diminution drastique des heures d'enseignement au collège et au lycée et on arrivait en classe préparatoire nettement mieux armé qu'à l'heure actuelle) ; je voudrais en profiter pour remercier D. Monasse du riche et beau cours qu'il nous a offert cette année-là, et dont j'utilise le contenu tous les jours de ma vie de mathématicien.

3. Avec des démonstrations en petits caractères pour ceux qui aiment bien pouvoir vérifier que l'on n'est pas en train de leur raconter des sornettes ; certaines de ces démonstrations sont d'ailleurs assez belles

4. Lire la solution d'une question à laquelle on n'a pas réfléchi est la recette idéale pour ne rien apprendre ; par contre essayer de résoudre une question soi-même est la meilleure manière pour préparer le cerveau à recevoir et assimiler la solution. Les puristes prétendront qu'il ne faut jamais aller voir la solution et tout résoudre soi-même (c'est la position des japonais en ce qui concerne les problèmes de go ; celle des chinois est plutôt qu'il faut réfléchir dix minutes et aller voir la solution si on ne trouve pas ; il y a 30 ans, les japonais étaient de loin les plus forts, mais ils se sont depuis fait dépasser par les chinois et les coréens...).

se faire une idée de la manière dont les concepts s'articulent, mais s'acharner à les retenir est plutôt une perte de temps).

Les autres ajouts notables sont :

— un appendice (annexe E) démontrant la transcendance de π et l'existence d'une infinité de $\zeta(2n+1)$ irrationnels (en écho au prob. H.12),

— une construction complète de la fonction zêta p-adique (§ D.4),

— des remarques sur les équations diophantiennes (§ F.2).

J'ai appris énormément de choses en écrivant ce texte, et j'espère que le lecteur y trouvera de quoi satisfaire sa curiosité. Étant arithméticien, j'ai privilégié les problèmes issus de la théorie des nombres pour illustrer l'unité [5] des mathématiques ; quelqu'un de plus proche de la physique aurait probablement pu écrire autant d'appendices inspirés de problèmes physiques et mettant en jeu les mathématiques du Vocabulaire et des chapitres I à VII. La géométrie et les probabilités sont presque totalement absentes ; c'est fort regrettable car la vision que ces théories apportent est fondamentale (en particulier en théorie des nombres ou en physique), mais c'est un reflet de l'organisation de l'enseignement des mathématiques dans notre pays.

5. Il est assez fascinant de voir comment les concepts se répondent d'une théorie ou d'un monde à l'autre. La note 50 du Vocabulaire en fournit une illustration assez frappante. De même, le prob. H.9 m'a été inspiré par le th. D.3.2 du monde p-adique, dont je me suis demandé ce qu'il pouvait bien devenir dans le monde réel (ou complexe) ; j'ai réalisé par la suite qu'il s'agissait d'un résultat parfaitement classique dans la veine du th. de Paley-Wiener.

Notations standard

On note $\mathbf{N}$ l'ensemble $\{0, 1, 2, \ldots\}$ des entiers naturels, $\mathbf{Z}$ l'anneau des entiers relatifs, $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{R}$ le corps des nombres réels et $\mathbf{C}$ le corps des nombres complexes. On note $\mathbf{Q}^*$, $\mathbf{R}^*$ et $\mathbf{C}^*$ les groupes multiplicatifs de $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$.

On note $\mathbf{R}_+$ (resp. $\mathbf{R}_+^*$) l'ensemble des nombres réels positifs (resp. strictement positifs) et $\mathbf{R}_-$ (resp. $\mathbf{R}_-^*$) l'ensemble des nombres réels négatifs (resp. strictement négatifs).

On note $\overline{\mathbf{R}} = \mathbf{R} \cup \{\pm\infty\}$ la droite réelle achevée, et $\overline{\mathbf{R}}_+ = \mathbf{R}_+ \cup \{+\infty\}$ la demi-droite réelle achevée.

Si $t \in \mathbf{R}$, on note $[t]$ sa partie entière, et $\{t\} = t - [t]$, sa partie fractionnaire.

Si X est un ensemble, on note $|\mathrm{X}| \in \mathbf{N} \cup \{+\infty\}$ son cardinal ; si $\mathrm{Y} \subset \mathrm{X}$, on note $\mathbf{1}_\mathrm{Y} : \mathrm{X} \to \{0, 1\}$ la fonction caractéristique de Y (elle est définie par $\mathbf{1}_\mathrm{Y}(x) = 1$ si $x \in \mathrm{Y}$, et $\mathbf{1}_\mathrm{Y}(x) = 0$ si $x \notin \mathrm{Y}$). Si X et Y sont deux sous-ensembles d'un ensemble E, on note $\mathrm{X} - (\mathrm{X} \cap \mathrm{Y})$ ou simplement $\mathrm{X} - \mathrm{Y}$ le complémentaire de $\mathrm{X} \cap \mathrm{Y}$ dans X.

Si I et X sont des ensembles, on note X^I l'ensemble des applications de I dans X ; un élément de X^I est noté $i \mapsto x_i$ ou $i \mapsto x(i)$ ou encore $(x_i)_{i \in \mathrm{I}}$ (par exemple si $\mathrm{I} = \mathbf{N}$).

On écrit très souvent « $a, b \in \mathrm{X}$ » pour « $a \in \mathrm{X}$ et $b \in \mathrm{X}$ », et on n'explicite pas tous les quantificateurs : par exemple, on ecrit souvent « $|f(x)| \leqslant \varepsilon$ si $|x| \leqslant \delta$ » au lieu de « $|f(x)| \leqslant \varepsilon$ pour tout $|x| \leqslant \delta$ »

Si A est un anneau, et si $n \in \mathbf{N} - \{0\}$, on note $\mathbf{M}_n(\mathrm{A})$ l'anneau des matrices $n \times n$ à coefficients dans A, $\mathbf{GL}_n(\mathrm{A}) \subset \mathbf{M}_n(\mathrm{A})$ le groupe des matrices inversibles (celles dont le déterminant est inversible dans A), et $\mathbf{SL}_n(\mathrm{A})$ le sous-groupe de $\mathbf{GL}_n(\mathrm{A})$ des matrices de déterminant 1.

$x \gg 0$ (resp. $x \ll 0$) désigne un nombre réel suffisamment grand (resp. petit).

Si f, g sont deux fonctions d'un espace topologique X dans $\mathbf{R}$ ou $\mathbf{C}$, la notation $f = \mathrm{O}(g)$ au voisinage de x_0 signifie qu'il existe un voisinage V de x_0 et une constante $\mathrm{C} > 0$ telle que $|f(x)| \leqslant \mathrm{C}|g(x)|$ pour $x \in \mathrm{V}$; la notation $f = o(g)$ au voisinage de x_0 signifie qu'il existe un voisinage V de x_0 et une fonction $\varepsilon : \mathrm{V} \to \mathbf{R}_+$, tendant vers 0 en x_0, telle que $|f(x)| \leqslant \varepsilon(x)|g(x)|$, pour tout $x \in \mathrm{V}$.

VOCABULAIRE MATHÉMATIQUE

La nécessité de définir précisément les objets avec lesquels ils travaillent s'est imposée graduellement aux mathématiciens confrontés à des contradictions d'ordre presque métaphysique. L'avènement de la théorie des ensembles (à partir des travaux fondateurs de G. Cantor datant des années 1870) et l'axiomatisation croissante des mathématiques ont d'une part fait disparaître un certain nombre d'obstacles psychologiques à la création d'objets nouveaux [6], et d'autre part débouché sur la création d'un vocabulaire extrêmement précis, qui a rendu possible l'explosion des mathématiques au cours du XX^{e} siècle.

Ce mouvement a fini par atteindre l'enseignement avec l'introduction des « maths modernes » au collège (et même en grande section de maternelle). Dans les années 70, le programme enseigné dans le secondaire et dans les classes préparatoires reposait sur le slogan : « Dieu créa l'ensemble vide et l'homme fit le reste ». C'était un peu radical, mais avait le mérite de présenter les mathématiques de manière cohérente et de montrer que l'on pouvait créer de nouveaux objets à partir d'objets déjà existants. La présentation en était malheureusement extrêmement dogmatique, et l'impression qu'on en retirait était plutôt que Dieu avait créé l'ensemble vide et la théorie des ensembles, et sur sa lancée, les entiers, les entiers relatifs, les nombres rationnels, puis les groupes, les anneaux, les corps et les espaces vectoriels, puis les nombres réels, ensuite il avait introduit des ε et des δ, puis créé la topologie..., et quand il avait enfin été content du résultat, il avait fait don aux hommes d'une théorie immuable et parfaite, à la beauté froide et lisse.

6. Les nombres complexes ont mis près de deux siècles à être acceptés (et même les nombres négatifs ont eu leurs détracteurs ; un cas extrême est Augustus de Morgan qui continuait à les considérer, au milieu du XIX^{e}-siècle, comme dénués de tout fondement, et a passé une bonne partie de sa vie à essayer de prouver qu'on pouvait fort bien s'en passer), alors que, de nos jours, des objets nettement plus compliqués sont acceptés dès qu'ils ont fait la preuve de leur utilité pour résoudre, ou même formuler proprement, certains problèmes ; c'est par exemple le cas de l'anneau des « nombres complexes p-adiques » construit par J.-M. Fontaine (1982). Les obstacles psychologiques n'ont toutefois pas complètement disparu ; l'apparition d'un objet nouveau ne se fait pas sans heurt, et provoque des conflits parfois brutaux entre les anciens, dont le point de vue « On a fait de très bonnes maths pendant 2000 ans sans avoir besoin de ces horreurs » reflète l'appréhension devant la perspective de devoir étudier un nouveau sujet "incompréhensible", et les modernes qui voient dans le nouvel objet la solution à tous les problèmes...

Le dogme a changé vers le milieu des années 90, et on est reparti sur le mode : « Dieu a créé les nombres réels, puis les nombres complexes, et envoyé Gauss sur terre pour expliquer qu'il n'y avait pas besoin de chercher plus loin. ». Tout procédé de construction a été soigneusement banni du programme officiel, et une grande partie du vocabulaire mathématique de base a disparu ou a été vidé de sa substance [7]. C'est fort regrettable car la maîtrise du vocabulaire mathématique demande du temps : il décrit des concepts qui reposent souvent sur d'autres concepts, et il faut voir fonctionner ces concepts pour saisir véritablement le sens des mots. Or ce temps fait cruellement défaut une fois passée la période des classes préparatoires.

Ce chapitre essaie de pallier ces disparitions ; la plus grande partie de son contenu n'est pas utilisée dans le texte principal [8], mais est incluse car elle est susceptible de faire son apparition dans n'importe quel domaine utilisant des mathématiques. Il ne prend pas les mathématiques à leur début [9], et le lecteur est supposé avoir déjà des notions même vagues de la plupart des sujets qui suivent. Plutôt qu'un cours organisé, il s'agit d'une espèce de dictionnaire, et comme dans un dictionnaire, il n'est pas rare que certains passages fassent appel à des notions définies ultérieurement.

1. Grammaire élémentaire

L'*axiome du choix* postule qu'un produit d'ensembles non vides est non vide (i.e. si $\mathrm{X}_i \neq \varnothing$, pour $i \in \mathrm{I}$, alors $\prod_{i\in\mathrm{I}} \mathrm{X}_i \neq \varnothing$). Autrement dit, on peut choisir *simultanément* un élément dans chacun des X_i, si les X_i sont non vides. Cet axiome a l'air évident, mais il est indépendant des axiomes de la théorie des ensembles sur lesquels reposent les mathématiques modernes, ce qui veut dire qu'on peut choisir de l'inclure ou non (en analyse, on peut difficilement se passer de l'axiome du choix dénombrable, qui est de toute façon assez raisonnable : on peut imaginer que face au problème de choisir un nombre dénombrable d'éléments, on devienne de plus en plus performant, et donc arriver à choisir tous ces éléments en un temps fini ; avec un nombre non dénombrable d'éléments, ceci est voué à l'échec, si on doit les choisir un par un). L'inclure a d'énormes avantages pour démontrer des résultats d'existence, mais il a l'inconvénient

7. Le programme de la filière PC est à cet égard assez catastrophique, puisque sa dernière mouture a vu l'introduction de faux concepts, et même de définitions fausses.

8. Les résultats exposés dans le cours sont en grande partie antérieurs à la mise en valeur des concepts présentés dans ce chapitre, ce qui fait que l'on peut les présenter, en se contorsionnant un peu, sans recourir à ces concepts. D'un autre côté, lire « Les misérables » ou les « Disquisitiones arithmeticae » à la lumière d'une lampe électrique est nettement plus confortable qu'à la lueur d'une chandelle, même si ces œuvres datent d'avant l'invention de l'ampoule électrique et si la chandelle a un charme certain...

9. Il a été écrit de la manière suivante. J'ai d'abord, pour chaque concept de base, fait une liste des énoncés que j'utilise régulièrement sans me poser de question. C'est plus ou moins ce qui se trouve en gros caractères. J'ai ensuite rajouté les démonstrations (en général en petits caractères). Une exception à ce principe est le traitement de la réduction des endomorphismes, où j'ai remplacé le point de vue enseigné en classes préparatoires par une autre qui donne des résultats plus puissants. J'ai aussi rajouté, pour les amateurs, une collection de monstres mathématiques, et quelques résultats plus culturels comme la construction des nombres p-adiques, les théorèmes de Sylow ou la simplicité de A_n.

de rendre ces résultats d'existence ineffectifs, et on est toujours plus content quand on peut s'en passer. J'ai essayé de signaler dans le texte les endoits où utiliser l'axiome du choix fait une différence.

1.1. Coefficients binomiaux

On note $\binom{\mathrm{X}}{k} \in \mathbf{Q}[\mathrm{X}]$, pour $k \in \mathbf{N}$, les *polynômes binomiaux*; ils sont définis par $\binom{\mathrm{X}}{0} = 1$ et $\binom{\mathrm{X}}{k} = \frac{\mathrm{X}(\mathrm{X}-1)\cdots(\mathrm{X}-k+1)}{k!}$, si $k \geqslant 1$; on a donc $\binom{\mathrm{X}}{1} = \mathrm{X}$, $\binom{\mathrm{X}}{2} = \frac{\mathrm{X}(\mathrm{X}-1)}{2}$, etc.

• Si $k \geqslant 1$, alors $\binom{\mathrm{X}+1}{k} - \binom{\mathrm{X}}{k} = \binom{\mathrm{X}}{k-1}$.

On a : $\binom{\mathrm{X}+1}{k} - \binom{\mathrm{X}}{k} = \frac{\big((\mathrm{X}+1)-(\mathrm{X}-k+1)\big)\mathrm{X}(\mathrm{X}-1)\cdots(\mathrm{X}-k+2)}{k!} = \frac{\mathrm{X}(\mathrm{X}-1)\cdots(\mathrm{X}-k+2)}{(k-1)!} = \binom{\mathrm{X}}{k-1}$.

• Les *nombres binomiaux* $\binom{n}{k}$, pour $k \in \mathbf{N}$ et $n \in \mathbf{Z}$ sont des entiers vérifiant la relation $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ du triangle de Pascal.

La relation du triangle de Pascal résulte du point précédent. Montrons, par récurrence sur k, que $\binom{n}{k} \in \mathbf{Z}$ pour tout $n \in \mathbf{Z}$. C'est clair si $k = 0$ puisqu'alors $\binom{n}{k} = 1$. Si $k \geqslant 1$, on a $\binom{0}{k} = 0$, et la formule $\binom{n+1}{k} - \binom{n}{k} = \binom{n}{k-1}$ permet de déduire de l'hypothèse de récurrence $\binom{n}{k-1} \in \mathbf{Z}$ pour tout n, que $\binom{n}{k} \in \mathbf{Z}$ pour tout $n \geqslant 0$, par récurrence montante sur n, et $\binom{n}{k} \in \mathbf{Z}$ pour tout $n \leqslant 0$, par récurrence descendante sur n. Ceci prouve que le résultat est vrai pour k et permet de conclure.

• Si $k, n \in \mathbf{N}$, alors $\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$ est aussi le nombre C_n^k de parties à k éléments dans un ensemble à n éléments.

La formule $\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$ est immédiate sur la définition. Maintenant, $\mathrm{C}_{n+1}^k = \mathrm{C}_n^k + \mathrm{C}_n^{k-1}$ car les parties à k éléments de $\{1, \ldots, n+1\}$ se partitionnent en celles qui ne contiennent pas $n+1$ (il y en a C_n^k) et celles qui contiennent $n+1$ et donc ne contiennent que $k-1$ éléments de $\{1, \ldots, n\}$ (il y en a C_n^{k-1}). Les C_n^k et les $\binom{n}{k}$ vérifient donc les mêmes relations de récurrence. Comme $\mathrm{C}_n^0 = 1 = \binom{n}{0}$ pour tout n, et comme $\mathrm{C}_0^k = 0 = \binom{0}{k}$, si $k \geqslant 1$, on en déduit, par récurrence sur k, que $\mathrm{C}_n^k = \binom{n}{k}$ pour tout $n \in \mathbf{N}$ (ce dernier énoncé se démontre, k étant fixé, par récurrence sur n). On trouvera une démonstration plus conceptuelle dans l'ex. 3.8.

• On a $\binom{-1}{k} = (-1)^k$ et $\binom{-n}{k} = (-1)^k\binom{n+k-1}{k}$, si $k, n \in \mathbf{N}$.

Il suffit de revenir à la formule.

1.2. L'anneau Z des entiers relatifs

• Si A est un sous groupe de $\mathbf{Z}$ (muni de $+$), il existe $\mathrm{D} \geqslant 0$ unique, tel que $\mathrm{A} = \mathrm{D}\mathbf{Z}$.

Si $\mathrm{A} = \{0\}$, alors $\mathrm{D} = 0$. Si $\mathrm{A} \neq \{0\}$, alors A contient des éléments > 0 puisque A est stable par $x \mapsto -x$; soit D le plus petit de ces éléments. Une récurrence immédiate montre que A contient $n\mathrm{D}$, pour tout $n \in \mathbf{N}$, et donc aussi pour tout $n \in \mathbf{Z}$ puisque A est stable par $x \mapsto -x$. Autrement dit, $\mathrm{A} \supset \mathrm{D}\mathbf{Z}$.

Maintenant, soit $a \in \mathrm{A}$, et soit $r \in \{0, \ldots, \mathrm{D}-1\}$ le reste de la division euclidienne de a par D. Alors $a - r \in \mathrm{D}\mathbf{Z} \subset \mathrm{A}$, et donc $r = a - (a - r) \in \mathrm{A}$. Comme D est, par hypothèse, le plus petit élément strictement positif de A, cela implique $r = 0$, et donc $a \in \mathrm{D}\mathbf{Z}$. On en déduit l'inclusion $\mathrm{A} \subset \mathrm{D}\mathbf{Z}$ et l'égalité $\mathrm{A} = \mathrm{D}\mathbf{Z}$ que l'on cherchait à démontrer.

On écrit $a \mid b$ (pour a divise b) pour signifier que b est un multiple de a, et $a \nmid b$ pour signifier le contraire. Si $a, b \in \mathbf{Z}$, on définit le *plus grand diviseur commun* $\mathrm{pgcd}(a, b)$ de a

et b comme étant 0 si $a = b = 0$, et comme étant le plus grand entier $d > 0$ divisant à la fois a et b, si $a \neq 0$ ou $b \neq 0$. On dit que a et b sont *premiers entre eux*, si $\mathrm{pgcd}(a, b) = 1$.

Un élément p de $\mathbf{N}$ est *premier*, si $p \neq 1$ et si les seuls diviseurs de p sont 1 et p. On note $\mathscr{P} = \{2, 3, 5, \ldots\}$ l'ensemble des nombres premiers. Il est clair que si $p \in \mathscr{P}$, et si $a \in \mathbf{N}$, alors soit $p \mid a$ auquel cas $\mathrm{pgcd}(p, a) = p$, soit $p \nmid a$ auquel cas p est premier à a.

Remarquons que $a\mathbf{Z} + b\mathbf{Z} = \{ax + by,\ x, y \in \mathbf{Z}\}$ est un sous-groupe de $\mathbf{Z}$; et c'est le plus petit sous-groupe de $\mathbf{Z}$ contenant a et b (en effet, un sous-groupe de $\mathbf{Z}$ contenant a et b contient ax et by et donc aussi $ax + by$, pour tous $x, y \in \mathbf{Z}$). On note (a, b), l'élément de $\mathbf{N}$ tel que $a\mathbf{Z} + b\mathbf{Z} = (a, b)\mathbf{Z}$; cet élément existe et est unique d'après le point ci-dessus.

• Si $a, b \in \mathbf{Z}$, alors $(a, b) = \mathrm{pgcd}(a, b)$; en particulier, *a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbf{Z}$ tels que* $1 = au + bv$ (théorème de Bézout [10]).

Si $a = b = 0$, le résultat est immédiat. Suposons donc $a \neq 0$ ou $b \neq 0$. Par définition de (a, b), a et b sont des multiples de (a, b), et donc $(a, b) \leqslant \mathrm{pgcd}(a, b)$. Réciproquement, si $d \geqslant 1$ divise a et b, alors d divise $ax + by$, quels que soient $x, y \in \mathbf{Z}$; en particulier, d divise (a, b) et donc $d \leqslant (a, b)$. On en déduit l'inégalité $(a, b) \geqslant \mathrm{pgcd}(a, b)$ qui permet de conclure.

• Si a est premier avec b et c, alors a est premier avec bc ; si a divise bc et si a est premier avec b, alors a divise c (lemme de Gauss).

Si $(a, b) = (a, c) = 1$, il existe u_1, v_1 tels que $au_1 + bv_1 = 1$ et u_2, v_2 tels que $au_2 + cv_2 = 1$. On a donc $1 = (au_1 + bv_1)(au_2 + cv_2) = au + bcv$, avec $u = au_1u_2 + bv_1u_2 + cu_1v_2$ et $v = v_1v_2$, ce qui prouve que $(a, bc) = 1$. On en déduit le premier énoncé.

Si $bc = ad$ et $au + bv = 1$, alors $acu + adv = c$, et donc $a(cu + dv) = c$, ce qui prouve que a divise c ; d'où le second énoncé.

• Si $n \in \mathbf{Z} - \{0\}$, il existe des nombres premiers $p_1, \ldots, p_r$ tels que $n = \mathrm{sign}(n)\, p_1 \cdots p_r$; de plus, les p_i, pour $1 \leqslant i \leqslant r$, sont uniquement déterminés à l'ordre près. En d'autres termes, n peut se factoriser de manière unique comme un produit de facteurs premiers [11] (théorème fondamental de l'arithmétique).

Le cas $n < 0$ se déduit du cas $n > 0$; on peut donc supposer $n > 0$.

L'existence se démontre par récurrence. C'est évident pour $n = 1$, auquel cas, on a $r = 0$ (un produit vide vaut 1 par définition). Maintenant, si $n \geqslant 2$ est premier, alors $n = n$ est une factorisation de n sous la forme voulue. Si $n \geqslant 2$ n'est pas premier, alors $n = ab$, avec $2 \leqslant a \leqslant n - 1$ et $2 \leqslant b \leqslant n - 1$. On peut donc appliquer l'hypothèse de récurrence à a et b, ce qui permet d'écrire a sous la forme $a = p_1 \cdots p_s$, et b sous la forme $b = p_{s+1} \cdots p_r$, où $p_1, \ldots, p_r$ sont des nombres premiers. On a alors $n = p_1 \cdots p_r$, ce qui prouve que n admet une factorisation sous la forme voulue.

10. Il est en fait dû à C.-G. Bachet de Méziriac (1624) ; Bézout (1730-1783) a démontré l'énoncé analogue dans l'anneau K[X].

11. Si n est le produit de deux nombres premiers ayant chacun un millier de chiffres, on peut prouver, avec l'aide d'un ordinateur, que n n'est pas premier, mais il est impossible, à l'heure actuelle, de retrouver les deux nombres premiers qui divisent n. Ceci est à la base de la sécurité du système RSA, datant de 1977, en vigueur pour les transactions sur Internet. C'est aussi une bonne illustration de la différence entre la théorie et la pratique, qui en théorie sont la même chose, mais en pratique...

L'unicité se démontre en utilisant le lemme de Gauss. Si $p_1 \cdots p_r = q_1 \cdots q_s$ où les p_i et les q_j sont des nombres premiers, le lemme de Gauss montre que p_r divise l'un des q_j et donc lui est égal. Quitte à permuter les q_j, on peut supposer que $p_r = q_s$, et en divisant les deux membres par $p_r = q_s$, on se ramène à $r-1$ et $s-1$, ce qui permet de conclure par récurrence.

• Il y a une infinité de nombres premiers.

Supposons le contraire, et soient $p_1, \ldots, p_r$ les nombres premiers. Soit $n = (p_1 \cdots p_r) + 1$, et soit p un nombre premier divisant n (il en existe grâce au point précédent). Comme p ne peut pas être un des p_i puisque le reste de la division par p_i est 1, on aboutit à une contradiction qui permet de conclure.

• Si $n \in \mathbf{Z} - \{0\}$, et si p est un nombre premier, on note $v_p(n)$ le nombre de fois que p apparaît dans la décomposition en facteurs premiers de n ; alors $p^{v_p(n)}$ est aussi la plus grande puissance de p divisant n, et $v_p(n)$ est la *valuation p-adique* de n.

On étend cette définition à $n \in \mathbf{Z}$ en posant $v_p(0) = +\infty$. On dispose alors d'un critère de divisibilité assez utile : *a divise b si et seulement si $v_p(a) \leqslant v_p(b)$ pour tout nombre premier p.* En revenant à la définition de $\mathrm{pgcd}(a,b)$, on en déduit la formule $\mathrm{pgcd}(a,b) = \prod_p p^{\inf(v_p(a),v_p(b))}$.

Exercice 1.1. — Si $a, b \in \mathbf{Z}$, on définit le plus petit commun multiple $\mathrm{ppcm}(a,b)$ de a et b comme le plus petit entier $\geqslant 0$, multiple à la fois de a et b.

(i) Montrer que $a\mathbf{Z} \cap b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$, et que $a\mathbf{Z} \cap b\mathbf{Z} = \mathrm{ppcm}(a,b)\mathbf{Z}$.

(ii) Montrer que $\mathrm{ppcm}(a,b) = \prod_p p^{\sup(v_p(a),v_p(b))}$, si $a \neq 0$ et $b \neq 0$.

Exercice 1.2. — (i) Montrer que $v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a+b) \geqslant \inf(v_p(a), v_p(b))$, pour tous $a, b \in \mathbf{Z}$.

(ii) Montrer que v_p a un unique prolongement à $\mathbf{Q}$ tel que $v_p(xy) = v_p(x) + v_p(y)$, pour tous $x, y \in \mathbf{Q}$, et que l'on a alors $v_p(x+y) \geqslant \inf(v_p(x), v_p(y))$, quels que soient $x, y \in \mathbf{Q}$.

(iii) Montrer que $\sqrt{2}$ est irrationnel.

Exercice 1.3. — (i) Montrer que $v_p(a+b) = \inf(v_p(a), v_p(b))$, si $v_p(a) \neq v_p(b)$.

(ii) Montrer que $v_p\big(\sum_{i=1}^n a_i\big) = \inf_{1 \leqslant i \leqslant n} v_p(a_i)$, si l'inf. n'est atteint que pour une valeur de i.

(iii) Montrer que $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ n'est pas un entier, si $n \geqslant 2$.

Exercice 1.4. — (i) Soient $n \geqslant 1$ et p un nombre premier. Montrer que $v_p(n!) = \big[\frac{n}{p}\big] + \big[\frac{n}{p^2}\big] + \big[\frac{n}{p^3}\big] + \cdots$. En déduire que $v_p(n!) = \frac{n - \mathrm{S}_p(n)}{p-1}$, où $\mathrm{S}_p(n)$ est la somme des chiffres de n en base p.

(ii) Montrer que $[x] - \big[\frac{x}{2}\big] - \big[\frac{x}{3}\big] - \big[\frac{x}{5}\big] + \big[\frac{x}{30}\big]$ est toujours $\geqslant 0$. En déduire que $\frac{(30n)!\,n!}{(15n)!\,(10n)!\,(6n)!}$ est un entier [12], pour tout $n \in \mathbf{N}$.

(iii) Montrer que $v_p\big(\binom{a+b}{a}\big)$ est le nombre de retenues dans l'addition de $a+b$ en base p, si $a, b \in \mathbf{N}$.

(iv) Soit p un nombre premier. Montrer que $\binom{p}{i}$ est divisible par p, si $1 \leqslant i \leqslant p-1$. En déduire que $n^p - n$ est divisible par p pour tout $n \in \mathbf{Z}$ (petit th. de Fermat).

12. Cette observation, couplée avec la formule de Stirling, a permis à P. Tchebychev de montrer, en 1852, que le nombre $\pi(x)$ de nombres premiers $\leqslant x$ vérifie $(0,92 + o(1))\frac{x}{\log x} \leqslant \pi(x) \leqslant (1,05 + o(1))\frac{x}{\log x}$, encadrement que l'on pourra comparer avec le th. des nombres premiers de l'annexe A. En 2005, F. Rodriguez-Villegas a démontré que la série $\sum_{n=0}^{+\infty} \frac{(30n)!\,n!}{(15n)!\,(10n)!\,(6n)!}\mathrm{T}^n$ était algébrique, ce qui signifie qu'il existe un polynôme P à coefficients dans $\mathbf{Q}(\mathrm{T})$ qui l'annule ; il a aussi prouvé que le degré minimal d'un tel polynôme est 483840, ce qui rend son explicitation problématique...

1.3. Parallélisme entre logique élémentaire et langage ensembliste

Si p est un prédicat (i.e. une application à valeurs dans $\{\text{vrai, faux}\} \cong \{0,1\}$), alors p est aussi la fonction caractéristique de l'ensemble $\{x,\ p(x)\}$ des x pour lesquels $p(x) = 1$.

• La négation $p \mapsto \overline{p} = 1 - p$ correspond au passage au complémentaire : $\{x,\ \overline{p}(x)\}$ est le complémentaire de $\{x,\ p(x)\}$.

• $\wedge$ ("et") correspond à l'intersection : $\{x,\ p(x) \wedge q(x)\} = \{x,\ p(x)\} \cap \{x,\ q(x)\}$.

• $\vee$ ("ou") correspond à la réunion : $\{x,\ p(x) \vee q(x)\} = \{x,\ p(x)\} \cup \{x,\ q(x)\}$.

• La formule $\overline{p \vee q} = \overline{p} \wedge \overline{q}$ (resp. $\overline{p \wedge q} = \overline{p} \vee \overline{q}$) devient : le complémentaire de la réunion (resp. l'intersection) est l'intersection (resp. la réunion) des complémentaires.

• $\Rightarrow$ correspond à l'inclusion : $p \Rightarrow q$ si et seulement si $\{x,\ p(x)\} \subset \{x,\ q(x)\}$.

• $\forall$ correspond à une intersection : $\{x,\ \forall i \in \mathrm{I}, p_i(x)\} = \cap_{i\in\mathrm{I}}\{x,\ p_i(x)\}$.

• $\exists$ correspond à une réunion : $\{x,\ \exists i \in \mathrm{I}, p_i(x)\} = \cup_{i\in\mathrm{I}}\{x,\ p_i(x)\}$.

Considérons, par exemple, deux espaces métriques X et Y, et une suite de fonctions $(f_n)_{n\in\mathbf{N}}$ de X dans Y. Soit A l'ensemble des $x \in \mathrm{X}$ tels que $f_n(x)$ converge. Alors A peut s'écrire sous la forme :

$$\begin{aligned}\mathrm{A} =& \{x \in \mathrm{X},\ \exists y \in \mathrm{Y},\ \forall j \in \mathbf{N},\ \exists \mathrm{N} \in \mathbf{N},\ \forall n \geqslant \mathrm{N},\ d(f_n(x), y) < 2^{-j}\} \\ =& \cup_{y\in\mathrm{Y}} \cap_{j\in\mathbf{N}} \cup_{\mathrm{N}\in\mathbf{N}} \cap_{n\geqslant\mathrm{N}} f_n^{-1}(\{y' \in \mathrm{Y},\ d(y,y') < 2^{-j}\}).\end{aligned}$$

Si Y est complet, on peut utiliser le critère de Cauchy au lieu de donner un nom à la limite, et on obtient [en notant $f_{n,p} : \mathrm{X} \to \mathrm{Y} \times \mathrm{Y}$ la fonction $x \mapsto (f_n(x), f_p(x))$] :

$$\begin{aligned}\mathrm{A} =& \{x \in \mathrm{X},\ \ \forall j \in \mathbf{N},\ \exists \mathrm{N} \in \mathbf{N}, \forall n, p \geqslant \mathrm{N},\ d(f_n(x), f_p(x)) < 2^{-j}\} \\ =& \cap_{j\in\mathbf{N}} \cup_{\mathrm{N}\in\mathbf{N}} \cap_{n,p\geqslant\mathrm{N}} f_{n,p}^{-1}\big(\{(y,y') \in \mathrm{Y}\times\mathrm{Y},\ d(y,y') < 2^{-j}\}\big).\end{aligned}$$

La seconde formulation a l'avantage de ne faire intervenir que des intersections et réunions indexées par des ensembles dénombrables.

1.4. Ensembles dénombrables

Un ensemble est *dénombrable* s'il est fini ou s'il peut être mis en bijection avec $\mathbf{N}$.

• Un sous-ensemble d'un ensemble dénombrable est dénombrable.

> Il suffit de démontrer qu'un sous-ensemble X de $\mathbf{N}$, qui n'est pas fini, peut être mis en bijection avec $\mathbf{N}$. Si $x \in \mathrm{X}$, soit $\varphi(x) = |\{y \in \mathrm{X},\ y < x\}|$. Si x_0 est le plus petit élément de X, on a $\varphi(x_0) = 0$, ce qui montre que $\varphi(\mathrm{X})$ contient 0. Si $\varphi(x) = n$, et x' est le plus petit élément de X strictement supérieur à x, on a $\varphi(x') = n + 1$, ce qui prouve que φ est surjective. Par ailleurs, φ est injective car strictement croissante (si $x_1 < x_2$, alors $\{y \in \mathrm{X},\ y < x_2\}$ contient $\{y \in \mathrm{X},\ y < x_1\}$ et x_1). Ceci permet de conclure.

• Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est injective et si Y est dénombrable, alors X est dénombrable ; si $\varphi : \mathrm{X} \to \mathrm{Y}$ est surjective et si X est dénombrable, alors Y est dénombrable.

> Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est injective, alors φ réalise une bijection de X sur $\varphi(\mathrm{X})$ qui est dénombrable comme sous-ensemble d'un ensemble dénombrable, et X est dénombrable. Si $\varphi : \mathrm{X} \to \mathrm{Y}$ est surjective, on peut choisir (cela demande l'axiome du choix), pour tout $y \in \mathrm{Y}$, un antécédent $s(y) \in \mathrm{Y}$ de y par φ. Alors $s : \mathrm{Y} \to \mathrm{X}$ est injective car $s(y_1) = s(y_2)$ implique $y_1 = \varphi(s(y_1)) = \varphi(s(y_2)) = y_2$, et donc Y est dénombrable si X l'est, d'après ce qui précède.

• Un produit fini d'ensembles dénombrables est dénombrable.

Soient $\mathrm{X}_1, \ldots, \mathrm{X}_k$ des ensembles dénombrables, $\mathrm{X} = \mathrm{X}_1 \times \cdots \times \mathrm{X}_k$, et $p_1, \ldots, p_k$ des nombres premiers distincts. Soit $\varphi_i : \mathrm{X}_i \to \mathbf{N}$ injective, pour tout $i \in \{1, \ldots, k\}$. Alors $\varphi : \mathrm{X} \to \mathbf{N}$, définie par $\varphi(x_1, \ldots, x_k) = p_1^{\varphi_1(x_1)} \cdots p_k^{\varphi_k(x_k)}$ est injective d'après le « théorème fondamental de l'arithmétique » (unicité de la factorisation d'un entier naturel non nul en produit de nombres premiers).

• Une réunion dénombrable d'ensembles dénombrables est dénombrable.

Soit $(\mathrm{X}_i)_{i\in\mathrm{I}}$, avec I dénombrable et chacun des X_i aussi. Soient $\varphi_i : \mathrm{X}_i \to \mathbf{N}$, pour $i \in \mathrm{I}$, des applications injectives, et soit $\mathrm{Y} \subset \mathrm{I} \times \mathbf{N}$ l'ensemble des couples $(i, \varphi_i(x))$, pour $i \in \mathrm{I}$ et $x \in \mathrm{X}_i$. Alors Y est dénombrable comme sous-ensemble de l'ensemble dénombrable $\mathrm{I} \times \mathbf{N}$, et l'application $(i, y) \mapsto \varphi_i^{-1}(y)$ de Y dans $\cup_{i\in\mathrm{I}}\mathrm{X}_i$ est surjective, ce qui prouve que $\cup_{i\in\mathrm{I}}\mathrm{X}_i$ est dénombrable.

• $\mathbf{Z}$, $\mathbf{N}^d$, $\mathbf{Z}^d$, si $d \in \mathbf{N}$, et $\mathbf{Q}$ sont dénombrables [13].

L'application $(a, b) \mapsto a - b$ est une surjection de $\mathbf{N} \times \mathbf{N}$ sur $\mathbf{Z}$, et comme $\mathbf{N} \times \mathbf{N}$ est dénombrable, en tant que produit fini d'ensembles dénombrables, il en est de même de $\mathbf{Z}$. Les ensembles $\mathbf{N}^d$, $\mathbf{Z}^d$ sont dénombrables puisque ce sont des produits finis d'ensembles dénombrables. Enfin, $(a, b) \mapsto \frac{a}{b}$ induit une surjection de $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ sur $\mathbf{Q}$ qui, de ce fait est dénombrable, $\mathbf{Z}$ et $\mathbf{Z} - \{0\}$ l'étant.

• $\mathbf{R}$ et l'ensemble $\{0, 1\}^{\mathbf{N}}$ des suites à valeurs dans $\{0, 1\}$ ne sont pas dénombrables.

Supposons que $\{0, 1\}^{\mathbf{N}}$ est dénombrable. Il existe donc une bijection $n \mapsto x_n$ de $\mathbf{N}$ sur $\{0, 1\}^{\mathbf{N}}$. Chaque x_n est une suite $x_n = (x_{n,k})_{k\in\mathbf{N}}$, où $x_{n,k} \in \{0, 1\}$, ce qui permet de considérer la suite $y = (y_k)_{k\in\mathbf{N}}$, où $y_k = 1 - x_{k,k}$. Par construction, la suite y a sa n-ième valeur distincte de celle de x_n, pour tout n, et on a donc $y \neq x_n$, quel que soit $n \in \mathbf{N}$, ce qui est en contradiction avec l'hypothèse selon laquelle $n \mapsto x_n$ est surjective ; c'est donc que $\{0, 1\}^{\mathbf{N}}$ n'est pas dénombrable. Cet argument est *l'argument diagonal* de Cantor (1891).

Pour démontrer que $\mathbf{R}$ n'est pas dénombrable, il suffit de constater que si X désigne le sous-ensemble de $[0, 1[$ des nombres dont le développement décimal ne comporte que des 0 et des 1, alors X est en bijection avec $\{0, 1\}^{\mathbf{N}}$, et donc n'est pas dénombrable. Il en est a fortiori de même de $\mathbf{R}$, qui contient X.

Exercice 1.5. — Montrer que l'ensemble $\mathscr{P}(\mathbf{N})$ des parties de $\mathbf{N}$ n'est pas dénombrable, mais que l'ensemble des parties finies de $\mathbf{N}$ est dénombrable.

Exercice 1.6. — On rappelle que $x \in \mathbf{C}$ est *algébrique* s'il existe $\mathrm{P} \in \mathbf{Q}[\mathrm{X}]$ non nul tel que $\mathrm{P}(x) = 0$, et que $x \in \mathbf{C}$ est *transcendant* s'il n'est pas algébrique. Montrer que l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est dénombrable. En déduire qu'il existe des nombres transcendants.

Exercice 1.7. — Soit $(\mathrm{B}_j)_{j\in\mathrm{I}}$ une famille de disques ouverts non vides de $\mathbf{C}$. Montrer que si les B_j sont deux à deux disjoints, alors I est dénombrable.

13. Ces résultats, la non dénombrabilité de $\mathbf{R}$ et la dénombrabilité de l'ensemble des nombres algébriques sont le fruit d'un échange de lettres entre G. Cantor et R. Dedekind datant de la fin 1873. Cantor prouvera en 1877 que $[0, 1]$ et $[0, 1] \times [0, 1]$ peuvent être mis en bijection ; comme il l'écrit à Dedekind : « Je le vois, mais je ne le crois pas ».

Exercice 1.8. — Soit $f : \mathbf{R} \to \mathbf{R}$ une fonction croissante.

(i) Montrer que f admet une limite à droite et une limite à gauche en tout point et que, si $x_0 \in \mathbf{R}$, alors $f(x_0^+) = \inf_{x>x_0} f(x)$ et $f(x_0^-) = \sup_{x<x_0} f(x)$; en déduire que $f(x_0^-) \leqslant f(x_0) \leqslant f(x_0^+)$. A quelle condition f est-elle continue en x_0 ?

(ii) Montrer que, si $x_0 < x_1$, alors $f(x_0^+) \leqslant f(x_1^-)$.

(iii) Montrer que l'ensemble D des points où f est discontinue est dénombrable.

Exercice 1.9. — Soient X un sous-ensemble dénombrable de $\mathbf{R}$, dense (i.e. $]a, b[\cap \mathrm{X} \neq \varnothing$, pour tous $a < b$), et $n \mapsto x_n$ une bijection de $\mathbf{N}$ sur X. On définit, par récurrence, une suite $n \mapsto \varphi(n)$, en posant $\varphi(0) = 0$, $\varphi(1) = 1$ et en prenant pour $\varphi(n)$ le plus petit entier $i \geqslant \varphi(n-1)$ tel que x_i soit entre $x_{\varphi(n-1)}$ et $x_{\varphi(n-2)}$. Montrer que la suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ a une limite et que cette limite n'appartient pas à X. En déduire que $\mathbf{R}$ n'est pas dénombrable.

Exercice 1.10. — (difficile) Un « huit » est la réunion de deux cercles dans le plan, de même rayon (non nul), tangents en un point. Montrer que l'on peut mettre dans le plan au plus un nombre dénombrable de huit deux à deux disjoints.

Exercice 1.11. — (difficile) Un « tripode » est la figure formée de trois segments [G, A], [G, B] et [G, C], où A, B, C sont les sommets d'un triangle équilatéral (non réduit à un point) et G est le centre de gravité du triangle. Montrer que l'on peut mettre dans le plan au plus un nombre dénombrable de tripodes deux à deux disjoints.

2. Structures algébriques

Dans ce §, on réunit les définitions concernant les structures algébriques les plus courantes ; les exemples illustratifs utilisent des objets qui sont en général étudiés plus loin dans le texte. Les structures algébriques se sont imposées graduellement aux mathématiciens au cours du XIX$^{\mathrm{e}}$: le terme de « groupe » a été introduit par Galois (1830) dans son étude de la solubilité des équations polynomiales par radicaux, mais il a fallu attendre 1854 pour que Cayley donne une définition axiomatique d'un groupe abstrait (ce que Galois appelle groupe correspond plutôt à une orbite sous l'action d'un groupe fantôme). De même, les calculs dans $\mathbf{R}^2$, $\mathbf{R}^3$ remontent à assez loin, mais il a fallu attendre le développement de l'analyse fonctionnelle dans les années 1930 pour que la définition axiomatique d'espace vectoriel [proposée par Grassmann (1862) et précisée par Peano (1888)] soit universellement adoptée et que l'on remplace avantageusement [14] coordonnées et matrices par vecteurs et applications linéaires. Une des grandes forces des mathématiques réside dans ce processus en deux temps : identification de propriétés communes d'objets a priori très différents (comme les permutations de $\{1, \ldots, n\}$ où les isométries du plan, ou comme l'espace $\mathbf{R}^2$ et celui des fonctions continues sur $[0, 1]$), puis définition, à partir de ces propriétés, d'une catégorie d'objets (les groupes dans le premier cas, les espaces vectoriels dans le second) que l'on peut étudier pour eux-mêmes, ce qui fournit des outils

14. Nous encourageons le lecteur à essayer de résoudre directement l'équation $\mathrm{A}^2 + 1 = 0$ dans $\mathbf{M}_3(\mathbf{R})$ ou même $\mathbf{M}_2(\mathbf{R})$.

pour comprendre à la fois les objets initiaux ayant permis de dégager la notion et d'autres que l'on n'avait pas forcément pensé à mettre sur le même plan jusque-là.

2.1. Lois de composition

Soit X un ensemble. Une *loi de composition* $\heartsuit$ sur X est une règle permettant de fabriquer, à partir de deux éléments quelconques x, y de X, un élément $x\heartsuit y$ de X ; c'est donc une application de $\mathrm{X} \times \mathrm{X}$ dans X. Les exemples ne manquent pas :

◇ Si E est un ensemble, l'ensemble des applications $u : \mathrm{E} \to \mathrm{E}$ est muni de la composition $\circ$.

◇ L'ensemble des propositions logiques est muni des lois $\wedge$ (= et), $\vee$ (= ou) et de l'implication $\Rightarrow$.

◇ L'ensemble $\mathscr{P}(\mathrm{E})$ des parties d'un ensemble E est muni de la réunion $\cup$, l'intersection $\cap$, la différence symétrique $\triangle$ ($\mathrm{A} \triangle \mathrm{B}$ est le complémentaire $(\mathrm{A} \cup \mathrm{B}) - (\mathrm{A} \cap \mathrm{B})$ de $\mathrm{A} \cap \mathrm{B}$ dans $\mathrm{A} \cup \mathrm{B}$).

◇ L'ensemble $\mathbf{Z}$ des entiers relatifs est muni de l'addition $+$, la multiplication $\times$ (ou $\cdot$), la soustraction $-$.

La loi $\heartsuit$ est *commutative* [15] si $x\heartsuit y = y\heartsuit x$, pour tous $x, y \in \mathrm{X}$.

Elle est *associative* [16] si $(x\heartsuit y)\heartsuit z = x\heartsuit(y\heartsuit z)$, pour tous $x, y, z \in \mathrm{X}$. Si la loi est associative, on peut faire les opérations dans l'ordre que l'on veut, ce qui permet de supprimer les parenthèses : on écrira donc souvent $x\heartsuit y\heartsuit z$ au lieu de $(x\heartsuit y)\heartsuit z$ ou $x\heartsuit(y\heartsuit z)$, si la loi $\heartsuit$ est associative.

On dit que $e \in \mathrm{X}$ est un *élément neutre* [17] pour $\heartsuit$, si $e\heartsuit x = x\heartsuit e = x$, pour tout $x \in \mathrm{X}$. Un élément neutre est unique car $e = e\heartsuit e' = e'$ si e et e' sont des éléments neutres.

Si $\heartsuit$ admet un élément neutre, on dit que a est un *inverse à gauche* (resp. *à droite*) de x si $a\heartsuit x = e$ (resp. $x\heartsuit a = e$). Si $\heartsuit$ est associative, on dit que x est *inversible* s'il admet des inverses à droite et à gauche [18] ; ceux-ci sont alors uniquement déterminés et égaux puisque $a = a\heartsuit e = a\heartsuit(x\heartsuit b) = (a\heartsuit x)\heartsuit b = e\heartsuit b = b$, si a et b sont des inverses à gauche et à droite de x.

Si $\heartsuit$ et $\spadesuit$ sont deux lois de composition sur X, on dit que $\spadesuit$ est *distributive* par rapport [19] à $\heartsuit$, si $(a\heartsuit b)\spadesuit x = (a\spadesuit x)\heartsuit(b\spadesuit x)$ et $x\spadesuit(a\heartsuit b) = (x\spadesuit a)\heartsuit(x\spadesuit b)$, pour tous $a, b, x \in \mathrm{X}$.

---

15. C'est le cas de toutes les lois ci-dessus à l'exception de la composition $\circ$, de $\Rightarrow$ sur l'ensemble des propositions logiques et de $-$ sur $\mathbf{Z}$.

16. C'est le cas de toutes les lois ci-dessus à l'exception de $\Rightarrow$ et de $-$.

17. Les lois $\circ$, $\cup$, $\cap$, $\triangle$, $+$ et $\times$ possèdent des éléments neutres, à savoir id, $\varnothing$, E, $\varnothing$, 0 et 1.

18. Dans le cas de la loi $\circ$, une application $u : \mathrm{E} \to \mathrm{E}$ admet un inverse à gauche si et seulement si elle est injective ; elle admet un inverse à droite si et seulement si elle est surjective (cela demande l'axiome du choix dans le cas où E est l'infini), et elle est inversible si et seulement si elle est bijective ; pour la loi $\triangle$, tout élément est son propre inverse ; dans $\mathbf{Z}$, tout élément n admet un inverse $-n$ pour la loi $+$, mais seuls 1 et -1 admettent un inverse pour la loi $\times$.

19. Dans les exemples ci-dessus, $\wedge$ est distributive par rapport à $\vee$, et $\vee$ l'est par rapport à $\wedge$; $\cup$ est distributive par rapport à $\cap$ et $\triangle$, et $\cap$ l'est par rapport à $\cup$; $\times$ est distributive par rapport à $+$ et $-$.

2.2. Exemples de structures algébriques

2.2.1. *Groupes.* — Un groupe G est un ensemble non vide, muni d'une loi $(g, h) \to gh$, associative, possèdant un élément neutre e, et telle que tout élément g soit inversible (on note g^{-1} l'inverse de g).

Si la loi est commutative, on dit que G est *commutatif* ou *abélien*. La loi de groupe d'un groupe commutatif est souvent notée $+$, auquel cas l'élément neutre est noté 0 et l'inverse de $x \in \mathrm{G}$ est noté $-x$ et appelé *l'opposé* de x. Une loi notée $+$ ou $\oplus$ ou $\boxplus$ est implicitement commutative, à moins que l'auteur n'ait vraiment décidé de rendre son texte illisible.

Si la loi de groupe est notée multiplicativement, l'élément neutre de G est en général noté 1 au lieu de e ; s'il s'agit d'un groupe de bijections d'un ensemble X, l'élément neutre est l'identité de X, et est souvent noté id.

Comme groupes, citons le groupe $\boldsymbol{\mu}_{\mathrm{D}}$ des racines D-ièmes de l'unité dans $\mathbf{C}$ (alinéa 3.1.1), le groupe symétrique S_n et son sous-groupe A_n (n° 3.4), le groupe $\mathbf{GL}_n(\mathrm{A})$ des matrices $n \times n$ inversibles à coefficients dans un anneau A et son sous-groupe $\mathbf{SL}_n(\mathrm{A})$ des matrices de déterminant 1 (n° 7.7), le groupe des points rationnels sur une courbe elliptique (prob. H.8 et annexe F). Notons aussi qu'un anneau (cf. ci-après) est un groupe pour l'addition, et que l'ensemble de ses éléments inversibles (non nuls) est un groupe pour la multiplication (par exemple $(\mathbf{R}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}^*, \times)$, $(\mathbf{Q}^*, \times)$ sont des groupes).

2.2.2. *Anneaux.* — Un *anneau* A est un ensemble non vide muni d'une loi d'addition $+$ qui fait de A un groupe commutatif (d'élément neutre 0) et d'une loi de multiplication $\times$ ou $\cdot$, associative, possédant un élément neutre 1, et distributive par rapport à l'addition. On dit que A est *commutatif* si la multiplication est commutative. On dit que A est *intègre* si $\mathrm{A} \neq \{0\}$ et si $xy = 0 \Rightarrow x = 0$ ou $y = 0$; on dit que $x \in \mathrm{A}$ est un *diviseur de* 0 s'il existe $y \neq 0$ tel que $xy = 0$; un anneau A est donc intègre si et seulement si $\mathrm{A} \neq \{0\}$ et le seul diviseur de 0 est 0.

Comme anneaux commutatifs, citons l'anneau $\mathbf{Z}$ des entiers relatifs, l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ des entiers modulo D (n° 2.8), l'anneau $\mathbf{Z}_p$ des entiers p-adiques, l'anneau $\mathrm{A}[\mathrm{X}]$ des polynômes en la variable X à coefficients dans un anneau commutatif A (n° 4.1), l'anneau $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ des polynômes en n variables (alinéa 4.3.1), l'anneau $\mathrm{K}[[\mathrm{T}]]$ des séries formelles à coefficients dans un corps commutatif K (n° 1 du § V.1) ; comme anneau non commutatif, nous aurons surtout affaire à l'anneau $\mathbf{M}_n(\mathrm{A})$ des matrices $n \times n$ à coefficients dans un anneau commutatif A (n° 7.7).

• Si A est un anneau, l'ensemble A^* des éléments inversibles [20] non nuls de A est un groupe pour la multiplication s'il est non vide [21].

> Il s'agit de prouver que le produit de deux éléments inversibles est encore inversible, mais on a $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$ et $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = 1$, ce qui prouve que xy est inversible d'inverse $y^{-1}x^{-1}$ si x et y le sont.

• Si A est un anneau, on a $0 \cdot x = x \cdot 0 = 0$, pour tout $x \in \mathrm{A}$, et $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$ pour tous $x, y \in \mathrm{A}$.

---

20. Pour la multiplication ; l'inversibilité pour l'addition est incluse dans la définition d'un anneau.

21. Si $\mathrm{A} = \{0\}$, alors $0 = 1$ et 0 est inversible, mais A^* n'est pas un groupe car il est vide ; on remarquera que l'inversibilité de 0 pour la multiplication implique $\mathrm{A} = \{0\}$ d'après le point suivant.

$y \cdot x = (0+y)\cdot x = (0\cdot x)+(y\cdot x)$, et donc $0 = 0\cdot x$, comme on le voit en ajoutant $-(y\cdot x)$ des deux côtés ; de même $x\cdot y = x\cdot(y+0) = (x\cdot y)+(x\cdot 0)$, et donc $0 = x\cdot 0$. De même $x\cdot(-y)+x\cdot y = x\cdot(-y+y) = x\cdot 0 = 0$, et donc $x\cdot(-y) = -(x\cdot y)$, et $(-x)\cdot y + x\cdot y = (-x+x)\cdot y = 0\cdot y = 0$, et donc $(-x)\cdot y = -(x\cdot y)$.

2.2.3. *Corps.* — Un *corps* K est un anneau dans lequel tout élément non nul est inversible (on note x^{-1} ou $\frac{1}{x}$ l'inverse de $x \neq 0$), et $\mathrm{K}^* = \mathrm{K} - \{0\}$ est non vide [22] (c'est donc un groupe). Un tel corps est dit *commutatif* si la multiplication est commutative.

Comme corps, citons le corps $\mathbf{Q}$ des nombres rationnels (n° 20.2), le corps $\mathbf{R}$ des nombres réels (n° 20.3), le corps $\mathbf{C}$ des nombres complexes, le corps $\mathbf{Q}_p$ des nombres p-adiques (n° 20.4), le corps K(X) des fractions rationnelles à coefficients dans un corps K (alinéa 4.2.3), ou encore le corps $\mathbf{F}_q$ à q éléments, si q est une puissance d'un nombre premier (n° 8.7).

• Si A est un anneau commutatif intègre, on construit son *corps des fractions* Fr(A) comme l'ensemble des classes d'équivalence de couples $(a,b) \in \mathrm{A}\times(\mathrm{A}-\{0\})$ pour la relation [23] $(a,b)\sim(a',b')$ si et seulement si $ab'-a'b=0$, muni des lois $+$ et $\cdot$ définies par $(a,b)+(a',b') = (ab'+a'b, bb')$ et $(a,b)\cdot(a',b') = (aa',bb')$. La classe de (a,b) est notée $\frac{a}{b}$, celle de $(a,1)$ est simplement notée a, ce qui permet de considérer A comme un sous-ensemble de Fr(A), et on a $\frac{a}{b} = b^{-1}a$ dans Fr(A). Les lois d'addition et de multiplication prennent alors les formes plus habituelles $\frac{a}{b}+\frac{a'}{b'} = \frac{ab'+a'b}{bb'}$ et $\frac{a}{b}\,\frac{a'}{b'} = \frac{aa'}{bb'}$.

Par exemple, on a $\mathrm{Fr}(\mathbf{Z}) = \mathbf{Q}$, $\mathrm{Fr}(\mathrm{K}[\mathrm{X}]) = \mathrm{K}(\mathrm{X})$ et, plus généralement, le corps des fractions de $\mathrm{K}[\mathrm{X}_1,\dots,\mathrm{X}_n]$ est le corps $\mathrm{K}(\mathrm{X}_1,\dots,\mathrm{X}_n)$ des fractions rationnelles en n variables.

2.2.4. *Modules et espaces vectoriels.* — Si A est un anneau, un A-*module* M (ou un *module sur* A) est un groupe commutatif pour une loi $+$ (d'élément neutre 0), muni d'une action $(a,x)\mapsto ax$ de A, vérifiant :

$$1\,x = x, \quad a(x+y) = ax+ay, \quad (a+b)x = ax+bx, \quad (ab)x = a(bx),$$

quels que soient $x,y \in \mathrm{M}$ et $a,b \in \mathrm{A}$. On a alors $0x = 0$, $a0 = 0$ et $(-a)x = -(ax) = a(-x)$, si $a \in \mathrm{A}$ et $x \in \mathrm{M}$ pour les mêmes raisons que ci-dessus.

Si K est un corps commutatif, un K-module est en général appelé un K-*espace vectoriel* ou un *espace vectoriel sur* K.

L'analyse fournit une pléthore d'espaces vectoriels sur $\mathbf{R}$ ou $\mathbf{C}$, par exemple les espaces de fonctions $\mathscr{C}(\mathbf{R}^m)$, $\mathscr{C}^\infty(\mathbf{R}^m)$, $\mathscr{S}(\mathbf{R}^m)$, $\mathrm{L}^1(\mathbf{R}^m)$, continues, $\mathscr{C}^\infty$, de Schwartz (§ IV.3, n° 3), sommables (§ III.2, n° 1) sont des $\mathbf{C}$-espaces vectoriels. Il est souvent profitable de considérer un K-espace vectoriel de dimension fini muni d'un endomorphisme u comme un K[X]-module (n° 10.2).

• Une différence fondamentale entre les espaces vectoriels et les modules sur un anneau qui n'est pas un corps est que $\lambda x = 0$ et $\lambda \neq 0$ impliquent $x = 0$ dans un espace vectoriel (car $x = \lambda^{-1}\lambda x = \lambda^{-1}0 = 0$), mais pas dans un module sur un anneau qui n'est pas un corps (par exemple, on a $2\cdot 3 = 0$ dans le $\mathbf{Z}$-module $\mathbf{Z}/6\mathbf{Z}$ sans que 3 soit nul dans $\mathbf{Z}/6\mathbf{Z}$).

22. On impose donc $1 \neq 0$ dans un corps ; l'anneau $\{0\}$ n'est pas un corps.

23. Cf. n° 2.7. La transitivité résulte de la relation $b'(ab''-a''b) = b''(ab'-a'b) - b(a''b'-a'b'')$ qui implique, car A est intègre et $b' \neq 0$, que $ab''-a''b = 0$ si $ab'-a'b = a''b'-a'b'' = 0$.

• Tout groupe commutatif (et donc tout anneau, tout corps, tout module sur un anneau, etc.) est naturellement un **Z**-module, en définissant nx par récurrence sur n, par $0x = 0$, $(n+1)x = nx + x$ si $n \in \mathbf{N}$, et $nx = -((-n)x)$, si $n \leqslant 0$.

Montrer que ceci définit bien une action de **Z** est un exercice fastidieux qui n'est pas sans rappeler la démonstration du fait que **Z** est un anneau en partant des axiomes de Peano.

2.2.5. *Algèbres.* — Si A est un anneau commutatif, une A-*algèbre* Λ est un A-module muni d'une multiplication notée $\cdot$, associative, distributive par rapport à l'addition, et qui vérifie $a\,(x\cdot y) = (a\,x)\cdot y = x\cdot(a\,y)$, pour tous $a \in \mathrm{A}$ et $x, y \in \Lambda$ (i.e. l'action de A commute à la multiplication). Une algèbre est *commutative* si la multiplication est commutative, *unitaire* si elle possède un élément neutre pour la multiplication (c'est alors un anneau).

• Tout anneau est naturellement une **Z**-algèbre ; toute A-algèbre est une **Z**-algèbre, si A est un anneau commutatif.

Il s'agit de vérifier que la structure de **Z**-module définie ci-dessus satisfaît les relations $n\,(xy) = (nx)\,y = x\,(ny)$, ce qui se démontre par une récurrence sans mystère pour $n \geqslant 0$, et par passage à l'opposé pour $n \leqslant 0$.

Si Λ est une **Z**-algèbre, et si $x \in \Lambda$, on définit x^n, pour $n \geqslant 1$, par $x^1 = x$ et $x^{n+1} = x^n x$, si $n \geqslant 1$, et on vérifie, par récurrence sur m, que $x^{n+m} = x^n x^m$, si $n, m \in \mathbf{N}$. Si Λ est unitaire, on pose $x^0 = 1$ pour tout $x \in \Lambda$ (y compris $x = 0$), et si x est inversible dans Λ, on pose $x^n = (x^{-1})^{-n}$, si $n \leqslant 0$; on vérifie que $x^{n+m} = x^n x^m$ pour tous $n, m \in \mathbf{Z}$, et donc que $n \mapsto x^n$ est un morphisme de groupes de **Z** dans A^*.

• Si $a, b \in \Lambda$ commutent, alors :
◇ $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$, si n est un entier $\geqslant 2$,
◇ $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots \binom{n}{n}b^n$, si n est un entier $\geqslant 1$ (*formule du binôme* qui peut se condenser en $(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i$, pour $n \in \mathbf{N}$, si Λ est unitaire).

La première formule se démontre en développant le membre de droite, la seconde se prouve par récurrence : elle est immédiate si $n = 1$, et on passe de n à $n+1$ en utilisant l'identité $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$, et en traitant directement les termes a^{n+1} et b^{n+1}.

Si Λ est une **Z**-algèbre, on dit que $x \in \mathrm{A}$ est *nilpotent* s'il existe $m \in \mathbf{N}$ tel que $x^m = 0$, et si Λ est unitaire, on dit que x est *unipotent* si $x - 1$ est nilpotent.

• Si $x \in \Lambda$ est unipotent, alors x est inversible et $x^n = \sum_{k\in\mathbf{N}}\binom{n}{k}(x-1)^k$, pour tout $n \in \mathbf{Z}$, où la somme dans le membre de droite est finie car $(x-1)^k = 0$ si k est assez grand ; en particulier, si Λ est une **Q**-algèbre, x^n est un polynôme en n .

Il suffit de vérifier que $(1 + (x-1))\big(\sum_{k=0}^{m-1}\binom{n}{k}(x-1)^k\big) = \sum_{k=0}^{m-1}\binom{n+1}{k}(x-1)^k$, si $n \in \mathbf{N}$, et si $m \in \mathbf{N}$ est tel que $(x-1)^m = 0$. En effet, une récurrence montante (la même que ci-dessus) permet d'établir la formule pour $n \in \mathbf{N}$, et pour $n = -1$ la formule prouve que x est inversible (son inverse étant $1 + (1-x) + \cdots (1-x)^{m-1}$ puisque $\binom{-1}{k} = (-1)^k$) et une récurrence descendante permet d'en déduire la formule pour $n \leqslant 0$. Comme $(x-1)^m = 0$, le membre de gauche se réécrit sous la forme $1 + \sum_{k=1}^{m-1}\big(\binom{n}{k} + \binom{n}{k-1}\big)(x-1)^k$, et la formule est donc une conséquence de l'identité $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ entre nombres binomiaux.

Exercice 2.1. — Soit A un anneau.

(i) Montrer que $x+y$ est nilpotent si x et y commutent et sont nilpotents ; le résultat est-il encore vrai si x et y ne commutent pas ?

(ii) Montrer que ax est nilpotent si x l'est et si a et x commutent ; le résultat est-il encore vrai si a et y ne commutent pas ?

(iii) On suppose A commutatif. Montrer que l'ensemble des éléments nilpotents est un idéal de A.

2.3. Sous-trucs de trucs

Un sous-truc d'un truc est un sous-ensemble non vide stable par les lois définissant la structure de truc. Dans les cas considérés plus haut, cela se traduit de la manière suivante.

Si G est un groupe, un *sous-groupe* H de G est un sous-ensemble de G contenant l'élément neutre, stable par la loi de groupe (i.e. $xy \in \mathrm{H}$, si $x, y \in \mathrm{H}$) et par passage à l'inverse ($x^{-1} \in \mathrm{H}$ si $x \in \mathrm{H}$) ; il suffit pour cela que $\mathrm{H} \neq \varnothing$ et que $xy^{-1} \in \mathrm{H}$ si $x, y \in \mathrm{H}$.

Si A est un anneau, un *sous-anneau* A' de A est un sous-groupe de A pour l'addition, qui contient 1 et qui est stable par multiplication (i.e. $x \cdot y \in \mathrm{A}'$, si $x, y \in \mathrm{A}'$).

Si K est un corps, un *sous-corps* K' de K est un sous-anneau de K stable par passage à l'inverse (i.e. $x^{-1} \in \mathrm{K}'$ si $x \in \mathrm{K}' - \{0\}$).

Si M est un A-module, un *sous*-A-*module* M' de M est un sous-groupe de M pour l'addition qui est stable pour l'action de A (i.e. $a\,x \in \mathrm{M}'$ si $a \in \mathrm{A}$ et $x \in \mathrm{M}'$). Un sous-A-module de A est appelé un *idéal* de A.

Si V est un K-espace vectoriel, un *sous-espace* de V est un sous-K-module de V.

Si Λ est une A-algèbre, une *sous*-A-*algèbre* de Λ est un sous-A-module de Λ stable par multiplication.

Exercice 2.2. — (Quaternions de Hamilton, 1843) Soit $\mathbf{H} = \left\{ \left(\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix} \right),\ a, b \in \mathbf{C} \right\}$

(i) Montrer que $\mathbf{H}$ est un sous-anneau de $\mathbf{M}_2(\mathbf{C})$, puis que c'est un corps non commutatif.

(ii) Résoudre l'équation $x^2 + 1 = 0$ dans $\mathbf{H}$; le résultat est-il surprenant ?

Dans tous les cas ci-dessus, un sous-truc d'un truc est encore un truc (i.e. un sous-groupe d'un groupe est un groupe, un sous-anneau d'un anneau est un anneau, etc.) avec les lois et actions héritées de celles du truc initial.

• L'intersection d'une famille quelconque de sous-trucs est un sous-truc ; on définit le sous-truc *engendré* par un sous-ensemble X d'un truc T comme l'intersection de tous les sous-trucs de T contenant X ; c'est aussi le plus petit sous-truc de T contenant X.

Montrons par exemple (les autres démonstrations sont exactement du même type) que $\mathrm{H} = \cap_{i \in \mathrm{I}} \mathrm{G}_i$ est un sous-groupe de G, si les G_i sont des sous-groupes d'un groupe G.

◇ L'élément neutre e de G appartient à tous les G_i, et donc $e \in \cap_{i \in \mathrm{I}} \mathrm{G}_i$ et $\mathrm{H} \neq \varnothing$.

◇ Si $x \in \mathrm{H}$, alors $x \in \mathrm{G}_i$, pour tout i, et donc $x^{-1} \in \mathrm{G}_i$ pour tout i puisque G_i est un sous-groupe de G, et donc $x^{-1} \in \mathrm{H}$.

◇ Si $x, y \in \mathrm{H}$, alors $x, y \in \mathrm{G}_i$, pour tout i, et donc $xy \in \mathrm{G}_i$ pour tout i puisque G_i est un sous-groupe de G, et donc $xy \in \mathrm{H}$.

Ceci prouve que $\cap_{i \in \mathrm{I}} \mathrm{G}_i$ est un sous-groupe de G.

2.4. Morphismes

Un morphisme entre des trucs est une application qui commute aux lois définissant la structure de trucs. Dans les cas qui nous intéressent, cela se traduit de la manière suivante.

Si $\mathrm{G}_1, \mathrm{G}_2$ sont des groupes, un *morphisme de groupes* $\varphi : \mathrm{G}_1 \to \mathrm{G}_2$ est une application qui commute aux lois de groupe (i.e. $\varphi(xy) = \varphi(x)\varphi(y)$, pour tous $x, y \in \mathrm{G}_1$).

• Si $\varphi : \mathrm{G}_1 \to \mathrm{G}_2$ est un morphisme de groupes et si e_i est l'élément neutre de G_i, pour $i = 1, 2$, alors $\varphi(e_1) = e_2$; si $x \in \mathrm{G}_1$, alors $\varphi(x^{-1}) = \varphi(x)^{-1}$.

On a $e_1e_1 = e_1$, et donc $\varphi(e_1)\varphi(e_1) = \varphi(e_1)$. En multipliant les deux membres à droite par $\varphi(e_1)^{-1}$, on obtient $\varphi(e_1) = e_2$. Maintenant, $\varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, et comme $xx^{-1} = e_1$ et $\varphi(e_1) = e_2$, cela nous donne $\varphi(x)\varphi(x^{-1}) = e_2$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Si $\mathrm{A}_1, \mathrm{A}_2$ sont des anneaux, un *morphisme d'anneaux* $\varphi : \mathrm{A}_1 \to \mathrm{A}_2$ est une application qui commute aux additions et multiplications (i.e. $\varphi(x + y) = \varphi(x) + \varphi(y)$ et $\varphi(xy) = \varphi(x)\varphi(y)$, pour tous $x, y \in \mathrm{A}_1$), et qui vérifie $\varphi(1) = 1$; c'est en particulier, un morphisme du groupe $(\mathrm{A}_1, +)$ dans le groupe $(\mathrm{A}_2, +)$, et sa restriction à A_1^* est un morphisme de groupes (multiplicatifs) de A_1^* dans A_2^*.

• Si $\varphi : \mathrm{A}_1 \to \mathrm{A}_2$ est un morphisme d'anneaux, on dispose d'une action de A_1 sur A_2, à savoir celle définie par $a \cdot x = \varphi(a)x$, et donc A_2 peut être considéré comme une A_1-algèbre. Réciproquement, si A_2 est une A_1-algèbre unitaire, alors $a \mapsto a \cdot 1$ est un morphisme d'anneaux de A_1 dans A_2 ; en particulier, si A est un anneau, il existe un unique morphisme d'anneaux de $\mathbf{Z}$ dans A à savoir le morphisme envoyant $n \in \mathbf{Z}$ sur $n \cdot 1$ (que l'on note encore $n \in \mathrm{A}$).

Si $\mathrm{K}_1, \mathrm{K}_2$ sont des corps, un *morphisme de corps* $\varphi : \mathrm{K}_1 \to \mathrm{K}_2$ est juste un morphisme d'anneaux (mais il induit en prime un morphisme de groupes de K_1^* dans K_2^*).

Si $\mathrm{M}_1, \mathrm{M}_2$ sont des A-modules, un *morphisme de* A*-modules* $\varphi : \mathrm{M}_1 \to \mathrm{M}_2$ est une application qui commute aux additions et qui est A*-linéaire*, ce qui signifie qu'elle commute à l'action de A (i.e $\varphi(a\,x) = a\,\varphi(x)$, pour tous $a \in \mathrm{A}$ et $x \in \mathrm{M}_1$) ; c'est en particulier, un morphisme du groupe $(\mathrm{M}_1, +)$ dans le groupe $(\mathrm{M}_2, +)$. Dans le cas particulier où A est un corps commutatif, on parlera de *morphisme d'espaces vectoriels* ou d'*application linéaire*.

Si Λ_1, Λ_2 sont des A-algèbres, un *morphisme de* A*-algèbres* $\varphi : \Lambda_1 \to \Lambda_2$ est un morphisme de A-modules qui commute aux multiplications.

• Si $\mathrm{T}_1, \mathrm{T}_2, \mathrm{T}_3$ sont des trucs, et si $\varphi_1 : \mathrm{T}_1 \to \mathrm{T}_2$ et $\varphi_2 : \mathrm{T}_2 \to \mathrm{T}_3$ sont des morphismes de trucs, alors $\varphi_2 \circ \varphi_1 : \mathrm{T}_1 \to \mathrm{T}_3$ est un morphisme de trucs.

Montrons, par exemple (les autres démonstrations sont exactement du même type), que le composé de deux morphismes de groupes est encore un morphisme de groupes. Si $x, y \in \mathrm{T}_1$, alors $\varphi_2 \circ \varphi_1(xy) = \varphi_2(\varphi_1(xy)) = \varphi_2(\varphi_1(x)\varphi_1(y)) = \varphi_2(\varphi_1(x))\varphi_2(\varphi_1(y)) = \varphi_2 \circ \varphi_1(x)\varphi_2 \circ \varphi_1(y)$. (On a utilisé successivement la définition de $\circ$, le fait que φ_1 est un morphisme de groupes, le fait que φ_2 est un morphisme de groupes, et la définition de $\circ$.)

Un morphisme de trucs qui est en plus bijectif est appelé un *isomorphisme* de trucs.

• Si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un isomorphisme de trucs, alors $\varphi^{-1} : \mathrm{T}_2 \to \mathrm{T}_1$ est un isomorphisme de trucs.

Considérons par exemple le cas d'un isomorphisme $\varphi : \mathrm{A}_1 \to \mathrm{A}_2$ d'anneaux.

◇ $\varphi(\varphi^{-1}(x+y)-\varphi^{-1}(x)-\varphi^{-1}(y)) = \varphi(\varphi^{-1}(x+y))-\varphi(\varphi^{-1}(x))-\varphi(\varphi^{-1}(y))$ car φ est un morphisme d'anneaux. Par ailleurs $\varphi(\varphi^{-1}(z)) = z$ pour tout $z \in \mathrm{A}_2$, par définition de φ^{-1}. On obtient donc $\varphi(\varphi^{-1}(x+y)-\varphi^{-1}(x)-\varphi^{-1}(y)) = x+y-x-y = 0$, et comme φ est injectif, cela implique $\varphi^{-1}(x+y)-\varphi^{-1}(x)-\varphi^{-1}(y) = 0$. Autrement dit, φ^{-1} est un morphisme de groupes de $(\mathrm{A}_2, +)$ dans $(\mathrm{A}_1, +)$.

◇ $\varphi(\varphi^{-1}(xy)-\varphi^{-1}(x)\varphi^{-1}(y)) = \varphi(\varphi^{-1}(xy))-\varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y))$ car φ est un morphisme d'anneaux. Il s'ensuit que $\varphi(\varphi^{-1}(xy)-\varphi^{-1}(x)\varphi^{-1}(y)) = xy-xy = 0$, et comme φ est injectif, cela implique $\varphi^{-1}(xy)-\varphi^{-1}(x)\varphi^{-1}(y) = 0$. Autrement dit, φ^{-1} commute aux multiplications.

◇ $\varphi(1) = 1$ et donc $\varphi^{-1}(1) = 1$.

Ce qui précède prouve que φ^{-1} est un morphisme d'anneaux, et comme il est bijectif, c'est un isomorphisme d'anneaux.

On dit que des trucs T_1, T_2 sont *isomorphes*, ce qui s'écrit $\mathrm{T}_1 \cong \mathrm{T}_2$, s'il existe un isomorphisme de trucs $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$. On fera attention au fait que cela dépend de la structure considérée sur T_1 et T_2.

Par exemple, les anneaux $\mathbf{R} \times \mathbf{R}$ et $\mathbf{C}$ ne sont pas isomorphes ($\mathbf{R} \times \mathbf{R}$ n'est pas intègre puisque $(1,0)\cdot(0,1) = (0,0)$), par contre $\mathbf{R} \times \mathbf{R}$ et $\mathbf{C}$ sont isomorphes en tant que groupes additifs, ou que $\mathbf{R}$-espaces vectoriels (on peut prendre le même isomorphisme dans les deux cas, à savoir $(x,y) \mapsto x+iy$).

Si T est un truc, un isomorphisme de trucs $\varphi : \mathrm{T} \to \mathrm{T}$, s'appelle un *automorphisme* de T ; l'ensemble $\mathrm{Aut}(\mathrm{T})$ des automorphismes de T est un groupe pour la composition d'après les deux points précédents. On fera attention que $\mathrm{Aut}(\mathrm{T})$ dépend de la structure mise sur T.

Par exemple, le groupe $\mathrm{Aut}(\mathbf{C})$ des automorphismes du corps $\mathbf{C}$ (i.e. les bijections σ de $\mathbf{C}$ vérifiant $\sigma(1) = 1$, et $\sigma(x+y) = \sigma(x)+\sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$ pour tous $x, y \in \mathbf{C}$) est un groupe gigantesque [24] que l'on aimerait bien arriver à comprendre ; le groupe des automorphismes de $\mathbf{C}$, vu comme un $\mathbf{R}$-espace vectoriel, est isomorphe au groupe $\mathbf{GL}_2(\mathbf{R})$ des matrices 2×2 inversibles, à coefficients dans $\mathbf{R}$.

2.5. Noyau et image

• Si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un morphisme de trucs, l'*image* $\mathrm{Im}\,\varphi = \{y \in \mathrm{T}_2,\ \exists x \in \mathrm{T}_1,\ y = \varphi(x)\}$ de φ est un sous-truc de T_2, et φ est surjectif si et seulement si $\mathrm{Im}\,\varphi = \mathrm{T}_2$.

Que φ soit surjective si et seulement si $\mathrm{Im}\,\varphi = \mathrm{T}_2$ est une simple traduction. Maintenant, montrons, par exemple (les autres démonstrations sont exactement du même type), que l'image d'un morphisme d'anneaux $\varphi : \mathrm{A}_1 \to \mathrm{A}_2$ est un sous-anneau de A_2.

◇ On a $\varphi(1) = 1$ par hypothèse, et donc $1 \in \mathrm{Im}\,\varphi$.

◇ Si $y_1, y_2 \in \mathrm{Im}\,\varphi$, il existe $x_1, x_2 \in \mathrm{A}_1$ tels que $y_1 = \varphi(x_1)$ et $y_2 = \varphi(x_2)$. Mais alors $y_1+y_2 = \varphi(x_1+x_2)$ et $y_1y_2 = \varphi(x_1x_2)$ appartiennent à $\mathrm{Im}\,\varphi$, qui est donc stable par addition et multiplication.

24. Du moins si on accepte l'axiome du choix ; dans le cas contraire, ce groupe peut fort bien ne comporter que deux éléments : l'identité et la conjugaison complexe.

◇ Si $y \in \operatorname{Im}\varphi$, il existe $x \in \mathrm{A}_1$ tel que $y = \varphi(x)$. Mais alors $-y = \varphi(-x)$ appartient à $\operatorname{Im}\varphi$ qui est donc stable par passage à l'opposé.

Il s'ensuit que $\operatorname{Im}\varphi$ est un sous-groupe de A_2 pour l'addition, contient 1 et est stable par multiplication ; c'est donc un sous-anneau de A_2.

• Si $\varphi : \mathrm{G}_1 \to \mathrm{G}_2$ est un morphisme de groupes, on note $\operatorname{Ker}\varphi = \{x \in \mathrm{G}_1,\ \varphi(x) = 1\}$ le *noyau* de φ. Alors $\operatorname{Ker}\varphi$ est un sous-groupe de G_1 et φ est injectif si et seulement si $\operatorname{Ker}\varphi = \{1\}$ (on dit que *le noyau est trivial*, si $\operatorname{Ker}\varphi = \{1\}$).

◇ $\varphi(1) = 1$, et $1 \in \operatorname{Ker}\varphi$ qui est donc non vide.

◇ Si $x, y \in \operatorname{Ker}\varphi$, on a $\varphi(xy) = \varphi(x)\varphi(y) = 1$, et donc $xy \in \operatorname{Ker}\varphi$.

◇ Enfin, si $x \in \operatorname{Ker}\varphi$, on a $\varphi(x^{-1}) = \varphi(x)^{-1} = 1$.

Ceci prouve que $\operatorname{Ker}\varphi$ est un sous-groupe de G_1. Maintenant, si φ est injectif, $\operatorname{Ker}\varphi$ a au plus un élément puisque c'est l'image inverse de $1 \in \mathrm{G}_2$, et comme il contient l'élément neutre de G_1, on a $\operatorname{Ker}\varphi = \{1\}$. Réciproquement, supposons $\operatorname{Ker}\varphi = \{1\}$. Si $\varphi(x) = \varphi(y)$, alors $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1$, et donc $xy^{-1} \in \operatorname{Ker}\varphi$. Comme on a supposé $\operatorname{Ker}\varphi = \{1\}$, on en déduit $xy^{-1} = 1$, et donc $x = y$. L'injectivité de φ s'en déduit.

• Plus généralement, le noyau d'un morphisme de trucs $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est le noyau de φ vu comme morphisme de groupes [25] en oubliant les structures additionnelles sur T_1 et T_2 ; un tel morphisme est donc injectif si et seulement si le noyau est trivial.

• Si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un morphisme d'anneaux, son noyau est un idéal de A ; si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un morphisme de corps, alors $\operatorname{Ker}\varphi = \{0\}$, et donc un morphisme de corps est injectif ; si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un morphisme de A-modules, de K-espaces vectoriels ou de A-algèbres, son noyau est un sous-truc de T_1.

Montrons, par exemple (les autres démonstrations sont du même type), que le noyau d'un morphisme d'anneaux $\varphi : \mathrm{A}_1 \to \mathrm{A}_2$ est un idéal de A_1 (i.e. un sous-A_1-module de A_1).

◇ Comme φ est un morphisme de groupes additifs, on a $\varphi(0) = 0$, et donc $\operatorname{Ker}\varphi$ est non vide puisqu'il contient 0.

◇ Si $x, y \in \operatorname{Ker}\varphi$, on a $\varphi(x - y) = \varphi(x) - \varphi(y) = 0 - 0$, et donc $x - y \in \operatorname{Ker}\varphi$. (Ceci prouve déjà que $\operatorname{Ker}\varphi$ est un sous-groupe additif de A_1.)

◇ Si $a \in \mathrm{A}_1$ et si $x \in \operatorname{Ker}\varphi$, alors $\varphi(ax) = \varphi(a)\varphi(0) = \varphi(a) \cdot 0 = 0$, ce qui prouve que $\operatorname{Ker}\varphi$ est stable par multiplication par un élément de A_1, et donc est un sous-A_1-module de A_1, ce que l'on cherchait à établir.

Enfin, si φ est un morphisme de corps, et si $\operatorname{Ker}\varphi$ contient un élément x non nul, alors il contient $1 = xx^{-1}$ d'après ce qui précède, et comme on a $\varphi(1) = 1$ par hypothèse, on obtient $1 = 0$ dans T_2 ce qui est en contradiction avec l'hypothèse que T_2 est un corps.

• Si $\varphi : \mathrm{T}_1 \to \mathrm{T}_2$ est un morphisme de trucs, et si T est un sous-truc de T_2, alors $\varphi^{-1}(\mathrm{T}_2)$ est un sous-truc de T_1.

C'est une démonstration du même type que celle prouvant que le noyau est un sous-truc. La seule différence est que le résultat est aussi valable dans le cas des anneaux car $\mathrm{T} \ni 1$ et donc $\varphi^{-1}(\mathrm{T}) \ni 1$, et dans le cas des corps.

25. Tous les trucs autres que les groupes sont en particulier des groupes pour la loi $+$, ce qui fait que $\operatorname{Ker}\varphi = \{x \in \mathrm{T}_1,\ \varphi(x) = 0\}$ dans le cas d'un morphisme de trucs plus riches que des groupes.

• Si A est un anneau commutatif intègre, tout corps K contenant A contient aussi Fr(A) : si ι est un morphisme d'anneaux injectif de A dans K, il existe un unique morphisme de corps (automatiquement injectif) de Fr(A) dans K dont la restriction à A est ι.

On doit avoir $\iota(\frac{a}{b}) = \frac{\iota(a)}{\iota(b)}$, et on vérifie que ceci définit bien un morphisme de corps.

2.6. Produits et sommes

2.6.1. *Produits de trucs*

Si $(\mathrm{T}_i)_{i\in\mathrm{I}}$ est une famille de trucs, on munit le produit $\prod_{i\in\mathrm{I}} \mathrm{T}_i$ des lois et actions définies composante par composante [i.e. en posant $(x_i)_{i\in\mathrm{I}}(y_i)_{i\in\mathrm{I}} = (x_iy_i)_{i\in\mathrm{I}}$ dans le cas d'une loi multiplicative, $(x_i)_{i\in\mathrm{I}} + (y_i)_{i\in\mathrm{I}} = (x_i + y_i)_{i\in\mathrm{I}}$ dans le cas d'une loi additive, et $a \cdot (x_i)_{i\in\mathrm{I}} = (a \cdot x_i)_{i\in\mathrm{I}}$ pour une action extérieure (dans le cas d'un A-module ou d'une A-algèbre)]. Les éléments neutres et inverses s'obtiennent alors aussi composante par composante (i.e. si y_i est l'inverse de x_i pour tout i pour une loi de T_i, alors $(y_i)_{i\in\mathrm{I}}$ est l'inverse de $(x_i)_{i\in\mathrm{I}}$ pour la loi produit).

• Un produit de trucs est encore un truc dans le cas des groupes, des anneaux, des A-modules, des K-espaces vectoriels, ou des A-algèbres ; par contre, un produit de plus de deux corps n'est pas intègre $[(1,0)(0,1) = (0,0)]$ et donc est un anneau, mais pas un corps. On dispose, pour tout i, d'une *projection naturelle* $p_j : \prod_{i\in\mathrm{I}} \mathrm{T}_i \to \mathrm{T}_j$ envoyant $(x_i)_{i\in\mathrm{I}}$ sur x_j, qui est un morphisme surjectif de trucs (d'anneaux si les T_i sont des corps).

• Le produit vérifie la *propriété universelle* suivante : si T est un truc, et si $f_j : \mathrm{T} \to \mathrm{T}_j$ est un morphisme de trucs pour tout $j \in \mathrm{I}$, il existe un unique morphisme de trucs $f : \mathrm{T} \to \prod_{i\in\mathrm{I}} \mathrm{T}_i$ tel que $p_j \circ f = f_j$, quel que soit $j \in \mathrm{I}$.

On doit poser $f(x) = (f_i(x))_{i\in\mathrm{I}}$. Il est alors évident que f est un morphisme de trucs, et que $p_j \circ f = f_j$, quel que soit $j \in \mathrm{I}$.

2.6.2. *Somme directe de trucs*

Si $(\mathrm{M}_i)_{i\in\mathrm{I}}$ est une famille de groupes commutatifs (de loi notée additivement), on définit leur *somme directe* $\oplus_{i\in\mathrm{I}}\mathrm{M}_i$ comme le sous-groupe du produit $\prod_{i\in\mathrm{I}} \mathrm{M}_i$ des $(x_i)_{i\in\mathrm{I}}$ vérifiant $x_i = 0$ pour presque tout i (i.e. à l'exception d'un nombre fini de i). On dispose alors, pour tout j, d'une injection naturelle $\iota_j : \mathrm{M}_j \to \oplus_{i\in\mathrm{I}}\mathrm{M}_i$, envoyant $a \in \mathrm{M}_j$ sur $(x_i)_{i\in\mathrm{I}}$, avec $x_j = a$ et $x_i = 0$, si $i \neq j$, qui est un morphisme de groupes.

Si les M_i sont en plus des A-modules alors $\oplus_{i\in\mathrm{I}}\mathrm{M}_i$ est stable par l'action de A et donc est un sous-A-module de $\prod_{i\in\mathrm{I}} \mathrm{M}_i$ (idem pour des K-espaces vectoriels).

Les M_i n'ont pas de raison d'être distincts : par exemple, si $\mathrm{K} = \mathbf{C}$, et si $\mathrm{M}_1 = \mathrm{M}_2 = \mathbf{C}$, alors $\mathrm{M}_1 \oplus \mathrm{M}_2 = \mathbf{C}^2$, et $\iota_1(\mathrm{M}_1)$ (resp. $\iota_2(\mathrm{M}_2)$) est la droite engendrée par $\iota_1(1) = (1,0)$ (resp. $\iota_2(1) = (0,1)$) ; autrement dit, $\mathbf{C} \oplus \mathbf{C}$ est égal à $\mathbf{C}^2$, muni de sa base canonique.

• Si I est fini, la somme directe est égale au produit, mais pas si I est infini [26].

26. Le lecteur désireux de comprendre plus en profondeur la différence entre les notions de produit et de somme est invité à se munir d'une loupe et à consulter l'alinéa 2.6.3.

• La somme directe de trucs [27] vérifie la *propriété universelle* suivante : si M est un truc, et si $f_i : \mathrm{M}_i \to \mathrm{M}$ est un morphisme de trucs pour tout $i \in \mathrm{I}$, il existe un unique morphisme de trucs $f : \oplus_{i\in\mathrm{I}}\mathrm{M}_i \to \mathrm{M}$ tel que $f \circ \iota_i = f_i$, quel que soit $i \in \mathrm{I}$.

On doit poser $f((x_i)_{i\in\mathrm{I}}) = \sum_{i\in\mathrm{I}} f_i(x_i)$, ce qui a un sens car la somme est en fait finie. Il est alors évident que f est un morphisme de trucs, et que $f \circ \iota_i = f_i$, quel que soit $i \in \mathrm{I}$.

• Si M est un truc, et si $(\mathrm{M}_i)_{i\in\mathrm{I}}$ est une famille de sous-trucs de M, on dispose d'un morphisme naturel de trucs de $\oplus_{i\in\mathrm{I}}\mathrm{M}_i$ dans M, induit par l'identité sur M_i, pour tout i. On note $\sum_{i\in\mathrm{I}}\mathrm{M}_i$ l'image de ce morphisme ; c'est le sous-truc de M engendré par les M_i. On dit que les M_i sont *en somme directe dans* M, si l'application naturelle de $\oplus_{i\in\mathrm{I}}\mathrm{M}_i$ dans M est injective. On dit que M *est la somme directe des* M_i si cette application est un isomorphisme, et on écrit alors que $\mathrm{M} = \oplus_{i\in\mathrm{I}}\mathrm{M}_i$, ce qui signifie que tout $x \in \mathrm{M}$ peut s'écrire, de manière unique, sous la forme $x = \sum_{i\in\mathrm{I}} x_i$, avec $x_i \in \mathrm{M}_i$ pour tout i, et $x_i = 0$ pour presque tout i.

• Si $\mathrm{M} = \mathrm{M}_1 \oplus \mathrm{M}_2$, on dit que M_1 et M_2 sont *supplémentaires* ; c'est le cas si et seulement si $\mathrm{M}_1 \cap \mathrm{M}_2 = \{0\}$ et tout $x \in \mathrm{M}$ est somme d'un élément de M_1 et d'un élément de M_2.

2.6.3. *Produit et somme dans une catégorie*

On définit la notion de *catégorie* pour mettre sous un même chapeau les objets ayant les mêmes propriétés. Le lecteur connaît déjà, sans en avoir forcément conscience, un certain nombre de ces catégories (celle des ensembles, celle des groupes ou celle des espaces vectoriels sur **R** ou **C** par exemple ; il y en a beaucoup d'autres comme celle des espaces topologiques, des espaces de Banach...).

Une catégorie C est une collection d'objets (les objets de la catégorie), et de flèches entre ces objets (les morphismes de la catégorie) : si X et Y sont deux objets de C, on note $\mathrm{Hom}_\mathrm{C}(\mathrm{X},\mathrm{Y})$ les morphismes de X vers Y dans la catégorie C. On impose que l'identité id_X soit un morphisme de X dans X, et que l'on puisse composer les morphismes : si X, Y et Z sont trois objets de C, on dispose d'une application $(f,g) \mapsto f \circ g$ de $\mathrm{Hom}_\mathrm{C}(\mathrm{X},\mathrm{Y}) \times \mathrm{Hom}_\mathrm{C}(\mathrm{Y},\mathrm{Z}) \to \mathrm{Hom}_\mathrm{C}(\mathrm{X},\mathrm{Z})$ vérifiant les propriétés évidentes :

$$f \circ \mathrm{id}_\mathrm{X} = f,\ \mathrm{id}_\mathrm{Y} \circ f = f \text{ et } (f \circ g) \circ h = f \circ (g \circ h).$$

Les exemples les plus simples de catégories sont les suivants :
— La catégorie des ensembles ; les morphismes de X dans Y sont les applications de X dans Y.
— La catégorie des groupes ; les morphismes sont les morphismes de groupes.
— La catégorie des groupes commutatifs ; les morphismes sont les morphismes de groupes.
— La catégorie des anneaux commutatifs ; les morphismes sont les morphismes d'anneaux.
— La catégorie des K-espaces vectoriels, K un corps ; les morphismes sont les applications K-linéaires.
— La catégorie des espaces topologiques ; les morphismes sont les applications continues.
— La catégorie des espaces métriques ; les morphismes sont les applications continues.
— La catégorie des **K**-espaces de Banach, $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$; les morphismes sont les applications **K**-linéaires continues.

Dans une catégorie, on définit les notions de *produit* et *somme* par les propriétés universelles suivantes (la propriété universelle implique l'unicité d'un tel objet, mais pas son existence qui doit se démontrer cas par cas).

Si C est une catégorie et les $(\mathrm{X}_i)_{i\in\mathrm{I}}$ sont des objets de C, le produit $\mathrm{X} = \prod_{i\in\mathrm{I}}\mathrm{X}_i$ des X_i est un objet de C muni de morphismes $p_i \in \mathrm{Hom}_\mathrm{C}(\mathrm{X},\mathrm{X}_i)$, pour $i \in \mathrm{I}$, tel que, si Y est n'importe quel objet de C, et si $f_i \in \mathrm{Hom}_\mathrm{C}(\mathrm{Y},\mathrm{X}_i)$, pour tout $i \in \mathrm{I}$, alors il existe $f \in \mathrm{Hom}_\mathrm{C}(\mathrm{Y},\mathrm{X})$, unique, tel que $p_i \circ f = f_i$ pour tout $i \in \mathrm{I}$.

27. Ici truc signifie « groupe commutatif », « A-modules » ou « K-espaces vectoriels ».

La somme $\mathrm{X} = \coprod_{i\in\mathrm{I}} \mathrm{X}_i$ des X_i est un objet de C muni de morphismes $\iota_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}_i, \mathrm{X})$, pour $i \in \mathrm{I}$, tel que, si Y est n'importe quel objet de C, et si $f_i \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}_i, \mathrm{Y})$, pour tout $i \in \mathrm{I}$, alors il existe $f \in \mathrm{Hom}_{\mathrm{C}}(\mathrm{X}, \mathrm{Y})$, unique, tel que $f \circ \iota_i = f_i$ pour tout $i \in \mathrm{I}$.

Montrons par exemple l'unicité du produit. Si X (resp. X′), muni des $p_i : \mathrm{X} \to \mathrm{X}_i$ (resp. des $p'_i : \mathrm{X}' \to \mathrm{X}_i$), est un produit des X_i, alors en particulier, il existe $f : \mathrm{X}' \to \mathrm{X}$, unique, tel que $p_i \circ f = p'_i$ pour tout i, et il existe $g : \mathrm{X} \to \mathrm{X}'$, unique, tel que $p'_i \circ g = p_i$ pour tout i. Alors $f \circ g : \mathrm{X} \to \mathrm{X}$ vérifie $p_i \circ (f \circ g) = p_i$ pour tout i, ce qui implique que $f \circ g = \mathrm{id}_{\mathrm{X}}$ puisque id_{X} vérifie la même propriété, et que par hypothèse, il n'y a qu'un seul morphisme de X dans X ayant cette propriété. Pour la même raison, on a $g \circ f = \mathrm{id}_{\mathrm{X}}$, ce qui prouve que X et X′ sont isomorphes (à isomorphisme unique près puisque f et g étaient uniques). Cette démonstration s'étend à tout objet solution d'un problème universel.

On dit qu'une catégorie admet des produits (resp. des sommes), si tout couple (et donc toute famille finie) d'objets de la catégorie admet un produit (resp. une somme). Toutes les catégories ci-dessus admettent des produits, car on peut munir le produit ensembliste de deux objets des structures additionnelles demandées. Elles admettent aussi toutes une somme, mais celle-ci peut prendre des formes assez variées.

— Dans la catégorie des ensembles, la somme d'une famille $(\mathrm{X}_i)_{i\in\mathrm{I}}$ d'ensembles est leur réunion disjointe $\coprod_{i\in\mathrm{I}} \mathrm{X}_i = \cup_{i\in\mathrm{I}}(\{i\} \times \mathrm{X}_i)$.

— Dans la catégorie des K-espaces vectoriels, ou dans celle des groupes commutatifs, la somme est la somme directe, et la somme d'un nombre fini d'objets est isomorphe à leur produit comme on l'a vu ci-dessus.

— Dans la catégorie des groupes, la somme de deux groupes A et B est leur produit libre $\mathrm{A} \star \mathrm{B}$: les éléments de $\mathrm{A} \star \mathrm{B}$ sont les mots finis composés d'éléments de A et B modulo la relation d'équivalence selon laquelle on peut remplacer toute lettre x dans un mot par deux lettres x_1, x_2 appartenant au même groupe si $x_1 x_2 = x$, et réciproquement, on peut remplacer deux lettres consécutives appartenant au même groupe par leur produit. La somme de deux groupes commutatifs n'est donc pas la même dans la catégorie des groupes que dans celle des groupes commutatifs. Par exemple, on a $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) = (\mathbf{Z}/6\mathbf{Z})$, alors que $(\mathbf{Z}/2\mathbf{Z}) \star (\mathbf{Z}/3\mathbf{Z})$ est un groupe infini, isomorphe au groupe $\mathbf{PSL}_2(\mathbf{Z})$, quotient de $\mathbf{SL}_2(\mathbf{Z})$ par son centre $\left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$.

2.7. Relations d'équivalence

2.7.1. *Relations d'équivalence et partitions*

Si E est un ensemble, une *partition* de E est une famille de sous-ensembles non vides de E, deux à deux disjoints, dont la réunion est E.

Par exemple, $\{\mathbf{R}^*_+, \mathbf{R}^*_-, \{0\}\}$ est une partition de $\mathbf{R}$. Si $\mathrm{D} \in \mathbf{N} - \{0\}$, les $r + \mathrm{D}\mathbf{Z}$, pour $r \in \{0, \ldots, \mathrm{D}-1\}$ forment une partition de $\mathbf{Z}$.

Une *relation* R sur E est un sous-ensemble de $\mathrm{E} \times \mathrm{E}$. Si $(x, y) \in \mathrm{E} \times \mathrm{E}$, on écrit souvent $x\mathrm{R}y$ pour signifier $(x, y) \in \mathrm{R}$.

Une relation R sur E est une *relation d'équivalence* si elle est *réflexive* ($x\mathrm{R}x$ quel que soit $x \in \mathrm{E}$), *symétrique* ($x\mathrm{R}y$ implique $y\mathrm{R}x$) et *transitive* ($x\mathrm{R}y$ et $y\mathrm{R}z$ impliquent $x\mathrm{R}z$).

Si R est une relation d'équivalence sur E, et si $x \in \mathrm{E}$, la *classe d'équivalence de* x est l'ensemble $\mathrm{C}_x = \{y \in \mathrm{E},\ y\mathrm{R}x\}$. Un sous-ensemble C de E est *une classe d'équivalence* (pour R), s'il existe $x \in \mathrm{E}$ tel que $\mathrm{C} = \mathrm{C}_x$. Si $x, y \in \mathrm{E}$, alors $\mathrm{C}_x \cap \mathrm{C}_y \neq \varnothing$ si et seulement si $x\mathrm{R}y$, et on a alors $\mathrm{C}_x = \mathrm{C}_y$. Les classes d'équivalence forment donc une partition de E.

Réciproquement, si les $(\mathrm{C}_i)_{i\in\mathrm{I}}$ forment une partition de E, alors la relation R définie par $x\mathrm{R}y$ si et seulement si il existe $i \in \mathrm{I}$ tel que $\{x, y\} \subset \mathrm{C}_i$ est une relation d'équivalence dont les classes d'équivalence sont les C_i. En d'autres termes, il revient au même de munir un ensemble d'une relation d'équivalence ou de faire une partition de cet ensemble.

Par exemple, la partition de $\mathbf{R}$ ci-dessus correspond à la relation d'équivalence « $x \sim y$ si et seulement si x et y ont même signe » ; celle de $\mathbf{Z}$ correspond à la relation d'équivalence « $a \sim b$ si et seulement si a et b ont même reste dans la division euclidienne par D ».

2.7.2. *Passage au quotient par une relation d'équivalence.* — Si R est une relation d'équivalence sur E, on définit *le quotient* E/R *de* E *par la relation d'équivalence* R comme l'ensemble des classes d'équivalence. On dispose d'une application naturelle de E dans E/R, à savoir l'application qui à x associe sa classe d'équivalence (souvent notée $\overline{x}$) ; cette application est surjective par construction de E/R. Un sous-ensemble S de E est *un système de représentants* de E/R, s'il contient un et un seul élément de chaque classe d'équivalence [28]. Autrement dit, $S \subset E$ est un système de représentants de E/R si et seulement si l'application naturelle de E dans E/R induit une bijection de S sur E/R.

Cette manière de définir de nouveaux objets en passant au quotient par une relation d'équivalence est une des plus universelles qui soit [29]. Pour le petit enfant, le nombre 5 est la classe d'équivalence des ensembles pouvant être mis en bijection avec l'ensemble {un,deux,trois,quatre,cinq} (ce n'est pas une raison pour le lui définir de cette manière...). Pour le commun des mortels, un nombre réel est un nombre avec une infinité de chiffres derrière la virgule, et comme certains nombres ont deux écritures, il faut passer

28. Si E/R est infini, l'existence d'un système de représentants peut demander l'axiome du choix, mais celui-ci peut vous tirer de situations délicates. Par exemple, un dictateur démoniaque a enfermé un ensemble infini I de mathématiciens et leur offre l'alternative suivante : je vais placer dans le dos de chacun de vous un nombre réel tiré au hasard et demander a chacun de deviner quel est le nombre qui se cache derrière son dos (vous verrez les nombres dans le dos des autres mais ne pourrez rien dire) ; si tout le monde, sauf un nombre fini, a raison, je vous libère, dans le cas contraire, vous êtes condamnés à résoudre des systèmes linéaires à perpétuité. La situation a l'air assez désespérée mais si nos mathématiciens croient en l'axiome du choix, il leur suffit de choisir un système S de représentants de $\mathbf{R}^{\mathrm{I}}$ modulo la relation d'équivalence $(x_i)_{i\in \mathrm{I}} \sim (y_i)_{i\in \mathrm{I}}$ si et seulement si $x_i = y_i$ pour tout i sauf un nombre fini. Voir ce qu'il y a dans le dos des autres suffit à déterminer dans quelle classe d'équivalence on est, et si $(s_i)_{i\in \mathrm{I}} \in \mathrm{S}$ est le représentant de cette classe d'équivalence, il suffit au mathématicien i d'annoncer qu'il a le nombre s_i dans son dos pour qu'au plus un nombre fini d'entre eux se trompent.

29. L'expérience montre que les premiers passages au quotient que l'on rencontre sont un peu traumatisants, mais on finit par s'y faire... Il fut un temps pas si lointain, où l'on définissait $\mathbf{Z}$ comme le quotient de $\mathbf{N}\times\mathbf{N}$ par la relation d'équivalence $(a,b) \sim (a',b')$ si et seulement si $a+b' = a'+b$, l'idée étant que (a,b) représente l'entier relatif $a-b$. Au bout de 3 semaines, on avait enfin le droit d'écrire $2-3+5-7=-3$, ce que n'importe qui ayant regardé un thermomètre comprend très bien. Pour en arriver là, il avait fallu passer par $(2,0)+(0,3)+(5,0)+(0,7) = (7,10) = (0,3)$, puis par $(+2)+(-3)+(+5)+(-7) = (-3)$. On achevait de traumatiser les élèves (et leur parents) en définissant, en classe de $4^{\text{ème}}$, un vecteur comme une classe d'équipollence de bipoints (un bipoint (i.e. un couple de points) (A, B) est *équipollent* à (C, D), si (A, B, D, C) est un parallélogramme). Dans une période plus récente, les aléas de la conjoncture ayant provoqué un tarissement des vocations de professeurs de mathématiques, on s'est retrouvé avec une pénurie que l'on a traitée en diminuant l'horaire de mathématiques dans l'enseignement, et on en a profité pour jeter allègrement à la poubelle toutes ces horribles mathématiques modernes...

au quotient... Une couleur aussi est définie par un passage au quotient nettement plus délicat que les passages au quotient mathématiques...

En général, on aime bien que E/R hérite des propriétés que pouvait avoir E (i.e. on aime bien que les propriétés de E *passent au quotient*), ce qui impose des contraintes aux relations d'équivalence que l'on peut considérer. Par exemple, une fonction $f : \mathrm{E} \to \mathrm{X}$ passe au quotient si et seulement si on a $f(x) = f(y)$ pour tout couple d'éléments de E vérifiant $x\mathrm{R}y$ (si c'est le cas, on définit $\overline{f} : \mathrm{E/R} \to \mathrm{X}$ par $\overline{f}(z) = f(x)$ pour n'importe quel élément x de E ayant pour image z dans E/R. Si $\pi : \mathrm{E} \to \mathrm{E/R}$ est l'application naturelle, on a $f = \overline{f} \circ \pi$; on dit que f *se factorise à travers* E/R ou que f se factorise à travers π, ce qui est une terminologie assez parlante puisqu'elle signifie que l'équation $f = g \circ \pi$ a une solution $g = \overline{f}$).

2.8. L'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ des entiers relatifs modulo D

Dans tout ce qui suit, D est un entier $\geqslant 1$. On note $\mathrm{D}\mathbf{Z}$ l'ensemble des multiples de D. On définit une relation *de congruence modulo* D sur $\mathbf{Z}$, en disant que a est congru à b modulo D (ou modulo $\mathrm{D}\mathbf{Z}$), ce qui se note $a \equiv b$ [D] ou $a \equiv b \bmod \mathrm{D}$, si $b - a \in \mathrm{D}\mathbf{Z}$.

• La relation de congruence modulo D est une relation d'équivalence sur $\mathbf{Z}$. On note $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ l'ensemble des classes d'équivalence. L'image d'un entier dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est sa *réduction modulo* D.

> Cette relation est réflexive car 0 est un multiple de D, symétrique car si $b-a$ est un multiple de D, il en est de même de $a - b$, et transitive car si $b - a$ et $c - b$ sont des multiples de D, il en est de même $c - a = (c - b) + (b - a)$.

• Un système naturel de représentants de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans $\mathbf{Z}$ est l'ensemble $\{0, 1, \ldots, \mathrm{D} - 1\}$; en particulier, $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est de cardinal D.

> Si $a, b \in \{0, 1, \ldots, \mathrm{D} - 1\}$ sont distincts, et si $b > a$, alors $1 \leqslant b - a \leqslant \mathrm{D} - 1$. En particulier $b - a$ n'est pas un multiple de D, ce qui prouve que b et a sont dans des classes distinctes modulo D, et donc que l'application naturelle de $\{0, 1, \ldots, \mathrm{D} - 1\}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est injective. Par ailleurs, si $a \in \mathbf{Z}$ est quelconque, et si $r \in \{0, 1, \ldots, \mathrm{D} - 1\}$ est le reste de la division de a par D, alors $a - r$ est un multiple de D et a est dans la même classe que r modulo D ; l'application naturelle de $\{0, 1, \ldots, \mathrm{D} - 1\}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est donc surjective.

• L'addition et la multiplication sur $\mathbf{Z}$ passent au quotient, et $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ muni des lois d'addition et multiplication ainsi définies est un anneau commutatif [30].

> Si $x - x'$ et $y - y'$ sont divisibles par D, alors $(x + y) - (x' + y') = (x - x') + (y - y')$ et $xy - x'y' = x(y - y') + y'(x - x')$ sont divisibles par D, ce qui prouve que le résultat modulo D de l'addition et la multiplication de deux entiers ne dépend que de leurs réductions modulo D ;

30. La manière qui est probablement la plus efficace pour penser à l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est de le voir comme étant l'anneau $\mathbf{Z}$ auquel on a rajouté la relation $\mathrm{D} = 0$; on fait donc les additions et les multiplications comme si on était dans $\mathbf{Z}$, mais on se permet d'enlever le multiple de D que l'on veut au résultat. Par exemple, dans $\mathbf{Z}/21\mathbf{Z}$, on a $6 \times 14 = 4 \times 21 = 0$ et $4 \times 16 = 1 + 3 \times 21 = 1$, ce qui montre que 6 et 14 sont des diviseurs de 0, alors que 4 est inversible, d'inverse 16

en d'autres termes, l'addition et la multiplication passent au quotient. Par ailleurs, les identités à vérifier pour prouver que $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est un anneau sont déjà vraies dans l'anneau $\mathbf{Z}$; elles le sont donc, a fortiori, dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

• $a \in \mathbf{Z}$ est inversible (pour la multiplication) dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ si et seulement si a est premier à D. On note $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$ l'ensemble des éléments inversibles ; c'est un groupe dont le cardinal est traditionnellement noté $\varphi(\mathrm{D})$, et la fonction φ est la *fonction indicatrice d'Euler*.

Si a est premier à D, il existe, d'après le théorème de Bézout (n° 1.2), $u, v \in \mathbf{Z}$ tels que $au + \mathrm{D}v = 1$, ce qui prouve que a est inversible dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, d'inverse u. Réciproquement, si $ab = 1$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, cela signifie que $ab - 1$ est divisible par D, et donc qu'il existe $v \in \mathbf{Z}$ tel que $ab + \mathrm{D}v = 1$; d'après le théorème de Bézout, cela implique que a et D sont premiers entre eux, ce qui permet de conclure.

• D est premier si et seulement si $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est un corps.

L'anneau $\{0\}$ n'est pas un corps (si K est un corps, $\mathrm{K} - \{0\}$ est un groupe pour la multiplication et donc est non vide) et 1 n'est pas un nombre premier ; on peut supposer $\mathrm{D} \geqslant 2$.

Si $\mathrm{D} \geqslant 2$ n'est pas premier, on peut le factoriser sous la forme $\mathrm{D} = ab$, avec $a \in \{2, \ldots, \mathrm{D}-1\}$ et $b \in \{2, \ldots, \mathrm{D}-1\}$. Donc a et b ne sont pas nuls dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ alors que $ab = \mathrm{D} = 0$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$; l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ admet donc des diviseurs de 0 et n'est pas un corps.

Si D est premier, et si a n'est pas divisible par D, alors a est premier à D et donc inversible dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ d'après le point précédent. Ceci permet de conclure.

Un nombre premier a tendance à être noté p, et si on veut insister sur le fait que $\mathbf{Z}/p\mathbf{Z}$ est un corps, on le note $\mathbf{F}_p$. Par exemple, on parlera d'espaces vectoriels sur $\mathbf{F}_2$ au lieu d'espaces vectoriels sur $\mathbf{Z}/2\mathbf{Z}$ pour parler des objets qui peuplent Internet [31] et dans lesquels vivent les codes correcteurs d'erreurs.

• Tout corps de cardinal p est isomorphe à $\mathbf{F}_p$, et donc $\mathbf{F}_p$ est *le corps à p éléments* [32].

Soit K un corps à p élément. On dispose d'un morphisme d'anneaux $f : \mathbf{Z} \to \mathrm{K}$ envoyant 1 sur 1. Ce morphisme d'anneaux est en particulier un morphisme de groupes additifs. Son image est donc un sous-groupe du groupe $(\mathrm{K}, +)$, et son cardinal est un diviseur de $|\mathrm{K}| = p$, d'après le th. de Lagrange (n° 3.3), et comme cette image a au moins deux éléments, à savoir 0 et 1, c'est K tout entier. On en déduit que f induit un isomorphisme de $\mathbf{Z}/\mathrm{Ker}\, f$ sur K, et comme $|\mathrm{K}| = p$, on a $\mathrm{Ker}\, f = p\mathbf{Z}$, et donc $\mathrm{K} \cong \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$. Ceci permet de conclure.

---

31. Internet aime beaucoup $\mathbf{Z}/\mathrm{D}\mathbf{Z}$. Non content de faire voyager des milliards de $\mathbf{F}_2$-espaces vectoriels, Internet est très gourmand de grands nombres premiers, par exemple pour le système RSA de sécurité à clé publique (1977). Ce système et la fabrication de grands nombres premiers reposent sur l'arithmétique dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ qui s'avère être nettement plus subtile que ce que l'on pourrait attendre d'un objet aussi petit. On peut saluer la clairvoyance de la commission ayant accouché des programmes actuels, qui a fait disparaître $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ des programmes de la filière PC au moment même où Internet prenait son envol...

32. Plus généralement (cf. n° 8.7), si q est une puissance d'un nombre premier, il y a, à isomorphisme près, un unique corps à q élément, et ce corps est noté $\mathbf{F}_q$. On a beaucoup fantasmé ces dernières années autour du corps $\mathbf{F}_1$ « à 1 élément » dont on voit la trace dans plusieurs phénomènes sans comprendre quel genre d'objet cela pourrait bien être (pas l'anneau $\{0\}$ en tout cas). Certains y voient la clef d'une démonstration de l'hypothèse de Riemann.

• Si D′ est un diviseur de D, alors l'application naturelle $\mathbf{Z} \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ se factorise à travers une application naturelle $(\mathbf{Z}/\mathrm{D}\mathbf{Z}) \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ qui est un morphisme d'anneaux.

Si D′ est un diviseur de D, alors un multiple de D est aussi un multiple de D′. On en déduit que, si $a \equiv b \bmod \mathrm{D}$, alors $a \equiv b \bmod \mathrm{D}'$; autrement dit l'application naturelle $\mathbf{Z} \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$ se factorise à travers une application naturelle $(\mathbf{Z}/\mathrm{D}\mathbf{Z}) \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})$. On obtient un morphisme d'anneaux car les identités à vérifier sont déjà valables en remontant à $\mathbf{Z}$.

• Si a et b sont premiers entre eux, l'application naturelle $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un isomorphisme d'anneaux qui induit un isomorphisme de groupes de $(\mathbf{Z}/ab\mathbf{Z})^*$ sur $(\mathbf{Z}/a\mathbf{Z})^* \times (\mathbf{Z}/b\mathbf{Z})^*$ (th. des restes chinois).

L'application naturelle $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un morphisme d'anneaux d'après le point précédent. Il est injectif car, si $x \in \mathbf{Z}$ a une réduction modulo ab qui est dans le noyau, c'est que x est divisible par a et par b, et donc par ab puisqu'on a supposé a et b premiers entre eux ; autrement dit, le noyau est réduit à 0. Comme les deux ensembles considérés ont même cardinal ab, une application injective est aussi bijective, ce qui montre que $\mathbf{Z}/ab\mathbf{Z} \to (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est un isomorphisme. On conclut en remarquant que si A et B sont deux anneaux, alors $(\mathrm{A} \times \mathrm{B})^* = \mathrm{A}^* \times \mathrm{B}^*$.

En fait, on peut décrire explicitement l'isomorphisme inverse. Comme a et b sont premiers entre eux, il existe $u, v \in \mathbf{Z}$ tels que $1 = au + bv$. Si $(x, y) \in (\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$, et si $\tilde{x}, \tilde{y} \in \mathbf{Z}$ ont pour image x et y dans $\mathbf{Z}/a\mathbf{Z}$ et $\mathbf{Z}/b\mathbf{Z}$ respectivement, alors l'image de $bv\tilde{x} + au\tilde{y}$ dans $\mathbf{Z}/ab\mathbf{Z}$ ne dépend pas des choix de $\tilde{x}$ et $\tilde{y}$ et s'envoie sur (x, y) dans $(\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$, comme le montre un petit calcul immédiat. On remarque que $x \mapsto bv\tilde{x}$ induit un isomorphisme de $\mathbf{Z}/a\mathbf{Z}$ sur le sous-groupe $b\mathbf{Z}/ab\mathbf{Z}$ de $\mathbf{Z}/ab\mathbf{Z}$ et que $y \mapsto au\tilde{y}$ induit un isomorphisme de $\mathbf{Z}/b\mathbf{Z}$ sur le sous-groupe $a\mathbf{Z}/ab\mathbf{Z}$ de $\mathbf{Z}/ab\mathbf{Z}$. On en déduit le résultat suivant :

• Si a et b sont premiers entre eux, $\mathbf{Z}/ab\mathbf{Z}$ est la somme directe de ses sous-groupes $b\mathbf{Z}/ab\mathbf{Z}$ et $a\mathbf{Z}/ab\mathbf{Z}$; de plus, on a des isomorphismes de groupes additifs $b\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/a\mathbf{Z}$ et $a\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/b\mathbf{Z}$, et donc $\mathbf{Z}/ab\mathbf{Z} \cong (\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$, comme groupe additif.

Exercice 2.3. — Montrer que si $a \neq 0$ et $b \neq 0$ ne sont pas premiers entre eux, les groupes additifs $\mathbf{Z}/ab\mathbf{Z}$ et $(\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$ ne sont pas isomorphes.

Exercice 2.4. — Résoudre les équations $4x + 3 = 0$, $14x + 2 = 0$ et $14x + 7 = 0$ dans $\mathbf{Z}/21\mathbf{Z}$.

Exercice 2.5. — Résoudre l'équation $x^2 + x + 1 = 0$ dans $\mathbf{Z}/91\mathbf{Z}$. (Comme 91 est relativement petit [33], on peut tester chaque élément de $\mathbf{Z}/91\mathbf{Z}$ et voir lesquels conviennent, mais c'est un peu fastidieux...)

33. Essayer de résoudre de la même manière l'équation $x^2 = 5$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, avec $\mathrm{D} = 2^{2802} - 2^{521} - 2^{2281} + 1$ est voué à l'échec, même avec l'aide d'un ordinateur. Par contre, en partant de $\mathrm{D} = (2^{521} - 1)(2^{2281} - 1)$, si on sait que $p_1 = 2^{521} - 1$ et $p_2 = 2^{2281} - 1$ sont premiers (ce sont des *nombres premiers de Mersenne* découverts par Robinson en 1952), alors on peut sans trop d'effort calculer le nombre de solutions de l'équation et, avec l'aide d'un ordinateur et d'algorithmes astucieux, calculer explicitement ces solutions. Le calcul du nombre de solutions repose sur la *loi de réciprocité quadratique* conjecturée par Euler en 1783 et démontrée par Gauss en 1801. Si p est un nombre premier, et si $a \in \mathbf{Z}$ n'est pas divisible par p, on pose $(\frac{a}{p}) = 1$, si a est un carré modulo p (i.e. si l'équation $x^2 = a$ a des solutions dans $\mathbf{F}_p$) et $(\frac{a}{p}) = -1$ si a n'est pas un carré modulo p (si l'équation $x^2 = a$ n'a pas de solutions dans $\mathbf{F}_p$). La loi de réciprocité quadratique s'énonce alors ainsi : *si p et q sont deux nombres premiers impairs distincts,*

Exercice 2.6. — (i) Soit $p \in \mathscr{P}$. Montrer que si $p \neq 3$, et si l'équation $x^2 + x + 1 = 0$ a une solution dans $\mathbf{F}_p$, alors elle en a deux.

(ii) (difficile) Montrer qu'il existe une infinité de nombres premiers p tels que l'équation $x^2 + x + 1 = 0$ ait deux solutions dans $\mathbf{F}_p$.

(iii) En déduire que quel que soit $\mathrm{M} > 0$, il existe $\mathrm{D} \in \mathbf{N}$ tel que $x^2 + x + 1 = 0$ ait plus de M solutions dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

Exercice 2.7. — Montrer qu'il y a une infinité de nombres premiers de la forme $4n - 1$.

Exercice 2.8. — (i) Soit $\mathrm{X}(p_1, \ldots, p_r, x)$ l'ensemble des entiers $\leqslant x$ dont tous les facteurs premiers appartiennent à l'ensemble fini $\{p_1, \ldots, p_r\}$. Montrer que $|\mathrm{X}(p_1, \ldots, p_r, x)| = \mathrm{O}(\log^r x)$.

(ii) Montrer que tout nombre premier divisant $4k^2 + 1$ est de la forme $4n + 1$. (On pourra utiliser le petit th. de Fermat.)

(iii) En déduire que l'ensemble des nombres premiers de la forme $4n + 1$ est infini.

Exercice 2.9. — Montrer que si $p \in \mathscr{P}$, alors $\mathbf{Z}/p^n\mathbf{Z}$ a $p^n - p^{n-1}$ éléments inversibles. En déduire que, si $\mathrm{D} \geqslant 2$, alors $\varphi(\mathrm{D}) = \mathrm{D} \cdot \prod_{p|\mathrm{D}}(1 - \frac{1}{p})$, où φ est la fonction indicatrice d'Euler.

2.9. Quotients d'espaces vectoriels et de A-modules

Soit E un espace vectoriel sur un corps K, soit R une relation d'équivalence sur E, et soit $\mathrm{F} \subset \mathrm{E}$ la classe d'équivalence de 0. Pour que la structure d'espace vectoriel de E passe au quotient, on doit en particulier avoir $\lambda x \in \mathrm{F}$ si $\lambda \in \mathrm{K}$ et $x \in \mathrm{F}$ (puisque $\lambda 0 = 0$ dans E/R) et $x + y \in \mathrm{F}$ si $x, y \in \mathrm{F}$ (puisque $0 + 0 = 0$ dans E/R) ; en d'autres termes, F doit être un sous-espace vectoriel de E. De plus, comme $a + 0 = a$ dans E/R, les classes d'équivalence doivent être de la forme $a + \mathrm{F}$.

Réciproquement, si F est un sous-espace vectoriel de E, la relation $\sim_{\mathrm{F}}$, définie sur E par $x \sim_{\mathrm{F}} y$ si et seulement si $x - y \in \mathrm{F}$, est une relation d'équivalence. Le quotient $\mathrm{E}/\sim_{\mathrm{F}}$ est traditionnellement noté E/F. Comme « $x - y \in \mathrm{F}$ »⇒ « $\lambda x - \lambda y \in \mathrm{F}$ » , et comme « $x - y \in \mathrm{F}$ et $x' - y' \in \mathrm{F}$ »⇒« $(x + x') - (y + y') \in \mathrm{F}$ », la structure d'espace vectoriel sur E passe au quotient.

Si $\mathrm{F}' \subset \mathrm{E}$ est un sous-espace vectoriel supplémentaire de F, les classes d'équivalence pour $\sim_{\mathrm{F}}$ sont les $a + \mathrm{F}$, pour $a \in \mathrm{F}'$, et l'application naturelle $\mathrm{F}' \to \mathrm{E/F}$ est un isomorphisme d'espaces vectoriels. En d'autres termes, *dans le cas des espaces vectoriels*, un quotient est toujours isomorphe à un sous-objet, mais il est très souvent nocif de remplacer, dans les raisonnements, un quotient par un sous-objet qui lui est isomorphe. Par exemple, si F est un sous-espace vectoriel d'un espace vectoriel E, le dual F^* de F (i.e. l'ensemble des formes linéaires de F dans K) est naturellement un quotient du dual E^* de E (on peut restreindre à F une forme linéaire sur E, et F^* est le quotient de E^* par le sous-espace des formes linéaires identiquement nulles sur F), et n'est pas, en général, un sous-espace de E^*, de manière naturelle.

• L'espace E/F vérifie la propriété universelle suivante : si $u : \mathrm{E} \to \mathrm{E}'$ est une application K-linéaire, et si $\operatorname{Ker} u$ contient F, alors u *se factorise à travers* E/F (i.e. il existe une

alors $(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}(\frac{p}{q})$. On applique ce qui précède à $p = p_1$ et $q = 5$. Comme $p_1 = 2^{521} - 1 = 2^{4 \cdot 130 + 1} - 1 = 2 \cdot (2^4)^{130} - 1 = 2 - 1 = 1$ dans $\mathbf{F}_5$, on a $(\frac{p_1}{5}) = 1$ et donc $(\frac{5}{p_1}) = 1$, d'après la loi de réciprocité quadratique. On en déduit que l'équation $x^2 = 5$ a deux solutions dans $\mathbf{F}_{p_1}$. Pour la même raison, elle en a aussi 2 dans $\mathbf{F}_{p_2}$ et donc 4 dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

unique application linéaire $\overline{u} : \mathrm{E/F} \to \mathrm{E}'$, telle que $u = \overline{u} \circ \pi$, où $\pi : \mathrm{E} \to \mathrm{E/F}$ est la projection canonique).

• Si $u : \mathrm{E} \to \mathrm{E}'$ est une application linéaire, alors u se factorise à travers $\mathrm{E}/\mathrm{Ker}\, u$, et l'application induite $\overline{u} : \mathrm{E}/\mathrm{Ker}\, u \to \mathrm{Im}\, u$ est un isomorphisme d'espaces vectoriels.

Ce qui précède s'étend au cas des A-modules, si A est un anneau : si R est une relation d'équivalence sur un A-module M, la structure de A-module passe au quotient si et seulement si la classe d'équivalence de 0 est un sous-A-module N et celle de x est $x + \mathrm{N}$, pour tout $x \in \mathrm{M}$. On note M/N le A-module quotient ; il vérifie la propriété universelle suivante : si $u : \mathrm{M} \to \mathrm{M}'$ est une application A-linéaire, et si $\mathrm{Ker}\, u$ contient N, alors u se factorise à travers M/N ; en particulier u se factorise à travers $\mathrm{M}/\mathrm{Ker}\, u$, et l'application induite $\overline{u} : \mathrm{M}/\mathrm{Ker}\, u \to \mathrm{Im}\, u$ est un isomorphisme de A-modules.

Contrairement à ce qui se passe dans le cas des espaces vectoriels, le module M/N n'est pas, en général, isomorphe à un sous-module de M. Par exemple $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ n'est pas isomorphe à un sous-$\mathbf{Z}$-module de $\mathbf{Z}$.

2.10. Anneaux quotients, idéaux

Dans ce n°, les anneaux sont supposés commutatifs.

2.10.1. *Quotient d'un anneau par un idéal*

Soit A un anneau, soit R une relation d'équivalence sur A, et soit $\mathrm{I} \subset \mathrm{E}$ la classe d'équivalence de 0. Pour que la structure d'anneau de A passe au quotient, on doit en particulier avoir $\lambda x \in \mathrm{I}$ si $\lambda \in \mathrm{A}$ et $x \in \mathrm{I}$ (puisque $\lambda 0 = 0$ dans A/R) et $x + y \in \mathrm{I}$ si $x, y \in \mathrm{I}$ (puisque $0 + 0 = 0$ dans A/R) ; un sous-ensemble de A vérifiant ces deux propriétés est un *idéal* de A. De plus, comme $a + 0 = a$ dans A/R, les classes d'équivalence doivent être de la forme $a + \mathrm{I}$.

Réciproquement, si I est un idéal de A, la relation $\sim_{\mathrm{I}}$, définie sur E par $x \sim_{\mathrm{I}} y$ si et seulement si $x - y \in \mathrm{I}$, est une relation d'équivalence. Le quotient $\mathrm{A}/\sim_{\mathrm{I}}$ est traditionnellement noté A/I. Comme « $x - y \in \mathrm{I}$ et $x' - y' \in \mathrm{I}$ »⇒« $(x + x') - (y + y') \in \mathrm{I}$ », et comme « $x - y \in \mathrm{I}$ et $x' - y' \in \mathrm{I}$ »⇒« $xx' - yy' = x(y - y') + y'(x - x') \in \mathrm{I}$ », la structure d'anneau sur A passe au quotient.

• L'anneau A/I vérifie la propriété universelle suivante : si $f : \mathrm{A} \to \mathrm{A}'$ est un morphisme d'anneaux, et si $\mathrm{Ker}\, f$ contient I, alors f se factorise à travers A/I (i.e. il existe un unique morphisme d'anneaux $\overline{f} : \mathrm{A/I} \to \mathrm{A}'$, tel que $f = \overline{f} \circ \pi$, où $\pi : \mathrm{A} \to \mathrm{A/I}$ est la projection canonique).

• Si $f : \mathrm{A} \to \mathrm{A}'$ est un morphisme d'anneaux, alors $\mathrm{Ker}\, f$ est un idéal de A, f se factorise à travers $\mathrm{A}/\mathrm{Ker}\, f$ et l'application induite $\overline{f} : \mathrm{A}/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ est un isomorphisme d'anneaux.

Le lecteur connaît déjà beaucoup d'anneaux définis de cette manière. Par exemple :

– le corps $\mathbf{F}_p$, quotient de $\mathbf{Z}$ par l'idéal $p\mathbf{Z}$ (p étant un nombre premier),

– l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ quotient de $\mathbf{Z}$ par l'idéal $\mathrm{D}\mathbf{Z}$ (D entier quelconque),

– l'anneau $\mathbf{Z}[X]/(10X-1)$ des nombres décimaux (prendre le quotient de $\mathbf{Z}[X]$ par $(10X-1)$ revient à rajouter à $\mathbf{Z}$ un élément X vérifiant $10X = 1$, et $a_nX^n + \cdots + a_0 \in \mathbf{Z}[X]$ devient le nombre décimal $\frac{a_n}{10^n} + \cdots + \frac{a_1}{10} + a_0$),

– le corps des nombres complexes [34] $\mathbf{C} = \mathbf{R}[X]/(X^2+1)$ (prendre le quotient de $\mathbf{R}[X]$ par l'idéal [35] (X^2+1) revient à rajouter à $\mathbf{R}$ un élément X vérifiant $X^2+1=0$, et donc X devient une racine carrée de -1 dans le quotient).

On en rencontre beaucoup d'autres, par exemple les anneaux suivants.

– $\mathbf{Z}[X]/(X^2+1)$, anneau des *entiers de Gauss*; en envoyant X sur i ou $-i$, cet anneau s'identifie au sous-anneau $\mathbf{Z}[i] = \{a+ib,\ a,b \in \mathbf{Z}\}$ de $\mathbf{C}$.

– $\mathbf{Z}[X]/(X^3-2)$. Il s'identifie à un sous-anneau de $\mathbf{C}$ de trois manières différentes : on peut envoyer X sur $\sqrt[3]{2}$, ou sur $e^{2i\pi/3}\sqrt[3]{2}$ ou sur $e^{4i\pi/3}\sqrt[3]{2}$. Dans le premier cas, l'image est un sous-anneau de $\mathbf{R}$, dans les autres cas, elle n'est pas incluse dans $\mathbf{R}$.

– L'anneau $K[\varepsilon]/(\varepsilon^2)$ des *nombres duaux*, où K est un corps; ε est alors l'analogue algébrique d'un infiniment petit [36].

– L'anneau $\mathbf{C}[X,Y]/(DY^2-(X^3-X))$ des fonctions rationnelles sur la courbe algébrique C_D d'équation $DY^2 = X^3 - X$ dans $\mathbf{C}^2$ (si $f \in \mathbf{C}[X,Y]$, la restriction de f à C_D ne dépend que de l'image de f modulo l'idéal engendré par $P(X,Y) = DY^2 - (X^3-X)$, puisque P est identiquement nul sur C_D).

Exercice 2.10. — Montrer que, si D' est un diviseur de D, alors $\mathbf{Z}/D'\mathbf{Z}$ est le quotient de $\mathbf{Z}/D\mathbf{Z}$ par l'idéal engendré par D'.

2.10.2. *Idéal premier, idéal maximal*

Rappelons qu'un anneau A est *intègre* s'il n'est pas réduit à 0 (i.e. si $0 \neq 1$ dans A), et s'il ne possède pas de *diviseur de* 0 (i.e. $xy = 0 \Rightarrow x = 0$ ou $y = 0$). Un idéal I de A est dit *premier* si l'anneau A/I est intègre, ce qui équivaut, en remontant dans A, à « $I \neq A$ et $xy \in I \Rightarrow x \in I$ ou $y \in I$ ». En particulier, l'*idéal nul* $\{0\}$ est premier si et seulement si A est intègre.

• Si I est un idéal de A, distinct de A, les conditions suivantes sont équivalentes (I est dit *maximal* s'il les satisfait) :

(i) A/I est un corps.

(ii) Si $x \in A - I$, l'idéal engendré par I et x contient 1.

(iii) Les seuls idéaux de A contenant I, sont A et I.

Si I vérifie (iii) et si $x \notin I$, alors l'idéal engendré par I et x contient strictement I et donc est égal à A; en particulier, il contient 1, ce qui démontre l'implication (iii)⇒(ii).

34. Cette définition de $\mathbf{C}$ est due à Cauchy (1847).

35. De manière générale, si A est un anneau, et si a est un élément de A, on note souvent (a) l'idéal de A engendré par A; on a donc $(a) = a\mathrm{A}$.

36. On peut difficilement faire plus petit puisque $\varepsilon \neq 0$, alors que $\varepsilon^2 = 0$; si $P \in K[X]$ est un polynôme, on a $P(X+\varepsilon) = P(X) + P'(X)\varepsilon$ dans $K[\varepsilon]/(\varepsilon^2)$, comme le montre la formule de Taylor pour les polynômes. Peut-on rêver de développements limités plus sympathiques ?

Si I vérifie (ii), et si $x \notin \mathrm{I}$, alors il existe $b \in \mathrm{I}$ et $u \in \mathrm{A}$ tels que $b+ux = 1$. On en déduit que x est inversible dans A/I d'inverse u, et donc que tout élément non nul de A/I est inversible ; autrement dit, A/I est un corps. D'où l'implication (ii)⇒(i).

Enfin, si A/I est un corps, et si J est un idéal de A contenant I, alors J/I est un idéal de A/I, et donc est soit réduit à 0 (ce qui implique J = I), soit égal à A/I (ce qui implique J = A). On en déduit l'implication (i)⇒(iii), ce qui permet de conclure.

• Un corps étant intègre, un idéal maximal est premier, mais la réciproque est fausse. Par exemple, l'idéal (X) de $\mathbf{Z}[\mathrm{X}]$ est premier puisque $\mathbf{Z}[\mathrm{X}]/(\mathrm{X}) = \mathbf{Z}$ est intègre, mais il n'est pas maximal puisque $\mathbf{Z}$ n'est pas un corps.

2.11. Groupes quotients

2.11.1. *Groupe opérant sur un ensemble.* — Soit G un groupe d'élément neutre 1, et soit X un ensemble. On dit que G *opère à gauche* sur X ou que l'on a une *action à gauche de* G *sur* X si on dispose d'une application $(g, x) \mapsto g \cdot x$ de $\mathrm{G} \times \mathrm{X}$ dans X telle que $1 \cdot x = x$, quel que soit $x \in \mathrm{X}$, et $g \cdot (g' \cdot x) = gg' \cdot x$, quels que soient $g, g' \in \mathrm{G}$ et $x \in \mathrm{X}$. On remarquera que si $g \in \mathrm{G}$, alors $x \mapsto \sigma_g(x) = g \cdot x$ est une bijection de X dans X, la bijection réciproque étant $x \mapsto \sigma_{g^{-1}}(x) = g^{-1} \cdot x$, et que l'on a $\sigma_{gg'} = \sigma_g \circ \sigma_{g'}$, quels que soient $g, g' \in \mathrm{G}$. Définir une action de G sur X revient donc à se donner un morphisme de G dans le groupe des *permutations* de X (i.e. les bijections de X dans X) muni de la composition.

On dit que G *opère à droite* sur X si on a une application $(g, x) \mapsto x \star g$ de $\mathrm{G} \times \mathrm{X}$ dans X telle que $x \star 1 = x$, quel que soit $x \in \mathrm{X}$, et $(x \star g) \star g' = x \star gg'$, quels que soient $g, g' \in \mathrm{G}$ et $x \in \mathrm{X}$. On peut toujours transformer une action à gauche en action à droite (et vice-versa), en posant $x \star g = g^{-1} \cdot x$.

Par exemple, si K est un corps commutatif, le groupe $\mathbf{GL}_n(\mathrm{K})$ opère naturellement (à gauche) sur beaucoup d'objets :
— par définition, il opère sur l'espace vectoriel K^n ;
— comme l'action est linéaire, elle transforme une droite vectorielle en droite vectorielle et donc $\mathbf{GL}_n(\mathrm{K})$ opère sur l'ensemble $\mathbf{P}^{n-1}(\mathrm{K})$ des droites vectorielles de K^n (*espace projectif* de dimension $n-1$ sur K) ;
— il opère sur l'ensemble $\mathbf{M}_n(\mathrm{K})$ des matrices $n \times n$ à coefficients dans K, par multiplication à gauche (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}$), par multiplication à droite (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{MA}^{-1}$) et par *similitude* (i.e. $\mathrm{A} \cdot \mathrm{M} = \mathrm{AMA}^{-1}$, ce qui correspond à un changement de base).
— Il opère sur les ensembles des matrices symétriques et antisymétriques par $\mathrm{A} \cdot \mathrm{M} = \mathrm{AM}\,{}^t\mathrm{A}$,
— Le groupe $\mathbf{GL}_n(\mathbf{C})$ opère sur l'ensemble des matrices auto-adjointes (i.e. vérifiant ${}^t\mathrm{M} = \overline{\mathrm{M}}$) par $\mathrm{A} \cdot \mathrm{M} = \mathrm{AMA}^*$, avec $\mathrm{A}^* = {}^t\overline{\mathrm{A}}$.

Exercice 2.11. — Soit K un corps commutatif. On rajoute à K un élément ∞, et on étend l'arithmétique de K en posant $\frac{a}{0} = \infty$, si $a \neq 0$ (on ne donne pas de sens à $\frac{0}{0}$), et $\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$, si $a \neq 0$ ou $c \neq 0$.

(i) Montrer que l'application qui à $v = (x, y) \in \mathrm{K}^2 - \{(0,0)\}$ associe $\lambda(v) = \frac{x}{y} \in \mathrm{K} \cup \{\infty\}$ induit une bijection de la droite projective $\mathbf{P}^1(\mathrm{K})$, ensemble des droites vectorielles de K^2, sur $\mathrm{K} \cup \{\infty\}$.

(ii) Montrer que l'action de $\mathbf{GL}_2(\mathrm{K})$ sur $\mathrm{K} \cup \{\infty\}$ qui s'en déduit est donnée par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}$.

Si G opère (à gauche ou à droite) sur X, et si $x \in X$, un *translaté* de x est un point de X dans l'image de $G \times \{x\}$, et *l'orbite* O_x de x est l'ensemble des translatés de X (i.e. l'image de $G \times \{x\}$ dans X). Une *orbite* pour l'action de G est un sous-ensemble O de X de la forme O_x pour un certain $x \in X$.

• La relation $\sim_G$ définie sur X par « $x \sim_G y$ si et seulement si il existe $g \in G$ tel que $y = g \cdot x$ (si l'action est à gauche) ou $y = x \star g$ (si l'action est à droite) » est une relation d'équivalence sur X dont les classes d'équivalence sont les orbites.

On peut se contenter de traiter le cas d'une action à gauche. On a $x = 1 \cdot x$, et donc $\sim_G$ est reflexive. Si $y = g \cdot x$, alors $x = g^{-1} \cdot y$, et donc $\sim_G$ est symétrique. Enfin, si $y = g \cdot x$ et $z = h \cdot y$, alors $z = hg \cdot x$, et donc $\sim_G$ est transitive. Cela prouve que $\sim_G$ est une relation d'équivalence sur X. La classe d'équivalence de x est O_x par définition de O_x, ce qui prouve que les classes d'équivalence sont les orbites.

L'espace quotient $X/\sim_G$, ensemble des orbites, est traditionnellement noté $G\backslash X$ si l'action est à gauche, et X/G si l'action est à droite. On dit que G *agit transitivement* sur X s'il n'y a qu'une orbite. Un système de représentants de $G\backslash X$ ou X/G dans X est parfois appelé un *domaine fondamental*.

• Si $x \in X$, l'ensemble G_x des $g \in G$ fixant x (i.e. $g \cdot x = x$) est un sous-groupe de G, appelé *stabilisateur* de x.

Comme $1 \cdot x = x$, on a $1 \in G_x$. Si $g \cdot x = x$, alors $x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, et donc G_x est stable par passage à l'inverse. Enfin, si $g \cdot x = x$ et $h \cdot x = x$, alors $gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, ce qui prouve que G_x est stable par la loi de groupe de G, et donc est un sous-groupe de G.

On fabrique des tas de groupes intéressants en considérant les stabilisateurs d'éléments d'ensembles munis d'actions de groupes.
— Si M est une matrice symétrique, le stabilisateur de M dans $\mathbf{GL}_n(K)$ pour l'action $A \cdot M = AM\,{}^tA$ est le *groupe orthogonal* associé à M ; si $M = I_n$, ce groupe est noté $\mathbf{O}_n(K)$. Si $K = \mathbf{R}$, si $p + q = n$, et si M est la matrice diagonale avec p fois 1 et q fois -1 sur la diagonale, le groupe obtenu est noté $\mathbf{O}(p, q)$; en particulier $\mathbf{O}(n) = \mathbf{O}_n(\mathbf{R})$.
— Si M est une matrice antisymétrique, le stabilisateur de M dans $\mathbf{GL}_n(K)$ pour l'action $A \cdot M = AM\,{}^tA$ est le *groupe symplectique* associé à M ; si $n = 2m$ est pair, et si M est la matrice par bloc $\left(\begin{smallmatrix} 0 & I_m \\ -I_m & 0 \end{smallmatrix}\right)$, ce groupe est noté $\mathbf{Sp}_n(K)$.
— Le stabilisateur de I_n pour l'action $A \cdot M = AMA^*$ de $\mathbf{GL}_n(\mathbf{C})$ est le *groupe unitaire* $\mathbf{U}(n)$.

Exercice 2.12. — Montrer que, si $y = g \cdot x$, alors $G_y = gG_xg^{-1} = \{gxg^{-1},\ x \in G_x\}$. En déduire que, si G est fini, le cardinal du stabilisateur est constant dans chaque orbite.

Exercice 2.13. — (i) Montrer que le groupe D_4 des isométries du carré de sommets $A = (1, 1)$, $B = (-1, 1)$, $C = (-1, -1)$ et $D = (1, -1)$ est un groupe d'ordre 8, et expliciter ses éléments.

(ii) Soit $O = (0, 0)$, et soit $S = \{O, A, B, C, D\}$. Montrer que S est stable sous l'action de D_4, et déterminer les orbites sous l'action de D_4, ainsi que le stabilisateur d'un des éléments de chaque orbite.

(iii) Soit T l'ensemble des paires d'éléments distincts de S. Déterminer les orbites de T sous l'action de D_4, ainsi que le stabilisateur d'un élément de chaque orbite.

(iv) Quel lien y a-t-il entre le cardinal d'une orbite et celui du stabilisateur dans tous les cas ci-dessus ?

2.11.2. *Classes de conjugaison*

• Si G est un groupe, alors $(g, x) \mapsto g \cdot x = gxg^{-1}$ est une action (à gauche) de G sur lui-même.

Si $g, h, x \in \mathrm{G}$, alors $gh \cdot x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g \cdot (hxh^{-1}) = g \cdot (h \cdot x)$.

L'action de G sur lui-même ainsi définie est l'action *par conjugaison*. L'orbite de $x \in \mathrm{G}$ est alors la *classe de conjugaison de* x, les éléments de la classe de conjugaison de x sont dits *conjugués à* x (et donc x et y *sont conjugués* dans G s'il existe $h \in \mathrm{G}$ tel que $y = hxh^{-1}$), et l'ensemble Conj(G) des orbites est *l'ensemble des classes de conjugaison de* G. Le stabilisateur Z_x de x pour cette action est appelé le *centralisateur* de x ; c'est l'ensemble des $g \in \mathrm{G}$ qui commutent à x.

• G est commutatif si et seulement si les classes de conjugaison sont réduites à un élément.

La classe de conjugaison de $x \in \mathrm{G}$ est l'ensemble des gxg^{-1}, pour $g \in \mathrm{G}$. Comme elle contient x, elle est réduite à un élément si et seulement si $gxg^{-1} = x$, quel que soit $g \in \mathrm{G}$, et donc si et seulement si x commute à tous les éléments de G. Ceci permet de conclure.

• Le *centre* Z de G est l'ensemble des $x \in \mathrm{G}$ commutant à tout élément de G ; c'est aussi l'ensemble des $x \in \mathrm{G}$ dont la classe de conjugaison est réduite à un point, et c'est un sous-groupe de G.

Si $xg = gx$ et $yg = gy$ quel que soit $g \in \mathrm{G}$, alors $xyg = xgy = gxy$, ce qui montre que xy commute à tous les éléments de G et donc que Z est stable par la loi de groupe. De même, si $xg = gx$ quel que soit $g \in \mathrm{G}$, alors $gx^{-1} = x^{-1}xgx^{-1} = x^{-1}gxx^{-1} = x^{-1}g$, ce qui prouve que Z est stable par passage à l'inverse. Comme il contient l'élément neutre ; c'est un sous-groupe de G. Le reste ayant été démontré ci-dessus, cela permet de conclure.

Exercice 2.14. — (i) Soient X un ensemble et G un groupe opérant sur X. Si $g \in \mathrm{G}$, on note X_g l'ensemble $\{x \in \mathrm{X},\ g \cdot x = x\}$ des points fixes de g.

(a) Si $g, h \in \mathrm{G}$, quel lien y a-t-il entre les points fixes de g et ceux de hgh^{-1} ?

(b) Montrer que si X est fini et si g, g' sont conjugués dans G, alors ils ont le même nombre de points fixes.

(ii) Soient V un espace vectoriel sur un corps K et G un groupe. On dit que G *opère linéairement* sur V si G opère sur V et si $v \mapsto g \cdot v$ est une application linéaire de V dans V, pour tout $g \in \mathrm{G}$ (on dit alors que V est une *représentation* de G).

(a) Montrer que, si c'est le cas et si $g \in \mathrm{G}$, l'ensemble des points fixes de g est un sous-espace espace vectoriel de V.

(b) Montrer que, si V est de dimension finie et si g, g' sont conjugués dans G, alors leurs points fixes sont des espaces vectoriels de même dimension.

2.11.3. *Quotients de groupes.* — Si G est un groupe, et si H est un sous-groupe de G, on peut utiliser la multiplication dans G pour faire agir H sur G à gauche ($h \cdot x = hx$) et à droite ($x \star h = xh$). Une classe à gauche est alors de la forme $\mathrm{H}x = \{hx,\ h \in \mathrm{H}\}$, pour $x \in \mathrm{G}$, et une classe à droite, de la forme $x\mathrm{H} = \{xh,\ h \in \mathrm{H}\}$, pour $x \in \mathrm{G}$. Les quotients $\mathrm{H}\backslash\mathrm{G}$ (à gauche) et G/H (à droite) de G par H ne sont, en général, pas des groupes, mais la multiplication dans G les munit d'actions de G (à droite pour $\mathrm{H}\backslash\mathrm{G}$ et à

gauche pour G/H). Réciproquement, si R est une relation d'équivalence sur G telle que la multiplication dans G induise une action à gauche (resp. à droite) de G sur G/R, et si H est la classe d'équivalence de e, alors H est un sous-groupe de G et G/R = G/H (resp. G/R = H\G).

• Si G opère (à gauche) sur un ensemble X, si $x \in X$, et si G_x est le stabilisateur de x dans G, alors $g \mapsto g \cdot x$ induit un isomorphisme de G/G_x sur l'orbite O_x de x (c'est un isomorphisme de G-*ensembles*, i.e. d'ensembles munis d'une action de G).

Commençons par remarquer que, si g_1, g_2 ont même image dans G/G_x, alors il existe $h \in G_x$ tel que $g_2 = g_1 h$, ce qui implique que $g_2 \cdot x = (g_1 h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x$; l'application $g \mapsto g \cdot x$ passe donc au quotient et nous définit une application $\iota : G/G_x \to O_x$ qui est surjective par définition de O_x. Maintenant, si $g_1 \cdot x = g_2 \cdot x$, alors $g_2^{-1} g_1 \cdot x = x$ et donc $g_2^{-1} g_1 \in G_x$; on en déduit que $g_1 \in g_2 G_x$ et donc que g_1 et g_2 ont même image dans G/G_x, ce qui prouve que ι est injective et donc bijective. Enfin, si $h \in G$ et $g \in G/G_x$, alors $h \cdot \iota(g) = h \cdot (g \cdot x) = hg \cdot x = \iota(hg)$, ce qui prouve que ι commute à l'action de G et donc est un morphisme de G-ensembles.

• La classe de conjugaison de x est isomorphe à G/Z_x, où Z_x est le centralisateur de x.

C'est un cas particulier du point précédent.

Pour que la structure de groupe de G passe au quotient G/H, il faut et il suffit que, quels que soient $x, x' \in G$ et $h, h' \in H$, on puisse trouver $h'' \in H$ tel que $xhx'h' = xx'h''$. Comme $h''(h')^{-1} = (x')^{-1} h x'$, on voit que la condition précédente est équivalente à ce que H soit laissé stable par la conjugaison $h \mapsto ghg^{-1}$, quel que soit $g \in G$. Si tel est le cas on dit que H est *distingué* (*normal* en "franglais") dans G.

Un *groupe simple* est un groupe dont les seuls sous-groupes distingués sont $\{1\}$ et le groupe lui-même.

• Le groupe G/H vérifie la propriété universelle suivante : si $f : G \to G'$ est un morphisme de groupes, et si $\operatorname{Ker} f$ contient H, alors f se factorise à travers G/H (i.e. il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$, tel que $f = \overline{f} \circ \pi$, où $\pi : G \to G/H$ est la projection canonique).

• Si $u : G \to G'$ est un morphisme de groupes, alors $\operatorname{Ker} u$ est distingué dans G et u se factorise à travers $G/\operatorname{Ker} u$ et induit un isomorphisme de groupes de $G/\operatorname{Ker} u$ sur $\operatorname{Im} u$. Si G est simple, alors u est soit injectif soit trivial ($u(g) = 1$, quel que soit $g \in G$).

3. Groupes finis

3.1. Groupes cycliques

3.1.1. *Structure des groupes cycliques, ordre d'un élément*

Si G est un groupe d'élément neutre 1 et si $x \in G$, on définit x^n, pour $n \in \mathbf{Z}$, en posant $x^0 = 1$, et $x^{n+1} = x^n x$, si $n \in \mathbf{N}$, et $x^n = (x^{-1})^{-n}$, si $n \leqslant 0$. On vérifie facilement que si $n \in \mathbf{Z}$, alors $x^{n+1} = x^n x$ et $x^{n-1} = x^n x^{-1}$, ce qui permet de montrer, par récurrence sur m, que $x^{m+n} = x^m x^n$ quels que soient $m, n \in \mathbf{N}$. Autrement dit, $n \mapsto x^n$ *est un*

morphisme de groupes de $\mathbf{Z}$ *dans* G. Si x et y commutent, on a $(xy)^n = x^n y^n$, mais s'ils ne commutent pas, c'est en général faux (et si $n = 2$ ou si $n = -1$, cela n'est vrai que si x et y commutent).

Si G est commutatif et si la loi est notée $+$, l'élément x^n est noté nx, et on a $0x = 0$ et $(-1)x = -x$.

• Si $x \in \mathrm{G}$, le sous-groupe $\langle x \rangle$ engendré par x est l'ensemble des x^n, pour $n \in \mathbf{Z}$.

> En effet, d'une part un sous-groupe qui contient x contient x^n, pour $n \in \mathbf{N}$, comme le montre une récurrence immédiate, et comme il contient x^{-1}, il contient aussi x^n, pour $n \leqslant 0$; d'autre part, l'ensemble des x^n, pour $n \in \mathbf{Z}$, est un groupe qui contient x, puisque c'est l'image de $\mathbf{Z}$ par le morphisme $x \mapsto x^n$.

Un groupe est *cyclique* s'il peut être engendré par un seul élément. Autrement dit, G est cyclique, s'il existe $x \in \mathrm{G}$ tel que le morphisme $x \mapsto x^n$ de $\mathbf{Z}$ dans G soit surjectif. Si G est cyclique, un *générateur* de G est un élément x de G tel que le morphisme $x \mapsto x^n$ de $\mathbf{Z}$ dans G soit surjectif.

• Le groupe $\mathbf{Z}$ est cyclique, et il admet deux générateurs 1 et -1. Si $\mathrm{D} \geqslant 1$, le groupe $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est cyclique et les générateurs de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sont les éléments de $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$, c'est-à-dire les (réductions modulo D des) entiers premiers à D.

> L'énoncé concernant $\mathbf{Z}$ est immédiat. Il est aussi immédiat que $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est cyclique et que 1 en est un générateur. Maintenant, si $a \in \mathbf{Z}/\mathrm{D}\mathbf{Z}$ en est un générateur, alors il existe en particulier $b \in \mathbf{Z}$ tel que $ba = 1$, ce qui fait que la réduction modulo D de b est un inverse de a, et donc que a est inversible. Réciproquement, si a est inversible, alors $n \mapsto na$ est bijectif de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ et donc $n \mapsto na$ est surjectif de $\mathbf{Z}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, ce qui prouve que a est un générateur de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

• Le groupe $\boldsymbol{\mu}_\mathrm{D}$ des racines D-ièmes de l'unité dans $\mathbf{C}$ est cyclique, engendré par $e^{2i\pi/\mathrm{D}}$, et $n \mapsto e^{2i\pi\, n/\mathrm{D}}$ induit un isomorphisme de groupes $\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \boldsymbol{\mu}_\mathrm{D}$. Un générateur de $\boldsymbol{\mu}_\mathrm{D}$ est une *racine primitive* D*-ième de l'unité*, et les racines primitives D-ièmes de l'unité sont, d'après le point précédent, les racines de la forme $e^{2i\pi\, a/\mathrm{D}}$, pour a premier à D.

• Un groupe cyclique infini est isomorphe à $\mathbf{Z}$; un groupe cyclique de cardinal D est isomorphe [37] à $\mathbf{Z}/\mathrm{D}\mathbf{Z}$. En particulier, un groupe cyclique est commutatif.

---

37. Un groupe cyclique est donc un objet parfaitement ennuyeux d'un point de vue théorique. La situation est, en pratique, assez différente : il est très difficile, étant donné un groupe cyclique G de cardinal N très grand ($\sim 10^{100}$), un générateur g de G et $x \in \mathrm{G}$, de déterminer l'élément n de $\mathbf{Z}/\mathrm{N}\mathbf{Z}$ tel que $x = g^n$ (problème du *logarithme discret*), alors que calculer g^n se fait sans problème. Ceci est à la base des signatures électroniques : G, N et g sont publics et on attribue à chaque personne P un code $n(\mathrm{P}) \in \mathbf{Z}/\mathrm{N}\mathbf{Z}$ (tenu secret), à partir duquel P fabrique une signature publique $s(\mathrm{P}) = g^{n(\mathrm{P})}$. Deux personnes P et Q peuvent s'assurer de leur identité mutuelle de la manière suivante : P calcule $s(\mathrm{Q})^{n(\mathrm{P})}$ et Q calcule $s(\mathrm{P})^{n(\mathrm{Q})}$, chacun de son côté ; si les résultats sont les mêmes (à savoir $g^{n(\mathrm{P})n(\mathrm{Q})}$), alors P et Q sont bien P et Q (sinon, cela veut dire que quelqu'un a réussi à retrouver le code de l'un des deux à partir de sa signature publique, ce qui est réputé être impossible). Les groupes cycliques utilisés sont en général construits à partir de courbes elliptiques sur les corps finis (cf. annexe F).

Soit G un groupe cyclique, et soit x un générateur de G. Alors $f : \mathbf{Z} \to \mathrm{G}$ défini par $f(n) = x^n$ est un morphisme surjectif, et il y a deux cas :
— f est injectif et alors G est isomorphe à $\mathbf{Z}$;
— le noyau de f est non nul et donc de la forme $\mathrm{D}\mathbf{Z}$, avec $\mathrm{D} \geqslant 1$, puisque c'est un sous-groupe de $\mathbf{Z}$; alors f se factorise à travers $\overline{f} : \mathbf{Z}/\mathrm{D}\mathbf{Z} \to \mathrm{G}$, et $\overline{f}$ est surjectif puisque f l'est et injectif puisqu'on a factorisé modulo $\mathrm{Ker}\, f$; autrement dit $\overline{f}$ est un isomorphisme de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sur G et, en particulier, G et $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ ont même cardinal.
Ceci permet de conclure.

• Si G est un groupe quelconque et $x \in \mathrm{G}$, le sous-groupe $\langle x \rangle$ de G engendré par x est cyclique par définition. On définit *l'ordre de* x comme le cardinal du groupe $\langle x \rangle$. Si x est d'ordre D, le noyau du morphisme $n \to x^n$ de $\mathbf{Z}$ dans G est $\mathrm{D}\mathbf{Z}$ d'après ce qui précède, et *l'ordre de* x *est aussi le plus petit entier* $n > 0$ *tel que* x^n *soit égal à l'élément neutre.*

3.1.2. *Sous-groupes des groupes cycliques*

• Si $\mathrm{D} \geqslant 1$, l'application $d \mapsto d\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est une bijection de l'ensemble des diviseurs de D sur celui des sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$.

Si G est un sous-groupe de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, on peut considérer son image inverse dans $\mathbf{Z}$, qui est un sous-groupe de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$; on obtient ainsi une bijection de l'ensemble des sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dans celui des sous-groupes de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$, la bijection inverse étant $\tilde{\mathrm{G}} \to \tilde{\mathrm{G}}/\mathrm{D}\mathbf{Z}$. Comme un sous-groupe de $\mathbf{Z}$ contenant $\mathrm{D}\mathbf{Z}$ est de la forme $d\mathbf{Z}$, avec d diviseur de D, cela permet de conclure.

• Si G est un groupe cyclique, tous les sous-groupes de G sont cycliques, et si G est de cardinal D, alors G admet exactement un sous-groupe de cardinal D′, pour tout diviseur D′ de D.

Si G est infini, alors G est isomorphe à $\mathbf{Z}$, et tous les sous-groupes non nuls de G sont isomorphes à $\mathbf{Z}$, et donc cycliques.

Si G est fini de cardinal D, alors G est isomorphe à $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, et on sait que les sous-groupes de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ sont de la forme $d\mathbf{Z}/\mathrm{D}\mathbf{Z}$, pour d diviseur de D. Or $n \mapsto dn$ induit une surjection de $\mathbf{Z}$ sur $d\mathbf{Z}/\mathrm{D}\mathbf{Z}$ dont le noyau est $\mathrm{D}'\mathbf{Z}$, où $\mathrm{D}' = \mathrm{D}/d$, ce qui montre que $d\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \mathbf{Z}/\mathrm{D}'\mathbf{Z}$. Comme $d \mapsto \mathrm{D}' = \mathrm{D}/d$ est une permutation de l'ensemble des diviseurs de D, cela permet de conclure.

3.2. Groupes abéliens finis

Soit $\mathscr{P}$ l'ensemble des nombres premiers. D'après le théorème des restes chinois, si $\mathrm{D} \in \mathbf{N} - \{0\}$, alors $\mathbf{Z}/\mathrm{D}\mathbf{Z} \cong \oplus_{p \in \mathscr{P}}(\mathbf{Z}/p^{v_p(\mathrm{D})}\mathbf{Z})$. La somme ci-dessus est en fait une somme finie car $v_p(\mathrm{D}) = 0$, sauf pour un nombre fini de nombres premiers. Ce résultat se généralise à tous les groupes abéliens finis sous la forme (cf. n° 10.3 du § 10 pour la démonstration).

Théorème 3.1. — (Kronecker, 1867) *Soit* G *un groupe abélien fini et, si* $p \in \mathscr{P}$*, soit* G_p *l'ensemble des éléments de* G *d'ordre une puissance de* p*.*

(i) G_p *est un sous-groupe de* G*, nul pour presque tout* p*, et* $\mathrm{G} = \oplus_{p \in \mathscr{P}} \mathrm{G}_p$*.*

(ii) *Si $p \in \mathscr{P}$, il existe une suite finie d'entiers $a_{p,i} \geqslant 1$, décroissante et uniquement déterminée, telle que l'on ait* $\mathrm{G}_p \cong \oplus_i (\mathbf{Z}/p^{a_{p,i}}\mathbf{Z})$.

Remarque 3.2. — Avec les notations du théorème, $|\mathrm{G}| = \prod_p \prod_i p^{a_i}$, et donc $|\mathrm{G}|$ est un multiple de p^{a_i}, pour tous p et i, ce qui prouve que la multiplication par $|\mathrm{G}|$ annule tout élément de G, puisqu'elle annule tous les $\mathbf{Z}/p^{a_{p,i}}\mathbf{Z}$. Autrement dit, dans un groupe commutatif, l'ordre d'un élément divise l'ordre du groupe (cas particulier du th. de Lagrange).

Exercice 3.3. — Décomposer $(\mathbf{Z}/108\mathbf{Z})^*$ et $(\mathbf{Z}/200\mathbf{Z})^*$ sous la forme ci-dessus.

Exercice 3.4. — (i) Soit K un corps fini commutatif[38]. Montrer que le groupe K^* est cyclique (on pourra considérer le nombre de solutions de l'équation $x^p = 1$, pour p premier divisant $|\mathrm{K}^*|$ et utiliser le th. 3.1).

(ii) Soit $p \neq 2$ un nombre premier. Montrer que x est un carré dans $\mathbf{F}_p^*$ (i.e. $x = y^2$, avec $y \in \mathbf{F}_p^*$) si et seulement si $x^{(p-1)/2} = 1$.

(iii) En déduire que -1 est un carré dans $\mathbf{F}_p^*$ si et seulement si p est de la forme $4n+1$.

(iv) Soit p de la forme $4n+3$. Montrer que l'équation $a^2 + b^2 = p$ n'a pas de solution avec $a, b \in \mathbf{Z}$.

Exercice 3.5. — (i) Soit p un nombre premier. Montrer que, si $x \equiv 1 + p^k a \bmod p^{k+1}$, et si $k \geqslant 1$ ($k \geqslant 2$, si $p = 2$), alors $x^p \equiv 1 + p^{k+1}a \bmod p^{k+2}$. En déduire que $(1+p)^{p^{n-2}} \neq 1$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, si $p \neq 2$ et $n \geqslant 2$, et que $(1+4)^{p^{n-3}} \neq 1$ dans $(\mathbf{Z}/2^n\mathbf{Z})^*$, si $n \geqslant 3$.

(ii) Soit N le noyau de la réduction modulo p de $(\mathbf{Z}/p^n\mathbf{Z})^*$ dans $\mathbf{F}_p^*$ (dans $(\mathbf{Z}/4\mathbf{Z})^*$, si $p = 2$). Montrer que N est isomorphe à $\mathbf{Z}/p^{n-1}\mathbf{Z}$ (à $\mathbf{Z}/2^{n-2}\mathbf{Z}$, si $p = 2$).

(iii) En utilisant le résultat de l'ex. 3.4, montrer que $(\mathbf{Z}/p^n\mathbf{Z})^* \cong (\mathbf{Z}/(p-1)\mathbf{Z}) \oplus (\mathbf{Z}/p^{n-1}\mathbf{Z})$ en tant que groupe commutatif, si $p \neq 2$ et $n \geqslant 1$.

(iv) Montrer que $(\mathbf{Z}/2^n\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2^{n-2}\mathbf{Z})$, si $n \geqslant 2$.

3.3. Le théorème de Lagrange et ses variantes

Si G est un groupe fini, et si H est un sous-groupe de G, alors $h \mapsto xh$ induit une bijection de H sur xH, ce qui fait que les classes à droite xH ont toutes le même cardinal $|\mathrm{H}|$. Comme G est la réunion disjointe des xH, pour $x \in \mathrm{G}/\mathrm{H}$, on en déduit la formule

$$|\mathrm{G}| = |\mathrm{G}/\mathrm{H}| \cdot |\mathrm{H}|.$$

En particulier, $|\mathrm{H}|$ divise $|\mathrm{G}|$, ce qui se traduit par :

• Si G est un groupe fini, alors le cardinal de tout sous-groupe de G divise celui de G (th. de Lagrange).

On peut spécialiser cela au sous-groupe engendré par un élément x de G : le cardinal de ce sous-groupe est, par définition, l'ordre de x, ce qui nous donne :

• Dans un groupe fini l'ordre d'un élément divise le cardinal du groupe.

Enfin, $|\mathrm{G}/\mathrm{H}|$ divise aussi $|\mathrm{G}|$. Si X est un ensemble sur lequel G agit, si O est une orbite, si $x \in \mathrm{O}$, et si H est le stabilisateur de x, on sait que $\mathrm{O} \cong \mathrm{G}/\mathrm{H}$. On en déduit que :

• Dans un ensemble sur lequel agit un groupe fini, le cardinal d'une orbite divise le cardinal

38. Cette hypothèse est en fait superflue car tout corps fini est commutatif (théorème de Wedderburn).

du groupe et, plus précisément, le produit du cardinal de l'orbite par celui du stabilisateur d'un de ses éléments est égal au cardinal du groupe.

En particulier, en appliquant ceci à l'action de G sur lui-même par conjugaison intérieure, on obtient :

• Dans un groupe fini, le cardinal d'une classe de conjugaison divise le cardinal du groupe.

• Si X est un ensemble fini sur lequel agit un groupe fini G, on peut découper X en orbites pour cette action. Si on choisit un élément par orbite, et si on utilise l'isomorphisme $\mathrm{O}_x \cong \mathrm{G}/\mathrm{G}_x$, où G_x est le stabilisateur de x, on obtient la *formule des classes* :

$$|\mathrm{X}| = \sum_{x \in \mathrm{G}\backslash\mathrm{X}} |\mathrm{O}_x| = |\mathrm{G}| \cdot \sum_{x \in \mathrm{G}\backslash\mathrm{X}} \frac{1}{|\mathrm{G}_x|}.$$

Exercice 3.6. — Montrer que tout élément $x \in \mathbf{F}_p^*$ vérifie $x^{p-1} = 1$. En déduire le petit théorème de Fermat [39] (si $n \in \mathbf{Z}$, alors $n^p - n$ est divisible [40] par p).

Exercice 3.7. — (démonstration combinatoire du petit th. de Fermat). Soient $n \geqslant 1$ et X l'ensemble des applications de $\mathbf{Z}/p\mathbf{Z}$ dans $\{1, \ldots, n\}$. Si $g \in \mathbf{Z}/p\mathbf{Z}$ et $\phi \in \mathrm{X}$, on définit $g \cdot \phi$ par $(g \cdot \phi)(x) = \phi(x + g)$, pour tout $x \in \mathbf{Z}/p\mathbf{Z}$ (la loi de groupe de $\mathbf{Z}/p\mathbf{Z}$ est notée additivement).

(i) Vérifier que ceci définit une action de groupe.

(ii) Quels sont les points fixes de cette action ? Combien y en a-t-il ?

(iii) Combien d'éléments a une orbite non réduite à un point ?

(iv) Calculer le nombre de ces orbites, et en déduire le petit théorème de Fermat.

3.4. Le groupe symétrique S_n

3.4.1. *Permutations*

Si $n \in \mathbf{N} - \{0\}$, on note S_n le groupe des bijections de $\{1, \ldots, n\}$. Comme il y a n manières de choisir l'image de 1, $n-1$ de choisir celle de 2 une fois celle de 1 choisie, etc. le cardinal de S_n est $n(n-1)\cdots 1 = n!$. Par définition, S_n opère sur $\{1, \ldots, n\}$; il opère donc aussi sur toutes sortes d'objets construits à partir de $\{1, \ldots, n\}$ comme l'ensemble des parties de $\{1, \ldots, n\}$ (l'image d'une partie $\{i_1, \ldots, i_p\}$ par σ est $\{\sigma(i_1), \ldots, \sigma(i_p)\}$).

39. Énoncé dans une lettre à Frenicle du 18 octobre 1640.

40. Il n'y a pas de réciproque au petit théorème de Fermat : il existe des entiers n dit *de Carmichael* tels que $a^n - a$ soit divisible par n pour tout a, et qui ne sont pas premiers. Le résultat le plus proche est le test de primalité de Lucas (1876) généralisé par Lehmer (1927) : s'il existe $a \in \{2, \ldots, n-1\}$ tel que $a^{n-1} \equiv 1 \bmod n$ et $a^{(n-1)/p} \not\equiv 1 \bmod n$ pour tout diviseur premier p de $n-1$, alors n est premier. En effet, la première congruence montre que a est premier à n, et que son ordre m dans $(\mathbf{Z}/n\mathbf{Z})^*$ est un diviseur de $n-1$; les non congruences montrent $v_p(m) = v_p(n-1)$ pour tout premier p divisant $n-1$, et donc m est un multiple de $n-1$ et $m = n-1$. Comme $|(\mathbf{Z}/n\mathbf{Z})^*|$ est un multiple de l'ordre m de a et est $\leqslant n-1$, il en résulte que $|(\mathbf{Z}/n\mathbf{Z})^*| = n-1$ et donc n est premier. Prendre $a = 5$ suffit à prouver que $2^{1001}3^{1600} + 1$ est premier (les calculs prennent une poignée de secondes sur un ordinateur ; par contre pour un entier n quelconque, il faut d'abord factoriser $n-1$, ce qui est plus dur que de prouver que n est premier par d'autres méthodes).

Exercice 3.8. — On fait agir S_n sur l'ensemble des parties de $\{1,\dots,n\}$ comme ci-dessus.
(i) Si $p \leqslant n$, quelle est l'orbite de $\{1,\dots,p\}$?
(ii) Quel est le stabilisateur de $\{1,\dots,p\}$; quel est son cardinal ?
(iii) Retrouver la valeur $\frac{n!}{p!\,(n-p)!}$ pour le nombre de parties à p éléments d'un ensemble à n éléments.

Un élément de S_n est une *permutation*. Si $\sigma \in \mathrm{S}_n$, on définit le *support* de σ comme l'ensemble des $i \in \{1,\dots,n\}$ tels que $\sigma(i) \neq i$. Il est plus ou moins évident que *deux permutations de supports disjoints commutent entre elles*.

On peut représenter une permutation σ de S_n sous la forme d'une matrice à 2 lignes et n colonnes en mettant les nombres de 1 à n sur la première ligne et leurs images par σ juste en-dessous. Cette représentation est très commode pour faire le produit de deux permutations (en n'oubliant pas que c'est la matrice de droite qui agit en premier).

Par exemple, si σ et τ sont les permutations de S_6 définies par $\sigma(1)=2$, $\sigma(2)=4$, $\sigma(3)=5$, $\sigma(4)=6$, $\sigma(5)=1$ et $\sigma(6)=3$, et $\tau(1)=4$, $\tau(2)=2$, $\tau(3)=1$, $\tau(4)=6$, $\tau(5)=5$ et $\tau(6)=3$, alors

$$\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6\\2&4&5&6&1&3\end{smallmatrix}\right),\quad \tau = \left(\begin{smallmatrix}1&2&3&4&5&6\\4&2&1&6&5&3\end{smallmatrix}\right) \quad\text{et}\quad \sigma\tau = \left(\begin{smallmatrix}1&2&3&4&5&6\\2&4&5&6&1&3\end{smallmatrix}\right)\left(\begin{smallmatrix}1&2&3&4&5&6\\4&2&1&6&5&3\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3&4&5&6\\6&4&2&3&1&5\end{smallmatrix}\right).$$

Une permutation $\sigma \in \mathrm{S}_n$ est un *k-cycle* s'il existe $i_1,\dots,i_k$ distincts, tels que

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\dots,\ \sigma(i_k) = i_1, \quad \text{et } \sigma(j) = j, \text{ si } j \notin \{i_1,\dots,i_k\}.$$

On note $(i_1, i_2, \dots, i_k)$ le k-cycle défini ci-dessus ; son support est l'ensemble $\{i_1,\dots,i_k\}$; il est d'ordre k. On remarquera que le k-cycle $(i_1, i_2, \dots, i_k)$ est aussi égal au k-cycle $(i_a, i_{a+1}, \dots, i_{a+k-1})$, si on écrit les indices modulo k, et a est n'importe quel élément de $\mathbf{Z}/k\mathbf{Z}$. Pour rétablir une unicité de l'écriture, il suffit d'imposer que i_1 soit le plus petit élément de $\{i_1,\dots,i_k\}$. Il est commode d'étendre la notation ci-dessus aux « cycles de longueur 1 » (qui sont tous égaux à l'identité...).

- Si σ est un k-cycle, alors $\sigma^k = \mathrm{id}$.
- Une permutation peut s'écrire comme un produit de cycles de supports disjoints.

  Si σ est une permutation, on fabrique une partition de $\{1,\dots,n\}$ en prenant les orbites $\mathrm{O}_1,\dots,\mathrm{O}_s$ sous l'action de σ (i.e. sous l'action du sous-groupe cyclique de S_n engendré par σ). Si O_i est une de ces orbites, de cardinal k_i, on peut considérer le cycle $c_i = (a, \sigma(a), \dots, \sigma^{k_i-1}(a))$, où a est le plus petit élément de O_i ; c'est un cycle de longueur k_i et de support O_i, et σ est le produit des c_i, pour $i \in \{1,\dots,s\}$.

Comme des cycles ayant des supports deux à deux disjoints commutent entre eux, on peut faire le produit dans n'importe quel ordre dans la décomposition d'une permutation en cycles de supports disjoints.

Par exemple, soit $\sigma \in \mathrm{S}_6$ la permutation définie par : $\sigma(1)=3$, $\sigma(2)=2$, $\sigma(3)=5$, $\sigma(4)=6$, $\sigma(5)=1$ et $\sigma(6)=4$. Alors on a $\sigma = (1,3,5)(4,6)(2) = (4,6)(2)(1,3,5)$... Très souvent on omet les cycles de longueur 1 de la décomposition ; on écrit donc plutôt la permutation précédente sous la forme $\sigma = (1,3,5)(4,6)$ ou $\sigma = (4,6)(1,3,5)$.

- Tout élément de S_n est conjugué à un unique élément de la forme

$$(1,\dots,\ell_1)(\ell_1+1,\dots,\ell_1+\ell_2)\cdots(\ell_1+\cdots+\ell_{s-1}+1,\dots,\ell_1+\cdots+\ell_{s-1}+\ell_s),$$

où $(\ell_1, \dots, \ell_s)$ est une *partition* de n (i.e. une suite décroissante d'entiers $\geqslant 1$ dont la somme est n). Les classes de conjugaison de S_n sont donc en bijection naturelle avec les partitions de n.

Soit $\sigma \in \mathrm{S}_n$. La conjugaison $\sigma \mapsto \alpha\sigma\alpha^{-1}$ par un élément α de S_n transforme un k-cycle $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$, en le k-cycle $\alpha(i_1) \mapsto \alpha(i_2) \mapsto \cdots \mapsto \alpha(i_k) \mapsto \alpha(i_1)$. Les longueurs des cycles apparaissant dans les décompositions de deux permutations conjuguées sont donc les mêmes, ce qui implique l'unicité d'un conjugué de la forme voulue, puisque les ℓ_j sont les longueurs des cycles apparaissant dans la décomposition de σ rangées dans l'ordre décroissant. Écrivons donc σ comme un produit de cycles $\tau_1 \dots \tau_s$ à supports disjoints. Soit ℓ_j la longueur de τ_j. On a $\ell_1 + \cdots + \ell_s = n$, et quitte à permuter les τ_j, on peut supposer que $\ell_1 \geqslant \ell_2 \cdots \geqslant \ell_s$. On peut alors écrire τ_j sous la forme $\tau_j = (i_{\ell_1+\cdots+\ell_{j-1}+1}, \dots, i_{\ell_1+\cdots+\ell_{j-1}+\ell_j})$, et $k \mapsto i_k$ nous définit une permutation α de $\{1, \dots, n\}$, car les supports des τ_j forment une partition de $\{1, \dots, n\}$. Alors $\alpha^{-1}\sigma\alpha$ est un conjugué de σ de la forme voulue, ce qui permet de conclure.

• Un 2-cycle est appelé une *transposition*, et S_n est engendré par les transpositions ; plus précisément, tout élément de S_n est produit de moins de $n-1$ transpositions.

La démonstration se fait par récurrence sur n. Pour $n = 1$ (et $n = 2$), le résultat est immédiat. Si $n \geqslant 2$, et si $\sigma \in \mathrm{S}_n$ vérifie $\sigma(n) \neq n$, alors $\tau = (\sigma(n), n)$ est une transposition et $\tau\sigma$ fixe n, et donc peut être vu comme un élément de S_{n-1}. D'après l'hypothèse de récurrence, $\tau\sigma$ est un produit de moins de $n-2$ transpositions à support dans $\{1, \dots, n-1\}$, et donc $\sigma = \tau(\tau\sigma)$ est un produit de moins de $n-1$ transpositions. On en déduit le résultat, le cas $\sigma(n) = n$ se traitant directement.

Exercice 3.9. — Calculer $(1,2)(2,3)(3,4)(4,5)$ dans S_5.

Exercice 3.10. — Montrer que S_n est engendré par les transpositions $(1,2), (2,3), \dots, (n-1, n)$.

Exercice 3.11. — Soit $\sigma \in \mathrm{S}_n$ dont la décomposition en cycles disjoints est $\tau_1 \cdots \tau_s$, chaque τ_i étant de longueur ℓ_i. Quel est l'ordre de σ ?

Exercice 3.12. — (i) Combien y a-t-il de cycles de longueur k dans S_n.

(ii) Montrer que le nombre moyen de cycles dans la décomposition d'un éléments de S_n tend vers l'infini avec n. (On pourra se demander dans combien de permutations apparaît un cycle donné.)

Exercice 3.13. — (difficile mais très surprenant) Le DGAE voulant tester le niveau de compréhension des X a décidé de les mettre à l'épreuve. Pour ce faire, il réunit les 500 membres de la promotion dans l'amphi Poincaré et leur tient ce langage : « J'ai disposé dans l'amphi Arago vos 500 noms dans des casiers numérotés de 1 à 500, à raison d'un par casier. Je vais vous appeler un par un, et demander à chacun d'entre vous d'ouvrir des casiers un par un à la recherche de son nom puis de les refermer sans changer le contenu et de regagner sa chambre sans possibilité de communiquer quoi que ce soit à ses camarades restés dans l'amphi Poincaré. Si tout le monde trouve son nom dans les 250 premiers casiers qu'il a ouverts, vous pouvez partir en vacances. Si l'un d'entre vous ne trouve pas son nom, on recommence le jour suivant (et je change le contenu des casiers bien évidemment). Voilà, vous avez deux heures pour concevoir une stratégie. » Désespoir des X qui se rendent compte que chacun a une chance sur deux de tomber sur son nom, et qu'au total ils ont une chance sur 2^{500} de partir en vacances au bout d'un jour, et donc qu'ils ne partiront pas en vacances. Pourtant au bout d'un certain temps, l'un de nos X déclare : « pas de panique, avec un peu de discipline, on a 9 chances sur 10 de partir en vacances avant la fin de la semaine ». Saurez-vous retrouver son raisonnement ?

3.4.2. *Signature d'une permutation*

Si $\sigma \in \mathrm{S}_n$, on définit la *signature* $\mathrm{sign}(\sigma)$ de σ par la formule

$$\mathrm{sign}(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

• $\mathrm{sign} : \mathrm{S}_n \to \{\pm 1\}$ est un morphisme de groupes.

Si $\sigma, \tau \in \mathrm{S}_n$, on a

$$\mathrm{sign}(\sigma\tau) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} = \Big(\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \Big) \Big(\prod_{1 \leqslant i < j \leqslant n} \frac{\tau(i) - \tau(j)}{i - j} \Big).$$

Le second terme est égal à $\mathrm{sign}(\tau)$, et le premier à $\mathrm{sign}(\sigma)$ car $\frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}$, ce qui permet d'écrire le produit sous la forme $\prod_{1 \leqslant \tau(i) < \tau(j) \leqslant n} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} = \mathrm{sign}(\sigma)$.

• Si τ est un k-cycle, alors $\mathrm{sign}(\tau) = (-1)^{k-1}$.

On a $\mathrm{sign}(\alpha\sigma\alpha^{-1}) = \mathrm{sign}(\alpha)\mathrm{sign}(\sigma)\mathrm{sign}(\alpha)^{-1} = \mathrm{sign}(\sigma)$, ce qui prouve que la signature est invariante par conjugaison et donc que tous les k-cycles ont même signature. Cela permet de prendre $\tau = (n-1, n)$ pour calculer la signature d'une transposition. On a alors

$$\begin{aligned} \mathrm{sign}(\tau) =& \Big(\prod_{1 \leqslant i < j \leqslant n-2} \frac{\tau(i) - \tau(j)}{i - j} \Big) \Big(\prod_{i \leqslant n-2} \frac{\tau(i) - \tau(n-1)}{i - (n-1)} \Big) \Big(\prod_{i \leqslant n-2} \frac{\tau(i) - \tau(n)}{i - n} \Big) \cdot \frac{\tau(n-1) - \tau(n)}{(n-1) - n} \\ =& \Big(\prod_{i \leqslant n-2} \frac{i - n}{i - (n-1)} \Big) \Big(\prod_{i \leqslant n-2} \frac{i - (n-1)}{i - n} \Big) \cdot (-1) = -1, \end{aligned}$$

ce qui prouve le résultat pour une transposition. Maintenant, le k-cycle $\sigma_k = (i_1, \ldots, i_k)$ est le produit des transpositions $(i_1, i_2) \cdots (i_{k-1}, i_k)$, et comme il y a $k-1$ transpositions dans ce produit, on a $\mathrm{sign}(\sigma_k) = (-1)^{k-1}$, ce qu'on cherchait à démontrer.

Exercice 3.14. — Montrer que $\mathrm{sign}(\sigma) = (-1)^{n - \omega(\sigma)}$, où $\omega(\sigma)$ est le nombre d'orbites de σ.

Exercice 3.15. — Si $\sigma \in \mathrm{S}_n$, on note u_σ l'endomorphisme de $\mathbf{C}^n$ envoyant un élément e_i de la base canonique de $\mathbf{C}^n$ sur $e_{\sigma(i)}$.

(i) Montrer que $\sigma \mapsto u_\sigma$ est un morphisme de groupes de S_n dans $\mathbf{GL}_n(\mathbf{C})$.

(ii) Montrer que si τ est une transposition, alors u_τ est une symétrie par rapport à un hyperplan que l'on déterminera. Que vaut $\det u_\tau$?

(iii) En déduire que $\det u_\sigma = \mathrm{sign}(\sigma)$ pour tout $\sigma \in \mathrm{S}_n$.

3.4.3. *Groupe alterné*

Le *groupe alterné* A_n est le noyau de la signature. Comme $\mathrm{sign} : \mathrm{S}_n \to \{\pm 1\}$ est surjective, on a $|\mathrm{A}_n| = \frac{1}{2}|\mathrm{S}_n| = \frac{n!}{2}$. Un k-cycle est dans A_n, si et seulement si k est impair.

• A_n est engendré par les 3-cycles.

Cela se démontre par récurrence sur n. Le résultat est évident (et vide) si $n \leqslant 2$. Soit $n \geqslant 3$, et soit $\sigma \in \mathrm{A}_n$. Si $\sigma(n) \neq n$, on peut choisir un 3-cycle $(n, \sigma(n), c)$, où $c \notin \{n, \sigma(n)\}$, et alors $\tau^{-1}\sigma$ fixe n et peut être écrit comme un produit de 3-cycles à support dans $\{1, \ldots, n-1\}$ d'après l'hypothèse de récurrence ; donc $\sigma = \tau(\tau^{-1}\sigma)$ peut être écrit comme un produit de 3-cycles. On en déduit le résultat, le cas $\sigma(n) = n$ se traitant directement.

• Si $n \geqslant 5$, tous les 3-cycles sont conjugués dans A_n.

Il suffit de prouver qu'ils sont tous conjugués à $\sigma_0 = (1,2,3)$. Soit σ un 3-cycle. Comme les 3-cycles sont tous conjugués dans S_n, il existe $\alpha \in \mathrm{S}_n$ tel que $\sigma = \alpha\sigma_0\alpha^{-1}$. Si $\alpha \in \mathrm{A}_n$, on a gagné. Sinon, $\tau = (4,5)$ commute avec σ_0 puisque leurs supports sont disjoints, et $\beta = \alpha\tau \in \mathrm{A}_n$ vérifie $\beta\sigma_0\beta^{-1} = \alpha\tau\sigma_0\tau^{-1}\alpha^{-1} = \alpha\sigma_0\alpha^{-1} = \sigma$, ce qui montre que σ est conjugué à σ_0 dans A_n.

• Le groupe A_5 est un groupe simple.

Soit H un sous-groupe distingué de A_5 non réduit à l'identité. On veut prouver que $\mathrm{H} = \mathrm{A}_5$ et il suffit de prouver que H contient un 3-cycle, car ceci implique qu'il contient tous les 3-cycles puisque ceux-ci sont conjugués dans A_5, et donc $\mathrm{H} = \mathrm{A}_5$ puisque les 3-cycles engendrent A_5.

Soit donc $\sigma \in \mathrm{H} - \{1\}$. Il y a trois possibilités : σ est un 3-cycle et il n'y a rien à faire, ou σ est un 5-cycle ou c'est le produit de 2 tranpositions de supports disjoints.

• Si σ est le 5-cycle (a,b,c,d,e), soit $\tau = (a,b,c)$. Alors H contient $\tau^{-1}\sigma^{-1}\tau$ puisqu'il est distingué et donc aussi $h = \sigma\tau^{-1}\sigma^{-1}\tau$. Or τ^{-1} est le 3-cycle (c,b,a) et $\sigma\tau^{-1}\sigma^{-1}$ est le 3-cycle $(\sigma(c),\sigma(b),\sigma(a)) = (d,c,b)$. Donc $h = (d,c,b)(a,b,c)$ laisse fixe e et $a \mapsto b \mapsto d$, $b \mapsto c \mapsto b$, $c \mapsto a \mapsto a$, et $d \mapsto d \mapsto c$; c'est donc le 3-cycle (a,d,c).

• Si $\sigma = \sigma_1\sigma_2$, avec $\sigma_1 = (a,b)$, $\sigma_2 = (c,d)$, et a,b,c,d distincts deux à deux, et si $\tau = (c,d,e)$, où $e \notin \{a,b,c,d\}$, alors H contient $h = \sigma\tau^{-1}\sigma^{-1}\tau$. Or σ_1 commute à σ_2 et τ, donc $h = \sigma_2\tau^{-1}\sigma_2^{-1}\tau$. Maintenant, $\tau^{-1}\sigma_2^{-1}\tau$ est la transposition $(\tau^{-1}(c),\tau^{-1}(d)) = (e,c)$ et donc $h = (c,d)(e,c) = (c,e,d)$ est un 3-cycle.

• Si $n \geqslant 5$, le groupe A_n est un groupe simple [41].

Soit $n \geqslant 5$, soit H un sous-groupe distingué de A_n, et soient $\sigma \neq \mathrm{id}$ un élément de H et $\tau = (a,b,c)$ un 3-cycle. Alors H contient $h = \tau\sigma\tau^{-1}\sigma^{-1}$ qui est le produit des 3-cycles τ et $\sigma\tau^{-1}\sigma^{-1} = (\sigma(c),\sigma(b),\sigma(a))$. Soit alors $b = \sigma(a)$, et soit $c \notin \{a,\sigma(a),\sigma^2(a)\}$, non fixé par σ si jamais σ échange a et $\sigma(a)$ (un tel c existe toujours, sinon σ serait une transposition, ce qui est impossible puisque $\sigma \in \mathrm{A}_n$). La condition mise sur c fait que $h \neq \mathrm{id}$, et celle mise sur b implique que le support de h est inclus dans $\{a,\sigma(a),\sigma^2(a),c,\sigma(c)\}$ et donc comporte au plus 5 éléments. Soit X de cardinal 5 contenant le support de h, et soit Perm(X) le groupe des permutations de X. Alors $\mathrm{H} \cap \mathrm{Perm(X)}$ est un sous-groupe distingué de Perm(X), et donc contient un 3-cycle d'après l'étude du cas $n = 5$. On en déduit que $\mathrm{H} = \mathrm{A}_n$ comme-ci-dessus puisque A_n est engendré par les 3-cycles qui sont tous conjugués dans A_n.

Exercice 3.16. — (i) Montrer que si G est un groupe fini abélien, et si d divise $|\mathrm{G}|$, alors G a un sous-groupe de cardinal d. (On pourra utiliser le théorème de structure.)

(ii) Montrer que si $f : \mathrm{S}_5 \to \mathrm{S}_3$ est un morphisme de groupes, alors $\mathrm{Im}(f)$ a 1 ou 2 éléments.

(iii) Montrer que S_5 n'a pas de sous-groupe d'ordre 40.

3.5. Les théorèmes de Sylow

Cauchy a démontré (cf. ex. 3.18) que, si G est un groupe fini d'ordre (*l'ordre d'un groupe* est, par définition, son cardinal) divisible par un nombre premier p, alors G contient un élément d'ordre p (et donc un sous-groupe (cyclique) d'ordre p). D'un autre côté, l'ordre d'un sous-groupe divisant l'ordre du groupe (théorème de Lagrange), tout sous-p-groupe

41. Ce résultat, conjugué avec la théorie de Galois, explique que l'on ne puisse pas trouver de formule générale donnant les racines d'une équation de degré n, si $n \geqslant 5$.

(un *p-groupe* est un groupe dont l'ordre est une puissance de p) de G d'ordre p^a vérifie $a \leqslant v_p(|\mathrm{G}|)$. Un *p-Sylow* de G est un sous-groupe d'ordre $p^{v_p(|\mathrm{G}|)}$. (Dans le cas $v_p(|\mathrm{G}|) = 0$, un tel sous-groupe est donc réduit à l'élément neutre.)

• Si G est un groupe commutatif d'ordre divisible par p, alors G contient un sous-groupe cyclique d'ordre p.

Si $x \in \mathrm{G}$, soit n_x l'ordre de x. Par définition cela signifie que le morphisme de groupes de $\mathbf{Z}$ dans G envoyant $a \in \mathbf{Z}$ sur x^a admet pour noyau $n_x\mathbf{Z}$, et donc induit un isomorphisme de $\mathbf{Z}/n_x\mathbf{Z}$ sur le sous-groupe de G engendré par x. Soit alors $\mathrm{X} \subset \mathrm{G}$ engendrant G (on peut prendre $\mathrm{X} = \mathrm{G}$ par exemple). Comme G est commutatif, l'application $\oplus_{x\in\mathrm{X}}(\mathbf{Z}/n_x\mathbf{Z}) \to \mathrm{G}$, envoyant $(a_x)_{x\in\mathrm{X}}$ sur $\prod_{x\in\mathrm{X}} x^{a_x}$ est un morphisme de groupes, et comme X engendre G, ce morphisme est surjectif. L'ordre de G est donc un diviseur de $\prod_{x\in\mathrm{X}} n_x$. Comme p divise $|\mathrm{G}|$, cela implique que p divise un des n_x, et alors $y = x^{n_x/p}$ est d'ordre p et le sous-groupe de G engendré par y est d'ordre p. Ceci permet de conclure.

Théorème 3.17. — (Sylow, 1872) *Si* G *est un groupe fini, l'ensemble des p-Sylow de* G *est non vide. De plus :*

(i) *Tous les p-Sylow de* G *sont conjugués.*

(ii) *Si* Q *est un sous-p-groupe de* G*, alors il existe un p-Sylow de* G *contenant* Q *; en particulier, tout élément d'ordre p est contenu dans un p-Sylow de* G.

La démonstration se fait par récurrence sur $|\mathrm{G}|$, le cas $|\mathrm{G}| = 1$ étant évident (et vide). Soit Z le centre de G, et soit $k = v_p(|\mathrm{G}|)$.

• Si p divise l'ordre de Z, alors Z contient, d'après le point précédent, un sous-groupe cyclique C d'ordre p. On peut appliquer l'hypothèse de récurrence à $\mathrm{H} = \mathrm{G}/\mathrm{C}$ qui est d'ordre mp^{k-1}. Si $\mathrm{P_H}$ est un p-Sylow de H, l'image inverse de $\mathrm{P_H}$ dans G est un sous-groupe d'ordre $|\mathrm{P_H}| \cdot |\mathrm{C}| = p^{k-1}p = p^k$; c'est donc un p-Sylow de G.

• Si p ne divise pas $|\mathrm{Z}|$, on fait agir G par conjugaison intérieure ($g \cdot x = gxg^{-1}$) sur G. Par définition du centre, les orbites (qui ne sont autres que les classes de conjugaison de G) ne comportant qu'un seul élément pour cette action, sont exactement les $\{c\}$, pour $c \in \mathrm{Z}$. Comme $|\mathrm{Z}|$ est premier à p et comme $|\mathrm{G}|$ est divisible par p, il y a une orbite O, non réduite à un élément, de cardinal premier à p. Si $x \in \mathrm{O}$, et si H est l'ensemble des éléments de G commutant à x, on a $\mathrm{O} = \mathrm{G}/\mathrm{H}$. On en déduit que $|\mathrm{H}| = \frac{|\mathrm{G}|}{|\mathrm{O}|}$. Comme $v_p(|\mathrm{O}|) = 0$, on a $v_p(|\mathrm{H}|) = v_p(|\mathrm{G}|) = k$, et comme $|\mathrm{O}| > 1$, on a $|\mathrm{H}| < |\mathrm{G}|$. L'hypothèse de récurrence montre que H contient un sous-groupe d'ordre p^k, et donc que G aussi ; d'où l'existence de p-Sylow.

Maintenant, si P est un p-Sylow de G, et si Q est un sous-p-groupe de G, on peut faire agir Q sur G/P par translation à gauche. Comme G/P est de cardinal premier à p, puisque P est un p-Sylow, au moins une des orbites O a un cardinal premier à p. Mais O est de la forme Q/H, où H est un sous-groupe de Q, et comme Q est un p-groupe, on a $|\mathrm{Q}/\mathrm{H}|$ premier à p si et seulement si $\mathrm{H} = \mathrm{Q}$. Il existe donc $x \in \mathrm{G}/\mathrm{P}$ fixe par Q tout entier. En prenant un représentant $\tilde{x}$ de x dans G, cela se traduit par $\mathrm{Q}\tilde{x}\mathrm{P} \subset \tilde{x}\mathrm{P}$, ou encore par $\mathrm{Q} \subset \tilde{x}\mathrm{P}\tilde{x}^{-1}$.

Si Q est un p-Sylow, on en déduit que $\mathrm{Q} = \tilde{x}\mathrm{P}\tilde{x}^{-1}$ pour des raisons de cardinal, ce qui démontre le (i). Si Q est un sous-p-groupe, cela montre que Q est contenu dans un sous-groupe d'ordre p^k, c'est-à-dire dans un p-Sylow. Ceci démontre le (ii) et permet de conclure.

Exercice 3.18. — Soient p un nombre premier et G un groupe fini de cardinal divisible par p. On fait agir $\mathbf{Z}/p\mathbf{Z}$ sur G^p par $i\cdot(x_0,\dots,x_{p-1})=(x_i,x_{i+1},\dots,x_{i-1})$ (i.e. on décale les indices de i, en identifiant $\mathbf{Z}/p\mathbf{Z}$ et $\{0,\dots,p-1\}$). Soit X le sous-ensemble de G^p des $(x_0,\dots,x_{p-1})$ vérifiant $x_0\cdots x_{p-1}=1$.

(i) Montrer que X est stable par $\mathbf{Z}/p\mathbf{Z}$. Quels sont les points fixes de cette action ?

(ii) Montrer que $|\mathrm{X}|$ est divisible par p ; en déduire que G admet des éléments d'ordre p.

4. Polynômes

4.1. Polynômes en une variable

4.1.1. *Polynômes*

Si A est un anneau commutatif, on note A[X] l'ensemble des *polynômes* à coefficients dans A, en la variable X, i.e. l'ensemble des expressions de la forme $\mathrm{P}=\sum_{n\in\mathbf{N}}a_n\mathrm{X}^n$, avec $a_n=0$ sauf pour un nombre fini de $n\in\mathbf{N}$; les a_n sont les *coefficients* de P, et on dit que P est nul (ou $\mathrm{P}=0$) si tous ses coefficients son nuls.

On munit A[X] d'une structure d'anneau (et même de A-algèbre unitaire) en posant [42] :

◇ $c\cdot\big(\sum_{n\in\mathbf{N}}a_n\mathrm{X}^n\big)=\sum_{n\in\mathbf{N}}(c\,a_n)\mathrm{X}^n$, si $c\in\mathrm{A}$,

◇ $\big(\sum_{n\in\mathbf{N}}a_n\mathrm{X}^n\big)+\big(\sum_{n\in\mathbf{N}}b_n\mathrm{X}^n\big)=\sum_{n\in\mathbf{N}}(a_n+b_n)\mathrm{X}^n$,

◇ $\big(\sum_{n\in\mathbf{N}}a_n\mathrm{X}^n\big)\big(\sum_{n\in\mathbf{N}}b_n\mathrm{X}^n\big)=\sum_{n\in\mathbf{N}}c_n\mathrm{X}^n$, avec $c_n=\sum_{i+j=n}a_ib_j$.

L'anneau ainsi obtenu est l'*anneau des polynômes à coefficients dans* A *en la variable* X ; on définirait de même les anneaux A[T], A[Y], $\mathrm{A}[\mathrm{X}_1]$, etc. des polynômes à coefficients dans A en la variable X, Y, X_1 etc. Tous ces anneaux sont isomorphes entre eux [43] de manière naturelle [44] et donc sont « les mêmes », mais il est commode de pouvoir changer de variable.

Si $\mathrm{P}\in\mathrm{A}[\mathrm{X}]$ est non nul, le *degré* $\deg\mathrm{P}$ de P est le plus grand $n\in\mathbf{N}$ tel que $a_n\neq0$; par convention [45], on pose $\deg0=-\infty$. Si $\mathrm{N}\geqslant\deg\mathrm{P}$, on peut se permettre d'ignorer les termes de degré $>\mathrm{N}$, et donc d'écrire P sous la forme $a_{\mathrm{N}}\mathrm{X}^{\mathrm{N}}+\cdots+a_0$ ou $\sum_{i=0}^{\mathrm{N}}a_i\mathrm{X}^i$. Si $\deg\mathrm{P}=d$, le coefficient a_d est le *coefficient dominant* et P est *unitaire* si ce coefficient est 1 ; si c'est le cas, P s'écrit sous la forme $\mathrm{X}^d+a_{d-1}\mathrm{X}^{d-1}+\cdots+a_0$.

---

42. Vérifier que ceci définit bien une structure de A-algèbre unitaire est fastidieux mais sans difficulté

43. L'isomorphisme consiste à envoyer $\sum_{n\in\mathbf{N}}a_n\mathrm{X}^n$ sur $\sum_{n\in\mathbf{N}}a_n\mathrm{T}^n$, $\sum_{n\in\mathbf{N}}a_n\mathrm{Y}^n$, etc. En fait, on peut d'éfinir l'anneau des polynômes à coefficients dans A, sans référence à une variable, comme l'ensemble $\mathrm{A}^{(\mathbf{N})}$ des suites $(a_n)_{n\in\mathbf{N}}$ presque nulles (i.e. $a_n=0$ sauf pour un nombre fini de n), muni de l'addition $(a_n)_{n\in\mathbf{N}}+(b_n)_{n\in\mathbf{N}}=(a_n+b_n)_{n\in\mathbf{N}}$ et de la multiplication $(a_n)_{n\in\mathbf{N}}\cdot(b_n)_{n\in\mathbf{N}}=(c_n)_{n\in\mathbf{N}}$, avec $c_n=\sum_{i+j=n}a_ib_j$, mais ce point de vue n'est pas utilisé en pratique car on préfère l'autre écriture qui suggère fortement qu'un polynôme est aussi une fonction.

44. Signalons le problème suivant : soient A, B des anneaux commutatifs. On suppose qu'il existe un isomorphisme d'anneaux $\varphi:\mathrm{A}[\mathrm{X}]\to\mathrm{B}[\mathrm{X}]$; est-ce-que cela implique que les anneaux A et B sont isomorphes (l'isomorphisme φ n'est pas supposé envoyer A dans B ni X sur X) ?

45. Une des raisons est que l'on veut que la formule $\deg\mathrm{PQ}=\deg\mathrm{P}+\deg\mathrm{Q}$ ait une chance d'être vraie.

• Si $P, Q \in A[X]$, alors $\deg(P+Q) \leqslant \sup(\deg P, \deg Q)$ et $\deg PQ \leqslant \deg P + \deg Q$ avec égalité si le coefficient dominant de P ou de Q n'est pas un diviseur de zéro ; si A est intègre, alors A[X] est intègre et $\deg PQ = \deg P + \deg Q$, pour tous $P, Q \in A[X]$.

Les inégalités $\deg(P+Q) \leqslant \sup(\deg P, \deg Q)$ et $\deg PQ \leqslant \deg P + \deg Q$ sont immédiates. Maintenant, si $P = a_n X^n + \cdots + a_0$ et $Q = b_m X^m + \cdots + b_0$ sont de degrés n et m respectivement (i.e. $a_n \neq 0$ et $b_m \neq 0$), le coefficient de X^{n+m} dans PQ est $a_n b_m$; il est donc non nul si a_n ou b_m n'est pas un diviseur de zéro et alors $\deg PQ = m+n = \deg P + \deg Q$. C'est automatiquement le cas si A est intègre, et donc $PQ \neq 0$ si $P \neq 0$ et $Q \neq 0$, ce qui prouve que A[X] est intègre si A l'est.

4.1.2. *Fonctions polynomiales*

Si B est une A-algèbre unitaire (par exemple, si B = A), alors $P = \sum_{n \in \mathbf{N}} a_n X^n \in A[X]$ définit une *fonction polynomiale* $P : B \to B$ par la formule $P(x) = \sum_n a_n x^n$, où la somme est en fait une somme finie puisqu'il n'y a qu'un nombre fini de termes non nuls, et $x^0 = 1$ (unité de B) par convention. L'application $P \mapsto P(x)$ est un morphisme d'anneaux (et même de A-algèbres unitaires) de A[X] dans B.

La fonction polynomiale définie par $P \in A[X]$ sur B est aussi celle de $\varphi(B) \in B[X]$, où $\varphi : A[X] \to B[X]$ est le morphisme d'anneaux défini par $\varphi(\sum a_n X^n) = \sum \varphi(a_n) X^n$, et $a \mapsto \varphi(a) = a \cdot 1$ est le morphisme d'anneaux de A dans B déjà rencontré au n° 2.4.

Par exemple, $P \in \mathbf{Z}[X]$ définit une fonction polynomiale sur $\mathbf{F}_p$, pour tout $p \in \mathscr{P}$; ceci est souvent utilisé pour étudier la factorisation de P dans $\mathbf{Z}[X]$.

Si V est un K-espace vectoriel et si $u \in \mathrm{End}(V)$, alors $P \mapsto P(u)$ est un morphisme d'anneaux de K[X] dans End(V) qui joue un grand rôle dans la réduction de l'endomorphsime u (cf. n° 10.1).

Si $x_0 \in B$ vérifie $P(x_0) = 0$, on dit que x_0 est une *racine* de P (dans B), ou que x_0 est un *zéro* de P (dans B).

• Si $P = a_d X^d + \cdots + a_0 \in A[X]$, où $d \geqslant 1$ et $a_d \neq 0$, et si $x_0 \in B$, alors $P - P(x_0)$ peut se factoriser dans B[X] sous la forme $P - P(x_0) = (X - x_0)Q$, avec $Q \in B[X]$, et $\deg Q = d - 1$, si $a_d \neq 0$ dans B.

On utilise la formule $X^n - x_0^n = (X - x_0)(X^{n-1} + x_0 X^{n-2} + \cdots + x_0^{n-1})$. On en déduit la factorisation $P - P(x_0) = (X - x_0)\big(a_d(X^{d-1} + x_0 X^{d-2} + \cdots + x_0^{d-1}) + \cdots + a_2(X + x_0) + a_1\big)$ et le résultat.

• Si A est intègre (par exemple, si A est un corps), et si $P \in A[X]$, non nul, admet $x_1, \ldots, x_r$ comme racines distinctes dans A, alors P peut se factoriser sous la forme $P = (X - x_1) \cdots (X - x_r)Q$, et $\deg Q = \deg P - r$; en particulier, P a au plus [46] $\deg P$ racines distinctes dans A ; si P de degré $\leqslant n$ s'annule en $n+1$ points distincts, alors $P = 0$.

On raisonne par récurrence sur r, le cas $r = 0$ étant vide. Si $P(x_1) = 0$, on peut, d'après le point précédent, écrire $P = P - P(x_1)$ sous la forme $P = (X - x_1)P_1$, avec $\deg P_1 = \deg P - 1$. Maintenant, $0 = P(x_i) = (x_i - x_1)P_1(x_i)$, si $i = 2, \ldots, r$, et comme $x_i \neq x_1$ et A est intègre, cela

46. Ce résultat est faux si A n'est pas intègre, cf. ex. 2.5 et 2.6 ; il est aussi faux dans le cas non commutatif, cf. ex. 2.2.

implique $x_i - x_1 \neq 0$ et $\mathrm{P}_1(x_i) = 0$. On conclut en utilisant l'hypothèse de récurrence appliquée à P_1, dont on déduit que $\mathrm{P}_1 = (\mathrm{X}-x_2)\cdots(\mathrm{X}-x_r)\mathrm{Q}$, avec $\deg \mathrm{Q} = \deg \mathrm{P}_1 - (r-1) = \deg \mathrm{P} - r$.

• Si K est un corps infini, $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ est identiquement nul sur K si et seulement si $\mathrm{P} = 0$.

C'est une conséquence immédiate du point précédent. Notons que le résultat est faux si K est fini : le polynôme $\prod_{\alpha\in\mathrm{K}}(\mathrm{X}-\alpha)$ est identiquement nul sur K, mais n'est pas nul.

• Soient $\alpha_0, \ldots, \alpha_n$ des éléments distincts d'un corps K, et soit $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$, de degré n. Alors $\mathrm{P} = \sum_{i=0}^{n} \mathrm{P}(\alpha_i) \prod_{j\neq i} \frac{\mathrm{X}-\alpha_j}{\alpha_i-\alpha_j}$ (polynômes d'interpolation de Lagrange).

Le polynôme $\mathrm{P} - \sum_{i=0}^{n} \mathrm{P}(\alpha_i) \prod_{j\neq i} \frac{\mathrm{X}-\alpha_j}{\alpha_i-\alpha_j}$ est de degré n, et il s'annule en $\alpha_0, \ldots, \alpha_n$; il a donc $n+1$ zéros, ce qui implique qu'il est nul, d'où le résultat.

Si $\mathrm{P} = \sum_{i=0}^{d} a_i \mathrm{X}^i \in \mathrm{K}[\mathrm{X}]$, on définit la *dérivée* P' de P par $\mathrm{P}' = \sum_{i=0}^{d} i a_i \mathrm{X}^{i-1}$, et on définit la *dérivée n-ième* $\mathrm{P}^{(n)}$ de P, par récurrence, en posant $\mathrm{P}^{(0)} = \mathrm{P}$ et $\mathrm{P}^{(n+1)} = (\mathrm{P}^{(n)})'$. On a donc $\mathrm{P}^{(n)} = \sum_{i=0}^{d} i(i-1)\cdots(i-n+1)a_i\mathrm{X}^{n-i} = n!\mathrm{P}^{[n]}$, où $\mathrm{P}^{[n]} = \sum_{i=0}^{d} \binom{i}{n} a_i \mathrm{X}^{n-i}$ est la *dérivée divisée n*-ième de P.

• Si $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ est de degré $\leqslant d$, et si $\alpha \in \mathrm{A}$, alors $\mathrm{P}(\mathrm{X}) = \sum_{n=0}^{d} \mathrm{P}^{[n]}(\alpha)(\mathrm{X}-\alpha)^n$ (formule de Taylor pour les polynômes). Si $d!$ est inversible dans A (par exemple, si A est un corps contenant $\mathbf{Q}$), cette formule peut se réécrire sous la forme $\mathrm{P}(\mathrm{X}) = \sum_{n=0}^{d} \mathrm{P}^{(n)}(\alpha)\frac{(\mathrm{X}-\alpha)^n}{n!}$.

On a $\mathrm{X}^i = (\mathrm{X}-\alpha+\alpha)^i = \sum_{n=0}^{i} \binom{i}{n}(\mathrm{X}-\alpha)^n\alpha^{i-n}$. Ceci permet de mettre $\mathrm{P}(\mathrm{X}) = \sum_{i=0}^{d} a_i\mathrm{X}^i$ sous la forme $\mathrm{P}(\mathrm{X}) = \sum_{i=0}^{d} a_i\big(\sum_{n=0}^{i}\binom{i}{n}(\mathrm{X}-\alpha)^n\alpha^{i-n}\big) = \sum_{n=0}^{d}(\mathrm{X}-\alpha)^n\big(\sum_{i=n}^{d}\binom{i}{n}a_i\alpha^{i-n}\big) = \sum_{n=0}^{d}\mathrm{P}^{[n]}(\alpha)(\mathrm{X}-\alpha)^n$. Ceci permet de conclure.

4.2. Anneaux euclidiens et principaux

4.2.1. *Division euclidienne*

• Soit $\mathrm{B} \in \mathrm{A}[\mathrm{X}]$, non nul, de coefficient dominant inversible [47]. Alors tout $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ peut s'écrire de manière unique sous la forme $\mathrm{P} = \mathrm{BQ} + \mathrm{R}$, avec $\deg \mathrm{R} < \deg \mathrm{B}$ (on dit que R est le *reste* de la *division euclidienne* de P par B).

Notons m le degré de B et b le coefficient de son terme dominant ; par hypothèse, il a un inverse b^{-1} dans A.

L'existence se démontre par récurrence sur $n = \deg \mathrm{P}$. Si $n < m$, on peut prendre $\mathrm{Q} = 0$ et $\mathrm{R} = \mathrm{P}$. Si $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0$, avec $n \geqslant m$, alors $\mathrm{P} - b^{-1}a_n\mathrm{X}^{n-m}\mathrm{B}$ est de degré $\leqslant n-1$ car on s'est débrouillé pour tuer le terme de degré n. Grâce à l'hypothèse de récurrence on peut donc l'écrire sous la forme $\mathrm{BQ}' + \mathrm{R}$, avec $\deg \mathrm{R} < m$, et $\mathrm{P} = (b^{-1}a_n\mathrm{X}^{n-m} + \mathrm{Q}')\mathrm{B} + \mathrm{R}$ est une écriture de P sous la forme voulue.

Maintenant, si $\mathrm{P} = \mathrm{BQ}_1 + \mathrm{R}_1 = \mathrm{BQ}_2 + \mathrm{R}_2$, avec $\deg \mathrm{R}_1 < \deg \mathrm{B}$ et $\deg \mathrm{R}_2 < \deg \mathrm{B}$, on obtient $(\mathrm{R}_1 - \mathrm{R}_2) = \mathrm{B}(\mathrm{Q}_2 - \mathrm{Q}_1)$. Le coefficient du terme dominant de B n'étant pas un diviseur de zéro, cela implique que $\deg(\mathrm{R}_1 - \mathrm{R}_2) = \deg \mathrm{B} + \deg(\mathrm{Q}_2 - \mathrm{Q}_1)$, et comme $\deg(\mathrm{R}_1 - \mathrm{R}_2) < \deg \mathrm{B}$, on en déduit que $\deg(\mathrm{Q}_2 - \mathrm{Q}_1) < 0$, et donc $\mathrm{Q}_1 = \mathrm{Q}_2$ et $\mathrm{R}_1 = \mathrm{R}_2$. D'où l'unicité.

Si A est un anneau commutatif, un idéal de A est *principal* s'il est engendré par un élément. Un *anneau principal* est un anneau intègre dans lequel tout idéal est principal.

47. C'est automatiquement le cas si A est un corps.

• $\mathbf{Z}$ est un anneau principal.

Un idéal est en particulier un sous-groupe pour l'addition, et on a vu que tout sous-groupe de $\mathbf{Z}$ est de la forme $D\mathbf{Z}$, avec $D \in \mathbf{N}$; c'est donc aussi un idéal principal, et tout idéal de $\mathbf{Z}$ est principal.

• Si K est un corps commutatif, K[X] est un anneau principal.

Soit I un idéal de K[X] non réduit à 0, et soit $B \in I - \{0\}$ de degré minimal. Soit $P \in I$, et soit R le reste de la division euclidienne de P par B. Alors $R = P - BQ \in I$ puisque $P \in I$ et $B \in I$, et $\deg R < \deg B$ par définition du reste. Ceci implique que $R = 0$, par construction de B, et donc P est un multiple de B et $I = (B)$ est principal.

Dans les deux cas ci-dessus ($A = \mathbf{Z}$ et $A = K[X]$), le fait que A est principal découle de l'existence d'une division euclidienne dans A ; un anneau qui est muni d'une division euclidienne est dit *euclidien* [de manière précise, cela signifie que l'on dispose d'une application $N : A - \{0\} \to \mathbf{N}$ permettant de mesurer la *taille* des éléments de A, telle que si $b \neq 0$ et si $x \in A$, il existe $q \in A$ et $r \in A$ vérifiant $N(r) < N(b)$ ou $r = 0$, avec $x = bq + r$; on n'impose pas de condition d'unicité à b et r], et un anneau euclidien est principal [48] pour les mêmes raisons que ci-dessus.

Exercice 4.1. — Si $x \in \mathbf{R}$, on peut écrire x de manière unique sous la forme $n + u$, avec $n \in \mathbf{Z}$ et $u \in [\frac{-1}{2}, \frac{1}{2}[$. Ceci permet d'écrire $z = x + iy \in \mathbf{C}$, de manière unique, sous la forme $z = [z] + \{z\}$, où $[z] = n + im$, avec $n, m \in \mathbf{Z}$ et $\{z\} = u + iv$, avec $u, v \in [\frac{-1}{2}, \frac{1}{2}[$.

(i) Vérifier que $K = \{x + iy,\ x, y \in \mathbf{Q}\}$ est un sous-corps de $\mathbf{C}$ et que $A = \{x + iy,\ x, y \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$ (c'est l'anneau des entiers de Gauss).

(ii) Si $z = x + iy \in K$, soit $N(z) = x^2 + y^2$. Vérifier que $N(z_1 z_2) = N(z_1)N(z_2)$, pour tous $z_1, z_2 \in K$.

(iii) Montrer que u est inversible dans A si et seulement si $N(u) = 1$. En déduire que $A^* = \{1, -1, i, -i\}$.

(iv) Si $a \in A$ et $b \in A - \{0\}$, soit $r = b\{\frac{a}{b}\}$. Montrer que $N(r) < N(b)$. En déduire que l'on peut écrire a sous la forme $a = bc + r$, avec $c, r \in A$ et $N(r) < N(b)$.

(v) Montrer que A est un anneau principal.

4.2.2. *Factorisation dans un anneau principal*

• Si A est un anneau principal, et si I est un idéal premier non nul de A, alors A/I est un corps, et donc un idéal non nul de A est maximal si et seulement si il est premier.

Soit J un idéal de A contenant strictement I. Soient a un générateur de J et p un générateur de I. Comme $I \subset J$, il existe $b \in A$ tel que $p = ab$. Comme $J \neq I$, on a $a \notin I$, et comme I est premier, l'égalité $p = ab$ implique que $b \in I$, et donc qu'il existe $c \in A$ tel que $b = pc$. On a alors $p(1 - ac) = 0$, et comme A est intègre et $p \neq 0$, cela implique que a est inversible, d'inverse c, et donc que $J = A$. On en déduit que I est maximal, ce qui permet de conclure.

• Toute suite croissante d'idéaux de A est stationnaire. (Un anneau vérifiant cette propriété est dit *noethérien*, et donc *un anneau principal est noethérien.*).

48. Il existe des anneaux principaux non euclidiens comme $\mathbf{Z}[\frac{1+\sqrt{-19}}{2}]$, mais ils sont plutôt rares ; à la surprise générale des experts du sujet, un sous-anneau naturel du corps des nombres complexes p-adiques de Fontaine (l'anneau $\mathbf{B}_{\text{cris}}^{\varphi=1}$ pour être précis) s'est révélé, en 2009, être principal et non euclidien.

Soit $(\mathrm{I}_n)_{n\in\mathbf{N}}$ une suite croissante d'idéaux de A, et soit $\mathrm{I} = \cup_{n\in\mathbf{N}}\mathrm{I}_n$. Si $a, b \in \mathrm{I}$, il existe $n, m \in \mathbf{N}$ tels que $a \in \mathrm{I}_n$ et $b \in \mathrm{I}_m$, et comme la suite est croissante, a et b appartiennent à $\mathrm{I}_{\sup(n,m)}$, et donc $a+b \in \mathrm{I}_{\sup(n,m)} \subset \mathrm{I}$. Comme I est aussi stable par multiplication par $\lambda \in \mathrm{A}$, cela montre que I est un idéal. Maintenant, I est principal puisqu'on a supposé A principal ; il est donc de la forme (λ), pour un certain $\lambda \in \mathrm{I}$, et il existe $n \in \mathbf{N}$ tel que $\lambda \in \mathrm{I}_n$. On a alors $(\lambda) \subset \mathrm{I}_n \subset \mathrm{I} = (\lambda)$, ce qui montre que $\mathrm{I}_m = \mathrm{I}_n$, quel que soit $m \geqslant n$. Ceci permet de conclure.

• Tout idéal propre de A est contenu dans un idéal maximal.

Supposons le contraire. Soit $\mathrm{I} \neq \mathrm{A}$ un idéal de A contenu dans aucun idéal maximal. En particulier, I n'est pas maximal et il existe $\mathrm{I}_1 \neq \mathrm{A}$ contenant strictement I. Alors I_1 n'est contenu dans aucun idéal maximal, sinon un idéal maximal qui contiendrait I_1 contiendrait aussi I, ce qui permet de réitérer le processus, et donc de construire une suite strictement croissante $(\mathrm{I}_n)_{n\in\mathbf{N}}$ d'idéaux de A. Comme ceci est contraire au point précédent, cela permet de conclure.

• Si $b \in \mathrm{A} - \{0\}$, et si p est premier et divise b, l'idéal (b/p) contient strictement (b).

Supposons le contraire. Il existe alors $a \in \mathrm{A}$ tel que $b/p = ba$, et donc $b(1-ap) = 0$. Comme A est intègre, cela implique que p est inversible dans A d'inverse a, ce qui est contraire à l'hypothèse selon laquelle p est premier. Ceci permet de conclure.

On dit que a et b sont *premiers entre eux*, si l'idéal (a, b) de A engendré par a et b est égal à A, ce qui équivaut à l'existence de $u, v \in \mathrm{A}$ tels que $au + bv = 1$ puisque $(a, b) = \{au + bv,\ u, v \in \mathrm{A}\}$, et qu'un idéal de A contenant 1 est égal à A. On écrit souvent $(a, b) = 1$, pour dire que a et b sont premiers entre eux.

• (lemme de Gauss)

◇ Si a est premier avec b et c, alors a est premier avec bc.

◇ Si a divise bc et si a est premier avec b, alors a divise c.

Si $(a, b) = (a, c) = 1$, il existe u_1, v_1 tels que $au_1 + bv_1 = 1$ et u_2, v_2 tels que $au_2 + cv_2 = 1$. On a donc $1 = (au_1 + bv_1)(au_2 + cv_2) = au + bcv$, avec $u = au_1u_2 + bv_1u_2 + cu_1v_2$ et $v = v_1v_2$, ce qui prouve que $(a, bc) = 1$. On en déduit le premier énoncé.

Si $bc = ad$ et $au + bv = 1$, alors $acu + adv = c$, et donc $a(cu + dv) = c$, ce qui prouve que a divise c ; d'où le second énoncé.

Si A est un anneau, on dit que $x \in \mathrm{A}$ est *irréductible* si $x = ab$ implique $a \in \mathrm{A}^*$ ou $b \in \mathrm{A}^*$; autrement dit, x est irréductible s'il ne peut pas se factoriser.

• Si A est principal, et si $x \in \mathrm{A}$ est non nul, alors l'idéal (x) engendré par x est premier si et seulement si x est irréductible.

Si x n'est pas irréductible, on peut l'écrire sous la forme $x = ab$, où a et b ne sont pas inversible. Mais alors x ne divise ni a ni b car s'il divisait a (par exemple) on aurait $a = xa'$, et donc $x = xa'b$ et $a'b = 1$ puisque A est intègre, ce qui contredit le fait que b n'est pas inversible. Il s'ensuit que (x) n'est pas premier.

Si x n'est pas premier, il existe $a, b \in \mathrm{A}$, non divisibles par P, tels que ab soit divisible par x sans que ni a ni b le soit. L'idéal (a, x) ne contient pas 1 car sinon, x serait premier à a et x diviserait b d'après le lemme de Gauss, et il n'est pas égal à (x) car x ne divise pas a. Si d en est un générateur, alors d divise x et on peut factoriser x sous la forme $x = d(x/d)$, ce qui

prouve que x n'est pas irréductible car ni d ni x/d n'est une unité de A puisque (d) n'est égal ni à (1) ni à (x).

Exercice 4.2. — Soit $\mathrm{A} = \mathbf{Z}[\sqrt{-5}]$.
(i) Montrer que A est un sous-anneau de $\mathbf{C}$.
(ii) Montrer que les seuls diviseurs de 2 sont $\pm 1, \pm 2$; en déduire que 2 est irréductible.
(iii) Montrer que $(2, 1+\sqrt{-5})$ n'est pas un idéal principal et que (2) n'est pas un idéal premier.

On choisit un générateur de tout idéal premier non nul de A, et on note $\mathscr{P}_\mathrm{A}$ l'ensemble de ces générateurs. Dans le cas de $\mathbf{Z}$ (resp. K[X]), le choix naturel est de prendre l'ensemble des nombres premiers (resp. des polynômes irréductibles unitaires).

• Si $a \in \mathrm{A} - \{0\}$, il existe $u \in \mathrm{A}^*$ et $p_1, \ldots, p_r \in \mathscr{P}_\mathrm{A}$ tels que $a = u\, p_1 \cdots p_r$; de plus, les p_i, pour $1 \leqslant i \leqslant r$, sont uniquement déterminés à l'ordre près. En d'autres termes, a peut se factoriser de manière unique comme produit de facteurs premiers.

Commençons par montrer l'existence d'une telle factorisation. Si a est une unité, il n'y a rien à faire puisque $a = a$ est une factorisation sous la forme souhaitée. Si a n'est pas une unité, il existe un idéal maximal I de A contenant a, et donc $p_1 \in \mathscr{P}_\mathrm{A}$ divisant a. On pose $a_1 = a/p_1$; alors, d'après un point ci-dessus, l'idéal (a_1) contient strictement (a). En réitérant le processus, on construit une suite d'éléments p_i de $\mathscr{P}_\mathrm{A}$ et une suite d'éléments a_i de A, avec $a_{i+1}p_{i+1} = a_i$. La suite d'idéaux (a_i) est alors strictement croissante, ce qui implique que le processus s'arrête puisque A est noethérien. Autrement dit, il existe s tel que a_s soit une unité de A, et $a = a_s p_1 \cdots p_s$ est une factorisation de a sous la forme voulue.

L'unicité se démontre en utilisant le lemme de Gauss. Si $u\, p_1 \cdots p_r = v\, q_1 \cdots q_s$ où les p_i et les q_j sont des nombres premiers et u, v des unités de A, le lemme de Gauss montre que p_r divise l'un des q_j et donc lui est égal. Quitte à permuter les q_j, on peut supposer que $p_r = q_s$, et en divisant les deux membres par $p_r = q_s$ (ce qui est licite car A est intègre), on se ramène à $r-1$ et $s-1$, ce qui permet de conclure par récurrence.

• $\mathbf{Z}^* = \{\pm 1\}$ et $\mathrm{K[X]}^* = \mathrm{K}^*$, si K est un corps.

Si $\mathrm{D} \in \mathbf{Z}$, alors $|\mathbf{Z}/\mathrm{D}\mathbf{Z}| = |\mathrm{D}|$, et donc $\mathrm{D}\mathbf{Z} = \mathbf{Z}$ si et seulement si $\mathrm{D} = \pm 1$; autrement dit, $\mathrm{D} \in \mathbf{Z}^*$ si et seulement si $\mathrm{D} = \pm 1$.

Si $\mathrm{P} \in \mathrm{K[X]}^*$, il existe Q tel que $\mathrm{PQ} = 1$. Mais alors $0 = \deg \mathrm{PQ} = \deg \mathrm{P} + \deg \mathrm{Q}$, et donc $\deg \mathrm{P} = 0$. On en déduit le résultat.

Exercice 4.3. — Soit $\mathrm{A} = \mathrm{K}[\varepsilon]/(\varepsilon^2)$ l'anneau des nombres duaux, et soit $\varphi : \mathrm{A[X]} \to \mathrm{K[X]}$ la réduction modulo ε. Montrer que $\mathrm{P} \in \mathrm{A[X]}^*$ si et seulement si $\varphi(\mathrm{P}) \in \mathrm{K}^*$.

Exercice 4.4. — (Tout nombre premier de la forme $4n+1$ est somme de deux carrés (Fermat, 1640)). On aura à utiliser le fait que, si $p \neq 2$ est un nombre premier, l'équation $x^2 + 1$ a une solution dans $\mathbf{F}_p$ si et seulement si p est de la forme $4n+1$ (ex. 3.4). Soit $\mathrm{A} = \mathbf{Z}[i]$. D'après l'ex. 4.1, A est un anneau principal et $\mathrm{A}^* = \{1, -1, i, -i\}$ est aussi l'ensemble des $z = x + iy \in \mathrm{A}$ vérifiant $\mathrm{N}(z) = 1$, où $\mathrm{N}(z) = x^2 + y^2$ est multiplicative (i.e. $\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1)\mathrm{N}(z_2)$, si $z_1, z_2 \in \mathrm{A}$).

Notons A^+ l'ensemble des $x + iy \in \mathrm{A}$, avec $x > 0$ et $y \geqslant 0$. Tout élément non nul de A peut alors s'écrire de manière unique sous la forme ua, avec $u \in \mathrm{A}^*$ et $a \in \mathrm{A}^+$. On dit que q est un nombre premier de A si $q \in \mathrm{A}^+$ et si l'idéal (q) est premier ; on note $\mathscr{P}_\mathrm{A}$ l'ensemble des nombres premiers de A et, comme d'habitude, $\mathscr{P}$ celui des nombres premiers usuels.

(i) Montrer que, si $q \in \mathscr{P}_\mathrm{A}$, alors $\mathbf{Z} \cap (q)$ est un idéal premier de $\mathbf{Z}$. En déduire que q divise un unique

$p \in \mathscr{P}$ et que $\mathrm{N}(q) = p$ ou $\mathrm{N}(q) = p^2$.

(ii) Soit $q \in \mathrm{A}^+$. Montrer que $q \in \mathscr{P}_\mathrm{A}$ si $\mathrm{N}(q) \in \mathscr{P}$.

(iii) Soit $p \in \mathscr{P}$ de la forme $4n+1$. Montrer qu'il existe $a \in \mathrm{A} - \{0\}$ tel que $p \mid \mathrm{N}(a)$ et $0 < \mathrm{N}(a) < p^2$, et que $\mathrm{pgcd}(a, p)$ est premier dans A et divise strictement p.

(iv) Montrer que tout nombre premier de la forme $4n+1$ est somme de deux carrés.

(v) Soit $p \in \mathscr{P}$ impair. Montrer que, si $p \notin \mathscr{P}_\mathrm{A}$, il existe $q_p = x + iy \in \mathrm{A}^+$, unique, avec $x > y$, vérifiant $\mathrm{N}(q_p) = p$ et que la factorisation de p est $p = (-i)q_p q_p^*$, où $q_p^* = i\overline{q_p}$.

(vi) Montrer que tout $p \in \mathscr{P}$ de la forme $4n+3$ est premier dans A.

(vii) Montrer que les éléments de $\mathscr{P}_\mathrm{A}$ sont $1+i$, les $p \in \mathscr{P}$ de la forme $4n+3$, et les q_p, q_p^*, pour $p \in \mathscr{P}$ de la forme $4n+1$.

On note $v_p(a)$ le nombre de fois que p apparaît dans la factorisation de a en facteurs premiers. Alors $p^{v_p(a)}$ est la plus grande puissance de p divisant a ; on a donc $v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a+b) \geqslant \inf(v_p(a), v_p(b))$.

Si $a_1, \ldots, a_n \in \mathrm{A} - \{0\}$, on définit $\mathrm{pgcd}(a_1, \ldots, a_n)$ par $\mathrm{pgcd}(a_1, \ldots, a_n) = \prod_p p^{\inf_i v_p(a_i)}$, ce qui fait de $\mathrm{pgcd}(a_1, \ldots, a_n)$ le plus grand diviseur commun des a_i (à multiplication près par une unité de A)

• $\mathrm{pgcd}(a_1, \ldots, a_n)$ est un générateur de l'idéal engendré par les a_i. (th. de Bézout)

Commençons par démontrer le résultat pour $n = 2$, et posons $a_1 = a$ et $a_2 = b$. Il est clair que tout élément de (a, b) est un multiple de $\mathrm{pgcd}(a, b)$; il suffit donc de prouver que $d = \mathrm{pgcd}(a, b) \in (a, b)$. Pour cela, écrivons a et b sous la forme $a = udp_1 \cdots p_r$ et $b = vdq_1 \cdots q_s$, où u, v sont des unités de A et $p_1, \ldots, p_r, q_1, \ldots q_s$ des éléments de $\mathscr{P}_\mathrm{A}$. Par définition de d, on a $p_i \neq q_j$ quels que soient i et j, ce qui prouve, d'après le lemme de Gauss, que a/d et b/d sont premiers entre eux. Il existe donc $x, y \in \mathrm{A}$ tels que $(a/d)x + (b/d)y = 1$, et alors $d = ax + by \in (a, b)$, ce que l'on cherchait à démontrer.

Maintenant, comme $\inf_{i \leqslant n} v_p(a_i) = \inf(\inf_{i \leqslant n-1} v_p(a_i), v_p(a_n))$, on a

$$\mathrm{pgcd}(a_1, \ldots, a_n) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \ldots, a_{n-1}), a_n).$$

De même, l'idéal $(a_1, \ldots, a_n)$ est l'idéal engendré par $(a_1, \ldots, a_{n-1})$ et par a_n, ce qui permet de déduire, par récurrence, le cas général du cas $n = 2$.

Les a_i sont dits *premiers entre eux dans leur ensemble* si $\mathrm{pgcd}(a_1, \ldots, a_n) = 1$, ce qui équivaut (cf. point précédent) à l'existence de $\alpha_1, \ldots, \alpha_n \in \mathrm{A}$ tels que $\alpha_1 a_1 + \cdots + \alpha_n a_n = 1$.

Exercice 4.5. — Soient $\mathrm{A}, \mathrm{B}, \mathrm{C} \in \mathbf{C}[\mathrm{X}]$, non tous constants, premiers entre eux deux à deux, et vérifiant $\mathrm{A} + \mathrm{B} = \mathrm{C}$, et soit $\Delta = \mathrm{AB}' - \mathrm{BA}'$ (où P' désigne la dérivée de P ; on a aussi $\Delta = \mathrm{AC}' - \mathrm{CA}' = \mathrm{CB}' - \mathrm{BC}'$).

(i) Montrer que $\Delta \neq 0$ et $\deg \Delta \leqslant \inf(\deg \mathrm{A} + \deg \mathrm{B}, \deg \mathrm{B} + \deg \mathrm{C}, \deg \mathrm{C} + \deg \mathrm{A}) - 1$.

(ii) Montrer que, si z est un zéro de ABC de multiplicité $m_z \geqslant 1$, alors la multiplicité de z comme zéro de Δ est $m_z - 1$.

(iii) Si $\mathrm{Q} \in \mathbf{C}[\mathrm{X}]$ est non nul, on note $r(\mathrm{Q})$ le nombre de ses zéros (sans multiplicité [49]). Montrer que

49. Plus généralement, si K est un corps, et si $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ est non nul, on définirait $r(\mathrm{Q})$ comme le degré du *radical* $\mathrm{rad}(\mathrm{P})$ de P, produit des polynômes unitaires irréductibles divisant P [e.g. si $\mathrm{K} = \mathbf{R}$, alors $\mathrm{rad}(\mathrm{X}^5(\mathrm{X}^2+1)^2(\mathrm{X}-2)) = \mathrm{X}(\mathrm{X}^2+1)(\mathrm{X}-2)$].

l'on a la minoration [50] $r(\mathrm{ABC}) \geqslant \sup(\deg \mathrm{A}, \deg \mathrm{B}, \deg \mathrm{C}) + 1$.

(iv) Montrer que, si $n \geqslant 3$, si $\mathrm{A}, \mathrm{B}, \mathrm{C}$ sont des éléments de $\mathbf{C}[\mathrm{X}]$, premiers entre eux deux à deux, et si $\mathrm{A}^n + \mathrm{B}^n = \mathrm{C}^n$, alors A, B et C sont constants (th. de Fermat pour les polynômes).

4.2.3. *Décomposition en éléments simples*

On note F le corps des fractions de A. Si $\mathrm{A} = \mathbf{Z}$, on a $\mathrm{F} = \mathbf{Q}$, et si $\mathrm{A} = \mathrm{K}[\mathrm{X}]$, alors $\mathrm{F} = \mathrm{K}(\mathrm{X})$ est le corps des *fractions rationnelles* en une variable à coefficients dans K.

• Soit $x = \frac{a}{b} \in \mathrm{F}$, avec $a, b \in \mathrm{A}$ premiers entre eux. On suppose donné, pour tout $p \in \mathscr{P}_\mathrm{A}$ divisant b, un système $\mathrm{S}_p \subset \mathrm{A}$ de représentants de $(\mathrm{A}/p)^*$. Alors on peut écrire x, de manière unique, sous la forme $x = a_0 + \sum_{p|b} \sum_{i=1}^{v_p(b)} \frac{s_{p,i}}{p^i}$, avec $a_0 \in \mathrm{A}$, et $s_{i,p} \in \mathrm{S}_p$ pour tous p et i (décomposition en éléments simples).

> On raisonne par récurrence sur $n(x) = \sup_{p|b} v_p(b) = -\inf_{p \in \mathscr{P}_\mathrm{A}} v_p(x)$. Si $n(x) = 0$, alors $x \in \mathrm{A}$, et $x = x$ est l'écriture cherchée. Si $n(x) \geqslant 1$, on pose $c = \prod_{p|b} p^{v_p(b)}$. Alors $cx \in \mathrm{A}$, et les images $\overline{cx}$ de cx modulo p et $\overline{c_p}$ de $c_p = p^{-v_p(b)}c$ sont des unités de A/p, car $v_p(cx) = 0$ et $v_p(c_p) = 0$. Soit $s_p \in \mathrm{S}_p$ le représentant de $\overline{c_p}^{-1}\overline{cx}$ dans A. Alors $cx - c_p s_p$ est divisible par p, et donc $v_p(x - \frac{s_p}{p^{v_p(b)}}) \geqslant -v_p(b) + 1$, et s_p est le seul élément de S_p pour lequel ceci soit vrai. Soit $x' = x - \sum_{p|b} \frac{s_p}{p^{v_p(b)}}$. D'après ce qui précède, $n(x') \leqslant n(x) - 1$, ce qui permet de lui appliquer l'hypothèse de récurrence. On en déduit le résultat, avec $s_{p,i} = s_p$ si $i = -v_p(x)$.

Le résultat précédent est particulièrement utile dans le cas $\mathrm{A} = \mathrm{K}[\mathrm{X}]$. Dans ce cas, il y a un choix canonique pour S_P si P est irréductible et unitaire, de degré n, à savoir $\mathrm{K}[\mathrm{X}]^{(n-1)} - \{0\}$. On obtient donc les résultats suivants.

• Tout $\mathrm{F} \in \mathrm{K}(\mathrm{X})$ peut s'écrire, de manière unique, sous la forme $\mathrm{R} + \sum_{\mathrm{P} \in \mathscr{P}_{\mathrm{K}[\mathrm{X}]}} \sum_{i=1}^{-v_\mathrm{P}(\mathrm{F})} \frac{\mathrm{S}_{\mathrm{P},i}}{\mathrm{P}^i}$, où $\mathrm{R} \in \mathrm{K}[\mathrm{X}]$ et $\mathrm{S}_{\mathrm{P},i}$ est un élément non nul de $\mathrm{K}[\mathrm{X}]$ de degré $< \deg \mathrm{P}$, pour tous P et i. Si tous les polynômes irréductibles P divisant le dénominateur de F sont de degré 1 (c'est automatique si K est algébriquement clos), alors F peut s'écrire, de manière unique, sous la forme $\mathrm{R} + \sum_{\lambda \in \mathrm{K}} \sum_{i=1}^{-v_\lambda(\mathrm{F})} \frac{s_{\lambda,i}}{(\mathrm{X}-\lambda)^i}$, où $\mathrm{R} \in \mathrm{K}[\mathrm{X}]$, et $s_{\lambda,i} \in \mathrm{K}^*$ pour tous λ et i.

Exercice 4.6. — (i) Soit $\mathrm{F} = \frac{\mathrm{Q}(\mathrm{X})}{(\mathrm{X}-\lambda_0)\cdots(\mathrm{X}-\lambda_n)}$, où $\deg \mathrm{Q} \leqslant n$ et les λ_i sont distincts deux à deux. Déterminer la décomposition de F en éléments simples.

---

50. On dispose d'un dictionnaire heuristique entre $\mathrm{K}[\mathrm{X}]$ et $\mathbf{Z}$ qui est un guide précieux pour essayer de deviner ce qui peut être vrai en théorie des nombres. Dans ce dictionnaire, $\deg \mathrm{P}$ devient $\log|n|$ (voir ci-dessous), et l'énoncé ci-dessus devient (en définissant le *radical* $\mathrm{rad}(n)$ d'un entier n, non nul, comme le produit des nombres premiers divisant n (le radical de $720 = 6!$ est $2 \cdot 3 \cdot 5 = 30$)) : pour tout $\varepsilon > 0$, il existe $\mathrm{C}(\varepsilon) > 0$ tel que, si a, b, c sont des entiers, non nuls, premiers entre eux deux à deux, et vérifiant $a + b = c$, alors

$$\sup(\log|a|, \log|b|, \log|c|) \leqslant (1+\varepsilon)\log(\mathrm{rad}(abc)) + \mathrm{C}(\varepsilon).$$

Cet énoncé, connu sous le nom de « conjecture *abc* », date de 1985, et ne semble pas sur le point d'être démontré (comme quoi, l'équation $a+b=c$ est plus subtile qu'elle n'en a l'air...). Nous laissons au lecteur le plaisir d'expliciter ce que cet énoncé implique au sujet du théorème de Fermat. Pour justifier l'analogie entre $\deg \mathrm{P}$ et $\log|n|$, on peut regarder le cas où K est un corps fini, par exemple $\mathbf{F}_p$: dans ce cas, le cardinal de l'anneau $\mathbf{F}_p[\mathrm{X}]/\mathrm{P}$ est lié à $\deg \mathrm{P}$ par la formule $\log|\mathbf{F}_p[\mathrm{X}]/\mathrm{P}| = \deg \mathrm{P} \cdot \log p$, que l'on peut mettre en parallèle avec la formule $\log|n| = \log|\mathbf{Z}/n\mathbf{Z}|$.

(ii) Si $\lambda \in \mathrm{K}$ et $\mathrm{Q} \in \mathrm{K}[\mathrm{X}]$, déterminer la décomposition en éléments simples de $\frac{\mathrm{Q}(\mathrm{X})}{(\mathrm{X}-\lambda)^n}$.

(iii) Déterminer, en fonction des zéros et des pôles de F, la décomposition de $\frac{\mathrm{F}'}{\mathrm{F}}$ en éléments simples, si $\mathrm{F} \in \mathrm{K}(\mathrm{X}) - \{0\}$, où K est algébriquement clos.

(iv) Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$. Montrer que les zéros de P' sont dans l'enveloppe convexe des zéros de P.

4.3. Polynômes en plusieurs variables

4.3.1. *L'anneau* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$

On définit par récurrence $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ comme étant $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}][\mathrm{X}_n]$, si A est un anneau. Alors $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ s'écrit, de manière unique, sous la forme $\sum_{\mathbf{k}} a_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}$, où :

◇ $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbf{N}^n$

◇ $a_{\mathbf{k}} \in \mathrm{A}$ est nul sauf pour un nombre fini de $\mathbf{k}$,

◇ $\mathrm{X}^{\mathbf{k}} = \prod_{i=1}^n \mathrm{X}_i^{k_i}$.

Si $\mathbf{i}, \mathbf{j} \in \mathbf{N}^n$, on pose $\mathbf{i} + \mathbf{j} = (i_1 + j_1, \ldots, i_n + j_n)$. L'addition et la multiplication dans $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ sont alors données par :

◇ $\big(\sum_{\mathbf{k}} a_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}\big) + \big(\sum_{\mathbf{k}} b_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}\big) = \sum_{\mathbf{k}} (a_{\mathbf{k}} + b_{\mathbf{k}}) \mathrm{X}^{\mathbf{k}}$,

◇ $\big(\sum_{\mathbf{k}} a_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}\big)\big(\sum_{\mathbf{k}} b_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}\big) = \sum_{\mathbf{k}} (c_{\mathbf{k}}) \mathrm{X}^{\mathbf{k}}$, avec $c_{\mathbf{k}} = \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} a_{\mathbf{i}} b_{\mathbf{j}}$.

L'anneau $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est une $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$-algèbre, et donc en particulier une A-algèbre, l'action de A étant donnée par $c \cdot \big(\sum_{\mathbf{k}} a_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}\big) = \sum_{\mathbf{k}} (c\, a_{\mathbf{k}}) \mathrm{X}^{\mathbf{k}}$, si $c \in \mathrm{A}$. Il est clair sur ces formules que les variables $\mathrm{X}_1, \ldots, \mathrm{X}_n$ jouent exactement le même rôle contrairement à ce que la construction par récurrence pourrait laisser croire.

Si B est une A algèbre commutative [51] unitaire, alors $\mathrm{P} = \sum_{\mathbf{n}} a_{\mathbf{n}} \mathrm{X}^{\mathbf{n}}$ définit une *fonction polynomiale* $\mathrm{P} : \mathrm{B}^n \to \mathrm{B}$ par la formule $\mathrm{P}(x) = \sum_{\mathbf{n}} a_{\mathbf{n}} \prod_{i=1}^n x_i^{n_i}$, si $x = (x_1, \ldots, x_n)$, où la somme sur $\mathbf{n}$ est une somme finie car tous les termes sauf un nombre fini sont nuls. L'application $\mathrm{P} \mapsto \mathrm{P}(x)$ est un morphisme d'anneaux (et même de A-algèbres unitaires) de $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ dans B.

• Si K est un corps infini, alors $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est identiquement nul sur K^n si et seulement si $\mathrm{P} = 0$.

> Montrons que $\mathrm{P} = 0$ si P est identiquement nul sur K^n. La démonstration se fait par récurrence sur n, le cas $n = 1$ ayant déjà été démontré. On écrit P sous la forme $\sum_{i=0}^d \mathrm{P}_i \mathrm{X}_n^i$, avec $\mathrm{P}_i \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$. Par hypothèse, si $x_1, \ldots, x_{n-1}$ sont fixés, alors $\mathrm{P}_{x_1,\ldots,x_{n-1}}(\mathrm{X}_n) = \sum_{i=0}^d \mathrm{P}_i(x_1, \ldots, x_{n-1}) \mathrm{X}_n^i \in \mathrm{K}[\mathrm{X}_n]$ est identiquement nul sur K, et donc est nul. On en déduit que $\mathrm{P}_i(x_1, \ldots, x_{n-1})$ est, pour tout i, identiquement nul sur K^{n-1}, et donc $\mathrm{P}_i = 0$ d'après l'hypothèse de récurrence. D'où la nullité de P. La réciproque étant immédiate, cela permet de conclure.

Si $\mathbf{k} \in \mathbf{N}^n$, on note $|\mathbf{k}|$ la quantité $\sum_{i=1}^n k_i \in \mathbf{N}$. Alors $|\mathbf{k} + \boldsymbol{\ell}| = |\mathbf{k}| + |\boldsymbol{\ell}|$. On définit le *degré total* $\deg \mathrm{P}$ du polynôme $\mathrm{P} = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathrm{X}^{\mathbf{k}}$ comme le maximum des $|\mathbf{k}|$ pour les $\mathbf{k}$ vérifiant $a_{\mathbf{k}} \neq 0$, si P est non nul ; si $\mathrm{P} = 0$, alors $\deg \mathrm{P} = -\infty$. Si $1 \leqslant i \leqslant n$, on définit le

51. On a besoin que $x_1, \ldots, x_n$ commutent si on veut que $\mathrm{P}(x)\mathrm{Q}(x) = \mathrm{PQ}(x)$.

degré partiel $\deg_{X_i}$ *de* P *en la variable* X_i comme le maximum des k_i, pour les $\mathbf{k}$ vérifiant $a_{\mathbf{k}} \neq 0$, si P est non nul ; si $P = 0$, alors $\deg_{X_i} P = -\infty$.

• Si $d = \deg, \deg_{X_i}$, alors $d(P+Q) \leqslant \sup(d(P), d(Q))$ et $d(PQ) \leqslant d(P) + d(Q)$; si A est intègre, alors $A[X_1, \dots, X_n]$ est intègre et $d(PQ) = d(P) + d(Q)$.

Les énoncés pour $\deg_{X_i}$ se démontrent en utilisant le cas des polynômes en une variable et l'isomorphisme $A[X_1, \dots, X_n] \cong A[X_1, \dots, \hat{X}_i, \dots, X_n][X_i]$. Ceux concernant le degré total peuvent se démontrer en faisant les changements de variables $X_i = TY_i$ et en utilisant $\deg_T$ sur $A[Y_1, \dots, Y_n, T]$, car $\deg_T(P(TY_1, \dots, TY_n)) = \deg P$.

On dit que $P = \sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}}$ est *homogène* de degré d, si $a_{\mathbf{k}} = 0$ pour tout $\mathbf{k}$ vérifiant $|\mathbf{k}| \neq d$. Tout polynôme peut s'écrire, de manière unique, comme une somme de polynômes homogènes de degrés distincts : si $P = \sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}}$, alors $P = \sum_{i \in \mathbf{N}} P_i$, où $P_i = \sum_{|\mathbf{k}|=i} a_{\mathbf{k}} X^{\mathbf{k}}$ est la *partie homogène de degré* i de P.

Exercice 4.7. — Soient K un corps infini et $P \in K[X_1, \dots, X_n]$, de degré total d. Montrer qu'il existe $t_1, \dots, t_{n-1} \in K$, tels que $P_{t_1,\dots,t_{n-1}} = P(X_1 + t_1 X_n, \cdots, X_{n-1} + t_{n-1} X_n, X_n)$, soit de degré d en X_n, à coefficient dominant appartenant à K^*.

4.3.2. *Polynômes en une famille de variables*

Soit A un anneau. Si I est un ensemble (éventuellement infini [52]), on note $A[X_i,\ i \in I]$ l'ensemble des polynômes en les variables X_i, pour $i \in I$. Un élément P de $A[X_i,\ i \in I]$ s'écrit, de manière unique, sous la forme $\sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}}$, où :

◇ $\mathbf{k}$ parcourt l'ensemble $\mathbf{N}^{(I)}$ des applications $i \mapsto n_i$ de I dans $\mathbf{N}$ ne prenant qu'un nombre fini de valeurs non nulles,

◇ $a_{\mathbf{k}} \in A$ est nul sauf pour un nombre fini de $\mathbf{k}$,

◇ $X^{\mathbf{k}}$ est un symbole représentant le monôme $\prod_{i \in I} X_i^{k_i}$, ce produit étant en fait un produit fini puisque presque tous les exposants sont égaux à 0 et $X_i^0 = 1$ par convention.

On fait de $A[X_i,\ i \in I]$ un anneau grâce aux formules :

◇ $\left(\sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}}\right) + \left(\sum_{\mathbf{k}} b_{\mathbf{k}} X^{\mathbf{k}}\right) = \sum_{\mathbf{k}} (a_{\mathbf{k}} + b_{\mathbf{k}}) X^{\mathbf{k}}$,

◇ $\left(\sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}}\right)\left(\sum_{\mathbf{k}} b_{\mathbf{k}} X^{\mathbf{k}}\right) = \sum_{\mathbf{k}} (c_{\mathbf{k}}) X^{\mathbf{k}}$, avec $c_{\mathbf{k}} = \sum_{\mathbf{j}+\mathbf{l}=\mathbf{k}} a_{\mathbf{j}} b_{\mathbf{l}}$.

Si $I = \{1, \dots, n\}$, on retombe sur l'anneau $A[X_1, \dots, X_n]$ du n° précédent.

Si B est une A algèbre commutative unitaire, alors $P = \sum_{\mathbf{k}} a_{\mathbf{k}} X^{\mathbf{k}} \in A[X_i,\ i \in I]$ définit une *fonction polynomiale* $P : B^I \to B$ par la formule $P(x) = \sum_{\mathbf{k}} a_{\mathbf{k}} \prod_{i \in I} x_i^{k_i}$, si $x = (x_i)_{i \in I}$, où le produit infini $\prod_{i \in I} x_i^{k_i}$ est en fait un produit fini car tous les termes sauf un nombre fini valent 1, et la somme sur $\mathbf{k}$ est une somme finie car tous les termes sauf un nombre fini sont nuls. Si $x = ((x_i)_{i \in I}) \in B^I$, l'application $P \mapsto P(x)$ est un morphisme d'anneaux (et même de A-algèbres) de $A[X_i,\ i \in I]$ dans B.

52. S'il y a une infinité de variables, on n'en utilise qu'un nombre fini dans chaque calcul, ce qui fait que l'on peut toujours raisonner comme si on travaillait dans $A[X_1, \dots, X_n]$. Par ailleurs, même dans le cas où I est fini, il est souvent utile de ne pas numéroter ses éléments ; par exemple, si on veut parler d'un polynôme en les coefficients d'une matrice $n \times n$, on préfère que l'ensemble des indices soit $\{1, \dots, n\} \times \{1, \dots, n\}$ plutôt que $\{1, \dots, n^2\}$.

Si $i \in \mathrm{I}$, on définit le degré $\deg_{\mathrm{X}_i}$ de P en la variable X_i comme dans le cas de $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, et on définit le degré total $\deg \mathrm{P}$ de P comme dans le cas de $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ en posant $|\mathbf{k}| = \sum_{i \in \mathrm{I}} k_i \in \mathbf{N}$.

Remarque 4.8. — Tout anneau commutatif est une $\mathbf{Z}$-algèbre unitaire. Il en résulte qu'une identité entre polynômes à coefficients dans $\mathbf{Z}$ induit, pour tout anneau commutatif Λ, une identité entre les fonctions polynomiales associées.

Par ailleurs, pour vérifier que $\mathrm{P}, \mathrm{Q} \in \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ sont égaux il suffit de vérifier que $\mathrm{P} = \mathrm{Q}$ dans $\mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ puisque $\mathbf{Z}$ s'injecte dans $\mathbf{C}$, et il suffit donc de vérifier que les fonctions polynomiales qu'ils définissent sur $\mathbf{C}^n$ sont les mêmes.

Par exemple, si on cherche à montrer que les polynômes caractéristiques de AB et BA sont les mêmes pour deux matrices $\mathrm{A} = (a_{i,j}), \mathrm{B} = (b_{i,j}) \in \mathbf{M}_n(\Lambda)$, où Λ est un anneau commutatif quelconque, il suffit de prouver que $\mathrm{P} = \det(\mathrm{X} - \mathrm{AB})$ et $\mathrm{Q} = \det(\mathrm{X} - \mathrm{BA})$ sont égaux dans l'anneau Λ_{univ} des polynômes en les $1 + 2n^2$ variables X et $a_{i,j}, b_{i,j}$,pour $1 \leqslant i, j \leqslant n$. Maintenant, si $\mathrm{A} \in \mathbf{M}_n(\mathbf{C})$ est inversible, on a $\det(\mathrm{X} - \mathrm{AB}) = \det(\mathrm{A}^{-1}(\mathrm{X} - \mathrm{AB})\mathrm{A}) = \det(\mathrm{X} - \mathrm{BA})$. On en déduit que la fonction polynomiale $(\mathrm{P} - \mathrm{Q})\mathrm{R}$, où $\mathrm{R} = \det \mathrm{A} \in \Lambda_{\mathrm{univ}}$, est identiquement nulle sur $\mathbf{C} \times \mathbf{M}_n(\mathbf{C}) \times \mathbf{M}_n(\mathbf{C})$. Il s'ensuit que $(\mathrm{P} - \mathrm{Q})\mathrm{R} = 0$ dans Λ_{univ}, et comme $\mathrm{R} \neq 0$ et Λ_{univ} est intègre, cela implique $\mathrm{P} = \mathrm{Q}$.

4.4. Polynômes symétriques

On dit que $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est *symétrique* en $\mathrm{X}_1, \ldots, \mathrm{X}_n$, si $\mathrm{P}(\mathrm{X}_{\sigma(1)}, \ldots, \mathrm{X}_{\sigma(n)}) = \mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, pour toute permutation $\sigma \in \mathrm{S}_n$. Par exemple, $\Sigma_1, \ldots, \Sigma_n$, définis en développant le polynôme

$$\mathrm{P}(\mathrm{X}) = \prod_{i=1}^{n} (\mathrm{X} - \mathrm{X}_i) = \mathrm{X}^n - \Sigma_1 \mathrm{X}^{n-1} + \Sigma_2 \mathrm{X}^{n-2} + \cdots + (-1)^n \Sigma_n,$$

sont symétriques en $\mathrm{X}_1, \ldots, \mathrm{X}_n$ car P l'est ; ce sont les *fonctions symétriques élémentaires* de $\mathrm{X}_1, \ldots, \mathrm{X}_n$, et ce sont aussi, au signe près, les coefficients du polynôme dont les racines sont $\mathrm{X}_1, \ldots, \mathrm{X}_n$. On a

$$\Sigma_1 = \mathrm{X}_1 + \cdots + \mathrm{X}_n, \quad \Sigma_n = \mathrm{X}_1 \cdots \mathrm{X}_n, \quad \text{et, en général, } \Sigma_k = \sum_{i_1 < i_2 < \cdots < i_k} \mathrm{X}_{i_1} \cdots \mathrm{X}_{i_k}.$$

• Soit K un corps. Si $\mathrm{P} = a_n \mathrm{X}^n + a_{n-1} \mathrm{X}^{n-1} + \cdots + a_0 \in \mathrm{K}[\mathrm{X}]$, avec $a_n \neq 0$, a pour racines $\alpha_1, \ldots, \alpha_n$ dans un corps contenant K, alors $a_{n-i} = (-1)^i a_n \Sigma_i(\alpha_1, \ldots, \alpha_n)$; en particulier, la somme des racines de P est $-\frac{a_{n-1}}{a_n}$, le produit est $(-1)^n \frac{a_0}{a_n}$, et $\Sigma_i(\alpha_1, \ldots, \alpha_n) \in \mathrm{K}$, pour tout i.

On a $\frac{1}{a_n}\mathrm{P} = \prod_{i=1}^{n}(\mathrm{X} - \alpha_i) = \mathrm{X}^n + \sum_{i=1}^{n} (-1)^i \Sigma_i(\alpha_1, \ldots, \alpha_n)\mathrm{X}^{n-i}$. On en déduit le résultat.

• Un polynôme en $\Sigma_1, \ldots, \Sigma_n$ est symétrique en $\mathrm{X}_1, \ldots, \mathrm{X}_n$. Réciproquement, tout polynôme symétrique en $\mathrm{X}_1, \ldots, \mathrm{X}_n$ est un polynôme en les fonctions symétriques élémentaires : si $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est symétrique, il existe $\mathrm{Q} \in \mathrm{A}[\Sigma_1, \ldots, \Sigma_n]$ tel que

$$\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \mathrm{Q}(\Sigma_1(\mathrm{X}_1, \ldots, \mathrm{X}_n), \ldots, \Sigma_n(\mathrm{X}_1, \ldots, \mathrm{X}_n)).$$

La symétrie d'un polynôme en $\Sigma_1, \dots, \Sigma_n$ résulte de celle de $\Sigma_1, \dots, \Sigma_n$. La démonstration de la réciproque se fait par récurrence sur n, le cas $n = 1$ étant tautologique puisque $X_1 = \Sigma_1$. Supposons le résultat vrai pour $n-1$, et notons $\Sigma_i^{(n-1)}$, pour $i \leqslant n-1$, les fonctions symétriques élémentaires en $X_1, \dots, X_{n-1}$. Alors $\Sigma_i^{(n-1)} = \Sigma_i(X_1, \dots, X_{n-1}, 0)$, si $i \leqslant n-1$ et $\Sigma_n(X_1, \dots, X_{n-1}, 0) = 0$. Soit P, symétrique en $X_1, \dots, X_n$. Alors $P(X_1, \dots, X_{n-1}, 0)$ est symétrique en $X_1, \dots, X_{n-1}$ et peut donc s'écrire sous la forme $Q(\Sigma_1^{(n-1)}, \dots, \Sigma_{n-1}^{(n-1)})$. Maintenant, $R = P - Q(\Sigma_1, \dots, \Sigma_{n-1})$ est symétrique en $X_1, \dots, X_n$ et, par construction, vérifie $R(X_1, \dots, X_{n-1}, 0) = 0$. Cette dernière condition montre que R est divisible par X_n et, par symétrie, par X_i, pour tout i. On peut donc l'écrire sous la forme $X_1 \cdots X_n S = \Sigma_n S$, où S est symétrique. En fait R est constitué des monômes de P qui sont divisibles par Σ_n, et donc $\deg R \leqslant \deg P$ et $\deg S = \deg R - n < \deg P$, et on conclut par récurrence sur le degré de P.

Exercice 4.9. — Soit $P \in \mathbf{Q}[X]$ de degré $n \geqslant 1$, et soient $\alpha_1, \dots, \alpha_n \in \mathbf{C}$ les racines de P.
(i) Montrer que $\sum_{i=1}^n \alpha_i^k \in \mathbf{Q}$, pour tout $k \in \mathbf{N}$.
(ii) Montrer que $\prod_{i=1}^n (X - \alpha_i^3) \in \mathbf{Q}[X]$.

Exercice 4.10. — Si $k \geqslant 1$, on définit la *somme de Newton* S_k par $S_k = X_1^k + \cdots + X_n^k$.
(i) Établir la formule $\sum_{i=1}^n \frac{1}{X - X_i} = \frac{nX^{n-1} - (n-1)\Sigma_1 X^{n-1} + (n-2)\Sigma_2 X^{n-2} \cdots}{X^n - \Sigma_1 X^{n-1} + \Sigma_2 X^{n-2} + \cdots}$.
(ii) En déduire l'identité $\sum_{k=1}^{+\infty} S_k T^k = \frac{\Sigma_1 T - 2\Sigma_2 T^2 + 3\Sigma_3 T^3 \cdots}{1 - \Sigma_1 T + \Sigma_2 T^2 - \Sigma_3 T^3 + \cdots}$, et calculer S_2, S_3.
(iii) Soit $M \in M_n(\mathbf{C})$ tel que $\mathrm{Tr}(M^k) = 0$, pour tout $k \geqslant 1$. Montrer que M est nilpotente.

Exercice 4.11. — $\alpha \in \mathbf{C}$ est un *entier algébrique* s'il existe $P \in \mathbf{Z}[X]$, unitaire, tel que $P(\alpha) = 0$.
(i) Soient α, β deux entiers algébriques. Montrer que $\alpha + \beta$ et $\alpha\beta$ sont des entiers algébriques. (On pourra considérer les polynômes $\prod_{(i,j) \in I \times J} (X - \alpha_i - \beta_j)$ et $\prod_{(i,j) \in I \times J} (X - \alpha_i \beta_j)$, où les α_i, pour $i \in I$ (resp. β_j, pour $j \in J$) sont les racines d'un polynôme unitaire P (resp. Q), à cofficients dans $\mathbf{Z}$, tel que $P(\alpha) = 0$ (resp. $Q(\beta) = 0$).)
(ii) En déduire que les entiers algébriques forment un anneau. Cet anneau contient-il $\frac{1}{2}$?

4.5. Anneaux noethériens

Un anneau A est *noethérien* si toute suite croissante d'idéaux est stationnaire (i.e., si $I_0 \subset I_1 \subset \dots$ sont des idéaux de A, il existe $n_0 \in \mathbf{N}$ tel que $I_n = I_{n_0}$ pour tout $n \geqslant n_0$).

Un corps K est noethérien car il n'a que deux idéaux $\{0\}$ et K ; un anneau principal est noethérien (cf. n° 4.2), et dans un anneau noethérien [53] tout idéal propre est contenu dans un idéal maximal (cf. n° 4.2).

Si A est un anneau, on dit qu'un A-module M est *de type fini*, si on peut trouver une famille finie $x_1, \dots, x_n$ d'éléments de M engendrant M, ce qui équivaut à ce que l'application $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i x_i$ soit une surjection de A^n sur M.

• A est noethérien si et seulement si tout idéal de A est de type fini.

Supposons que tout idéal soit engendré par un nombre fini d'éléments, et soit $I_0 \subset I_1 \subset \dots$ une suite croissante d'idéaux de A. Alors $I = \cup_{n \in \mathbf{N}} I_n$ est un idéal de A car la suite est croissante, et il existe $x_1, \dots, x_m$ tel que $I = (x_1, \dots, x_m)$. Comme les x_i appartiennent à I, il existe n_i tel que $x_i \in I_{n_i}$, et comme la suite est croissante les x_i appartiennent à I_n pour

53. C'est vrai pour un anneau quelconque, si on admet l'axiome du choix.

tout $n \geqslant \sup_{1\leqslant i\leqslant m} n_i$. Mais alors I_n contient l'idéal engendré par les x_i, c'est-à-dire I, et donc $I_n = I$ pour tout $n \geqslant \sup_{1\leqslant i\leqslant m} n_i$; la suite est donc stationnaire, et A est noethérien.

Réciproquement, si I est un idéal de A, on construit une suite d'éléments de I de la manière suivante. On part de $x_0 \in I$ quelconque. Si $x_0, \ldots, x_n$ sont construits, on note I_n l'idéal $(x_0, \ldots, x_n)$ engendré par $x_0, \ldots, x_n$. Si $I = I_n$, cela prouve que I est engendré par un nombre fini d'éléments. Si $I_n \neq I$, on choisit $x_{n+1} \in I - I_n$, et donc I_{n+1} contient strictement I_n. Si A est noethérien, le processus doit s'arrêter sinon on aurait une suite strictement croissante d'idéaux de A ; on a donc $I = I_n$ pour un certain n, ce qui prouve que I est engendré par un nombre fini d'éléments.

Ceci permet de conclure.

Exercice 4.12. — Soit K un corps commutatif et soit I_n l'idéal de $K[X, Y]$ engendré par les produits de n éléments de (X, Y). Montrer que I_n ne peut pas être engendré par moins de $n+1$ éléments. (Considérer le $K[X, Y]$-module I_n/I_{n+1} ; la solution demande de savoir ce qu'est la dimension d'un K-espace vectoriel.)

• Si A est noethérien et I est un idéal de A, alors A/I est noethérien ; autrement dit, tout quotient d'un anneau noethérien est noethérien.

Soit J un idéal de A/I. Alors l'image inverse $\tilde{J}$ de J dans A est un idéal de A ; il est donc de type fini puisque A est noethérien, et l'image d'une famille génératrice finie de $\tilde{J}$ est une famille génératrice de J, ce qui prouve que J est de type fini, et que A/I est noethérien.

• Si A est noethérien, alors A[X] est noethérien (th. de la base de Hilbert, 1890).

Soit I un idéal de A[X]. Soit J l'idéal de A engendré par les coefficients dominants des éléments de I, et si $n \in \mathbf{N}$, soit J_n l'idéal engendré par les coefficients de X^n des éléments de degré $\leqslant n$ de I. Comme A est noethérien, J et les J_n sont de type fini, et on peut trouver $Q_1, \ldots, Q_m \in I$ dont les coefficients dominants engendrent I, et $R_{n,1}, \ldots, R_{n,m_n} \in I$, de degré $\leqslant n$, dont les coefficients de X^n engendrent J_n. Soit N le maximum des degrés des Q_i. Montrons que I est engendré par les Q_i et les $R_{n,j}$, pour $n \leqslant N - 1$. Pour ce faire, notons I' cet idéal, et prouvons, par récurrence sur $n = \deg P$, que $P \in I'$ si $P = a_n X^n + \cdots + a_0 \in I$.

◇ Si $n \leqslant N-1$, alors $a_n \in J_n$, et il existe donc $\lambda_1, \ldots, \lambda_{m_n} \in A$ tels que $P' = P - \sum_{i=1}^{m_n} \lambda_i R_{n,i}$ soit de degré $\leqslant n-1$. Alors $P' \in I$ puisque P et les $R_{n,i}$ sont des éléments de I, et l'hypothèse de récurrence implique que $P' \in I'$, et donc $P \in I'$ puisque les $R_{n,i}$ sont des éléments de I'.

◇ Si $n \geqslant N$, alors $a_n \in J$, et il existe donc $\lambda_1, \ldots, \lambda_m \in A$ tels que $P' = P - \sum_{i=1}^{m} \lambda_i X^{n-\deg Q_i} Q_i$ soit de degré $\leqslant n-1$. On en déduit, comme ci-dessus, que $P \in I'$.

Ceci permet de conclure.

• $K[X_1, \ldots, X_n]$, si K est un corps, et $\mathbf{Z}[X_1, \ldots, X_n]$ sont noethériens.

Cela suit, par récurrence, du point précédent et de ce que K et $\mathbf{Z}$ sont noethériens.

• Si A est noethérien, tout sous-A-module d'un A-module de type fini est de type fini.

Commençons par prouver, par récurrence sur n, qu'un sous-A-module de A^n est de type fini. Le résultat a déjà été établi pour $n = 1$ (tout idéal de A est de type fini). Supposons donc $n \geqslant 2$, et soit M un sous-A-module de A^n. Notons $\pi : A^n \to A$ la projection sur le dernier facteur : $\pi(x_1, \ldots, x_n) = x_n$. Le noyau de π est $A^{n-1} \times \{0\}$ et est naturellement isomorphe à A^{n-1}. Soient $M_1 = M \cap \operatorname{Ker} \pi$, et $M_2 = \pi(M) \subset A$. Alors M_2 est un sous-A-module de A et donc est de type fini, et on peut trouver $x_1, \ldots, x_r \in M$ tels que $\pi(x_1), \ldots, \pi(x_r)$ engendrent M_2 ; de même M_1 est un sous-A-module de $\operatorname{Ker} \pi \cong A^{n-1}$, et on peut, grâce à l'hypothèse de récurrence,

trouver $y_1, \dots, y_s \in \mathrm{M}_1$ engendrant M_1. Montrons que $x_1, \dots, x_r, y_1, \dots, y_s$ engendrent M, ce qui permettra de conclure. Si $z \in \mathrm{M}$, on a $\pi(z) \in \mathrm{M}_2$, et il existe $a_1, \dots, a_r \in \mathrm{A}$ tels que $\pi(z) = a_1\pi(x_1) + \cdots + a_r\pi(x_r)$. Mais alors $z' = z - a_1x_1 - \cdots - a_rx_r$ vérifie $\pi(z') = 0$, et donc $z' \in \operatorname{Ker}\pi$. Comme $z' \in \mathrm{M}$ puisque z et les x_i sont des éléments de M, on a $z \in \mathrm{M}_1$ et il existe $b_1, \dots, b_s \in \mathrm{A}$ tels que $z = a_1x_1 + \cdots + a_rx_r + b_1y_1 + \cdots + b_sy_s$. D'où le résultat.

Maintenant, si M est de type fini sur A, alors M est un quotient de A^n (si $x_1, \dots, x_n$ engendrent M, alors M est le quotient de A^n par le noyau de $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_ix_i$ car ce morphisme de A^n dans M est surjectif par hypothèse). Si M' est un sous-A-module de M, son image inverse $\tilde{\mathrm{M}}'$ est un sous-A-module de A^n et donc est de type fini d'après ce qui précède ; mais alors l'image dans M' d'une famille génératrice finie de $\tilde{\mathrm{M}}'$ est une famille génératrice finie de M', et donc M' est de type fini.

Ceci permet de conclure.

5. Algèbre linéaire

Dans tout ce qui suit, K est un corps commutatif.

5.1. Espaces vectoriels

Rappelons (cf. alinéa 2.2.4) qu'un *espace vectoriel* V sur K (ou un K-*espace vectoriel*) est un groupe commutatif pour une loi $+$, muni d'une action de K (i.e. une application $(\lambda, x) \mapsto \lambda \cdot x$ de $\mathrm{K} \times \mathrm{V}$ dans V) vérifiant les propriétés suivantes :

$$1 \cdot x = x,\ \lambda \cdot (x+y) = (\lambda \cdot x) + (\lambda \cdot y),\ (\lambda+\mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x),\ \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x,$$

pour tous $x, y \in \mathrm{V}$ et $\lambda\mu \in \mathrm{K}$. En général, on note simplement λx l'élément $\lambda \cdot x$ de V. Un élément d'un espace vectoriel est un *vecteur* un élément de K est un *scalaire*.

Si V est un K-espace vectoriel, un *sous-espace vectoriel* (ou simplement *sous-espace*) de V est un sous-groupe de V stable sous l'action de K ; c'est donc naturellement un K-espace vectoriel, l'action de K étant celle induite par celle sur V.

• Si $n \in \mathbf{N}$, alors K^n muni de l'action $\lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n)$ est un K-espace vectoriel. (Si $n = 0$, on a $\mathrm{K}^n = \{0\}$ par convention.)

• Plus généralement, si I est un ensemble, l'ensemble K^{I} des fonctions $i \mapsto x_i$ ou $i \mapsto x(i)$ (notées aussi $(x_i)_{i\in\mathrm{I}}$) de I dans K, ou celui $\mathrm{K}^{(\mathrm{I})}$ des fonctions nulles presque partout (i.e. des $(x_i)_{i\in\mathrm{I}}$ avec $x_i = 0$ sauf pour un nombre fini de i) sont des K-espaces vectoriels (avec $(x_i)_{i\in\mathrm{I}} + (y_i)_{i\in\mathrm{I}} = (x_i+y_i)_{i\in\mathrm{I}}$ et $\lambda \cdot (x_i)_{i\in\mathrm{I}} = (\lambda x_i)_{i\in\mathrm{I}}$). De plus, $\mathrm{K}^{(\mathrm{I})}$ est un sous-espace vectoriel de K^{I}, strictement inclus dans K^{I} si I est infini ; par contre, on a $\mathrm{K}^{(\mathrm{I})} = \mathrm{K}^{\mathrm{I}}$ si I est fini, et si $\mathrm{I} = \{1, 2, \dots, n\}$, on retombe sur l'espace K^n du point précédent.

• L'intersection $\cap_{i\in\mathrm{I}}\mathrm{V}_i$ d'une famille quelconque de sous-espaces est un sous-espace vectoriel (cf. n° 2.3). La *somme* $\sum_{i\in\mathrm{I}}\mathrm{V}_i$ d'une famille quelconque de sous-espaces est un sous-espace vectoriel (c'est l'image de l'application linéaire $(x_i)_{i\in\mathrm{I}} \mapsto \sum_{i\in\mathrm{I}} x_i$ de $\oplus_{i\in\mathrm{I}}\mathrm{V}_i$ dans V, cf. alinéa 2.6.2) ; c'est aussi le sous-espace de V engendré par les V_i. On rappelle que les V_i sont *en somme directe dans* V, si $(x_i)_{i\in\mathrm{I}} \mapsto \sum_{i\in\mathrm{I}} x_i$ est injective, et que V *est la*

somme directe des V_i si c'est une bijection (ce que l'on note sous la forme $V = \oplus_{i\in I} V_i$) ; si $V = V_1 \oplus V_2$, on dit que V_1 et V_2 sont *supplémentaires*.

• Voici quelques exemples moins banals d'espaces vectoriels :

◇ Si X est un espace topologique, l'espace $\mathscr{C}(X, \mathbf{K})$ des fonctions continues $f : X \to \mathbf{K}$ est un sous-$\mathbf{K}$-espace vectoriel de $\mathbf{K}^X$, si $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$ (ou plus généralement un corps muni d'une norme de corps) : cela suit de ce que la somme de deux fonctions continues est continue et le produit d'une fonction continue par une constante aussi.

◇ Si I est un intervalle de $\mathbf{R}$, l'espace $\mathscr{C}^k(I)$ des $f : I \to \mathbf{C}$ de classe $\mathscr{C}^k$ (avec $k \in \mathbf{N} \cup \{\infty\}$) est un sous-$\mathbf{C}$-espace vectoriel de $\mathscr{C}(I, \mathbf{C})$.

◇ L'anneau K[X] des polynômes à coefficients dans K est un K-espace vectoriel ; il en est de même du sous-espace des polynômes de degré $\leqslant n$, pour tout $n \in \mathbf{N}$.

◇ Si E est un ensemble, l'ensemble $\mathscr{P}(E)$ des parties de E est un espace vectoriel sur $K = \mathbf{F}_2$: l'application $A \mapsto \mathbf{1}_A$ l'identifie à l'espace vectoriel K^E, l'addition dans K^E correspondant à la différence symétrique $(A \cup B) - (A \cap B)$ dans $\mathscr{P}(E)$ pour laquelle l'élément neutre est $\varnothing$ (c'est en fait une $\mathbf{F}_2$-algèbre, la multiplication des fonctions correspondant à l'intersection dans $\mathscr{P}(E)$).

5.2. Morphismes d'espaces vectoriels

Un *morphisme* $u : V_1 \to V_2$ de K-espaces vectoriels [54] est aussi appelé une *application linéaire*. Si u est en plus *bijectif*, on dit que c'est un *isomorphisme* de K-espaces vectoriels. Si $V_1 = V_2 = V$, on parle aussi d'*endomorphisme* de V (et d'*automorphisme* dans le cas bijectif) pour souligner le fait que l'espace d'arrivée est le même que celui de départ. Un endomorphisme s'appelle aussi souvent un *opérateur* (en particulier en analyse fonctionnelle). On note $\mathrm{Hom}(V_1, V_2)$ l'espace des morphismes de V_1 dans V_2 et $\mathrm{End}(V)$ celui des endomorphismes de V.

• Si $u \in \mathrm{Hom}(V_1, V_2)$ et $u' \in \mathrm{Hom}(V_2, V_3)$, alors $u' \circ u \in \mathrm{Hom}(V_1, V_3)$, et l'ensemble des automorphismes de V est un groupe pour la composition (cf. n° 2.4) ; la tradition veut qu'on le note $\mathrm{GL}(V)$ (pour « groupe général linéaire ») au lieu de $\mathrm{Aut}(V)$.

Si $u : V_1 \to V_2$ est un morphisme de K-espaces vectoriels, le noyau $\mathrm{Ker}\, u$ et l'image $\mathrm{Im}\, u$ de u, définis par $\mathrm{Ker}\, u = \{x \in V_1,\ u(x) = 0\}$ et $\mathrm{Im}\, u = \{y \in V_2,\ \exists x \in V_1,\ u(x) = y\}$, sont des sous-espaces vectoriels de V_1 et V_2 respectivement. De plus, u est injectif si et seulement si $\mathrm{Ker}\, u = \{0\}$, et surjectif si et seulement si $\mathrm{Im}\, u = V_2$.

• $\mathrm{Hom}(V_1, V_2)$ est naturellement un K-espace vectoriel (avec $(u_1 + u_2)(x) = u_1(x) + u_2(x)$ et $(\lambda u)(x) = \lambda u(x)$).

La vérification est un pur jeu d'écriture.

• $\mathrm{End}(V)$ muni de $+$ et $\circ$ est un anneau et même une K-algèbre, dont $\mathrm{GL}(V)$ est le groupe des éléments inversibles (cf. alinéa 2.2.2).

Comme $\mathrm{End}(V)$ est déjà un K-espace vectoriel, il s'agit de vérifier la distributivité de la composition par rapport à l'addition, ainsi que l'identité $u \circ (\lambda u') = \lambda(u \circ u') = (\lambda u) \circ u'$.

54. On renvoie aux n^{os} 2.4 et 2.5 pour les propriétés de base des morphismes, en particulier ce qui concerne noyau et image.

◇ $((u_1+u_2)\circ u')(x) = (u_1+u_2)(u'(x)) = u_1(u'(x))+u_2(u'(x)) = (u_1\circ u'+u_2\circ u')(x)$, pour tout $x \in \mathrm{V}$, et donc $(u_1+u_2)\circ u' = u_1\circ u'+u_2\circ u'$,

◇ $(u\circ(u'_1+u'_2))(x) = u((u'_1+u'_2)(x)) = u(u'_1(x)+u'_2(x)) = u(u'_1(x))+u(u'_2(x))$ par linéarité ; on en déduit la formule $u\circ(u'_1+u'_2) = u\circ u'_1+u\circ u'_2$,

◇ $(u\circ(\lambda u'))(x) = u((\lambda u')(x)) = u(\lambda u'(x)) = \lambda u(u'(x))$ par linéarité, et donc $u\circ(\lambda u') = \lambda(u\circ u')$; de même $((\lambda u)\circ u')(x) = (\lambda u)(u'(x)) = \lambda u(u'(x))$, et donc $(\lambda u)\circ u' = \lambda(u\circ u')$.

Si $u \in \mathrm{End}(\mathrm{V})$ on dit que $\lambda \in \mathrm{K}$ est une *valeur propre* de u s'il existe $x \in \mathrm{V}$, non nul, tel que $u(x) = \lambda x$. Si $\lambda \in \mathrm{K}$ est une valeur propre de u, l'*espace propre* associé à λ est l'ensemble V_λ des $x \in \mathrm{V}$ vérifiant $u(x) = \lambda x$; alors V_λ est aussi le noyau de $u - \lambda\,\mathrm{id}$, et donc est un sous-espace vectoriel de V ; les éléments de V_λ sont les *vecteurs propres pour la valeur propre* λ, et on dit que $x \in \mathrm{V}$ est un *vecteur propre* s'il existe $\lambda \in \mathrm{K}$ tel que $u(x) = \lambda x$.

• Si les λ_i, pour $i \in \mathrm{I}$, sont des valeurs propres distinctes de u, les V_{λ_i} sont en somme directe dans V.

Soit $\mathrm{J} \subset \mathrm{I}$ fini, et soient $x_j \in \mathrm{V}_{\lambda_j}$ pour $j \in \mathrm{J}$, tels que $\sum_{j\in\mathrm{J}} x_j = 0$. Montrons, par récurrence sur $|\mathrm{J}|$ que tous les x_j sont nuls, ce qui permettra de conclure. Si $|\mathrm{J}| = 1$, le résultat est évident. Supposons donc $|\mathrm{J}| \geqslant 2$. Alors $0 = u\big(\sum_{j\in\mathrm{J}} x_j\big) = \sum_{j\in\mathrm{J}} \lambda_j x_j$, et si $j_0 \in \mathrm{J}$, on a aussi $\sum_{j\in\mathrm{J}-\{j_0\}}(\lambda_j-\lambda_{j_0})x_j = 0$. L'hypothèse de récurrence implique que $(\lambda_j-\lambda_{j_0})x_j = 0$, et donc que $x_j = 0$ puisque $\lambda_j - \lambda_{j_0} \neq 0$, pour tout $j \neq j_0$; d'où le résultat.

5.2.1. *Homothéties, projections, symétries*

• Si $\lambda \in \mathrm{K}$, on note encore λ l'*homothétie* de rapport λ : c'est l'élément de End(V) défini par $\lambda(v) = \lambda v$, pour tout $v \in \mathrm{V}$. Si $u \in \mathrm{End}(\mathrm{V})$, on a $\lambda\circ u = \lambda u = u\circ\lambda$, et donc l'homothétie de rapport λ est dans le centre de End(V) (i.e elle commute à tout élément de End(V)), et l'homothétie de rapport 1 est l'élément neutre de End(V) pour la multiplication.

On a $\lambda\circ u(v) = \lambda(u(v)) = \lambda u(v) = (\lambda u)(v)$, et $u\circ\lambda(v) = u(\lambda(v)) = u(\lambda v) = \lambda u(v) = (\lambda u)(v)$, pour tout $v \in \mathrm{V}$. On en déduit que $\lambda\circ u = \lambda u = u\circ\lambda$. Le reste s'en déduit.

• On dit que $p \in \mathrm{End}(\mathrm{V})$ est une *projection* si $p\circ p = p$. Si p est une projection, alors $\mathrm{Im}\,p$ est un supplémentaire de $\mathrm{Ker}\,p$ et on a $p(v_1+v_2) = v_1$, si $v_1 \in \mathrm{Im}\,p$ et $v_2 \in \mathrm{Ker}\,p$; en particulier, $\mathrm{Im}\,p$ est l'ensemble des points fixes de p, et les valeurs propres de p sont 0 et 1 sauf si $p = 0$ (resp. $p = 1$) où 0 (resp. 1) est la seule valeur propre.

Réciproquement, si V_1,V_2 sont deux sous-espaces supplémentaires de V, l'application $p : \mathrm{V} \to \mathrm{V}$, définie par $p(v_1+v_2) = v_1$ si $v_1 \in \mathrm{V}_1$ et $v_2 \in \mathrm{V}_2$, est une projection dont l'image est V_1 et le noyau V_2 : c'est la *projection sur* V_1 *parallèlement à* V_2.

On peut écrire $v \in \mathrm{V}$ sous la forme $v = v_1+v_2$, avec $v_1 = p(v) \in \mathrm{Im}\,p$ et $v_2 = v-p(v) \in \mathrm{Ker}\,p$ car $p(v-p(v)) = p(v)-p\circ p(v) = p(v)-p(v) = 0$. Par ailleurs, si $v \in \mathrm{Im}\,p \cap \mathrm{Ker}\,p$, alors $v = p(v')$ et $p(v) = p\circ p(v') = p(v') = v$ car $v \in \mathrm{Im}\,p$, et $p(v) = 0$, puisque $v \in \mathrm{Ker}\,p$, et donc $v = 0$. On en déduit que $\mathrm{Im}\,p$ et $\mathrm{Ker}\,p$ sont des sous-espaces supplémentaires dans V, et que ce sont les espaces propres associées aux valeurs propres 0 et 1 ; il n'y a donc pas d'autre valeur propre que 0 et 1. Le reste de l'énoncé est immédiat.

• On dit que $s \in \mathrm{End}(\mathrm{V})$ est une *symétrie* si $s \circ s = 1$. Si s est une symétrie, alors V est la somme directe des espaces propres V^+ et V^- associés aux valeurs propres 1 et -1, et on a $s(v_1 + v_2) = v_1 - v_2$, si $v_1 \in \mathrm{V}^+$ et $v_2 \in \mathrm{V}^-$.

Réciproquement, si V_1,V_2 sont deux sous-espaces supplémentaires de V, l'application $s : \mathrm{V} \to \mathrm{V}$, définie par $s(v_1+v_2) = v_1-v_2$ si $v_1 \in \mathrm{V}_1$ et $v_2 \in \mathrm{V}_2$, est une symétrie vérifiant $\mathrm{Ker}\,(s-1) = \mathrm{V}_1$ et $\mathrm{Ker}(s+1) = \mathrm{V}_2$: c'est la *symétrie par rapport à* V_1 *parallèlement à* V_2, et on a $s = 2p - 1$, si p est la projection sur V_1 parallèlement à V_2.

Soit $p = \frac{s+1}{2}$. Alors $p \circ p = \frac{(s+1)\circ(s+1)}{4} = \frac{s\circ s+s\circ 1+1\circ s+1}{4} = \frac{1+s+s+1}{4} = p$. Comme $s(v) = v$ équivaut à $p(v) = v$ et $s(v) = -v$ à $p(v) = 0$, on peut déduire l'énoncé de celui concernant les projections. En particulier, $v_1 = p(v) = \frac{v+s(v)}{2}$ et $v_2 = (1-p)(v) = \frac{v-s(v)}{2}$. (On pourrait aussi raisonner directement en modifiant convenablement la démonstration faite pour les projections.)

Exercice 5.1. — Notons $\mathscr{C}^\infty(\mathbf{R})$ le $\mathbf{C}$-espace vectoriel des $\phi : \mathbf{R} \to \mathbf{C}$, de classe $\mathscr{C}^\infty$. Soient $u : \mathscr{C}^\infty(\mathbf{R}) \to \mathscr{C}^\infty(\mathbf{R})$ et $v : \mathscr{C}^\infty(\mathbf{R}) \to \mathscr{C}^\infty(\mathbf{R})$ définies par $u(\phi) = \phi'$ et $(v(\phi))(x) = \int_0^x \phi(t)\,dt$.

(i) Vérifier que u et v sont linéaires.

(ii) Que vaut $u \circ v$? Montrer que $v \circ u$ est une projection, et déterminer son noyau et son image.

Exercice 5.2. — Notons $\mathscr{C}(\mathbf{R})$ le $\mathbf{C}$-espace vectoriel des $\phi : \mathbf{R} \to \mathbf{C}$, continues. Si $\phi \in \mathscr{C}(\mathbf{R})$, on note $s(\phi)$ la fonction définie par $(s(\phi))(x) = \phi(-x)$.

(i) Vérifier que s est une symétrie de $\mathscr{C}(\mathbf{R})$.

(ii) On dit que $\phi \in \mathscr{C}(\mathbf{R})$ est *paire* si $\phi(-x) = \phi(x)$ pour tout $x \in \mathbf{R}$ et *impaire* si $\phi(-x) = -\phi(x)$ pour tout $x \in \mathbf{R}$. Montrer que tout $\phi \in \mathscr{C}(\mathbf{R})$ peut s'écrire de manière unique sous la forme $\phi = \phi^+ + \phi^-$, avec $\phi^+ \in \mathscr{C}(\mathbf{R})$ paire, et $\phi^- \in \mathscr{C}(\mathbf{R})$ impaire.

5.3. Familles libres, familles génératrices, bases

Soit V un K-espace vectoriel et soit $(v_i)_{i\in \mathrm{I}}$ une famille d'éléments de V. On dit que $v \in \mathrm{V}$ est une *combinaison linéaire* des v_i si v est dans l'image de l'application de $\mathrm{K}^{(\mathrm{I})}$ dans V, qui envoie $(x_i)_{i\in \mathrm{I}}$ sur $\sum_{i\in \mathrm{I}} x_i v_i$ (notons que cette somme est en fait finie puisqu'il n'y a qu'un nombre fini de $x_i \neq 0$; par ailleurs $(x_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} x_i v_i$ est linéaire de manière évidente) ; autrement dit, v est une combinaison linéaire des v_i s'il existe $\mathrm{J} \subset \mathrm{I}$ *fini* et des $x_j \in \mathrm{K}$, pour $j \in \mathrm{J}$, tels que $v = \sum_{j\in \mathrm{J}} x_j v_j$.

• L'ensemble $\mathrm{Vect}(v_i,\ i \in \mathrm{I})$ des combinaisons linéaires des v_i est le plus petit sous-espace vectoriel de V contenant les v_i ; autrement dit, c'est le sous-espace vectoriel de V *engendré* par les v_i. On dit que les v_i forment une *famille génératrice* de V si le sous-espace vectoriel de V engendré par les v_i est V tout entier, ce qui équivaut à la surjectivité de l'application $(x_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} x_i v_i$ de $\mathrm{K}^{(\mathrm{I})}$ dans V.

L'ensemble des combinaisons linéaires des v_i est l'image de $\mathrm{K}^{(\mathrm{I})}$ par l'application linéaire $(x_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} x_i v_i$; c'est donc un sous-espace vectoriel de V. Par ailleurs, si V' est un sous-espace vectoriel de V qui contient les v_i, alors V' contient toute combinaison linéaire des v_i puisqu'il est stable par multiplication par un élément de K et par addition.

• On dit que les v_i forment une *famille libre* si $(x_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} x_i v_i$, de $\mathrm{K}^{(\mathrm{I})}$ dans V, est injective. Dans le cas contraire, on dit que la famille est *liée*. Comme une application

linéaire est injective si et seulement si son noyau est nul, les v_i forment une famille libre si et seulement si la nullité de $\sum_{j\in \mathrm{J}} x_j v_j$, où $\mathrm{J} \subset \mathrm{I}$ est fini, implique celle des x_j.

• Si les v_i forment une famille libre et si $v \in \mathrm{V}$ n'appartient pas à $\mathrm{Vect}(v_i,\ i \in \mathrm{I})$, la famille formée de v et des v_i est encore libre.

Soi $xv + \sum_{j\in \mathrm{J}} x_j v_j$, avec $\mathrm{J} \subset \mathrm{I}$ fini, une combinaison linéaire nulle de v et des v_i. Si $x \neq 0$, on obtient $v = \sum_{j\in \mathrm{J}} \frac{-x_j}{x} v_j$, ce qui montre que $v \in \mathrm{Vect}(v_i,\ i \in \mathrm{I})$ contrairement à l'hypothèse. On a donc $x = 0$ et $\sum_{j\in \mathrm{J}} x_j v_j = 0$, et comme les v_i forment une famille libre, cela implique que $x_j = 0$ pour tout j. On en déduit le résultat.

• On dit que les v_i forment une *base* de V si c'est une famille libre et génératrice, ce qui équivaut à ce que l'application linéaire $(x_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} x_i v_i$ soit un isomorphisme de $\mathrm{K}^{(\mathrm{I})}$ sur V. Autrement dit, les v_i forment une base de V si et seulement si tout élément v de V peut s'écrire, de manière unique, sous la forme $\sum_{i\in \mathrm{I}} x_i v_i$; les x_i sont les *coordonnées* de v dans la base des v_i (elles sont donc nulles sauf pour un nombre fini).

• Si $n \geqslant 1$, les vecteurs $e_i = (0, \dots, 0, 1, 0, \dots 0)$ (le 1 est à la i-ième place), pour $1 \leqslant i \leqslant n$, forment une base de K^n ; c'est la *base canonique* de K^n (en particulier, l'ensemble vide $\varnothing$ est une base de l'espace vectoriel $\{0\}$).

Tout $x = (x_1, \dots, x_n) \in \mathrm{K}^n$ peut s'écrire de manière unique comme une combinaison linéaire des e_i, à savoir $x = \sum_{i=1}^{n} x_i e_i$.

• Les monômes X^n, pour $n \in \mathbf{N}$, forment une base de $\mathrm{K}[\mathrm{X}]$; c'est la *base canonique* de $\mathrm{K}[\mathrm{X}]$; de même, les X^i, pour $i \leqslant n$, forment une base de l'espace $\mathrm{K}[\mathrm{X}]^{(n)}$ des polynômes de degré $\leqslant n$.

• Plus généralement, soit $e_i : \mathrm{I} \to \mathrm{K}$ est la fonction définie par $e_i(j) = 1$ si $i = j$ et $e_i(j) = 0$ si $i \neq j$; alors les e_i, pour $i \in \mathrm{I}$, forment une base de $\mathrm{K}^{(\mathrm{I})}$; c'est la *base canonique* de $\mathrm{K}^{(\mathrm{I})}$.

• Soit $u : \mathrm{V}_1 \to \mathrm{V}_2$ un morphisme de K-espaces vectoriels. Si $(e_i)_{i\in \mathrm{I}}$ est une base de V_1, alors :

◇ u est surjectif, si et seulement si $(u(e_i))_{i\in \mathrm{I}}$ est une famille génératrice de V_2 ;
◇ u est injectif, si et seulement si $(u(e_i))_{i\in \mathrm{I}}$ est une famille libre de V_2 ;
◇ u est bijectif, si et seulement si $(u(e_i))_{i\in \mathrm{I}}$ est une base de V_2.

$\mathrm{Im}\, u$ est le sous-espace de V_2 engendré par les $u(e_i)$ puisque les e_i engendrent V_1 ; on en déduit le premier point.

$\sum_{i\in \mathrm{I}} \lambda_i e_i \in \mathrm{Ker}\, u$ si et seulement si $\sum_{i\in \mathrm{I}} \lambda_i u(e_i) = 0$. Il s'ensuit que $\mathrm{Ker}\, u$ n'est pas réduit à $\{0\}$ (ce qui équivaut à u non injectif) si et seulement si les $u(e_i)$ forment une famille liée ; d'où le second point.

Le dernier point résultant des deux premiers, cela permet de conclure.

Exercice 5.3. — Soient $\alpha_0, \dots, \alpha_n \in \mathrm{K}$, distincts. Montrer que les polynômes d'interpolation de Lagrange $\mathrm{Q}_i = \prod_{j\neq i} \frac{\mathrm{X}-\alpha_j}{\alpha_i-\alpha_j}$ forment une base sur K de $\mathrm{K}[\mathrm{X}]^{(n)}$. Quelles sont les coordonnées de P dans cette base ?

Exercice 5.4. — (i) Montrer que les polynômes binomiaux $\binom{\mathrm{X}}{n}$ forment une base de $\mathbf{C}[\mathrm{X}]$, et que les $\binom{\mathrm{X}}{i}$, pour $i \leqslant n$, forment une base de $\mathbf{C}[\mathrm{X}]^{(n)}$.

(ii) Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]^{(n)}$. Calculer les coordonnées de P dans la base des $\binom{\mathrm{X}}{i}$, pour $i \leqslant n$. (On pourra remarquer que $\binom{\mathrm{X}+1}{i} - \binom{\mathrm{X}}{i} = \binom{\mathrm{X}}{i-1}$, si $i \geqslant 1$.)

(iii) En déduire que $\mathrm{P}(k) \in \mathbf{Z}$ pour tout $k \in \mathbf{Z}$, si $\mathrm{P}(0), \mathrm{P}(1), \ldots, \mathrm{P}(n) \in \mathbf{Z}$.

Exercice 5.5. — Montrer que les $x \mapsto |x - a|$, pour $a \in \mathbf{R}$, forment une famille libre dans $\mathscr{C}(\mathbf{R})$.

Exercice 5.6. — Montrer que les familles suivantes de fonctions de $\mathbf{R}$ dans $\mathbf{C}$ sont libres dans $\mathscr{C}(\mathbf{R})$.

(i) Les $x \mapsto e^{ax}$, pour $a \in \mathbf{R}$. (Regarder le comportement en $+\infty$.)

(ii) Les $x \mapsto e^{iax}$, pour $a \in \mathbf{R}$. (Intégrer contre e^{-ibx}.)

(iii) Les $x \mapsto e^{\lambda x}$, pour $\lambda \in \mathbf{C}$. (Dériver ou translater.)

(iv) Montrer que la famille des $x \mapsto \sin ax$ et $x \mapsto \cos ax$, pour $a \in \mathbf{R}_+^*$, est libre et que l'espace engendré ne contient pas les fonctions constantes non nulles.

Exercice 5.7. — Si $k \in \mathbf{N}$, on définit le polylogarithme $\mathrm{Li}_k(x)$ sur $]-1, 1[$, par $\mathrm{Li}_k(x) = \sum_{n \geqslant 1} \frac{x^n}{n^k}$. Montrer que les Li_k, pour $k \in \mathbf{N}$, forment une famille libre. (On pourra calculer $x\frac{d}{dx}\mathrm{Li}_k$.)

Exercice 5.8. — Un *caractère linéaire* χ d'un groupe G est un morphisme de groupes de G dans $\mathbf{C}^*$.

(i) Montrer que les caractères linéaires d'un groupe G forment une famille libre. (Remplacer g par hg dans une relation de longueur minimale.)

(ii) Retrouver les résultats de l'ex. 5.6.

Exercice 5.9. — Montrer que les $\log p$, pour p nombre premier, sont linéairement indépendants sur $\mathbf{Q}$.

5.4. Espaces vectoriels de dimension finie

5.4.1. *Dimension d'un espace vectoriel*

Soit V un K-espace vectoriel. On dit que V est *de dimension finie* s'il possède une famille génératrice finie. Dans le cas contraire, on dit que V est *de dimension infinie*.

• Un K-espace vectoriel de dimension finie possède des bases : on peut extraire de toute famille génératrice finie une base [55].

> Soit $(v_i)_{i \in \mathrm{I}}$ une famille génératrice finie. Il y a deux cas :
>
> ◇ Cette famille est libre, et alors c'est une base et il n'y a rien à faire.
>
> ◇ Il existe une combinaison linéaire $\sum_{i \in \mathrm{I}} x_i v_i$ nulle, sans que les x_i soient tous nuls. Soit $i_0 \in \mathrm{I}$ tel que $x_{i_0} \neq 0$; alors v_{i_0} appartient au sous-espace engendré par les v_i, pour $i \in \mathrm{I} - \{i_0\}$, et donc les v_i, pour $i \in \mathrm{I} - \{i_0\}$, forment une famille génératrice de V puisque l'espace qu'ils engendrent contient la famille génératrice des v_i, pour $i \in \mathrm{I}$.
>
> Dans le second cas, on a réussi à extraire de $(v_i)_{i \in \mathrm{I}}$ une famille génératrice strictement plus petite (pour l'inclusion). En réitérant le processus, on construit de la sorte, tant que l'on n'est pas dans le premier cas, une suite de familles génératrices strictement décroissante (pour l'inclusion) et, le cardinal de I étant supposé fini, le processus s'arrête en un nombre fini d'étapes, et la famille obtenue est une base d'après la discussion ci-dessus, extraite de la famille des v_i par construction.

Si V est de dimension finie, on définit la *dimension* de V comme le minimum des cardinaux des bases de V.

• Si V est de dimension n, toutes les bases de V sont de cardinal n.

55. L'axiome du choix permet d'en faire autant en dim. infinie, à partir d'une famille génératrice infinie.

La démonstration se fait par récurrence sur n, l'énoncé étant vide si $n = 0$. Soit donc V de dimension $n \geqslant 1$, et soit $e_1, \dots, e_n$ une base de V. Soit $v_1, \dots, v_m$ une autre base de V ; on a donc $m \geqslant n$ et on veut prouver que $m = n$. Comme $v_1, \dots, v_m$ est une famille génératrice de V, il existe i tel que v_i n'appartienne pas au sous-espace vectoriel W engendré par $e_2, \dots, e_n$ et on peut supposer, quitte à renuméroter les v_i, que c'est v_1. On écrit v_i dans la base des e_j sous la forme $v_i = \sum_{j=1}^{n} x_{i,j} e_j$, et on a $x_{1,1} \neq 0$ puisque $v_1 \notin \mathrm{W}$, ce qui nous permet de définir des vecteurs $f_i = v_i - \frac{x_{i,1}}{x_{1,1}} v_1$, pour $2 \leqslant i \leqslant m$. Par construction, les f_i appartiennent à W. Montrons qu'ils en forment une base, ce qui permettra de conclure puisque W est de dimension $n-1$ (car de base $e_2, \dots, e_n$, et donc de dimension $\leqslant n-1$ et donc exactement $n-1$ par l'hypothèse de récurrence) et donc le cardinal de la famille des f_i (c'est-à-dire $m-1$) est égal à $n-1$, et $m = n$ comme souhaité.

◇ Si $\sum_{i=2}^{m} \lambda_i f_i = 0$, on a $\big(-\sum_{i=2}^{m} \lambda_i \frac{x_{i,1}}{x_{1,1}}\big) v_1 + \sum_{i=2}^{m} \lambda_i v_i = 0$, et donc $\lambda_2 = \cdots = \lambda_m = 0$, puisque les v_i forment une famille libre. Il s'ensuit que les f_i forment une famille libre.

◇ Comme les v_i forment une famille génératrice de V, on peut écrire tout $v \in \mathrm{W}$ sous la forme $\sum_{i=1}^{n} \lambda_i v_i = \sum_{i=2}^{n} \lambda_i f_i + \big(\lambda_1 - \sum_{i=2}^{m} \lambda_i \frac{x_{i,1}}{x_{1,1}}\big) v_1$. L'appartenance de v et des f_i à W entraine alors celle de $\big(\lambda_1 - \sum_{i=2}^{m} \lambda_i \frac{x_{i,1}}{x_{1,1}}\big) v_1$ à W, et comme v_1 n'appartient pas à W par hypothèse, cela implique que $\lambda_1 - \sum_{i=2}^{m} \lambda_i \frac{x_{i,1}}{x_{1,1}} = 0$ et $v = \sum_{i=2}^{n} \lambda_i f_i$. Il s'ensuit que les f_i forment une famille génératrice de W, ce qui permet de conclure.

• Si V_1 et V_2 sont de dimension finie, alors $\mathrm{V}_1 \oplus \mathrm{V}_2$ aussi et $\dim(\mathrm{V}_1 \oplus \mathrm{V}_2) = \dim \mathrm{V}_1 + \dim \mathrm{V}_2$.

Si $e_1, \dots, e_n$ est une base de V_1 et si $f_1, \dots, f_m$ est une base de V_2, alors $e_1, \dots, e_n, f_1, \dots, f_m$ est une base de $\mathrm{V}_1 \oplus \mathrm{V}_2$.

• Si $v_1, \dots, v_r$ est une famille libre, on peut trouver une base de V contenant $v_1, \dots, v_r$; plus précisément, si $w_1, \dots, w_s$ est une famille génératrice de V, on peut compléter $v_1, \dots, v_r$ en une base de V en lui ajoutant des w_i (th. de la base incomplète).

Soit X l'ensemble des parties I de $\{1, \dots, s\}$ telles que $v_1, \dots, v_r$ et les w_i, pour $i \in \mathrm{I}$, forment une famille libre. Soit $\mathrm{J} \subset \mathrm{X}$ maximale pour l'inclusion. Alors $v_1, \dots, v_r$ et les w_j, pour $j \in \mathrm{J}$, forment une famille libre par hypothèse. Par ailleurs, comme J est maximale, le sous-espace vectoriel W qu'ils engendrent contient w_i, si $i \notin \mathrm{J}$; il s'ensuit que W contient tous les w_i, et donc est égal à V puisque les w_i engendrent V. On en déduit que $v_1, \dots, v_r$ et les w_j, pour $j \in \mathrm{J}$, forment une famille génératrice et donc une base, ce qui permet de conclure.

• Si V est de dimension n, une famille libre de V a au plus n éléments ; la dimension de V est donc aussi le maximum des cardinaux des familles libres de V.

C'est, compte-tenu de ce qu'une base a (au plus) n éléments, une conséquence immédiate du point précédent.

• Si V n'est pas de dimension finie, alors V possède des familles libres infinies.

Commençons par remarquer qu'une famille infinie est libre si et seulement si toutes ses sous-familles finies le sont (une combinaison linéaire ne fait intervenir qu'un nombre fini de vecteurs). Pour construire une famille libre infinie, il suffit donc de construire par récurrence des vecteurs $v_1, \dots, v_n, \dots$ telle que $v_1, \dots, v_n$ soit libre pour tout n, et pour cela il suffit, $v_1, \dots, v_n$ étant donnés et formant une famille libre, de prendre v_{n+1} n'appartenant pas à l'espace engendré par $v_1, \dots, v_n$, ce qui est possible car V ne possède pas de famille génératrice finie (et donc $v_1, \dots, v_n$ n'engendrent pas V tout entier).

• Si V est de dimension n, et si $v_1, \dots, v_n$ sont des vecteurs de V, alors :

« $v_1, \dots, v_n$ est libre » $\Leftrightarrow$ « $v_1, \dots, v_n$ est génératrice » $\Leftrightarrow$ « $v_1, \dots, v_n$ est une base ».

Si $v_1, \dots, v_n$ est libre mais pas génératrice, on peut la compléter en une base de cardinal $> n$, ce qui est absurde et donc $v_1, \dots, v_n$ est aussi génératrice. Si $v_1, \dots, v_n$ est génératrice mais pas libre, on peut en extraire une base de cardinal $< n$, ce qui est absurde et donc $v_1, \dots, v_n$ est aussi libre.

• Si V est de dimension finie, et si W est un sous-espace vectoriel de V, alors W est de dimension finie et on a $\dim \mathrm{W} \leqslant \dim \mathrm{V}$ avec égalité si et seulement si $\mathrm{W} = \mathrm{V}$.

Une famille libre de W est aussi libre dans V, et donc toute famille libre de W est de cardinal $\leqslant \dim \mathrm{V}$. On en déduit que W est de dimension finie et que $\dim \mathrm{W} \leqslant \dim \mathrm{V}$. Maintenant, supposons que $\dim \mathrm{W} = \dim \mathrm{V}$; alors une base de W est une famille libre de V de cardinal $\dim \mathrm{V}$; c'est donc aussi une base de V d'après le point précédent ; on en déduit que $\mathrm{W} = \mathrm{V}$ ce qui conclut la démonstration.

• Si V est de dimension finie, et si W est un sous-espace de V, alors W possède des supplémentaires, et si W' est un supplémentaire de W, alors $\dim \mathrm{W}' = \dim \mathrm{V} - \dim \mathrm{W}$.

Pour construire un supplémentaire [56] de W, il suffit de partir d'une base $e_1, \dots, e_r$ de W, de la compléter en une base $e_1, \dots, e_n$ de V, et de prendre pour W' l'espace engendré par $e_{r+1}, \dots, e_n$: si $x = x_1e_1 + \cdots + x_ne_n \in \mathrm{V}$, alors $x = y + y'$ avec $y = x_1e_1 + \cdots + x_re_r \in \mathrm{W}$ et $y' = x_{r+1}e_{r+1} + \cdots + x_ne_n \in \mathrm{W}'$, et donc $\mathrm{V} = \mathrm{W} + \mathrm{W}'$. par ailleurs, si $x \in \mathrm{W} \cap \mathrm{W}'$, on peut écrire x sous la forme $x_1e_1 + \cdots + x_re_r$ et sous la forme $x_{r+1}e_{r+1} + \cdots + x_ne_n$, et donc $x_1e_1 + \cdots + x_re_r - x_{r+1}e_{r+1} - \cdots - x_ne_n = 0$, ce qui implique $x_1 = \cdots = x_n = 0$, puisque les e_i forment une base de V ; on a donc $\mathrm{W} \cap \mathrm{W}' = \{0\}$, et $\mathrm{V} = \mathrm{W} \oplus \mathrm{W}'$.

Enfin, si W' est un supplémentaire de W, on a $\mathrm{V} = \mathrm{W} \oplus \mathrm{W}'$, et donc $\dim \mathrm{V} = \dim \mathrm{W} + \dim \mathrm{W}'$ et $\dim \mathrm{W}' = \dim \mathrm{V} - \dim \mathrm{W}$.

5.4.2. *Morphismes*

• Soit $u : \mathrm{V}_1 \to \mathrm{V}_2$ un morphisme de K-espaces vectoriels. Alors V_1 est de dimension finie si et seulement si $\operatorname{Ker} u$ et $\operatorname{Im} u$ le sont, et $\dim \mathrm{V}_1 = \dim(\operatorname{Ker} u) + \dim(\operatorname{Im} u)$. (La dimension de $\operatorname{Im} u$ s'appelle le *rang* de u, et est aussi notée $\operatorname{rg} u$; la formule précédente peut donc aussi s'écrire $\dim \mathrm{V}_1 = \dim(\operatorname{Ker} u) + \operatorname{rg} u$.)

Supposons V_1 de dimension finie. Alors $\operatorname{Ker} u$ l'est aussi puisque c'est un sous-espace de V_1 et $\operatorname{Im} u$ l'est car l'image par u d'une famille génératrice de V_1 engendre $\operatorname{Im} u$.

Supposons maintenant $\operatorname{Ker} u$ et $\operatorname{Im} u$ de dimension finie, et choisissons une base $e_1, \dots, e_r$ de $\operatorname{Ker} u$, une base $f_1, \dots, f_r$ de $\operatorname{Ker} u$ et un relèvement g_i de f_i dans V_1 (i.e. un $g_i \in \mathrm{V}_1$ tel que $u(g_i) = f_i$). Montrons que $e_1, \dots, e_r, g_1, \dots, g_s$ est une base de V_1, ce qui prouvera à la fois que V_1 est de dimension finie et que $\dim \mathrm{V}_1 = \dim(\operatorname{Ker} u) + \dim(\operatorname{Im} u)$.

◇ Si $\sum_{i=1}^{r} \lambda_i e_i + \sum_{j=1}^{s} \mu_j g_j = 0$, appliquer u à cette relation nous donne $\sum_{j=1}^{s} \mu_j f_j = 0$, ce qui implique que les μ_j sont tous nuls ; on a alors $\sum_{i=1}^{r} \lambda_i e_i = 0$, ce qui implique que les λ_i sont aussi tous nuls. On en déduit que $e_1, \dots, e_r, g_1, \dots, g_s$ est une famille libre.

56. La même construction marche en dimension infinie, si on admet l'axiome du choix.

◇ Si $v \in \mathrm{V}_1$, il existe $\mu_1, \dots, \mu_s$ tels que $u(v) = \sum_{j=1}^{s} \mu_j f_j$. Alors $v - \sum_{j=1}^{s} \mu_j g_j$ appartient à $\operatorname{Ker} u$ et il existe $\lambda_1, \dots, \lambda_r$ tels que l'on ait $v - \sum_{j=1}^{s} \mu_j g_j = \sum_{i=1}^{r} \lambda_i e_i$. On en déduit que $e_1, \dots, e_r, g_1, \dots, g_s$ est une famille génératrice.

Ceci permet de conclure.

• Soit $u : \mathrm{V}_1 \to \mathrm{V}_2$ un morphisme de K-espaces vectoriels de dimension finie.

◇ Si u est surjectif, alors $\dim \mathrm{V}_1 \geqslant \dim \mathrm{V}_2$.

◇ Si u est injectif, alors $\dim \mathrm{V}_1 \leqslant \dim \mathrm{V}_2$.

◇ Si u est un isomorphisme, alors $\dim \mathrm{V}_1 = \dim \mathrm{V}_2$: deux espace isomorphes ont la même dimension.

Si u est surjectif, alors $\operatorname{Im} u = \mathrm{V}_2$ et $\dim \mathrm{V}_1 - \dim \mathrm{V}_2 = \dim(\operatorname{Ker} u) \geqslant 0$. Si u est injectif, alors $\operatorname{Ker} u = 0$ et donc $\operatorname{Im} u$ est de dimension $\dim \mathrm{V}_1$; comme c'est un sous-espace de V_2, on a $\dim \mathrm{V}_1 \leqslant \mathrm{V}_2$. Enfin, si u est un isomorphisme, alors u est surjectif et injectif, et on a $\dim \mathrm{V}_1 \geqslant \dim \mathrm{V}_2$ et $\dim \mathrm{V}_1 \leqslant \dim \mathrm{V}_2$ et donc $\dim \mathrm{V}_1 = \dim \mathrm{V}_2$.

• Soient $\mathrm{V}_1, \mathrm{V}_2$ des sous-K-espaces vectoriels de dimension finie d'un K-espace vectoriel W. Alors $\mathrm{V}_1 + \mathrm{V}_2$ et $\mathrm{V}_1 \cap \mathrm{V}_2$ sont de dimension finie et

$$\dim(\mathrm{V}_1 + \mathrm{V}_2) + \dim(\mathrm{V}_1 \cap \mathrm{V}_2) = \dim \mathrm{V}_1 + \dim \mathrm{V}_2 \qquad \text{(Grassmann, 1862).}$$

On applique le point précédent à $u : \mathrm{V}_1 \oplus \mathrm{V}_2 \to \mathrm{W}$ défini par $u(x, y) = x + y$; l'image de u est $\mathrm{V}_1 + \mathrm{V}_2$ et le noyau est l'ensemble des $(x, -x)$ avec $x \in \mathrm{V}_1 \cap \mathrm{V}_2$ (il est donc isomorphe à $\mathrm{V}_1 \cap \mathrm{V}_2$, en particulier il a la même dimension). Comme $\dim(\mathrm{V}_1 \oplus \mathrm{V}_2) = \dim \mathrm{V}_1 + \dim \mathrm{V}_2$, cela permet de conclure.

• Soit $u : \mathrm{V}_1 \to \mathrm{V}_2$ un morphisme de K-espaces vectoriels. Si $\dim \mathrm{V}_1 = \dim \mathrm{V}_2 < +\infty$,

« u est injectif » ⇔ « u est surjectif » ⇔ « u est un isomorphisme ».

« u est inversible » ⇔ « u a un inverse à droite » ⇔ « u a un inverse à gauche ».

Si u est injectif, on a $\dim(\operatorname{Ker} u) = 0$, $\dim(\operatorname{Im} u) = \dim \mathrm{V}_1 = \dim \mathrm{V}_2$ et donc $\operatorname{Im} u = \mathrm{V}_2$ et u est surjectif. Si u est surjectif, on a $\dim(\operatorname{Im} u) = \dim \mathrm{V}_2 = \dim \mathrm{V}_1$, et donc $\dim(\operatorname{Ker} u) = 0$ et u est injectif.

Maintenant, si $u \circ v = \mathrm{id}$, cela implique en particulier que u est surjectif et donc bijectif ; l'existence d'un inverse à droite implique donc que u est inversible. Si $v \circ u = \mathrm{id}$, cela implique en particulier que u est injectif et donc bijectif ; l'existence d'un inverse à gauche implique donc que u est inversible.

Notons que le résultat est faux en dimension infinie (cf. ex. 5.1).

5.5. Dualité

5.5.1. *Espace dual, orthogonal, morphisme transposé*

Si V est un K-espace vectoriel, une *forme linéaire* sur V est une application linéaire de V dans K. On note V^* le *dual* de V, c'est-à-dire l'espace $\operatorname{Hom}(\mathrm{V}, \mathrm{K})$ des formes linéaires sur V (c'est un K-espace vectoriel comme cas particulier de $\operatorname{Hom}(\mathrm{V}_1, \mathrm{V}_2)$). Si $\lambda \in \mathrm{V}^*$ et $x \in \mathrm{V}$, nous noterons souvent $\langle \lambda, x \rangle$ l'élément $\lambda(x)$ de K, de manière à établir une certaine symétrie entre V et V^*. En effet, si $x \in \mathrm{V}^*$, l'application $\lambda \mapsto \langle \lambda, x \rangle$ est linéaire par

définition de la structure d'espace vectoriel sur V^*, ce qui nous fournit une application naturelle [57] $\iota_V : V \to (V^*)^*$ avec $\langle \iota_V(x), \lambda \rangle = \langle \lambda, x \rangle$, qui est linéaire de manière évidente.

Si W est un sous-espace vectoriel de V, on définit l'*orthogonal* $W^\perp$ de W dans V^* comme l'ensemble des $\lambda \in V^*$ tels que $\langle \lambda, x \rangle = 0$ pour tout $x \in W$ (c'est donc l'intersection des noyaux des $\iota_V(x)$, pour $x \in W$, ce qui prouve que c'est un sous-espace vectoriel de V^*). Symétriquement, si W est un sous-espace vectoriel de V^*, on définit l'*orthogonal* $W^\perp$ de W dans V comme l'ensemble des $x \in V$ tels que $\langle \lambda, x \rangle = 0$ pour tout $\lambda \in W$. Il est immédiat que $W \subset (W^\perp)^\perp$ si $W \subset V$ ou si $W \subset V^*$.

Si $u : V_1 \to V_2$ est linéaire, on définit sa *transposée* ${}^t u : V_2^* \to V_1^*$ par ${}^t u(\lambda) = \lambda \circ u$; on a donc $\langle {}^t u(\lambda), x \rangle = \langle \lambda, u(x) \rangle$, pour tout $x \in V_1$ et $\lambda \in V_2^*$.

• Si $u : V_1 \to V_2$ et $v : V_2 \to V_3$ sont linéaires, alors ${}^t(v \circ u) = {}^t u \circ {}^t v$.

On a $\langle \lambda, v \circ u(x) \rangle = \langle {}^t v(\lambda), u(x) \rangle = \langle {}^t u \circ {}^t v(\lambda), x \rangle$; d'où le résultat.

5.5.2. *Le dual d'un espace de dimension finie*

Dans le reste de ce n°, les espaces sont implicitement de dimension finie.

• Si V est de dimension n, alors V^* est de dimension n ; plus précisément, si $e_1, \dots, e_n$ est une base de V, il existe une (unique) base $e_1^*, \dots, e_n^*$ de V^*, la *base duale* de $e_1, \dots, e_n$, telle que $\langle e_i^*, e_i \rangle = 1$ et $\langle e_i^*, e_j \rangle = 0$, si $j \neq i$.

Soit $\lambda \in V^*$ et soit $a_i = \langle \lambda, e_i \rangle$. Alors $\langle \lambda, x \rangle = a_1 x_1 + \cdots + a_n x_n$ par linéarité, si $x = x_1 e_1 + \cdots + x_n e_n$; réciproquement, si $a_1, \dots, a_n \in K^n$, alors $x \mapsto a_1 x_1 + \cdots + a_n x_n$ est l'unique forme linéaire λ sur V vérifiant $\langle \lambda, e_i \rangle = a_i$. En d'autres termes $\lambda \mapsto (\langle \lambda, e_1 \rangle, \dots, \langle \lambda, e_n \rangle)$ est un isomorphisme de V^* sur K^n. L'énoncé s'en déduit, la base duale de $e_1, \dots, e_n$ étant l'image réciproque de la base canonique de K^n par cet isomorphisme.

• L'application naturelle $\iota_V : V \to (V^*)^*$ est un isomorphisme ; autrement dit le dual de V^* est V. De plus, si $e_1, \dots, e_n$ est une base de V, et si $e_1^*, \dots, e_n^*$ est la base de V^* duale de $e_1, \dots, e_n$, alors la base de V, duale de $e_1^*, \dots, e_n^*$, est $e_1, \dots, e_n$.

Soit $x = x_1 e_1 + \cdots + x_n e_n \in \operatorname{Ker} \iota_V$; alors $\langle \lambda, x \rangle = 0$, pour tout $\lambda \in V^*$ et donc $0 = \langle e_i^*, x \rangle = x_i$, pour tout i. On a donc $\operatorname{Ker} \iota_V = 0$, ce qui prouve que ι_V est injective. Comme $\dim (V^*)^* = \dim V^* = \dim V$, l'injectivité de ι_V entraîne sa bijectivité. Le résultat s'en déduit (l'énoncé sur la dualité des bases est immédiat).

• Si $u : V_1 \to V_2$ est linéaire, alors ${}^t({}^t u) = u$.

${}^t({}^t u)$ est un morphisme de $(V_1^*)^*$ dans $(V_2^*)^*$, et pour le voir comme un morphisme de V_1 dans V_2, il faut utiliser les identifications naturelles $\iota_{V_1} : V_1 \cong (V_1^*)^*$ et $\iota_{V_2} : V_2 \cong (V_2^*)^*$. Cela dit, le résultat suit de ce que $\langle {}^t({}^t u)(\iota_{V_1}(x)), \lambda \rangle = \langle \iota_{V_1}(x), {}^t u(\lambda) \rangle = \langle {}^t u(\lambda), x \rangle = \langle \lambda, u(x) \rangle = \langle \iota_{V_2}(u(x)), \lambda \rangle$, pour tous $x \in V_1$ et $\lambda \in V_2^*$, ce qui nous donne ${}^t({}^t u) \circ \iota_{V_1} = \iota_{V_2} \circ u$.

57. Comme nous le verrons ci-dessous cette application est un isomorphisme si V est de dimension finie, ce qui permet d'identifier le dual de V^* à V et donc de faire jouer des rôles totalement symétriques à V et V^* ; si V est de dimension infinie, la situation est plus compliquée : si on admet l'axiome du choix, alors ι_V est injective, mais très loin d'être surjective car $(V^*)^*$ a un cardinal beaucoup plus grand que celui de V ; si on n'admet pas l'axiome du choix, on peut construire des espaces pour lesquels $V^* = \{0\}$.

• Si W est un sous-espace de V, alors $\dim \mathrm{W}^\perp = \dim \mathrm{V} - \dim \mathrm{W}$. En particulier, $\mathrm{V}^\perp = \{0\}$.

Soit $e_1, \dots, e_r$ une base de W, que l'on complète en une base $e_1, \dots, e_n$ de V (c'est possible d'après le th. de la base incomplète). Alors $\mathrm{W}^\perp$ est le sous-espace de V^* engendré par $e^*_{r+1}, \dots, e^*_n$ (en effet, on a $0 = \langle e^*_j, e_i\rangle$ si $j \geqslant r+1$ et $i \leqslant r$, ce qui prouve, par linéarité, que $e^*_j \in \mathrm{W}^\perp$; réciproquement, si $\lambda = \sum_{j=1}^n \lambda_j e^*_j \in \mathrm{W}^\perp$, on a $0 = \langle \lambda, e_i\rangle = \lambda_i$ si $i \leqslant r$, ce qui prouve que les e^*_j, pour $j \geqslant r+1$, engendrent $\mathrm{W}^\perp$). On en déduit le résultat.

• Si W est un sous-espace de V, alors $(\mathrm{W}^\perp)^\perp = \mathrm{W}$.

On a $\mathrm{W} \subset (\mathrm{W}^\perp)^\perp$, et cette inclusion est une égalité car

$$\dim(\mathrm{W}^\perp)^\perp = \dim \mathrm{V}^* - \dim \mathrm{W}^\perp = \dim \mathrm{V} - (\dim \mathrm{V} - \dim \mathrm{W}) = \dim \mathrm{W}.$$

• Si $u : \mathrm{V}_1 \to \mathrm{V}_2$ est linéaire, alors

$$\mathrm{Ker}\, {}^t u = (\mathrm{Im}\, u)^\perp, \ \ \mathrm{Im}\, {}^t u = (\mathrm{Ker}\, u)^\perp, \ \text{ et } \ \mathrm{rg}\, {}^t u = \mathrm{rg}\, u.$$

« $\lambda \in (\mathrm{Im}\, u)^\perp$ » $\Leftrightarrow$ « $\langle \lambda, u(x)\rangle = 0$, $\forall x \in \mathrm{V}_1$ » $\Leftrightarrow$ « $\langle {}^t u(\lambda), x\rangle = 0$, $\forall x \in \mathrm{V}_1$ » $\Leftrightarrow$ « ${}^t u(\lambda) \in \mathrm{V}_1^\perp$ »,
et comme $\mathrm{V}_1^\perp = \{0\}$, la dernière propriété équivaut à $\lambda \in \mathrm{Ker}\, {}^t u$. On en déduit la première égalité. La seconde s'obtient alors en échangeant les rôles de u et ${}^t u$ ce qui est loisible car ${}^t({}^t u) = u$, et en prenant les orthogonaux.

Enfin, $\mathrm{rg}\, {}^t u = \dim(\mathrm{Im}\, {}^t u) = \dim(\mathrm{Ker}\, u)^\perp = \dim \mathrm{V}_1 - \dim(\mathrm{Ker}\, u) = \dim(\mathrm{Im}\, u) = \mathrm{rg}\, u$.

6. Déterminants

Les déterminants et les formes multilinéaires alternées interviennent dans des contextes variés. En algèbre linéaire, ils peuvent servir à décider si des vecteurs sont liés ou pas (n° 6.2) ou si des polynômes ont des zéros communs (résultant de deux polynômes, alinéa 9.2.1), à donner des formules pour les solutions d'un système linéaire (formules de Cramer, alinéa 9.1.1) ; en géométrie, ils permettent de calculer des volumes (le volume du parallèlépipède supporté par des vecteurs $v_1, \dots, v_n$ de $\mathbf{R}^n$ est la valeur absolue de leur déterminant, ex. III.3.11).

6.1. Formes multilinéaires alternées

Soit V un K-espace vectoriel. Une *forme bilinéaire* f sur V est une application de $\mathrm{V} \times \mathrm{V}$ dans K, telle que $x \mapsto f(x, y)$ soit linéaire pour tout $y \in \mathrm{V}$ (i.e. f est linéaire en la première variable) et $y \mapsto f(x, y)$ soit linéaire pour tout $x \in \mathrm{V}$ (i.e. f est linéaire en la seconde variable). Plus généralement, une *forme k-linéaire* sur V est une application de $\mathrm{V}^k = \mathrm{V} \times \cdots \times \mathrm{V}$ dans K, linéaire en chacune des variable, ce qui signifie que, quel que soit $i \in \{1, \dots, k\}$, $v_i \mapsto f(v_1, \dots, v_k)$ est linéaire pour tout [58] $(v_1, \dots, \hat{v}_i, \dots, v_k) \in \mathrm{V}^{k-1}$.

Une forme k-linéaire f est dite *alternée* si elle change de signe quand on échange deux vecteurs consécutifs : i.e. si $f(v_1, \dots, v_i, v_{i+1}, \dots v_k) = -f(v_1, \dots, v_{i+1}, v_i, \dots, v_k)$ pour tous $i \in \{1, \dots, k\}$ et $(v_1, \dots, v_k) \in \mathrm{V}^k$.

Comme S_k est engendré par les transpositions $(i, i+1)$, pour $1 \leqslant i \leqslant k-1$, on obtient :

58. On utilise la notation standard $(v_1, \dots, \hat{v}_i, \dots, v_k)$ pour dénoter le $(k-1)$-uplet obtenu en retirant v_i à $(v_1, \dots, v_k)$.

• Si f est k-linéaire alternée, alors $f(v_{\sigma(1)},\dots,v_{\sigma(k)}) = \mathrm{sign}(\sigma) f(v_1,\dots,v_k)$, pour tous $\sigma \in \mathrm{S}_k$ et $(v_1,\dots,v_k) \in \mathrm{V}^k$.

En utilisant le point précédent pour amener les deux termes égaux aux deux premières places, on obtient :

• Si f est k-linéaire alternée, alors $f(v_1,\dots,v_k) = 0$ si deux des v_i sont égaux.
• Si f est k-linéaire alternée, alors $f(v_1,\dots,v_k)$ ne change pas si on rajoute à un des v_i une combinaison linéaire des autres ou des multiples d'un des v_i aux autres :

$$f(v_1,\dots,v_{i-1},v_i+\textstyle\sum_{j\neq i}\lambda_j v_j, v_{i+1},\dots,v_k) = f(v_1,\dots,v_k)$$
$$f(v_1+\lambda_1 v_i,\dots,v_{i-1}+\lambda_{i-1}v_i, v_i, v_{i+1}+\lambda_{i+1}v_i,\dots,v_k+\lambda_k v_i) = f(v_1,\dots,v_k)\,.$$

Établissons la seconde formule par exemple. La k-linéarité montre que le membre de gauche est égal à $f(v_1,\dots,v_k)+\sum_{\mathrm{I}\subset\{1,\dots,k\}-\{i\},\,\mathrm{I}\neq\varnothing}\big(\prod_{j\in\mathrm{I}}\lambda_j\big) f(v_{1,\mathrm{I}},\dots,v_{k,\mathrm{I}})$, où $v_{j,\mathrm{I}} = v_i$ si $j \in \mathrm{I}\cup\{i\}$ et $v_{j,\mathrm{I}} = v_j$ sinon. Comme $\mathrm{I}\neq\varnothing$, il y a au moins deux $v_{j,\mathrm{I}}$ qui sont égaux et $f(v_{1,\mathrm{I}},\dots,v_{k,\mathrm{I}}) = 0$ pour tout I, ce qui permet de conclure.

6.2. Déterminant de n vecteurs

On suppose dorénavant que V est de dimension n. Soit $e_1,\dots,e_n$ une base de V.

• Si $x = \sum_{i=1}^n x_i e_i$ et si f est une forme linéaire sur V, alors $f(x) = \sum_{i=1}^n x_i f(e_i)$.
Si $x = \sum_{i=1}^n x_i e_i$, si $y = \sum_{j=1}^n y_j e_j$ et si f est bilinéaire, $f(x,y) = \sum_{i=1}^n\sum_{j=1}^n x_i y_j f(e_i,e_j)$.
Plus généralement, si $x_j = \sum_{i=1}^n x_{j,i} e_i$, et si f est k-linéaire, alors

$$f(x_1,\dots,x_k) \sum_{1\leqslant i_1,\dots,i_k\leqslant n} x_{1,i_1}\cdots x_{k,i_k} f(e_{i_1},\dots,e_{i_k}) \tag{6.1}$$

L'énoncé est immédiat pour une forme linéaire. Si f est bilinéaire, la linéarité par rapport à la seconde variable nous donne $f(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j) = \sum_{j=1}^n y_j f(\sum_{i=1}^n x_i e_i, e_j)$; on obtient donc $f(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j) = \sum_{i=1}^n\sum_{j=1}^n x_i y_j f(e_i,e_j)$ en utilisant la linéarité par rapport à la première variable. Le cas d'une forme k-linéaire se démontre par récurrence sur k, en utilisant la linéarité par rapport à la dernière variable.

• Si V est de dimension n, l'espace $\det \mathrm{V}^*$ des formes n-linéaires alternées sur V est de dimension 1. De plus, si $e_1,\dots,e_n$ est une base de V, il existe un unique élément $\det_{e_1,\dots,e_n}$ (le *déterminant de n vecteurs dans la base* $e_1,\dots,e_n$) de $\det \mathrm{V}^*$ prenant la valeur 1 sur $(e_1,\dots,e_n)$, et on a :
◇ $\det_{e_1,\dots,e_n}(v_1,\dots,v_n) = 0$ si et seulement si $v_1,\dots,v_n$ est une famille liée ;
◇ $\det_{e_1,\dots,e_n}(v_1,\dots,v_n) \neq 0$ si et seulement si $v_1,\dots,v_n$ est une base ;
◇ si $f_1,\dots,f_n$ est une autre base de V, alors $\det_{f_1,\dots,f_n}(v_1,\dots,v_n) = \frac{\det_{e_1,\dots,e_n}(v_1,\dots,v_n)}{\det_{e_1,\dots,e_n}(f_1,\dots,f_n)}$,
pour tout $(v_1,\dots,v_n) \in \mathrm{K}^n$.

En utilisant le point précédent, on peut éliminer de la formule (6.1) (avec $k = n$) les n-uplets $(i_1,\dots,i_n)$ où deux i_j sont les mêmes, on a alors une somme portant sur des n-uplets $(i_1,\dots,i_n)$ où tous les termes sont distincts, c'est-à-dire sur les permutations de $\{1,\dots,n\}$ (il existe une unique $\sigma \in \mathrm{S}_n$ telle que $i_j = \sigma(j)$, pour tout $j \in \{1,\dots,n\}$, si les i_j sont tous

distincts). Comme $f(e_{\sigma(1)},\dots,e_{\sigma(n)}) = \mathrm{sign}(\sigma) f(e_1,\dots,e_n)$, on obtient :

$$f(v_1,\dots,v_n) = f(e_1,\dots,e_n)\Big(\sum_{\sigma\in \mathrm{S}_n} \mathrm{sign}(\sigma)\prod_{i=1}^n x_{i,\sigma(i)}\Big), \quad \text{si } v_i = \sum_{j=1}^n x_{i,j}e_j.$$

Notons $\det_{e_1,\dots,e_n}$ la forme $(v_1,\dots,v_n)\mapsto \sum_{\sigma\in \mathrm{S}_n}\mathrm{sign}(\sigma)\prod_{i=1}^n x_{i,\sigma(i)}$. La formule ci-dessus se réécrit sous la forme $f = f(e_1,\dots,e_n)\det_{e_1,\dots,e_n}$, ce qui prouve que $\det \mathrm{V}^*$ est de dimension au plus 1, engendré par $\det_{e_1,\dots,e_n}$ si cette forme est alternée.

On a $\det_{e_1,\dots,e_n}(e_1,\dots,e_n) = 1$ car tous les termes de la somme sont nuls sauf celui correspondant à $\sigma = \mathrm{id}$, ce qui prouve que $\det_{e_1,\dots,e_n} \neq 0$. Par ailleurs, si $\tau\in \mathrm{S}_n$, alors

$$\det_{e_1,\dots,e_n}(v_{\tau(1)},\dots,v_{\tau(n)}) = \sum_{\sigma\in \mathrm{S}_k}\mathrm{sign}(\sigma)\prod_{j=1}^k x_{\tau(j),i_{\sigma(j)}}.$$

On écrit $\sigma(j)$ sous la forme $\sigma\tau^{-1}(\tau(j))$ et $\mathrm{sign}(\sigma)$ sous la forme $\mathrm{sign}(\sigma\tau^{-1})\mathrm{sign}(\tau)$, et on fait les changements de variables $j' = \tau(j)$ et $\sigma' = \sigma\tau^{-1}$. On obtient

$$\det_{e_1,\dots,e_n}(v_{\tau(1)},\dots,v_{\tau(n)}) = \mathrm{sign}(\tau)\Big(\sum_{\sigma'\in \mathrm{S}_k}\mathrm{sign}(\sigma')\prod_{j=1}^k x_{j',i_{\sigma'(j')}}\Big) = \mathrm{sign}(\tau)\det_{e_1,\dots,e_n}(v_1,\dots,v_n).$$

Ceci prouve que $\det_{e_1,\dots,e_n}$ est alternée. Comme $\det_{e_1,\dots,e_n}\neq 0$, il en résulte que $\det \mathrm{V}^*$ est de dimension au moins 1, et donc de dimension exactement 1, et que $\det_{e_1,\dots,e_n}$ en est une base.

Si $f\in \det \mathrm{V}^*$, il existe donc $\lambda\in \mathrm{K}$ tel que $f = \lambda\det_{e_1,\dots,e_n}$, et si f vérifie $f(e_1,\dots,e_n) = 1$, cela implique $\lambda = 1$, et donc que f est la forme $\det_{e_1,\dots,e_n}$ définie ci-dessus (en particulier, il y a unicité d'une telle forme).

Maintenant, si $f_1,\dots,f_n$ est une autre base de V, il existe $\lambda\in \mathrm{K}$ tel que $\det_{f_1,\dots,f_n} = \lambda\det_{e_1,\dots,e_n}$ puisque $\det_{e_1,\dots,e_n}$ est une base de l'espace $\det \mathrm{V}^*$ dont $\det_{f_1,\dots,f_n}$ est élément. En évaluant les deux membres en $(f_1,\dots,f_n)$, on obtient $1 = \lambda\det_{e_1,\dots,e_n}(f_1,\dots,f_n)$ (en particulier $\det_{e_1,\dots,e_n}(f_1,\dots,f_n)\neq 0$), et donc $\lambda = \frac{1}{\det_{e_1,\dots,e_n}(f_1,\dots,f_n)}$.

Si $v_1,\dots,v_n$ est libre, c'est une base et $\det_{e_1,\dots,e_n}(v_1,\dots,v_n)\neq 0$, d'après ce qui précède. Si $v_1,\dots,v_n$ est liée, on peut exprimer l'un des v_i comme une combinaison linéaire des autres et donc $\det_{e_1,\dots,e_n}(v_1,\dots,v_n) = 0$ (c'est vrai pour n'importe quelle forme alternée).

Ceci termine la démonstration.

- $\det_{e_1,\dots,e_n}(v_1,\dots,v_n) = \sum_{\sigma\in \mathrm{S}_n}\mathrm{sign}(\sigma)\prod_{i=1}^n x_{i,\sigma(i)}$, si $v_i = \sum_{j=1}^n x_{i,j}e_j$.

  Cela a été établi au cours de la démonstration du point précédent.

Exercice 6.1. — Soit V un espace vectoriel de dimension n, et soit $e_1,\dots,e_n$ une base de V. On note $\wedge^k\mathrm{V}^*$ l'espace des formes k-linéaires alternées sur V.

(i) Si $1\leqslant i_1<\dots<i_k\leqslant n$, on note $e_{i_1}^*\wedge\dots\wedge e_{i_k}^*$ la forme k-linéaire définie par

$$(e_{i_1}^*\wedge\dots\wedge e_{i_k}^*)(v_1,\dots,v_k) = \sum_{\sigma\in \mathrm{S}_k}\mathrm{sign}(\sigma)\prod_{j=1}^k x_{j,i_{\sigma(j)}}, \quad \text{si } v_j = \sum_{i=1}^n x_{j,i}e_i, \text{ pour } 1\leqslant j\leqslant k.$$

Montrer que $e_{i_1}^*\wedge\dots\wedge e_{i_k}^*$ est alternée.

(ii) Calculer $(e_{i_1}^*\wedge\dots\wedge e_{i_k}^*)(e_{\ell_1},\dots,e_{\ell_k})$, si $1\leqslant\ell_1<\dots<\ell_k\leqslant n$. En déduire que les $e_{i_1}^*\wedge\dots\wedge e_{i_k}^*$ forment une famille libre de $\wedge^k\mathrm{V}^*$.

(iii) Montrer que $\wedge^k\mathrm{V}^*$ est un espace de dimension $\binom{n}{k}$ et que les $e_{i_1}^*\wedge\dots\wedge e_{i_k}^*$ en forment une base.

6.3. Déterminant d'un endomorphisme

On suppose toujours que V est de dimension n.

• Si $u \in \mathrm{End}(\mathrm{V})$, il existe un unique $\lambda \in \mathrm{K}$ tel que $f(u(v_1), \dots, u(v_n)) = \lambda f(u_1, \dots, u_n)$, pour tous $f \in \det \mathrm{V}^*$ et $v_1, \dots, v_n \in \mathrm{V}$. Ce λ est le *déterminant* $\det u$ de u, et on a :

◇ $\det u = \det_{e_1,\dots,e_n}(u(e_1), \dots, u(e_n))$ pour toute base $e_1, \dots, e_n$ de V ;

◇ $\det u = 0 \iff u$ non injectif $\iff u$ non surjectif $\iff u$ non bijectif ;

◇ $\det u \neq 0 \iff u$ injectif $\iff u$ surjectif $\iff u$ bijectif ;

◇ $\det u \circ v = \det u \det v$, pour tous $u, v \in \mathrm{End}(\mathrm{V})$.

L'application $(v_1, \dots, v_n) \mapsto f_u(v_1, \dots, v_n) = f(u(v_1), \dots, u(v_n))$ est n-linéaire car f est n-linéaire et u linéaire. Par ailleurs, elle est alternée car f l'est, et donc $f \mapsto f_u$ est une application de $\det \mathrm{V}^*$ dans lui-même. Soit alors e une base de $\det \mathrm{V}^*$; notons $\det u$ l'élément de K défini par $e_u = (\det u)e$. Comme $f \mapsto f_u$ est linéaire de manière évidente, on a $f_u = (\det u)f$, pour tout $f \in \det \mathrm{V}^*$, et donc $f(u(v_1), \dots, u(v_n)) = (\det u)f(u_1, \dots, u_n)$, pour toute forme n-linéaire alternée f sur V et tous $v_1, \dots, v_n \in \mathrm{V}$.

On peut appliquer l'identité précédente à $f = \det_{e_1,\dots,e_n}$ et à $v_i = e_i$, où $e_1, \dots, e_n$ est une base de V. On en déduit la formule $\det u = \det_{e_1,\dots,e_n}(u(e_1), \dots, u(e_n))$. Il s'ensuit que $\det u = 0$ si et seulement si $u(e_1), \dots, u(e_n)$ est une famille liée, et donc si et seulement si u n'est pas injectif (cf. n° 5.2). On en déduit les deux premiers points (cf. alinéa 5.4.2), le second étant obtenu en niant les propositions équivalentes du premier.

Enfin, on a

$$\det u \circ v = \det_{e_1,\dots,e_n}(u(v(e_1)), \dots, u(v(e_n))) = (\det u) \det_{e_1,\dots,e_n}(v(e_1), \dots, v(e_n)) = \det u \det v.$$

7. Matrices

7.1. Matrices à coefficients dans un corps

Soit K un corps commutatif. Si n, m sont des entiers $\geqslant 1$, on note $\mathbf{M}_{n\times m}(\mathrm{K})$ l'ensemble des *matrices* $\mathrm{A} = (a_{i,j})_{i\leqslant n,\, j\leqslant m}$ à n lignes et à m colonnes à coefficients dans K (i.e. $a_{i,j} \in \mathrm{K}$ pour tous i, j). Pour les calculs, il est souvent commode de représenter $\mathrm{A} = (a_{i,j})_{i\leqslant n,\, j\leqslant m}$ (notée simplement $(a_{i,j})$, si n et m sont clairs) sous la forme d'un tableau $n \times m$

$$\mathrm{A} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}.$$

L'ensemble $\mathbf{M}_{n\times m}(\mathrm{K})$ des matrices $n \times m$ est, de manière naturelle, un espace vectoriel avec l'addition et la multiplication par un scalaire définies composante par composante :

$$(a_{i,j})_{i\leqslant n,\, j\leqslant m} + (b_{i,j})_{i\leqslant n,\, j\leqslant m} = (a_{i,j} + b_{i,j})_{i\leqslant n,\, j\leqslant m} \text{ et } \lambda(a_{i,j})_{i\leqslant n,\, j\leqslant m} = (\lambda a_{i,j})_{i\leqslant n,\, j\leqslant m}.$$

• $\dim \mathbf{M}_{n\times m}(\mathrm{K}) = nm$

$(a_{i,j}) \mapsto (b_k)_{k\leqslant mn}$, avec $b_{m(i-1)+j} = a_{i,j}$, est un isomorphisme de $\mathbf{M}_{n\times m}(\mathrm{K})$ sur K^{nm}.

Si $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n\times m}(\mathrm{K})$, on note ${}^{\mathrm{t}}\mathrm{A} = ({}^{\mathrm{t}}a_{i,j}) \in \mathbf{M}_{m\times n}(\mathrm{K})$, où ${}^{\mathrm{t}}a_{i,j} = a_{j,i}$ la matrice *transposée* de A (c'est la symétrique de A par rapport à la diagonale).

$$\text{Par exemple, } {}^{\mathrm{t}}\mathrm{A} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \\ 6 & 7 \end{pmatrix} \text{ si } \mathrm{A} = \begin{pmatrix} 2 & 4 & 6 \\ 3 & 5 & 7 \end{pmatrix}.$$

On identifie K^n aux matrices $n \times 1$ (i.e. à n lignes et 1 colonne), mais pour économiser le papier, on écrit un élément de K^n sous la forme ${}^{\mathrm{t}}(x_1, \dots, x_n)$ (i.e. comme le transposé d'une matrice $1 \times n$). On note en général X ou Y un élément générique de K^n ; la base canonique de K^n est notée $e_1^{(n)}, \dots, e_n^{(n)}$ (ou simplement $e_1, \dots, e_n$ si la dimension est claire).

Si $\mathrm{A} = (a_{i,j})_{i \leqslant n,\, j \leqslant m} \in \mathbf{M}_{n \times m}(\mathrm{K})$, on note u_{A} le morphisme de K^m dans K^n donné par $u_{\mathrm{A}}({}^{\mathrm{t}}(x_1, \dots, x_m)) = {}^{\mathrm{t}}(y_1, \dots, y_n)$, avec $y_i = \sum_{j=1}^m a_{i,j} x_j$, ce qui fait que les colonnes de A sont les $u_{\mathrm{A}}(e_j^{(m)})$, pour $j \in \{1, \dots, m\}$.

• $\mathrm{A} \mapsto u_{\mathrm{A}}$ est un isomorphisme d'espaces vectoriels de $\mathbf{M}_{n \times m}(\mathrm{K})$ sur $\mathrm{Hom}(\mathrm{K}^m, \mathrm{K}^n)$, l'isomorphisme réciproque étant celui qui envoie $u : \mathrm{K}^m \to \mathrm{K}^n$ sur la matrice $\mathrm{Mat}(u)$ dont la j-ième colonne est $u(e_j^{(m)}) \in \mathrm{K}^n$.

La linéarité de $\mathrm{A} \mapsto u_{\mathrm{A}}$ est un jeu d'écriture. Par ailleurs, si $u(e_j^{(m)}) = \sum_{i=1}^n a_{i,j} e_i^{(n)}$, et si $x = \sum_{j=1}^m x_j e_j^{(m)}$, alors

$$u(x) = \sum_{j=1}^m x_j u(e_j^{(m)}) = \sum_{j=1}^m x_j \Big(\sum_{i=1}^n a_{i,j} e_i^{(n)} \Big) = \sum_{i=1}^n \Big(\sum_{j=1}^m x_j a_{i,j} \Big) e_i^{(n)}.$$

On reconnaît les formules pour u_{A}, où $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n \times m}(\mathrm{K})$. Le résultat s'en déduit.

7.2. Produit de matrices

Si $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n \times m}(\mathrm{K})$ et $\mathrm{B} = (b_{j,k}) \in \mathbf{M}_{m \times \ell}(\mathrm{K})$, leur produit $\mathrm{AB} \in \mathbf{M}_{n \times \ell}(\mathrm{K})$ est défini par $\mathrm{AB} = (c_{i,k})$, avec $c_{i,k} = \sum_{j=1}^m a_{i,j} b_{j,k}$.

• $u_{\mathrm{A}}(\mathrm{X}) = \mathrm{AX}$, si $\mathrm{X} \in \mathrm{K}^m = \mathbf{M}_{m \times 1}(\mathrm{K})$.

• $u_{\mathrm{AB}} = u_{\mathrm{A}} \circ u_{\mathrm{B}}$,

Par linéarité, il suffit de vérifier que $u_{\mathrm{A}} \circ u_{\mathrm{B}}$ et u_{AB} coïncident sur la base canonique de K^ℓ, ce qui résulte de :

$$\begin{aligned} u_{\mathrm{A}} \circ u_{\mathrm{B}}(e_k^{(\ell)}) = u_{\mathrm{A}}\Big(\sum_{j=1}^m b_{j,k} e_j^{(m)} \Big) = \sum_{j=1}^m b_{j,k} u_{\mathrm{A}}(e_j^{(m)}) &= \sum_{j=1}^m b_{j,k} \Big(\sum_{i=1}^n a_{i,j} e_i^{(n)} \Big) \\ &= \sum_{i=1}^n \Big(\sum_{j=1}^m a_{i,j} b_{j,k} \Big) e_i^{(n)} = u_{\mathrm{AB}}(e_k^{(\ell)}), \end{aligned}$$

• Le produit de matrices est associatif et distributif par rapport à l'addition :

$$\mathrm{A(BC)} = \mathrm{(AB)C}, \;\; \mathrm{A(B_1 + B_2)} = \mathrm{AB_1 + AB_2}, \;\; \text{et} \;\; \mathrm{(A_1 + A_2)B} = \mathrm{A_1B + A_2B}.$$

Pour pouver que $\mathrm{A(BC)} = \mathrm{(AB)C}$, il suffit de prouver que $u_{\mathrm{A(BC)}} = u_{\mathrm{(AB)C}}$, mais cela résulte de ce que $u_{\mathrm{A(BC)}} = u_{\mathrm{A}} \circ u_{\mathrm{BC}} = u_{\mathrm{A}} \circ u_{\mathrm{B}} \circ u_{\mathrm{C}}$ et $u_{\mathrm{(AB)C}} = u_{\mathrm{AB}} \circ u_{\mathrm{C}} = u_{\mathrm{A}} \circ u_{\mathrm{B}} \circ u_{\mathrm{C}}$. On démontre les autres formules de la même manière en remarquant que $u_{\mathrm{A}} \circ (u_{\mathrm{B}_1} + u_{\mathrm{B}_2}) = (u_{\mathrm{A}} \circ u_{\mathrm{B}_1}) + (u_{\mathrm{A}} \circ u_{\mathrm{B}_2})$ par linéarité de u_{A}, et $(u_{\mathrm{A}_1} + u_{\mathrm{A}_2}) \circ u_{\mathrm{B}} = (u_{\mathrm{A}_1} \circ u_{\mathrm{B}}) + (u_{\mathrm{A}_2} \circ u_{\mathrm{B}})$ par définition.

• ${}^{\mathrm{t}}(\mathrm{AB}) = {}^{\mathrm{t}}\mathrm{B}\,{}^{\mathrm{t}}\mathrm{A}$.

Posons $AB = C = (c_{i,k})$. On pose ${}^t a_{j,k} = a_{k,j}$, ${}^t b_{i,j} = b_{j,i}$ et ${}^t c_{k,i} = c_{i,k}$ de telle sorte que ${}^t A = ({}^t a_{j,k})$, ${}^t B = ({}^t b_{i,j})$ et ${}^t C = ({}^t c_{i,k})$. On a donc ${}^t c_{i,k} = c_{k,i} = \sum_{j=1}^m a_{k,j} b_{j,i} = \sum_{j=1}^m {}^t b_{i,j} {}^t a_{j,k}$, et on reconnait dans le membre de droite les coefficients de ${}^t B {}^t A$; d'où le résultat.

7.3. Le théorème fondamental de l'algèbre linéaire

• L'accouplement $\langle\ ,\ \rangle : K^n \times K^n \to K$ donné par $\langle X, Y\rangle = {}^t X\, Y$, où $K^n = \mathbf{M}_{n\times 1}(K)$, identifie le dual de K^n à K^n (i.e. toute forme linéaire sur K^n est la forme $Y \mapsto {}^t X\, Y$ pour un unique $X \in K^n$).

Une forme linéaire sur K^n est de la forme ${}^t(y_1, \dots, y_n) \mapsto a_1 y_1 + \cdots + a_n y_n$, pour un unique ${}^t(a_1, \dots, a_n) \in K^n$; elle est donc aussi de la forme $Y \mapsto {}^t X\, Y$, pour un unique $X = {}^t(a_1, \dots, a_n)$.

Si $A \in \mathbf{M}_{n\times m}(K)$, le morphisme transposé ${}^t u_A$ de $u_A : K^m \to K^n$ est un morphisme de K^n dans K^m si on utilise l'identification $(K^n)^* = K^n$ précédente.

• ${}^t u_A = u_{{}^t A}$; autrement dit la matrice de la transposée est la transposée de la matrice.

Cela résulte de ce que $\langle X, u_A(Y)\rangle = \langle X, AY\rangle = {}^t XAY = {}^t({}^t AX)Y = \langle {}^t AX, Y\rangle = \langle u_{{}^t A}(X), Y\rangle$.

Le *rang* d'une famille de vecteurs d'un espace vectoriel V est la dimension du sous-espace engendré par cette famille ; c'est aussi le maximal du cardinal d'une sous-famille libre. Le *rang* $\operatorname{rg} A$ d'une matrice A est le rang de ses colonnes ; on a donc $\operatorname{rg} A = \operatorname{rg} u_A$.

• Le rang d'une matrice est égal à celui de sa transposée ; autrement dit les dimensions des espaces engendrés par les colonnes et les lignes d'une matrice sont égales.

Cela résulte de ce que $\operatorname{rg} A = \operatorname{rg} u_A = \operatorname{rg} {}^t u_A = \operatorname{rg} {}^t A$ (cf. alinéa 5.5.2).

• La dimension du sous espace de K^m (resp. K^n) orthogonal de l'espace engendré par les lignes (resp. colonnes) de A est $m - \operatorname{rg} A$ (resp. $n - \operatorname{rg} A$).

Cela résulte de ce que $\dim W + \dim W^\perp = d$, si W est un sous-espace de K^d (cf. alinéa 5.5.2), et de ce que les dimensions des espaces engendrés par les colonnes et les lignes sont égales à $\operatorname{rg} A$.

7.4. Matrice d'une application linéaire

Si V est un espace vectoriel de dimension n, le choix d'une base $\mathbf{e} = (e_1, \dots, e_n)$ fournit un isomorphisme $\iota_{\mathbf{e}} : V \cong K^n$, à savoir celui qui envoie un vecteur $x \in V$ sur l'élément de K^n formé des coordonnées de x dans la base $\mathbf{e}$; l'isomorphisme réciproque est ${}^t(x_1, \dots, x_n) \mapsto x_1 e_1 + \cdots + x_n e_n$. Nous noterons [59] $\mathbf{e}\backslash x$ l'élément $\iota_{\mathbf{e}}(x)$ vu comme une matrice $n \times 1$. Plus généralement, si $\mathbf{v} = (v_1, \dots, v_m)$ est un m-uplet de vecteurs de V, on note $\mathbf{e}\backslash\mathbf{v}$ la matrice $n \times m$ dont les colonnes sont $\mathbf{e}\backslash v_1, \dots, \mathbf{e}\backslash v_m$.

Si $u : V_1 \to V_2$ est un morphisme, on note $u{\cdot}x$ au lieu de $u(x)$ l'image de x par u. De même, si $\mathbf{v} = (v_1, \dots, v_m)$ est un m-uplet de vecteurs de V_1, on note $u{\cdot}\mathbf{v}$ le m-uplet $(u{\cdot}v_1, \dots, u{\cdot}v_m)$. Si maintenant, V_1 est de dimension m et V_2 de dimension n, et si

59. Ce n'est pas une notation standard, mais elle a des propriétés assez agréables : une base est une unité de mesure en dimension supérieure, et pour mesurer un vecteur on fait le rapport de ce vecteur par l'unité de mesure, mais il faut spécifier de quel côté se fait la division, car on est dans un monde non commutatif.

$\mathbf{e} = (e_1, \dots, e_m)$ est une base de V_1 et $\mathbf{f} = (f_1, \dots, f_n)$ est une base de V_2, on définit la *matrice de u relativement aux bases* $\mathbf{e}$ *et* $\mathbf{f}$ comme $\mathbf{f}\backslash u{\cdot}\mathbf{e}$; les colonnes de cette matrice sont donc $u(e_1), \dots, u(e_m)$ écrits dans la base $f_1, \dots, f_n$.

• Si $x \in \mathrm{V}_1$, on a [60] $\mathbf{f}\backslash u{\cdot}x = (\mathbf{f}\backslash u{\cdot}\mathbf{e})(\mathbf{e}\backslash x)$.

Soit A la matrice $\mathbf{f}\backslash u{\cdot}\mathbf{e}$. L'identité à vérifier équivaut à $\iota_{\mathbf{f}}(u(x)) = u_{\mathrm{A}}(\iota_{\mathbf{e}}(x))$ et, par linéarité, il suffit de le vérifier pour $e_1, \dots, e_m$. On tombe alors sur un pur exercice de traduction en revenant aux définition de $\iota_{\mathbf{e}}$, $\iota_{\mathbf{f}}$ et u_{A}. Notons que le résultat se réécrit aussi sous la forme $u_{\mathrm{A}} = \iota_{\mathbf{f}} \circ u \circ \iota_{\mathbf{e}}^{-1}$.

• Si $\mathbf{e}$ et $\mathbf{f}$ sont deux bases de V, la *matrice de passage de* $\mathbf{e}$ *à* $\mathbf{f}$ est la matrice $\mathbf{f}\backslash\mathbf{e}$ dont les colonnes sont les vecteurs [61] de $\mathbf{e}$ exprimés dans la base $\mathbf{f}$. Si $x \in \mathrm{V}$, on a $\mathbf{f}\backslash x = (\mathbf{f}\backslash\mathbf{e})(\mathbf{e}\backslash x)$. Autrement dit, on obtient les coordonnées de x dans la base $\mathbf{f}$ à partir de celles dans la base $\mathbf{e}$ en multipliant par la matrice de passage de $\mathbf{e}$ à $\mathbf{f}$.

Il suffit d'appliquer le point précédent à $\mathrm{id} : \mathrm{V} \to \mathrm{V}$, en munissant le V de départ de la base $\mathbf{e}$ et celui d'arrivée de la base $\mathbf{f}$.

• Si $\mathrm{V}_1, \dots, \mathrm{V}_k$ sont des espaces de dimension finie, si $\mathbf{e}_i$ est une base de V_i, et si $u_i : \mathrm{V}_i \to \mathrm{V}_{i+1}$ est un morphisme pour $1 \leqslant i \leqslant k-1$, alors

$$\mathbf{e}_k\backslash(u_{k-1} \circ \cdots \circ u_1){\cdot}\mathbf{e}_1 = (\mathbf{e}_k\backslash u_{k-1}{\cdot}\mathbf{e}_{k-1}){\cdot}(\mathbf{e}_{k-1}\backslash u_{k-2}{\cdot}\mathbf{e}_{k-2}) \cdots (\mathbf{e}_2\backslash u_1{\cdot}\mathbf{e}_1).$$

Il suffit de démontrer le résultat pour $k = 3$; le cas général s'en déduit par récurrence. Si V_i est de dimension n_i, on dispose d'un isomorphisme $\iota_i = \iota_{\mathbf{e}_i} : \mathrm{V}_i \cong \mathrm{K}^{n_i}$. Notons A la matrice $\mathbf{e}_3\backslash u_2{\cdot}\mathbf{e}_2$, B la matrice $\mathbf{e}_2\backslash u_1{\cdot}\mathbf{e}_1$ et C la matrice $\mathbf{e}_3\backslash(u_2 \circ u_1){\cdot}\mathbf{e_1}$. Alors, par construction, $u_{\mathrm{A}} = \iota_3 \circ u_2 \circ \iota_2^{-1}$, $u_{\mathrm{B}} = \iota_2 \circ u_1 \circ \iota_1^{-1}$, et $u_{\mathrm{C}} = \iota_3 \circ (u_2 \circ u_1) \circ \iota_1^{-1}$. Le résultat est donc une traduction de l'identité $u_{\mathrm{A}} \circ u_{\mathrm{B}} = (\iota_3 \circ u_2 \circ \iota_2^{-1}) \circ (\iota_2 \circ u_1 \circ \iota_1^{-1}) = \iota_3 \circ u_2 \circ u_1 \circ \iota_1^{-1} = u_{\mathrm{C}}$, qui est équivalente à $\mathrm{AB} = \mathrm{C}$.

• Si $\mathbf{e}$ et $\mathbf{f}$ sont deux bases de V, alors $(\mathbf{f}\backslash\mathbf{e})(\mathbf{e}\backslash\mathbf{f}) = 1$. Autrement dit, les matrices de passage de $\mathbf{e}$ à $\mathbf{f}$ et de $\mathbf{f}$ à $\mathbf{e}$ sont inverses l'une de l'autre.

Il suffit d'appliquer le point précédent à $\mathrm{V}_1 = \mathrm{V}_2 = \mathrm{V}_3 = \mathrm{V}$ et $u_2 = u_1 = \mathrm{id}$, en munissant le premier V de la base $\mathbf{f}$, le second de la base $\mathbf{e}$ et le troisième de la base $\mathbf{f}$.

• Soit $u : \mathrm{V} \to \mathrm{V}'$ un morphisme. Si $\mathbf{e}$ et $\mathbf{f}$ sont des bases de V et $\mathbf{e}'$ et $\mathbf{f}'$ sont des bases de V', alors

$$\mathbf{f}'\backslash u{\cdot}\mathbf{f} = (\mathbf{f}'\backslash\mathbf{e}')(\mathbf{e}'\backslash u{\cdot}\mathbf{e})(\mathbf{e}\backslash\mathbf{f}).$$

Autrement dit, si M est la matrice de u dans les bases $\mathbf{e}$ et $\mathbf{e}'$, M' celle dans les bases $\mathbf{f}$ et $\mathbf{f}'$, P' la matrice de passage de $\mathbf{e}'$ à $\mathbf{f}'$, P celle de $\mathbf{f}$ à $\mathbf{e}$, on a $\mathrm{M}' = \mathrm{P}'\mathrm{M}\mathrm{P}^{-1}$.

60. On obtient donc le membre de gauche en « simplifiant » par la base $\mathbf{e}$ dans le membre de droite ; cela constitue une contrainte assez forte sur les expressions permises : pour pouvoir simplifier, il faut que la base apparaisse au numérateur du terme précédant celui où elle apparaît en dénominateur.

61. Notons qu'en général, on connaît les coordonnées de x et des f_i dans la bas $\mathbf{e}$, et donc la matrice que l'on peut écrire sans effort est $\mathrm{P} = \mathbf{e}\backslash\mathbf{f}$; comme $\mathbf{f}\backslash\mathbf{e} = (\mathbf{e}\backslash\mathbf{f})^{-1}$ d'après un des points suivants, la formule de changement de base prend la forme $\mathrm{X}' = \mathrm{P}^{-1}\mathrm{X}$, si $\mathrm{X} = \mathbf{e}\backslash x$ et $\mathrm{X}' = \mathbf{f}\backslash x$.

Il suffit d'appliquer le résultat ci-dessus à $V_1 = V_2 = V$, $V_3 = V_4 = V'$, en munissant V_1 de $\mathbf{f}$, V_2 de $\mathbf{e}$, V_3 de $\mathbf{e}'$, V_4 de $\mathbf{f}'$, et en prenant $u_1 = \mathrm{id}$, $u_2 = u$ et $u_3 = \mathrm{id}$.

• Soit $u : V \to V$ un endomorphisme. Si $\mathbf{e}$ est une base de V, la *matrice de u dans la base* $\mathbf{e}$ est la matrice $\mathbf{e}\backslash u\cdot\mathbf{e}$. Si $\mathbf{e}$ et $\mathbf{f}$ sont des bases de V, alors

$$\mathbf{f}\backslash u\cdot\mathbf{f} = (\mathbf{f}\backslash\mathbf{e})(\mathbf{e}\backslash u\cdot\mathbf{e})(\mathbf{e}\backslash\mathbf{f}).$$

Autrement dit, si on note M la matrice de u dans la base $\mathbf{e}$, M′ celle dans la base $\mathbf{f}$ et P la matrice de passage de $\mathbf{e}$ à $\mathbf{f}$, on a $M' = PMP^{-1}$.

La formule correspond au cas particulier du point précédent où $V = V'$ et $\mathbf{e} = \mathbf{e}'$, $\mathbf{f} = \mathbf{f}'$; sa traduction résulte de ce que $\mathbf{f}\backslash\mathbf{e} = P$ par définition, et donc $\mathbf{e}\backslash\mathbf{f} = P^{-1}$.

7.5. Matrices carrées

Si $n \geqslant 1$, on note simplement $\mathbf{M}_n(K)$ l'espace $\mathbf{M}_{n\times n}(K)$. D'après ce qui précède, c'est une K-algèbre de dimension n^2, unitaire ayant pour unité la matrice 1_n (notée en général simplement 1, si n est fixé) ayant des 1 sur la diagonale et des 0 ailleurs (l'endomorphisme u_{1_n} de K^n associé est l'identité) :

$$1_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

• Si $A \in \mathbf{M}_n(K)$, alors

« A est inversible » ⇔ « A a un inverse à droite » ⇔ « A a un inverse à gauche ».

A est inversible (resp. a un inverse à droite, resp. a un inverse à gauche) si et seulement si c'est le cas pour u_A ; les trois conditions sont donc équivalentes puisqu'on est en dimension finie (cf. alinéa 5.4.2).

Une matrice de la forme $\lambda \cdot 1_n$, avec $\lambda \in K$, est dite *scalaire*, et souvent notée simplement λ ; si $A = \lambda$ est scalaire, alors u_A est l'homothétie de rapport λ, et on a $AB = BA = \lambda B$ pour tout $B \in \mathbf{M}_n(K)$.

Une matrice $n \times n$ est *diagonale* si tous les coefficients non diagonaux sont nuls (une matrice scalaire est diagonale), elle est *triangulaire supérieure* (resp. *inférieure* si tous les coefficients en-dessous (resp. au-dessus) de la diagonale sont nuls (une matrice diagonale est à la fois triangulaire supérieure et triangulaire inférieure) :

par exemple, les matrices D, A et B sont respectivement diagonale, triangulaire supérieure et triangulaire inférieure,

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 4 \\ 0 & 0 & 5 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 5 & 2 & 0 \\ 2 & 0 & 5 \end{pmatrix}.$$

On dit qu'une matrice est *triangulaire* si elle est triangulaire supérieure ou inférieure.

• Si A est triangulaire inférieure (resp. supérieure), alors ${}^{\mathrm{t}}\mathrm{A}$ est triangulaire supérieure (resp. inférieure).

• Le produit de deux matrices diagonales est une matrice diagonale, le produit de deux matrices triangulaires supérieures (resp. inférieures) est une matrice triangulaire supérieure (resp. inférieure), et dans les trois cas, les coefficients diagonaux du produit sont les produits des coefficients diagonaux.

A est diagonale si et seulement si $\mathrm{K}e_i$ est stable par u_{A}, pour tout $i \in \{1, \dots, n\}$. Comme cette condition est stable par composition, on en déduit le premier énoncé. De même, A est triangulaire supérieure si et seulement si les sous-espaces $\mathrm{V}_i = \mathrm{K}e_1 \oplus \cdots \oplus \mathrm{K}e_i$ de K^n sont stables par u_{A} pour tout $i \in \{1, \dots, n\}$. Comme cette condition est stable par composition, on en déduit le fait que le produit de deux matrices triangulaires supérieures $\mathrm{A} = (a_{i,j})$ et $\mathrm{B} = (b_{i,j})$ est une matrice triangulaire supérieure $\mathrm{C} = (c_{i,j})$. De plus, $u_{\mathrm{B}}(e_i) - b_{i,i}e_i \in \mathrm{V}_{i-1}$, et donc $u_{\mathrm{A}}(u_{\mathrm{B}}(e_i)) - b_{i,i}u_{\mathrm{A}}(e_i) \in \mathrm{V}_{i-1}$ puisque V_{i-1} est stable par u_{A}. On en déduit que $u_{\mathrm{C}}(e_i) - a_{i,i}b_{i,i}e_i \in \mathrm{V}_{i-1}$, et donc que $c_{i,i} = a_{i,i}b_{i,i}$, ce que l'on cherchait à établir. Le cas de deux matrices triangulaires inférieures s'en déduisant en passant aux transposées, cela permet de conclure.

• Une matrice triangulaire est nilpotente (resp. unipotente) si et seulement si ses coefficients diagonaux sont nuls (resp. égaux à 1) ; de plus $\mathrm{A}^n = 0$ si A est nilpotente.

Il suffit de traiter le cas nilpotent puisque A est unipotente si et seulement si $\mathrm{A} - 1$ est nilpotente. Maintenant, les coefficients diagonaux de A^m sont les puissances n-ièmes des coefficients diagonaux de A. S'il existe m tel que $\mathrm{A}^m = 0$, cela implique donc que les coefficients diagonaux de A sont nuls. Réciproquement, si ces coefficients diagonaux sont nuls, on a $u_{\mathrm{A}}(\mathrm{V}_i) \subset \mathrm{V}_{i-1}$, si $\mathrm{V}_i = \mathrm{K}e_1 \oplus \cdots \oplus \mathrm{K}e_i$. Il en résulte que $u_{\mathrm{A}^k}(\mathrm{K}^n) \subset \mathrm{V}_{n-k}$, et donc que $\mathrm{A}^n = 0$; d'où le résultat.

$\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$ est dite *symétrique* (resp. *antisymétrique*) si ${}^{\mathrm{t}}\mathrm{A} = \mathrm{A}$ (resp. si ${}^{\mathrm{t}}\mathrm{A} = -\mathrm{A}$).

• Tout $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$ est, de manière unique, la somme d'une matrice symétrique et d'une matrice antisymétrique.

$\mathrm{A} \mapsto {}^{\mathrm{t}}\mathrm{A}$ est une symétrie du K-espace vectoriel $\mathbf{M}_n(\mathrm{K})$, et les matrices symétriques (resp. antisymétriques) sont l'espace propre de cette symétrie associé à la valeur propre 1 (resp. -1). Le résultat s'en déduit.

7.6. Déterminant d'une matrice carrée

7.6.1. *Trace et déterminant d'une matrice*

Si $\mathrm{A} = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(\mathrm{K})$, on note $\operatorname{Tr}\mathrm{A}$ sa *trace* (c'est la somme $\sum_{i=1}^n a_{i,i}$ des coefficients diagonaux).

• $\operatorname{Tr}(\mathrm{AB}) = \operatorname{Tr}(\mathrm{BA})$.

Si $\mathrm{A} = (a_{i,j})$ et $\mathrm{B} = (b_{j,k})$, alors $\operatorname{Tr}(\mathrm{AB}) = \sum_{i=1}^n \left(\sum_{j=1}^n a_{i,j}b_{j,i}\right)$, et $\operatorname{Tr}(\mathrm{BA}) = \sum_{j=1}^n \left(\sum_{k=1}^n b_{j,k}a_{k,j}\right)$, et l'identité cherchée s'en déduit en remplaçant k par i dans la seconde somme.

Si $\mathrm{A} = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(\mathrm{K})$, on définit son *déterminant* $\det \mathrm{A}$ par la formule

$$\det \mathrm{A} = \sum_{\sigma \in \mathrm{S}_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Alors $\det \mathrm{A}$ est aussi le déterminant des colonnes de A dans la base canonique de K^n (n° 6.2) ; c'est donc aussi le déterminant de l'endomorphisme u_A (n° 6.3).

• $\det(\lambda \mathrm{A}) = \lambda^n \det \mathrm{A}$, si $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$ et $\lambda \in \mathrm{K}$.

C'est une conséquence de la n-linéarité du déterminant de n vecteurs.

• Si V est de dimension finie sur K, et si $u \in \mathrm{End}(\mathrm{V})$, le déterminant de u est égal au déterminant de la matrice de u dans n'importe quelle base.

Si $e_1, \ldots, e_n$ est une base de V, la matrice de u dans la base $e_1, \ldots, e_n$ est la matrice dont les colonnes sont $u(e_1), \ldots, u(e_n)$ exprimés dans la base $e_1, \ldots, e_n$, et le résultat suit (cf. n° 6.3) de ce que $\det u = \det_{e_1,\ldots,e_n}(u(e_1), \ldots, u(e_n))$.

• Si $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$, alors :

$$\text{« } \det \mathrm{A} \neq 0 \text{ »} \iff \text{« } u_\mathrm{A} \text{ est bijectif »} \iff \text{« A est inversible ».}$$

On note $\mathbf{GL}_n(\mathrm{K})$ l'ensemble des matrice $n \times n$ vérifiant ces propriétés ; c'est le groupe des éléments inversibles de l'anneau $\mathbf{M}_n(\mathrm{K})$.

« $\det \mathrm{A} \neq 0$ »$\Leftrightarrow \det u_\mathrm{A} \neq 0 \Leftrightarrow$ « u_A bijectif » $\Leftrightarrow$ « u_A a un inverse v » $\Leftrightarrow$ « A a un inverse $\mathrm{Mat}(v)$ ».

• $\det \mathrm{AB} = (\det \mathrm{A})\,(\det \mathrm{B})$ si $\mathrm{A}, \mathrm{B} \in \mathbf{M}_n(\mathrm{K})$ (Cauchy, 1815).

On a $u_\mathrm{AB} = u_\mathrm{A} \circ u_\mathrm{B}$ et donc $\det u_\mathrm{AB} = \det(u_\mathrm{A} \circ u_\mathrm{B}) = (\det u_\mathrm{A})\,(\det u_\mathrm{B}) = (\det \mathrm{A})\,(\det \mathrm{B})$, puisque $\det(u \circ v) = (\det u)(\det v)$, cf. n° 6.3.

• $\mathbf{SL}_n(\mathrm{K}) = \{\mathrm{A} \in \mathbf{M}_n(\mathrm{K}),\ \det \mathrm{A} = 1\}$ est un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

D'après le point précédent, $\mathrm{A} \mapsto \det \mathrm{A}$ est un morphisme de groupes de $\mathbf{GL}_n(\mathrm{K})$ dans K^*, et $\mathbf{SL}_n(\mathrm{K})$ est le noyau de ce morphisme ; c'est donc un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

Exercice 7.1. — On note B (resp. D) l'ensemble des matrices triangulaires supérieures (resp. diagonales) dont les coefficients diagonaux sont non nuls, et $\mathrm{U} \subset \mathrm{B}$ l'ensemble des matrices ayant des 1 sur la diagonale.

(i) Montrer qu'une matrice diagonale A est inversible si et seulement si elle appartient à D. Quel est l'inverse de A si c'est le cas ? En déduire que D est un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

(ii) Montrer que $\mathrm{T} \in \mathrm{B}$ peut s'écrire de manière unique sous la forme AN, où $\mathrm{A} \in \mathrm{D}$ et $\mathrm{N} \in \mathrm{U}$.

(iii) En déduire que B est un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

(iv) Montrer que $\mathrm{T} \mapsto \mathrm{A}$ est un morphisme de groupes de B dans D. Quel est le noyau ? En déduire que U est un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

• On dit que $\lambda \in \mathrm{K}$ est une *valeur propre* de $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$, si c'est une valeur propre de u_A, ce qui équivaut à ce que $u_\mathrm{A} - \lambda$ ne soit pas inversible, et donc à $\det(\lambda - \mathrm{A}) = 0$.

7.6.2. *Méthodes de calcul de déterminants*

• $\det \mathrm{A} = \det {}^{\mathrm{t}}\mathrm{A}$.

Si $\sigma \in \mathrm{S}_n$, on a $\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma^{-1})$. Donc $\det \mathrm{A} = \sum_{\sigma\in\mathrm{S}_n} \mathrm{sign}(\sigma^{-1}) \prod_{i=1}^n a_{\sigma^{-1}(\sigma(i)),\sigma(i)}$, et on obtient $\det \mathrm{A} = \sum_{\tau\in\mathrm{S}_n} \mathrm{sign}(\tau) \prod_{i=1}^n a_{\tau(i'),i'} = \sum_{\tau\in\mathrm{S}_n} \mathrm{sign}(\tau) \prod_{i=1}^n a'_{i',\tau(i')}$, où $a'_{i,j} = a_{j,i}$ est le coefficient de la i-ème ligne et j-ième colonne de ${}^{\mathrm{t}}\mathrm{A}$, en faisant le changement de variables $\tau = \sigma^{-1}$ et $i' = \sigma(i)$. On reconnaît alors dans le membre de droite la définition de $\det {}^{\mathrm{t}}\mathrm{A}$, ce qui permet de conclure.

• Si A est triangulaire, son déterminant est le produit des termes diagonaux.

Si $\sigma \neq \mathrm{id}$, il existe au moins un i tel que $\sigma(i) > i$ et un i tel que $\sigma(i) < i$, et le terme $\prod_{i=1}^n a_{i,\sigma(i)}$ est nul, si A est triangulaire supérieure ou inférieure. Le seul terme qui contribue à $\det \mathrm{A}$ est donc $\sigma = \mathrm{id}$, ce qui permet de conclure.

• $\det \mathrm{A}$ ne change pas si on rajoute des multiples d'une ligne fixée aux autres ou des multiples d'une colonne fixée aux autres ; si on fait une permutation des lignes ou des colonnes, il est multiplié par la signature de la permutation.

L'énoncé concernant les colonnes vient juste de ce que le déterminant est une forme linéaire alternée sur les colonnes de la matrice ; on ramène le cas des lignes à celui des colonnes en prenant la transposée.

Par exemple, en échangeant la première et la dernière ligne, puis en retranchant 3 fois la première (resp. 2 fois) à la seconde (à la troisième), puis en échangeant la seconde et la dernière colonne, puis en ajoutant 2 fois la troisième ligne à la dernière, on obtient :

$$\begin{vmatrix} 0 & 1 & 2 & 0 \\ 3 & 2 & -1 & 5 \\ 2 & 4 & 3 & -2 \\ 1 & 3 & 2 & -1 \end{vmatrix} = - \begin{vmatrix} 1 & 3 & 2 & -1 \\ 3 & 2 & -1 & 5 \\ 2 & 4 & 3 & -2 \\ 0 & 1 & 2 & 0 \end{vmatrix} = - \begin{vmatrix} 1 & 3 & 2 & -1 \\ 0 & -7 & -7 & 8 \\ 0 & -2 & -1 & 0 \\ 0 & 1 & 2 & 0 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & -1 & 2 & 3 \\ 0 & 8 & -7 & -7 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & -1 & 2 & 3 \\ 0 & 8 & -7 & -7 \\ 0 & 0 & -1 & -2 \\ 0 & 0 & 0 & -3 \end{vmatrix} = 1 \cdot 8 \cdot (-1) \cdot (-3) = 24.$$

Si $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$, et si $1 \leqslant \alpha, \beta \leqslant n$, on note $\mathrm{A}_{\alpha,\beta}$ la matrice $(n-1) \times (n-1)$ obtenue en retirant la α-ième ligne et la β-ième colonne de A, et $\left|\mathrm{A}_{\alpha,\beta}\right|$ son déterminant.

• Si $\alpha \in \{1, \ldots, n\}$, alors $\det \mathrm{A} = \sum_{\beta=1}^n (-1)^{\alpha+\beta} a_{\alpha,\beta} \left|\mathrm{A}_{\alpha,\beta}\right|$ (développement par rapport à la α-ième ligne) et, si $\beta \in \{1, \ldots, n\}$ $\det \mathrm{A} = \sum_{\alpha=1}^n (-1)^{\alpha+\beta} a_{\alpha,\beta} \left|\mathrm{A}_{\alpha,\beta}\right|$ (développement par rapport à la β-ième colonne).

On ramène l'énoncé concernant le développement par rapport à une colonne à celui par rapport à une ligne en passant à la transposée.

Posons $\lambda(\mathrm{A}) = \sum_{\beta=1}^n (-1)^{\alpha+\beta} a_{\alpha,\beta} \left|\mathrm{A}_{\alpha,\beta}\right|$. On doit vérifier que $\lambda(\mathrm{A}) = \det \mathrm{A}$ pour tout A.

◇ Si $\mathrm{A} = 1_n$, on a $\left|\mathrm{A}_{\alpha,\beta}\right| = 0$ si $\beta \neq \alpha$ car on a supprimé deux 1 de la matrice, et donc il ne reste que $n-2$ coefficients non nuls et le produit de $n-1$ coefficients est toujours nul. Si $\beta = \alpha$, on a $\mathrm{A}_{\alpha,\beta} = 1_{n-1}$, et donc $\left|\mathrm{A}_{\alpha,\beta}\right| = 1$. On obtient donc $\lambda(1_n) = 1 = \det 1_n$.

◇ Pour conclure, il suffit donc de prouver que $A \mapsto \lambda(A)$ est n-linéaire alternée en les colonnes de A puisqu'il existe une unique telle forme prenant la valeur 1 sur la base canonique de K^n. La n-linéarité est évidente sur les formules ; vérifions que $\lambda(A)$ change de signe quand on permute deux colonnes consécutives de A. Soit donc $k \in \{1, \dots, n-1\}$, et soit A' la matrice obtenue en échangeant les deux colonnes d'indice k et $k+1$ de A. Alors $\left|A'_{\alpha,\beta}\right| = -\left|A_{\alpha,\beta}\right|$ sauf si $\beta = k$ ou $\beta = k+1$, et on a $\left|A'_{\alpha,k}\right| = \left|A_{\alpha,k+1}\right|$ et $\left|A'_{\alpha,k+1}\right| = \left|A_{\alpha,k}\right|$, ainsi que $a'_{\alpha,k} = a_{\alpha,k+1}$ et $a'_{\alpha,k+1} = a_{\alpha,k}$ On obtient donc $\lambda(A') = \sum_{\beta \neq k,k+1}(-1)^{\alpha+\beta+1} a_{\alpha,\beta}\left|A_{\alpha,\beta}\right| + (-1)^{\alpha+\beta} a_{\alpha,k+1}\left|A_{\alpha,k+1}\right| + (-1)^{\alpha+\beta+1} a_{\alpha,k}\left|A_{\alpha,k}\right| = -\sum_\beta (-1)^{\alpha+\beta} a_{\alpha,\beta}\left|A_{\alpha,\beta}\right| = -\lambda(A)$.
Ceci permet de conclure.

Par exemple, en développant par rapport à la première ligne, puis en développant les déterminants 3×3 par rapport à la première colonne, et enfin en utilisant la formule $\left|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right| = ad - bc$, on obtient :

$$\begin{vmatrix} 0 & 1 & 2 & 0 \\ 3 & 2 & -1 & 5 \\ 2 & 4 & 3 & -2 \\ 1 & 3 & 2 & -1 \end{vmatrix} = -\begin{vmatrix} 3 & -1 & 5 \\ 2 & 3 & -2 \\ 1 & 2 & -1 \end{vmatrix} + 2\begin{vmatrix} 3 & 2 & 5 \\ 2 & 4 & -2 \\ 1 & 3 & -1 \end{vmatrix}$$

$$= -\Big(3\begin{vmatrix} 3 & -2 \\ 2 & -1 \end{vmatrix} - 2\begin{vmatrix} -1 & 5 \\ 2 & -1 \end{vmatrix} + \begin{vmatrix} -1 & 5 \\ 3 & -2 \end{vmatrix}\Big) + 2\Big(3\begin{vmatrix} 4 & -2 \\ 3 & -1 \end{vmatrix} - 2\begin{vmatrix} 2 & 5 \\ 3 & -1 \end{vmatrix} - \begin{vmatrix} 2 & 5 \\ 4 & -2 \end{vmatrix}\Big)$$

$$= -\big(3 \cdot 1 - 2 \cdot (-9) + 1 \cdot (-13)\big) + 2\big(3 \cdot 2 - 2 \cdot (-17) + 1 \cdot (-24)\big) = -8 + 32 = 24.$$

• Soient $\mathrm{cof}(A) = ((-1)^{\alpha+\beta}\left|A_{\alpha,\beta}\right|)_{\alpha,\beta \leqslant n}$ la *matrice des cofacteurs* de A et ${}^t\mathrm{cof}(A)$ sa transposée. Alors $A\,{}^t\mathrm{cof}(A) = (\det A) \cdot 1_n = {}^t\mathrm{cof}(A)\,A$; si $\det A \neq 0$, alors $A^{-1} = \frac{1}{\det A}\,{}^t\mathrm{cof}(A)$.

En développant $\det A$ par rapport à la α-ième ligne, on obtient $\det A = \sum_{\beta=1}^n (-1)^{\alpha+\beta} x_{\alpha,\beta}\left|A_{\alpha,\beta}\right|$. Si $\alpha' \neq \alpha$, alors $\sum_{\beta=1}^n (-1)^{\alpha+\beta} x_{\alpha',\beta}\left|A_{\alpha,\beta}\right|$ est le déterminant de la matrice obtenue en remplaçant la α-ième ligne de A par la α'-ième, et comme la matrice ainsi obtenue a deux lignes égales, son déterminant est nul. On a donc $\sum_{\beta=1}^n (-1)^{\alpha+\beta} x_{\alpha',\beta}\left|A_{\alpha,\beta}\right| = 0$, si $\alpha' \neq \alpha$. Les identités ci-dessus sont équivalentes à $A\,{}^t\mathrm{cof}(A) = (\det A) \cdot 1_n$. La formule $(\det A) \cdot 1_n = {}^t\mathrm{cof}(A)\,A$ se démontre de même, en considérant les colonnes au lieu des lignes.

• Soient $\alpha_1, \dots, \alpha_n \in K$. Le *déterminant de Vandermonde* $\mathrm{VdM}(\alpha_1, \dots, \alpha_n)$ est le déterminant dont la i-ième ligne est $1, \alpha_i, \dots, \alpha_i^{n-1}$; on a $\mathrm{VdM}(\alpha_1, \dots, \alpha_n) = \prod_{i<j}(\alpha_j - \alpha_i)$, et donc $\mathrm{VdM}(\alpha_1, \dots, \alpha_n) = 0$ si et seulement si deux des α_i sont égaux.

On soustrait la première ligne aux autres, ce qui fait apparaître des 0 dans la première colonne, puis $\alpha_1 \times$ la i-ième colonne à la $(i+1)$-ième, pour $1 \leqslant i \leqslant n-1$. On peut alors mettre en facteur $\alpha_i - \alpha_1$ en facteur dans la i-ième ligne, et le déterminant qui apparaît est égal à $\mathrm{VdM}(\alpha_2, \dots, \alpha_n)$, et donc $\mathrm{VdM}(\alpha_1, \dots, \alpha_n) = \mathrm{VdM}(\alpha_2, \dots, \alpha_n) \prod_{i=2}^n (\alpha_i - \alpha_1)$. On conclut par récurrence.

Exercice 7.2. — Montrer que $\det A = 0$ si $A \in \mathbf{M}_n(K)$ est antisymétrique et si n est impair.

Exercice 7.3. — (déterminant de Cauchy) Soient a_i et b_j, pour $1 \leqslant i, j \leqslant n$ des éléments d'un corps K, tels que $a_i + b_j \neq 0$ pour tous i, j. Calculer le déterminant $C(a_1, \dots, a_n, b_1, \dots, b_n)$ de la matrice des $\frac{1}{a_i + b_j}$. (On pourra retirer la première ligne aux autres.)

Exercice 7.4. — (déterminant circulant) Soient $a_0, \dots, a_{n-1} \in \mathbf{C}$ et soit $\mathrm{A} = (a_{r(i+j)})_{0 \leqslant i,j \leqslant n-1}$, où $r(k) \in \{0, \dots, n-1\}$ est le reste de la division de k par n. Montrer [62] que $\det \mathrm{A}$ est un produit de formes linéaires en les a_i. (On pourra considérer le produit de A par $\mathrm{B} = (\eta^{ij})_{0 \leqslant i,j \leqslant n-1}$, où $\eta = e^{2i\pi/n}$.)

Exercice 7.5. — (i) Soit $a \in \mathbf{C}^*$ et, si $n \geqslant 1$, soit $\mathrm{A}_n \in \mathbf{M}_n(\mathbf{C})$ la matrice avec des $a + a^{-1}$ sur la diagonale, des 1 juste en-dessous et juste au-dessus de la diagonale, et des 0 partout ailleurs. Montrer que $\det \mathrm{A}_n = \frac{a^{n+1} - a^{-1-n}}{a - a^{-1}}$ si $a \neq \pm 1$. Que vaut $\det \mathrm{A}_n$ si $a = \pm 1$?

(ii) Soit U_n la matrice $n \times n$ ayant des 0 sur la diagonale, des -1 juste en-dessous et juste au-dessus de la diagonale, et des 0 partout ailleurs. Montrer que les valeurs propres de cette matrice sont les $2\cos\frac{k\pi}{n+1}$, pour $1 \leqslant k \leqslant n$.

Exercice 7.6. — Soit $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{Z})$, avec $a_{i,j} = \mathrm{pgcd}(i,j)$. Montrer que $\det \mathrm{A} = \prod_{i=1}^{n} \varphi(i)$, où φ est la fonction indicatrice d'Euler. (On pourra commencer par montrer que $\sum_{d|n} \varphi(d) = n$.)

7.6.3. *Calcul du rang d'une matrice*

Si $\mathrm{A} \in \mathbf{M}_{n \times m}(\mathrm{K})$, et si $r \leqslant \inf(n,m)$, un *mineur d'ordre* r de A est le déterminant d'une matrice $r \times r$ obtenue en ne gardant que r lignes et r colonnes de A (il y a $\binom{n}{r}\binom{m}{r}$ tels mineurs, un pour chaque choix de r lignes parmi n et de r colonnes parmi m).

• Soient $v_1, \dots, v_r$ des vecteurs de K^n, et soit $\mathrm{A} \in \mathbf{M}_{n \times r}(\mathrm{K})$ la matrice dont les colonnes sont $v_1, \dots, v_r$. Alors $v_1, \dots, v_r$ est une famille libre si et seulement si $r \leqslant n$ et il existe un mineur d'ordre r de A qui est non nul.

> La condition $r \leqslant n$ est obligatoire car une famille libre de K^n a au plus n éléments. Supposons la donc satisfaite. Si $\mathrm{I} \subset \{1, \dots, n\}$ est de cardinal r, le mineur obtenu en ne gardant que les lignes de A d'indice dans I est aussi égal, au signe près, au déterminant de $v_1, \dots, v_r$ et des e_j, pour $j \notin \mathrm{I}$. Le résultat suit donc du th. de la base incomplète dont il résulte que $v_1, \dots, v_r$ est libre si et seulement si on peut compléter $v_1, \dots, v_r$ par des e_j pour obtenir une base de K^n.

• Si $\mathrm{A} \in \mathbf{M}_{n \times m}(\mathrm{K})$, le rang de A est le maximum des ordres des mineurs non nuls de A.

> C'est une traduction du point précédent. Comme les mineurs de A et ${}^{\mathrm{t}}\mathrm{A}$ sont les mêmes, on retrouve le résultat selon lequel le rang d'une matrice est égal à celui de sa transposée.

7.7. Matrices à coefficients dans un anneau

Si Λ est un anneau commutatif, on note $\mathbf{M}_{n \times m}(\Lambda)$ l'ensemble des matrices à n lignes et m colonnes à coefficients dans Λ. Alors $\mathbf{M}_{n \times m}(\Lambda)$ est, de manière naturelle, un A-module avec l'addition et la multiplication par un scalaire définies composante par composante.

Si $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n \times m}(\Lambda)$ et $\mathrm{B} = (b_{j,k}) \in \mathbf{M}_{m \times \ell}(\Lambda)$, on définit le produit AB de A et B par $\mathrm{AB} = (c_{i,k}) \in \mathbf{M}_{n \times \ell}(\Lambda)$, avec $c_{i,k} = \sum_{j=1}^{m} a_{i,j} b_{j,k}$.

62. Si on utilise $\mathbf{Z}/n\mathbf{Z}$ au lieu de $\{0, \dots, n-1\}$ pour numéroter les a_i, la matrice A devient celle des a_{i+j}, pour $i, j \in \mathbf{Z}/n\mathbf{Z}$. On peut remplacer $\mathbf{Z}/n\mathbf{Z}$ par n'importe quel groupe fini G, et regarder le déterminant de la matrice des a_{gh}, pour $g, h \in \mathrm{G}$ (on obtient un polynôme homogène de degré $|\mathrm{G}|$ en $|\mathrm{G}|$ variables). La factorisation de ce déterminant par Frobenius est à l'origine de la théorie des caractères ; la présentation moderne de la théorie, via le lemme de Schur (th. I.2.9), occulte complètement cet aspect.

On note simplement $\mathbf{M}_n(\Lambda)$ l'ensemble des matrices carrées $n \times n$ à coefficients dans Λ, et si $\mathrm{A} \in \mathbf{M}_n(\Lambda)$, on définit son déterminant $\det \mathrm{A} \in \Lambda$ par la formule habituelle

$$\det \mathrm{A} = \sum_{\sigma \in \mathrm{S}_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Toutes les formules des n$^{\mathrm{os}}$ 7.2, 7.5 et 7.6 sont encore valables dans ce cadre. La raison en est que l'on peut considérer les coefficients des matrices intervenant dans les formules comme des variables, et on est alors ramené à prouver que des polynômes à coefficients dans $\mathbf{Z}$ en ces variables coïncident. Pour ce faire, il suffit de prouver que les fonctions polynomiales complexes qu'ils définissent sont les mêmes, ce qui est assuré par le fait que la formule qui nous intéresse est vraie pour des matrices à coefficients dans $\mathbf{C}$. Les énoncés dont il s'agit sont les suivants.

- $\mathrm{A}(\mathrm{BC}) = (\mathrm{AB})\mathrm{C}$, $\mathrm{A}(\mathrm{B}_1 + \mathrm{B}_2) = \mathrm{AB}_1 + \mathrm{AB}_2$ et $(\mathrm{A}_1 + \mathrm{A}_2)\mathrm{B} = \mathrm{A}_1\mathrm{B} + \mathrm{A}_2\mathrm{B}$.
- ${}^{\mathrm{t}}(\mathrm{AB}) = {}^{\mathrm{t}}\mathrm{B}\,{}^{\mathrm{t}}\mathrm{A}$.
- Si $\mathrm{A} = \lambda$ est scalaire, alors $\mathrm{AB} = \mathrm{BA} = \lambda\mathrm{B}$ pour tout $\mathrm{B} \in \mathbf{M}_n(\Lambda)$.
- Le produit de deux matrices diagonales (resp. triangulaires supérieures, resp. triangulaires inférieures) est une matrice diagonale (resp. triangulaire supérieure, resp. triangulaire inférieure).
- $\det \mathrm{AB} = (\det \mathrm{A})(\det \mathrm{B})$ et $\det \mathrm{A} = \det {}^{\mathrm{t}}\mathrm{A}$.
- Si A est triangulaire, son déterminant est le produit des termes diagonaux.
- Le déterminant d'une matrice est une forme multilinéaire alternée des colonnes ou des lignes de la matrice ; il ne change pas si on rajoute des multiples d'une ligne (resp. colonne) fixée aux autres ou si on rajoute à une ligne (resp. colonne) une combinaison linéaire des autres.
- Le déterminant d'une matrice peut se calculer en développant par rapport à une ligne ou une colonne.
- $\mathrm{A}\,{}^{\mathrm{t}}\mathrm{cof}(\mathrm{A}) = (\det \mathrm{A})1_n = {}^{\mathrm{t}}\mathrm{cof}(\mathrm{A})\,\mathrm{A}$.
- Le déterminant de Vandermonde $\mathrm{VdM}(\alpha_1, \ldots, \alpha_n)$ est égal à $\prod_{i<j}(\alpha_j - \alpha_i)$.

Par exemple, si on veut prouver la formule $\det \mathrm{AB} = (\det \mathrm{A})(\det \mathrm{B})$ pour des matrices $\mathrm{A} = (a_{i,j}), \mathrm{B} = (b_{i,j}) \in \mathbf{M}_n(\Lambda)$, où Λ est quelconque, on commence par travailler dans l'anneau Λ_{univ} des polynômes à coefficients dans $\mathbf{Z}$ en les variables $\mathrm{A}_{i,j}$ et $\mathrm{B}_{i,j}$ pour $1 \leqslant i, j \leqslant n$ (si $n = 2$, on a $\Lambda_{\mathrm{univ}} = \mathbf{Z}[\mathrm{A}_{1,1}, \mathrm{A}_{1,2}, \mathrm{A}_{2,1}, \mathrm{A}_{2,2}, \mathrm{B}_{1,1}, \mathrm{B}_{1,2}, \mathrm{B}_{2,1}, \mathrm{B}_{2,2}]$). Soient $\mathrm{A}_{\mathrm{univ}} = (\mathrm{A}_{i,j})$ et $\mathrm{B}_{\mathrm{univ}} = (\mathrm{B}_{i,j})$; ce sont des éléments de $\mathbf{M}_n(\Lambda_{\mathrm{univ}})$ que l'on voit comme un couple *universel* de matrices $n \times n$ dans le sens où tout couple d'éléments de $\mathbf{M}_n(\Lambda)$, pour un anneau commutatif Λ, s'obtient en donnant des valeurs dans Λ aux $\mathrm{A}_{i,j}$ et aux $\mathrm{B}_{i,j}$. Alors $\mathrm{R} = \det(\mathrm{A}_{\mathrm{univ}}\mathrm{B}_{\mathrm{univ}}) - (\det \mathrm{A}_{\mathrm{univ}})(\det \mathrm{B}_{\mathrm{univ}})$ est un élément de Λ_{univ}. La fonction polynomiale qu'il définit sur $\mathbf{M}_n(\mathbf{C}) \times \mathbf{M}_n(\mathbf{C})$ est identiquement nulle puisque $\det \mathrm{AB} = (\det \mathrm{A})(\det \mathrm{B})$, si $\mathrm{A}, \mathrm{B} \in \mathbf{M}_n(\mathbf{C})$. On a donc $\mathrm{R} = 0$, et la fonction polynomiale définie par R sur n'importe quel anneau Λ est identiquement nulle, ce qui prouve que $\det \mathrm{AB} - (\det \mathrm{A})(\det \mathrm{B}) = 0$, pour tous $\mathrm{A}, \mathrm{B} \in \mathbf{M}_n(\Lambda)$, quel que soit Λ.

Exercice 7.7. — On se place dans l'anneau $\mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

(i) Quel est le degré en X_n de $\mathrm{VdM}(X_1, \ldots, X_n)$ et quel est le coefficient dominant ? (On pourra développer par rapport à la dernière colonne.)

(ii) Calculer $\mathrm{VdM}(X_1, \ldots, X_n)$; en déduire que $\mathrm{VdM}(\alpha_1, \ldots, \alpha_n) = \prod_{i<j}(\alpha_j - \alpha_i)$, si $\alpha_1, \ldots, \alpha_n$ appartiennent à un anneau commutatif Λ quelconque.

Si Λ est un anneau, $\mathbf{M}_n(\Lambda)$ est un anneau, et même une Λ-algèbre unitaire, puisque la multiplication est associative et distributive par rapport à l'addition (cf. premier point ci-dessus).

• $A \in \mathbf{M}_n(\Lambda)$ est inversible si et seulement si $\det A \in \Lambda^*$; on note $\mathbf{GL}_n(\Lambda)$ le groupe des éléments inversibles de l'anneau $\mathbf{M}_n(\Lambda)$.

Si B est l'inverse de A, alors $\det B$ est l'inverse de $\det A$ puisque $\det AB = (\det A)(\det B)$. Réciproquement, si $\det A$ est inversible, alors A l'est et son inverse est $(\det A)^{-1}\,{}^t\mathrm{cof}(A)$.

• L'ensemble $\mathbf{SL}_n(\Lambda)$ des $A \in \mathbf{M}_n(\Lambda)$ vérifiant $\det A = 1$ est un sous-groupe de $\mathbf{GL}_n(\Lambda)$.

C'est le noyau du morphisme de groupes $A \mapsto \det A$.

• Si $\varphi : \Lambda_1 \to \Lambda_2$ est un morphisme d'anneaux, alors $(a_{i,j}) \mapsto (\varphi(a_{i,j}))$ induit des morphismes d'anneaux $\varphi : \mathbf{M}_n(\Lambda_1) \to \mathbf{M}_n(\Lambda_2)$ et de groupes $\varphi : \mathbf{GL}_n(\Lambda_1) \to \mathbf{GL}_n(\Lambda_2)$ et $\varphi : \mathbf{SL}_n(\Lambda_1) \to \mathbf{SL}_n(\Lambda_2)$.

La vérification est un peu fastidieuse mais complètement automatique.

Exercice 7.8. — Montrer que l'ensemble $B(\Lambda)$ des matrices triangulaires supérieures de $\mathbf{M}_n(\Lambda)$ dont les coefficients diagonaux sont inversibles est un sous-groupe de $\mathbf{GL}_n(\Lambda)$.

Exercice 7.9. — Soit $D \geqslant 1$ un entier.

(i) Montrer que l'ensemble $\Gamma(D)$ des $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z})$ telles que D divise $a-1, d-1, b$ et c, est un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$.

(ii) Montrer que l'ensemble $\Gamma_0(D)$ des $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z})$ telles que D divise c, est un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$.

7.7.1. *Polynôme caractéristique et trace*

Si $A \in \mathbf{M}_n(\Lambda)$, on définit le *polynôme caractéristique* $\mathrm{Car}_A \in \Lambda[X]$ de A comme le déterminant de $X - A \in \mathbf{M}_n(\Lambda[X])$.

• Si $A = (a_{i,j}) \in \mathbf{M}_n(\Lambda)$ est triangulaire supérieure, alors $\mathrm{Car}_A = \prod_{i=1}^n (X - a_{i,i})$.

$X - A$ est triangulaire supérieure ; son déterminant est donc le produit des termes diagonaux $X - a_{1,1}, \ldots, X - a_{n,n}$.

• Une matrice et sa transposée ont le même polynôme caractéristique.

On a ${}^t(X - A) = X - {}^tA$, et donc $\det(X - {}^tA) = \det(X - A)$.

• Deux matrices *semblables* ont le même polynôme caractéristique : $\mathrm{Car}_{PAP^{-1}} = \mathrm{Car}_A$ si $P \in \mathbf{GL}_n(\Lambda)$.

Si $B = P^{-1}AP$, alors $X - B = P^{-1}(X - A)P$ puisque X est une matrice scalaire, et donc $\det(X - B) = (\det P^{-1})(\det(X - A))(\det P) = \det(X - A)$.

• Si Λ est un corps K, les valeurs propres de A sont les racines de Car_A.

$\lambda \in \mathrm{K}$ est une valeur propre de A, si et seulement si $u_\mathrm{A} - \lambda$ n'est pas inversible, et donc si et seulement si $\det(\lambda - \mathrm{A}) = 0$.

• $\mathrm{Car}_\mathrm{A} = \mathrm{X}^n - (\mathrm{Tr}\,\mathrm{A})\mathrm{X}^{n-1} + \cdots + (-1)^n \det \mathrm{A}$; en particulier Car_A est unitaire, de degré n.

Le terme constant de Car_A est $\det(-\mathrm{A}) = (-1)^n \det \mathrm{A}$. Maintenant, si on revient à la définition du déterminant, on voit que le seul terme comportant des termes en X^n et X^{n-1} est celui correspondant à $\sigma = \mathrm{id}$. Il s'ensuit que $\mathrm{Car}_\mathrm{A} - \prod_{i=1}^n (\mathrm{X} - a_{i,i})$ est de degré $\leqslant n-2$, et donc que $\mathrm{Car}_\mathrm{A} = \mathrm{X}^n - (\sum_{i=1}^n a_{i,i})\mathrm{X}^{n-1} + \cdots$ D'où le résultat.

• $\mathrm{Car}_\mathrm{AB} = \mathrm{Car}_\mathrm{BA}$ si $\mathrm{A}, \mathrm{B} \in \mathbf{M}_n(\mathrm{K})$; en particulier, $\mathrm{Tr}(\mathrm{AB}) = \mathrm{Tr}(\mathrm{BA})$.

L'identité $\mathrm{Car}_\mathrm{AB} = \mathrm{Car}_\mathrm{BA}$ a été établie dans la rem. 4.8. La formule $\mathrm{Tr}(\mathrm{AB}) = \mathrm{Tr}(\mathrm{BA})$ s'en déduit en identifiant les termes de degré $n-1$.

• Si V est un K-espace vectoriel de dimension finie, et si $u \in \mathrm{End}(\mathrm{V})$, le polynôme caractéristique de la matrice de u dans une base ne dépend pas du choix de la base ; on le note Car_u : c'est le *polynôme caractéristique* de u ; les valeurs propres de u sont les racines de Car_u.

Comme les matrices A et B de u dans deux bases différentes sont semblables ($\mathrm{B} = \mathrm{PAP}^{-1}$), l'indépendance du choix de la base résulte de ce que deux matrices semblables ont le même polynôme caractéristique ; le reste en découle en choisissant une base quelconque de V.

• Si Car_u est scindé sur K, il existe une base de V dans laquelle la matrice de u est triangulaire supérieure ; les coefficients diagonaux sont alors les racines de Car_u (i.e. les valeurs propres de u) répétées avec multiplicité.

Le second énoncé est une conséquence de ce que $\mathrm{Car}_\mathrm{A} = \prod_{i=1}^n (\mathrm{X} - a_{i,i})$, si $\mathrm{A} = (a_{i,j})$ est triangulaire supérieure.

La démonstration du premier se fait par récurrence sur $n = \dim \mathrm{V}$; il n'y a rien à prouver si $n = 1$. Supposons donc $n \geqslant 2$. Comme Car_u est scindé, u a au moins une valeur propre λ_1. Soit e_1 un vecteur propre non nul pour λ_1, et soit $\mathrm{V}_1 = \mathrm{K}\,e_1$. Soit W un supplémentaire de V_1 dans V et soit p la projection sur W parallèlement à V_1. Alors la restriction de $p \circ u$ à W est un endomorphisme de W et l'hypothèse de récurrence nous fournit une base $e_2, \ldots, e_n$ de W dans laquelle la matrice A_1 de $p \circ u$ est triangulaire supérieure. Celle de u dans la base $e_1, e_2, \ldots, e_n$ est alors $\left(\begin{smallmatrix} \lambda_1 & \mathrm{C} \\ 0 & \mathrm{A}_1 \end{smallmatrix}\right)$, où $\mathrm{C} = (\alpha_2, \ldots, \alpha_n)$ et $\alpha_k e_1 = u(e_k) - p \circ u(e_k)$ est la projection de $u(e_k)$ sur V_1 parallèlement à W ; elle est donc triangulaire supérieure, ce qui permet de conclure.

Théorème 7.10. — (Cayley-Hamilton, 1858) *Si* Λ *est un anneau commutatif et si* $\mathrm{A} \in \mathbf{M}_n(\Lambda)$, *alors* $\mathrm{Car}_\mathrm{A}(\mathrm{A}) = 0$ *; autrement dit une matrice est annulée par son polynôme caractéristique.*

Soit Λ_univ l'anneau $\mathbf{Z}[\mathrm{X}_{i,j},\ 1 \leqslant i, j \leqslant n]$, et soient $\mathrm{A}_\mathrm{univ} = (\mathrm{X}_{i,j}) \in \mathbf{M}_n(\Lambda_\mathrm{univ})$ et $\mathrm{B}_\mathrm{univ} = \mathrm{Car}_{\mathrm{A}_\mathrm{univ}}(\mathrm{A}_\mathrm{univ}) \in \mathbf{M}_n(\Lambda_\mathrm{univ})$. Il suffit de prouver que $\mathrm{B}_\mathrm{univ} = 0$ (car $\mathrm{Car}_\mathrm{A}(\mathrm{A})$ est la valeur de B_univ en $\mathrm{X}_{i,j} = a_{i,j}$, pour $1 \leqslant i, j \leqslant n$, si $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_n(\Lambda)$, où Λ est un anneau commutatif quelconque) et, pour ce faire, il suffit de prouver que les fonctions polynomiales définies par les coefficients de B_univ sont identiquement nulles sur $\mathbf{M}_n(\mathbf{C})$. Autrement dit, on peut supposer $\Lambda = \mathbf{C}$.

Comme $\mathbf{C}$ est algébriquement clos, il existe (cf. point précédent) une base $f_1, \ldots, f_n$ de $\mathbf{C}^n$ dans laquelle la matrice $(c_{i,j})$ de u_A est triangulaire supérieure, et alors $\mathrm{Car}_\mathrm{A} = \prod_{i=1}^n (\mathrm{X} - c_{i,i})$.

Si $1 \leqslant i \leqslant n$, soit V_i le sous-espace de $\mathbf{C}^n$ engendré par $f_1, \dots, f_i$ (on a donc $\mathrm{V}_n = \mathbf{C}^n$ et on pose $\mathrm{V}_0 = \{0\}$). Alors $(u_{\mathrm{A}} - c_{i,i})(\mathrm{V}_i) \subset \mathrm{V}_{i-1}$, puisque $(c_{i,j})$ est triangulaire supérieure, et une petite récurence montre que $\big(\prod_{i=k}^{n}(u_{\mathrm{A}} - c_{i,i})\big)(\mathbf{C}^n) \subset \mathrm{V}_{k-1}$, si $k \leqslant n$. Pour $k = 1$, cela prouve que $(\mathrm{Car}_{\mathrm{A}}(u_{\mathrm{A}}))(\mathbf{C}^n) = \{0\}$, et donc que $\mathrm{Car}_{\mathrm{A}}(u_{\mathrm{A}}) = 0$ et $\mathrm{Car}_{\mathrm{A}}(\mathrm{A}) = 0$ car $\mathrm{Car}_{\mathrm{A}}(u_{\mathrm{A}})$ est l'endomorphisme de $\mathbf{C}^n$ associé à $\mathrm{Car}_{\mathrm{A}}(\mathrm{A})$.

Si $\dim \mathrm{V} = n$, on a $\mathrm{Car}_u(\mathrm{X}) = \mathrm{X}^n - \mathrm{Tr}(u)\mathrm{X}^{n-1} + \cdots + (-1)^n \det u$, où $\mathrm{Tr}(u)$ est, par définition, la *trace* de u : c'est la somme des termes diagonaux de la matrice de u dans une base quelconque de V.

• Si $u_1, u_2 \in \mathrm{End}(\mathrm{V})$, alors $\mathrm{Tr}(u_1 u_2) = \mathrm{Tr}(u_2 u_1)$.

Le choix d'une base permet de déduire l'énoncé du résultat correspondant pour les matrices.

7.8. Matrices par blocs

Si $\mathbf{n} = (n_1, \dots, n_r)$, on pose $|\mathbf{n}| = n_1 + \cdots + n_r$. Si $\mathbf{n} = (n_1, \dots, n_r)$ et $\mathbf{m} = (m_1, \dots, m_s)$, et si $\mathrm{A} = (a_{\alpha,\beta}) \in \mathbf{M}_{|\mathbf{n}|\times|\mathbf{m}|}(\Lambda)$, on peut écrire A par blocs sous la forme $(\mathrm{A}_{i,j})_{i\leqslant r,\, j\leqslant s}$, où

$$\mathrm{A}_{i,j} = (a_{\alpha,\beta})_{n_1+\cdots+n_{i-1}+1\leqslant\alpha\leqslant n_1+\cdots+n_i,\ m_1+\cdots+m_{j-1}+1\leqslant\beta\leqslant m_1+\cdots+m_j} \in \mathbf{M}_{n_i\times m_j}(\Lambda).$$

Par exemple, si $n = 3 = 1 + 2$ et $m = 4 = 1 + 3$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 5 & 2 & 7 \\ 8 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} \mathrm{A}_{1,1} & \mathrm{A}_{1,2} \\ \mathrm{A}_{2,1} & \mathrm{A}_{2,2} \end{pmatrix}, \text{ avec } \mathrm{A}_{1,1} = (1),\ \mathrm{A}_{1,2} = (2,3,4),\ \mathrm{A}_{2,1} = \begin{pmatrix} 0 \\ 8 \end{pmatrix},\ \mathrm{A}_{2,2} = \begin{pmatrix} 5 & 2 & 7 \\ 1 & 2 & 4 \end{pmatrix}.$$

La décomposition par blocs induit un isomorphisme de $\mathbf{M}_{|\mathbf{n}|\times|\mathbf{m}|}(\Lambda)$ sur l'espace $\mathbf{M}_{\mathbf{n}\times\mathbf{m}}(\Lambda)$, des matrices par blocs $(\mathrm{A}_{i,j})_{i\leqslant r,\, j\leqslant s}$, où $\mathrm{A}_{i,j} \in \mathbf{M}_{n_i\times m_j}(\Lambda)$, pour tout Λ.

Maintenant, si $\boldsymbol{\ell} = (\ell_1, \dots, \ell_t)$, on peut utiliser l'isomorphisme précédent pour définir le produit

$$\mathbf{M}_{\mathbf{n}\times\mathbf{m}}(\Lambda) \times \mathbf{M}_{\mathbf{m}\times\boldsymbol{\ell}}(\Lambda) \cong \mathbf{M}_{|\mathbf{n}|\times|\mathbf{m}|}(\Lambda) \times \mathbf{M}_{|\mathbf{m}|\times|\boldsymbol{\ell}|}(\Lambda) \to \mathbf{M}_{|\mathbf{n}|\times|\boldsymbol{\ell}|}(\Lambda) \cong \mathbf{M}_{\mathbf{n}\times\boldsymbol{\ell}}(\Lambda)$$

des matrices par blocs.

• Ce produit peut se calculer par blocs : si $\mathrm{A} = (\mathrm{A}_{i,j})_{i\leqslant r,\, j\leqslant s}$ et si $\mathrm{B} = (\mathrm{B}_{j,k})_{j\leqslant s,\, k\leqslant t}$ sont deux matrices par blocs avec $\mathrm{A}_{i,j} \in \mathbf{M}_{n_i\times m_j}(\Lambda)$ et $\mathrm{B}_{j,k} \in \mathbf{M}_{m_j\times\ell_k}(\Lambda)$, le produit $\mathrm{C} = \mathrm{AB}$ est la matrice par blocs $(\mathrm{C}_{i,k})_{i\leqslant r,\ k\leqslant t}$, où $\mathrm{C}_{i,k} = \sum_{j=1}^{s} \mathrm{A}_{i,j}\mathrm{B}_{j,k}$.

Par exemple, si on découpe $\mathrm{A} \in \mathbf{M}_{n\times m}(\Lambda)$ suivant ses lignes $\mathrm{X}^*_{i,\mathrm{A}} = (a_{i,1}, \dots, a_{i,m})$ et $\mathrm{B} \in \mathbf{M}_{m\times\ell}(\Lambda)$ suivant ses colonnes $\mathrm{X}_{k,\mathrm{B}} = {}^{\mathrm{t}}(b_{1,k}, \dots, b_{m,k})$, alors AB est la matrice par blocs (ses blocs sont des matrices 1×1) des $\mathrm{X}^*_{i,\mathrm{A}}\mathrm{X}_{k,\mathrm{B}} = \sum_{j=1}^{m} a_{i,j}b_{j,k}$.

La formule $\mathrm{AB} = (\mathrm{X}^*_{i,\mathrm{A}}\mathrm{X}_{k,\mathrm{B}})_{i\leqslant n,\, k\leqslant\ell}$ est immédiate sur la définition du produit de deux matrices. On en déduit que $\left(\begin{smallmatrix} \mathrm{A}' \\ \mathrm{A}'' \end{smallmatrix}\right)(\mathrm{B}', \mathrm{B}'') = \left(\begin{smallmatrix} \mathrm{A}'\mathrm{B}' & \mathrm{A}'\mathrm{B}'' \\ \mathrm{A}''\mathrm{B}' & \mathrm{A}''\mathrm{B}'' \end{smallmatrix}\right)$ en découpant A' et A'' en lignes et B' et B'' en colonnes. Maintenant, si $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n\times m}(\Lambda)$ est découpé sous la forme $\mathrm{A} = (\mathrm{A}', \mathrm{A}'')$, avec $\mathrm{A}' = (a_{i,j}) \in \mathbf{M}_{n\times m_1}(\Lambda)$, $\mathrm{A}'' = (a_{i,j+m_1}) \in \mathbf{M}_{n\times m_2}(\Lambda)$, et si $\mathrm{B} = (b_{j,k}) \in \mathbf{M}_{m\times\ell}(\Lambda)$ est découpé sous la forme $\mathrm{B} = \left(\begin{smallmatrix} \mathrm{B}' \\ \mathrm{B}'' \end{smallmatrix}\right)$, avec $\mathrm{B}' = (b_{j,k}) \in \mathbf{M}_{m_1\times\ell}(\Lambda)$, $\mathrm{B}'' = (b_{j+m_1,k}) \in \mathbf{M}_{m_2\times\ell}(\Lambda)$, l'identité $\mathrm{AB} = \mathrm{A}'\mathrm{B}' + \mathrm{A}''\mathrm{B}''$ est une traduction de la décomposition $\sum_{j=1}^{m} a_{i,j}b_{j,k} = \sum_{j=1}^{m_1} a_{i,j}b_{j,k} + \sum_{j=1}^{m_2} a_{i,j+m_1}b_{j+m_1,k}$. On a donc vérifié le résultat dans

le cas d'un découpage en deux blocs. Le cas général s'en déduit par récurrence sur la somme des nombres de colonnes et lignes de blocs : quand on découpe une ligne de blocs ou une colonne de blocs en deux, on rajoute des produits de blocs 1×2 et 2×1 que l'on sait traiter.

Si $n = m$, $r = s$ et $n_1 = m_1, \ldots, n_r = m_r$, on obtient des *matrices carrées par blocs*. On note simplement $\mathbf{M_n}(\Lambda)$ l'espace des matrices carrées $\mathbf{n} \times \mathbf{n}$ par blocs. Le produit de deux éléments de $\mathbf{M_n}(\Lambda)$ est encore un élément de $\mathbf{M_n}(\Lambda)$.

Une matrice carrée par blocs est dite *diagonale* (resp. *triangulaire supérieure*, resp. *triangulaire inférieure*) si tous les blocs en dehors (resp. en-dessous, resp. au-dessus) de la diagonale sont nuls ; elle est *triangulaire* si elle est triangulaire inférieure ou supérieure.

• Le produit de deux matrices diagonales (resp. triangulaires supérieures, resp. triangulaires inférieures) par blocs est une matrice diagonale (resp. triangulaire supérieure, resp. triangulaire inférieure) par blocs.

Si $i \in \{1, \ldots r\}$, on note V_i le sous-espace de $\mathrm{K}^{|\mathbf{n}|}$ engendré par $e_{n_1+\cdots+n_{i-1}+1}, \ldots, e_{n_1+\cdots+n_i}$. Alors A est diagonale par blocs si et seulement si V_i est stable par u_A, pour tout $i \in \{1, \ldots, s\}$ et A est triangulaire supérieure si et seulement si les sous-espaces $\mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_i$ de $\mathrm{K}^{|\mathbf{n}|}$ sont stables par u_A pour tout $i \in \{1, \ldots, r\}$. Comme ces conditions sont stables par composition, on en tire les deux premiers énoncés. Le cas triangulaire inférieur s'en déduit en passant aux transposées.

• Le déterminant d'une matrice triangulaire par blocs est le produit des déterminants des blocs diagonaux.

Le cas triangulaire inférieure se ramène au cas triangulaire supérieure en prenant la transposée. Par ailleurs, une récurrence immédiate montre qu'il suffit de traiter le cas d'une matrice 2×2 par blocs. Soit donc $\mathrm{A} = (\mathrm{A}_{i,j}) \in \mathbf{M}_{(n_1,n_2)}(\Lambda)$ une matrice triangulaire supérieure. On note $(a_{\alpha,\beta})_{\alpha,\beta \leqslant n_1+n_2}$ les coefficients de A. L'hypothèse selon laquelle A est triangulaire supérieure par blocs se traduit par le fait que $a_{\alpha,\beta} = 0$ si $\alpha \leqslant n_1$ et $\beta > n_1$. Il s'ensuit que dans le déterminant $\det \mathrm{A} = \sum_{\sigma \in \mathrm{S}_{n_1+n_2}} \mathrm{sign}(\sigma) \prod_{\alpha=1}^{n_1+n_2} a_{\alpha,\sigma(\alpha)}$, les seuls termes non nuls sont ceux correspondant aux σ qui stabilisent $\mathrm{I}_1 = \{1, \ldots, n_1\}$ et donc aussi $\mathrm{I}_2 = \{n_1 + 1, \ldots, n_1 + n_2\}$. Une telle permutation s'écrit alors sous la forme $\sigma_1\sigma_2$, où σ_i est une permutation de I_i, que l'on voit comme une permutation de $\{1, \ldots, n_1 + n_2\}$ laissant fixe I_{3-i}, et cette écriture induit un isomorphisme de $\mathrm{Perm}(\mathrm{I}_1) \times \mathrm{Perm}(\mathrm{I}_2)$ sur le sous-groupe de $\mathrm{S}_{n_1+n_2}$ stabilisant I_1 et I_2. Comme $\mathrm{sign}(\sigma_1\sigma_2) = \mathrm{sign}(\sigma_1)\mathrm{sign}(\sigma_2)$, on obtient

$$\det \mathrm{A} = \sum_{\sigma_1,\sigma_2} \prod_{i=1}^{2} \mathrm{sign}(\sigma_i) \prod_{i=1}^{2} \prod_{\alpha \in \mathrm{I}_i} a_{\alpha,\sigma_i(\alpha)} = \prod_{i=1}^{2} \Big(\sum_{\sigma_i} \mathrm{sign}(\sigma_i) \prod_{\alpha \in \mathrm{I}_i} a_{\alpha,\sigma_i(\alpha)} \Big) = \prod_{i=1}^{2} \det \mathrm{A}_{i,i},$$

ce que l'on voulait.

8. Fragments de théorie des corps (commutatifs)

Tous les corps de ce § sont supposés commutatifs.

• Si F est un corps, et si $\varphi : \mathrm{F} \to \mathrm{A}$ est un morphisme d'anneaux où $\mathrm{A} \neq \{0\}$, alors φ est injectif. Un morphisme φ d'un corps F dans un anneau $\mathrm{A} \neq \{0\}$ s'appelle un *plongement*

de F dans A. Si $F \subset K$ sont des corps, et si φ est un plongement de F dans K, un *prolongement* de φ à K est un plongement de K dans A dont la restriction à F est φ.

• Si K est un corps, et si $\iota : A \to K$ est une injection d'anneaux (A est donc intègre), alors ι se prolonge en une injection de corps de Fr(A) dans K, en posant $\iota\left(\frac{a}{b}\right) = \frac{\iota(a)}{\iota(b)}$.

• Si F est un corps, il existe un unique morphisme d'anneaux de $\mathbf{Z}$ dans F, et on dit que F est de *caractéristique* 0 si ce morphisme est injectif, auquel cas F contient $\mathrm{Fr}(\mathbf{Z}) = \mathbf{Q}$. Dans le cas contraire, comme l'image de $\mathbf{Z}$ dans F est intègre (et que c'est un quotient de $\mathbf{Z}$ et donc de la forme $\mathbf{Z}/\mathrm{D}\mathbf{Z}$), il existe un nombre premier p tel que cette image soit le corps $\mathbf{F}_p$ à p éléments, auquel cas on dit que F est de *caractéristique* p. Alors F est un $\mathbf{F}_p$-espace vectoriel et on a, en particulier, $px = 0$, pour tout $x \in F$.

• Si F est de caractéristique p, alors $\varphi : F \to F$, défini par $\varphi(x) = x^p$, est un morphisme (le *morphisme de Frobenius*) de corps.

> On a $\varphi(1) = 1$, $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$ et, comme $\binom{p}{i}$ est divisible par p si $1 \leqslant i \leqslant p-1$, on a $\varphi(x+y) = (x+y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p = x^p + y^p = \varphi(x) + \varphi(y)$. Ceci permet de conclure.

On rappelle que si F est un corps, et si $P \in F[X]$ est irréductible, l'idéal engendré par P est maximal et donc F[X]/P est un corps, ce qui nous fournit un procédé de construction de corps. Plus généralement, si A est un anneau commutatif, et si I est un idéal distinct de A, on peut trouver un idéal maximal [63] $\mathfrak{m}$ qui contient I, et alors $A/\mathfrak{m}$ est un corps.

8.1. Sous-extensions finies

Si F et K sont des corps, avec $F \subset K$, on dit que F est un sous-corps de K et que K est une *extension de* F. Alors K est un espace vectoriel sur F et sa dimension, en tant qu'espace vectoriel sur F, est le *degré* $[K : F]$ de *l'extension* K/F. On dit que K est une *extension finie* de F si $[K : F] < +\infty$; dans le cas contraire, on dit que K est une *extension infinie* de F.

Si K est un corps, et si Z est un sous-ensemble de K, l'intersection de tous les sous-corps (resp. sous-anneaux) de K contenant Z est un sous-corps (resp. sous-anneau) de K : c'est le sous-corps (resp. sous-anneau) de K *engendré* par Z.

— Si F est un sous-corps de K et si $\alpha \in K$, on note respectivement $F(\alpha)$ et $F[\alpha]$ les sous-corps et sous-anneau de K engendrés par F et α.

— Plus généralement, si $\alpha_1, \ldots, \alpha_n \in K$, on note respectivement $F(\alpha_1, \ldots, \alpha_n)$ et $F[\alpha_1, \ldots, \alpha_n]$ les sous-corps et sous-anneau de K engendrés par F et $\alpha_1, \ldots, \alpha_n$.

— Si F_1, F_2 sont deux sous-corps de K, on note $F_1 \cdot F_2$ le sous-corps de K qu'ils engendrent.

• Si K/F est une extension de corps et si M est un sous-F-espace vectoriel de dimension finie $\geqslant 1$ de K, stable par multiplication, alors M est un sous-corps de K.

63. L'existence d'un tel idéal, pour un anneau quelconque, repose sur l'axiome du choix.

L'hypothèse selon laquelle M est un sous-F-espace vectoriel de K implique que c'est un sous-groupe additif. Comme il est stable par multiplication par hypothèse, il suffit de prouver $1 \in \mathrm{M}$ et que tout élément non nul γ de M a un inverse dans M. Soit $\alpha \in \mathrm{M} - \{0\}$. L'application $x \mapsto \gamma x \alpha$ de M dans M est F-linéaire ; par ailleurs elle est injective car γ est inversible dans K ; elle est donc surjective puisque M est de dimension finie, et il existe $x \in \mathrm{M}$ tel que $\gamma x \alpha = \alpha$, ce qui implique que $\gamma x = 1$, et donc que $1 \in \mathrm{M}$ et que x est l'inverse de γ. Ceci permet de conclure.

• Si K est une extension finie de F, et si L est une extension finie de K, alors L est une extension finie de F et on a $[\mathrm{L} : \mathrm{F}] = [\mathrm{L} : \mathrm{K}]\,[\mathrm{K} : \mathrm{F}]$.

Supposons que $[\mathrm{K} : \mathrm{F}] = r$ et $[\mathrm{L} : \mathrm{K}] = s$. Soient $\alpha_1, \ldots, \alpha_r$ une base de K sur F et $\beta_1, \ldots, \beta_s$ une base de L sur K. Les $\alpha_i \beta_j$, pour $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant s$, sont des éléments de L ; montrons qu'ils forment une base de L sur K, ce qui permettra de conclure.

• Soit $x \in \mathrm{L}$. Comme les β_j forment une base de L sur K, on peut écrire x sous la forme $x = \sum_{j=1}^{s} x_j \beta_j$, avec $x_j \in \mathrm{K}$, et comme les α_i forment une base de K sur F, on peut écrire chaque x_j sous la forme $\sum_{i=1}^{r} x_{j,i} \alpha_i$, avec $x_{i,j} \in \mathrm{F}$. On en déduit que $x = \sum_{j=1}^{s} \sum_{i=1}^{r} x_{j,i} \alpha_i \beta_j$ est combinaison linéaire des $\alpha_i \beta_j$ à coefficients dans F, et que les $\alpha_i \beta_j$ forment une famille génératrice de L sur F.

• Si $\sum_{j=1}^{s} \sum_{i=1}^{r} x_{j,i} \alpha_i \beta_j = 0$, avec $x_{i,j} \in \mathrm{F}$, on a $\sum_{j=1}^{s} \big(\sum_{i=1}^{r} x_{j,i} \alpha_i \big) \beta_j = 0$. Or les β_j forment une famille libre sur K et $\sum_{i=1}^{r} x_{j,i} \alpha_i \in \mathrm{K}$; on a donc $\sum_{i=1}^{r} x_{j,i} \alpha_i = 0$ pour tout i, et comme les α_i forment une famille libre sur F et $x_{i,j} \in \mathrm{F}$, on en déduit la nullité des $x_{i,j}$, ce qui prouve que les $\alpha_i \beta_j$ forment une famille libre sur F.

Ceci permet de conclure.

• Soient F un corps et L une extension de F. Si $\mathrm{F}_1, \mathrm{F}_2$ sont deux extensions finies de F contenues dans L, il existe une extension finie K de F, contenue dans L, et contenant F_1 et F_2. En particulier, $\mathrm{F}_1 \cdot \mathrm{F}_2$ est une extension finie de F.

Si $1 = \alpha_1, \ldots, \alpha_r$ (resp. $1 = \beta_1, \ldots, \beta_s$) est une famille génératrice de F_1 (resp. F_2), on peut prendre pour K le sous-F-espace vectoriel de L engendré par les $\alpha_i \beta_j$. En effet, K contient F_1 (resp. F_2) car il contient les $\alpha_i = \alpha_i \beta_1$ (resp. les $\beta_j = \alpha_1 \beta_j$) ; de plus,

— K est de dimension finie $\leqslant rs$ sur F.

— K contient $\alpha\beta$ si $\alpha \in \mathrm{F}_1$ et $\beta \in \mathrm{F}_2$ (il suffit d'écrire $\alpha = \sum_{i=1}^{r} a_i \alpha_i$ et $\beta = \sum_{j=1}^{s} b_j \beta_j$, où les a_i et b_j appartiennent à F, et de développer) ; il contient donc les $(\alpha_i \beta_j)(\alpha_k \beta_\ell) = (\alpha_i \alpha_k)(\beta_j \beta_\ell)$, ce qui permet de montrer qu'il est stable par multiplication.

On peut donc conclure en utilisant le premier point.

8.2. Algébricité, transcendance

• Les conditions suivantes sont équivalentes (on dit que α est *algébrique* sur F si elles sont vérifiées, dans le cas contraire on dit que α est *transcendant* sur F) :

(a) l'extension $\mathrm{F}(\alpha)/\mathrm{F}$ est finie,

(b) il existe une extension finie F' de F contenue dans K et contenant α,

(c) il existe $\mathrm{P} \in \mathrm{F}[\mathrm{X}]$, non nul, tel que $\mathrm{P}(\alpha) = 0$.

• (a)⇒(b) est une évidence (prendre $\mathrm{F}' = \mathrm{F}(\alpha)$), et sa réciproque aussi puisque $\mathrm{F}(\alpha) \subset \mathrm{F}'$.

• Si $\alpha \in \mathrm{F}'$ et si $[\mathrm{F}' : \mathrm{F}] = d$, alors $1, \alpha, \ldots, \alpha^d$ forment une famille liée dans le F-espace vectoriel F′ qui est de dimension d. Il existe donc $a_0, \ldots, a_d \in \mathrm{F}$, non tous nuls, tels que $\sum_{i=0}^{d} a_i \alpha^i = 0$, et on peut prendre $\mathrm{P} = \sum_{i=0}^{d} a_i \mathrm{X}^i$ pour démontrer l'implication (b)⇒(c).

• Si $\mathrm{P}(\alpha) = 0$, avec $\mathrm{P} \in \mathrm{F}[\mathrm{X}]$ de degré $n \geqslant 1$, on peut écrire α^n sous la forme $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_0$, avec $a_0, \ldots, a_{n-1} \in \mathrm{F}$. Il en résulte que le sous-F-espace vectoriel M de K engendré par $1, \alpha, \ldots, \alpha^{n-1}$ est stable par multiplication par α ; il l'est donc aussi par multiplication par α^i, pour tout $i \in \mathbf{N}$, et donc aussi par toute combinaison linéaire $\sum_{i=0}^{n-1} \lambda_i \alpha^i$. Autrement dit, il est stable par multiplication, et comme il est de dimension finie sur F, c'est un sous-corps de K d'après le premier point du n° 8.1. On en déduit l'implication (c)⇒(b), ce qui permet de conclure.

• Si α est algébrique sur F, l'ensemble des $\mathrm{Q} \in \mathrm{F}[\mathrm{X}]$ tels que $\mathrm{Q}(\alpha) = 0$ est un idéal non nul de F[X] ; son générateur unitaire P (le *polynôme minimal* de α) est irréductible, et $\mathrm{F}(\alpha)$ est isomorphe à F[X]/P.

Que l'ensemble des $\mathrm{Q} \in \mathrm{F}[\mathrm{X}]$ tels que $\mathrm{Q}(\alpha) = 0$ soit un idéal de F[X] est une évidence ; il est non nul car α est supposé algébrique. Si P est le générateur unitaire, et si $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$, avec $\mathrm{P}_1, \mathrm{P}_2$ unitaires, alors $\mathrm{P}_1(\alpha)\mathrm{P}_2(\alpha) = 0$, ce qui implique que $\mathrm{P}_1(\alpha) = 0$ ou $\mathrm{P}_2(\alpha) = 0$ puisque L est un corps. Il s'ensuit que P divise P_1 ou P_2, et donc lui est égal pour des questions de degré ; le polynôme P est donc irréductible.

Maintenant, $\mathrm{F}(\alpha)$ étant un sous-anneau de K contenant F et α, il contient tout polynôme en α à coefficients dans F ; autrement dit, il contient l'image L de F[X] par l'application $\mathrm{Q} \mapsto \mathrm{Q}(\alpha)$. Or le noyau de cette application est l'idéal engendré par P ; elle induit donc un isomorphisme du corps F[X]/P sur L, et donc L est un sous-corps de K contenant F et α, et donc aussi $\mathrm{F}(\alpha)$. On en déduit que $\mathrm{L} = \mathrm{F}(\alpha)$, ce qui permet de conclure.

• Si α est algébrique sur F, et si P est son polynôme minimal, alors $[\mathrm{F}(\alpha) : \mathrm{F}] = \deg \mathrm{P}$ (c'est le *degré* de α sur F).

Soit $\mathrm{P} = \mathrm{X}^d + a_{d-1}\mathrm{X}^{d-1} + \cdots + a_0 \in \mathrm{F}[\mathrm{X}]$, irréductible. Compte-tenu du point précédent, il suffit de prouver que $\mathrm{K} = \mathrm{F}[\mathrm{X}]/\mathrm{P}$ est une extension de degré d de F et, pour ce faire, il suffit de prouver que $1, \mathrm{X}, \ldots, \mathrm{X}^{d-1}$ forment une base de K sur F.

• Ils forment une famille libre, sinon il existerait $b_0, \ldots, b_{d-1}$, non tous nuls, tels que $\sum_{i=0}^{d-1} b_i \mathrm{X}^i = 0$, ce qui se traduit par la divisibilité de $\sum_{i=0}^{d-1} b_i \mathrm{X}^i$ par P et est absurde pour des raisons de degré.

• Pour prouver qu'ils forment une famille génératrice, il suffit de prouver que X^n est une combinaison linéaire de $1, \mathrm{X}, \ldots, \mathrm{X}^{d-1}$, pour tout $n \in \mathbf{N}$. C'est clair pour $n \leqslant d-1$; pour $n \geqslant d$, si $\mathrm{X}^{n-1} = \sum_{i=0}^{d-1} c_{n-1,i}\mathrm{X}^i$, on a $\mathrm{X}^n = \sum_{i=0}^{d-1} c_{n-1,i}\mathrm{X}^{i+1} = \sum_{i=0}^{d-1} c_{n,i}\mathrm{X}^i$, avec $c_{n,i} = c_{n-1,i-1} - a_i$, ce qui permet, par récurrence, de conclure.

On dit que $\alpha, \beta \in \mathrm{K}$, algébriques sur F, sont *conjugués* sur F, s'ils ont le même polynôme minimal. Deux éléments conjugués ont en particulier le même degré. Si $\alpha \in \mathrm{K}$ a comme polynôme minimal P sur F, les *conjugués* de α dans K sont les racines de P appartenant à K. Si K est algébriquement clos, et si α est de degré d, alors α a d conjugués dans K, comptés avec multiplicité. On dit que α est *séparable* si son polynôme minimal n'a pas de racine double, ce qui est automatique en caractéristique 0, mais pas en caractéristique p.

Si P est iréductible, il est premier à P′, si $\mathrm{P}' \neq 0$ (sinon il le diviserait, ce qui est absurde puisque $\deg \mathrm{P}' < \deg \mathrm{P}$), et donc P n'a pas de racine double si $\mathrm{P}' \neq 0$. Cette dernière condition

est automatique si F est de caractéristique 0, mais pas en caractéristique p comme le montre l'exemple de $X^p - T$ sur $\mathbf{F}_p(T)$.

• Si α est transcendant sur F, alors $F(\alpha)$ est isomorphe au corps $F(T)$ des fractions rationnelles en une variable.

Le morphisme d'anneaux de $F[X]$ dans K envoyant T sur α a un noyau réduit à 0 puisque α est transcendant. Il peut donc s'étendre en un morphisme d'anneaux du corps $F(T)$ dans K, en envoyant $\frac{P}{Q}$ sur $\frac{P(\alpha)}{Q(\alpha)}$. Comme $F(T)$ est un corps, l'image L de $F(T)$ par ce morphisme est aussi un corps, et $\frac{P}{Q} \mapsto \frac{P(\alpha)}{Q(\alpha)}$ est un isomorphisme de $F(T)$ sur L.

Maintenant, L contient F et α ; il contient donc $F(\alpha)$. Réciproquement, $F(\alpha)$ contient α^n, pour tout n, et donc $P(\alpha)$, pour tout $P \in F[X]$, et donc aussi $\frac{P(\alpha)}{Q(\alpha)}$, pour tout $P \in F[X]$ et tout $Q \in F[X] - \{0\}$; il contient donc L, ce qui prouve que $L = F(\alpha)$ et permet de conclure.

8.3. Extensions algébriques, clôture intégrale

• Si α et β sont algébriques sur F, alors $\alpha+\beta$, $\alpha\beta$ aussi, ainsi que α^{-1}, si $\alpha \neq 0$. L'ensemble des éléments de K qui sont algébriques sur F (la *clôture intégrale* de F dans K) est donc un sous-corps de K.

L'algébricité de α^{-1} résulte de son appartenance à l'extension finie $F(\alpha)$ de F. Maintenant, si α et β sont algébriques sur F, alors $F(\alpha)$ et $F(\beta)$ sont des extensions finies de F et, d'après le 3-ième point du n° 8.1, il existe une extension finie L de F contenue dans F et contenant $F(\alpha)$ et $F(\beta)$. Alors L contient $\alpha + \beta$ et $\alpha\beta$, ce qui prouve que $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur F. Ceci permet de conclure. (On pourrait utiliser les fonctions symétriques des racines pour aboutir au résultat, cf. ex. 4.11.)

On dit que l'extension K/F est *algébrique* si tout $\alpha \in K$ est algébrique sur F ; dans le cas contraire, on dit que l'extension K/F est *transcendante*.

• Si les extensions L/K et K/F sont algébriques, il en est de même de l'extension L/F.

Soit $\alpha \in L$. Par hypothèse, α est algébrique sur K, et il existe donc $P \in K[X]$, de degré $\geqslant 1$, tel que $P(\alpha) = 0$. Par ailleurs, K/F étant algébrique, le sous-corps F′ de K engendré par les coefficients de P et par F est une extension finie de F. On a alors $[F'(\alpha) : F'] \leqslant \deg P$, ce qui fait que $[F'(\alpha) : F]$ est fini ; il en est donc *a fortiori* de même de $[F(\alpha) : F]$ ce qui prouve que α est algébrique sur F. On en déduit le résultat.

Soit K/F une extension de corps. On dit que $P \in F[X]$ *se factorise complètement dans* K ou encore que P *a toutes ses racines dans* K, si on peut l'écrire, dans $K[X]$, comme un produit de facteurs de degré 1.

On dit que K est *algébriquement clos* si tout $P \in K[X]$ se factorise complètement dans K, ce qui équivaut à ce que les polynômes irréductibles de $K[X]$ soient de degré 1, ou encore à ce que tout $P \in K[X]$, de degré $n \geqslant 1$, a n racines (comptées avec multiplicité) dans K. Une récurrence immédiate, portant sur le degré, montre qu'il suffit de vérifier que tout polynôme $P \in K[X]$ de degré $\geqslant 1$ a au moins une racine dans K. L'exemple fondamental de corps algébriquement clos est celui du corps $\mathbf{C}$ des nombres complexes (th. fondamental de l'algèbre, cf. ex. 8.3 pour une démonstration).

• Un corps est algébriquement clos si et seulement si il n'a pas d'extension algébrique.

Cela résulte de ce que F[X]/P est une extension algébrique de degré deg P, si P ∈ F[X] est irréductible.

On dit que K est une *clôture algébrique* de F si K est algébriquement clos et si K est une extension algébrique de F. Par exemple, $\mathbf{C}$ est une clôture algébrique de $\mathbf{R}$. On verra au n° suivant comment, si P ∈ F[X] est fixé, construire une extension algébrique de F contenant toutes les racines de P et, au n° 8.8, comment construire une clôture algébrique de F en rajoutant les racines de tous les P ∈ F[X] (ceci demande d'utiliser l'axiome du choix si on part d'un corps quelconque, mais pas si on part d'un sous-corps de $\mathbf{C}$ comme le montre le point suivant).

• Si K/F est une extension de corps et si K est algébriquement clos, la clôture intégrale $\overline{\mathrm{F}}$ de F dans K est une clôture algébrique de F. Par exemple, l'ensemble $\overline{\mathbf{Q}}$ des *nombres algébriques* (i.e. l'ensemble des $\alpha \in \mathbf{C}$, algébriques sur $\mathbf{Q}$) est une clôture algébrique de $\mathbf{Q}$.

Il suffit de prouver que $\overline{\mathrm{F}}$ est algébriquement clos. Soit donc P ∈ $\overline{\mathrm{F}}$[X] irréductible. Si $\deg \mathrm{P} = n > 1$, alors P a une racine α dans K, n'appartenant pas à $\overline{\mathrm{F}}$, et $\overline{\mathrm{F}}(\alpha)$ est une extension algébrique de $\overline{\mathrm{F}}$ contenue dans K et contenant strictement $\overline{\mathrm{F}}$. Comme $\overline{\mathrm{F}}$ est algébrique sur F, il en est de même de $\overline{\mathrm{F}}(\alpha)$ d'après le point précédent, et on aboutit à une contradiction avec la définition de $\overline{\mathrm{F}}$. Ceci permet de conclure.

Exercice 8.1. — (i) Montrer que $\mathrm{X}^3+\mathrm{X}+1$ est irréductible dans $\mathbf{Q}$[X] (on pourra commencer par montrer qu'une racine éventuelle de $\mathrm{X}^3 + \mathrm{X} + 1$ dans $\mathbf{Q}$ appartient à $\mathbf{Z}$).

(ii) Soient $\alpha \in \mathbf{C}$ vérifiant $\alpha^3 + \alpha + 1 = 0$, et $\mathrm{K} \subset \mathbf{C}$ une extension finie de $\mathbf{Q}$ contenant α. Montrer que [L : $\mathbf{Q}$] est divisible par 3.

(iii) Montrer que α n'appartient pas au sous-corps de $\mathbf{C}$ engendré par $\mathbf{Q}$ et les $\sqrt{n}$, pour $n \in \mathbf{N}$.

Exercice 8.2. — (i) Montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ est une extension de degré 4 de $\mathbf{Q}$.

(ii) Soient $\alpha_1, \alpha_2, \alpha_3$ les racines de $\mathrm{X}^3 - 2$ dans $\mathbf{C}$. Montrer que $[\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbf{Q}] = 6$.

(iii) Soit K/F une extension de corps, et soient $\alpha, \beta \in \mathrm{K}$, algébriques sur F, de degrés respectifs r et s. Montrer que si r et s sont premiers entre eux, alors α est de degré r sur $\mathrm{F}(\beta)$. Le résultat est-il toujours vrai si $(r, s) \neq 1$?

8.4. Constructions à la règle et au compas

Les grecs étaient facinés par les constructions à la règle et au compas, et il nous ont légué trois problèmes sur lesquels ils se sont cassé les dents, à savoir :

◇ la *duplication du cube* : construire un cube de volume moitié d'un cube donné,

◇ la *trissection de l'angle* : couper un angle en 3 angles égaux (il est très facile de bissecter un angle avec une règle et un compas),

◇ la *quadrature du cercle* : construire un carré dont l'aire est égale à celle d'un disque donné.

Les deux premiers problèmes ont été résolus (négativement : la duplication du cube est impossible et la trissection d'un angle quelconque aussi) par Wantzel (1837), le troisième l'a été (négativement : la quadrature du cercle est impossible) par Lindemann (1882) en prouvant que π est un nombre transcendant

(cf. annexe E pour une démonstration de cette transcendance). Pour expliquer comment on peut arriver à démontrer un tel résultat [64], nous allons avoir besoin de formaliser un peu le problème.

Si I est un ensemble de cardinal $\geqslant 2$ de points du plan identifié au plan des nombres complexes, on se permet de tracer toutes les droites joignant deux points de I et tous les cercles de centre un point de I et de rayon la distance entre deux points de I. On note I' la réunion de I et des points d'intersection des droites et cercles ainsi obtenus. On définit alors, par récurrence, une suite croissante d'ensembles de points du plan en posant $\mathrm{I}^{[0]} = \mathrm{I}$ et $\mathrm{I}^{[n+1]} = (\mathrm{I}^{[n]})'$, et on dit que P est *constructible à la règle et au compas à partir de* I s'il appartient à l'un des $\mathrm{I}^{[n]}$ ($\mathrm{I}^{[n]}$ est l'ensemble des points constructibles en moins de n étapes). On peut toujours faire un changement de repère dans le plan complexe et supposer que I contient 0 et 1. La duplication du cube demande une construction de $\sqrt[3]{2}$ à partir de 0 et 1, la trissection de l'angle demande une construction de $e^{i\alpha/3}$ à partir de $0, 1$ et $e^{i\alpha}$, et la quadrature du cercle demande une construction de $\sqrt{\pi}$ à partir de 0 et 1.

Comme on a supposé que I contient 0 et 1, un peu d'astuce permet de montrer que l'ensemble des nombres constructibles à partir de I est un sous-corps de $\mathbf{C}$ [par exemple, en prouvant que z est constructible si et seulement si ses parties réelle et imaginaire le sont, et en utilisant le th. de Thalès pour faire des multiplications et des divisions de nombres réels (on peut construire la parallèle à une droite donnée passant par un point donnée)]. De plus, une petite analyse des équations donnant l'intersection de cercles et de droites montre que le corps des nombres constructibles s'obtient par une suite d'extensions de degré 2 du corps engendré par les parties imaginaires et réelles des éléments de I (un peu plus d'astuce montre que, réciproquement, tout élément d'un corps obtenu par une suite d'extensions de degré 2 du corps engendré par les parties imaginaires et réelles des éléments de I est constructible à partir de I).

Pour démontrer l'impossibilité de la duplication du cube, il suffit de prouver que $\sqrt[3]{2}$ n'appartient à aucun sous-corps L de $\mathbf{C}$ obtenu à partir de $\mathbf{Q}$ par une suite d'extensions de degré 2, ce qui suit de ce que $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$, alors que le degré d'un tel L est de la forme 2^n qui n'est pas divisible par 3.

De même, on peut par exemple montrer que les angles aigus du triangle rectangle de côtés $3, 4, 5$ ne sont pas trissectables. En effet, si $\beta = \frac{3+4i}{5}$, on a $\beta = \frac{2+i}{2-i}$, et $2+i$ et $2-i$ engendrent des idéaux premiers distincts de $\mathbf{Z}[i]$, et donc $v_{2+i}(\beta) = 1$, ce qui prouve que β n'est pas un cube dans $\mathbf{Q}(i) = \mathbf{Q}(\beta)$, et donc que le polynôme $\mathrm{X}^3 - \beta$ est irréductible dans $\mathbf{Q}(i)[\mathrm{X}]$. Il en résulte que les racines cubiques de β sont de degré 3 sur $\mathbf{Q}(i)$ et ne sont donc pas constructibles à partir de β (dont les parties réelle et imaginaire sont rationnelles). Il existe toutefois des angles trissectables : par exemple, comme $\left(\frac{-4+3i}{5}\right)^3 = \frac{117+44i}{125}$, les angles du triangle rectangle de côtés $117, 44, 125$ sont trissectables.

8.5. Degré de transcendance

Soit K/F une extension de corps. On dit que $x_1, \ldots, x_n \in \mathrm{K}$ sont *algébriquement indépendants* sur F s'il n'existe pas de $\mathrm{P} \in \mathrm{F}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ non nul, tel $\mathrm{P}(x_1, \ldots, x_n) = 0$ (si $n = 1$, on retombe sur la définition d'un élément transcendant) ; cela se traduit aussi par l'injectivité du morphisme d'anneaux $\mathrm{P} \mapsto \mathrm{P}(x_1, \ldots, x_n)$ de $\mathrm{F}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ dans K ou par la transcendance de x_i sur $\mathrm{F}(x_1, \ldots, \hat{x}_i, \ldots, x_n)$ pour tout i. Si c'est le cas, le sous-corps de K engendré par F et $x_1, \ldots, x_n$ est isomorphe au corps $\mathrm{F}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ des fractions rationnelles en n variables.

64. Il y a beaucoup de mathématiciens amateurs qui ont du mal à concevoir ce qu'un tel énoncé signifie exactement, et qui croient que cette absence de solution n'est qu'un constat d'échec d'une méthode particulière et qu'il existe une autre méthode (la leur) permettant de résoudre le problème positivement.

On dit que $x_1, \dots, x_n$ est une *base de transcendance* de K sur F si les x_i sont algébriquement indépendants et si K est une extension algébrique de $\mathrm{F}(x_1, \dots, x_n)$; on dit que K est de *degré de transcendance* fini sur F s'il possède une base de transcendance finie sur F ; dans le cas contraire on dit que K est de degré de transcendance infini sur F. Si K est de degré de transcendance fini sur F, on définit le degré de transcendance de K/F comme le minimum des cardinaux des bases de transcendances. Une extension de degré de transcendance 0 est donc une extension algébrique.

• Si K/F est de degré de transcendance n, toutes les bases de transcendance de K/F sont de cardinal n, et $x_1, \dots, x_n$ forment une base de transcendance si et seulement si ils sont algébriquement indépendants sur F.

La démonstration se fait par récurrence sur n. Pour $n = 0$, l'énoncé se réduit au fait qu'une extension algébrique ne contient pas d'élément transcendant. Si $n \geqslant 1$, et si $x_1, \dots, x_n$ et $y_1, \dots, y_m$ sont des bases de transcendance de K sur F, il existe j tel que y_j soit transcendant sur $\mathrm{F}' = \mathrm{F}(x_1, \dots, x_{n-1})$, sinon K serait une extension algébrique de F' ce qui contredit l'hypothèse que $x_1, \dots, x_n$ sont algébriquement indépendants. Quitte à réordonner les y_j, on peut supposer que $j = m$, et alors y_m est transcendant sur F' et algébrique sur $\mathrm{F}'(x_n)$. Le polynôme minimal de y_m sur $\mathrm{F}'(x_n)$ est donc de la forme $y_m^d + f_{d-1}y_m^{d-1} + \cdots + f_0$, où les f_i n'appartiennent pas tous à F'. En multipliant par le ppcm des dénominateurs, on obtient une équation du type $\mathrm{P}(x_n, y_m) = 0$ où $\mathrm{P} \in \mathrm{F}'[\mathrm{X}, \mathrm{Y}]$ est de degré $\geqslant 1$ en X, ce qui montre que x_n est algébrique sur $\mathrm{F}'(y_m)$, et donc que $x_1, \dots, x_{n-1}, y_m$ est une base de transcendance de K sur F. Mais alors $x_1, \dots, x_{n-1}$ et $y_1, \dots, y_{m-1}$ sont des bases de transcendance de K sur $\mathrm{F}(y_m)$, et l'hypothèse de récurrence permet d'en déduire que $n - 1 = m - 1$, et donc que $n = m$, ce qui démontre le premier énoncé.

Si $x_1, \dots, x_n$ sont algébriquement indépendants sur F, et si $y_1, \dots, y_n$ est une base de transcendance de K sur F, on peut compléter $x_1, \dots, x_n$ par des y_i de manière à obtenir une base de transcendance (il suffit de prendre une partie I maximale de $\{1, \dots, n\}$ telle que les x_j et les y_i pour $i \in \mathrm{I}$ soient algébriquement indépendants : la maximalité de I assure que les autres sont algébriques sur l'extension F' engendrée par les x_j et les y_i pour $i \in \mathrm{I}$, et donc que K est algébrique sur F'). La base ainsi obtenue étant de cardinal n d'après ce qui précède et contenant les x_j, cela prouve que $x_1, \dots, x_n$ est une base de transcendance de K sur F. Ceci permet de conclure.

8.6. Constructions d'extensions algébriques

• Si $\mathrm{P} \in \mathrm{F}[\mathrm{X}]$ est irréductible, alors $\mathrm{K} = \mathrm{F}[\mathrm{X}]/\mathrm{P}$ est une extension finie de F, dans laquelle P a une racine.

On a déjà vérifié, au n° précédent, que K est une extension finie de F (de degré $\deg \mathrm{P}$). Par ailleurs, $\mathrm{P}(\mathrm{X}) = 0$ dans K (par construction), et donc X est une racine de P dans K.

• $\mathrm{K} = \mathrm{F}[\mathrm{X}]/\mathrm{P}$ est « la plus petite » extension de F ayant cette propriété (on l'appelle le *corps de rupture* de P) : si ι est un plongement de F dans un corps L, l'ensemble des prolongements de ι à $\mathrm{K} = \mathrm{F}[\mathrm{X}]/\mathrm{P}$ est en bijection avec celui des racines de [65] P^ι dans

65. Si $\mathrm{Q} = \sum_{i=0}^n a_n \mathrm{X}^n \in \mathrm{F}[\mathrm{X}]$, on note Q^ι l'élément $\sum_{i=0}^n \iota(a_n)\mathrm{X}^n$ de $\mathrm{L}[\mathrm{X}]$; il est immédiat que $\mathrm{Q} \mapsto \mathrm{Q}^\iota$ est un morphisme d'anneaux de $\mathrm{F}[\mathrm{X}]$ dans $\mathrm{L}[\mathrm{X}]$.

L ; en particulier, il existe un tel prolongement si L contient une racine de P^ι et il y a au plus [K : F] tels prolongements.

Si $\alpha \in L$, il existe un unique morphisme d'anneaux de F[X] dans L coïncidant avec ι sur F et envoyant X sur α (à savoir celui envoyant $Q(X)$ sur $Q^\iota(\alpha)$). Ce morphisme se factorise à travers $F[X]/P = K$ (et donc fournit un prolongement de ι à K), si et seulement si $P^\iota(\alpha) = 0$, ce qui nous fournit la bijection annoncée entre les prolongements de ι à K et les racines de P^ι dans L.

• Soient K/F une extension finie et ι un plongement de F dans un corps L. Si L est algébriquement clos, il existe [66] un prolongement de ι à K, et si L est quelconque, il y a au plus [K : F] tels prolongements.

Soient $\alpha_1, \ldots, \alpha_n$ tels que $K = F(\alpha_1, \ldots, \alpha_n)$ (on peut par exemple prendre une base de l'espace vectoriel K sur F). On fait une récurrence sur n, le cas $n = 0$, qui correspond à $K = F$, étant évident. Soient $F' = F(\alpha_1, \ldots, \alpha_{n-1})$ et $P \in F'[X]$ le polynôme minimal de α_n. D'après le point précédent, l'ensemble des prolongements de ι à K est en bijection avec la réunion, pour ι' prolongement de ι à F′, de l'ensemble des racines de $\iota'(P)$ dans L.

• Si L est algébriquement clos, cet ensemble est non vide pour chaque ι' et il y a donc au moins un prolongement de ι à K pour chaque prolongement de ι à F′, ce qui prouve qu'il y a au moins un prolongement de ι à K.

• Si L est quelconque, pour chaque choix de ι', il y a au plus [K : F′] racines de $\iota(P)$ dans L, et comme il y a au plus [F′ : F] choix de ι' d'après l'hypothèse de récurrence, on en déduit qu'il y a au plus $[K : F'][F' : F] = [K : F]$ prolongements de ι à K. Ceci permet de conclure.

• Si $P_1, \ldots, P_n \in F[X]$ sont unitaires, il existe une extension finie K de F dans laquelle les P_j se factorisent complètement ; autrement dit, il existe une extension finie de F contenant toutes les racines des P_j (une telle extension est un *corps de décomposition* pour $P_1, \ldots, P_n$ si elle est engendrée par les racines des P_j ; si L est un corps algébriquement clos contenant F, le sous-corps de L engendré par F et les racines des P_i est un corps de décomposition pour $P_1, \ldots, P_n$).

On déduit le cas n quelconque du cas $n = 1$ en considérant le polynôme $P = P_1 \cdots P_n$. On construit K en rajoutant les racines de P une à une ; l'extension ainsi obtenue est donc un corps de décomposition de P puisqu'elle est engendrée par les racines de P. Si tous les facteurs irréductibles de P sont de degré 1, il n'y a rien à faire. Sinon, on choisit un facteur irréductible Q_1 de P de degré $\geqslant 2$, et on pose $K_1 = F[X]/Q_1$, de telle sorte que Q_1 (et donc aussi P) acquiert un facteur irréductible de degré 1 dans K_1. On factorise P dans K_1, et on recommence : si tous les facteurs irréductibles de P sont de degré 1, il n'y a rien à faire, sinon, on choisit un facteur irréductible Q_2 de P de degré $\geqslant 2$, et on pose $K_2 = K_1[X]/Q_2$. Comme le nombre de facteurs irréductibles de degré 1 augmente strictement à chaque étape, au bout d'au plus $d - 1$ étapes [67], on obtient un corps dans lequel tous les facteurs irréductibles de P sont de degré 1, ce que l'on voulait.

66. Ce résultat est aussi valable pour une extension infinie, voir plus loin. Il permet, si on dispose d'un corps algébriquement clos L contenant F, de supposer que toutes les extensions algébriques de F considérées sont des sous-corps de L.

67. Remarquons que le procédé peut converger en beaucoup moins de $d - 1$ étapes.

• Si K/F est un corps de décomposition de $P_1, \dots, P_n$, si ι est un plongement de F dans un corps L dans lequel les $\iota(P_i)$ se factorisent complètement, alors il existe un prolongement de ι à K.

Soit $P = P_1 \cdots P_n$. Par hypothèse, on peut factoriser P sous la forme $P = \prod_{i=1}^{d}(X - \alpha_i)$ dans K, et on a $K = F(\alpha_1, \dots, \alpha_d)$. Prouvons, par récurrence sur i, que l'on peut prolonger ι à $F_i = F(\alpha_1, \dots, \alpha_i)$. Il n'y a rien à faire si $i = 0$, et si $i \geqslant 0$, notons $Q_i \in F_i[X]$ le polynôme minimal de α_{i+1} sur F_i. Alors Q_i divise P, et donc $\iota_i(Q_i)$ divise $\iota(P)$, si ι_i est un prolongement de ι à F_i. comme $\iota(P)$ est complètement factorisable dans L par hypothèse, $\iota_i(Q_i)$ a toutes ses racines dans L, et tout choix de racine nous fournit un prolongement de ι à F_{i+1}. Ceci permet de conclure.

• Deux corps de décomposition sont isomorphes [68].

Soient K_1, K_2 deux corps de décomposition de $P_1, \dots, P_n$. Le point précédent fournit des plongements de K_1 dans K_2 et de K_2 dans K_1, et $[K_1 : F] \leqslant [K_2 : F]$ et $[K_2 : F] \leqslant [K_1 : F]$. On en déduit que $[K_1 : F] = [K_2 : F]$; les plongements précédents sont donc des isomorphismes, ce qui permet de conclure.

Exercice 8.3. — Soit $P \in \mathbf{R}[X]$, unitaire, de degré $n \geqslant 1$, et soit L une extension finie de $\mathbf{R}$, contenant $\mathbf{C}$, dans laquelle P se factorise complètement sous la forme $P = \prod_{i=1}^{n}(X - \alpha_i)$. Si $t \in \mathbf{R}$, on note $Q_t \in L[X]$ le polynôme $\prod_{i<j}(X - \alpha_i - \alpha_j - t\alpha_i\alpha_j)$.

(i) Montrer que $Q_t \in \mathbf{R}[X]$.

(ii) Comparer $v_2(\deg Q_t)$ et $v_2(\deg P)$, si $v_2(\deg P) \geqslant 1$ (où v_2 désigne la valuation 2-adique) ; en déduire, par récurrence sur $r = v_2(\deg P)$, que P a une racine dans $\mathbf{C}$. (On pourra commencer par vérifier qu'un polynôme de degré 2 de $\mathbf{C}[X]$ a deux racines dans $\mathbf{C}$.)

(iii) Montrer que $\mathbf{C}$ est algébriquement clos.

8.7. Corps finis

Si F est un corps fini, alors F ne peut pas être de caractéristique 0, il est donc de caractéristique p pour un certain p, et F est une extension finie de $\mathbf{F}_p$. Dans tout ce qui suit, on note φ le morphisme de Frobenius $x \mapsto x^p$ sur tout corps de caractéristique p. Si $i \in \mathbf{N}$, on note φ^i le composé i fois de φ ; c'est le morphisme de corps $x \mapsto x^{p^i}$.

• Si K est de caractéristique p, et si $i \in \mathbf{N}$, alors $\{x \in K,\ \varphi^i(x) = x\}$ est un sous-corps de K qui est égal à $\mathbf{F}_p$ si $i = 1$.

• Si $P(X) = X^p - 1 \in \mathbf{Q}[X]$, avec p premier, alors $P = (X-1)(X^{p-1} + \cdots + 1)$, et si on rajoute une racine du polynôme $X^{p-1} + \cdots + 1$ à $\mathbf{Q}$ (i.e. une racine primitive p-ième ζ de l'unité), alors P se factorise complètement sous la forme $P = (X-1)\prod_{i=1}^{p-1}(X - \zeta^i)$. Il ne faut donc qu'une étape dans ce cas.

• Si $P(X) = X^p - 2 \in \mathbf{Q}[X]$, et si on rajoute une racine α de P à $\mathbf{Q}$, alors P se factorise sous la forme $P = (X - \alpha)(X^{p-1} + \alpha X^{p-2} + \cdots + \alpha^{p-1})$. Si on rajoute une seconde racine β de P, alors $\zeta = \frac{\beta}{\alpha}$ est une racine primitive p-ième de l'unité, et P se factorise dans $\mathbf{Q}(\alpha, \beta)[X]$ sous la forme $(X - \alpha)\prod_{i=1}^{p-1}(X - \alpha\zeta^i)$. Il ne faut donc que deux étapes dans ce cas.

• Par contre, si on part de $P \in \mathbf{Q}[X]$ choisi au hasard, alors il faut en général $d - 1$ étapes pour obtenir toutes les racines de P (th. d'irréductibilité de Hilbert, 1892).

68. La structure d'un corps de décomposition fait l'objet de la théorie de Galois.

Comme φ^i est un morphisme de corps, l'ensemble de ses points fixes est stable par addition, multiplication, et passage à l'inverse ; c'est donc un sous-corps de K.

Maintenant, $\varphi(x) = x^p$, et donc l'équation $\varphi(x) = x$ a au plus p solutions dans K ; comme l'ensemble des solutions contient $\mathbf{F}_p$ d'après le petit th. de Fermat, le sous-corps de K fixé par φ est exactement $\mathbf{F}_p$.

• Le cardinal de F est une puissance de p : si $[\mathrm{F} : \mathbf{F}_p] = n$, alors $|\mathrm{F}| = p^n$.

Si $[\mathrm{F} : \mathbf{F}_p] = n$, le choix d'une base de F sur $\mathbf{F}_p$ fournit une bijection de $\mathbf{F}_p^n$ sur F ; on a donc $|\mathrm{F}| = |\mathbf{F}_p^n| = p^n$.

• Soit $\mathrm{P} \in \mathbf{F}_p[\mathrm{X}]$, irréductible, unitaire de degré d, et soit K une extension de $\mathbf{F}_p$ dans laquelle P a une racine α. Alors $\varphi^d(\alpha) = \alpha$ et $\mathrm{P} = \prod_{i=0}^{d-1}(\mathrm{X} - \varphi^i(\alpha))$ dans $\mathrm{K}[\mathrm{X}]$; autrement dit, les conjugués de α sont les α^{p^i}, pour $0 \leqslant i \leqslant d-1$.

Écrivons P sous la forme $\mathrm{X}^d + a_{d-1}\mathrm{X}^{d-1} + \cdots + a_0$, et appliquons φ à l'identité $\mathrm{P}(\alpha) = 0$. Comme $a_i \in \mathbf{F}_p$, on a $\varphi(a_i) = a_i$, pour tout i, et comme φ est un morphisme de corps, on obtient $\mathrm{P}(\varphi(\alpha)) = 0$. Il en résulte que $\varphi(\alpha)$ est une racine de P ; il en est donc de même, par récurrence, de $\varphi^i(\alpha)$, pour tout $i \in \mathbf{N}$.

Comme P est de degré fini, l'application $i \mapsto \varphi^i(\alpha)$ n'est pas injective et il existe $i < j$ tels que $\varphi^i(\alpha) - \varphi^j(\alpha) = 0$. Comme $\varphi^i(\alpha) - \varphi^j(\alpha) = \varphi^i(\alpha - \varphi^{j-i}(\alpha))$, on en déduit qu'il existe $k \geqslant 1$ tel que $\varphi^k(\alpha) = \alpha$, et les $\varphi^i(\alpha)$, pour $0 \leqslant i \leqslant k-1$, soient distincts deux à deux. Alors $\mathrm{Q} = \prod_{i=0}^{k-1}(\mathrm{X} - \varphi^j(\alpha)) = \mathrm{X}^k + b_{k-1}\mathrm{X}^{k-1} + \cdots + b_0$ divise P.

Pour conclure, il suffit donc de prouver que P divise Q, et comme P est le polynôme minimal de α sur $\mathbf{F}_p$ puisqu'il est irréductible, et que $\mathrm{Q}(\alpha) = 0$, il suffit de vérifier que Q est à coefficients dans $\mathbf{F}_p$. Or $b_{k-i} = \pm\Sigma_i(\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha))$, et $\varphi\big(\Sigma_i(\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha))\big) = \Sigma_i(\varphi(\alpha), \ldots, \varphi^k(\alpha))$ est égal à $\Sigma_i(\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha))$ puisque $\varphi^k(\alpha) = \alpha$ et que Σ_i est invariant par permutation des variables. On en déduit l'appartenance de $\Sigma_i(\alpha, \varphi(\alpha), \ldots, \varphi^{k-1}(\alpha))$ à $\mathbf{F}_p$, et donc aussi celle de b_{k-i}, ce qui permet de conclure.

• Soit K un corps de caractéristique p. Si F est un sous-corps fini de K, de cardinal q, alors $\mathrm{F} = \{\alpha \in \mathrm{K},\ \alpha^q = \alpha\}$.

Posons $q = p^n$ de telle sorte que $[\mathrm{F} : \mathbf{F}_p] = n$. Soit $\alpha \in \mathrm{F}$. Alors $d = [\mathbf{F}_p(\alpha) : \mathbf{F}_p]$ divise n, et comme $\alpha^{p^d} = \alpha$ d'après le point précédent, on $\alpha^q = \alpha$. Autrement dit $\mathrm{F} \subset \{\alpha \in \mathrm{K},\ \alpha^q = \alpha\}$.

Cette inclusion est une égalité car $|\mathrm{F}| = q$, alors que $|\{\alpha \in \mathrm{K},\ \alpha^q = \alpha\}| \leqslant q$, un polynôme de degré q ayant au plus q racines dans K.

Exercice 8.4. — Soient F de cardinal q, $\mathrm{P} \in \mathrm{F}[\mathrm{X}]$, irréductible, unitaire de degré d, et K une extension de F dans laquelle P a une racine α. Montrer que $\alpha^{q^d} = \alpha$ et $\mathrm{P} = \prod_{i=0}^{d-1}(\mathrm{X} - \alpha^{q^i})$ dans $\mathrm{K}[\mathrm{X}]$.

• Si $q = p^n$, il existe, à isomorphisme près, un unique corps $\mathbf{F}_q$ de cardinal q. De plus, les automorphismes de $\mathbf{F}_q$ sont $\mathrm{id}, \varphi, \ldots \varphi^{n-1}$, et $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$ si et seulement si $d \mid n$.

D'après le point précédent, un corps de cardinal q est un corps de décomposition pour $\mathrm{X}^q - \mathrm{X}$; on en déduit l'existence de $\mathbf{F}_q$ et son unicité à à isomorphisme près.

Maintenant, $\mathrm{id}, \varphi, \ldots \varphi^{n-1}$ sont des plongements de $\mathbf{F}_q$ dans $\mathbf{F}_q$ laissant fixe $\mathbf{F}_p$ et comme il y a au plus $[\mathbf{F}_q : \mathbf{F}_p] = n$ tels plongements, il suffit de vérifier qu'ils sont tous distincts pour prouver que ce sont tous les automorphismes de $\mathbf{F}_q$. Si $\varphi^i = \varphi^j$ avec $j > i$, on a $\varphi^{j-i} = \mathrm{id}$, ce

qui se traduit par $x^{p^{j-i}} = x$, pour tout $x \in \mathbf{F}_q$, et est impossible si $j - i < n$ car le polynôme $\mathrm{X}^{p^{j-i}} - \mathrm{X}$ a au plus p^{j-i} racines ; d'où le résultat.

Enfin, si $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$, alors $d = [\mathbf{F}_{p^d} : \mathbf{F}_p]$ divise $n = [\mathbf{F}_{p^n} : \mathbf{F}_p]$. Réciproquement, si $d \mid n$, les points fixes de φ^d (à savoir $\mathbf{F}_{p^d}$) sont aussi des points fixes de φ^n, et donc $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$.

• Si on choisit un plongement de $\mathbf{F}_{p^{n!}}$ dans $\mathbf{F}_{p^{(n+1)!}}$, pour tout n, alors $\overline{\mathbf{F}}_p = \cup_{n\in\mathbf{N}}\mathbf{F}_{p^{n!}}$ est une clôture algébrique [69] de $\mathbf{F}_p$.

Soit $\mathrm{P} \in \overline{\mathbf{F}}_p[\mathrm{X}]$. Il existe $n \in \mathbf{N}$ tel que $\mathrm{P} \in \mathbf{F}_{p^{n!}}[\mathrm{X}]$. Maintenant, il existe une extension finie K de $\mathbf{F}_{p^{n!}}$ dans laquelle P se factorise complètement ; K est alors un corps fini, et donc de la forme $\mathbf{F}_{p^m}$, et il est inclus dans $\mathbf{F}_{p^{m!}}$ et donc aussi dans $\overline{\mathbf{F}}_p$. Il s'ensuit que P se factorise complètement dans $\overline{\mathbf{F}}_p$, ce qui prouve que $\overline{\mathbf{F}}_p$ est algébriquement clos. Comme c'est une extension algébrique de $\mathbf{F}_p$, puisque les $\mathbf{F}_{p^{n!}}$ le sont, c'est une clôture algébrique de $\mathbf{F}_p$.

8.8. La clôture algébrique d'un corps

• Si L est une extension algébrique de K dans laquelle tout $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ a une racine, alors L est une clôture algébrique de K.

Il suffit de prouver que L est algébriquement clos. Soient donc $\mathrm{P} \in \mathrm{L}[\mathrm{X}]$ irréductible, $\mathrm{L}' = \mathrm{K}[\mathrm{X}]/\mathrm{P}$ et $\alpha \in \mathrm{L}'$ l'image de X. Alors α est algébrique sur K puisque L est algébrique sur K ; on note Q son polynôme minimal, et on choisit une extension finie L'' de L dans laquelle Q est scindé et donc se factorise sous la forme $\mathrm{Q}(\mathrm{X}) = \prod_{i=1}^{d}(\mathrm{X} - \alpha_i)$, avec $\alpha_1 = \alpha$.

• Si K est fini, l'hypothèse implique que l'un des α_i appartient à L, et on montre directement (cf. n° 8.7) que les autres α_j sont des puissances de α_i, et donc en particulier que $\alpha \in \mathrm{L}$, ce qui permet de conclure dans ce cas.

• Soit K infini. Si $t_1, \dots, t_d \in \mathrm{K}$, le polynôme $\mathrm{R}_{\mathbf{t}}(\mathrm{X}) = \prod_{\sigma\in\mathrm{S}_d}\big(\mathrm{X} - (t_1\alpha_{\sigma(1)} + \cdots + t_d\alpha_{\sigma(d)})\big)$ est symétrique en $\alpha_1, \dots, \alpha_d$ (on s'est débrouillé pour) ; ses coefficients sont donc des polynômes en les t_i et les coefficients de Q, et $\mathrm{R}_{\mathbf{t}}(\mathrm{X}) \in \mathrm{K}[\mathrm{X}]$. Il découle de l'hypothèse qu'il existe $\sigma \in \mathrm{S}_d$ tel que $t_1\alpha_{\sigma(1)} + \cdots + t_d\alpha_{\sigma(d)} \in \mathrm{L}$, ce qui équivaut à $t_{\tau(1)}\alpha_1 + \cdots + t_{\tau(d)}\alpha_d \in \mathrm{L}$, où $\tau = \sigma^{-1}$.

Soit $\mathrm{W} = \{(t_1, \dots, t_d) \in \mathrm{K}^n,\ t_1\alpha_1 + \cdots t_d\alpha_d \in \mathrm{L}\}$. Alors W est un sous-espace vectoriel de K^n, et on a $\mathrm{K}^n = \cup_{\tau\in\mathrm{S}_d} u_\tau(\mathrm{W})$ d'après ce qui précède, où $u_\tau : \mathrm{K}^n \to \mathrm{K}^n$ est l'endomorphisme défini par la formule $u_\tau(t_1, \dots, t_d) = (t_{\tau(1)}, \dots, t_{\tau(d)})$. Comme K est infini, il résulte de l'ex. 8.5 que l'un des $u_\tau(\mathrm{W})$ est égal à K^n, et donc que $\mathrm{W} = \mathrm{K}^n$. On en déduit l'appartenance de α à L, ce qui permet de conclure.

• Tout corps K possède une clôture algébrique (Steinitz, 1910).

Partons de l'anneau $\mathrm{K}[\mathrm{X}_\mathrm{P},\ \deg \mathrm{P} \geqslant 1]$ des polynômes en une infinité de variables (une pour chaque $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$, non constant). L'idéal engendré par les $\mathrm{P}(\mathrm{X}_\mathrm{P})$, pour $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ non constant, ne contient pas 1 (en effet, s'il contenait 1, on aurait une relation $1 = \sum \mathrm{Q}_\mathrm{P}\mathrm{P}(\mathrm{X}_\mathrm{P})$, où les Q_P sont presque tous nuls ; cette relation ne fait intervenir qu'un ensemble fini de X_P, et donc un ensemble fini Z de polynômes P, et on peut construire une extension finie L de K dans laquelle tout $\mathrm{P} \in \mathrm{Z}$ a une racine α_P ; si on évalue l'identité $1 = \sum \mathrm{Q}_\mathrm{P}\mathrm{P}(\mathrm{X}_\mathrm{P})$ en $\mathrm{X}_\mathrm{P} = \alpha_\mathrm{P}$, pour $\mathrm{P} \in \mathrm{Z}$, on obtient $1 = 0$, d'où une contradiction qui montre que cet idéal ne contient pas 1) ;

69. On a $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$ si n divise m. Or n divise 0 pour tout n, ce qui permet, avec un peu d'audace, d'espérer une "inclusion" $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^0}$, pour tout n, et donc une "inclusion" de $\overline{\mathbf{F}}_p$ dans $\mathbf{F}_1$. Il s'ensuit que le corps $\mathbf{F}_1$ "à un élément" doit être un objet assez énorme, s'il existe, puisqu'il doit "contenir" $\overline{\mathbf{F}}_p$, pour tout p (remarque due à Zagier).

on peut donc trouver un idéal maximal I qui le contient. Le quotient L de $K[X_P,\ \deg P \geqslant 1]$ par I est alors un corps, algébrique sur K puisque engendré par les images des X_P qui sont algébriques [70] sur K puisque, par construction, $P(X_P) = 0$ dans L, et tout $P \in K[X]$ non constant a une racine dans L, à savoir X_P. Il résulte du point précédent que L est une clôture algébrique de K.

Exercice 8.5. — Soient F un corps infini et V un sous-espace vectoriel sur F. Soient $W_1, \ldots, W_n$ des sous-espaces vectoriels de V tels que $W = W_1 \cup \cdots \cup W_n$ soit un sous-espace vectoriel de V. Montrer qu'il existe $i \in \{1, \ldots, n\}$ tel que $W_j \subset W_i$, pour tout $j \in \{1, \ldots, n\}$.

• Soit K/F une extension algébrique. Si L est algébriquement clos, et si ι est un plongement de F dans K, alors ι a un prolongement à K.

On peut écrire K comme le quotient de l'anneau $F[X_\alpha,\ \alpha \in K]$ par l'idéal I des relations polynomiales entre les α (i.e. I est l'ensemble des $P((X_\alpha)_{\alpha\in K})$ s'annulant si on pose $X_\alpha = \alpha$, pour tout α).

L'idéal I′ de $L[X_\alpha,\ \alpha \in K]$, engendré par l'image de I par ι (on applique ι aux coefficients des polynômes) ne contient pas 1 : si $1 = \sum_\alpha Q_\alpha \iota(P_\alpha)$, où la somme est finie, $Q_\alpha \in L[X_\alpha,\ \alpha \in K]$ et $P_\alpha \in I$, on choisit une base de L sur $\iota(F)$ contenant 1 (cela demande l'axiome du choix), et on écrit les coefficients des Q_α dans cette base ; en ne gardant que la composante de l'élément 1 de la base, cela nous fournit une relation $1 = \sum_\alpha R_\alpha \iota(P_\alpha)$, où les coefficients des R_α sont tous dans $\iota(F)$; on en déduit une relation $1 = \sum_\alpha \iota^{-1}(R_\alpha)P_\alpha$ dans $F[X_\alpha,\ \alpha \in K]$, ce qui est absurde car I ne contient pas 1.

On peut inclure I′ dans un idéal maximal $\mathfrak{m}$, et $L[X_\alpha,\ \alpha \in K]/\mathfrak{m}$ est une extension algébrique de L (elle est engendrée par les X_α, et on a $\iota(P_\alpha)(X_\alpha) = 0$, si $P_\alpha \in F[X]$ est le polynôme minimal de α) ; il s'ensuit que l'injection de L dans $L[X_\alpha,\ \alpha \in K]/\mathfrak{m}$ est un isomorphisme puisque L est algébriquement clos. Le plongement $\iota : K \to L$ cherché s'obtient alors en composant l'application naturelle $K \cong F[X_\alpha,\ \alpha \in K]/I \to L[X_\alpha,\ \alpha \in K]/I'$ avec celle de $L[X_\alpha,\ \alpha \in K]/I'$ dans $L[X_\alpha,\ \alpha \in K]/\mathfrak{m}$ puis avec l'inverse de l'isomorphisme $L[X_\alpha,\ \alpha \in K]/\mathfrak{m} \cong L$ induit par l'injection de L dans $L[X_\alpha,\ \alpha \in K]/\mathfrak{m}$.

• Si K et K′ sont deux clôtures algébriques de F, il existe un isomorphisme de corps de K sur K′ induisant l'identité sur F ; autrement dit, une clôture algébrique d'un corps est unique à isomorphisme près [71].

Le point précédent fournit une injection ι de K dans K′ ; notons L l'image de K par ι de telle sorte que L est une clôture algébrique de F contenue dans K′. Soit $\alpha \in K'$. Comme α est algébrique sur F, il l'est a fortiori sur L, et donc $\alpha \in L$ puisque L est algébriquement clos. On en déduit que $L = K'$ et donc que ι est surjective ce qui permet de conclure.

• Si $\overline{F}$ est une clôture algébrique de F, et si $\alpha, \beta \in \overline{F}$ sont conjugués sur F, il existe un isomorphisme de $\overline{F}$ fixant F et envoyant α sur β.

70. Quotienter $K[X_P,\ \deg P \geqslant 1]$ par l'idéal engendré par les $P(X_P)$ revient à rajouter une racine de chaque polynôme non constant. L'anneau ainsi obtenu n'est pas un corps car les racines ainsi rajoutées n'ont aucune cohérence, et c'est le passage au quotient par un idéal maximal qui restaure cette cohérence.

71. Il est toutefois dangereux de parler de « la » clôture algébrique de F.

Soit $P \in F[X]$ le polynôme minimal de α ; c'est aussi celui de β puisque α et β sont conjugués. Les deux extensions $F(\alpha)$ et $F(\beta)$ de F étant isomorphe à $F[X]/P$, on dispose d'un isomorphisme ι de $F(\alpha)$ sur $F(\beta)$ induisant l'identité sur F et envoyant α sur β. Comme $\overline{F}$ est algébrique sur $F(\alpha)$ et est algébriquement clos, on peut prolonger ι en un plongement de $\overline{F}$ dans $\overline{F}$, et la démonstration du point précédent montre que ce plongement est un isomorphisme, ce qui permet de conclure.

9. Systèmes d'équations

Beaucoup de questions se ramènent à chercher les solutions simultanées de plusieurs équations en plusieurs variables. Dans ce §, on explique comment l'algèbre linéaire développée dans les § précédents permet de résoudre ce genre de problème dans le cas de systèmes d'équations linéaires ou polynomiales.

9.1. Systèmes linéaires

9.1.1. *Théorie générale*

Un système de n équations linéaires à m inconnues $\sum_{j=1}^{m} a_{i,j}x_j = 0$ pour $1 \leqslant i \leqslant n$ peut s'encoder sous la forme $AX = 0$ avec $A = (a_{i,j}) \in \mathbf{M}_{n\times m}(K)$ et $X = {}^t(x_1, \dots, x_n) \in \mathbf{M}_{m\times 1}(K) = K^m$; autrement dit, on est en train de calculer le noyau de $u_A : K^m \to K^n$. On définit le *rang du système* comme le rang de la matrice A.

• Si $A \in \mathbf{M}_{n\times m}(K)$ est de rang r, l'ensemble des solutions du système $AX = 0$ est un sous-espace vectoriel de dimension $m - r$ de K^m.

On a $\dim(\operatorname{Ker} u_A) + \dim(\operatorname{Im} u_A) = m$. Comme $\dim(\operatorname{Im} u_A) = \operatorname{rg} u_A = \operatorname{rg} A = r$, on obtient $\dim(\operatorname{Ker} u_A) = m - r$, ce qui permet de conclure.

Il arrive souvent que les équations qui nous intéressent comportent un second membre (i.e. soient de la forme $\sum_{j=1}^{m} a_{i,j}x_j = y_i$) auquel cas on est ramené à une équation du type $AX = Y$ avec $Y = {}^t(y_1, \dots, y_n)$.

• Si $A \in \mathbf{M}_{n\times m}(K)$ est de rang r, alors :

◇ le système $AX = Y$ n'a pas de solution si Y n'est pas dans l'image de u_A ;

◇ si Y est dans l'image de u_A et si $X_0 \in K^m$ vérifie $u_A(X_0) = Y$ et donc $AX_0 = Y$, l'ensemble des solutions du système $AX = Y$ est $X_0 + \operatorname{Ker} u_A = \{X_0 + X,\ AX = 0\}$; autrement dit, on obtient les solutions de $AX = Y$ en rajoutant à une solution particulière X_0 une solution de l'équation sans second membre $AX = 0$.

Le premier cas est la définition de $\operatorname{Im} u_A$ puisque $u_A(X) = AX$. Dans le second, il suffit de remarquer que $A(X - X_0) = 0$ si $AX = AX_0 = Y$.

• Un cas particulier intéressant est celui où $n = m$ (autant d'inconnues que d'équations) et le rang du système est n (ce qui équivaut à $\det A \neq 0$ ou à ce que l'équation $AX = 0$ a 0 comme unique solution) ; un tel système est dit *de Cramer*. Si $Y = {}^t(y_1, \dots, y_n) \in K^n$, l'équation $AX = Y$ a une unique solution $X = {}^t(x_1, \dots, x_n) \in K^n$, et on a $x_k = \frac{\det A_k}{\det A}$,

où A_k est la matrice obtenue en remplaçant la k-ième colonne de A par Y (*formules de Cramer*, 1750).

Si le rang du système est n, cela signifie que celui de u_A est n, et que u_A est surjective et donc bijective. Autrement dit l'équation $u_A(X) = Y$, équivalente à $AX = Y$, a une et une seule solution dans K^n. Cette solution est $X = A^{-1}Y$, et on pourrait déduire les formules de Cramer de la formule $A^{-1} = \frac{1}{\det A}{}^t\mathrm{cof}(A)$, mais nous allons procéder autrement.

Notons $X_1, \dots, X_n$ les colonnes de A. Le système $AX = 0$ peut encore s'écrire sous la forme $\sum_{i=1}^n x_i X_i = Y$, et comme $\det A = \det(X_1, \dots, X_n) \neq 0$, les formules de Cramer sont équivalentes à l'identité $\sum_{i=1}^n \det(X_1, \dots, X_{i-1}, Y, X_{i+1}, X_n)X_i = \det(X_1, \dots, X_n)Y$. On peut réécrire cette identité à vérifier de manière plus symétrique en posant $Y = X_0$, en ordonnant les X_i dans l'ordre croissant des indices dans les déterminants (cela demande de faire passer Y de la i-ième place à la première, et donc de faire un i-cycle sur les i premiers vecteurs, ce qui multiplie le déterminant correspondant par $(-1)^{i-1}$), et en faisant tout passer au second membre. On obtient alors $0 = \sum_{i=0}^n (-1)^i \det(X_0, \dots, \hat{X}_i, \dots X_n)X_i$. Si on regarde la j-ième coordonnée du second membre, on reconnait le développement par rapport à la ligne d'ordre 0 du déterminant $(n+1) \times (n+1)$ (les lignes et les colonnes sont numérotées de 0 à n) dont la i-ième colonne est formée de X_i (pour les lignes de 1 à n), et de la j-ième coordonnée de X_i (sur la ligne d'ordre 0) ; les lignes d'ordre 0 et j étant égales, le déterminant est nul. On en déduit que le second membre a toutes ses coordonnées nulles, ce qui permet de conclure.

• Si $A \in \mathbf{M}_{n\times m}(K)$ est de rang r, on peut utiliser les formules de Cramer pour décrire les solutions du système $AX = 0$: il suffit d'isoler un mineur d'ordre r non nul et de faire passer dans le second membre les inconnues n'intervenant pas dans le mineur pour se retrouver avec un système de Cramer avec second membre de r équations à r inconnues.

Exercice 9.1. — Montrer que les $x \mapsto \log(x + a)$, pour $a > 0$ forment une famille libre dans les fonctions de $\mathbf{R}_+$ dans $\mathbf{C}$. (Dériver.)

Exercice 9.2. — Soit $(x_{i,j})_{0\leqslant i,j\leqslant n+1}$ un carré de nombres complexes. On dit que ce carré vérifie la *propriété de la moyenne* si tout nombre intérieur est la moyenne des 8 nombres qui l'entourent (i.e. si $x_{i,j} = \frac{1}{8}\sum_{(a,b)\in\{-1,0,1\}^2-\{(0,0)\}} x_{i+a,j+b}$, si $1 \leqslant i, j \leqslant n$).

(i) Montrer que si $(x_{i,j})$ vérifie la propriété de la moyenne, alors $|x_{i,j}|$ est atteint sur le bord du carré (principe du maximum).

(ii) Montrer que si $(x_{i,j})$ vérifie la propriété de la moyenne, et si $x_{i,j} = 0$ sur le bord, alors $x_{i,j} = 0$ pour tous i, j.

(iii) En déduire que pour tout choix de valeurs sur le bord, il existe un unique carré vérifiant la propriété de la moyenne avec ces valeurs au bord.

9.1.2. *La méthode du pivot de Gauss*

Les formules de Cramer sont très utiles pour l'étude théorique des solutions d'un système linéaire ; par exemple pour comprendre comment ces solutions varient si on fait dépendre les coefficients des équations de paramètres. En pratique, si on cherche à résoudre un système linéaire, on utilise en général la *méthode du pivot de Gauss*, ce qui est un nom

un peu ronflant pour un procédé aussi évident... Il s'agit d'un algorithme qui fonctionne [72] comme suit (on cherche à résoudre le système $\mathrm{A\,X} = \mathrm{Y}$, avec $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_{n\times m}(\mathrm{K})$ et $\mathrm{Y} = {}^{\mathrm{t}}(y_1, \dots, y_n) \in \mathrm{K}^n$ donné) :

◇ Si $a_{i,j} = 0$ pour tous i, j, et si $y_i = 0$ pour tout i, alors tout $\mathrm{X} \in \mathrm{K}^m$ est solution, tandis que si un des y_i est non nul, il n'y a pas de solution.

◇ Si les $a_{i,j}$ ne sont pas tous nuls, on choisit un a_{i_1,j_1} qui ne l'est pas (c'est le pivot) ; l'équation $\sum_{j=1}^{m} a_{i_1,j}x_j = y_{i_1}$ permet d'exprimer x_{j_1} en fonction des autres x_j : en effet, on a $x_{j_1} = \frac{1}{a_{i_1,j_1}}\big(y_{i_1} - \sum_{j\neq j_1} a_{i_1,j}x_j\big)$. On peut alors reporter la valeur de x_{j_1} dans les autres équations et obtenir, en ne considérant que ces équations, un système de $n-1$ équations en $m-1$ variables (puisque x_{i_1} a disparu), auquel on peut appliquer ce qui précède.

Au bout de r étapes, avec $r \leqslant \inf(n, m)$, on se retrouve avec un système de la forme suivante :

$$x_{j_1} = \ell_1(\mathrm{Y}) + \sum_{j\neq j_1} \alpha_{i_1,j}x_j,\ \ x_{j_2} = \ell_2(\mathrm{Y}) + \sum_{j\neq j_1,j_2} \alpha_{i_2,j}x_j, \cdots, x_{j_r} = \ell_r(\mathrm{Y}) + \sum_{j\neq j_1,\dots,j_r} \alpha_{i_r,j}x_j$$
$$0 = \ell_{r+1}(\mathrm{Y}) = \cdots = \ell_n(\mathrm{Y})$$

où les $\alpha_{i,j}$ sont des éléments de K, les ℓ_i sont des formes linéaires sur K^n (si $r = n$, la seconde ligne n'apparaît pas). Soit $\mathrm{J} = \{1, \dots, m\} - \{j_1, \dots, j_r\}$; on a $|\mathrm{J}| = m - r$. Il est alors apparent sur la forme de ce système qu'il n'y a pas de solution si $\ell_i(\mathrm{Y}) \neq 0$ pour au moins un $i \in \{r+1, \dots, n\}$ et que si $\ell_i(\mathrm{Y}) = 0$ pour tout $i \in \{r+1, \dots, n\}$ (condition vide si $r = n$), alors pour tout $(x_j)_{j\in\mathrm{J}} \in \mathrm{K}^{\mathrm{J}}$, le système a une unique solution : la dernière équation fournit x_{j_r} ; en reportant cette valeur de x_{j_r} dans la précédente, on en déduit $x_{j_{r-1}}$, etc.

En posant $x_j = 0$ pour tout $j \in \mathrm{J}$, cela nous fournit une solution particulière X_0 de l'équation $\mathrm{A\,X} = \mathrm{Y}$. On en obtient $m-r$ autres, X_k pour $k \in \mathrm{J}$, en posant $x_k = 1$ et $x_j = 0$ si $j \in \mathrm{J}-\{k\}$. Les $\mathrm{X}_k - \mathrm{X}_0$, pour $k \in \mathrm{J}$, sont des solutions de l'équation $\mathrm{A\,X} = 0$ qui forment une base de l'espace vectoriel $\operatorname{Ker} u_{\mathrm{A}}$. L'application $(x_k)_{k\in\mathrm{J}} \mapsto \mathrm{X}_0 + \sum_{k\in\mathrm{J}} x_k(\mathrm{X}_k - \mathrm{X}_0)$ est alors une bijection de K^{J} sur l'ensemble des solutions du système $\mathrm{A\,X} = \mathrm{Y}$, ce qui en fournit une description paramétrée.

72. Les gens ne se sont bien sûr pas privés de programmer cet algorithme, ce qui fait que la résolution de systèmes linéaires explicites assez gros (à partir de 5×5, une résolution à la main commence à devenir vraiment fastidieuse) peut être confiée à un ordinateur sans trop de risques. Notons que la résolution d'un système numérique demande de faire attention aux choix des pivots : il est assez périlleux de diviser par quelque chose de trop petit. Par ailleurs, certains sont amenés à résoudre des systèmes vraiment gigantesques et je ne sais pas comment ils font pour s'assurer qu'il n'y a pas d'erreur dans la saisie des données (par exemple pour un système 1000×1000, cela demande rentrer un million de données, ce qui demande un temps non négligeable et est incroyablement ennuyeux, et donc propice aux erreurs d'inattention...).

9.1.3. *Méthode du pivot et opérations sur les matrices*

La méthode du pivot ne permet pas uniquement de résoudre des systèmes linéaires ; on peut aussi l'utiliser pour démontrer de vrais résultats.

Si $\sigma \in \mathrm{S}_n$, on note P_σ la matrice $n \times n$ de l'endomorphisme u_σ de K^n envoyant e_i sur $e_{\sigma(i)}$, si $1 \leqslant i \leqslant n$. Cette matrice a exactement un 1 par ligne et par colonne, et tous ses autres coefficients sont nuls ; une telle matrice est dite *de permutation*.

• $\sigma \mapsto \mathrm{P}_\sigma$ est un morphisme de groupes de S_n dans $\mathbf{GL}_n(\mathrm{K})$.

C'est une traduction du (i) de l'ex. 3.15.

• Si $\mathrm{A} \in \mathbf{M}_{n\times m}(\mathrm{K})$, multiplier A à droite (resp. à gauche) par une matrice de permutation P_σ avec $\sigma \in \mathrm{S}_m$ (resp. $\sigma \in \mathrm{S}_n$) revient à permuter les colonnes (resp. les lignes) de A ; de manière précise, la j-ième colonne de AP_σ est la $\sigma(j)$-ième colonne de A et la i-ième ligne de $\mathrm{P}_\sigma\mathrm{A}$ est la $\sigma^{-1}(i)$-ième colonne de A.

On a $u_\mathrm{A} \circ u_\sigma(e_j) = u_\mathrm{A}(e_{\sigma(j)})$; on en déduit l'énoncé concernant les colonnes de AP_σ. De même, $u_\sigma \circ u_\mathrm{A}(e_j) = u_\sigma\big(\sum_{i=1}^n a_{i,j}e_i\big) = \sum_{i=1}^n a_{i,j}e_{\sigma(i)} = \sum_{i=1}^n a_{\sigma^{-1}(i),j}e_i$; on en déduit l'énoncé concernant les lignes de $\mathrm{P}_\sigma\mathrm{A}$.

Soit $\mathrm{I}_{n,m}(r)$ la matrice $n \times m$ dont tous les coefficients sont nuls sauf les r premiers coefficients diagonaux qui valent 1.

• Si $\mathrm{A} \in \mathbf{M}_{n\times m}(\mathrm{K})$ est de rang r, il existe des matrices de permutations $\mathrm{P} \in \mathbf{GL}_n(\mathrm{K})$ et $\mathrm{P}' \in \mathbf{GL}_m(\mathrm{K})$, et des matrices $\mathrm{T} \in \mathbf{GL}_n(\mathrm{K})$, triangulaire inférieure, et $\mathrm{T}' \in \mathbf{GL}_m(\mathrm{K})$, triangulaire supérieure, telles que $\mathrm{TPAP}'\mathrm{T}' = \mathrm{I}_{n,m}(r)$.

Reprenons la méthode du pivot. Quitte à faire des permutations des inconnues (ce qui revient à permuter les colonnes de A et donc à multiplier A à droite par une matrice de permutation P') et des équations (ce qui revient à permuter les lignes de A et donc à multiplier A à gauche par une matrice de permutation P), on peut supposer que $i_1 = j_1 = 1, \dots, i_r = j_r = r$ (ce qui implique en particulier que $a_{1,1} \neq 0$ puisqu'on peut le prendre comme pivot). Reporter la valeur de x_1 dans les équations suivantes revient alors à multiplier A à gauche par la matrice

$$\mathrm{T}_1 = \begin{pmatrix} \frac{1}{a_{1,1}} & 0 & \cdots & 0 \\ \frac{-a_{2,1}}{a_{1,1}} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \frac{-a_{n,1}}{a_{1,1}} & 0 & \cdots & 1 \end{pmatrix} \text{ pour obtenir } \mathrm{A}' = \mathrm{T}_1\mathrm{A} = \begin{pmatrix} 1 & a'_{1,2} & \cdots & a'_{1,m} \\ 0 & a'_{2,2} & \cdots & a'_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{n,2} & \cdots & a'_{n,m} \end{pmatrix}$$

On multiplie alors A' à gauche par la matrice

$$\mathrm{T}_2 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \frac{1}{a'_{2,2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{-a'_{n,2}}{a'_{2,2}} & \cdots & 1 \end{pmatrix} \text{ pour obtenir } \mathrm{A}'' = \mathrm{T}_2\mathrm{T}_1\mathrm{A} = \begin{pmatrix} 1 & a'_{1,2} & a'_{1,3} & \cdots & a'_{1,m} \\ 0 & 1 & a''_{2,3} & \cdots & a''_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a''_{n,3} & \cdots & a'_{n,m} \end{pmatrix}$$

Au bout de r étape, on aboutit à $\mathrm{A}^{(r)} = \mathrm{TA}$, où $\mathrm{A}^{(r)}$ a tous ses coefficients nuls en-dessous de la diagonale ou en-dessous de la r-ième ligne, et ses coefficients diagonaux $a^{(r)}_{1,1}, \dots, a^{(r)}_{r,r}$ sont égaux à 1, et T est triangulaire inférieure inversible car $\mathrm{T} = \mathrm{T}_r \cdots \mathrm{T}_1$ et T_j est triangulaire

inférieure inversible (ses coefficients en dehors de la j-ième colonne sont des 1 sur la diagonale et des 0 ailleurs, et le coefficient diagonal de la j-ième ligne est l'inverse du j-ième pivot, et donc est inversible). On peut alors faire subir le même traitement à la transposée de $\mathrm{A}^{(r)}$ en remarquant que l'on peut prendre les coefficients diagonaux comme pivots successifs, ce qui permet de trouver une matrice triangulaire inférieure inversible T_0 telle que $\mathrm{T}_0{}^{\mathrm{t}}\mathrm{A}^{(r)} = \mathrm{I}_{m,n}(r)$. Alors $\mathrm{A}^{(r)}{}^{\mathrm{t}}\mathrm{T}_0 = \mathrm{I}_{n,m}(r)$ et $\mathrm{TA}^{\mathrm{t}}\mathrm{T}_0 = \mathrm{I}_{n,m}(r)$, et comme $\mathrm{T}' = {}^{\mathrm{t}}\mathrm{T}_0$ est triangulaire supérieure inversible, cela permet de conclure.

Exercice 9.3. — (i) Montrer que $\mathrm{rg}(\mathrm{UAV}) = \mathrm{rg}(\mathrm{A})$, si $\mathrm{A} \in \mathbf{M}_{n\times m}(\mathrm{K})$, si $\mathrm{U} \in \mathbf{GL}_n(\mathrm{K})$ et si $\mathrm{V} \in \mathbf{GL}_m(\mathrm{K})$.

(ii) Soit $\mathrm{G} = \mathbf{GL}_n(\mathrm{K}) \times \mathbf{GL}_m(\mathrm{K})$. Montrer que $((\mathrm{U},\mathrm{V}),\mathrm{M}) \mapsto (\mathrm{U},\mathrm{V})\cdot\mathrm{M} = \mathrm{UMV}^{-1}$ définit une action de G sur $\mathbf{M}_{n\times m}(\mathrm{K})$.

(iii) Combien cette action a-t-elle d'orbites ?

9.2. Systèmes d'équations polynomiales

Soient $\mathrm{P}_1,\ldots,\mathrm{P}_n \in \mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_m]$. Si L est un corps contenant K, notons V(L) l'ensemble des solutions dans L^m du système $\mathrm{P}_1(x) = \cdots = \mathrm{P}_n(x) = 0$.

Si $\mathrm{P}_1,\ldots,\mathrm{P}_n$ sont de degré 1, le système ainsi obtenu est un système linéaire avec second membre, et la méthode du pivot nous fournit une description de V(K) : si V(K) est non vide, il existe $d \in \{0,1,\ldots,m\}$ tel que, quitte à permuter les variables, la projection de K^m sur K^d induise une surjection de V(K) sur K^d et l'image inverse de $x \in \mathrm{K}^d$ consiste en exactement un point qui peut se calculer à partir de x en résolvant successivement $m-d$ équations en 1 variable, de degré 1.

Dans le cas général, la théorie de l'élimination fournit, *si* K *est algébriquement clos*, une description analogue de V(K). Pour que le résultat soit plus esthétique, il faut se permettre un changement linéaire de variable $\mathrm{X}_i = \sum_{j=1}^m a_{i,j}\mathrm{Y}_j$ avec $\mathrm{A} = (a_{i,j}) \in \mathbf{GL}_m(\mathrm{K})$, ce qui est un peu plus général que de permuter les coordonnées, mais ne présente pas vraiment d'inconvénient pour décrire les solutions du système initial, étant donné qu'on les retrouve, à partir des solutions du système modifié, en résolvant le système de Cramer exprimant les X_i en fonction des Y_j. La description de l'ensemble des solutions est alors la suivante [73] : si V(K) est non vide, il existe $d \in \{0,1,\ldots,m\}$ tel que, quitte à faire un changement linéaire de variables, la projection de K^m sur K^d induit une surjection de V(K) sur K^d et l'image inverse de $x \in \mathrm{K}^d$ est finie, et peut se calculer à partir de x en résolvant successivement $m-d$ équations polynomiales en 1 variable dont les degrés ne dépendent pas de x.

73. Cette description est relativement satisfaisante d'un point de vue ensembliste mais ne dit rien de la géométrie des solutions ; ceci fait l'objet de la géométrie algébrique. L'étude des solutions d'un tel système sur un corps K non algébriquement clos (par exemple $\mathbf{Q}$ ou un corps fini) est nettement plus délicate et fait l'objet de la géométrie arithmétique ; de manière assez surprenante la géométrie des solutions du même système sur un corps algébriquement clos contenant K (par exemple $\mathbf{C}$ si $\mathrm{K} = \mathbf{Q}$) a une très forte influence (pas encore complètement comprise) sur la taille de l'ensemble des solutions sur K.

9.2.1. *Résultant de deux polynômes, discriminant*

On note $\mathbf{Z}[\mathbf{A},\mathbf{B}]$ l'anneau des polynômes à coefficients dans $\mathbf{Z}$ en les indéterminées $A_0,\dots,A_n,B_0,\dots,B_m$. On note $P_{\mathbf{A}}$, $Q_{\mathbf{B}}$ les éléments $A_nX^n+\cdots+A_n$ et $B_mX^m+\cdots+B_0$ de $\mathbf{Z}[\mathbf{A},\mathbf{B},X]$ (et donc $P_{\mathbf{A}}$, $Q_{\mathbf{B}}$ sont les *polynômes universels* de degrés $\leqslant n$ et $\leqslant m$).

On note $\mathrm{Sylv}_{n,m}$ la matrice (dite *de Sylvester*) de $P_{\mathbf{A}}$ et $Q_{\mathbf{B}}$ dont les colonnes sont les coordonnées de $X^{m-1}P_{\mathbf{A}},\dots,P_{\mathbf{A}},X^{n-1}Q_{\mathbf{B}},\dots,Q_{\mathbf{B}}$ dans la base $X^{n+m-1},\dots,1$: par exemple, si $n=3$ et $m=2$, on obtient la matrice

$$\begin{pmatrix} A_3 & 0 & B_2 & 0 & 0\\ A_2 & A_3 & B_1 & B_2 & 0\\ A_1 & A_2 & B_0 & B_1 & B_2\\ A_0 & A_1 & 0 & B_0 & B_1\\ 0 & A_0 & 0 & 0 & B_0 \end{pmatrix}.$$

On note $\mathrm{Res}_{n,m}\in\mathbf{Z}[\mathbf{A},\mathbf{B}]$ le déterminant de la matrice de Sylvester $\mathrm{Sylv}_{n,m}$; c'est le *résultant* des polynômes universels $P_{\mathbf{A}}$ et $Q_{\mathbf{B}}$.

• Il existe $U,V\in\mathbf{Z}[\mathbf{A},\mathbf{B},X]$ tels que $\mathrm{Res}_{n,m}=UP_{\mathbf{A}}+VQ_{\mathbf{B}}$.

On ajoute à la dernière ligne du déterminant la combinaison linéaire des autres où le coefficient de la i-ième ligne est X^{n+m-i}. Ceci ne change pas la valeur du déterminant, et la dernière ligne devient $(X^{m-1}P_{\mathbf{A}},\dots,P_{\mathbf{A}},X^{n-1}Q_{\mathbf{B}},\dots,Q_{\mathbf{B}})$. Un développement du déterminant par rapport à la dernière ligne fournit l'identité cherchée.

Si Λ est un anneau, et si $P=a_nX^n+\cdots+a_n$ et $Q=b_mX^m+\cdots+b_0$ sont des éléments de $\Lambda[X]$, on définit le *résultant* $\mathrm{Res}_{n,m}(P,Q)\in\Lambda$ de P et Q comme la valeur en $(a_0,\dots,a_n,b_0,\dots,b_m)$ de $\mathrm{Res}_{n,m}$; c'est donc aussi le déterminant de la matrice de Sylvester de P et Q (obtenue en évaluant $\mathrm{Sylv}_{n,m}$ en $(a_0,\dots,a_n,b_0,\dots,b_m)$). Si $P,Q\in K[X]$ sont de degrés n et m, le résultant de P et Q est $\mathrm{Res}_{n,m}(P,Q)$ (i.e. les entiers n et m sont implicitement les degrés des polynômes P et Q s'ils ne sont pas explicitement mentionnés).

• Il existe $U,V\in\Lambda[X]$ tels que $\mathrm{Res}_{n,m}(P,Q)=UP+VQ$.

Il suffit de spécialiser la relation $\mathrm{Res}_{n,m}=UP_{\mathbf{A}}+VQ_{\mathbf{B}}$ en $(a_0,\dots,a_n,b_0,\dots,b_m)$.

On suppose dans la suite que l'anneau Λ est un corps K. Si $a_n=b_m=0$, la première ligne de la matrice de Sylvester est nulle et donc le résultant est nul. On suppose donc $a_n\neq0$ ou $b_m\neq0$ dans ce qui suit.

• Les conditions suivantes sont équivalentes :
- ◇ $\mathrm{Res}_{n,m}(P,Q)=0$,
- ◇ $\mathrm{pgcd}(P,Q)\neq1$,
- ◇ il existe un corps contenant K dans lequel P et Q ont une racine commune,
- ◇ P et Q ont une racine commune dans tout corps algébriquement clos contenant K.

Posons $D=\mathrm{pgcd}(P,Q)$. Si $D\neq1$, et si L est un corps algébriquement clos contenant K, alors D se factorise complètement dans L, et toute racine de D est une racine commune de P et Q ; la seconde condition implique donc la quatrième, et celle-ci implique la troisième de manière évidente. Maintenant, si α est une racine commune de P et Q dans un corps L

contenant K, alors α est algébrique sur K et le polynôme minimal de α divise P et Q, ce qui prouve que la troisième condition implique la seconde et donc que les trois dernières conditions sont équivalentes.

La matrice de Sylvester est la matrice de $(U, V) \mapsto UP + VQ$ dans les bases canoniques de $K[X]^{(m-1)} \oplus K[X]^{(n-1)}$ et $K[X]^{(n+m-1)}$. Si $D \neq 1$, on peut factoriser P et Q sous la forme $P = DP_1$ et $Q = DQ_1$, et alors $P_1 \in K[X]^{(n-1)}$ et $Q_1 \in K[X]^{(m-1)}$ et $(Q_1, -P_1)$ est dans le noyau de $(U, V) \mapsto PU + QV$, ce qui prouve que $\mathrm{Res}_{n,m}(P, Q) = 0$. Ceci montre que la seconde condition implique la première. Réciproquement, si P et Q sont premiers entre eux, alors $PU + QV = 0$ implique que P divise V et Q divise U, et comme $a_n \neq 0$ ou $b_m \neq 0$, cela implique $U = 0$ ou $V = 0$ (et donc $U = V = 0$), puisque $\deg U \leqslant m-1$, $\deg V \leqslant n-1$. Il s'ensuit que $(U, V) \mapsto PU + QV$ est injective et donc bijective, et que $\mathrm{Res}_{n,m}(P, Q) \neq 0$. La première condition implique donc la seconde, ce qui permet de conclure.

• Si $a_n \neq 0$ et $b_m \neq 0$, et si L est une extension de K dans laquelle P et Q se factorisent complètement sous la forme $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$ et $Q = b_m \prod_{j=1}^{m}(X - \beta_j)$, alors

$$\mathrm{Res}_{n,m}(P, Q) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} Q(\alpha_i) = (-1)^{pq} b_m^n \prod_{j=1}^{m} P(\beta_j).$$

On a $\mathrm{Res}_{n,m}(P, Q) = \det_{X^{n+m-1},\dots,1}(X^{m-1}P, \dots, P, X^{n-1}Q, \dots, Q)$. On peut écrire X^iQ sous la forme $PA_i + Q_i$, avec $\deg Q_i \leqslant n-1$ et $\deg A_i = i + m - n \leqslant m-1$, si $i + m - n \geqslant 0$ (dans le cas contraire, $A_i = 0$). Donc PA_i est une combinaison linéaire de $X^{m-1}P, \dots, P$, et le déterminant ne change pas si on retranche PA_i à X^iQ, ce qui revient à remplacer X^iQ par Q_i. La matrice obtenue est alors triangulaire par blocs $\left(\begin{smallmatrix} A_1 & 0 \\ A_2 & B \end{smallmatrix}\right)$, avec $A_1 \in \mathbf{M}_m(K)$, $A_2 \in \mathbf{M}_{n\times m}(K)$, $B \in \mathbf{M}_n(K)$; de plus A_1 est triangulaire inférieure avec des a_n sur la diagonale et on obtient $\mathrm{Res}_{n,m}(P, Q) = a_n^m \det B$.

Maintenant, B est la matrice de la multiplication par Q sur K[X]/P, dans la base $X^{n-1}, \dots, 1$. Or le polynôme caractéristique de la muliplication par X sur K[X]/P est P (ex. 10.4) ; il s'ensuit que les valeurs propres de la multiplication par X sont $\alpha_1, \dots, \alpha_n$, et donc celles de la multiplication par Q sont $Q(\alpha_1), \dots, Q(\alpha_n)$. Comme le déterminant est le produit des valeurs propres (alinéa 10.1.6), on obtient $\det B = \prod_{i=1}^{n} Q(\alpha_i)$. On en déduit les deux premières égalités. La dernière s'obtient en échangeant les rôles de P et Q.

• Soit $\Delta_n \in \mathbf{Z}[\mathbf{A}]$ défini par $\Delta_n = (-1)^{n(n-1)/2}\mathrm{Res}_{n,n-1}(P_{\mathbf{A}}, P'_{\mathbf{A}})$; c'est le *discriminant* du polynôme universel de degré n. Si Λ est un anneau et $P = a_nX^n + \cdots + a_0 \in \Lambda[X]$, on définit le *discriminant* $\Delta(P)$ de Λ comme la valeur de Δ_n en $a_0, \dots, a_n$.

• Si K est un corps, si L est une extension de K dans laquelle $P = X^n + \cdots + a_0 \in K[X]$ se factorise sous la forme $\prod_{i=1}^{n}(X - \alpha_i)$, alors $\Delta(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, et $\Delta(P) = 0$ si et seulement si P a une racine double.

On a $\mathrm{Res}_{n,m}(P, P') = \prod_{i=1}^{n} P'(\alpha_i) = \prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i - \alpha_j)$. La formule $\Delta(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ s'en déduit en regroupant les termes (i, j) et (j, i). Le reste est alors immédiat.

9.2.2. *Théorie de l'élimination*

Soit K un corps infini. Soient $P_1, \dots, P_n \in K[X_1, \dots, X_m]$. Si L est un corps contenant K et si $A = (a_{i,j}) \in \mathbf{GL}_m(K)$, on note $V_A(L)$ l'ensemble des solutions dans L^m du système $P_{1,A}(y) = \cdots = P_{n,A}(y) = 0$, où $P_{1,A}, \dots, P_{n,A} \in K[Y_1, \dots, Y_m]$ sont les polynômes

obtenus à partir de $P_1, \dots, P_n$ via le changement linéaire de variable $X = AY$ (i.e. on a $X_i = \sum_{j=1}^{m} a_{i,j} Y_j$, si $1 \leqslant i \leqslant m$).

On dit qu'un système polynomial est *triangulaire de dimension d* s'il est de la forme $Q_1(x) = \cdots = Q_{m-d}(x) = 0$, avec $Q_i \in K[X_1, \dots, X_{d+i}]$, unitaire en X_{d+i}. Un tel système se résoud sans problème (à condition de savoir résoudre les équations en une variable) : si on fixe $(x_1, \dots, x_d)$, les autres x_i s'obtiennent successivement en résolvant une équation polynomiale en une variable (en particulier, il n'y a qu'un nombre fini de solutions pour $x_{d+1}, \dots, x_m$ si $x_1, \dots, x_d$ sont fixés).

Théorème 9.4. — *On est dans l'un des deux cas (exclusifs) suivants :*

◇ $V(L) = \varnothing$ *pour tout corps algébriquement clos* L *contenant* K.

◇ *Il existe un changement de variable* $X = AY$, *un entier* $d \in \{0, \dots, m\}$, *et un système triangulaire* $Q_1(y) = \cdots Q_{m-d}(y) = 0$ *de dimension d tels que, si* L *est un corps algébriquement clos contenant* K, $V_A(L)$ *soit inclus dans les solutions de ce système et se surjecte sur* L^d *; si* $c_1, \dots, c_d \in L^d$ *l'ensemble* V_c *des* $y = (y_1, \dots, y_m) \in V_A(L)$ *vérifiant* $y_1 = c_1, \dots, y_d = c_d$ *est donc non vide et fini.*

La démonstration se fait par récurrence sur m. L'idée est la même que pour la méthode du pivot de Gauss. On a besoin d'une équation dans laquelle X_m apparaît, et on l'utilise pour éliminer X_m des autres équations, ce qui se fait en utilisant les résultants. Pour que le résultat soit le plus sympathique possible, il faut que le polynôme utilisé soit unitaire en X_m : dans le cas d'un système linéaire, il suffit de diviser l'équation correspondante par le coefficient de X_m après avoir permuté les variables, dans le cas général, cela peut demander d'effectuer un changement linéaire de variable.

Pour $m = 1$, il y a deux cas suivant que tous les P_i sont nuls (auquel cas on est dans le second cas de l'alternative du théorème avec $d = 1$ et pas de Q_i puisque tout $x \in L$ est solution), ou que l'un d'entre eux ne l'est pas (auquel cas, l'idéal engendré par les P_i est principal, engendré par un polynôme unitaire Q, et les solutions du système sont les racines de Q ; si $Q = 1$, on est dans le premier cas de l'alternative du théorème, si $Q \neq 1$, on est dans le second cas avec $d = 0$ et $Q_1 = Q$).

Supposons maintenant $m \geqslant 2$. Si tous les P_i sont nuls, on est dans le second cas de l'alternative du théorème avec $d = m$, et pas de Q_i car tout $x \in L^m$ est solution. Dans le cas contraire, quitte à réordonner les P_i, on peut supposer que $P_1 \neq 0$. Si $\deg P_1 = 0$, alors P_1 est une constante et l'équation $P_1(x) = 0$ n'a de solution dans aucun corps L contenant K, et on est dans le premier cas de l'alternative du théorème. Si $\deg P_1 = k_1 \geqslant 1$, on peut, quitte à faire un changement linéaire de variable et à muliplier par un élément de K^*, supposer (cf. ex. 4.7) que P_1 est unitaire en X_m.

Pour condenser un peu les expressions, posons $X = (X_1, \dots, X_m)$ et $X' = (X_1, \dots, X_{m-1})$; on a donc $X = (X', X_m)$. Par ailleurs, L désigne un corps algébriquement clos contenant K dans tout ce qui suit. On définit $P \in K[T, X]$ par $P = P_2 + TP_3 + \cdots + T^{n-2}P_n$, et on note R le résultant de P_1 et P par rapport à X_m ; on peut écrire R sous la forme $R_0 + R_1 T + \cdots$, où les R_i appartiennent à $K[X']$. Maintenant R appartient à l'idéal de $K[T, X]$ engendré par P et P_1 ; on a donc une relation du type $R = UP + VP_1$, où $U = U_0 + U_1 T + \cdots$ et $V = V_0 + V_1 T + \cdots$, et les U_i et les V_i sont des éléments de K[X]. En identifiant les puissances de T des deux cotés, on obtient $R_0 = U_0 P_2 + V_0 P_1$, $U_1 = U_0 P_3 + U_1 P_2 + V_1 P_1$, etc., ce qui montre que si

$x = (x', x_m) \in \mathrm{L}^m$ est une solution du système des P_i, alors x' est une solution du système des R_i.

Réciproquement, si $x' \in \mathrm{L}$ est une solution du système des R_i, alors, pour tout $t \in \mathrm{K}$, le résultant des polynômes $\mathrm{P}_1(x', \mathrm{X}_m)$ et $\mathrm{P}(t, x', \mathrm{X}_m)$ est nul, et comme le coefficient dominant de $\mathrm{P}_1(x', \mathrm{X}_m)$ ne l'est pas puisqu'on s'est arrangé pour qu'il vaille 1, cela implique que $\mathrm{P}_1(x', \mathrm{X}_m)$ et $\mathrm{P}(t, x', \mathrm{X}_m)$ ont un zéro commun dans L. Or les zéros de $\mathrm{P}_1(x', \mathrm{X}_m)$ sont en nombre fini et ne dépendent pas de t ; il en résulte que l'un d'entre eux a est racine de $\mathrm{P}(t, x', \mathrm{X}_m)$ pour une infinité de t, et donc que le polynôme $\mathrm{P}(\mathrm{T}, x', a)$ est identiquement nul puisqu'il a une infinité de zéros. Cela implique que $\mathrm{P}_2(x', a) = \cdots = \mathrm{P}_n(x', a)$, et comme $\mathrm{P}_1(x', a) = 0$, on vient de prouver l'équivalence des conditions suivante pour $x' \in \mathrm{L}^{m-1}$: « x' est solution du système des R_i » et « il existe $a \in \mathrm{L}$ tel que (x', a) soit solution du système des P_i ».

On a donc réussi à éliminer X_m et à construire un système polynomial en $\mathrm{X}' = (\mathrm{X}_1, \ldots, \mathrm{X}_{m-1})$ dont les solutions $\mathrm{V}'(\mathrm{L})$ sont exactement les projections des solutions du système initial. On peut alors appliquer l'hypothèse de récurrence à ce système. Quitte à faire un changement linéaire de variable $\mathrm{X}' = \mathrm{A}'\mathrm{Y}'$ (ce qui ne change pas X_m), on peut supposer que l'on est dans un des deux cas exclusifs suivants :

◇ Pour tout L, on a $\mathrm{V}'(\mathrm{L}) = \varnothing$, et donc $\mathrm{V}(\mathrm{L}) = \varnothing$, et on est dans le premier cas de l'alternative du théorème.

◇ Il existe un entier $d \in \{0, \ldots, m-1\}$ et un système $\mathrm{Q}_1(x) = \cdots = \mathrm{Q}_{m-1-d}(x) = 0$, triangulaire de dimension d tel que $\mathrm{V}'(\mathrm{L})$ soit inclus dans l'ensemble des solutions de ce système et se surjecte sur L^d, pour tout L. Alors le système $\mathrm{Q}_1(x) = \cdots = \mathrm{Q}_{m-1-d}(x) = \mathrm{P}_1(x) = 0$ est triangulaire de dimension d, et $\mathrm{V}(\mathrm{L})$ est inclus dans les solutions de ce système et se surjecte sur L^d d'après l'équivalence ci-dessus.

Ceci permet de conclure.

Corollaire 9.5. — (th. des zéros de Hilbert, 1893). *Si* $\mathrm{P}_1, \ldots, \mathrm{P}_n \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$, *et si le système* $\mathrm{P}_1(x) = \cdots = \mathrm{P}_n(x) = 0$ *n'a pas de solution dans une clôture algébrique de* K, *alors l'idéal de* $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ *engendré par* $\mathrm{P}_1, \ldots, \mathrm{P}_n$ *contient*[74] 1, *et le système n'a de solutions dans aucun corps contenant* K.

Si cet idéal ne contient pas 1, on peut l'inclure dans un idéal maximal $\mathfrak{m}$, et alors le système $\mathrm{P}_1(x) = \cdots = \mathrm{P}_n(x) = 0$ a une solution dans le corps $\mathrm{L}_0 = \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathfrak{m}$, à savoir l'image de $(\mathrm{X}_1, \ldots, \mathrm{X}_m)$, et donc il en a dans une clôture algébrique de ce corps qui est un corps algébriquement clos contenant K car L_0 contient K. Il s'ensuit que l'on est dans le second cas de l'alternative du th. 9.4, et donc que le système a des solutions dans tout corps algébriquement clos contenant K.

• Si K est algébriquement clos, Tout idéal maximal de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ est de la forme $\mathfrak{m}_x = (\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_m - x_m)$, avec $x = (x_1, \ldots, x_m) \in \mathrm{K}^m$, et $x \mapsto \mathfrak{m}_x$ est une bijection de K^m sur l'ensemble des idéaux maximaux de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$.

Un idéal I de la forme $(\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_m - x_m)$ est maximal (le quotient est K puisque les constantes forment un supplémentaire de I dans $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$).

Réciproquement, soit I un idéal maximal de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$. Comme $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ est noethérien, I est de type fini ; soient $\mathrm{P}_1, \ldots, \mathrm{P}_n$ engendrant I. Comme I ne contient pas 1, il existe

74. I.e. il existe $\mathrm{U}_1, \ldots, \mathrm{U}_n \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ tels que $\mathrm{U}_1\mathrm{P}_1 + \cdots + \mathrm{U}_n\mathrm{P}_n = 1$.

$x = (x_1, \ldots, x_m) \in \mathrm{K}^m$ solution du système $\mathrm{P}_1(x) = \cdots = \mathrm{P}_n(x) = 0$. Or $\mathrm{P}(x) = 0$ implique que P est dans l'idéal $(\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_m - x_m)$ (écrire X_i sous la forme $(\mathrm{X}_i - x_i) + x_i$ et développer) ; il s'ensuit que I est inclus dans $(\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_m - x_m)$, et donc lui est égal par maximalité. Ceci prouve le premier énoncé.

On en tire la surjectivité de $x \mapsto \mathfrak{m}_x$. L'injectivité résulte de ce que, si $x = (x_1, \ldots, x_m)$ et $y = (y_1, \ldots, y_m)$ sont distincts, il existe i tel que $x_i \neq y_i$, et alors $\mathfrak{m}_x + \mathfrak{m}_y$ contient $x_i - y_i = (\mathrm{X}_i - y_i) - (\mathrm{X}_i - x_i)$, et donc aussi 1, ce qui prouve que $\mathfrak{m}_x \neq \mathfrak{m}_y$.

On suppose K algébriquement clos. Si I est un idéal de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$, on note V(I) l'ensemble des $x \in \mathrm{K}^m$ vérifiant $\mathrm{P}(x) = 0$ pour tout $\mathrm{P} \in \mathrm{I}$ (il suffit de vérifier ceci pour des P_i engendrant I) ; c'est la *sous-variété algébrique* de K^m définie par I. Si $x \in \mathrm{V(I)}$, le morphisme d'anneaux $\mathrm{P} \mapsto \mathrm{P}(x)$ de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ dans K est identiquement nul sur I, et donc se factorise à travers $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathrm{I}$; son image étant le corps K, son noyau est un idéal maximal $\mathfrak{m}_x$ de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathrm{I}$.

• L'application $x \mapsto \mathfrak{m}_x$ est une bijection [75] de V(I) sur l'ensemble des idéaux maximaux de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathrm{I}$.

Les idéaux maximaux de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathrm{I}$ sont en bijection avec les idéaux maximaux de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ qui contiennent I (l'image inverse d'un idéal maximal de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]/\mathrm{I}$ dans $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ est un idéal maximal de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$). D'après le point précédent, un tel idéal est de la forme $(\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_m - x_m)$, avec $x = (x_1, \ldots, x_m) \in \mathrm{K}^m$; c'est alors l'idéal des $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ vérifiant $\mathrm{P}(x) = 0$, et il contient I si et seulement si $x \in \mathrm{V(I)}$. Les idéaux maximaux de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ contenant I sont donc en bijection avec V(I). On en déduit le résultat.

10. Réduction des endomorphismes

Dans le n° 10.1, on rappelle (et complète) sans démonstration les résultats vus en classe préparatoire concernant la réduction des endomorphismes (diagonalisation, mise sous forme de Jordan...). Au n° 10.2, on explique comment on peut retrouver ces résultats en utilisant le théorème de structure des modules de torsion sur les anneaux principaux démontré au n° 10.3. L'intérêt de cette nouvelle approche est de ne rien supposer sur le corps K, alors que l'approche vue en classe préparatoire impose plus ou moins à K d'être

75. Cette bijection entre points et idéaux maximaux est à l'origine de la théorie des schémas de Grothendieck (1955) : si A est un anneau, on définit l'espace topologique Spec A (le *spectre* de A) comme l'ensemble des idéaux premiers de A, muni de la *topologie de Zariski* (un fermé pour cette topologie est un sous-ensemble de la forme V(I), où I est un idéal de A et V(I) est l'ensemble des idéaux premiers de A contenant I). L'anneau A devient alors l'anneau des fonctions continues sur Spec A ; la valeur de $f \in \mathrm{A}$ en un idéal $\mathfrak{p}$ étant l'image de f dans $\mathrm{A}/\mathfrak{p}$. Il y avait eu plusieurs tentatives en ce sens avant Grothendieck, mais celui-ci a réalisé que l'on obtenait une théorie parfaitement satisfaisante en ne mettant aucune condition sur les anneaux considérés (contrairement à ses prédécesseurs), et en considérant des idéaux premiers au lieu d'idéaux maximaux ; cela donne à la théorie des schémas une souplesse et une richesse assez phénoménales.

algébriquement clos (ce qui, il faut le reconnaître, est le cas de $\mathbf{C}$ (cf. ex. 8.3, th. V.4.15 et ex. V.3.13, VI.3.21, V.3.2), mais est loin d'être celui de $\mathbf{F}_2$).

10.1. Généralités

Soit K un corps commutatif, et soit V un K-espace vectoriel *de dimension finie*.

10.1.1. *Endomorphismes*

On note End(V) l'ensemble des *endomorphismes* de V, c'est-à-dire, l'ensemble des applications $u : \mathrm{V} \to \mathrm{V}$ qui sont linéaires. Muni de l'addition $(u_1 + u_2)(v) = u_1(v) + u_2(v)$, et de la composition des endomorphismes, End(V) est un anneau non commutatif (sauf en dimension 1), possédant un élément unité (que nous noterons 1) en la personne de l'application identité $\mathrm{id} : \mathrm{V} \to \mathrm{V}$ (cf. n° 5.1). L'*homothétie de rapport* λ est l'application $v \mapsto \lambda v$. On la note simplement λ, ce qui est compatible avec le fait que l'identité (que l'on a notée 1) peut aussi être vue comme l'homothétie de rapport 1.

10.1.2. *Le théorème de Cayley-Hamilton*

Si $u \in \mathrm{End}(\mathrm{V})$, on note $\det(u) \in \mathrm{K}$ son déterminant (cf. n° 6.3). Si $u_1, u_2 \in \mathrm{End}(\mathrm{V})$, alors $\det(u_1\, u_2) = \det(u_1)\det(u_2)$. On note $\mathrm{Car}_u(\mathrm{X})$ le *polynôme caractéristique* de u défini par $\mathrm{Car}_u(\mathrm{X}) = \det(\mathrm{X} - u)$ (cf. alinéa 7.7.1). Si V est de dimension d, c'est un polynôme de degré d, dont le développement est donné par

$$\mathrm{Car}_u(\mathrm{X}) = \mathrm{X}^d - \mathrm{Tr}(u)\mathrm{X}^{d-1} + \cdots + (-1)^d \det(u),$$

où $\mathrm{Tr}(u)$ est, par définition, la *trace* de u. On a $\mathrm{Tr}(u_1u_2) = \mathrm{Tr}(u_2u_1)$, si $u_1, u_2 \in \mathrm{End}(\mathrm{V})$.

L'ensemble des $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{P}(u) = 0$ est un idéal de K[X], non nul car End(V) est de dimension $(\dim \mathrm{V})^2$ et donc $1, u, \ldots, u^{(\dim \mathrm{V})^2}$ forment une famille liée. On note Min_u le générateur unitaire de cet idéal. C'est le *polynôme minimal* de u et, d'après le théorème de Cayley-Hamilton (1858), Car_u annule u ; autrement dit, Car_u est un multiple de Min_u (cf. cor 10.8).

10.1.3. *Automorphismes*

Si $u \in \mathrm{End}(\mathrm{V})$, le noyau et l'image de u, définis par

$$\mathrm{Ker}(u) = \{v \in \mathrm{V},\ u(v) = 0\} \text{ et } \mathrm{Im}(u) = \{v \in \mathrm{V},\ \exists v' \in \mathrm{V},\ u(v') = v\},$$

sont des sous-espaces vectoriels de V, et on a les équivalences (cf. alinéa 5.4.2) :

$$\det u \neq 0 \Leftrightarrow \mathrm{Ker}(u) = 0 \Leftrightarrow u \text{ injectif} \Leftrightarrow u \text{ bijectif} \Leftrightarrow u \text{ surjectif} \Leftrightarrow \mathrm{Im}(u) = \mathrm{V}.$$

Un *automorphisme* de V est un élément de End(V) vérifiant les conditions ci-dessus. On note $\mathrm{GL}(\mathrm{V}) \subset \mathrm{End}(\mathrm{V})$ l'ensemble des automorphismes de V ; c'est le groupe des éléments inversibles de l'anneau End(V).

10.1.4. *Matrices*

Si V est de dimension d, et si on choisit une base $e_1, \dots, e_d$ de V, on peut associer à tout élément u de End(V) sa matrice dans la base $e_1, \dots, e_d$ (cf. n° 7.4). C'est l'élément $(a_{i,j})_{1 \leqslant i,j \leqslant d}$ de $\mathbf{M}_d(\mathrm{K})$ défini par $u(e_j) = \sum_{i=1}^{d} a_{i,j} e_i$. La trace de u est alors la somme $\sum_{i=1}^{d} a_{i,i}$ des coefficients diagonaux de la matrice de u ; cette somme ne dépend donc pas du choix de la base. Le groupe GL(V) s'identifie au groupe $\mathbf{GL}_d(\mathrm{K})$ des matrices $d \times d$ inversibles (ce qui équivaut à ce que le déterminant soit non nul) à coefficients dans K.

Si $f_1, \dots, f_d$ est une autre base de V, si P est la matrice dont les colonnes sont $f_1, \dots, f_d$ exprimés dans la base $e_1, \dots, e_d$, les matrices M et M′ de u dans les bases $e_1, \dots, e_d$ et $f_1, \dots, f_d$ sont reliées par la formule $\mathrm{M}' = \mathrm{P}^{-1}\mathrm{MP}$.

10.1.5. *Espaces propres, espaces caractéristiques*

Soit $u \in \mathrm{End(V)}$. On dit que $\lambda \in \mathrm{K}$ est une *valeur propre* de u, si $u - \lambda$ n'est pas inversible, ce qui équivaut à $\mathrm{Ker}(u - \lambda) \neq 0$, et donc à l'existence de $v \in \mathrm{V}$, non nul, tel que $u(v) = \lambda v$; un tel v est un *vecteur propre* de u pour la valeur propre λ (cf. n° 5.2). Le *spectre* $\mathrm{Spec}\, u$ de u est l'ensemble des valeurs propres de u. C'est aussi l'ensemble des racines du polynôme caractéristique $\mathrm{Car}_u(\mathrm{X}) = \det(\mathrm{X} - u)$ de u.

Si $\lambda \in \mathrm{Spec}\, u$, le noyau de $\mathrm{Ker}(u - \lambda)$ est l'*espace propre* associé à la valeur propre λ. On dit que u est *diagonalisable*, si $\mathrm{V} = \oplus_{\lambda \in \mathrm{Spec}\, u} \mathrm{Ker}(u - \lambda)$. Ceci équivaut à l'existence d'une base $(e_i)_{i \in \mathrm{I}}$ de V (constituée de vecteurs propres) dans laquelle la matrice de u est une *matrice diagonale* (i.e. $a_{i,j} = 0$ si $i \neq j$). Le polynôme minimal de u est alors le produit des $(\mathrm{X} - \lambda)$, pour $\lambda \in \mathrm{Spec}\, u$ (cor. 10.9) ; en particulier, tous ses zéros sont dans K et ces zéros sont simples. Réciproquement, *s'il existe* $\mathrm{P} \in \mathrm{K[X]}$*, dont tous les zéros sont simples et appartiennent à* K*, avec* $\mathrm{P}(u) = 0$*, alors* u *est diagonalisable* (cor. 10.9).

Si $\lambda \in \mathrm{Spec}\, u$, la suite des $\mathrm{Ker}\,(u - \lambda)^k$ est croissante, et donc stationnaire (i.e. constante à partir d'un certain rang). On note e_λ le plus petit k tel que $\mathrm{Ker}\,(u - \lambda)^{k'} = \mathrm{Ker}\,(u - \lambda)^k$, quel que soit $k' \geqslant k$. Alors $\mathrm{Ker}\,(u - \lambda)^{e_\lambda}$ est le *sous-espace caractéristique* associé à λ. Si Car_u est scindé sur K, alors V est la somme directe $\oplus_{\lambda \in \mathrm{Spec}\, u} \mathrm{V}_\lambda$ de ses sous-espaces caractéristiques (cor. 10.10). On note d_λ la dimension de V_λ ; c'est la *multiplicité* de la valeur propre λ, et c'est aussi la multiplicité de λ en tant que racine de Car_u.

10.1.6. *Mise sous forme de Jordan*

Un *bloc de Jordan* $\mathrm{J}_{\lambda,r}$ d'ordre r pour λ est une matrice $r \times r$ avec des λ sur la diagonale, des 1 juste au-dessus de la diagonale et des 0 partout ailleurs. Les polynômes minimal et caractéristique de $\mathrm{J}_{\lambda,r}$ sont tous deux égaux à $(\mathrm{X} - \lambda)^r$. Une matrice est *sous forme de Jordan* si elle est diagonale par blocs, et si chacun des blocs est un bloc de Jordan (on ne demande pas aux blocs d'être de la même taille, ni d'être associés au même λ).

On peut trouver une base de V_λ dans laquelle la matrice de u est sous forme de Jordan (ex. 10.5 et cor. 10.11). La taille des blocs $r_{\lambda,1} \geqslant r_{\lambda,2} \geqslant \cdots \geqslant r_{\lambda,k_\lambda}$ est alors indépendante du choix de la base, et on a $r_{\lambda,1} = e_\lambda$ et $\sum_{j=1}^{k_\lambda} r_{\lambda,j} = d_\lambda \geqslant e_\lambda$. En juxtaposant les bases

des V_λ, pour $\lambda \in \operatorname{Spec} u$, cela permet, si Car_u est scindé, de mettre la matrice de u sous forme de Jordan. On en déduit que les polynômes minimal Min_u et caractéristique Car_u de u sont donnés par

$$\mathrm{Min}_u(X) = \prod_{\lambda \in \operatorname{Spec} u} (X-\lambda)^{e_\lambda} \quad \text{et} \quad \mathrm{Car}_u(X) = \prod_{\lambda \in \operatorname{Spec} u} (X-\lambda)^{d_\lambda}.$$

On déduit aussi de l'existence de la forme de Jordan que $\mathrm{Tr}(u)$ (resp. $\det(u)$) est la somme (resp. le produit) des valeurs propres de u, comptées avec multiplicité.

10.2. Modules de torsion sur K[X] et réduction des endomorphismes

10.2.1. *Anneaux et modules.* — Nous renvoyons au § 2 pour des compléments sur les points rappelés ci-dessous. Si A est un anneau (avec élément unité 1), un A-*module* M est un groupe commutatif pour une loi $+$, muni d'une action $(a,x) \mapsto ax$ de A, vérifiant :

$$0\,x = 0, \quad 1\,x = x, \quad a(x+y) = ax + ay, \quad (a+b)x = ax + bx, \quad (ab)x = a(bx),$$

quels que soient $x, y \in \mathrm{M}$ et $a, b \in \mathrm{A}$.

• Si A est un corps commutatif, on retombe sur la définition d'un espace vectoriel, et il y a de grandes similarités entre la théorie des modules sur un anneau commutatif et celle des espaces vectoriels sur un corps commutatif. La grosse différence est que $ax = 0$ et $a \neq 0$ n'impliquent pas forcément $x = 0$.

• Tout groupe commutatif est naturellement un $\mathbf{Z}$-module, en définissant nx par récurrence sur n, par $0x = 0$, $(n+1)x = nx + x$ si $n \in \mathbf{N}$, et $nx = -((-n)x)$, si $n \leqslant 0$.

• Si A est commutatif, un sous-A-module de A n'est autre qu'un idéal de A.

• Si K est un corps commutatif, et si V est un K-espace vectoriel, alors V est un module sur l'anneau $\mathrm{End}(\mathrm{V})$ (non commutatif si $\dim \mathrm{V} \geqslant 2$).

• Si $(\mathrm{M}_i)_{i\in \mathrm{I}}$ est une famille de A-modules, les groupes commutatifs $\oplus_{i\in \mathrm{I}} \mathrm{M}_i$ et $\prod_{i\in \mathrm{I}} \mathrm{M}_i$ sont naturellement munis d'une action de A, et sont donc des A-modules.

• Si $\mathrm{M}' \subset \mathrm{M}$ sont deux A-modules, le groupe commutatif quotient M/M' est muni d'une action de A et donc est un A-module.

• Un *morphisme* $u : \mathrm{M}_1 \to \mathrm{M}_2$ *de* A-*modules* est un morphisme de groupes additifs commutant à l'action de A (i.e. $u(ax) = a\,u(x)$, si $x \in \mathrm{M}_1$ et $a \in \mathrm{A}$) ; si A est un corps commutatif, on retombe sur la définition d'une application linéaire entre espaces vectoriels.

• Si $u : \mathrm{M}_1 \to \mathrm{M}_2$ est un morphisme de A-modules, alors $\operatorname{Ker} u$ et $\operatorname{Im} u$ sont des A-modules, et u induit un isomorphisme de A-modules de $\mathrm{M}_1/\operatorname{Ker} u$ sur $\operatorname{Im} u$. En particulier, u est injectif si et seulement si $\operatorname{Ker} u = \{0\}$ et u est surjectif si et seulement si $\operatorname{Im} u = \mathrm{M}_2$.

Si M est un A-module et si les M_i, pour $i \in \mathrm{I}$, sont des sous-A-modules de M, alors l'intersection des M_i est un A-module. Ceci permet de définir le *sous*-A-*module engendré* par une famille $(e_j)_{j\in \mathrm{J}}$ d'éléments de M, comme l'intersection de tous les sous-A-modules

de M contenant les e_j. Comme dans le cas des espaces vectoriels, ce module est l'ensemble des combinaisons linéaires finies, à coefficients dans A, en les e_j.

A l'exception (importante) de l'anneau End(V), où V est un espace vectoriel, tous les anneaux que nous considérerons sont commutatifs ; *sauf mention explicite du contraire, « anneau » signifie « anneau commutatif » dans tout ce qui suit.*

Un A-module M est *de type fini* si on peut trouver un ensemble fini $e_1, \dots, e_d$ d'éléments de M tels que l'application $(a_1, \dots, a_d) \mapsto a_1e_1 + \cdots + a_de_d$ soit une surjection de A^d sur M ; autrement dit, M est de type fini s'il admet une famille génératrice finie. Une différence essentielle avec le cas des espaces vectoriels est qu'un A-module ne possède pas, en général, de base sur A. Un module qui possède une base finie est dit *libre* de type fini.

• Un A-module M, libre de type fini, est isomorphe à A^r pour un unique $r \in \mathbf{N}$ appelé le *rang* de M.

Par définition, un A-module M, libre de type fini, est isomorphe à A^r pour un certain r (le choix d'une base $e_1, \dots, e_r$ fournit un isomorphisme $(x_1, \dots, x_r) \mapsto \sum_{i=1}^r x_i e_i$ de A^r sur M). Il s'agit donc de prouver que $\mathrm{A}^r \cong \mathrm{A}^s$ implique $r = s$.

Supposons que $s > r$, et notons $\mathrm{B} \in \mathrm{M}_{s\times r}(\mathrm{A})$ la matrice de l'isomorphisme $\mathrm{A}^r \to \mathrm{A}^s$ et $\mathrm{C} \in \mathrm{M}_{r\times s}(\mathrm{A})$ la matrice de son inverse ; on a alors $\mathrm{BC} = 1_s$ et donc $\det \mathrm{BC} = 1$. Par ailleurs, les s colonnes de BC sont des combinaisons linéaires des r colonnes $c_1, \dots, c_r$ de C. En utilisant la multilinéarité du déterminant, vu comme une fonction des colonnes, on voit que $\det \mathrm{BC}$ est une combinaison linéaire de termes de la forme $\det(c_{j_1}, \dots, c_{j_s})$. Or tous ces termes sont nuls car $s > r$, ce qui fait que deux des j_k sont égaux. Il s'ensuit que $\det \mathrm{BC} = 0$, ce qui conduit à une contradiction qui permet de conclure.

Un A-module M est *de torsion* si, pour tout $x \in \mathrm{M}$, on peut trouver $a \in \mathrm{A} - \{0\}$, tel que $ax = 0$. Un A-module de torsion non nul est un exemple de module ne possédant pas de base puisque toute famille ayant plus d'un élément est liée. Un exemple typique de A-module de torsion est A/I ou plus généralement J/I, où $\mathrm{I} \subset \mathrm{J}$ sont des idéaux de A et $\mathrm{I} \neq \{0\}$; par exemple, $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est un $\mathbf{Z}$-module de torsion, si $\mathrm{D} \geqslant 2$.

• Si A est intègre, et si M est un A-module, l'ensemble $\mathrm{M}_{\mathrm{tors}}$ des éléments de torsion (i.e l'ensemble des $x \in \mathrm{M}$ tels qu'il existe $a \in \mathrm{A} - \{0\}$ vérifiant $a \cdot x = 0$) est un sous-A-module de M (c'est le plus grand sous-module de torsion de M).

Si $ax = 0$ et $by = 0$, alors $ab(x + y) = 0$ et $ab \neq 0$ si $a \neq 0$ et $b \neq 0$; il s'ensuit que $\mathrm{M}_{\mathrm{tors}}$ est un sous-groupe de $(\mathrm{M}, +)$. De plus $a(\lambda x) = 0$ si $ax = 0$, ce qui prouve que $\mathrm{M}_{\mathrm{tors}}$ est stable sous l'action de A, et permet de conclure.

Exercice 10.1. — (i) Soit A un anneau intègre noethérien, et soit M un A-module de type fini. Montrer qu'il existe $a \in \mathrm{A} - \{0\}$ tel que $ax = 0$ pour tout $x \in \mathrm{M}_{\mathrm{tors}}$.

(ii) Soit M un $\mathbf{Z}$-module de type fini. Montrer que $\mathrm{M}_{\mathrm{tors}}$ est fini. Un $\mathbf{Z}$-module de torsion est-il nécessairement fini ?

10.2.2. *Structure des modules de torsion sur* K[X]. — Soit K un corps commutatif. Comme le montre la discussion suivant le th 10.3 ci-dessous, un K-espace vectoriel de

dimension finie muni d'un endomorphisme K-linéaire u est la même chose qu'un K[X]-module de torsion et de type fini. Ce changement de point de vue est particulièrement intéressant à cause du théorème de structure (th. 10.3) ci-dessous, que le lecteur pourra comparer avec le théorème de structure (th. 3.1) pour les groupes finis abéliens (nous démontrons les deux simultanément au n° 10.3).

Un polynôme $P \in K[X]$ est dit *irréductible* s'il est de degré $\geqslant 1$ et si on ne peut pas le factoriser sous la forme $P = Q_1Q_2$, avec $Q_1, Q_2 \in K[X]$ et $\deg Q_1 \geqslant 1$, $\deg Q_2 \geqslant 1$. Un corps K est algébriquement clos si et seulement si les polynômes irréductibles de K[X] sont de degré 1 ; les polynômes irréductibles de $\mathbf{R}[X]$ sont de degré 1 ou 2, ceux de $\mathbf{Q}[X]$ ou de $\mathbf{F}_p[X]$ ont des degrés arbitraires. On note $\mathscr{P}_{K[X]}$ l'ensemble des polynômes unitaires irréductibles de degré $\geqslant 1$.

Si $Q \in K[X]$, on note K[X]/Q (au lieu de K[X]/QK[X] ou K[X]/(Q)) le quotient de K[X] par l'idéal engendré par Q.

Exercice 10.2. — Montrer que K[X]/Q est un corps si $Q \in \mathscr{P}_{K[X]}$.

Théorème 10.3. — *Soit* M *un* K[X]*-module de torsion et de type fini. Si* $P \in \mathscr{P}_{K[X]}$*, soit* M_P *l'ensemble des* $x \in M$ *tués par une puissance de* P.

(i) M_P *est un sous-*K[X]*-module de* M*, nul sauf pour un nombre fini de* $P \in \mathscr{P}_{K[X]}$*, et* $M = \oplus_{P \in \mathscr{P}_{K[X]}} M_P$.

(ii) *Il existe* $r_P \in \mathbf{N}$ *et une unique famille décroissante d'entiers* $a_{P,i} \geqslant 1$*, tels que* $M_P = \oplus_{1 \leqslant i \leqslant r_P} K[X]/P^{a_{P,i}}$.

10.2.3. *Exemples.* — Soit M un K[X]-module de torsion et de type fini, et soient $e_1, \ldots, e_d$ engendrant M. Par définition, cela veut dire que $(x_1, \ldots, x_d) \mapsto x_1e_1 + \cdots + x_de_d$, de $(K[X])^d$ dans M, est surjective. Par ailleurs, si $P_i \in K[X] - \{0\}$, pour $i \in \{1, \ldots, d\}$, vérifie $P_ie_i = 0$ (de tels P_i existent puisque M est de torsion), alors le noyau de l'application précédente contient $(P_1) \times \cdots \times (P_d)$, et donc M est un quotient de $K[X]/P_1 \times \cdots \times K[X]/P_d$, qui est un K-espace vectoriel de dimension finie $\deg P_1 \cdots \deg P_d$. On en déduit que M est un K-espace vectoriel de dimension finie. De plus, la multiplication par X sur M est K-linéaire, ce qui munit M d'un élément privilégié u_M de End(M).

Réciproquement, si V est un K-espace vectoriel de dimension finie, et si u est un endomorphisme de V, alors $P \mapsto P(u)$ induit un morphisme d'anneaux de K[X] dans End(V). Comme V est un End(V)-module, cela muni V d'une action de K[X] (où $P \in K[X]$ agit par $P(u) \in \mathrm{End}(V)$), ce qui permet de voir V comme un K[X]-module ; par construction, on a $u_V = u$. De plus, le K[X]-module V est de torsion car $\mathrm{Min}_u \in K[X]$ tue tous les éléments de V puisque, par définition, Min_u agit par $\mathrm{Min}_u(u)$ sur V, et $\mathrm{Min}_u(u) = 0$.

• Si V est un K-espace vectoriel de dimension finie, $u, u' \in \mathrm{End}(V)$ sont conjugués (i.e. il existe $g \in \mathrm{GL}(V)$ tel que $u' = gug^{-1}$) si et seulement si les K[X]-modules associés sont isomorphes.

Il s'agit d'un pur exercice de traduction. Si M et M′ sont des K[X]-modules, un isomorphisme $\iota : M \cong M'$ de K[X]-modules est une application K-linéaire qui commute aux actions de X, ce qui se traduit par $u_{M'} \circ \iota = \iota \circ u_M$. Maintenant, si M et M′ sont associés à (V, u) et (V, u'), on a $M = M' = V$ en tant que K-espace vectoriel, avec $u_M = u$ et $u_{M'} = u'$. L'hypothèse $M \cong M'$ se traduit donc par l'existence de $\iota \in GL(V)$ vérifiant $u' \circ \iota = \iota \circ u$, ce qui se traduit par $u' = gug^{-1}$ si $g = \iota^{-1}$. Pour montrer que $M \cong M'$ si $u' = gug^{-1}$, il suffit de reprendre les traductions précédentes dans l'autre sens.

Exemple 10.4. — (Modules cycliques) Soit $Q = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$, avec $d \geqslant 1$, et soit $M = K[X]/Q$. Alors la matrice de u_M dans la base $1, X, \ldots, X^{d-1}$ est

$$A_Q = \begin{pmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ddots & \vdots & -a_1 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \ldots & 1 & -a_{d-1} \end{pmatrix}$$

et les polynômes minimal et caractéristique de u_M sont tous deux égaux à Q.

Par construction Q(X) est la multiplication par 0 sur M, et donc $Q(u_M) = 0$, ce qui implique que le polynôme minimal de u_M divise Q. Par ailleurs, si $P(u_M) = 0$, alors en particulier, $P(u_M) \cdot 1 = P(X)$ est nul dans $M = K[X]/Q$, et donc P est un multiple de Q. Ceci prouve que le polynôme minimal de u_M est bien Q.

Le polynôme caractéristique de u_M, qui n'est autre que le déterminant de $X - u_M$, peut se calculer en développant par rapport à la dernière colonne. Le coefficient de $X + a_{d-1}$ est le déterminant d'une matrice $(d-1)\times(d-1)$, triangulaire inférieure, avec des X sur la diagonale, et donc est égal à X^{d-1}. Si $i \geqslant 2$, le coefficient de a_{d-i} est $(-1)^{i-1}\times$ le déterminant d'une matrice diagonale par blocs, un des blocs de dimension $(d-i)\times(d-i)$ étant triangulaire inférieur avec des X sur la diagonale, et l'autre, de dimension $(i-1)\times(i-1)$, étant triangulaire supérieur avec des -1 sur la diagonale ; il est donc égal à $(-1)^{i-1}X^{d-i}(-1)^{i-1} = X^{d-i}$, et on a

$$\det(X - u_M) = (X + a_{d-1})X^{d-1} + a_{d-2}X^{d-2} + \cdots + a_0 = Q(X).$$

Exemple 10.5. — (Modules nilpotents) Soit $\lambda \in K$, et soit $M = K[X]/(X-\lambda)^d$. Alors la matrice de u_M dans la base $f_1 = (X-\lambda)^{d-1}, f_2 = (X-\lambda)^{d-2}, \ldots, f_d = 1$ est un bloc de Jordan $J_{\lambda,d}$.

On a $X(X-\lambda)^{d-i} = (X-\lambda)^{d-(i-1)} + \lambda(X-\lambda)^{d-i}$, ce qui se traduit par $u_M(f_i) = f_{i-1} + \lambda f_i$, si $i \neq 1$, et par $u_M(f_1) = \lambda f_1$ car $(X-\lambda)^d = 0$ dans M.

10.2.4. *Application à la réduction des endomorphismes*

Lemme 10.6. — *Soit $(Q_i)_{i\in I}$ une famille finie d'éléments de K[X] de degrés $\geqslant 1$. Si $M = \oplus_{i\in I} K[X]/Q_i$, alors le polynôme minimal de u_M est le* ppcm *des Q_i, pour $i \in I$, et le polynôme caractéristique de u_M est le produit des Q_i, pour $i \in I$.*

Le polynôme minimal de u_M doit en particulier annuler $K[X]/Q_i$ pour tout i ; il doit donc être divisible par Q_i d'après les résultats de l'exemple 10.4, et donc aussi par le ppcm des Q_i. Réciproquement, le ppcm des Q_i est divisible par Q_i ; il annule donc $K[X]/Q_i$ pour tout i et

est un multiple du polynôme minimal de u_{M} ; d'où le résultat en ce qui concerne le polynôme minimal de u_{M}.

Pour calculer le polynôme caractéristique de u_{M}, on remarque que chaque $\mathrm{K[X]}/\mathrm{Q}_i$ est stable par u_{M}, et donc que la matrice de u_{M} est diagonale par blocs, avec un bloc pour chaque i correspondant à l'action de u_{M} sur $\mathrm{K[X]}/\mathrm{Q}_i$. Comme le polynôme caractéristique d'une matrice diagonale par blocs est le produit des polynômes caractéristiques des blocs, les résultats de l'exemple 10.4 permettent de conclure.

Soit V un espace vectoriel de dimension finie muni d'un endomorphisme u. On peut supposer que V est un K[X]-module de torsion et de type fini, et que u est la multiplication par X. Si on note $\operatorname{Spec} u$ l'ensemble des $\mathrm{P} \in \mathscr{P}_{\mathrm{K[X]}}$ tels que $\mathrm{V}_{\mathrm{P}} \neq 0$ (dans les notations du théorème 10.3), on déduit du lemme 10.6 le résultat suivant.

Corollaire 10.7. — *Si les $a_{\mathrm{P},i}$ sont les entiers définis au th. 10.3, alors*

$$\mathrm{Min}_u(\mathrm{X}) = \prod_{\mathrm{P}\in\operatorname{Spec} u} \mathrm{P}^{a_{\mathrm{P},1}} \quad \text{et} \quad \mathrm{Car}_u(\mathrm{X}) = \prod_{\mathrm{P}\in\operatorname{Spec} u} \mathrm{P}^{a_{\mathrm{P},1}+\cdots+a_{\mathrm{P},r_{\mathrm{P}}}}.$$

Corollaire 10.8. — (Cayley-Hamilton) *Le polynôme minimal de u divise le polynôme caractéristique de u.*

C'est, modulo le résultat précédent, une traduction de l'inégalité $a_{\mathrm{P},1} \leqslant a_{\mathrm{P},1} + \cdots + a_{\mathrm{P},r_{\mathrm{P}}}$.

Corollaire 10.9. — *Les conditions suivantes sont équivalentes.*

(i) *u est diagonalisable.*

(ii) *u est annulé par un polynôme scindé, sans racine double.*

(iii) $\operatorname{Spec} u$ *est constitué de polynômes de degré* 1, *et*[76] $\mathrm{Min}_u = \prod_{\lambda\in\operatorname{Spec} u}(\mathrm{X}-\lambda)$.

(iv) *Dans la décomposition* $\mathrm{V} \cong \oplus_{\mathrm{P}\in\operatorname{Spec} u}\big(\oplus_{1\leqslant i\leqslant r_{\mathrm{P}}} \mathrm{K[X]}/\mathrm{P}^{a_{\mathrm{P},i}}\big)$, *les éléments de* $\operatorname{Spec} u$ *sont de degré* 1 *et les $a_{\mathrm{P},i}$ sont tous égaux à* 1.

L'équivalence des conditions (iii) et (iv) résulte du cor. 10.7.

Si u est diagonalisable, V est la somme directe de ses espaces propres V_λ, pour $\lambda \in \operatorname{Spec} u$. Alors $u - \lambda$ est nul sur V_λ et donc $\prod_{\lambda\in\operatorname{Spec} u}(u-\lambda)$ est nul sur tous les V_λ, et donc aussi sur V. Comme $\prod_{\lambda\in\operatorname{Spec} u}(\mathrm{X}-\lambda)$ est scindé, sans racine double, cela prouve que (i)⇒(ii).

Comme Min_u divise tout polynôme annulant u, l'hypothèse (ii) entraîne que Min_u est scindé, sans racine double. Il s'ensuit, d'après le cor. 10.7, que les éléments de $\operatorname{Spec} u$ sont de la forme $\mathrm{X}-\lambda$, avec $\lambda \in \mathrm{K}$, et que $\mathrm{V} \cong \oplus_{\lambda\in\mathrm{Spec(u)}}(\mathrm{K[X]}/(\mathrm{X}-\lambda))^{d_\lambda}$, ce qui prouve que (i)⇒(iv).

Enfin, comme X agit par multiplication par λ sur $\mathrm{K[X]}/(\mathrm{X}-\lambda)$, on voit que $(\mathrm{K[X]}/(\mathrm{X}-\lambda))^{d_\lambda}$ est contenu dans l'espace propre pour λ, et un isomorphisme $\mathrm{V} \cong \oplus_{\lambda\in\mathrm{Spec(u)}}(\mathrm{K[X]}/(\mathrm{X}-\lambda))^{d_\lambda}$ est donc équivalent à exhiber une base de V constituée de vecteurs propres, ce qui prouve que u est diagonalisable, et que (iv)⇒(i).

Ceci termine la démonstration.

Corollaire 10.10. — *Si* V *est un* K*-espace vectoriel de dimension finie, et si* $u \in \mathrm{End}(\mathrm{V})$ *est annulé par un polynôme scindé, alors* V *est la somme directe des sous-espaces caractéristiques de u.*

76. On se permet d'identifier un polynôme $\mathrm{X}-\lambda$ de degré 1 avec sa racine λ.

Pour les mêmes raisons que ci-dessus, le polynôme minimal de u est scindé, et donc les éléments de Spec u sont de la forme $\mathrm{X}-\lambda$, avec $\lambda \in \mathrm{K}$. Le (i) du th. 10.3 nous fournit donc une décomposition de V sous la forme $\oplus_\lambda \mathrm{V}_{\mathrm{X}-\lambda}$, et $\mathrm{V}_{\mathrm{X}-\lambda}$ est exactement l'ensemble des $x \in \mathrm{V}$ tués par une puissance de $u-\lambda$; autrement dit $\mathrm{V}_{\mathrm{X}-\lambda}$ est le sous-espace caractéristique de u associé à la valeur propre λ, et comme $\mathrm{V} = \oplus_\lambda \mathrm{V}_{\mathrm{X}-\lambda}$, cela permet de conclure.

Corollaire 10.11. — *Si* V *est un* K*-espace vectoriel de dimension finie, et si* $u \in \mathrm{End}(\mathrm{V})$ *est annulé par un polynôme scindé, alors il existe une base de* V *dans laquelle la matrice de* u *est sous forme de Jordan.*

Comme ci-dessus, on déduit du th. 10.3 une décomposition $\mathrm{V} \cong \oplus_{i\in \mathrm{I}} \mathrm{K}[\mathrm{X}]/(\mathrm{X}-\lambda_i)^{a_i}$ (dans laquelle plusieurs λ_i peuvent être égaux). On conclut en utilisant le résultat de l'exemple 10.5, selon lequel la matrice de la multiplication par X sur $\mathrm{K}[\mathrm{X}]/(\mathrm{X}-\lambda_i)^{a_i}$ peut se mettre sous forme de Jordan.

Corollaire 10.12. — (décomposition de Dunford) *Si* V *est un* K*-espace vectoriel de dimension finie, et si* $u \in \mathrm{End}(\mathrm{V})$ *est annulé par un polynôme scindé, alors* u *peut se décomposer de manière unique sous la forme* $u = \mathrm{D} + \mathrm{N}$*, où* D *est diagonalisable,* N *est nilpotent, et* D *et* N *commutent.*

L'hypothèse implique que V est la somme directe des sous-espaces caractéristiques V_λ de u. Soit $\mathrm{D} \in \mathrm{End}(\mathrm{V})$ défini par $\mathrm{D}(x) = \lambda x$, si $x \in \mathrm{V}_\lambda$. Alors D est diagonalisable par construction, et commute à u car u laisse stable les V_λ et la restriction de D à V_λ est une homothétie. De plus, $u-\lambda$ est nilpotent sur V_λ par définition de V_λ, et donc $u-\mathrm{D}$ est nilpotent sur V (on a $(u-\mathrm{D})^{e_\lambda} = 0$ sur V_λ et donc $(u-\mathrm{D})^e = 0$ sur V, si $e = \sup_\lambda e_\lambda$). Enfin, D commute à $u-\mathrm{D}$ puisqu'il commute à u, ce qui prouve que la décomposition $u = \mathrm{D}+\mathrm{N}$, avec $\mathrm{N} = u-\mathrm{D}$, est de la forme voulue. (On aurait aussi pu utiliser l'existence d'une base dans laquelle la matrice A de u est sous forme de Jordan : on a $\mathrm{A} = \mathrm{D}+\mathrm{N}$ où D est la matrice diagonale ayant les mêmes coefficients diagonaux que A, et N est triangulaire supérieure avec des 0 sur la diagonale, et donc est nilpotente (et on a $\mathrm{N}^d = 0$, si $\dim \mathrm{V} = d$) ; la commutation de D et N se vérifie bloc par bloc.)

Réciproquement, si D et N commutent, ils commutent aussi à u et donc aussi à tout polynôme en u. Soit λ une valeur propre de u, et soit V_λ le sous-espace caractéristique associé. Si $x \in \mathrm{V}_\lambda$, on a $0 = \mathrm{D}((u-\lambda)^{e_\lambda}(x)) = (u-\lambda)^{e_\lambda}(\mathrm{D}(x))$, et donc V_λ est stable par D. Maintenant, par hypothèse, $u-\mathrm{D}$ est nilpotent, et donc sa restriction à V_λ l'est. Par ailleurs, $u-\lambda$ est nilpotent sur V_λ par définition, et comme $u-\mathrm{D}$ et $u-\lambda$ commutent puisque u et D commutent, il s'ensuit que $\mathrm{D}-\lambda = (u-\lambda)-(u-\mathrm{D})$ est nilpotent sur V_λ (cf. ex. 2.1). Enfin, D étant supposé diagonalisable, il est annulé par un polynôme P, scindé sans racine double. La restriction de D à V_λ est aussi annulée par P, et donc est diagonalisable ; il en est donc de même de $\mathrm{D}-\lambda$, et la nilpotence de $\mathrm{D}-\lambda$ entraîne que $\mathrm{D} = \lambda$ sur V_λ. D'où l'unicité.

La décomposition de Dunford est particulièrement utile pour calculer les puissances d'un endomorphisme (ou d'un matrice) : comme D et N commutent, et comme $\mathrm{N}^d = 0$, la formule du binôme devient $u^n = \mathrm{D}^n + n\mathrm{D}^{n-1}\mathrm{N} + \cdots + \binom{n}{d-1}\mathrm{D}^{n-d+1}\mathrm{N}^{d-1}$, et si l'on dispose d'une base dans laquelle D est diagonal, calculer les puissances de D se fait sans effort. Ceci s'applique, par exemple, à l'étude d'une suite récurrente du type $\mathrm{X}_{n+1} = \mathrm{AX}_n$, où $\mathrm{A} \in \mathbf{M}_d(\mathrm{K})$, ce qui inclut les suites numériques vérifiant une relation de

récurrence du type $u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n$, pour tout $n \in \mathbf{N}$; elles correspondent [77] à prendre $\mathrm{X}_n = {}^{\mathrm{t}}(u_n, \ldots, u_{n+d-1})$ et

$$\mathrm{A} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \\ a_d & \cdots & a_2 & a_1 \end{pmatrix}$$

10.3. Modules de torsion sur les anneaux principaux

Les anneaux $\mathbf{Z}$ et $\mathrm{K}[\mathrm{X}]$ sont principaux (cf. alinéa 4.2.1), ce qui fait que le théorème 10.13 ci-dessous a pour conséquences les th. 3.1 et 10.3.

Soit A un anneau principal (cf. alinéa 4.2.2), et soit $\mathscr{P}_\mathrm{A}$ l'ensemble des idéaux premiers non nuls de A. Choisissons pour tout élément de $\mathscr{P}_\mathrm{A}$ un générateur, et identifions $\mathscr{P}_\mathrm{A}$ à l'ensemble de ces générateurs. Si $p \in \mathscr{P}_\mathrm{A}$, alors A/p est un corps.

De plus, tout élément non nul x de A se factorise, de manière unique, sous la forme $x = u \prod_{p \in \mathscr{P}_\mathrm{A}} p^{v_p(x)}$, où u est inversible dans A. Si $x_1, \ldots, x_n \in \mathrm{A}$, soit $\mathrm{pgcd}(x_1, \ldots, x_n)$ le générateur $\prod_{p \in \mathscr{P}_\mathrm{A}} p^{\inf_i(v_p(x_i))}$ de l'idéal $(x_1, \ldots, x_n)$: cet idéal est A (ce qui équivaut à ce que $x_1, \ldots, x_n$ sont premiers entre eux), si et seulement si $\inf_i(v_p(x_i)) = 0$ pour tout $p \in \mathscr{P}_\mathrm{A}$.

Si M est un A-module, et si $a \in \mathrm{A}$, on note $a\mathrm{M} \subset \mathrm{M}$ l'image du morphisme $x \mapsto ax$ de A-modules. C'est un sous-A-module de M, et le quotient $\mathrm{M}/a\mathrm{M}$ est, par construction, tué par a ; l'action de A sur $\mathrm{M}/a\mathrm{M}$ se factorise donc à travers A/a, ce qui fait de $\mathrm{M}/a\mathrm{M}$ un A/a-module. En particulier, si $p \in \mathscr{P}_\mathrm{A}$, alors $\mathrm{M}/p\mathrm{M}$ est un espace vectoriel sur le corps A/p.

Théorème 10.13. — *Soit* M *un* A*-module de torsion et de type fini. Si* $p \in \mathscr{P}_\mathrm{A}$*, soit* M_p *l'ensemble des* $x \in \mathrm{M}$ *tués par une puissance de* p*.*

(i) M_p *est un sous-*A*-module de* M*, nul sauf pour un nombre fini de* p*, et* $\mathrm{M} = \oplus_{p \in \mathscr{P}_\mathrm{A}} \mathrm{M}_p$*.*

(ii) *Si* $r_p = \dim_{\mathrm{A}/p}(\mathrm{M}/p\mathrm{M})$*, alors il existe une unique famille décroissante d'entiers* $a_{p,i} \geqslant 1$*, pour* $1 \leqslant i \leqslant r_p$*, telle que* $\mathrm{M}_p = \oplus_{1 \leqslant i \leqslant r_p} \mathrm{A}/p^{a_{p,i}}$*.*

Si $p^a x = 0$ et $p^b y = 0$, alors $p^{\sup(a,b)}(\lambda x + \mu y) = 0$ quels que soient $\lambda, \mu \in \mathrm{A}$. On en déduit que M_p est un sous-A-module de M.

Soient $x_1, \ldots, x_d$ engendrant M. Si $i \in \{1, \ldots, d\}$, soit $\lambda_i \in \mathrm{A}$ tel que $\lambda_i x_i = 0$, et soit $\lambda = \lambda_1 \cdots \lambda_d$. On a $\lambda x = 0$ quel que soit $x \in \mathrm{M}$. Si $p \in \mathscr{P}_\mathrm{A}$ ne divise pas λ, et si $x \in \mathrm{M}_p$ est tué par p^a, alors x est tué par tout élément de l'idéal (λ, p^a) de A engendré par λ et p^a, c'est-à-dire par A, puisque λ et p^a sont premiers entre eux. On a donc $x = 0$, et $\mathrm{M}_p = 0$ si p ne divise pas λ.

Soit $\mathscr{P}_\mathrm{A}(\lambda) \subset \mathscr{P}_\mathrm{A}$ l'ensemble des diviseurs premiers de λ, et soit $\lambda = \prod_{p \in \mathscr{P}_\mathrm{A}(\lambda)} p^{n_p}$ la factorisation de λ en facteurs premiers. Les $\frac{\lambda}{p^{n_p}}$, pour $p \in \mathscr{P}_\mathrm{A}(\lambda)$ sont premiers entre eux dans

77. Cela dit, pour étudier une telle suite, il vaut mieux considérer la série génératrice $\sum_{n=0}^{+\infty} u_n \mathrm{T}^n$, la multiplier par $1 - a_1\mathrm{T} - \cdots - a_d\mathrm{T}^d$ pour obtenir un polynôme P, et décomposer la fraction rationnelle $\frac{\mathrm{P}}{1 - a_1\mathrm{T} - \cdots - a_d\mathrm{T}^d}$ en éléments simples.

leur ensemble. Il existe donc, d'après le théorème de Bézout, des éléments α_p de A tels que l'on ait $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)}\alpha_p\frac{\lambda}{p^{n_p}}=1$. On en déduit que l'on peut décomposer tout élément x de M sous la forme $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)}x_p$, avec $x_p=\frac{\alpha_p\lambda}{p^{n_p}}x$, et $x_p\in\mathrm{M}_p$ car x_p est tué par p^{n_p}. En résumé, $\mathrm{M}=\sum_{p\in\mathscr{P}}\mathrm{M}_p$.

Enfin, si $x_p\in\mathrm{M}_p$, pour $p\in\mathscr{P}_{\mathrm{A}}(\lambda)$, et si $\sum_{p\in\mathscr{P}_{\mathrm{A}}(\lambda)}x_p=0$, alors $x_p=-\sum_{\ell\neq p}x_\ell$ est à la fois tué par p^{n_p} et par $p^{-n_p}\lambda$, qui sont premiers entre eux par définition de n_p. On a donc $x_p=0$ quel que soit p, ce qui termine de démontrer le (i).

Passons à la démonstration du (ii). Commençons par montrer que l'on peut calculer r_p en ne considérant que M_p. Si $\ell\in\mathscr{P}_{\mathrm{A}}$ est distinct de p, la multiplication par p induit une surjection sur M_ℓ : en effet, il existe n tel que $\ell^n\mathrm{M}_\ell=0$, et comme p et ℓ^n sont premiers entre eux, il existe $a,b\in\mathrm{A}$ tels que $ap+b\ell^n=1$. Les multiplications par a et p sont inverses l'une de l'autre sur M_ℓ, et donc $\mathrm{M}_\ell/p\mathrm{M}_\ell=0$. Il en résulte que r_p est aussi la dimension de $\mathrm{M}_p/p\mathrm{M}_p$ sur A/p.

La démonstration du (ii) va se faire en deux étapes. On commence par démontrer, par récurrence sur $r=r_p$ (le cas $r=0$ étant vide), l'existence d'une décomposition sous la forme voulue, puis on démontre, toujours par récurrence, l'unicité de la famille $a_{p,i}$.

Si $x\in\mathrm{M}_p$, on note $n(x)$ le plus petit $n\in\mathbf{N}$ tel que $p^nx=0$. Donc $p^{n(x)}x=0$ et $p^{n(x)-1}x\neq0$, si $n(x)\geqslant1$. Soient $e_1\in\mathrm{M}_p$ réalisant le maximum de $n(x)$, pour $x\in\mathrm{M}_p$ (comme $n(x)\leqslant n_p$, pour tout $x\in\mathrm{M}_p$, il existe un tel e_1), et $a_1=n(e_1)$. Soit $\mathrm{N}=\mathrm{M}_p/(\mathrm{A}/p^{a_1})e_1$. Alors $\mathrm{N}/p\mathrm{N}$ est, d'après le lemme 10.14 ci-dessous (avec $\mathrm{M}=\mathrm{M}_p$, $\mathrm{M}'=p\mathrm{M}_p$ et $\mathrm{M}''=(\mathrm{A}/p^{a_1})e_1$), le quotient de $\mathrm{M}_p/p\mathrm{M}_p$ par le sous-(A/p)-espace vectoriel engendré par l'image de e_1, et comme cette image est non nulle (sinon, on aurait $e_1=pf$ et $n(f)=n(e_1)+1>n(e_1)$), on en déduit que $\dim_{\mathrm{A}/p}(\mathrm{N}/p\mathrm{N})=r-1$, ce qui permet d'appliquer l'hypothèse de récurrence à N. Il existe donc $\overline{e}_2,\dots,\overline{e}_r\in\mathrm{N}$ et $a_2\geqslant\cdots\geqslant a_r$ tels que $\mathrm{N}=\oplus_{2\leqslant i\leqslant r}(\mathrm{A}/p^{a_i})\overline{e}_i$.

Soit $e_i'\in\mathrm{M}_p$ un relèvement quelconque de $\overline{e}_i$. On a alors $p^{a_i}e_i'=b_ie_1$, avec $b_i\in\mathrm{A}$, bien défini modulo p^{a_1}. Comme $p^{a_1}e_i'=0$, on en déduit que $p^{a_1-a_i}b_i\in p^{a_1}\mathrm{A}$, et donc que $b_i\in p^{a_i}\mathrm{A}$. Soit $c_i=p^{-a_i}b_i\in\mathrm{A}$, et soit $e_i=e_i'-c_ie_1$. On a alors $p^{a_i}e_i=0$. Maintenant, soit $x\in\mathrm{M}_p$, et soit $\overline{x}$ son image dans N. Il existe alors $\lambda_2\in\mathrm{A}/p^{a_2},\dots,\lambda_r\in\mathrm{A}/p^{a_r}$, uniques, tels que $\overline{x}=\lambda_2\overline{e}_2+\cdots+\lambda_r\overline{e}_r$. Comme $p^{a_i}e_i=0$, l'élément λ_ie_i de M_p est bien défini, et $x-\sum_{i=2}^r\lambda_ie_i\in(\mathrm{A}/p^{a_1})e_1$, et donc $\mathrm{M}_p=(\mathrm{A}/p^{a_1})e_1+\big((\mathrm{A}/p^{a_2})e_2\oplus\cdots\oplus(\mathrm{A}/p^{a_r})e_r\big)$. De plus, $(\mathrm{A}/p^{a_1})e_1\cap\big((\mathrm{A}/p^{a_2})e_2\oplus\cdots\oplus(\mathrm{A}/p^{a_r})e_r\big)=0$ car un élément de l'intersection a une image nulle dans N, et que $x\mapsto\overline{x}$ induit une bijection de $(\mathrm{A}/p^{a_2})e_2\oplus\cdots\oplus(\mathrm{A}/p^{a_r})e_r$ sur N. Il en résulte que $\mathrm{M}_p=(\mathrm{A}/p^{a_1})e_1\oplus(\mathrm{A}/p^{a_2})e_2\oplus\cdots\oplus(\mathrm{A}/p^{a_r})e_r$. Comme $a_1\geqslant a_2$, cela fournit une décomposition de M_p sous la forme voulue.

Il reste l'unicité des $a_{p,i}$. Supposons que $\mathrm{M}_p=\oplus_{1\leqslant i\leqslant r}(\mathrm{A}/p^{a_i})e_i=\oplus_{1\leqslant j\leqslant s}(\mathrm{A}/p^{b_j})f_j$, avec $a_1\geqslant a_2\geqslant\cdots a_r\geqslant1$ et $b_1\geqslant b_2\geqslant\cdots\geqslant b_s\geqslant1$. Soit $n(\mathrm{M}_p)$ le maximum des $n(x)$, pour $x\in\mathrm{M}_p$. Alors $n(\mathrm{M}_p)=a_1$ et $n(\mathrm{M}_p)=b_1$, et donc $a_1=b_1$. Maintenant, on peut écrire e_1 sous la forme $e_1=\sum_{j=1}^s\lambda_jf_j$, et comme $p^{a_1-1}e_1\neq0$, cela implique qu'il existe j tel que $p^{a_1-1}\lambda_jf_j\neq0$. En particulier, on a $p^{a_1-1}f_j\neq0$, ce qui prouve que $b_j\geqslant a_1=b_1$ et donc que $b_j=b_1$. Quitte à permuter les f_j, on peut donc supposer $j=1$. La propriété $p^{a_1-1}\lambda_1f_1\neq0$ implique alors (car $a_1=b_1$) que $\lambda_1\notin p\mathrm{A}$, et donc que λ_1 est premier à p et p^{a_1}, et est inversible dans $\mathrm{A}/p^{a_1}\mathrm{A}$. En notant μ_1 son inverse, cela permet d'écrire f_1 sous la forme $\mu_1e_1-\sum_{j=2}^s\mu_1\lambda_jf_j$, ce qui prouve que l'on a aussi $\mathrm{M}_p=(\mathrm{A}/p^{b_1})e_1\oplus_{2\leqslant j\leqslant s}(\mathrm{A}/p^{b_j})f_j$. On en déduit que $\mathrm{M}_p/(\mathrm{A}/p^{b_1})e_1=\oplus_{2\leqslant i\leqslant r}(\mathrm{A}/p^{a_i})e_i=\oplus_{2\leqslant j\leqslant s}(\mathrm{A}/p^{b_j})f_j$, et une récurrence

immédiate permet d'en conclure que l'on a $a_i = b_i$ quel que soit i (et donc aussi que $r = s$). Ceci termine la démonstration.

Lemme 10.14. — *Soient* M *un* A*-module, et* M', M'' *deux sous-modules de* M*. Alors :*

(i) $M' + M'' = \{x + y,\ x \in M',\ y \in M''\}$ *est un sous-module de* M *;*

(ii) *l'image de* M' *dans* M/M'' *est*[78] $M'/(M' \cap M'')$ *et celle de* M'' *dans* M/M' *est* $M''/(M' \cap M'')$ *;*

(iii) *les* A*-modules* $(M/M'')/(M'/(M' \cap M''))$ *et* $(M/M')/(M''/(M' \cap M''))$ *sont naturellement isomorphes à* $M/(M' + M'')$ *; en particulier, ils sont isomorphes entre eux.*

Le (i) est immédiat. Maintenant, la composée de l'injection de M' dans M avec la projection de M sur M/M'' fournit un morphisme de A-modules dont le noyau est $M' \cap M''$; l'image est donc isomorphe à $M'/(M' \cap M'')$. L'argument étant le même dans l'autre cas, en inversant les rôles de M' et M'', cela démontre le (ii).

Enfin, l'application naturelle de M' dans $(M' + M'')/M''$ est surjective (si $x \in M'$ et $y \in M''$, alors l'image de $x + y$ est aussi celle de x), et son noyau est $M' \cap M''$. L'image de M' dans M/M'' est donc aussi $(M' + M'')/M''$, ce qui fait que

$$(M/M'')/(M'/(M' \cap M'')) = (M/M'')/((M' + M'')/M'') = M/(M' + M'').$$

(Le noyau de la projection de M sur $M/(M' + M'')$ contient M' et donc cette projection se factorise à travers M/M' ; comme l'application induite est surjective et que son noyau est $(M' + M'')/M''$, cela fournit l'isomorphisme $(M/M'')/((M' + M'')/M'') = M/(M' + M'')$ ci-dessus.) On en déduit le (iii).

Exercice 10.15. — Soit G un groupe, et soient G', G'' deux sous-groupes distingués de G.

(i) Montrer que $G' \cap G''$ et $G'G'' = \{xy,\ x \in G'\ y \in G''\}$ sont des sous-groupes distingués de G.

(ii) Montrer que $(G/G')/(G''/(G' \cap G''))$ et $(G/G'')/(G'/(G' \cap G''))$ sont isomorphes. (On pourra les comparer à $G/(G'G'')$.)

10.4. Modules sur les anneaux principaux

On continue à supposer que A est un anneau principal. Nous allons étendre le théorème de structure aux A-modules de type fini pas nécessairement de torsion. Un tel module M peut se décomposer sous la forme (cf. alinéa 10.4.3), $M = A^r \oplus M_{\text{tors}}$, où M_{tors} est l'ensemble des éléments de torsion de M, et est un module de type fini et de torsion (on peut donc utiliser le th. 10.13 pour le décrire), et r est le *rang* de M. En particulier, un groupe commutatif de type fini M peut se décomposer sous la forme $M = \mathbf{Z}^r \oplus M_{\text{tors}}$, où M_{tors} est un groupe fini (cf. ex. 10.1).

10.4.1. *Opérations matricielles*

Si $M \in \mathbf{M}_{n\times m}(A)$, et si $j \leqslant \inf(n, m)$, on note $I_j(M)$ l'idéal de A engendré par les mineurs d'ordre j de M.

• $I_j(UMV) = I_j(M)$, si $U \in \mathbf{GL}_n(A)$ et $V \in \mathbf{GL}_m(A)$.

78. Plus exactement : « est naturellement isomorphe à »

Il suffit de prouver que l'idéal engendré par les mineurs d'ordre j ne change pas si on multiplie M à gauche ou à droite par une matrice inversible, et il suffit de traiter l'un des deux cas, l'autre s'en déduisant par passage à la transposée. Une colonne de MV est une combinaison linéaire à coefficients dans A des colonnes de M. Il s'ensuit qu'un mineur de MV, vu comme une forme alternée sur les colonnes de MV, est une combinaison linéaire, à coefficients dans A, de mineurs de M, et donc que $\mathrm{I}_j(\mathrm{MV}) \subset \mathrm{I}_j(\mathrm{M})$. Si V est inversible, on peut appliquer ce qui précède à MV et V^{-1} au lieu de M et V pour en déduire l'inclusion dans l'autre sens. On en déduit le résultat.

Si $s = \inf(n, m)$, on note $\mathrm{Diag}(\delta_1, \ldots, \delta_s)$ la matrice $(a_{i,j}) \in \mathbf{M}_{n\times m}(\mathrm{A})$ définie par $a_{i,i} = \delta_i$, si $i \leqslant s$, et $a_{i,j} = 0$ si $i \neq j$ (si $n = m$, les matrices de ce type sont exactement les matrices diagonales).

• Soit $\mathrm{M} \in \mathbf{M}_{n\times m}(\mathrm{A})$.

◇ Il existe $\delta_1, \ldots, \delta_s$, uniquement déterminés à multiplication près par des unités de A, tels que $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_s$ et $\mathrm{I}_1(\mathrm{M}) = (\delta_1)$, $\mathrm{I}_2(\mathrm{M}) = (\delta_1\delta_2)$,... (les δ_j sont les *diviseurs élémentaires de* M).

◇ Il existe $\mathrm{U} \in \mathbf{GL}_n(\mathrm{A})$ et $\mathrm{V} \in \mathbf{GL}_m(\mathrm{A})$ telles que $\mathrm{UMV} = \mathrm{Diag}(\delta_1, \ldots, \delta_s)$.

Remarquons que $\mathrm{I}_j(\mathrm{Diag}(\delta_1, \ldots, \delta_s)) = (\delta_1 \cdots \delta_j)$, si $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_s$. Le premier point résulte donc du second et du résultat précédent.

Passons à la démonstration du second point. On peut faire agir $\mathrm{G} = \mathbf{GL}_n(\mathrm{A}) \times \mathbf{GL}_m(\mathrm{A})$ sur $\mathbf{M}_{n\times m}(\mathrm{A})$ par $(\mathrm{U}, \mathrm{V}) \cdot \mathrm{M} = \mathrm{UMV}^{-1}$. L'énoncé à démontrer peut alors se paraphraser sous la forme : dans l'orbite de M sous l'action de G (cette orbite est l'ensemble des UMV^{-1} pour $(\mathrm{U}, \mathrm{V}) \in \mathrm{G}$, et donc aussi celui des UMV, puisque $(\mathrm{U}, \mathrm{V}^{-1}) \in \mathrm{G}$ si $(\mathrm{U}, \mathrm{V}) \in \mathrm{G}$), il existe une matrice $\mathrm{Diag}(\delta_1, \ldots, \delta_s)$, avec $\delta_1 \mid \cdots \mid \delta_s$. Nous allons démontrer [79] l'existence de M_0 par récurrence sur s, le cas $s = 0$ étant vide.

Si $\mathrm{M} = (a_{i,j}) \in \mathbf{M}_{n\times m}(\mathrm{A})$, on note $\delta(\mathrm{M})$ le pgcd des $a_{i,j}$ (c'est un générateur de $\mathrm{I}_1(\mathrm{M})$). Notons que $\delta(\mathrm{UMV}) = \delta(\mathrm{M})$ si $\mathrm{U} \in \mathbf{GL}_n(\mathrm{A})$ et $\mathrm{V} \in \mathbf{GL}_m(\mathrm{A})$, puisque $\mathrm{I}_1(\mathrm{UMV}) = \mathrm{I}_1(\mathrm{M})$.

Si $a \in \mathrm{A} - \{0\}$, notons $\ell(a)$ la *longueur* de a, i.e. le nombre de facteurs premiers de a, comptés avec multiplicité (par exemple, si $\mathrm{A} = \mathbf{Z}$, et $a = -120 = -2^3 \cdot 3 \cdot 5$, on a $\ell(a) = 3 + 1 + 1 = 5$). Si $\mathrm{M} = (a_{i,j}) \in \mathbf{M}_{n\times m}(\mathrm{A})$, on note $\ell(\mathrm{M})$ le minimum des $\ell(a_{i,j})$, et on choisit un couple (i, j) tel que $\ell(a_{i,j}) = \ell(\mathrm{M})$. Quitte à multiplier M à droite et à gauche par des matrices de permutation, ce qui fournit un élément de l'orbite de M, on peut supposer que $(i, j) = (1, 1)$, et donc que $\ell(a_{1,1}) = \inf_{i,j} \ell(a_{i,j})$. Comme $\delta(\mathrm{M})$ divise $a_{1,1}$, on a $\ell(a_{1,1}) \geqslant \ell(\delta(\mathrm{M}))$ et il y a deux cas :

◇ $\ell(a_{1,1}) = \ell(\delta(\mathrm{M}))$, ce qui signifie que $a_{1,1} = \alpha\delta(\mathrm{M})$, où α est une unité dans A, et donc que $a_{1,1}$ divise $a_{i,j}$ pour tout (i, j). On peut alors écrire M, par blocs, sous la forme

79. La démonstration fournit une construction algorithmique de U, V et M_0, à condition de savoir vraiment exprimer le pgcd d de deux éléments a et b de A sous la forme $d = au + bv$; si A est euclidien, on peut utiliser l'algorithme d'Euclide pour ce faire. On peut même combiner les deux algorithmes en essayant de minimiser le minimum de la taille des coefficients de UMV au lieu de leur longueur ; cela permet de montrer que l'on peut imposer à U et V d'être des produits de matrices ayant des 1 sur la diagonale, et un seul coefficient non diagonal non nul. Le résultat est que l'on peut parfaitement, de nos jours, demander à un ordinateur de calculer les diviseurs élémentaires d'un sous-$\mathbf{Z}$-module de $\mathbf{Z}^n$ ou d'un sous-K[X]-module de $(\mathrm{K}[\mathrm{X}])^n$.

$\left(\begin{smallmatrix}\alpha\delta(\mathrm{M}) & \alpha\delta(\mathrm{M})v\\ \alpha\delta(\mathrm{M})u & \delta(\mathrm{M})\mathrm{M}'\end{smallmatrix}\right)$, avec $u \in \mathbf{M}_{(n-1)\times 1}(\mathrm{A})$, $v \in \mathbf{M}_{1\times(m-1)}(\mathrm{A})$ et $\mathrm{M}' \in \mathbf{M}_{(n-1)\times(m-1)}(\mathrm{A})$. Soient $\mathrm{U}_0 = \left(\begin{smallmatrix}\alpha^{-1} & 0\\ -u & 1_{n-1}\end{smallmatrix}\right)$ et $\mathrm{V}_0 = \left(\begin{smallmatrix}1 & -v\\ 0 & 1_{m-1}\end{smallmatrix}\right)$; alors $\mathrm{U}_0\mathrm{M}\mathrm{V}_0 = \left(\begin{smallmatrix}1 & 0\\ 0 & \delta(\mathrm{M})\mathrm{M}'_0\end{smallmatrix}\right)$. Maintenant, on peut appliquer l'hypothèse de récurrence à M'_0 et trouver $\mathrm{U}' \in \mathbf{GL}_{n-1}(\mathrm{A})$ et $\mathrm{V}' \in \mathbf{GL}_{m-1}(\mathrm{A})$ tels que $\mathrm{U}'\mathrm{M}'_0\mathrm{V}' = \mathrm{Diag}(\delta'_1, \dots, \delta'_{s-1})$, avec $\delta'_1 \mid \cdots \mid \delta'_{s-1}$. Si $\mathrm{U} = \left(\begin{smallmatrix}1 & 0\\ 0 & \mathrm{U}'\end{smallmatrix}\right)$ et $\mathrm{V} = \left(\begin{smallmatrix}1 & 0\\ 0 & \mathrm{V}'\end{smallmatrix}\right)$, alors $\mathrm{U}\mathrm{U}_0\mathrm{M}\mathrm{V}_0\mathrm{V} = \left(\begin{smallmatrix}\delta(\mathrm{M}) & 0\\ 0 & \delta(\mathrm{M})\mathrm{U}'\mathrm{M}'_0\mathrm{V}'\end{smallmatrix}\right) = \mathrm{Diag}(\delta(\mathrm{M}), \delta(\mathrm{M})\delta'_1, \dots, \delta(\mathrm{M})\delta'_{s-1})$ est de la forme voulue.

◇ $\ell(a_{1,1}) > \ell(\delta(\mathrm{M}))$. Dans ce cas, nous allons construire $\mathrm{U} \in \mathbf{GL}_n(\mathrm{A})$ et $\mathrm{V} \in \mathbf{GL}_m(\mathrm{A})$ tels que $\ell(\mathrm{UMV}) < \ell(\mathrm{M})$, ce qui nous permettra de recommencer en partant de UMV au lieu de M. Comme $\ell(\mathrm{M})$ ne peut pas baisser indéfiniment, au bout d'un nombre fini d'étapes, on se retrouve dans le cas $\ell(\mathrm{M}) = \ell(\delta(\mathrm{M}))$, ce qui permet de conclure d'après ce qui précède. L'hypothèse $\ell(a_{1,1}) > \ell(\delta(\mathrm{M}))$ implique qu'il existe $a_{i,j}$ tel que $\ell(\mathrm{pgcd}(a_{1,1}, a_{i,j})) < \ell(a_{1,1})$ [sinon $a_{1,1}$ diviserait $a_{i,j}$ pour tout (i,j), et on aurait $a_{1,1} \mid \delta(\mathrm{M})$ et $\ell(a_{1,1}) \leqslant \ell(\delta(\mathrm{M}))$]. Il y a trois cas :

◇ Il existe j tel que $a_{1,1}$ ne divise pas $a_{1,j}$. Quitte à multiplier par une matrice de permutation à droite, on peut supposer $j = 2$. D'après le théorème de Bézout, il existe alors $u, v \in \mathrm{A}$ tels que $ua_{1,1} + va_{1,2} = \alpha$, si $\alpha = \mathrm{pgcd}(a_{1,1}, a_{1,j})$ (on a donc $\ell(\alpha) < \ell(\mathrm{M})$). Soit V la matrice par blocs $\left(\begin{smallmatrix}\mathrm{V}' & 0\\ 0 & 1_{m-2}\end{smallmatrix}\right)$, avec $\mathrm{V}' = \left(\begin{smallmatrix}u & -(a_{1,2}/\alpha)\\ v & a_{1,1}/\alpha\end{smallmatrix}\right)$. Alors V' est à coefficients dans A puisque α divise $a_{1,1}$ et $a_{1,2}$ et son déterminant vaut 1. Il en résulte que $\mathrm{V} \in \mathbf{GL}_m(\mathrm{A})$ (et même $\mathrm{V} \in \mathbf{SL}_n(\mathrm{A})$). Par ailleurs, si $\mathrm{MV} = (b_{i,j})$, on a $b_{1,1} = ua_{1,1} + va_{1,2} = \alpha$, et donc $\ell(\mathrm{MV}) < \ell(\mathrm{M})$, ce que l'on cherchait.

◇ Il existe j tel que $a_{1,1}$ ne divise pas $a_{j,1}$. Ce cas se ramène au précédent en prenant les transposées.

◇ $a_{1,1}$ divise $a_{1,j}$ et $a_{j,1}$ pour tous j. Auquel cas, on peut trouver U et V inversibles tels que UMV soit une matrice par blocs de la forme $\left(\begin{smallmatrix}a_{1,1} & 0\\ 0 & \mathrm{M}'\end{smallmatrix}\right)$ (cf. le cas $\ell(a_{1,1}) = \ell(\delta(\mathrm{M}))$). Quite à remplacer M par UMV, on peut donc supposer que $\mathrm{M} = \left(\begin{smallmatrix}a_{1,1} & 0\\ 0 & \mathrm{M}'\end{smallmatrix}\right)$. L'hypothèse $\ell(a_{1,1}) > \ell(\delta(\mathrm{M}))$ implique qu'il existe $a_{i,j}$ non divisible par $a_{1,1}$ et, quitte à multiplier M par des matrices de la forme $\left(\begin{smallmatrix}1 & 0\\ 0 & \mathrm{U}'\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}1 & 0\\ 0 & \mathrm{V}'\end{smallmatrix}\right)$, où U' et V' sont des matrices de permutation, on peut supposer que $a_{1,1}$ ne divise pas $a_{2,2}$. Comme ci-dessus, il existe $u, v \in \mathrm{A}$ tels que $\ell(ua_{1,1} + va_{2,2}) < \ell(a_{1,1})$. Or on a $\left(\begin{smallmatrix}1 & 0\\ u & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}a & 0\\ 0 & d\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ v & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}a & 0\\ au+dv & d\end{smallmatrix}\right)$; on en déduit que si U et V sont les matrices par blocs $\mathrm{U} = \left(\begin{smallmatrix}\mathrm{U}' & 0\\ 0 & 1_{n-2}\end{smallmatrix}\right)$ $\mathrm{V} = \left(\begin{smallmatrix}\mathrm{V}' & 0\\ 0 & 1_{m-2}\end{smallmatrix}\right)$, avec $\mathrm{U}' = \left(\begin{smallmatrix}1 & 0\\ u & 1\end{smallmatrix}\right)$ et $\mathrm{V}' = \left(\begin{smallmatrix}1 & 0\\ v & 1\end{smallmatrix}\right)$, alors UMV admet $ua_{1,1} + va_{2,2}$ parmi ses coefficients (2-ième ligne et 1-ère colonne) et donc que $\ell(\mathrm{UMV}) < \ell(\mathrm{M})$, ce que l'on cherchait à obtenir.

10.4.2. *Sous-modules de modules libres*

On note F le corps des fraction de A.

• Soit Λ un sous-A-module de A^n. Alors il existe une base $f_1, \dots, f_n$ de A^n sur A, un entier $r \leqslant n$, et des éléments $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_r$ non nuls de A tels que $\delta_1 f_1, \dots, \delta_r f_r$ soit une base de Λ sur A. De plus, r et $\delta_1, \dots, \delta_r$ sont déterminés de manière unique (r est appelé le *rang* du A-module Λ ; c'est la dimension du sous-F-espace vectoriel de F^n engendré par Λ).

Soit r la dimension du sous-F-espace vectoriel V de F^n engendré par Λ. Soit I l'idéal de A engendré par les mineurs d'ordre r de toutes les matrices $n \times m$, pour $m \geqslant r$, obtenues en écrivant m éléments de Λ dans la base canonique de A^n sur A. Comme A est noethérien, il existe une famille finie $(\mathrm{M}_j)_{j\in\mathrm{J}}$ de telles matrices dont les mineurs d'ordre r engendrent I,

et la matrice M obtenue en utilisant tous les éléments de Λ apparaissant dans les M_j a pour propriété que ses mineurs d'ordre r engendrent I.

D'après le point précédent, on peut trouver des matrices $U \in \mathbf{GL}_n(A)$ et $V \in \mathbf{GL}_m(A)$ telle que $UMV = \mathrm{Diag}(\delta_1, \ldots, \delta_s)$, avec $\delta_j = 0$ si $j \geqslant r+1$ et $(\delta_1 \cdots \delta_r) = I$. Or multiplier à droite par V revient à faire des combinaisons linéaires des colonnes de M, ce qui nous donne d'autres éléments de Λ, et multiplier à gauche par U revient à changer la base de A^n sur A dans laquelle on calcule les coordonnées des éléments de A^n. On a donc trouvé une base $f_1, \ldots, f_n$ de A^n sur A telle que $\delta_1 f_1, \ldots, \delta_r f_r$ appartiennent à Λ. De plus, si $x_1, \ldots, x_m \in \Lambda$, les mineurs d'ordre r de la matrice des x_j dans la base des f_i sont aussi ceux de UM', où M' est la matrice des x_j dans la base canonique de A^n, et comme $I_r(UM') = I_r(M')$, on déduit de la définition de I et de ce que $(\delta_1 \cdots \delta_r) = I$ que $\Delta = \delta_1 \ldots \delta_n$ divise tout mineur d'ordre r de la matrice des x_j dans la base des f_i. Montrons que ceci implique que $\delta_1 f_1, \ldots, \delta_r f_r$ est une base de Λ sur A, ce qui prouvera l'existence.

Comme $f_1, \ldots, f_r$ est libre sur F, il en est de même de $\delta_1 f_1, \ldots, \delta_r f_r$ qui est donc une base de V sur F, puisque V est de dimension r par définition de r. Si $x \in \Lambda$, on peut donc écrire x, de manière unique, sous la forme $\sum_{i=1}^{r} \lambda_i \delta_i f_i$, avec $\lambda_1, \ldots, \lambda_r \in F$, et on cherche à prouver que $\lambda_j \in A$, pour tout j. Les mineurs d'ordre r de la matrice dont les colonnes sont $\delta_1 f_1, \ldots, \delta_r f_r, x$ dans la base $f_1, \ldots, f_n$ appartiennent à A et sont divisibles par Δ d'après la discussion ci-dessus. En considérant le mineur obtenu en ne gardant que les r premières lignes en enlevant la j-ième colonne, on en déduit que $\Delta\lambda_j$ est divisible par Δ, ce qui prouve que $\lambda_j \in A$ pour tout j, et donc que $\delta_1 f_1, \ldots, \delta_r f_r$ engendrent Λ.

Ceci prouve l'existence. L'unicité se déduit de l'alinéa 10.4.3 appliqué à $M = A^n/\Lambda$.

• Un sous-A-module d'un A-module libre de rang fini est libre de rang plus petit.

C'est une paraphrase un peu appauvrie du point précédent.

Un sous-A-module de F^n est un *réseau* (ou un A-réseau) s'il est de type fini et s'il engendre F^n ; par exemple A^n est un réseau de F^n : c'est le *réseau standard.*

• Si Λ est un réseau de F^n, il existe une base $f_1, \ldots, f_n$ de A^n sur A et $\delta_1, \ldots, \delta_n \in F^*$, tels que $\delta_1 f_1, \ldots, \delta_n f_n$ soit une base de Λ sur A ; en particulier, un réseau Λ de F^n est libre de rang n sur A et une base de Λ sur A est aussi une base de F^n sur F.

Soient $x_1, \ldots, x_m$ engendrant Λ sur A. Il existe alors $b_i \in A - \{0\}$ tel que $b_i x_i \in A^n$ [si $x_i = \sum_{j=1}^{n} \frac{a_{i,j}}{b_{i,j}} e_j$, on peut prendre $b_i = \prod_{j=1}^{n} b_{i,j}$], et on a donc $bx_i \in A^n$ pour tout i, si $b = \prod_{i=1}^{m} b_i$. Il s'ensuit que $b\Lambda$ est un sous-A-module de A^n, et comme il engendre F^n, il est de rang n et il existe une base $f_1, \ldots, f_n$ de A^n sur A et $\delta'_1, \ldots, \delta'_n \in A$, tels que $\delta'_1 f_1, \ldots, \delta'_n f_n$ soit une base de $b\Lambda$ sur A. Alors $b^{-1}\delta'_1 f_1, \ldots, b^{-1}\delta'_n f_n$ est une base de Λ sur A.

• Si Λ_1, Λ_2 sont des réseaux de F^n avec $\Lambda_1 \subset \Lambda_2$, il existe une base $f_1, \ldots, f_n$ de Λ_2 sur A et $\delta_1, \ldots, \delta_n \in A$, tels que $\delta_1 f_1, \ldots, \delta_n f_n$ soit une base de Λ_1 sur A.

D'après le point précédent, Λ_2 est libre de rang n sur A et le choix d'une base permet de se ramener au cas $\Lambda_2 = A^n$ qui découle de ce qui précède.

Exercice 10.16. — Soient $n \geqslant 2$ et $a_1, \ldots, a_n \in \mathbf{Z}$, premiers entre eux dans leur ensemble. Montrer qu'il existe $A \in \mathbf{SL}_n(\mathbf{Z})$ dont la première colonne est ${}^t(a_1, \ldots, a_n)$.

10.4.3. *Modules de type fini*

• Si M est un A-module de type fini, il existe $r \in \mathbf{N}$, $\delta_1, \dots, \delta_s \in \mathrm{A}$, avec $\delta_1 \notin \mathrm{A}^*$ et $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_s$, tels que $\mathrm{M} \cong \mathrm{A}^r \oplus \mathrm{A}/\delta_1 \oplus \cdots \oplus \mathrm{A}/\delta_s$. De plus, r et les idéaux $(\delta_1), \dots, (\delta_s)$ sont uniquement déterminés.

Soient $x_1, \dots, x_n$ une famille génératrice de M. On dispose donc d'un morphisme surjectif $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i x_i$ de A-modules de A^n sur M. Notons Λ le noyau, de telle sorte que $\mathrm{M} \cong \mathrm{A}^n/\Lambda$. D'après l'alinéa précédent, il existe une base $f_1, \cdots, f_n$ de A^n, et des éléments $\delta'_1, \dots, \delta'_t$ de A, avec $\delta'_1 \mid \cdots \mid \delta'_t$, tels que $\delta'_1 f_1, \dots, \delta'_t f_t$ soit une base de Λ sur A. Alors $\mathrm{M} \cong \mathrm{A}/\delta'_1 \oplus \cdots \oplus \mathrm{A}/\delta'_t \oplus \mathrm{A}^{n-t}$, et on en déduit l'existence avec $r = n - t$, en supprimant les δ'_i qui sont des unités.

Passons à l'unicité. On est ramené à prouver que si l'on dispose d'isomorphismes de A-modules $\mathrm{M} \cong \mathrm{A}^n \oplus \mathrm{A}/(\delta_1) \oplus \cdots \oplus \mathrm{A}/(\delta_s)$ et $\mathrm{M} \cong \mathrm{A}^m \oplus \mathrm{A}/(\delta'_1) \oplus \cdots \oplus \mathrm{A}/(\delta'_{s'})$, où $r, r' \in \mathbf{N}$, et $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_s$ et $\delta'_1 \mid \delta'_2 \mid \cdots \mid \delta'_{s'}$, alors $n = m$, $s = s'$, et $(\delta_i) = (\delta'_i)$ pour tout $i \leqslant s$. Commençons par constater que $\mathrm{A}/(\delta_1) \oplus \cdots \oplus \mathrm{A}/(\delta_s)$ et $\mathrm{A}/(\delta'_1) \oplus \cdots \oplus \mathrm{A}/(\delta'_{s'})$ sont isomorphes au sous-A-module $\mathrm{M}_{\mathrm{tors}}$ de M. Les isomorphismes ci-dessus induisent donc un isomorphisme $\mathrm{A}^n \cong \mathrm{M}/\mathrm{M}_{\mathrm{tors}} \cong \mathrm{A}^m$, et donc $n = m$.

On est donc ramené au cas où $\mathrm{M} = \mathrm{M}_{\mathrm{tors}}$ et $n = m = 0$. Si $p \in \mathscr{P}_{\mathrm{A}}$, soit $a_{p,i} = v_p(\delta_{s-i})$ et $b_{p,i} = v_p(\delta'_{s'-i})$. Alors $a_{p,i} \geqslant a_{p,i+1}$ puisque $\delta_{s-i-1} \mid \delta_{s-i}$ et $b_{p,i} \geqslant b_{p,i+1}$ puisque $\delta'_{s'-i-1} \mid \delta'_{s'-i}$. D'après le th. des restes chinois, on a $\mathrm{A}/(\delta_{s-i}) \cong \oplus_{p \in \mathscr{P}_{\mathrm{A}}} \mathrm{A}/p^{a_{p,i}}$ et $\mathrm{A}/(\delta'_{s'-i}) \cong \oplus_{p \in \mathscr{P}_{\mathrm{A}}} \mathrm{A}/p^{b_{p,i}}$, et on déduit de l'unicité dans le th. 10.13 que $a_{p,i} = b_{p,i}$ pour tous p, i, ce qui prouve que $(\delta_{s-i}) = (\delta_{s'-i})$ pour tout i, et donc que $s = s'$ et $(\delta_i) = (\delta'_i)$ pour tout i.

• Si $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$, le K[X]-module correspondant à K^n muni de l'endomorphisme u_{A} est le quotient M de $(\mathrm{K}[\mathrm{X}])^n$ par le sous-K[X]-module engendré par les $\mathrm{X}e_i - u_{\mathrm{A}}(e_i)$, où $e_1, \dots, e_n$ est la base canonique de K^n et $\mathrm{K}[\mathrm{X}]^n$. On peut donc utiliser l'algorithme décrit dans l'alinéa 10.4.1 pour mettre M sous une forme sympathique ou pour déterminer son polynôme minimal et son polynôme caractéristique.

L'application naturelle $\mathrm{K}^n \subset (\mathrm{K}[\mathrm{X}])^n \to \mathrm{M}$ est surjective car $\mathrm{X}^n e_i$ a même image que $u_{\mathrm{A}}^n(e_i)$, si $n \in \mathbf{N}$; elle est injective car $\sum_{i=1}^n \lambda_i e_i = \sum_{i=1}^n \mathrm{P}_i\,(\mathrm{X}e_i - u_{\mathrm{A}}(e_i))$ dans $(\mathrm{K}[\mathrm{X}])^n$ implique, en regardant les termes de plus haut degré, que les P_i sont nuls et donc aussi les λ_i ; elle est donc bijective, et on s'est débrouillé pour que la multiplication par X dans M correspondent à l'action de u_{A} sur K^n.

Maintenant, si $\mathrm{M} \cong (\mathrm{K}[\mathrm{X}]/\mathrm{P}_1) \oplus \cdots \oplus (\mathrm{K}[\mathrm{X}]/\mathrm{P}_n)$, avec $\mathrm{P}_1 \mid \cdots \mid \mathrm{P}_n$, le polynôme minimal de la multiplication par X est P_n et son polynôme caractéristique est $\mathrm{P}_1 \cdots \mathrm{P}_n$ (lemme 10.6).

10.5. Extension des scalaires

La réduction des endomorphismes est plus agréable sur un corps algébriquement clos ; on peut s'y ramener en étendant les scalaires : par exemple, un **R**-espace vectoriel peut se complexifier en un **C**-espace vectoriel.

10.5.1. *Complexification d'un espace vectoriel réel*

Si V est un **R**-espace vectoriel, on note $\mathrm{V}_{\mathbf{C}}$ le **R**-espace vectoriel $\mathrm{V} \oplus i\mathrm{V}$ (un élément de $\mathrm{V}_{\mathbf{C}}$ s'écrit de manière unique sous la forme $x + iy$, avec $x, y \in \mathrm{V}$) ; en particulier, V

est un sous-$\mathbf{R}$-espace vectoriel de $\mathrm{V}_{\mathbf{C}}$. On fait [80] de $\mathrm{V}_{\mathbf{C}}$ un $\mathbf{C}$-espace vectoriel en faisant agir $a+ib \in \mathbf{C}$ sur $\mathrm{V}_{\mathbf{C}}$ par la formule évidente $(a+ib)(x+iy) = (ax-by)+i(ay+bx)$; le $\mathbf{C}$-espace vectoriel ainsi obtenu est le *complexifié* du $\mathbf{R}$-espace vectoriel V.

• Si V est de dimension finie, et si $e_1, \ldots, e_n$ est une base de V sur $\mathbf{R}$, alors c'est aussi une base de $\mathrm{V}_{\mathbf{C}}$ sur $\mathbf{C}$.

On peut écrire tout élément de V, de manière unique, sous la forme $\sum_{i=k}^{n} x_k e_k$, avec $x_1, \ldots, x_n \in \mathbf{R}$, et donc on peut écrire tout élément de $\mathrm{V}_{\mathbf{C}} = \mathrm{V} \oplus i\mathrm{V}$, de manière unique, sous la forme $\sum_{i=k}^{n} x_k e_k + i\sum_{i=k}^{n} y_k e_k$, avec $x_1, \ldots, x_n, y_1, \ldots, y_k \in \mathbf{R}$, ce qui prouve que l'on peut écrire tout élément de $\mathrm{V}_{\mathbf{C}}$, de manière unique, sous la forme $\sum_{i=k}^{n} z_k e_k$, avec $z_k = x_k + iy_k \in \mathbf{C}$.

• $\mathrm{V}_{\mathbf{C}}$ vérifie la propriété universelle suivante : si $u : \mathrm{V} \to \mathrm{W}$ est $\mathbf{R}$-linéaire, et si W est un $\mathbf{C}$-espace vectoriel, alors il existe une unique application $\mathbf{C}$-linéaire $u_{\mathbf{C}} : \mathrm{V}_{\mathbf{C}} \to \mathrm{W}$ dont la restriction à V est u.

Si $u_{\mathrm{C}} : \mathrm{V}_{\mathbf{C}} \to \mathrm{W}$ est $\mathbf{C}$-linéaire et coïncide avec u sur V, alors $u_{\mathbf{C}}(x+iy) = u(x) + iu(y)$, si $x, y \in \mathrm{V}$; on en déduit l'unicité d'une application linéaire $u_{\mathbf{C}}$ étendant u à $\mathrm{V}_{\mathbf{C}}$. Maintenant, la formule $u_{\mathbf{C}}(x+iy) = u(x) + iu(y)$ définit une application de $\mathrm{V}_{\mathbf{C}}$ dans W qui est $\mathbf{R}$-linéaire de manière évidente ; sa $\mathbf{C}$-linéarité résulte du calcul suivant : $u_{\mathbf{C}}((a+ib)(c+iy)) = u_{\mathbf{C}}((ax-by)+i(ay+bx)) = u(ax-by)+iu(ay+bx) = (au(x)-bu(y))+i(au(y)+bu(x)) = (a+ib)(u(x)+iu(y)) = (a+ib)u_{\mathbf{C}}(x+iy)$. D'où l'existence.

Si $u : \mathrm{V}_1 \to \mathrm{V}_2$ est un morphisme de $\mathbf{R}$-espaces vectoriels, on peut composer u avec l'injection de V_2 dans $\mathrm{V}_{2,\mathbf{C}}$, et le point précédent implique que le résultat s'étend, de manière unique, en une application $\mathbf{C}$-linéaire $u_{\mathbf{C}} : \mathrm{V}_{1,\mathbf{C}} \to \mathrm{V}_{2,\mathbf{C}}$. Si V_1 et V_2 sont de dimension finies, si $e_1, \ldots, e_m$ est une base de V_1 sur $\mathbf{R}$ (et donc aussi une base de $\mathrm{V}_{1,\mathbf{C}}$ sur $\mathbf{C}$) et $f_1, \ldots, f_n$ est une base de V_2 (et donc aussi une base de $\mathrm{V}_{2,\mathbf{C}}$ sur $\mathbf{C}$), les matrices de u et $u_{\mathbf{C}}$ dans ces bases sont les mêmes puisque $u_{\mathbf{C}}(e_j) = u(e_j)$. En particulier, si $\mathrm{V}_1 = \mathrm{V}_2$, alors u et $u_{\mathbf{C}}$ ont le même polynôme caractéristique, et donc les mêmes valeurs propres (réelles).

• Si $u \in \mathrm{End}(\mathrm{V})$ n'a pas de valeur propre, u laisse stable un sous-espace de dimension 2.

Si u n'a pas de valeur propre, toutes les valeurs propres de $u_{\mathbf{C}}$ sont non réelles. Si $\lambda = a+ib$, avec $b \neq 0$, est une valeur propre non réelle de $u_{\mathbf{C}}$, et si $z = x+iy \in \mathrm{V}_{\mathbf{C}} - \{0\}$, avec $x, y \in \mathrm{V}$, est un vecteur propre de $u_{\mathbf{C}}$ pour la valeur propre λ, cela se traduit par $u(x) + iu(y) = (a+ib)(x+iy) = (ax-by)+i(ay+bx)$, et donc par $u(x) = ax-by$ et $u(y) = ay+bx$. De plus, x et y ne sont pas colinéaires car si $y = cx$, cela nous donne $u(x) = (a-bc)x$ et $cu(x) = (ac+b)x$, et donc $ac+b = ca-bc^2$, et $b = 0$. Il en résulte que le plan engendré par x et y est stable par u, et que la matrice de u dans la base x, y de ce plan est $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$.

• Si μ est une valeur propre de $u_{\mathbf{C}}$, alors $\overline{\mu}$ aussi et les multiplicités de μ et $\overline{\mu}$ sont les mêmes ; si $u_{\mathbf{C}}$ est diagonalisable et si ses valeurs propres (répétées avec multiplicité) sont $\lambda_1, \ldots, \lambda_r, \mu_1, \overline{\mu_1}, \ldots, \mu_s, \overline{\mu_s}$, où $\lambda_1, \ldots, \lambda_r$ sont réelles, et $\mu_j = a_j + ib_j$, avec $a_j, b_j \in \mathbf{R}$ et $b_j \neq 0$, alors il existe une base de V dans laquelle la matrice de u est la matrice diagonale par blocs $\mathrm{Diag}\big(\lambda_1, \ldots, \lambda_r, \left(\begin{smallmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix} a_s & b_s \\ -b_s & a_s \end{smallmatrix}\right)\big)$.

80. Nous laissons au lecteur le soin de vérifier que l'on obtient bien ainsi un $\mathbf{C}$-espace vectoriel.

Comme $\mathbf{C}$ est algébriquement clos, les valeurs propres de $u_{\mathbf{C}}$ (avec multiplicité) sont les racines de $\mathrm{Car}_{u_{\mathbf{C}}} = \mathrm{Car}_u$. Le premier énoncé résulte donc de ce que $\mathrm{Car}_u \in \mathbf{R}[\mathrm{X}]$.

On peut supposer que V est un $\mathbf{R}[\mathrm{X}]$-module de torsion, et que u est la multiplication par X, et le th. 10.3 nous fournit une décomposition $\mathrm{V} \cong \oplus_{\mathrm{P}\in\mathrm{Spec}\,u}\big(\oplus_{1\leqslant i\leqslant r_\mathrm{P}} \mathbf{R}[\mathrm{X}]/\mathrm{P}^{a_{\mathrm{P},i}}\big)$, où les P sont irréductibles (de degré 1 ou 2). Alors $\mathrm{V}_{\mathbf{C}} \cong \oplus_{\mathrm{P}\in\mathrm{Spec}\,u}\big(\oplus_{1\leqslant i\leqslant r_\mathrm{P}} \mathbf{C}[\mathrm{X}]/\mathrm{P}^{a_{\mathrm{P},i}}\big)$. Par ailleurs, $\mathbf{C}[\mathrm{X}]/\mathrm{P}^{a_{\mathrm{P},i}} \cong (\mathbf{C}[\mathrm{X}]/(\mathrm{X}-\mu)^{a_{\mathrm{P},i}}) \oplus (\mathbf{C}[\mathrm{X}]/(\mathrm{X}-\overline{\mu})^{a_{\mathrm{P},i}})$, d'après le th. des restes chinois, si $\mathrm{P} = (\mathrm{X}-\mu)(\mathrm{X}-\overline{\mu})$ et $\mu \neq \overline{\mu}$. L'hypothèse selon laquelle $u_{\mathbf{C}}$ est diagonalisable implique donc, d'après l'équivalence entre les (i) et (iv) du cor. 10.9, que les $a_{\mathrm{P},i}$ sont tous égaux à 1. On en déduit une décomposition $\mathrm{V} \cong \big(\oplus_{i=1}^{s}\mathbf{R}[\mathrm{X}]/(\mathrm{X}-\lambda_i)\big)\oplus\big(\oplus_{j=1}^{s}\mathbf{R}[\mathrm{X}]/(\mathrm{X}^2-2a_j\mathrm{X}+a_j^2+b_j^2)\big)$, et pour conclure il suffit de remarquer que dans la base $\mathrm{X}-a, b$ de $\mathbf{R}[\mathrm{X}]/(\mathrm{X}^2-2a\mathrm{X}+a^2+b^2)$, où $b \neq 0$, la matrice de la multiplication par X est $\left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right)$ car $\mathrm{X}\,(\mathrm{X}-a) = a(\mathrm{X}-a)-b\,b+(\mathrm{X}^2-2a\mathrm{X}+a^2+b^2)$ et $\mathrm{X}\,b = b(\mathrm{X}-a)+a\,b$.

10.5.2. *Extension des scalaires à un sur-corps*

Si $\mathrm{K} \subset \mathrm{L}$ sont des corps, et si V est un K-espace vectoriel, on peut transformer V en un L-espace vectoriel en étendant les scalaires de K à L (si $\mathrm{K} = \mathbf{R}$ et $\mathrm{L} = \mathbf{C}$, cette opération correspond à la complexification d'un espace vectoriel réel étudiée dans le n° précédent) ; le L-espace vectoriel V_L (noté aussi $\mathrm{L} \otimes_\mathrm{K} \mathrm{V}$) que l'on obtient est l'*extension des scalaires de* K *à* L de V ; il est caractérisé (à isomorphisme unique près) par la propriété universelle suivante : V est un sous-K-espace vectoriel de V_L engendrant V_L et, si $u : \mathrm{V} \to \mathrm{W}$ est une application K-linéaire de V dans un L-espace vecoriel W, il existe une unique application L-linéaire $u_\mathrm{L} : \mathrm{V}_\mathrm{L} \to \mathrm{W}$ dont la restriction à V est u.

Si V_L et V'_L sont deux extensions de scalaires de V, ce sont des en particulier des L-espaces vectoriels, et $\mathrm{id} : \mathrm{V} \to \mathrm{V}$ s'étend, de manière unique, en des applications L-linéaires $u : \mathrm{V}_\mathrm{L} \to \mathrm{V}'_\mathrm{L}$ et $u' : \mathrm{V}'_\mathrm{L} \to \mathrm{V}_\mathrm{L}$. Mais alors $u' \circ u : \mathrm{V}_\mathrm{L} \to \mathrm{V}_\mathrm{L}$ est une application L-linéaire dont la restriction à V est l'identité ; par unicité d'une telle application, on en déduit que $u' \circ u$ est l'identité de V_L. De même, $u \circ u'$ est l'identité de V_L, ce qui prouve que u et u' sont des isomorphismes inverses l'un de l'autre et donc que V_L est uniquement déterminé à isomorphisme unique près (s'il existe).

Il nous reste à construire V_L. Pour cela, partons du L-espace vectoriel $\mathrm{L}^{(\mathrm{V})}$ des applications de V dans L ne prenant qu'un nombre fini de valeurs non nulles. Si $x \in \mathrm{V}$, on note e_x l'élément de $\mathrm{L}^{(\mathrm{V})}$ défini par $e_x(x) = 1$ et $e_x(y) = 0$ pour tout $y \neq x$. Alors $(e_x)_{x\in\mathrm{V}}$ est une base de $\mathrm{L}^{(\mathrm{V})}$. On définit V_L comme le quotient de $\mathrm{L}^{(\mathrm{V})}$ par le sous-L-espace vectoriel R engendré par les $e_{x+y} - e_x - e_y$, pour $x, y \in \mathrm{V}$, et les $e_{\lambda x} - \lambda e_x$,pour $x \in \mathrm{V}$ et $\lambda \in \mathrm{K}$. Si $x \in \mathrm{V}$, on note $\iota_\mathrm{L}(x)$ l'image de e_x dans V_L. Alors ι_L est K-linéaire car on s'est débrouillé pour (on $e_{x+y}-e_x-e_y = 0$ et $e_{\lambda x}-\lambda e_x = 0$ dans V_L, si $x, y \in \mathrm{V}$ et $\lambda \in \mathrm{K}$). Par ailleurs ι_L est injective comme le montre le point suivant, ce qui permet d'identifier V à son image par ι_L dans V_L, et donc de considérer V comme un sous-K-espace vectoriel de V_L. Comme les e_x engendrent $\mathrm{L}^{(\mathrm{V})}$, leurs images engendrent V_L, et donc V engendre V_L. Enfin, si $u : \mathrm{V} \to \mathrm{W}$ est K-linéaire et W est un L-espace vectoriel, on définit une application L-linéaire $\tilde{u}_\mathrm{L} : \mathrm{L}^{(\mathrm{V})} \to \mathrm{W}$, en posant $\tilde{u}_\mathrm{L}(e_x) = u(x)$, si $x \in \mathrm{V}$ (une telle application existe et est unique car les e_x forment une base de $\mathrm{L}^{(\mathrm{V})}$). Alors $\tilde{u}_\mathrm{L}(e_{x+y} - e_x - e_y) = u(x + y) - u(x) - u(y) = 0$ et $\tilde{u}_\mathrm{L}(e_{\lambda x} - \lambda e_x) = u(\lambda x) - \lambda u(x) = 0$ pour tous $x, y \in \mathrm{V}$ et $\lambda \in \mathrm{K}$. Il s'ensuit que $\mathrm{R} \subset \mathrm{Ker}\,\tilde{u}_\mathrm{L}$, et donc que $\tilde{u}_\mathrm{L}$ se factorise à travers $\mathrm{L}^{(\mathrm{V})}/\mathrm{R} = \mathrm{V}_\mathrm{L}$, et l'application L-linéaire $u_\mathrm{L} : \mathrm{V}_\mathrm{L} \to \mathrm{W}$ ainsi obtenue coïncide avec u sur V par

construction. Comme V engendre V_L, il y au plus une telle application, ce qui prouve que V_L vérifie la propriété universelle demandée.

• Si $v_1, \dots, v_n \in K$ sont liés dans V_L (sur L), ils sont liés dans V (sur K) ; s'ils sont libres dans V (sur K), ils le sont dans V_L (sur L) ; si $(e_i)_{i\in I}$ est une base de V sur K, c'est aussi une base de V_L sur L.

Les deux premiers énoncés se déduisent l'un de l'autre par contraposée ; le troisième résulte du second puisqu'il implique que $(e_i)_{i\in I}$ est libre (sur L) dans V_L et comme, par ailleurs, $(e_i)_{i\in I}$ est une famille génératrice de V qui engendre V_L, c'est aussi une famille génératrice, et donc une base de V_L. Il suffit donc de prouver le premier énoncé.

Si $\sum_{i=1}^n x_i v_i = 0$ dans V_L, cela signifie que l'on dispose dans $L^{(V)}$ d'une relation du type

$$S = \sum_{i=1}^{n} x_i e_{v_i} - \Big(\sum_{x,y} \mu_{x,y}(e_{x+y} - e_x - e_y) + \sum_{\lambda,z} \nu_{\lambda,z}(e_{\lambda z} - \lambda e_z) \Big) = 0,$$

où les $\mu_{x,y}$ et $\nu_{\lambda,z}$ sont des éléments de L nuls sauf un nombre fini, les x, y, z sont des éléments de V et les λ des éléments de K. Le sous-K-espace vectoriel de L engendré par les x_i, les $\mu_{x,y}$ et les $\nu_{\lambda,z}$ est de dimension finie sur K ; choisissons en une base $f_1, \dots, f_r$. En décomposant les x_i, les $\mu_{x,y}$ et les $\nu_{\lambda,z}$ dans cette base, cela permet de mettre S sous la forme $S = \sum_{j=1}^r S^{(j)} f_j$, avec $S^{(j)} = \sum_{i=1}^n x_i^{(j)} e_{v_i} - \Big(\sum_{x,y} \mu_{x,y}^{(j)}(e_{x+y} - e_x - e_y) + \sum_{\lambda,z} \nu_{\lambda,z}^{(j)}(e_{\lambda z} - \lambda e_z) \Big) \in K^{(V)}$, et il suffit de prouver que $S = 0$ implique $S^{(1)} = \cdots = S^{(r)} = 0$ car cela implique que $\sum_{i=1}^n x_i^{(j)} v_i = 0$ dans V, pour tout j ; si les x_j n'étaient pas tous nuls, il existe un j tel que les $x_i^{(j)}$ ne sont pas tous nuls, ce qui prouve que $v_1, \dots, v_n$ sont liés dans V s'ils le sont dans V_L.

Soient donc $S^{(j)} = \sum_x \lambda_{j,x} e_x$, pour $1 \leqslant j \leqslant r$, des éléments de $K^{(V)}$ tels que $\sum_{j=1}^r f_j S^{(j)} = 0$ dans $L^{(V)}$. Alors $\sum_x (\sum_{j=1}^r \lambda_{j,x} f_j) e_x = 0$, et donc $\sum_{j=1}^r \lambda_{j,x} f_j = 0$ pour tout x, puisque les e_x forment une base de $L^{(V)}$ sur L, et donc $\lambda_{j,x} = 0$ pour tous j, x puisque les f_j forment une famille libre sur K. Ceci permet de conclure.

10.5.3. *Extension des scalaires à un sur-anneau*

Si M est un module sur un anneau A, et si $\varphi : A \to B$ est un morphisme d'anneaux, on peut étendre les scalaires de A à B pour obtenir un B-module M_B (aussi noté $B \otimes_A M$), muni d'une application A-linéaire $\iota : M \to M_B$ (i.e. $\iota(ax) = \varphi(a)\iota(x)$, si $a \in A$ et $x \in M$), et vérifiant la propriété universelle suivante : si $u : M \to M'$ est une application A linéaire de M dans un B-module M′, il existe une unique application B-linéaire $u_B : M_B \to M'$ telle que $u_B \circ \iota = u$. On construit M_B comme V_L : on prend le quotient de $B^{(M)}$ par le sous-B-module engendré par les $e_{x+y} - e_x - e_y$ et les $e_{ax} - \varphi(a)e_x$, pour $x, y \in M$ et $a \in A$. Alors M_B est engendré, en tant que B-module, par $\iota(M)$, mais ι n'est, en général, pas injectif.

Par exemple, si $A = \mathbf{Z}$ et $B = \mathbf{F}_p$, alors $M_B = M/pM$ et ι est la réduction modulo p.

Si $A = \mathbf{Z}$, si $B = \mathbf{Q}$, et si M est un $\mathbf{Z}$-module de torsion, alors $M_B = 0$: en effet, si $x \in M$, et si $n \in \mathbf{N} - \{0\}$ est tel que $nx = 0$ dans M, alors $n\iota(x) = \iota(nx) = 0$ dans M_B, et comme n est inversible dans B, cela implique que $\iota(x) = 0$; on a donc $\iota(M) = 0$, et $M_B = 0$.

Si $A = \mathbf{Z}$, si $B = \mathbf{Q}$, et si $M = \mathbf{Z}^n$, alors $M_B = \mathbf{Q}^n$ et ι est l'inclusion : en effet, si u est un morphisme de $\mathbf{Z}$-modules de $\mathbf{Z}^n$ dans un $\mathbf{Q}$-espace vectoriel V, l'application $\mathbf{Q}$-linéaire de $\mathbf{Q}^n$ dans V envoyant e_i sur $u(e_i)$ est l'unique telle application coïncidant avec u sur $\mathbf{Z}^n$.

Ce qui précède marche de la même manière si A est un anneau principal et si $B = \mathrm{Fr}(A)$. On en déduit que si M est un A-module de type fini, alors M_B est un B-espace vectoriel de dimension le rang de M, ce qui donne une définition un peu plus conceptuelle du rang de M.

10.5.4. *Application à la similitude des matrices*

• Soient $A, B \in \mathbf{M}_n(K)$. S'il existe un corps L contenant K et $Q \in \mathbf{GL}_n(L)$ tel que $B = QAQ^{-1}$, alors il existe $P \in \mathbf{GL}_n(K)$ tel que $B = PAP^{-1}$; autrement dit, s'il existe une extension de K sur lequel A et B sont semblables, alors A et B sont semblables sur K.

Notons u et u' les endomorphismes de $V = K^n$ associés à A et B ; les endomorphismes u_L et u'_L de $V_L = L^n$ qui s'en déduisent par extension des scalaires sont encore ceux associés à A et B. Il s'agit donc de prouver que si u_L et u'_L sont conjugués, alors u et u' le sont. En passant aux K[X] et L[X]-modules associés, on est ramené à prouver que si M et M′ sont deux K[X]-modules et si les L[X]-modules M_L et M'_L sont isomorphes, alors $M \cong M'$. Autrement dit, on doit prouver que si M est un K[X]-module, la connaissance du L[X]-module M_L permet de retrouver M (à isomorphisme près).

On a $M \cong \oplus_{P\in\mathscr{P}_{K[X]}}(\oplus_{i\in\mathbf{N}}(K[X]/P^i)^{n_{P,i}})$, où les $n_{P,i}$ sont des entiers presque tous nuls, et uniquement déterminés (th. de structure des modules de torsion sur K[X]). Il s'ensuit que $M_L = \oplus_{P\in\mathscr{P}_{K[X]}}(\oplus_{i\in\mathbf{N}}(L[X]/P^i)^{n_{P,i}})$. Maintenant, tout $P \in \mathscr{P}_{K[X]}$ peut se factoriser, de manière unique, sous la forme $P = \prod_{Q\in\mathscr{P}_P} Q^{e_Q}$, où $\mathscr{P}_P$ est l'ensemble des polynômes unitaires irréductibles de L[X] qui divisent P dans L[X]. Le th. des restes chinois nous fournit un isomorphisme $L[X]/P^i \cong \oplus_{Q\in\mathscr{P}_P} L[X]/Q^{e_Q i}$, et la décomposition de M_L est donc $M_L = \oplus_{P\in\mathscr{P}_{K[X]}} \oplus_{Q\in\mathscr{P}_P} (\oplus_{i\in\mathbf{N}}(L[X]/Q^{e_Q i})^{n_{P,i}})$, et comme les $\mathscr{P}_P$ sont disjoints 2 à 2, on voit que $n_{P,i} = n_{Q,i}/e_Q$ pour n'importe quel $Q \in \mathscr{P}_{L[X]}$ divisant P. On peut donc retrouver les $n_{P,i}$ à partir des $n_{Q,i}$, et donc aussi la structure de M comme K[X]-module à partir de celle de M_L comme L[X]-module. Ceci permet de conclure.

Exercice 10.17. — Soient $A, B \in \mathbf{M}_n(\mathbf{Q})$. On suppose qu'il existe $P_0 \in \mathbf{GL}_n(\mathbf{C})$ tel que $A = P_0 B P_0^{-1}$.

(i) Soient $M_1, \ldots, M_r \in \mathbf{M}_n(\mathbf{Q})$, libres sur $\mathbf{Q}$; montrer que $M_1, \ldots, M_r$ sont libres sur $\mathbf{C}$. (On pourra s'intéresser à la matrice des M_k dans la base constituée des $U_{i,j}$, où $U_{i,j}$ est la matrice dont tous les coefficients sont nuls sauf le coefficient $a_{i,j}$ qui vaut 1.)

(ii) Montrer que l'ensemble $E_{\mathbf{C}}$ des $M \in \mathbf{M}_n(\mathbf{C})$ vérifiant $AM = MB$ est un $\mathbf{C}$-espace vectoriel qui possède une base $M_1, \ldots, M_r$ constituée d'éléments de $\mathbf{M}_n(\mathbf{Q})$.

(iii) Soit $Q(X_1, \ldots, X_r) = \det(X_1M_1 + \cdots + X_rM_r)$. Montrer que $Q \in \mathbf{Q}[X_1, \ldots, X_r]$ et que $Q \neq 0$.

(iv) En déduire qu'il existe $P \in \mathbf{GL}_n(\mathbf{Q})$ tel que $A = PBP^{-1}$.

11. Topologie

Les notions de topologie générale interviennent directement dans toutes les branches des mathématiques, comme on s'en est aperçu graduellement à partir des travaux de Hausdorff (1906). Parmi les espaces topologiques, les espaces métriques (dont les espaces vectoriels normés sont un cas particulier fondamental [81]), définis par Fréchet (1906), forment une catégorie d'objets aux propriétés particulièrement agréables. Les suites y jouent un rôle privilégié permettant souvent de simplifier les démonstrations qui, pour un espace topologique général, utilisent le langage de la théorie des ensembles. Chaque fois que

81. Mais il y a quand même des exemples parfaitement naturels de distances qui ne sont pas induites par une norme sur un espace vectoriel ambiant ; par exemple, la distance sur la terre n'est pas induite par une norme sur l'espace (à moins que la terre ne soit redevenue plate...).

c'est le cas, nous avons doublé la démonstration dans le cas général d'une démonstration propre aux espaces métriques afin de diversifier les approches.

11.1. Espaces topologiques

11.1.1. *Ouverts, fermés, voisinages*

Si X est un ensemble, une *topologie* $\mathscr{T}$ sur X est un sous-ensemble de l'ensemble des parties de X, contenant X et $\varnothing$, stable par intersection finie et par réunion quelconque. Avec des quantificateurs, cela se traduit par :

- $\varnothing \in \mathscr{T}$ et $\mathrm{X} \in \mathscr{T}$;
- si I est un ensemble fini, et si $\mathrm{U}_i \in \mathscr{T}$, pour $i \in \mathrm{I}$, alors $\cap_{i\in \mathrm{I}} \mathrm{U}_i \in \mathscr{T}$;
- si I est un ensemble quelconque, et si $\mathrm{U}_i \in \mathscr{T}$, pour $i \in \mathrm{I}$, alors $\cup_{i\in \mathrm{I}} \mathrm{U}_i \in \mathscr{T}$.

Si $(\mathrm{X}, \mathscr{T})$ est un *espace topologique* (i.e. un ensemble X muni d'une topologie $\mathscr{T}$), les éléments de $\mathscr{T}$ sont *les ouverts*. On dit que $\mathrm{F} \subset \mathrm{X}$ est *fermé*, si son complémentaire est ouvert. Donc X et $\varnothing$ sont des fermés, et les fermés sont stables par réunion finie et intersection quelconque.

Une *base d'ouverts* pour une topologie $\mathscr{T}$ est un sous-ensemble $\mathscr{B}$ de $\mathscr{T}$ tel que tout élément de $\mathscr{T}$ soit réunion d'éléments de $\mathscr{B}$. Par exemple, dans un espace métrique (voir plus loin), les boules ouvertes forment une base d'ouverts.

Si $(\mathrm{X}, \mathscr{T})$ est un espace topologique, et si $x \in \mathrm{X}$, un *voisinage* V de x est un sous-ensemble de X contenant un ouvert contenant x. Un ensemble est donc ouvert si et seulement si il est voisinage de chacun de ses points.

Une *base de voisinages* de x est une famille de voisinages de x telle que tout ouvert contenant x contienne un élément de la famille. Par exemple, dans un espace métrique, les boules ouvertes de centre x ou les boules fermées de centre x et de rayon non nul forment une base de voisinages de x.

11.1.2. *Exemples*

- La *topologie discrète* sur un ensemble X est celle pour laquelle $\mathscr{T} = \mathscr{P}(\mathrm{X})$, ensemble des parties de X. De manière équivalente, X est muni de la topologie discrète si les singletons sont des ouverts (en effet toute partie de X est la réunion des singletons qu'elle contient).
- La *topologie grossière* sur X est la topologie dont les seuls ouverts sont X et $\varnothing$.
- La topologie naturelle sur $\mathbf{R}$ est celle pour laquelle les segments ouverts forment une base d'ouverts.
- Si E est un espace vectoriel sur $\mathbf{R}$ ou $\mathbf{C}$ muni d'une norme $\| \ \|$, la topologie sur E associée à $\| \ \|$ est celle pour laquelle les boules ouvertes forment une base d'ouverts.
- La *topologie de Zariski* sur $\mathbf{C}^n$ est définie de la manière suivante : $\mathrm{F} \subset \mathbf{C}^n$ est un *fermé de Zariski* si et seulement si il existe une famille de polynômes $\mathrm{P}_i \in \mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, pour $i \in \mathrm{I}$, telle que F soit l'ensemble des zéros communs des P_i (i.e. $\mathrm{F} = \cap_{i\in \mathrm{I}} \{z \in \mathbf{C}^n,\ \mathrm{P}_i(z) = 0\}$). Alors $\mathbf{C}^n$ est un fermé de Zariski (en prenant une famille vide), $\varnothing$ est un fermé de Zariski

(en prenant $P_1 = X_1$ et $P_2 = X_1 - 1$), et une intersection quelconque de fermés de Zariski est un fermé de Zariski (si F_j, pour $j \in J$, est l'ensemble des zéros communs de la famille $(P_{i,j})_{i\in I_j}$, alors $\cap_{j\in J} F_j$ est l'ensemble des zéros communs de la famille $(P_{i,j})_{j\in J, i\in I_j}$), ce qui montre qu'en définissant un ouvert de $\mathbf{C}^n$ pour la topologie de Zariski comme le complémentaire d'un fermé de Zariski, on obtient bien une topologie dont les fermés sont les fermés de Zariski.

• On peut munir un ensemble quelconque de la *topologie du filtre des complémentaires des parties finies*, pour laquelle une partie non vide est un ouvert si et seulement si elle a un complémentaire fini.

11.1.3. *Comparaison de topologies*

Si $\mathscr{T}_1$ et $\mathscr{T}_2$ sont deux topologies sur X, on dit que $\mathscr{T}_1$ est *plus fine* que $\mathscr{T}_2$ si $\mathscr{T}_1$ contient $\mathscr{T}_2$. Le summum de la finesse est donc la discrétion ; à l'opposé, la topologie la moins fine est la topologie grossière. On fera attention au fait que, si on prend deux topologies quelconques, il n'y a aucune raison pour qu'il y en ait une qui soit plus fine que l'autre (cf. ex. 17.3).

11.2. Espaces métriques

Si X est un ensemble, une application $d : X \times X \to \mathbf{R}_+$ est une *distance* sur X si elle vérifie les propriétés suivantes :

• $d(x, y) = 0$ si et seulement si $x = y$ (séparation) ;

• $d(x, y) = d(y, x)$ quels que soient $x, y \in X$;

• $d(x, z) \leqslant d(x, y) + d(y, z)$ quels que soient $x, y, z \in X$ (inégalité triangulaire).

• Si la distance vérifie l'inégalité $d(x, z) \leqslant \sup(d(x, y), d(y, z))$, plus forte que l'inégalité triangulaire, on dit qu'elle est *ultramétrique* ou *non archimédienne*.

Si $x \in X$ et $r > 0$, on note $B(x, r) = \{y \in X,\ d(x, y) \leqslant r\}$ la *boule fermée de centre x et de rayon r*, et $B(x, r^-) = \{y \in X,\ d(x, y) < r\}$ la *boule ouverte de centre x et de rayon r*.

• Une boule ouverte contient une boule ouverte centrée en chacun de ses points.

> L'inégalité triangulaire montre que, si $r > 0$, si $y \in B(x, r^-)$, et si $s = r - d(x, y)$, alors $B(y, s^-) \subset B(x, r^-)$.

• L'ensemble $\mathscr{T}_d$ constitué de $\varnothing$ et des réunions (quelconques) de boules ouvertes est une topologie sur X, et $U \in \mathscr{T}_d$ si et seulement si, quel que soit $x \in U$, il existe $r > 0$ tel que $B(x, r^-) \subset U$.

> Par construction $\mathscr{T}_d$ contient $\varnothing$ et X et est stable par réunion quelconque. Il suffit donc de prouver que $\mathscr{T}_d$ est stable par intersection finie. Soit $U \in \mathscr{T}_d$ non vide, et soit $x \in U$. Par définition de $\mathscr{T}_d$, il existe $y \in X$ et $r > 0$ tels que $B(y, r^-) \subset U$ et $x \in B(y, r^-)$; le point ci-dessus montre qu'il existe $s > 0$ tel que $B(x, s^-) \subset B(y, r^-) \subset U$. La stabilité par intersection finie s'en déduit puisque si $(U_i)_{i\in I}$ est une famille finie d'éléments de $\mathscr{T}_d$, et si $x \in \cap_{i\in I} U_i$, alors pour tout i, il existe $s_i > 0$ tel que $B(x, s_i^-) \subset U_i$, ce qui fait que $\cap_{i\in I} U_i$ contient $B(x, s^-)$, si $s = \inf_{i\in I} s_i$ (et $s \neq 0$ car I est fini).

On note en général (X, d) au lieu de $(\mathrm{X}, \mathscr{T}_d)$ l'espace topologique ainsi obtenu. Un espace topologique obtenu de cette manière est appelé un *espace métrique*. Par construction, les boules ouvertes forment une base d'ouverts de la topologie.

Deux distances sur X sont *équivalentes* si elles définissent la même topologie.

Un espace topologique $(\mathrm{X}, \mathscr{T})$ est *métrisable* s'il existe une distance d sur X telle que l'on ait $\mathscr{T} = \mathscr{T}_d$.

• Dans un espace métrique, les boules fermées sont des fermés.

Si $x \notin \mathrm{B}(x_0, r)$, et si $s = d(x, x_0) - r$, alors $s > 0$ et le complémentaire de $\mathrm{B}(x_0, r)$ contient $\mathrm{B}(x, s^-)$. On en déduit que ce complémentaire est ouvert et donc que $\mathrm{B}(x_0, r)$ est fermée.

• Si (X, d) est un espace métrique, et si $x \in \mathrm{X}$, les $\mathrm{B}(x, r^-)$ forment une base de voisinages de x ; il en est de même des $\mathrm{B}(x, r)$, pour $r > 0$.

On a vu ci-dessus que si U est un ouvert non vide contenant x, alors U contient une boule ouverte $\mathrm{B}(x, r^-)$, avec $r > 0$, ce qui prouve que les $\mathrm{B}(x, r^-)$ forment une base de voisinages de x. De plus, $\mathrm{B}(x, r^-)$ contient $\mathrm{B}(x, r/2)$ qui contient $\mathrm{B}(x, (r/2)^-)$, ce qui prouve que les $\mathrm{B}(x, r)$ forment aussi une base de voisinages de x.

• Deux distances d_1 et d_2 sur un ensemble X sont équivalentes si et seulement si, pour tout $x \in \mathrm{X}$, toute boule ouverte de centre x pour d_1 contient une boule ouverte de centre x pour d_2 et réciproquement.

Si d_1 et d_2 sont équivalentes, la boule ouverte $\mathrm{B}(x, r_1^-)$ pour d_1 est ouverte pour d_2 et donc contient une boule ouverte $\mathrm{B}(x, r_2^-)$ pour d_2, ce qui prouve une des deux implications. Réciproquement, si toute boule ouverte de centre x pour d_1 contient une boule ouverte de centre x pour d_2, et si $\mathrm{U} \neq \varnothing$ est un ouvert pour d_1, alors $\mathrm{U} = \cup_{x \in \mathrm{U}} \mathrm{B}(x, r_{1,x}^-)$, où les $\mathrm{B}(x, r_{1,x}^-)$ sont des boules ouvertes pour d_1. Alors $\mathrm{B}(x, r_{1,x}^-)$ contient une boule ouverte $\mathrm{B}(x, r_{2,x}^-)$ pour d_2, et donc U est ouvert pour d_2 car c'est la réunion des $\mathrm{B}(x, r_{2,x}^-)$. On en déduit l'autre implication.

• Si d est une distance sur X, il existe une distance d', équivalente à d, telle que $d'(x, y) \leqslant 1$, pour tous $x, y \in \mathrm{X}$.

Il suffit de poser $d'(x, y) = \inf(d(x, y), 1)$. Alors

$$d'(x, y) + d'(y, z) = \inf(d(x, y) + d(y, z), 1 + d(y, z), d(x, y) + 1, 2) \geqslant \inf(d(x, z), 1) = d'(x, z),$$

ce qui montre que d' est une distance. De plus, d' est équivalente à d car les boules de rayon $\leqslant 1$ sont les mêmes pour d et d'.

Exercice 11.1. — Montrer que, si (X, d) est un espace métrique, et si $x \in \mathrm{X}$, les $\mathrm{B}(x, 2^{-j})$, pour $j \in \mathbf{N}$, forment une base de voisinages de x.

Exercice 11.2. — Soit X un ensemble. Montrer que $d : \mathrm{X} \times \mathrm{X} \to \mathbf{R}_+$, définie par $d(x, y) = 0$ si $x = y$ et $d(x, y) = 1$, si $x \neq y$, est une distance (*la distance triviale*) sur X. Quelle est la topologie associée ?

Exercice 11.3. — Soit $f : \mathbf{R} \to \mathbf{R}$ définie par $f(x) = \frac{x}{1+|x|}$. Montrer que $(x, y) \mapsto d'(x, y) = |f(x) - f(y)|$ est une distance sur $\mathbf{R}$, qui est équivalente à la distance usuelle $d(x, y) = |x - y|$.

11.3. Continuité

Si X et Y sont deux espaces topologiques, si $f : \mathrm{X} \to \mathrm{Y}$ est une application, et si $x \in \mathrm{X}$, on dit que f est *continue en* x, si quel que soit l'ouvert V de Y contenant $f(x)$, il existe un ouvert U de X, contenant x, tel que $f(\mathrm{U}) \subset \mathrm{V}$. De manière équivalente, f est continue en x si, quel que soit le voisinage V de $f(x)$ dans Y, il existe un voisinage U de x tel que $f(\mathrm{U}) \subset \mathrm{V}$. Il suffit de vérifier ceci pour V dans une base de voisinages de $f(x)$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est *continue*, si elle est continue en tout point $x \in \mathrm{X}$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est un *homéomorphisme* si f est continue bijective, et si sa réciproque $f^{-1} : \mathrm{Y} \to \mathrm{X}$ est continue. On dit que X et Y sont *homéomorphes*[82] s'il existe un homéomorphisme $f : \mathrm{X} \to \mathrm{Y}$.

Si (X, d) est un espace métrique, si $(\mathrm{Y}, \mathscr{T})$ est un espace topologique, et si $x_0 \in \mathrm{X}$, on voit, en revenant à la définition, que $f : \mathrm{X} \to \mathrm{Y}$ est continue en x_0 si et seulement si, pour tout U ouvert de Y contenant $f(x_0)$, il existe $\delta > 0$ tel que $d(x_0, x) < \delta$ implique $f(x) \in \mathrm{U}$. Si Y est aussi métrique, cela se traduit (au choix) par :

- pour tout $\varepsilon > 0$, il existe $\delta = \delta(x, \varepsilon) > 0$ tel que $d_{\mathrm{X}}(x_0, x) < \delta \Rightarrow d_{\mathrm{Y}}(f(x_0), f(x)) < \varepsilon$;
- pour tout $j \in \mathbf{N}$, il existe $\delta = \delta(x, j) > 0$ tel que $d_{\mathrm{X}}(x_0, x) < \delta \Rightarrow d_{\mathrm{Y}}(f(x_0), f(x)) \leqslant 2^{-j}$.

On dit que $f : \mathrm{X} \to \mathrm{Y}$ est *uniformément continue* sur X, si pour tout $\varepsilon > 0$ il existe $\delta = \delta(\varepsilon) > 0$ tel que $d_{\mathrm{X}}(x, x') < \delta$ implique $d_{\mathrm{Y}}(f(x), f(x')) < \varepsilon$. La différence entre la continuité et la continuité uniforme est que δ ne dépend pas de x ; en particulier, une application uniformément continue est continue.

Si $\kappa \in \mathbf{R}_+$, on dit que $f : \mathrm{X} \to \mathrm{Y}$ est *κ-lipschitzienne* (ou *lipschitzienne de rapport κ*), si on a $d_{\mathrm{Y}}(f(x), f(x')) \leqslant \kappa\, d_{\mathrm{X}}(x, x')$, quels que soient $x, x' \in \mathrm{X}$. Une application lipschitzienne est uniformément continue et donc aussi continue.

Exercice 11.4. — Soit (X, d) un espace métrique. Montrer que $d : \mathrm{X} \times \mathrm{X} \to \mathbf{R}$ est continue.

- Les conditions suivantes sont équivalentes :

(i) $f : \mathrm{X} \to \mathrm{Y}$ est continue ;

(ii) il existe une base d'ouverts $\mathscr{B}$ de Y telle que l'image réciproque par f de tout $\mathrm{U} \in \mathscr{B}$ est un ouvert de X ;

(iii) l'image réciproque par f de tout ouvert de Y est un ouvert de X ;

(iv) l'image réciproque par f de tout fermé de Y est un fermé de X.

L'équivalence de (iii) et (iv) vient juste de ce que l'image réciproque du complémentaire est le complémentaire de l'image réciproque (si $\mathrm{A} \subset \mathrm{Y}$, alors $f^{-1}(\mathrm{Y} - \mathrm{A}) = \mathrm{X} - f^{-1}(\mathrm{A})$).

Si f est continue, si V est un ouvert de Y, et si $y \in \mathrm{V} \cap f(\mathrm{X})$, il existe, pour tout $x \in \mathrm{X}$ vérifiant $f(x) = y$, un ouvert U_x de X qui contient x et vérifie $f(\mathrm{U}_x) \subset \mathrm{V}$. Alors $\mathrm{U} = \cup_{y \in \mathrm{V} \cap f(\mathrm{X})} \big(\cup_{x \in f^{-1}(y)} \mathrm{U}_x \big)$ est un ouvert qui contient $\cup_{y \in \mathrm{V} \cap f(\mathrm{X})} f^{-1}(y) = f^{-1}(\mathrm{V})$, et qui

82. Montrer que deux espaces topologiques ne sont pas homéomorphes est loin d'être évident en général (le lecteur est invité à essayer de prouver qu'un pneu et un ballon de football ne sont pas homéomorphes) ; la topologie algébrique (Analysis in situ de Poincaré) fournit des tas d'outils permettant de le faire.

vérifie $f(\mathrm{U}) \subset \mathrm{V}$, ce qui prouve que $f^{-1}(\mathrm{V}) = \mathrm{U}$ et donc que $f^{-1}(\mathrm{V})$ est ouvert. On en déduit l'implication (i)⇒(iii), et comme l'implication (iii)⇒(i) est immédiate (si V est un ouvert contenant $f(x)$, alors $\mathrm{U} = f^{-1}(\mathrm{V})$ est un ouvert de X qui contient x et qui vérifie $f(\mathrm{U}) \subset \mathrm{V}$), cela prouve que les propriétés (i) et (iii) sont équivalentes.

L'implication (iii)⇒(ii) est immédiate. Réciproquement, soit $\mathscr{B}$ une base d'ouverts de Y, et soit V un ouvert de Y. Il existe alors une famille $(\mathrm{V}_i)_{i\in\mathrm{V}}$ d'éléments de $\mathscr{B}$ telle que $\mathrm{V} = \cup_{i\in\mathrm{I}}\mathrm{V}_i$. On a alors $f^{-1}(\mathrm{V}) = \cup_{i\in\mathrm{I}} f^{-1}(\mathrm{V}_i)$, et si $f^{-1}(\mathrm{V}_i)$ est ouvert pour tout i, il en est de même de $f^{-1}(\mathrm{V})$. On en déduit l'équivalence des propriétés (ii) et (iii), ce qui permet de conclure.

• Soient X, Y, Z des espaces topologiques. Si $f : \mathrm{X} \to \mathrm{Y}$ est continue en x, et si $g : \mathrm{Y} \to \mathrm{Z}$ est continue en $f(x)$, alors $g \circ f : \mathrm{X} \to \mathrm{Z}$ est continue en x ; si $f : \mathrm{X} \to \mathrm{Y}$ et $g : \mathrm{Y} \to \mathrm{Z}$ sont continues, alors $g \circ f : \mathrm{X} \to \mathrm{Z}$ est continue.

Soit W un ouvert de Z contenant $g(f(x))$. Comme g est continue en $f(x)$, il existe un ouvert V de Y qui contient $f(x)$ et qui vérifie $g(\mathrm{V}) \subset \mathrm{W}$, et comme f est continue en x, il existe un ouvert U de X qui contient x et qui vérifie $f(\mathrm{U}) \subset \mathrm{V}$. Alors $g \circ f(\mathrm{U}) \subset \mathrm{W}$, ce qui permet de démontrer le premier énoncé ; le second en est une conséquence immédiate

11.4. Sous-espaces, produits, quotients

11.4.1. *Topologie induite*

Si $(\mathrm{X}, \mathscr{T})$ est un espace topologique, et si $\mathrm{Y} \subset \mathrm{X}$, alors $\mathscr{T}_\mathrm{Y} = \{\mathrm{U} \cap \mathrm{Y},\ \mathrm{U} \in \mathscr{T}\}$ est une topologie sur Y appelée la *topologie induite*. Autrement dit, tout sous-ensemble d'un espace topologique est naturellement un espace topologique.

11.4.2. *Topologie produit*

Si $(\mathrm{X}_i, \mathscr{T}_i)_{i\in\mathrm{I}}$ est une famille (éventuellement infinie) d'espaces topologiques, on appelle *topologie produit* sur $\mathrm{X} = \prod_{i\in\mathrm{I}} \mathrm{X}_i$, la topologie la moins fine rendant continues les *projections naturelles* $p_i : \mathrm{X} \to \mathrm{X}_i$, pour $i \in \mathrm{I}$. De manière explicite, une base d'ouverts pour cette topologie est constituée des $\prod_{i\in\mathrm{J}} \mathrm{U}_i \times \prod_{i\in\mathrm{I}-\mathrm{J}} \mathrm{X}_i$, où J décrit les sous-ensembles *finis* de I, et U_i est, si $i \in \mathrm{J}$, un ouvert de X_i.

• Si Y est un espace topologique, alors $f : \mathrm{Y} \to \prod_{i\in\mathrm{I}} \mathrm{X}_i$ est continue si et seulement si $p_i \circ f : \mathrm{Y} \to \mathrm{X}_i$ est continue, quel que soit $i \in \mathrm{I}$.

Comme la composée d'applications continues est continue, si $f : \mathrm{Y} \to \prod_{i\in\mathrm{I}} \mathrm{X}_i$ est continue, alors $p_i \circ f : \mathrm{Y} \to \mathrm{X}_i$ est continue, quel que soit $i \in \mathrm{I}$. Réciproquement, si les $p_i \circ f$, pour $i \in \mathrm{I}$, sont continues, et si $\mathrm{U} = \prod_{i\in\mathrm{J}} \mathrm{U}_i \times \prod_{i\in\mathrm{I}-\mathrm{J}} \mathrm{X}_i$, où $\mathrm{J} \subset \mathrm{I}$ est fini, est un élément de la base d'ouverts ci-dessus, alors $f^{-1}(\mathrm{U}) = \cap_{i\in\mathrm{J}} (p_i \circ f)^{-1}(\mathrm{U}_i)$ est un ouvert comme intersection finie d'ouverts. Ceci implique que f est continue, ce qui permet de conclure.

On fera attention qu'il ne suffit pas de vérifier que $x \mapsto f(x, y)$ est continue sur X pour tout y et $y \mapsto f(x, y)$ est continue sur Y pour tout x, pour en déduire que f est continue sur $\mathrm{X} \times \mathrm{Y}$. Par exemple, si $f : \mathbf{R}^2 \to \mathbf{R}$ est définie par $f(x, y) = \frac{xy}{x^2+y^2}$ si $(x, y) \neq (0, 0)$ et $f(0, 0) = 0$, alors f est continue en chaque variable séparément, mais n'est pas continue en 0 car $f(\varepsilon, \varepsilon) = \frac{1}{2}$ et donc $f^{-1}(]\frac{-1}{2}, \frac{1}{2}[)$, qui contient 0, ne contient aucun point de la forme $(\varepsilon, \varepsilon)$ et donc n'est pas ouvert.

• Si $(\mathrm{X}, d_\mathrm{X})$ et $(\mathrm{Y}, d_\mathrm{Y})$ sont deux espaces métriques, toute distance sur $\mathrm{X}\times\mathrm{Y}$, équivalente à $d_{\mathrm{X}\times\mathrm{Y}}((x,y),(x',y')) = \sup(d_\mathrm{X}(x,x'), d_\mathrm{Y}(y,y'))$ (par exemple $\sqrt{d_\mathrm{X}(x,x')^2 + d_\mathrm{Y}(y,y')^2}$), définit la topologie produit.

La distance $d_{\mathrm{X}\times\mathrm{Y}}$ fait qu'une boule de $\mathrm{X}\times\mathrm{Y}$ est le produit d'une boule de X et d'une boule de Y, ce qui prouve que la topologie qu'elle définit est bien la topologie produit.

• Un produit dénombrable d'espaces métriques est métrisable. Plus précisément, si les (X_n, d_n), pour $n \in \mathbf{N}$, sont des espaces métriques, alors d, définie sur $\mathrm{X} = \prod_{n\in\mathbf{N}} \mathrm{X}_n$ par $d((x_n)_{n\in\mathbf{N}}, (y_n)_{n\in\mathbf{N}}) = \sum_{n\in\mathbf{N}} \frac{1}{2^n} \inf(d_n(x_n,y_n), 1)$, est une distance induisant la topologie produit.

Soient $x = (x_n)_{n\in\mathbf{N}}$, $y = (y_n)_{n\in\mathbf{N}}$ et $z = (z_n)_{n\in\mathbf{N}}$ des éléments de X. Quitte à remplacer d_n par la distance d'_n définie par $d'_n(x_n,y_n) = \inf(d_n(x_n,y_n),1)$ (cf. n° 11.2, dernier point), on peut supposer que $d_n(x_n,y_n) \leqslant 1$ pour tous $x_n, y_n \in \mathrm{X}_n$, et alors $d(x,y) = \sum_{n\in\mathbf{N}} \frac{1}{2^n} d_n(x_n,y_n)$.

◇ Si $d(x,y) = 0$, alors $d_n(x_n,y_n) = 0$ et $x_n = y_n$, pour tout n, et donc $x = y$.

◇ $d(x,y) = d(y,x)$ car $d_n(x_n,y_n) = d_n(y_n,x_n)$ pour tout n.

◇ $d(x,z) = \sum_{n\in\mathbf{N}} \frac{1}{2^n} d_n(x_n,z_n) \leqslant \sum_{n\in\mathbf{N}} \frac{1}{2^n}(d_n(x_n,y_n) + d_n(y_n,z_n)) = d(x,y) + d(y,z)$.

Ceci prouve que d est une distance sur X. Maintenant, soit U un ouvert de (X, d) et soit $x = (x_n)_{n\in\mathbf{N}} \in \mathrm{U}$. Il existe $r > 0$ tel que U contienne $\mathrm{B}_\mathrm{X}(x, 4r^-)$. Soit N tel que $\frac{1}{2^\mathrm{N}} \leqslant 2r$; alors $\sum_{n\leqslant\mathrm{N}} \frac{1}{2^n} r + \sum_{n\geqslant\mathrm{N}+1} \frac{1}{2^n} \leqslant 2r + \frac{1}{2^\mathrm{N}} \leqslant 4r$, et U contient $\prod_{n\leqslant\mathrm{N}} \mathrm{B}_{\mathrm{X}_n}(x_n, r^-) \times \prod_{n\geqslant\mathrm{N}+1} \mathrm{X}_n$, qui est un ouvert de X pour la topologie produit. On en déduit que U est aussi ouvert pour la topologie produit.

Réciproquement, si U est ouvert pour la topologie produit, et si $x = (x_n)_{n\in\mathbf{N}} \in \mathrm{U}$, il existe $r > 0$ et $\mathrm{N} \in \mathbf{N}$ tels que U contienne $\prod_{n\leqslant\mathrm{N}} \mathrm{B}_{\mathrm{X}_n}(x_n, r^-) \times \prod_{n\geqslant\mathrm{N}+1} \mathrm{X}_n$. Alors U contient $\mathrm{B}_\mathrm{X}(x, \frac{r^-}{2^\mathrm{N}})$ car $d(x,y) < \frac{r}{2^\mathrm{N}}$ implique $d(x_n,y_n) < \frac{2^n r}{2^\mathrm{N}} \leqslant r$, si $n \leqslant \mathrm{N}$, et U est ouvert pour d.

Ceci permet de conclure.

11.4.3. *Topologie quotient*

Si X est un espace topologique et $\sim$ est une relation d'équivalence sur X, on définit la *topologie quotient* sur $\mathrm{X}/\sim$ en disant que U est ouvert dans $\mathrm{X}/\sim$ si et seulement si son image inverse dans X est ouverte dans X. C'est la topologie la plus fine rendant continue la surjection canonique $\pi : \mathrm{X} \to \mathrm{X}/\sim$.

• Si Y est un espace topologique, alors $f : \mathrm{X}/\sim \to \mathrm{Y}$ est continue si et seulement si $f\circ\pi : \mathrm{X} \to \mathrm{Y}$ est continue.

$f : \mathrm{X}/\sim \to \mathrm{Y}$ est continue est continue si et seulement si $f^{-1}(\mathrm{U})$ est ouvert pour tout ouvert U de Y, ce qui équivaut, par définition de la topologie quotient, à ce que $\pi^{-1}(f^{-1}(\mathrm{U}))$ est ouvert dans X, pour tout ouvert U de Y, et donc à ce que $f\circ\pi : \mathrm{X} \to \mathrm{Y}$ soit continue.

Exercice 11.5. — Quelle est la topologie quotient sur $\mathbf{R}/\mathbf{Q}$?

Voici quelques espaces que l'on peut construire par des passages au quotient. Le lecteur est invité à s'armer de ciseaux et de colle pour voir à quoi ressemblent les trois premiers espaces, et à chercher sur Internet (par exemple sur le site `http://www.mathcurve.com/surfaces/surfaces.shtml` de R. Ferréol) des images des deux derniers (on ne peut pas les plonger physiquement dans $\mathbf{R}^3$).

— Le *cylindre* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0) \sim (x,1)$, si $x \in [0,1]$.

— La *bande de Moebius* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(1-x,1)$, si $x\in[0,1]$.

— Le *tore* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,y)$, si $y\in[0,1]$. C'est aussi le quotient de $\mathbf{R}^2$ par $\mathbf{Z}^2$ ou encore le produit $(\mathbf{R}/\mathbf{Z})^2$ de deux cercles.

— La *bouteille de Klein* : c'est le quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,1-y)$, si $y\in[0,1]$.

— Le *plan projectif réel* : c'est le quotient de la sphère unité de $\mathbf{R}^3$ par la relation d'équivalence $x\sim -x$; il est homéomorphe au quotient de $[0,1]\times[0,1]$ par la relation d'équivalence $(x,0)\sim(1-x,1)$, si $x\in[0,1]$ et $(0,y)\sim(1,1-y)$, si $y\in[0,1]$.

11.5. Espaces séparés

Une topologie est *séparée* si, quels que soient $x,y\in\mathrm{X}$, avec $x\neq y$, on peut trouver des ouverts U,V de X, avec $x\in\mathrm{U}$, $y\in\mathrm{V}$, et $\mathrm{U}\cap\mathrm{V}=\varnothing$. Par exemple, la topologie discrète est séparée (prendre $\mathrm{U}=\{x\}$ et $\mathrm{V}=\{y\}$), et la topologie grossière est on ne peut moins séparée (sauf si X a 0 ou 1 élément). Dans un espace séparé, les points sont fermés, mais la réciproque n'est pas vraie [83].

• Un espace métrique est séparé.

Si $x\neq y$, on a $d(x,y)>0$, et si $r=\frac{1}{2}d(x,y)$, alors $\mathrm{B}(x,r^-)\cap\mathrm{B}(y,r^-)=\varnothing$, d'après l'inégalité triangulaire.

• Si les X_i sont séparés, alors $\mathrm{X}=\prod_{i\in\mathrm{I}}\mathrm{X}_i$ est séparé.

Si $x=(x_i)_{i\in\mathrm{I}}$ et $y=(y_i)_{i\in\mathrm{I}}$ sont deux éléments distincts de X, il existe $j\in\mathrm{I}$ tel que $x_j\neq y_j$, et comme X_j est séparé, il existe des ouverts disjoints U_j et V_j de X_j contenant x_j et y_j respectivement. Alors $\mathrm{U}=\mathrm{U}_j\times\prod_{i\neq j}\mathrm{X}_i$ et $\mathrm{V}=\mathrm{V}_j\times\prod_{i\neq j}\mathrm{X}_i$ sont des ouverts disjoints de X contenant x et y respectivement. On en déduit la séparation de X.

• X est séparé si et seulement si la diagonale $\Delta=\{(x,x),\ x\in\mathrm{X}\}$ est fermée dans $\mathrm{X}\times\mathrm{X}$.

Si X est séparé, alors quels que soient $x,y\in\mathrm{X}$ distincts, il existe des ouverts $\mathrm{U}_{x,y}$, $\mathrm{V}_{x,y}$ disjoints, avec $x\in\mathrm{U}_{x,y}$ et $y\in\mathrm{V}_{x,y}$. La condition « $\mathrm{U}_{x,y}$, $\mathrm{V}_{x,y}$ disjoints » est équivalente à ce que l'ouvert $\mathrm{W}_{x,y}=\mathrm{U}_{x,y}\times\mathrm{V}_{x,y}$ de $\mathrm{X}\times\mathrm{X}$ ne rencontre pas Δ. De plus, $\mathrm{W}_{x,y}$ contient (x,y), ce qui fait que la réunion des $\mathrm{W}_{x,y}$, pour $x\neq y$, est égale à $(\mathrm{X}\times\mathrm{X})-\Delta$ qui est donc ouvert en tant que réunion d'ouverts. On en déduit que Δ est fermée.

Réciproquement, si Δ est fermée, alors $(\mathrm{X}\times\mathrm{X})-\Delta$ est ouvert. Par définition de la topologie produit, cela implique que si $(x,y)\in(\mathrm{X}\times\mathrm{X})-\Delta$ (i.e. si $x\neq y$), alors il existe U,V ouverts

83. Par exemple, dans $\mathbf{C}^n$ muni de la topologie de Zariski, les points sont fermés puisque $z=(z_1,\ldots,z_n)$ est l'ensemble des zéros communs de la famille de polynômes X_i-z_i, pour $i\in\mathrm{I}$, mais la topologie de Zariski est fort peu séparée puisque tout ouvert de Zariski non vide est dense (pour la topologie de Zariski et aussi pour la topologie usuelle de $\mathbf{C}^n$). Il a fallu attendre les travaux de A. Weil (1952) et J-P. Serre (*Géométrie algébrique et géométrie analytique*, connu sous le nom de GAGA, 1956) pour que l'on se rende compte que cette topologie, loin d'être une curiosité pathologique, permet de retrouver, de manière algébrique, la plupart des invariants que l'on peut définir en utilisant la topologie usuelle. Ceci servit de point de départ à la révolution grothendieckienne.

de X tels que $U \times V \subset (X \times X) - \Delta$ et $(x, y) \in U \times V$. Alors $x \in U$, $y \in V$ et $U \cap V = \varnothing$. On en déduit la séparation de X.

Exercice 11.6. — Montrer que, si $f : X \to Y$ est injective et continue, et si Y est séparé, alors X est séparé.

Un espace métrique est séparé grâce à la *condition de séparation* « $d(x, y) = 0 \Rightarrow x = y$ ». Si on supprime la condition de séparation, on obtient une *semi-distance* qui permet encore de définir une topologie $\mathscr{T}_d$ dans laquelle un ouvert non vide est une réunion (quelconque) de boules ouvertes. L'espace topologique $(X, \mathscr{T}_d)$ n'est plus forcément séparé (si $x \neq y$, mais $d(x, y) = 0$, alors tout ouvert de X contenant x contient aussi y). C'est le cas des espaces $\mathscr{L}^1(\mathbf{R}^m)$ et $\mathscr{L}^2(\mathbf{R}^m)$ du § III.2, par exemple.

On peut fabriquer un espace séparé à partir de (X, d), en identifiant deux points dont la distance est nulle. De manière précise, on définit une relation $\sim$ sur X par $x \sim y$ si et seulement si $d(x, y) = 0$; la relation $\sim$ est une relation d'équivalence grâce à la symétrie de d et à l'inégalité triangulaire. De plus, $d(x, y) = d(x', y')$ si $x \sim x'$ et $y \sim y'$, toujours grâce à l'inégalité triangulaire. On en déduit le fait que d définit une distance sur l'ensemble $X/\sim$ des classes d'équivalence pour la relation $\sim$, et le séparé de (X, d) est l'ensemble $X/\sim$ muni de la distance induite par d.

Un exemple de cette construction est le passage de $\mathscr{L}^1(\mathbf{R}^m)$ à $L^1(\mathbf{R}^m)$ ou de $\mathscr{L}^2(\mathbf{R}^m)$ à $L^2(\mathbf{R}^m)$ rencontré dans le cours (cf. § III.2).

11.6. Intérieur, adhérence, densité

Si X est un espace topologique, et $Y \subset X$, alors la réunion $\overset{\circ}{Y}$ de tous les ouverts de X contenus dans Y est un ouvert, et donc est le plus grand ouvert contenu dans Y ; c'est *l'intérieur* de Y. On dit que Y *est d'intérieur vide* si $\overset{\circ}{Y} = \varnothing$.

De même, l'intersection $\overline{Y}$ de tous les fermés de X contenant Y est un fermé appelé *l'adhérence* de Y. On dit que Y est *dense dans* X si $\overline{Y} = X$. De manière équivalente, Y est dense dans X si et seulement si $Y \cap U \neq \varnothing$ pour tout ouvert non vide U de X, ou encore si et seulement si tout point de X admet au moins un point de Y dans chacun de ses voisinages. Si (X, d) est un espace métrique, cela se traduit encore par : Y est dense dans X si et seulement si, pour tous $x \in X$ et $\varepsilon > 0$, il existe $y \in Y$ tel que $d(x, y) < \varepsilon$.

• $\mathbf{Q}$ est dense dans $\mathbf{R}$ et $\mathbf{Q}_p$ (par construction).

• Les polynômes sont denses dans l'espace des fonctions continues sur $[0, 1]$ muni de la norme $\|\phi\|_\infty = \sup_{x \in [0,1]} |\phi(x)|$ de la convergence uniforme (th. de Weierstrass, ex. II.1.10).

• Si X est muni de la topologie grossière, tout point est dense dans X.

• Si Y est dense dans X, si Z est séparé, et si $f, g : X \to Z$ sont continues et coïncident sur Y, alors $f = g$.

Il suffit de prouver que l'ensemble A des $x \in X$ vérifiant $f(x) = g(x)$ est fermé dans X, puisque A contenant Y, et Y étant dense dans X, cela implique $A = X$. Or A est l'image inverse de la diagonale $\Delta = \{(x, x),\ x \in X\}$ dans $X \times X$ par l'application $x \mapsto (f(x), g(x))$, qui est continue, et l'hypothèse Z séparé est équivalente à ce que Δ soit fermé dans $X \times X$, ce qui fait que A est fermé comme image inverse d'un fermé par une application continue.

Exercice 11.7. — Soit X un espace topologique. Montrer que $Y \subset X$ est d'intérieur vide si et seulement si son complémentaire est dense dans X.

Exercice 11.8. — (i) Montrer que si Y_1 est dense dans X_1 et si Y_2 est dense dans X_1, alors $Y_1 \times Y_2$ est dense dans $X_1 \times X_2$.

(ii) Soit $f : Y \to Z$ une application continue entre espaces métriques. Montrer que si X est dense dans Y, et si la restriction de f à X est une isométrie, alors f est une isométrie.

Exercice 11.9. — (i) Montrer que si U est ouvert, l'intérieur de l'adhérence de U contient U, et qu'on n'a pas toujours égalité, mais que l'adhérence de l'intérieur de l'adhérence de U est l'adhérence de U.

(ii) Montrer que, si F est fermé, l'adhérence de l'intérieur de F est contenu dans F, et qu'on n'a pas toujours égalité, mais que l'intérieur de l'adhérence de l'intérieur de F est l'intérieur de F.

Exercice 11.10. — Montrer que $A = \{(n, e^n),\ n \in \mathbf{N}\}$ est dense dans $\mathbf{C}^2$ muni de la topologie de Zariski. Est-t-il dense dans $\mathbf{C}^2$ pour la topologie usuelle ?

11.7. Suites dans un espace topologique

11.7.1. *Suites, suites extraites*

Soit X un espace topologique. Si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de X, et si $a \in X$, on dit que x_n *tend vers* a ou que x_n *a pour limite* a, si pour tout voisinage V de a, il existe $N \in \mathbf{N}$, tel que $x_n \in V$, si $n \geqslant N$. Il suffit bien évidemment de vérifier ceci pour V dans une base de voisinages de a.

On peut remplacer $\mathbf{N}$ par un ensemble I quelconque : on dit que $(x_i)_{i\in I}$ tend vers a quand $i \to \infty$ (i.e. suivant la topologie du filtre des complémentaires des parties finies) si pour tout voisinage V de a l'ensemble des $i \in I$ tel que $x_i \notin V$ est fini.

Si X est séparé, une suite a au plus une limite comme on le constate aisément en revenant à la définition d'espace séparé. On prendra garde au fait que ce n'est plus forcément le cas, si l'espace n'est pas séparé. On dit qu'une suite est *convergente* si elle a au moins une limite. On réserve la notation $\lim_{n\to+\infty} x_n = a$ au cas où l'espace est séparé et donc la limite est unique.

On obtient une traduction agréable de la notion de suite convergente en introduisant l'espace topologique $\overline{\mathbf{N}} = \mathbf{N} \cup \{+\infty\}$, muni de la topologie pour laquelle les ouverts sont les parties de $\mathbf{N}$ auxquelles on a rajouté les complémentaires dans $\overline{\mathbf{N}}$ des parties finies de $\mathbf{N}$. C'est alors un simple exercice de montrer que $\lim_{n\to+\infty} x_n = a$ si et seulement si la suite x_n se prolonge en une fonction continue de $\overline{\mathbf{N}}$ dans X prenant la valeur a en $+\infty$ (i.e. l'application de $\overline{\mathbf{N}}$ dans X obtenue en envoyant n sur x_n et $+\infty$ sur a est continue).

Une suite $(y_n)_{n\in\mathbf{N}}$ est dite *extraite* de $(x_n)_{n\in\mathbf{N}}$ s'il existe $\varphi : \mathbf{N} \to \mathbf{N}$ tendant vers $+\infty$ quand n tend vers $+\infty$, telle que $y_n = x_{\varphi(n)}$, pour tout $n \in \mathbf{N}$.

• Si a est une limite de $x = (x_n)_{n\in\mathbf{N}}$, alors a est aussi limite de toute suite extraite.

Soit $\varphi : \mathbf{N} \to \mathbf{N}$ tendant vers $+\infty$ quand n tend vers $+\infty$, ce qui se traduit par le fait que φ peut s'étendre par continuité à $\overline{\mathbf{N}}$, en posant $\varphi(+\infty) = +\infty$. Si a est une limite de x, alors x peut aussi s'étendre par continuité à $\overline{\mathbf{N}}$, en posant $x(+\infty) = a$ et donc $x \circ \varphi$ est continue sur $\overline{\mathbf{N}}$, ce qui se traduit par le fait que a est limite de la suite extraite $(x_{\varphi(n)})_{n\in\mathbf{N}}$.

On peut aussi se passer de $\overline{\mathbf{N}}$, et revenir à la définition. Si V est un voisinage de a, alors il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in \mathrm{V}$, pour tout $n \geqslant \mathrm{N}$. Par ailleurs, si $\varphi : \mathbf{N} \to \mathbf{N}$ tend vers $+\infty$ quand n tend vers $+\infty$, il existe $\mathrm{N}' \in \mathbf{N}$ tel que $\varphi(n) \geqslant \mathrm{N}$, si $n \geqslant \mathrm{N}'$. On a donc $x_{\varphi(n)} \in \mathrm{V}$, pour tout $n \geqslant \mathrm{N}'$, ce qui permet de montrer que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ tend vers a.

• Soit $\mathrm{X} = \prod_{i\in\mathrm{I}} \mathrm{X}_i$ un produit d'espaces topologiques séparés, et soient $u^{(n)} = (u_i^{(n)})_{i\in\mathrm{I}}$, pour $n \in \mathbf{N}$, une suite d'éléments de X et $a = (a_i)_{i\in\mathrm{I}} \in \mathrm{X}$. Alors $u^{(n)} \to a$ si et seulement si $u_i^{(n)} \to a_i$ pour tout $i \in \mathrm{I}$.

L'implication « $u^{(n)} \to a$ » $\Rightarrow$ « $u_i^{(n)} \to a_i$ pour tout $i \in \mathrm{I}$ » est une conséquence de la continuité des projections $\mathrm{X} \to \mathrm{X}_i$. Réciproquement, supposons que $u_i^{(n)} \to a_i$ pour tout $i \in \mathrm{I}$. Soit U un ouvert de X contenant a. Alors U contient un ouvert de la forme $\prod_{i\in\mathrm{J}} \mathrm{U}_i \times \prod_{i\in\mathrm{I}-\mathrm{J}} \mathrm{X}_i$, où J est fini et U_i est un ouvert de X_i contenant a_i si $i \in \mathrm{J}$. Comme $u_i^{(n)} \to a_i$, il existe $\mathrm{N}_i \in \mathbf{N}$ tel que $u_i^{(n)} \in \mathrm{U}_i$ pour tout $n \geqslant \mathrm{N}_i$, et alors $u^{(n)} \in \mathrm{U}$, pour tout $n \geqslant \sup_{i\in\mathrm{J}} \mathrm{N}_i$. On en déduit que $u^{(n)} \to a$, ce qui termine la démonstration.

11.7.2. *Suites et continuité*

• Si $f : \mathrm{X} \to \mathrm{Y}$ est continue, et si $x = (x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de X admettant a comme limite, alors $(f(x_n))_{n\in\mathbf{N}}$ admet $f(a)$ pour limite.

La suite x se prolonge en une fonction continue de $\overline{\mathbf{N}}$ dans X prenant la valeur a en $+\infty$, et comme f est continue, $f \circ x$ est continue sur $\overline{\mathbf{N}}$, ce qui se traduit par le fait que $f(a)$ est limite de la suite $(f(x_n))_{n\in\mathbf{N}}$.

On peut aussi se passer de $\overline{\mathbf{N}}$, et dire que si V est un voisinage de $f(a)$, alors $f^{-1}(\mathrm{V})$ contient un voisinage U de a puisque f est continue, et qu'il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in \mathrm{U}$, si $n \geqslant \mathrm{N}$, ce qui implique $f(x_n) \in \mathrm{V}$, si $n \geqslant \mathrm{N}$.

• Si X est un espace métrique, alors $f : \mathrm{X} \to \mathrm{Y}$ est continue en x si et seulement si pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$.

On a déjà démontré (dans le cas d'espaces topologiques généraux) que si $f : \mathrm{X} \to \mathrm{Y}$ est continue en x, alors pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$. Maintenant, si f est non continue en x, il existe un voisinage V de $f(x)$, tel que, pour tout $n \in \mathbf{N}$, il existe $x_n \in \mathrm{B}(x, 2^{-n})$ avec $f(x_n) \notin \mathrm{V}$. Alors $x_n \to x$ dans X, tandis que $f(x_n) \not\to f(x)$. En prenant la contraposée, on en déduit que, si pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X tendant vers x, la suite $(f(x_n))_{n\in\mathbf{N}}$ tend vers $f(x)$, alors f est continue en x. Ceci permet de conclure.

On prendra garde au fait que cette caractérisation de la continuité par les suites n'est pas valable pour un espace topologique général.

Exercice 11.11. — Soit X un espace métrique (ou métrisable).

(i) Soit $\mathrm{Z} \subset \mathrm{X}$. Montrer que $a \in \mathrm{X}$ est dans l'adhérence $\overline{\mathrm{Z}}$ de Z si et seulement si il existe une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de Z, ayant a pour limite.

(ii) Montrer que Z est dense dans X si et seulement si tout $a \in \mathrm{X}$ est limite d'une suite d'éléments de Z.

(iii) Montrer que, si Y est un espace métrique, si f, g sont deux applications continues de X dans Y, telles que l'on ait $f(x) = g(x)$, pour tout $x \in \mathrm{Z}$, où Z est dense dans X, alors $f = g$.

12. Compacité

12.1. Espaces compacts

Un espace topologique X est dit *compact* s'il est séparé, et si de tout recouvrement de X par des ouverts, on peut extraire un sous-recouvrement fini [84]. Autrement dit, X (séparé) est compact si, quelle que soit la famille $(U_i)_{i\in I}$ d'ouverts de X telle que $\cup_{i\in I}U_i = X$, il existe $J \subset I$ fini tel que $\cup_{i\in J}U_i = X$. En passant aux complémentaires, on voit que la compacité de X (séparé) est équivalente à ce que de toute famille de fermés de X d'intersection vide, on puisse extraire une famille finie d'intersection vide.

• Un ensemble fini, muni de la topologie discrète, est compact.

• L'espace $\overline{\mathbf{N}} = \mathbf{N} \cup \{+\infty\}$, muni de la topologie pour laquelle les ouverts sont les parties de $\mathbf{N}$ et les complémentaires dans $\overline{\mathbf{N}}$ des parties finies de $\mathbf{N}$, est un espace compact.

> $\overline{\mathbf{N}}$ est séparé car, si $x \neq y$, alors $x \neq +\infty$ ou $y \neq +\infty$, ce qui fait que l'un des deux singletons $\{x\}$ ou $\{y\}$ est ouvert, ainsi que son complémentaire. Par ailleurs, si les $(U_i)_{i\in I}$ forment un recouvrement ouvert de $\overline{\mathbf{N}}$, alors un des U_i contient $+\infty$, et son complémentaire est fini ; on peut donc extraire du recouvrement par les U_i un sous-recouvrement fini.

• Le segment $[0, 1]$ est compact.

> Soit $(U_i)_{i\in I}$ une famille d'ouverts de $[0, 1]$ formant un recouvrement. Soit A l'ensemble des $a \in [0, 1]$ tels que $[0, a]$ puisse être recouvert par un nombre fini de U_i, et soit M la borne supérieure de A. Par hypothèse, il existe $i(M) \in I$ et $\varepsilon > 0$ tels que $]M-\varepsilon, M+\varepsilon[\cap[0, 1] \subset U_{i(M)}$, et par définition de M, il existe $a \in]M - \varepsilon, M[$ et $J \subset I$ fini, tels que $[0, a] \subset \cup_{i\in J}U_i$. Mais alors $[0, b] \subset \cup_{i\in J\cup\{i(M)\}}U_i$, quel que soit $b \in [M, M + \varepsilon[\cap[0, 1]$, et donc $[M, M + \varepsilon[\cap[0, 1] \subset A$. Par définition de M, ceci implique $M = 1$, et permet de conclure.

Exercice 12.1. — (i) Soit X un sous-ensemble dénombrable de $[0, 1]$. Montrer que pour tout $\varepsilon > 0$, il existe une suite de segments ouverts $]a_n, b_n[$ telle que $\sum_{n\in\mathbf{N}}(b_n - a_n) < \varepsilon$ et $\cup_{n\in\mathbf{N}}]a_n, b_n[$ contienne X.

(ii) Soit $]a_n, b_n[$, pour $n \in \mathbf{N}$, une suite de segments ouverts tels que $[0, 1] \subset \cup_{n\in\mathbf{N}}]a_n, b_n[$. Montrer que $\sum_{n\in\mathbf{N}}(b_n - a_n) > 1$. (On pourra admettre que le résultat est vrai pour une famille finie.)

(iii) Montrer que $[0, 1]$ et $\mathbf{R}$ ne sont pas dénombrables.

12.2. Compacité et suites

Si X est un espace topologique, et si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de X, on dit que $a \in X$ est une *valeur d'adhérence* de la suite $(x_n)_{n\in\mathbf{N}}$, si tout voisinage de a contient une infinité de termes de la suite. Ceci équivaut à ce que a soit dans l'adhérence F_k de $\{x_n,\ n \geqslant k\}$, pour tout $k \in \mathbf{N}$. En particulier, l'ensemble des valeurs d'adhérence d'une suite est un fermé, puisque c'est l'intersection des fermés F_k, pour $k \in \mathbf{N}$.

• Si X est un espace métrique, alors a est une valeur d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$, si et seulement si on peut extraire une sous-suite de la suite $(x_n)_{n\in\mathbf{N}}$ ayant pour limite a.

84. La notion de compacité a été dégagée en 1894 par Borel (pour des questions de mesure, cf. (ii) de l'ex. 12.1, auquel Borel se référait sous le nom de *théorème fondamental de la théorie de la mesure*) et par Cousin (pour des applications aux fonctions de plusieurs variables complexes).

Si on peut extraire de $(x_n)_{n\in\mathbf{N}}$, une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ de limite a, et si V est un voisinage de a, alors $x_{\varphi(n)} \in \mathrm{V}$, pour tout n assez grand, ce qui prouve que a est une valeur d'adhérence de la suite (noter que ce sens n'utilise pas le fait que X est métrique). Réciproquement, si X est métrique, et si a est une valeur d'adhérence de $(x_n)_{n\in\mathbf{N}}$, alors pour tout $n \in \mathbf{N}$, il existe une infinité de termes de la suite dans $\mathrm{B}(a, 2^{-n})$, et donc on peut choisir $\varphi(n) \geqslant n$ tel que $x_\varphi(n) \in \mathrm{B}(a, 2^{-n})$. La suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ est alors extraite de la suite $(x_n)_{n\in\mathbf{N}}$ et converge vers a. Ceci permet de conclure.

• Dans un compact, toute suite admet une valeur d'adhérence ; dans un compact métrique, on peut extraire de toute suite une sous-suite convergente.

Soit X un compact, et soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de X. Soit F_n, si $n \in \mathbf{N}$, l'adhérence de l'ensemble $\{x_{n+p},\ p \in \mathbf{N}\}$; l'intersection des F_n est, par définition ou presque, l'ensemble des valeurs d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$. Comme l'intersection d'un nombre fini de F_n est toujours non vide puisqu'elle contient les x_n, pour n assez grand, la compacité de X assure que l'intersection des fermés F_n, pour $n \in \mathbf{N}$, est non vide, ce qui permet de conclure.

Exercice 12.2. — (i) Montrer que dans un compact, une suite ayant une seule valeur d'adhérence converge.
(ii) Le résultat est-il valable dans $\mathbf{R}$?

• Un espace métrique est compact si et seulement si toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X admet une valeur d'adhérence [85] (th. de Borel-Lebesgue).

On sait déjà que dans un compact (même non métrique), toute suite admet une valeur d'adhérence ; montrons la réciproque dans le cas d'un espace métrique. Soit $(\mathrm{U}_i)_{i\in\mathrm{I}}$ un recouvrement ouvert de X. Alors, quel que soit $x \in \mathrm{X}$, il existe $k(x) \geqslant 0$ et $i \in \mathrm{I}$, tels que $\mathrm{B}(x, r(x)^-) \subset \mathrm{U}_i$, où $r(x) = 2^{-k(x)}$. On cherche à prouver qu'on peut extraire du recouvrement par les U_i un recouvrement fini, et il suffit de prouver qu'on peut en faire autant du recouvrement par les $\mathrm{B}(x, r(x)^-)$.

Pour cela, construisons par récurrence une suite x_n d'éléments de X vérifiant :
• $x_n \in \mathrm{Y}_n$, où Y_n est le fermé complémentaire de $\cup_{j\leqslant n-1}\mathrm{B}(x_j, r(x_j)^-)$,
• $k(x_n) \leqslant k(y)$, quel que soit $y \in \mathrm{Y}_n$.
Si la construction s'arrête, c'est que les $\mathrm{B}(x_j, r(x_j)^-)$, pour $j \leqslant n-1$ recouvrent X, ce que l'on veut. Sinon, la suite $(x_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence y_0, et on a $y_0 \in \mathrm{Y}_n$, quel que soit $n \in \mathbf{N}$, car Y_n est fermé et $x_{n+p} \in \mathrm{Y}_n$, quel que soit $p \in \mathbf{N}$. Par construction de la suite $(x_n)_{n\in\mathbf{N}}$, on a $d(x_n, x_{n+p}) \geqslant 2^{-k(x_n)}$, quels que soient $n, p \in \mathbf{N}$. Comme on peut extraire une sous-suite de Cauchy de la suite $(x_n)_{n\in\mathbf{N}}$, on en déduit que $k(x_n) \to +\infty$. En particulier, il existe n tel que $k(x_n) \geqslant k(y_0) + 1$, en contradiction avec la construction de x_n (puisque $y_0 \in \mathrm{Y}_n$). Ceci permet de conclure.

12.3. Propriétés de base des compacts

Les énoncés qui suivent sont d'un usage constant.

85. Cette caractérisation est parfois prise comme définition des espaces compacts. Elle est effectivement d'un maniement plus facile que la caractérisation en termes de recouvrements ouverts si on cherche à vérifier qu'un espace (métrique) est compact. Par contre, si on veut utiliser la compacité d'un espace pour en tirer des conséquences, c'est en général la caractérisation par les recouvrements ouverts qui est la plus naturelle et la plus puissante.

12.3.1. *Compacts d'un espace topologique*

• Si X est compact, alors $Y \subset X$ est compact, si et seulement si Y est fermé.

Supposons Y fermé. Soit $(U_i)_{i\in I}$ un recouvrement [86] ouvert de Y. Par définition, il existe, pour tout $i \in I$, un ouvert V_i de X tel que $U_i = V_i \cap Y$, et comme $U = X - Y$ est ouvert, les V_i, pour $i \in I$, et U forment un recouvrement ouvert de X. Comme X est supposé compact, il existe $J \subset I$ fini, tel que $X \subset U \cup \left(\cup_{i\in J} V_i\right)$, et les U_i, pour $i \in J$ forment un recouvrement ouvert de Y extrait du recouvrement initial. On en déduit la compacité de Y.

Réciproquement, supposons $Y \subset X$ compact. Soit $a \notin Y$. Comme X est séparé, pour tout $y \in Y$, il existe des ouverts U_y, V_y tels que $y \in U_y$, $a \in V_y$ et $U_y \cap V_y = \varnothing$. Les U_y, pour $y \in Y$, forment un recouvrement ouvert de Y ; il existe donc $J \subset Y$ fini tel que $Y \subset \cup_{y\in J} U_y$. Mais alors $V = \cap_{y\in J} V_y$ est un ouvert de X contenant a et ne rencontrant pas Y, ce qui prouve que a n'appartient pas à l'adhérence $\overline{Y}$ de Y. On a donc $\overline{Y} \subset Y$, ce qui prouve que Y est fermé.

• L'image d'un compact X par une application continue $f : X \to Y$, où Y est séparé, est un compact.

Soit $(U_i)_{i\in I}$ un recouvrement [87] ouvert de $f(X)$. Par définition, si $i \in I$, il existe U'_i ouvert de Y tel que $U_i = U'_i \cap f(X)$, et comme f est continue, $V_i = f^{-1}(U'_i)$ est ouvert dans X, et $(V_i)_{i\in I}$ est donc un recouvrement ouvert de X. Comme X est compact, il existe $J \subset I$ fini tels que les V_i, pour $i \in J$, recouvrent X, et les U_i, pour $i \in J$, forment alors un recouvrement ouvert fini de $f(X)$ extrait du recouvrement initial. On en déduit la compacité de $f(X)$.

• Si X est compact, et si $f : X \to Y$ est bijective continue avec Y séparé, alors f est un homéomorphisme.

Notons $g : Y \to X$ l'application réciproque de f de telle sorte que si $F \subset X$, alors on a $g^{-1}(F) = \{y \in Y, \exists x \in F, g(y) = x\} = \{y \in Y\ , \exists x \in F, y = f(g(y)) = f(x)\} = f(F)$. On veut prouver que $g^{-1}(F)$ est fermé dans Y si F l'est dans X. Or $g^{-1}(F) = f(F)$, et comme F est compact puisque fermé dans un compact, et que Y est séparé, $f(F)$ est compact et donc fermé. Ceci permet de conclure.

• Si X est compact, et $f : X \to \mathbf{R}$ est continue, alors f atteint son maximum et son minimum.

Comme X est compact et f continue, cela implique que $f(X)$ est compact, et donc admet des bornes inférieure et supérieure finies [sinon on peut construire une suite d'éléments de $f(X)$ tendant vers $\pm\infty$ et donc n'ayant pas de valeur d'adhérence dans $f(X)$], et les contient car il est fermé.

---

86. Si X est un espace métrique, on peut passer par les suites. Comme X est compact, une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de Y a une valeur d'adhérence dans X, et si Y est fermé, cette valeur d'adhérence est dans Y, ce qui prouve que Y est compact. Réciproquement, si Y est compact, si a est dans l'adhérence de Y, il existe une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de Y ayant pour limite a dans X, et sa seule valeur d'adhérence dans X est alors a. Comme Y est supposé compact, cette suite admet une valeur d'adhérence dans Y, et comme sa seule valeur d'adhérence dans X est a, cela implique $a \in Y$. On en déduit que Y est fermé.

87. Si X et Y sont des espaces métriques, on peut raisonner en termes de suites. Soit $(y_n)_{n\in\mathbf{N}}$ une suite d'éléments de $f(Y)$, et, si $n \in \mathbf{N}$, soit $x_n \in X$ tel que $y_n = f(x_n)$. Comme X est compact, la suite $(x_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence $a \in X$, et comme f est continue, $f(a)$ est une valeur d'adhérence de la suite $(y_n)_{n\in\mathbf{N}}$. On en déduit la compacité de $f(X)$.

• Si X_1 et X_2 sont compacts, alors $X_1 \times X_2$ est compact.

Soit $(U_i)_{i\in I}$ une famille d'ouverts de $X_1 \times X_2$ formant un recouvrement [88]. Si $y \in X_2$, soit $I(y)$ l'ensemble des $i \in I$ tels que $U_i \cap (X_1 \times \{y\}) \neq \varnothing$. Si $i \in I(y)$, et si $(a, y) \in U_i$, il existe $V_{i,y,a}$ ouvert de X_1 contenant a et $W_{i,y,a}$ ouvert de X_2 contenant y tels que $U_i \supset V_{i,y,a} \times W_{i,y,a}$. Les U_i, pour i dans I, formant un recouvrement de $X_1 \times X_2$, les $V_{i,y,a}$, pour $i \in I(y)$ et $(a, y) \in U_i$, forment un recouvrement de X_1. Comme X_1 est compact, il existe un ensemble fini $J(y)$ de couples (i, a), avec $i \in I(y)$ et $(a, y) \in U_i$ tels que $X_1 = \cup_{(i,a)\in J(y)} V_{i,y,a}$. Soit alors $W_y = \cap_{(i,a)\in J(y)} W_{i,y,a}$. C'est un ouvert de X_2 contenant y, et U_i contient $V_{i,y,a} \times W_y$, quel que soit $(i, a) \in J(y)$. Comme X_2 est compact, on peut trouver Y fini tel que $X_2 = \cup_{y\in Y} W_y$, et alors

$$\cup_{y\in Y} \cup_{(i,a)\in J(y)} U_i \supset \cup_{y\in Y} \big(\cup_{(i,a)\in J(y)} V_{i,y,a} \times W_y \big) = \cup_{y\in Y} (X_1 \times W_y) = X_1 \times X_2,$$

ce qui montre que l'on peut extraire du recouvrement par les U_i un sous-recouvrement fini.

• Un produit dénombrable de compacts métriques est compact [89].

Soient X_i, pour $i \in \mathbf{N}$, des compacts métriques, et soit $X = \prod_{i\in\mathbf{N}} X_i$. Comme un produit dénombrable d'espaces métriques est métrisable (alinéa 11.4.2), il suffit de prouver que toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de X admet une sous-suite extraite convergente.

Écrivons $x_n \in X = \prod_{i\in\mathbf{N}} X_i$ sous la forme $x_n = (x_{n,i})_{i\in\mathbf{N}}$, avec $x_{n,i} \in X_i$ pour tout i. Comme X_0 est compact, on peut extraire une sous-suite $(x_{\varphi_0(n)})_{n\in\mathbf{N}}$ telle que $(x_{\varphi_0(n),0})_{n\in\mathbf{N}}$ ait une limite a_0 dans X_0. Pour la même raison, on peut extraire de la suite $(x_{\varphi_0(n)})_{n\in\mathbf{N}}$ une sous-suite $(x_{\varphi_1(n)})_{n\in\mathbf{N}}$ telle que $(x_{\varphi_1(n),1})_{n\in\mathbf{N}}$ ait une limite a_1 dans X_1, et on a encore $x_{\varphi_1(n),0} \to a_0$ puisque $(x_{\varphi_1(n),0})_{n\in\mathbf{N}}$ est extraite de $(x_{\varphi_0(n),0})_{n\in\mathbf{N}}$. Par récurrence, cela permet de définir $a_k \in X_k$ et une suite $(x_{\varphi_k(n)})_{n\in\mathbf{N}}$, extraite de $(x_{\varphi_{k-1}(n)})_{n\in\mathbf{N}}$, telle que $x_{\varphi_k(n),i} \to a_i$, pour tout $i \leqslant k$. La suite $(x_{\varphi_n(n)})_{n\in\mathbf{N}}$ est alors extraite (par *extraction diagonale*) de $(x_n)_{n\in\mathbf{N}}$, et aussi de $(x_{\varphi_k(n)})_{n\in\mathbf{N}}$ pour $n \geqslant k$; il s'ensuit que $x_{\varphi_n(n),i} \to a_i$, pour tout $i \in \mathbf{N}$, et donc que $x_{\varphi_n(n)} \to a$ dans X, si $a = (a_i)_{i\in\mathbf{N}}$. Ceci permet de conclure

Exercice 12.3. — Montrer que $[0, 1]$ est compact en passant par les suites.

12.3.2. *Compacts d'un espace métrique*

• Si E est un espace métrique, un compact X de E est fermé dans E et borné, mais la réciproque est en générale fausse.

On a déjà vu qu'un compact est toujours fermé. Par ailleurs, si X est compact, et si $x_0 \in X$, alors $x \mapsto d(x_0, x)$ est continue sur X et donc est bornée puisque toute fonction continue à valeurs réelles sur un compact est bornée. Autrement dit, il existe $M \in \mathbf{R}_+$ tel que $X \subset B(x_0, M)$, et X est borné.

88. Si X_1 et X_2 sont des espaces métriques, on peut raisonner en termes de suites. Soit $(x_n, y_n)_{n\in\mathbf{N}}$ une suite d'éléments de $X_1 \times X_2$. Comme X_1 est compact, on peut extraire de la suite $(x_n)_{n\in\mathbf{N}}$ une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ ayant une limite a dans X_1. Comme X_2 est compact, on peut extraire de la suite $(y_{\varphi(n)})_{n\in\mathbf{N}}$ une sous-suite $(y_{\psi(n)})_{n\in\mathbf{N}}$ ayant une limite b dans X_2, et alors $(x_{\psi(n)}, y_{\psi(n)})_{n\in\mathbf{N}}$ admet (a, b) comme limite dans $X_1 \times X_2$ puisque $(x_{\psi(n)})_{n\in\mathbf{N}}$ est extraite de $(x_{\varphi(n)})_{n\in\mathbf{N}}$, et donc tend vers a dans X_1. Autrement dit la suite $(x_n, y_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence.

89. Plus généralement, un produit de compacts est toujours compact (Tychonov, 1935), mais la démonstration du cas général est un peu plus délicate et utilise l'axiome du choix.

Soit E le segment $[-1,1[$ de $\mathbf{R}$ muni de la distance induite par la valeur absolue sur $\mathbf{R}$; c'est un espace métrique parfaitement respectable. Alors $X = [0,1[$ est fermé dans E puisque c'est l'intersection de E avec le fermé $\mathbf{R}_+$ de $\mathbf{R}$, et il est borné. Il n'est pas compact car on ne peut pas extraire de recouvrement fini du recouvrement de X par les ouverts $U_n = X \cap]\frac{-1}{2}, 1 - \frac{1}{n}[$.

• Si E est un espace vectoriel *de dimension finie* sur $\mathbf{R}$ ou $\mathbf{C}$, alors les compacts de E sont les fermés bornés [90].

Par définition de la norme $\| \ \|_\infty$ sur $\mathbf{R}^n$, un borné de $\mathbf{R}^n$ est inclus dans $[-M, M]^n$, si M est assez grand. Or $[-M, M]$ est compact, puisque c'est l'image de $[0,1]$ par l'application continue $x \mapsto (2x-1)M$, et donc $[-M, M]^n$ est compact comme produit de compacts. Comme un fermé d'un compact est compact, on en déduit qu'un fermé borné de $(\mathbf{R}^n, \| \ \|_\infty)$ est compact. Le résultat dans le cas d'un $\mathbf{R}$ ou $\mathbf{C}$-espace vectoriel de dimension finie quelconque s'en déduit si on sait que deux normes sur un $\mathbf{R}$-espace vectoriel de dimension finie sont équivalentes (cf. n° 17.4), et donc que les fermés bornés sont les mêmes, quelle que soit la norme.

• Une fonction continue sur un compact non vide d'un espace métrique est uniformément continue (théorème de [91] Heine, 1872).

$f : X \to Y$, où X et Y sont des espaces métriques, est *uniformément continue* si

$$\forall \varepsilon > 0, \ \exists \delta > 0, \text{ tel que } d_X(x, x') < \delta \Rightarrow d_Y(y, y') < \varepsilon.$$

Supposons X compact. Soit $\varepsilon > 0$. Comme f est continue, pour tout $x \in X$, il existe $\delta_x > 0$ tel que $d_X(x, x') < 2\delta_x \Rightarrow d_Y(f(x), f(x')) < \frac{\varepsilon}{2}$. Les $B_X(x, \delta_x)$ forment un recouvrement [92] ouvert de X ; on peut donc en extraire un recouvrement fini $X = \cup_{x \in J} B_X(x, \delta_x)$, où $J \subset X$ est fini. Alors, par construction, si $x' \in X$, il existe $x \in J$ tel que $d_X(x, x') < \delta_x$. Soit alors $\delta = \inf_{x \in J} \delta_x$. Si $x_1, x_2 \in X$ vérifient $d_X(x_1, x_2) < \delta$, et si $x \in J$ est tel que $d_X(x, x_1) < \delta_x$, alors $d_X(x, x_2) < 2\delta_x$, et donc $d_Y(f(x), f(x_1)) < \frac{\varepsilon}{2}$, $d_Y(f(x), f(x_2)) < \frac{\varepsilon}{2}$ et $d_Y(f(x_2), f(x_1)) < \varepsilon$. Ceci montre que f est uniformément continue.

---

90. En filière PC, cette propriété est prise comme définition de compact ; on peut difficilement imaginer un point de vue plus nocif : être fermé est une notion relative (un ensemble est toujours fermé dans lui-même), alors que la compacité est une notion intrinsèque. Qui plus est, cette propriété devient fausse en dimension infinie, et les espaces de dimension infinie ne sont pas qu'une lubie de mathématicien.

91. Ce théorème a en fait été démontré par Dirichlet en 1854, pour les fonctions continues sur un segment, mais Heine a donné son nom à la continuité uniforme alors que Dirichlet se contentait de démontrer le résultat avec des ε et des δ en vue de justifier l'intégration de Cauchy pour les fonctions continues, ce que Cauchy avait omis de faire en confondant les notions de continuité et continuité uniforme.

92. Comme on travaille avec des espaces métriques, on peut aussi passer par les suites. Supposons donc que X est compact, que $f : X \to Y$ est continue mais pas uniformément continue. En niant la définition de la continuité uniforme rappelée ci-dessus, on voit qu'il existe $\varepsilon > 0$, tel que, quel que soit $n \in \mathbf{N}$, il existe $(x_n, x'_n) \in X \times X$ tels que $d_X(x_n, x'_n) \leqslant 2^{-n}$ et $d_Y(f(x_n), f(x'_n)) \geqslant \varepsilon$. Comme X est supposé compact, il en est de même de $X \times X$, et la suite $(x_n, x'_n)_{n \in \mathbf{N}}$ admet une valeur d'adhérence (a, b) dans $X \times X$. De plus, comme $d_X(x_n, x'_n) \to 0$, on a $a = b$, et comme f est continue, $(f(a), f(b))$ est une valeur d'adhérence de la suite $(f(x_n), f(x'_n))_{n \in \mathbf{N}}$ dans $Y \times Y$. Comme $f(a) = f(b)$, cela est en contradiction avec le fait que $d_Y(f(x_n), f(x'_n)) \geqslant \varepsilon$, quel que soit $n \in \mathbf{N}$ (en effet, $(y, y') \mapsto d_Y(y, y')$ est continue sur $Y \times Y$, et une valeur d'adhérence (c, c') de la suite $(f(x_n), f(x'_n))_{n \in \mathbf{N}}$ doit donc vérifier $d_Y(c, c') \geqslant \varepsilon > 0$). Ceci permet de conclure.

Exercice 12.4. — Soit $f : [a, b] \to \mathbf{R}$ une fonction dérivable.

(i) Montrer que si $f(a) = f(b)$, il existe $c \in]a, b[$ tel que $f'(c) = 0$ (lemme de Rolle).

(ii) Dans le cas général, montrer qu'il existe $c \in]a, b[$ tel que $f(b) - f(a) = f'(c)(b - a)$ (th. des accroissements finis [93]).

(iii) En déduire que f est strictement croissante sur $[a, b]$, si $f'(c) > 0$ pour tout $c \in]a, b[$.

Exercice 12.5. — Soit $(\mathrm{E}, \| \ \|)$ un espace vectoriel normé de dimension finie. On dit que $f : \mathrm{E} \to \mathbf{C}$ tend vers 0 à l'infini, si pour tout $\varepsilon > 0$, il existe $\mathrm{M} > 0$, tel que $|f(x)| < \varepsilon$, si $\|x\| \geqslant \mathrm{M}$. Montrer que, si $f : \mathrm{E} \to \mathbf{C}$ est continue et tend vers 0 à l'infini, alors f est bornée et $|f|$ atteint son maximum.

Exercice 12.6. — Soit (X, d) un espace métrique. Si $\mathrm{F} \subset \mathrm{X}$, et si $x \in \mathrm{X}$, on définit la distance $d(x, \mathrm{F})$ de x à F comme la borne inférieure des $d(x, y)$, pour $y \in \mathrm{F}$.

(i) Montrer que $x \mapsto d(x, \mathrm{F})$ est continue et même 1-lipschitzienne sur X.

(ii) Montrer que $d(x, \mathrm{F}) = 0$ si et seulement si x est dans l'adhérence $\overline{\mathrm{F}}$ de F.

(iii) En déduire que si F_1 et F_2 sont des fermés disjoints, il existe des ouverts disjoints U_1, U_2 avec $\mathrm{F}_1 \subset \mathrm{U}_1$ et $\mathrm{F}_2 \subset \mathrm{U}_2$.

(iv) On définit la distance entre F_1 et F_2 par $d(\mathrm{F}_1, \mathrm{F}_2) = \inf_{x \in \mathrm{F}_1,\ y \in \mathrm{F}_2} d(x, y)$. Montrer que si F_1 et F_2 sont des compacts disjoints, alors $d(\mathrm{F}_1, \mathrm{F}_2) > 0$.

(v) Montrer que si $\mathrm{F}_1 \cap \mathrm{F}_2 = \varnothing$, si F_1 est fermé et si F_2 est compact, alors $d(\mathrm{F}_1, \mathrm{F}_2) \neq 0$.

(vi) Construire des fermés disjoints de $\mathbf{R}$ ou $\mathbf{R}^2$ dont la distance est nulle.

Exercice 12.7. — Soient X un compact métrique et $f : \mathrm{X} \to \mathrm{X}$ une application contractante (i.e. vérifiant $d(f(x), f(y)) < d(x, y)$, quels que soient $x \neq y$).

(i) Montrer que f a un unique point fixe x_0.

(ii) Montrer que si $x \in \mathrm{X}$, et si $f^n = f \circ \cdots \circ f$ (n fois), alors $f^n(x) \to x_0$.

(iii) Montrer que $f^n \to x_0$ uniformément sur X (i.e. $\sup_{x \in \mathrm{X}} d(f^n(x), x_0) \to 0$ quand $n \to +\infty$).

Exercice 12.8. — (difficile) Soit X un espace métrique. Montrer que si toute fonction continue de X dans $\mathbf{R}$ est bornée, alors X est compact.

12.3.3. *Compacité locale*

La compacité d'un espace est une propriété très agréable, mais rarement vérifiée. Dans les applications, il suffit souvent que cette propriété soit vraie localement : on dit qu'un espace est *localement compact* si tout point possède une base de voisinages constituée de compacts.

• $\mathbf{R}$, $\mathbf{C}$ et, plus généralement, un espace vectoriel de dimension finie sur $\mathbf{R}$ ou $\mathbf{C}$ sont localement compacts.

• Un espace compact est localement compact.

> Soient X un compact et $x \in \mathrm{X}$. Comme X est séparé, il existe, pour tout $y \neq x$, des ouverts $\mathrm{U}_{x,y}$ et $\mathrm{V}_{x,y}$, d'intersection vide, contenant x et y respectivement. Il en résulte que y n'appartient pas à l'adherence $\mathrm{F}_{x,y}$ de $\mathrm{U}_{x,y}$, et donc que, si V est un ouvert contenant x et si F est son complémentaire, alors $\mathrm{F} \cap \big(\cap_{y \in \mathrm{X} - \{x\}} \mathrm{F}_{x,y} \big) = \varnothing$. Or F est compact, en tant que fermé d'un compact, et $\mathrm{F} \cap \mathrm{F}_{x,y}$ est fermé dans F pour tout y ; on en déduit l'existence d'un sous-ensemble fini Y de $\mathrm{X} - \{x\}$ tel que $\mathrm{F} \cap \big(\cap_{y \in \mathrm{Y}} \mathrm{F}_{x,y} \big) = \varnothing$. Soit $\mathrm{U}_{\mathrm{V}} = \cap_{y \in \mathrm{Y}} \mathrm{U}_{x,y}$; alors U_{V}

93. Voir l'ex. 15.6 pour une généralisation.

est un ouvert de X, en tant qu'intersection finie d'ouverts, qui contient x, et dont l'adhérence $\mathrm{F_V}$ est contenue dans V, puisque cette adhérence est contenue dans le fermé $\mathrm{F}_{x,y}$, pour tout $y \in \mathrm{Y}$. Comme $\mathrm{F_V}$ est compact, il résulte de ce qui précède, que tout ouvert V contenant x contient un compact $\mathrm{F_V}$ qui, lui-même, contient un ouvert $\mathrm{U_V}$ dont x est élément. Ceci prouve que les compacts forment une base de voisinage de x, et permet de conclure.

12.4. La droite réelle achevée

12.4.1. *Les espaces topologiques ordonnés* $\overline{\mathbf{R}}$ *et* $\overline{\mathbf{R}}_+$

On note $\overline{\mathbf{R}} = \mathbf{R} \cup \{\pm\infty\}$ la *droite réelle achevée*. On étend $\leqslant$ de manière naturelle en une relation d'ordre totale sur $\overline{\mathbf{R}}$, en convenant que $-\infty \leqslant a \leqslant +\infty$, quel que soit $a \in \overline{\mathbf{R}}$. On fait de $\overline{\mathbf{R}}$ un espace topologique, en prenant les $]a, b[$, pour $a < b \in \mathbf{R}$, et les $[-\infty, a[$ et $]a, +\infty]$, pour $a \in \mathbf{R}$, comme base d'ouverts. La topologie induite sur $\mathbf{R}$ est donc la topologie usuelle.

• Une suite de nombres réels x_n tend vers $+\infty$ dans $\overline{\mathbf{R}}$ si et seulement si x_n tend vers $+\infty$ au sens classique. (Idem pour $-\infty$.)

Les $]a, +\infty]$ forment une base de voisinages de $+\infty$, et donc $x_n \to +\infty$ dans $\overline{\mathbf{R}}$ si et seulement si, quel que soit $a \in \mathbf{R}$, il existe $\mathrm{N} \in \mathbf{N}$ tel que $x_n \in]a, +\infty]$, si $n \geqslant \mathrm{N}$.

• L'espace topologique $\overline{\mathbf{R}}$ est isomorphe à $[-1, 1]$ en tant qu'espace ordonné et en tant qu'espace topologique ; en particulier, il est compact et métrisable, et tout sous-ensemble non vide de $\overline{\mathbf{R}}$ admet une bonne inférieure et une borne supérieure.

L'application $x \mapsto f(x)$, avec $f(x) = \frac{x}{1+|x|}$, si $x \in \mathbf{R}$, $f(+\infty) = 1$ et $f(-\infty) = -1$, est un homéomorphisme strictement croissant de $\overline{\mathbf{R}}$ sur $[-1, 1]$, dont l'inverse est g défini par $g(x) = \frac{x}{1-|x|}$, si $x \in \mathbf{R}$, $g(1) = +\infty$, $g(-1) = -\infty$ (nous laissons au lecteur le soin de vérifier que f et g sont bien des applications continues inverses l'une de l'autre).

• Une suite $(x_n)_{n\in\mathbf{N}}$ croissante (resp. décroissante) d'éléments de $\overline{\mathbf{R}}$ converge vers la borne supérieure (resp. inférieure) de $\{x_n,\ n \in \mathbf{N}\}$.

• Si $\mathrm{X} \subset \overline{\mathbf{R}}$ est non vide, alors $\sup \mathrm{X}$ et $\inf \mathrm{X}$ sont dans l'adhérence de X.

En utilisant l'homéomorphisme $f : \overline{\mathbf{R}} \to [-1, 1]$, qui est strictement croissant, on se ramène à démontrer le même énoncé pour $\mathrm{X} \subset [-1, 1]$ ce qui permet de traiter tous les cas de la même manière. Maintenant, si la borne supérieure M de X appartient à X, elle appartient a fortiori à son adhérence. Si M n'appartient pas à X, alors pour tout $n > 0$, il existe $x_n \in \mathrm{X}$ avec $\mathrm{M} - 2^{-n} < x_n < \mathrm{M}$, ce qui prouve que M est limite d'une suite d'éléments de X et donc est dans son adhérence. Ceci permet de conclure.

On note $\overline{\mathbf{R}}_+$ la *demi-droite achevée*. C'est l'ensemble des $x \in \overline{\mathbf{R}}$ vérifiant $x \geqslant 0$. On étend l'addition à $\overline{\mathbf{R}}_+$ de la manière évidente, en posant $x + (+\infty) = +\infty$, si $x \in \overline{\mathbf{R}}_+$.

Comme toute suite croissante d'éléments de $\overline{\mathbf{R}}_+$ admet une limite dans $\overline{\mathbf{R}}_+$, on en déduit que :

• Toute série $\sum_{n\in\mathbf{N}} u_n$ à termes dans $\overline{\mathbf{R}}_+$ converge dans $\overline{\mathbf{R}}_+$. Si les u_n sont dans $\mathbf{R}_+$, alors $\sum_{n\in\mathbf{N}} u_n < +\infty$ si et seulement si la série $\sum_{n\in\mathbf{N}} u_n$ converge au sens usuel.

12.4.2. *Limite supérieure, limite inférieure*

• Toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ admet une plus grande valeur d'adhérence $\limsup x_n$, *limite supérieure* de la suite x_n et une plus petite valeur d'adhérence $\liminf x_n$, *limite inférieure* de la suite x_n. De plus, $(x_n)_{n\in\mathbf{N}}$ converge si et seulement si ses limites supérieure et inférieure sont égales, et la limite de la suite est alors la valeur commune des limites supérieure et inférieure [94].

La compacité de $\overline{\mathbf{R}}$ implique que l'ensemble des valeurs d'adhérence d'une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ est non vide. Comme cet ensemble est fermé, les bornes inférieure et supérieure de cet ensemble sont encore des valeurs d'adhérence ; autrement dit toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\overline{\mathbf{R}}$ admet une plus grande et une plus petite valeur d'adhérence. De plus, comme $\overline{\mathbf{R}}$ est un espace compact métrisable, une suite converge si et seulement si elle a une seule valeur d'adhérence et donc si et seulement si ses limites supérieure et inférieure sont égales. On en déduit le résultat.

• On a aussi $\limsup x_n = \inf\limits_{k\in\mathbf{N}} \big(\sup\limits_{n\geqslant k} x_n\big)$ et $\liminf x_n = \sup\limits_{k\in\mathbf{N}} \big(\inf\limits_{n\geqslant k} x_n\big)$.

Pour éviter d'avoir à traiter séparément les cas où une des limites est infinie, on utilise l'homéomorphisme $f : \overline{\mathbf{R}} \to [-1,1]$ ci-dessus pour se ramener au cas de suites à valeurs dans $[-1,1]$. Soient $a = \limsup x_n$ et $b = \inf_{k\in\mathbf{N}} \big(\sup_{n\geqslant k} x_n\big)$, et soit $\varepsilon > 0$. Comme a est une valeur d'adhérence, il existe pour tout $k \in \mathbf{N}$, un entier $n \geqslant k$ tel que $|x_n - a| < \varepsilon$. On a donc $\sup_{n\geqslant k} x_n \geqslant a - \varepsilon$, pour tout k, et donc $b \geqslant a - \varepsilon$, pour tout $\varepsilon > 0$. On en déduit que $b \geqslant a$. Par ailleurs, comme a est la plus grande valeur d'adhérence, il n'y a qu'un nombre fini de n tels que $x_n \geqslant a + \varepsilon$, et donc $\sup_{n\geqslant k} x_n \leqslant a + \varepsilon$, si k est assez grand, et $b \leqslant a + \varepsilon$, pour tout $\varepsilon > 0$. On en déduit que $b \leqslant a$, ce qui permet de démontrer la première égalité. La seconde se démontre de même en renversant les inégalités.

12.5. L'espace topologique $\mathbf{T} = \mathbf{R}/\mathbf{Z}$

$\mathbf{Z}$ étant un sous-groupe de $\mathbf{R}$ pour l'addition, on peut considérer le quotient $\mathbf{R}/\mathbf{Z}$ qui est un groupe commutatif ; on le munit de la topologie quotient, ce qui en fait un espace topologique.

• Si $\pi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ est l'application naturelle, l'application $f \mapsto f \circ \pi$ est une bijection de l'ensemble des fonctions sur $\mathbf{R}/\mathbf{Z}$ sur celui des fonctions sur $\mathbf{R}$ vérifiant $f(x+n) = f(x)$ pour tous $x \in \mathbf{R}$ et $n \in \mathbf{Z}$. Autrement dit, une fonction sur $\mathbf{R}/\mathbf{Z}$ est la même chose qu'une fonction périodique de période 1 sur $\mathbf{R}$. Par ailleurs, par définition de la topologie quotient, une fonction f sur $\mathbf{R}/\mathbf{Z}$ est continue si et seulement si $f \circ \pi$ est continue sur $\mathbf{R}$. Autrement dit, l'espace $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ des fonctions continues sur $\mathbf{R}/\mathbf{Z}$ s'identifie naturellement à l'espace des fonctions continues sur $\mathbf{R}$, périodiques de période 1.

94. Ça a l'air un peu tautologique, mais il est très utile de disposer des quantités $\limsup x_n$ et $\liminf x_n$ sans aucune hypothèse sur la suite $(x_n)_{n\in\mathbf{N}}$.

• L'application $x \mapsto \exp(2i\pi\, x)$ induit des homéomorphismes de $\mathbf{R}/\mathbf{Z}$ et $[0,1]/(0 \sim 1)$, munis de la topologie quotient, sur le cercle [95] $\mathrm{S}^1 = \{z \in \mathbf{C},\ |z| = 1\}$ muni de la topologie induite par celle de $\mathbf{C}$. En particulier, $\mathbf{R}/\mathbf{Z}$ est un espace compact métrisable.

Notons $\pi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ l'application naturelle et $f : \mathbf{R} \to \mathrm{S}^1$ l'application $x \mapsto \exp(2i\pi\, x)$. Comme f est périodique de période 1, elle induit une application $\overline{f}$ de $\mathbf{R}/\mathbf{Z}$ dans S^1 qui est bijective de manière évidente, et on a $f = \overline{f} \circ \pi$ par construction. De plus, f est continue de $\mathbf{R}$ dans $\mathbf{C}$, et donc $\overline{f}$ est continue de $\mathbf{R}/\mathbf{Z}$ (muni de la topologie quotient) dans S^1 (muni de la topologie induite par celle de $\mathbf{C}$). Comme f est injective et comme S^1 est séparé car métrique, on en déduit que $\mathbf{R}/\mathbf{Z}$ est séparé (cf. ex. 11.6).

Maintenant, l'application $x \mapsto x$ de $[0,1]$ dans $\mathbf{R}$ est continue, et donc la composée avec π est une application continue de $[0,1]$ dans $\mathbf{R}/\mathbf{Z}$ qui est surjective. Comme la seule relation modulo $\mathbf{Z}$ entre les éléments de $[0,1]$ est $0 \sim 1$, cette application continue induit, par passage au quotient, une injection continue $\iota : [0,1]/(0 \sim 1) \to \mathbf{R}/\mathbf{Z}$, et comme elle est surjective, c'est une bijection continue de $[0,1]/(0 \sim 1)$ sur $\mathbf{R}/\mathbf{Z}$. Comme $\mathbf{R}/\mathbf{Z}$ est séparé, on en déduit, par le même argument que ci-dessus, que $[0,1]/(0 \sim 1)$ est séparé. Comme $[0,1]$ est compact et comme l'application naturelle de $[0,1]$ dans $[0,1]/(0 \sim 1)$ est continue par définition de la topologie quotient, on en déduit, en utilisant les deux avant-derniers points de l'alinéa 12.3.1, que :

- $[0,1]/(0 \sim 1)$ est compact ;
- $\iota : [0,1]/(0 \sim 1) \to \mathbf{R}/\mathbf{Z}$ est un homéomorphisme et $\mathbf{R}/\mathbf{Z}$ est compact ;
- $\overline{f} : \mathbf{R}/\mathbf{Z} \to \mathrm{S}^1$ est un homéomorphisme.

Ceci permet de conclure.

Ces diverses identifications permettent de voir un *lacet* γ dans un espace topologique X comme, au choix :

- une application continue $\gamma : \mathrm{S}^1 \to \mathrm{X}$,
- une application continue $\gamma : \mathbf{R} \to \mathrm{X}$, périodique de période 1,
- une application continue $\gamma : \mathbf{R}/\mathbf{Z} \to \mathrm{X}$,
- une application continue $\gamma : [0,1] \to \mathrm{X}$ vérifiant $\gamma(1) = \gamma(0)$.

C'est cette dernière description qui est utilisée la plupart du temps dans le cours.

13. Connexité

13.1. Ensembles connexes

• Si X est un espace topologique, les propriétés suivantes sont équivalentes :

(i) toute application continue de X dans $\{0,1\}$ (muni de la topologie discrète) est constante ;

(ii) toute application continue de X dans un espace topologique discret Y est constante ;

(iii) X ne peut pas s'écrire comme réunion de deux ouverts non vides disjoints ;

(iv) X ne peut pas s'écrire comme réunion de deux fermés non vides disjoints ;

(v) si $\mathrm{Y} \subset \mathrm{X}$ est à la fois ouvert et fermé, alors $\mathrm{Y} = \varnothing$ ou $\mathrm{Y} = \mathrm{X}$.

95. Visuellement, si on prend un segment et qu'on attache ses deux extrémités, on obtient un cercle.

L'implication (ii)⇒(i) suit juste de ce que $\{0,1\}$ est un ensemble discret. Réciproquement, si Y est discret, toute application $g : \mathrm{Y} \to \{0,1\}$ est continue ; on en déduit que si X vérifie (i), et $f : \mathrm{X} \to \mathrm{Y}$ est continue, alors toute application composée $g \circ f : \mathrm{X} \to \{0,1\}$ est constante, ce qui implique que f est constante. Les conditions (i) et (ii) sont équivalentes.

Maintenant, si $f : \mathrm{X} \to \{0,1\}$ est continue, alors $\mathrm{U}_1 = f^{-1}(\{0\})$ et $\mathrm{U}_2 = f^{-1}(\{1\})$ sont ouverts puisque $\{0\}$ et $\{1\}$ sont ouverts dans $\{0,1\}$, sont disjoints, et $\mathrm{X} = \mathrm{U}_1 \cup \mathrm{U}_2$. Réciproquement, si U_1 et U_2 sont ouverts, disjoints, et si $\mathrm{X} = \mathrm{U}_1 \cup \mathrm{U}_2$, l'application $f : \mathrm{X} \to \{0,1\}$ définie par $f(x) = 0$, si $x \in \mathrm{U}_1$ et $f(x) = 1$ si $x \in \mathrm{U}_2$ est continue. On en déduit qu'il existe $f : \mathrm{X} \to \{0,1\}$ continue non constante si et seulement si on peut écrire X comme réunion de deux ouverts non vides disjoints ; d'où l'équivalence de (i) et (iii). L'équivalence des autres propriétés avec (iii) est immédiate.

Un espace topologique X est *connexe* s'il est non vide et vérifie une des (et donc toutes les) propriétés équivalentes précédentes.

• Si X_1 et X_2 sont deux ensembles connexes avec $\mathrm{X}_1 \cap \mathrm{X}_2 \neq \varnothing$, alors $\mathrm{X}_1 \cup \mathrm{X}_2$ est connexe.

Soit $f : \mathrm{X}_1 \cup \mathrm{X}_2 \to \{0,1\}$ continue. Les restrictions de f à X_1 et X_2 sont continues et donc constantes. Comme on a supposé $\mathrm{X}_1 \cap \mathrm{X}_2 \neq \varnothing$, on peut choisir $y \in \mathrm{X}_1 \cap \mathrm{X}_2$, et f vaut $f(y)$ sur X_1 et X_2 ; par suite elle est constante sur $\mathrm{X}_1 \cup \mathrm{X}_2$. On en déduit la connexité de $\mathrm{X}_1 \cup \mathrm{X}_2$.

Ceci permet, si X est un espace topologique quelconque, et $x \in \mathrm{X}$, de définir la *composante connexe* C_x de x dans X comme le plus grand sous-ensemble connexe de X contenant x ; c'est la réunion de tous les connexes de X contenant x. On appelle *composante connexe de* X tout sous-ensemble de la forme C_x, pour $x \in \mathrm{X}$. On a $y \in \mathrm{C}_x$ si et seulement si $\mathrm{C}_y = \mathrm{C}_x$, ce qui fait que les composantes connexes de X forment une partition de X, *la partition en composantes connexes*. Un ensemble est *totalement discontinu* si les composantes connexes sont réduites à un point.

• Dans $\mathbf{R}$, les connexes sont les segments (tous les segments, i.e. les $[a,b]$, $[a,b[$, $]a,b]$, $]a,b[$, pour $a, b \in \mathbf{R}$, ainsi que les demi-droites ou $\mathbf{R}$ tout entier obtenus en permettant à a ou b de prendre les valeurs $\pm\infty$).

Si $\mathrm{X} \subset \mathbf{R}$ n'est pas un segment, c'est qu'il existe $a \notin \mathrm{X}$ et $x_1, x_2 \in \mathrm{X}$, avec $x_1 < a$ et $x_2 > a$. Alors $\mathrm{U}_1 = \mathrm{X} \cap]-\infty, a[$ et $\mathrm{U}_2 = \mathrm{X} \cap]a, +\infty[$ sont des ouverts de X, qui sont non vides, disjoints, et dont la réunion est X, ce qui prouve que X n'est pas connexe. Autrement dit, si X est connexe, alors X est un segment.

Maintenant, soient $a \leqslant b$, et soit $f : [a,b] \to \{0,1\}$ continue. Quitte à remplacer f par $1-f$, on peut supposer que $f(a) = 0$. Soit $\mathrm{X} = \{x \in [a,b],\ f(x) = 1\}$, et soit c la borne inférieure de X, si X n'est pas vide. Par définition de c, il existe une suite d'éléments de X (qui peut être la suite constante c, si $c \in \mathrm{X}$) ayant pour limite c, et comme f est continue, on a $f(c) = 1$. En particulier, on a $c \neq a$, et si $x \in [a,c[$, alors $f(x) = 0$, par définition de c. Comme f est continue et comme c est dans l'adhérence de $[a,c[$, cela implique que $f(c) = 0$. D'où une contradiction qui prouve que X est vide et donc que f est constante sur $[a,b]$. On en déduit la connexité du segment $[a,b]$.

Pour prouver la connexité de $[a,b[$, on prend une suite croissante b_n tendant vers b, et on écrit $[a,b[$ comme réunion croissante des segments $[a,b_n]$ qui sont connexes d'après ce qui précède. Comme une réunion de connexes dont l'intersection est non vide est connexe, cela

prouve que $[a, b[$ est connexe. Les autres cas se traitant de la même manière, cela permet de conclure.

• L'image d'un ensemble connexe par une application continue est un ensemble connexe.

Si X est connexe, si $f : \mathrm{X} \to \mathrm{Y}$ est continue, et si $g : f(\mathrm{X}) \to \{0, 1\}$ est continue, alors $g \circ f : \mathrm{X} \to \{0, 1\}$ est continue, et donc constante puisque X est connexe. Comme $f : \mathrm{X} \to f(\mathrm{X})$ est surjective, cela implique que g est constante. On en déduit la connexité de $f(\mathrm{X})$.

• Soit $f : [a, b] \to \mathbf{R}$ continue. Si $f(a)$ et $f(b)$ sont de signes opposés, alors il existe $x \in [a, b]$ tel que $f(x) = 0$ (théorème des valeurs intermédiaires).

Comme $[a, b]$ est connexe, son image par f l'est aussi et donc est un segment de $\mathbf{R}$, et comme cette image contient des réels négatifs et positifs par hypothèse, elle contient 0.

• Si X et Y sont connexes, alors $\mathrm{X} \times \mathrm{Y}$ est connexe.

Soit $f : \mathrm{X} \times \mathrm{Y} \to \{0, 1\}$ continue. Si $x \in \mathrm{X}$, la restriction de f à $\{x\} \times \mathrm{Y}$ est continue et donc constante, et si $y \in \mathrm{Y}$, la restriction de f à $\mathrm{X} \times \{y\}$ est continue et donc constante. Ceci implique que si $(x_1, y_1), (x_2, y_2) \in \mathrm{X} \times \mathrm{Y}$, alors $f(x_2, y_2) = f(x_2, y_1) = f(x_1, y_1)$, et donc que f est constante. On en déduit la connexité de $\mathrm{X} \times \mathrm{Y}$.

• Si X est un espace topologique, et si $\mathrm{Y} \subset \mathrm{X}$ est connexe, alors l'adhérence de Y dans X est connexe.

Soit $f : \overline{\mathrm{Y}} \to \{0, 1\}$ continue. Comme Y est connexe, la restriction de f à Y est constante. Soit $a \in \{0, 1\}$ l'image de Y. Alors $f^{-1}(a)$ est un fermé de $\overline{\mathrm{Y}}$ contenant Y, et donc est égal à $\overline{\mathrm{Y}}$ par définition de l'adhérence. Autrement dit, f est constante. On en déduit la connexité de $\overline{\mathrm{Y}}$.

• Les composantes connexes d'un espace topologique sont fermées.

Exercice 13.1. — (i) Peut-on trouver $f : \mathbf{R} \to \mathbf{R}$, continue, prenant chaque valeur exactement 2 fois ?

(ii) Pour quelles valeurs de $n \geqslant 1$ peut-on trouver une fonction continue $f : \mathbf{R} \to \mathbf{R}$ prenant chaque valeur exactement n fois ?

13.2. Connexité par arcs

Un espace topologique X est dit *connexe par arcs* si, quels que soient $x, y \in \mathrm{X}$, il existe $u : [0, 1] \to \mathrm{X}$ continue, avec $u(0) = x$ et $u(1) = y$ (i.e. si on peut joindre n'importe quelle paire d'éléments de X par un chemin continu). Si X_1 et X_2 sont connexes par arcs, et si $\mathrm{X}_1 \cap \mathrm{X}_2$ est non vide, alors $\mathrm{X}_1 \cup \mathrm{X}_2$ est connexe par arcs puisqu'on peut joindre n'importe quel point de $\mathrm{X}_1 \cup \mathrm{X}_2$ a un point de l'intersection par un chemin continu, et donc n'importe quel couple de points de $\mathrm{X}_1 \cup \mathrm{X}_2$. Ceci permet, comme ci-dessus, de parler des *composantes connexes par arcs de* X.

• Un espace connexe par arcs est connexe [96], mais il existe des ensembles connexes qui ne sont pas connexes par arcs.

96. C'est le principal intérêt de la connexité par arcs ; la connexité est d'utilisation nettement plus facile.

Soit X connexe par arc, et soit $x_0 \in X$. Par hypothèse, il existe, pour tout $x \in X$, une application continue $u : [0,1] \to X$ avec $u(0) = x_0$ et $u(1) = x$. Comme $[0,1]$ est connexe et comme l'image d'un connexe par une application continue est connexe, cela montre que x est dans la composante connexe de x_0. Par suite la composante connexe de x_0 est X tout entier qui, de ce fait, est connexe.

Pour des exemples de connexes non connexes par arcs, voir la rubrique tératologie.

• Un ouvert connexe de $\mathbf{R}^n$ est connexe par arcs.

Soit U un ouvert connexe de $\mathbf{R}^n$, et soient $x_0 \in U$ et X la composante connexe par arcs de x_0. Soit $x \in X$. Comme U est ouvert, il existe $r > 0$ tel que $B(x,r)$ soit incluse dans U. Si $y \in B(x,r)$, le segment $[x,y]$ est inclus dans U, et comme il existe un chemin continu joignant x_0 à x dans U, il suffit de composer ce chemin avec le segment $[x,y]$ pour obtenir un chemin joignant x_0 à y dans U. On en déduit l'appartenance de y à X, et donc l'inclusion de $B(0,r)$ dans X, ce qui prouve que X est ouvert. Maintenant, soit x dans l'adhérence de X dans U, et soit $r > 0$ tel que $B(x,r)$ soit incluse dans U. Par définition de l'adhérence, il existe $y \in X \cap B(x,r)$, et comme le segment $[y,x]$ est contenu dans U, on déduit comme ci-dessus que $x \in X$, ce qui prouve que X est fermé. On a donc prouvé que X est à la fois ouvert et fermé dans U, et comme il est non vide et que U est supposé connexe, cela implique que $X = U$. Ceci permet de conclure.

• Un ouvert de $\mathbf{R}^n$ est une réunion dénombrable d'ouverts connexes. Un ouvert de $\mathbf{R}$ est une réunion dénombrable de segments ouverts.

Soit U un ouvert de $\mathbf{R}^n$. Si $x \in U$, il existe $r > 0$ tel que $B(x,r) \subset U$, et comme $B(x,r)$ est connexe par arcs (et même par segments), la composante connexe de x contient $B(x,r)$. On en déduit que les composantes connexes de U sont des ouverts. Maintenant, un ouvert de $\mathbf{R}^n$ contient un point dont toutes les coordonnées sont rationnelles, et comme les composantes connexes de U sont disjointes, on obtient une injection de l'ensemble de ces composantes connexes dans $\mathbf{Q}^n$, en choisissant un point à coordonnées rationnelles dans chacune d'entre elles. Comme $\mathbf{Q}^n$ est dénombrable, cela montre que l'ensemble des composantes connexes de U est dénombrable. On en déduit le premier énoncé. Le second en est une conséquence immédiate puisqu'un ouvert connexe de $\mathbf{R}$ est un segment ouvert.

Exercice 13.2. — Montrer que si $n \geqslant 2$, et si U est un ouvert connexe de $\mathbf{R}^n$, alors $U - \{x\}$ est connexe, quel que soit $x \in U$.

Exercice 13.3. — (i) Montrer que $\mathbf{R}$ et $\mathbf{R}^2$ ne sont pas homéomorphes ; que $[0,1]$ et $[0,1]^2$ ne sont pas homéomorphes.

(ii) Montrer que $[0,1]$ et le cercle $C = \{z \in \mathbf{C},\ |z| = 1\}$ ne sont pas homéomorphes.

Exercice 13.4. — Montrer que $[0,1]$ et $]0,1[$ ne sont pas homéomorphes.

Exercice 13.5. — Soit X le sous-ensemble de $\mathbf{R}$ constitué de trois cercles de rayon 1 dont les centres forment les trois sommets d'un triangle équilatéral dont la longueur des côtés est 2 (chacun des cercles est donc tangent aux deux autres). Soit Y formé de trois cercles de rayon 1 centrés en $(0,0)$, $(2,0)$ et $(4,0)$. Montrer que X et Y ne sont pas homéomorphes.

Exercice 13.6. — (difficile)

(i) Soit $(F_n)_{n\in\mathbf{N}}$ une suite décroissante $(F_{n+1} \subset F_n)$ de fermés connexes de $\mathbf{R}^2$, et soit $F = \cap_{n\in\mathbf{N}} F_n$.

(a) Donner un exemple où F n'est pas connexe.

(b) Montrer que, si F_0 est compact, alors F est connexe.

(ii) Soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathbf{R}^2$ telle que $d(x_{n+1}, x_n) \to 0$.

(a) Montrer que, si la suite est bornée, l'ensemble de ses valeurs d'adhérence est connexe.

(b) Est-ce forcément le cas si la suite n'est pas bornée ?

Exercice 13.7. — (difficile, sa solution utilise la notion d'espace contractile introduite plus tard dans le cours) Montrer que le cylindre et la bande de Moebius ne sont pas homéomorphes.

14. Complétude

14.1. Suites de Cauchy

Soit (X, d) un espace métrique. Une suite $(x_n)_{n\in\mathbf{N}}$ est *de Cauchy* (ou vérifie le *critère de Cauchy*) si le diamètre de $\{x_k,\ k \geqslant n\}$ tend vers 0 quand $n \to +\infty$, ce qui se traduit, au choix, par :

- quel que soit $\varepsilon > 0$, il existe $N \in \mathbf{N}$, tel que $d(x_{n+p}, x_n) < \varepsilon$, si $n \geqslant N$ et $p \in \mathbf{N}$;
- $\lim_{n\to+\infty} \big(\sup_{p\in\mathbf{N}} d(x_{n+p}, x_n)\big) = 0$.

On remarquera qu'une suite de Cauchy est en particulier bornée.

Exercice 14.1. — (i) Montrer que si d est ultramétrique, alors $(x_n)_{n\in\mathbf{N}}$ est de Cauchy si et seulement si $d(x_{n+1}, x_n) \to 0$.

(ii) Construire une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{R}$, vérifiant $d(x_{n+1}, x_n) \to 0$, mais pas de Cauchy.

- Une suite de Cauchy ayant au moins une valeur d'adhérence a une limite.

  Soit $(x_n)_{n\in\mathbf{N}}$ une suite de Cauchy. Supposons que a en soit une valeur d'adhérence. Comme X est un espace métrique, il existe une suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ extraite de $(x_n)_{n\in\mathbf{N}}$ ayant a pour limite. Soit alors $\varepsilon > 0$. Comme $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, il existe $N_0 \in \mathbf{N}$ tel que $d(x_{m+p}, x_m) < \varepsilon$, si $m \geqslant N_0$ et $p \in \mathbf{N}$. Comme $\varphi(n)$ tend vers $+\infty$, il existe $N_1 \in \mathbf{N}$ tel que $\varphi(n) \geqslant N_0$, si $n \geqslant N_1$, et comme $x_{\varphi(n)} \to a$, il existe $N_2 \geqslant N_1$ tel que $d(x_{\varphi(n)}, a) < \varepsilon$, si $n \geqslant N_2$. Alors $d(x_{\varphi(n)+p}, a) < 2\varepsilon$, si $n \geqslant N_2$ et $p \in \mathbf{N}$, et donc $d(x_m, a) < 2\varepsilon$, si $m \geqslant \varphi(N_2)$. On en déduit que $x_n \to a$, ce qui permet de conclure.

L'espace (X, d) est *complet* si toute suite de Cauchy admet une valeur d'adhérence ou, ce qui revient au même, une limite. Le critère qui suit permet de ne considérer que des suites convergeant "normalement".

- (X, d) est complet si et seulement si la condition $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$ implique que $(x_n)_{n\in\mathbf{N}}$ a une limite.

  Si $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$, alors $\sup_{p\in\mathbf{N}} d(x_n, x_{n+p}) \leqslant \sum_{k=0}^{+\infty} d(x_{n+k+1}, x_{n+k})$ tend vers 0 quand $n \to +\infty$ puisque majoré par le reste d'une série convergente. On en déduit que la suite $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, et donc converge si (X, d) est complet.

  Réciproquement, si toute suite $(x_n)_{n\in\mathbf{N}}$ telle que $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$ a une limite, et si $(y_n)_{n\in\mathbf{N}}$ est une suite de Cauchy, on peut en extraire une sous-suite $(y_{\varphi(n)})_{n\in\mathbf{N}}$ telle que $\sup_{p\in\mathbf{N}} d(y_{\varphi(n+p)}, y_{\varphi(n)}) \leqslant 2^{-n}$ quel que soit $n \in \mathbf{N}$. Il suffit de définir $\varphi(n)$ comme le N correspondant à $\varepsilon = 2^{-n}$ dans la définition d'une suite de Cauchy. La suite $x_n = y_{\varphi(n)}$ vérifie $\sum_{n=0}^{+\infty} d(x_{n+1}, x_n) < +\infty$; elle converge donc, et comme elle est extraite de $(y_n)_{n\in\mathbf{N}}$,

cela prouve que $(y_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence et donc une limite puisqu'elle est de Cauchy. On en déduit la complétude de X.

• Si (X, d) est complet, et si Y est fermé dans X, alors (Y, d) est complet.

Si $(x_n)_{n\in\mathbf{N}}$ est une suite de Cauchy dans Y, alors c'est une suite de Cauchy dans X ; elle a donc une limite dans X qui appartient à Y puisque Y est fermé. D'où la complétude de Y.

• Un espace métrique compact est complet.

Si $(x_n)_{n\in\mathbf{N}}$ est de Cauchy dans un espace métrique compact X, alors $(x_n)_{n\in\mathbf{N}}$ admet une valeur d'adhérence puisque X est compact, et donc converge d'après le point ci-dessus, ce qui prouve que X est complet.

D'après le point précédent, un espace compact est complet quelle que soit la distance utilisée pour définir la topologie. Ce n'est pas le cas en général : *la complétude est une propriété métrique et pas topologique.*

Exercice 14.2. — (i) Montrer que $d'(x,y) = |f(y) - f(x)|$, avec $f(x) = \frac{x}{1-|x|}$ est une distance sur $]-1,1[$ équivalente à la distance usuelle.
(ii) Montrer que $]-1,1[$ est complet pour d' mais pas pour la distance usuelle.

• $\mathbf{R}$ est complet.

Soit $(x_n)_{n\in\mathbf{N}}$ une suite de Cauchy d'éléments de $\mathbf{R}$. En particulier, la suite est bornée et il existe $\mathrm{M} > 0$ telle que $(x_n)_{n\in\mathbf{N}}$ soit à valeurs dans $[-\mathrm{M}, \mathrm{M}]$. Comme $[-\mathrm{M}, \mathrm{M}]$ est compact, cela implique que $(x_n)_{n\in\mathbf{N}}$ a une valeur d'adhérence, et donc qu'elle a une limite puisqu'elle est de Cauchy. Ceci permet de conclure.

• Si X et Y sont complets, alors $\mathrm{X} \times \mathrm{Y}$ est complet.

Si $(x_n, y_n)_{n\in\mathbf{N}}$ est une suite de Cauchy dans $\mathrm{X} \times \mathrm{Y}$, alors $(x_n)_{n\in\mathbf{N}}$ est de Cauchy dans X et $(y_n)_{n\in\mathbf{N}}$ est de Cauchy dans Y, et si a et b désignent les limites respectives de $(x_n)_{n\in\mathbf{N}}$ et $(y_n)_{n\in\mathbf{N}}$, alors $(x_n, y_n)_{n\in\mathbf{N}}$ tend vers (a, b). On en déduit la complétude de $\mathrm{X} \times \mathrm{Y}$.

14.2. Principales propriétés des espaces complets

L'intérêt principal de travailler dans un espace complet est que les problèmes d'existence sont nettement plus faciles. Le théorème du point fixe ci-dessous a de multiples applications à l'existence d'objets (solutions d'équations différentielles, racines de polynômes à coefficients réels, complexes, ou p-adiques, inversion locale de fonctions de classe $\mathscr{C}^1$...). Le lemme de Baire est un autre de ces outils magiques fournissant l'existence d'une in-

finité de solutions à des problèmes pour lesquels on a du mal à en exhiber une [97] ; son utilisation nécessite nettement plus d'astuce que celle du théorème du point fixe.

• Dans un espace complet, une application strictement contractante admet un unique point fixe, et la suite des itérés de tout point tend vers ce point fixe (th. du point fixe).

Soit (X, d) un espace métrique complet, soit $f : \mathrm{X} \to \mathrm{X}$ une application strictement contractante (i.e. il existe $\alpha < 1$ tel que $d(f(x), f(y)) \leqslant \alpha d(x, y)$ pour tous $x, y \in \mathrm{X}$), et soit $x \in \mathrm{X}$. Définissons par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ en posant $x_0 = x$ et $x_{n+1} = f(x_n)$, si $n \in \mathbf{N}$ (en notant f^n l'application $f \circ \cdots \circ f$ composée n fois, on a aussi $x_n = f^n(x)$). Soit $a = d(x_0, x_1)$. Une récurrence immédiate montre que $d(x_n, x_{n+1}) \leqslant \alpha^n a$ quel que soit $n \in \mathbf{N}$. On a donc, si $p \in \mathbf{N}$, et $n \in \mathbf{N}$

$$d(x_{n+p}, x_n) \leqslant d(x_n, x_{n+1}) + \cdots + d(x_{n+p-1}, x_{n+p}) \leqslant a(\alpha^n + \cdots + \alpha^{n+p-1}) \leqslant \alpha^n \frac{a}{1-\alpha}.$$

La suite $(x_n)_{n\in\mathbf{N}}$ est donc de Cauchy puisque α^n tend vers 0 quand n tend vers $+\infty$. Notons ℓ sa limite. Une application contractante étant en particulier continue, on a

$$f(\ell) = f(\lim_{n\to+\infty} x_n) = \lim_{n\to+\infty} f(x_n) = \lim_{n\to+\infty} x_{n+1} = \ell,$$

ce qui prouve que ℓ est un point fixe de f. On a donc prouvé que, si x est un point quelconque de X, alors la suite des itérés de x par f tend vers un point fixe de f. Maintenant, si x et y sont deux points fixes de f, on a $d(x, y) = d(f(x), f(y)) \leqslant \alpha d(x, y)$, et donc $d(x, y) = 0$, et $x = y$, ce qui prouve que f a un unique point fixe. Ceci permet de conclure.

• Dans un espace complet, l'intersection d'une suite de fermés emboités, non vides, dont le diamètre tend vers 0, est non vide et réduite à un point (th. des fermés emboités).

Soit (X, d) un espace métrique complet, et soit $(\mathrm{F}_n)_{n\in\mathbf{N}}$ une suite de fermés emboités (i.e. $\mathrm{F}_{n+1} \subset \mathrm{F}_n$ quel que soit $n \in \mathbf{N}$), non vides, dont le diamètre tend vers 0 (le *diamètre* d'un sous-ensemble Y de X est la borne supérieure de l'ensemble des $d(x, y)$, pour $x, y \in \mathrm{Y}$).

Choisissons, pour tout $n \in \mathbf{N}$, un élément x_n de F_n, et notons d_n le diamètre de F_n. Par hypothèse d_n tend vers 0 quand n tend vers $+\infty$. Par ailleurs, x_{n+p} et x_n sont deux éléments de F_n et donc $d(x_{n+p}, x_n) \leqslant d_n$ quels que soient $n, p \in \mathbf{N}$. La suite $(x_n)_{n\in\mathbf{N}}$ est donc de Cauchy. Comme X est supposé complet, cette suite admet une limite x. De plus, si on fixe m, alors $x_n \in \mathrm{F}_n \subset \mathrm{F}_m$, si $n \geqslant m$, et comme F_m est fermé, cela implique que $x \in \mathrm{F}_m$. Ceci étant vrai pour tout $m \in \mathbf{N}$, on a $x \in \mathrm{F} = \cap_{n\in\mathbf{N}}\mathrm{F}_n$, ce qui prouve que F est non vide. Enfin, si x, y sont deux éléments de F, on a $x, y \in \mathrm{F}_n$ pour tout $n \in \mathbf{N}$, et donc $d(x, y) \leqslant d_n$ quel que soit $n \in \mathbf{N}$. On en déduit la nullité de $d(x, y)$, ce qui implique $x = y$, et permet de conclure.

• Dans un espace complet, une intersection dénombrable d'ouverts denses est dense et donc, en particulier, est non vide (lemme de Baire).

Soit (X, d) un espace métrique complet, et soit $(\mathrm{U}_n)_{n\in\mathbf{N}}$ une suite d'ouverts denses de X. Notre but est de prouver que, si $x_0 \in \mathrm{X}$, et si $r_0 > 0$, alors $\mathrm{B}(x_0, r_0^-) \cap (\cap_{n\in\mathbf{N}}\mathrm{U}_n)$ est non vide. Pour cela, nous allons contruire une suite $\mathrm{B}(x_n, r_n)$ de boules fermées vérifiant :

$$0 < r_{n+1} \leqslant \tfrac{r_n}{2} \quad \text{et} \quad \mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-).$$

Supposons $\mathrm{B}(x_n, r_n)$ construite. Comme U_{n+1} est dense dans X, $\mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ est non vide. Prenons $x_{n+1} \in \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ quelconque. Comme $\mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$ est un ouvert,

97. On tombe alors sur le problème quasi-théologique de savoir si on peut vraiment prétendre avoir démontré qu'un ensemble est non vide si on est incapable d'en produire un élément.

il existe $r_{n+1} \in]0, \frac{r_n}{2}]$ tel que $\mathrm{B}(x_{n+1}, 2r_{n+1}^-) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$, et donc $\mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{U}_{n+1} \cap \mathrm{B}(x_n, r_n^-)$, ce qui permet de faire la construction à l'ordre $n+1$.

Maintenant, par construction, les $\mathrm{B}(x_n, r_n)$ forment une suite de fermés emboités (car on a imposé $\mathrm{B}(x_{n+1}, r_{n+1}) \subset \mathrm{B}(x_n, r_n^-)$) dont le diamètre tend vers 0 (car $r_{n+1} \leqslant \frac{r_n}{2}$), et $\mathrm{B}(x_n, r_n) \subset \mathrm{B}(x_0, r_0^-) \cap (\cap_{k \leqslant n} \mathrm{U}_k)$, si $n \geqslant 1$, ce qui implique que $\cap_{n \in \mathbf{N}} \mathrm{B}(x_n, r_n)$, qui est non vide d'après le théorème des fermés emboités, est inclus dans

$$\cap_{n \in \mathbf{N}} (\mathrm{B}(x_0, r_0^-) \cap (\cap_{k \leqslant n} \mathrm{U}_k)) = \mathrm{B}(x_0, r_0^-) \cap (\cap_{n \in \mathbf{N}} \mathrm{U}_n).$$

Ceci permet de conclure.

Le lemme de Baire s'utilise souvent en passant aux complémentaires.

• Dans un espace complet, une réunion dénombrable de fermés d'intérieur vide est d'intérieur vide ; autrement dit, si une réunion dénombrable de fermés est d'intérieur non vide, alors au moins un des fermés est d'intérieur non vide.

Exercice 14.3. — (i) Montrer qu'une intersection dénombrable d'ouverts denses de $\mathbf{R}$ est non dénombrable.

(ii) Peut-on trouver une suite $(f_n)_{n \in \mathbf{N}}$ de fonctions continues sur $\mathbf{R}$ telle que la suite des $f_n(x)$, pour $n \in \mathbf{N}$, soit bornée pour tout x irrationnel et non bornée pour tout x rationnel ?

14.3. Complétion d'un espace métrique

Un espace métrique n'est pas forcément complet, mais il peut se compléter de manière unique. Plus précisément :

• Si (X, d) est un espace métrique, il existe, à isométrie près, un unique espace métrique complet $(\widehat{\mathrm{X}}, d)$, contenant X comme sous-espace dense, qui vérifie la *propriété universelle* suivante : toute application uniformément continue f de X dans un espace métrique Y *complet* se prolonge de manière unique en une application continue de $\widehat{\mathrm{X}}$ dans Y.

Cet espace est le *complété de* X, et un espace complet est son propre complété ; plus généralement, si X est dense dans Y, et si Y est complet, alors Y est le complété de X.

L'unicité suit du résultat plus général (et très utile) suivant appliqué au cas où Y et Z sont deux complétés de X, et f est l'identité sur X, l'application $f : \mathrm{Y} \to \mathrm{Z}$ qu'on en tire est alors une isométrie puisque c'en est une sur X (cf. ex. 11.8).

• Soient $(\mathrm{Y}, d_{\mathrm{Y}})$ et $(\mathrm{Z}, d_{\mathrm{Z}})$ deux espaces complets. Si X est dense dans Y, et si $f : \mathrm{X} \to \mathrm{Z}$ est telle qu'il existe $\rho > 0$, tel que f soit uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x, \rho)$, pour tout $x \in \mathrm{X}$, alors f s'étend de manière unique en une application continue de Y dans Z.

Soit $y \in \mathrm{Y}$, et soit $(x_n)_{n \in \mathbf{N}}$ une suite d'éléments de X tendant vers y quand n tend vers $+\infty$. La suite $(x_n)_{n \in \mathbf{N}}$ est alors de Cauchy, et il existe $n \in \mathbf{N}$ tel que $x_n \in \mathrm{B}_{\mathrm{X}}(x_{n_0}, \rho)$, quel que soit $n \geqslant n_0$. Comme on a supposé que f est uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x_{n_0}, \rho)$, la suite $(f(x_n))_{n \in \mathbf{N}}$ est de Cauchy dans Z, et comme Z est complet, cette suite a une limite, et cette limite ne dépend pas de la suite $(x_n)_{n \in \mathbf{N}}$ de limite y (sinon on pourrait construire une telle suite de telle sorte que que $(f(x_n))_{n \in \mathbf{N}}$ ait deux valeurs d'adhérence). Notons cette limite $f(y)$.

Maintenant, soit $\varepsilon > 0$ et soit $x_0 \in \mathrm{X}$. Comme f est uniformément continue sur $\mathrm{B}_{\mathrm{X}}(x_0, \rho)$, il existe $\delta > 0$ tel que $d_{\mathrm{Z}}(f(x), f(x')) \leqslant \varepsilon$, si $d_{\mathrm{Y}}(x, x') < \delta$ et $x, x' \in \mathrm{B}_{\mathrm{X}}(x_0, \rho)$. Si $y_1, y_2 \in$

$\mathrm{B_Y}(x_0,\rho)$ vérifient $d_\mathrm{Y}(y_1,y_2)<\delta$, et si $(x_{1,n})_{n\in\mathbf{N}}$ et $(x_{2,n})_{n\in\mathbf{N}}$ sont des suites d'éléments de X tendant vers y_1 et y_2 respectivement, alors $x_{1,n},x_{2,n}\in\mathrm{B_X}(x_0,\rho)$ et $d_\mathrm{Y}(x_{1,n},x_{2,n})<\delta$ si n est assez grand. On a donc $d_\mathrm{Z}(f(x_{1,n}),f(x_{2,n}))\leqslant\varepsilon$ pour tout n assez grand, et un passage à la limite montre que $d_\mathrm{Z}(f(y_1),f(y_2))\leqslant\varepsilon$, ce qui prouve que f est uniformément continue sur $\mathrm{B_Y}(x_0,\rho)$. Comme les $\mathrm{B_Y}(x_0,\rho)$, pour $x_0\in\mathrm{X}$, recouvrent Y, puisque X est dense dans Y, cela permet de conclure.

L'existence se démontre en rajoutant [98] de force les limites des suites de Cauchy.

Pour ce faire, notons Cauchy(X) l'ensemble des suites de Cauchy à valeurs dans X. Si $\hat{x}=(x_n)_{n\in\mathbf{N}}$ et $\hat{y}=(y_n)_{n\in\mathrm{N}}$ sont deux éléments de Cauchy(X), la suite $(d(x_n,y_n))_{n\in\mathbf{N}}$ est de Cauchy dans $\mathbf{R}$ car

$$|d(x_{n+p},y_{n+p})-d(x_n,y_n)|=|d(x_{n+p},y_{n+p})-d(x_n,y_{n+p})+d(x_n,y_{n+p})-d(x_n,y_n)|\leqslant d(x_{n+p},x_n)+d(y_{n+p},y_n)$$

d'après l'inégalité triangulaire. Comme $\mathbf{R}$ est complet, cette suite admet une limite que l'on note $\hat{d}(\hat{x},\hat{y})$. De plus, si $\hat{x}=(x_n)_{n\in\mathbf{N}},\hat{y}=(y_n)_{n\in\mathbf{N}},\hat{z}=(z_n)_{n\in\mathbf{N}}$ sont trois éléments de Cauchy(X), un passage à la limite dans l'inégalité triangulaire $d(x_n,z_n)\leqslant d(x_n,y_n)+d(y_n,z_n)$ montre que $\hat{d}$ vérifie l'inégalité triangulaire $\hat{d}(\hat{x},\hat{z})\leqslant\hat{d}(\hat{x},\hat{y})+\hat{d}(\hat{y},\hat{z})$. De même, $\hat{d}$ vérifie la symétrie $\hat{d}(\hat{x},\hat{y})=\hat{d}(\hat{y},\hat{x})$, mais elle ne vérifie pas la séparation de la distance (i.e. il n'est pas vrai que $\hat{d}(\hat{x},\hat{y})=0$ implique $\hat{x}=\hat{y}$). De fait, il est assez clair que $\hat{d}(\hat{x},\hat{y})=0$ équivaut au fait que $\hat{x}$ et $\hat{y}$ ont moralement la même limite. Cela nous conduit à introduire la relation $\sim$ sur Cauchy(X) définie par, $\hat{x}\sim\hat{y}$ si et seulement si $\hat{d}(\hat{x},\hat{y})=0$, ce qui fait de $\sim$ une relation d'équivalence, et nous permet de considérer le quotient $\widehat{\mathrm{X}}$ de Cauchy(X) par cette relation d'équivalence (ce qui revient à considérer comme égaux deux éléments $\hat{x},\hat{y}$ de Cauchy(X) vérifiant $\hat{d}(\hat{x},\hat{y})=0$).

Il n'y a plus qu'à vérifier que l'objet que l'on a construit est bien celui que l'on voulait.

L'inégalité triangulaire montre que $\hat{d}(\hat{x},\hat{y})=\hat{d}(\hat{x}',\hat{y}')$ si $\hat{x}\sim\hat{x}'$ et $\hat{y}\sim\hat{y}'$, ce qui montre que $\hat{d}$ passe au quotient, et définit une distance sur $\widehat{\mathrm{X}}$ puisque, par définition de $\widehat{\mathrm{X}}$, la condition $\hat{d}(\hat{x},\hat{y})=0$ implique $\hat{x}=\hat{y}$.

On peut identifier $x\in\mathrm{X}$, à la classe dans $\widehat{\mathrm{X}}$ de la suite constante $\iota(x)=(x_n)_{n\in\mathbf{N}}$, avec $x_n=x$ pour tout $n\in\mathbf{N}$. Si $x,y\in\mathrm{X}$, on a $\hat{d}(x,y)=\hat{d}(\iota(x),\iota(y))=\lim_{n\to+\infty}d(x,y)=d(x,y)$, ce qui montre que $\hat{d}$ induit la distance d sur X. Par ailleurs, si $\hat{x}=(x_n)_{n\in\mathbf{N}}$ est un élément de Cauchy(X), alors $\hat{d}(\hat{x},\iota(x_k))=\lim_{n\to+\infty}d(x_n,x_k)\leqslant\sup_{n\geqslant k}d(x_n,x_k)$, et comme la suite $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, $\sup_{n\geqslant k}d(x_n,x_k)$ tend vers 0 quand k tend vers $+\infty$. On a donc $\hat{x}=\lim_{k\to+\infty}x_k$ dans $\widehat{\mathrm{X}}$, ce qui prouve que X est dense dans $\widehat{\mathrm{X}}$.

Il reste à prouver que $\widehat{\mathrm{X}}$ est complet. Pour cela soit $(\hat{x}_n)_{n\in\mathbf{N}}$ une suite de Cauchy dans $\widehat{\mathrm{X}}$. Comme X est dense dans $\widehat{\mathrm{X}}$, on peut trouver, quel que soit $n\in\mathbf{N}$, un élément x_n de X tel que $\hat{d}(\hat{x}_n,x_n)\leqslant 2^{-n}$. Soit $\hat{x}=(x_n)_{n\in\mathbf{N}}$. On a

$$d(x_n,x_{n+p})=\hat{d}(x_n,x_{n+p})\leqslant\hat{d}(x_n,\hat{x}_n)+\hat{d}(\hat{x}_n,\hat{x}_{n+p})+\hat{d}(\hat{x}_{n+p},x_{n+p})\leqslant 2^{1-n}+\hat{d}(\hat{x}_n,\hat{x}_{n+p}),$$

et comme la suite $(\hat{x}_n)_{n\in\mathbf{N}}$ est de Cauchy, on en déduit que $\hat{x}\in$ Cauchy(X). De plus,

$$\hat{d}(\hat{x}_n,\hat{x})\leqslant\hat{d}(\hat{x}_n,x_n)+\hat{d}(x_n,\hat{x})\leqslant 2^{-n}+\lim_{m\to+\infty}d(x_n,x_m)\leqslant 2^{-n}+\sup_{p\in\mathbf{N}}d(x_n,x_{n+p}),$$

98. Beaucoup d'objets mathématiques sont obtenus de cette manière, à commencer par $\mathbf{R}$ qui est le complété de $\mathbf{Q}$ pour la distance usuelle $d(x,y)=|x-y|$, où $|x-y|$ est la valeur absolue de $x-y$, et $\mathbf{Q}_p$ qui est le complété de $\mathbf{Q}$ pour la norme p-adique.

et comme $(x_n)_{n\in\mathbf{N}}$ est de Cauchy, $\sup_{p\in\mathbf{N}} d(x_n, x_{n+p}) \to 0$. Autrement dit, $\hat{x}_n \to \hat{x}$ dans $\widehat{\mathrm{X}}$. On en déduit la complétude de $\widehat{\mathrm{X}}$.

15. Séries numériques

Dans ce §, on passe en revue la théorie des séries de nombres complexes. Il s'agit d'un cas particulier de la théorie de l'intégration (on intègre sur un ensemble discret, dénombrable), et les énoncés sont formulés avec ce point de vue en tête.

15.1. Séries à termes positifs

Soit I un ensemble dénombrable [99]. Si $(x_i)_{i\in\mathrm{I}}$ est une famille d'éléments de $\overline{\mathbf{R}}_+$, on note $\sum_{i\in\mathrm{I}} x_i \in \overline{\mathbf{R}}_+$ la borne supérieure de l'ensemble des $\sum_{i\in\mathrm{J}} x_i$, où J décrit l'ensemble des parties finies de I : c'est la *somme* de la *série* $\sum_{i\in\mathrm{I}} x_i$ (noter de la même manière une série et sa somme peut parfois prêter à confusion, mais c'est le système que nous adopterons). On dit que la série $\sum x_i$ est *convergente* ou qu'elle *converge* si $\sum_{i\in\mathrm{I}} x_i < +\infty$; dans le cas contraire on dit que la série est *divergente* ou qu'elle *diverge*.

• Si $\sum_{i\in\mathrm{I}} x_i$ converge, alors $x_i \to 0$ quand [100] $i \to \infty$, mais il existe des familles vérifiant $x_i \to 0$ quand $i \to \infty$ sans que la série $\sum_{i\in\mathrm{I}} x_i$ converge [101].

On a $\frac{1}{n} \to 0$, mais $\sum_{n\geqslant 1} \frac{1}{n} = +\infty$ (voir ci-dessous [102]), ce qui prouve le second point. On démontre le premier en prenant la contraposée : si $x_i \not\to 0$, il existe $k \in \mathbf{N}$ et un sous-ensemble infini I′ de I tel que $x_i \geqslant 2^{-k}$, pour tout $i \in \mathrm{I}'$; on a alors $\sum_{i\in\mathrm{J}} x_i \geqslant 2^{-k}|\mathrm{J}|$, pour toute partie finie J de I contenue dans I′, et donc $\sup_{\mathrm{J}\subset\mathrm{I}'} \sum_{i\in\mathrm{J}} x_i = +\infty$, ce qui prouve que $\sum_{i\in\mathrm{I}} x_i = +\infty$, et permet de conclure.

• Si $x_i \leqslant y_i$, pour tout $i \in \mathrm{I}$, alors $\sum_{i\in\mathrm{I}} x_i \leqslant \sum_{i\in\mathrm{I}} y_i$ (monotomie de la somme).

On a $\sum_{i\in\mathrm{J}} x_i \leqslant \sum_{i\in\mathrm{J}} y_i$, pour tout $\mathrm{J} \subset \mathrm{I}$ fini. La borne supérieure de l'ensemble des $\sum_{i\in\mathrm{J}} x_i$ est donc inférieure ou égale à celle des $\sum_{i\in\mathrm{J}} y_i$.

• Si $\sum_{i\in\mathrm{I}} x_i < +\infty$, alors pour tout $\varepsilon > 0$, il existe $\mathrm{I}(\varepsilon) \subset \mathrm{I}$, fini, tel que $\sum_{i\in\mathrm{J}} x_i \leqslant \varepsilon$ pour tout $\mathrm{J} \subset \mathrm{I} - \mathrm{I}(\varepsilon)$. (Le reste d'une série convergente tend vers 0.)

Soit $\mathrm{S} = \sum_{i\in\mathrm{I}} x_i$. Par définition de S, il existe $\mathrm{I}(\varepsilon)$, fini, tel que $\sum_{i\in\mathrm{I}(\varepsilon)} x_i \geqslant \mathrm{S} - \varepsilon$. Maintenant, si $\mathrm{J} \subset \mathrm{I} - \mathrm{I}(\varepsilon)$ est fini, on a $\left(\sum_{i\in\mathrm{J}} x_i\right) + \left(\sum_{i\in\mathrm{I}(\varepsilon)} x_i\right) = \sum_{i\in\mathrm{J}\cup\mathrm{I}(\varepsilon)} x_i \leqslant \mathrm{S}$, et donc $\sum_{i\in\mathrm{J}} x_i \leqslant \varepsilon$. En passant à la borne supérieure, on voit que l'on a encore $\sum_{i\in\mathrm{J}} x_i \leqslant \varepsilon$, si $\mathrm{J} \subset \mathrm{I} - \mathrm{I}(\varepsilon)$ n'est pas fini.

---

99. On peut définir de même la somme d'un nombre non dénombrable d'éléments de $\overline{\mathbf{R}}_+$ mais comme $\overline{\mathbf{R}}_+ - \{0\} = \cup_{n\in\mathbf{N}}[2^{-n}, +\infty]$, on voit que l'on est dans un des deux cas exclusifs suivants :
• il existe $n \in \mathbf{N}$ tel que $[2^{-n}, +\infty]$ contient un nombre non dénombrable de x_i et alors $\sum_{i\in\mathrm{I}} x_i = +\infty$,
• l'ensemble J des i tels que $x_i \neq 0$ est dénombrable et $\sum_{i\in\mathrm{I}} x_i = \sum_{i\in\mathrm{J}} x_i$.
L'étude des séries convergentes se ramène donc au cas dénombrable.

100. Cela veut dire que, pour tout $\varepsilon > 0$, l'ensemble des $i \in \mathrm{I}$ vérifiant $|x_i| > \varepsilon$ est fini.

101. Ce désagrément est absent du monde p-adique ou, plus généralement, ultramétrique... (alinéa 20.4.1)

102. La divergence de la série harmonique $\sum_{n\geqslant 1} \frac{1}{n}$ est due à N. Oresme (1360).

• Si $n \mapsto i(n)$ est une bijection de $\mathbf{N}$ sur I, alors $\sum_{i\in \mathrm{I}} x_i$ est la limite de la suite des sommes partielles $\sum_{n\leqslant \mathrm{N}} x_{i(n)}$. Autrement dit, on peut sommer une série à termes positifs dans l'ordre que l'on veut : l'addition des nombres positifs est commutative !

Posons $\mathrm{S} = \sum_{i\in \mathrm{I}} x_i$. La suite $y_{\mathrm{N}} = \sum_{n\leqslant \mathrm{N}} x_{i(n)}$ est croissante ; elle a donc une limite ℓ dans $\overline{\mathbf{R}}_+$ qui est aussi la borne supérieure de $\{y_{\mathrm{N}},\ \mathrm{N}\in\mathbf{N}\}$. Maintenant, l'ensemble des y_{N}, pour $\mathrm{N}\in\mathbf{N}$, est inclus dans celui des $\sum_{i\in \mathrm{J}} x_i$, pour J décrivant les parties finies de I ; on en déduit l'inégalité $\ell \leqslant \mathrm{S}$ des bornes supérieures. Réciproquement, soit $\mathrm{M} < \mathrm{S}$. Par définition de S, il existe $\mathrm{J}\subset \mathrm{I}$, fini, tel que $\sum_{i\in \mathrm{J}} x_i \geqslant \mathrm{M}$, et comme $n\mapsto i(n)$ est surjective, il existe $\mathrm{N}\in\mathbf{N}$ tel que $\mathrm{J}\subset\{i(n),\ n\leqslant \mathrm{N}\}$; on a alors $y_{\mathrm{N}}\geqslant \mathrm{M}$ et donc $\ell\geqslant \mathrm{M}$. Ceci étant vrai pour tout $\mathrm{M}<\mathrm{S}$, on en déduit l'inégalité $\ell\geqslant \mathrm{S}$ qui permet de conclure.

• Si $\lambda,\mu\in\mathbf{R}_+$, alors $\sum_{i\in \mathrm{I}}(\lambda x_i+\mu y_i) = \lambda\big(\sum_{i\in \mathrm{I}} x_i\big)+\mu\big(\sum_{i\in \mathrm{I}} y_i\big)$, avec la convention $0\cdot(+\infty)=0$ et $a\cdot(+\infty)=+\infty$ si $a>0$ (linéarité de la somme).

Il suffit de choisir une bijection $n\mapsto i(n)$ de $\mathbf{N}$ sur I, et de passer à la limite dans l'égalité de sommes finies $\sum_{n\leqslant \mathrm{N}}(\lambda x_{i(n)}+\mu y_{i(n)}) = \lambda\big(\sum_{n\leqslant \mathrm{N}} x_{i(n)}\big)+\mu\big(\sum_{n\leqslant \mathrm{N}} y_{i(n)}\big)$.

• Si les I_j, pour $j\in\mathrm{J}$, forment une partition de I, alors $\sum_{i\in \mathrm{I}} x_i = \sum_{j\in \mathrm{J}}\big(\sum_{i\in \mathrm{I}_j} x_i\big)$. Autrement dit, dans une série à termes positifs, on peut regrouper les termes comme on veut : l'addition des nombres positifs est associative !

Soit $\mathrm{S}=\sum_{i\in \mathrm{I}} x_i$ et $\mathrm{S}_j=\sum_{i\in \mathrm{I}_j} x_i$, si $j\in\mathrm{J}$. Avant de prouver que $\mathrm{S}=\sum_{j\in \mathrm{J}}\mathrm{S}_j$, commençons par montrer que, si K est fini, et si Y_k, pour $k\in\mathrm{K}$, est un sous-ensemble de $\overline{\mathbf{R}}_+$ de borne supérieure M_k, alors la borne supérieure M de l'ensemble des $\sum_{k\in \mathrm{K}} y_k$, où $(y_k)_{k\in \mathrm{K}}$ décrit $\prod_{k\in \mathrm{K}}\mathrm{Y}_k$, est $\sum_{k\in \mathrm{K}}\mathrm{M}_k$. En effet, on a $y_k\leqslant \mathrm{M}_k$ pour tout k, et donc $\sum_{k\in \mathrm{K}} y_k\leqslant\sum_{k\in \mathrm{K}}\mathrm{M}_k$, pour tout $(y_k)_{k\in \mathrm{K}}\in\prod_{k\in \mathrm{K}}\mathrm{Y}_k$, ce qui nous fournit l'inégalité $\mathrm{M}\leqslant\sum_{k\in \mathrm{K}}\mathrm{M}_k$; réciproquement, si $\mathrm{M}'<\sum_{k\in \mathrm{K}}\mathrm{M}_k$, on peut écrire M' sous la forme $\sum_{k\in \mathrm{K}}\mathrm{M}'_k$, avec $\mathrm{M}'_k<\mathrm{M}_k$, pour tout $k\in\mathrm{K}$, et il existe $y_k\in\mathrm{Y}_k$ tel que $y_k\geqslant \mathrm{M}'_k$, ce qui implique que $\sum_{k\in \mathrm{K}} y_k\geqslant \mathrm{M}'$, et donc $\mathrm{M}\geqslant\mathrm{M}'$, d'où l'inégalité $\mathrm{M}\geqslant\sum_{k\in \mathrm{K}}\mathrm{M}_k$.

On peut appliquer ce qui précède à un sous-ensemble fini K de J et, pour $k\in\mathrm{K}$, à l'ensemble Y_k des $\sum_{i\in \mathrm{I}'} x_i$, où I' décrit l'ensemble des parties finies de I_k, de telle sorte que $\mathrm{M}_k=\sum_{i\in \mathrm{I}_k} x_i$. Comme l'ensemble des $\sum_{k\in \mathrm{K}} y_k$, pour $(y_k)_{k\in \mathrm{K}}\in\prod_{k\in \mathrm{K}}\mathrm{Y}_k$ est inclus dans celui des $\sum_{i\in \mathrm{L}} x_i$, pour L décrivant l'ensemble des parties finies de I, on a $\sum_{k\in \mathrm{K}}\mathrm{S}_k\leqslant\mathrm{S}$, pour tout sous-ensemble fini K de J. On en déduit l'inégalité $\sum_{j\in \mathrm{J}}\mathrm{S}_j\leqslant\mathrm{S}$.

Réciproquement, soit $\mathrm{M}<\mathrm{S}$. Il existe alors $\mathrm{L}\subset\mathrm{I}$, fini, tel que $\sum_{i\in \mathrm{L}} x_i\geqslant\mathrm{M}$, et $\mathrm{K}\subset\mathrm{J}$, fini, tel que $\mathrm{L}\subset\cup_{j\in \mathrm{K}}\mathrm{I}_k$. On a alors $\mathrm{M}\leqslant\sum_{k\in \mathrm{K}}\mathrm{S}_k$, et donc $\mathrm{M}\leqslant\sum_{j\in \mathrm{J}}\mathrm{S}_j$; on en déduit l'inégalité $\mathrm{S}\leqslant\sum_{j\in \mathrm{J}}\mathrm{S}_j$, ce qui permet de conclure.

• Si $(x_{i,j})_{(i,j)\in \mathrm{I}\times\mathrm{J}}$ est à termes positifs, $\sum_{j\in \mathrm{J}}\big(\sum_{i\in \mathrm{I}} x_{i,j}\big) = \sum_{(i,j)\in \mathrm{I}\times\mathrm{J}} x_{i,j} = \sum_{i\in \mathrm{I}}\big(\sum_{j\in \mathrm{J}} x_{i,j}\big)$ (Fubini pour les séries à termes positifs).

C'est un cas particulier du point précédent : on partitionne $\mathrm{I}\times\mathrm{J}$ comme la réunion des $\mathrm{I}\times\{j\}$, pour $j\in\mathrm{J}$, ou comme la réunion des $\{i\}\times\mathrm{J}$, pour $i\in\mathrm{I}$.

• Si $(x_i^{(n)})_{i\in \mathrm{I}}$, pour $n\in\mathbf{N}$, est une suite croissante [103] de familles d'éléments de $\overline{\mathbf{R}}_+$, alors $\lim_{n\to+\infty}\sum_{i\in \mathrm{I}} x_i^{(n)} = \sum_{i\in \mathrm{I}}\big(\lim_{n\to+\infty} x_i^{(n)}\big)$ (th. de convergence monotone pour les séries).

103. I.e. $x_i^{(n)}\leqslant x_i^{(n+1)}$, pour tout $i\in\mathrm{I}$ et tout $n\in\mathbf{N}$.

Posons $x_{0,i} = x_i^{(0)}$ et $x_{n,i} = x_i^{(n)} - x_i^{(n-1)}$, si $n \geqslant 1$ (avec la convention $(+\infty) - (+\infty) = 0$). L'hypothèse de croissance fait que $x_{n,i} \in \overline{\mathbf{R}}_+$, et on a $x_i^{(\mathrm{N})} = \sum_{n \leqslant \mathrm{N}} x_{n,i}$, et donc $\lim_{n\to+\infty} x_i^{(n)} = \sum_{n\in\mathbf{N}} x_{n,i}$, si $i \in \mathrm{I}$. Maintenant, $\sum_{i\in\mathrm{I}} x_i^{(n)} = \sum_{j\leqslant n}\sum_{i\in\mathrm{I}} x_{j,i}$ par linéarité de la somme, et donc $\lim_{n\to+\infty}\sum_{i\in\mathrm{I}} x_i^{(n)} = \sum_{j\in\mathbf{N}}\sum_{i\in\mathrm{I}} x_{j,i}$. D'aprés le th. de Fubini, ceci est aussi égal à $\sum_{i\in\mathrm{I}}\sum_{j\in\mathbf{N}} x_{j,i}$, c'est-à-dire à $\sum_{i\in\mathrm{I}}\big(\lim_{n\to+\infty} x_i^{(n)}\big)$, ce qui permet de conclure.

• Soient $(x_i)_{i\in\mathrm{I}}$ et $(y_i)_{i\in\mathrm{I}}$ deux familles de nombres positifs. On suppose qu'il existe $\mathrm{C} \in \mathbf{R}_+^*$ tel que $x_i \leqslant \mathrm{C}y_i$ pour tout $i \in \mathrm{I}$. Alors la convergence de $\sum_{i\in\mathrm{I}} y_i$ implique celle de $\sum_{i\in\mathrm{I}} x_i$ et la divergence de $\sum_{i\in\mathrm{I}} x_i$ implique celle de $\sum_{i\in\mathrm{I}} y_i$.

On a $\sum_{i\in\mathrm{J}} x_i \leqslant \mathrm{C}\sum_{i\in\mathrm{J}} y_i$ pour toute partie finie J de I, et donc $\sum_{i\in\mathrm{I}} x_i \leqslant \mathrm{C}\sum_{i\in\mathrm{I}} y_i$. On en déduit le résultat.

Le critère précédent, couplé avec les résultats concernant les séries de référence ci-dessous, permet de démontrer la convergence ou la divergence de la plupart des séries raisonnables.

15.2. Séries standard

• *séries géométriques.*— Soit $a \in \mathbf{R}_+^*$. Alors $\sum_{n\in\mathbf{N}} a^n$ converge si $a < 1$ et diverge si $a \geqslant 1$.

Si $a \geqslant 1$, la suite a^n ne tend pas vers 0, et donc la série diverge. Si $a < 1$, alors $\sum_{n\leqslant\mathrm{N}} a^n = \frac{1-a^{n+1}}{1-a} \leqslant \frac{1}{1-a}$ pour tout N, et donc la série converge (sa somme est égale à $\frac{1}{1-a}$).

• *séries de Riemann.*— Soit $s \in \mathbf{R}$. Alors $\sum_{n\geqslant 1} \frac{1}{n^s}$ converge si $s > 1$ et diverge si $s \leqslant 1$.

Il y a plusieurs manières d'arriver au résultat. La plus naturelle est probablement de comparer la série avec l'intégrale de la fonction x^{-s}.

• Si $s > 1$, on a $x^{-s} \geqslant n^{-s}$ sur $[n-1, n]$, on en déduit que $\sum_{n=1}^{\mathrm{N}} n^{-s} \leqslant 1 + \sum_{n=2}^{\mathrm{N}}\int_{n-1}^{n} x^{-s}\,dx \leqslant 1 + \int_1^{\mathrm{N}} x^{-s}\,dx = 1 + \frac{1}{s-1}(1 - \mathrm{N}^{1-s}) \leqslant 1 + \frac{1}{s-1}$, ce qui prouve la convergence de la série.

• Si $s = 1$, on a $\frac{1}{n} \geqslant \frac{1}{x}$ sur $[n, n+1]$ et donc $\sum_{n=1}^{\mathrm{N}} \frac{1}{n} \geqslant \sum_{n=1}^{\mathrm{N}}\int_n^{n+1} \frac{1}{x}\,dx = \int_1^{\mathrm{N}+1} \frac{1}{x}\,dx = \log(\mathrm{N}+1)$, ce qui prouve la divergence de la série.

On peut aussi remarquer que, si on pose $u_n = \log(n+1) - \log n - \frac{1}{n} = \log(1+\frac{1}{n}) - \frac{1}{n}$, alors $u_n = \mathrm{O}(\frac{1}{n^2})$, ce qui prouve que la série $\sum_{n\geqslant 1} u_n$ converge puisque $\sum_{n\geqslant 1} \frac{1}{n^2} < +\infty$ d'après ce qui précède. Or $\sum_{n=1}^{\mathrm{N}} u_n = \log(\mathrm{N}+1) - \sum_{n=1}^{\mathrm{N}} \frac{1}{n}$; on en déduit que la suite de terme général $\sum_{n=1}^{\mathrm{N}} \frac{1}{n} - \log \mathrm{N}$ a une limite quand $\mathrm{N} \to \infty$ (cette limite est la *constante d'Euler*; elle est souvent notée γ), ce qui prouve, en particulier, que $\sum_{n\geqslant 1} \frac{1}{n}$ diverge.

• si $s < 1$, on a $\frac{1}{n^s} \geqslant \frac{1}{n}$, et on déduit la divergence de $\sum_{n\geqslant 1} \frac{1}{n^s}$ de celle de $\sum_{n\geqslant 1} \frac{1}{n}$.

Exercice 15.1. — Soit $(a_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathbf{R}_+^*$ telle que $\sum_{n\in\mathbf{N}} a_n = +\infty$. Si $n \in \mathbf{N}$, on note S_n la somme partielle $\sum_{i\leqslant n} a_i$.

(i) Montrer que $\sum_{n\in\mathbf{N}} \frac{a_n}{\mathrm{S}_n^2} < +\infty$. (On comparera la série à une intégrale.)

(ii) Montrer que $\sum_{n\in\mathbf{N}} \frac{a_n}{\mathrm{S}_n} = +\infty$. (On pourra séparer les cas $\limsup \frac{a_n}{\mathrm{S}_n} = 1$ et $\limsup \frac{a_n}{\mathrm{S}_n} < 1$.)

• *séries de Riemann en plusieurs variables.*— Soient $d \in \mathbf{N}$, $\|\ \|$ une norme sur $\mathbf{R}^d$ (par exemple la norme euclidienne), et $s \in \mathbf{R}$. Alors $\sum_{\mathbf{n}} \frac{1}{\|\mathbf{n}\|^s}$ converge si $s > d$ et diverge si $s \leqslant d$, la somme portant sur $\mathbf{n} = (n_1, \ldots, n_d) \in \mathbf{Z}^d - \{(0, \ldots, 0)\}$.

Toutes les normes étant équivalentes sur $\mathbf{R}^d$, il suffit de prouver le résultat pour l'une d'entre elles, par exemple $\|(x_1,\dots,x_d)\| = \sup_{1\leqslant i\leqslant d}|x_i|$. Si $\mathrm{N}\in\mathbf{N}$ il y a $(2n+1)^d-(2n-1)^d$ d-uplets $\mathbf{n}$ vérifiant $\|\mathbf{n}\|=n$, et la convergence de la série qui nous intéresse est équivalente à celle de $\sum_{n\geqslant 1}\frac{(2n+1)^d-(2n-1)^d}{n^s}$. Comme $(2n+1)^d-(2n-1)^d = 2d(2n)^{d-1}+\mathrm{O}(n^{d-2})$, cette convergence est équivalente à celle de $\sum_{n\geqslant 1}\frac{n^{d-1}}{n^s}$, ce qui permet de déduire le résultat du cas des séries de Riemann ordinaires.

15.3. Séries absolument convergentes

Si $z\in\mathbf{C}$, on note $\mathrm{Re}^+(z)$ l'élément $\sup(0,\mathrm{Re}(z))$ de $\mathbf{R}_+$. On a alors [104]

$$z=\sum_{k=0}^{3}\mathbf{i}^k\mathrm{Re}^+(\mathbf{i}^{-k}z)\ \text{ et }\ 0\leqslant\sup_{0\leqslant k\leqslant 3}\mathrm{Re}^+(\mathbf{i}^{-k}z)\leqslant|z|\leqslant\sum_{k=0}^{3}\mathrm{Re}^+(\mathbf{i}^{-k}z).$$

Soit I un ensemble dénombrable. Si $(x_i)_{i\in\mathrm{I}}$ est une famille d'éléments de $\mathbf{C}$, on dit que la série $\sum_{i\in\mathrm{I}}x_i$ est *absolument convergente* si $\sum_{i\in\mathrm{I}}|x_i|<+\infty$ (i.e. si la série des modules est convergente). Il résulte des encadrements ci-dessus que cette condition équivaut à $\sum_{i\in\mathrm{I}}\mathrm{Re}^+(\mathbf{i}^kx_i)<+\infty$, pour $k\in\{0,1,2,3\}$, et on définit la *somme de la série* $\sum_{i\in\mathrm{I}}x_i$ par la formule

$$\sum_{i\in\mathrm{I}}x_i=\sum_{k=0}^{3}\mathbf{i}^k\Big(\sum_{i\in\mathrm{I}}\mathrm{Re}^+(\mathbf{i}^{-k}x_i)\Big).$$

• $\sum_{i\in\mathrm{I}}x_i$ est absolument convergente si et seulement si elle vérifie le *critère de Cauchy* : pour tout $\varepsilon>0$, il existe $\mathrm{I}(\varepsilon)\subset\mathrm{I}$ fini tel que $\big|\sum_{i\in\mathrm{J}}x_i\big|\leqslant\varepsilon$ pour tout $\mathrm{J}\subset\mathrm{I}-\mathrm{I}(\varepsilon)$ fini.

Si $\sum_{i\in\mathrm{I}}|x_i|<+\infty$ et si $\varepsilon>0$, il existe $\mathrm{I}(\varepsilon)\subset\mathrm{I}$, fini, tel que $\sum_{i\in\mathrm{I}(\varepsilon)}|x_i|\geqslant\big(\sum_{i\in\mathrm{I}}|x_i|\big)-\varepsilon$, par définition de $\sum_{i\in\mathrm{I}}|x_i|$ comme borne supérieur de l'ensemble des sommes partielles finies. On a alors $\sum_{i\in\mathrm{I}-\mathrm{I}(\varepsilon)}|x_i|\leqslant\varepsilon$, et donc $\big|\sum_{i\in\mathrm{J}}x_i\big|\leqslant\varepsilon$ pour tout $\mathrm{J}\subset\mathrm{I}-\mathrm{I}(\varepsilon)$ fini, ce qui prouve que $\sum_{i\in\mathrm{I}}x_i$ vérifie le critère de Cauchy.

Si $\sum_{i\in\mathrm{I}}|x_i|=+\infty$, il existe $k\in\{0,1,2,3\}$ tel que $\sum_{i\in\mathrm{I}}\mathrm{Re}^+(\mathbf{i}^{-k}x_i)=+\infty$ et, quitte à remplacer x_i par $\mathbf{i}^{-k}x_i$, on peut supposer que $k=0$. Soit $\mathrm{I}'=\{i\in\mathrm{I},\ \mathrm{Re}(x_i)>0\}$; on a $\sum_{i\in\mathrm{I}'}\mathrm{Re}(x_i)=\sum_{i\in\mathrm{I}}\mathrm{Re}^+(x_i)=+\infty$ puique $\mathrm{Re}^+(x_i)=0$ si $\mathrm{Re}(x_i)\leqslant 0$. On en déduit que, quel que soit $\mathrm{J}\subset\mathrm{I}$ fini, il existe $\mathrm{J}'\subset\mathrm{I}'-(\mathrm{J}\cap\mathrm{I}')$ avec $\sum_{i\in\mathrm{J}'}\mathrm{Re}(x_i)\geqslant 1$, et donc $\big|\sum_{i\in\mathrm{J}'}x_i\big|\geqslant 1$, ce qui prouve que $\sum_{i\in\mathrm{I}}x_i$ ne vérifie pas le critère de Cauchy, et permet de conclure.

• Si $\sum_{i\in\mathrm{I}}x_i$ est absolument convergente, et si $n\mapsto i(n)$ est une bijection de $\mathbf{N}$ sur I, alors $\sum_{i\in\mathrm{I}}x_i$ est la limite de la suite des sommes partielles $\sum_{n\leqslant\mathrm{N}}x_{i(n)}$. Autrement dit, on peut sommer une série absolument convergente dans l'ordre que l'on veut.

On a $\sum_{n\leqslant\mathrm{N}}x_{i(n)}=\sum_{k=0}^{3}\mathbf{i}^k\big(\sum_{n\leqslant\mathrm{N}}\mathrm{Re}^+(\mathbf{i}^{-k}x_{i(n)})\big)$, et il résulte du cas des séries à termes positifs que $\sum_{n\leqslant\mathrm{N}}\mathrm{Re}^+(\mathbf{i}^{-k}x_{i(n)})\to\sum_{i\in\mathrm{I}}\mathrm{Re}^+(\mathbf{i}^{-k}x_i)$. On en déduit le résultat.

• Si $\sum_{i\in\mathrm{I}}x_i$ est absolument convergente, alors $\big|\sum_{i\in\mathrm{I}}x_i\big|\leqslant\sum_{i\in\mathrm{I}}|x_i|$.

On choisit une bijection de $\mathbf{N}$ sur I et on passe à la limite dans l'inégalité pour les sommes finies $\big|\sum_{n\leqslant\mathrm{N}}x_{i(n)}\big|\leqslant\sum_{n\leqslant\mathrm{N}}|x_{i(n)}|$.

104. Dans ce n°, on note $\mathbf{i}$ une racine carrée de -1 pour pouvoir continuer à utiliser i comme un indice dans les termes des séries.

• Si $\sum_{i\in I} x_i$ et $\sum_{i\in I} y_i$ sont absolument convergentes, et si $\lambda, \mu \in \mathbf{C}$, alors $\sum_{i\in I}(\lambda x_i + \mu y_i)$ l'est aussi et $\sum_{i\in I}(\lambda x_i + \mu y_i) = \lambda\big(\sum_{i\in I} x_i\big) + \mu\big(\sum_{i\in I} y_i\big)$ (linéarité de la somme).

On a $|\lambda x_i + \mu y_i| \leqslant |\lambda|\,|x_i| + |\mu|\,|y_i|$, et donc, par linéarité de la somme des séries à termes positifs, $\sum_{i\in I} |\lambda x_i + \mu y_i| \leqslant \sum_{i\in I}\big(|\lambda|\,|x_i| + |\mu|\,|y_i|\big) = |\lambda|\big(\sum_{i\in I}|x_i|\big) + |\mu|\big(\sum_{i\in I}|y_i|\big) < +\infty$. On en déduit la convergence absolue de $\sum_{i\in I}(\lambda x_i + \mu y_i)$.

Enfin, si on choisit une bijection de $\mathbf{N}$ sur I et si on passe à la limite dans l'identité $\sum_{n\leqslant N}(\lambda x_{i(n)} + \mu y_{i(n)}) = \lambda\big(\sum_{n\leqslant N} x_{i(n)}\big) + \mu\big(\sum_{n\leqslant N} y_{i(n)}\big)$, on obtient la formule désirée.

• Si $\sum_{i\in I} x_i$ converge absolument et si les I_j, pour $j \in J$, forment une partition de I, alors :
◇ pour tout $j \in J$, la série $\sum_{i\in I_j} x_i$ est absolument convergente,
◇ si on pose $S_j = \sum_{i\in I_j} x_i$, la série $\sum_{j\in J} S_j$ est absolument convergente,
◇ $\sum_{i\in I} x_i = \sum_{j\in J}\big(\sum_{i\in I_j} x_i\big)$. Autrement dit, dans une série absolument convergente, on peut regrouper les termes comme on veut.

Si $j \in J$, on a $I_j \subset I$ et donc $\sum_{i\in I_j}|x_i| \leqslant \sum_{i\in I}|x_i|$, ce qui prouve que $\sum_{i\in I_j} x_i$ est absolument convergente ; de plus, la somme S_j de la série $\sum_{i\in I_j} x_i$ vérifie $|S_j| \leqslant \sum_{i\in I_j}|x_i|$. On a donc, en utilisant le cas des séries à termes positifs, $\sum_{j\in J}|S_j| \leqslant \sum_{j\in J}\big(\sum_{i\in I_j}|x_i|\big) = \sum_{i\in I}|x_i| < +\infty$, d'où la convergence absolue de la série $\sum_{j\in J} S_j$.

Maintenant, soit $\varepsilon > 0$, et soit $I(\varepsilon) \subset I$, fini de cardinal M, tel que $\sum_{i\in I-I(\varepsilon)}|x_i| \leqslant \varepsilon$. On a $\big(\sum_{i\in I} x_i\big) - \big(\sum_{i\in I(\varepsilon)} x_i\big) = \sum_{i\in I-I(\varepsilon)} x_i$ [en effet, on peut choisir une bijection $n \mapsto i(n)$ de $\mathbf{N}$ sur I, telle que $[0, M-1]$ soit en bijection avec $I(\varepsilon)$ et $[M, +\infty[$ avec $I - I(\varepsilon)$, et on obtient l'identité $\sum_{i\in I} x_i = \sum_{i\in I(\varepsilon)} x_i + \sum_{i\in I-I(\varepsilon)} x_i$ en passant à la limite dans l'identité $\sum_{n\leqslant N} x_{i(n)} = \sum_{n=0}^{M-1} x_{i(n)} + \sum_{i=M}^{N} x_{i(n)}$] ; on en déduit que $\big|\big(\sum_{i\in I} x_i\big) - \big(\sum_{i\in I(\varepsilon)} x_i\big)\big| \leqslant \varepsilon$.

Maintenant, soit $I_j(\varepsilon) = I_j \cap I(\varepsilon)$ et soit $J(\varepsilon) = \{j \in J,\ I_j(\varepsilon) \neq \varnothing\}$; alors $J(\varepsilon)$ est un sous-ensemble fini de J et $\big|\big(\sum_{j\in J} S_j\big) - \big(\sum_{j\in J(\varepsilon)} S_j\big)\big| \leqslant \sum_{j\in J-J(\varepsilon)}|S_j| \leqslant \sum_{j\in J-J(\varepsilon)}\sum_{i\in I_j}|x_i|$ pour les mêmes raisons que précédemment. De plus, $\big|S_j - \big(\sum_{i\in I_j(\varepsilon)} x_i\big)\big| \leqslant \sum_{i\in I_j-(I_j(\varepsilon))}|x_i|$, si $j \in J(\varepsilon)$, ce qui nous donne, en remarquant que $I(\varepsilon)$ est la réunion disjointe des $I_j(\varepsilon)$ pour $j \in J(\varepsilon)$,

$$\begin{aligned}\Big|\Big(\sum_{j\in J} S_j\Big) - \Big(\sum_{i\in I(\varepsilon)} x_i\Big)\Big| &\leqslant \Big|\Big(\sum_{j\in J} S_j\Big) - \Big(\sum_{j\in J(\varepsilon)} S_j\Big)\Big| + \sum_{j\in J(\varepsilon)}\Big|S_j - \Big(\sum_{i\in I_j(\varepsilon)} x_i\Big)\Big| \\ &\leqslant \Big(\sum_{j\in J-J(\varepsilon)}\sum_{i\in I_j}|x_i|\Big) + \sum_{j\in J(\varepsilon)}\sum_{i\in I_j-I_j(\varepsilon)}|x_i| = \sum_{i\in I-I(\varepsilon)}|x_i| \leqslant \varepsilon\end{aligned}$$

Donc $\big|\big(\sum_{i\in I} x_i\big) - \big(\sum_{j\in J} S_j\big)\big| \leqslant 2\varepsilon$ pour tout $\varepsilon > 0$, et $\big(\sum_{i\in I} x_i\big) = \big(\sum_{j\in J} S_j\big)$, ce que l'on cherchait à démontrer.

• Si $\sum_{(i,j)\in I\times J} x_{i,j}$ est absolument convergente, alors :
◇ $\sum_{j\in J} x_{i,j}$ est absolument convergente pour tout $i \in I$, et $\sum_{i\in I}\big(\sum_{j\in J} x_{i,j}\big)$ aussi,
◇ $\sum_{i\in I} x_{i,j}$ est absolument convergente pour tout $j \in J$, et $\sum_{j\in J}\big(\sum_{i\in I} x_{i,j}\big)$ aussi,
◇ $\sum_{j\in J}\big(\sum_{i\in I} x_{i,j}\big) = \sum_{(i,j)\in I\times J} x_{i,j} = \sum_{i\in I}\big(\sum_{j\in J} x_{i,j}\big)$ (Fubini pour les séries).

C'est un cas particulier du point précédent : on partitionne $I \times J$ comme la réunion des $I \times \{j\}$, pour $j \in J$, ou comme la réunion des $\{i\} \times J$, pour $i \in I$.

• Soit $(x_i^{(n)})_{i\in I}$, pour $n \in \mathbf{N}$, des familles de nombres complexes. On suppose :
◇ $x_i^{(n)}$ a une limite x_i quand $n \to +\infty$,

$\diamond$ il existe $(y_i)_{i\in \mathrm{I}}$ telle que $|x_i^{(n)}| \leqslant y_i$, pour tous n et i, et $\sum_{i\in \mathrm{I}} y_i < +\infty$ (domination). Alors $\sum_{i\in \mathrm{I}} |x_i| < +\infty$ et $\sum_{i\in \mathrm{I}} x_i = \lim\limits_{n\to+\infty} \sum_{i\in \mathrm{I}} x_i^{(n)}$ (th. de convergence dominée).

On a $|x_i| \leqslant y_i$ par passage à la limite ; d'où la convergence absolue de $\sum_{i\in \mathrm{I}} x_i$. Maintenant, soit $\varepsilon > 0$. Comme le reste d'une série convergente tend vers 0, Il existe $\mathrm{I}(\varepsilon) \subset \mathrm{I}$, fini, tel que $\sum_{i\in \mathrm{I}-\mathrm{I}(\varepsilon)} y_i \leqslant \varepsilon$. Soit n_0 tel que $|x_i^{(n)} - x_i| \leqslant \frac{\varepsilon}{|\mathrm{I}(\varepsilon)|}$, pour tous $n \geqslant n_0$ et $i \in \mathrm{I}(\varepsilon)$ (l'existence d'un tel n_0 résulte de l'hypothèse $x_i^{(n)} \to x_i$ et de la finitude de $\mathrm{I}(\varepsilon)$). On obtient, si $n \geqslant n_0$,

$$\begin{aligned} \Big|\sum_{i\in \mathrm{I}} x_i - \sum_{i\in \mathrm{I}} x_i^{(n)}\Big| &\leqslant \sum_{i\in \mathrm{I}(\varepsilon)} |x_i - x_i^{(n)}| + \sum_{i\in \mathrm{I}-\mathrm{I}(\varepsilon)} |x_i| + \sum_{i\in \mathrm{I}-\mathrm{I}(\varepsilon)} |x_i^{(n)}| \\ &\leqslant |\mathrm{I}(\varepsilon)|\frac{\varepsilon}{|\mathrm{I}(\varepsilon)|} + 2\sum_{i\in \mathrm{I}-\mathrm{I}(\varepsilon)} y_i \leqslant 3\varepsilon. \end{aligned}$$

On en déduit que $\lim_{n\to+\infty} \sum_{i\in \mathrm{I}} x_i^{(n)} = \sum_{i\in \mathrm{I}} x_i$, ce qui permet de conclure.

15.4. Séries entières

Une *série entière* est une série de la forme $\mathrm{F}(z) = \sum_{n\in \mathbf{N}} a_n z^n$, où $(a_n)_{n\in \mathbf{N}}$ est une suite de nombres complexes, et $z \in \mathbf{C}$ varie.

• Il existe un unique $\rho(\mathrm{F}) \in \overline{\mathbf{R}}_+$, le *rayon de convergence* de F, tel que $\sum_{n\in \mathbf{N}} a_n z^n$ soit absolument convergente si $|z| < \rho(\mathrm{F})$ et $a_n z^n$, pour $n \in \mathbf{N}$, ne soit pas borné (et donc $\sum_{n\in \mathbf{N}} a_n z^n$ soit divergente) si $|z| > \rho(\mathrm{F})$.

Soit X l'ensemble des $z \in \mathbf{C}$ tels que $(a_n z^n)_{n\in \mathbf{N}}$ ne soit pas bornée. Comme $|a_n z^n|$ est une fonction croissante de $|z|$, on a $z \in \mathrm{X}$, si $|z| \geqslant |z_0|$ et $z_0 \in \mathrm{X}$. Notons $\rho(\mathrm{F})$ la borne inférieure de l'ensemble des $|z|$, pour $z \in \mathrm{X}$. Si $|z| > \rho(\mathrm{F})$, il existe $z_0 \in \mathrm{X}$ avec $|z_0| < |z|$, par définition de $\rho(\mathrm{F})$, et donc $(a_n z^n)_{n\in \mathbf{N}}$ n'est pas bornée. Si $|z| < \rho(\mathrm{F})$, et si $|z| < |z_0| < \rho(\mathrm{F})$, alors $(a_n z_0^n)_{n\in \mathbf{N}}$ est bornée, et donc il existe $\mathrm{C} > 0$ tel que l'on ait $|a_n z^n| \leqslant |a_n z_0^n|\big(\frac{|z|}{|z_0|}\big)^n \leqslant \mathrm{C}\big(\frac{|z|}{|z_0|}\big)^n$, pour tout n. Comme $\frac{|z|}{|z_0|} < 1$, cela implique que $\sum_{n\in \mathbf{N}} a_n z^n$ est absolument convergente. Ceci permet de conclure.

• $\rho(\mathrm{F})^{-1} = \limsup |a_n|^{1/n}$.

Si $|z| < \rho(\mathrm{F})$, la suite $|a_n z^n|$ tend vers 0, et donc est $\leqslant 1$ à partir d'un certain rang. Il s'ensuit que $\limsup |a_n z^n|^{1/n} \leqslant 1$, et donc que $\limsup |a_n|^{1/n} \leqslant \frac{1}{|z|}$, ce qui nous fournit l'inégalité $\limsup |a_n|^{1/n} \leqslant \rho(\mathrm{F})^{-1}$.

Si $|z| > \rho(\mathrm{F})$, la suite $(a_n z^n)_{n\in \mathbf{N}}$ n'est pas bornée, et donc il existe une infinité de n tels que $|a_n z^n| \geqslant 1$. Il s'ensuit que $\limsup |a_n z^n|^{1/n} \geqslant 1$, et donc que $\limsup |a_n|^{1/n} \geqslant \frac{1}{|z|}$, ce qui nous fournit l'inégalité $\limsup |a_n|^{1/n} \geqslant \rho(\mathrm{F})^{-1}$ inverse, et permet de conclure.

• La fonction $x \mapsto \mathrm{F}(x) = \sum_{n\in \mathbf{N}} a_n x^n$ est de classe $\mathscr{C}^\infty$ sur $]-\rho(\mathrm{F}), \rho(\mathrm{F})[$, et sa dérivée k-ième est la série entière $\sum_{n\in \mathbf{N}} k!\binom{n+k}{k} x^n$, qui a même rayon de convergence que F.

$\sum_{n\in \mathbf{N}} \binom{n+k}{k} a_{n+k} x^n$ a même rayon de convergence que $\sum_{n\geqslant k} \binom{n}{k} a_n x^n$ (on s'est contenté de multiplier par x^k et de changer les indices), et comme $\binom{n}{k}^{1/n} = \exp\big(\frac{1}{n}\log\binom{n}{k}\big) \to 1$ quand $n \to +\infty$, elle a aussi même rayon que convergence que $\sum_{n\in \mathbf{N}} a_n x^n$, d'après la formule du point précédent pour $\rho(\mathrm{F})$.

Maintenant, $(x+h)^n = x^n + nhx^{n-1} + h^2 \int_0^1 (1-t)n(n-1)(x+th)^{n-2}\,dt$ d'après la formule de Taylor avec reste intégral ; d'où la majoration $\left|\frac{(x+h)^n - x^n}{h} - nx^{n-1}\right| \leqslant |h|\binom{n}{2}(|x|+|h|)^{n-2}$. Si $|x| < \rho(\mathrm{F})$, on peut choisir $\delta > 0$ tel que $|x| + \delta < \rho(\mathrm{F})$, et on obtient, pour tout $h \in]-\delta, \delta[$,

$$\left|\tfrac{\mathrm{F}(x+h)-\mathrm{F}(x)}{h} - \sum_{n\in\mathbf{N}} n a_n x^{n-1}\right| \leqslant \mathrm{C}|h|, \text{ où } \mathrm{C} = \sum_{n\in\mathbf{N}} |a_n|\tbinom{n}{2}(|x|+\delta)^{n-2} < +\infty,$$

puisque $|x| + \delta < \rho(\mathrm{F})$ et $\sum_{n\in\mathbf{N}} \binom{n}{2}|a_n|z^{n-2}$ est de rayon de convergence $\rho(\mathrm{F})$, d'après ce qui précède. Il s'ensuit que F est dérivable en x, de dérivée $\sum_{n\in\mathbf{N}} n a_n x^{n-1}$. Une récurrence immédiate permet d'en déduire que F est de classe $\mathscr{C}^\infty$ sur $]-\rho(\mathrm{F}), \rho(\mathrm{F})[$, et que sa dérivée k-ième est la série entière $\sum_{n\in\mathbf{N}} (n+k)\cdots(n+1)\,a_{n+k}x^n$, ce qui permet de conclure.

15.5. L'exponentielle complexe

• Si $z \in \mathbf{C}$, la série $\sum_{n\in\mathbf{N}} \frac{z^n}{n!}$ est absolument convergente ; on note e^z ou $\exp(z)$ sa somme.

Si a est la partie entière de $|z|$, alors $n! \geqslant a!(a+1)^{n-a}$, et donc $\left|\frac{z^n}{n!}\right| \leqslant \mathrm{C}\left(\frac{|z|}{a+1}\right)^n$, avec $\mathrm{C} = \frac{(a+1)^a}{a!}$ Comme $\frac{|z|}{a+1} < 1$, on en déduit la convergence absolue de la série.

• La fonction exponentielle $z \mapsto e^z$ [ou $z \mapsto \exp(z)$] vérifie les propriétés suivantes :

◇ C'est un morphisme de groupes de $(\mathbf{C}, +)$ dans $(\mathbf{C}^*, \times)$ (i.e. $e^{z_1+z_2} = e^{z_1}e^{z_2}$, et donc $e^0 = 1$ et $e^{-z} = 1/e^z$).

◇ Sa restriction à $\mathbf{R}$ est un isomorphisme de groupes sur $\mathbf{R}_+^*$, et $e^x \to +\infty$ quand $x \to +\infty$ et $e^x \to 0$ quand $x \to -\infty$ (et même $x^{-\mathrm{N}}e^x \to +\infty$ quand $x \to +\infty$ et $x^{\mathrm{N}}e^x \to 0$ quand $x \to -\infty$, si $\mathrm{N} \in \mathbf{N}$) ; de plus $x \mapsto e^x$ est solution de l'équation différentielle $y' = y$.

◇ Sa restriction à $i\mathbf{R}$ est un morphisme surjectif sur le groupe $\mathrm{U} = \{z \in \mathbf{C}^*,\ |z| = 1\}$ dont le noyau est $2i\pi\mathbf{Z}$, où [105] $\pi = \int_{-\infty}^{+\infty} \frac{dx}{1+x^2}$; si $a \in \mathbf{R}$, la restriction de $t \mapsto e^{it}$ à $[a, a+2\pi[$ est un paramétrage du cercle unité U.

◇ Le morphisme $z \mapsto e^z$ est surjectif de $\mathbf{C}$ sur $\mathbf{C}^*$ et son noyau est $2i\pi\mathbf{Z}$; la fonction exponentielle est périodique de période $2i\pi$.

$$\textstyle\sum_{(k,m)\in\mathbf{N}^2} \frac{|z_1|^k}{k!}\frac{|z_2|^m}{m!} = \sum_{k\in\mathbf{N}} \left(\sum_{m\in\mathbf{N}} \frac{|z_1|^k}{k!}\frac{|z_2|^m}{m!}\right) = \sum_{k\in\mathbf{N}} \frac{|z_1|^k}{k!} e^{|z_2|} = e^{|z_1|}e^{|z_2|} < +\infty.$$

La série $\sum_{(k,m)\in\mathbf{N}^2} \frac{z_1^k}{k!}\frac{z_2^m}{m!}$ est donc absolument convergente, ce qui permet de regrouper les termes comme on veut. En sommant d'abord sur m, puis sur k, on voit que sa somme est $\exp(z_1)\exp(z_2)$, et en sommant sur $m+k=n$, puis sur n, on obtient

$$\sum_{(k,m)\in\mathbf{N}^2} \frac{z_1^k}{k!}\frac{z_2^m}{m!} = \sum_{n\in\mathbf{N}} \Big(\sum_{k=0}^{n} \frac{1}{n!}\tbinom{n}{k} z_1^k z_2^{n-k}\Big) = \sum_{n\in\mathbf{N}} \frac{(z_1+z_2)^n}{n!} = \exp(z_1+z_2),$$

ce qui prouve le premier point.

Maintenant, il est clair sur la formule que exp est strictement croissante sur $\mathbf{R}_+$ car $x \mapsto x^n$ l'est pour tout n, et que $e^x \geqslant \frac{x^{\mathrm{N}+1}}{(\mathrm{N}+1)!}$ ce qui prouve que $x^{-\mathrm{N}}e^x \to +\infty$ quand $x \to +\infty$. Il s'ensuit que $x \mapsto e^x$ est une bijection strictement croissante de $\mathbf{R}_+$ sur $[1, +\infty[$. Comme

105. Ceci est une définition possible du nombre π. Comme $t \mapsto e^{it}$ est un paramétrage du cercle unité par $[-\pi, \pi[$, la longueur de ce cercle est $\int_{-\pi}^{\pi} \left|(e^{it})'\right| dt = \int_{-\pi}^{\pi} dt = 2\pi$, puisque $(e^{it})' = ie^{it}$ comme il est établi au cours de la démonstration. Cette définition est donc équivalente à celle utilisée depuis la plus haute antiquité.

$e^x = 1/e^{-x}$ et $x^{\mathrm{N}}e^x = (-1)^n/((-x)^{-\mathrm{N}}e^{-x})$, on en déduit que $x \mapsto e^x$ est une bijection strictement croissante de $\mathbf{R}_-$ sur $]0,1]$ et $x^{\mathrm{N}}e^x \to 0$ quand $x \to -\infty$. Enfin, la dérivée de $x \mapsto e^x$ est $\sum_{n\geqslant 1} \frac{nx^{n-1}}{n!} = \sum_{n\geqslant 1} \frac{x^{n-1}}{(n-1)!} = e^x$, ce qui permet de prouver le second point.

On a $\exp \overline{z} = \overline{\exp(z)}$ par continuité de $z \mapsto \overline{z}$. Il s'ensuit que le conjugué complexe de $u = e^{it}$ est e^{-it} si $t \in \mathbf{R}$, et donc que $|u| = 1$ puisque $|u|^2 = u\overline{u} = e^{it}e^{-it} = 1$; l'image de $i\mathbf{R}$ par exp est donc incluse dans U. Par ailleurs, la dérivée de $x \mapsto e^{it} = \sum_{n\in\mathbf{N}} \frac{(it)^n}{n!}$ est $\sum_{n\geqslant 1} \frac{i\,n(it)^{n-1}}{n!} = i\sum_{n\in\mathbf{N}} \frac{(it)^n}{n!} = ie^{it}$; celle de $t \mapsto e^{if(t)}$ est donc $if'(t)e^{if(t)}$. Soit $g(t) = e^{if(t)}\big(\frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}\big)$, où $f(t) = -2\int_0^t \frac{dx}{1+x^2}$ (sa dérivée est $f'(t) = \frac{-2}{1+t^2}$). On obtient $g'(t) = e^{if(t)}\big(\frac{-4t}{(1+t^2)^2} + i\frac{2(1-t^2)}{(1+t^2)^2}\big) + i\frac{-2}{1+t^2}e^{if(t)}\big(\frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}\big) = 0$, ce qui prouve que la fonction $t \mapsto g(t)$ est constante sur $\mathbf{R}$, et comme elle vaut 1 en 0, on a $e^{-if(t)} = \frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}$, si $t \in \mathbf{R}$. Maintenant, $\frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}$ est l'intersection du cercle $\mathrm{U} - \{-1\}$ avec la droite de pente t passant par -1, il s'ensuit que $t \mapsto e^{-if(t)}$ induit une bijection de $\mathbf{R}$ sur $\mathrm{U} - \{-1\}$ et que $t \mapsto e^{it}$ induit une bijection de $]-\pi,\pi[$ sur $\mathrm{U} - \{-1\}$ et, en passant à la limite, que $e^{i\pi} = e^{-i\pi} = -1$; il en résulte que $t \mapsto e^{it}$ est surjectif de $\mathbf{R}$ sur U. De plus, $e^{2i\pi} = e^{i\pi}(e^{-i\pi})^{-1} = 1$, ce qui prouve que le noyau de $t \mapsto e^{it}$ contient $2\pi\mathbf{Z}$. Par ailleurs, si $t < 2\pi$, on a $t = a - b$ avec $-\pi < a, b < \pi$ et $e^{it} = e^{ia}/e^{ib} \neq 1$ puique $t \mapsto e^{it}$ est injectif sur $]-\pi,\pi[$; le noyau de $t \mapsto e^{it}$ est donc exactement $2\pi\mathbf{Z}$ (cf. (i) de l'ex. 15.2). Enfin, si $a \in \mathbf{R}$ et si $n = \big[\frac{a+\pi}{2\pi}\big]$, on peut découper $[a, a+2\pi[$ en $[a,(2n+1)\pi[$ et $[(2n+1)\pi, a+2\pi[$, et $[(2n+1)\pi, a+2\pi[$ est le translaté de $[-\pi, a-2n\pi[$ par $2(n+1)\pi$ et $[a,(2n+1)\pi[$ est celui de $[a-2n\pi,\pi[$ par $2n\pi$. On montre que $t \mapsto e^{it}$ est un paramétrage de U par $[a, a+2\pi[$ en constatant que c'est le cas si $a = -\pi$ d'après ce qui précède, et en utilisant la 2π-périodicité de $t \mapsto e^{it}$ et le fait que $[-\pi, a-2n\pi[$ et $[a-2n\pi,\pi[$ forment une partition de $[-\pi,\pi[$.

Pour prouver la surjectivité de $z \mapsto e^z$, il suffit d'écrire $w \in \mathbf{C}^*$ sous la forme $w = |w|\frac{w}{|w|}$; il existe alors $x, y \in \mathbf{R}$ tels que $e^x = |w|$ et $e^{iy} = \frac{w}{|w|}$ d'après les second et troisième points, et on a $e^{x+iy} = w$. Enfin, $e^{x+iy} = 1$ implique $|e^{x+iy}| = 1$ et donc $e^x = 1$ et $x = 0$; le noyau de exp est donc inclus dans $i\mathbf{R}$, et est donc $2i\pi\mathbf{Z}$ d'après le troisième point.

Exercice 15.2. — (i) Soit Λ un sous-groupe de $(\mathbf{R}, +)$. Montrer que Λ est dense dans $\mathbf{R}$ ou bien est de la forme $\mathbf{Z}\cdot a = \{na,\ n \in \mathbf{Z}\}$, avec $a \in \mathbf{R}_+$.

(ii) Existe-t-il $n \in \mathbf{N}$ tel que $2^n = 3141592a_0a_1\cdots$ en base 10 ?

(iii) Montrer que les solutions de $a^2 - 2b^2$, avec $(a,b) \in \mathbf{N}^2$ sont les (a_n, b_n), pour $n \in \mathbf{N}$, avec $a_n + b_n\sqrt{2} = (3+2\sqrt{2})^n$. (On pourra commencer par vérifier que si $a_1, b_1, a_2, b_2 \in \mathbf{Z}$ vérifient $a_1^2 - 2b_1^2 = 1$ et $a_2 - 2b_2^2 = 1$, alors $a_3^2 - 2b_3^2 = 1$, si $a_3 + b_3\sqrt{2} = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$.)

15.6. Sommation de séries divergentes

Il y a beaucoup de séries naturelles qui ne sont pas absolument convergentes, mais auxquelles on aimerait bien donner un sens. On dispose de tout un arsenal de recettes en ce sens, mais celles-ci demandent toujours de faire attention au sens exact que revêt la somme (cf. ex. 15.5).

Le cas le plus simple est celui d'une série $\sum_{n\in\mathbf{N}} x_n$ dont la suite des sommes partielles $\sum_{n\leqslant \mathrm{N}} x_n$ converge ; une telle série est dite *semi-convergente* et on définit sa somme comme la limite des sommes partielles (il est clair que ceci redonne la somme de la série au sens précédent si la série est absolument convergente). Dans le même genre d'idées, une série

de Fourier $\sum_{n\in\mathbf{Z}} a_n e^{2i\pi nx}$ se somme souvent en regardant la limite (si elle existe) des sommes symétriques $\sum_{n=-\mathrm{N}}^{\mathrm{N}} a_n e^{2i\pi nx}$. On remarquera que dans le premier cas, la semi-convergence de $\sum_{n\leqslant \mathrm{N}} x_n$ implique que $x_n \to 0$ quand $n \to +\infty$, mais que cette condition n'est pas suffisante comme le montre l'exemple de la série $\sum_{n\in\mathbf{N}} \frac{1}{n+1}$. Un des rares résultats généraux simples dont on dispose est celui des *séries alternées* ci-dessous.

• Soit $(u_n)_{n\in\mathbf{N}}$ une suite décroissante d'éléments de $\mathbf{R}_+$, tendant vers 0, alors la série $\sum_{n\in\mathbf{N}}(-1)^n u_n$ est semi-convergente (critère de Leibnitz, 1675).

Notons $\mathrm{S_N}$ la somme partielle $\sum_{n\leqslant \mathrm{N}}(-1)^n u_n$. Nous allons utiliser la *formule sommatoire d'Abel*[106] $\sum_{n=0}^{\mathrm{N}} a_n b_n = \sum_{n=0}^{\mathrm{N}} (\sum_{i=0}^{n} a_i)(b_n - b_{n+1}) + b_{\mathrm{N}+1}\sum_{i=0}^{\mathrm{N}} a_i$ qui se démontre en remarquant que le terme en facteur de b_n est a_0 si $n = 0$, $\sum_{i=0}^{n} a_i - \sum_{i=0}^{n-1} a_i = a_n$ si $1 \leqslant n \leqslant \mathrm{N}$, et $\sum_{i=0}^{\mathrm{N}} a_i - \sum_{i=0}^{\mathrm{N}} a_i = 0$ si $n = \mathrm{N}+1$. On applique ceci à $a_n = (-1)^n$ et $b_n = u_n$, et on pose $s_n = \sum_{i=0}^{n} a_i = \frac{1}{2}(1 + (-1)^n)$; on obtient donc $\mathrm{S_N} = \sum_{n=0}^{\mathrm{N}} s_n(u_n - u_{n+1}) + s_{\mathrm{N}} u_{\mathrm{N}+1}$. Maintenant, comme u_n est décroissante, la série $\sum_{n\in\mathbf{N}}(u_n - u_{n+1})$ est à termes positifs, convergente de somme $u_0 - \lim_{\mathrm{N}\to+\infty} u_{\mathrm{N}} = u_0$; comme $|s_n| \leqslant 1$ pour tout n, il en résulte que $\sum_{n\in\mathbf{N}} s_n(u_n - u_{n+1})$ est absolument convergente, et donc que $\sum_{n\leqslant \mathrm{N}} s_n(u_n - u_{n+1})$ a une limite. Enfin, $s_{\mathrm{N}} u_{\mathrm{N}+1} \to 0$, ce qui prouve que $\mathrm{S_N}$ tend vers la somme de la série $\sum_{n\in\mathbf{N}} s_n(u_n - u_{n+1})$, et permet de conclure.

• Un exemple[107] : $\sum_{n\in\mathbf{N}} \frac{(-1)^n}{2n+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}$.

On peut écrire $\mathrm{S_N} = \sum_{n\leqslant \mathrm{N}} \frac{(-1)^n}{2n+1}$ sous la forme

$$\mathrm{S_N} = \sum_{n\leqslant \mathrm{N}} \int_0^1 (-x^2)^n\, dx = \int_0^1 \frac{1-(-x^2)^{\mathrm{N}+1}}{1+x^2}\, dx = \frac{\pi}{4} - \int_0^1 \frac{(-x^2)^{\mathrm{N}+1}}{1+x^2}\, dx.$$

Le résultat suit donc de ce que $\left|\frac{(-x^2)^{\mathrm{N}+1}}{1+x^2}\right| \leqslant x^{2\mathrm{N}+2}$, et donc $\left|\int_0^1 \frac{(-x^2)^{\mathrm{N}+1}}{1+x^2}\, dx\right| \leqslant \frac{1}{2\mathrm{N}+3}$, ce qui montre que $\int_0^1 \frac{(-x^2)^{\mathrm{N}+1}}{1+x^2}\, dx \to 0$ quand $\mathrm{N} \to +\infty$.

Exercice 15.3. — Montrer que $\sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n}$ est semi-convergente de somme $\log 2$.

Exercice 15.4. — (i) Soit $\sum_{n\in\mathbf{N}} u_n$ une série semi-convergente de somme S. Montrer que $\sum_{n\in\mathbf{N}} u_n x^n$ est absolument convergente si $x \in]-1, 1[$ et que[108] $\mathrm{S} = \lim_{x\to 1^-} \left(\sum_{n\in\mathbf{N}} u_n x^n\right)$. (On utilisera la formule sommatoire d'Abel.)

(ii) Si $\sum_{n\in\mathbf{N}} a_n$ et $\sum_{n\in\mathbf{N}} b_n$ sont deux séries, on définit leur *produit de Cauchy* $\sum_{n\in\mathbf{N}} c_n$, où l'on a

106. On peut s'en passer, mais cette formule est extrèmement utile pour l'étude des séries ; c'est l'analogue discret de l'intégration par partie.

107. Cette formule est en général attribuée à Leibnitz (1682) qui en était, à juste titre, très fier, mais il avait été précédé de quelques siècles par le mathématicien Madhava (∼1350–∼1425) du Kerala (en Inde). C'est l'ancètre de toutes les formules concernant les valeurs de fonctions L aux entiers : si $\chi_4 : (\mathbf{Z}/4\mathbf{Z})^* \to \{\pm 1\}$ est le caractère de Dirichlet (cf. n° VII.4) défini par $\chi_4(1) = 1$ et $\chi_4(-1) = -1$, la fonction L associée est $\mathrm{L}(\chi_4, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots$ et la formule de Madhava-Leibnitz devient $\mathrm{L}(\chi_4, 1) = \frac{\pi}{4}$.

108. Cet exercice permet de montrer que le procédé de convergence $\lim_{x\to 1^-} \left(\sum_{n\in\mathbf{N}} u_n x^n\right)$ donne le même résultat que la sommation naturelle quand celle-ci converge, mais qu'il permet de sommer beaucoup plus de séries, y compris des séries pour lesquels u_n ne tend pas vers 0. C'est aussi le cas du procédé de l'ex. 15.6.

posé $c_n = \sum_{i+j=n} a_i b_j$. Montrer que si $\sum_{n\in\mathbf{N}} a_n$ et $\sum_{n\in\mathbf{N}} b_n$ sont absolument convergentes, il en est de même de $\sum_{n\in\mathbf{N}} c_n$ et que $\sum_{n\in\mathbf{N}} c_n = \big(\sum_{n\in\mathbf{N}} a_n\big)\cdot\big(\sum_{n\in\mathbf{N}} b_n\big)$.

(iii) En déduire que si les séries $\sum_{n\in\mathbf{N}} a_n$, $\sum_{n\in\mathbf{N}} b_n$ et $\sum_{n\in\mathbf{N}} c_n$ sont semi-convergentes, alors $\sum_{n\in\mathbf{N}} c_n = \big(\sum_{n\in\mathbf{N}} a_n\big)\cdot\big(\sum_{n\in\mathbf{N}} b_n\big)$.

(iv) Donner un exemple où $\sum_{n\in\mathbf{N}} a_n$ et $\sum_{n\in\mathbf{N}} b_n$ sont semi-convergentes, mais pas $\sum_{n\in\mathbf{N}} c_n$. La limite en 1^- de $\sum_{n\in\mathbf{N}} c_n x^n$ existe-t-elle ? Si oui, que vaut-elle ?

Exercice 15.5. — Soit $\sum_{n\in\mathbf{N}} x_n$, une série semi-convergente, à termes réels, non absolument convergente.

(i) Montrer que, pour tout $\ell \in \mathbf{R}$, il existe une bijection $\varphi : \mathbf{N} \to \mathbf{N}$ telle que $\lim_{\mathrm{N}\to+\infty} \sum_{n\leqslant \mathrm{N}} x_{\varphi(n)} = \ell$.

(ii) Montrer que le groupe des bijections de $\mathbf{N}$ dans $\mathbf{N}$ n'est pas dénombrable.

On peut souvent améliorer la convergence d'une série alternée en remplaçant les sommes partielles par la moyenne $\mathrm{S}'_\mathrm{N} = \frac{1}{2}(\mathrm{S}_\mathrm{N} + \mathrm{S}_{\mathrm{N}+1})$ (il est clair que S'_N converge et a même limite que S_N si S_N converge), et rien n'empêche de recommencer et de définir par récurrence sur k une suite $\mathrm{S}^{[k]} = (\mathrm{S}^{[k]}_\mathrm{N})_{\mathrm{N}\in\mathbf{N}}$ par $\mathrm{S}^{[0]}_\mathrm{N} = \mathrm{S}_\mathrm{N}$ et $\mathrm{S}^{[k]}_\mathrm{N} = \frac{1}{2}(\mathrm{S}^{[k-1]}_\mathrm{N} + \mathrm{S}^{[k-1]}_{\mathrm{N}+1})$, si $k \geqslant 1$; on a donc $\mathrm{S}^{[k]}_\mathrm{N} = \frac{1}{2^k}\big(\sum_{j=0}^k \binom{k}{j}\mathrm{S}_{\mathrm{N}+j}\big)$. Par exemple, en partant de $\sum_{n\in\mathbf{N}}(-1)^n(n+1)$, on obtient $\mathrm{S}^{[0]} = (1,-1,2,-2,3,-3,4,-4,5,-5,\dots)$, $\mathrm{S}^{[1]} = (0,\frac{1}{2},0,\frac{1}{2},0,\frac{1}{2},0,\frac{1}{2},\dots)$ et $\mathrm{S}^{[2]} = (\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\dots)$, d'où la formule $1-2+3-4+5-6+7-8+\cdots = \frac{1}{4}$ d'Euler. Nous encourageons le lecteur à appliquer le même procédé à $1-4+9-16+25-36+\cdots$. L'exercice suivant fournit une explication du phénomène.

Exercice 15.6. — On s'intéresse à $\sum_{n\in\mathbf{N}}(-1)^n f(n)$, où $f : \mathbf{R}_+ \to \mathbf{R}$ est une fonction. On note $\mathrm{S}^{[k]}$, pour $k \in \mathbf{N}$, les suites obtenues à partir de la suite des sommes partielles de la série comme ci-dessus. On définit une suite de fonctions $f^{[k]}$ par récurrence, en posant $f^{[0]} = f$ et $f^{[k+1]}(x) = f^{[k]}(x+1) - f^{[k]}(x)$.

(i) Établir l'identité $\mathrm{S}^{[k]}_\mathrm{N} - \mathrm{S}^{[k]}_{\mathrm{N}-1} = \frac{(-1)^{\mathrm{N}+k}}{2^k} f^{[k]}(\mathrm{N})$.

(ii) Que vaut $\mathrm{P}^{[k]}$ si P est un polynôme de degré $\leqslant k$?

(iii) On suppose f de classe $\mathscr{C}^k$. Soit $a \in \mathbf{R}_+$. Montrer qu'il existe $c \in [a, a+k]$ tel que l'on ait $f^{[k]}(a) = f^{(k)}(c)$, où $f^{(k)}$ désigne la dérivée k-ième de f. (On pourra considérer un polynôme ayant les mêmes valeurs que f en $a, a+1, \dots, a+k$.)

(iv) Soit $f(x) = (x+1)^{-s}$, avec $s \in \mathbf{R}$. Montrer qu'il existe k tel que $\mathrm{S}^{[k]}$ ait une limite $\mathrm{F}(s)$.

(v) Montrer que $\mathrm{F}(s) = (1-2^{1-s})\zeta(s)$, où $\zeta(s) = \sum_{n\geqslant 1} \frac{1}{n^s}$, si $s > 1$.

(vi) On définit [109] $\zeta(s)$ par $\zeta(s) = \frac{1}{1-2^{1-s}}\mathrm{F}(s)$, si $s < 1$. Montrer [110] que $\zeta(-m) \in \mathbf{Q}$, si $m \in \mathbf{N}$.

16. Convergence de fonctions

16.1. Convergence simple

Si X et Y sont deux espaces topologiques, une suite de fonctions $f_n : \mathrm{X} \to \mathrm{Y}$ *converge simplement vers* f si, pour tout $x \in \mathrm{X}$, la suite $f_n(x)$ a pour limite $f(x)$ dans Y. Si c'est le cas, on dit que f est la *limite simple* de la suite f_n.

Il est, en pratique, largement inutile de savoir quelle topologie se cache derrière la convergence simple. Cette topologie n'a rien de mystérieux : c'est la topologie produit sur l'espace des fonctions Y^X de X dans Y. En effet, les conditions suivantes sont équivalentes :

- $f_n(x) \to f(x)$, pour tout $x \in \mathrm{X}$;

109. C'est une des manières de prolonger la fonction zêta de Riemann là où la série de converge pas ; on trouvera des procédés plus sophistiqués un peu plus loin, cf. n° VII.3.

110. On a par exemple $\zeta(-1) = \frac{-1}{12}$, et donc $1+2+3+4+5+\cdots = \frac{-1}{12}$, comme l'aurait écrit Euler.

• $(f_n(x))_{x\in \mathrm{I}} \to (f(x))_{x\in \mathrm{I}}$ pour tout $\mathrm{I} \subset \mathrm{X}$ fini ;

• pour tout $\mathrm{I} \subset \mathrm{X}$ fini, et tout ouvert de Y^{I} de la forme $\mathrm{U} = \prod_{x\in \mathrm{I}} \mathrm{U}_x$ qui contient $(f(x))_{x\in \mathrm{I}}$, il existe $\mathrm{N} \in \mathbf{N}$, tel que $(f_n(x))_{x\in \mathrm{I}} \in \mathrm{U}$, si $n \geqslant \mathrm{N}$;

• pour tout $\mathrm{I} \subset \mathrm{X}$ fini, et tout ouvert de Y^{X} de la forme $\mathrm{U} = \big(\prod_{x\in \mathrm{I}} \mathrm{U}_x\big) \times \big(\prod_{x\notin \mathrm{I}} \mathrm{Y}\big)$ qui contient $(f(x))_{x\in \mathrm{X}}$, il existe $\mathrm{N} \in \mathbf{N}$, tel que $(f_n(x))_{x\in \mathrm{X}} \in \mathrm{U}$, si $n \geqslant \mathrm{N}$;

• $f_n \to f$ dans Y^{X}.

D'après l'exercice ci-dessous, les fonctions continues sont denses dans l'ensemble $\mathbf{C}^{\mathbf{R}}$ des fonctions de $\mathbf{R}$ dans $\mathbf{C}$ pour la topologie produit. Or, Baire a montré qu'une limite simple de fonctions continues de $\mathbf{R}$ dans $\mathbf{C}$ est continue en au moins un point. Donc il existe des éléments de $\mathbf{C}^{\mathbf{R}}$ qui ne sont pas limite simple d'une suite de fonctions continues, ce qui n'est possible que si la topologie ci-dessus sur $\mathbf{C}^{\mathbf{R}}$ n'est pas définissable par une distance. Cela explique qu'il existe des fonctions qui sont limites simples de limites simples de fonctions continues, mais qui ne sont pas limites simples de fonctions continues (ex. II.1.11).

Exercice 16.1. — Montrer que l'ensemble des fonctions continues de $\mathbf{R}$ dans $\mathbf{C}$ est dense dans $\mathbf{C}^{\mathbf{R}}$ (muni de la topologie produit).

16.2. Convergence uniforme

Soient X un ensemble et Y un espace métrique (par exemple $\mathrm{Y} = \mathbf{C}$). Soient f et f_n, pour $n \in \mathbf{N}$, des fonctions de X dans Y. On dit que f_n *converge uniformément* vers f sur X ou que f est la *limite uniforme* des f_n, si $\lim_{n\to+\infty} \big(\sup_{x\in \mathrm{X}} d_{\mathrm{Y}}(f(x), f_n(x))\big) = 0$. Ceci peut se réécrire sous la forme : pour tout $\varepsilon > 0$, il existe $\mathrm{N} = \mathrm{N}(\varepsilon)$ tel que $d_{\mathrm{Y}}(f(x), f_n(x)) < \varepsilon$, pour tous $n \geqslant \mathrm{N}$ et $x \in \mathrm{X}$.

La différence avec la convergence simple est que $\mathrm{N}(\varepsilon)$ est le même pour tout $x \in \mathrm{X}$; en particulier, la convergence uniforme [111] implique la convergence simple.

• Si X est un espace topologique, si $f_n \to f$ uniformément sur X, et si f_n est continue en x_0, pour tout $n \in \mathbf{N}$, alors f est continue en x_0. Si les f_n sont continues sur X, il en est de même de f.

Soit $\varepsilon > 0$, et soit $n \in \mathbf{N}$ tel que $\sup_{x\in \mathrm{X}} d_{\mathrm{Y}}(f(x), f_n(x)) < \varepsilon$. Comme f_n est continue en x_0, il existe V ouvert de X contenant x_0 tel que $d_{\mathrm{Y}}(f_n(x), f_n(x_0)) < \varepsilon$, pour tout $x \in \mathrm{V}$. Alors

$$d_{\mathrm{Y}}(f(x), f(x_0)) \leqslant d_{\mathrm{Y}}(f(x), f_n(x)) + d_{\mathrm{Y}}(f_n(x), f_n(x_0)) + d_{\mathrm{Y}}(f_n(x_0), f(x_0)) < 3\varepsilon,$$

pour tout $x \in \mathrm{V}$. On en déduit la continuité de f en x_0. Le second énoncé en étant une conséquence immédiate, cela permet de conclure.

Exercice 16.2. — Soient $u = (u_k)_{k\in\mathbf{N}}$ et $u^{(n)} = (u_k^{(n)})_{k\in\mathbf{N}}$, pour $n \in \mathbf{N}$, des suites à valeurs dans $\mathbf{C}$. On suppose que $u^{(n)} \to u$ uniformément sur $\mathbf{N}$ et que $\lim_{k\to+\infty} u_k^{(n)} = 0$, pour tout n. Montrer que $\lim_{k\to+\infty} u_k = 0$.

Exercice 16.3. — (i) Montrer que $(a_n)_{n\in\mathbf{N}} \mapsto \sum_{n\in\mathbf{N}} \frac{a_n}{10^{n+1}}$ est continue sur $\{0, 1, \ldots, 9\}^{\mathbf{N}}$.

(ii) En déduire que $[0, 1]$ est compact.

111. En filière PC, la convergence uniforme (concept universellement reconnu) a été remplacée par les deux demi-concepts que constituent la convergence normale (pour une norme qui n'est autre que celle de la convergence uniforme), et par l'approximation uniforme d'une fonction par des fonctions d'un certain ensemble. J'avoue avoir du mal à saisir la subtile différence.

Si X est un ensemble et si Y est un espace métrique, une suite de fonctions $f_n : \mathrm{X} \to \mathrm{Y}$ vérifie le *critère de Cauchy uniforme* sur X si $\lim_{n\to+\infty} \big(\sup_{x\in\mathrm{X},\, p\in\mathbf{N}} d_\mathrm{Y}(f_n(x), f_{n+p}(x))\big) = 0$.

• Si X est un espace topologique, si Y est un espace métrique complet, et si $(f_n)_{n\in\mathbf{N}}$ est une suite de fonctions continues de X dans Y vérifiant le critère de Cauchy uniforme, alors $(f_n)_{n\in\mathbf{N}}$ a une limite simple f qui est continue, et f_n converge uniformément vers f sur X.

Si $x \in \mathrm{X}$, la suite $(f_n(x))_{n\in\mathbf{N}}$ est de Cauchy, et donc admet admet une limite $f(x)$, puisque Y est complet. Soit $\delta_n = \sup_{x\in\mathrm{X},\, p\in\mathbf{N}} d_\mathrm{Y}(f_{n+p}(x), f_n(x))$; par hypothèse, on a $\delta_n \to 0$. Un passage à la limite montre que $d_\mathrm{Y}(f(x), f_n(x)) \leqslant \delta_n$, pour tout x, et comme $\delta_n \to 0$, cela prouve que $f_n \to f$ uniformément sur X, ce qui permet de conclure puisqu'une limite uniforme de fonctions continues est continue.

Exercice 16.4. — Soit $(\mathrm{E}, \|\ \|)$ un espace vectoriel normé (sur $\mathbf{R}$ ou $\mathbf{C}$). On dit que $f : \mathrm{E} \to \mathbf{C}$ *tend vers* ℓ *à l'infini*, si pour tout $\varepsilon > 0$, il existe $\mathrm{M} > 0$ tel que $|f(x) - \ell| < \varepsilon$ pour tout x vérifiant $\|x\| > \mathrm{M}$. Soient f et f_n, pour $n \in \mathbf{N}$, des fonctions de E dans $\mathbf{C}$. On suppose que $f_n \to f$ uniformément sur E, et que f_n tend vers ℓ_n à l'infini. Montrer que $(\ell_n)_{n\in\mathbf{N}}$ a une limite $\ell \in \mathbf{C}$, et que f tend vers ℓ à l'infini.

Exercice 16.5. — Soit $f : [0,1] \to \mathbf{C}$ continue.
(i) Montrer que $f_n = \sum_{i=0}^{2^n-1} f\big(\frac{i}{2^n}\big)\mathbf{1}_{[i/2^n,(i+1)/2^n[}$ tend uniformément vers f sur $[0,1[$.
(ii) Montrer que $u_n = \frac{1}{2^n}\sum_{i=0}^{2^n-1} f\big(\frac{i}{2^n}\big)$ a une limite quand $n \to +\infty$ (déf. de l'intégrale de Cauchy).

17. Espaces vectoriels normés

17.1. Corps normés

Si K est un corps, une *norme* sur K est une application $x \mapsto |x|$ de K dans $\mathbf{R}_+$ vérifiant les trois propriétés suivantes :

$$\text{(i) } |x| = 0 \Leftrightarrow x = 0, \quad \text{(ii) } |xy| = |x||y|, \quad \text{(iii) } |x+y| \leqslant |x| + |y|.$$

Une norme qui vérifie l'inégalité $|x+y| \leqslant \sup(|x|, |y|)$ est dite *ultramétrique*.

Des exemples de tels objets sont, bien évidemment, $\mathbf{R}$ et $\mathbf{C}$ munis de la norme usuelle, mais il y en a bien d'autres, comme le corps $\mathbf{Q}_p$ des nombres p-adiques, muni de la norme $|\ |_p$, que nous verrons au n° 20.4, ou le corps des fractions $\mathrm{K}((\mathrm{T}))$ de l'anneau $\mathrm{K}[[\mathrm{T}]]$ du n° 1 du § V.1. Le théorème d'Ostrowski (th. G.2.1) classifie toutes les normes que l'on peut mettre sur $\mathbf{Q}$.

Si K est un corps muni d'une norme $|\ |$, et x, y sont deux éléments de K, on pose $d(x,y) = |x-y|$. Les propriétés (i) et (iii) des normes assurent que d est une distance sur K et donc définit une topologie sur K. Deux normes sur un corps K sont dites *équivalentes* si elle définissent la même topologie. Une norme est dite *triviale* si elle induit la topologie discrète sur K (on a alors $|x| = 1$ quel que soit $x \neq 0$). On dit que K est *complet* s'il l'est pour la distance d [c'est le cas de $\mathbf{R}$ et $\mathbf{C}$; c'est aussi celui de $\mathbf{Q}_p$ et $\mathrm{K}((\mathrm{T}))$].

17.2. Normes et applications linéaires continues

Soit $(\mathbf{K}, |\ |)$ un corps normé complet (par exemple, $\mathbf{R}$ ou $\mathbf{C}$). Si E est un espace vectoriel sur $\mathbf{K}$, une *norme* $\|\ \|$ sur E est une application $x \mapsto \|x\|$ de E dans $\mathbf{R}_+$ vérifiant :

(i) $\|x\| = 0$ si et seulement si $x = 0$;

(ii) $\|\lambda x\| = |\lambda| \cdot \|x\|$, si $x \in \mathrm{E}$ et $\lambda \in \mathbf{K}$;

(iii) $\|x + y\| \leqslant \|x\| + \|y\|$, si $x, y \in \mathrm{E}$.

Si $\|\ \|$ est une norme sur E, alors $d : \mathrm{E} \times \mathrm{E} \to \mathbf{R}_+$ définie par $d(x, y) = \|x - y\|$ est une distance sur E, ce qui permet de voir un espace vectoriel normé $(\mathrm{E}, \|\ \|)$ comme un cas particulier d'espace métrique.

• Si $(\mathrm{E}, \|\ \|_{\mathrm{E}})$ et $(\mathrm{F}, \|\ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés, et si $u : \mathrm{E} \to \mathrm{F}$ est une application *linéaire*, les conditions suivantes sont équivalentes :

(i) u est continue ;

(ii) u est uniformément continue ;

(iii) il existe $\mathrm{M} \in \mathbf{R}_+$ tel que $\|u(x)\|_{\mathrm{F}} \leqslant \mathrm{M} \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$.

Si u est continue, l'image inverse de la boule unité ouverte de F contient un voisinage de 0 dans E, et donc une boule ouverte $\mathrm{B}(0, r^-)$, avec $r > 0$. Autrement dit, $\|x\|_{\mathrm{E}} < r$ implique $\|u(x)\|_{\mathrm{F}} < 1$, et donc, quel que soit $x \in \mathrm{E} - \{0\}$,

$$\|u(x)\|_{\mathrm{F}} = \frac{\|x\|_{\mathrm{E}}}{r} \cdot \Big\|\frac{r}{\|x\|_{\mathrm{E}}} u(x)\Big\|_{\mathrm{F}} \leqslant \frac{\|x\|_{\mathrm{E}}}{r}.$$

On en déduit l'implication (i)⇒(iii) (avec $\mathrm{M} = \frac{1}{r}$). Maintenant, si $\|u(x)\|_{\mathrm{F}} \leqslant \mathrm{M} \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$, alors u est lipschitzienne de rapport M, et donc uniformément continue. On en déduit l'implication (iii)⇒(ii), et comme l'implication (ii)⇒(i) est une évidence, cela permet de conclure.

• Si $(\mathrm{E}, \|\ \|_{\mathrm{E}})$ et $(\mathrm{F}, \|\ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés avec F complet, et si $u : \mathrm{E} \to \mathrm{F}$ est linéaire continue, alors u se prolonge, par continuité, en une application linéaire continue du complété $\widehat{\mathrm{E}}$ de E dans F.

C'est une conséquence de la propriété universelle vérifiée par $\widehat{\mathrm{E}}$.

17.3. La norme d'un opérateur

Si $(\mathrm{E}, \|\ \|_{\mathrm{E}})$ et $(\mathrm{F}, \|\ \|_{\mathrm{F}})$ sont deux espaces vectoriels normés, et si $u : \mathrm{E} \to \mathrm{F}$ est une application linéaire continue, la *norme d'opérateur* $\|u\|$ de u est la borne supérieure de l'ensemble des $\|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}}$, pour $x \in \mathrm{E} - \{0\}$. On a donc $\|u(x)\|_{\mathrm{F}} \leqslant \|u\| \cdot \|x\|_{\mathrm{E}}$, quel que soit $x \in \mathrm{E}$, et $\|u\|$ est le plus petit réel ayant cette propriété.

• La norme d'opérateur est une norme sur l'espace vectoriel $\mathrm{Hom}(\mathrm{E}, \mathrm{F})$ des applications linéaires continues de E dans F.

Si $\|u\| = 0$, alors $u(x) = 0$, pour tout x, et donc $u = 0$. Si $u \in \mathrm{End}(\mathrm{E}, \mathrm{F})$ et $\lambda \in \mathbf{K}$, alors

$$\|\lambda\, u\| = \sup_{x \in \mathrm{E} - \{0\}} \|x\|_{\mathrm{E}}^{-1} \|\lambda u(x)\|_{\mathrm{F}} = \sup_{x \in \mathrm{E} - \{0\}} |\lambda| \cdot \|x\|_{\mathrm{E}}^{-1} \|u(x)\|_{\mathrm{F}} = |\lambda| \sup_{x \in \mathrm{E} - \{0\}} \|x\|_{\mathrm{E}}^{-1} \|u(x)\|_{\mathrm{F}} = |\lambda| \cdot \|u\|.$$

On conclut en remarquant que, si $u, v \in \mathrm{End}(\mathrm{E}, \mathrm{F})$, alors

$$\|u+v\| = \sup_{x\in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|u(x)+v(x)\|_{\mathrm{F}} \leqslant \sup_{x\in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}(\|u(x)\|_{\mathrm{F}} + \|v(x)\|_{\mathrm{F}})$$
$$\leqslant \big(\sup_{x\in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|u(x)\|_{\mathrm{F}}\big) + \big(\sup_{x\in \mathrm{E}-\{0\}} \|x\|_{\mathrm{E}}^{-1}\|v(x)\|_{\mathrm{F}}\big) = \|u\| + \|v\|.$$

• La norme d'opérateur est une norme d'algèbre sur l'anneau End(E) des endomorphismes linéaires continus de E.

Compte-tenu du point précédent, il ne reste plus que l'inégalité $\|u\circ v\| \leqslant \|u\|\cdot\|v\|$ à vérifier. Or $\|u\circ v(x)\|_{\mathrm{E}} \leqslant \|u\|\cdot\|v(x)\|_{\mathrm{E}} \leqslant \|u\|\cdot\|v\|\cdot\|x\|_{\mathrm{E}}$, pour tout $x \in \mathrm{E}$, par définition de $\|u\|$ et $\|v\|$. On en déduit l'inégalité cherchée.

Exercice 17.1. — (i) On munit $\mathrm{E} = \mathbf{R}^n$ ou $\mathbf{C}^n$ de la norme $\| \ \|_\infty$ définie par $\|x\|_\infty = \sup_{1\leqslant j\leqslant n} |x_j|$, si $x = (x_1, \ldots, x_n)$. Soit $u : \mathrm{E} \to \mathrm{E}$ linéaire, et soit $(a_{i,j})_{1\leqslant i,j\leqslant n}$ la matrice de u. Montrer que $\|u\|_\infty = \sup_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}|$.

(ii) Montrer que $1-u$ est inversible si $\sum_{j=1}^n |a_{i,j}| < 1$, pour $1 \leqslant i \leqslant n$. (Exprimer $(1-u)^{-1}$ comme une série en u.)

17.4. Normes équivalentes

Deux normes $\| \ \|_1$ et $\| \ \|_2$ sur E sont *équivalentes*, si l'identité est un homéomorphisme de $(\mathrm{E}, \| \ \|_1)$ sur $(\mathrm{E}, \| \ \|_2)$ (i.e. est continue ainsi que son inverse). D'après l'alinéa précédent, cela équivaut à l'existence de $\mathrm{C} > 0$ tel que $\mathrm{C}^{-1}\|x\|_1 \leqslant \|x\|_2 \leqslant \mathrm{C}\|x\|_1$, pour tout $x \in \mathrm{E}$.

• Soit E un espace vectoriel de dimension finie sur $\mathbf{K}$. Alors toutes les normes sur E sont équivalentes et E est complet pour n'importe laquelle d'entre elles.

Soit $(e_1, \ldots, e_n)$ une base de E sur $\mathbf{K}$. Comme $\mathbf{K}$ est complet, il suffit de prouver que toute norme sur E est équivalente à la norme $\| \ \|_\infty$ définie par

$$\|x_1e_1 + \cdots + x_ne_n\|_\infty = \sup(|x_1|, \ldots, |x_n|),$$

ce qui se fait par récurrence sur la dimension de E. Si cette dimension est 1, il n'y a rien à faire. Sinon, soit $\| \ \|$ une norme sur E. On déduit de l'inégalité triangulaire que

$$\|x_1e_1 + \cdots + x_ne_n\| \leqslant (\|e_1\| + \cdots + \|e_n\|)\sup(|x_1|, \ldots, |x_n|),$$

d'où l'une des deux inégalités à vérifier. Pour démontrer l'autre, raisonnons par l'absurde. Supposons qu'il existe une suite $x_1^{(k)}e_1 + \cdots + x_n^{(k)}e_n$ qui tende vers 0 pour la norme $\| \ \|$ mais pas pour la norme $\| \ \|_\infty$. Il existe alors $\mathrm{C} > 0$, $i \in \{1, \ldots, n\}$ et une sous-suite infinie telle que l'on ait $|x_i^{(k)}| \geqslant \mathrm{C}$, et donc la suite de terme général $v_k = \frac{x_1^{(k)}}{x_i^{(k)}}e_1 + \cdots + \frac{x_n^{(k)}}{x_i^{(k)}}e_n$ tend encore vers 0 pour $\| \ \|$. On en déduit que e_i est dans l'adhérence de $\mathrm{W} = \mathrm{Vect}(e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n)$, qui est complet d'après l'hypothèse de récurrence, ce qui implique $e_i \in \mathrm{W}$ et est absurde puisque les e_i forment une base de E.

• L'énoncé précédent devient *totalement faux en dimension infinie* : les normes sur un espace E de dimension infinie ne sont pas toutes équivalentes [112], et E peut être complet pour certaines d'entre elles, mais il y en a "beaucoup plus" pour lesquelles il ne l'est pas.

112. Un des problèmes de base en analyse fonctionnelle est précisément de choisir la bonne norme en fonction du problème à résoudre.

Exercice 17.2. — Soit $\mathrm{E} = \mathscr{C}([0,1])$ l'espace des fonctions continues de $[0,1]$ dans $\mathbf{C}$.

(i) Montrer que, si $\phi \in \mathrm{E}$, alors $\|\phi\|_\infty = \sup_{x\in[0,1]} |\phi(x)|$ est fini et que $\| \ \|_\infty$ est une norme sur E pour laquelle E est complet.

(ii) Montrer que $\| \ \|_1$ définie par $\|\phi\|_1 = \int_0^1 |\phi(t)|\, dt$ est une norme sur E pour laquelle E n'est pas complet.

(iii) Les normes $\| \ \|_\infty$ et $\| \ \|_1$ sont-elles équivalentes ?

Exercice 17.3. — (i) Montrer que, si $\mathscr{T}_1$ et $\mathscr{T}_2$ sont des topologies sur X, alors $\mathscr{T}_1$ est plus fine que $\mathscr{T}_2$ si et seulement si $\mathrm{id} : (\mathrm{X}, \mathscr{T}_1) \to (\mathrm{X}, \mathscr{T}_2)$ est continue.

(ii) Soit $\mathscr{T}_1$ la topologie sur l'espace $\mathscr{C}_c(\mathbf{R})$ des fonctions continues à support compact définie par la norme $\| \ \|_1$ et $\mathscr{T}_\infty$ celle définie par la norme $\| \ \|_\infty$. Montrer qu'aucune des deux topologies $\mathscr{T}_1$ et $\mathscr{T}_\infty$ n'est plus fine que l'autre.

17.5. Norme spectrale d'un opérateur

Soit $(\mathrm{E}, \| \ \|)$ un espace vectoriel normé. Si $u : \mathrm{E} \to \mathrm{E}$ est linéaire continu, on note u^n le composé $u \circ \cdots \circ u$ de n copies de u.

• La suite $(\|u^n\|^{1/n})_{n\geqslant 1}$ admet une limite, la *norme spectrale* $\|u\|_{\mathrm{sp}}$ de l'opérateur u.

On a $\|u^{n+m}\| \leqslant \|u^n\| \cdot \|u^m\|$, pour tous $n, m \geqslant 1$; l'exercice 17.4 ci-dessous permet donc, en passant aux logarithmes, de montrer que la suite $(\|u^n\|^{1/n})_{n\geqslant 1}$ admet une limite.

Exercice 17.4. — Soit $(a_n)_{n\geqslant 1}$ une suite de nombres réels. On suppose que $a_{n+k} \leqslant a_n + a_k$, pour tous $k, n \geqslant 1$. Montrer que la suite $(\frac{a_n}{n})_{n\geqslant 1}$ tend vers son inf. (dans $\overline{\mathbf{R}}$).

• Si $\| \ \|_1$ et $\| \ \|_2$ sont deux normes équivalentes sur E, alors $\|u\|_{1,\mathrm{sp}} = \|u\|_{2,\mathrm{sp}}$ pour tout $u : \mathrm{E} \to \mathrm{E}$ linéaire continu (pour $\| \ \|_1$ ou $\| \ \|_2$, les deux conditions sont équivalentes).

Il existe $\mathrm{C} > 1$ tel que $\mathrm{C}^{-1}\|x\|_1 \leqslant \|x\|_2 \leqslant \mathrm{C}\|x\|_1$, pour tout $x \in \mathrm{E}$. On en déduit que $\|u^n\|_2 = \sup_{x\neq 0} \frac{\|u^n(x)\|_2}{\|x\|_2} \leqslant \sup_{x\neq 0} \frac{\mathrm{C}\|u^n(x)\|_1}{\mathrm{C}^{-1}\|x\|_1} = \mathrm{C}^2\|u^n\|_1$. On a donc $\|u^n\|_2^{1/n} \leqslant \mathrm{C}^{2/n}\|u^n\|_1^{1/n}$, pour tout $n \geqslant 1$, et un passage à la limite nous fournit l'inégalité $\|u\|_{2,\mathrm{sp}} \leqslant \|u\|_{1,\mathrm{sp}}$. L'inégalité inverse s'obtenant en échangeant les rôles de $\| \ \|_1$ et $\| \ \|_2$, cela permet de conclure.

• Si [113] $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$, et si E est de dimension finie, alors $\|u\|_{\mathrm{sp}} = \sup_{\lambda\in \mathrm{Spec}\, u} |\lambda|$.

Comme E est de dimension finie, toutes les normes sont équivalentes, et on peut faire le calcul de $\| \ \|_{\mathrm{sp}}$ en utilisant celle que l'on veut d'après le point précédent.

Commençons par supposer que $\mathbf{K} = \mathbf{C}$. La matrice de u peut se mettre sous forme de Jordan, ce qui signifie qu'il existe une base $e_{\lambda,i}$, où λ décrit $\mathrm{Spec}\, u$ avec multiplicités éventuelles et $1 \leqslant i \leqslant a(\lambda)$ (et donc $\sum_\lambda a(\lambda) = \dim \mathrm{E}$), avec $u(e_{\lambda,i}) = \lambda e_{\lambda,i} + e_{\lambda,i-1}$ (avec la convention $e_{\lambda,j} = 0$, si $j \leqslant 0$). On a alors $u^n(e_{\lambda,i}) = \sum_{j\leqslant a(\lambda)-1} \binom{n}{j} \lambda^{n-j} e_{\lambda,i-j}$, pour tout $n \geqslant 1$, et tout $i \leqslant a(\lambda)$. On munit E de la norme $\| \sum_{\lambda,i} x_{\lambda,i} e_{\lambda,i}\| = \sup_{\lambda,i} |x_{\lambda,i}|$. On choisit $\mu \in \mathrm{Spec}\, u$ tel que $|\mu|$ réalise le maximum de $|\lambda|$, pour $\lambda \in \mathrm{Spec}\, u$, et on doit prouver que $\|u\|_{\mathrm{sp}} = |\mu|$.

• $u^n(e_{\mu,1}) = \mu^n e_{\mu,1}$, et donc $\|u^n\| \geqslant |\mu|^n$ et $\|u^n\|^{1/n} \geqslant |\mu|$, pour tout $n \geqslant 1$. On en déduit que $\|u\|_{\mathrm{sp}} \geqslant |\mu|$.

113. L'énoncé est encore valable si $\mathbf{K}$ est un corps normé complet quelconque, mais la démonstration demande d'étendre $|\ |$ à une extension de $\mathbf{K}$ contenant les valeurs propres de u ; on peut utiliser les techniques de l'alinéa 20.4.5 pour ce faire.

• Si $x = \sum_{\lambda,i} x_{\lambda,i} e_{\lambda,i}$, alors $\|u^n(x)\| \leqslant \|x\| \sum_{\lambda,i} \|u^n(e_{\lambda,i})\|$. Maintenant, si $a = \sup_\lambda a(\lambda)$, on a $\|u^n(e_{\lambda,i})\| \leqslant \sum_{j \leqslant a(\lambda)-1} \binom{n}{j} |\lambda|^{n-j} \leqslant |\mu|^n \sum_{j \leqslant a-1} \binom{n}{j} = |\mu|^n \binom{n+1}{a-1}$. On en déduit que $\|u^n\| \leqslant (\dim \mathrm{E}) |\mu|^n \binom{n+1}{a-1}$, ce qui permet, en prenant les racines n-ièmes et en passant à la limite, de prouver que $\|u\|_{\mathrm{sp}} \leqslant |\mu|$.

Ceci permet de conclure dans le cas $\mathbf{K} = \mathbf{C}$. Si $\mathbf{K} = \mathbf{R}$, on choisit une base, ce qui permet de supposer que $\mathrm{E} = \mathbf{R}^n$ que l'on munit de la norme $\| \ \|_\infty$. Si $u : \mathrm{E} \to \mathrm{E}$ est linéaire, on note $u_{\mathbf{C}} : \mathbf{C}^n \to \mathbf{C}^n$ l'application $\mathbf{C}$-linéaire dont la matrice est la même que celle de u. Il résulte de l'ex. 17.1 qu'on a alors $\|u\|_\infty = \|u_{\mathbf{C}}\|_\infty$. En utilisant cette identité pour u^n, puis en prenant les racines n-ièmes et en passant à la limite, on en déduit que $\|u\|_{\mathrm{sp}} = \|u_{\mathbf{C}}\|_{\mathrm{sp}}$, ce qui permet de se ramener au cas $\mathbf{K} = \mathbf{C}$ traité ci-dessus.

Ceci permet de conclure.

Exercice 17.5. — (i) Soient $u = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ et $v = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ (agissant sur $\mathrm{E} = \mathbf{R}^2$). Calculer $\|u\|_{\mathrm{sp}}$, $\|v\|_{\mathrm{sp}}$, $\|uv\|_{\mathrm{sp}}$ et $\|u+v\|_{\mathrm{sp}}$.

(ii) Soit $(\mathrm{E}, \| \ \|)_{\mathrm{sp}}$ un espace vectoriel normé, et soient u, v deux opérateurs linéaires continus sur E qui commutent. Montrer que $\|uv\|_{\mathrm{sp}} \leqslant \|u\|_{\mathrm{sp}} \|v\|_{\mathrm{sp}}$ et (difficile) $\|u+v\|_{\mathrm{sp}} \leqslant \|u\|_{\mathrm{sp}} + \|v\|_{\mathrm{sp}}$ (on pourra se ramener au cas où $\|u\|_{\mathrm{sp}} < 1$ et $\|v\|_{\mathrm{sp}} < 1$).

17.6. La boule unité d'un espace vectoriel normé

On suppose que $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$.

• Si E est de dimension finie, la boule unité fermée est compacte.

Par définition, la boule unité fermée est bornée, et comme elle est fermée, et que l'on est en dimension finie, elle est compacte.

• Soit E un espace vectoriel normé. Si la boule unité fermée $\mathrm{B}(0,1)$ est compacte, alors E est de dimension finie (théorème de Riesz, 1918).

Si $\mathrm{B}(0,1)$ est compacte, on peut extraire un recouvrement fini du recouvrement de $\mathrm{B}(0,1)$ par les $\mathrm{B}(x, (\frac{1}{2})^-)$, pour $x \in \mathrm{B}(0,1)$. Autrement dit, on peut trouver un sous-ensemble fini $\{e_i,\ i \in \mathrm{I}\}$ d'éléments de E tels que $\mathrm{B}(0,1) \subset \cup_{i \in \mathrm{I}} \mathrm{B}(e_i, \frac{1}{2})$. Nous allons montrer que le sous-espace E′, engendré par les $(e_i)_{i \in \mathrm{I}}$, est égal à E, ce qui permettra de conclure. Comme E′ est fermé, puisque complet, car de dimension finie (n° 17.4), il suffit de montrer que E′ est dense dans E. Soit donc $x \in \mathrm{E}$, et soient $a \in \mathbf{Z}$ et $y \in \mathrm{E}'$ tels que $\|x - y\| \leqslant 2^{-a}$ (un tel couple existe : il suffit de prendre $y = 0$ et a assez petit pour que $\|x\| \leqslant 2^{-a}$). On a $2^a(x-y) \in \mathrm{B}(0,1)$ et, par définition de la famille $(e_i)_{i \in \mathrm{I}}$, il existe $i \in \mathrm{I}$ tel que $\|2^a(x-y) - e_i\| \leqslant \frac{1}{2}$. Mais alors $y' = y + 2^{-a} e_i \in \mathrm{E}'$ et $\|x - y'\| \leqslant 2^{-a-1}$. Ceci permet de construire, par récurrence, une suite $(y_n)_{n \in \mathrm{N}}$ d'éléments de E′ vérifiant $\|x - y_n\| \leqslant 2^{-n-a}$, ce qui prouve que x est dans l'adhérence de E′, et permet de conclure.

Exercice 17.6. — Soient $\mathbf{K}$ un corps normé complet et E un $\mathbf{K}$-espace vectoriel normé.

(i) Montrer que $\mathbf{K}$ est localement compact si et seulement si $\mathrm{B}(0,1)$ est compacte.

(ii) Montrer que $\mathrm{B}_{\mathrm{E}}(0,1)$ est compacte, si $\mathbf{K}$ est localement compact et si E est de dimension finie.

(iii) Montrer, réciproquement, que $\mathbf{K}$ est localement compact et E est de dimension finie, si $\mathrm{B}_{\mathrm{E}}(0,1)$ est compacte.

17.7. Applications bilinéaires continues

Si $(\mathrm{E}_1, \| \ \|_1)$ et $(\mathrm{E}_2, \| \ \|_2)$ sont deux espaces vectoriels normés, l'espace topologique $\mathrm{E}_1 \times \mathrm{E}_2$ est aussi un espace vectoriel normé, la topologie produit étant celle associée à la norme $\|(x_1, x_2)\| = \sup(\|x_1\|_1, \|x_2\|_2)$ ou à toute autre norme équivalente comme par exemple $\|(x_1, x_2)\| = (\|x_1\|_1^2 + \|x_2\|_2^2)^{1/2}$.

• Soient $(\mathrm{E}_1, \| \ \|_1)$, $(\mathrm{E}_2, \| \ \|_2)$ et $(\mathrm{F}, \| \ \|_\mathrm{F})$ des espaces vectoriels normés, et $b : \mathrm{E}_1 \times \mathrm{E}_2 \to \mathrm{F}$ une application *bilinéaire*. Alors :

(i) b est continue si et seulement si il existe $\mathrm{C} > 0$ tel que $\|b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C} \cdot \|x_1\|_1 \cdot \|x_2\|_2$ quels que soient $x_1 \in \mathrm{E}_1$ et $x_2 \in \mathrm{E}_2$;

(ii) si F est complet et b continue, alors b s'étend par continuité en une application bilinéaire du complété $\widehat{\mathrm{E}}_1 \times \widehat{\mathrm{E}}_2$ de $\mathrm{E}_1 \times \mathrm{E}_2$ dans F.

Si b est continue, il existe $r_1, r_2 > 0$ tels que $b^{-1}(\mathrm{B}_\mathrm{F}(0, 1^-))$ contienne $\mathrm{B}_{\mathrm{E}_1}(0, r_1^-) \times \mathrm{B}_{\mathrm{E}_2}(0, r_2^-)$. Autrement dit, $\|b(x_1, x_2)\|_\mathrm{F} < 1$ si $\|x_1\|_1 < r_1$ et $\|x_2\|_2 < r_2$. Par bilinéarité, cela implique que

$$\|b(x_1, x_2)\|_\mathrm{F} = \frac{\|x_1\|_1 \cdot \|x_2\|_2}{r_1 r_2} \Big\| b\Big(\frac{r_1}{\|x_1\|_1} x_1, \frac{r_2}{\|x_2\|_2} x_2\Big)\Big\|_\mathrm{F} \leqslant \frac{\|x_1\|_1 \cdot \|x_2\|_2}{r_1 r_2}.$$

Réciproquement, s'il existe $\mathrm{C} > 0$ tel que $\|b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C} \cdot \|x_1\|_1 \cdot \|x_2\|_2$, quels que soient $x_1 \in \mathrm{E}_1$ et $x_2 \in \mathrm{E}_2$, alors

$$\|b(x_1 + h_1, x_2 + h_2) - b(x_1, x_2)\|_\mathrm{F} \leqslant \mathrm{C}(\|x_1\|_1 \cdot \|h_2\|_2 + \|h_1\|_1 \cdot \|x_2\|_2 + \|h_1\|_1 \cdot \|h_2\|_2),$$

ce qui prouve que b est lipschitzienne de rapport $\mathrm{C} \cdot (\|x_1\|_1 + \|x_2\|_2 + 1)$ sur $\mathrm{B}_{\mathrm{E}_1}(x_1, 1^-) \times \mathrm{B}_{\mathrm{E}_2}(x_2, 1^-)$. Ceci prouve que b est continue (et donc termine la démonstration du (i)), et permet de déduire le (ii) du deuxième point du n° 14.3.

Exercice 17.7. — Soit $\mathbf{K}$ un corps normé complet.

(i) Montrer que $(a, b) \mapsto a + b$ et $(a, b) \mapsto ab$ sont continues sur $\mathbf{K}^2$.

(ii) En déduire que si X est un espace topologique, et si $f : \mathrm{X} \to \mathbf{K}$ et $g : \mathrm{X} \to \mathbf{K}$ sont continues, alors $f + g : \mathrm{X} \to \mathbf{K}$ et $fg : \mathrm{X} \to \mathbf{K}$ sont continues.

18. Espaces préhilbertiens

Dans tout ce §, $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$.

18.1. Produits scalaires

Soit E un espace vectoriel sur $\mathbf{K}$.

• Un *produit scalaire* sur E est une application $\langle \ , \ \rangle : \mathrm{E} \times \mathrm{E} \to \mathbf{K}$ qui est :

– *sesquilinéaire*, i.e. linéaire par rapport à y (i.e. $\langle x, y_1 + y_2\rangle = \langle x, y_1\rangle + \langle x, y_2\rangle$ et $\langle x, \lambda y\rangle = \lambda\langle x, y\rangle$, si $\lambda \in \mathbf{K}$, $x, y, y_1, y_2 \in \mathrm{E}$), et semi-linéaire [114] par rapport à x (i.e. $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$ et $\langle \lambda x, y\rangle = \overline{\lambda}\langle x, y\rangle$, si $\lambda \in \mathbf{K}$, $x, y, x_1, x_2 \in \mathrm{E}$) ;

– *symétrique*, i.e. $\langle y, x\rangle = \overline{\langle x, y\rangle}$, quels que soient $x, y \in \mathrm{E}$;

114. Si $\mathbf{K} = \mathbf{R}$, on a $\overline{x} = x$, et donc la sesquilinérarité n'est autre que la bilinéarité.

– *définie positive*, i.e $\langle x, x\rangle \geqslant 0$, si $x \in \mathrm{E}$, et $\langle x, x\rangle = 0$, si et seulement si $x = 0$.

• Un *espace préhilbertien* est un espace vectoriel muni d'un produit scalaire. Si E est préhilbertien, on définit $\| \ \| : \mathrm{E} \to \mathbf{R}$ en posant $\|x\| = \langle x, x\rangle^{1/2}$. Alors $\| \ \|$ est une norme, et on a $|\langle x, y\rangle| \leqslant \|x\| \cdot \|y\|$ pour tous $x, y \in \mathrm{E}$ (*inégalite de Cauchy-Schwarz*) : l'application $\mathbf{R}$-bilinéaire $(x, y) \mapsto \langle x, y\rangle$, de $\mathrm{E} \times \mathrm{E}$ dans $\mathbf{K}$, est continue.

$\|x+ty\|^2 = \|x\|^2 + 2t\,\mathrm{Re}(\langle x, y\rangle) + t^2\|y\|^2$ est toujours $\geqslant 0$, pour $t \in \mathbf{R}$; son discriminant est donc $\leqslant 0$, ce qui se traduit par $|\mathrm{Re}(\langle x, y\rangle)| \leqslant \|x\| \cdot \|y\|$ pour tous $x, y \in \mathrm{E}$. Choisissons alors $\theta \in \mathbf{R}$ tel que $e^{-i\theta}\langle x, y\rangle \in \mathbf{R}_+$. En utilisant la majoration précédente pour $e^{i\theta}x$ et y au lieu de x et y, on obtient $|\langle x, y\rangle| = \mathrm{Re}(\langle e^{i\theta}x, y\rangle) \leqslant \|e^{i\theta}x\| \cdot \|y\| = \|x\| \cdot \|y\|$, ce qui prouve l'inégalité de Cauchy-Schwarz. L'inégalité triangulaire s'en déduit car

$$\|x + y\|^2 = \|x\|^2 + 2\mathrm{Re}(\langle x, y\rangle) + \|y\|^2 \leqslant \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.$$

L'identité $\|\lambda\, x\| = |\lambda|\, \|x\|$ étant immédiate, $\| \ \|$ est une norme, ce qui permet de conclure.

• $\mathbf{C}^n$ et $\mathbf{R}^n$, muni des *produits scalaires usuels* $\langle x, y\rangle = \sum_{i=1}^n \overline{x}_i y_i$ et $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$, sont des espaces préhilbertiens. Si on utilise l'identification $\mathbf{K}^n = \mathrm{M}_{n\times 1}(\mathbf{K})$, les produits scalaires usuels s'écrivent aussi sous la forme $\langle \mathrm{X}, \mathrm{Y}\rangle = {}^{\mathrm{t}}\overline{\mathrm{X}}\mathrm{Y}$ (resp. $\langle \mathrm{X}, \mathrm{Y}\rangle = {}^{\mathrm{t}}\mathrm{XY}$) si $\mathrm{X} = {}^{\mathrm{t}}(x_1, \ldots, x_n)$ et $\mathrm{Y} = {}^{\mathrm{t}}(y_1, \ldots, y_n)$ sont des éléments de $\mathbf{C}^n$ (resp. de $\mathbf{R}^n$).

• Si E est un espace préhilbertien réel, on peut étendre le produit scalaire $\langle \ , \ \rangle$ sur E au complexifié $\mathrm{E}_{\mathbf{C}} = \mathrm{E} \oplus i\mathrm{E}$ de E en posant $\langle x'+iy', x+iy\rangle_{\mathbf{C}} = \langle x', x\rangle - i\langle y', x\rangle + i\langle x', y\rangle + \langle y', y\rangle$, ce qui fait de $\mathrm{E}_{\mathbf{C}}$ un espace préhilbertien complexe.

Exercice 18.1. — Montrer que $(f, g) \mapsto \langle f, g\rangle = \int_0^1 \overline{f(t)}\, g(t)\, dt$ est un produit scalaire sur $\mathscr{C}([0, 1])$.

18.2. Orthogonalité

Dans tout ce qui suit, E est un espace préhilbertien réel ou complexe.

• On dit que $x, y \in \mathrm{E}$ sont *orthogonaux* si $\langle x, y\rangle = 0$. Si x et y sont orthogonaux, ils vérifient la *relation de Pythagore* [115] $\|x + y\|^2 = \|x\|^2 + \|y\|^2$. Dans le cas général, ils vérifient *l'identité de la médiane* $\|x\|^2 + \|y\|^2 = 2\left\|\frac{x+y}{2}\right\|^2 + \frac{1}{2}\|x - y\|^2$, qui se démontre sans problème en développant le membre de droite.

• Une famille $(e_i)_{i\in \mathrm{I}}$ d'éléments de E est dite *orthonormale*, si $\|e_i\| = 1$ pour tout i, et si e_i et e_j sont orthogonaux pour $i \neq j$. On a alors $\langle x, y\rangle = \sum_{i\in \mathrm{I}} \overline{x}_i y_i$ et $\|x\| = \sum_{i\in \mathrm{I}} |x_i|^2$, si $x = \sum_{i\in \mathrm{I}} x_i e_i$ et $y = \sum_{i\in \mathrm{I}} y_i e_i$, pour tous $(x_i)_{i\in \mathrm{I}}, (y_i)_{i\in \mathrm{I}} \in \mathbf{K}^{(\mathrm{I})}$.

• Si F est un sous-espace vectoriel de E, et si $x \in \mathrm{E}$, il existe au plus un élément $p_{\mathrm{F}}(x)$ de F, appelé (s'il existe) *projection orthogonale de x sur* F, tel que $x - p_{\mathrm{F}}(x)$ soit orthogonal à F tout entier.

115. Si $\mathbf{K} = \mathbf{R}$, la relation de Pythagore entraîne l'orthogonalité (« théorème » de Pythagore, pauvre Pythagore...) ; ce n'est plus le cas si $\mathbf{K} = \mathbf{C}$: en développant $\|x + y\|^2$, on obtient $\langle x, y\rangle + \langle y, x\rangle = 0$ dont on peut juste déduire que $\langle x, y\rangle$ est imaginaire pur.

Si $y_1, y_2 \in \mathrm{F}$ sont tels que $x - y_1$ et $x - y_2$ sont orthogonaux à F tout entier, alors $y_1 - y_2 = (x - y_1) - (x - y_2)$ est orthogonal à F, et comme $y_1 - y_2 \in \mathrm{F}$, on a $\langle y_1 - y_2, y_1 - y_2 \rangle = 0$, ce qui implique $y_1 = y_2$.

• Si F est un sous-espace de dimension finie de E muni d'une base orthonormale $(e_1, \dots, e_d)$, alors p_F est partout définie, et $p_\mathrm{F}(x) = \sum_{i=1}^{d} \langle e_i, x \rangle\, e_i$. En particulier, si $x \in \mathrm{F}$, ses coordonnées dans la base $(e_1, \dots, e_d)$ sont les $\langle e_i, x \rangle$, et $\|x\|^2 = \sum_{i=1}^{d} |\langle e_i, x \rangle|^2$.

Soit $y = \sum_{i=1}^{d} \langle e_i, x \rangle\, e_i$. Alors $\langle e_j, x - y \rangle = \langle e_j, x \rangle - \sum_{i=1}^{d} \langle e_i, x \rangle \langle e_j, e_i \rangle = 0$, pour tout j. On en déduit que $x - y$ est orthogonal à chacun des e_j, et donc à F tout entier par linéarité. De plus, $y \in \mathrm{F}$ par construction, et donc $y = p_\mathrm{F}(x)$. On en déduit le résultat.

• Le *procédé d'orthonormalisation de Schmidt*, décrit ci-dessous, permet, si $(f_i)_{i \in \mathrm{I}}$ est une famille libre d'éléments de E, avec I dénombrable, de fabriquer une base orthonormale de l'espace F engendré par les f_i.

On se ramène, en numérotant les éléments de I, au cas où I est un intervalle de $\mathbf{N}$ contenant 0. On note F_n le sous-espace de F engendré par les f_i, pour $i \leqslant n$. On construit par récurrence une famille orthonormale e_i d'éléments de F telle que $(e_0, \dots, e_n)$ soit une base (orthonormale) de F_n, pour tout n. Pour cela, on pose $e_0 = \frac{1}{\|f_0\|} f_0$, et en supposant $e_0, \dots, e_{n-1}$ construits (et donc F_{n-1} muni d'une base orthonormale), on note $g_n = f_n - p_{\mathrm{F}_{n-1}}(f_n)$. On a $g_n \neq 0$ puisque $f_n \notin \mathrm{F}_{n-1}$, la famille des f_j étant supposée libre. On pose $e_n = \frac{1}{\|g_n\|} g_n$. Par construction, g_n (et donc aussi e_n) est orthogonal à chacun des e_i, pour $i \leqslant n - 1$, et comme $\|e_n\| = 1$, cela permet de faire marcher la récurrence.

• Tout sous-espace de dimension finie de E possède des bases orthonormales.

Il suffit d'appliquer le procédé d'orthonormalisation de Schmidt à une base quelconque.

• Si E est de dimension n, et si $e_1, \dots, e_n$ est une base othonormale de E, les coordonnées de $x \in \mathrm{E}$ dans cette base sont $\langle e_1, x \rangle, \dots \langle e_n, x \rangle$, et on a $\langle x, y \rangle = \sum_{i=1}^{n} \overline{\langle e_i, x \rangle} \langle e_i, y \rangle$, si $x, y \in \mathrm{E}$; autrement dit, un espace préhilbertien de dimension n sur $\mathbf{K}$ est isomorphe à $\mathbf{K}^n$ muni du produit scalaire usuel.

On a $\langle e_i, \sum_{j=1}^{n} \lambda_j e_j \rangle = \lambda_i$. Le résultat s'en déduit.

• Si F est un sous-espace de dimension finie de E, la projection orthogonale p_F sur F est partout définie, est linéaire et vérifie $p_\mathrm{F} \circ p_\mathrm{F} = p_\mathrm{F}$; c'est donc une projection, son image est F et son noyau est l'*orthogonal* $\mathrm{F}^\perp$ de F (i.e. l'ensemble des $x \in \mathrm{E}$ tels que $\langle x, y \rangle = 0$ pour tout $y \in \mathrm{F}$) qui est donc un supplémentaire de F. De plus :

◇ $\|p_\mathrm{F}(x)\| \leqslant \|x\|$ pour tout $x \in \mathrm{E}$.

◇ $\|x - p_\mathrm{F}(x)\| \leqslant \|x - y\|$, pour tout $y \in \mathrm{F}$; en d'autres termes, $\|x - p_\mathrm{F}(x)\|$ est la distance $d(x, \mathrm{F})$ de x à F.

Pour montrer que p_F est partout définie, il suffit de prendre une base orthonormale $e_1, \dots, e_d$ de F, et d'utiliser un des points précédents selon lequel $p_\mathrm{F}(x) = \sum_{i=1}^{d} \langle e_i, x \rangle e_i$; la linéarité de p_F s'en déduit en utilisant celle de $\langle\ ,\ \rangle$ par rapport à la seconde variable.

Maintenant, $p_\mathrm{F}(x) = x$ si $x \in \mathrm{F}$ (car $x - x$ est orthogonal à F tout entier), et $p_\mathrm{F}(x) \in \mathrm{F}$ par définition ; on en tire la relation $p_\mathrm{F} \circ p_\mathrm{F} = p_\mathrm{F}$. Il s'ensuit que p_F est une projection et son

image est F d'après ce qui précède. En revenant à la définition, on voit que $p_{\mathrm{F}}(x) = 0$ si et seulement si x est orthogonal à F, et donc $\operatorname{Ker} p_{\mathrm{F}} = \mathrm{F}^{\perp}$.

Enfin, $x - p_{\mathrm{F}}(x)$ et $p_{\mathrm{F}}(x)$ étant orthogonaux, on a $\|p_{\mathrm{F}}(x)\|^2 = \|x\|^2 - \|x - p_{\mathrm{F}}(x)\|^2$, et donc $\|p_{\mathrm{F}}(x)\| \leqslant \|x\|$; si $y \in \mathrm{F}$, alors $x - p_{\mathrm{F}}(x)$ et $y - p_{\mathrm{F}}(x)$ sont orthogonaux, et donc $\|x - y\|^2 = \|x - p_{\mathrm{F}}(x)\|^2 + \|p_{\mathrm{F}}(x) - y\|^2$, et $\|x - y\| \geqslant \|x - p_{\mathrm{F}}(x)\|$.

Ceci termine la démonstration.

Si $v_1, \ldots, v_n \in \mathrm{E}$, soit $\mathrm{G}(v_1, \ldots, v_n) = (\langle v_i, v_j \rangle)_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(\mathbf{C})$ la *matrice de Gram* de $v_1, \ldots, v_n$; son déterminant $|\mathrm{G}(v_1, \ldots, v_n)|$ est le *déterminant de Gram* de $v_1, \ldots, v_n$.

• $|\mathrm{G}(v_1, \ldots, v_n)| = d(v_1, \mathrm{Vect}(v_2, \ldots, v_n))^2 |\mathrm{G}(v_2, \ldots, v_n)|$.

On écrit v_1 sous la forme $v_1^{\perp} + \sum_{j=2}^{n} \lambda_j v_j$, avec $v_1^{\perp}$ orthogonal à $\mathrm{F} = \mathrm{Vect}(v_2, \ldots, v_n)$, et donc $v_1^{\perp} = v_1 - p_{\mathrm{F}}(v_1)$. On ne change pas $|\mathrm{G}(v_1, \ldots, v_n)|$, si on retire à la première colonne de la matrice de Gram la combinaison linéaire des autres où le coefficient de la j-ième est λ_j, ce qui à pour effet de remplacer $\langle v_i, v_1 \rangle$ par $\langle v_i, v_1^{\perp} \rangle$. Or $\langle v_i, v_1^{\perp} \rangle = 0$ si $i \geqslant 2$, et $\langle v_1, v_1^{\perp} \rangle = \|v_1^{\perp}\|^2$, ce qui permet, en développant $|\mathrm{G}(v_1, \ldots, v_n)|$ par rapport à la première colonne, d'obtenir la formule $|\mathrm{G}(v_1, \ldots, v_n)| = \|v_1^{\perp}\|^2 |\mathrm{G}(v_2, \ldots, v_n)|$. On conclut en remarquant que $\|v_1^{\perp}\| = d(v_1, \mathrm{F})$.

• Le rang de $\mathrm{G}(v_1, \ldots, v_n)$ est le même que celui de $v_1, \ldots, v_n$; en particulier, $v_1, \ldots, v_n$ est une famille libre si et seulement si son déterminant de Gram est non nul.

Quitte à réordonner les v_i, ce qui ne fait que permuter les lignes et les colonnes de la matrice de Gram et ne change pas son rang, on peut supposer que $v_1, \ldots, v_r$ est une famille libre, et $v_j = \sum_{j=1}^{r} a_{i,j} v_i$, si $j \geqslant r + 1$. Si on note $\mathrm{X}_j = {}^{\mathrm{t}}(\langle v_1, v_j \rangle, \ldots, \langle v_n, v_j \rangle)$ la j-ième colonne de la matrice de Gram, la linéarité de $\langle\ ,\ \rangle$ par rapport à la seconde variable, nous fournit la relation $\mathrm{X}_j = \sum_{j=1}^{r} a_{i,j} \mathrm{X}_i$ si $j \geqslant r + 1$. Il s'ensuit que les colonnes de la matrices sont de rang $\leqslant r$, et donc que le rang de la matrice de Gram est $\leqslant r$.

Par ailleurs, le mineur $r \times r$ en haut à gauche est le déterminant de Gram de $v_1, \ldots, v_r$. D'après le point précèdent, il est égal à $\prod_{i=1}^{r} d(v_i, \mathrm{F}_{i-1})^2$, où F_{i-1} est l'espace engendré par $v_1, \ldots, v_{i-1}$; il est donc non nul puisque $v_i \notin \mathrm{F}_{i-1}$ étant donné que $v_1, \ldots, v_r$ est libre. Il s'ensuit que le rang de la matrice de Gram est $\geqslant r$. Ceci permet de conclure.

Exercice 18.2. — Soit $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{C})$. Exprimer ${}^{\mathrm{t}}\overline{\mathrm{A}}\mathrm{A}$ comme une matrice de Gram ; en déduire que $|\det \mathrm{A}|^2 \leqslant \prod_{j=1}^{n} (|a_{1,j}|^2 + \cdots + |a_{n,j}|^2)$.

Exercice 18.3. — (i) Soit $\mathrm{A} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{R})$, à coefficients non diagonaux tous égaux à $k \geqslant 0$, et à coefficients diagonaux $k_1, \ldots, k_n$ vérifiant $k_i > 0$, et $k_i \geqslant k$ pour tout i, avec égalité pour au plus un i. Montrer que A est inversible. (On pourra s'intéresser aux signes des solutions de $\mathrm{AX} = 0$.)

(ii) Soit I un ensemble de parties non vides de $\{1, \ldots, m\}$ tel qu'il existe $k \in \mathbf{N}$ tel que $|\mathrm{E} \cap \mathrm{E}'| = k$, pour tous $\mathrm{E}, \mathrm{E}' \in \mathrm{I}$ avec $\mathrm{E} \neq \mathrm{E}'$. Montrer que $|\mathrm{I}| \leqslant m$.

(iii) Peut-on avoir $|\mathrm{I}| = m$, si $k \geqslant 1$?

18.3. Unitarité

18.3.1. *Endomorphisme unitaire*

Un endomorphisme u de E est dit *unitaire* si $\langle u(x), u(y) \rangle = \langle x, y \rangle$ pour tous x, y.

• u est unitaire si et seulement si c'est une *isométrie* (i.e. $\|u(x)\| = \|x\|$, pour tout x).

Si u est unitaire, $\|u(x)\|^2 = \langle u(x), u(x)\rangle = \langle x, x\rangle = \|x\|^2$ pour tout x, et u est une isométrie.

Si u est une isométrie, $\|u(x) + u(y)\|^2 - \|u(x)\|^2 - \|u(y)\|^2 = \|x + y\|^2 - \|x\|^2 - \|y\|^2$, et donc $\mathrm{Re}(\langle u(x), u(y)\rangle) = \mathrm{Re}(\langle x, y\rangle)$, pour tous $x, y \in \mathrm{E}$. En appliquant ceci à ix et y au lieu de x et y, on obtient $\mathrm{Im}(\langle u(x), u(y)\rangle) = \mathrm{Im}(\langle x, y\rangle)$, et donc $\langle u(x), u(y)\rangle = \langle x, y\rangle$, ce qui prouve que u est unitaire.

• Si E est de dimension finie, les endomorphisme unitaires forment un sous-groupe de GL(E).

Notons H l'ensemble des endomorphismes unitaires. Alors H contient id et donc n'est pas vide. Si $u, v \in \mathrm{H}$, alors $\|u \circ v(x)\| = \|u(v(x))\| = \|v(x)\| = \|x\|$, ce qui prouve que $u \circ v$ est une isométrie et donc est unitaire. Enfin, si $u \in \mathrm{H}$, alors $\operatorname{Ker} u = \{0\}$, puisque $u(x) = 0$ implique $\|x\| = \|u(x)\| = 0$, et donc u est injectif et, par suite, bijectif puisque nous sommes en dimension finie. Si $u^{-1} \in \mathrm{GL(E)}$ est son inverse, alors $\|x\| = \|u \circ u^{-1}(x)\| = \|u^{-1}(x)\|$ pour tout x, puisque u est une isométrie. Il s'ensuit que u^{-1} est une isométrie et donc est unitaire, ce qui montre que tout élément de H a un inverse dans H. Ceci permet de conclure.

• Si $u \in \mathrm{End(E)}$ est unitaire, et si F est un sous-espace de dimension finie de E stable par u, alors $\mathrm{F}^\perp$ est stable par u.

Si u est unitaire, alors u est une isométrie et donc u est injectif ; sa restriction à F est a fortiori injective et donc bijective puisque F est de dimension finie. Si $y \in \mathrm{F}$, il existe donc $u^{-1}(y) \in \mathrm{F}$ tel que $u(u^{-1}(y)) = y$. Il s'ensuit que, si $x \in \mathrm{F}^\perp$, alors $\langle x, u^{-1}(y)\rangle = 0$, et donc $\langle u(x), y\rangle = \langle u(x), u(u^{-1}(y))\rangle = \langle x, u^{-1}(y)\rangle = 0$, pour tout $y \in \mathrm{F}$. Ceci équivaut à $u(x) \in \mathrm{F}^\perp$, ce qui permet de conclure.

• Si E est de dimension finie sur $\mathbf{C}$, et si $u \in \mathrm{End(E)}$ est unitaire, les valeurs propres de u sont de module 1, et il existe une base orthonormale dans laquelle u se diagonalise.

Si $u(x) = \lambda x$ et $x \neq 0$, l'égalité $\|u(x)\| = \|x\|$ se traduit par $|\lambda| = 1$. Les valeurs propres de u sont donc de module 1. Prouvons, par récurrence sur $n = \dim \mathrm{E}$, qu'un opérateur unitaire u se diagonalise dans une base orthonormée. Si $n = 1$, tout x non nul est vecteur propre et $e_1 = \frac{1}{\|x\|}x$ est une base de E formée de vecteurs propres. Si $n \geqslant 2$, alors u admet une valeur propre λ_1 puisque E est de dimension finie. Il existe donc un vecteur propre e_1 de u pour la valeur propre λ_1, vérifiant $\|e_1\| = 1$, et le supplémentaire orthogonal F de $\mathbf{C}e_1$, qui est de dimension $n - 1$, est stable par u. La restriction u_F de u à F est unitaire, et on peut donc lui appliquer l'hypothèse de récurrence, ce qui nous fournit une base orthonormale $e_2, \ldots, e_n$ de F dans laquelle u_F se diagonalise, et donc une base orthonormale $e_1, \ldots, e_n$ de E dans laquelle u se diagonalise.

• Une symétrie s est unitaire si et seulement si les espaces propres V^+ et V^- pour les valeurs propres 1 et -1 sont orthogonaux ; si c'est le cas, on dit que s est la *symétrie orthogonale* par rapport à V^+.

D'après le point précédent, si s est unitaire, alors s peut se diagonaliser dans une base orthonormée et donc les espaces propres associés à deux valeurs propres distinctes sont orthogonaux. Réciproquement, si V^+ et V^- sont orthognaux, alors s est une symétrie et donc est unitaire car $\mathrm{V} = \mathrm{V}^+ \oplus \mathrm{V}^-$ et $\|s(v^+ + v^-)\|^2 = \|v^+ - v^-\|^2 = \|v^+\|^2 + \|v^-\|^2 = \|v^+ + v^-\|^2$, si $v^+ \in \mathrm{V}^+$ et $v^- \in \mathrm{V}^-$.

Exercice 18.4. — On suppose E de dimension n sur $\mathbf{K}$.

(i) Si $v_1 \neq v_2$ et si $\|v_1\| = \|v_2\|$, montrer qu'il existe une symétrie orthogonale s par rapport à un hyperplan telle que $s(v_1) = v_2$.

(ii) En déduire, par récurrence sur n, que tout endomorphisme unitaire u de déterminant ± 1 est le composé d'au plus n symétries orthogonales par rapport à des hyperplans (où $n = 0$ est permis).

18.3.2. *Le groupe unitaire et ses sous-groupes*

$\mathrm{P} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{K})$ est dite *unitaire* si ${}^t\overline{\mathrm{P}}\mathrm{P} = 1$. Une matrice unitaire à coefficients réels est aussi dite *orthogonale*, et la condition devient ${}^t\mathrm{P}\mathrm{P} = 1$ puisque $\overline{\mathrm{P}} = \mathrm{P}$.

• Si $\mathrm{P} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{K})$, les conditions suivantes sont équivalentes :
- ◇ P est unitaire,
- ◇ les colonnes de P forment une base orthonormale de $\mathbf{K}^n$,
- ◇ les lignes de P forment une base orthonormale de $\mathbf{K}^n$.

Si P est une matrice, ${}^t\overline{\mathrm{P}}\mathrm{P}$ est la matrice de Gram des colonnes de P. On a donc ${}^t\overline{\mathrm{P}}\mathrm{P} = 1$ si et seulement si les colonnes de P forment une base orthonormale. Maintenant, si ${}^t\overline{\mathrm{P}}\mathrm{P} = 1$, alors $\mathrm{P}{}^t\overline{\mathrm{P}} = 1$, et donc $\overline{\mathrm{P}}{}^t\mathrm{P} = 1$ (en appliquant la conjugaison complexe). Il s'ensuit que P est unitaire si et seulement si ${}^t\mathrm{P}$ est unitaire, ce qui, d'après ce qui précède, équivaut à ce que les colonnes de ${}^t\mathrm{P}$, qui sont les lignes de P, forment une base orthonormale de $\mathbf{K}^n$.

• Si P est unitaire, alors $u_\mathrm{P} : \mathbf{K}^n \to \mathbf{K}^n$ est unitaire. Réciproquement, si E est de dimension finie et si $u \in \mathrm{End}(\mathrm{E})$ est unitaire, la matrice de u dans une base orthonormée est unitaire.

Si $\mathrm{X}, \mathrm{Y} \in \mathbf{K}^n$, on a $\langle u_\mathrm{P}(\mathrm{X}), u_\mathrm{P}(\mathrm{Y})\rangle = \langle \mathrm{PX}, \mathrm{PY}\rangle = {}^t(\overline{\mathrm{PX}})\mathrm{PY} = {}^t\overline{\mathrm{X}}{}^t\overline{\mathrm{P}}\mathrm{PY} = {}^t\overline{\mathrm{X}}\mathrm{Y} = \langle \mathrm{X}, \mathrm{Y}\rangle$, si P est unitaire, et donc u_P est unitaire.

Réciproquement, si u est unitaire, alors l'image $u(e_1), \ldots, u(e_n)$ d'une base orthonormale $e_1, \ldots, e_n$ par u est encore orthonormale puisque $\langle u(e_i), u(e_j)\rangle = \langle e_i, e_j\rangle$. Comme l'application $x \mapsto \mathbf{e}\backslash x$, qui envoie un vecteur sur la colonne de ses coordonnées dans la base $e_1, \ldots, e_n$, est un isomorphisme d'espaces préhilbertiens E sur $\mathbf{K}^n$ muni du produit scalaire usuel, il s'ensuit que $\mathbf{e}\backslash u{\cdot}e_1, \ldots, \mathbf{e}\backslash u{\cdot}e_n$ est une base orthonormée de $\mathbf{K}^n$, et donc que la matrice $\mathbf{e}\backslash u{\cdot}\mathbf{e}$ de u dans la base $e_1, \ldots, e_n$, dont les colonnes sont $\mathbf{e}\backslash u{\cdot}e_1, \ldots, \mathbf{e}\backslash u{\cdot}e_n$, est unitaire d'après le point précédent. Ceci permet de conclure.

On note $\mathbf{U}(n) \subset \mathbf{GL}_n(\mathbf{C})$ l'ensemble des matrices unitaires et $\mathbf{O}(n) \subset \mathbf{GL}_n(\mathbf{R})$ l'ensemble des matrices orthogonales.

• $\mathbf{U}(n)$ et $\mathbf{O}(n)$ sont des sous-groupes de $\mathbf{GL}_n(\mathbf{C})$ et $\mathbf{GL}_n(\mathbf{R})$; il en est de même de leurs intersections respectives $\mathbf{SU}(n)$ et $\mathbf{SO}(n)$ avec le $\mathbf{SL}_n(\mathbf{C})$: les groupes $\mathbf{U}(n)$, $\mathbf{O}(n)$, $\mathbf{SU}(n)$ et $\mathbf{SO}(n)$ sont appelés respectivement *groupe unitaire*, *groupe orthogonal*, *groupe spécial unitaire*, et *groupe spécial orthogonal* (de degré n).

$\mathrm{P} \mapsto u_\mathrm{P}$ induit un isomorphisme de $\mathbf{U}(n)$ sur le sous-groupe de $\mathrm{GL}(\mathbf{C}^n)$ des endomorphismes unitaires de $\mathbf{C}^n$ muni du produit scalaire usuel ; il en résulte que $\mathbf{U}(n)$ est un groupe. Une intersection de sous-groupes étant un sous-groupe, on en déduit que $\mathbf{O}(n)$, qui est égal à $\mathbf{U}(n) \cap \mathbf{GL}_n(\mathbf{R})$, est un groupe, et que $\mathbf{SU}(n)$ et $\mathbf{SO}(n)$ sont des groupes.

• Si $\mathrm{Q} \in \mathbf{U}(n)$, il existe $\mathrm{P} \in \mathbf{U}(n)$ et D diagonale, avec des termes diagonaux de module 1, telles que $\mathrm{Q} = \mathrm{PDP}^{-1} = \mathrm{PD}{}^t\overline{\mathrm{P}}$.

C'est une traduction du fait que $u_{\mathrm{Q}} : \mathbf{C}^n \to \mathbf{C}^n$ se diagonalise dans une base orthonormée et que toutes ses valeurs propres sont de module 1, puisqu'il est unitaire.

Exercice 18.5. — Montrer que $\mathbf{U}(n)$ et $\mathbf{SU}(n)$ sont connexes par arcs.

• Si $\mathrm{P} \in \mathbf{SO}(2)$, il existe un unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$, tel que P soit la matrice $\mathrm{R}_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ de la *rotation d'angle* θ, et $\theta \mapsto \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ induit un isomorphisme de groupes de $\mathbf{R}/2\pi\mathbf{Z}$ sur $\mathbf{SO}(2)$.

Si $\mathrm{P} = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$, l'orthogonalité des colonnes se traduit par $ac+bd=0$, et donc par l'existence de $\lambda \in \mathbf{R}$ tel que $(c,d) = \lambda(-b,a)$. Comme $\det \mathrm{P} = 1$, cela donne $\lambda(a^2+b^2) = 1$, et comme les colonnes sont de norme 1, on a $a^2+b^2=1$ et $\lambda = 1$. Maintenant, la relation $a^2+b^2=1$ montre qu'il existe un unique $\theta \in \mathbf{R}/2\pi\mathbf{Z}$ avec $\cos\theta = a$ et $\sin\theta = b$.

Il en résulte que $\theta \mapsto \mathrm{R}_\theta$ est une bijection de $\mathbf{R}/2\pi\mathbf{Z}$ sur $\mathbf{SO}(2)$. C'est aussi un morphisme de groupes car R_θ est la matrice de la multiplication par $e^{i\theta}$ dans la base $1, i$ de $\mathbf{C}$ sur $\mathbf{R}$, et $\theta \mapsto e^{i\theta}$ est un morphisme de groupes.

• Si $\mathrm{P} \in \mathbf{O}(2) - \mathbf{SO}(2)$, alors P est la matrice d'une symétrie orthogonale.

Les deux racines du polynôme caractéristique de P sont réelles car $\det \mathrm{P} = -1$, et comme elles sont de module 1 et quel leur produit est égal à -1, ce sont 1 et -1. D'où le résultat.

• Si $\mathrm{P} \in \mathbf{SO}(n)$, il existe $\mathrm{Q} \in \mathbf{O}(n)$, et $\theta_1, \dots, \theta_m \in \mathbf{R}/2\pi\mathbf{Z}$, avec $m = \left[\frac{n}{2}\right]$, uniquement déterminés à l'ordre et au signe près, tels que QPQ^{-1} soit la matrice diagonale par blocs $\mathrm{Diag}\big(\mathrm{R}_{\theta_1}, \dots, \mathrm{R}_{\theta_m}\big)$ ou $\mathrm{Diag}\big(1, \mathrm{R}_{\theta_1}, \dots, \mathrm{R}_{\theta_m}\big)$ suivant que n est pair ou impair.

Soient $\lambda_1, \dots, \lambda_r, \mu_1, \overline{\mu}_1, \dots, \mu_s, \overline{\mu}_s$ les valeurs propres de P, répétées avec multiplicité, où les λ_i sont réelles et les μ_i ne le sont pas. Comme P est unitaire, on a $\lambda_i = \pm 1$ et $\mu_j\overline{\mu}_j = 1$, et comme $\det \mathrm{P} = 1$, il y a un nombre pair de λ_i égaux à -1.

La démonstration de l'existence de Q se fait par récurrence sur n. Si $n=1$ le résultat est trivial, et si $n=2$, il est inclus dans un point précédent. Il y a deux cas :

• 1 est valeur propre de u_{P} : si f_1 est un vecteur de norme 1 fixe par u_{P}, l'hyperplan W orthogonal à f_1 est stable par u_{P}. Il s'ensuit que si $f_2, \dots, f_n$ est une base orthonormée de W, et si Q_0 est la matrice de colonnes $f_1, \dots, f_n$, alors $\mathrm{Q}_0 \in \mathbf{O}(n)$ et $\mathrm{Q}_0^{-1}\mathrm{PQ}_0$ est de la forme $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mathrm{P}_1 \end{smallmatrix}\right)$, avec $\mathrm{P}_1 \in \mathbf{SO}(n-1)$. On peut alors appliquer l'hypothèse de récurrence à P_1 et trouver $\mathrm{Q}_1 \in \mathbf{O}(n-1)$ telle que $\mathrm{Q}_1\mathrm{P}_1\mathrm{Q}_i^{-1}$ soit diagonale par blocs de rotations. Si $\mathrm{Q}_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \mathrm{Q}_1 \end{smallmatrix}\right)$, alors $\mathrm{Q}_2 \in \mathbf{O}(n)$ et $\mathrm{Q}_2\mathrm{Q}_0^{-1}\mathrm{PQ}_0\mathrm{Q}_2^{-1}$ est de la forme voulue (si n est pair, les deux 1 se combinent pour former la matrice de la rotation d'angle 0). On peut donc prendre $\mathrm{Q} = \mathrm{Q}_2\mathrm{Q}_0^{-1}$.

• 1 n'est pas valeur propre de u_{P}, auquel cas u_{P} laisse fixe un plan de $\mathbf{C}^n$ (éventuellement inclus dans l'espace propre associé à -1), et la restriction de u_{P} à ce plan est une rotation puisqu'elle est unitaire et n'admet pas 1 comme valeur propre. L'orthogonal de ce plan est stable par u_{P}, et on peut appliquer l'hypothèse de récurrence à la matrice de la restriction de u_{P} dans une base orthonormée. On en déduit, comme ci-dessus l'existence de Q.

L'unicité, à l'ordre et au signe près, des θ_j vient de ce que les valeurs propres de R_θ sont $e^{i\theta}$ et $e^{-i\theta}$, et donc que les $e^{\pm i\theta_j}$ (auquel il faut ajouter 1 si n est impair) sont les valeurs propres de P, répétées avec multiplicité.

Exercice 18.6. — Montrer que $\mathbf{SO}(n)$ est connexe par arcs. Qu'en est-il de $\mathbf{O}(n)$?

18.3.3. *Décomposition d'Iwasawa d'une matrice*

• On peut écrire tout $A \in \mathbf{GL}_n(\mathbf{C})$ (resp. tout $A \in \mathbf{GL}_n(\mathbf{R})$), de manière unique, sous la forme [116] $A = PM$, où $M \in \mathbf{GL}_n(\mathbf{C})$ (resp. $M \in \mathbf{GL}_n(\mathbf{R})$) est triangulaire supérieure avec des coefficients diagonaux réels > 0, et P est unitaire (resp. orthogonale).

Soient $v_1, \ldots, v_n \in \mathbf{K}^n$ les colonnes de A. Comme A est inversible, $v_1, \ldots, v_n$ est une base de $\mathbf{K}^n$, et le procédé d'orthonormalisation de Schmidt nous fournit une base orthonormale $f_1 = b_{1,1}v_1$, $f_2 = b_{2,2}v_2 + b_{1,2}v_1$, …, $f_n = b_{n,n}v_n + b_{1,n}v_1 + \cdots + b_{n-1,n}v_{n-1}$, avec $b_{i,i}$ réel > 0 (on a $b_{i,i} = \frac{1}{\|v_i - p_{i-1}(v_i)\|}$, où p_{i-1} est la projection orthogonale sur le sous-espace engendré par $v_1, \ldots, v_{i-1}$). Si on note P la matrice dont les colonnes sont les f_j, et M la matrice triangulaire supérieure dont les coefficients sur la diagonale ou au-dessus sont les $b_{i,j}$, les relations ci-dessus se traduisent par $AM = P$. Or P est unitaire (resp. orthogonale) et M^{-1} est triangulaire supérieure, et $A = PM^{-1}$ est une écriture de A sous la forme voulue.

Maintenant, si $P_1M_1 = P_2M_2$, avec P_1, P_2 unitaires, et M_1, M_2 triangulaires supérieures avec des coefficients diagonaux > 0, alors $B = P_2^{-1}P_1 = M_2M_1^{-1}$ est à la fois unitaire et triangulaire supérieure avec des coefficients diagonaux > 0. Il s'ensuit que ses valeurs propres sont à la fois de module 1 et réelles > 0 ; elles sont donc toutes égales à 1, et comme $B = P_2^{-1}P_1$ est diagonalisable car unitaire, cela implique que $B = 1$ et donc que $P_1 = P_2$ et $M_1 = M_2$. D'où l'unicité, ce qui permet de conclure.

Exercice 18.7. — (i) Montrer que $\mathbf{GL}_n(\mathbf{C})$ et $\mathbf{SL}_n(\mathbf{C})$ sont connexes par arcs.
(ii) Montrer que $\mathbf{SL}_n(\mathbf{R})$ est connexe par arcs. Qu'en est-il de $\mathbf{GL}_n(\mathbf{R})$

Exercice 18.8. — (i) Montrer que $\mathbf{U}(n)$ est un sous-groupe compact de $\mathbf{GL}_n(\mathbf{C})$
(ii) Soit M une matrice triangulaire supérieure avec des 1 sur la diagonale. Montrer que $(M-1)^n = 1$; en déduire que M^m est un polynôme en m, et que la suite des M^k est bornée si et seulement si $M = 1$.
(iii) Montrer que $\mathbf{U}(n)$ est un sous-groupe compact maximal de $\mathbf{GL}_n(\mathbf{C})$: si H est un sous-groupe compact de $\mathbf{GL}_n(\mathbf{C})$ qui contient $\mathbf{U}(n)$, alors $H = \mathbf{U}(n)$.

18.4. Opérateur autoadjoint, matrice hermitienne

18.4.1. *Réduction des opérateurs autodajoint*

Soit $u \in \mathrm{End}(E)$ un opérateur sur E. Si $\langle u(x), y\rangle = \langle x, u(y)\rangle$ pour tous $x, y \in E$, on dit que u est *hermitien* ou *autoadjoint*.

• Si $u : E \to E$ est autoadjoint, et si F est un sous-espace de E stable par u, alors $F^\perp$ est stable par u.

Soit $x \in F^\perp$. Alors $\langle x, u(y)\rangle = 0$, pour tout $y \in F$, puisque $u(F) \subset F$. Comme u est autoadjoint, on en déduit que $\langle u(x), y\rangle = \langle x, u(y)\rangle = 0$ pour tout $y \in F$, et donc que $u(x) \in F^\perp$.

• Si $u : E \to E$ est autoadjoint, les valeurs propres de u (de $u_{\mathbf{C}}$ si E est réel) sont réelles.

116. On peut écrire M sous la forme DN ou D est diagonale à coefficients diagonaux > 0, et N est triangulaire supérieure avec des 1 sur la diagonale, et donc est unipotente, ce qui nous fournit la décomposition $A = PDN$. Une telle décomposition existe dans un cadre nettement plus général ; elle est connue sous le nom de décomposition d'Iwasawa.

Commençons par traiter le cas $\mathbf{K} = \mathbf{C}$. Si $x \neq 0$ est un vecteur propre de u pour la valeur propre λ, la relation $\langle x, u(x)\rangle = \langle u(x), x\rangle$ devient $\langle x, \lambda x\rangle = \langle \lambda x, x\rangle$, et donc $\lambda\|x\|^2 = \overline{\lambda}\|x\|^2$. Il en résulte que λ est réel.

Si $\mathbf{K} = \mathbf{R}$, on peut étendre u en un endomorphisme $u_{\mathbf{C}}$ du complexifié $\mathrm{E}_{\mathbf{C}} = \mathrm{E} \oplus i\mathrm{E}$ de E qui est un espace préhilbertien complexe. En utilisant successivement la définition de $u_{\mathbf{C}}$, celle de $\langle\ ,\ \rangle_{\mathbf{C}}$, le fait que u est autoadjoint, la définition de $\langle\ ,\ \rangle_{\mathbf{C}}$, et enfin celle de $u_{\mathbf{C}}$, on obtient, si $z = x + iy$ et $z' = x' + iy'$ sont des éléments de $\mathrm{E}_{\mathbf{C}}$:

$$\langle u_{\mathbf{C}}(z'), z\rangle_{\mathbf{C}} = \langle u(x') + iu(y'), x + iy\rangle_{\mathbf{C}} = \langle u(x'), x\rangle - i\langle u(y'), x\rangle + i\langle u(x'), y\rangle + \langle u(y'), y\rangle$$
$$= \langle x', u(x)\rangle - i\langle y', u(x)\rangle + i\langle x', u(y)\rangle + \langle y', u(y)\rangle = \langle x' + iy', u(x) + iu(y)\rangle_{\mathbf{C}} = \langle z', u_{\mathbf{C}}(z)\rangle_{\mathbf{C}},$$

et donc $u_{\mathbf{C}}$ est autoadjoint, et ses valeurs propres sont réelles d'après ce qui précède.

• Une homothétie est hermitienne si et seulement si son rapport est réel ; une projection est hermitienne si et seulement si c'est une projection orthogonale (i.e. si noyau et image sont orthogonaux, ce qui est le cas de la projection orthogonale sur un sous-espace de dimension finie), et une symétrie est hermitienne si et seulement si elle est orthogonale.

Dans un sens, cela résulte des deux points précédents ; dans l'autre, c'est presque immédiat.

• Si E est de dimension finie et si $u : \mathrm{E} \to \mathrm{E}$ est autoadjoint, alors u se diagonalise dans une base orthonormée.

Prouvons le résultat par récurrence sur $n = \dim \mathrm{E}$. Si $n = 1$, le résultat est immédiat. Si $n \geqslant 2$, alors u a au moins une valeur propre λ_1 (c'est clair si E est complexe, puisqu'on est en dimension finie ; si E est réel, alors $u_{\mathbf{C}}$ a une valeur propre, qui est réelle d'après la démonstration du point précédent, et donc u admet une valeur propre (alinéa 10.5.1)). Soit e_1 un vecteur propre associé vérifiant $\|e_1\| = 1$, et soit F l'orthogonal de $\mathbf{C}e_1$. Alors F est stable par u puisque $\mathbf{C}e_1$ l'est, et on peut donc lui appliquer l'hypothèse de récurrence : il existe une base orthonormée $e_2, \ldots, e_n$ de F formée de vecteurs propres pour u. Alors $e_1, \ldots, e_n$ est une base orthonormée de E formée de vecteurs propres pour u, ce qui prouve que u se diagonalise dans une base orthonormée.

18.4.2. *Réduction des matrices et des formes hermitiennes*

$\mathrm{A} = (a_{i,j}) \in \mathbf{M}_n(\mathbf{C})$ est dite *hermitienne* si $\mathrm{A} = {}^{\mathrm{t}}\overline{\mathrm{A}}$, ce qui se traduit par $a_{i,j} = \overline{a_{j,i}}$, pour tous i, j. On dit aussi que A est *autoadjointe* si A est hermitienne (la matrice $\mathrm{A}^* = {}^{\mathrm{t}}\overline{\mathrm{A}}$ est l'adjointe de A). Notons que si $\mathrm{A} \in \mathbf{M}_n(\mathbf{R})$, alors A est hermitienne si et seulement si elle est symétrique (i.e. ${}^{\mathrm{t}}\mathrm{A} = \mathrm{A}$).

• Si $\mathrm{A} \in \mathbf{M}_n(\mathbf{C})$ est hermitienne, et si $\mathrm{M} \in \mathbf{M}_n(\mathbf{C})$, alors ${}^{\mathrm{t}}\overline{\mathrm{M}}\mathrm{AM}$ est hermitienne ; en particulier, ${}^{\mathrm{t}}\overline{\mathrm{M}}\mathrm{M}$ est hermitienne [117] pour tout $\mathrm{M} \in \mathbf{M}_n(\mathbf{C})$.

Si $\mathrm{B} = {}^{\mathrm{t}}\overline{\mathrm{M}}\mathrm{AM}$, alors ${}^{\mathrm{t}}\mathrm{B} = {}^{\mathrm{t}}\mathrm{M}\,{}^{\mathrm{t}}\mathrm{A}\overline{\mathrm{M}}$ et ${}^{\mathrm{t}}\overline{\mathrm{B}} = {}^{\mathrm{t}}\overline{\mathrm{M}}\,{}^{\mathrm{t}}\overline{\mathrm{A}}\mathrm{M} = \mathrm{B}$, puisque ${}^{\mathrm{t}}\overline{\mathrm{A}} = \mathrm{A}$.

• Si $\mathrm{A} \in \mathbf{M}_n(\mathbf{K})$ est hermitienne, alors $u_{\mathrm{A}} : \mathbf{K}^n \to \mathbf{K}^n$ est hermitien. Réciproquement, la matrice d'un opérateur hermitien u dans une base orthonormée est hermitienne.

117. Un calcul immédiat montre que ${}^{\mathrm{t}}\overline{\mathrm{M}}\mathrm{M}$ est la matrice de Gram des colonnes de M.

$u_{\mathrm{A}}(\mathrm{X}) = \mathrm{AX}$, et donc $\langle \mathrm{X}, u_{\mathrm{A}}(\mathrm{Y})\rangle = {}^{\mathrm{t}}\overline{\mathrm{X}}\mathrm{AY}$. Comme une matrice 1×1 est égale à sa transposée, $\langle \mathrm{X}, u_{\mathrm{A}}(\mathrm{Y})\rangle = {}^{\mathrm{t}}\mathrm{Y}{}^{\mathrm{t}}\mathrm{A}\overline{\mathrm{X}}$ et donc $\langle u_{\mathrm{A}}(\mathrm{Y}), \mathrm{X}\rangle = \overline{\langle \mathrm{X}, u_{\mathrm{A}}(\mathrm{Y})\rangle} = {}^{\mathrm{t}}\overline{\mathrm{Y}}{}^{\mathrm{t}}\overline{\mathrm{A}}\mathrm{X} = {}^{\mathrm{t}}\overline{\mathrm{Y}}\mathrm{AX} = \langle \mathrm{Y}, u_{\mathrm{A}}(\mathrm{X})\rangle$, ce qui prouve que u_{A} est hermitien.

Réciproquement, si u est un endomorphisme de E, sa matrice $\mathrm{A} = (a_{i,j})$ dans une base $e_1, \dots, e_n$ a pour colonnes les coordonnées de $u(e_j)$ dans la base $e_1, \dots, e_n$. Si la base est orthonormée, ces coordonnés sont les $\langle e_i, u(e_j)\rangle$, et donc $a_{i,j} = \langle e_i, u(e_j)\rangle$. Si u est hermitien, cela implique que $a_{i,j} = \langle u(e_i), e_j\rangle = \overline{\langle e_j, u(e_i)\rangle} = \overline{a_{j,i}}$, et donc A est hermitienne.

• Si $\mathrm{A} \in \mathbf{M}(\mathbf{C})$ (resp. $\mathrm{A} \in \mathbf{M}(\mathbf{R})$) est hermitienne (resp. symétrique), il existe $\mathrm{P} \in \mathbf{U}(n)$ (resp. $\mathbf{O}(n)$) et D diagonale à coefficients réels, telles que $\mathrm{A} = \mathrm{PDP}^{-1} = \mathrm{PD}{}^{\mathrm{t}}\overline{\mathrm{P}}$.

C'est une traduction du fait que $u_{\mathrm{A}} : \mathbf{C}^n \to \mathbf{C}^n$ a toutes ses valeurs propres réelles et se diagonalise dans une base orthonormée puisqu'il est hermitien.

Soit V un espace de dimension finie sur $\mathbf{C}$ ou sur $\mathbf{R}$. On dit que $(x, y) \mapsto \mathrm{H}(x, y)$ est une *forme hermitienne* sur V si elle est sesquilinéaire et symétrique (un produit scalaire est une forme hermitienne définie positive ; si V est réel, une forme hermitienne est une forme bilinéaire symétrique).

◇ Si $\mathbf{e} = (e_1, \dots, e_n)$ est une base de V, la *matrice de* H *dans la base* $\mathbf{e}$ est celle des $\mathrm{H}(e_i, e_j)$; c'est une matrice hermitienne par symétrie de H ; on la note ${}^{\mathrm{t}}\overline{\mathbf{e}}\mathrm{H}\mathbf{e}$.

◇ La sesquilinéarité de H fait que $\mathrm{H}(x, y) = {}^{\mathrm{t}}(\overline{\mathbf{e}\backslash x})({}^{\mathrm{t}}\overline{\mathbf{e}}\mathrm{H}\mathbf{e})(\mathbf{e}\backslash y)$, si $x, y \in \mathrm{V}$.

◇ Si $\mathbf{f} = (f_1, \dots, f_n)$ est une autre base de V, on a ${}^{\mathrm{t}}\overline{\mathbf{e}}\mathrm{H}\mathbf{e} = {}^{\mathrm{t}}(\overline{\mathbf{e}\backslash\mathbf{f}})({}^{\mathrm{t}}\overline{\mathbf{e}}\mathrm{H}\mathbf{e})(\mathbf{e}\backslash\mathbf{f})$, où $\mathbf{e}\backslash\mathbf{f}$ est, comme d'habitude, la matrice dont les colonnes sont les f_j dans la base $\mathbf{e}$.

• Si V est préhilbertien, et si H est une forme hermitienne sur V, il existe une base orthonormée $\mathbf{e}$ de V dans laquelle la matrice de H est diagonale à coefficients réels.

Si H est une forme hermitienne sur $\mathbf{C}^n$ (resp. $\mathbf{R}^n$), il existe une matrice $\mathrm{P} = (p_{i,j})$ unitaire (resp. orthogonale), et $d_1, \dots, d_n \in \mathbf{R}$, tels que $\mathrm{H}(x, y) = \sum_{i=1}^n d_i \overline{\mathrm{L}_i(x)}\mathrm{L}_i(y)$, avec $\mathrm{L}_i({}^{\mathrm{t}}(z_1, \dots, z_n)) = \sum_{j=1}^n p_{i,j} z_j$.

Soit $\mathbf{f}$ une base orthonormée de V. La matrice A de H dans cette base est hermitienne, et il existe donc $\mathrm{P} \in \mathbf{U}(n)$ telle que $\mathrm{A} = \mathrm{PDP}^{-1}$ où D est diagonale à coefficients réels. Les vecteurs dont les coordonnés dans la base $\mathbf{f}$ sont les colonnes de P forment une base orthonormée $\mathbf{e}$ de V, et la matrice de H dans cette base est ${}^{\mathrm{t}}\overline{\mathrm{P}}\mathrm{AP}$, et comme ${}^{\mathrm{t}}\overline{\mathrm{P}} = \mathrm{P}^{-1}$, cette matrice n'est autre que D, ce qui prouve le premier énoncé.

Pour le second, on part de la matrice A de H dans la base canonique. Cette matrice est hermitienne et il existe Q unitaire (resp. orthogonale), et $d_1, \dots, d_n \in \mathbf{R}$, tels que $\mathrm{A} = \mathrm{Q}\,\mathrm{Diag}(d_1, \dots, d_n){}^{\mathrm{t}}\overline{\mathrm{Q}}$. Alors $\mathrm{P} = (p_{i,j}) = {}^{\mathrm{t}}\overline{\mathrm{Q}}$ est encore unitaire (resp. orthogonale), et on a $\mathrm{H}(\mathrm{X}, \mathrm{Y}) = {}^{\mathrm{t}}\overline{\mathrm{X}}\mathrm{AY} = {}^{\mathrm{t}}\overline{\mathrm{X}}{}^{\mathrm{t}}\overline{\mathrm{P}}\mathrm{Diag}(d_1, \dots, d_n)\mathrm{PY} = \sum_{i=1}^n d_i \overline{\mathrm{L}_i(x)}\mathrm{L}_i(y)$, où L_i est la forme linéaire $\mathrm{L}_i({}^{\mathrm{t}}(z_1, \dots, z_n)) = \sum_{j=1}^n p_{i,j} z_j$.

18.4.3. *Décomposition polaire d'une matrice*

• Si $\mathrm{A} \in \mathbf{M}_n(\mathbf{K})$, alors $(\mathrm{X}, \mathrm{Y}) \mapsto {}^{\mathrm{t}}\overline{\mathrm{X}}\mathrm{AY}$ est sesquilinéaire sur $\mathbf{K}^n$, hermitienne si et seulement si A est hermitienne, et de plus définie positive si et seulement si les valeurs propres de A sont > 0.

La sesquilinéarité est immédiate. La symétrie équivaut à ${}^{\mathrm{t}}\overline{\mathrm{Y}}\mathrm{AX} = {}^{\mathrm{t}}\mathrm{X}\overline{\mathrm{AY}}$, et donc à ${}^{\mathrm{t}}\overline{\mathrm{Y}}\mathrm{AX} = {}^{\mathrm{t}}\overline{\mathrm{Y}}{}^{\mathrm{t}}\overline{\mathrm{A}}\mathrm{X}$ (car une matrice 1×1 est sa propre transposée), pour tous X, Y, et donc aussi à $\mathrm{A} = {}^{\mathrm{t}}\overline{\mathrm{A}}$

(dans un sens c'est clair, dans l'autre on utilise le fait que le coefficient $b_{i,j}$ d'une matrice $B = (b_{i,j}) \in \mathbf{M}_n(\mathbf{K})$ est égal à ${}^t\overline{e}_i B e_j$).

Maintenant, si A est hermitienne, on peut l'écrire sous la forme $PD{}^t\overline{P}$, où P est unitaire et D est diagonale à coefficients diagonaux $d_1, \dots, d_n$ réels (les d_i sont alors les valeurs propres de A, car ${}^t\overline{P} = P^{-1}$). Si $X \in \mathbf{K}^n$, soit $X' = {}^t\overline{P}X = {}^t(x'_1, \dots, x'_n)$. Alors $X \mapsto X'$ est un isomorphisme de $\mathbf{K}^n$ sur $\mathbf{K}^n$, puisque ${}^t\overline{P}$ est inversible, et on a ${}^t\overline{X}AX = \sum_{i=1}^n d_i |x'_i|^2$. Il s'ensuit que ${}^t\overline{X}AX > 0$ pour tout $X \neq 0$ équivaut à ce que les d_i soient > 0. D'où le résultat.

Une matrice hermitienne $A \in \mathbf{M}_n(\mathbf{C})$ (resp. symétrique $A \in \mathbf{M}_n(\mathbf{R})$) est *définie positive* si $(X, Y) \mapsto {}^t\overline{X}AY$ est un produit scalaire sur $\mathbf{K}^n$. D'après le point précédent, c'est le cas si et seulement si les valeurs propres de A sont > 0.

• Si $A \in \mathbf{GL}_n(\mathbf{C})$, alors ${}^t\overline{A}\,A$ est une matrice hermitienne définie positive.

On a déjà démontré que $B = {}^t\overline{A}\,A$ est hermitienne. Maintenant, ${}^t\overline{X}BX = \langle AX, AX\rangle$, et comme le noyau de $X \mapsto AX$ est trivial puisque A est inversible, cela implique que ${}^t\overline{X}BX > 0$, si $X \neq 0$, et donc que B est définie positive.

• On peut écrire tout $A \in \mathbf{GL}_n(\mathbf{C})$ (resp. $A \in \mathbf{GL}_n(\mathbf{R})$), de manière unique, sous la forme PS, où P est unitaire (resp. orthogonale), et S est hermitienne (resp. symétrique) et définie positive.

Le cas réel se déduit du cas complexe en utilisant l'unicité de l'écriture et l'observation selon laquelle $A = \overline{P}\,\overline{S}$ est aussi une écriture si A est réelle et si $A = PS$ en est une.

Si $A = PS$, alors ${}^t\overline{A}\,A = {}^t\overline{S}{}^t\overline{P}\,PS = S^2$, car ${}^t\overline{P}\,P = 1$ et ${}^t\overline{S} = S$. Donc S est une solution de l'équation $S^2 = {}^t\overline{A}\,A$. Réciproquement, si S est une matrice hermitienne, définie positive, solution de cette équation, alors $P = AS^{-1}$ vérifie ${}^t\overline{P}\,P = {}^t\overline{S}^{-1}{}^t\overline{A}\,AS^{-1} = S^{-1}{}^t\overline{A}\,AS^{-1} = S^{-1}({}^t\overline{A}\,AS^{-2})S = S^{-1}S = 1$, ce qui prouve que P est unitaire et que $A = PS$ est une écriture de A sous la forme voulue. On est donc ramené à prouver que l'équation $S^2 = B$ a une et une seule solution dans les matrices hermitiennes définies positives, si B est hermitienne et définie positive.

◇ Pour prouver l'existence, on met B sous la forme QDQ^{-1}, avec Q unitaire et D diagonale à coefficients diagonaux $d_1, \dots, d_n > 0$. Soit $\sqrt{D}$ la matrice diagonale dont les coefficients diagonaux sont $\sqrt{d_1}, \dots, \sqrt{d_n}$. Alors $S = Q\sqrt{D}Q^{-1}$ vérifie $S^2 = B$. Par ailleurs, on a aussi $S = Q\sqrt{D}{}^t\overline{Q}$, ce qui prouve que S est hermitienne, et définie positive puisque ses valeurs propres $\sqrt{d_1}, \dots, \sqrt{d_n}$ sont > 0.

◇ Maintenant supposons que $S^2 = B$, où S est définie positive. Les valeurs propres $\lambda_1, \dots, \lambda_r$ de S sont donc > 0, et $\mathbf{K}^n = V_1 \oplus \cdots \oplus V_r$, où V_i et l'espace propre de u_S associé à la valeur propre λ_i. Par ailleurs V_i est inclus dans l'espace propre W_i de u_B pour la valeur propre λ_i^2, et comme les λ_i^2 sont distincts deux à deux puisque les λ_i sont > 0, cela prouve que $V_i = W_i$ (car $n \geqslant \sum_i \dim W_i \geqslant \sum_i \dim V_i = n$, et donc $\dim W_i = \dim V_i$, pour tout i). On en déduit l'unicité de S (en effet, u_S doit être l'homothétie de rapport $\sqrt{d_i}$ sur l'espace propre de u_B pour la valeur propre d_i).

Ceci permet de conclure.

Exercice 18.9. — (i) Montrer que $(f, g) \mapsto \langle f, g\rangle \int_0^1 \overline{f}(t)g(t)\,dt$ est un produit scalaire sur l'espace $\mathscr{C}^\infty(\mathbf{R}/\mathbf{Z})$ des fonctions $\mathscr{C}^\infty$ sur $\mathbf{R}$, périodiques de période 1.

(ii) Montrer que le *laplacien* $\Delta = -\frac{d^2}{dt^2}$ est autoadjoint ; quelles sont ses valeurs propres ?

(iii) L'opérateur Δ est-il continu sur $\mathscr{C}^\infty$ muni de la norme définie par le produit scalaire ?

Exercice 18.10. — (Polynômes orthogonaux).

Soit $\phi : [0,1] \to \mathbf{R}_+^*$ continue, et soit $\langle\ ,\ \rangle$ le produit scalaire défini par $\langle \mathrm{P}, \mathrm{Q}\rangle = \int_0^1 \mathrm{P}(t)\mathrm{Q}(t)\,\phi(t)dt$, si $\mathrm{P}, \mathrm{Q} \in \mathbf{R}[\mathrm{X}]$. On note $(\mathrm{P}_n)_{n\in\mathbf{N}}$ la base orthonormée de $\mathbf{R}[\mathrm{X}]$ obtenue par le procédé d'orthonormalisation de Schmidt à partir de la base canonique $1, \mathrm{X}, \mathrm{X}^2, \ldots$ de $\mathbf{R}[\mathrm{X}]$.

(i) Montrer que P_n est de degré n, de coefficient dominant $p_n > 0$.

(ii) Montrer que P_n a n racines distinctes dans $]0,1[$.

(iii) Montrer que $\mathrm{P} \mapsto \mathrm{RP}$ est autoadjoint si $\mathrm{R} \in \mathbf{R}[\mathrm{X}]$.

(iv) Calculer $\langle \mathrm{P}_n, \mathrm{XP}_{n-1}\rangle$ en fonction des p_i.

(v) Montrer qu'il existe $a_n, b_n, c_n \in \mathbf{R}$, avec $a_n, c_n > 0$, tels que $\mathrm{P}_n - (a_n\mathrm{X} + b_n)\mathrm{P}_{n-1} + c_n\mathrm{P}_{n-2} = 0$, si $n \geqslant 2$. (On pourra faire le produit scalaire avec $\mathrm{Q} \in \mathbf{R}[\mathrm{X}]^{(n-3)}$ bien choisi.)

(vi) Montrer que les racines de P_n et de P_{n-1} sont entrelacées : si $x_{m,1} < x_{m,2} < \cdots < x_{m,m}$ sont celles de P_m, alors $x_{n,1} < x_{n-1,1} < x_{n,2} < \cdots < x_{n-1,n-1} < x_{n,n}$. (On s'intéressera au signe de $\mathrm{P}_n(x_{n-1,i})$.)

19. Tératologie

Ce § rassemble un certain nombre de monstres mathématiques.

19.1. Fonctions continues dérivables nulle part

Jusqu'au début du XIX$^{\mathrm{e}}$ siècle (au moins), il était évident pour tout le monde qu'une fonction continue de $\mathbf{R}$ dans $\mathbf{R}$ était dérivable, et même somme de sa série de Taylor, sauf en des points isolés. C'est malheureusement loin d'être le cas puisque Weierstrass (1875) a construit une fonction continue dérivable nulle part, et Banach a montré que l'ensemble de ces fonctions était dense dans celui des fonctions continues.

Soit $\mathrm{E} = \mathscr{C}^0([0,1], \|\ \|_\infty)$. Nous nous proposons de construire un sous-ensemble X, dense dans E, constitué de fonctions dérivables nulle part. Pour ce faire, fixons $a \in]\frac{1}{2}, 1[$. Si $n \in \mathbf{N}$, et si $k \in \{0, 1, \ldots, 2^n - 1\}$, soit

$$\mathrm{U}_{n,k} = \big\{\phi \in \mathrm{E},\ \big|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)\big| > a^n\big\}.$$

• $\mathrm{U}_{n,k}$ est un ouvert de E : en effet $\phi \mapsto \big|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)\big|$ est continue sur E comme composée de l'application linéaire continue $\phi \mapsto \Lambda_{n,k}(\phi) = \phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)$ (la continuité de $\Lambda_{n,k}$ résulte de la majoration $|\Lambda_{n,k}(\phi)| \leqslant 2\|\phi\|_\infty$), et de la valeur absolue.

On en déduit que $\mathrm{U}_n = \cap_{k=0}^{2^n-1}\mathrm{U}_{n,k}$ et $\mathrm{V}_n = \cup_{m\geqslant n}\mathrm{U}_m$ sont des ouverts de E.

• V_n est dense dans E. En effet, soit $\phi \in \mathrm{E}$, et soit $\varepsilon > 0$. Comme $[0,1]$ est compact, ϕ est uniformément continue, et il existe $n_0 \in \mathbf{N}$ tel que $|\phi\big(\frac{k+1}{2^n}\big) - \phi\big(\frac{k}{2^n}\big)\big| \leqslant \varepsilon$, quels que soient $n \geqslant n_0$ et $k \in \{0, 1, \ldots, 2^n - 1\}$. Soit $m \geqslant \sup(n_0, n)$ tel que $a^m < \varepsilon$, et soit $\psi \in \mathrm{E}$ définie par $\psi(x) = \phi(x) + \varepsilon\sin(2^m\pi x)$. Si $k \in \{0, 1, \ldots, 2^m - 1\}$, on a $\|\psi - \phi\|_\infty \leqslant \varepsilon$ et

$$\big|\psi\big(\frac{k+1}{2^m}\big) - \psi\big(\frac{k}{2^m}\big)\big| = \big|\pm 2\varepsilon + \phi\big(\frac{k+1}{2^m}\big) - \phi\big(\frac{k}{2^m}\big)\big| \geqslant 2\varepsilon - \varepsilon > a^m,$$

ce qui prouve que $\psi \in \mathrm{U}_m \subset \mathrm{V}_n$. On en déduit que, pour tout $\phi \in \mathrm{E}$, on peut trouver un élément de V_n dans tout voisinage de ϕ, et donc que V_n est effectivement dense dans E.

Comme E est complet, il résulte du lemme de Baire que $\mathrm{X} = \cap_{n\in\mathbf{N}} \mathrm{V}_n$ est dense dans E, et pour conclure, il suffit donc de prouver que, si $\phi \in \mathrm{X}$, et si $x_0 \in [0,1]$, alors ϕ n'est pas dérivable en x_0. Pour cela, remarquons que $\phi \in \mathrm{X}$ signifie que ϕ appartient à une infinité de U_n, et donc qu'il existe $b : \mathbf{N} \to \mathbf{N}$, tendant vers $+\infty$ en $+\infty$, telle que $|\phi\big(\frac{k+1}{2^{b(n)}}\big) - \phi\big(\frac{k}{2^{b(n)}}\big)| > a^{b(n)}$, pour tout $n \in \mathbf{N}$ et tout $k \in \{0, 1, \dots, 2^{b(n)} - 1\}$. Soient k_n la partie entière de $2^{b(n)}x_0$, et $u_n = \frac{k_n}{2^{b(n)}}$, $v_n = \frac{k_n+1}{2^{b(n)}}$ (si $x_0 = 1$, on pose $u_n = 1 - \frac{1}{2^{b(n)}}$ et $v_n = 1$). Par construction, $u_n \leqslant x_0 \leqslant v_n$ et $v_n - u_n = \frac{1}{2^{b(n)}}$; en particulier, $u_n \to x_0$ et $v_n \to x_0$. Par ailleurs, pour tout $n \in \mathbf{N}$, on a $\big|\frac{\phi(v_n)-\phi(u_n)}{v_n-u_n}\big| > (2a)^{b(n)}$, et comme $2a > 1$, cela montre que $\big|\frac{\phi(v_n)-\phi(u_n)}{v_n-u_n}\big|$ tend vers $+\infty$, et donc que ϕ n'est pas dérivable en x_0 (si elle l'était, on aurait $\frac{\phi(v_n)-\phi(u_n)}{v_n-u_n} \to \phi'(x_0)$). Ceci permet de conclure.

Exercice 19.1. — Adapter la dernière partie de l'argument pour montrer que $\sum_{n\geqslant 1} \frac{\sin(10^n \pi x)}{2^n}$ est continue sur $\mathbf{R}$, mais n'est dérivable nulle part.

19.2. L'escalier du diable

Il s'agit d'une fonction $f : [0,1] \to \mathbf{R}$, continue, croissante, valant 0 en 0 et 1 en 1, mais qui croît subrepticement : il existe une famille de segments ouverts $]a_n, b_n[$ disjoints, pour $n \in \mathbf{N}$, tels que f soit constante sur chacun des segments $]a_n, b_n[$, et tels que la somme totale $\sum_{n\in\mathbf{N}}(b_n - a_n)$ des longueurs des segments soit égale à 1. La fonction f représente un contrexemple assez frappant à une extension naturelle du théorème fondamental de l'analyse $[\int_a^b f'(t)\,dt = f(b) - f(a)]$.

On construit f, par un procédé fractal, comme la limite de $f_n : [0,1] \to [0,1]$, continues, croissantes, affines sur chaque intervalle $\mathrm{I}_{n,i} = [\frac{i}{3^n}, \frac{i+1}{3^n}]$, pour $0 \leqslant i \leqslant 3^n - 1$, construites par récurrence à partir de $f_0(x) = x$ en utilisant la recette suivante : l'image de $\mathrm{I}_{n,i}$ par f_{n+1} est la même que par f_n, mais le graphe de f_{n+1} sur cet intervalle est obtenu en coupant en trois le segment constituant le graphe de f_n, et en introduisant un palier horizontal au milieu.

De manière plus précise, si on note $a_{n,i}$ et $b_{n,i}$ les valeurs de f_n en $\frac{i}{3^n}$ et $\frac{i+1}{3^n}$, alors les fonctions f_n et f_{n+1} sont données par les formules suivantes sur $\mathrm{I}_{n,i}$:

$$f_n(x) = a_{n,i} + (b_{n,i} - a_{n,i})(3^n x - i)$$

$$f_{n+1}(x) = \begin{cases} a_{n,i} + \frac{3}{2}(b_{n,i} - a_{n,i})(3^n x - i) & \text{si } x \in \mathrm{I}_{n+1,3i}, \\ \frac{b_{n,i}+a_{n,i}}{2} & \text{si } x \in \mathrm{I}_{n+1,3i+1}, \\ b_{n,i} + \frac{3}{2}(b_{n,i} - a_{n,i})(3^n x - i - 1) & \text{si } x \in \mathrm{I}_{n+1,3i+2}. \end{cases}$$

En particulier, si f_n est constante sur $\mathrm{I}_{n,i}$, alors $f_{n+1} = f_n$ sur $\mathrm{I}_{n,i}$, et dans le cas général, on a

$$b_{n+1,i} - a_{n+1,i} = \begin{cases} \frac{b_{n,i}-a_{n,i}}{2} & \text{si le chiffre des unités dans l'écriture de } i \text{ en base 3 est 0 ou 2,} \\ 0 & \text{si le chiffre des unités dans l'écriture de } i \text{ en base 3 est un 1.} \end{cases}$$

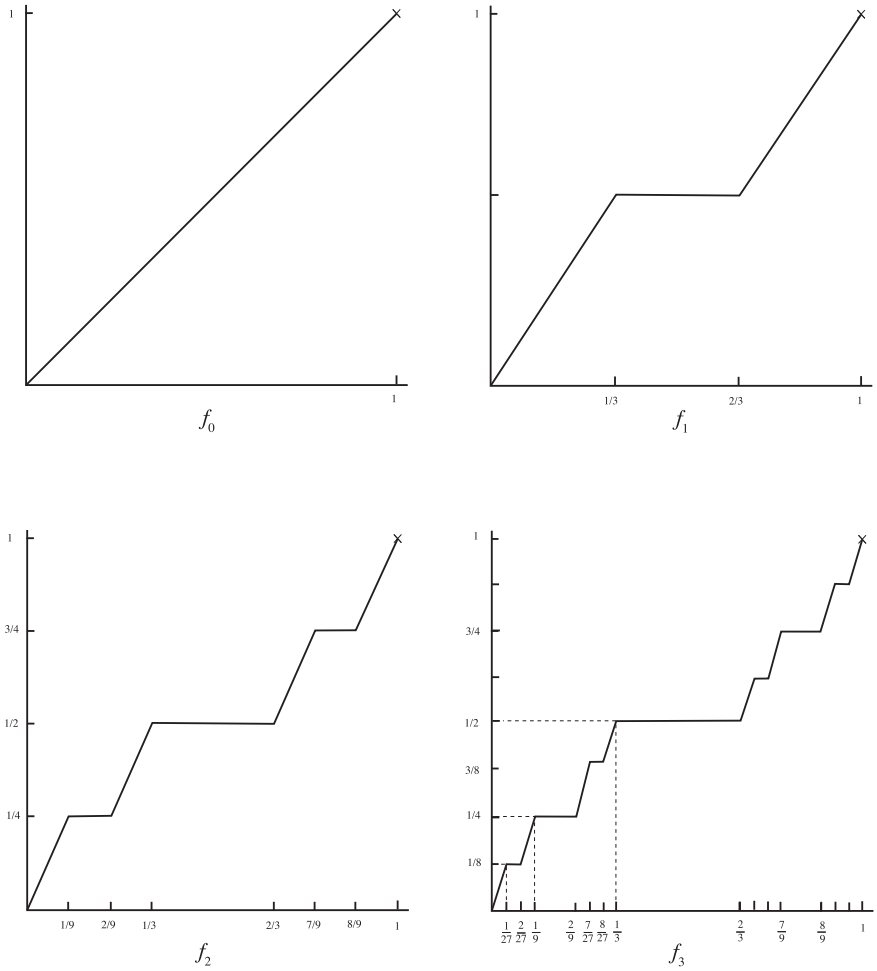


FIGURE 1. Graphes de f_0, f_1, f_2 et f_3.

$$|f_{n+1}(x) - f_n(x)| \leqslant \frac{b_{n,i} - a_{n,i}}{6}, \quad \text{si } x \in \mathrm{I}_{n,i}.$$

Une récurrence immédiate permet d'en déduire que $\|f_{n+1} - f_n\|_\infty \leqslant \frac{1}{6 \cdot 2^n}$, et

$$b_{n,i} - a_{n,i} = \begin{cases} \frac{1}{2^n} & \text{si tous les chiffres de l'écriture de } i \text{ en base 3 sont des 0 ou des 2,} \\ 0 & \text{si un des chiffres de l'écriture de } i \text{ en base 3 est un 1.} \end{cases}$$

Comme $\sum_{n \in \mathbf{N}} \frac{1}{6 \cdot 2^n} < +\infty$, la série $f_0 + \sum_{n=0}^{+\infty} (f_{n+1} - f_n)$ converge normalement, et sa somme f, qui est aussi la limite de la suite $(f_n)_{n \in \mathbf{N}}$, est continue. Chaque f_n étant croissante, il en est de même de la limite f. Enfin, f est constante sur $\mathrm{I}_{n,i}$, si un des chiffres de i dans le développement en base 3 est un 1. Il y a $3^n - 2^n$ tels i, ce qui fait que la réunion F_n des $\mathrm{I}_{n,i}$, pour i vérifiant la condition précédente, est de longueur totale égale à $1 - \frac{2^n}{3^n}$. Comme f est constante sur (chacun des intervalles composant) F_n, un passage à la limite montre que f est constante sur la réunion des F_n qui est de longueur totale

égale à 1. D'un autre côté, on a $f_n(0) = 0$ et $f_n(1) = 1$, pour tout n, et donc $f(0) = 0$ et $f(1) = 1$ par passage à la limite. On a donc bien construit une fonction continue qui croît subrepticement de 0 à 1.

19.3. L'ensemble triadique de Cantor

C'est un fermé K de $\mathbf{R}$ inclus dans $[0,1]$, de mesure nulle, mais quand même assez gros pour qu'il existe une surjection de K sur $[0,1]$. C'est l'ensemble des points de $[0,1]$ en lesquels l'escalier du diable croît.

On construit par récurrence une suite $(\mathrm{K}_n)_{n\in\mathbf{N}}$ de fermés de $[0,1]$, chaque K_n étant la réunion de 2^n segments fermés. On part de $\mathrm{K}_0 = [0,1]$, et si K_n est construit, on obtient K_{n+1} en coupant chacun des segments fermés constituant K_n en 3 segments de même longueur et en enlevant le morceau du milieu (ouvert pour que K_{n+1} soit fermé). On a donc

$$\mathrm{K}_1 = [0,1] -]\tfrac{1}{3},\tfrac{2}{3}[= [0,\tfrac{1}{3}] \cup [\tfrac{2}{3},1], \quad \mathrm{K}_2 = \mathrm{K}_1 - \big(]\tfrac{1}{9},\tfrac{2}{9}[\cup]\tfrac{7}{9},\tfrac{8}{9}[\big) = [0,\tfrac{1}{9}] \cup [\tfrac{2}{9},\tfrac{3}{9}] \cup [\tfrac{6}{9},\tfrac{7}{9}] \cup [\tfrac{8}{9},1].$$

On note K l'intersection des K_n ; c'est un fermé de $[0,1]$ comme intersection de fermés. La somme des longueurs des segments constituant K_n est $(\frac{2}{3})^n$ qui tend vers 0 quand $n \to +\infty$, ce qui fait que K est de mesure nulle, puisque $\mathrm{K} \subset \mathrm{K}_n$ pour tout n.

Par ailleurs, K est l'ensemble des $x \in [0,1]$ dont un des développements en base 3 ne comporte que des 0 et des 2 (les seuls nombres ayant deux développements sont ceux de la forme $\frac{k}{3^n}$, avec $k \in \mathbf{Z}$ et $n \in \mathbf{N}$). En effet, les nombres que l'on retire pour passer de K_n à K_{n+1} sont précisément ceux dont tous les développements en base 3 ont un 1 en n-ième position et pas de 1 avant. L'application $(a_n)_{n\geqslant 1} \mapsto \sum_{n=1}^{+\infty} \frac{a_n}{3^n}$ induit donc une bijection de l'ensemble $\{0,2\}^{\mathbf{N}-\{0\}}$ sur K, ce qui nous permet de définir une surjection $f : \mathrm{K} \to [0,1]$, en passant de la base 3 à la base 2, c'est-à-dire en envoyant $\sum_{n=1}^{+\infty} \frac{a_n}{3^n}$ sur $\sum_{n=1}^{+\infty} \frac{b_n}{2^n}$, où $b_n = a_n/2 \in \{0,1\}$.

Exercice 19.2. — (i) Adapter la construction ci-dessus pour construire un fermé de $[0,1]$ d'intérieur vide, mais de mesure non nulle.

(ii) Montrer qu'un tel ensemble est totalement discontinu.

19.4. La courbe de Peano

Il s'agit d'une courbe fractale qui remplit tout le carré, ce qui montre que la notion de dimension est plus problématique que ce qu'on pourrait croire (un probabiliste dirait que pour obtenir une courbe ayant (presque) cette propriété, il suffit de lancer un mouvement brownien qui se chargera de remplir (presque) le plan tout seul).

On construit la courbe de Peano $f : [0,1] \to [0,1]^2$ comme une limite de fonctions f_n, affines par morceaux, construites par récurrence. La fonction f_0 est juste $t \mapsto (t,t)$; son image est donc la diagonale du carré $[0,1]^2$. La fonction f_n est une fonction affine

sur chaque intervalle de la forme $\mathrm{I}_{n,i} = [\frac{i}{9^n}, \frac{i+1}{9^n}]$, et le passage de f_{n+1} à f_n se fait en remplaçant chacun des 9^n segments qui constituent l'image de f_n par 9 segments par le procédé indiqués à la figure 2. La figure 3 montre ce que cela donne pour f_2 (les fonctions f_0 et f_1 sont représentées sur la figure 2).

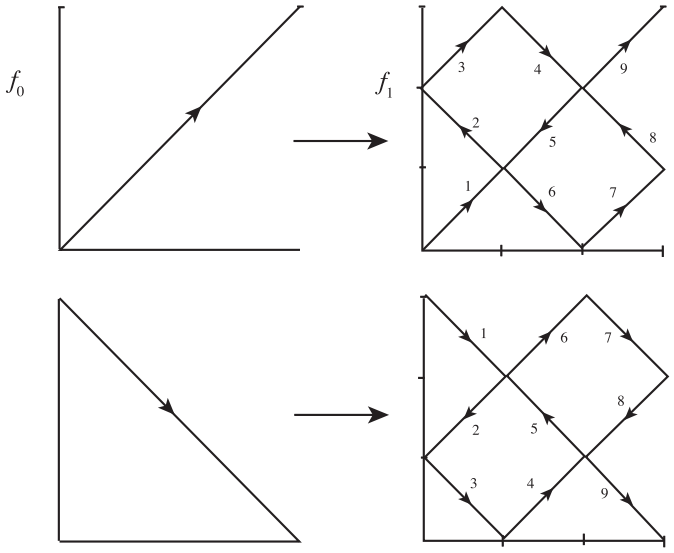


FIGURE 2. Procédé d'obtention de f_{n+1} à partir de f_n ; pour un segment allant dans l'autre sens, on renverse juste le sens de parcours.

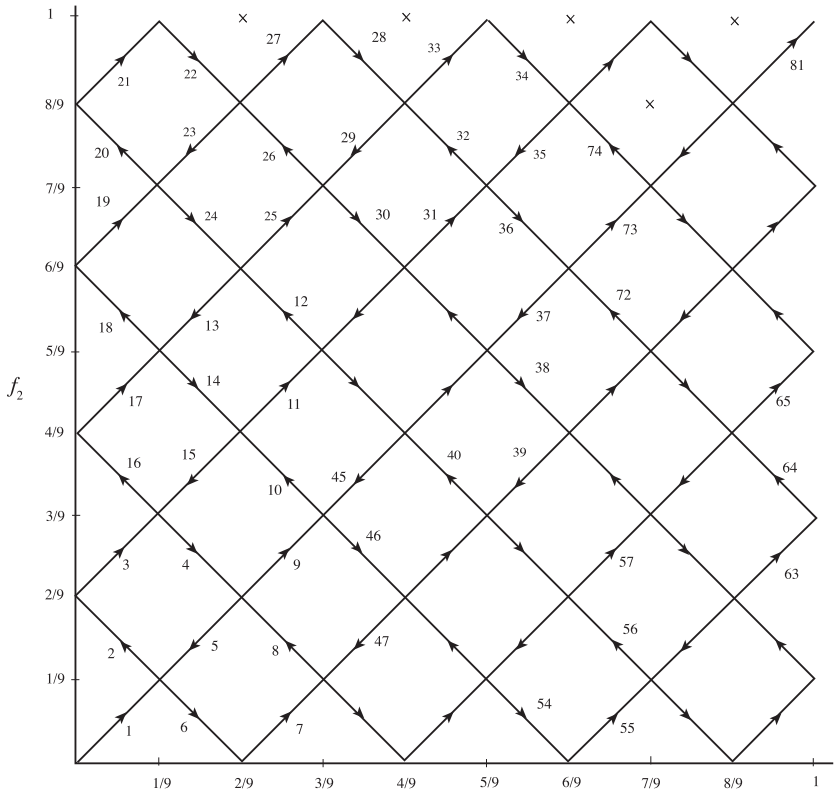


FIGURE 3. La fonction f_2 : les nombres apparaissant sur la figure correspondent à l'ordre dans lequel les $9^2 = 81$ segments sont parcourus.

Par construction, les fonctions f_{n+1} et f_n ont une image incluse dans le même sous-carré de côté de longueur $\frac{1}{3^n}$, sur chacun des segments $\mathrm{I}_{n,i}$, pour $0 \leqslant i \leqslant 9^n - 1$. On a donc $\|f_{n+1} - f_n\|_\infty \leqslant \frac{1}{3^n}$, si on munit $\mathbf{R}^2$ de la norme $\|(x, y)\| = \sup(|x|, |y|)$. On en déduit que f_n converge uniformément sur $[0, 1]$, et comme les f_n sont continues, il en est de même de la limite f.

On a $f_{n+1}\big(\frac{i}{9^n}\big) = f_n\big(\frac{i}{9^n}\big)$, si $0 \leqslant i \leqslant 9^n$, et donc $f(\frac{i}{9^n}) = f_n\big(\frac{i}{9^n}\big)$, si $n \in \mathbf{N}$ et $0 \leqslant i \leqslant 9^n$. Or l'image de $\big\{\frac{i}{9^n},\ 0 \leqslant i \leqslant 9^n - 1\big\}$ par f_n est l'ensemble A_n des couples $\big(\frac{a}{3^n}, \frac{b}{3^n}\big)$, avec a, b entiers, $0 \leqslant a, b \leqslant 3^n$, et $a + b$ pair. La réunion des A_n est dense dans $[0, 1]^2$, et est contenue dans l'image de f d'après ce qui précède ; l'image de f est donc dense dans $[0, 1]^2$. Pour montrer que f remplit tout le carré $[0, 1]^2$, il n'y a plus qu'à remarquer que $[0, 1]$ étant compact et f continue, $f([0, 1])$ est compacte et donc fermée dans $[0, 1]^2$, et comme elle est dense, c'est $[0, 1]^2$ tout entier !

19.5. Ensembles connexes non connexes par arcs

19.5.1. *Le graphe de* $\sin\frac{1}{x}$

Soit X le graphe de la fonction $x \mapsto \phi(x) = \sin\frac{1}{x}$, pour $x > 0$. L'ensemble X est connexe par arcs, vu que c'est un arc en tant qu'image de $\mathbf{R}_+^*$ par $x \mapsto (x, \phi(x))$ qui est

une application continue de $\mathbf{R}_+^*$ dans $\mathbf{R}^2$. Son adhérence $\overline{\mathrm{X}}$ dans X est donc connexe ; nous allons montrer qu'elle n'est pas connexe par arc.

Commençons par montrer que $\overline{\mathrm{X}} = \mathrm{X} \cup \mathrm{I}$, où I est le segment vertical $\mathrm{I} = \{(0, y),\ y \in [-1, 1]\}$.

• Comme $\mathbf{R}^2$ est métrique, un point (a, b) est dans l'adhérence de X, s'il existe une suite $(x_n, y_n)_{n\in\mathbf{N}}$ d'éléments de X convergeant vers (a, b) dans $\mathbf{R}^2$. Or $y_n = \phi(x_n)$ et ϕ est continue sur $\mathbf{R}_+^*$, ce qui fait que, si $a > 0$, on doit avoir $b = \phi(a)$ par continuité. L'intersection de $\overline{\mathrm{X}}$ avec $\mathbf{R}_+^* \times \mathbf{R}$ est donc réduite à X.

• Comme X est contenu dans le fermé $\mathbf{R}_+ \times [-1, 1]$, il en est de même de son adhérence ; on en déduit l'inclusion $\overline{\mathrm{X}} \subset \mathrm{X} \cup \mathrm{I}$.

• Si $b \in [-1, 1]$, alors $(0, b)$ est la limite de $\left(\frac{1}{2n\pi + \arcsin(b)}, b\right) \in \mathrm{X}$, quand $n \to +\infty$, ce qui montre que $(0, b) \in \overline{\mathrm{X}}$, et donc que $\mathrm{I} \subset \overline{\mathrm{X}}$. On en déduit l'égalité $\overline{\mathrm{X}} = \mathrm{X} \cup \mathrm{I}$ que l'on cherchait à établir.

Démontrons, par l'absurde, que $\overline{\mathrm{X}}$ n'est pas connexe par arcs. Supposons donc le contraire ; il existe alors $u : [0, 1] \to \overline{\mathrm{X}}$, continue, telle que $u(0) = (0, 0)$, et $u(1) = (\pi^{-1}, 0)$. Soient $\mathrm{A} = \{t,\ u(t) \in \mathrm{I}\}$ et $a \in [0, 1]$ la borne supérieure de A. Alors $u(a) \in \mathrm{I}$ car I est fermé et u est continue, et $u(t) \notin \mathrm{I}$, si $t > a$. On a donc $u(a) = (0, b)$, et $u(t) = (x(t), y(t))$, avec $x(t) > 0$, si $t > a$. On peut supposer, sans nuire à la généralité, que $b \neq 1$ (sinon, on remplace 1 par -1 dans ce qui suit). Comme u est continue, il existe $\delta > 0$ tel que $y(t) \neq 1$, si $t \in [a, a + \delta]$. Comme $y(t) = \phi(x(t))$, cela implique que $x(t)$ n'est pas de la forme $\frac{1}{2n\pi + (\pi/2)}$, si $t \in [a, a + \delta]$, Or le seul intervalle de $\mathbf{R}_+$ contenant 0 et ne contenant aucun point de la forme $\frac{1}{2n\pi + (\pi/2)}$, pour $n \in \mathbf{N}$, est $\{0\}$. Comme $t \mapsto x(t)$ est continue sur $[a, a + \delta]$, cela implique $x(t) = 0$, si $t \in [a, a + \delta]$, ce qui est contraire à la définition de a. Ceci permet de conclure.

19.5.2. *Le tipi de Cantor*

C'est un sous-ensemble T du plan qui défie un peu l'entendement car il est connexe, et il existe $\mathrm{S} \in \mathrm{T}$ tel que, si on retire S à T, le résultat est totalement discontinu (ce qui signifie, rappelons-le, que les composantes connexes de $\mathrm{T} - \mathrm{S}$ sont réduites à des points).

Pour construire T, on part de l'ensemble triadique de Cantor K que l'on partitionne en un ensemble K_1 dénombrable et dense [118] et son complémentaire K_2.

On identifie K à un sous-ensemble de $\mathbf{R}^2$ par $t \mapsto (t, 0)$, ce qui permet de voir K comme un sous-ensemble du segment horizontal $\mathrm{L} = [0, 1] \times \{0\}$. On note S le point $(0, 1)$, et si $\mathrm{P} = (t, 0)$, avec $t \in \mathrm{K}_1$ (resp. $t \in \mathrm{K}_2$), on définit le *rayon* $\mathrm{T_P}$ comme l'ensemble des (x, y) appartenant au segment $[\mathrm{P}, \mathrm{S}[$, avec $y \in \mathbf{Q}$ (resp. $y \notin \mathbf{Q}$). On définit le *tipi de Cantor* T comme la réunion des $\mathrm{T_P}$, pour $\mathrm{P} \in \mathrm{K}$, auquel on rajoute le *sommet* S de T. Nous allons montrer que T est connexe, mais que T privé de S est totalement discontinu.

Pour montrer que T est connexe, considérons une partition de T en deux ouverts U_1 et U_2, et supposons que $\mathrm{S} \in \mathrm{U}_1$. Comme U_1 est non vide, il s'agit de montrer que U_2 l'est. Comme il est plus confortable de travailler dans un carré que dans un triangle, on remarque que $(x, y) \mapsto ((1-y)x, y)$ induit un homéomorphisme de $[0, 1] \times [0, 1[$ sur le triangle de sommets $\mathrm{A} = (0, 0)$, $\mathrm{B} = (1, 0)$ et $\mathrm{S} = (0, 1)$, privé de son sommet S ; l'homéomorphisme réciproque étant $(x, y) \mapsto (\frac{x}{1-y}, y)$. Via cet homéomorphisme, le rayon $\mathrm{T_P}$ devient $\mathrm{T'_P} = \{\mathrm{P}\} \times ([0, 1] \cap \mathbf{Q})$, si

118. On peut, par exemple, prendre pour K_1 l'ensemble des éléments de K dont le développement en base 3 est limité, i.e. l'ensemble des nombres de la forme $\sum_{i=1}^{n} \frac{a_i}{3^n}$, avec $n \in \mathbf{N}$, et $a_i \in \{0, 2\}$, si $1 \leqslant i \leqslant n$.

$P \in K_1$, et $T'_P = \{P\} \times ([0,1] \cap (\mathbf{R} - \mathbf{Q}))$, si $P \in K_2$, et $T - S$ devient la réunion T' de $K_1 \times ([0,1] \cap \mathbf{Q})$, et de $K_2 \times ([0,1] \cap (\mathbf{R} - \mathbf{Q}))$. L'ouvert $U_1 - S$ devient un ouvert U'_1 de T' contenant $([0,1]\times]1-\delta, 1[) \cap T'$, si $\delta > 0$ est assez petit, U_2 devient un ouvert U'_2 de T', et U'_1 et U'_2 forment une partition de T'.

On est alors ramené à prouver que U'_2 est vide. On définit une fonction $h : K \to [0,1]$, par $h(P) = 0$, si $T'_P \cap U'_2 = \varnothing$, et $h(P) = \sup\{y,\ (P,y) \in T'_P \cap U'_2\}$, si $T'_P \cap U'_2 \neq \varnothing$. Comme U'_2 est ouvert, sa vacuité est équivalente à $h = 0$ sur K ; on va donc s'intéresser aux points où $h \neq 0$.

• $h(P) < 1$ pour tout $P \in K$, car $U'_1 \cap U'_2 = \varnothing$ et U'_1 contient $([0,1]\times]1-\delta, 1[) \cap T'$, si $\delta > 0$ est assez petit.

• $h(P) \in \mathbf{Q}$ si $P \in K_2$, car sinon le point $(P, h(P))$ de T'_P appartiendrait à U'_i, pour $i = 1$ ou $i = 2$, et comme U'_i est ouvert, il existerait un segment ouvert $J \subset]0,1[$, contenant $h(P)$, tel que $\{(P,t),\ t \in J\} \cap T'$, soit contenu dans U'_i. Dans les deux cas $i = 1$ et $i = 2$, on obtient une contradiction avec la définition de $h(P)$.

• Si $q \in]0,1[\cap \mathbf{Q}$, et si $P \in K_1$, il existe un ouvert I de K contenant P tel que $h(Q) \neq q$ pour tout $Q \in I$. En effet, le point (P,q) appartient à T'_P par construction, et donc appartient à U'_i, pour $i = 1$ ou $i = 2$. Comme U'_i est ouvert et contient (P,q), il contient un ouvert de la forme $(I \times J) \cap T'$, où I est un ouvert de K contenant P, et J est un ouvert de $]0,1[$, contenant q ; la définition de h montre que l'on a $h(Q) \notin J$, si $Q \in I$.

Si $q \in]0,1[\cap \mathbf{Q}$, soit F_q l'adhérence de $\{P \in K,\ h(P) = q\}$. C'est un fermé de K par construction, et il ne rencontre pas K_1 d'après le point précédent. Il est donc d'intérieur vide puisque K_1 est dense dans K. Comme K est un compact métrique, il est complet, et le lemme de Baire implique que la réunion X de K_1 et des F_q, pour $q \in \mathbf{Q} \cap]0,1[$, est d'intérieur vide, puisque c'est une réunion dénombrable de fermés d'intérieur vide ($\mathbf{Q} \cap]0,1[$ est dénombrable et K_1 est dénombrable et donc est une réunion dénombrable de singletons). L'ensemble $K - X$ est donc dense dans K. Or $P \in K - X$ implique $h(P) = 0$, et donc aussi $\{P\} \times (]0,1[\cap (\mathbf{R} - \mathbf{Q})) \subset U'_1$. Donc U'_1 contient $(K - X) \times (]0,1[\cap (\mathbf{R} - \mathbf{Q}))$ qui est dense dans T' car il l'est dans $K \times [0,1[$ qui contient T'. Son complémentaire U'_2 est donc d'intérieur vide, et comme il est ouvert, il est vide. On en déduit la connexité de T.

Il reste à montrer que $T - S$ est totalement discontinu, et comme $T - S$ est homéomorphe à T', il suffit de prouver que T' l'est. Pour cela considérons deux points distincts (P_1, y_1) et (P_2, y_2) de T'. Si $P_1 \neq P_2$, il existe $Q \notin K$ dans l'intervalle ouvert d'extrémités P_1 et P_2 puisque K est d'intérieur vide. La droite verticale $\{Q\} \times \mathbf{R}$ ne rencontre pas T', et les deux demi-plans ouverts qu'elle délimite partitionnent T' en deux ouverts, l'un contenant (P_1, y_1), l'autre (P_2, y_2). On en déduit que (P_2, y_2) n'est pas dans la composante connexe de (P_1, y_1). Une composante connexe de T' est donc incluse dans un rayon T'_P, or un tel ensemble est totalement discontinu puisqu'il est homéomorphe à $\mathbf{Q} \cap [0,1[$ ou à $(\mathbf{R} - \mathbf{Q}) \cap [0,1[$. Les composantes connexes de T' sont donc des points, ce qui permet de conclure.

20. Construction de nombres

Dans ce §, on explique rapidement (sans démonstration) comment construire toutes les quantités usuelles à partir d'un système minimal d'axiomes. Cette problématique n'est apparue que relativement récemment dans l'histoire des mathématiques puisqu'il a fallu attendre 1872 pour que Weierstrass s'aperçoive que les nombres réels n'avaient pas été

définis, ce qui aurait pu avoir des conséquences fâcheuses... Une des raisons qui ont poussé les mathématiciens à s'intéresser à ces questions de fondements a été l'apparition de monstres (cf. § précédent) montrant que l'intuition pouvait se révéler fort trompeuse, et de paradoxes menaçant de faire s'écrouler tout l'édifice.

20.1. Entiers naturels

La première présentation axiomatique des entiers remonte à 1888 (Dedekind), simplifiée l'année suivante par Peano. L'ensemble des nombres entiers qui semble être constitué des objets les plus évidents (tout le monde comprend ce que sont $0, 1, 2, \ldots$; le problème est dans le « ... »), ne peut pas être construit ; on est plus ou moins forcé de postuler son existence et d'espérer que le ciel ne va pas nous tomber sur la tête.

• La présentation la plus efficace postule l'existence d'un ensemble $\mathbf{N}$, l'ensemble des entiers naturels, muni d'un élément 0 et d'une application « successeur » $s : \mathbf{N} \to \mathbf{N}$, vérifiant les axiomes (de Peano) suivants :

(A1) l'application s est injective ;

(A2) 0 n'est le successeur d'aucun entier naturel ;

(A3) Si $\mathrm{X} \subset \mathbf{N}$ est tel que $0 \in \mathrm{X}$ et $s(n) \in \mathrm{X}$ pour tout $n \in \mathrm{X}$, alors $\mathrm{X} = \mathbf{N}$ (axiome de récurrence).

On définit alors l'addition et la multiplication par récurrence par $a+0 = a$ et $a+s(b) = s(a+b)$ (pour l'addition) ; $a\,0 = 0$ et $a\,s(b) = ab + a$ (pour la multiplication). On pose $1 = s(0)$, et on a $s(a) = s(a+0) = a + s(0) = a+1$, ce qui permet de supprimer l'application successeur et de la remplacer par $a \mapsto a+1$. Vérifier, à partir des axiomes de Peano, que l'addition et la multiplication sont commutatives et que la multiplication est distributive par rapport à l'addition, est un exercice un peu répétitif mais très satisfaisant pour l'esprit.

• On obtient une présentation plus intuitive en partant de l'idée que se fait le petit enfant du nombre 5. On dit qu'un ensemble X est fini s'il ne peut pas être mis en bijection avec $\mathrm{X} \cup \{x\}$, si $x \notin \mathrm{X}$. On postule l'existence d'un ensemble infini Ω (axiome de l'infini), et on munit l'ensemble des parties de Ω de la relation d'équivalence $\sim$ définie par $\mathrm{X}_1 \sim \mathrm{X}_2$ s'il existe une bijection de X_1 sur X_2. On définit alors l'ensemble $\mathbf{N}$ des entiers naturels comme l'ensemble des classes d'équivalence de parties finies de Ω pour cette relation d'équivalence. Si X est une partie finie de Ω, on note $|\mathrm{X}| \in \mathbf{N}$ sa classe d'équivalence ; c'est un entier naturel que l'on appelle le cardinal de X, et une analyse *a posteriori* de la construction précédente, montre que l'on a défini l'entier n comme la classe d'équivalence de tous les ensembles (inclus dans notre Ω) de cardinal n.

On note 0 le cardinal de l'ensemble vide, 1 celui d'un singleton (i.e. un ensemble X, non vide, tel que $x, y \in \mathrm{X} \Rightarrow x = y$)... Si $a, b \in \mathbf{N}$, on choisit $\mathrm{X}, \mathrm{Y} \subset \Omega$ disjoints, de cardinaux respectifs a et b, et on définit $a+b$ comme le cardinal de $\mathrm{X} \cup \mathrm{Y}$, et ab comme le cardinal de (tout sous-ensemble de Ω pouvant être mis en bijection avec) $\mathrm{X} \times \mathrm{Y}$. Il est alors quasi-immédiat que $a+b = b+a$ (car $\mathrm{X} \cup \mathrm{Y} = \mathrm{Y} \cup \mathrm{X}$), que $ab = ba$ (car $(x, y) \mapsto (y, x)$ induit une bijection de $\mathrm{X} \times \mathrm{Y}$ sur $\mathrm{Y} \times \mathrm{X}$), que $0 \cdot a = 0$ pour tout $a \in \mathbf{N}$ (l'ensemble $\varnothing \times \mathrm{X}$ est vide quel que soit X), et que $a(b+c) = ab + ac$ (car $\mathrm{X} \times (\mathrm{Y} \cup \mathrm{Z}) = (\mathrm{X} \times \mathrm{Y}) \cup (\mathrm{X} \times \mathrm{Z})$).

Les choses se compliquent quand on essaie de montrer que $\mathbf{N}$ vérifie l'axiome de récurrence pour l'application successeur $x \mapsto x+1$.

20.2. Entiers relatifs, nombres rationnels

En partant des entiers naturels, on fait les constructions suivantes.

• On construit $\mathbf{Z}$ comme quotient de $\mathbf{N} \times \mathbf{N}$ par la relation d'équivalence $(a, b) \sim (a', b')$ si et seulement si $a + b' = a' + b$, l'idée étant que (a, b) représente l'entier relatif $a - b$. L'application $n \mapsto (n, 0)$ induit une injection de $\mathbf{N}$ dans $\mathbf{Z}$, ce qui permet de voir $\mathbf{N}$ comme un sous-ensemble de $\mathbf{Z}$.

L'addition $(a, b) + (a', b') = (a + a', b + b')$ passe au quotient, et définit une loi qui fait de $\mathbf{Z}$ un groupe commutatif, l'élément neutre étant (la classe de) $(0, 0)$ (ou de (a, a), pour tout $a \in \mathbf{N}$), et l'opposé de (a, b) étant (b, a). L'opposé $-n$ de n est donc représenté par $(0, n)$, et on peut maintenant définir $a - b$, si a et $b \in \mathbf{Z}$, et si $a, b \in \mathbf{N}$, on a $a - b = (a, 0) + (0, b) = (a, b)$, ce que l'on cherchait à obtenir.

La multiplication [119] $(a, b)(a', b') = (aa' + bb', ab' + ba')$ passe au quotient, et $\mathbf{Z}$ muni de l'addition et de la multiplication est un anneau commutatif.

Enfin, on dit que $a \geqslant b$, si $a - b \in \mathbf{N}$, et on obtient de la sorte une relation d'ordre totale sur $\mathbf{Z}$.

• On construit $\mathbf{Q}$ comme quotient de $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ par la relation d'équivalence $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$, l'idée étant que (a, b) représente le nombre rationnel $\frac{a}{b}$. L'application $n \mapsto (n, 1)$ induit une injection de $\mathbf{Z}$ dans $\mathbf{Q}$, ce qui permet de voir $\mathbf{Z}$ comme un sous-ensemble de $\mathbf{Q}$.

L'addition et la multiplication sur $\mathbf{Q}$ sont définies par les formules $(a, b) + (a', b') = (ab' + ba', bb')$ et $(a, b)(a', b') = (aa', bb')$ qui passent au quotient, et $\mathbf{Q}$ muni de l'addition et de la multiplication est un corps commutatif :l'élément neutre pour $+$ est 0, la classe de $(0, b)$, pour tout $b \in \mathbf{N}$, l'opposé de (a, b) est $(-a, b)$, l'élement neutre pour $\times$ est 1, classe de (b, b), pour tout $b \in \mathbf{Z} - \{0\}$, et l'inverse de (a, b), si $(a, b) \neq 0$ (ce qui équivaut à $a \neq 0$) est (b, a). Si $a \in \mathbf{Z}$ et $b \in \mathbf{Z} - \{0\}$, on peut maintenant diviser a par b dans $\mathbf{Q}$, et $b^{-1}a$ est la classe de $(1, b)(a, 1) = (a, b)$, ce que l'on cherchait à obtenir.

Enfin, on dit que q est positif, si q a un représentant (a, b) avec $b \geqslant 0$ et $a \geqslant 0$, et que $q_1 \geqslant q_2$, si $q_1 - q_2$ est positif. On obtient de la sorte une relation d'ordre total sur $\mathbf{Q}$.

20.3. Nombres réels, nombres complexes

Pour construire $\mathbf{R}$ à partir de $\mathbf{Q}$, on dispose essentiellement de trois possibilités.

• On peut utiliser les *coupures de Dedekind* (1872), c'est-à-dire l'ensemble des couples (A, B) de parties non vides de $\mathbf{Q}$ tels que $\mathrm{A} \cup \mathrm{B} = \mathbf{Q}$, et tout élément de A est $\leqslant$ à tout élément de B. L'idée étant que si $r \in \mathbf{R}$, alors r correspond à la coupure $(\mathrm{A}_r, \mathrm{B}_r)$ donnée par $\mathrm{A}_r = \{x \in \mathbf{Q},\ x \leqslant r\}$ et $\mathrm{B}_r = \{x \in \mathbf{Q},\ x \geqslant r\}$. Les rationnels s'identifient aux coupures (A, B) telles que $\mathrm{A} \cap \mathrm{B}$ est non vide. Il est alors facile de montrer que l'ensemble

119. On rappelle que (a, b) représente $b-a$, et donc que $(aa'+bb', ab'+ba')$ représente $aa'+bb'-ab'-ba' = (a - b)(a' - b')$, ce qui explique comment la formule pour la multiplication a été obtenue.

R ainsi construit vérifie la propriété de la borne supérieure (toute partie majorée non vide admet une borne supérieure), puis qu'il est complet.

• On peut aussi, comme G. Cantor (1872), compléter **Q** pour la valeur absolue, en rajoutant de force les limites des suites de Cauchy d'éléments de **Q**. On considère l'ensemble Cauchy(**Q**) des suites de Cauchy d'éléments de **Q** (i.e. l'ensemble des suites $(a_n)_{n\in\mathbf{N}} \in \mathbf{Q}^{\mathbf{N}}$, telles que, pour tout $j \in \mathbf{N}$, il existe $\mathrm{N}_j \in \mathbf{N}$ tel que $|a_p - a_n| < 2^{-j}$, quels que soient $n, p \geqslant \mathrm{N}_j$). Alors Cauchy(**Q**) est un anneau pour l'addition et la multiplication terme à terme dans lequel l'ensemble I des suites tendant vers 0 est un idéal. On définit **R** comme le quotient de Cauchy(**Q**) par I, ce qui revient à identifier deux suites de Cauchy ayant même limite (i.e. dont la différence tend vers 0), et donc « à identifier une suite de Cauchy avec sa limite ». Le résultat **R** est un corps [120], muni d'une relation d'ordre [121] stricte, totale, dans lequel **Q** (identifié à l'image des suites constantes) est dense [122].

• On peut aussi utiliser la construction de « l'homme de la rue » qui part du fait qu'un réel a un développement décimal. Cela conduit à définir **R** comme l'ensemble des développements décimaux $a_n \dots a_0, a_{-1}a_{-2}\dots$ avec un nombre fini de chiffres avant la virgule et un nombre infini après, modulo la relation d'équivalence $\sim$, identifiant $a_n \dots a_m 999999\dots$ à $a_n \dots a_{m+1}(a_m + 1)00000\dots$, si $a_m \neq 9$. Nous laissons au lecteur le soin de définir l'addition et la multiplication de deux réels de « l'homme de la rue »...

• Une fois les nombres réels construits, on obtient le corps des nombres complexes **C** en rajoutant à **R** une racine carrée i de -1, ce qui revient à poser $\mathbf{C} = \mathbf{R}[\mathrm{X}]/(\mathrm{X}^2 + 1)$. Le résultat est un corps complet pour la norme $|z| = \sqrt{x^2 + y^2}$, si $z = x + iy$, et qui est algébriquement clos (résultat connu sous le nom de « théorème fondamental de l'algèbre » bien qu'il n'existe aucune démonstration de ce résultat qui n'utilise pas de technique d'analyse).

20.4. Nombres p-adiques

20.4.1. *Le corps* $\mathbf{Q}_p$. — La construction de **R** de G. Cantor, bien que plus compliquée, est nettement plus souple que celle de R. Dedekind, et se généralise facilement. Il n'a fallu que 25 ans après la construction des nombres réels (qui avait pris quelque deux millénaires...), pour que K. Hensel envisage la construction (1897) des nombres p-adiques,

120. si $(a_n)_{n\in\mathbf{N}}$ est une suite de Cauchy qui ne tend pas vers 0, alors $a_n \neq 0$ si $n \geqslant n_0$, et la suite $(1, \dots, 1, a_{n_0}^{-1}, \dots, a_n^{-1}, \dots)$ est de Cauchy et son image dans **R** est l'inverse de celle de la suite $(a_n)_{n\in\mathbf{N}}$.

121. Si $a, b \in \mathbf{R}$, on dit que $a < b$, si $a \neq b$ et si, pour tous représentants $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ de a et b, on a $a_n < b_p$ si n et p sont assez grands ; on constate sans problème que si c'est vrai pour un choix de représentants, alors c'est vrai pour tous.

122. Cela signifie qu'entre deux éléments de **R** on peut toujours trouver un élément de **Q**. Si $a < b$ sont deux éléments de **R**, et si $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ sont des représentants de a et b, alors $a_n < b_p$, si $n, p \geqslant n_0$, et $r = \frac{a_{n_0} + b_{n_0}}{2}$ est un élément de **Q** vérifiant $a < r < b$.

et une petite dizaine d'années pour qu'il leur donne une forme maniable. De nos jours, on procède de la manière suivante.

Soit p un nombre premier. Si $a \in \mathbf{Z} - \{0\}$, on définit la valuation p-adique $v_p(a)$ comme le plus grand entier v tel que p^v divise a. On a $v_p(ab) = v_p(a) + v_p(b)$ si $a, b \in \mathbf{Z} - \{0\}$, ce qui permet d'étendre v_p à $\mathbf{Q}$ en posant $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$, si $a, b \in \mathbf{Z} - \{0\}$, et $v_p(0) = +\infty$. On a alors $v_p(x + y) \geqslant \min(v_p(x), v_p(y))$, si $x, y \in \mathbf{Q}$ car, si x et y sont divisibles par p^v, il en est de même de $x + y$. On en déduit le fait que, si on pose $|x|_p = p^{-v_p(x)}$, alors $|x+y|_p \leqslant \sup(|x|_p, |y|_p)$ et donc que $d_p(x, y) = |x-y|_p$ est une distance sur $\mathbf{Q}$ (la *distance p-adique*), l'inégalité ci-dessus, dite *ultramétrique*, étant plus forte que l'inégalité triangulaire.

On définit $\mathbf{Q}_p$, corps des nombres p-adiques, comme le complété de $\mathbf{Q}$ pour la norme p-adique $|\ |_p$, c'est-à-dire que l'on prend, comme pour définir $\mathbf{R}$, l'anneau des suites de Cauchy (pour la norme $|\ |_p$) d'éléments de $\mathbf{Q}$, et on quotiente par l'idéal des suites tendant vers 0. Si $x \in \mathbf{Q}_p$, et si $(a_n)_{n\in\mathbf{N}}$ est un représentant de x, alors $|a_n|_p$ tend vers une limite dans $\mathbf{R}$ (et même dans $p^{\mathbf{Z}} \cup \{0\}$, car tous ses termes sont dans $p^{\mathbf{Z}} \cup \{0\}$ qui est fermé dans $\mathbf{R}_+$) qui ne dépend que de x, et qu'on note $|x|_p$. Par construction, $|\ |_p$ est une norme ultramétrique sur $\mathbf{Q}_p$, ce qui signifie que $|x|_p = 0$ si et seulement si $x = 0$, que $|xy|_p = |x|_p|y|_p$, quels que soient $x, y \in \mathbf{Q}_p$, et que $|x + y|_p \leqslant \sup(|x|_p, |y|_p)$, et donc $d_p(x, y) = |x - y|_p$ est une distance ultramétrique sur $\mathbf{Q}_p$ pour laquelle $\mathbf{Q}_p$ est complet. On étend v_p à $\mathbf{Q}_p$ par continuité, et on a encore $|x|_p = p^{-v_p(x)}$, si $x \in \mathbf{Q}_p$.

• Dans $\mathbf{Q}_p$, une suite $(x_n)_{n\in\mathbf{N}}$ converge si et seulement si $x_{n+1} - x_n$ tend vers 0 et une série $\sum_{n\in\mathbf{N}} u_n$ converge si et seulement si u_n tend vers 0.

D'après l'inégalité ultramétrique, on a $|x_{n+k} - x_n|_p \leqslant \sup_{0\leqslant i\leqslant k-1} |x_{n+i+1} - x_{x+i}|_p$, ce qui montre que si $|x_{n+1} - x_n|_p$ tend vers 0, alors la suite est de Cauchy. La complétude de $\mathbf{Q}_p$ permet de conclure (l'argument est le même pour une série).

Exercice 20.1. — Montrer que la série $1 + 2 + 4 + 8 + \cdots$ converge vers -1 dans $\mathbf{Q}_2$.

Exercice 20.2. — (i) Montrer que $|x + y|_p = |x|_p$, si $|x|_p > |y|_p$.
(ii) Montrer que $\sum_{n\in\mathbf{N}} u_n \neq 0$, et $\big|\sum_{n\in\mathbf{N}} u_n\big|_p = |u_0|_p$, si $u_n \to 0$, et si $|u_0|_p > |u_n|_p$, pour tout $n \geqslant 1$.

• La topologie de $\mathbf{Q}_p$ possède des propriétés un peu déroutantes au premier abord.
(i) Tout point d'une boule de $\mathbf{Q}_p$ en est « le » centre.
(ii) Deux boules de $\mathbf{Q}_p$ sont soit disjointes soit l'une est contenue dans l'autre (comme des billes de mercure).
(iii) Les boules de $\mathbf{Q}_p$ sont à la fois ouvertes et fermées.
(iv) La topologie de $\mathbf{Q}_p$ est totalement discontinue.

Si $x_1 \in \mathrm{B}(x_0, r)$ et $y \in \mathrm{B}(x_1, r)$, alors $d_p(x_0, y) \leqslant \sup(d_p(x_0, x_1), d_p(x_1, y)) \leqslant r$ (ou $< r$ si on parle de boules ouvertes), et donc $\mathrm{B}(x_1, r) \subset \mathrm{B}(x_0, r)$. L'inclusion dans l'autre sens s'obtient en échangeant les rôles de x_0 et x_1, ce qui permet de démontrer le (i).

D'après le (i), si deux boules ont une intersection non vide, tout élément de l'intersection est le centre des deux boules, ce qui démontre le (ii).

Si B est une boule ouverte de rayon r, le complémentaire de B contient la boule ouverte de rayon r autour de chacun de ses points d'après le (ii), ce qui montre que ce complémentaire est ouvert et donc que B est fermée. Si B est une boule fermée de rayon non nul, alors B est un voisinage de chacun de ses points puisque ceux-ci en sont "le" centre. On en déduit le (iii).

Enfin, si $x \in \mathbf{Q}_p$, si C_x est la composante connexe de x, et si $r > 0$, alors $\mathrm{C}_x \cap \mathrm{B}(x, r)$ est à la fois ouvert et fermé dans C_x, et non vide puisque contenant x. Comme C_x est connexe, cela implique $\mathrm{C}_x \cap \mathrm{B}(x, r) = \mathrm{C}_x$, quel que soit $r > 0$, et donc $\mathrm{C}_x = \{x\}$. On en déduit le (iv).

20.4.2. *Construction algébrique de* $\mathbf{Q}_p$

L'alinéa précédent a donné une construction analytique de $\mathbf{Q}_p$ comme complété de $\mathbf{Q}$ pour la norme p-adique. Dans cet alinéa, on présente une autre construction de $\mathbf{Q}_p$, à partir des $\mathbf{Z}/p^n\mathbf{Z}$, qui est purement algébrique. L'existence de ces deux points de vue sur les nombres p-adiques offre la possibilité de jongler avec un mélange de techniques d'analyse et d'algèbre, ce qui s'avère précieux pour de nombreuses questions.

• L'ensemble $\mathbf{Z}_p = \{x \in \mathbf{Q}_p,\ |x|_p \leqslant 1\}$ est un sous-anneau fermé de $\mathbf{Q}_p$ qui contient $\mathbf{Z}$.

La multiplicativité de $|\ |_p$ montre que $\mathbf{Z}_p$ est stable par multiplication et l'inégalité ultramétrique montre que $\mathbf{Z}_p$ est stable par addition. C'est donc un sous-anneau de $\mathbf{Q}_p$ qui contient $\mathbf{Z}$ de manière évidente et qui est fermé puisque c'est l'image inverse de $[0, 1]$ par $x \mapsto |x|_p$.

• $\mathbf{Z}_p^*$ est l'ensemble des $x \in \mathbf{Z}_p$ vérifiant $|x|_p = 1$; c'est aussi $\mathbf{Z}_p - p\mathbf{Z}_p$.

Si $x \in \mathbf{Z}_p - \{0\}$, l'inverse x^{-1} de x dans $\mathbf{Q}_p$ vérifie $|x^{-1}|_p|x|_p = 1$. Comme $|x|_p \leqslant 1$, cet inverse appartient à $\mathbf{Z}_p$ si et seulement si $|x|_p = 1$. Maintenant, pour les mêmes raisons que ci-dessus, l'ensemble des $x \in \mathbf{Z}_p$ vérifiant $|x|_p < 1$ est un idéal de $\mathbf{Z}_p$, et comme $|x|_p < 1$ implique $|x|_p \leqslant p^{-1}$, c'est l'idéal $p\mathbf{Z}_p$. On a donc $\mathbf{Z}_p^* = \mathbf{Z}_p - p\mathbf{Z}_p$.

• L'application naturelle de $\mathbf{Z}/p^n\mathbf{Z}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$ est un isomorphisme.

Si x est un élément de $\mathbf{Z} \cap p^n\mathbf{Z}_p$, on a $v_p(x) \geqslant n$, ce qui signifie que x est divisible par p^n dans $\mathbf{Z}$. On en déduit l'injectivité. Prouvons la surjectivité. Soient $\overline{x} \in \mathbf{Z}_p/p^n\mathbf{Z}_p$ et $x \in \mathbf{Z}_p$ ayant pour image $\overline{x}$ modulo p^n. Comme $\mathbf{Q}$ est dense dans $\mathbf{Q}_p$, il existe $r \in \mathbf{Q}$ vérifiant $v_p(x - r) \geqslant n$; en particulier $v_p(r) \geqslant 0$. Écrivons r sous la forme $\frac{a}{b}$ avec $a, b \in \mathbf{Z}$. Comme $v_p(r) \geqslant 0$, on a $v_p(b) \leqslant v_p(a)$ et quitte à tout diviser par $p^{v_p(b)}$, on peut supposer $v_p(b) = 0$, et donc $(b, p) = 1$, ce qui implique que b est premier à p^n et donc est inversible dans $\mathbf{Z}/p^n\mathbf{Z}$. Soit $\overline{c}$ l'inverse de b dans $\mathbf{Z}/p^n\mathbf{Z}$ et $c \in \mathbf{Z}$ dont la réduction modulo p^n est $\overline{c}$. On a alors $v_p(r - ac) = v_p(a) - v_p(b) + v_p(1 - bc) \geqslant n$ et donc $v_p(x - ac) \geqslant n$, ce qui prouve que ac a pour image $\overline{x}$ dans $\mathbf{Z}_p/p^n\mathbf{Z}_p$, et permet de conclure.

• L'application ι, qui à $x \in \mathbf{Z}_p$ associe la suite de ses réductions modulo p^n, est un isomorphisme d'anneaux de $\mathbf{Z}_p$ sur la *limite projective* [123] $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ des $\mathbf{Z}/p^n\mathbf{Z}$.

L'inclusion $p^n\mathbf{Z} \subset p^{n-1}\mathbf{Z}$, induit un morphisme d'anneaux $\pi_n : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{Z}/p^{n-1}\mathbf{Z}$, surjectif. Si $x \in \mathbf{Z}_p$, la réduction x_n de x modulo p^n peut être vue comme un élément de $\mathbf{Z}/p^n\mathbf{Z}$ d'après le point précédent, et on a $\pi_n(x_n) = x_{n-1}$. Il en résulte que l'application ι est un

123. Si $(\mathrm{X}_n)_{n\in\mathbf{N}}$ est une suite d'ensembles munis d'applications $\pi_n : \mathrm{X}_n \to \mathrm{X}_{n-1}$, pour $n \geqslant 1$, on définit la *limite projective* $\varprojlim \mathrm{X}_n$ des X_n (relativement aux π_n) comme le sous-ensemble de $\prod_{n\in\mathbf{N}} \mathrm{X}_n$ des suites $(x_n)_{n\in\mathbf{N}}$, avec $x_n \in \mathrm{X}_n$ et $\pi_n(x_n) = x_{n-1}$, si $n \geqslant 1$.

morphisme d'anneaux de $\mathbf{Z}_p$ dans $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$. Si $x \in \operatorname{Ker}\iota$, on a $x \in p^n\mathbf{Z}_p$ et donc $|x|_p \leqslant p^{-n}$, pour tout $n \in \mathbf{N}$, ce qui implique $x = 0$ et prouve que ι est injectif. Si $(y_n)_{n\in\mathbf{N}} \in \varprojlim \mathbf{Z}/p^n\mathbf{Z}$ et si $\hat{y}_n$ est un relèvement de y_n dans $\mathbf{Z}_p$, alors $\hat{y}_{n+1} - \hat{y}_n \in p^n\mathbf{Z}_p$ puisque $\pi_{n+1}(y_{n+1}) = y_n$; la suite $(\hat{y}_n)_{n\in\mathbf{N}}$ a donc une limite y dans $\mathbf{Z}_p$ et, par construction, $y - \hat{y}_n \in p^n\mathbf{Z}_p$, pour tout $n \in \mathbf{N}$; autrement dit, $\iota(y) = (y_n)_{n\in\mathbf{N}}$, d'où la surjectivité de ι.

• Le point précédent permet de définir $\mathbf{Z}_p$, algébriquement [124], comme étant $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$, et comme $\mathbf{Q}_p = \mathbf{Z}_p[\frac{1}{p}]$, cela fournit une définition algébrique de $\mathbf{Q}_p$.

20.4.3. *Topologie de* $\mathbf{Q}_p$

• Tout élément de $\mathbf{Q}_p$ peut s'écrire de manière unique sous la forme $x = \sum_{i=-k}^{+\infty} a_i p^i$, avec $a_i \in \{0, \dots, p-1\}$ pour tout i. Il admet donc une unique *écriture en base p*

$$x = \dots a_{n-1} \dots a_0, a_{-1} \dots a_{-k}\,,$$

et on a $|x|_p = p^k$, si $a_{-k} \neq 0$. Une différence avec les nombres réels est qu'il y a une infinité de chiffres avant la virgule et un nombre fini après. Les éléments de $\mathbf{Z}_p$ sont ceux dont l'écriture en base p n'a pas de chiffre après la virgule (du point de vue de l'écriture en base p, ils correspondent au segment $[0, 1]$ de $\mathbf{R}$).

Si $n \in \mathbf{N}$, alors $\{0, \dots, p^n - 1\}$ est un système de représentants de $\mathbf{Z}/p^n\mathbf{Z}$. Soit alors $x \in \mathbf{Q}_p^*$, et soit $k = -v_p(x)$ de telle sorte que $y = p^k x \in \mathbf{Z}_p^*$. Si $n \geqslant -k$, soit $y_n \in \{0, \dots, p^{n+k} - 1\}$ le représentant de l'image de y dans $\mathbf{Z}_p/p^{n+k}\mathbf{Z}_p \cong \mathbf{Z}/p^{n+k}\mathbf{Z}$ (en particulier, $y_{-k} = 0$ et $y_{1-k} \neq 0$, car $y \notin p\mathbf{Z}_p$). Alors $y_{n+1} - y_n$ est divisible par p^{n+k}, ce qui permet de définir $a_n \in \{0, \dots, p-1\}$ par $a_n = p^{-n-k}(y_{n+1} - y_n)$. On a alors $y_n = \sum_{i=0}^{n+k-1} a_{i-k} p^i$; autrement dit, $a_{n-1}a_{n-2} \dots a_{-k}$ est l'écriture de y_n en base p. Par suite, $a_{n-1} \dots a_0, a_{-1} \dots a_{-k}$ est l'écriture de $x_n = p^{-k} y_n$ en base p. Or $y_n - p^k x \in p^{n+k}\mathbf{Z}_p$ par construction, ce qui se traduit par $|y_n - p^k x|_p \leqslant p^{-(n+k)}$, ou encore par $|x_n - x|_p \leqslant p^{-n}$, et montre que $x_n \to x$ dans $\mathbf{Q}_p$. On a donc $x = \sum_{i=-k}^{+\infty} a_i p^i$ (la somme converge puisque son terme général tend vers 0). On en déduit l'existence d'une écriture sous la forme voulue.

Pour démontrer l'unicité, il suffit de constater que si $\sum_{i=-k}^{+\infty} a_i p^i = \sum_{i=-k}^{+\infty} b_i p^i$, alors en multipliant les deux membres par p^k, et en regardant modulo $p\mathbf{Z}_p$, on obtient $a_{-k} - b_{-k} \in p\mathbf{Z}_p$. Comme les a_i et les b_i sont dans un système de représentants modulo $p\mathbf{Z}_p$, cela prouve que $a_{-k} = b_{-k}$. Une récurrence immédiate permet d'en déduire que $a_i = b_i$ pour tout i. Le reste découle de la manière dont les a_i ont été construits ci-dessus.

124. On dit que $\mathbf{Z}_p$ est le complété de $\mathbf{Z}$ pour la topologie (p)-adique. Cette construction est un cas particulier d'une construction générale permettant d'analytifier beaucoup d'objets algébriques : si A est un anneau et si I est un idéal de A, on peut définir le complété $\widehat{\mathrm{A}}$ de A pour la topologie I-adique (un cas particulier de cette construction (cf. note 1 du chap. V) est l'anneau K[[T]] des séries entières qui est obtenu à partir de K[T] en complétant pour la topologie (T)-adique ; c'est d'ailleurs par analogie avec cette situation que Hensel a été amené à la construction des nombres p-adiques). De manière précise, si $n \in \mathbf{N}$, on définit l'idéal I^n de A comme l'ensemble des sommes de produits de n éléments de A (on a $\mathrm{I}^0 = \mathrm{A}$ par convention). On a $\mathrm{I}^n \subset \mathrm{I}^{n-1}$ et l'identité de A induit un morphisme (surjectif) d'anneaux $\pi_n : \mathrm{A}/\mathrm{I}^n \to \mathrm{A}/\mathrm{I}^{n-1}$. On définit $\widehat{\mathrm{A}}$ comme la limite projective $\varprojlim \mathrm{A}/\mathrm{I}^n$ des A/I^n (relativement aux morphismes π_n), et on dispose d'une application naturelle $\iota : \mathrm{A} \to \widehat{\mathrm{A}}$ qui n'est pas forcément injective (par exemple, si $\mathrm{I} = \mathrm{A}$, alors $\widehat{\mathrm{A}} = 0$).

• $\mathbf{N}$ et $\mathbf{Z}$ sont denses dans $\mathbf{Z}_p$ et $\mathbf{Z}[\frac{1}{p}]$ est dense dans $\mathbf{Q}_p$.

Cela résulte de l'existence de l'écriture en base p d'un nombre p-adique (si on coupe cette écriture au n-ième chiffre avant la virgule, on obtient un élément x de $\mathbf{N}$ (resp. $\mathbf{Z}[\frac{1}{p}]$), si on est parti d'un élément de $\mathbf{Z}_p$ (resp. $\mathbf{Q}_p$), et la suite de nombres ainsi obtenue converge vers x).

• $\mathbf{Z}_p$ est compact.

$\mathbf{Z}_p = \varprojlim (\mathbf{Z}/p^n\mathbf{Z})$ est un fermé de $\prod_{n\in\mathbf{N}}(\mathbf{Z}/p^n\mathbf{Z})$ qui est compact en tant que produit de compacts [et même en tant que produit dénombrable de compacts métriques car les $\mathbf{Z}/p^n\mathbf{Z}$ sont discrets, et donc métrisables (ex. 11.2)]. On aurait aussi pu, si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{Z}_p$, construire, par extraction diagonale, une sous-suite $(x_{\varphi_n(n)})$ telle que les k premiers termes du développement en base p de $x_{\varphi_n(n)}$ ne dépendent pas de n, si $n \geqslant k$; la suite extraite converge alors vers l'élément de $\mathbf{Z}_p$ dont les k premiers termes développement en base p sont les mêmes que ceux de $x_{\varphi_k(k)}$, pour tout $k \in \mathbf{N}$.

• $\mathbf{Q}_p$ est localement compact.

Une boule ouverte $\mathrm{B}(a, r^-)$ de $\mathbf{Q}_p$ est aussi de la forme $a + p^n\mathbf{Z}_p$, où n est le plus grand élément de $\mathbf{Z}$ tel que $p^{-n} < r$. Elle est donc homéomorphe à $\mathbf{Z}_p$, et la compacité de $\mathbf{Z}_p$ permet de conclure.

20.4.4. *Une description arboricole des nombres p-adiques*

La figure 4 ci-après fournit une description de $\mathbf{Z}_2$ comme limite (projective) des $\mathbf{Z}/2^n\mathbf{Z}$:

• Les éléments de $\mathbf{Z}_2$ correspondent aux bouts des branches de l'arbre infini (pour obtenir une description analogue de $\mathbf{Z}_p$, il suffit de remplacer l'arbre de la figure par un arbre dans lequel il part, de chacun des noeuds, p branches, numérotées de 0 à $p-1$, au lieu de 2).

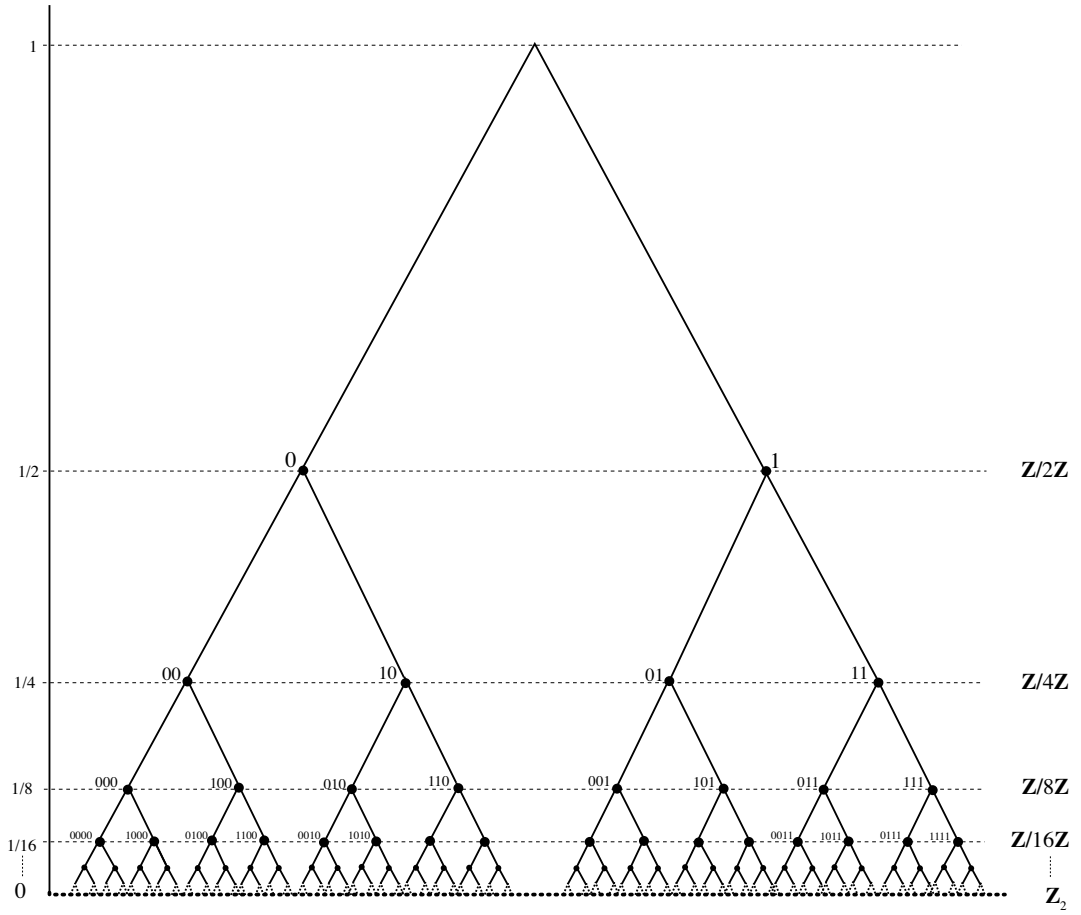


FIGURE 4. L'arbre des entiers 2-adiques.

• Les ensembles $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, etc. sont identifiés à $\{0,1\}$, $\{0,1,2,3\}$, etc., mais les nombres sont tous écrits en base 2 (si on prend la ligne correspondant à $\mathbf{Z}/8\mathbf{Z}$, ces nombres apparaissent dans l'ordre $0,4,2,6,1,5,3,7$).

• On passe (en montant) de la ligne correspondant à $\mathbf{Z}/2^n\mathbf{Z}$ à celle correspondant à $\mathbf{Z}/2^{n-1}\mathbf{Z}$ en supprimant le premier chiffre du développement en base 2 (celui correspondant à 2^{n-1} dans ce développement), ce qui représente la réduction modulo 2^{n-1} de $\mathbf{Z}/2^n\mathbf{Z}$ dans $\mathbf{Z}/2^{n-1}\mathbf{Z}$.

• Dans l'autre sens, les deux branches partant d'un noeud a de la ligne correspondant à $\mathbf{Z}/2^{n-1}\mathbf{Z}$ aboutissent aux deux classes a et $a+2^{n-1}$ modulo 2^n ; si l'écriture en base 2 de a est $a_{n-2}\dots a_0$, celles de a et $a+2^{n-1}$ sont respectivement $0a_{n-2}\dots a_0$ et $1a_{n-2}\dots a_0$. A la limite, on obtient donc l'écriture en base 2 de l'élément de $\mathbf{Z}_2$ correspondant à la branche infinie de l'arbre.

• La distance entre deux entiers 2-adiques x et y se lit aussi sur l'arbre : c'est la moitié de la hauteur verticale parcourue pour aller de x à y en suivant l'arbre (ou, de manière

équivalente, c'est la hauteur du noeud le plus bas appartenant aux branches de x et y). Par exemple, pour aller de 0 à -1, il faut remonter tout en haut, et donc la distance est 1 ; pour aller de $2 = \ldots 00010$ à $\frac{-2}{3} = \ldots 101010$, il faut passer par le noeud 010 et la distance est $\frac{1}{8}$.

20.4.5. *L'anneau des nombres complexes p-adiques*

• Si F est une extension finie de $\mathbf{Q}_p$, il existe une unique norme sur F dont la restriction à $\mathbf{Q}_p$ est $|\ |_p$.

Supposons que l'on en ait deux $|\ |_1$ et $|\ |_2$. Alors $|\ |_1$ et $|\ |_2$ sont deux normes sur le $\mathbf{Q}_p$-espace vectoriel F, de dimension finie, et comme $\mathbf{Q}_p$ est complet, $|\ |_1$ et $|\ |_2$ sont équivalentes. Il existe donc $C > 1$ tel que l'on ait $C^{-1}|a|_1 \leqslant |a|_2 \leqslant C|a|_1$ pour tout $a \in F$. En utilisant cet encadrement pour a^n, et en prenant les racines n-ièmes, cela permet de montrer, par un passage à la limite, que $|a|_1 = |a|_2$. D'où l'unicité.

On peut associer à $a \in F$ l'élément $\tilde{a}$ de $\mathrm{End}_{\mathbf{Q}_p}(F)$ correspondant à la multiplication par a. Nous allons vérifier que [125] $|a| = \|\tilde{a}\|_{\mathrm{sp}}$ convient, où $\|\ \|_{\mathrm{sp}}$ est la norme spectrale sur $\mathrm{End}_{\mathbf{Q}_p}(F)$. On choisit une norme $\|\ \|_0$ de $\mathbf{Q}_p$-espace vectoriel sur F (on peut par exemple prendre une base $e_1, \ldots, e_d$ de F sur $\mathbf{Q}_p$, et poser $\|\sum_{i=1}^d x_i e_i\|_0 = \sup_{1 \leqslant i \leqslant d} |x_i|_p$), et on note $\|\ \|$ la norme d'opérateur sur $\mathrm{End}_{\mathbf{Q}_p}(F)$ qui s'en déduit. On a alors $|a| = \lim \|\tilde{a}^n\|^{1/n}$.

• Si $a \in \mathbf{Q}_p$, on a $\|\tilde{a}\| = |a|_p$ car $\|ax\|_0 = |a|_p \|x\|_0$ pour tout $x \in F$, et donc $\|\tilde{a}\| = |a|_p$, ce qui fait que $|a| = \|\tilde{a}\|_{\mathrm{sp}} = \lim \|\tilde{a}^n\|^{1/n} = \lim |a^n|_p^{1/n} = |a|_p$.

• Comme a et b commutent, on a $\|(\tilde{a}\tilde{b})^n\| = \|\tilde{a}^n \tilde{b}^n\| \leqslant \|\tilde{a}^n\|\,\|\tilde{b}^n\|$; on en déduit l'inégalité $|ab| \leqslant |a|\,|b|$.

• De même (car $\left|\binom{n}{i}\right|_p \leqslant 1$), on a

$$\|(\tilde{a}+\tilde{b})^n\| \leqslant \sum_{0 \leqslant i \leqslant n} \|\tilde{a}^i\|\,\|\tilde{b}^{n-i}\| \leqslant (n+1)\sup(\|\tilde{a}\|^n, \|\tilde{b}\|^n)$$

on en déduit l'inégalité $|a+b| \leqslant \sup(|a|, |b|)$.

• L'ensemble des $u \in \mathrm{End}_{\mathbf{Q}_p}(F)$ tels que $p^{-1} \leqslant \|u\| \leqslant 1$ est fermé et borné ; il est donc compact puisque $\mathbf{Q}_p$ est localement compact. Son intersection S avec l'image de F par $a \mapsto \tilde{a}$ est donc aussi compacte puisque l'image de F est fermée dans $\mathrm{End}_{\mathbf{Q}_p}(F)$ car elle est complète en tant que $\mathbf{Q}_p$-espace vectoriel de dimension finie. Par ailleurs, $\|p^n u\| = p^{-n}\,\|u\|$ si $n \in \mathbf{Z}$ et $u \in \mathrm{End}_{\mathbf{Q}_p}(F)$; il existe donc $n \in \mathbf{Z}$ tel que $p^n \tilde{x} \in S$, si $x \in F^*$.

Maintenant, l'application $(u, v) \mapsto \|uv\|$ de $S \times S$ dans $\mathbf{R}$ est continue ; elle atteint donc son minimum C qui est strictement positif car $\|u\| = 0$ si et seulement si $u = 0$. On a alors $\|uv\| \geqslant C\|u\|\,\|v\|$ pour tous $u, v \in S$. Soient alors $a, b \in F^*$; il existe $i, j \in \mathbf{Z}$ tels que $p^i\tilde{a}, p^j\tilde{b} \in S$ et on a $\|\tilde{a}\tilde{b}\| = p^{i+j}\|p^i\tilde{a}p^j\tilde{b}\| \geqslant p^{i+j}C\|p^i\tilde{a}\|\,\|p^j\tilde{b}\| = C\,\|\tilde{a}\|\,\|\tilde{b}\|$. On peut appliquer ceci à a^n et b^n, ce qui nous donne $\|(\tilde{a}\tilde{b})^n\| \geqslant C\,\|\tilde{a}^n\|\,\|\tilde{b}^n\|$, quel que soit $n \in \mathbf{N}$. En prenant les racines n-ièmes et en passant à la limite, on en déduit l'inégalité $|ab| \geqslant |a|\,|b|$. Comme on a déjà démontré l'autre inégalité, on en déduit que $|ab| = |a|\,|b|$ pour tous $a, b \in F$ (le cas où $a = 0$ ou $b = 0$, non couvert par la discussion précédente, étant trivial).

• Enfin, l'équivalence « $|x| = 0 \Leftrightarrow x = 0$ » résulte des égalités $|xy| = |x|\,|y|$ et $|1| = 1$.

• Si $\overline{\mathbf{Q}}_p$ est une clôture algébrique de $\mathbf{Q}_p$, alors $|\ |_p$ a un unique prolongement à $\overline{\mathbf{Q}}_p$.

125. Nous encourageons le lecteur à examiner ce que donne ce procédé pour l'extension $\mathbf{C}/\mathbf{R}$.

Compte-tenu du point précédent, cela résulte des deux propriétés suivantes de $\overline{\mathbf{Q}}_p$:

• $\overline{\mathbf{Q}}_p$ est réunion d'extensions finies de $\mathbf{Q}_p$: si $\alpha \in \overline{\mathbf{Q}}_p$, alors $\mathbf{Q}_p(\alpha)$ est une extension finie de $\mathbf{Q}_p$ contenant α.

• Si $\mathrm{F}_1, \mathrm{F}_2$ sont deux extensions finies de $\mathbf{Q}_p$ contenues dans $\overline{\mathbf{Q}}_p$, il existe une extension finie F de $\mathbf{Q}_p$, contenue dans $\overline{\mathbf{Q}}_p$, et contenant F_1 et F_2 (cf. n° 8.1 du Vocabulaire).

• Si η est une racine de l'unité d'ordre une puissance de p, alors $|\eta - 1|_p < 1$.

$\eta - 1$ est racine du polynôme $(\mathrm{T}+1)^{p^n} - 1$ dont tous les coefficients a_i, pour $i \leqslant p^n - 1$, sont divisible par p et donc vérifient $|a_i|_p < 1$. Comme $(\eta-1)^{p^n} = -\sum_{i=0}^{p^n-1} a_i(\eta-1)^i$, on a $|\eta-1|_p^{p^n} < \sup_{i \leqslant p^n-1} |\eta-1|_p^i$. Il s'ensuit que l'on ne peut pas avoir $|\eta-1|_p \geqslant 0$.

Exercice 20.3. — (i) Soit $\rho_n = p^{-1/(p-1)p^{n-1}}$. Montrer que $|\eta-1|_p = \rho_n$, si η est une racine primitive p^n-ième de l'unité. (On pourra raisonner par récurrence sur n, en remarquant que $\eta - 1$ est racine du polynôme $\frac{(1+\mathrm{X})^p-1}{\mathrm{X}}$, si $n = 1$.)

(ii) En déduire que $\overline{\mathbf{Q}}_p$ est une extension infinie de $\mathbf{Q}_p$.

• On note $\mathbf{C}_p$ le complété de $\overline{\mathbf{Q}}_p$ pour la norme $|\ |_p$. Alors $\mathbf{C}_p$ est algébriquement clos.

Il s'agit de prouver que tout $\mathrm{P} \in \mathbf{C}_p[\mathrm{X}]$, unitaire, a un zéro dans $\mathbf{C}_p$. Pour cela, on prend $\mathrm{Q} \in \overline{\mathbf{Q}}_p[\mathrm{X}]$ dont les coefficients sont proches de ceux de P. Si $\alpha \in \overline{\mathbf{Q}}_p$ est un zéro de Q, alors $\mathrm{P}(\alpha)$ est petit, ce qui permet d'appliquer l'algorithme de Newton pour construire un zéro de P.

Le corps $\mathbf{C}_p$ qui est complet et algébriquement clos, est abstraitement isomorphe à $\mathbf{C}$. Le seul problème est que J. Tate (1966) a démontré que $\mathbf{C}_p$ ne contient pas d'analogue raisonnable de $2i\pi$, ce qui est un peu ennuyeux vu le rôle joué par $2i\pi$ dans le monde usuel (cf. la formule de Cauchy par exemple). Le problème a été résolu par J.-M. Fontaine (1982) qui a construit un anneau $\mathbf{B}_{\mathrm{dR}}^+$ (sa construction est assez compliquée...), l'anneau des *nombres complexes p-adiques*, qui contient un $2i\pi$ naturel, et qui est muni d'un morphisme d'anneaux surjectif $\theta : \mathbf{B}_{\mathrm{dR}}^+ \to \mathbf{C}_p$ dont le noyau est engendré par le $2i\pi$ de Fontaine (ce qui explique qu'on ne le voit pas dans $\mathbf{C}_p$).

20.4.6. *Fragments d'analyse p-adique*

L'analyse p-adique a, au moins au début, un petit côté paradisiaque quand on la compare à l'analyse réelle (la vie serait nettement plus agréable si on disposait d'une description de $\mathscr{C}([0,1], \mathbf{R})$ aussi simple que celle de $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ fournie par le théorème de Mahler ci-dessous).

Soit $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ l'ensemble des fonctions continues de $\mathbf{Z}_p$ dans $\mathbf{Q}_p$. Comme $\mathbf{Z}_p$ est compact, une fonction continue sur $\mathbf{Z}_p$ est bornée. Ceci permet de munir $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ de la norme $\|\ \|_\infty$ de la convergence uniforme, définie par $\|f\|_\infty = \sup_{x \in \mathbf{Z}_p} |f(x)|_p$. Une limite uniforme de fonctions continues étant continue, l'espace $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ est complet. Par ailleurs, la norme $\|\ \|_\infty$ vérifie l'inégalité ultramétrique $\|f+g\|_\infty \leqslant \sup(\|f\|_\infty, \|g\|_\infty)$; en effet, on a $|(f+g)(x)|_p \leqslant \sup(|f(x)|_p, |g(x)|_p)$, pour tout $x \in \mathbf{Z}_p$.

Si $n \in \mathbf{N}$, soit $\binom{x}{n}$ le *polynôme binomial*, défini par

$$\binom{x}{n} = \begin{cases} 1 & \text{si } n = 0 \\ \dfrac{x(x-1)\dots(x-n+1)}{n!} & \text{si } n \geqslant 1. \end{cases}$$

• $\|\binom{x}{n}\|_\infty = 1$.

On a $\binom{n}{n} = 1$ et donc $\|\binom{x}{n}\|_\infty \geqslant 1$. D'autre part, $\binom{k}{n}$ est le nombre de manières de choisir n objets parmi k et est donc entier. On en déduit que $|\binom{k}{n}|_p \leqslant 1$, pour tout $k \in \mathbf{N}$, et $\mathbf{N}$ étant dense dans $\mathbf{Z}_p$, cela implique que $|\binom{x}{n}|_p \leqslant 1$ quel que soit $x \in \mathbf{Z}_p$; d'où le résultat.

On définit la k-ième *dérivée discrète* $f^{[k]}$ d'une fonction f par récurrence à partir des formules $f^{[0]} = f$ et $f^{[k+1]}(x) = f^{[k]}(x+1) - f^{[k]}(x)$, et le k-ième *coefficient de Mahler* de f par $a_k(f) = f^{[k]}(0)$. On a aussi

$$f^{[k]}(x) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x+k-i) \quad \text{et} \quad a_k(f) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(k-i).$$

• Si k est un entier $\geqslant 1$, alors $\binom{p^k}{i}$ est divisible par p, si $1 \leqslant i \leqslant p^k - 1$.

En écrivant de deux manières la dérivée de $(1+\mathrm{X})^{p^k}$, on obtient $i\binom{p^k}{i} = p^k\binom{p^k-1}{i-1}$; on en déduit la divisibilité de $i\binom{p^k}{i}$ par p^k et celle de $\binom{p^k}{i}$ par p, si $1 \leqslant i \leqslant p^k - 1$.

• Si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$, il existe $k \in \mathbf{N}$ tel que $\|f^{[p^k]}\|_\infty \leqslant p^{-1}\|f\|_\infty$.

Comme $\mathbf{Z}_p$ est compact, f est uniformément continue et il existe $k \in \mathbf{N}$ tel que l'on ait $|f(x+p^k) - f(x)|_p \leqslant p^{-1}\|f\|_\infty$, quel que soit $x \in \mathbf{Z}_p$. Maintenant,

$$f^{[p^k]}(x) = f(x+p^k) - f(x) + \Big(\sum_{i=1}^{p^k-1} (-1)^i \binom{p^k}{i} f(x+p^k-i)\Big) + (1+(-1)^{p^k}) f(x).$$

Tous les termes de la somme $\sum_{i=1}^{p^k-1}$ ont, d'après le point précédent, une norme $\leqslant p^{-1}\|f\|_\infty$, et $(1+(-1)^{p^k})f(x)$ est nul si $p \neq 2$ et de norme $\leqslant p^{-1}\|f\|_\infty$ si $p = 2$. Comme on a choisi k de telle sorte que $|f(x+p^k) - f(x)|_p \leqslant p^{-1}\|f\|_\infty$ quel que soit $x \in \mathbf{Z}_p$, l'ultramétricité de $\| \ \|_\infty$ implique que $\|f^{[p^k]}\|_\infty \leqslant p^{-1}\|f\|_\infty$, ce qui permet de conclure.

Théorème 20.4. — (Mahler, 1958) *Si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$, alors*

(i) $\lim_{n\to+\infty} a_n(f) = 0$,

(ii) *f est la somme de la série $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$; en particulier, pour tout $x \in \mathbf{Z}_p$, on a $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n} = f(x)$.*

(iii) $\|f\|_\infty = \sup_{n\in\mathbf{N}} |a_n(f)|_p$.

Une utilisation répétée du point précédent permet de montrer que, si $f \in \mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ et si $\varepsilon > 0$, il existe $k \in \mathbf{N}$ tel que $\|f^{[p^k]}\|_\infty \leqslant \varepsilon$. Maintenant, si $n \geqslant p^k$, alors $a_n(f)$ est une combinaison linéaire à coefficients entiers des $f^{[p^k]}(i)$, avec $i \in \mathbf{N}$. On en déduit l'inégalité $|a_n(f)| \leqslant \|f^{[p^k]}\|_\infty$ si $n \geqslant p^k$, qui montre que $a_n(f) \to 0$ quand $n \to +\infty$; d'où le (i).

Il résulte du (i), de ce que $\|\binom{x}{n}\|_\infty = 1$, et de l'ultramétricité de $\| \ \|_\infty$, que la série $\sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$; notons g sa somme. Comme $\binom{x+1}{n+1} - \binom{x}{n+1} = \binom{x}{n}$, une récurrence immédiate nous fournit la formule $g^{[k]}(x) = \sum_{n=0}^{+\infty} a_{n+k}(f)\binom{x}{n}$, et on a donc $a_k(g) = g^{[k]}(0) = a_k(f)$, pour tout k. En revenant à la formule donnant $a_k(f)$ en fonction des valeurs de f sur $\mathbf{N}$, on en déduit que $f(k) = g(k)$, pour tout $k \in \mathbf{N}$; comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$ et f et g sont continues sur $\mathbf{Z}_p$, cela implique $f = g$, ce qui démontre le (ii).

Enfin, $\|f\|_\infty \leqslant \sup_{n\in\mathbf{N}} |a_n(f)|_p$ car $f = \sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ et $\|\binom{x}{n}\|_\infty = 1$, et $|a_n(f)|_p \leqslant \|f\|_\infty$ car $a_n(f)$ est une combinaison linéaire, à coefficients entiers des $\phi(k)$, pour $k \in \mathbf{N}$. On a donc $\|f\|_\infty \geqslant \sup_{n\in\mathbf{N}} |a_n(f)|_p$, ce qui permet de conclure.

Remarque 20.5. — On a démontré en passant que, si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{Q}_p$ tendant vers 0, alors $\sum_{n=0}^{+\infty} a_n\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ vers une fonction dont les coefficients de Mahler sont les a_n.

Exercice 20.6. — Si X, Y sont des espaces topologiques, on dit que $f : \mathrm{X} \to \mathrm{Y}$ est *localement constante* si tout $x \in \mathrm{X}$ admet un voisinage sur lequel f est constante.

(i) Montrer que f est localement constante si et seulement si $\{x \in \mathrm{X},\ f(x) = y\}$ est ouvert pour tout $y \in \mathrm{Y}$. En déduire qu'une fonction localement constante est continue.

(ii) Quelles sont les fonctions localement constantes sur $[0, 1]$?

(iii) Montrer que la fonction caractéristique $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ de $a + p^n\mathbf{Z}_p$ est localement constante pour tous $a \in \mathbf{Z}_p$ et $n \in \mathbf{N}$.

(iv) Montrer que, si $\phi : \mathbf{Z}_p \to \mathrm{Y}$ est localement constante, il existe $n \in \mathbf{N}$ tel que ϕ soit constante sur $a + p^n\mathbf{Z}_p$, pour tout $a \in \mathbf{Z}_p$.

(v) Montrer que, si $\mathrm{Y} = \mathbf{R}$ ou $\mathbf{Q}_p$, les fonctions localement constantes de $\mathbf{Z}_p$ dans Y sont denses dans les fonctions continues (munies de la norme de la convergence uniforme).

(vi) Construire une fonction continue surjective de $\mathbf{Z}_p$ sur $[0, 1]$. Quelles sont les fonctions continues de $[0, 1]$ dans $\mathbf{Z}_p$?

Exercice 20.7. — (i) Montrer que $\sum_{n=0}^{+\infty} \binom{1/2}{n}\left(\frac{7}{9}\right)^n$ converge vers $\frac{-4}{3}$ dans $\mathbf{Q}_7$. (On pourra considérer la fonction $x \mapsto \sum_{n=0}^{+\infty} \left(\frac{7}{9}\right)^n\binom{x}{n}$ et ses valeurs aux entiers.)

(ii) Quelle la somme de la série $\sum_{n=0}^{+\infty} \binom{1/2}{n}\left(\frac{7}{9}\right)^n$ dans $\mathbf{R}$?

21. Corrigé des exercices

Exercice 1.1. (i) Si $a = 0$ ou $b = 0$, on a $a\mathbf{Z} \cap b\mathbf{Z} = \{0\}$ et $\mathrm{ppcm}(a, b) = 0$ puisque le seul multiple de 0 est 0. Si $a \neq 0$ et $b \neq 0$, alors $a\mathbf{Z} \cap b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ comme intersection de deux sous-groupes, qui n'est pas réduit à 0 puisqu'il contient ab. Il existe donc $m \in \mathbf{N}$ tel que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$. Alors m est un multiple de a (car $a \in m\mathbf{Z}$) et de b (car $b \in m\mathbf{Z}$). Donc $\mathrm{ppcm}(a, b) \mid m$. Réciproquement, si c est un multiple de a et b, alors $c \in a\mathbf{Z}$ et $c \in b\mathbf{Z}$ et donc $c \in m\mathbf{Z}$ et $m \mid c$. En particulier, $m \mid \mathrm{ppcm}(a, b)$, et donc $m = \mathrm{ppcm}(a, b)$, ce qu'il fallait démontrer.

(ii) On a $a \mid c$ (resp. $b \mid c$) si et seulement si $v_p(a) \leqslant v_p(c)$ (resp. $v_p(b) \leqslant v_p(c)$), pour tout $p \in \mathscr{P}$. Donc c est un multiple de a et b si et seulement si $v_p(c) \geqslant \sup(v_p(a), v_p(b))$, pour tout $p \in \mathscr{P}$. Le plus petit entier multiple de a et b est donc $\prod_{p\in\mathscr{P}} p^{\sup(v_p(a),v_p(b))}$, ce qu'il fallait démontrer.

Exercice 1.2. (i) Si $a = 0$ ou $b = 0$, on a $v_p(ab) = v_p(a) + v_p(b)$ car les deux membres valent $+\infty$. Si $a \neq 0$ et $b \neq 0$, on a $a = \mathrm{sign}(a)\prod_{p\in\mathscr{P}} p^{v_p(a)}$, $b = \mathrm{sign}(b)\prod_{p\in\mathscr{P}} p^{v_p(b)}$ et

$$ab = \mathrm{sign}(ab)\prod_{p\in\mathscr{P}} p^{v_p(ab)} = \mathrm{sign}(a)\mathrm{sign}(b)\prod_{p\in\mathscr{P}} p^{v_p(a)+v_p(b)}.$$

On déduit de l'unicité de la décomposition en produit de facteurs premiers que $\mathrm{sign}(ab) = \mathrm{sign}(a)\mathrm{sign}(b)$ et $v_p(ab) = v_p(a) + v_p(b)$, pour tout $p \in \mathscr{P}$.

Maintenant, si $m = \inf(v_p(a), v_p(b))$, alors $p^m \mid a$ et $p^m \mid b$, ce qui implique $p^m \mid a + b$ et donc $v_p(a + b) \geqslant m$, ce qu'on cherchait à démontrer.

(ii) Si $x = \frac{a}{b}$, avec $a \in \mathbf{Z}$ et $b \in \mathbf{Z} - \{0\}$, on doit avoir $v_p(x) = v_p(a) - v_p(b)$, et il faut vérifier que cela ne dépend pas de l'écriture choisie. Or, si $\frac{a'}{b'} = \frac{a}{b}$, on a $ab' = ba'$ et donc $v_p(a) + v_p(b') = v_p(b) + v_p(a')$ et $v_p(a) - v_p(b) = v_p(a') - v_p(b')$, ce qui prouve que $v_p(x)$ est bien défini. De plus, si $y = \frac{c}{d}$, alors $v_p(xy) = v_p(\frac{ac}{bd}) = v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p(x) + v_p(y)$. Enfin, si $x, y \in \mathbf{Q}$ et si $c \in \mathbf{N} - \{0\}$ est tel que $cx, cy \in \mathbf{Z}$, on a $v_p(c(x+y)) \geqslant \inf(v_p(cx), v_p(cy))$ et donc

$$v_p(c) + v_p(x+y) \geqslant \inf(v_p(c) + v_p(x), v_p(c) + v_p(y)) = v_p(c) + \inf(v_p(x), v_p(y)),$$

et comme $v_p(c)$ est fini, cela permet de conclure.

(iii) Si $\sqrt{2}$ est rationnel, il existe $x \in \mathbf{Q}$ tel que $x^2 = 2$. On a alors $2v_2(x) = 1$, ce qui est impossible puisque $v_2(x) \in \mathbf{Z}$.

Exercice 1.3 (i) Quitte à échanger a et b, on peut supposer $v_p(a) < v_p(b)$. Alors $v_p(a+b) \geqslant v_p(a)$ puisque $\inf(v_p(a), v_p(b)) = v_p(a)$. Par ailleurs, on a $v_p(a) \geqslant \inf(v_p(a+b), v_p(b))$, puisque $a = (a+b) - b$, et comme $v_p(a) < v_p(b)$, cela nous donne $v_p(a) \geqslant v_p(a+b)$, d'où le résultat.

(ii) On peut ordonner les a_i de telle sorte que $v_p(a_1) < v_p(a_i)$ pour tout $i \geqslant 2$. Une récurrence immédiate utilisant le (i) montre qu'alors $v_p\big(\sum_{i=1}^k a_i\big) = v_p(a_1)$, pour tout k (et donc aussi pour $k = n$).

(iii) Il existe $k = \big[\frac{\log n}{\log 2}\big]$ tel que $2^k \leqslant n < 2^{k+1}$. Il existe alors un unique $i \leqslant n$ divisible par 2^k, à savoir 2^k. Il s'ensuit que le minimum de $v_2\big(\frac{1}{i}\big)$ est atteint une seule fois, pour $i = 2^k$, et vaut $-k$. Le (ii) montre alors que $v_2\big(1 + \frac{1}{2} + \cdots + \frac{1}{n}\big) = -k$; en particulier, $1 + \frac{1}{2} + \cdots + \frac{1}{n}$ n'est pas un entier.

Exercice 1.4. (i) On a $n! = \prod_{k=1}^n k$ et donc $v_p(n!) = \sum_{k=1}^n v_p(k)$. Or il y a exactement $[\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]$ entiers $\leqslant n$ vérifiant $v_p(k) = i$ (les multiples de p^i privés des multiples de p^{i+1}). On en déduit que $v_p(n!) = \sum_{i=1}^{+\infty} i\big([\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]\big) = \sum_{i=1}^{+\infty} [\frac{n}{p^i}](i - (i-1)) = \sum_{i=1}^{+\infty} [\frac{n}{p^i}]$.

Maintenant, si $n = a_0 + a_1 p + \cdots + a_r p^r$, où $a_i \in \{0, \ldots, p-1\}$, pour tout i, alors $[\frac{n}{p^i}] = a_i + \cdots + a_r p^{r-i}$ et donc

$$\begin{aligned}\sum_{i=1}^{+\infty} [\frac{n}{p^i}] &= \sum_{i=1}^{r} \big(\sum_{s=i}^{r} a_s p^{s-i}\big) = \sum_{s=1}^{r}\sum_{i=1}^{s} a_s p^{s-i} \\ &= \sum_{s=1}^{r} a_s p^{s-1}\big(\frac{1-p^{-s}}{1-p^{-1}}\big) = \sum_{s=1}^{r} a_s\big(\frac{p^s-1}{p-1}\big) = \sum_{s=0}^{r} a_s\big(\frac{p^s-1}{p-1}\big) = \frac{n - \mathrm{S}_p(n)}{p-1}.\end{aligned}$$

(ii) La fonction $x \mapsto [x] - \big[\frac{x}{2}\big] - \big[\frac{x}{3}\big] - \big[\frac{x}{5}\big] + \big[\frac{x}{30}\big]$ prend des valeurs entières. Par ailleurs, elle est aussi égale à $\big\{\frac{x}{2}\big\} + \big\{\frac{x}{3}\big\} + \big\{\frac{x}{5}\big\} - \big\{\frac{x}{30}\big\}$, ce qui montre qu'elle est périodique de période 30 et > -1 sur $[0, 30[$; elle est donc toujours $\geqslant 0$. L'intégralité de $a_n = \frac{(30n)!\, n!}{(15n)!\,(10n)!\,(6n)!}$ s'en déduit en calculant la valuation p-adique de a_n, pour tout p.

(iii) Comme $\binom{a+b}{a} = \frac{(a+b)!}{a!\,b!}$, on a, d'après ce qui précède, $v_p\big(\binom{a+b}{a}\big) = \frac{\mathrm{S}_p(a) + \mathrm{S}_p(b) - \mathrm{S}_p(a+b)}{p-1}$. Maintenant, faire une retenue dans une addition revient à écrire un 'chiffre' u sous la forme $1\,u-p$, ce qui fait passer la somme des chiffres de u à $1 + u - p$, et donc diminue la somme des chiffres de $p-1$. On en déduit le résultat.

(iv) Si $1 \leqslant i \leqslant p-1$, il y a une retenue dans l'addition de $i + (p-i)$ en base p, et donc $v_p\big(\binom{p}{i}\big) = 1$ et $\binom{p}{i}$ est divisible par p (cela peut se voir aussi en remarquant que $p!$ est divisible par p alors que $i!$ et $(p-i)!$ ne le sont pas car i et $p-i$ sont $< p$). Ceci permet de montrer (par récurrence montante ou descendante, le cas $n = 0$ étant trivial) que $n^p - n$, qui est égal à $(n-1+1)^p - (n-1) - 1 = (n-1)^p - (n-1) + \sum_{i=1}^{p-1} \binom{p}{i}(n-1)^i$, est divisible par p, ce que l'on voulait.

Exercice 1.5. L'ensemble $\mathscr{P}(\mathbf{N})$ est en bijection avec $\{0,1\}^{\mathbf{N}}$ (on associe à $\mathrm{X} \subset \mathbf{N}$ la suite $(x_k)_{k \in \mathbf{N}}$ définie par $x_k = 1$ si $k \in \mathrm{X}$ et $x_k = 0$ si $k \notin \mathrm{X}$) ; il n'est donc pas dénombrable.

L'ensemble des parties finies de $\mathbf{N}$ est la réunion, pour $n \in \mathbf{N}$, de l'ensemble des parties de $\{0, \ldots, n\}$; il est donc dénombrable en tant que réunion dénombrable d'ensembles finis. En fait, on peut donner une

bijection explicite de cet ensemble sur $\mathbf{N}$, à savoir l'application $\mathrm{I} \mapsto \sum_{i\in \mathrm{I}} 2^i$ (dans l'autre sens, n est envoyé sur son codage en base 2).

Exercice 1.6. Si n est fixé, l'ensemble $\mathbf{Q}[\mathrm{X}]^{(n)}$ des polynômes de $\mathbf{Q}[\mathrm{X}]$ de degré n s'injecte dans $\mathbf{Q}^{n+1}$ en envoyant $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0$ sur $(a_n, \ldots, a_0)$; il est donc dénombrable puisque $\mathbf{Q}$ l'est. On en déduit que $\mathbf{Q}[\mathrm{X}] = \cup_{n\in\mathbf{N}}\mathbf{Q}[\mathrm{X}]^{(n)}$ est dénombrable comme réunion dénombrable d'ensembles dénombrables. Enfin, un polynôme n'ayant qu'un nombre fini de racines dans $\mathbf{C}$, l'ensemble $\overline{\mathbf{Q}}$ est une réunion dénombrable (d'après ce qui précède) d'ensembles finis, et donc est dénombrable.

L'ensemble des nombres transcendants n'est pas dénombrable (sinon $\mathbf{R}$ le serait comme réunion de deux ensembles dénombrables) ; en particulier, il est non vide.

Exercice 1.7. Si on choisit dans chaque disque un point de la forme $a + ib$, avec $a, b \in \mathbf{Q}$, on obtient une injection de I dans $\mathbf{Q}^2$, et comme $\mathbf{Q}^2$ est dénombrable puisque $\mathbf{Q}$ l'est, cela permet de conclure.

Exercice 1.8. (i) Soit $a = \inf_{x>x_0} f(x)$. Par définition de a, on a $f(x) \geqslant a$, si $x > x_0$, et pour tout $\varepsilon > 0$, il existe $x_\varepsilon > x_0$ tel que $f(x_\varepsilon) < a + \varepsilon$. Soit $\delta = x_\varepsilon - x_0$. Comme f est croissante, on a $a \leqslant f(x) < a + \varepsilon$, pour tout $x \in]x_0, x_0 + \delta[$, ce qui prouve que f a une limite à droite $f(x_0^+)$ en x_0, égale à a. La limite à gauche s'étudie exactement de la même manière (ou peut se déduire de ce qu'on vient de faire en étudiant $g(x) = -f(-x)$ en $-x_0$).

Maintenant, comme f est croissante, on a $f(x_0^-) = \sup_{x<x_0} f(x) \leqslant f(x_0) \leqslant \inf_{x>x_0} f(x) = f(x_0^+)$. Comme f admet des limites à gauche et à droite en x_0, elle est continue en x_0 si et seulement si $f(x_0^-) = f(x_0) = f(x_0^+)$, et donc si et seulement si $f(x_0^-) = f(x_0^+)$.

(ii) Comme f est croissante, on a $f(x_0^+) = \inf_{x>x_0} f(x) = \inf_{x_1>x>x_0} f(x) \leqslant \sup_{x_0<x<x_1} f(x) = \sup_{x<x_1} f(x) = f(x_1^-)$.

(iii) Soit $x \in \mathrm{D}$ un point de discontinuité. On a alors $f(x^-) < f(x^+)$, ce qui permet de choisir un élément $r(x) \in \mathbf{Q}$ dans l'intervalle $]f(x^-), f(x^+)[$. Si $x_1 < x_2$ sont deux éléments de D, on a $r(x_1) < f(x_1^+) \leqslant f(x_2^-) < r(x_2)$, ce qui prouve que $x \mapsto r(x)$ est une injection de D dans $\mathbf{Q}$, et $\mathbf{Q}$ étant dénombrable, cela implique que D est dénombrable.

Exercice 1.9. Par construction, la suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ est alternée ; l'intersection des $[x_{\varphi(n)}, x_{\varphi(n+1)}]$ (ou $[x_{\varphi(n+1)}, x_{\varphi(n)}]$) est donc un intervalle $[a, b]$, et il s'agit de prouver qu'il est réduit à un point pour prouver que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ a une limite. Si ce n'est pas le cas, il existe $i \in \mathbf{N}$ tel que $x_i \in [a, b]$, et il existe $n \in \mathbf{N}$ tel que $\varphi(n) < i < \varphi(n+1)$. Alors x_i est entre $x_{\varphi(n)}$ et $x_{\varphi(n-1)}$, ce qui est contraire à la définition de $\varphi(n+1)$. Si la limite de $(x_{\varphi(n)})_{n\in\mathbf{N}}$ appartient à X, alors cette limite est de la forme x_i, et si $\varphi(n) < i < \varphi(n+1)$, on aboutit, comme ci-dessus, à une contradiction avec la définition de $\varphi(n+1)$. La limite n'appartient donc pas à X.

Maintenant, si $\mathbf{R}$ était dénombrable, on pourrait lui appliquer ce qui précède et construire un élément de $\mathbf{R}$ n'appartenant pas à $\mathbf{R}$...

Exercice 1.10. Soit $(\mathrm{H}_i)_{i\in\mathrm{I}}$ une famille de huit dans le plan, deux à deux disjoints. Si H_i est constitué des cercles $\mathrm{C}_{i,1}$ et $\mathrm{C}_{i,2}$, choisissons un point $\mathrm{P}_{i,1}$ (resp. $\mathrm{P}_{i,2}$) à coordonnées rationnelles dans le disque $\mathrm{D}_{i,1}$ (resp. $\mathrm{D}_{i,2}$) délimité par $\mathrm{C}_{i,1}$ (resp. $\mathrm{C}_{i,2}$). On obtient de la sorte une application de I dans $\mathbf{Q}^4$. Soient $i \neq j$ deux éléments de I. Si $\mathrm{P}_{i,1} = \mathrm{P}_{j,1}$, alors l'un des disques $\mathrm{D}_{i,1}$ et $\mathrm{D}_{j,1}$ contient l'autre puisque les cercles $\mathrm{C}_{i,1}$ et $\mathrm{C}_{j,1}$ sont disjoints. Quitte à permuter i et j, on peut supposer que c'est $\mathrm{D}_{i,1}$ qui contient $\mathrm{D}_{j,1}$, mais alors $\mathrm{D}_{i,1}$ contient aussi le point de contact entre $\mathrm{C}_{j,1}$ et $\mathrm{C}_{j,2}$, et donc aussi le cercle $\mathrm{C}_{j,2}$ tout entier puisque $\mathrm{C}_{j,2}$ et $\mathrm{C}_{i,1}$ sont disjoints, et donc aussi le disque $\mathrm{D}_{j,2}$ et le point $\mathrm{P}_{j,2}$. Comme il ne contient pas $\mathrm{P}_{i,2}$ par construction, on en déduit que $i \mapsto (\mathrm{P}_{i,1}, \mathrm{P}_{i,2})$ est injective, et comme $\mathbf{Q}^4$ est dénombrable, il en est de même de I.

Exercice 1.11. L'idée est de prouver que deux tripodes disjoints ne peuvent pas être trop proches. Soient donc Y et Y′ deux tripodes de sommets respectifs $(\mathrm{A}, \mathrm{B}, \mathrm{C})$ et $(\mathrm{A}', \mathrm{B}', \mathrm{C}')$ et de centres de gravité G

et G′. Soit $r = d(\mathrm{G}, \mathrm{A})$. Si $d(\mathrm{A}, \mathrm{A}')$, $d(\mathrm{B}, \mathrm{B}')$ et $d(\mathrm{C}, \mathrm{C}')$ sont toutes trois $< \frac{r}{2}$, on a aussi $d(\mathrm{G}, \mathrm{G}') < \frac{r}{2}$ et un petit dessin montre que suivant le tiers de plan dans lequel se trouve G′, l'un des segments $[\mathrm{G}', \mathrm{A}']$, $[\mathrm{G}', \mathrm{B}']$ ou $[\mathrm{G}', \mathrm{C}']$ rencontre Y. Maintenant, soit $(\mathrm{Y}_i)_{i\in\mathrm{I}}$ une famille de tripodes dans le plan, deux à deux disjoints. Si $i \in \mathrm{I}$, soient $\mathrm{A}_i, \mathrm{B}_i, \mathrm{C}_i$ les sommets de Y_i, G_i le centre de gravité de $(\mathrm{A}_i, \mathrm{B}_i, \mathrm{C}_i)$ et $r_i = d(\mathrm{G}_i, \mathrm{A}_i)$. Choisissons pour tout i un triplet $(\mathrm{P}_{i,1}, \mathrm{P}_{i,2}, \mathrm{P}_{i,3})$ de points à coordonnées rationnelles, avec $d(\mathrm{A}_i, \mathrm{P}_{i,1}) < \frac{r_i}{4}$, $d(\mathrm{B}_i, \mathrm{P}_{i,2}) < \frac{r_i}{4}$ et $d(\mathrm{C}_i, \mathrm{P}_{i,3}) < \frac{r_i}{4}$. Il résulte de la discussion préliminaire que l'on obtient ainsi une injection de I dans $\mathbf{Q}^6$, ce qui prouve que I est dénombrable.

Exercice 2.1. (i) Si $x^m = 0$ et $y^m = 0$, alors $(x+y)^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} x^{2m-k} y^k = 0$ car $2m-k$ ou k est $\geqslant m$, et donc $x^{2m-k} = 0$ ou $y^k = 0$. Le résultat n'est plus vrai, en général, si x et y ne commutent pas : les matrices $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ sont nilpotentes, mais leur somme $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ ne l'est pas [elle est même inversible puisque son carré est $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$].

(ii) Si a et x commutent, on montre, par récurrence sur n, que a commute à x^n, et que $(ax)^n = a^n x^n$; on a donc $(ax)^m = 0$ si $x^m = 0$, et donc ax est nilpotent si x l'est. Le résultat n'est plus vrai, en général, si a et x ne commutent pas : la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ est nilpotente, mais pas $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ qui est égale à $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

(iii) C'est une traduction des (i) et (ii) puisque tout commute.

Exercice 2.2. (i) On a $\left(\begin{smallmatrix} a_1 & b_1 \\ -\overline{b}_1 & \overline{a}_1 \end{smallmatrix}\right) - \left(\begin{smallmatrix} a_2 & b_2 \\ -\overline{b}_2 & \overline{a}_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right)$, avec $a = a_1 - a_2$ et $b = b_1 - b_2$, et donc $\mathbf{H}$ est un sous-groupe de $(\mathbf{M}_2(\mathbf{C}), +)$. Par ailleurs $\mathbf{H}$ contient $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} a_1 & b_1 \\ -\overline{b}_1 & \overline{a}_1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a_2 & b_2 \\ -\overline{b}_2 & \overline{a}_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right)$, avec $a = a_1 a_2 - b_1 \overline{b}_2$ et $b = a_1 b_2 + b_1 \overline{a}_2$, ce qui prouve que $\mathbf{H}$ est stable par multiplication, et donc est un sous-anneau de $\mathbf{M}_2(\mathbf{C})$. Enfin, l'inverse de $\left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right)$ est $\frac{1}{|a|^2+|b|^2}\left(\begin{smallmatrix} \overline{a} & -\overline{b} \\ b & a \end{smallmatrix}\right)$, si $(a,b) \neq (0,0)$; il s'ensuit que tout élément non nul de $\mathbf{H}$ a un inverse dans $\mathbf{H}$, et donc que $\mathbf{H}$ est un corps. Il n'est pas commutatif car $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$.

(ii) Si $x = \left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right)$, alors $x^2 = \left(\begin{smallmatrix} a^2-|b|^2 & b(a+\overline{a}) \\ -\overline{b}(a+\overline{a}) & \overline{a}-|b|^2 \end{smallmatrix}\right)$, et $x^2+1 = 0$ équivaut à $a^2 - |b|^2 = -1$ et $b(a+\overline{a}) = 0$. Si $b = 0$, cela nous donne $a = \pm i$, et si $b \neq 0$, cela implique que a est imaginaire pur ; donc dans tous les cas $a = i\alpha$, avec $\alpha \in \mathbf{R}$. Si $b = \beta + i\gamma$, avec $\beta, \gamma, \in \mathbf{R}$, on voit que $x^2+1 = 0$ équivaut $\alpha^2 + \beta^2 + \gamma^2 = 1$. L'ensemble des solutions de l'équation $x^2+1 = 0$ est donc en bijection avec la sphère de rayon 1 de $\mathbf{R}^3$; en particulier, il est infini, ce qui est un peu surprenant pour une équation du second degré.

Exercice 2.3. Soit $m = \mathrm{ppcm}(a, b)$. Comme a et b ne sont pas premiers entre eux, on a $m < |ab|$. Or m annule tout élément de $\mathbf{Z}/a\mathbf{Z}$ puisque c'est un multiple de a et tout élément de $\mathbf{Z}/b\mathbf{Z}$ puisque c'est un multiple de b ; on a donc $mx = 0$, pour tout $x \in (\mathbf{Z}/a\mathbf{Z}) \oplus (\mathbf{Z}/b\mathbf{Z})$. Or m n'annule pas 1 dans $\mathbf{Z}/ab\mathbf{Z}$ puisque $m < |ab|$ n'est pas un multiple de ab.

Exercice 2.4. 4 admet 16 comme inverse dans $\mathbf{Z}/21\mathbf{Z}$; l'équation $4x + 3 = 0$ est donc équivalente à $x + 48 = 0$, soit $x = -48 = 3 \times 21 - 48 = 15$.

$14x$ est multiple de 7 dans $\mathbf{Z}/21\mathbf{Z}$, ce que -2 n'est pas. L'équation $14x+2 = 0$ n'a donc pas de solution dans $\mathbf{Z}/21\mathbf{Z}$.

$14x+7 = 0$ dans $\mathbf{Z}/21\mathbf{Z}$ équivaut à $7(2x+1) = 0$ dans $\mathbf{Z}/21\mathbf{Z}$, soit encore à $2x+1$ multiple de 3 dans $\mathbf{Z}/21\mathbf{Z}$. Les solutions sont donc 1, 4, 7, 10, 13, 16 et 19 modulo 21.

Exercice 2.5. On a $91 = 7 \times 13$ et donc $\mathbf{Z}/91\mathbf{Z} = \mathbf{F}_7 \times \mathbf{F}_{13}$, ce qui nous ramène à trouver les solutions dans les corps $\mathbf{F}_7$ et $\mathbf{F}_{13}$. On remarque que 2 est racine dans $\mathbf{F}_7$, et comme la somme des racines vaut -1, l'autre est $-3 = 4$. De même 3 est racine dans $\mathbf{F}_{13}$, et donc l'autre est $-1-3 = -4 = 9$. On est alors confronté au problème de trouver quels sont les éléments de $\mathbf{Z}/91\mathbf{Z}$ correspondant aux couples $(2,3)$, $(2,9)$, $(4,3)$ et $(4,9)$ de $\mathbf{F}_7 \times \mathbf{F}_{13}$. Pour cela, on remarque que $1 = 2 \times 7 - 13$, et donc que $14 = 2 \times 7$ a pour image 0 dans $\mathbf{F}_7$ et pour image 1 dans $\mathbf{F}_{13}$, alors que -13 a pour image 1 dans $\mathbf{F}_7$ et pour image 0 dans $\mathbf{F}_{13}$. On en déduit, que si $(a,b) \in \mathbf{Z}$, alors $-13a + 14b \in \mathbf{Z}$ ne dépend modulo 91 que des réductions de a et b modulo 7 et 13 respectivement, et l'image de $-13a+14b$ dans $\mathbf{F}_7 \times \mathbf{F}_{13}$ est (a,b). Les solutions

de l'équation $x^2+x+1=0$ dans $\mathbf{Z}/91\mathbf{Z}$ sont donc $-13\cdot 2+14\cdot 3=16$, $-13\cdot 2+14\cdot 9=100=9$, $-13\cdot 4+14\cdot 3=-10$ et $-13\cdot 4+14\cdot 9=74=-17$.

Exercice 2.6. (i) Si a est solution de l'équation $x^2+x+1=0$, alors $-1-a$ aussi. Or le système d'équations $x^2+x+1=0$ et $2x=-1$ est équivalent à $2x=-1$ et $x(x-1)=0$. Comme $\mathbf{F}_p$ est un corps, $x(x-1)=0$ équivaut à $x=0$ ou $x=1$, ce qui est incompatible avec $2x=-1$, sauf si $2\cdot 1=-1$, c'est-à-dire si $3=0$, et donc si $p=3$. On en déduit que, si $p\neq 3$, l'équation $x^2+x+1=0$ a deux solutions dans $\mathbf{F}_p$ si et seulement si elle en a au moins une.

(ii) D'après le (i), si $p\neq 3$, l'équation $x^2+x+1=0$ a deux solution modulo p, s'il existe $n\in\mathbf{N}$ tel que p divise n^2+n+1. Supposons, par l'absurde, que l'ensemble des p vérifiant ceci est fini. Cela signifie qu'il existe des nombres premiers $p_1,\cdots,p_k$ tels que pour tout $n\in\mathbf{N}$, il existe $a_1,\ldots,a_k\in\mathbf{N}$ tels que $n^2+n+1=p_1^{a_1}\cdots p_k^{a_k}$. Si $n\leqslant \mathrm{X}-1$, cela implique que $n^2+n+1\leqslant \mathrm{X}^2$, et donc que chacun des a_i vérifie $a_i\leqslant \frac{\log \mathrm{X}^2}{\log p_i}\leqslant \frac{2}{\log 2}\log \mathrm{X}$; on en déduit que n^2+n+1 peut prendre au plus $(\frac{2}{\log 2}\log \mathrm{X})^k$ valeurs pour $n\leqslant \mathrm{X}-1$, ce qui est absurde pour X tendant vers $+\infty$, les valeurs de n^2+n+1 étant toutes distinctes pour $n\geqslant 0$.

(iii) Il existe un ensemble infini $\{p_1,p_2,\ldots\}$ de nombres premiers tels que l'équation $x^2+x+1=0$ ait deux solutions dans $\mathbf{F}_p$. Soit $\mathrm{D}_k=p_1\cdots p_k$. D'après le théorème des restes chinois, $\mathbf{Z}/\mathrm{D}_k\mathbf{Z}=\prod_{i=1}^k \mathbf{F}_{p_i}$, et comme l'équation $x^2+x+1=0$ a deux solutions dans $\mathbf{F}_{p_i}$, pour tout i, elle en a 2^k dans $\mathbf{Z}/\mathrm{D}_k\mathbf{Z}$. Comme 2^k peut être rendu arbitrairement grand, cela permet de conclure.

Exercice 2.7. Si cet ensemble est fini, constitué de $p_1,\ldots,p_r$, tous les diviseurs de $4p_1\cdots p_r-1$ sont de la forme $4n+1$, ce qui conduit à une contradiction en regardant modulo 4.

Exercice 2.8. (i) Si $p_1^{a_1}\cdots p_r^{a_r}\leqslant x$, on a $a_i\leqslant \frac{\log x}{\log p_i}$. On en déduit que $|\mathrm{X}(p_1,\ldots,p_r,x)|\leqslant \frac{\log^r x}{\log p_1\cdots\log p_r}$, ce qui permet de conclure.

(ii) Si $p\mid (4k^2+1)$, alors p est impair, et $-1=(2k)^2$ dans $\mathbf{F}_p$. Comme $a^{p-1}=1$ pour tout $a\in\mathbf{F}_p^*$ (petit th. de Fermat), on en déduit que $(-1)^{(p-1)/2}=(2k)^{p-1}=1$, et donc que $\frac{p-1}{2}=2n$ et $p=4n+1$.

(iii) Si cet ensemble est fini, constitué de $p_1,\ldots,p_r$, l'ensemble $\mathrm{S}(x)$ des $4k^2+1$, avec $k\leqslant \frac{1}{2}\sqrt{x-1}$ est inclus dans $\mathrm{X}(p_1,\ldots,p_r,x)$. Or ceci est absurde puisque $|\mathrm{X}(p_1,\ldots,p_r,x)|=\mathrm{O}(\log^r x)$, d'après le (i), alors que $|\mathrm{S}(x)|\sim\frac{1}{2}\sqrt{x}$.

Exercice 2.9. Les éléments inversibles de $\mathbf{Z}/p^n\mathbf{Z}$ sont en bijection avec les éléments de $\{0,1,\ldots,p^n-1\}$ qui sont premiers à p^n. Or être premier à p^n est équivalent à être premier à p d'après le lemme de Gauss et donc aussi à ne pas être divisible par p, puisque p est premier. Comme il y a p^{n-1} multiples de p dans $\{0,1,\ldots,p^n-1\}$, on en déduit que $|(\mathbf{Z}/p^n\mathbf{Z})^*|=p^n-p^{n-1}$.

Maintenant, si $\mathrm{D}\geqslant 2$ est quelconque, on peut factoriser D sous la forme $\mathrm{D}=\prod_{p|\mathrm{D}}p^{n_p}$, avec $n_p\geqslant 1$, et le théorème des restes chinois nous dit que l'anneau $\mathbf{Z}/\mathrm{D}\mathbf{Z}$ est isomorphe à $\prod_{p|\mathrm{D}}(\mathbf{Z}/p^{n_p}\mathbf{Z})$. On a donc $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*=\prod_{p|\mathrm{D}}(\mathbf{Z}/p^{n_p}\mathbf{Z})^*$, ce qui nous donne

$$\varphi(\mathrm{D})=\prod_{p|\mathrm{D}}(p^{n_p}-p^{n_p-1})=\mathrm{D}\prod_{p|\mathrm{D}}\big(1-\frac{1}{p}\big).$$

Exercice 2.11. (i) Si $v_1=(x_1,y_1)$ et $v_2=(x_2,y_2)$ engendrent la même droite, il existe $\alpha\in\mathrm{K}^*$ tel que $v_2=\alpha v_1$, et on a $\lambda(v_2)=\frac{x_2}{y_2}=\frac{\alpha x_1}{\alpha y_1}=\frac{x_1}{y_1}=\lambda(v_1)$, ce qui prouve que $\lambda(v)$ ne dépend que de la droite engendrée par v, et donc que λ induit une application de $\mathbf{P}^1(\mathrm{K})$ dans $\mathrm{K}\cup\{\infty\}$. Cette application est injective car « $\lambda(v_1)=\lambda(v_2)$ » équivaut à « $x_1y_2=x_2y_1$ », et donc « à v_1 et v_2 colinéaires ». Elle est surjective car $(1,0)$ s'envoie sur ∞ et $(z,1)$ sur z, si $z\in\mathrm{K}$. C'est donc une bijection.

(ii) Soit $z\in\mathrm{K}\cup\{\infty\}$, et soit $v=(x,y)$ tel que $\frac{x}{y}=\lambda(v)=z$. Alors, par définition, $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\cdot z=\lambda\big(\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\cdot v\big)=\lambda(ax+by,cx+dy)=\frac{ax+by}{cx+dy}=\frac{az+b}{cz+d}$.

Exercice 2.13. (i) Une isométrie u du carré permute ses sommets et laisse fixe son centre de gravité O. En particulier u est linéaire et est déterminée par l'image de deux points non colinéaires avec O, par exemple A et B. L'image de A doit appartenir à $\{A, B, C, D\}$, et comme l'angle $\{u(A), O, u(B)\}$ doit être un angle droit, cela ne laisse que deux possibilités pour $u(B)$ pour chaque choix de $u(A)$. On en déduit que D_4 a au plus 8 éléments. Comme il contient l'identité id, la symétrie $-\mathrm{id}$ par rapport à O, les rotations ρ^+ et ρ^- de centre O et d'angles respectifs $\frac{\pi}{2}$ et $\frac{-\pi}{2}$, les symétries $\sigma_{A,C}$ et $\sigma_{C,D}$ par rapport aux deux diagonales, et les symétries σ_H et σ_V par rapport aux droites horizontale et verticale, on voit que D_4 a exactement 8 éléments qui sont ceux que nous venons d'énumérer.

(ii) S est de toute évidence stable par D_4, et il y a deux orbites :

• O est fixe par tout élément de D_4 ; son orbite est donc $\{O\}$ et son stablisateur est D_4 ;

• on passe de A à B, C et D en itérant ρ^+, ce qui montre que l'orbite de A est $\{A, B, C, D\}$ (elle ne peut contenir O puisque les orbites sont distinctes), et on détermine par inspection que le stabilisateur de A est le groupe à 2 éléments $\{\mathrm{id}, \sigma_{A,C}\}$.

(iii) Les orbites de T sous l'action de D_4 sont au nombre de 3 :

• l'orbite de $\{O, A\}$ consiste en les 4 paires contenant O (on passe de $\{O, A\}$ aux autres en itérant ρ^+), et le stabilisateur de $\{O, A\}$ est $\{\mathrm{id}, \sigma_{A,C}\}$;

• l'orbite de $\{A, B\}$ consiste en les 4 paires de sommets consécutifs (on passe de $\{A, B\}$ aux autres en itérant ρ^+), et le stabilisateur de $\{A, B\}$ est $\{\mathrm{id}, \sigma_V\}$;

• l'orbite de $\{A, C\}$ consiste en les 2 paires de sommets oppososés $\{A, C\}$ et $\{B, D\}$, et le stabilisateur de $\{A, C\}$ est $\{\mathrm{id}, -\mathrm{id}, \sigma_{A,C}, \sigma_{B,D}\}$.

(iv) On remarque que dans tous les cas, le produit du cardinal de l'orbite par celui du stablisateur d'un de ses éléments est $8 = |D_4|$; il s'agit d'un cas particulier d'un théorème général (si G opère sur X, si $x \in X$, et si G_x est le stabilisateur de x, alors l'orbite O_x est isomorphe à G/G_x, et donc $|O_x| = |G|/|G_x|$).

Exercice 2.14. (i) Les conditions $g \cdot x = x$ et $hgh^{-1} \cdot (h \cdot x) = h \cdot x$ sont équivalentes. Il en résulte que $x \mapsto h \cdot x$ induit une bijection de X_g sur $X_{hgh^{-1}}$, ce qui répond au (a). Le (b) s'en déduit puisque si g et g' sont conjugués dans G, il existe h tel que $g' = hgh^{-1}$ et donc $x \mapsto h \cdot x$ induit une bijection de X_g sur $X_{g'}$ qui, de ce fait, ont le même nombre d'éléments.

(ii) L'ensemble V_g des points fixes de g est l'espace propre associé à la valeur propre 1 ; c'est donc un sous-espace vectoriel de V. Par ailleurs, si $g' = hgh^{-1}$, alors $x \mapsto h \cdot x$ induit une bijection de V_g sur $V_{g'}$ qui est linéaire puisque G opère linéairement. On en déduit que si l'un des deux espaces est de dimension finie, alors l'autre aussi et les deux dimensions sont les mêmes.

Exercice 3.3. $108 = 2^2 \times 3^3$, et donc $(\mathbf{Z}/108\mathbf{Z})^* \cong (\mathbf{Z}/4\mathbf{Z})^* \oplus (\mathbf{Z}/27\mathbf{Z})^*$. Or $(\mathbf{Z}/4\mathbf{Z})^* = \{\pm 1\}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$, et $(\mathbf{Z}/27\mathbf{Z})^*$ est un groupe de cardinal $\varphi(27) = 2 \cdot 9$ qui est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/9\mathbf{Z})$ ou à $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z})$. Dans le second cas, tout élément de $(\mathbf{Z}/27\mathbf{Z})^*$ vérifierait $x^6 = 1$, or $2^6 = 64 \neq 1$ dans $(\mathbf{Z}/27\mathbf{Z})^*$. On a donc $(\mathbf{Z}/27\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/9\mathbf{Z})$ et $(\mathbf{Z}/108\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/9\mathbf{Z})$.

$200 = 2^3 \cdot 5^2$, et donc $(\mathbf{Z}/200\mathbf{Z})^* \cong (\mathbf{Z}/8\mathbf{Z})^* \oplus (\mathbf{Z}/25\mathbf{Z})^*$. Or $(\mathbf{Z}/8\mathbf{Z})^*$ est un groupe d'ordre 4 dans lequel tout les éléments sont d'ordre 2 (en effet, 1^2, 3^2, 5^2 et 7^2 sont congrus à 1 modulo 8) ; il est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$. Par ailleurs, $\mathbf{Z}/25\mathbf{Z})^*$ est un groupe de cardinal $\varphi(25) = 4 \cdot 5$ qui est donc isomorphe à $(\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ ou à $(\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/5\mathbf{Z})$. Dans le second cas, toute puissance 5-ième serait d'ordre 2, or $2^5 = 32 = 7$ a un carré égal à $49 = -1 \neq 1$, et donc $(\mathbf{Z}/25\mathbf{Z})^* \cong (\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ et $(\mathbf{Z}/200\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$.

La solution ci-dessus est un peu artisanale ; on peut aller plus vite en utilisant les résultats de l'ex. 3.5.

Exercice 3.4. (i) Soit $\oplus_{p \in \mathscr{P}}(\oplus_i(\mathbf{Z}/p^{a_{p,i}}\mathbf{Z}))$ la décomposition de K^* fournie par le th. 3.1. Si K^* n'est pas cyclique, il existe p tel que $a_{p,2} \neq 0$; en effet, sinon on aurait $K^* \cong \mathbf{Z}/D\mathbf{Z}$, où $D = \prod_p p^{a_{p,1}}$, d'après le théorème des restes chinois, et K^* serait cyclique. Mais alors l'équation $x^p = 1$ a au moins p^2

solutions dans K [les éléments de $(p^{a_{p,1}-1}\mathbf{Z}/p^{a_{p,1}}\mathbf{Z}) \oplus (p^{a_{p,2}-1}\mathbf{Z}/p^{a_{p,2}}\mathbf{Z})$], ce qui est impossible dans un corps commutatif.

(ii) Il résulte du (i) que le groupe $\mathbf{F}_p^*$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$ (l'isomorphisme envoie l'élément neutre 1 de $\mathbf{F}_p^*$ sur celui de $\mathbf{Z}/(p-1)\mathbf{Z}$, à savoir 0). Via cet isomorphisme, l'ensemble des carrés devient $2\mathbf{Z}/(p-1)\mathbf{Z}$. Soit alors $x \in \mathbf{Z}/(p-1)\mathbf{Z}$, et soit $\tilde{x} \in \mathbf{Z}$ ayant pour image x modulo $p-1$. On a les équivalences : « $x \in 2\mathbf{Z}/(p-1)\mathbf{Z}$ » $\Leftrightarrow$ « $\tilde{x} \in 2\mathbf{Z}$ » $\Leftrightarrow$ « $\frac{p-1}{2}\tilde{x} \in (p-1)\mathbf{Z}$ » $\Leftrightarrow$ « $\frac{p-1}{2}x = 0$ ». On en déduit le résultat.

(iii) On a $(-1)^{(p-1)/2} = 1$ dans $\mathbf{F}_p^*$ si et seulement si p est de la forme $4n+1$, ce qui permet de conclure en utilisant le (ii).

(iv) Si $a^2 + b^2 = p$ et si $p \mid a$, alors $p \mid b^2 = p - a^2$, et donc $p \mid b$ et $p^2 \mid p$, ce qui est absurde. On en déduit que a et b sont premiers à p, et donc que leurs réductions $\overline{a}$, $\overline{b}$ modulo p appartiennent à $\mathbf{F}_p^*$. Soit $x = \overline{a}^{-1}\overline{b} \in \mathbf{F}_p^*$. En réduisant modulo p la relation $a^2 + b^2 = p$, on obtient $\overline{a}^2(1 + x^2) = 0$, et donc $1 + x^2 = 0$ puisque $\overline{a} \in \mathbf{F}_p^*$. Comme ceci est en contradiction avec le (iii), cela permet de conclure.

Exercice 3.5. (i) On a $(1 + p^k a)^p = 1 + p^{k+1}a + \frac{p(p-1)}{2}p^{2k}a^2 + p^{3k}a^3\big(\sum_{i=3}^{p}\binom{p}{i}(p^k a)^{p-i}\big)$. Dans cette somme, tous les termes sauf les deux premiers sont divisibles par p^{k+2}, si $k \geqslant 1$ (ou si $k \geqslant 2$, dans le cas $p = 2$, où $\frac{p(p-1)}{2}$ n'est pas divisible par p). On a donc bien $x \equiv 1 + p^{k+1}a \bmod p^{k+2}$, dans les cas considérés, et une récurrence immédiate montre que $(1+p)^{p^{n-2}} = 1 + p^{n-1} \neq 1$ dans $\mathbf{Z}/p^n\mathbf{Z}$, si $p \neq 2$ et $n \geqslant 2$, et que $(1+4)^{p^{n-3}} = 1 + 2^{n-1} \neq 1$ dans $\mathbf{Z}/2^n\mathbf{Z}$, si $n \geqslant 3$.

(ii) Supposons p impair. Alors N est le sous-groupe image de $1+p\mathbf{Z}$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, qui est de cardinal p^{n-1} (car $x \mapsto 1 + px$ induit une bijection de $\mathbf{Z}/p^{n-1}\mathbf{Z}$ sur $1 + p\mathbf{Z}$ modulo $p^n\mathbf{Z}$). Comme $(1+p)^{p^{n-2}} \neq 1$ dans $(\mathbf{Z}/p^n\mathbf{Z})^*$, dans la décomposition $\oplus_i(\mathbf{Z}/p^{a_i}\mathbf{Z})$ du groupe N (dont le cardinal est une puissance de p), au moins un des a_i est $\geqslant n-1$, et donc $\mathrm{N} \cong \mathbf{Z}/p^{n-1}\mathbf{Z}$. Le cas $p = 2$ se traite de la même manière.

(iii) La réduction modulo p fournit une surjection $\pi : \mathrm{G} = (\mathbf{Z}/p^n\mathbf{Z})^* \to \mathbf{F}_p^*$, et $\mathbf{F}_p^*$ est un groupe isomorphe à $(\mathbf{Z}/(p-1)\mathbf{Z})$ d'après l'ex. 3.4. Comme $p-1$ et p^{n-1} sont premiers entre eux, il résulte du th. 3.1, que $\mathrm{G}_p = \mathrm{N} \cong \mathbf{Z}/p^{n-1}\mathbf{Z}$ et que G est de la forme $(\mathbf{Z}/p^{n-1}\mathbf{Z}) \oplus \mathrm{G}'$, avec $\mathrm{G}' = \oplus_{\ell \neq p}\mathrm{G}_\ell$. Alors $\mathrm{G}/\mathrm{N} \cong \mathrm{G}'$, et comme $\mathrm{G}/\mathrm{N} \cong \mathbf{F}_p^*$ par définition de N et surjectivité de π, cela permet de conclure.

(iv) Le groupe $(\mathbf{Z}/2^n\mathbf{Z})^*$ est de cardinal $\mathbf{Z}/2^{n-1}\mathbf{Z}$, et contient les sous-groupes N et $\{\pm 1\}$ dont l'intersection est nulle. Ceci implique que N et $\{\pm 1\}$ sont en somme directe, et comme $|\mathrm{N}|\cdot|\{\pm 1\}| = |(\mathbf{Z}/2^n\mathbf{Z})^*|$, cela prouve que $(\mathbf{Z}/2^n\mathbf{Z})^* = \mathrm{N} \oplus \{\pm 1\}$, ce qui permet de conclure puisque $\mathrm{N} \cong \mathbf{Z}/2^{n-2}\mathbf{Z}$ et $\{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z}$.

Exercice 3.6. Comme $|\mathbf{F}_p^*| = p - 1$, on a $x^{p-1} = 1$ pour tout $x \in \mathbf{F}_p^*$ d'après le théorème de Lagrange. On en déduit que $x^p = x$ pour tout $x \in \mathbf{F}_p$, ce qui se traduit, en remontant dans $\mathbf{Z}$, par $p | n^p - n$, pour tout $n \in \mathbf{Z}$.

Exercice 3.7. (i) Si $\phi \in \mathrm{X}$, alors $(g \cdot (h \cdot \phi))(x) = (h \cdot \phi)(x + g) = \phi((x + h) + g) = \phi(x + (g + h)) = ((g + h) \cdot \phi)(x)$, pour tout $x \in \mathbf{Z}_p/p\mathbf{Z}_p$. On en déduit que $g \cdot (h \cdot \phi) = (g + h) \cdot \phi$, pour tout $\phi \in \mathrm{X}$, ce qui prouve que l'on a bien affaire à une action de groupe.

(ii) Les points fixes sont les fonctions constantes : si $g \cdot \phi = \phi$, pour tout $g \in \mathbf{Z}/p\mathbf{Z}$, évaluer en 0 donne $\phi(g) = \phi(0)$, pour tout $g \in \mathbf{Z}/p\mathbf{Z}$. Il y a n telles fonctions.

(iii) Le cardinal d'une orbite divisant celui du groupe, il est égal à p si l'orbite n'est pas réduite à un point.

(iv) Le cardinal de X est n^p et comme il y a n orbites réduites à un point, cela laisse $n^p - n$ éléments qui se répartissent en orbites à p éléments ; il en résulte que $\frac{n^p - n}{p}$ est entier puisque c'est le nombre d'orbites à p éléments.

Exercice 3.8. (i) C'est l'ensemble des parties à p éléments de $\{1, \ldots, n\}$.

(ii) Le stabilisateur de $\{1,\dots,p\}$ est l'ensemble des permutations de $\{1,\dots,n\}$ qui permutent les éléments de $\{1,\dots,p\}$ et ceux de $\{p+1,\dots,n\}$; il est donc isomorphe à $\mathrm{S}_p \times \mathrm{S}_{n-p}$ et son cardinal est $p!(n-p)!$.

(iii) Le cardinal d'une orbite est le quotient du cardinal du groupe par celui du stabilisateur d'un de ses éléments (cf. n° 3.3) ; en appliquant ceci à l'orbite de $\{1,\dots,p\}$ sous l'action de S_n, on obtient le fait que le cardinal de l'ensemble des parties à p éléments de $\{1,\dots,n\}$ est $\frac{n!}{p!(n-p)!}$.

Exercice 3.9. On obtient le 5-cycle $(1,2,3,4,5)$.

Exercice 3.10. La démonstration se fait par récurrence sur n. Le résultat est trivial si $n=2$. Soit $n \geqslant 3$, et soient $\sigma \in \mathrm{S}_n$, et $a = \sigma(n)$. Si $a \neq n$, alors $\sigma' = (n-1,n)\cdots(a,a+1)\sigma$ fixe n, et est dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-2,n-1)$ d'après l'hypothèse de récurrence. Donc $\sigma = (a,a+1)\cdots(n-1,n)\sigma'$ est dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-1,n)$. Si $a=n$, alors σ est déjà dans le sous-groupe engendré par $(1,2),(2,3),\dots,(n-2,n-1)$, ce qui prouve que le sous-groupe engendré par $(1,2),(2,3),\dots,(n-1,n)$ est S_n.

Exercice 3.11. Comme les τ_i commutent deux à deux, on a $\sigma^n = \tau_1^n \cdots \tau_s^n$, et comme les τ_i^n sont à supports disjoints, on a $\sigma^n = 1$ si et seulement si $\tau_i^n = 1$ pour tout i. On en déduit que l'ordre de σ est le ppcm des ordres des τ_i, et comme τ_i est d'ordre ℓ_i, l'ordre de σ est le ppcm des ℓ_i.

Exercice 3.12. (i) Choisir un cycle de longueur k revient à choisir les k éléments (n choix pour le premier,..., $n-k+1$ pour le dernier), en tenant compte du fait que les k permutations circulaires des éléments donnent le même cycle ; il y a donc $\frac{1}{k}(n(n-1)\cdots(n-k+1))$ cycles de longueur k.

(ii) Soit $\tau = (i_1,\dots,i_k)$ un cycle de longueur k. Alors τ apparaît dans la décomposition de σ si et seulement si la restriction de σ à $\{i_1,\dots,i_k\}$ est τ, et σ peut permuter les autres éléments comme il veut, et donc τ apparaît dans la décomposition de $(n-k)!$ permutations.

Maintenant, le nombre total de cycles apparaissant dans les permutations de S_n est aussi la somme pour chaque cycle du nombre de permutations dans lequel il apparaît. Ce nombre total est donc, d'après ce qui précède, égal à $\sum_{k=1}^n \frac{1}{k}(n(n-1)\dots(n-k+1))\cdot(n-k)! = n!(1+\frac{1}{2}+\cdots+\frac{1}{n})$, et le nombre moyen de cycles est $1+\frac{1}{2}+\cdots+\frac{1}{n}$ qui tend bien vers $+\infty$.

Exercice 3.14. Si $\tau_1\dots\tau_r$ est la décomposition de σ en cycles (en incluant les cycles de longueur 1), et si τ_i est de longueur ℓ_i, alors $\omega(\sigma) = r$, $\sum_{i=1}^r \ell_i = n$ et

$$\mathrm{sign}(\sigma) = \prod_{i=1}^r \mathrm{sign}(\tau_i) = \prod_{i=1}^r (-1)^{\ell_i - 1} = (-1)^{n-r} = (-1)^{n-\omega(\sigma)}.$$

Exercice 3.15. (i) On a $u_{\sigma\tau}(e_i) = e_{\sigma\tau(i)} = e_{\sigma(\tau(i))} = u_\sigma(e_{\tau(i)}) = u_\sigma(u_\tau(e_i))$, ce qui prouve que les endomorphisme $u_{\sigma\tau}$ et $u_\sigma u_\tau$ coïncident sur la base canonique, et donc sont égaux. De plus, l'image de la base canonique est une base (vu que c'est la base canonique à l'ordre près) ; u_σ est donc élément de $\mathbf{GL}_n(\mathbf{C})$ et $\sigma \mapsto u_\sigma$ est un morphisme de groupes de S_n dans $\mathbf{GL}_n(\mathbf{C})$.

(ii) Si τ est la transposition (i,j), alors u_τ est la symétrie par rapport à l'hyperplan engendré par $\frac{e_i+e_j}{2}$ et les e_ℓ, pour $\ell \notin \{i,j\}$, de direction la droite engendrée par $\frac{e_i-e_j}{2}$. Ceci implique que u_τ a $n-1$ valeurs propres égales à 1 et une égale à -1 et donc $\det u_\tau = -1$.

(iii) Comme $\det : \mathbf{GL}_n(\mathbf{C}) \to \mathbf{C}^*$ est un morphisme de groupes, l'application $\sigma \mapsto \det u_\sigma$ est un morphisme de groupes. Par ailleurs, il ressort du (ii) que l'on a $\det u_\sigma = -1 = \mathrm{sign}(\sigma)$, si σ est une transposition, et comme les transpositions engendrent S_n, cela implique que les deux morphismes de groupes $\sigma \mapsto \det u_\sigma$ et $\sigma \mapsto \mathrm{sign}(\sigma)$ coïncident sur S_n.

Exercice 3.16. (i) D'après le théorème de structure, G est isomorphe à une somme directe $\oplus_{i\in\mathrm{I}}(\mathbf{Z}/p_i^{a_i}\mathbf{Z})$, où les p_i sont des nombres premiers (pas forcément distincts). On a alors $|\mathrm{G}| = \prod_{i\in\mathrm{I}} p_i^{a_i}$, et si d divise $|\mathrm{G}|$, on peut trouver des entiers b_i, avec $b_i \leqslant a_i$, tels que $d = \prod_{i\in\mathrm{I}} p_i^{b_i}$. Comme $\mathbf{Z}/p_i^{a_i}\mathbf{Z}$ est cyclique, et comme

$p^{b_i}|p^{a_i}$, le groupe $\mathbf{Z}/p_i^{a_i}\mathbf{Z}$ contient un sous-groupe H_i d'ordre p^{b_i}, et $\oplus_{i\in\mathrm{I}}\mathrm{H}_i$ est un sous-groupe de G de cardinal d.

(ii) Comme $|\mathrm{A}_5| = 60 > 6 = |\mathrm{S}_3|$, la restriction de f à A_5 n'est pas injective, et comme A_5 est simple, cela implique que $f(\mathrm{A}_5) = \{\mathrm{id}\}$, et donc que f se factorise à travers $\mathrm{S}_5/\mathrm{A}_5$. Comme le cardinal de $\mathrm{S}_5/\mathrm{A}_5$ est 2, l'image de f a 1 ou 2 éléments.

(iii) Soit H un sous-groupe de S_5 d'ordre 40, et soit $\mathrm{X} = \mathrm{S}_5/\mathrm{H}$. Alors $|\mathrm{X}| = |\mathrm{S}_5|/|\mathrm{H}| = 3$. Par ailleurs, S_5 agit sur X par translation à droite, et permute les éléments de X. On en déduit l'existence d'un morphisme de groupes de S_5 dans $\mathrm{Perm}(\mathrm{X}) \cong \mathrm{S}_3$ dont l'image a au moins 3 éléments. Ceci étant en contradiction avec le (ii), cela prouve que H n'existe pas.

Exercice 3.18. (i) Comme $\mathbf{Z}/p\mathbf{Z}$ est engendré par 1, il suffit de vérifier que $x_0\cdots x_{p-1} = 1$ implique $x_1\cdots x_{p-1}x_0 = 1$, ce qui se démontre en multipliant la première relation à gauche par x_0^{-1} et à droite par x_0. Un point fixe de cette action est de la forme $(x,\dots,x)$ et son appartenance à X se traduit par $x^p = 1$; les points fixes sont donc en bijection avec les éléments de G d'ordre divisible par p.

(ii) La condition $x_0\cdots x_{p-1} = 1$ peut se réécrire sous la forme $x_0 = x_{p-1}^{-1}\cdots x_1^{-1}$; on en déduit que $(x_0,\dots,x_{p-1}) \mapsto (x_1,\dots,x_{p-1})$ induit une bijection de X sur G^{p-1} et donc que $|\mathrm{X}| = |\mathrm{G}|^{p-1}$. Comme p divise $|\mathrm{G}|$ par hypothèse, il divise aussi $|\mathrm{X}|$. Maintenant, X est la réunion disjointe des orbites sous l'action de $\mathbf{Z}/p\mathbf{Z}$, et comme le cardinal d'une orbite divise celui du groupe, ces orbites ont pour cardinal 1 ou p. Comme $|\mathrm{X}|$ est divisible par p, le nombre d'orbites de cardinal 1 est divisible par p, et comme il y en a au moins une, à savoir $(1,\dots,1)$, il y en a au moins p. Les orbites de cardinal 1 étant en bijection avec les éléments de G d'ordre divisible par p, et comme un tel élément est d'ordre p s'il n'est pas égal à 1, cela prouve que G contient des éléments d'ordre p.

Exercice 4.1. (i) K et A sont clairement stables par addition, passage à l'opposé, et multiplication. Ce sont donc des sous-anneaux de $\mathbf{C}$. De plus, l'inverse de $x+iy$ est $\frac{1}{x^2+y^2}(x-iy)$ qui appartient à K, si $x, y \in \mathbf{Q}$; il en résulte que K est aussi stable par passage à l'inverse et donc est un sous-corps de $\mathbf{C}$.

(ii) On a $\mathrm{N}(z) = |z|^2$, et le résultat suit de ce que $|z_1z_2| = |z_1|\,|z_2|$ (on peut aussi vérifier le résultat en développant).

(iii) Si $u \in \mathrm{A}^*$, et si v est son inverse, on a $\mathrm{N}(u)\mathrm{N}(v) = \mathrm{N}(uv) = 1$. Comme $\mathrm{N}(u)$ et $\mathrm{N}(v)$ sont des entiers $\geqslant 0$, cela implique que $\mathrm{N}(u) = 1$. Réciproquement, si $\mathrm{N}(u) = 1$, alors $u\,\overline{u} = 1$ et donc u est inversible, d'inverse $\overline{u}$. Enfin, si $x, y \in \mathbf{Z}$ vérifient $x^2+y^2 = 1$, alors l'un des deux vaut 0 et l'autre ± 1, et donc $\mathrm{A}^* = \{1,-1,i,-i\}$.

(iv) On a $\mathrm{N}(r) = \mathrm{N}(b)\mathrm{N}(\{\frac{a}{b}\})$, et comme $\mathrm{N}(\{z\}) \leqslant \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$, pour tout $z \in \mathbf{C}$, on en déduit que $\mathrm{N}(r) \leqslant \frac{1}{2}\mathrm{N}(b) < \mathrm{N}(b)$. Soit $c = [\frac{a}{b}]$. Alors $c \in \mathrm{A}$ par construction, et $c + \frac{r}{b} = \frac{a}{b}$, ce qui nous donne $a = bc + r$, et prouve que $r = a - bc \in \mathrm{A}$. D'où le résultat.

(v) Soient I un idéal de A et $b \in \mathrm{A}^+ \cap \mathrm{I}$ tel que $\mathrm{N}(b)$ réalise le minimum des $\mathrm{N}(x)$, pour $x \in \mathrm{I} - \{0\}$. Si $a \in \mathrm{I}$, on peut, d'après le (iv), écrire a sous la forme $a = bc+r$, avec $\mathrm{N}(r) < \mathrm{N}(b)$. Mais alors $r = a-bc \in \mathrm{I}$, et la définition de b implique $r = 0$. Il en résulte que I est l'idéal principal engendré par b. Ceci permet de conclure.

Exercice 4.2. (i) A contient 1, est stable par addition car $(a+b\sqrt{-5})+(a'+b'\sqrt{-5}) = (a+a')+(b+b')\sqrt{-5}$ et par multiplication puisque $(a+b\sqrt{-5})(a'+b'\sqrt{-5}) = (aa'-5bb')+(a'b+ab')\sqrt{-5}$. C'est donc un sous-anneau de $\mathbf{C}$.

(ii) Si $\alpha = a+b\sqrt{-5}$ divise 2, alors $|\alpha|^2 = a^2+5b^2$ divise $|2|^2 = 4$, et donc $b = 0$ et $a \in \{\pm 1, \pm 2\}$. Il s'ensuit que $2 = \alpha\beta$ implique $\alpha = \pm 1$ ou $\beta = \pm 1$, ce qui prouve que 2 est irréductible.

(iii) Si $(2, 1+\sqrt{-5}) = (\alpha)$, alors α divise 2, et donc $\alpha = \pm 1$ ou $\alpha = \pm 2$. Le second cas n'est pas possible car ± 2 ne divise par $1+\sqrt{-5}$, et le premier non plus car un élément $a+b\sqrt{-5}$ de $(2, 1+\sqrt{-5})$ vérifie $a \equiv b \bmod 2$, ce qui n'est pas le cas de ± 1. On en déduit que $(2, 1+\sqrt{-5})$ n'est pas principal.

Maintenant, $1+\sqrt{-5}$ n'est pas divisible par 2 alors que $(1+\sqrt{-5})^2 = -4+2\sqrt{-5}$ l'est. Il s'ensuit que (2) n'est pas un idéal premier.

Exercice 4.3. Si $\mathrm{P} \in \mathrm{A[X]}^*$, alors $\varphi(\mathrm{P}) \in \mathrm{K[X]}^* = \mathrm{K}^*$; la condition est donc nécessaire. Réciproquement, si $\varphi(\mathrm{P}) = a \in \mathrm{K}^*$, on peut écrire P sous la forme $\mathrm{P} = a + \varepsilon\mathrm{Q}$, avec $\mathrm{Q} \in \mathrm{K[X]}$, et alors P est inversible d'inverse $a^{-1} - a^{-2}\varepsilon\mathrm{Q}$ car $\varepsilon^2 = 0$.

Exercice 4.4. (i) Que $\mathbf{Z} \cap (q)$ soit un idéal de $\mathbf{Z}$ est immédiat. Soient $a, b \in \mathbf{Z}$ tels que $ab \in \mathbf{Z} \cap (q)$. Comme (q) est un idéal premier de A, on a $a \in (q)$ ou $b \in (q)$, et donc $a \in \mathbf{Z} \cap (q)$ ou $b \in \mathbf{Z} \cap (q)$, ce qui prouve que $\mathbf{Z} \cap (q)$ est un idéal premier de $\mathbf{Z}$. Notons p l'élément de $\mathscr{P}$ correspondant. L'appartenance de p à $\mathbf{Z} \cap (q)$ se traduit par la divisibilité de p par q dans A ; on en déduit que p est l'unique élément de $\mathscr{P}$ divisible par q dans A. Enfin, $\mathrm{N}(q)$ divise $\mathrm{N}(p) = p^2$ et n'est pas égal à 1 sinon q serait inversible ; il ne reste donc que $\mathrm{N}(q) = p$ et $\mathrm{N}(q) = p^2$ comme possibilités.

(ii) Si $\mathrm{N}(q) = p \in \mathscr{P}$ et si $q = ab$, on a $\mathrm{N}(a)\mathrm{N}(b) = p$, et donc $\mathrm{N}(a) = 1$ ou $\mathrm{N}(b) = 1$; il en résulte que a ou b est inversible, et que $a \in (q)$ ou $b \in (q)$. L'idéal (q) est donc premier.

(iii) Comme a est de la forme $4n+1$, l'équation $x^2 + 1 = 0$ a une solution dans $\mathbf{F}_p$, et il existe $\tilde{x} \in \{1, \ldots, p-1\}$ tel que $\tilde{x}^2 + 1$ soit divisible par p. Alors $a = \tilde{x} + i$ vérifie les conditions demandées.

Maintenant, soit $u\prod q_i$ la factorisation de a en produit de facteurs premiers dans A. Alors $\mathrm{N}(a) = \prod \mathrm{N}(q_i)$, et comme $p \mid \mathrm{N}(a)$, il existe i tel que $p \mid \mathrm{N}(q_i)$, ce qui, d'après le (i) implique que q_i divise p dans A. Il en résulte que $q_i | \mathrm{pgcd}(a,p)$, et donc que $b = \mathrm{pgcd}(a,p)$ n'est pas inversible. De plus, $\mathrm{N}(b) \leqslant \mathrm{N}(a) < p^2$, et comme $\mathrm{N}(b) | p^2$, cela implique que $\mathrm{N}(b) = p$. Le (ii) montre alors que b est premier, ce qui permet de conclure.

(iv) D'après le (iii), il existe $q \in \mathscr{P}_\mathrm{A}$ divisant strictement p, ce qui implique $\mathrm{N}(q) = p$. Il n'y a plus qu'à écrire q sous la forme $x + iy$, avec $x, y \in \mathbf{Z}$, pour obtenir une écriture de $p = x^2 + y^2$ comme somme de deux carrés.

(v) Si $p \in \mathscr{P}$ impair n'est pas premier dans A, et si $q = x + iy$ est un diviseur premier de p, on a $\mathrm{N}(q) = p$. Or $\mathrm{N}(q) = (-i)qq^*$, et $\mathrm{N}(q^*) = \mathrm{N}(q)$ puisque $q^* = y + ix$. D'après le (ii), cela implique que $q^* \in \mathscr{P}_\mathrm{A}$ et donc que la factorisation de p est $(-i)qq^*$. Enfin, comme p est impair, on a $x \neq y$, et on peut, quitte à échanger les rôles de q et q^*, supposer que $x > y$ et poser $q_p = q$.

(vi) Voir la solution du (iv) de l'ex. 3.4.

(vii) D'après le (i), les éléments de $\mathscr{P}_\mathrm{A}$ sont les diviseurs premiers des éléments de $\mathscr{P}$. Le résultat est donc une combinaison des (v), (vi) et de ce que la factorisation de 2 est $2 = (-i)(1+i)^2$.

Exercice 4.5. (i) La nullité de Δ implique, car A est premier à B, que A divise A′ (lemme de Gauss), ce qui n'est possible que si $\mathrm{A}' = 0$, et donc si A est constant. De même, cette nullité implique que B et C sont constants, ce qui est contraire à l'hypothèse. On en déduit que $\Delta \neq 0$; l'inégalité est alors évidente.

(ii) Si z est un zéro de ABC, alors c'est un zéro d'un seul des polynômes A, B ou C puisque ceux-ci sont premiers entre eux. On peut donc, sans nuire à la généralité, supposer que c'est un zéro de multiplicité $m_z \geqslant 1$ de A. Sa multiplicité comme zéro de A′ est alors $m_z - 1$, et comme B ne s'annule pas en z, sa multiplicité comme zéro de $\mathrm{AB}' - \mathrm{BA}'$ est exactement $m_z - 1$.

(iii) On déduit du (ii) que Δ est divisible par le produit des $(\mathrm{T}-z)^{m_z-1}$, où z parcourt les zéros de ABC, ce qui nous fournit l'inégalité $\deg\Delta \geqslant \sum(m_z - 1)$, et comme $\sum m_z = \deg\mathrm{ABC} = \deg\mathrm{A} + \deg\mathrm{B} + \deg\mathrm{C}$ et $\sum_z 1 = r(\mathrm{Q})$ (par définition de $r(\mathrm{Q})$), on obtient $\deg\Delta \geqslant \deg\mathrm{A} + \deg\mathrm{B} + \deg\mathrm{C} - r(\mathrm{Q})$. Le résultat demandé s'obtient alors en comparant cette inégalité avec celle du (i).

(iv) Supposons que $\mathrm{A}^n + \mathrm{B}^n = \mathrm{C}^n$, et que $\mathrm{A}, \mathrm{B}, \mathrm{C}$ ne sont pas tous constants. Comme les zéros de $\mathrm{A}^n\mathrm{B}^n\mathrm{C}^n$ sont ceux de ABC, on déduit du (iii) l'inégalité $r(\mathrm{ABC}) > n\sup(\deg\mathrm{A}, \deg\mathrm{B}, \deg\mathrm{C})$, ce qui est absurde, si $n \geqslant 3$, car $r(\mathrm{ABC}) \leqslant \deg\mathrm{ABC} = \deg\mathrm{A} + \deg\mathrm{B} + \deg\mathrm{C}$.

Exercice 4.6. (i) On peut utiliser les polynômes d'interpolation de Lagrange pour écrire Q sous la forme $\sum_{i=0}^{n} \mathrm{Q}(\lambda_i) \prod_{j\neq i} \frac{\mathrm{X}-\lambda_j}{\lambda_i-\lambda_j}$, et obtenir $\mathrm{F} = \sum_{i=0}^{n} \frac{\mathrm{Q}(\lambda_i)}{\prod_{j\neq i}(\lambda_i-\lambda_j)} \frac{1}{\mathrm{X}-\lambda_i}$. On peut aussi dire que la décomposition en éléments simples de F est de la forme $\sum_{i=0}^{n} \frac{\alpha_i}{\mathrm{X}-\lambda_i}$ pour des raisons de degré, multiplier les deux côtés par $\mathrm{X}-\lambda_i$ et évaluer le tout en $\mathrm{X}=\lambda_i$ pour obtenir α_i.

(ii) Si $\deg \mathrm{Q} = d$, alors $\mathrm{Q}(\mathrm{X}) = \sum_{i=0}^{d} \mathrm{Q}^{[i]}(\lambda)(\mathrm{X}-\lambda)^i$, d'après la formule de Taylor pour les polynômes. On en déduit que la décomposition en éléments simples de $\frac{\mathrm{Q}(\mathrm{X})}{(\mathrm{X}-\lambda)^n}$ est $\mathrm{R} + \sum_{i=0}^{n-1} \frac{\mathrm{Q}^{[i]}(\lambda)}{(\mathrm{X}-\lambda)^{n-i}}$, où $\mathrm{R} = \sum_{i=n}^{d} \mathrm{Q}^{[i]}(\lambda)(\mathrm{X}-\lambda)^{i-n} \in \mathrm{K}[\mathrm{X}]$.

(iii) Comme K est algébriquement clos, on peut écrire F sous la forme $u\prod_{i=1}^{n}(\mathrm{X}-\lambda_i)^{k_i}$, où $u \in \mathrm{K}^*$, les $\lambda_i \in \mathrm{K}$ sont distincts deux à deux et les k_i sont des entiers relatifs. Alors $\frac{\mathrm{F}'}{\mathrm{F}} = \sum_{i=1}^{n} \frac{k_i}{\mathrm{X}-\lambda_i}$, et cette identité fournit la décomposition de $\frac{\mathrm{F}'}{\mathrm{F}}$ en éléments simples.

(iv) Soient $z_1, \dots, z_r$ les zéros de P, et soit m_i la multiplicité de z_i. Si z est un zéro de P' distinct des z_i (le résultat est clair si z est l'un des z_i), alors $0 = \frac{\mathrm{P}'(z)}{\mathrm{P}(z)} = \sum_{i=1}^{r} \frac{m_i}{z-z_i}$. Si z était à l'extérieur de l'enveloppe convexe des z_i, il existerait $\theta \in [-\pi, \pi]$ tel que $\mathrm{Im}(e^{-i\theta}(z-z_i)) > 0$ pour tout i. Mais alors $\mathrm{Im}\big(e^{i\theta}\frac{m_i}{z-z_i}\big) < 0$ pour tout i, ce qui contredit la relation $\sum_{i=1}^{r} \frac{m_i}{z-z_i} = 0$.

Exercice 4.7. Commençons par remarquer que le changement de variable ci-dessus n'augmente pas le degré total de P ; on a donc $\deg_{\mathrm{X}_n} \mathrm{P}_{t_1,\dots,t_{n-1}} \leqslant \deg \mathrm{P}_{t_1,\dots,t_{n-1}} \leqslant \deg \mathrm{P} = d$. Soit Q la partie homogène de degré d de P. Le coefficient de X_n^d dans $\mathrm{P}_{t_1,\dots,t_{n-1}}$ est $\mathrm{R}(t_1,\dots,t_{n-1}) = \mathrm{Q}(t_1,\dots,t_{n-1},1)$, et on a $\mathrm{Q}(\mathrm{X}_1,\dots,\mathrm{X}_n) = \mathrm{X}_n^d \mathrm{R}\big(\frac{\mathrm{X}_1}{\mathrm{X}_n},\dots,\frac{\mathrm{X}_{n-1}}{\mathrm{X}_n}\big)$, ce qui prouve que $\mathrm{R} \neq 0$. Comme K est infini, on peut donc trouver $t_1,\dots,t_{n-1} \in \mathrm{K}$, tels que $\mathrm{R}(t_1,\dots,t_{n-1}) \neq 0$, ce qui permet de conclure.

Exercice 4.9. (i) L'expression $\sum_{i=1}^{n} \alpha_i^k$ est un polynôme symétrique, à coefficients dans $\mathbf{Z}$, en $\alpha_1,\dots,\alpha_n$; c'est donc un polynôme à coefficients dans $\mathbf{Z}$ en les coefficients de P qui sont rationnels par hypothèse ; d'où le résultat.

(ii) Les coefficients de $\prod_{i=1}^{n}(\mathrm{X}-\alpha_i^3)$ sont des polynômes symétriques, à coefficients dans $\mathbf{Z}$, en $\alpha_1,\dots,\alpha_n$. On peut donc conclure comme dans le (i).

Exercice 4.10. (i) On reconnaît dans le membre de droite $\frac{\mathrm{P}'}{\mathrm{P}}$, où $\mathrm{P} = \prod_{i=1}^{n}(\mathrm{X}-\mathrm{X}_i)$; la formule résulte donc de ce que $\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}$.

(ii) On multiplie les deux membres par X et on fait le changement de variable $\mathrm{X} = \frac{1}{\mathrm{T}}$. Le membre de droite devient $\frac{n-(n-1)\Sigma_1\mathrm{T}+(n-2)\Sigma_2\mathrm{T}^2\cdots}{1-\Sigma_1\mathrm{T}+\Sigma_2\mathrm{T}^2+\cdots} = n + \frac{\Sigma_1\mathrm{T}-2\Sigma_2\mathrm{T}^2+3\Sigma_3\mathrm{T}^3\cdots}{1-\Sigma_1\mathrm{T}+\Sigma_2\mathrm{T}^2-\Sigma_3\mathrm{T}^3+\cdots}$ tandis que celui de gauche devient $\sum_{i=1}^{n} \frac{1}{1-\mathrm{TX}_i} = \sum_{i=1}^{n} \sum_{k=0}^{+\infty} \mathrm{T}^k\mathrm{X}_i^k = \sum_{k=0}^{+\infty} \mathrm{T}^k\mathrm{S}_k$; d'où l'identité cherchée. Un développement limité nous donne alors $\mathrm{S}_2 = \Sigma_1^2 - 2\Sigma_2$ et $\mathrm{S}_3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

(iii) Si $\lambda_1,\dots,\lambda_n$ sont les valeurs propres de M, comptées avec multiplicité, on a $\mathrm{Tr}(\mathrm{M}^k) = \mathrm{S}_k(\lambda_1,\dots,\lambda_n)$. L'hypothèse équivaut donc à $\mathrm{S}_k(\lambda_1,\dots,\lambda_n) = 0$ pour tout $k \geqslant 1$, et les (i) et (ii) montrent que ceci implique que $\frac{\mathrm{P}'}{\mathrm{P}} = \frac{n}{\mathrm{X}}$, si $\mathrm{P} = \prod_{i=1}^{n}(\mathrm{X}-\lambda_i)$. On en déduit la nullité des λ_i, ce qui permet de conclure.

Exercice 4.11. (i) Le polynôme $\mathrm{R} = \prod_{(i,j)\in \mathrm{I}\times\mathrm{J}}(\mathrm{X}-\alpha_i-\beta_j) \in \mathbf{Z}[\mathrm{X},\alpha_i,\beta_j,\ (i,j)\in\mathrm{I}\times\mathrm{J}]$ est symétrique en les β_j (et les α_i), et donc est un polynôme à coefficients dans $\mathbf{Z}[\mathrm{X},\alpha_i,\ i\in\mathrm{I}]$ (symétrique en les α_i) en les coefficients de Q qui sont des entiers par hypothèse ; c'est donc un élément de $\mathbf{Z}[\mathrm{X},\alpha_i,\ i\in\mathrm{I}]$ (symétrique en les α_i), et comme il est symétrique en les α_i, c'est un polynôme à coefficients dans $\mathbf{Z}[\mathrm{X}]$ en les coefficients de P. Comme les coefficients de P appartiennent à $\mathbf{Z}$, on en déduit que $\mathrm{R} \in \mathbf{Z}[\mathrm{X}]$, et comme R est unitaire et admet $\alpha+\beta$ comme racine, cela prouve que $\alpha+\beta$ est un entier algébrique. Le raisonnement est le même pour $\alpha\beta$ en partant du polynôme $\prod_{(i,j)\in\mathrm{I}\times\mathrm{J}}(\mathrm{X}-\alpha_i\beta_j)$.

(ii) Le fait que l'ensemble des nombres algébriques soit un anneau est une conséquence directe du (i). Il ne contient pas $\frac{1}{2}$ car on ne peut pas avoir $\big(\frac{1}{2}\big)^n = a_{n-1}\big(\frac{1}{2}\big)^{n-1} + \cdots + a_0$, avec $a_0,\dots,a_{n-1} \in \mathbf{Z}$, puisque la valuation 2-adique du membre de gauche est $-n$, et celle du membre de droite est $\geqslant 1-n$.

Exercice 4.12. Si $\mathrm{P}_1, \dots, \mathrm{P}_m$ engendrent I_n, alors a fortiori $\mathrm{P}_1, \dots, \mathrm{P}_m$ engendrent $\mathrm{I}_n/\mathrm{I}_{n+1}$ qui est un K-espace vectoriel de dimension $n+1$ (les images de $\mathrm{X}^n, \mathrm{YX}^{n-1}, \dots, \mathrm{Y}^n$ en sont une base). Or I_1 tue $\mathrm{I}_n/\mathrm{I}_{n+1}$; il s'ensuit que l'application $(\mathrm{Q}_1, \dots, \mathrm{Q}_m) \mapsto \sum_{i=1}^m \mathrm{Q}_i\mathrm{P}_i$ de $\mathrm{K}[\mathrm{X}, \mathrm{Y}]^m$ dans $\mathrm{I}_n/\mathrm{I}_{n+1}$ se factorise à travers $(\mathrm{K}[\mathrm{X}, \mathrm{Y}]/\mathrm{I}_1)^m = \mathrm{K}^m$, et est K-linéaire. Comme elle est surjective par hypothèse, la dimension m de l'espace de départ est $\geqslant n+1$, ce qu'il fallait démontrer.

Exercice 5.1 (i) La linéarité de la dérivation et de l'intégration sont des résultats de base.

(ii) On a $u \circ v = \mathrm{id}$ (th. fondamental de l'analyse). On en déduit que $(v \circ u) \circ (v \circ u) = v \circ (u \circ v) \circ u = v \circ u$, et donc que $v \circ u$ est une projection. En fait, $(v \circ u)(\phi)$ est la fonction $x \mapsto \phi(x) - \phi(0)$, et donc $v \circ u$ est la projection sur les fonction nulles en 0 parallèlement à l'espace des fonctions constantes.

Exercice 5.2 (i) On a $s(s(\phi))(x) = s(\phi)(-x) = \phi(x)$, et donc $s \circ s = \mathrm{id}$. Comme s est linéaire, c'est une symétrie.

(ii) Une fonction ϕ est paire si $s(\phi) = \phi$ et impaire si $s(\phi) = -\phi$; l'existence et l'unicité de la décomposition $\phi = \phi^+ + \phi^-$ est donc un cas particulier de la théorie générale. On a $\phi^+ = \frac{\phi + s(\phi)}{2}$ et $\phi^- = \frac{\phi - s(\phi)}{2}$, ce qui se traduit par $\phi^+(x) = \frac{\phi(x) + \phi(-x)}{2}$ et $\phi^-(x) = \frac{\phi(x) - \phi(-x)}{2}$.

Exercice 5.3 Si $\mathrm{P} = \sum_{i=0}^n \lambda_i \mathrm{Q}_i$, on a $\lambda_i = \mathrm{P}(\alpha_i)$; on en déduit que $(\lambda_0, \cdots, \lambda_n) \mapsto \sum_{i=0}^n \lambda_i \mathrm{Q}_i$ est injective. Par ailleurs, $\mathrm{P} - \sum_{i=0}^n \mathrm{P}(\alpha_i)\mathrm{Q}_i$ est de degré $\leqslant n$, et a $n+1$ zéros, à savoir $\alpha_0, \dots, \alpha_n$; il est donc nul, ce qui prouve que $(\lambda_0, \cdots, \lambda_n) \mapsto \sum_{i=0}^n \lambda_i \mathrm{Q}_i$ est surjective, et donc que les Q_i forment une base de $\mathrm{K}[\mathrm{X}]^{(n)}$. Les coordonnées de P dans cette base sont $(\mathrm{P}(\alpha_0), \dots, \mathrm{P}(\alpha_n))$.

Exercice 5.4. (i) Il s'agit de prouver que $(\lambda_i)_{i \in \mathbf{N}} \mapsto \sum_{i \in \mathbf{N}} \lambda_i \binom{\mathrm{X}}{i}$ est une bijection de $\mathrm{K}^{(\mathbf{N})}$ sur $\mathrm{K}[\mathrm{X}]$. Comme $\mathrm{K}^{(\mathbf{N})}$ est la réunion croissante des $\mathrm{K}^{\{0,\dots,n\}}$ et $\mathrm{K}[\mathrm{X}]$ celle des $\mathrm{K}[\mathrm{X}]^{(n)}$, il suffit de prouver que $(\lambda_0, \dots, \lambda_n) \mapsto \sum_{i=0}^n \lambda_i \binom{\mathrm{X}}{i}$ est une bijection de $\mathrm{K}^{\{0,\dots,n\}}$ sur $\mathrm{K}[\mathrm{X}]^{(n)}$. L'injectivité résulte de ce que $\sum_{i=0}^n \lambda_i \binom{\mathrm{X}}{i}$ est de degré le plus grand i vérifiant $\lambda_i \neq 0$, et donc est nul si et seulement si tous les λ_i sont nuls. Pour la surjectivité, on raisonne par récurrence sur n, le cas $n = 0$ étant évident. Si $\mathrm{P} = a_n \mathrm{X}^n + \cdots + a_0$, alors $\mathrm{P} - n! a_n \binom{\mathrm{X}}{n}$ est de degré $\leqslant n-1$ et peut donc s'écrire sous la forme $\sum_{i=0}^{n-1} \lambda_i \binom{\mathrm{X}}{i}$ d'après l'hypothèse de récurrence. On a alors $\mathrm{P} = n! a_n \binom{\mathrm{X}}{n} + \sum_{i=0}^{n-1} \lambda_i \binom{\mathrm{X}}{i}$, ce qui pouve la surjectivité pour n. (Le même argument prouverait que toute famille de polynômes $(\mathrm{P}_n)_{n \in \mathbf{N}}$, telle que P_n soit de degré n pour tout n, est une base de $\mathrm{K}[\mathrm{X}]$.)

(ii) Si $\mathrm{P} = \sum_{i=0}^n \lambda_i \binom{\mathrm{X}}{i}$, alors $\mathrm{P}(0) = \lambda_0$. Maintenant, $\mathrm{P}(\mathrm{X}+1) - \mathrm{P}(\mathrm{X}) = \sum_{i=1}^n \lambda_i \binom{\mathrm{X}}{i-1}$, et donc $\mathrm{P}(1) - \mathrm{P}(0) = \lambda_1$. En réitérant ce procédé, on obtient $\lambda_k = \mathrm{P}^{[k]}(0)$, où l'on a défini $\mathrm{P}^{[k]}$ par récurrence par $\mathrm{P}^{[0]} = \mathrm{P}$ et $\mathrm{P}^{[k+1]}(\mathrm{X}) = \mathrm{P}^{[k]}(\mathrm{X}+1) - \mathrm{P}^{[k]}(\mathrm{X})$, si $k \geqslant 0$. De manière plus explicite, on a $\lambda_k = \sum_{i=0}^k (-1)^i \binom{k}{i} \mathrm{P}(k-i)$.

(iii) Il résulte de la question précédente que si $\mathrm{P}(0), \dots, \mathrm{P}(n) \in \mathbf{Z}$, alors $\mathrm{P} = \sum_{i=0}^n \lambda_i \binom{\mathrm{X}}{i}$, avec $\lambda_0, \dots, \lambda_n \in \mathbf{Z}$. Comme $\binom{m}{i} \in \mathbf{Z}$ si $m \in \mathbf{Z}$, cela permet de conclure.

Exercice 5.5. Si $\sum_{i=1}^n \lambda_i |x - a_i| = 0$ pour tout $x \in \mathbf{R}$, où les a_i sont distincts deux à deux, et si un des λ_i est non nul, on aboutit à une contradiction car le membre de gauche n'est pas dérivable en a_i, alors que le membre de droite l'est. Les λ_i sont donc tous nuls, ce que l'on devait démontrer.

Exercice 5.6. (i) Soit $x \mapsto \phi(x) = \sum_{k=1}^n \lambda_k e^{a_k x}$ une combinaison linéaire identiquement nulle des $x \mapsto e^{ax}$, où les a_k sont distincts deux à deux. Quitte à rénuméroter les a_k, on peut supposer que $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n$, auquel cas $\lim_{x \to +\infty} e^{-a_n x} \phi(x) = \lambda_n$. Comme $e^{-a_n x}\phi(x) = 0$ pour tout x, cela nous donne $\lambda_n = 0$ et une récurrence montre que les λ_i sont tous nuls, ce que l'on voulait.

(ii) Soit $x \mapsto \phi(x) = \sum_{k=1}^n \lambda_k e^{i a_k x}$ une combinaison linéaire identiquement nulle des $x \mapsto e^{iax}$, où les a_i sont distincts deux à deux. Alors $\frac{1}{\mathrm{M}} \int_0^{\mathrm{M}} e^{-i a_k x} \phi(x)\, dx$ tend vers λ_k quand $\mathrm{M} \to +\infty$, et comme $\phi(x)$ est identiquement nulle, cela implique que $\lambda_k = 0$ pour tout k, ce qu'il fallait démontrer.

(iii) $x \mapsto e^{ax}$ est vecteur propre de $\frac{d}{dx}$ pour la valeur propre a. Le résultat suit donc de ce que les espaces propres associées à des valeurs propres distinctes sont en somme directe. (On peut aussi remarquer que

$x \mapsto e^{ax}$ est vecteur propre de τ_b définie par $\tau_b(\phi)(x) = \phi(x+b)$ pour la valeur propre e^{ab}, et choisir b de telle sorte que les $e^{a_k b}$ soient tous distincts si $x \mapsto \phi(x) = \sum_{k=1}^n \lambda_k e^{a_k x}$ une combinaison linéaire identiquement nulle des $x \mapsto e^{ax}$.)

(iv) Si $\sum_{k=1}^n (\lambda_k \cos a_k x + \mu_k \sin a_k x) = c$, pour tout $x \in \mathbf{R}$, où les $a_k \in \mathbf{R}_+^*$ sont distincts deux à deux, alors $-2ce^{0x} + \sum_{k=1}^n (\lambda_k - i\mu_k)e^{ia_k x} + \sum_{k=1}^n (\lambda_k + i\mu_k)e^{-ia_k x}$ est identiquement nul, et comme 0, les a_k et les $-a_k$ sont distincts deux à deux, cela implique, d'après le (ii) que $c = 0$ (et donc que les fonctions constantes non nulles ne sont pas dans l'espace engendré par les $x \mapsto \cos ax$ et les $x \mapsto \sin ax$), et que $\lambda_k - i\mu_k = \lambda_k + i\mu_k = 0$, et $\lambda_k = \mu_k = 0$, pour tout k (et donc que les $x \mapsto \sin ax$ et $x \mapsto \cos ax$ forment une famille libre).

Exercice 5.7. On a $x\frac{d}{dx}\mathrm{Li}_k(x) = x\sum_{n\geqslant 1} n\frac{x^{n-1}}{n^k} = \mathrm{Li}_{k-1}(x)$, si $k \geqslant 1$. Maintenant, soit $\sum_{k=0}^n \lambda_k \mathrm{Li}_k$ identiquement nulle sur $]-1,1[$. Montrons, par récurrence sur n, que les λ_k sont tous nuls. On a $\mathrm{Li}_0(x) = \frac{1}{1-x}$, $\mathrm{Li}_1(x) = -\log(1-x)$, et $\mathrm{Li}_k(x)$ a une limite finie $\sum_{n\geqslant 1}\frac{1}{n^k}$ en 1^-, si $k \geqslant 2$. Il s'ensuit que $(1-x)\sum_{k=0}^n \lambda_k \mathrm{Li}_k$ tend vers λ_0 en 1^-, et donc que $\lambda_0 = 0$ puisque $\sum_{k=0}^n \lambda_k \mathrm{Li}_k$ est identiquement nulle. En appliquant l'opérateur $x\frac{d}{dx}$, on obtient donc la relation $\sum_{k=0}^{n-1} \lambda_{k+1}\mathrm{Li}_k = 0$ et l'hypothèse de récurrence entraîne que $\lambda_k = 0$, si $k \geqslant 1$. Ceci permet de conclure.

Exercice 5.8. (i) Si les caractères forment une famille liée, il existe $n \geqslant 2$ minimal tel que l'on puisse trouver une combinaison linéaire $\sum_{k=1}^n \lambda_k \chi_k$ identiquement nulle sur G, où les χ_k sont distincts deux à deux, et alors aucun λ_k n'est nul puisque n est minimal. Si $h \in \mathrm{G}$, alors $\sum_{k=1}^n \lambda_k \chi_k(hg) = 0$ pour tout $g \in \mathrm{G}$, et comme $\chi_k(hg) = \chi_k(h)\chi_k(g)$, on obtient une seconde relation $\sum_{k=1}^n \lambda_k \chi_k(h)\chi_k = 0$. Comme $\chi_1 \neq \chi_2$, on peut trouver $h \in \mathrm{G}$ tel que $\chi_2(h) \neq \chi_1(h)$, et on obtient $0 = \chi_1(h)\big(\sum_{k=1}^n \lambda_k\chi_k\big) - \sum_{k=1}^n \lambda_k\chi_k(h)\chi_k = \sum_{k=2}^n \lambda_k(\chi_1(h)-\chi_k(h))\chi_k$. Par minimalité de n, cela implique $\lambda_k(\chi_1(h)-\chi_k(h)) = 0$ pour tout k, ce qui est en contradiction avec les hypothèses $\chi_2(h) \neq \chi_1(h)$ et $\lambda_2 \neq 0$. On en déduit le résultat.

(ii) Si $a \in \mathbf{C}$, alors $x \mapsto e^{ax}$ est un caractère linéaire de $(\mathbf{R}, +)$, et le (i) montre donc que les $x \mapsto e^{ax}$, pour $a \in \mathbf{C}$, sont linéairement indépendants, ce qui permet retrouver le (iii) de l'ex. 5.6 qui contient les (i) et (ii).

Exercice 5.9. Soit $\sum_{i=1}^n \lambda_i \log p_i$, où les λ_i sont des rationnels et les p_i distincts deux à deux, une combinaison linéaire nulle des $\log p$. Quitte à multiplier par le ppcm des dénominateurs des λ_i, on peut supposer que les λ_i sont des entiers. Alors $\prod_{i=1}^n p_i^{\lambda_i} = 1$, et donc $\lambda_j = v_{p_j}\big(\prod_{i=1}^n p_i^{\lambda_i}\big) = v_{p_j}(1) = 0$, pour tout j, ce qu'il fallait démontrer.

Exercice 6.1. (i) On a $(e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*)\big(v_{\tau(1)}, \ldots, v_{\tau(k)}\big) = \sum_{\sigma\in \mathrm{S}_k} \mathrm{sign}(\sigma) \prod_{j=1}^k x_{\tau(j),i_{\sigma(j)}}$, si $\tau \in \mathrm{S}_k$. On écrit $\sigma(j)$ sous la forme $\sigma\tau^{-1}(\tau(j))$ et $\mathrm{sign}(\sigma)$ sous la forme $\mathrm{sign}(\sigma\tau^{-1})\mathrm{sign}(\tau)$, et on fait les changements de variables $j' = \tau(j)$ et $\sigma' = \sigma\tau^{-1}$. On obtient

$$(e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*)\big(v_{\tau(1)}, \ldots, v_{\tau(k)}\big) = \mathrm{sign}(\tau)\Big(\sum_{\sigma'\in \mathrm{S}_k} \mathrm{sign}(\sigma') \prod_{j=1}^k x_{j',i_{\sigma'(j')}}\Big) = \mathrm{sign}(\tau)\big((e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*)(v_1, \ldots, v_k)\big).$$

Ceci prouve que $e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*$ est alternée.

(ii) On a $(e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*)(e_{i_1}, \ldots, e_{i_k}) = 1$ et $(e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*)(e_{\ell_1}, \ldots, e_{\ell_k}) = 0$ si $1 \leqslant \ell_1 < \cdots < \ell_k \leqslant n$, et si $(i_1, \ldots, i_k) \neq (\ell_1, \ldots, \ell_k)$. (En effet, $x_{j,i_{\sigma(j)}} = 0$ sauf si $\ell_j = i_{\sigma(j)}$, et donc $\prod_{j=1}^k x_{j,i_{\sigma(j)}} \neq 0$ implique $\{i_1, \ldots, i_k\} = \{\ell_1, \ldots, \ell_k\}$, et donc $i_1 = \ell_1, \ldots, i_k = \ell_k$, et $\sigma = \mathrm{id}$). On en déduit que les $e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*$ forment une famille libre (il suffit d'évaluer en $(e_{i_1}, \ldots, e_{i_k})$ une combinaison linéaire nulle pour en déduire la nullité du coefficient de $e_{i_1}^* \wedge \cdots \wedge e_{i_k}^*$).

(iii) Soit $f \in \wedge^k \mathrm{V}^*$. On a $f(\sum_{i=1}^n x_{1,i}e_i, \ldots, \sum_{i=1}^n x_{k,i}e_i) = \sum_{1\leqslant i_1,\ldots,i_k\leqslant n} f(e_{i_1}, \ldots, e_{i_k}) \prod_{j=1}^k x_{j,i_j}$, par k-linéarité de f. On utilise le fait que f est alternée pour éliminer les k-uplets où deux des i_j sont égaux, ce qui nous fournit une somme portant sur les k-uplets $(i_1, \ldots, i_k)$ où tous les termes sont

distincts. On utilise alors la formule $f(e_{i_{\sigma(1)}},\dots,e_{i_{\sigma(k)}}) = \mathrm{sign}(\sigma) f(e_{i_1},\dots,e_{i_k})$ pour ordonner les i_j, et on obtient $f(\sum_{i=1}^n x_{1,i}e_i,\dots,\sum_{i=1}^n x_{k,i}e_i) = \sum_{1\leqslant i_1<\dots<i_k\leqslant n}\sum_{\sigma\in \mathrm{S}_k}\mathrm{sign}(\sigma) f(e_{i_1},\dots,e_{i_k})\prod_{j=1}^k x_{j,i_{\sigma(j)}}$. Cette formule peut se réécrire sous la forme $f = \sum_{1\leqslant i_1<\dots<i_k\leqslant n} f(e_{i_1},\dots,e_{i_k}) e^*_{i_1}\wedge\dots\wedge e^*_{i_k}$, ce qui prouve que les $e^*_{i_1}\wedge\dots\wedge e^*_{i_k}$ forment une famille génératrice de $\wedge^k \mathrm{V}^*$, et donc une base d'après le (ii).

La dimension de $\wedge^k \mathrm{V}^*$ est donc le cardinal de l'ensemble des k-uplets $1\leqslant i_1<\dots<i_k\leqslant n$. Or cet ensemble est en bijection naturelle avec l'ensemble des parties à k éléments de $\{1,\dots,n\}$ (si I est une telle partie, on lui associe le k-uplet formé par ses éléments écrits dans l'ordre croissant), qui est de cardinal $\binom{n}{k}$. Cela permet de conclure.

Exercice 7.1 (i) Soient $\lambda_1,\dots,\lambda_n$ les coefficients diagonaux de A. On a alors $u_{\mathrm{A}}(e_i) = \lambda_i e_i$, et donc u_{A} n'est pas injective et A n'est pas inversible si l'un des λ_i est nul (car alors e_i est dans le noyau de u_{A}). Réciproquement, si tous les λ_i sont non nuls, soit A' la matrice diagonale dont les coefficients diagonaux sont les λ_i^{-1} ; alors $u_{\mathrm{A}'}\circ u_{\mathrm{A}}(e_i) = u_{\mathrm{A}'}(\lambda_i e_i) = \lambda_i u_{\mathrm{A}'}(e_i) = \lambda_i\lambda_i^{-1}e_i = e_i$, ce qui prouve que $u_{\mathrm{A}'}\circ u_{\mathrm{A}}$ est l'identité et donc que $\mathrm{A}'\mathrm{A} = 1$, et A est inversible d'inverse A'. Comme D est stable pour le produit de matrices puisque $\mathrm{Diag}(\lambda_1,\dots,\lambda_n)\mathrm{Diag}(\mu_1,\dots,\mu_n) = \mathrm{Diag}(\lambda_1\mu_1,\dots,\lambda_n\mu_n)$ et $\lambda_i\mu_i\neq 0$ si $\lambda_i\neq 0$ et $\mu_i\neq 0$, cela prouve que D est un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

(ii) Si A est diagonale et N triangulaire supérieure avec des 1 sur la diagonale, les coefficients diagonaux de AN sont ceux de A ; il s'ensuit que A doit être la matrice diagonale formée des coefficients diagonaux de T, et comme $\mathrm{N} = \mathrm{A}^{-1}\mathrm{T}$ est triangulaire supérieure en tant que produit de matrices triangulaires supérieures, et a des 1 sur la diagonale puisque les coefficients diagonaux de $\mathrm{A}^{-1}\mathrm{T}$ sont les quotients de ceux de T par ceux de A (qui sont égaux par construction), cela montre que $\mathrm{T} = \mathrm{AN}$ est une écriture de la forme voulue.

(iii) B est stable par multiplication puisque le produit de deux matrices triangulaires supérieures T_1 et T_2 est une matrice triangulaire supérieure dont les coefficients diagonaux sont les produits de ceux de T_1 et T_2, et donc sont non nuls si ceux de T_1 et T_2 le sont. Par ailleurs, si N est triangulaire supérieure avec des 1 sur la diagonale, alors N est unipotente, et donc N est inversible d'inverse $1+(1-\mathrm{N})+(1-\mathrm{N})^2+\cdots$ triangulaire supérieure puisque tous les termes de la somme le sont. Il s'ensuit que $\mathrm{T} = \mathrm{AN}\in\mathrm{B}$ est inversible d'inverse $\mathrm{T}^{-1}\mathrm{A}^{-1}\in\mathrm{B}$ puisque $\mathrm{T}^{-1}\in\mathrm{B}$ et $\mathrm{A}^{-1}\in\mathrm{B}$, et donc que B est stable par passage à l'inverse ; c'est donc un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

(iv) Que $\mathrm{T}\mapsto\mathrm{A}$ soit un morphisme de groupes est une traduction du fait que les coefficients diagonaux de $\mathrm{T}_1\mathrm{T}_2$ sont les produits de ceux de T_1 et T_2, si $\mathrm{T}_1,\mathrm{T}_2\in\mathrm{B}$. Le noyau de ce morphisme est U, et donc U est un sous-groupe de B, et donc aussi un sous-groupe de $\mathbf{GL}_n(\mathrm{K})$.

Exercice 7.2. $\det {}^{\mathrm{t}}\mathrm{A} = \det \mathrm{A}$, et comme ${}^{\mathrm{t}}\mathrm{A} = -\mathrm{A}$, on a aussi $\det {}^{\mathrm{t}}\mathrm{A} = (-1)^n \det \mathrm{A}$; d'où le résultat.

Exercice 7.3. Si on retire la première ligne aux autres, on peut mettre $a_1 - a_i$ en facteur dans la i-ième ligne et $\frac{1}{a_1+b_j}$ dans la j-ième colonne. La matrice ainsi obtenue a des 1 sur la première ligne et les autres lignes sont celles de la matrice initiale. Si on retranche alors la première colonne aux autres, on fait apparaître des 0 sur la première ligne et, comme précédemment, on peut mettre $b_1 - b_j$ en facteur dans la j-ième colonne et $\frac{1}{a_i+b_j}$ dans la i-ième ligne, si $i\geqslant 2$; la matrice obtenue est la même que la matrice initiale à part la première ligne qui devient $(1,0,\dots,0)$ et la première colonne qui devient ${}^{\mathrm{t}}(1,1\dots,1)$. On en déduit que

$$\mathrm{C}(a_1,\dots,a_n,b_1,\dots,b_n) = \prod_{i=2}^n (a_1-a_i)\prod_{j=2}^n (b_1-b_j)\prod_{i=1\text{ ou }j=1}\frac{1}{a_i+b_j}\mathrm{C}(a_2,\dots,a_n,b_2,\dots,b_n).$$

Une petite récurrence donne donc $\mathrm{C}(a_1,\dots,a_n,b_1,\dots,b_n) = \prod_{i<i'}(a_i-a_{i'})\prod_{j<j'}(b_j-b_{j'})\prod_{1\leqslant i,j\leqslant n}\frac{1}{a_i+b_j}$.

Exercice 7.4. Un petit calcul montre que AB est le produit de $\overline{\mathrm{B}}$ par la matrice diagonale dont les cofficients diagonaux sont les $a_0 + \eta^i a_1 + \cdots + a_{n-1}\eta^{(n-1)i}$, pour $0 \leqslant i \leqslant n-1$, et donc que

$$\det \mathrm{A} = (\det \overline{\mathrm{B}})(\det \mathrm{B})^{-1} \prod_{i=0}^{n-1} (a_0 + \eta^i a_1 + \cdots + a_{n-1}\eta^{(n-1)i}),$$

ce qui permet de conclure. (On peut calculer explicitement $(\det \overline{\mathrm{B}})(\det \mathrm{B})^{-1}$: en effet, B et $\overline{\mathrm{B}}$ sont des matrices de Vandermonde et leurs déterminants sont $\prod_{0\leqslant i,j\leqslant n-1}(\eta^j - \eta^i)$ et $\prod_{0\leqslant i,j\leqslant n-1}(\eta^{-j} - \eta^{-i})$ respectivement. Dans les deux produits ci-dessus, chaque paire de racines n-ième de l'unité apparaît exactement une fois, et le signe est le même si $i = 0$ (i.e. si une des racines est 1) ; pour les $\frac{(n-1)(n-2)}{2}$ paires $\{\eta_1, \eta_2\}$ restantes, $\eta_1 - \eta_2$ apparaît avec des signes opposés dans $\det \mathrm{B}$ et $\det \overline{\mathrm{B}}$. Il s'ensuit que $(\det \overline{\mathrm{B}})(\det \mathrm{B})^{-1} = (-1)^{(n-1)(n-2)/2}$.)

Exercice 7.5. (i) Un développement par rapport à la première colonne nous fournit la relation de récurrence $\det \mathrm{A}_{n+1} = (a + a^{-1})(\det \mathrm{A}_n) - \det \mathrm{A}_{n-1}$. Le résultat s'en déduit par une récurrence sans mystère si $a \neq \pm 1$. Si $a = \pm 1$, la même récurrence (ou un passage à la limite) donne $\det \mathrm{A}_n = 2n - 1$ si $a = 1$, et $\det \mathrm{A}_n = (-1)^n(2n-1)$ si $a = -1$.

(ii) λ est une valeur propre si et seulement si $\det(\lambda - \mathrm{U}_n) = 0$. On peut écrire λ sous la forme $a + a^{-1}$, et le (i) montre que $\det(\lambda - \mathrm{U}_n) = 0$ si et seulement si $a^{2(n+1)} = 1$ et $a \neq \pm 1$. On en déduit le résultat.

Exercice 7.6. La formule $\sum_{d|n} \varphi(d) = n$ s'obtient en remarquant que $i \mapsto i/d$ induit une bijection de l'ensemble des $i \in \{1, \ldots, n\}$ vérifiant $\mathrm{pgcd}(i, n) = d$ sur $(\mathbf{Z}/(n/d)\mathbf{Z})^*$.

Soient alors $\mathrm{B} = (b_{i,j})$ et $\mathrm{C} = (\mathrm{C}_{j,k})$ les matrices définies par $b_{i,j} = 1$ si $j \mid i$ et $b_{i,j} = 0$ si $j \nmid i$, et $c_{j,k} = \varphi(j)$ si $j \mid k$ et $c_{j,k} = 0$ si $j \nmid k$. Alors $\sum_{j=1}^{n} b_{i,j}c_{j,k} = \sum_{j|i,\, j|k} \varphi(j) = \sum_{j|\mathrm{pgcd}(i,k)} \varphi(j) = \mathrm{pgcd}(i, k)$, et donc $\mathrm{A} = \mathrm{BC}$. Comme B est triangulaire inférieure avec des 1 sur la diagonale et C est triangulaire supérieure avec les $\varphi(i)$ sur la diagonale, on obtient la formule demandée.

Cette solution peut paraître un peu miraculeuse, mais on obtient naturellement la factorisation de A ci-dessus en faisant des combinaisons linéaires des lignes de manière à faire apparaître un maximum de 0 : on retire la première ligne aux autres, puis les lignes correspondant aux nombres premiers à celles de leurs multiples, puis celles correspondant aux produits de 2 nombres premiers à celles de leurs multiples, etc.

Exercice 7.7. (i) Un développement de $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ par rapport à la dernière ligne montre que $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ est un polynôme de degré $n-1$ en X_n, de coefficient dominant $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_{n-1})$.

(ii) $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ s'annule en $\mathrm{X}_n = \mathrm{X}_1, \ldots, \mathrm{X}_n = \mathrm{X}_{n-1}$ car alors deux lignes du déterminant sont égales. Comme $\mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$ est intègre, et comme $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ est de degré $n-1$ en X_n, cela implique que $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = a_{n-1}(\mathrm{X}_n - \mathrm{X}_1) \cdots (\mathrm{X}_n - \mathrm{X}_{n-1})$, où a_{n-1} est le coefficient dominant et est égal à $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_{n-1})$, d'après le (i). On en déduit que $\mathrm{VdM}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \prod_{i<j}(\mathrm{X}_j - \mathrm{X}_i)$, par récurrence, et le résultat pour $\mathrm{VdM}(\alpha_1, \ldots, \alpha_n)$ s'obtient en spécialisant en $\mathrm{X}_1 = \alpha_1, \ldots, \mathrm{X}_n = \alpha_n$.

Exercice 7.8. Il suffit de recopier la solution de l'ex. 7.1.

Exercice 7.9. (i) $\Gamma(\mathrm{D})$ est le noyau de la réduction modulo D de $\mathbf{SL}_2(\mathbf{Z})$ dans $\mathbf{SL}_2(\mathbf{Z}/\mathrm{D}\mathbf{Z})$ (induite par la réduction modulo D de $\mathbf{Z}$ dans $\mathbf{Z}/\mathrm{D}\mathbf{Z}$) ; c'est donc un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$.

(ii) $\Gamma_0(\mathrm{D})$ est l'image inverse dans $\mathbf{SL}_2(\mathbf{Z})$ de l'ensemble B des matrices triangulaires supérieures de $\mathbf{SL}_2(\mathbf{Z}/\mathrm{D}\mathbf{Z})$. Or une matrice triangulaire supérieure appartenant à $\mathbf{SL}_2(\mathbf{Z}/\mathrm{D}\mathbf{Z})$ a ses coefficients diagonaux inversibles puisque leur produit est égal à 1, et son inverse est encore triangulaire supérieure. Il en résulte que B est un sous-groupe de $\mathbf{SL}_2(\mathbf{Z}/\mathrm{D}\mathbf{Z})$ et donc que $\Gamma_0(\mathrm{D})$ est un sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$.

Exercice 8.1. (i) Si $\mathrm{X}^3 + \mathrm{X} + 1$ n'est pas irréductible, on peut le factoriser sous la forme PQ, avec $\deg \mathrm{P} + \deg \mathrm{Q} = 3$, ce qui fait que l'un des deux polynômes est de degré 1, et donc que $\mathrm{X}^3 + \mathrm{X} + 1$ a une racine α dans $\mathbf{Q}$. Soit p un nombre premier. Si $v_p(\alpha) < 0$, alors $v_p(\alpha^3) = 3v_p(\alpha) < v_p(\alpha) \leqslant v_p(-\alpha - 1)$,

et donc $\alpha^3 \neq -\alpha - 1$. Il s'ensuit que $v_p(\alpha) \geqslant 0$, pour tout p ; autrement dit, $\alpha \in \mathbf{Z}$. Mais ceci n'est pas possible car $\alpha^3 + \alpha + 1 \geqslant 1$, si $\alpha \in \mathbf{N}$, et $\alpha^3 + \alpha + 1 \leqslant -1$, si $\alpha \leqslant -1$.

(ii) Comme $\mathrm{X}^3 + \mathrm{X} + 1$ est irréductible, c'est le polynôme minimal de α, et donc $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$. Maintenant, si K contient α, il contient $\mathbf{Q}(\alpha)$, et l'identité $[\mathrm{K} : \mathbf{Q}] = [\mathrm{K} : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 3\,[\mathrm{K} : \mathbf{Q}(\alpha)]$ permet de conclure.

(iii) Supposons le contraire, alors il existe $n_1, \ldots, n_r$ tel que α appartienne à $\mathrm{F} = \mathbf{Q}(\sqrt{n_1}, \ldots, \sqrt{n_r})$. Notons F_i le sous-corps $\mathbf{Q}(\sqrt{n_1}, \ldots, \sqrt{n_i})$ de F_i, et posons $\mathrm{F}_0 = \mathbf{Q}$. On a $\mathrm{F}_{i+1} = \mathrm{F}_i(\sqrt{n_{i+1}})$, ce qui prouve que $[\mathrm{F}_{i+1} : \mathrm{F}_i]$ est égal à 1 ou 2. On en déduit que $[\mathrm{F} : \mathbf{Q}]$, qui est égal à $[\mathrm{F}_r : \mathrm{F}_{r-1}] \cdots [\mathrm{F}_1 : \mathrm{F}_0]$ est une puissance de 2, ce qui est en contradiction avec l'hypothèse $\alpha \in \mathrm{F}$ qui implique que $3 = [\mathbf{Q}(\alpha) : \mathbf{Q}]$ divise $[\mathrm{F} : \mathbf{Q}]$. On en déduit le résultat.

Exercice 8.2. (i) On a $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})]\,[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$. Or $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ car le polynôme minimal de $\sqrt{2}$ sur $\mathbf{Q}$ est $\mathrm{X}^2 - 2$ (irrationalité de $\sqrt{2}$). Comme le polynôme minimal de $\sqrt{3}$ sur $\mathbf{Q}(\sqrt{2})$ divise $\mathrm{X}^2 - 3$, il est de degré 1 ou 2, et pour conclure, il suffit donc de prouver qu'il n'est pas de degré 1 ou, autrement dit, que $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$. Supposons le contraire ; on a alors $\sqrt{3} = a + b\sqrt{2}$, avec $a, b \in \mathbf{Q}$. On en déduit que $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, et comme $1, \sqrt{2}$ sont libres sur $\mathbf{Q}$, cela implique que $ab = 0$ et $a^2 = 3$ ou $2b^2 = 3$, ce qui est impossible pour les mêmes raisons que $\sqrt{2}$ est irrationnel.

(ii) On peut numéroter les racines de telle sorte que $\alpha_1 = \sqrt[3]{2}$ soit réel et α_2, α_3 soient complexes conjugués. Le polynôme $\mathrm{X}^3 - 2$ est irréductible dans $\mathbf{Q}[\mathrm{X}]$, sinon il aurait une racine rationnelle α et on aurait $3v_2(\alpha) = 1$, ce qui est absurde. Il en résulte que $[\mathbf{Q}(\alpha_i) : \mathbf{Q}] = 3$, si $i = 1, 2, 3$. Ceci est en particulier vrai pour la racine réelle $\alpha_1 = \sqrt[3]{2}$. Maintenant, $\mathrm{X}^3 - 2$ se factorise sous la forme $(\mathrm{X} - \alpha_1)(\mathrm{X}^2 + \alpha_1\mathrm{X} + \alpha_1^2)$ dans $\mathbf{Q}(\alpha_1)$. Il en résulte que α_2 est de degré 1 ou 2 sur $\mathbf{Q}(\alpha_1)$, et comme α_2 n'est pas réel, il ne peut pas appartenir à $\mathbf{Q}(\alpha_1)$, et on a $[\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}(\alpha_1)] = 2$. Enfin, comme $\alpha_1 + \alpha_2 + \alpha_3 = 0$, on a $\alpha_3 \in \mathbf{Q}(\alpha_1, \alpha_2)$ et donc $\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbf{Q}(\alpha_1, \alpha_2)$. On en déduit le résultat.

(iii) Comme $\mathrm{F}(\alpha, \beta)$ contient $\mathrm{F}(\alpha)$ et $\mathrm{F}(\beta)$, son degré est divisible par $[\mathrm{F}(\alpha) : \mathrm{F}] = r$ et $[\mathrm{F}(\beta) : \mathrm{F}] = s$, et donc par rs puisque $(r, s) = 1$. Il s'ensuit que $[\mathrm{F}(\alpha, \beta) : \mathrm{F}(\beta)] = \frac{[\mathrm{F}(\alpha,\beta):\mathrm{F}]}{[\mathrm{F}(\beta):\mathrm{F}]}$ est divisible par r et donc que le degré de α sur $\mathrm{F}(\beta)$ est un multiple de r. Comme ce degré est le degré du polynôme minimal de α sur $\mathrm{F}(\beta)$, et que ce polynôme divise le polynôme minimal de α sur F, il est $\leqslant r$, et donc égal à r, ce que l'on cherchait à prouver.

Le (ii) montre que le résultat n'est pas forcément vrai si $(r, s) \neq 1$.

Exercice 8.3 (i) Q_t est symétrique en $\alpha_1, \ldots, \alpha_d$; ses coefficients sont donc des polynômes en t et les coefficients de P, qui sont réels par hypothèse ; on en déduit l'appartenance de Q_t à $\mathbf{R}[\mathrm{X}]$.

(ii) On a $\deg \mathrm{Q}_t = \frac{n(n-1)}{2}$, et comme l'hypothèse $v_2(\deg \mathrm{P}) \geqslant 1$ entraîne $v_2(n-1) = 0$, on a $v_2(\deg \mathrm{Q}_t) = v_2(n) - 1 = v_2(\deg \mathrm{P}) - 1$.

Maintenant, si $r = v_2(\deg \mathrm{P}) = 0$, cela veut dire que P est de degré impair et donc $\lim_{x\to+\infty} \mathrm{P}(x) = +\infty$, et $\lim_{x\to-\infty} \mathrm{P}(x) = -\infty$ et P a un zéro dans $\mathbf{R}$ (et donc dans $\mathbf{C}$) d'après le th. des valeurs intermédiaires ; l'hypothèse est donc vraie pour $r = 0$.

Si $r \geqslant 1$, on peut appliquer l'hypothèse de récurrence à Q_t, pour tout t, puisque $v_2(\deg \mathrm{Q}_t) = r - 1$. On en déduit que, pour tout $t \in \mathbf{R}$, il existe $i(t) < j(t)$ tel que $\alpha_{i(t)} + \alpha_{j(t)} + t\alpha_{i(t)}\alpha_{j(t)} \in \mathbf{C}$. L'application $t \mapsto (i(t), j(t))$ n'est pas injective pour des raisons de cardinal ; il existe donc $i < j$ et $t_1 \neq t_2$ tels que $\alpha_i + \alpha_j + t_k\alpha_i\alpha_j \in \mathbf{C}$, si $k = 1, 2$. On en déduit que $s = \alpha_i + \alpha_j$ et $p = \alpha_i\alpha_j$ appartiennent à $\mathbf{C}$ et donc que α_i, α_j, qui sont les racines de $\mathrm{X}^2 - s\mathrm{X} + p$, appartiennent à $\mathbf{C}$ (les racines de ce polynôme sont $\frac{1}{2}(s \pm \sqrt{s^2 - 4p})$, et $\pm\sqrt{s^2 - 4p} = \pm\sqrt{r}e^{i\alpha/2}$, si $s^2 - 4p = re^{i\alpha}$).

(iii) Il s'agit de prouver que tout $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$, unitaire de degré $\geqslant 1$, a une racine dans $\mathbf{C}$. Or $\mathrm{P}\overline{\mathrm{P}} \in \mathbf{R}[\mathrm{X}]$ et donc a une racine $\alpha \in \mathbf{C}$. On a donc $0 = \mathrm{P}(\alpha)\overline{\mathrm{P}}(\alpha) = \mathrm{P}(\alpha)\overline{\mathrm{P}(\bar{\alpha})} = 0$, ce qui prouve que α ou $\bar{\alpha}$ est une racine de P, et permet de conclure.

Exercice 8.4. Il suffit de recopier la démonstration du cas $\mathrm{F} = \mathbf{F}_p$ en remplaçant p par q, et en utilisant le fait que $\mathrm{F} = \{x \in \mathrm{K},\ x^q = x\}$ d'après le point précédant l'exercice.

Exercice 8.5. Supposons le contraire, et choisisons $v_1 \in \mathrm{W} - \mathrm{W}_1, \ldots, v_n \in \mathrm{W} - \mathrm{W}_n$. Si $t \in \mathrm{F}$, soit $v(t) = v_1 + tv_2 + \cdots + t^{n-1}v_n$; c'est un élément de W puisque W est un espace vectoriel par hypothèse, et il existe donc $i(t)$ tel que $v(t) \in \mathrm{W}_{i(t)}$. Comme F est infini, il existe $i \in \{1, \ldots, n\}$ tel que $i(t) = i$ pour une infinité de t. Soient $t_1, \ldots, t_n \in \mathrm{F}$, distincts, tels que $i(t_j) = i$, pour $j \in \{1, \ldots, n\}$. Le déterminant du système exprimant les $v(t_j)$ en fonction des v_k est non nul (c'est un déterminant de Vandermonde qui vaut $\prod_{i<j}(t_j - t_i)$), ce qui fait que l'on peut exprimer les v_k comme des combinaisons linéaires des $v(t_j)$. En particulier, on a $v_i \in \mathrm{W}_i$, contrairement à l'hypothèse, d'où une contradiction qui permet de conclure.

Exercice 9.1. Soit $x \mapsto \sum_{k=1}^n \lambda_k \log(x + a_k)$ une combinaison linéaire des $x \mapsto \log(x + a)$, où les a_k sont distincts deux à deux, identiquement nulle sur $\mathbf{R}_+$. En dérivant i fois, on obtient la relation $\sum_{k=1}^n \lambda_k \frac{1}{(x+a_k)^i} = 0$ pour tout $x \in \mathbf{R}_+^*$. En prenant $i = 1, \ldots, n$ et $x = 0$, on voit que les $a_k^{-1}\lambda_k$ sont solutions d'un système $\sum_{k=1}^n b_{i,k}a_k^{-1}\lambda_k = 0$, pour $1 \leqslant i \leqslant n$, avec $b_{i,k} = a_k^{1-i}$. Le déterminant de ce système est non nul (c'est un déterminant de Vandermonde), et la seule solution de ce système est donc $\lambda_1 = \cdots = \lambda_n = 0$. On en déduit le résultat.

Exercice 9.2. (i) Si $z_k \in \mathbf{C}$, pour $1 \leqslant k \leqslant \mathrm{N}$, alors $\left|\frac{1}{\mathrm{N}}\sum_{k=1}^{\mathrm{N}} z_k\right| \leqslant \sup_{1\leqslant k\leqslant \mathrm{N}} |z_k|$, avec égalité si et seulement si les z_k sont tous égaux. On en déduit que si $|x_{i,j}|$ atteint son maximum pour i_0, j_0 qui n'est pas sur le bord, alors $x_{i,j} = x_{i_0,j_0}$ si $|i - i_0| \leqslant 1$ et $|j - j_0| \leqslant 1$. Mais alors $|x_{i,j}|$ est maximum pour tout (i, j) vérifiant $|i - i_0| \leqslant 1$ et $|j - j_0| \leqslant 1$. On peut donc recommencer et en déduire que $x_{i,j} = x_{i_0,j_0}$ si $|i - i_0| \leqslant 2$ et $|j - j_0| \leqslant 2$. Une petite récurrence permet donc de prouver que $x_{i,j} = x_{i_0,j_0}$ pour tout couple (i, j), et donc en particulier pour un couple sur le bord, ce qui prouve que le maximum de $|x_{i,j}|$ est atteint sur le bord aussi.

(ii) Si $x_{i,j} = 0$ sur le bord, alors $\sup_{i,j} |x_{i,j}| = 0$ d'après le (i), et donc $x_{i,j} = 0$ pour tous i, j.

(iii) On obtient les valeurs au centre du carré en fonction des valeurs au bord en résolvant un système linéaire de n^2 équations à n^2 inconnues, avec second membre. D'après le (ii), la seule solution de ce système est la solution nulle si le second membre est nul ; il s'ensuit que le système est de Cramer, et donc qu'il y a une et une seule solution pour tout choix de second membre. Ceci permet de conclure.

Exercice 9.3. (i) $\mathrm{rg}(\mathrm{UAV}) = \dim(u_\mathrm{U} \circ u_\mathrm{A} \circ u_\mathrm{V}(\mathrm{K}^m))$. Or $u_\mathrm{V}(\mathrm{K}^m) = \mathrm{K}^m$, et $\dim u_\mathrm{U}(\mathrm{V}) = \dim \mathrm{V}$, si V est un sous-espace de K^n, puisque u_U est injective. On a donc $\dim(u_\mathrm{U} \circ u_\mathrm{A} \circ u_\mathrm{V}(\mathrm{K}^m)) = \dim u_\mathrm{A}(\mathrm{K}^m) = \mathrm{rg}(\mathrm{A})$.

(ii) $(\mathrm{U}_2, \mathrm{V}_2)\cdot((\mathrm{U}_1, \mathrm{V}_1)\cdot \mathrm{M}) = (\mathrm{U}_2, \mathrm{V}_2)\cdot \mathrm{U}_1\mathrm{M}\mathrm{V}_1^{-1} = \mathrm{U}_2\mathrm{U}_1\mathrm{M}\mathrm{V}_1^{-1}\mathrm{V}_2^{-1} = (\mathrm{U}_2\mathrm{U}_1, \mathrm{V}_2\mathrm{V}_1)\cdot \mathrm{M}$, ce qui prouve que l'on a bien défini une action de groupe.

(iii) Il résulte du point précédant l'exercice que toute matrice de rang r est dans l'orbite de $\mathrm{I}_{n,m}(r)$, et donc les matrices de rang r sont incluses dans une orbite. Par ailleurs, le (i) montre que des matrices de rangs différents sont dans des orbites différentes ; l'ensemble des orbites est donc en bijection avec l'ensemble des rangs possibles, et il y a $s + 1$ orbites, si $s = \inf(n, m)$.

Exercice 10.1. (i) Comme A est noethérien, tout sous-module d'un module de type fini, et donc $\mathrm{M}_{\mathrm{tors}}$ est de type fini. Soient $x_1, \ldots, x_n$ engendrant $\mathrm{M}_{\mathrm{tors}}$ et, si $1 \leqslant i \leqslant n$, soit $a_i \in \mathrm{A} - \{0\}$ tel que $a_i x_i = 0$. Alors $a = \prod_{i=1}^n a_i \neq 0$ puisque A est intègre, et $ax_i = 0$ pour tout i. Il s'ensuit que $ax = 0$ pour toute combinaison linéaire x des x_i, et donc pour tout $x \in \mathrm{M}_{\mathrm{tors}}$ puisque les x_i engendrent $\mathrm{M}_{\mathrm{tors}}$.

(ii) Comme $\mathbf{Z}$ est noethérien, $\mathrm{M}_{\mathrm{tors}}$ est de type fini. Si $x_1, \ldots, x_n$ engendrent $\mathrm{M}_{\mathrm{tors}}$, on dispose d'une surjection $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i x_i$ de $\mathbf{Z}^n$ sur $\mathrm{M}_{\mathrm{tors}}$. Par ailleurs, il existe $d_i \in \mathbf{N} - \{0\}$ tel que $d_i x_i = 0$; la surjection précédente se factorise donc à travers $\prod_{i=1}^n (\mathbf{Z}/d_i\mathbf{Z})$ qui est un groupe fini, de cardinal $\prod_{i=1}^n d_i$; il en résulte que $\mathrm{M}_{\mathrm{tors}}$ est fini, de cardinal $\leqslant \prod_{i=1}^n d_i$. Le groupe des racines de l'unité de $\mathbf{C}^*$ (isomorphe à $\mathbf{Q}/\mathbf{Z}$) est un $\mathbf{Z}$-module de torsion qui n'est pas fini (et donc pas de type fini non plus).

Exercice 10.2. C'est un cas particulier du fait que tout idéal premier d'un anneau principal est maximal, mais on peut en donner une démonstration plus directe. Soit $d = \deg \mathrm{Q}$. Alors $\mathrm{K[X]/Q}$ est un K-espace vectoriel de dimension d (de base $(1, \ldots, \mathrm{X}^{d-1})$), et si $\mathrm{P} \in \mathrm{K[X]}$ n'est pas divisible par Q, la multiplication par P est injective sur $\mathrm{K[X]/Q}$ (si R est dans le noyau, alors PR est divisible par Q, et comme Q est irréductible, P est premier à Q, et cela implique que R est divisible par Q, et donc est nul dans $\mathrm{K[X]/Q}$), et donc est surjective, ce qui prouve que tout élément non nul de $\mathrm{K[X]/Q}$ a un inverse (la surjectivité entraîne en particulier l'existence de R tel que $\mathrm{PR} = 1$).

Exercice 10.16. Soit $f = {}^{\mathrm{t}}(a_1, \ldots, a_n)$, et soit Λ le sous-$\mathbf{Z}$-module de $\mathbf{Z}^n$ engendré par Λ. Comme Λ est de rang 1, il existe une base $f_1, \ldots, f_n$ de $\mathbf{Z}^n$ sur $\mathbf{Z}$ et $\delta \in \mathbf{Z}$, tels que δf_1 soit une base de Λ. Or les bases de Λ sont $\pm f$, et on peut donc, quitte à changer f_1 de signe, supposer que $\delta f_1 = f$ et $\delta > 0$. Par ailleurs, comme les a_i sont premiers entre eux, on a $\delta \in \mathbf{Z}^*$, et donc $\delta = 1$. Il s'ensuit que la matrice A, dont les colonnes sont $f, f_2, \ldots, f_n$, appartient à $\mathbf{GL}_2(\mathbf{Z})$; son déterminant est donc ± 1 et, quitte à changer f_n en $-f_n$, on peut s'arranger pour que $\det \mathrm{A} = 1$. La matrice A répond alors à la question.

Exercice 10.17. (i) Les M_k forment une famille libre sur $\mathbf{Q}$ si et seulement si il existe un mineur d'ordre r non nul dans la matrice des M_k dans la base des $\mathrm{U}_{i,j}$. Cette condition ne fait pas intervenir le corps sur lequel on travaille, ce qui prouve que les M_k sont libres sur $\mathbf{Q}$ si et seulement si ils le sont sur $\mathbf{C}$.

(ii) L'équation $\mathrm{AM} = \mathrm{MB}$ est une équation linéaire à coefficients dans $\mathbf{Q}$. La dimension de l'espace de ses solutions $\mathrm{E}_{\mathbf{Q}}$ sur $\mathbf{Q}$ ou $\mathrm{E}_{\mathbf{C}}$ sur $\mathbf{C}$ est la même puisqu'elle s'exprime en termes de rang de la matrice du système. On déduit donc du (i) qu'une base de $\mathrm{E}_{\mathbf{Q}}$ sur $\mathbf{Q}$ est aussi une base de $\mathrm{E}_{\mathbf{C}}$ sur $\mathbf{C}$.

(iii) Comme $\mathrm{M}_1, \ldots, \mathrm{M}_r \in \mathbf{M}_n(\mathbf{Q})$, on a $\det(\mathrm{X}_1\mathrm{M}_1 + \cdots \mathrm{X}_r\mathrm{M}_r) \in \mathbf{Q}[\mathrm{X}_1, \ldots, \mathrm{X}_r]$. Par ailleurs, $\mathrm{P}_0 \in \mathrm{E}_{\mathbf{C}}$ et comme $\det \mathrm{P}_0 \neq 0$, il s'ensuit que la fonction polynomiale sur $\mathbf{C}^r$ définie par Q n'est pas identiquement nulle, et donc $\mathrm{Q} \neq 0$.

(iv) Comme $\mathrm{Q} \neq 0$ et comme $\mathbf{Q}$ est un corps infini, il existe $x_1, \ldots, x_r \in \mathbf{Q}$ tels que $\mathrm{Q}(x_1, \ldots, x_r) \neq 0$. la matrice $\mathrm{P} = x_1\mathrm{M}_1 + \cdots + x_r\mathrm{M}_r$ répond à la question.

Exercice 11.2. La vérification de ce que d est une distance ne pose pas de problème, et comme les singletons sont ouverts puisque $\{x\} = \mathrm{B}(x, (1/2)^-)$, la topologie associée est la topologie discrète.

Exercice 11.3. Si $d'(x, y) = 0$, on a $f(x) = f(y)$ et donc $x = y$ car f est injective (strictement croissante). La symétrie est évidente et l'inégalité triangulaire résulte de ce que $d'(x, z) = |f(x) - f(z)| \leqslant |f(x) - f(y)| + |f(y) - f(z)| = d'(x, y) + d'(y, z)$. Il reste à prouver que si $x \in \mathbf{R}$ et si $\varepsilon > 0$, il existe $\delta > 0$ tel que $d(x, y) < \delta$ implique $d'(x, y) < \varepsilon$ et $d'(x, y) < \delta$ implique $d(x, y) < \varepsilon$, ce qui résulte de la continuité de f et de sa réciproque $g(x) = \frac{x}{1-|x|}$, si $x \in]-1, 1[$.

Exercice 11.5. C'est la topologie grossière : si $x \in \mathbf{R}$ et si U est un ouvert non vide de $\mathbf{R}$, alors U contient un élément de la forme $x + r$, avec $r \in \mathbf{Q}$, et donc tout ouvert non vide de $\mathbf{R}/\mathbf{Q}$ contient l'image de x, pour tout x, et donc est égal à $\mathbf{R}/\mathbf{Q}$.

Exercice 11.6. Soient $a \neq b$ deux points de X. Comme f est injective, on a $f(a) \neq f(b)$, et comme Y est séparé, on peut trouver des ouverts disjoints U et V de Y tels que $f(a) \in \mathrm{U}$ et $f(b) \in \mathrm{V}$. Maintenant, comme f est continue, $f^{-1}(\mathrm{U})$ et $f^{-1}(\mathrm{V})$ sont des ouverts de X, qui sont disjoints car U et V le sont, et qui contiennent respectivement a et b. Ceci permet de conclure.

Exercice 11.7. Il suffit de passer aux complémentaires.

Exercice 11.8. (i) Soit $\mathrm{U} \neq \varnothing$ un ouvert de $\mathrm{X}_1 \times \mathrm{X}_2$. Il existe alors $\mathrm{U}_1 \neq \varnothing$ ouvert de X_1 et $\mathrm{U}_2 \neq \varnothing$ ouvert de X_2 tels que U contienne $\mathrm{U}_1 \times \mathrm{U}_2$. Comme Y_1 est dense, $\mathrm{Y}_1 \cap \mathrm{U}_1$ est non vide et comme Y_2 est dense, il en est de même de $\mathrm{Y}_2 \cap \mathrm{U}_2$, ce qui montre que $(\mathrm{Y}_1 \times \mathrm{Y}_2) \cap \mathrm{U}$ qui contient $(\mathrm{Y}_1 \times \mathrm{Y}_2) \cap (\mathrm{U}_1 \times \mathrm{U}_2) = (\mathrm{Y}_1 \cap \mathrm{U}_1) \times (\mathrm{Y}_2 \cap \mathrm{U}_2)$ est non vide. On en déduit la densité de $\mathrm{Y}_1 \times \mathrm{Y}_2$.

(ii) Soient $g : \mathrm{Y} \times \mathrm{Y} \to \mathbf{R}_+$ définie par $g(x, x') = d_{\mathrm{Y}}(x, x')$ et $h : \mathrm{Y} \times \mathrm{Y} \to \mathbf{R}_+$ définie par $g(x, x') = d_{\mathrm{Z}}(f(x'), f(x'))$. On cherche à prouver que g et h sont égales. Or elles sont égales sur $\mathrm{X} \times \mathrm{X}$ par hypothèse,

et comme $X \times X$ est dense dans $Y \times Y$, et Z est séparé car métrique, on peut en conclure qu'elles sont égales sur $Y \times Y$, en utilisant le point précédant l'exercice (ou l'ex. 11.11).

Exercice 11.9. (i) Comme $\overline{U}$ contient U, son intérieur, qui est le plus grand ouvert contenu dans $\overline{U}$ contient U. Si U est l'ouvert $]0,1[\cup]1,2[$ de $\mathbf{R}$, alors $\overline{U} = [0,2]$ et l'intérieur de $\overline{U}$ est $]0,2[$ qui contient strictement U. Revenons au cas d'un ouvert général U et notons V l'intérieur de son adhérence. Comme $U \subset V$, on a $\overline{U} \subset \overline{V}$, et comme $\overline{U}$ est un fermé qui contient V, on a $\overline{V} \subset \overline{U}$, et donc $\overline{V} = \overline{U}$, ce qui termine la démonstration du (i).

Le (ii) se déduit du (i) en passant aux complémentaires.

Exercice 11.10. Si A n'est pas dense, son adhérence n'est pas $\mathbf{C}^2$, et il existe un polynôme $P \in \mathbf{C}[X,Y]$ non nul s'annulant sur A. Soit donc $P \in \mathbf{C}[X,Y]$ tel que $P(n, e^n) = 0$ pour tout $n \in \mathbf{N}$. On écrit P sous la forme $P(X,Y) = P_d(X)Y^d + \cdots + P_0(X)$, avec $P_0, \ldots, P_d \in \mathbf{C}[X]$. On a donc $P_d(n)e^{dn} + \cdots + P_0(n) = 0$ pour tout n, et en divisant par e^{dn}, on en déduit que $P_d(n) \to 0$ quand $n \to +\infty$. Ceci n'est possible que si $P_d = 0$. On en déduit que $P = 0$; d'où la densité de A dans $\mathbf{C}^2$.

A n'est pas dense dans $\mathbf{C}^2$ pour la topologie usuelle car A ne contient aucun point de l'ouvert $\{z = (z_1, z_2),\ \sup(|z_1|, |z_2|) < 1\}$. En fait, il n'est pas difficile de voir que A est fermé dans $\mathbf{C}^2$ pour la topologie usuelle.

Exercice 11.11. Si X est métrisable, la topologie peut être définie par une métrique d, ce qui permet de supposer que (X,d) est métrique dans tout ce qui suit.

(i) Soit $a \in X$. Comme les $B(a, 2^{-n})$ forment une base de voisinages de a, on voit que si $a \in \overline{Z}$, alors, pour tout $n \in \mathbf{N}$, il existe $x_n \in Z$ avec $d(a, x_n) \leqslant 2^{-n}$; la suite $(x_n)_{n\in\mathbf{N}}$ a alors a comme limite. Réciproquement, si $(x_n)_{n\in\mathbf{N}}$ est une suite d'éléments de Z ayant a pour limite, et si U est un voisinage de a, alors $x_n \in U$, pour tout n assez grand, ce qui prouve que U contient des éléments de Z, et permet de montrer que $a \in \overline{Z}$ (noter que ce sens n'a pas utilisé le fait que X est métrique).

(ii) Z est dense dans X si et seulement si $\overline{Z} = X$, et donc le résultat suit du (i).

(iii) Si $x \in X$, il existe une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de Z tendant vers x. Mais alors $f(x_n)$ tend vers $f(x)$ et $g(x_n)$ tend vers $g(x)$ puisque f et g sont continues, et comme $f(x_n) = g(x_n)$ pour tout n, cela implique que $f(x)$ et $g(x)$ sont des limites de la suite $(f(x_n))_{n\in\mathbf{N}}$. Comme Y est supposé métrique et donc séparé, il y a unicité de la limite d'une suite et donc $f(x) = g(x)$.

Exercice 12.1. (i) Soit $n \mapsto x_n$ une bijection de $\mathbf{N}$ sur X. Il suffit de prendre $]a_n, b_n[=]x_n - \frac{\varepsilon}{2^{n+3}}, x_n + \frac{\varepsilon}{2^{n+3}}[$.

(ii) Comme $[0,1]$ est compact, si les $]a_n, b_n[$, pour $n \in \mathbf{N}$, recouvrent $[0,1]$, on peut en extraire un recouvrement fini, et le résultat suit du cas d'une famille finie. (Pour démontrer le résultat dans le cas d'une famille finie, on peut remarquer que $\sum_{n\in J}(b_n - a_n)$ est l'intégrale (de Riemann) de la fonction continue par morceaux $\phi = \sum_{n\in J} \mathbf{1}_{]a_n,b_n[}$. Or l'hypothèse $[0,1] \subset \cup_{n\in J}]a_n, b_n[$ se traduit par $\phi(x) \geqslant 1$, si $x \in [0,1]$, et donc l'intégrale de ϕ est supérieure ou égale à celle de $\mathbf{1}_{[0,1]}$ qui vaut 1. L'exercice permet de montrer que l'intégrale de Lebesgue de $\mathbf{1}_{[0,1]}$ est supérieure ou égale à 1 et donc aussi égale à 1, ce qui est rassurant...)

(iii) Si $[0,1]$ était dénombrable, il existerait d'après le (i) une suite de segments $]a_n, b_n[$ recouvrant $[0,1]$ et telle que $\sum_{n\in\mathbf{N}}(b_n - a_n) \leqslant \frac{1}{2}$, ce qui contredit le (ii). Le segment $[0,1]$ n'est donc pas dénombrable ; il en est a fortiori de même de $\mathbf{R}$ qui le contient.

Exercice 12.2. (i) Soit X un compact métrique, et soient $(x_n)_{n\in\mathbf{N}}$ ayant une unique valeur d'adhérence a, et U un ouvert contenant a. Alors $X - U$ ne contient qu'un nombre fini de termes de la suite, sinon on pourrait extraire une sous-suite $(x_{\varphi(n)})_{n\in\mathbf{N}}$ de $(x_n)_{n\in\mathbf{N}}$, dont tous les termes sont dans $X - U$, et comme $X - U$ est compact puisque fermé dans un compact, cela implique que $(x_{\varphi(n)})_{n\in\mathbf{N}}$ et donc aussi $(x_n)_{n\in\mathbf{N}}$, a une valeur d'adhérence dans $X - U$, contrairement à l'hypothèse. Il existe donc $N \in \mathbf{N}$ tel que $x_n \in U$, si $n \geqslant N$, ce qui prouve que a est la limite de la suite $(x_n)_{n\in\mathbf{N}}$.

(ii) La suite $(1+(-1)^n)n$ admet 0 comme unique valeur d'adhérence dans $\mathbf{R}$, mais ne converge pas.

Exercice 12.3. Il suffit d'adapter la démonstration de la compacité d'un produit, en partant du développement décimal des éléments de $[0,1]$.

Exercice 12.4. (i) Si f est constante, tout c convient. Sinon, le minimum ou le maximum de f n'est pas égal à $f(a)$. Soit donc $c \in]a,b[$ tel que $f(c)$ soit extrémal (un tel c existe par compacité de $[a,b]$). Alors $f(x)-f(c)$ est de signe constant et donc $\frac{f(x)-f(c)}{x-c}$ change de signe en c, ce qui fait que les dérivées à droite et à gauche sont de signes opposées, et comme on a supposé f dérivable en c, ces dérivées sont toutes les deux égales à $f'(c)$, et donc $f'(c)=0$.

(ii) On applique le (i) à $g(x)=f(x)-\frac{f(b)-f(a)}{b-a}(x-a)$; on a $g(b)=g(a)$ et $g'(c)=0$ implique $f'(c)=\frac{f(b)-f(a)}{b-a}$.

(iii) C'est immédiat.

Exercice 12.5. Si f est identiquement nulle, il n'y a rien à démontrer. Sinon, il existe $x_0 \in \mathrm{E}$ tel que $|f(x_0)|>0$, et comme f tend vers 0 à l'infini, il existe $\mathrm{M}>0$, tel que $|f(x)|<\frac{|f(x_0)|}{2}$, si $\|x\|>\mathrm{M}$. Mais alors la boule $\mathrm{B}(0,\mathrm{M})$ contient x_0 et est compacte, puisque E est de dimension finie. Cela implique que $|f|$ atteint son maximum sur cette boule en un point x_1, et on a $|f(x_1)| \geqslant |f(x_0)| > \frac{|f(x_0)|}{2}$, ce qui prouve que $|f(x_1)|$ est aussi le maximum de $|f|$ sur E tout entier. Ceci permet de conclure.

Exercice 12.6. (i) Si $x_1, x_2 \in \mathrm{X}$, on a $d(x_1,y) \leqslant d(x_1,x_2)+d(x_2,y)$ pour tout $y \in \mathrm{F}$. En passant à la borne inférieure sur $y \in \mathrm{F}$, on en déduit que $d(x_1,\mathrm{F}) \leqslant d(x_1,x_2)+d(x_2,\mathrm{F})$. Par symétrie, on a $d(x_2,\mathrm{F}) \leqslant d(x_1,x_2)+d(x_1,\mathrm{F})$. On en déduit que $|d(x_1,\mathrm{F})-d(x_2,\mathrm{F})| \leqslant d(x_1,x_2)$, et donc que $d(x,\mathrm{F})$ est 1-lipschitzienne.

(ii) On a $d(x,\mathrm{F})=0$, si $x \in \mathrm{F}$, et donc, par continuité, $d(x,\mathrm{F})=0$, si $x \in \overline{\mathrm{F}}$. Réciproquement, si $x \in \overline{\mathrm{F}}$, alors pour tout $n>0$, il existe $x_n \in \mathrm{F}$ avec $d(x,x_n)<2^{-n}$, ce qui implique que $d(x,\mathrm{F})<2^{-n}$, pour tout n, et donc $d(x,\mathrm{F})=0$.

(iii) La fonction $f(x)=d(x,\mathrm{F}_1)-d(x,\mathrm{F}_2)$ est continue sur X, et donc $\mathrm{U}_1=f^{-1}(\mathbf{R}_+^*)$ et $\mathrm{U}_2=f^{-1}(\mathbf{R}_-^*)$ sont deux ouverts de X (en tant qu'images inverses d'ouverts de $\mathbf{R}$ par une fonction continue) qui sont disjoints puisque $\mathbf{R}_+^*$ et $\mathbf{R}_-^*$ sont disjoints. Maintenant, si $x \in \mathrm{F}_1$, alors $d(x,\mathrm{F}_2)>0$ puisque F_2 est fermé et $x \notin \mathrm{F}_2$; donc $f(x)>0$. On en déduit que $\mathrm{F}_1 \subset \mathrm{U}_1$. De même, $\mathrm{F}_2 \subset \mathrm{U}_2$, ce qui permet de conclure.

(iv) La fonction $(x,y) \mapsto d(x,y)$ est continue sur $\mathrm{X}\times\mathrm{X}$. Comme $\mathrm{F}_1\times\mathrm{F}_2$ est compact comme produit de deux compacts, le minimum de $d(x,y)$ sur $\mathrm{F}_1\times\mathrm{F}_2$ est atteint en (x_0,y_0), et comme $\mathrm{F}_1\cap\mathrm{F}_2=\varnothing$, on a $d(x_0,y_0)\neq 0$, et donc $d(\mathrm{F}_1,\mathrm{F}_2)>0$.

(v) La fonction $x \mapsto d(x,\mathrm{F}_1)$ est continue sur F_2 et ne s'annule pas car $\mathrm{F}_1\cap\mathrm{F}_2=\varnothing$ et F_1 est fermé. Comme F_2 est compact, elle atteint son mimimum qui, de ce fait est >0. Or ce minimum est $\inf_{x\in\mathrm{F}_2} d(x,\mathrm{F}_1)=\inf_{x\in\mathrm{F}_2}\inf_{y\in\mathrm{F}_1} d(x,y)=d(\mathrm{F}_1,\mathrm{F}_2)$, ce qui permet de conclure.

(vi) Dans $\mathbf{R}$, on peut prendre $\mathrm{F}_1=\mathbf{N}$ et $\mathrm{F}_2=\{n+2^{-n-1},\ n\in\mathbf{N}\}$. Dans $\mathbf{R}^2$, on peut prendre $\mathrm{F}_1=\{(x,y),\ xy=1\}$ et $\mathrm{F}_2=\{(x,y),\ xy=0\}$.

Exercice 12.7. (i) Soit $g:\mathrm{X}\to\mathbf{R}$ définie par $g(x)=d(x,f(x))$. Alors g est continue comme composée de $g_1:\mathrm{X}\to\mathrm{X}\times\mathrm{X}$ envoyant x sur $(x,f(x))$ et $g_2:\mathrm{X}\times\mathrm{X}\to\mathbf{R}$ envoyant (x,y) sur $d(x,y)$. Elle atteint donc son minimum en un point x_0, et on a $f(x_0)=x_0$, sinon $d(f(f(x_0)),f(x_0))<d(f(x_0),x_0)$, ce qui est contraire à la définition de x_0. La fonction f admet donc au moins un point fixe. Si elle en admet deux $x_1\neq x_2$, on a $d(f(x_1),f(x_2))<d(x_1,x_2)$, ce qui est contraire à l'hypothèse $f(x_1)=x_1$ et $f(x_2)=x_2$. Le point fixe de f est donc unique, ce qui permet de conclure.

(ii) Soit $\delta_n=d(f^n(x),x_0)$. Comme f est strictement contractante, $\delta_{n+1}=d(f(f^n(x)),f(x_0))<\delta_n$, si $f^n(x)\neq x_0$. Maintenant, soit a une valeur d'adhérence de la suite $(f^n(x))_{n\in\mathbf{N}}$, et soit $f^{\varphi(n)}(x)$ une suite extraite tendant vers a. Si $a\neq x_0$, on a

$$\delta_{\varphi(n_0)+1} \leqslant d(f^{\varphi(n_0)+1}(x),f(a))+d(f(a),x_0) < d(f^{\varphi(n_0)}(x),a)+d(f(a),x_0) \leqslant d(a,x_0),$$

si n_0 est assez grand. On aboutit à une contradiction car $\delta_m \leqslant \delta_{\varphi(n_0)} < d(a,x_0)$ pour tout $m > \varphi(n_0)$, et la suite extraite $\delta_{\varphi(n)}$ tend vers $d(a,x_0)$ quand n tend vers $+\infty$. On en déduit que $a = x_0$ et donc que $f^n(x)$ a x_0 comme unique valeur d'adhérence dans X. Comme X est compact, cela implique que $f^n(x) \to x_0$.

(iii) Soit $\delta_n = \sup_{x\in \mathrm{X}} d(f^n(x), x_0)$. Il s'agit de prouver que $\delta_n \to 0$. Comme f est compact et $x \mapsto d(f^n(x), x_0)$ est continue puisque f est continue, il existe $x_n \in \mathrm{X}$ tel que $d(f^n(x_n), x_0) = \delta_n$. On a alors $\delta_{n+1} = d(f^{n+1}(x), x_0) = d(f^n(f(x_{n+1})), x_0) \leqslant \delta_n$, ce qui montre que la suite δ_n est décroissante. Il suffit donc d'exhiber une suite extraite de $(\delta_n)_{n\in\mathbf{N}}$ tendant vers 0.

Soit a une valeur d'adhérence de la suite x_n, et soit $x_{\varphi(n)}$ une suite extraite tendant vers a. On a alors

$$\delta_{\varphi(n)} = d(f^{\varphi(n)}(x_{\varphi(n)}), x_0) \leqslant d(f^{\varphi(n)}(x_{\varphi(n)}), f^{\varphi(n)}(a)) + d(f^{\varphi(n)}(a), x_0) \leqslant d(x_{\varphi(n)}, a) + d(f^{\varphi(n)}(a), x_0),$$

ce qui montre que $\delta_{\varphi(n)} \to 0$ car $d(x_{\varphi(n)}, a) \to 0$ par construction, et $d(f^{\varphi(n)}(a), x_0) \to 0$ d'après le (ii). Ceci permet de conclure.

Exercice 12.8. La démonstration se fait par l'absurde. Supposons X non compact, et construisons une fonction continue $\phi : \mathrm{X} \to \mathbf{R}$ non bornée. Il existe une suite $(x_n)_{n\in\mathbf{N}}$ n'ayant pas de valeur d'adhérence dans X, ce qui se traduit, pour tout $a \in \mathrm{X}$, par l'existence de $\delta_a > 0$ tel que $\mathrm{B}(a, 2\delta_a^-)$ contienne au plus un x_n, à savoir a si l'un des x_n vaut a. Soit $\phi_n(x) = \sup(n - n^2 d(x, x_n), 0)$. C'est une fonction continue sur X, nulle en dehors de $\mathrm{B}(x_n, \frac{1}{n})$ et valant n en x_n. Si $a \in \mathrm{X}$, la restriction de ϕ_n à $\mathrm{B}(a, \delta_a^-)$ est identiquement nulle, si $\frac{1}{n} < \delta_a$ et si $x_n \neq a$. Comme il n'y a qu'un nombre fini de n ne vérifiant pas ces conditions, cela montre que $\phi(x) = \sum_{n\in\mathbf{N}} \phi_n(x)$ est la somme d'un nombre fini de fonctions continues sur $\mathrm{B}(a, \delta_a^-)$, pour tout a ; c'est donc une fonction continue sur X. Par ailleurs, on a $\phi(x_n) \geqslant n$, pour tout n, et donc ϕ est non bornée. Ceci permet de conclure.

Exercice 13.1 (i) Soit f une telle fonction. Soient $a < b$ les deux solutions de $f(x) = 0$. Alors f est, d'après le th. des valeurs intermédiaires, de signe constant sur $]-\infty, a[$, sur $]a, b[$, et sur $]b, +\infty[$ puisque f n'a pas d'autre zéro que a et b. Quitte à changer f en $-f$, on peut supposer $f > 0$ sur $]a, b[$. Soit $\mathrm{M} = \sup_{x\in[a,b]} f(x)$. Alors il existe $c \in]a, b[$ tel que $f(x) = c$ par compacité de $[a, b]$, et f prend toute valeur de $]0, \mathrm{M}[$ deux fois sur $]a, b[$ (une fois sur $]a, c[$ et une fois sur $]c, b[$). On en déduit le fait que f est $\leqslant 0$ en dehors de $]a, b[$, sinon son image contiendrait un segment de la forme $[0, \mathrm{M}'[$ et tout élément de $]0, \inf(\mathrm{M}, \mathrm{M}')[$ aurait plus de 3 antécédents. Mais alors f ne prend aucune valeur $\geqslant \mathrm{M}$, ce qui est en contradiction avec l'hypothèse. Il s'ensuit qu'il n'existe pas de fonction continue $f : \mathbf{R} \to \mathbf{R}$ prenant chaque valeur exactement 2 fois.

(ii) Il est très facile de construire une fonction continue prenant chaque valeur $2k + 1$ fois, si $k \in \mathbf{N}$; par exemple, la fonction f définie par $f(x) = \sin^2 \pi x$ sur $[0, k + \frac{1}{2}]$, prolongée par l'équation fonctionnelle $f(x + k + \frac{1}{2}) = f(x) + 1$ si $x \in \mathbf{R}$.

Par contre, si $n = 2k$, cela n'est pas possible. On raisonne par l'absurde comme pour le cas $n = 2$, et on note $a_1 < a_2 < \cdots < a_{2k}$ les solutions de $f(x) = 0$. Alors f est de signe constant sur $]-\infty, a_1[$, sur $]a_{2k}, +\infty[$ et sur chacun des $2k-1$ segments $]a_i, a_{i+1}[$. Quitte à changer f en $-f$, on peut supposer $f > 0$ sur au moins k de ces segments. On en déduit l'existence de $\mathrm{M} > 0$ tel que f prenne $2k$ fois la valeur y sur $]a_1, a_{2k}[$ si $y \in]0, \mathrm{M}[$, et on montre, comme ci-dessus, que cela implique que $f < 0$ en dehors de $[a_1, a_{2k}]$, puis que f est bornée supérieurement contrairement à l'hypothèse qui implique en particulier que f est surjective.

Exercice 13.2. On sait que U est connexe par arcs, et il suffit de prouver qu'il en est de même de $\mathrm{V} = \mathrm{U} - \{x\}$. Soient donc $y_1, y_2 \in \mathrm{V}$, et soit $u : [0, 1] \to \mathrm{U}$ un chemin continu joignant y_1 à y_2 dans U. Si u ne passe pas par x, il n'y a rien à faire. Sinon, il existe $r < \inf(d(x, y_1), d(x, y_2))$ tel que $\mathrm{B}(x, r) \subset \mathrm{U}$, et l'ensemble des t tels que $d(x, u(t)) \leqslant r$ admet un plus petit (resp. grand) élément t_1 (resp. t_2). Alors u permet de joindre y_1 à $u(t_1)$ et $u(t_2)$ à y_2 dans V, et on peut passer de $u(t_1)$ à $u(t_2)$ en restant sur la

sphère de rayon r [il suffit de prendre l'arc de cercle délimité par le cone de sommet x et dont les bords sont les demi-droites $[x, u(t_1))$ et $[x, u(t_2))$].

Exercice 13.3. Si f est un homéomorphisme de X sur Y, alors la restriction de f à $X - \{x\}$ est encore un homéomorphisme de $X - \{x\}$ sur $Y - \{f(x)\}$ pour tout $x \in X$. Il ne peut donc pas y avoir d'homéomorphisme de $\mathbf{R}$ sur $\mathbf{R}^2$ puisque $\mathbf{R}$ privé d'un point est non connexe, alors que $\mathbf{R}^2$ privé d'un point est connexe. Les autres cas se traitent de la même manière en enlevant à $[0,1]$ n'importe quel élément différent de 0 et 1.

Exercice 13.4. Si f est une bijection de $[0,1]$ sur $]0,1[$, alors $f(]0,1]) =]0,1[- \{f(0)\}$ est non connexe, tandis que $]0,1]$ est connexe, ce qui prouve que f ne peut pas être continue.

Exercice 13.5. Si on enlève de Y les deux points de contacts, on obtient un ensemble avec 4 composantes connexes, alors que si on enlève deux points à X, le mieux que l'on puisse obtenir est 3 composantes connexes.

Exercice 13.6. (i) (a) On peut prendre une échelle avec une infinité dénombrable de barreaux et, si on retire les barreaux un par un, il ne reste que les deux montants, ce qui n'est pas connexe (i.e. F_n est la réunion des deux demi-droites verticales partant de $(0,0)$ et $(1,0)$ et des segments horizontaux $[(0,k),(1,k)]$, pour $k \geqslant n$).

(b) Si F n'est pas connexe, alors $F = F' \cup F''$, où F' et F'' sont des fermés non vides disjoints de F. Par ailleurs, F est fermé, en tant qu'intersection de fermés, et comme $F \subset F_0$ qui est compact, F, F' et F'' sont compacts. La distance $d = d(F', F'')$ est donc > 0, et $U' = \{x \in \mathbf{R}^2,\ d(x, F') < \frac{d}{3}\}$ et $U'' = \{x \in \mathbf{R}^2,\ d(x, F'') < \frac{d}{3}\}$ sont des ouverts disjoints de $\mathbf{R}^2$ contenant F' et F'' respectivement. Soit $Z = \mathbf{R}^2 - (F' \cup F'')$. Alors Z est un fermé ne rencontrant pas F, et donc $\cap_{n\in\mathbf{N}}(Z \cap F_n) = \varnothing$. Comme $Z \cap F_n$ est un fermé de F_0 qui est compact, on en déduit l'existence de $n \in \mathbf{N}$ tel que $Z \cap F_n = \varnothing$. On a donc $F_n = (U' \cap F_n) \cup (U'' \cap F_n)$, ce qui est en contradiction avec l'hypothèse « F_n connexe » puisque $U' \cap F_n$ et $U'' \cap F_n$ sont des ouverts disjoints de F_n qui sont non vides puisqu'ils contiennent F' et F'' respectivement. L'hypothèse « F non connexe » était donc absurde, ce qui permet de conclure.

(ii) (a) Soit X_n la réunion des segments $[x_k, x_{k+1}]$, pour $k \geqslant n$, et soit F_n l'adhérence de X_n. Alors F_n est connexe car X_n est connexe (il est même connexe par arcs), F_0 est compact car fermé par construction et borné par hypothèse, et $F_{n+1} \subset F_n$ car $X_{n+1} \subset X_n$. Il s'ensuit, d'après le (i) (b), que $F = \cap_{n\in\mathbf{N}} F_n$ est connexe. Montrons que F est égal à l'ensemble G des valeurs d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$, ce qui permettra de conclure.

• Si $Y_n = \{x_k,\ k \geqslant n\}$ et G_n est l'adhérence de Y_n, alors $G = \cap_{n\in\mathbf{N}} G_n$. Or $Y_n \subset X_n$ et donc $G_n \subset F_n$, pour tout $n \in \mathbf{N}$, et $G \subset F$.

• Si $a \in F$, alors pour tout $\varepsilon > 0$ et tout $N \in \mathbf{N}$, il existe $n \geqslant N$ et $x \in [x_n, x_{n+1}]$ tel que $d(x,a) < \varepsilon$. Choisissons N de telle sorte que $d(x_k, x_{k+1}) \leqslant \varepsilon$, pour tout $k \geqslant N$ (c'est possible car on a supposé $d(x_{k+1}, x_k) \to 0$). On a alors $d(x_n, x) \leqslant \varepsilon$ et donc $d(x_n, a) \leqslant 2\varepsilon$. On en déduit que a est une valeur d'adhérence de la suite $(x_n)_{n\in\mathbf{N}}$, et donc que $F \subset G$.

Ceci permet de conclure.

(b) Il suffit de parcourir l'échelle du (i) (a) en allant d'un pied à l'autre en passant par le k-ième barreau ; comme ceci est un peu fatigant, les pas que l'on faits sont de plus en plus petits et l'adhérence de la suite ainsi construite est constituée des deux montants (il n'est pas sûr qu'ils résistent très longtemps à ce traitement...).

Exercice 13.7. Définissons le bord du cylindre et de la bande de Moebius comme l'image de $\{0,1\} \times [0,1]$. Dans le cyclindre, on obtient deux lacets disjoints, alors que dans la bande de Moebius on n'obtient qu'un seul lacet, car $(0,0)$ est identifié à $(1,1)$. Maintenant, si x est sur le bord, alors x admet une base de voisinages constituée de demi-disques de centre x, et si on prive un de ces demi-disques de x, on obtient un

ensemble contractile. Si x n'est pas sur le bord, alors tout voisinage de x contient un disque de centre x, et si on le prive de x, on obtient un ensemble non contractile. On en déduit qu'un homéomorphisme du cylindre sur la bande de Moebius induit un homéomorphisme entre les bords, mais ce n'est pas possible car le bord du cylindre n'est pas connexe, alors que celui de la bande de Moebius l'est.

Exercice 14.1. (i) On a $d(x_m, x_{m+p}) \leqslant \sup_{0\leqslant i\leqslant p-1} d(x_{m+i}, x_{m+i+1}) \leqslant \sup_{m\geqslant n} d(x_m, x_{m+1})$ par ultramétricité de d. On en déduit que si $d(x_{n+1}, x_n) \to 0$, et donc si $\lim_{n\to+\infty} \big(\sup_{m\geqslant n} d(x_{m+1}, x_m)\big) = 0$, alors $\lim_{m\to+\infty} \big(\sup_{p\in\mathbf{N}} d(x_{m+p}, x_m)\big) = 0$, et la suite est de Cauchy.

(ii) Si $n \geqslant 1$, soit $i = \big[\frac{\log n}{\log 2}\big]$, de telle sorte que $n = 2^i + j$, avec $0 \leqslant j \leqslant 2^i - 1$. Posons alors $x_n = \frac{j}{2^i}$, si i est pair et $x_n = 1 - \frac{j}{2^i}$, si i est impair. On vérifie que $x_{n+1} - x_n = \frac{1}{2^i}$ tend vers 0, mais que la suite $(x_n)_{n\in\mathbf{N}}$ balaie consciencieusement l'intervalle $[0, 1]$ et que l'ensemble de ses valeurs d'adhérence est $[0, 1]$. Elle n'est donc pas de Cauchy. On aurait aussi pu prendre $x_n = \log(n + 1)$ qui tend vers $+\infty$, et donc n'est pas de Cauchy.

Exercice 14.3. (i) Soit $(\mathrm{U}_n)_{n\in\mathbf{N}}$ une famille d'ouverts denses de $\mathbf{R}$. Supposons que $\mathrm{X} = \cap_{n\in\mathbf{N}}\mathrm{U}_n$ est dénombrable, et choisissons une surjection $n \mapsto x_n$ de $\mathbf{N}$ sur X. Alors $\mathrm{V}_n = \mathrm{U}_n - \{x_n\}$ est un ouvert dense de $\mathbf{R}$ pour tout n et $\cap_{n\in\mathbf{N}}\mathrm{V}_n = \varnothing$, ce qui est contraire au lemme de Baire.

(ii) Si $(f_n)_{n\in\mathbf{N}}$ est une telle suite, et si $\mathrm{N} \in \mathbf{N}$, soit $\mathrm{F}_\mathrm{N} = \{x \in \mathbf{R},\ |f_n(x)| \leqslant \mathrm{N},\ \forall n \in \mathbf{N}\}$. Alors F_N est un fermé puisque $\mathrm{F}_\mathrm{N} = \cap_{n\in\mathbf{N}}\{x \in \mathbf{R},\ |f_n(x)| \leqslant \mathrm{N}\}$ et que chacun des ensembles de l'intersection est fermé par continuité des f_n. Par ailleurs, l'hypothèse sur la suite $(f_n)_{n\in\mathbf{N}}$ se traduit par $\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{F}_\mathrm{N} = \mathbf{R} - \mathbf{Q}$. En notant U_N l'ouvert complémentaire de F_N, on obtient $\cap_{\mathrm{N}\in\mathbf{N}}\mathrm{U}_\mathrm{N} = \mathbf{Q}$, ce qui est en contradiction avec le (i) (chacun des U_N est dense dans $\mathbf{R}$ puisqu'il contient $\mathbf{Q}$).

Exercice 15.1 (i) Si $n \geqslant 1$, on a $\frac{a_n}{\mathrm{S}_n^2} = \int_{\mathrm{S}_{n-1}}^{\mathrm{S}_n} \frac{dx}{\mathrm{S}_n^2} \leqslant \int_{\mathrm{S}_{n-1}}^{\mathrm{S}_n} \frac{dx}{x^2}$ car $x \leqslant \mathrm{S}_n$ sur $[\mathrm{S}_{n-1}, \mathrm{S}_n]$. On en déduit que $\sum_{n\in\mathbf{N}} \frac{a_n}{\mathrm{S}_n^2} \leqslant \frac{a_0}{a_0^2} + \int_{a_0}^{+\infty} \frac{dx}{x^2} \leqslant \frac{2}{a_0} < +\infty$.

(ii) Si $\limsup \frac{a_n}{\mathrm{S}_n} = 1$, il y a une infinité de n tels que $\frac{a_n}{\mathrm{S}_n} \geqslant \frac{1}{2}$, et la série diverge. Si $\limsup \frac{a_n}{\mathrm{S}_n} < 1$, il existe $c < 1$ tel que $\frac{a_n}{\mathrm{S}_n} \leqslant c$, pour tout $n \geqslant 1$. On a alors $x \geqslant \mathrm{S}_n - a_n \geqslant (1 - c)\mathrm{S}_n$ sur $[\mathrm{S}_{n-1}, \mathrm{S}_n]$, et donc $\frac{a_n}{\mathrm{S}_n} \geqslant \int_{\mathrm{S}_{n-1}}^{\mathrm{S}_n} \frac{1-c}{x}\, dx$, si $n \geqslant 1$. On en tire la minoration $\sum_{n\in\mathbf{N}} \frac{a_n}{\mathrm{S}_n} \geqslant 1 + \int_{a_0}^{+\infty} \frac{1-c}{x}\, dx = +\infty$.

Exercice 15.2. (i) Si $\Lambda = \{0\}$, on a $\Lambda = \mathbf{Z} \cdot 0$; on suppose donc $\Lambda \neq \{0\}$ dans ce qui suit.

Si $\Lambda \cap \mathbf{R}_+^*$ admet un plus petit élément a, et si $x \in \Lambda$, alors $x - \big[\frac{x}{a}\big]a$ est un élément de Λ appartenant à $[0, a[$; il est donc nul par définition de a, ce qui prouve que $\Lambda = \mathbf{Z} \cdot a$.

Si la borne inférieure de $\Lambda \cap \mathbf{R}_+^*$ est 0, alors pour tout $\varepsilon > 0$, il existe $a \in \Lambda \in]0, \varepsilon[$. Maintenant, si $x \in \mathbf{R}$, alors $\big[\frac{x}{a}\big]a \in \Lambda$ et $x - \big[\frac{x}{a}\big]a \in [0, a[$, et donc $|x - \big[\frac{x}{a}\big]a| < \varepsilon$. Ceci montre que Λ est dense dans $\mathbf{R}$.

(ii) Soient $\mathrm{N} = 3141592$ et $\varepsilon = \log \frac{\mathrm{N}+1}{\mathrm{N}}$. La question peut se reformuler sous la forme : existe-t-il $n \in \mathbf{N}$ et $m \in \mathbf{Z}$ tels que $0 \leqslant n \log 2 - \log \mathrm{N} - m \log 10 < \varepsilon$? Or $\log 2$ et $\log 10$ sont linéairement indépendants sur $\mathbf{Q}$ car $2^n = 10^m$ implique $m = 0$ (en regardant la valuation 5-adique) et donc aussi $n = 0$. Il s'ensuit que le sous-groupe de $\mathbf{R}$ qu'ils engendrent ne peut pas être de la forme $\mathbf{Z} \cdot a$, sinon on aurait $\log 2 = ma$ et $\log 10 = na$ et $n \log 2 = m \log 10$; il est donc dense dans $\mathbf{R}$ d'après le (i). Par densité, il existe $n_1, m_1 \in \mathbf{Z}$ tels que $|n_1 \log 2 - \log \mathrm{N} - m_1 \log 10 - \frac{\varepsilon}{2}| \leqslant \frac{\varepsilon}{4}$, et il existe n_2, m_2 avec $n_2 > |n_1|$ et $m_2 > |m_1|$ tel que $|n_2 \log 2 - m_2 \log 10| < \frac{\varepsilon}{4}$; alors $n = n_1 + n_2$ et $m = m_1 + m_2$ conviennent.

(iii) Si $a_3 + b_3\sqrt{2} = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$, on a $a_3 = a_1a_2 + 2b_1b_2$ et $b_3 = a_1b_2 + a_2b_1$, ce qui nous donne $a_3 - b_3\sqrt{2} = (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2})$. On en déduit que $a_3^2 - 2b_3^2 = (a_3 + b_3\sqrt{2})(a_3 - b_3\sqrt{2})$ est aussi égal à $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})(a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) = (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) = 1$.

Maintenant, si $a^2 - 2b^2 = 1$ avec $a, b \in \mathbf{N}$, il existe n tel que $(3 + 2\sqrt{2})^n \leqslant a + b\sqrt{2} < (3 + 2\sqrt{2})^{n+1}$ (on a $n = \big[\frac{\log(a+b\sqrt{2})}{\log(3+2\sqrt{2})}\big]$). Alors $(3 - 2\sqrt{2})^n(a + b\sqrt{2}) = c + d\sqrt{2}$, avec $c, d \in \mathbf{Z}$ vérifiant $c^2 - 2d^2 = 1$ et $1 \leqslant c + d\sqrt{2} < 3 + 2\sqrt{2}$. Comme $(c - d\sqrt{2})(c + d\sqrt{2}) = 1$, cela implique $3 - 2\sqrt{2} < c - d\sqrt{2} \leqslant 1$. On en

tire donc l'encadrement $2-\sqrt{2}<c\leqslant 2+\sqrt{2}$, et donc $c=1,2$ ou 3 ; le seul couple possible vérifiant en plus $c^2-2d^2=1$ est donc $(c,d)=(1,0)$, ce qui nous donne $a+b\sqrt{2}=(3+2\sqrt{2})^n$, et permet de conclure.

Exercice 15.3. Il suffit de recopier les arguments de l'exemple précédent en écrivant $\sum_{n=1}^{\mathrm{N}}\frac{(-1)^{n-1}}{n}$ sous la forme $\sum_{n=1}^{\mathrm{N}}\int_0^1(-x)^{n-1}dx$.

Exercice 15.4. (i) Si $\sum_{n\in\mathbf{N}}u_n$ est semi-convergente, on a en particulier $u_n\to 0$ quand $n\to+\infty$, et donc $|u_n|\leqslant 1$ pour n assez grand ; on en déduit la convergence absolue de la série $\sum_{n\in\mathbf{N}}u_nx^n$, si $|u_n|<1$.

Soit $\mathrm{S_N}=\sum_{n\leqslant\mathrm{N}}u_n$. Si $\varepsilon>0$, on peut choisir N_0 tel que $|\mathrm{S_N}-\mathrm{S}_{\mathrm{N}_0}|\leqslant\varepsilon$ pour tout $\mathrm{N}\geqslant\mathrm{N}_0$, ce qui se traduit aussi par $\big|\sum_{n=\mathrm{N}_0+1}^{\mathrm{N}}u_n\big|\leqslant\varepsilon$, pour tout $\mathrm{N}\geqslant\mathrm{N}_0$. La sommation d'Abel nous fournit l'identité $\sum_{n=\mathrm{N}_0+1}^{\mathrm{N}}u_nx^n=\sum_{n=\mathrm{N}_0+1}^{\mathrm{N}}(x^n-x^{n+1})(\mathrm{S}_n-\mathrm{S}_{\mathrm{N}_0})+x^{\mathrm{N}+1}(\mathrm{S_N}-\mathrm{S}_{\mathrm{N}_0})$, ce qui nous donne la majoration $\big|\big(\sum_{n\leqslant\mathrm{N}}u_nx^n\big)-\mathrm{S_N}\big|\leqslant\sum_{n\leqslant\mathrm{N}_0}|u_n|(1-x^n)+\big(\sum_{n\leqslant\mathrm{N}}(x^n-x^{n+1})+(1-x^{\mathrm{N}+1})\big)\varepsilon\leqslant\sum_{n\leqslant\mathrm{N}_0}|u_n|(1-x^n)+2\varepsilon$. On peut alors choisir $\delta<1$ tel que $\sum_{n\leqslant\mathrm{N}_0}|u_n|(1-x^n)\leqslant\varepsilon$, si $x\in]\delta,1[$, et un passage à la limite quand $\mathrm{N}\to+\infty$ nous fournit la majoration $\big|\big(\sum_{n\in\mathbf{N}}u_nx^n\big)-\mathrm{S}\big|\leqslant 3\varepsilon$, si $x\in]\delta,1[$. Ceci prouve que $\mathrm{S}=\lim_{x\to1^-}\big(\sum_{n\in\mathbf{N}}u_nx^n\big)$.

(ii) La série double à termes positifs $\sum_{(i,j)\in\mathbf{N}}|a_i|\,|b_j|$ peut se calculer en sommant d'abord par rapport à i, puis par rapport à j, et elle vaut donc $\big(\sum_{i\in\mathbf{N}}|a_i|\big)\big(\sum_{j\in\mathbf{N}}|b_j|\big)$. On en déduit que la série double $\sum_{(i,j)\in\mathbf{N}}a_ib_j$ est absolument convergente, et donc que l'on peut calculer sa somme S en regroupant les termes comme on le veut. En sommant d'abord par rapport à i, puis par rapport à j, on obtient $\mathrm{S}=\big(\sum_{i\in\mathbf{N}}a_i\big)\big(\sum_{j\in\mathbf{N}}b_j\big)$; et en sommant sur $i+j=n$, puis sur n, on obtient $\mathrm{S}=\sum_{n\in\mathbf{N}}c_n$, où la série dans le membre de doite est absolument convergente. Ceci permet de conclure.

(iii) Comme $c_nx^n=\sum_{i+j=n}(a_ix^i)(b_jx^j)$, on a $\sum_{n\in\mathbf{N}}c_nx^n=\big(\sum_{n\in\mathbf{N}}a_nx^n\big)\cdot\big(\sum_{n\in\mathbf{N}}b_nx^n\big)$ d'après le (ii), si $|x|<1$, car alors les séries sont absolument convergentes. On en déduit, en passant à la limite en 1^- grâce au (i), l'identité $\sum_{n\in\mathbf{N}}c_n=\big(\sum_{n\in\mathbf{N}}a_n\big)\cdot\big(\sum_{n\in\mathbf{N}}b_n\big)$.

(iv) Si $a_n=b_n=\frac{(-1)^n}{(n+1)^s}$, avec $0<s<\frac12$, les séries $\sum_{n\in\mathbf{N}}a_n$ et $\sum_{n\in\mathbf{N}}b_n$ sont semi-convergentes d'après le critère de Leibnitz. Maintenant $c_n=(-1)^n\sum_{i+j=n}\frac{1}{((i+1)(j+1))^s}$. Or $\sqrt{(i+1)(j+1)}\leqslant\frac{i+j+2}{2}$, et donc $|c_n|\geqslant\frac{2^s(n+1)}{(n+1)^{2s}}$, et $|c_n|\to+\infty$ quand $n\to+\infty$. Par contre, la limite de $\sum_{n\in\mathbf{N}}c_nx^n=\big(\sum_{n\in\mathbf{N}}a_nx^n\big)\cdot\big(\sum_{n\in\mathbf{N}}b_nx^n\big)$ en 1^- existe et vaut $\big(\sum_{n\in\mathbf{N}}a_n\big)\cdot\big(\sum_{n\in\mathbf{N}}b_n\big)$ d'après les (i) et (ii).

Exercice 15.5. (i) L'idée est simple : on construit $\varphi(n)$ par récurrence en posant $\varphi(0)=0$ et en prenant pour $\varphi(n)$, le plus petit i n'appartenant pas à $\{\varphi(0),\dots,\varphi(n-1)\}$ tel que x_i soit $\geqslant 0$ (resp. <0) si $x_{\varphi(0)}+\cdots+x_{\varphi(n-1)}$ est $\leqslant\ell$ (resp. $>\ell$) de manière à osciller autour de ℓ et à n'omettre aucun x_i. Par construction φ est injective. Par ailleurs, l'hypothèse selon laquelle $\sum_{i\in\mathbf{N}}|x_i|=+\infty$ et $\sum_{i\in\mathbf{N}}x_i$ est semi-convergente implique que les sommes des $x_i\geqslant 0$ et des $x_i<0$ sont toutes les deux infinies. On en déduit que $x_{\varphi(n)}$ ne peut pas être $\geqslant 0$ ou <0 pour tout n assez grand, et donc qu'il existe une infinité de n pour lesquels $x_{\varphi(n)}<0$ et une autre infinité pour lesquels $x_{\varphi(n)}\geqslant 0$; comme on a pris à chaque fois le premier vérifiant une de ces conditions, cela montre que φ est surjective. Enfin, si on note $n_1,n_2,\dots$ les entiers n pour lesquels $x_{\varphi(0)}+\cdots+x_{\varphi(n-1)}-\ell$ est de signe différent de $x_{\varphi(0)}+\cdots+x_{\varphi(n)}-\ell$, on a $|x_{\varphi(0)}+\cdots+x_{\varphi(n)}-\ell|\leqslant\sup(|x_{\varphi(n_k)}|,|x_{\varphi(n_{k+1}-1)}|)$, si $n_k\leqslant n\leqslant n_{k+1}-1$. Or la semi-convergence de $\sum_{n\in\mathbf{N}}x_n$ implique que $x_n\to 0$ quand $n\to+\infty$; il en est de même de $\sup(|x_{\varphi(n_k)}|,|x_{\varphi(n_{k+1}-1)}|)$ quand $k\to+\infty$ car $\varphi(n_k)$ et $\varphi(n_{k+1}-1)$ tendent vers $+\infty$. La suite des $\sum_{n\leqslant\mathrm{N}}x_{\varphi(n)}$ a donc pour limite ℓ quand $\mathrm{N}\to+\infty$, ce qui démontre le (i).

(ii) Le (i) permet d'exhiber une surjection du groupe des permutations de $\mathbf{N}$ sur $\mathbf{R}$; ce groupe n'est donc pas dénombrable.

Exercice 15.6. (i) Si $k=0$, la formule est immédiate. La cas général s'en déduit par récurrence :

$$\mathrm{S}_{\mathrm{N}}^{[k+1]}-\mathrm{S}_{\mathrm{N}-1}^{[k+1]}=\frac12\big((\mathrm{S}_{\mathrm{N}+1}^{[k]}-\mathrm{S}_{\mathrm{N}}^{[k]})-(\mathrm{S}_{\mathrm{N}}^{[k]}-\mathrm{S}_{\mathrm{N}-1}^{[k]})\big)=\frac{(-1)^{\mathrm{N}+k+1}}{2^{k+1}}(f^{[k]}(\mathrm{N}+1)-f^{[k]}(\mathrm{N}))=\frac{(-1)^{\mathrm{N}+k+1}}{2^{k+1}}f^{[k+1]}(\mathrm{N}).$$

(ii) Si $\mathrm{P} = a_k x^k + \cdots + a_0$, alors $\mathrm{P}^{[1]}(x) = \mathrm{P}(x+1) - \mathrm{P}(x) = k a_k x^{k-1} + \cdots$. Une récurrence immédiate montre que $\mathrm{P}^{[i]}$ est de degré $\leqslant k-i$, et que le coefficient de x^{k-i} est $k(k-1)\cdots(k-i+1)a_k$. Pour $i=k$, cela nous dit que $\mathrm{P}^{[k]} = k! a_k$ est la dérivée k-ième de P.

(iii) Soit $\mathrm{P} = \sum_{i=0}^{k} f(a+i) \prod_{j\in\{0,\ldots,\hat{i},\ldots,k\}} \frac{x-j}{i-j}$ le polynôme de degré $\leqslant k$ prenant les mêmes valeurs que f en $a, a+1, \ldots, a+k$. On a donc $f^{[k]}(a) = \mathrm{P}^{[k]}(a)$. Alors $\mathrm{P} - f$ s'annule en $a, a+1, \ldots, a+k$. On en déduit, en utilisant le lemme de Rolle, que $\mathrm{P}' - f'$ s'annule en au moins k points distincts de $[a, a+k]$ (au moins un sur chacun des $]a+i, a+i+1[$), et une récurrence immédiate montre que $\mathrm{P}^{(i)} - f^{(i)}$ s'annule en au moins $k+1-i$ points distincts de $[a, a+k]$. Pour $i=k$, cela nous dit qu'il existe $c \in [a, a+k]$ tel que $f^{(k)}(c) = \mathrm{P}^{(k)}(c)$. On conclut en remarquant que $\mathrm{P}^{(k)}(c) = \mathrm{P}^{[k]}(a)$ d'après le (ii).

(iv) Soit k tel que $-s-k < -1$. Alors $f^{(k)}(x)$ est de la forme $\mathrm{C}(x+1)^{-t}$, avec $t = s+k > 1$, et $\mathrm{C} = (-s)(-s-1)\cdots(-s-k+1)$. Maintenant, en combinant le (i) et le (iii), on peut majorer $|\mathrm{S}_{\mathrm{N}}^{[k]} - \mathrm{S}_{\mathrm{N}-1}^{[k]}|$ par $|\mathrm{C}|(\mathrm{N}+1)^{-t}$ puisque $x \mapsto (x+1)^{-t}$ est décroissante sur $[\mathrm{N}, \mathrm{N}+k]$. On en déduit que $\sum_{\mathrm{N}\in\mathbf{N}} (\mathrm{S}_{\mathrm{N}}^{[k]} - \mathrm{S}_{\mathrm{N}-1}^{[k]})$ est absolument convergente, et donc que la suite $\mathrm{S}_{\mathrm{N}}^{[k]}$ a une limite quand $\mathrm{N} \to +\infty$.

(v) Si $s > 1$, la série $\sum_{n\in\mathbf{N}} \frac{(-1)^n}{(n+1)^s}$ converge absolument et donc $\mathrm{F}(s)$ en est la somme. En changeant $n+1$ en n, on obtient aussi $\mathrm{F}(s) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n^s}$. On a donc $\mathrm{F}(s) - \zeta(s) = -2\sum_{k=1}^{+\infty} \frac{1}{(2k)^s} = -2^{1-s}\zeta(s)$ et $\mathrm{F}(s) = (1-2^{1-s})\zeta(s)$.

(vi) Il suffit de prouver que $\mathrm{F}(-m) \in \mathbf{Q}$ si $m \in \mathbf{N}$. Si $k \geqslant m+2$, $\mathrm{F}(-m)$ est la limite de $\mathrm{S}_{\mathrm{N}}^{[k]}$ quand $\mathrm{N} \to +\infty$. Or les (i) et (iii), combinés avec le fait que la dérivée k-ième de $x \mapsto (1+x)^m$ est identiquement nulle, impliquent que $\mathrm{S}_{\mathrm{N}}^{[k]} - \mathrm{S}_{\mathrm{N}-1}^{[k]} = 0$ pour tout $\mathrm{N} \geqslant 1$. Autrement dit, la suite $\mathrm{S}^{[k]}$ est constante et $\mathrm{F}(-m) = \mathrm{S}_0^{[k]}$. On conclut en remarquant que $\mathrm{S}_0^{[k]} \in \mathbf{Q}$ car c'est une combinaison linéaire finie, à coefficients dans $\mathbf{Z}[\frac{1}{2}]$, de $f(0), \ldots, f(k)$.

Exercice 16.1. En revenant à la définition de la topologie produit, on voit qu'il suffit de prouver qu'on peut toujours construire une fonction continue de $\mathbf{R}$ dans $\mathbf{C}$ prenant des valeurs prescrites en un nombre fini de points. Ceci ne pose pas de problème (on peut par exemple prendre un polynôme d'interpolation de Lagrange).

Exercice 16.2. On peut prolonger $u^{(n)}$ en une fonction continue sur $\overline{\mathbf{N}}$ en posant $u^{(n)}(+\infty) = 0$. On prolonge aussi u en posant $u(+\infty) = 0$. Alors $u^{(n)} \to u$ uniformément sur $\overline{\mathbf{N}}$ et donc u est continue en $+\infty$, ce qui se traduit par $\lim_{k\to+\infty} u_k = 0$.

On peut aussi se passer de $\overline{\mathbf{N}}$, en recopiant la démonstration du point précédant l'exercice. Soit $\varepsilon > 0$. Comme $u^{(n)} \to u$ uniformément sur $\mathbf{N}$, il existe $\mathrm{N}_0 \in \mathbf{N}$ tel que $|u_k^{(n)} - u_k| < \varepsilon$, quels que soient $n \geqslant \mathrm{N}_0$ et $k \in \mathbf{N}$. Choisissons $n \geqslant \mathrm{N}_0$. Comme $\lim_{k\to+\infty} u_k^{(n)} = 0$, il existe $\mathrm{N} \in \mathbf{N}$ tel que $|u_k^{(n)}| < \varepsilon$, pour tout $k \geqslant \mathrm{N}$, et on a $|u_k| \leqslant |u_k^{(n)} - u_k| + |u_k^{(n)}| < 2\varepsilon$, pour tout $k \geqslant \mathrm{N}$. On en déduit que $\lim_{k\to+\infty} u_k = 0$.

Exercice 16.3. (i) $(a_n)_{n\in\mathbf{N}} \mapsto a_n$ est continue, et la série converge uniformément vers sa somme (le reste est majoré par $\frac{1}{10^{\mathrm{N}}}$) ; on en déduit la continuité de $(a_n)_{n\in\mathbf{N}} \mapsto \sum_{n\in\mathbf{N}} \frac{a_n}{10^{n+1}}$.

(ii) L'existence de l'écriture en base 10 montre que $[0,1]$ est l'image du compact $\{0,1,\ldots,9\}^{\mathbf{N}}$ (c'est un produit dénombrable de compacts métriques) par l'application continue $(a_n)_{n\in\mathbf{N}} \mapsto \sum_{n\in\mathbf{N}} \frac{a_n}{10^{n+1}}$; c'est donc un compact.

Exercice 16.4. Comme $f_n \to f$ uniformément sur E, elle vérifie le critère de Cauchy uniforme, et on a $\lim_{n\to+\infty} \big(\sup_{x\in\mathrm{E},\, p\in\mathbf{N}} |f_n(x) - f_{n+p}(x)| \big) = 0$. Or $|\ell_n - \ell_{n+p}| \leqslant \sup_{x\in\mathrm{E}} |f_n(x) - f_{n+p}(x)|$, et donc $\lim_{n\to+\infty} \big(\sup_{p\in\mathbf{N}} |\ell_n - \ell_{n+p}| \big) = 0$, ce qui prouve que $(\ell_n)_{n\in\mathbf{N}}$ est de Cauchy et comme $\mathbf{C}$ est complet, elle admet une limite ℓ.

Soit maintenant $\varepsilon > 0$. Comme $f_n \to f$ uniformément sur E, il existe $\mathrm{N}_0 \in \mathbf{N}$ tel que l'on ait $|f_n(x) - f(x)| < \varepsilon$, quels que soient $n \geqslant \mathrm{N}_0$ et $x \in \mathrm{E}$. Choisissons $n \geqslant \mathrm{N}_0$. En passant à la limite, on en

déduit que $|\ell_n - \ell| \leqslant \varepsilon$. Par ailleurs, il existe $M > 0$ tel que $|f_n(x) - \ell_n| < \varepsilon$, si $\|x\| > M$; on a donc

$$|f(x) - \ell| \leqslant |f(x) - f_n(x)| + |f_n(x) - \ell_n| + |\ell_n - \ell| < 3\varepsilon,$$

si $\|x\| > M$, ce qui prouve que f tend vers ℓ à l'infini.

Exercice 16.5. (i) Soit $\varepsilon > 0$. Comme f est continue sur $[0,1]$, qui est compact, elle est uniformément continue et il existe $\delta > 0$ tel que $|f(x) - f(y)| \leqslant \varepsilon$ si $|y - x| \leqslant \delta$. Soit $N \in \mathbf{N}$ tel que $\frac{1}{2^N} \leqslant \delta$. Alors $|f(x) - f\big(\frac{i}{2^n}\big)| \leqslant \varepsilon$ pour tout $x \in [i/2^n, (i+1)/2^n[$, si $n \geqslant N$, et donc $\|f - f_n\|_\infty \leqslant \varepsilon$ (la norme $\| \ \|_\infty$ étant relative à l'intervalle $[0,1[$), pour tout $n \geqslant N$. Il s'ensuit que $f_n \to f$, uniformément sur $[0,1[$.

(ii) Il s'agit de prouver que $(u_n)_{n\in\mathbf{N}}$ est de Cauchy. Soient $\varepsilon > 0$ et $N \in \mathbf{N}$ tels que $|f(x) - f\big(\frac{i}{2^n}\big)| \leqslant \varepsilon$ pour tout $x \in [i/2^n, (i+1)/2^n[$, si $n \geqslant N$. On a $u_n - u_{n+p} = \frac{1}{2^{n+p}} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^p-1} \big(f\big(\frac{i}{2^n}\big) - f\big(\frac{i}{2^n} + \frac{j}{2^{n+p}}\big)\big)$ et $\big|f\big(\frac{i}{2^n}\big) - f\big(\frac{i}{2^n} + \frac{j}{2^{n+p}}\big)\big| \leqslant \varepsilon$, pour tous i, j, si $n \geqslant N$ et $p \in \mathbf{N}$. On en déduit la majoration $|u_n - u_{n+p}| \leqslant \varepsilon$, pour tous $n \geqslant N$ et $p \in \mathbf{N}$, ce qui montre que $(u_n)_{n\in\mathbf{N}}$ est de Cauchy.

Exercice 17.1 (i) Comme $u(x)_i = \sum_{j=1}^n a_{i,j} x_j$, on a $|u(x)_i| \leqslant \|x\|_\infty \sum_{j=1}^n |a_{i,j}|$. On en déduit que $\|u\|_\infty \leqslant \sup_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}|$. Maintenant, si $x_j = e^{-\theta_j}$, où $\theta_j = \arg(a_{i,j})$ (resp. $x_j = 1$ si $a_{i,j} = 0$), alors $\|x\|_\infty = 1$ et $u(x)_i = \sum_{j=1}^n |a_{i,j}|$, et donc $\|u\|_\infty \geqslant \sum_{j=1}^n |a_{i,j}|$. Ceci étant vrai pour tout i, on obtient $\|u\|_\infty \geqslant \sup_{1\leqslant i\leqslant n} \sum_{j=1}^n |a_{i,j}|$, ce qui permet de conclure.

(ii) L'hypothèse équivaut à $\|u\|_\infty < 1$; elle implique qu'il existe $c < 1$ tel que $\|u^n\|_\infty \leqslant c^n$ pour tout $n \geqslant 1$. Si on note $a_{i,j}^{(n)}$ les coefficients de la matrice A^n de u^n, on a donc $|a_{i,j}^{(n)}| \leqslant c^n$ pour tous i, j, ce qui prouve que la série des A^n converge, et comme $(1 - A)(1 + A + \cdots + A^{n-1}) = 1 - A^n$, un passage à la limite montre que $1 - A$ est inversible d'inverse $\sum_{n\in\mathbf{N}} A^n$. On en déduit l'inversibilité de $1 - u$.

Exercice 17.2. (i) Si $\phi \in E$, alors $\|\phi\|_\infty$ est fini car $[0,1]$ est compact et une fonction continue sur un compact est bornée. Que $\| \ \|_\infty$ soit une norme sur E est alors immédiat. Maintenant, une suite $(\phi_n)_{n\in\mathbf{N}}$ est de Cauchy pour $\| \ \|_\infty$ si et seulement si elle vérifie le critère de Cauchy uniforme sur $[0,1]$, et $\mathbf{C}$ étant complet, on sait (alinéa 16.2) que $(\phi_n)_{n\in\mathbf{N}}$ admet une limite simple ϕ qui est continue sur $[0,1]$, et que $\phi_n \to \phi$ uniformément sur $[0,1]$, ce qui signifie exactement que $\phi_n \to \phi$ pour $\| \ \|_\infty$. On en déduit la complétude de $(E, \| \ \|_\infty)$.

(ii) Que $\| \ \|_1$ soit une norme est immédiat à part peut-être le fait que « $\|\phi\|_1 = 0$ » implique « $\phi = 0$ ». Mais si $\phi \neq 0$, il existe $x_0 \in [0,1]$ avec $\phi(x_0) \neq 0$, et comme ϕ est continue, il existe un intervalle I de longueur non nulle ℓ sur lequel $|\phi(x)| \geqslant |\phi(x_0)/2|$. On a alors $\|\phi\|_1 \geqslant \ell\,|\phi(x_0)/2| > 0$. Maintenant, soit $\phi_n = x^{-1/2}\mathbf{1}_{[1/n,1]}$. La suite $(\phi_n)_{n\geqslant 1}$ est de Cauchy car

$$\|\phi_{n+p} - \phi_n\|_1 = \int_{1/(n+p)}^{1/n} x^{-1/2}\,dx = 2\Big(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+p}}\Big) \leqslant \frac{2}{\sqrt{n}}.$$

Si cette suite avait une limite ϕ dans E, on aurait $\lim_{n\to+\infty} \int_0^1 |\phi - \phi_n| = 0$. Or, pour tous $a > 0$ et $n \geqslant 1/a$, on a $\int_0^1 |\phi - \phi_n| \geqslant \int_a^1 |\phi - \phi_n| = \int_a^1 |\phi(x) - x^{-1/2}|\,dx$. On devrait donc avoir $\int_a^1 |\phi(x) - x^{-1/2}|\,dx = 0$, quel que soit $a > 0$, et ϕ étant continue, cela implique que $\phi(x) = x^{-1/2}$, pour tout $x > a$ et tout $a > 0$, et donc que $\phi(x) = x^{-1/2}$ si $x \in]0,1]$. Ceci n'est pas possible car cette fonction n'est pas la restriction à $]0,1]$ d'une fonction continue sur $[0,1]$. En résumé $(\phi_n)_{n\in\mathbf{N}}$ n'a pas de limite dans E, et E n'est pas complet pour $\| \ \|_1$.

(iii) Si les normes étaient équivalentes, les suites de Cauchy seraient les mêmes dans les deux cas, et donc E serait simultanément complet ou non pour les deux normes, ce qui n'est pas le cas. On peut aussi remarquer que $\|\phi_n\|_1 \leqslant 2$ pour tout n, alors que $\|\phi_n\|_\infty \to +\infty$

Exercice 17.3. (i) $\mathrm{id} : (X, \mathscr{T}_1) \to (X, \mathscr{T}_2)$ est continue si et seulement si l'image réciproque de tout ouvert de $(X, \mathscr{T}_2)$ par id est un ouvert de $(X, \mathscr{T}_1)$, et donc si et seulement si tout élément de $\mathscr{T}_2$ est élément de $\mathscr{T}_1$.

(ii) Si $\phi_n(x) = \phi\big(\frac{x}{n}\big)$, où $\phi(x) = (1-|x|)\mathbf{1}_{[-1,1]}(x)$, alors $\|\phi_n\|_\infty = 1$, tandis que $\|\phi_n\|_1 = n$ tend vers $+\infty$, ce qui prouve que id : $(\mathscr{C}_c(\mathbf{R}), \|\ \|_\infty) \to (\mathscr{C}_c(\mathbf{R}), \|\ \|_1)$ n'est pas continue et donc que $\mathscr{T}_\infty$ n'est pas plus fine que $\mathscr{T}_1$.

De même, si $\phi_n(x) = \inf(n, |x|^{-1/2} - 1)\mathbf{1}_{[-1,1]}(x)$, alors $\|\phi_n\|_1 \leqslant \int_{-1}^{1} \big(|x|^{-1/2} - 1\big)\, dx = 2$, tandis que $\|\phi_n\|_\infty = n$ tend vers $+\infty$, ce qui prouve que id : $(\mathscr{C}_c(\mathbf{R}), \|\ \|_1) \to (\mathscr{C}_c(\mathbf{R}), \|\ \|_\infty)$ n'est pas continue et donc que $\mathscr{T}_1$ n'est pas plus fine que $\mathscr{T}_\infty$.

Exercice 17.4. Soit $b_n = \frac{a_n}{n}$ et soit $\ell = \inf_{n\geqslant 1} b_n$. Montrons que $b_n \to \ell$; il s'agit de vérifier que $v_n \leqslant c$, pour tout $n \gg 0$, si $c > \ell$. Soit $d \geqslant 1$ tel que $b_d < c$. On a $a_{dq+r} \leqslant qa_d + a_r$, comme le montre une récurence immédiate (sur q), et donc $b_{dq+r} \leqslant \frac{dq}{dq+r} b_d + \frac{r}{dq+r} b_r$. Soit $\mathrm{Q} \geqslant 1$ tel que $\sup_{0\leqslant r\leqslant d-1} \frac{rb_r}{dq+r} \leqslant \frac{c-b_d}{2}$, pour tout $q \geqslant \mathrm{Q}$. On a alors $b_n \leqslant b_d + \frac{c-b_d}{2} = \frac{c+b_d}{2} \leqslant c$, pour tout $n \geqslant d\mathrm{Q}$. Ceci permet de conclure.

Exercice 17.5. (i) On a $\|u\|_{\mathrm{sp}} = \|v\|_{\mathrm{sp}} = 0$ car $u^2 = v^2 = 0$, et $\|uv\|_{\mathrm{sp}} = \|u+v\|_{\mathrm{sp}} = 1$ car $(u+v)^2 = 1$ et $(uv)^2 = uv$.

(ii) Comme u et v commutent, on a $(uv)^n = u^n v^n$, et donc $\|(uv)^n\| \leqslant \|u^n\|\,\|v^n\|$. En prenant les racines n-ièmes et en passant à la limite, on en déduit l'une des deux inégalités $\|uv\|_{\mathrm{sp}} \leqslant \|u\|_{\mathrm{sp}}\,\|v\|_{\mathrm{sp}}$ à démontrer.

Passons à l'autre. Posons $a = \|u\|_{\mathrm{sp}}$ et $b = \|v\|_{\mathrm{sp}}$. Multiplier u et v par $\lambda \in \mathbf{C}^*$ multiplie $\|u\|$, $\|v\|$, $\|u+v\|$, a, b et $\|u+v\|_{\mathrm{sp}}$ par $|\lambda|$. On peut donc supposer $\|u\| < 1$ et $\|v\| < 1$; on a alors $\|u^i\| < 1$, $\|v^i\| < 1$, pour tout i, et $a < 1$, $b < 1$. Soit $\varepsilon > 0$ tel que $a + \varepsilon < 1$ et $b + \varepsilon < 1$. Il existe $\mathrm{I} \geqslant 1$ tel que $\|u^i\| \leqslant (a+\varepsilon)^i$ et $\|v^i\| \leqslant (b+\varepsilon)^i$, pour tout $i \geqslant \mathrm{I}$. On a alors, car u et v commutent,

$$\begin{aligned}
\|(u+v)^n\| = \Big\|\sum_{i=0}^{n} \binom{n}{i} u^i v^{n-i}\Big\| &\leqslant \sum_{i=0}^{n} \binom{n}{i} \|u\|^i \|v\|^{n-i} \\
&\leqslant \sum_{i=0}^{\mathrm{I}-1} \binom{n}{i} (b+\varepsilon)^{n-i} + \sum_{i=\mathrm{I}}^{n-\mathrm{I}} \binom{n}{i} (a+\varepsilon)^i (b+\varepsilon)^{n-i} + \sum_{i=n-\mathrm{I}+1}^{n} \binom{n}{i} (a+\varepsilon)^i \\
&\leqslant (a+b+2\varepsilon)^n + \sum_{i=0}^{\mathrm{I}-1} \binom{n}{i} \big((b+\varepsilon)^{n-i} + (a+\varepsilon)^{n-i}\big)
\end{aligned}$$

On peut mettre $(a+b+2\varepsilon)^n$ en facteur, et dans la parenthèse, il y a 1 plus deux termes du type $\delta^n \sum_{i=1}^{\mathrm{I}-1} \alpha_i \binom{n}{i}$, avec $\delta < 1$, qui tendent vers 0 (car produits d'un polynôme par une exponentielle de raison < 1). La parenthèse tend donc vers 1, et la limite de $\|u+v\|^{1/n}$ est donc $\leqslant a+b+2\varepsilon$. Le résultat s'en déduit en faisant tendre ε vers 0.

Exercice 17.7. (i) $(a,b) \mapsto a+b$ est linéaire, et on a $|a+b| \leqslant |a| + |b| \leqslant 2\|(a,b)\|_\infty$; on en déduit la continuité de $(a,b) \mapsto a+b$. De même, $(a,b) \mapsto ab$ est bilinéaire, et on a $|ab| = |a|\,|b| \leqslant |a|\,|b|$; on en déduit la continuité de $(a,b) \mapsto ab$.

(ii) $f+g$ est la composée de $x \mapsto (f(x), g(x))$ de X dans $\mathbf{K}^2$, et de $(a,b) \mapsto a+b$ de $\mathbf{K}^2$ dans $\mathbf{K}$; elle est donc continue comme composée d'applications continues. De même, fg est la composée de $x \mapsto (f(x), g(x))$ de X dans $\mathbf{K}^2$, et de $(a,b) \mapsto ab$ de $\mathbf{K}^2$ dans $\mathbf{K}$; elle est donc continue comme composée d'applications continues.

Exercice 18.1. La sesquilinéarité de $\langle\ ,\ \rangle$ suit facilement de la linéarité de l'intégration ; sa symétrie est une évidence. Enfin, si $f \neq 0$ et si $f(t_0) \neq 0$, il existe un intervalle I contenant t_0, ouvert dans $[0,1]$, tel que $|f(t) - f(t_0)| \leqslant \frac{|f(t_0)|}{2}$, et donc $|f(t)| \geqslant \frac{|f(t_0)|}{2}$, pour tout $t \in \mathrm{I}$; alors $\langle f, f\rangle = \int_0^1 |f(t)|^2\, dt \geqslant \frac{|f(t_0)|^2}{4} \lg(\mathrm{I}) > 0$, ce qui prouve que $\langle\ ,\ \rangle$ est défini positif.

Exercice 18.2. ${}^t\overline{\mathrm{A}}\mathrm{A}$ est la matrice de Gram des colonnes $\mathrm{X}_1, \dots, \mathrm{X}_n$ de A. Son déterminant $|\det \mathrm{A}|^2$ est donc $\prod_{j=1} d(\mathrm{X}_j, \mathrm{vect}(\mathrm{X}_1, \dots, \mathrm{X}_{j-1}))^2$. Par ailleurs, on a $|a_{1,j}|^2 + \cdots + |a_{n,j}|^2 = \|\mathrm{X}_j\|^2$, et on conclut en remarquant que $d(\mathrm{X}_j, \mathrm{vect}(\mathrm{X}_1, \dots, \mathrm{X}_{j-1})) \leqslant \|\mathrm{X}_j\|$.

Exercice 18.3. (i) Soit $X = {}^t(x_1, \dots, x_n) \in \mathbf{R}^n$ vérifiant $AX = 0$ et soit $s = \sum_{i=1}^n x_i$. La condition $AX = 0$ se traduit alors par $ks + (k_i - k)x_i = 0$ pour tout i. Si $k = 0$, alors A est diagonale et inversible puisque les coefficients diagonaux sont non nuls par hypothèse car > 0. On peut donc supposer $k > 0$, et il y a deux cas :

$\diamond$ $k_i = k$ pour un i et alors $s = 0$, $x_j = 0$ si $j \neq i$, et donc $x_i = 0$ aussi puisque $s = 0$.

$\diamond$ $k_i > k$ pour tout i, et alors x_i est de signe opposé à celui de s pour tout i, et donc $x_i = 0$ pour tout i puisque s est la somme des x_i.

Il s'ensuit que dans tous les cas, 0 est l'unique solution de $AX = 0$, et donc le système est de Cramer et A est inversible.

(ii) Si $E \subset \{1, \dots, m\}$ soit $X_E = {}^t(x_1, \dots, x_m) \in \mathbf{R}^m$ définie par $x_i = 1$ si $i \in E$, et $x_i = 0$ si $i \notin E$. On a alors ${}^tX_E X_F = |E \cap F|$, si $E, F \subset \{1, \dots, m\}$. Soit donc $I = \{E_1, \dots, E_n\}$ vérifiant les conditions de la question. Alors la matrice de Gram des E_i a tous ses coefficients non diagonaux égaux à k ; de plus ses coefficients diagonaux sont > 0 puisqu'on a supposé les E_i non vides, ils sont $\geqslant k$ puisque $|E_i| \geqslant |E_i \cap E_j|$, si $i \neq j$, et au plus un est égal à k car $|E_i| = |E_j| = |E_i \cap E_j|$ implique $E_i = E_j$. D'après le (i), ceci implique que la matrice de Gram est de rang n ; il s'ensuit que $X_{E_1}, \dots, X_{E_n}$ est aussi de rang n, et comme ces vecteurs vivent dans un espace de dimension m, on a $n \leqslant m$.

(iii) Si F est un corps fini, de cardinal q, deux droites distinctes du plan projectif $\mathbf{P}^2(F)$ se coupent en exactement 1 point, et il y a autant de droites que de points (une droite de $\mathbf{P}^2(F)$ est l'image d'un plan de F^3, et comme un plan est défini par une équation à scalaire près, cela fournit une bijection entre les plans de F^3 et les droites de F^3, et donc une bijection entre les droites de $\mathbf{P}^2(F)$ et les points de $\mathbf{P}^2(F)$). Ceci fournit un exemple avec $|I| = m = q^2 + q + 1$ et $k = 1$. Plus généralement, deux hyperplans distincts de $\mathbf{P}^k(F)$ se coupent en un sous-espace de codimension 2, ce qui fournit un exemple avec $|I| = m = q^k + \cdots + q + 1$ et $k = q^{k-2} + \cdots + 1$

Exercice 18.4. Utilisons « symétrie » pour désigner une symétrie orthogonale par rapport à un hyperplan.

(i) La symétrie orthogonale par rapport à $(v_1 - v_2)^\perp$ fait l'affaire (et c'est la seule).

(ii) Si $n = 1$, alors $s = \pm 1$ est le produit de 0 ou 1 symétries. Supposons donc $n \geqslant 2$. Si $u(v) = v$ pour tout v, alors u est le produit de 0 symétries. Sinon on choisit $v \in V$ tel que $u(v) \neq v$ et u étant unitaire, on a $\|u(v)\| = \|v\|$, et le (i) nous fournit une symétrie s_1 tel que $s(u(v)) = v$. Alors $s_1 \circ u$ est unitaire et laisse fixe v, et donc aussi son orthogonal V'. La restriction de $s_1 \circ u$ à V' est produit d'au plus $n - 1$ symétries $s'_2 \circ \cdots \circ s'_r$ d'après l'hypothèse de récurrence. On prolonge s'_i en une symétrie de V en posant $s_i(\lambda v + v') = \lambda v + s'_i(v')$ si $\lambda \in \mathbf{K}$ et $v' \in V'$ (ceci est bien une symétrie par rapport à un hyperplan, et elle est unitaire car s'_i l'est et λv est orthogonal à v' et $s'_i(v')$). Alors $s_1 \circ v = s_2 \circ \cdots \circ s_r$ car les deux membres coïncident sur v et sur son orthogonal V'. Comme $s_1^{-1} = s_1$, on obtient $u = s_1 \circ \cdots \circ s_r$, ce qui permet de conclure.

Exercice 18.5. Si $A \in \mathbf{U}(n)$, il existe $P \in \mathbf{U}(n)$ tel que $A = P\,\mathrm{Diag}(e^{i\theta_1}, \dots, e^{i\theta_n})P^{-1}$. Alors $A(t) = P\,\mathrm{Diag}(e^{i\theta_1 t}, \dots, e^{i\theta_n t})P^{-1} \in \mathbf{U}(n)$, pour tout $t \in [0, 1]$, et $t \mapsto A(t)$ est un chemin reliant 1 à A dans $\mathbf{U}(n)$. On en déduit la connexité de $\mathbf{U}(n)$ par arcs. Celle de $\mathbf{SU}(n)$ se démontre en remarquant que l'on peut imposer $\sum_{i=1}^n \theta_i = 0$ si $A \in \mathbf{SU}(n)$, et alors $A(t) \in \mathbf{SU}(n)$, pour tout $t \in [0, 1]$.

Exercice 18.6. Si $P \in \mathbf{SO}(n)$, il existe $Q \in \mathbf{O}(n)$ tel que QPQ^{-1} soit de la forme $\mathrm{Diag}(R_{\theta_1}, \dots, R_{\theta_m})$ ou $\mathrm{Diag}(1, R_{\theta_1}, \dots, R_{\theta_m})$ suivant que n est pair ou impair. Mais alors $t \mapsto Q^{-1}\mathrm{Diag}(R_{t\theta_1}, \dots, R_{t\theta_m})$ (resp. $t \mapsto Q^{-1}\mathrm{Diag}(1, R_{t\theta_1}, \dots, R_{t\theta_m})$) est un chemin dans $\mathbf{SO}(n)$ reliant 1 à P. Il s'ensuit que $\mathbf{SO}(n)$ est connexe par arcs.

$\mathbf{O}(n)$ n'est pas connexe car son image par l'application déterminant, qui est continue, est $\{1, -1\}$ qui n'est pas connexe.

Exercice 18.7. (i) Soit $A \in \mathbf{GL}_n(\mathbf{C})$. On peut écrire A sous la forme $A = PM$, avec $P \in \mathbf{U}(n)$, et M triangulaire supérieure à coefficients diagonaux > 0. Par ailleurs, d'après l'ex. 18.5, on peut trouver un chemin $t \mapsto P(t)$ joignant 1_n à P dans $\mathbf{U}(n)$. Alors $t \mapsto P(t)(tM + (1-t)1_n)$ est un chemin joignant 1_n à A dans $\mathbf{GL}_n(\mathbf{C})$. On en déduit la connexité par arcs de $\mathbf{GL}_n(\mathbf{C})$.

Si $A \in \mathbf{SL}_n(\mathbf{C})$, dans la décomposition $A = PM$, on a $P \in \mathbf{SU}(n)$ car $\det P$ est à la fois de module 1 et > 0. Par ailleurs, on peut écrire M sous la forme $\mathrm{Diag}(e^{a_1}, \dots, e^{a_n})N$, où $\sum_{i=1}^n a_i = 0$ et N est triangulaire supérieure avec des 1 sur la diagonale. D'après l'ex. 18.5, on peut trouver un chemin $t \mapsto P(t)$ joignant 1_n à P dans $\mathbf{SU}(n)$. Alors $t \mapsto P(t)\,\mathrm{Diag}(e^{a_1 t}, \dots, e^{a_n t})(tN + (1-t)1_n)$ est un chemin joignant 1_n à A dans $\mathbf{SL}_n(\mathbf{C})$. On en déduit la connexité par arcs de $\mathbf{SL}_n(\mathbf{C})$.

(ii) La démonstration dans le cas de $\mathbf{SL}_n(\mathbf{R})$ est la même que pour $\mathbf{SL}_n(\mathbf{C})$; il suffit de remplacer le résultat de l'ex. 18.5 par celui de l'ex. 18.6. Par contre $\mathbf{GL}_n(\mathbf{R})$ n'est pas connexe car son image par l'application déterminant est $\mathbf{R}^*$ qui n'est pas connexe.

Exercice 18.8. (i) L'application $P \mapsto {}^t\overline{P}P$ de $\mathbf{M}_n(\mathbf{C})$ dans $\mathbf{M}_n(\mathbf{C})$ est continue, et $\mathbf{U}(n)$ est l'image inverse du fermé $\{1\}$; il est donc fermé dans $\mathbf{M}_n(\mathbf{C})$. Par ailleurs, il est borné car ${}^t\overline{P}P = 1$ implique que les termes diagonaux $\sum_{j=1}^n |a_{i,j}|^2$ sont égaux à 1 pour tout j, et donc $|a_{i,j}| \leqslant 1$ pour tous i, j. Comme $\mathbf{M}_n(\mathbf{C})$ est un espace vectoriel de dimension finie sur $\mathbf{C}$, cela implique que $\mathbf{U}(n)$ est compact.

(ii) Le polynôme caractéristique de M est $(X-1)^n$; on a donc $(M-1)^n = 0$ d'après le th. de Cayley-Hamilton. Comme $(M-1)^n = 0$, la formule du binôme nous donne $M^m = (1 + (M-1))^m = \sum_{k=0}^{n-1} \binom{m}{k} (M-1)^k$, ce qui est effectivement un polynôme en m. Comme un polynôme est borné si et seulement si il est constant, il s'ensuit que $\{M^m,\ m \in \mathbf{Z}\}$ est borné si et seulement si $M^m = 1$, pour tout m, et donc $M = 1$ (pour $m = 1$).

(iii) Soit H un sous-groupe compact de $\mathbf{GL}_n(\mathbf{C})$ contenant $\mathbf{U}(n)$, et soit $A \in H$. On peut écrire A sous la forme $A = PM$, où $P \in \mathbf{U}(n)$, et M est triangulaire supérieure à coefficients diagonaux réels > 0, et comme H contient P^{-1}, il contient aussi M. Soient $\lambda_1, \dots, \lambda_n$ les coefficients diagonaux de M ; ceux de M^m, pour $m \in \mathbf{Z}$, sont alors $\lambda_1^m, \dots, \lambda_n^m$, et comme $M^m \in H$ qui est compact par hypothèse, on en déduit que $\{\lambda_i^m,\ m \in \mathbf{Z}\}$ est borné et donc que $\lambda_i = 1$ pour tout i. Le (ii) montre alors que $M = 1$ si $\{M^m,\ m \in \mathbf{Z}\}$ est borné, ce qui est le cas puisque $M^m \in H$ pour tout $m \in \mathbf{Z}$. On a donc prouvé que $A \in \mathbf{U}(n)$, ce qui permet de conclure.

Exercice 18.9. (i) La sesquilinéarité de $\langle\ ,\ \rangle$ résulte de la linéarité de l'intégration, la symétrie est évidente, et pour prouver que $\langle\ ,\ \rangle$ est définie positive, il suffit de recopier les arguments de l'ex. 18.1.

(ii) Une intégration par partie nous donne

$$\int_0^1 \overline{f}(t)\Delta g(t)\,dt = [-\overline{f}g']_0^1 + \int_0^1 \overline{f}'(t)g'(t)\,dt = [-\overline{f}g']_0^1 + [\overline{f}''g]_0^1 + \int_0^1 \Delta\overline{f}(t)g(t)\,dt.$$

Comme $[-\overline{f}g']_0^1 = [\overline{f}''g]_0^1 = 0$ par périodicité de f et g, on obtient $\int_0^1 \overline{f}(t)\Delta g(t)\,dt = \int_0^1 \Delta\overline{f}(t)g(t)\,dt = \int_0^1 \overline{\Delta f}(t)g(t)\,dt$, et donc $\langle f, \Delta g\rangle = \langle \Delta f, g\rangle$, ce qui prouve que Δ est autoadjoint.

Maintenant, $\lambda \in \mathbf{C}$ est valeur propre de Δ si et seulement si il existe $\phi : \mathbf{R} \to \mathbf{C}$, de classe $\mathscr{C}^\infty$, périodique de période 1, solution de l'équation différentielle $\phi'' + \lambda\phi = 0$. Les solutions de cette équation différentielle sont de la forme $t \mapsto \alpha e^{\sqrt{-\lambda}t} + \beta e^{-\sqrt{-\lambda}t}$ si $\lambda \neq 0$; une telle solution peut être périodique de période 1 si et seulement si $\sqrt{-\lambda} \in 2i\pi\mathbf{Z}$. Il s'ensuit que les valeurs propres de Δ sont les $4\pi^2 n^2$, pour $n \in \mathbf{N}$, l'espace propre associé étant engendré par ϕ_n et ϕ_{-n} avec $\phi_n(t) = e^{2i\pi nt}$, si $n \neq 0$ (l'espace propre associé à 0 est l'espace des fonctions constantes ; il est de dimension 1).

(iii) L'opérateur Δ n'est pas continu car $\frac{1}{\|\phi_n\|}\|\Delta\phi_n\| = 4\pi^2 n^2$ tend vers $+\infty$ quand $n \to +\infty$, et donc Δ n'est pas lipschitzien.

Exercice 18.10. (i) $P_n = \frac{1}{\|X^n - p_{n-1}(X^n)\|}(X^n - p_{n-1}(X^n))$, où p_{n-1} désigne la projection orthogonale de $\mathbf{R}[X]^{(n)}$ sur $\mathbf{R}[X]^{(n-1)}$. Il est apparent sur cette formule que P_n est de degré n, de coefficient dominant > 0.

(ii) Soient $\alpha_1, \dots, \alpha_r$ les zéros d'ordre impair de P_n dans $]0,1[$. Alors $P_n \prod_{i=1}^r (X - \alpha_i)$ est de signe constant sur $[0,1]$, et donc $\langle P_n, \prod_{i=1}^r (X - \alpha_i)\rangle$ est non nul. Comme P_n est orthogonal à $\mathbf{R}[X]^{(n-1)}$, cela implique que $r \geqslant n$, et donc que tous les zéros de P_n sont dans l'intervalle $]0,1[$ et sont de multiplicité 1.

(iii) Il s'agit de vérifier que $\langle P, RQ\rangle = \langle RP, Q\rangle$, pour tous P, Q, mais c'est immédiat sur la définition.

(iv) $XP_{n-1} = \frac{p_{n-1}}{p_n} P_n + Q$, où $Q \in \mathbf{R}[X]^{(n-1)}$, et donc $\langle P_n, Q\rangle = 0$ et $\langle P_n, XP_{n-1}\rangle = \frac{p_{n-1}}{p_n}$, car $\langle P_n, P_n\rangle = 1$.

(v) Si $a_n = \frac{p_n}{p_{n-1}}$, alors $P_n - a_n XP_{n-1}$ est de degré $\leqslant n-1$. Il existe donc b_n, c_n tels que $Q = P - a_n XP_{n-1} - (b_n P_{n-1} - c_n P_{n-2})$ soit de degré $< n-2$. Mais alors

$$\langle Q, P_n - (a_n X + b_n)P_{n-1} + c_n P_{n-2}\rangle = \langle Q, P_n\rangle - \langle (a_n X + b_n)Q, P_{n-1}\rangle + \langle c_n Q, P_{n-2}\rangle = 0,$$

car Q est orthogonal à P_n et P_{n-2} puisque $\deg Q < n-2$, et $(a_n X + b_n)Q$ est orthogonal à P_{n-1} puisque $\deg\big((a_n X + b_n)Q\big) < n-1$. On a donc $\langle Q, Q\rangle = 0$, ce qui prouve que $Q = 0$. Il reste à vérifier que $c_n > 0$. Or $0 = \langle P_{n-2}, P_n - (a_n X + b_n)P_{n-1} + c_n P_{n-2}\rangle = c_n - \langle P_{n-2}, a_n XP_{n-1}\rangle = c_n - a_n \frac{p_{n-2}}{p_{n-1}}$, et donc $c_n = \frac{p_{n-2}}{p_n} > 0$.

(vi) On raisonne par récurrence sur n. Il n'y a rien à prouver si $n = 1$. Si $n \geqslant 2$, l'hypothèse de récurrence $x_{n-1,1} < x_{n-2,1} < x_{n-1,2} < x_{n-2,2} < \cdots$ implique que $P_{n-2}(x_{n-1,n-1}) > 0$ puisque le coefficient dominant de P_{n-2} est > 0, et $P_{n-2}(x_{n-1,n-2}) < 0$,..., $P_{n-2}(x_{n-1,n-i})$ est de signe $(-1)^{i-1}$, car P_{n-2} change de signe en chacune de ses racines. Or $P_{n-2}(x_{n-1,i})$ et $P_n(x_{n-1,i})$ sont de signes opposés d'après le (v). On a donc $P_n(x_{n-1,n-1}) < 0$, $P_n(x_{n-1,n-2}) > 0$,..., $P_n(x_{n-1,1})$ de signe $(-1)^{n-1}$. Il y a donc une racine de P_n entre $x_{n-1,1}$ et $x_{n-1,2}$, une entre $x_{n-1,2}$ et $x_{n-1,3}$, etc., ce qui nous en fournit déjà $n-2$. De plus, le coefficient dominant de P_n étant > 0, on a $P_n(x) > 0$ pour $x \gg 0$, et donc P_n a une racine $> x_{n-1,n-1}$, et on a $P_n(x)$ de signe $(-1)^n$, pour $x \ll 0$, et donc P_n a une racine $< x_{n-1,1}$. Ceci permet de conclure.

Exercice 20.2. (i) On a $|x+y|_p \leqslant |x|_p$. Si $|x+y|_p < |x|_p$, alors $x = (x+y) - y$ et donc $|x|_p \leqslant \sup(|x+y|_p, |y|_p) < |x|_p$, ce qui est absurde. Donc $|x+y|_p = |x|_p$.

(ii) Comme $u_n \to 0$, la série $\sum_{n=1}^{+\infty} u_n$ converge et si on note y sa somme, alors $|y|_p \leqslant \sup_{n\geqslant 1} |u_n|_p$. Comme on a supposé $|u_0|_p > |u_n|_p$, pour tout $n \geqslant 1$, on en déduit $|y|_p < |u_0|$, puis $|u_0 + y|_p = |u_0|_p$; en particulier, $u_0 + y = \sum_{n\in\mathbf{N}} u_n \neq 0$.

Exercice 20.3. (i) Si $n = 1$, alors $\eta - 1$ est racine du polynôme $P(X) = \frac{(1+X)^p - 1}{X} = \sum_{i=0}^{p-1} a_i X^i$, où $a_i = \binom{p}{i+1}$, et donc $a_0 = p$, $a_{p-1} = 1$ et a_i est divisible par p, et donc vérifie $|a_i|_p \leqslant p^{-1}$ si $i \leqslant p-2$. Maintenant, si $|z|_p \neq \rho_1$, alors $|a_i z^i|_p = |a_i|_p |z|_p^i$ atteint son maximum pour un unique $i \in \{0, \dots, p-1\}$, à savoir $i = p-1$ si $|z|_p > \rho_1$ (auquel cas on a $|P(z)|_p = |z|_p^{p-1}$), et $i = 0$ si $|z| < \rho_1$ (et alors $|P(z)|_p = p^{-1}$). Il s'ensuit que $P(z) \neq 0$ pour un tel z, ce qui permet de conclure.

Si $n \geqslant 2$, et si η est une racine primitive p^n-ième de l'unité, alors $|\eta^p - 1|_p = \rho_{n-1}$, d'après l'hypothèse de récurrence, et $\eta - 1$ est racine du polynôme $P_n(X) = (X+1)^p - \eta^p = XP(X) + (1 - \eta^p)$. Comme $p^{-1} \leqslant \rho_{n-1} \leqslant 1$, la méthode précédente montre que $P_n(z) \neq 0$, si $|z|_p \neq \rho_{n-1}^{1/p}$. On a donc $|\eta - 1|_p = \rho_{n-1}^{1/p} = \rho_n$.

(ii) Supposons $[\overline{\mathbf{Q}}_p : \mathbf{Q}_p] = d < +\infty$, et soient n tel que $(p-1)p^{n-1} > d$, η une racine p^n-ième de l'unité et $\alpha = \eta - 1$, de telle sorte que $|\alpha|_p = \rho_n$. Comme $[\overline{\mathbf{Q}}_p : \mathbf{Q}_p] = d$, les α^i, pour $i \leqslant d$, forment une famille liée. Il existe donc $a_0, \dots, a_d \in \mathbf{Q}_p$, non tous nuls, tels que $\sum_{i=0}^d a_i \alpha^i = 0$. Mais ceci n'est pas possible car les $a_i \alpha^i$ pour lesquels $a_i \neq 0$ ont tous des normes différentes (la partie fractionnaire de $v_p(a_i \alpha^i)$ est $\frac{i}{(p-1)p^{n-1}}$, et ces parties fractionnaires sont deux à deux distinctes car $d < (p-1)p^{n-1}$), et donc $\big|\sum_{i=0}^d a_i \alpha^i\big|_p = \sup_{i\leqslant d} |a_i \alpha^i|_p \neq 0$.

Exercice 20.6. (i) Par définition f est localement constante si et seulement si $\{x \in X,\ f(x) = y\}$ est voisinage de chacun des ses points (ce qui équivaut à ce qu'il soit ouvert). Il en résulte que l'image inverse de tout ensemble (en particulier d'un ouvert) est ouverte, et donc que f est continue.

(ii) $\{x \in [0,1],\ f(x) = f(0)\}$ est ouvert et fermé d'après le (i), et comme il est non vide et que $[0,1]$ est connexe, c'est $[0,1]$ tout entier. Autrement dit, les seules fonctions localement constantes sur $[0,1]$ sont les fonctions constantes.

(iii) $a + p^n\mathbf{Z}_p$ est à la fois ouvert et fermé, et donc $\{x,\ \mathbf{1}_{a+p^n\mathbf{Z}_p}(x) = 0\}$ et $\{x,\ \mathbf{1}_{a+p^n\mathbf{Z}_p}(x) = 1\}$ sont ouverts, ce qui permet d'utiliser le (i).

(iv) Si $\phi : \mathbf{Z}_p \to \mathrm{Y}$ est localement constante et si $a \in \mathbf{Z}_p$, il existe $n_a \in \mathbf{N}$ tel que ϕ soit constante sur $a+p^{n_a}\mathbf{Z}_p$. Les $a+p^{n_a}\mathbf{Z}_p$ forment un recouvrement ouvert de $\mathbf{Z}_p$ et, $\mathbf{Z}_p$ étant compact, on peut en extraire un sous-recouvrement fini par des $a + p^{n_a}\mathbf{Z}_p$, avec $a \in \mathrm{A}$, où A est un ensemble fini. Soit $n = \sup_{a\in\mathrm{A}} n_a$. Si $b \in \mathbf{Z}_p$, il existe $a \in \mathrm{A}$ tel que $b \in a+p^{n_a}\mathbf{Z}_p$ et, comme $n \geqslant n_a$, on a $b+p^n\mathbf{Z}_p \subset a+p^{n_a}\mathbf{Z}_p$ (deux boules sont soit disjointes soit l'une est incluse dans l'autre). Il en résulte que ϕ est constante sur $b+p^n\mathbf{Z}_p$ pour tout $b \in \mathbf{Z}_p$.

(v) Comme $\mathbf{Z}_p$ est compact, une fonction continue f sur $\mathbf{Z}_p$ est uniformément continue. Ceci se traduit, en notant $\|\ \|$ la norme sur $\mathbf{R}$ ou la norme p-adique sur $\mathbf{Q}_p$, par l'existence, pour tout $\varepsilon > 0$, de $n \in \mathbf{N}$, tel que $\|f(x) - f(y)\|| \leqslant \varepsilon$, pour tous $x, y \in \mathbf{Z}_p$ vérifiant $|x - y|_p \leqslant p^{-n}$. Soit alors $\phi = \sum_{i=0}^{p^n-1} f(i)\mathbf{1}_{i+p^n\mathbf{Z}_p}$. Par construction, ϕ est localement constante, et on a $\|f(x) - \phi(x)\| \leqslant \varepsilon$ pour tout $x \in \mathbf{Z}_p$ (en effet, sur $i + p^n\mathbf{Z}_p$, on a $f(x) - \phi(x) = f(x) - f(i)$ et $|x - i|_p \leqslant p^{-n}$). Ceci permet de conclure.

(vi) On peut prendre la fonction qui envoie $x \in \mathbf{Z}_p$, dont l'écriture en base p est $\sum_{n=0}^{+\infty} a_n p^n$ (les a_n sont des éléments de $\{0, 1, \ldots, p-1\}$) sur $\sum_{n=0}^{+\infty} a_n p^{-1-n}$; nous laissons le soin au lecteur de vérifier que cette fonction est 1-lipschitzienne et d'imaginer à quoi elle correspond sur la description arboricole de $\mathbf{Z}_p$. L'image d'un connexe par une fonction continue est un connexe, et comme les composantes connexes de $\mathbf{Z}_p$ sont des points, toute fonction continue de $[0,1]$ dans $\mathbf{Z}_p$ est constante.

Exercice 20.7. (i) On a $\left|\left(\frac{7}{9}\right)^n\right|_7 = 7^{-n}$ et donc la série $\sum_{n=0}^{+\infty}\left(\frac{7}{9}\right)^n\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_7, \mathbf{Q}_7)$ vers une fonction continue f. De plus, si $k \in \mathbf{N}$, alors $f(k) = \left(\frac{16}{9}\right)^k$, d'après la formule du binôme. On en déduit que $f(2k) = f(k)^2$ pour tout $k \in \mathbf{N}$, ce qui implique, compte-tenu de la densité de $\mathbf{N}$ dans $\mathbf{Z}_7$ et de la continuité de f, que $f(2x) = f(x)^2$ pour tout $x \in \mathbf{Z}_7$. Il en résulte que la somme S de la série qui nous intéresse est une racine carrée de $\frac{16}{9}$; on a donc $\mathrm{S} = \pm\frac{4}{3}$. Par ailleurs, tous les termes de la série, sauf le premier, sont dans $7\mathbf{Z}_7$, et donc $\mathrm{S} - 1 \in 7\mathbf{Z}_7$ et $\mathrm{S} = \frac{-4}{3}$, ce que l'on cherchait à démontrer.

(ii) Dans $\mathbf{R}$ la somme de la série est $\frac{4}{3}$.

CHAPITRE I

REPRÉSENTATIONS DES GROUPES FINIS

Si G est un groupe, une représentation V de G est un espace vectoriel sur un corps K (ou, plus généralement, un module sur un anneau A) muni d'une action linéaire de G (i.e. on demande que $x \mapsto g \cdot x$ soit une application linéaire de V dans V, pour tout $g \in \mathrm{G}$). Il arrive souvent que G et V soient munis de topologies, et on demande alors, en général, que $(g, x) \mapsto g \cdot x$ soit continue de $\mathrm{G} \times \mathrm{V}$ dans V.

Les représentations de groupes interviennent de multiples façons en mathématique, en physique, ou en chimie. Par exemple, une des motivations initiales de la théorie des représentations des groupes finis, dont il sera question dans ce chapitre, est venue de la cristallographie. La physique des particules utilise grandement les représentations des groupes de Lie comme le groupe $\mathbf{SU}(2)$ des isométries de déterminant 1 de $\mathbf{C}^2$ (muni du produit scalaire usuel $\langle (x_1, x_2), (y_1, y_2) \rangle = \overline{x_1}\, y_1 + \overline{x_2}\, y_2$), ou le groupe d'Heisenberg des matrices 3×3 unipotentes supérieures (i.e. triangulaires supérieures avec des 1 sur la diagonale), à coefficients réels, ou encore ceux de Lorentz (i.e. $\mathbf{O}(1, 3)$) et Poincaré.

Si G est un groupe, la connaissance des représentations de G fournit des tas d'informations sur G, et certains groupes ne sont accessibles qu'à travers leurs représentations. Par exemple, l'existence du *monstre*, le plus grand des groupes finis simples sporadiques [(1)], de cardinal

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71,$$

1. Un groupe G est *simple* si ses seuls sous-groupes distingués sont $\{1\}$ et G. Si un groupe fini n'est pas simple, il possède un sous-groupe distingué non trivial H, et H et G/H sont deux groupes plus petits que G à partir desquels G est construit. En réitérant ce procédé, cela permet de casser n'importe quel groupe fini en une famille finie de groupes simples. La classification des groupes finis se ramène donc à celle des groupes finis simples, et à comprendre comment on peut composer ces groupes simples pour fabriquer des groupes plus gros. La classification des groupes finis simples s'est achevée au début des années 1980 (elle court sur quelques milliers de pages, et personne n'en maîtrise vraiment la totalité...). Il y a un certain nombre de familles infinies comme les $\mathbf{Z}/p\mathbf{Z}$, pour p premier, les groupes alternés A_n, pour $n \geqslant 5$, les quotients de $\mathbf{SL}_n(\mathbf{F}_q)$ par leur centre ($\mathbf{F}_q$ est le corps à q élément), et quelques autres découvertes par C. Chevalley en 1954. A côté de ces familles, il y a 26 groupes isolés, dits sporadiques.

n'a été démontrée en 1982, par R. Griess, que grâce à la construction d'une de ses représentations [2] (de dimension 196883), alors que l'existence du monstre avait été prédite en 1973 par R. Griess et B. Fischer (il y a une ressemblance certaine avec la chasse aux particules élémentaires).

De même, on n'a de prise sur $\mathscr{G}_{\mathbf{Q}}$, groupe des automorphismes du corps $\overline{\mathbf{Q}}$ des nombres algébriques (cf. annexe G), qu'à travers ses représentations. Celles-ci fournissent de précieuses informations sur $\overline{\mathbf{Q}}$, et permettent de résoudre des problèmes classiques de théorie des nombres. Par exemple, la démonstration du théorème de Fermat par A. Wiles (1994) consiste à relier, de manière à en tirer une contradiction, deux types de représentations de $\mathscr{G}_{\mathbf{Q}}$: d'une part celles provenant des solutions (dans $\overline{\mathbf{Q}}$) de l'équation $y^2 = x(x - a^p)(x + b^p)$, où $a^p + b^p = c^p$ est un contrexemple potentiel au théorème de Fermat, et d'autre part, des représentations provenant des formes modulaires.

L'exemple de $\mathscr{G}_{\mathbf{Q}}$ agissant sur $\overline{\mathbf{Q}}$ est en fait assez typique. Si on a un ensemble X sur lequel un groupe G agit, et si on connaît bien les représentations de G, alors on peut espérer en tirer des informations fines sur X. Ce *principe de symétrie* joue un grand rôle dans une partie non négligeable de la physique théorique moderne.

La théorie des représentations présente deux aspects. Le premier de ces aspects (décomposition d'une représentation en représentations irréductibles) est une généralisation de la réduction des endomorphismes (valeurs propres, espaces propres, diagonalisation), qui correspond, modulo un petit exercice de traduction (ex. I.1.2 et I.2.3, rem. I.2.4), au cas du groupe $\mathbf{Z}$. Le second aspect (théorie des caractères) est une première approche de l'analyse de Fourier dans un cadre non commutatif (ou commutatif, cf. alinéa 5.1 du n° I.2). A part le cas de $\mathbf{Z}$ qui permet de faire le lien avec l'algèbre linéaire classique, nous ne considérerons essentiellement que les représentations complexes des groupes finis dans ce cours. Ce cas présente l'avantage d'être à la fois simple (il n'y a pas à se battre avec les problèmes de convergence ou autres subtilités analytiques que l'on rencontre, par

2. C'est la plus petite des représentations non triviales du monstre ; le début de la liste des dimensions des représentations irréductibles du monstre est le suivant :

$$f_1 = 1,\ f_2 = 196883,\ f_3 = 21296876,\ f_4 = 842609326,\ f_5 = 18538750076,\ f_6 = 19360062527, \ldots$$

J. McKay a remarqué en 1977, que 196883 avait un rapport avec les coefficients de Fourier de la fonction modulaire j de l'ex. VII.6.10 : si on écrit $j(z)$ sous la forme $j(z) = \frac{1}{q} + 744 + \sum_{n \geqslant 1} c_n q^n$, avec $q = e^{2i\pi z}$, alors $c_1 = f_2 + f_1$, $c_2 = f_3 + f_2 + f_1$, $c_3 = f_4 + f_3 + 2f_2 + 2f_1$... Vu la taille des nombres en présence, il y avait peu de chance que ceci soit une coïncidence fortuite. Ce mystère, connu sous le nom de "monster's moonshine", a été résolu par R. Borcherds en 1992, en utilisant des objets venant de la physique mathématique, ce qui lui a valu la médaille Fields (1998). L'expression "monster's moonshine" est moins poétique que ce qu'elle suggère, car "moonshine" doit être pris dans le sens de "bêtise, faribole", comme dans la citation suivante de E. Rutherford : « The energy produced by the breaking down of the atom is a very poor kind of thing. Anyone who expects a source of power from the transformations of these atoms is talking moonshine. ».

exemple, dans l'étude des séries de Fourier qui correspondent au groupe $\mathbf{R}/\mathbf{Z}$), et tout à fait représentatif du genre d'énoncés que l'on peut espérer dans d'autres situations.

I.1. Représentations et caractères

1. Représentations de groupes, exemples

Le lecteur est renvoyé au Vocabulaire, n° 2.11.1, § 3 et n° 10.1, pour le vocabulaire et les résultats de base d'algèbre linéaire et de théorie des groupes.

Soit G un groupe, de loi de groupe $(g, h) \mapsto gh$. Une *représentation* V de G est un $\mathbf{C}$-espace vectoriel muni d'une action (à gauche) de G agissant de manière linéaire. Une telle représentation est équivalente à la donnée d'un morphisme de groupes ρ_{V} de G dans GL(V) : si $g \in \mathrm{G}$, l'application $v \mapsto g \cdot v$ est linéaire bijective et donc nous définit un élément $\rho_{\mathrm{V}}(g)$ de GL(V), et l'identité $g \cdot (h \cdot v) = gh \cdot v$, valable quels que soient $g, h \in \mathrm{G}$ et $v \in \mathrm{V}$, se traduit par l'identité $\rho_{\mathrm{V}}(gh) = \rho_{\mathrm{V}}(g)\rho_{\mathrm{V}}(h)$. Dans la suite on parlera indifféremment de la représentation V de G ou de la représentation ρ_{V} de G, suivant qu'on veut mettre l'accent sur l'espace vectoriel de la représentation ou sur le morphisme de G dans GL(V). On notera aussi parfois $\rho_{\mathrm{V},g}$ l'élément $\rho_{\mathrm{V}}(g)$ de GL(V), de manière à pouvoir écrire $\rho_{\mathrm{V},g}(v)$ au lieu de $\rho_{\mathrm{V}}(g)(v)$ l'image $g \cdot v$ de $v \in \mathrm{V}$ sous l'action de $g \in \mathrm{G}$.

Remarque I.1.1. — (i) L'exemple le plus banal de représentation est celui d'un sous-groupe G de GL(V) agissant sur V. Par exemple, l'inclusion du groupe orthogonal $\mathbf{O}(d)$ dans $\mathbf{GL}_d(\mathbf{R})$ fait de $\mathbf{R}^d$ une représentation de $\mathbf{O}(d)$.

(ii) Si ρ_{V} est injectif, on dit que V est une représentation *fidèle* de G, auquel cas ρ_{V} permet de représenter le groupe abstrait G, de manière concrète (d'où la terminologie), comme un sous-groupe de GL(V). Si V est dimension finie, le choix d'une base fournit une représentation encore plus concrète comme groupe de matrices.

Exemple I.1.2. — (Représentations de $\mathbf{Z}$)

(i) Si $\lambda \in \mathbf{C}^*$, alors $n \mapsto \lambda^n$ est un morphisme de groupes de $\mathbf{Z}$ dans $\mathbf{C}^*$, ce qui nous fabrique une représentation de $\mathbf{Z}$ que nous noterons $\mathbf{C}(\lambda)$; l'action de $n \in \mathbf{Z}$ sur $z \in \mathbf{C}$ étant donnée par $\rho_{\mathbf{C}(\lambda),n}(z) = \lambda^n z$ (ce qu'on peut aussi écrire sous la forme $n \cdot z = \lambda^n z$).

(ii) Si V est un $\mathbf{C}$-espace vectoriel, et si $u : \mathrm{V} \to \mathrm{V}$ est un isomorphisme linéaire, l'application $n \mapsto u^n$ est un morphisme de groupes de $\mathbf{Z}$ dans GL(V), ce qui fait de V une représentation du groupe additif $\mathbf{Z}$, l'action de $n \in \mathbf{Z}$ sur $v \in \mathrm{V}$ étant donnée par $n \cdot v = u^n(v)$. Réciproquement, si V est une représentation de $\mathbf{Z}$, alors $u = \rho_{\mathrm{V}}(1) \in \mathrm{GL}(\mathrm{V})$, et on a $\rho_{\mathrm{V}}(n) = u^n$ pour tout $n \in \mathbf{Z}$, et donc $n \cdot v = u^n(v)$, si $n \in \mathbf{Z}$ et $v \in \mathrm{V}$. En d'autres termes, une représentation de $\mathbf{Z}$ n'est rien d'autre que la donnée d'un $\mathbf{C}$-espace vectoriel V et d'un élément u de GL(V).

Exemple I.1.3. — (Représentations de $\mathbf{Z}/\mathrm{D}\mathbf{Z}$) Si V est un $\mathbf{C}$-espace vectoriel muni d'un isomorphisme linéaire u vérifiant $u^{\mathrm{D}} = 1$, l'application $n \mapsto u^n$ est un morphisme de

groupes de $\mathbf{Z}$ dans GL(V) dont le noyau contient $D\mathbf{Z}$; il induit donc un morphisme de $\mathbf{Z}/D\mathbf{Z}$ dans GL(V), ce qui fait de V une représentation de $\mathbf{Z}/D\mathbf{Z}$, l'action de $n \in \mathbf{Z}$ sur $v \in V$ étant donnée par $n \cdot v = u^n(v)$. Réciproquement, si V est une représentation de $\mathbf{Z}/D\mathbf{Z}$, et si $u = \rho_V(1) \in GL(V)$, alors $u^D = \rho_V(D) = \rho_V(0) = 1$, car $D = 0$ dans $\mathbf{Z}/D\mathbf{Z}$. En d'autres termes, une représentation de $\mathbf{Z}/D\mathbf{Z}$ n'est rien d'autre que la donnée d'un $\mathbf{C}$-espace vectoriel V et d'un élément u de GL(V) vérifiant $u^D = 1$.

Remarque I.1.4. — Dans les deux cas ci-dessus, on dispose d'une présentation du groupe à partir de générateurs (dans les deux cas G est engendré par 1) et de relations entre les générateurs (pas de relation dans le cas de $\mathbf{Z}$, une relation $D = 0$ pour $\mathbf{Z}/D\mathbf{Z}$). Ceci permet de décrire une représentation de G en disant ce que fait chaque générateur, les relations entre les générateurs imposant des relations entre leurs actions. Ce type de description est très efficace quand on dispose d'une présentation relativement simple du groupe G.

Par exemple, le groupe $\mathbf{Z}^2$ est engendré par $e_1 = (1, 0)$ et $e_2 = (0, 1)$, et est décrit par la relation de commutation $e_1 + e_2 = e_2 + e_1$. Une représentation de $\mathbf{Z}^2$ est donc la donnée d'un $\mathbf{C}$-espace vectoriel V et de deux éléments de GL(V) commutant entre eux.

Le groupe $\mathbf{SL}_2(\mathbf{Z})$ est engendré par les matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, et toute relation entre S et T est conséquence des relations $S^4 = I$, $S^2T = TS^2$ et $(ST)^3 = S^2$; une représentation de $\mathbf{SL}_2(\mathbf{Z})$ est donc la donnée d'un $\mathbf{C}$-espace vectoriel V et de deux éléments u et v de GL(V) vérifiant $u^4 = 1$, $u^2v = vu^2$ et $(uv)^3 = u^2$.

De même, l'exercice ci-dessous montre qu'une représentation du groupe S_3 des permutations de $\{1, 2, 3\}$ est juste un $\mathbf{C}$-espace vectoriel V muni de deux symétries s_1, s_2 vérifiant $s_1s_2s_1 = s_2s_1s_2$.

Exercice I.1.5. — Soient $\sigma_1, \sigma_2 \in S_3$ les permutations $(1, 2)$ et $(2, 3)$.

(i) Vérifier que $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ est la permutation $(1, 3)$.

(ii) Montrer que σ_1 et σ_2 engendrent S_3.

(iii) Montrer que toute relation entre σ_1 et σ_2 dans S_3 est conséquence des relations $\sigma_1^2 = \sigma_2^2 = 1$ et $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. (On montrera qu'une relation de longueur $n \geqslant 4$ peut toujours se ramener à une relation de longueur $n - 2$.)

La *dimension* $\dim V$ d'une représentation V est juste la dimension du $\mathbf{C}$-espace vectoriel V. Par exemple, $\dim \mathbf{C}(\lambda) = 1$, pour tout $\lambda \in \mathbf{C}^*$.

Dans tout ce qui suit, les représentations sont implicitement supposées de dimension finie. Si $\dim V = d$ et si $(e_1, \ldots, e_d)$ est une base de V, on note $R_V(g)$ ou $R_{V,g}$ la matrice de $\rho_V(g)$ dans la base $(e_1, \ldots, e_d)$ (qui dépend du choix de la base bien que ça n'apparaisse pas dans la notation). Alors $R_V : G \to \mathbf{GL}_d(\mathbf{C})$ est un morphisme de groupes.

Exemple I.1.6. — (Construction d'une représentation de dimension 2 de S_3)

Soient $A = (1, 0)$, $B = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$ et $C = (-\frac{1}{2}, -\frac{\sqrt{3}}{2})$. Les points A, B, C sont les sommets d'un triangle équilatéral de centre de gravité $O = (0, 0)$. Les isométries du plan laissant stable ce triangle fixent O et

donc sont linéaires ; elles forment donc un sous-groupe [3] D_3 de $\mathbf{O}(2) \subset \mathbf{GL}_2(\mathbf{C})$. L'injection de D_3 dans $\mathbf{GL}_2(\mathbf{C})$ fait de $\mathbf{C}^2$ une représentation du groupe D_3, et nous allons montrer que ce groupe est isomorphe à S_3 pour construire notre représentation de S_3. Un élément de D_3 laisse stable l'ensemble $\{A, B, C\}$, et fournit un morphisme de groupes f de D_3 dans le groupe des permutations $S_{\{A,B,C\}}$ de $\{A, B, C\}$. Comme A, B et C ne sont pas alignés, un élément de D_3 est uniquement déterminé par les images de A, B et C, ce qui signifie que f est injectif. Par ailleurs, f est surjectif car D_3 contient les symétries par rapport aux droites (OA), (OB) et (OC) qui s'envoient respectivement sur les transpositions (B, C), (A, C) et (A, B), et les rotations d'angles 0, $\frac{2\pi}{3}$ et $\frac{-2\pi}{3}$ dont les images respectives sont l'identité et les cycles (A, B, C) et (A, C, B). En résumé, $f : D_3 \to S_{\{A,B,C\}}$ est un isomorphisme de groupes. La bijection $1 \mapsto A$, $2 \mapsto B$, $3 \mapsto C$ de $\{1, 2, 3\}$ sur $\{A, B, C\}$ fournit un isomorphisme $g : S_3 \cong S_{\{A,B,C\}}$. On obtient un morphisme de groupes de S_3 dans $\mathbf{GL}_2(\mathbf{C})$ en composant $f^{-1} \circ g : S_3 \to D_3$ avec l'injection de D_3 dans $\mathbf{GL}_2(\mathbf{C})$. Ce morphisme fait de $\mathbf{C}^2$ une représentation de S_3.

Remarque I.1.7. — Soit G un groupe fini ; tout élément de G est alors d'ordre fini. Soit V une représentation de G. Si $g \in G$ est d'ordre n, on a $\rho_V(g)^n = \rho_V(g^n) = 1$. Comme le polynôme $X^n - 1$ n'a que des racines simples, cela prouve que $\rho_V(g)$ est diagonalisable, et comme les valeurs propres de $\rho_V(g)$ sont des racines de $X^n - 1$, ce sont des racines de l'unité.

Exercice I.1.8. — (i) Soit $V = \mathbf{C}^2$ la représentation de S_3 construite à l'exemple I.1.6. Montrer qu'il n'existe pas de base de V dans laquelle les matrices des actions de tous les éléments de S_3 sont simultanément diagonales.

(ii) Soient V un espace vectoriel de dimension finie sur $\mathbf{C}$, et u_1, u_2 deux endomorphismes diagonalisables de V commutant l'un à l'autre. Montrer que tout espace propre de u_1 est stable par u_2. En déduire qu'il existe une base de V dans laquelle les matrices de u_1 et u_2 sont toutes les deux diagonales.

(iii) Soit G un groupe commutatif fini, et soit V une représentation de G. Montrer qu'il existe une base de V dans laquelle les matrices $R_V(g)$, pour $g \in G$, sont toutes diagonales. En déduire qu'il existe une décomposition de V en somme directe de droites stables par l'action de G.

2. Caractère d'une représentation, exemples

Le *caractère* χ_V de V est l'application de G dans $\mathbf{C}$ définie par $\chi_V(g) = \mathrm{Tr}(\rho_V(g))$, où $\mathrm{Tr}(\rho_V(g))$ désigne la trace de l'endomorphisme $\rho_V(g)$; c'est aussi la trace de la matrice $R_V(g)$ dans n'importe quelle base de V, et c'est aussi la somme des valeurs propres de $\rho_V(g)$ comptées avec multiplicité.

On a en particulier $\chi_V(1) = \mathrm{Tr}(1) = \dim V$; la valeur de χ_V en l'élément neutre est donc un entier ; cet entier est appelé le *degré* du caractère χ_V ; d'après ce qui précède, c'est aussi la dimension de la représentation V ; cette observation est d'usage constant. De plus, comme $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, si A et B sont deux éléments de $\mathbf{M}_d(\mathbf{C})$, on a

$$\mathrm{Tr}(\rho_V(hgh^{-1})) = \mathrm{Tr}(\rho_V(h)\rho_V(g)\rho_V(h)^{-1}) = \mathrm{Tr}(\rho_V(g)),$$

ce qui montre que χ_V est une *fonction centrale* sur G (i.e. χ_V est constante sur chacune des classes de conjugaison de G : on a $\chi_V(hgh^{-1}) = \chi_V(g)$ quels que soient $h, g \in G$).

3. Plus généralement, on note D_n le groupe des isométries du plan fixant un polygone régulier à n côtés.

Remarque I.1.9. — Si G est fini, et si $g \in \mathrm{G}$, les valeurs propres de $\rho_{\mathrm{V}}(g)$ sont des racines de l'unité. En particulier, elles sont de module 1, et donc $\lambda^{-1} = \overline{\lambda}$, si λ est une valeur propre de $\rho_{\mathrm{V}}(g)$. Comme les valeurs propres de $\rho_{\mathrm{V}}(g^{-1}) = \rho_{\mathrm{V}}(g)^{-1}$ sont les inverses de celles de $\rho_{\mathrm{V}}(g)$, et comme la trace est la somme des valeurs propres, on en déduit que $\chi_{\mathrm{V}}(g^{-1}) = \overline{\chi_{\mathrm{V}}(g)}$, quel que soit $g \in \mathrm{G}$.

2.1. *Caractères linéaires*

Si V est de dimension 1, les endomorphismes de V sont les homothéties, et l'application qui à une homothétie associe son rapport induit un isomorphisme de GL(V) sur $\mathbf{C}^*$. Une représentation de dimension 1 n'est donc rien d'autre qu'un morphisme de groupes $\chi : \mathrm{G} \to \mathbf{C}^*$; un tel morphisme est aussi souvent appelé un *caractère linéaire* de G. On note $\widehat{\mathrm{G}}$ l'ensemble de ces caractères linéaires.

Si V est une représentation de dimension 1 correspondant au caractère linéaire χ, on a $\chi_{\mathrm{V}} = \chi$ de manière évidente. Autrement dit, *le caractère d'un caractère linéaire est le caractère linéaire lui-même.*

La *représentation triviale*, notée **1**, est la représentation de dimension 1 correspondant au *caractère trivial* $\chi : \mathrm{G} \to \mathbf{C}^*$, défini par $\chi(g) = 1$, pour tout $g \in \mathrm{G}$.

Si V est une représentation de G, et si $\chi \in \widehat{\mathrm{G}}$, on note $\mathrm{V}(\chi)$ ou $\mathrm{V} \otimes \chi$ *la tordue de* V *par le caractère linéaire* χ : c'est la représentation définie par $\rho_{\mathrm{V}(\chi)}(g) = \chi(g)\rho_{\mathrm{V}}(g)$ (l'espace vectoriel de $\mathrm{V}(\chi)$ est V, mais l'action est tordue par χ ; la matrice $\mathrm{R}_{\mathrm{V}(\chi)}(g)$ est le produit de $\mathrm{R}_{\mathrm{V}}(g)$ par $\chi(g)$). On a $\chi_{\mathrm{V}(\chi)}(g) = \chi(g)\chi_{\mathrm{V}}(g)$, si $g \in \mathrm{G}$.

Exercice I.1.10. — On définit le produit $\chi_1\chi_2$ de deux caractères linéaires par $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. Montrer que $\widehat{\mathrm{G}}$, muni de ce produit, est un groupe commutatif.

Exercice I.1.11. — (Orthogonalité des caractères linéaires)

(i) Soit G un groupe fini et soit $\chi \in \widehat{\mathrm{G}}$. Montrer que $\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \chi(g)$ vaut 1 si χ est le caractère trivial, et 0 sinon. (Multiplier la somme par $\chi(h)$, pour un $h \in \mathrm{G}$ bien choisi.)

(ii) En déduire que, si $\chi_1, \chi_2 \in \widehat{\mathrm{G}}$, et si $\langle \chi_1, \chi_2 \rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \overline{\chi_1(g)}\chi_2(g)$, alors $\langle \chi_1, \chi_2 \rangle = 1$ si $\chi_1 = \chi_2$, et $\langle \chi_1, \chi_2 \rangle = 0$ si $\chi_1 \neq \chi_2$.

2.2. *Sommes directes*

Si V_1 et V_2 sont deux représentations de G, on peut munir $\mathrm{V}_1 \oplus \mathrm{V}_2$, somme directe des espaces vectoriels V_1 et V_2, d'une action de G. Rappelons que $\mathrm{V}_1 \oplus \mathrm{V}_2$ est un espace vectoriel dont V_1 et V_2 sont des sous-espaces vectoriels qui sont en somme directe dans $\mathrm{V}_1 \oplus \mathrm{V}_2$. Comme on fait la somme directe d'un nombre fini d'espaces, on a une identification naturelle de $\mathrm{V}_1 \oplus \mathrm{V}_2$ avec le produit $\mathrm{V}_1 \times \mathrm{V}_2$, où $v_1 \in \mathrm{V}_1$ s'identifie à $(v_1, 0) \in \mathrm{V}_1 \times \mathrm{V}_2$ et $v_2 \in \mathrm{V}_2$ à $(0, v_2) \in \mathrm{V}_1 \times \mathrm{V}_2$. En utilisant cette identification, l'action de $g \in \mathrm{G}$ sur $(v_1, v_2) \in \mathrm{V}_1 \oplus \mathrm{V}_2$ est donnée par $g \cdot (v_1, v_2) = (g \cdot v_1, g \cdot v_2)$. La représentation de G ainsi obtenue est encore notée $\mathrm{V}_1 \oplus \mathrm{V}_2$, et appelée *somme directe de* V_1 *et* V_2. Si on choisit une base $e_1, \ldots, e_m$ de V_1 et une base $f_1, \ldots, f_n$ de V_2, alors $(e_1, 0), \ldots, (e_m, 0), (0, f_1), \ldots, (0, f_n)$

est une base de V, et la matrice $\mathrm{R_V}(g)$ dans cette base est la matrice diagonale par blocs $\left(\begin{smallmatrix}\mathrm{R_{V_1}}(g) & 0\\ 0 & \mathrm{R_{V_2}}(g)\end{smallmatrix}\right)$, dont la trace est la somme des traces de $\mathrm{R_{V_1}}(g)$ et $\mathrm{R_{V_2}}(g)$. On a donc

$$\chi_{\mathrm{V_1}\oplus\mathrm{V_2}} = \chi_{\mathrm{V_1}} + \chi_{\mathrm{V_2}}.$$

Le cas $\mathrm{V_1} = \mathrm{V_2}$ n'est pas exclu, et $\mathrm{V}\oplus\mathrm{V}$ est une représentation de G contenant deux copies de V d'intersection nulle et dont la somme est tout. Par exemple, la représentation $\mathbf{C}(\lambda)\oplus\mathbf{C}(\lambda)$ de $\mathbf{Z}$ est $\mathbf{C}^2$ muni de l'homothétie λ, les deux copies de $\mathbf{C}(\lambda)$ obtenue en identifiant la somme au produit étant $\mathbf{C}\times\{0\}$ et $\{0\}\times\mathbf{C}$ (il y a beaucoup d'autres copies de $\mathbf{C}(\lambda)$ dans $\mathbf{C}(\lambda)\oplus\mathbf{C}(\lambda)$ puisque toute droite en est une). Plus généralement, si $m\in\mathbf{N}$, on note $m\mathrm{V}$ la somme directe de m copies de V (pour $m=0$, on obtient l'espace vectoriel 0). Si les V_i, pour $i\in\mathrm{I}$ fini, sont des représentations de G, et si $m_i\in\mathbf{N}$, pour tout $i\in\mathrm{I}$, alors $\oplus_{i\in\mathrm{I}} m_i\mathrm{V}_i$ est une représentation de G de caractère

$$\chi_{\oplus_{i\in\mathrm{I}} m_i\mathrm{V}_i} = \sum_{i\in\mathrm{I}} m_i\chi_{\mathrm{V}_i}.$$

2.3. *Représentations de permutation, représentation régulière*

Si X est un ensemble fini muni d'une action (à gauche) de G donnée par $(g,x)\mapsto g\cdot x$, on définit la *représentation de permutation* $\mathrm{V_X}$, associée à X, comme l'espace vectoriel $\mathrm{V_X}$ de dimension $|\mathrm{X}|$, de base $(e_x)_{x\in\mathrm{X}}$, muni de l'action linéaire de G donnée, sur les vecteurs de la base, par $g\cdot e_x = e_{g\cdot x}$. Si $g_1, g_2\in\mathrm{G}$, et si $x\in\mathrm{X}$, on a $g_1\cdot(g_2\cdot e_x) = g_1\cdot e_{g_2\cdot x} = e_{g_1g_2\cdot x} = g_1g_2\cdot e_x$, ce qui prouve que la formule précédente définit bien une action de G sur $\mathrm{V_X}$. Dans la base $(e_x)_{x\in\mathrm{X}}$, la matrice de g est une *matrice de permutation* (i.e. a exactement un 1 par ligne et par colonne, et tous les autres coefficients sont nuls), et le terme diagonal $a_{x,x}$ est égal à 1 si et seulement si $g\cdot x = x$ (i.e. si x est un point fixe de g), sinon, il vaut 0. On en déduit que la trace de la matrice de g est le nombre de points fixes de g agissant sur X. Autrement dit, on a

$$\chi_{\mathrm{V_X}}(g) = |\{x\in\mathrm{X},\ g\cdot x = x\}|.$$

Un cas particulier intéressant est celui où G est fini, $\mathrm{X}=\mathrm{G}$, et l'action de G est donnée par la multiplication à gauche (i.e. $g\cdot h = gh$). La représentation $\mathrm{V_G}$ ainsi obtenue est la *représentation régulière* de G. Comme $gh = h$ implique $g=1$, on voit que le caractère de la représentation régulière est donné par la formule

$$\chi_{\mathrm{V_G}}(1) = |\mathrm{G}|,\quad \text{et}\quad \chi_{\mathrm{V_G}}(g) = 0,\ \text{si } g\in\mathrm{G}-\{1\}.$$

Exercice I.1.12. — Soit G un groupe agissant sur un ensemble fini X. Montrer que si g et g' sont conjugués dans G, ils ont le même nombre de points fixes dans X. Comment ceci se traduit-il en termes du caractère de $\mathrm{V_X}$?

3. Morphismes de représentations

3.1. *La représentation* $\mathrm{Hom}(\mathrm{V_1},\mathrm{V_2})$

Soient $\mathrm{V_1}$ et $\mathrm{V_2}$ deux représentations de G, et soit $u:\mathrm{V_1}\to\mathrm{V_2}$ une application linéaire. Si $g\in\mathrm{G}$, on définit $g\cdot u:\mathrm{V_1}\to\mathrm{V_2}$ par la formule $(g\cdot u)(v) = g\cdot u(g^{-1}\cdot v)$, quel que soit

$v \in \mathrm{V}_1$. Si $g_1, g_2 \in \mathrm{G}$, et si $v \in \mathrm{V}_1$, on a

$$(g_1 \cdot (g_2 \cdot u))(v) = g_1 \cdot \big((g_2 \cdot u)(g_1^{-1} \cdot v)\big)$$
$$= g_1 \cdot \big(g_2 \cdot u(g_2^{-1} \cdot g_1^{-1} \cdot v)\big) = g_1 g_2 \cdot u((g_1 g_2)^{-1} \cdot v) = (g_1 g_2 \cdot u)(v),$$

et donc $g_1 \cdot (g_2 \cdot u) = g_1 g_2 \cdot u$, ce qui prouve que l'on a défini de la sorte une action de G sur l'espace $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$ des applications linéaires de V_1 dans V_2.

Si $g \in \mathrm{G}$, l'endomorphisme $\rho_{\mathrm{Hom}(\mathrm{V}_1,\mathrm{V}_2),g}$ de $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$ est alors donné par la formule :

$$\rho_{\mathrm{Hom}(\mathrm{V}_1,\mathrm{V}_2),g}(u) = \rho_{\mathrm{V}_2,g} \circ u \circ \rho_{\mathrm{V}_1,g}^{-1}, \quad \text{si } u \in \mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2).$$

Proposition I.1.13. — *Si* G *est fini, et si* $g \in \mathrm{G}$*, alors*

$$\chi_{\mathrm{Hom}(\mathrm{V}_1,\mathrm{V}_2)}(g) = \overline{\chi_{\mathrm{V}_1}(g)}\chi_{\mathrm{V}_2}(g).$$

Démonstration. — Si g est fixé, on peut choisir une base $(e_i)_{i\in\mathrm{I}}$ de V_1 et une base $(f_j)_{j\in\mathrm{J}}$ de V_2 dans lesquelles les actions de g sont diagonales. Il existe donc des racines de l'unité α_i, pour $i \in \mathrm{I}$, et β_j, pour $j \in \mathrm{J}$, tels que $g \cdot e_i = \alpha_i e_i$, si $i \in \mathrm{I}$, et $g \cdot f_j = \beta_j f_j$, si $j \in \mathrm{J}$. On a alors $\chi_{\mathrm{V}_1}(g) = \sum_{i\in\mathrm{I}} \alpha_i$ et $\chi_{\mathrm{V}_2}(g) = \sum_{j\in\mathrm{J}} \beta_j$.

Si $(i, j) \in \mathrm{I} \times \mathrm{J}$, soit $u_{i,j} : \mathrm{V}_1 \to \mathrm{V}_2$ l'application linéaire définie par $u_{i,j}(e_i) = f_j$, et $u_{i,j}(e_{i'}) = 0$, si $i' \neq i$. Les $u_{i,j}$, pour $(i, j) \in \mathrm{I} \times \mathrm{J}$ forment une base de $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$, et on a $g \cdot u_{i,j} = \alpha_i^{-1}\beta_j u_{i,j} = \overline{\alpha_i}\beta_j u_{i,j}$. On a donc

$$\chi_{\mathrm{Hom}(\mathrm{V}_1,\mathrm{V}_2)}(g) = \sum_{(i,j)\in\mathrm{I}\times\mathrm{J}} \overline{\alpha_i}\beta_j = \Big(\sum_{i\in\mathrm{I}} \overline{\alpha_i}\Big)\Big(\sum_{j\in\mathrm{J}} \beta_j\Big) = \overline{\chi_{\mathrm{V}_1}(g)}\chi_{\mathrm{V}_2}(g).$$

Ceci permet de conclure.

Remarque I.1.14. — Si $\mathrm{V}_1 = \mathrm{V}$ et si V_2 est la représentation triviale, la représentation $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2) = \mathrm{Hom}(\mathrm{V}, \mathbf{C})$ est la *représentation duale* V^* de V. On a $\chi_{\mathrm{V}^*} = \overline{\chi_{\mathrm{V}}}$, d'après la prop. I.1.13.

3.2. *Opérateurs d'entrelacement, représentations isomorphes*

Notons $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ l'ensemble des applications linéaires de V_1 dans V_2 commutant à l'action de G. C'est un sous-espace vectoriel de $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$ et un élément u de $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$ est dans $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$, si et seulement si on a $g \cdot u(v) = u(g \cdot v)$, quel que soit $v \in \mathrm{V}_1$. Appliqué à $g^{-1} \cdot v$, ceci peut aussi se réécrire sous la forme $g \cdot u(g^{-1} \cdot v) = u(v)$, quel que soit $v \in \mathrm{V}_1$, ou encore, sous la forme $g \cdot u = u$. Autrement dit, $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ est le sous-espace vectoriel de $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$ des éléments fixes sous l'action de G. Les éléments de $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ sont souvent appelés des *opérateurs d'entrelacement.*

Exemple I.1.15. — Si V est une représentation de G, l'ensemble V^{G} des éléments de V fixes sous l'action de G est un sous-espace vectoriel de V (c'est l'intersection des noyaux des $g - 1$, pour $g \in \mathrm{G}$) qui est stable sous l'action de G, et sur lequel G agit trivialement par construction ; c'est donc une représentation de G. Maintenant, si G est fini, on peut

considérer *l'opérateur de moyenne* $\mathrm{M} : \mathrm{V} \to \mathrm{V}$ défini par $\mathrm{M}(v) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g\cdot v$. Alors M est un opérateur d'entrelacement entre V et V^{G}. En effet, si $h \in \mathrm{G}$, et si $v \in \mathrm{V}$, on a

$$h\cdot \mathrm{M}(v) = h\cdot\Big(\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g\cdot v\Big) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} h\cdot(g\cdot v) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} hg\cdot v$$

$$\mathrm{M}(h\cdot v) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g\cdot(h\cdot v) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} gh\cdot v$$

et comme $g \mapsto hg$ et $g \mapsto gh$ sont des bijections de G dans G, les deux quantités sont égales à $\mathrm{M}(v)$. Cela prouve à la fois que $\mathrm{M}(v) \in \mathrm{V}^{\mathrm{G}}$ et que $\mathrm{M} : \mathrm{V} \to \mathrm{V}^{\mathrm{G}}$ commute à l'action de G.

Remarque I.1.16. — L'idée, selon laquelle *il suffit de faire la moyenne sous l'action du groupe pour obtenir quelque chose de fixe par tout le groupe*, joue un rôle très important dans la théorie.

On dit que deux représentations V_1 et V_2 de G sont *isomorphes*, s'il existe un isomorphisme linéaire $u : \mathrm{V}_1 \to \mathrm{V}_2$ commutant à l'action de G, (autrement dit, s'il existe $u \in \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ bijectif, ce qui implique, en particulier, que V_1 et V_2 ont la même dimension). Traduit en termes des morphismes $\rho_{\mathrm{V}_1} : \mathrm{G} \to \mathrm{GL}(\mathrm{V}_1)$ et $\rho_{\mathrm{V}_2} : \mathrm{G} \to \mathrm{GL}(\mathrm{V}_2)$ attachés à V_1 et V_2, cette relation devient $u \circ \rho_{\mathrm{V}_1}(g) = \rho_{\mathrm{V}_2}(g) \circ u$, quel que soit $g \in \mathrm{G}$. Traduit en termes matriciels (après avoir choisi des bases de V_1 et V_2), cela se traduit par l'existence de $\mathrm{T} \in \mathbf{GL}_d(\mathbf{C})$, tel que $\mathrm{T}\,\mathrm{R}_{\mathrm{V}_1}(g) = \mathrm{R}_{\mathrm{V}_2}(g)\,\mathrm{T}$, quel que soit $g \in \mathrm{G}$, ce qui peut encore se mettre sous la forme $\mathrm{R}_{\mathrm{V}_2}(g) = \mathrm{T}\,\mathrm{R}_{\mathrm{V}_1}(g)\,\mathrm{T}^{-1}$. En particulier, $\chi_{\mathrm{V}_1}(g) = \chi_{\mathrm{V}_2}(g)$ quel que soit $g \in \mathrm{G}$.

Exercice I.1.17. — Exhiber deux représentations de $\mathbf{Z}/2\mathbf{Z}$ de même dimension, mais qui ne sont pas isomorphes.

Remarque I.1.18. — (i) On verra plus loin que, si G est fini, la réciproque est vraie : si V_1 et V_2 ont mêmes caractères, alors elles sont isomorphes, ce qui peut sembler un peu surprenant, le caractère ne permettant, a priori, que de calculer la trace des endomorphismes. L'exercice I.1.19 ci-dessous rend le résultat un peu plus envisageable.

(ii) Dans le cas de $\mathbf{Z}$, en notant R_i, pour $i = 1, 2$, la matrice de $\rho_{\mathrm{V}_i}(1)$, on voit que V_1 et V_2 sont isomorphes si et seulement s'il existe T inversible telle que $\mathrm{R}_2 = \mathrm{T}\mathrm{R}_1\mathrm{T}^{-1}$ (i.e. si et seulement si R_2 et R_1 sont des matrices semblables). Il en résulte que la classification des représentations de $\mathbf{Z}$ à isomorphisme près est équivalente à celle des matrices à similitude près, ce qui se fait en utilisant la forme de Jordan. Si on impose à $\mathrm{R} = \mathrm{R}_{\mathrm{V}}(1)$ d'être diagonalisable, alors V est donnée, à isomorphisme près, par les valeurs propres de R avec leurs multiplicités.

Exercice I.1.19. — Soit V une représentation d'un groupe fini G. Si $g \in \mathrm{G}$, soit $\mathrm{P}_g(\mathrm{T}) = \det(1 - \mathrm{T}\rho_{\mathrm{V}}(g))$. Montrer que l'on a l'identité des séries formelles $-\sum_{n=0}^{+\infty} \chi_{\mathrm{V}}(g^{n+1})\mathrm{T}^n = \frac{\mathrm{P}'_g(\mathrm{T})}{\mathrm{P}_g(\mathrm{T})}$. En déduire que χ_{V} permet de déterminer $\rho_{\mathrm{V}}(g)$, pour tout $g \in \mathrm{G}$, à conjugaison près par un élément de $\mathrm{GL}(\mathrm{V})$.

I.2. Décomposition des représentations

Quand on essaye de classifier les objets d'un certain type (par exemple les groupes finis, les représentations d'un groupe fini...), on est amené à comprendre quels sont les objets que l'on ne peut pas casser en morceaux (les groupes simples, si on s'intéresse aux groupes, les représentations irréductibles dans le cas des représentations d'un groupe fini...), et comment on peut assembler les morceaux pour décrire tous les objets qui nous intéressent. Dans le cas des représentations d'un groupe fini, le th. de Maschke (th. I.2.7) montre que cette seconde étape ne pose aucun problème ; le cor. I.2.16, quant à lui, montre que faire la liste des objets irréductibles n'est pas une entreprise vouée à l'échec.

1. Décomposition en somme directe de représentations irréductibles

Soient G un groupe et V une représentation de G. Une *sous-représentation* de V est un sous-espace vectoriel de V stable par G. Par exemple, si $v \in \mathrm{V} - \{0\}$, le sous-espace vectoriel de V engendré par les $g \cdot v$, pour $g \in \mathrm{G}$, est une sous-représentation de V ; c'est la sous-représentation de V *engendrée par* v (i.e. la plus petite sous-représentation de V contenant v). On dit que V est *irréductible* si V ne possède pas de sous-représentation autre que 0 ou V. De manière équivalente, V est irréductible si, quel que soit $v \in \mathrm{V} - \{0\}$, le sous-espace vectoriel de V engendré par les $g \cdot v$, pour $g \in \mathrm{G}$, est égal à V.

Exemple I.2.1. — La représentation de S_3 sur $\mathbf{C}^2$ de l'ex. I.1.6 est irréductible. En effet, comme elle est de dimension 2, une sous-représentation autre que 0 ou $\mathbf{C}^2$ serait une droite de $\mathbf{C}^2$. Une telle droite serait en particulier stable par les symétries orthogonales s_{OA} et s_{OB} par rapport aux droites (OA) et (OB), ce qui est impossible vu que les droites stables par s_{OA} sont les axes de coordonnées, et que ces axes ne sont pas stables par s_{OB}.

Exercice I.2.2. — Soient S_3 le groupe des permutations de l'ensemble $\{1, 2, 3\}$ et s et t les éléments (12) et (123) de S_3.

(i) Soient s et t les éléments (12) et (123) de S_3. Vérifier (ou admettre) que s et t engendrent S_3 et que $sts^{-1} = t^2$, et déterminer les classes de conjugaison de S_3.

(ii) Soit V une représentation de dimension finie de S_3, et soient W_0, W_1 et W_2 les espaces propres de t (i.e. de $\rho_{\mathrm{V}}(t)$) pour les valeurs propres 1, $j = e^{2i\pi/3}$ et j^2. Montrer que $\mathrm{V} = \mathrm{W}_0 \oplus \mathrm{W}_1 \oplus \mathrm{W}_2$.

(iii) Montrer que W_0 est stable par s, et que s échange W_1 etW_2.

(iv) Montrer que, si $v \in \mathrm{W}_1 - \{0\}$, alors le sous-espace de V engendré par v et $s \cdot v$ est stable par S_3, est irréductible comme représentation de S_3, et que la représentation ainsi obtenue ne dépend pas (à isomorphisme près) du choix de v.

(v) En déduire une décomposition de V en somme de représentations irréductibles de S_3 et la liste des représentations irréductibles de S_3.

Exemple I.2.3. — Soit V une représentation de $\mathbf{Z}$, et soit $u = \rho_{\mathrm{V}}(1)$. Comme $\mathbf{C}$ est algébriquement clos, u admet une valeur propre λ, non nulle car u est inversible. Soit $e_\lambda \in \mathrm{V}$ un vecteur propre pour la valeur propre λ. On a alors $n \cdot e_\lambda = u^n(e_\lambda) = \lambda^n e_\lambda$ pour tout $n \in \mathbf{Z}$, ce qui prouve que la droite $\mathbf{C}e_\lambda$ est stable sous l'action de $\mathbf{Z}$ et est une sous-représentation de $\mathbf{Z}$ isomorphe à la représentation $\mathbf{C}(\lambda)$ de l'ex. I.1.2. En particulier,

si V est de dimension $\geqslant 2$, alors V n'est pas irréductible, et donc toute représentation irréductible de $\mathbf{Z}$ est de dimension 1, isomorphe à $\mathbf{C}(\lambda)$, pour un $\lambda \in \mathbf{C}^*$ uniquement déterminé.

Supposons maintenant que u est diagonalisable. Soit $v_1, \ldots, v_d$ une base de V constituée de vecteurs propres de u, et soit λ_i la valeur propre associée à e_i. Alors V est la somme directe $\oplus_{i=1}^d \mathbf{C}e_i$ des droites $\mathbf{C}e_i$ qui sont des sous-représentations de V, chaque $\mathbf{C}e_i$ étant isomorphe à $\mathbf{C}(\lambda_i)$ en tant que représentation de $\mathbf{Z}$. On en déduit que V est, en tant que représentation de $\mathbf{Z}$, isomorphe à $\oplus_{i=1}^d \mathbf{C}(\lambda_i)$.

Remarque I.2.4. — (i) Dire que V est isomorphe à $\oplus_{i=1}^d \mathbf{C}(\lambda_i)$ signifie juste que $u = \rho_{\mathrm{V}}(1)$ est diagonalisable, et que son polynôme caractéristique est $\prod_{i=1}^d (\mathrm{X} - \lambda_i)$, ce qui est nettement moins précis que d'exhiber une base de vecteurs propres, et donc un isomorphisme de $\oplus_{i=1}^d \mathbf{C}(\lambda_i)$ sur V entre représentations de $\mathbf{Z}$.

(ii) Si u est diagonalisable, si les valeurs propres de u sont $\lambda_1, \ldots, \lambda_r$, avec $\lambda_i \neq \lambda_j$ si $i \neq j$, et si la multiplicité de λ_i est m_i, alors $\mathrm{V} \cong \oplus_{i=1}^r m_i \mathbf{C}(\lambda_i)$.

(iii) Si u n'est pas diagonalisable, la représentation V ne se décompose pas comme une somme directe de représentations irréductibles.

Exercice I.2.5. — Soit η un caractère linéaire de G. Montrer que, pour toute représentation irréductible V de G, la représentation $\mathrm{V} \otimes \eta$ est encore irréductible.

Nous allons prouver que, *si* G *est fini*, toute représentation de G est somme directe de représentations irréductibles. Cela revient, en choisissant une base de chacune de ces représentations irréductibles, à exhiber une base de V dans laquelle les $\rho_{\mathrm{V}}(g)$, pour $g \in \mathrm{G}$, se mettent simultanément sous une forme diagonale par blocs [4], la taille des blocs étant la plus petite possible. (C'est un peu analogue à la forme minimale d'une matrice de rotation dans $\mathbf{R}^n$.) Nous aurons besoin du résultat suivant.

Théorème I.2.6. — *Soit* V *une représentation de* G*. Il existe sur* V *un produit scalaire* $\langle\ ,\ \rangle_{\mathrm{V}}$ *invariant sous l'action de* G*.*

Démonstration. — Partons d'un produit scalaire quelconque $\langle\ ,\ \rangle$, et définissons $\langle\ ,\ \rangle_{\mathrm{V}}$ comme la moyenne des transformés de $\langle\ ,\ \rangle$ sous l'action de G. Autrement dit,

$$\langle v_1, v_2 \rangle_{\mathrm{V}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \langle g \cdot v_1, g \cdot v_2 \rangle.$$

4. C'est assez particulier aux représentations des groupes finis sur un corps de caractéristique 0. Même dans le cas des groupes finis, si on considère des représentations sur un corps de caractéristique > 0, le mieux que l'on puisse espérer est une mise sous forme triangulaire supérieure par blocs. Par exemple, si V est la représentation de dimension 2 de $\mathrm{G} = \mathbf{Z}/p\mathbf{Z}$ sur le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, la matrice de $n \in \mathbf{Z}$ dans une base (e_1, e_2) étant $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, alors le sous-espace V_1, engendré par e_1, est stable (et même fixe) par G, mais il est facile de voir que c'est le seul sous-espace propre de V ayant cette propriété. La représentation V n'est donc pas irréductible, mais n'est pas somme directe de représentations irréductibles.

L'action de G étant linéaire, le résultat est bien linéaire par rapport à v_2 et sesquilinéaire par rapport à v_1. De plus, $\langle v, v\rangle_{\mathrm{V}} \geqslant \frac{1}{|\mathrm{G}|}\langle v, v\rangle$, ce qui prouve que $\langle\ ,\ \rangle_{\mathrm{V}}$ est défini positif. Enfin, si $h \in \mathrm{G}$, on a

$$\langle h\cdot v_1, h\cdot v_2\rangle_{\mathrm{V}} = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\langle g\cdot(h\cdot v_1), g\cdot(h\cdot v_2)\rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\langle gh\cdot v_1, gh\cdot v_2\rangle = \langle v_1, v_2\rangle_{\mathrm{V}},$$

car $g \mapsto gh$ induit une bijection de G sur lui-même. Ceci permet de conclure.

Théorème I.2.7. — (Maschke, 1899) *Toute représentation de* G *est somme directe de représentations irréductibles.*

Démonstration. — La démonstration se fait par récurrence sur la dimension. Si V est de dimension 1 ou est irréductible, il n'y a rien à faire. Si V est de dimension $\geqslant 2$ et n'est pas irréductible, alors V possède une sous-représentation V_1 distincte de 0 et V. Si $\langle\ ,\rangle_{\mathrm{V}}$ est un produit scalaire sur V, invariant sous l'action de G, le supplémentaire orthogonal V_2 de V_1 est lui-aussi stable par G puisque que « v orthogonal à V_1 » équivaut à « $g\cdot v$ orthogonal à $g\cdot\mathrm{V}_1 = \mathrm{V}_1$ » par invariance du produit scalaire. On a alors $\mathrm{V} = \mathrm{V}_1 \oplus \mathrm{V}_2$, et V_1 et V_2 sont de dimensions strictement inférieures à celle de V. L'hypothèse de récurrence permet de les décomposer comme des sommes directes de représentations irréductibles, ce qui prouve qu'on peut en faire autant de V.

Remarque I.2.8. — Si G est cyclique engendré par g, la décomposition de V en somme de représentations irréductibles est équivalente à une décomposition de V en droites invariantes sous l'action de g. On sait bien que si g a une valeur propre de multiplicité > 1, cette décomposition n'est pas unique. Par contre, la décomposition en sous-espaces propres est, elle, parfaitement canonique. On verra plus loin (cor. I.2.20) que la situation est la même en ce qui concerne la décomposition en somme de représentations irréductibles d'une représentation d'un groupe fini quelconque.

2. Le lemme de Schur et ses conséquences immédiates

Théorème I.2.9. — (Lemme de Schur, 1905) *Soient* G *un groupe et* $\mathrm{V}_1, \mathrm{V}_2$ *des représentations irréductibles de* G.

(i) *Si* V_1 *et* V_2 *ne sont pas isomorphes, alors* $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2) = 0$.

(ii) *Si* $\mathrm{V}_1 = \mathrm{V}_2$, *alors* $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ *est la droite des homothéties.*

Démonstration. — Soit $u \in \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$. Le fait que u commute à l'action de G, montre que $\mathrm{Ker}(u) \subset \mathrm{V}_1$ et $\mathrm{Im}(u) \subset \mathrm{V}_2$ sont stables par G. Comme par hypothèse, V_1 et V_2 sont irréductibles, on a soit $\mathrm{Ker}(u) = \mathrm{V}_1$, auquel cas $u = 0$, soit $\mathrm{Ker}(u) = 0$, auquel cas $\mathrm{Im}(u) \neq 0$ et donc $\mathrm{Im}(u) = \mathrm{V}_2$. On en déduit que, si $u \neq 0$, alors u est à la fois injective (puisque $\mathrm{Ker}(u) = 0$) et surjective, et donc est un isomorphisme. Cela démontre le (i).

Passons au (ii). Comme on travaille avec des $\mathbf{C}$-espaces vectoriels, u admet une valeur propre λ. Donc $u - \lambda$, qui commute à l'action de G puisque u le fait et qu'une homothétie

commute à tout, a un noyau non nul. Le même raisonnement qu'au (i) montre que ce noyau doit donc être égal à V_1, ce qui se traduit par le fait que u est une homothétie de rapport λ. Ceci permet de conclure.

Remarque I.2.10. — Si V_1 et V_2 sont seulement isomorphes, et si $u : \mathrm{V}_1 \to \mathrm{V}_2$ est un isomorphisme de représentations, on déduit du (ii) du lemme de Schur que tout élément de $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$ est de la forme λu, avec $\lambda \in \mathbf{C}$.

Exercice I.2.11. — Soit G un groupe commutatif. Montrer que toute représentation irréductible de G est de dimension 1.

Proposition I.2.12. — *Soient* G *un groupe fini et* $\mathrm{V}_1, \mathrm{V}_2$ *des représentations de* G.

(i) *Si* V_1 *et* V_2 *sont irréductibles, non isomorphes, et si* $u \in \mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$, *alors* $\mathrm{M}(u) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g \cdot u = 0$.

(ii) *Si* V *est irréductible, et si* $u \in \mathrm{Hom}(\mathrm{V}, \mathrm{V})$, *alors* $\mathrm{M}(u) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g \cdot u$ *est l'homothétie de rapport* $\frac{1}{\dim \mathrm{V}}\mathrm{Tr}(u)$.

(iii) *Si* V *est irréductible, et si* ϕ *est une fonction centrale sur* G, *alors* $\sum_{g\in\mathrm{G}} \phi(g)\rho_{\mathrm{V}}(g)$ *est l'homothétie de rapport* $\frac{1}{\dim \mathrm{V}}\sum_{g\in\mathrm{G}} \phi(g)\chi(g)$.

Démonstration. — Si V_1 et V_2 sont deux représentations de G, si $u \in \mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$, et si $h \in \mathrm{G}$, on a $h \cdot (\sum_{g\in\mathrm{G}} g \cdot u) = \sum_{g\in\mathrm{G}} hg \cdot u$. Comme $g \mapsto hg$ est une bijection de G sur lui-même, cette dernière quantité est aussi égale à $\sum_{g\in\mathrm{G}} g \cdot u$. On en déduit que $\mathrm{M}(u) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g \cdot u$ appartient à $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$.

Le (i) est donc une conséquence du (i) du lemme de Schur. Le (ii) du lemme de Schur montre, quant à lui, que $\mathrm{M}(u)$ est une homothétie, si $u \in \mathrm{Hom}(\mathrm{V}, \mathrm{V})$ et V est irréductible. Pour déterminer le rapport de cette homothétie, il suffit d'en calculer la trace et de diviser par $\dim \mathrm{V}$. Or on a $\mathrm{M}(u) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \rho_{\mathrm{V}}(g)u\rho_{\mathrm{V}}(g)^{-1}$, et donc $\mathrm{M}(u)$ est la moyenne de $|\mathrm{G}|$ termes dont chacun a pour trace $\mathrm{Tr}(u)$, puisque la trace est invariante par conjugaison. On a donc $\mathrm{Tr}(\mathrm{M}(u)) = \mathrm{Tr}(u)$, ce qui permet d'en déduire le (ii).

Enfin, si ϕ est une fonction centrale (i.e., si $\phi(hgh^{-1}) = \phi(g)$ pour tous $h, g \in \mathrm{G}$), si $u_\phi = \sum_{g\in\mathrm{G}} \phi(g)\rho_{\mathrm{V}}(g) \in \mathrm{Hom}(\mathrm{V}, \mathrm{V})$, et si $h \in \mathrm{G}$, on a

$$\begin{aligned} h \cdot u_\phi &= \rho_{\mathrm{V}}(h)\big(\sum_{g\in\mathrm{G}} \phi(g)\rho_{\mathrm{V}}(g)\big)\rho_{\mathrm{V}}(h)^{-1} = \sum_{g\in\mathrm{G}} \phi(g)\rho_{\mathrm{V}}(hgh^{-1}) \\ &= \sum_{g\in\mathrm{G}} \phi(hgh^{-1})\rho_{\mathrm{V}}(hgh^{-1}) = \sum_{g\in\mathrm{G}} \phi(g)\rho_{\mathrm{V}}(g) = u_\phi. \end{aligned}$$

On conclut comme ci-dessus que u_ϕ est l'homothétie de rapport

$$\frac{1}{\dim \mathrm{V}}\mathrm{Tr}(u_\phi) = \frac{1}{\dim \mathrm{V}}\sum_{g\in\mathrm{G}} \phi(g)\mathrm{Tr}(\rho_{\mathrm{V}}(g)) = \frac{1}{\dim \mathrm{V}}\sum_{g\in\mathrm{G}} \phi(g)\chi_{\mathrm{V}}(g),$$

ce qui permet de conclure.

3. Orthogonalité des caractères

Soit G un groupe fini. On note $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$ l'espace vectoriel des fonctions centrales. Cet espace contient l'ensemble $\mathrm{R}^+(\mathrm{G})$ des caractères des représentations de G qui lui-même, contient l'ensemble Irr(G) des *caractères irréductibles* de G (i.e. les caractères des représentations irréductibles de G). Enfin, on note $\mathrm{R}_{\mathbf{Z}}(\mathrm{G})$ le groupe des *caractères virtuels* de G ; c'est le sous-groupe (additif) de $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$ engendré par $\mathrm{R}^+(\mathrm{G})$.

Exercice I.2.13. — Montrer que $\mathrm{R}^+(\mathrm{G})$ est stable par addition et que $\mathrm{R}_{\mathbf{Z}}(\mathrm{G})$ est l'ensemble des $\chi_1 - \chi_2$, avec $\chi_1, \chi_2 \in \mathrm{R}^+(\mathrm{G})$.

On munit $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$ du produit scalaire $\langle\ ,\ \rangle$ défini par

$$\langle \phi_1, \phi_2 \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\phi_1(g)} \phi_2(g).$$

Théorème I.2.14. — (Frobenius, 1897) *Les caractères irréductibles forment une base orthonormale de l'espace des fonctions centrales.*

Démonstration. — Soient χ_1 et χ_2 deux caractères, et soient V_1 et V_2 des représentations de G dont les caractères sont χ_1 etχ_2. En utilisant la prop. I.1.13, on peut réécrire $\langle \chi_1, \chi_2 \rangle$ sous la forme

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi_1(g)} \chi_2(g) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi_{\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)}(g).$$

Comme $\chi_{\mathrm{Hom}(\mathrm{V}_1,\mathrm{V}_2)}(g)$ est, par définition, la trace de g agissant sur $\mathrm{Hom}(\mathrm{V}_1, \mathrm{V}_2)$, cela permet de voir $\langle \chi_1, \chi_2 \rangle$ comme la trace de l'application linéaire $u \mapsto \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} g \cdot u = \mathrm{M}(u)$ définie dans la prop. I.2.12. On déduit alors des (i) et (ii) de cette proposition les faits suivants.

• Si χ_1 et χ_2 sont irréductibles et distincts, alors M est identiquement nul, et donc $\langle \chi_1, \chi_2 \rangle = \mathrm{Tr}(\mathrm{M}) = 0$.

• Si χ est irréductible, et si V est une représentation de caractère χ, alors M est l'application associant à $u \in \mathrm{Hom}(\mathrm{V}, \mathrm{V})$ l'homothétie de rapport $\frac{1}{\dim \mathrm{V}} \mathrm{Tr}(u)$. On en déduit que M admet comme valeurs propres 1 avec multiplicité 1, l'espace propre correspondant étant la droite des homothéties, et 0 avec multiplicité $(\dim \mathrm{V})^2 - 1$, le noyau de M étant l'hyperplan des endomorphismes de trace nulle. La trace de M est donc 1, ce qui se traduit par $\langle \chi, \chi \rangle = 1$.

Il résulte des deux points ci-dessus que les caractères irréductibles forment une famille orthonormale. Il reste à vérifier qu'ils forment une base de $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$, et pour cela, il suffit de vérifier qu'une fonction centrale ϕ, qui est orthogonale à tous les éléments de Irr(G), est nulle. Pour cela, considérons la représentation régulière V_{G} de G, que l'on décompose en somme directe $\mathrm{V}_1 \oplus \cdots \oplus \mathrm{V}_r$ de représentations irréductibles. Si ϕ est une fonction centrale orthogonale à χ_{V_i}, il résulte du (iii) de la prop. I.2.12, que l'endomorphisme $\sum_{g \in \mathrm{G}} \overline{\phi(g)} \rho_{\mathrm{V}_i}(g)$ de V_i est nul. Donc, si ϕ est orthogonale à tous les caractères

irréductibles, l'endomorphisme $\sum_{g\in G}\overline{\phi(g)}\rho_{V_G}(g)$ de V_G est nul. En faisant agir cet endomorphisme sur $e_1 \in V_G$, on en déduit que $0 = \sum_{g\in G}\overline{\phi(g)}g\cdot e_1 = \sum_{g\in G}\overline{\phi(g)}e_g$. Or les e_g, pour $g \in G$, forment une base de V_G ; la nullité de $\sum_{g\in G}\overline{\phi(g)}e_g$ implique donc celle de $\overline{\phi(g)}$, quel que soit $g \in G$, et donc aussi celle de ϕ. Ceci permet de conclure.

Remarque I.2.15. — Si V_1 et V_2 sont irréductibles et non isomorphes, l'application M est identiquement nulle et donc $\mathrm{Tr}(M) = 0$. Or il résulte de la démonstration du th. I.2.14 que $\mathrm{Tr}(M) = \langle\chi_{V_1}, \chi_{V_2}\rangle$. On en déduit en particulier que $\chi_{V_1} \neq \chi_{V_2}$. Autrement dit, l'application $W \mapsto \chi_W$ est une injection de l'ensemble des représentations irréductibles de G (à isomorphisme près) dans Irr(G). Comme, par définition de Irr(G), cette application est surjective, c'est une bijection, ce qui permet de voir Irr(G) aussi comme l'ensemble des représentations irréductibles de G. C'est cette interprétation de Irr(G) qui est utilisée dans la suite.

4. Applications du théorème principal

Le théorème I.2.14 a des tas de conséquences agréables.

4.1. *Nombre des représentations irréductibles*

Corollaire I.2.16. — *Le nombre de représentations irréductibles de* G *est égal au nombre* $|\mathrm{Conj}(G)|$ *de classes de conjugaison dans* G*. En particulier, il est fini.*

Démonstration. — D'après le th. I.2.14, le nombre de représentations irréductibles de G est égal à la dimension de l'espace $R_{\mathbf{C}}(G)$ des fonctions centrales. Or une fonction est centrale si et seulement si elle est constante sur chaque classe de conjugaison ; une fonction centrale ϕ peut donc s'écrire, de manière unique, sous la forme $\phi = \sum_{C\in\mathrm{Conj}(G)}\lambda_C\mathbf{1}_C$, où $\mathbf{1}_C$ est la fonction indicatrice de C, et $\lambda_C \in \mathbf{C}$ (on a $\lambda_C = \phi(g)$, où g est n'importe quel élément de C). Les $\mathbf{1}_C$, pour $C \in \mathrm{Conj}(G)$ forment donc une base de $R_{\mathbf{C}}(G)$ qui, de ce fait, est de dimension $|\mathrm{Conj}(G)|$. Ceci permet de conclure.

Remarque I.2.17. — L'ensemble des représentations irréductibles de G et celui des classes de conjugaison dans G ont le même cardinal mais il n'y a, en général, aucune bijection naturelle entre ces deux ensembles. Les groupes symétriques constituent une exception remarquable (cf. n° C.2).

4.2. *La décomposition canonique d'une représentation*

Le résultat suivant est un peu magique et très utile (par exemple pour décomposer une représentation obtenue par des procédés tensoriels comme au n° 2 du § I.3, ce qui sert beaucoup en physique des particules) ; on peut le voir comme une généralisation du calcul des valeurs propres d'un endomorphisme à partir du polynôme caractéristique. Dans les deux cas, on n'a pas besoin d'exhiber des vecteurs ayant le bon comportement ; on se contente de prouver qu'ils existent.

Corollaire I.2.18. — *Si* V *est une représentation de* G*, si* $\mathrm{V} = \mathrm{W}_1 \oplus \cdots \oplus \mathrm{W}_k$ *est une décomposition de* V *en somme directe de représentations irréductibles, et si* $\mathrm{W} \in \mathrm{Irr}(\mathrm{G})$*, alors le nombre* m_{W} *de* W_i *qui sont isomorphes à* W *est égal à* $\langle \chi_{\mathrm{W}}, \chi_{\mathrm{V}} \rangle$*. En particulier, il ne dépend pas de la décomposition, et* $\mathrm{V} \cong \oplus_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} \langle \chi_{\mathrm{W}}, \chi_{\mathrm{V}} \rangle \mathrm{W}$*.*

Démonstration. — On a $\chi_{\mathrm{V}} = \chi_{\mathrm{W}_1} + \cdots + \chi_{\mathrm{W}_k}$, et donc

$$\langle \chi_{\mathrm{W}}, \chi_{\mathrm{V}} \rangle = \langle \chi_{\mathrm{W}}, \chi_{\mathrm{W}_1} \rangle + \cdots + \langle \chi_{\mathrm{W}}, \chi_{\mathrm{W}_k} \rangle.$$

Or $\langle \chi_{\mathrm{W}}, \chi_{\mathrm{W}_i} \rangle$ est égal à 1 ou 0 suivant que W_i est ou n'est pas isomorphe à W ; on a donc $\langle \chi_{\mathrm{W}}, \chi_{\mathrm{V}} \rangle = m_{\mathrm{W}}$. Ceci permet de conclure.

Corollaire I.2.19. — *Deux représentations* V_1 *et* V_2 *de* G *ayant même caractère* χ *sont isomorphes.*

Démonstration. — Elles sont toutes les deux isomorphes à $\oplus_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} \langle \chi_{\mathrm{W}}, \chi \rangle \mathrm{W}$, d'après le cor. I.2.18.

Corollaire I.2.20. — (Décomposition d'une représentation en composantes isotypiques) *Si* V *est une représentation de* G*, et si* $\mathrm{W} \in \mathrm{Irr}(\mathrm{G})$*, alors*

$$p_{\mathrm{W}} = \frac{\dim \mathrm{W}}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi_{\mathrm{W}}(g)} \rho_{\mathrm{V}}(g),$$

est un projecteur commutant à l'action de G*. De plus, toutes les représentations irréductibles de* G *apparaissant dans la décomposition de* $p_{\mathrm{W}}(\mathrm{V})$ *sont isomorphes à* W*, et* V *est la somme directe des* $p_{\mathrm{W}}(\mathrm{V})$*, pour* $\mathrm{W} \in \mathrm{Irr}(\mathrm{G})$*.*

Démonstration. — Soit $\mathrm{V} = \mathrm{W}_1 \oplus \cdots \oplus \mathrm{W}_k$ une décomposition de V en somme directe de représentations irréductibles. D'après le (iii) de la proposition I.2.12, la restriction de p_{W} à W_i est l'homothétie de rapport

$$\frac{\dim \mathrm{W}}{|\mathrm{G}| \dim \mathrm{W}_i} \sum_{g \in \mathrm{G}} \overline{\chi_{\mathrm{W}}(g)} \chi_{\mathrm{W}_i}(g) = \frac{\dim \mathrm{W}}{\dim \mathrm{W}_i} \langle \chi_{\mathrm{W}}, \chi_{\mathrm{W}_i} \rangle.$$

D'après les relations d'orthogonalité des caractères, cela implique que p_{W} est l'identité sur W_i, si $\mathrm{W}_i \cong \mathrm{W}$, et est nulle dans le cas contraire. Le résultat s'en déduit.

4.3. *Un critère d'irréductibilité*

Corollaire I.2.21. — *Une représentation* V *de* G *est irréductible, si et seulement si* $\langle \chi_{\mathrm{V}}, \chi_{\mathrm{V}} \rangle = 1$

Démonstration. — Si $\mathrm{V} \cong \oplus_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} m_{\mathrm{W}} \mathrm{W}$, alors

$$\langle \chi_{\mathrm{V}}, \chi_{\mathrm{V}} \rangle = \langle \sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} m_{\mathrm{W}} \chi_{\mathrm{W}}, \sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} m_{\mathrm{W}} \chi_{\mathrm{W}} \rangle = \sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} m_{\mathrm{W}}^2.$$

Comme les m_{W} sont des entiers naturels, on en déduit que $\langle \chi_{\mathrm{V}}, \chi_{\mathrm{V}} \rangle = 1$ si et seulement si tous les m_{W} sont égaux à 0, sauf un qui est égal à 1. Ceci permet de conclure.

Exercice I.2.22. — Soit $\chi \in \mathrm{R}_{\mathbf{Z}}(\mathrm{G})$. Montrer que les conditions suivantes sont équivalentes.
(i) $\chi \in \mathrm{Irr}(\mathrm{G})$.
(ii) $\langle \chi, \chi \rangle = 1$ et $\chi(1) \geqslant 0$.

4.4. *La décomposition de la représentation régulière*

Corollaire I.2.23. — (i) *Si* W *est irréductible, alors* W *apparaît dans la représentation régulière avec la multiplicité* $\dim \mathrm{W}$.
(ii) *On a* $\sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} (\dim \mathrm{W})^2 = |\mathrm{G}|$ (formule de Burnside [5]).
(iii) *Si* $g \neq 1$, *alors* $\sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} \dim \mathrm{W}\, \chi_{\mathrm{W}}(g) = 0$.

Démonstration. — Le caractère $\chi_{\mathrm{V_G}}$ de la représentation régulière est donné (alinéa 2.3 du § I.1) par $\chi_{\mathrm{V_G}}(1) = |\mathrm{G}|$ et $\chi_{\mathrm{V_G}}(g) = 0$, si $g \neq 1$. Or la multiplicité de W dans $\mathrm{V_G}$ est, d'après le cor.I.2.18, égale à

$$\langle \chi_{\mathrm{W}}, \chi_{\mathrm{V_G}} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi_{\mathrm{W}}(g)} \chi_{\mathrm{V_G}}(g) = \frac{1}{|\mathrm{G}|} \overline{\chi_{\mathrm{W}}(1)} |\mathrm{G}| = \overline{\chi_{\mathrm{W}}(1)} = \dim \mathrm{W},$$

ce qui démontre le (i). On en déduit que $\chi_{\mathrm{V_G}} = \sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} \dim \mathrm{W}\, \chi_{\mathrm{W}}$. En appliquant cette identité à $g = 1$, on en déduit le (ii), et à $g \neq 1$, on en déduit le (iii).

5. Le cas des groupes commutatifs

5.1. *La transformée de Fourier*

Théorème I.2.24. — *Si* G *est commutatif, toute représentation irréductible de* G *est de dimension* 1. *Autrement dit* $\mathrm{Irr}(\mathrm{G})$ *coïncide avec l'ensemble* $\widehat{\mathrm{G}}$ *des caractères linéaires de* G.

Démonstration. — Si G est commutatif, les classes de conjugaison sont réduites à un élément, et donc $|\mathrm{Conj}(\mathrm{G})| = |\mathrm{G}|$. Comme $|\mathrm{Irr}(\mathrm{G})| = |\mathrm{Conj}(\mathrm{G})|$ d'après le cor. I.2.16, comme $\sum_{\mathrm{W} \in \mathrm{Irr}(\mathrm{G})} (\dim \mathrm{W})^2 = |\mathrm{G}|$, d'après le (ii) du cor. I.2.23, et comme $\dim \mathrm{W} \geqslant 1$, quel que soit $\mathrm{W} \in \mathrm{Irr}(\mathrm{G})$, on en déduit que $\dim \mathrm{W} = 1$, quel que soit $\mathrm{W} \in \mathrm{Irr}(\mathrm{G})$, ce que l'on voulait démontrer [6].

Corollaire I.2.25. — *Si* G *est commutatif, toute fonction de* G *dans* $\mathbf{C}$ *est combinaison linéaire de caractères linéaires.*

Démonstration. — D'après le th. I.2.14, toute fonction centrale (et donc toute fonction puisque G est commutatif) est combinaison linéaire de caractères irréductibles. Le th. I.2.24 permet de conclure.

Comme les caractères linéaires d'un groupe commutatif G forment une base orthonormale des fonctions de G dans $\mathbf{C}$, il est très facile de décomposer une fonction quelconque

5. Dans le cas de S_n, on dispose d'une démonstration directe de cette formule, cf. note 2 de l'annexe C
6. Des démonstrations plus terre-à-terre sont proposées dans les ex. I.1.8 et I.2.11.

comme une combinaison linéaire de caractères linéaires. Si ϕ est une fonction sur G, on définit la *transformée de Fourier* $\hat{\phi}$ comme la fonction définie sur $\widehat{\mathrm{G}}$ par

$$\hat{\phi}(\chi) = \langle \chi, \phi \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi(g)} \phi(g) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi(g)^{-1} \phi(g).$$

La *formule d'inversion de Fourier* s'exprime alors sous la forme

$$\phi = \sum_{\chi \in \widehat{\mathrm{G}}} \hat{\phi}(\chi)\, \chi;$$

c'est une conséquence immédiate du fait que les χ, pour $\chi \in \widehat{\mathrm{G}}$, forment une famille orthonormale. Par exemple, si on applique ce qui précède à la fonction $\phi_a : \mathrm{G} \to \mathbf{C}$ valant 1 en a et 0 ailleurs, on a $\hat{\phi}_a(\chi) = \frac{1}{|\mathrm{G}|}\overline{\chi}(a)$, et on obtient :

$$\frac{1}{|\mathrm{G}|} \sum_{\chi \in \widehat{\mathrm{G}}} \overline{\chi(a)} \chi(x) = \begin{cases} 1 & \text{si } x = a, \\ 0 & \text{sinon.} \end{cases}$$

Un caractère linéaire de $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$ est appelé un *caractère de Dirichlet modulo* D. On note Dir(D) l'ensemble de ces caractères. Le résultat suivant est un des ingrédients de la démonstration de Dirichlet du théorème de la progression arithmétique (cf. th. VII.4.7).

Proposition I.2.26. — *Si a est premier à* D*, alors*

$$\frac{1}{\varphi(\mathrm{D})} \sum_{\chi \in \mathrm{Dir(D)}} \overline{\chi(a)} \chi(n) = \begin{cases} 1 & \textit{si } n \equiv a \textit{ mod } \mathrm{D}, \\ 0 & \textit{sinon.} \end{cases}$$

Démonstration. — Il suffit d'appliquer ce qui précède au groupe $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$, dont le cardinal est $\varphi(\mathrm{D})$, et à la fonction $\phi_a : (\mathbf{Z}/\mathrm{D}\mathbf{Z})^* \to \mathbf{C}$ valant 1 en a et 0 ailleurs.

5.2. *Le groupe dual*

Remarque I.2.27. — Si G est un groupe, lors $\widehat{\mathrm{G}}$ est un groupe commutatif pour la multiplication des caractères linéaires [$\chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$, pour tout $x \in \mathrm{G}$, si $\chi_1, \chi_2 \in \widehat{\mathrm{G}}$], et on peut donc considérer le groupe $\widehat{\widehat{\mathrm{G}}}$ de ses caractères linéaires. La formule de multiplication ci-dessus montre que, si $x \in \mathrm{G}$, alors $\chi \mapsto \chi(x)$ est un caractère linéaire de $\widehat{\mathrm{G}}$; d'où une application naturelle $\iota : \mathrm{G} \to \widehat{\widehat{\mathrm{G}}}$, définie par $(\iota(x))(\chi) = \chi(x)$. Cette application est un morphisme de groupes puisque, si $x, y \in \mathrm{G}$, on a

$$(\iota(xy))(\chi) = \chi(xy) = \chi(x)\chi(y) = (\iota(x))(\chi)\,(\iota(y))(\chi),$$

pour tout $\chi \in \widehat{\mathrm{G}}$, et donc $\iota(xy) = \iota(x)\iota(y)$.

Proposition I.2.28. — *Si* G *est un groupe commutatif fini, alors $\iota : \mathrm{G} \to \widehat{\widehat{\mathrm{G}}}$ est un isomorphisme de groupes.*

Démonstration. — Compte-tenu de ce qui précède, il suffit de vérifier la bijectivité de ι. Si H est un groupe commutatif fini, on a $|\mathrm{Conj}(\mathrm{H})| = |\mathrm{H}|$, et $|\mathrm{Irr}(\mathrm{H})| = |\widehat{\mathrm{H}}|$ d'après le cor. I.2.25. On en déduit, en utilisant le cor. I.2.16, que $|\mathrm{H}| = |\widehat{\mathrm{H}}|$. En utilisant ce résultat pour G et $\widehat{\mathrm{G}}$, on en déduit que G et $\widehat{\widehat{\mathrm{G}}}$ ont le même cardinal. Il suffit donc de vérifier que ι est injective. Or la décomposition de Fourier de la fonction ϕ_a, introduite dans le paragraphe précédant la prop. I.2.26, montre que, si $\chi(a) = \chi(b)$ pour tout $\chi \in \widehat{\mathrm{G}}$, alors $\phi_a = \phi_b$, et donc $a = b$. Ceci permet de conclure.

Exercice I.2.29. — Montrer que le groupe dual de $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ (en fait à $\boldsymbol{\mu}_n$).

Lemme I.2.30. — *Soit* G *un groupe commutatif fini.*

(i) *Si* $x \in \mathrm{G}$ *est d'ordre* a*, si* $y \in \mathrm{G}$ *est d'ordre* b*, et si* a *et* b *sont premiers entre eux, alors* xy *est d'ordre* ab*.*

(ii) *Si* $a, b \in \mathbf{N} - \{0\}$*, et si* G *contient des éléments d'ordre* a *et* b*, alors il contient un élément d'ordre* $\mathrm{ppcm}(a, b)$*.*

(iii) *Soit* N *le maximum des ordres des éléments de* G*. Alors* $x^{\mathrm{N}} = 1$ *pour tout* $x \in \mathrm{G}$*.*

Démonstration. — (i) Comme x et y commutent, on a $(xy)^n = x^n y^n$, pour tout $n \in \mathbf{N}$. En particulier, $(xy)^{ab} = x^{ab}y^{ab} = 1$, et donc l'ordre de xy divise ab. Réciproquement, si $(xy)^n = 1$, alors $1 = (xy)^{an} = y^{an}$ et $1 = (xy)^{bn} = x^{bn}$, et donc an est un multiple de b et bn est un multiple de a. Comme a et b sont premiers entre eux, cela implique que n est un multiple de a et b et donc aussi de ab ; autrement dit l'ordre de xy est un multiple de ab. On en déduit le (i).

(ii) Soit $\mathscr{P}_1$ (resp. $\mathscr{P}_2$) l'ensemble des p premiers tels que $v_p(a) > 0$ et $v_p(a) \geqslant v_p(b)$ (resp. $v_p(b) > v_p(a)$). Alors $\mathscr{P}_1$ et $\mathscr{P}_2$ sont disjoints, ce qui fait que $k = \prod_{p \in \mathscr{P}_1} p^{v_p(a)}$ et $\ell = \prod_{p \in \mathscr{P}_2} p^{v_p(b)}$ sont premiers entre eux. De plus, on a $v_p(k\ell) = v_p(a)$, si $v_p(a) \geqslant v_p(b)$, et $v_p(k\ell) = v_p(b)$, si $v_p(a) < v_p(b)$, et donc $k\ell = \mathrm{ppcm}(a, b)$. Maintenant, soient $x \in \mathrm{G}$ d'ordre a et $y \in \mathrm{G}$ d'ordre b. Comme k divise a, cela implique que $x' = x^{a/k}$ est d'ordre k. De même $y' = y^{b/\ell}$ est d'ordre ℓ, et le (i) montre que $x'y'$ est d'ordre $k\ell = \mathrm{ppcm}(a, b)$. D'où le (ii).

(iii) Il résulte du (ii) que G contient un élément d'ordre $\mathrm{ppcm}(a, \mathrm{N})$, si $x \in \mathrm{G}$ est d'ordre a. Comme $\mathrm{ppcm}(a, \mathrm{N}) \geqslant \mathrm{N}$, cela implique que $\mathrm{ppcm}(a, \mathrm{N}) = \mathrm{N}$, par définition de N, et donc que a divise N. On en déduit le (iii).

Remarque I.2.31. — Le cas de S_3 montre que les trois résultats du lemme I.2.30 peuvent se trouver en défaut, si G n'est pas commutatif.

Si G est un groupe commutatif fini, l'entier N dont le (iii) du lemme I.2.30 décrit les propriétés est appelé *l'exposant* de G.

Lemme I.2.32. — *Si* G *est un groupe commutatif fini, alors* G *et* $\widehat{\mathrm{G}}$ *ont même exposant.*

Démonstration. — Si H est un groupe commutatif fini, notons N(H) son exposant. Si $\chi \in \widehat{\mathrm{H}}$, on a

$$\chi^{\mathrm{N(H)}}(x) = \chi(x)^{\mathrm{N(H)}} = \chi(x^{\mathrm{N(H)}}) = \chi(1) = 1, \quad \text{pour tout } x \in \mathrm{G},$$

et donc $\chi^{\mathrm{N(H)}} = 1$. On en déduit que l'exposant de $\widehat{\mathrm{H}}$ divise celui de H. En utilisant ce résultat pour H = G et H = $\widehat{\mathrm{G}}$, et l'isomorphisme $\widehat{\widehat{\mathrm{G}}} \cong \mathrm{G}$, on en déduit les inégalités $\mathrm{N(G)} = \mathrm{N}(\widehat{\widehat{\mathrm{G}}}) \leqslant \mathrm{N}(\widehat{\mathrm{G}}) \leqslant \mathrm{N(G)}$, qui permettent de conclure.

5.3. *Le théorème de structure des groupes finis commutatifs*

Théorème I.2.33. — *Si* G *est un groupe fini commutatif, il existe* $r \in \mathbf{N}$*, et des entiers* $\mathrm{N}_1, \ldots, \mathrm{N}_r$*, où* N_1 *est l'exposant de* G *et* $\mathrm{N}_{i+1} | \mathrm{N}_i$*, si* $i \leqslant r-1$*, tels que* $\mathrm{G} \cong \oplus_{i=1}^{r} \mathbf{Z}/\mathrm{N}_i\mathbf{Z}$*.*

Démonstration. — La démonstration se fait par récurrence sur |G|, le résultat étant évident (avec $r = 0$), si $|\mathrm{G}| = 1$. Suposons donc $|\mathrm{G}| > 1$, et notons $\mathrm{N} = \mathrm{N}_1$ l'exposant de G. Alors $\chi(x)$ est une racine N-ième de l'unité, pour tous $\chi \in \widehat{\mathrm{G}}$ et $x \in \mathrm{G}$. De plus, comme N est aussi l'exposant de $\widehat{\mathrm{G}}$ (lemme I.2.32), il existe χ_1 d'ordre N, et comme $\chi_1(\mathrm{G})$ est un sous-groupe du groupe cyclique $\boldsymbol{\mu}_{\mathrm{N}}$, c'est $\boldsymbol{\mu}_{\mathrm{N}}$ tout entier. Il existe donc $x_1 \in \mathrm{G}$ tel que $\chi_1(x_1) = e^{2i\pi/\mathrm{N}}$. Comme l'ordre de x_1 divise N, par définition de l'exposant d'un goupe, il en résulte que x_1 est d'ordre N, et donc que le sous-groupe H_1 de G engendré par x_1 est isomorphe à $\mathbf{Z}/\mathrm{N}\mathbf{Z}$. Montrons que G est la somme directe de H_1 et $\mathrm{G}_1 = \operatorname{Ker} \chi_1$, ce qui permettra de conclure en appliquant l'hypothèse de récurrence à G_1, l'exposant d'un sous-groupe divisant celui du groupe de manière évidente. Pour cela, constatons que χ_1 induit un isomorphisme de H_1 sur $\boldsymbol{\mu}_{\mathrm{N}}$, puisqu'il est surjectif et que les deux groupes ont le même cardinal N ; notons $\alpha : \boldsymbol{\mu}_{\mathrm{N}} \to \mathrm{H}_1$ son inverse. Si $x \in \mathrm{G}$, alors $a = \alpha(\chi_1(x)) \in \mathrm{H}_1$ et $b = a^{-1}x$ vérifie $\chi_1(b) = \chi_1(a)^{-1}\chi_1(x) = 1$, et donc $b \in \mathrm{G}_1$. On peut donc écrire tout élément x de G sous la forme $x = ab$, avec $a \in \mathrm{H}_1$ et $b \in \mathrm{G}_1$. Enfin $\mathrm{H}_1 \cap \mathrm{G}_1 = \{1\}$ puisque χ_1 est injectif sur H_1. Ceci montre que $\mathrm{G} = \mathrm{H}_1 \oplus \mathrm{G}_1$, et permet de conclure.

Exercice I.2.34. — Soit G un groupe commutatif fini. Montrer que $\widehat{\mathrm{G}}$ et G sont isomorphes.

6. Table des caractères d'un groupe fini

Soit G un groupe fini, et soit $c = |\mathrm{Conj(G)}|$. La *table des caractères* de G est un tableau $c \times c$ dont les coefficients sont les valeurs des caractères irréductibles sur les classes de conjugaison de G, le coefficient à l'intersection de la colonne correspondant au caractère χ et de la ligne correspondant à la classe de conjugaison C, étant $\chi(\mathrm{C})$. C'est en quelque sorte la carte du groupe G.

Remarque I.2.35. — Notons T_{G} la matrice $c \times c$ définie par la table des caractères. Notons aussi K la matrice diagonale dont le coefficient diagonal sur la ligne correspondant à une classe de conjugaison C est $\frac{|\mathrm{C}|}{|\mathrm{G}|}$. Alors les relations d'orthogonalité des caractères s'expriment de manière compacte par la relation $\mathrm{T}_{\mathrm{G}}^{*}\mathrm{K}\mathrm{T}_{\mathrm{G}} = \mathrm{I}$. On en déduit que $\mathrm{K} = (\mathrm{T}_{\mathrm{G}}^{*})^{-1}\mathrm{T}_{\mathrm{G}}^{-1}$ et $\mathrm{K}^{-1} = \mathrm{T}_{\mathrm{G}}\mathrm{T}_{\mathrm{G}}^{*}$. En particulier, les lignes de T_{G} forment une famille

orthogonale, ce qui permet de remplir la table des caractères en n'en connaissant qu'une partie.

Par exemple, le groupe $\{\pm 1\}$ a deux classes de conjugaison 1 et -1, et deux caractères irréductibles 1 et χ (de dimension 1 puisque $\{\pm 1\}$ est commutatif) ; sa table des caractères est très facile à établir :

	1	χ
1	1	1
-1	1	-1

FIGURE 1. Table des caractères de $\{\pm 1\}$

L'exemple du groupe $\{\pm 1\}$ est un peu trop trivial pour donner une idée de la manière dont on peut construire la table des caractères d'un groupe. L'exemple de A_4, traité ci-dessous, est nettement plus riche. Le lecteur trouvera dans les exercices d'autres techniques pour établir des tables de caractères de petits groupes. L'appendice C et les problèmes H.2, H.3 et H.4 contiennent des exemples un peu plus sophistiqués. Le contraste entre la simplicité et la puissance de la théorie générale et le côté artisanal du traitement des cas particuliers est assez saisissant.

Rappelons que A_4 est le sous-groupe des permutations de S_4 de signature 1. Comme S_4 a 24 éléments, on a $|A_4| = 12$, et les éléments de A_4 sont :

• l'élément neutre id,

• les trois produits de deux transpositions $s_2 = (12)(34)$, $s_3 = (13)(24)$ et $s_4 = (14)(23)$, qui sont d'ordre 2,

• les huit 3-cycles (123), (234), (341), (412) et (132), (243), (314), (421), qui sont d'ordre 3.

Nous nous proposons d'établir la table des caractères de A_4. Il y a plusieurs manières d'arriver au résultat. La manière la plus systématique consiste à déterminer les classes de conjugaison de A_4, construire toutes les représentations irréductibles de A_4, et calculer la valeur de leurs caractères sur les classes de conjugaison. C'est celle que nous explorons en premier [7] ; ensuite nous montrons un certain nombre de raccourcis possibles qui utilisent les théorèmes du cours.

(a) Soit t le 3-cycle (123). On a $t^2 = (132)$, et comme t est d'ordre 3, le sous-groupe $T = \{1, t, t^2\}$ de A_4 engendré par t est d'ordre 3.

(b) $H = \{\mathrm{id}, s_2, s_3, s_4\}$ est un sous-groupe commutatif distingué de A_4.

7. Nous n'avons pas cherché la solution la plus courte ; au contraire, nous avons essayé d'employer un maximum de techniques de base de la théorie des groupes finis. On pourrait aller plus vite en utilisant ce qu'on sait des classes de conjugaison de S_4 (n° 3.4 du Vocabulaire).

Cela peut se vérifier par un calcul un peu fastidieux. On peut aussi remarquer qu'un 2-Sylow de A_4 est de cardinal 4, et comme H est de cardinal 4 et contient tous les éléments de A_4 d'ordre divisant 4, cela prouve qu'il n'y a qu'un seul 2-Sylow (qui est donc distingué puisque la conjugaison transforme un 2-Sylow en un 2-Sylow), et que ce 2-Sylow est H. De plus, tous les éléments de H sont d'ordre divisant 2, et un groupe ayant cette propriété est commutatif car $(xy)^2 = 1 = x^2y^2$ implique $xy = yx$.

(c) Tout élément de A_4 peut s'écrire sous la forme $t^a h$, avec $a \in \{0, 1, 2\}$ et $h \in H$, et ceci, de manière unique.

Les sous-groupes T et H de A_4 ont une intersection réduite à $\{\mathrm{id}\}$. On en déduit que $(c, h) \mapsto ch$ est une injection de $T \times H$ dans A_4 ; en effet, si $c_1h_1 = c_2h_2$, alors $c_2^{-1}c_1 = h_2h_1^{-1}$, et comme $c_2^{-1}c_1 \in T$ et $h_2h_1^{-1} \in H$, on a $c_2 = c_1$ et $h_2 = h_1$. Comme $T \times H$ et A_4 ont le même cardinal, une injection est une bijection, ce qui permet de conclure.

(d) t et t^2 ne commutent à aucun élément de $H - \{\mathrm{id}\}$.

Cela peut se vérifier par un calcul un peu pénible. On peut aussi remarquer que si t et $s \in H - \{\mathrm{id}\}$ commutent, le sous-groupe G de A_4 engendré par s et t est commutatif et isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \cong \mathbf{Z}/6\mathbf{Z}$, car les sous-groupes $\{\mathrm{id}, s\}$ et T engendrés par s et t sont en somme directe. Ceci n'est pas possible car A_4 ne contient pas d'élément d'ordre 6. L'argument est le même pour n'importe quel 3-cycle, et donc en particulier pour t^2.

(e) Les classes de conjugaison de A_4 sont $B_1 = \{\mathrm{id}\}$, $B_2 = H - \{\mathrm{id}\}$, $B_3 = tH$ et $B_4 = t^2H$.

Un calcul particulièrement ennuyeux mènerait au résultat...

• Comme dans tout groupe, la classe de conjugaison de l'élément neutre n'a qu'un élément, et donc $B_1 \in \mathrm{Conj}(A_4)$.

• Si $s \in B_2$, et si $t^a h$, avec $a \in \{0, 1, 2\}$ et $h \in H$ commute à s, on a $t^a hs = st^a h$, et donc $t^a hsh = st^a h^2$, et comme H est commutatif et $h^2 = \mathrm{id}$, on obtient $t^a s = st^a$, ce qui implique $a = 0$. Le centralisateur de s est donc H, et le cardinal de la classe de conjugaison de s est égal à $\frac{|A_4|}{|H|} = 3$. Comme un conjugué de s est d'ordre 2, cette classe de conjugaison est incluse dans B_2, et donc lui est égale pour des raisons de cardinal.

• Enfin, le centralisateur de t et t^2 est T (si $t^a ht = tt^a h$, on a $ht = th$, et donc $h = \mathrm{id}$), ce qui fait que le cardinal de la classe de conjugaison de t est $\frac{|A_4|}{|T|} = 4$. Or on a $(t^a h)t(t^a h)^{-1} = t^a hth^{-1}t^{-a} = t(t^{a-1}ht^{1-a})(t^a h^{-1}t^{-a}) \in tH$, car H est distingué et donc $t^{a-1}ht^{1-a} \in H$ et $t^a h^{-1}t^{-a} \in H$. La classe de conjugaison de t est donc incluse dans B_3 et lui est égale pour des raisons de cardinal. De même, la classe de conjugaison de t^2 est B_4.

Ceci permet de conclure.

(f) Soit $\rho = e^{\frac{2i\pi}{3}}$ une racine primitive 3-ième de l'unité. Si $i \in \{0, 1, 2\}$, on définit $\eta^i : A_4 \to \boldsymbol{\mu}_3$ par $\eta^i(t^a h) = \rho^{ia}$, si $a \in \{0, 1, 2\}$ et si $h \in H$. Alors $\eta^0 = 1$, η et η^2 sont des caractères linéaires distincts de A_4.

Si $a, b \in \{0, 1, 2\}$, et si $h, g \in H$, alors $t^a ht^b g = t^{a+b}(t^{-b}ht^b)g$, et comme H est distingué, on a $t^{-b}ht^b \in H$, et donc $(t^{-b}ht^b)g \in H$ et $\eta^i(t^a ht^b g) = \rho^{i(a+b)} = \rho^{ia}\rho^{ib} = \eta^i(t^a h)\eta^i(t^b g)$.

(g) Soit V la représentation de permutation associée à l'action naturelle de A_4 sur $\{1, 2, 3, 4\}$. Rappelons que cette représentation est $\mathbf{C}^4$ muni de l'action de A_4 définie, dans

la base canonique $e_1, \dots, e_4$, par $g(e_i) = e_{g(i)}$. L'hyperplan W d'équation $x_1 + \cdots + x_4 = 0$ est stable par A_4, et la représentation que l'on obtient est irréductible de caractère donné par $\chi_W(\mathrm{id}) = 3$, $\chi_W(g) = -1$, si $g \in H - \{\mathrm{id}\}$, et $\chi_W(g) = 0$, si $g \notin H$.

La représentation V se décompose sous la forme $V' \oplus W$, où V' est la droite engendré par $e_1 + \cdots + e_4$ (isomorphe à $\mathbf{1}$ car $e_1 + \cdots + e_4$ est fixe par A_4). Comme V est une représentation de permutation, $\chi_V(g)$ est le nombre de points fixes de g agissant sur $\{1, 2, 3, 4\}$. On a donc $\chi_V(\mathrm{id}) = 4$, $\chi_V(g) = 0$, si $g \in H - \{\mathrm{id}\}$ et $\chi_V(g) = 1$, si $g \notin H$. On en déduit le caractère de W, car $\chi_V = \chi_{V'} + \chi_W$, et $\chi_{V'}(g) = 1$ pour tout $g \in A_4$, puisque $V' \cong \mathbf{1}$. Donc $\chi_W(\mathrm{id}) = 3$, $\chi_W(g) = -1$, si $g \in H - \{\mathrm{id}\}$, et $\chi_W(g) = 0$, si $g \notin H$.

Il reste à vérifier que W est irréductible. Commençons par constater que, si $g \in A_4$ et si $v = (x_1, \dots, x_4) \in \mathbf{C}^4$, alors $g \cdot v = x_1 e_{g(1)} + \cdots + x_4 e_{g(4)} = (x_{g^{-1}(1)}, \dots, x_{g^{-1}(4)})$. Maintenant, supposons $v \in W - \{0\}$ et soit W' le sous-espace de W engendré par les $g \cdot v$, pour $g \in A_4$ (il s'agit de prouver que $W' = W$, quel que soit v). Il existe donc $i \neq j$ tel que $x_i \neq x_j$ et, sans nuire à la généralité, on peut supposer que $x_1 \neq x_2$. L'image de v par le 3-cycle $t = (1, 2, 3)$ est alors (x_3, x_1, x_2, x_4) ; il en résulte que W', qui contient $t \cdot v$ et v, contient $w = t \cdot v - v = (x_3 - x_1, x_1 - x_2, x_2 - x_3, 0)$ (on a donc fait apparaître un 0). Le sous-espace W' contient aussi $w + g \cdot w$, si $g = (13)(24)$, et comme $w + g \cdot w = (x_1 - x_2)(e_2 + e_4 - e_1 - e_3)$ et $x_1 - x_2 \neq 0$, il contient le vecteur $f_1 = e_1 - e_2 + e_3 - e_4$. Il contient donc aussi les images $f_2 = e_1 + e_2 - e_3 - e_4$ et $f_3 = e_1 - e_2 - e_3 + e_4$ de ce vecteur par les 3-cycles (243) et (234), et comme f_1, f_2, f_3 forment une base de W, on a $W' = W$, ce qui permet de conclure.

(h) La table des caractères de A_4 est celle de la figure 2.

	$\mathbf{1}$	η	η^2	χ_W
B_1	1	1	1	3
B_2	1	1	1	-1
B_3	1	ρ	ρ^2	0
B_4	1	ρ^2	ρ	0

FIGURE 2. Table des caractères de A_4

En effet, A_4 ayant 4 classes de conjugaison, il a aussi 4 représentations irréductibles à isomorphisme près, qui sont donc les 3 caractères linéaires 1, η et η^2, et la représentation W de dimension 3. Les valeurs des caractères de ces représentations ont été calculées ci-dessus ; ce sont les valeurs reportées dans la table. Ceci permet de conclure.

• *Premier raccourci.* On peut utiliser le cor. I.2.21 pour démontrer l'irréductibilité de W : on a $\langle \chi_W, \chi_W \rangle = \frac{1}{12}(3^2 + 3 \cdot (-1)^2 + 8 \cdot 0) = 1$, ce qui prouve que W est irréductible.

• *Second raccourci.* Imaginons que l'on ait construit des représentations 1, η, η^2 et W dont les caractères prennent les valeurs de la table sur B_1, B_2, B_3 et B_4, mais qu'on ne sache pas quelles sont les classes de conjugaison de A_4. Alors on peut en déduire que ces classes sont exactement B_1, B_2, B_3 et B_4, ce qui permet de se passer des points (d) et (e) ci-dessus. En effet, comme $1^2 + 1^2 + 1^2 + 3^2 = 12$, la formule de Burnside ((ii) du cor. I.2.23) montre que 1, η, η^2 et χ_W sont les éléments de $\mathrm{Irr}(A_4)$, et donc (cor. I.2.16)

que A_4 a 4 classes de conjugaison. Or on remarque que, si $i \neq j$, il existe $\chi \in \mathrm{Irr}(\mathrm{A}_4)$ prenant des valeurs distinctes sur B_i et B_j. Comme un élément de $\mathrm{Irr}(\mathrm{A}_4)$ est constant sur une classe de conjugaison, on en déduit que si $\mathrm{C} \in \mathrm{Conj}(\mathrm{A}_4)$, il existe $i(\mathrm{C}) \in \{1,2,3,4\}$ tel que $\mathrm{C} \subset \mathrm{B}_{i(\mathrm{C})}$. Les éléments de C formant une partition de A_4, l'application $\mathrm{C} \mapsto i(\mathrm{C})$ est surjective, et comme les deux ensembles ont le même nombre d'éléments, elle est bijective ; de plus, on a $\mathrm{B}_{i(\mathrm{C})} = \mathrm{C}$, sinon un élément de $\mathrm{B}_{i(\mathrm{C})} - \mathrm{C}$ ne serait pas dans la réunion des classes de conjugaison. En résumé, les classes de conjugaison de A_4 sont les B_i.

• *Troisième raccourci.* Supposons W construite. La formule de Burnside ((ii) du cor. I.2.23) nous fournit alors l'identité $12 = |\mathrm{A}_4| = 9 + \sum_{\mathrm{W}' \in \mathrm{Irr}(\mathrm{A}_4) - \{\mathrm{W}\}} (\dim \mathrm{W}')^2$, et comme il y a une seule manière d'écrire 3 comme une somme de carrés, on en déduit que A_4 a trois caractères linéaires distincts. Autrement dit, le groupe $\widehat{\mathrm{A}}_4$ (cf. ex. I.1.10) est de cardinal 3 et donc isomorphe à $\mathbf{Z}/3\mathbf{Z}$; en particulier, il est cyclique et si on note η un générateur, les éléments de $\widehat{\mathrm{A}}_4$ sont η, η^2 et le caractère trivial qui est aussi égal à η^3. Comme η est d'ordre 3, il est à valeurs dans le groupe $\boldsymbol{\mu}_3$ des racines 3-ièmes de l'unité, et son image étant un sous-groupe de $\boldsymbol{\mu}_3$ non réduit à 1, c'est $\boldsymbol{\mu}_3$ tout entier. En particulier, l'image de η est de cardinal 3, et donc le noyau est de cardinal $|\mathrm{A}_4|/3 = 4$. Par ailleurs, on a $\mathrm{H} \subset \operatorname{Ker}\chi$ car le seul élément de $\boldsymbol{\mu}_3$ d'ordre divisant 2 est 1. On en déduit que $\operatorname{Ker}\chi = \mathrm{H}$, ce qui permet de redémontrer le point (b). Enfin, on a $\eta(t) \neq 1$ puisque $t \notin \mathrm{H}$, et donc $\eta(t) = \rho$ ou $\eta(t) = \rho^2$; quitte à remplacer η par η^2, on peut supposer que $\eta(t) = \rho$. On a alors $\eta(g) = 1$ si $g \in \mathrm{H} = \mathrm{B}_1 \cup \mathrm{B}_2$, $\eta(g) = \rho$ si $g \in \mathrm{B}_3 = t\mathrm{H}$, et $\eta(g) = \rho^2$ si $g \in \mathrm{B}_4 = t^2\mathrm{H}$. Ceci permet, en utilisant le second raccourci, de compléter la table des caractères de A_4 sans avoir utilisé un seul des points (a)-(e) au sujet de la structure de A_4 ni le point (f).

• *Quatrième raccourci.* On suppose ce coup-ci que l'on a construit η, ce qui utilise les points (a)-(c) et (f), mais pas les (d), (e) et (g). La formule de Burnside montre alors, qu'il y a a priori quatre possibilités pour les caractères irréductibles distincts des caractères linéaires 1, η et η^2 :

— un unique caractère χ_{W} de degré 3,

— deux caractères de degré 2 et un de degré 1, ou un de degré 2 et cinq de degré 1,

— neuf caractères de degré 1.

Si on est dans le premier cas, on a gagné car $1 + \eta + \eta^2 + 3\chi_{\mathrm{W}}$ est le caractère de la représentation régulière, ce qui permet de calculer χ_{W}, et donc de compléter la table en utilisant le second raccourci. Il suffit donc d'éliminer les autres possibilités.

⋆ La dernière implique que $|\mathrm{Irr}(\mathrm{A}_4)| = 12$, ce qui implique que A_4 a 12 classes de conjugaison (cor. I.2.16), et donc que celles-ci sont des singletons, et que A_4 est commutatif, ce qui n'est pas.

⋆ Si A_4 a au moins une représentation irréductible V de dimension 2, alors χ_{V}, $\chi_{\mathrm{V}}\eta$ et $\chi_{\mathrm{V}}\eta^2$ sont des caractères irréductibles de degré 2 (cf. alinéa 2.1), et comme il y a au plus deux tels caractères, il existe $\eta_1 \neq \eta_2 \in \{1, \eta, \eta^2\}$ tels que $\chi_{\mathrm{V}}\eta_1 = \chi_{\mathrm{V}}\eta_2$. Or la condition $\eta_1 \neq \eta_2$ implique que $\eta_1(t) \neq \eta_2(t)$, et la relation $\chi_{\mathrm{V}}\eta_1 = \chi_{\mathrm{V}}\eta_2$ entraine donc $\chi_{\mathrm{V}}(t) = 0$. Ceci n'est pas possible, car t est d'ordre 3, ce qui fait que les deux valeurs propres de $\rho_{\mathrm{V}}(t)$ sont des racines 3-ièmes de l'unité, et la somme de deux racines 3-ièmes de l'unité n'est jamais nulle. L'existence d'une représentation irréductible de dimension 2 est donc exclue, ce qui permet de conclure.

I.3. Construction de représentations

1. Restriction et inflation

Si H est un sous-groupe de G et si V est une représentation de G, on peut considérer la *restriction* $\mathrm{Res}^{\mathrm{H}}_{\mathrm{G}}\mathrm{V}$ de V à H en oubliant l'action des $g \in \mathrm{G} - \mathrm{H}$. Alors $\rho_{\mathrm{Res}^{\mathrm{H}}_{\mathrm{G}}\mathrm{V}} : \mathrm{H} \to \mathrm{GL}(\mathrm{V})$ est la restriction de $\rho_{\mathrm{V}} : \mathrm{G} \to \mathrm{GL}(\mathrm{V})$ à H, et $\chi_{\mathrm{Res}^{\mathrm{H}}_{\mathrm{G}}\mathrm{V}}(h) = \chi_{\mathrm{V}}(h)$, pour tout $h \in \mathrm{H}$.

Si $\varphi : \mathrm{G} \to \mathrm{H}$ est un morphisme de groupes, et si V est une représentation de H, alors V peut aussi être considérée comme une représentation de G, en faisant agir $g \in \mathrm{G}$ par $\varphi(g) \in \mathrm{H}$; la représentation de G ainsi obtenue est *l'inflation* $\mathrm{Inf}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ de V à G. Alors $\rho_{\mathrm{Inf}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}} : \mathrm{G} \to \mathrm{GL}(\mathrm{V})$ est égal à la composée $\rho_{\mathrm{H}} \circ \varphi$, et on a $\chi_{\mathrm{Inf}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}}(g) = \chi_{\mathrm{V}}(\varphi(g))$, pour tout $g \in \mathrm{G}$. Si χ est un caractère de H, il résulte de ce qui précède que $\chi \circ \varphi$ est un caractère de G : c'est *l'inflation* de χ à G.

Remarque I.3.1. — Supposons $\varphi : \mathrm{G} \to \mathrm{H}$ surjectif.

(i) Un sous-espace de V est stable par G si et seulement si il l'est par H, ce qui prouve que $\mathrm{Inf}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ est irréductible si et seulement si V l'est, et prouve que $\chi \mapsto \chi \circ \varphi$ induit une injection de Irr(H) dans Irr(G).

(ii) Si N est le noyau de φ, une représentation V de G est obtenue par inflation d'une représentation de H si et seulement si N agit trivialement sur V. En effet, si $\mathrm{V} = \mathrm{In}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W}$, alors $g \in \mathrm{N}$ agit par $\varphi(g) = 1$ sur W et donc N agit trivialement sur V ; réciproquement, si V est une représentation de G sur laquelle N agit trivialement, alors V est l'inflation de la représentation de H obtenue en définissant $h \cdot v$, pour $h \in \mathrm{H}$ et $v \in \mathrm{V}$, par $v \mapsto \tilde{h} \cdot v$, où $\tilde{h} \in \mathrm{H}$ vérifie $\varphi(\tilde{h}) = h$: ceci ne dépend pas du choix de $\tilde{h}$ car N agit trivialement, et $\varphi(\tilde{h}) = \varphi(\tilde{h}')$ implique l'existence de $n \in \mathrm{N}$ tel que $\tilde{h}' = \tilde{h}\, n$, et donc $\tilde{h}' \cdot v = \tilde{h} \cdot (n \cdot v) = \tilde{h} \cdot v$.

Exercice I.3.2. — Soient G un groupe fini et $\varphi : \mathrm{G} \to \mathrm{H}$ un morphisme de groupes surjectif, de noyau N. Montrer que $\chi \in \mathrm{Irr}(\mathrm{G})$ est l'inflation d'un caractère de H si et seulement si $\chi(g) = \chi(1)$ pour tout $g \in \mathrm{N}$.

2. Constructions tensorielles de représentations

2.1. *Produit tensoriel d'espaces vectoriels de dimension finie*

Soient V_1, V_2 deux espaces vectoriels de dimension finie, et soient $(e_1, \ldots, e_n)$ une base de V_1 et $(f_1, \ldots, f_m)$ une base de V_2. Soit $\mathrm{V}_1 \otimes \mathrm{V}_2$ le *produit tensoriel de* V_1 *et* V_2 : c'est l'espace vectoriel de base [8] les $e_i \otimes f_j$, pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant m$. Si $x = \sum_{i=1}^{n} \lambda_i e_i \in \mathrm{V}_1$ et $y = \sum_{j=1}^{m} \mu_j f_j \in \mathrm{V}_2$, on note $x \otimes y$ l'élément de $\mathrm{V}_1 \otimes \mathrm{V}_2$ défini par la formule

$$x \otimes y = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j \, e_i \otimes f_j.$$

Le produit tensoriel $\mathrm{V}_1 \otimes \mathrm{V}_2$ est en général un objet nouveau, mais il arrive qu'il puisse se décrire de manière plus explicite.

Exemple I.3.3. — (i) Si X est un ensemble fini, on note $\mathbf{C}^{\mathrm{X}}$ l'ensemble des fonctions $\phi : \mathrm{X} \to \mathbf{C}$. C'est un espace vectoriel dont une base est l'ensemble des ϕ_x, pour $x \in \mathrm{X}$, où $\phi_x(y) = 1$, si $y = x$ et $\phi_x(y) = 0$, si $y \neq x$. Il est facile de vérifier que, si I et J sont deux ensembles finis, alors $\phi_i \otimes \phi_j \mapsto \phi_{(i,j)}$, pour $i \in \mathrm{I}$ et $j \in \mathrm{J}$, induit un isomorphisme de $\mathbf{C}^{\mathrm{I}} \otimes \mathbf{C}^{\mathrm{J}}$ sur $\mathbf{C}^{\mathrm{I} \times \mathrm{J}}$.

8. On aurait pu noter $g_{i,j}$ la base de $\mathrm{V}_1 \otimes \mathrm{V}_2$, mais la notation $e_i \otimes f_j$ est plus parlante pour la suite.

(ii) Si V_1, V_2 sont deux espaces vectoriels, et si V_1^* et V_2^* sont leur duaux (V_i^* est l'espace des formes linéaires sur V_i), alors $V_1^* \otimes V_2^*$ est l'espace des formes bilinéaires sur $V_1 \times V_2$. Si $\lambda_1 \in V_1^*$ et $\lambda_2 \in V_2^*$, alors $\lambda_1 \otimes \lambda_2$ est la forme bilinéaire $(x, y) \mapsto \lambda_1(x)\lambda_2(y)$.

Exercice I.3.4. — Montrer que $V_1^* \otimes V_2 = \mathrm{Hom}(V_1, V_2)$.

Par construction, $(x, y) \mapsto x \otimes y$ est une application bilinéaire de $V_1 \times V_2$ dans $V_1 \otimes V_2$. Le lemme suivant montre que $V_1 \otimes V_2$ est *universel* pour les applications bilinéaires sur $V_1 \times V_2$.

Lemme I.3.5. — *Si* W *est un espace vectoriel, et si* $u : V_1 \times V_2 \to W$ *est bilinéaire, alors il existe une unique application linéaire* $\tilde{u} : V_1 \otimes V_2 \to W$, *telle que* $\tilde{u}(x \otimes y) = u(x, y)$, *quels que soient* $x \in V_1$ *et* $y \in V_2$.

Démonstration. — On définit $\tilde{u}$ par ses valeurs sur les éléments de la base des $e_i \otimes f_j$, en posant $\tilde{u}(e_i \otimes f_j) = u(e_i, f_j)$. Un calcul immédiat montre alors que la bilinéarité de u est équivalente à la relation $\tilde{u}(x \otimes y) = u(x, y)$, quels que soient $x \in V_1$ et $y \in V_2$. Ceci permet de conclure [9].

Maintenant, si $u_1 \in \mathrm{End}(V_1)$ et $u_2 \in \mathrm{End}(V_2)$, alors $(x, y) \mapsto u_1(x) \otimes u_2(y)$ est bilinéaire de $V_1 \times V_2$ dans $V_1 \otimes V_2$. D'après le lemme I.3.5, il existe $u_1 \otimes u_2 \in \mathrm{End}(V_1 \otimes V_2)$ unique, tel que $(u_1 \otimes u_2)(x \otimes y) = u_1(x) \otimes u_2(y)$, quels que soient $x \in V_1$ et $y \in V_2$. Si $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(\mathbf{C})$ est la matrice de u_1, et $B = (b_{i',j'})_{1 \leqslant i',j' \leqslant m} \in \mathbf{M}_m(\mathbf{C})$ est la matrice de u_2, alors la matrice $A \otimes B \in \mathbf{M}_{nm}(\mathbf{C})$ de $u_1 \otimes u_2$, dans la base des $e_i \otimes f_{i'} = g_{(i-1)m+i'}$, est la matrice des $c_{(i-1)m+i',(j-1)m+j'}$, avec $1 \leqslant i, j \leqslant n$ et $1 \leqslant i', j' \leqslant m$ et $c_{(i-1)m+i',(j-1)m+j'} = a_{i,j} b_{i',j'}$. En particulier, on a

$$\mathrm{Tr}(u_1 \otimes u_2) = \sum_{1 \leqslant k \leqslant nm} c_{k,k} = \sum_{i=1}^{n} \sum_{i'=1}^{m} a_{i,i} b_{i',i'} = \Big(\sum_{i=1}^{n} a_{i,i} \Big) \Big(\sum_{i'=1}^{m} b_{i',i'} \Big) = \mathrm{Tr}(u_1)\, \mathrm{Tr}(u_2).$$

9. Cette caractérisation de $V_1 \otimes V_2$ comme solution d'un problème universel permet de montrer son indépendance par rapport aux bases de V_1 et V_2 choisies pour sa construction. En effet, si X est un espace vectoriel muni d'une application bilinéaire $B : V_1 \times V_2 \to X$ tel que pour toute application bilinéaire $u : V_1 \times V_2 \to W$, il existe une unique application linéaire $\tilde{u} : X \to W$, telle que $\tilde{u}(B(x, y)) = u(x, y)$, quels que soient $x \in V_1$ et $y \in V_2$, alors il existe une unique application linéaire $f : V_1 \otimes V_2 \to X$ vérifiant $f(x \otimes y) = B(x, y)$, pour tout $(x, y) \in V_1 \times V_2$ et une unique application linéaire $g : X \to V_1 \otimes V_2$ vérifiant $g(B(x, y)) = x \otimes y$, pour tout $(x, y) \in V_1 \times V_2$. Comme l'identité est l'unique application linéaire h de $V_1 \otimes V_2$ (resp. X) dans lui même telle que $h(x \otimes y) = x \otimes y$ (resp. $h(B(x, y)) = B(x, y)$), pour tout $(x, y) \in V_1 \times V_2$, on a $f \circ g = \mathrm{id}_X$ et $g \circ f = \mathrm{id}_{V_1 \otimes V_2}$, ce qui montre que X et $V_1 \otimes V_2$ sont isomorphes, à isomorphisme unique près respectant les formes bilinéaires sur $V_1 \times V_2$. Une construction générale, sans choix de base, consiste à prendre le quotient de l'espace de base les $e_{x,y}$, pour $(x, y) \in V_1 \times V_2$, par les relations $e_{x,y_1+y_2} = e_{x,y_1} + e_{x,y_2}$, $e_{x_1+x_2,y} = e_{x_1,y} + e_{x_2,y}$ et $e_{\lambda x,y} = e_{x,\lambda y} = \lambda e_{x,y}$. Alors $x \otimes y$ est l'image de $e_{x,y}$ dans le quotient (cf. alinéa 10.5.2 du Vocabulaire pour une construction similaire). La construction du texte est moins canonique mais plus concrète... La construction générale a l'avantage de marcher aussi en dimension infinie où une base n'est pas toujours facile à exhiber.

Enfin, on déduit du lemme I.3.5 que, si $u'_1, u''_1 \in \mathrm{End}(V_1)$, et si $u'_2, u''_2 \in \mathrm{End}(V_2)$, alors

$$(u'_1 \circ u''_1) \otimes (u'_2 \circ u''_2) = (u'_1 \otimes u'_2) \circ (u''_1 \otimes u''_2).$$

(Il suffit de comparer l'image de $x \otimes y$ par les endomorphismes dans les deux membres.)

2.2. *Produit tensoriel de représentations*

Soient G un groupe fini, et V_1, V_2 deux représentations de G. D'après ce qui précède, si on définit une action de G sur $V_1 \otimes V_2$ par $g \cdot (x \otimes y) = (g \cdot x) \otimes (g \cdot y)$, on obtient une représentation de G. La formule ci-dessus pour la trace de $u_1 \otimes u_2$ montre que

$$\chi_{V_1 \otimes V_2}(g) = \chi_1(g)\, \chi_2(g).$$

Si V_2 est de dimension 1, on retrouve la construction de la tordue d'une représentation par un caractère linéaire (alinéa 2.1 du § I.1).

Remarque I.3.6. — (i) Si G_1 et G_2 sont deux groupes finis, et si V_1 et V_2 sont des représentations de G_1 et G_2 respectivement, on peut définir de la même manière une représentation $V_1 \boxtimes V_2$ de $G_1 \times G_2$, en faisant agir $g = (g_1, g_2) \in G_1 \times G_2$ sur l'espace vectoriel $V_1 \otimes V_2$ par $g \cdot (x \otimes y) = (g_1 \cdot x) \otimes (g_2 \cdot y)$.

(ii) Si $G_1 = G_2 = G$, la représentation $V_1 \otimes V_2$ de G définie précédemment est la restriction à G, vu comme ensemble des couples (g, g) de $G \times G$, de la représentation $V_1 \boxtimes V_2$ de $G \times G$ (c'est pour pouvoir faire la distinction que $V_1 \boxtimes V_2$ n'est pas notée $V_1 \otimes V_2$).

Exercice I.3.7. — Montrer que $R^+(G)$ est stable par produit, et que $R_{\mathbf{Z}}(G)$ est un anneau.

Exercice I.3.8. — Retrouver la formule $\chi_{V_1 \otimes V_2}(g) = \chi_1(g)\, \chi_2(g)$ en prenant des bases constituées de vecteurs propres de g.

2.3. *Carré symétrique et carré extérieur d'une représentation*

Si V est une représentation d'un groupe fini G, la représentation $V \otimes V$ n'est pas irréductible. En effet, les *tenseurs symétriques* (i.e. les expressions de la forme $xy = \frac{1}{2}(x \otimes y + y \otimes x)$, avec $x, y \in V$, et donc $xy = yx$, si $x, y \in V$) et les *tenseurs alternés* (les $x \wedge y = x \otimes y - y \otimes x$, et donc $x \wedge y = -y \wedge x$, si $x, y \in V$) sont stables sous l'action de G ; il en est donc de même des sous-espaces de $V \otimes V$ qu'ils engendrent.

On note $\mathrm{Sym}^2 V$ le *carré symétrique* de V ; c'est le sous-espace de $V \otimes V$ engendré par les tenseurs symétriques. Si V est de dimension d, de base $(e_1, \ldots, e_d)$, alors $\mathrm{Sym}^2 V$ est un espace de dimension $\frac{d(d+1)}{2}$ dont une base est constituée des $e_i e_j$, pour $1 \leqslant i \leqslant j \leqslant d$.

On note $\wedge^2 V$ le *carré extérieur* de V ; c'est le sous-espace de $V \otimes V$ engendré par les tenseurs alternés. C'est un espace de dimension $\frac{d(d-1)}{2}$ dont une base est constituée des $e_i \wedge e_j$, pour $1 \leqslant i < j \leqslant d$.

De plus, $V \otimes V = \mathrm{Sym}^2 V \oplus \wedge^2 V$ (c'est la décomposition en somme d'espaces propres pour la symétrie s de $V \otimes V$ obtenue en linéarisant l'application bilinéaire $(x, y) \mapsto y \otimes x$ de $V \times V$ dans $V \otimes V$; on a $s(x \otimes y) = (y \otimes x)$ pour tous $x, y \in V$).

Exemple I.3.9. — Si V^* est le dual de V, alors $\mathrm{Sym}^2 V^*$ est l'espace des formes bilinéaires symétriques sur V et $\wedge^2 V^*$ est celui des formes bilinéaires alternées.

Proposition I.3.10. — *Si* V *est une représentation de* G*, et si* $g \in G$*, alors*

$$\chi_{\mathrm{Sym}^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)) \quad \text{et} \quad \chi_{\wedge^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)).$$

Démonstration. — Choisissons une base $(e_1, \dots, e_d)$ de V formée de vecteurs propres de g. On a alors $g \cdot e_i = \lambda_i e_i$, $g^2 \cdot e_i = \lambda_i^2 e_i$, et $g \cdot e_i e_j = \lambda_i \lambda_j \, e_i e_j$, $g \cdot e_i \wedge e_j = \lambda_i \lambda_j \, e_i \wedge e_j$. On en déduit que

$$\chi_{\mathrm{Sym}^2 V}(g) = \sum_{i \leqslant j} \lambda_i \lambda_j \quad \text{et} \quad \chi_{\wedge^2 V}(g) = \sum_{i<j} \lambda_i \lambda_j,$$

et comme

$$\chi_V(g^2) = \sum_i \lambda_i^2 \quad \text{et} \quad \chi_V(g)^2 = \Big(\sum_i \lambda_i\Big)^2 = \sum_i \lambda_i^2 + 2\sum_{i<j} \lambda_i \lambda_j,$$

le résultat s'en déduit.

Remarque I.3.11. — Ce que l'on a fait avec deux copies de la même représentation V de G peut se généraliser à n copies de V. On note $\otimes^n V$ le produit tensoriel de n copies de V (avec une définition évidente). On note S_n le groupe des permutations de $\{1, \dots, n\}$, et $\mathrm{sign} : S_n \to \{\pm 1\}$ la signature. Un tenseur symétrique est un tenseur de la forme

$$x_1 \cdots x_n = \frac{1}{n!} \sum_{\sigma \in S_n} x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)},$$

et un tenseur alterné est un tenseur de la forme

$$x_1 \wedge \cdots \wedge x_n = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \, x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}.$$

La *puissance symétrique n-ième de* V est le sous-espace $\mathrm{Sym}^n V$ de $\otimes^n V$ engendré par les tenseurs symétriques, et la *puissance extérieure n-ième de* V est le sous-espace $\wedge^n V$ de $\otimes^n V$ engendré par les tenseurs alternés. Alors $\mathrm{Sym}^n V$ et $\wedge^n V$ sont des représentations de G de dimensions respectives $\binom{d+n-1}{n}$ et $\binom{d}{n}$. ($\mathrm{Sym}^n V \oplus \wedge^n V$ est un sous-espace strict de $\otimes^n V$, dès que $n \geqslant 3$.)

En particulier, $\wedge^n V = 0$ si $n > d$, et $\wedge^d V$ est de dimension 1 ; cette représentation est souvent notée $\det V$, l'action de g sur $\det V$ étant la multiplication par $\det \rho_V(g)$. (Voir l'alinéa 6.3 et l'ex. 6.1 du Vocabulaire pour des constructions analogues.)

3. Représentations induites

3.1. *Caractère d'une représentation induite*

Soit H un sous-groupe de G, et soit V une représentation de H. On définit l'espace vectoriel $\mathrm{Ind}_H^G V$ par

$$\mathrm{Ind}_H^G V = \{\varphi : G \to V, \ \varphi(hx) = h \cdot \varphi(x), \ \text{quels que soient } h \in H \text{ et } x \in G\}.$$

Soit $S \subset G$ un système de représentants de $H\backslash G$. Si $x \in G$, il existe alors un unique $h_x \in H$ tel que $h_x^{-1} x \in S$. Ceci permet d'établir un isomorphisme de $\mathrm{Ind}_H^G V$ sur l'espace V^S des applications de S dans V, en envoyant φ sur $(\varphi(s))_{s \in S}$; la bijection réciproque

envoie $(v_s)_{s\in \mathrm{S}} \in \mathrm{V}^{\mathrm{S}}$ sur l'application $\varphi : \mathrm{G} \to \mathrm{V}$ définie par $\varphi(x) = h_x \cdot v_{h_x^{-1}x}$. Pour vérifier que φ est bien un élément de $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$, il suffit de constater que, si $h \in \mathrm{H}$, alors $h_{hx} = hh_x$, et donc

$$\varphi(hx) = hh_x \cdot v_{(hh_x)^{-1}hx} = hh_x \cdot v_{h_x^{-1}x} = h \cdot (h_x \cdot v_{h_x^{-1}x}) = h \cdot \varphi(x).$$

On munit $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ d'une action de G en définissant $g \cdot \varphi$ comme la fonction $x \mapsto \varphi(xg)$. Si $h \in \mathrm{H}$, on a

$$(g \cdot \varphi)(hx) = \varphi(hxg) = h \cdot \varphi(xg) = h \cdot ((g \cdot \varphi)(x)),$$

ce qui prouve que $g \cdot \varphi$ est bien élément de $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$. De plus, si $g_1, g_2 \in \mathrm{G}$, alors

$$(g_1 \cdot (g_2 \cdot \varphi))(x) = (g_2 \cdot \varphi)(xg_1) = \varphi(xg_1g_2) = (g_1g_2 \cdot \varphi)(x),$$

ce qui prouve que l'on a bien défini une action de groupe de G sur $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$. La représentation de G ainsi obtenue est la *représentation induite de* H *à* G *de la représentation* V. L'isomorphisme de $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ sur V^{S} montre que la dimension de $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ est $|\mathrm{S}|\cdot\dim \mathrm{V} = \frac{|\mathrm{G}|}{|\mathrm{H}|}\dim \mathrm{V}$.

Par exemple, si $\mathrm{H} = 1$, et $\mathrm{V} = \mathbf{1}$ est la représentation triviale, la représentation $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ est l'espace des fonctions $\varphi : \mathrm{G} \to \mathbf{C}$. Il admet comme base les fonctions φ_h, pour $h \in \mathrm{G}$, définies par $\varphi_h(x) = 1$, si $xh = 1$, et $\varphi_h(x) = 0$, si $xh \neq 1$. Si $g \in \mathrm{G}$, on a alors $(g \cdot \varphi_h)(x) = \varphi_h(xg) = \varphi_{gh}(x)$. On en déduit que $\mathrm{Ind}_{\{1\}}^{\mathrm{G}}\mathbf{1}$ *est la représentation régulière de* G.

Remarque I.3.12. — Les représentations induites à partir de représentations de sous-groupes sont la principale source de représentations d'un groupe G. L'un de leurs intérêts est que leur caractère se calcule très facilement (cf. annexe C pour un certain nombre d'applications).

Théorème I.3.13. — *Soient* $\mathrm{H} \subset \mathrm{G}$ *deux groupes finis,* $\mathrm{S} \subset \mathrm{G}$ *un système de représentants de* $\mathrm{H}\backslash\mathrm{G}$*,* V *une représentation de* H*, et* $\mathrm{W} = \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$*. Alors, pour tout* $g \in \mathrm{G}$ *:*

$$\chi_{\mathrm{W}}(g) = \sum_{\substack{s\in \mathrm{S}\\ sgs^{-1}\in \mathrm{H}}} \chi_{\mathrm{V}}(sgs^{-1}) = \frac{1}{|\mathrm{H}|}\sum_{\substack{s\in \mathrm{G}\\ sgs^{-1}\in \mathrm{H}}} \chi_{\mathrm{V}}(sgs^{-1}).$$

Démonstration. — On utilise l'isomorphisme de W avec $\mathrm{V}^{\mathrm{S}} = \oplus_{s\in \mathrm{S}}\mathrm{V}_s$. Dans cet isomorphisme, si φ est l'image de $(v_s)_{s\in \mathrm{S}}$, on a $\varphi(x) = h_x \cdot v_{h_x^{-1}x}$, et $g \cdot \varphi$ est l'image de $((g \cdot \varphi)(s))_{s\in \mathrm{S}} = (\varphi(sg))_{s\in \mathrm{S}}$, ce qui fait que l'on obtient

$$g \cdot (v_s)_{s\in \mathrm{S}} = (h_{sg} \cdot v_{h_{sg}^{-1}sg})_{s\in \mathrm{S}}.$$

Choisissons une base $(e_i)_{i\in \mathrm{I}}$ de V, et notons $e_{i,s}$ l'élément $(v_t)_{t\in \mathrm{S}}$ de V^{S} défini par $v_s = e_i$, et $v_t = 0$, si $t \neq s$. Les $e_{i,s}$, pour $i \in \mathrm{I}$, forment une base de V_s, et les $e_{i,s}$, pour $(i, s) \in \mathrm{I} \times \mathrm{S}$, forment une base de V^{S}. La matrice de g dans cette base est constituée de blocs indexés par $(s, s') \in \mathrm{S} \times \mathrm{S}$, le bloc correspondant à (s, s') étant nul sauf si $s' = h_{sg}^{-1}sg$. En particulier, les seuls blocs qui vont contribuer à la trace sont ceux pour lesquels $s = h_{sg}^{-1}sg$, ce qui

peut se réécrire sous la forme $h_{sg} = sgs^{-1}$. L'action de g sur le V_s correspondant coïncide alors avec celle de $h_{sg} = sgs^{-1}$, et sa contribution à la trace est donc $\chi_{\mathrm{V}}(sgs^{-1})$. On en déduit la première égalité du théorème. La seconde s'en déduit en remarquant que $\chi_{\mathrm{V}}(hs\,g\,(hs)^{-1}) = \chi_{\mathrm{V}}(h(sgs^{-1})h^{-1}) = \chi_{\mathrm{V}}(sgs^{-1})$, si $h \in \mathrm{H}$ et $sgs^{-1} \in \mathrm{H}$, et en écrivant $s \in \mathrm{G}$ sous la forme $h_s^{-1}s$.

Exercice I.3.14. — Retrouver la formule $\dim(\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}) = \frac{|\mathrm{G}|}{|\mathrm{H}|}\dim \mathrm{V}$ en utilisant le th. I.3.13.

3.2. *La formule de réciprocité de Frobenius*

Soient $\mathrm{H} \subset \mathrm{G}$ deux groupes finis. On définit des applications linéaires

$$\mathrm{Res}_{\mathrm{G}}^{\mathrm{H}} : \mathrm{R}_{\mathbf{C}}(\mathrm{G}) \to \mathrm{R}_{\mathbf{C}}(\mathrm{H}) \quad \text{et} \quad \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}} : \mathrm{R}_{\mathbf{C}}(\mathrm{H}) \to \mathrm{R}_{\mathbf{C}}(\mathrm{G}),$$

de la manière suivante. Si $\phi \in \mathrm{R}_{\mathbf{C}}(\mathrm{G})$, alors $\mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\phi$ est juste la fonction centrale sur H, restriction de ϕ à H, et si $\phi \in \mathrm{R}_{\mathbf{C}}(\mathrm{H})$, alors $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi$ est la fonction centrale sur G donnée par la formule

$$\big(\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi\big)(g) = \frac{1}{|\mathrm{H}|}\sum_{\substack{s\in\mathrm{G}\\ sgs^{-1}\in\mathrm{H}}} \phi(sgs^{-1}).$$

Il est immédiat que, si W est une représentation de G, alors $\mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\chi_{\mathrm{W}}$ est le caractère de la représentation de H obtenue en ne considérant que l'action du sous-groupe H de G. Dans l'autre sens, si V est une représentation de H, alors $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\chi_{\mathrm{V}}$ est, d'après le th. I.3.13, le caractère de la représentation induite $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$.

Pour les distinguer, on note $\langle\ ,\ \rangle_{\mathrm{H}}$ et $\langle\ ,\ \rangle_{\mathrm{G}}$ les produits scalaires sur $\mathrm{R}_{\mathbf{C}}(\mathrm{H})$ et $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$. On a alors le résultat suivant.

Théorème I.3.15. — (formule de réciprocité de Frobenius) *Si ϕ_1 et ϕ_2 appartiennent à $\mathrm{R}_{\mathbf{C}}(\mathrm{H})$ et $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$ respectivement, alors*

$$\langle \phi_1, \mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\phi_2\rangle_{\mathrm{H}} = \langle \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi_1, \phi_2\rangle_{\mathrm{G}}.$$

Démonstration. — Par définition, on a

$$\begin{aligned}\langle \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi_1, \phi_2\rangle_{\mathrm{G}} =& \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \overline{\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi_1(g)}\,\phi_2(g)\\ =& \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\Big(\frac{1}{|\mathrm{H}|}\sum_{\substack{s\in\mathrm{G}\\ sgs^{-1}\in\mathrm{H}}} \overline{\phi_1(sgs^{-1})}\Big)\,\phi_2(g).\end{aligned}$$

En posant $h = sgs^{-1}$, et donc $g = s^{-1}hs$, on peut réécrire la somme ci-dessus sous la forme

$$\frac{1}{|\mathrm{G}|\,|\mathrm{H}|}\sum_{h\in\mathrm{H},\, s\in\mathrm{G}} \overline{\phi_1(h)}\phi_2(s^{-1}hs),$$

et comme ϕ_2 est une fonction centrale sur G, on a $\phi_2(s^{-1}hs) = \phi_2(h)$, quel que soit $s \in \mathrm{G}$. On obtient donc

$$\langle \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\phi_1, \phi_2\rangle_{\mathrm{G}} = \frac{1}{|\mathrm{H}|}\sum_{h\in\mathrm{H}} \overline{\phi_1(h)}\phi_2(h) = \langle \phi_1, \mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\phi_2\rangle_{\mathrm{H}},$$

ce qui permet de conclure.

Un cas particulier, extrèmement utile, de ce théorème, est le suivant.

Corollaire I.3.16. — *Si* W (*resp.* V) *est une représentation irréductible de* G (*resp. de* H), *la multiplicité de* W *dans* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ *est égale à celle de* V *dans* $\mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\mathrm{W}$.

Démonstration. — Il suffit d'utiliser la formule de réciprocité de Frobenius pour $\phi_1 = \chi_{\mathrm{V}}$ et $\phi_2 = \chi_{\mathrm{W}}$, combinée avec le cor. I.2.18.

Exercice I.3.17. — (i) Montrer que, si V, V_1, V_2 sont des représentations de G, alors

$$\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{V}_1 \oplus \mathrm{V}_2) = \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{V}_1) \oplus \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{V}_2)$$
$$\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1 \oplus \mathrm{V}_2, \mathrm{V}) = \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}) \oplus \mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_2, \mathrm{V}).$$

(ii) En déduire que, si V et V′ sont deux représentations de G, alors $\dim(\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{V}')) = \langle \chi_{\mathrm{V}}, \chi_{\mathrm{V}'}\rangle$.
(iii) Soit H un sous-groupe de G, et soient W une représentation de H et V une représentation de G. Si $u \in \mathrm{Hom}_{\mathrm{H}}(\mathrm{W}, \mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\mathrm{V})$, on note $\alpha_u : \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W} \to \mathrm{V}$ l'application qui à un élément $\phi : \mathrm{G} \to \mathrm{W}$ de $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W}$, associe $\alpha_u(\phi) = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} g^{-1}u(\phi(g))$. Montrer que $\alpha_u \in \mathrm{Hom}_{\mathrm{G}}(\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W}, \mathrm{V})$.
(iv) Montrer que $u \mapsto \alpha_u$, de $\mathrm{Hom}_{\mathrm{H}}(\mathrm{W}, \mathrm{Res}_{\mathrm{G}}^{\mathrm{H}}\mathrm{V})$ dans $\mathrm{Hom}_{\mathrm{G}}(\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W}, \mathrm{V})$, est une injection linéaire. En déduire que c'est un isomorphisme (réciprocité de Frobenius pour les représentations).

3.3. *Transitivité des inductions*

Proposition I.3.18. — *Soient* $\mathrm{K} \subset \mathrm{H} \subset \mathrm{G}$ *des groupes finis.*
(i) *Si* $\phi \in \mathrm{R}_{\mathbf{C}}(\mathrm{K})$, *alors* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{Ind}_{\mathrm{K}}^{\mathrm{H}}\phi) = \mathrm{Ind}_{\mathrm{K}}^{\mathrm{G}}\phi$.
(ii) *Si* W *est une représentation de* K, *alors* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{Ind}_{\mathrm{K}}^{\mathrm{H}}\mathrm{W}) = \mathrm{Ind}_{\mathrm{K}}^{\mathrm{G}}\mathrm{W}$.

Démonstration. — Le (ii) est, modulo le fait qu'une représentation est déterminée par son caractère (cor. I.2.19), une conséquence du (i) appliqué à $\phi = \chi_{\mathrm{W}}$. Pour démontrer le (i), on part de la formule

$$\begin{aligned}\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{Ind}_{\mathrm{K}}^{\mathrm{H}}\phi)(g) &= \frac{1}{|\mathrm{H}|}\sum_{\substack{s\in\mathrm{G}\\ sgs^{-1}\in\mathrm{H}}} (\mathrm{Ind}_{\mathrm{K}}^{\mathrm{H}}\phi)(sgs^{-1})\\ &= \frac{1}{|\mathrm{H}|}\sum_{\substack{s\in\mathrm{G}\\ sgs^{-1}\in\mathrm{H}}} \frac{1}{|\mathrm{K}|}\sum_{\substack{h\in\mathrm{H}\\ hsgs^{-1}h^{-1}\in\mathrm{K}}} \phi(hsgs^{-1}h^{-1}).\end{aligned}$$

On pose alors $hs = t$ de telle sorte que $s = h^{-1}t$, ce qui permet de réécrire la somme ci-dessus sous la forme

$$\frac{1}{|\mathrm{H}|\cdot|\mathrm{K}|}\sum_{\substack{h\in\mathrm{H},\ t\in\mathrm{G}\\ tgt^{-1}\in\mathrm{K},\ h^{-1}tgt^{-1}h\in\mathrm{H}}} \phi(tgt^{-1}).$$

Comme la condition $h^{-1}tgt^{-1}h \in \mathrm{H}$ est automatique, si $tgt^{-1} \in \mathrm{K}$ et $h \in \mathrm{H}$, la somme ci-dessus se simplifie et devient

$$\frac{1}{|\mathrm{K}|} \sum_{\substack{t \in \mathrm{G} \\ tgt^{-1} \in \mathrm{K}}} \phi(tgt^{-1}) = (\mathrm{Ind}_{\mathrm{K}}^{\mathrm{G}} \phi)(g),$$

ce qui permet de conclure.

3.4. *Les théorèmes d'Artin et de Brauer*

Théorème I.3.19. — (Artin, 1930) *Soit* G *un groupe fini, et soit* V *une représentation de* G*, alors il existe un entier non nul* d_{V}*, et une famille finie de couples* (C_i, χ_i)*, pour* $i \in \mathrm{I}$*, où* C_i *est un sous-groupe cyclique de* G*, et* $\chi_i \in \widehat{\mathrm{C}}_i$ *est un caractère linéaire de* C_i*, tels que l'on ait*

$$d_{\mathrm{V}} \chi_{\mathrm{V}} = \sum_{i \in \mathrm{I}} n_i \, \mathrm{Ind}_{\mathrm{C}_i}^{\mathrm{G}} \chi_i, \quad \textit{avec } n_i \in \mathbf{Z}\textit{, si } i \in \mathrm{I}.$$

Démonstration. — Commençons par démontrer que les $\mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \chi$, où C décrit les sous-groupes cycliques de G, et χ les éléments de $\widehat{\mathrm{C}}$, forment une famille génératrice de $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$. Dans le cas contraire, il existe $\phi \in \mathrm{R}_{\mathbf{C}}(\mathrm{G})$ non nulle, orthogonale à tous les $\mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \chi$. En utilisant la formule de réciprocité de Frobenius, on en déduit que $\langle \phi, \chi \rangle_{\mathrm{C}} = 0$, quel que soit $\chi \in \widehat{\mathrm{C}}$. Soit alors $c \in \mathrm{G}$. Le sous-groupe C de G engendré par c est cyclique par définition. Comme un groupe cyclique est en particulier commutatif, les $\chi \in \widehat{\mathrm{C}}$ engendrent l'espace vectoriel des fonctions de C dans $\mathbf{C}$ (cor. I.2.25). Si $\phi_c : \mathrm{C} \to \mathbf{C}$ est la fonction valant 1 en c, et 0 ailleurs, on a donc $0 = \langle \phi, \phi_c \rangle_{\mathrm{C}} = \frac{1}{|\mathrm{C}|} \overline{\phi(c)}$, et donc $\phi(c) = 0$. On en déduit le fait que ϕ est identiquement nulle, ce qui permet de prouver notre affirmation selon laquelle les $\mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \chi$ forment une famille génératrice de $\mathrm{R}_{\mathbf{C}}(\mathrm{G})$.

Extrayons-en une base $e_i = \mathrm{Ind}_{\mathrm{C}_i}^{\mathrm{G}} \chi_i$, pour $i \in \mathrm{I}$. Si $\chi \in \mathrm{Irr}(\mathrm{G})$, on a $\langle \chi, e_i \rangle \in \mathbf{N}$, puisque $\langle \chi, e_i \rangle$ est la multiplicité de la représentation correspondant à χ dans la décomposition de $\mathrm{Ind}_{\mathrm{C}_i}^{\mathrm{G}} \chi_i$ en représentations irréductibles. De plus, $e_i = \sum_{\chi \in \mathrm{Irr}(\mathrm{G})} \langle \chi, e_i \rangle \, \chi$. La matrice de passage de la base des e_i, pour $i \in \mathrm{I}$, à celle des χ, pour $\chi \in \mathrm{Irr}(\mathrm{G})$, est donc à coefficients rationnels, et comme χ_{V} a, pour la même raison que précédemment, des coordonnées entières dans la base des χ, pour $\chi \in \mathrm{Irr}(\mathrm{G})$, cela implique que χ_{V} a des coordonnées rationnelles dans la base des e_i, pour $i \in \mathrm{I}$. Il suffit alors de prendre pour d_{V} le p.p.c.m. des dénominateurs des coordonnées de χ_{V} dans la base des e_i, pour $i \in \mathrm{I}$, pour obtenir la décomposition voulue. Ceci permet de conclure.

Théorème I.3.20. — (R. Brauer, 1947) *Soit* G *un groupe fini, et soit* V *une représentation de* G*, alors il existe une famille finie de couples* (H_i, χ_i)*, pour* $i \in \mathrm{I}$*, où* H_i *est un sous-groupe de* G*, et* $\chi_i \in \widehat{\mathrm{H}}_i$ *est un caractère linéaire de* H_i*, tels que l'on ait*

$$\chi_{\mathrm{V}} = \sum_{i \in \mathrm{I}} n_i \, \mathrm{Ind}_{\mathrm{H}_i}^{\mathrm{G}} \chi_i, \quad \textit{avec } n_i \in \mathbf{Z}\textit{, si } i \in \mathrm{I}.$$

La principale différence avec le théorème d'Artin est la disparition de l'entier d_{V}, ce qui a des conséquences assez remarquables (une de ces conséquences est évoquée au n° 3 du § G.1). L'autre différence est que l'on ne peut pas se restreindre aux groupes cycliques (R. Brauer montre que l'on peut se restreindre aux *groupes élémentaires* : un groupe fini H est dit élémentaire s'il existe un nombre premier p tel que H soit le produit d'un p-groupe (un groupe d'ordre une puissance de p) par un groupe cyclique d'ordre premier à p). La démonstration demande d'utiliser des propriétés d'intégralité des $\chi_{\mathrm{V}}(g)$, et déborde un peu du cadre de ce cours. Signalons que ces propriétés d'intégralité permettent aussi de démontrer le résultat suivant.

Proposition I.3.21. — *Si* G *est un groupe fini et si* V *est une représentation irréductible de* G, *alors* $\dim \mathrm{V}$ *divise* $|\mathrm{G}|$.

4. Exercices

4.1. *Tables de caractères*

On rappelle que S_n (resp. A_n) désigne le groupe symétrique (resp. alterné), cf. n° 3.4 du Vocabulaire.

Exercice I.3.22. — Soit n un entier $\geqslant 1$. Quelles sont les représentations irréductibles de $\mathbf{Z}/n\mathbf{Z}$?

Exercice I.3.23. — Soit G un groupe non commutatif d'ordre 6.

(i) Quels sont les ordres des éléments de G ?

(ii) Montrer que G a deux caractères irréductibles de degré 1 (notés $\mathbf{1}$ et η) et un de degré 2 (noté χ).

(iii) Montrer que G a 3 classes de conjugaison ; quelles sont-elles ?

(iv) Montrer que $\eta(g) = 1$, si g est d'ordre 3, et que $\eta(g) = -1$, si g est d'ordre 2 (on s'intéressera à $\eta(g^2)$). En déduire le cardinal de chaque classe de conjugaison.

(v) Dresser la table des caractères de G.

Exercice I.3.24. — (i) Montrer qu'un groupe non commutatif d'ordre 8 a quatre représentations irréductibles de dimension 1 et une de dimension 2.

(ii) Soit D_4 le groupe des symétries du carré. Montrer que D_4 est d'ordre 8, et dresser la table des caractères de D_4.

(iii) Soit H_4 le groupe des quaternions. C'est l'ensemble des $\left(\begin{smallmatrix} a & -\bar{b} \\ b & \bar{a} \end{smallmatrix}\right)$, avec $\{a, b\} \subset \{0, 1, -1, i, -i\}$, et $a = 0$ ou $b = 0$. Montrer que H_4 est un groupe d'ordre 8 non isomorphe à D_4, et dresser sa table de caractères.

Exercice I.3.25. — On fait agir S_n sur $\mathbf{C}^n$ par permutation des éléments de la base canonique. Montrer que l'hyperplan $\sum_{i=1}^n x_i = 0$ est stable par S_n et que la représentation ainsi obtenue est irréductible (considérer $v - \sigma \cdot v$, où σ est une transposition). En déduire une décomposition de $\mathbf{C}^n$ en somme de représentations irréductibles de S_n.

Exercice I.3.26. — (o) Quelles sont les classes de conjugaison de S_4 ?

(i) Montrer que $\mathrm{C} = \{1, (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe distingué de S_4 et $\mathrm{S}_4/\mathrm{C} = \mathrm{S}_3$. (On pourra faire agir S_4 sur $\mathrm{C} - \{1\}$ par conjugaison.)

(ii) En déduire une représentation irréductible de S_4 de dimension 2 et deux de dimension 1.

(iii) On fait agir S_4 sur $\mathbf{C}^4$ par permutation des éléments de la base canonique. Montrer que l'hyperplan $\mathrm{V} = \{x_1 + x_2 + x_3 + x_4 = 0\}$ est stable par S_4, et calculer le caractère χ_{V}.

(iv) Montrer que V est irréductible, non isomorphe à $\mathrm{V} \otimes \mathrm{sign}$. En déduire la table des caractères de S_4.

Exercice I.3.27. — (o) Montrer que S_5 a 7 classes de conjugaison, et calculer le cardinal de chaque classe.

(i) On note U la représentation de S_5 sur l'hyperplan $\sum_{i=1}^5 x_i = 0$ de $\mathbf{C}^5$. Calculer χ_{U}, et montrer que U et $\mathrm{U} \otimes \mathrm{sign}$ sont irréductibles non isomorphes.

(ii) Calculer $\chi_{\wedge^2\mathrm{U}}$ et montrer que $\wedge^2\mathrm{U}$ est irréductible.

(iii) Calculer $\chi_{\mathrm{Sym}^2\mathrm{U}}$ et montrer que $\mathrm{Sym}^2\mathrm{U} = \mathbf{1} \oplus \mathrm{U} \oplus \mathrm{V}$, où V est irréductible.

(iv) Dresser la table des caractères de S_5.

Exercice I.3.28. — Soit $n \geqslant 3$, et soient D_n le groupe des symétries d'un polygone régulier à n sommets et $\mathrm{C}_n \subset \mathrm{D}_n$ le sous-groupe des rotations.

(i) Montrer que C_n est un groupe cyclique d'indice 2 dans D_n. Montrer que, si n est pair (resp. impair), les symétries forment deux (resp. une) classes de conjugaison, et les rotations $\frac{n}{2} + 1$ (resp. $\frac{n+1}{2}$).

(ii) Montrer que, si on identifie la rotation d'angle α avec la multiplication par $e^{i\alpha}$ dans le plan complexe, les représentations irréductibles de C_n sont les χ_a, pour $a \in \mathbf{Z}/n\mathbf{Z}$, définies par $\chi_a(e^{i\alpha}) = e^{a\,i\alpha}$.

(iii) Si $a \in \mathbf{Z}/n\mathbf{Z}$, calculer le caractère ϕ_a de $\mathrm{Ind}_{\mathrm{C}_n}^{\mathrm{D}_n}\chi_a$.

(iv) Calculer $\langle \phi_a, \phi_a \rangle$; en déduire dans quel cas $\mathrm{Ind}_{\mathrm{C}_n}^{\mathrm{D}_n}\chi_a$ est irréductible.

(v) Dresser la table des caractères de D_n.

4.2. *Exercices plus théoriques*

Exercice I.3.29. — Soit G un sous-groupe fini de $\mathbf{GL}_n(\mathbf{C})$. Montrer que $\sum_{\mathrm{M}\in\mathrm{G}} \mathrm{Tr}(\mathrm{M})$ est un entier. Comment cet entier s'interprète-t-il ?

Exercice I.3.30. — (i) Si $\sigma \in \mathrm{S}_n$, soit $f(\sigma)$ le nombre de points fixes de la permutation σ. Montrer que $\sum_{\sigma\in\mathrm{S}_n} f(\sigma)^2 = 2n!$. (Utiliser l'ex. I.3.25.)

(ii) Quel est le nombre moyen de points fixes d'un élément de S_n ?

Exercice I.3.31. — Si N est un entier $\geqslant 1$, on note $\boldsymbol{\mu}_{\mathrm{N}}$ l'ensemble des racines N-ièmes de l'unité et $\boldsymbol{\mu}_{\mathrm{N}}^* \subset \boldsymbol{\mu}_{\mathrm{N}}$ l'ensemble des racines primitives, et on pose $\mathrm{S}(\mathrm{N}) = \sum_{\eta\in\boldsymbol{\mu}_{\mathrm{N}}} \eta$ et $\mathrm{S}^*(\mathrm{N}) = \sum_{\eta\in\boldsymbol{\mu}_{\mathrm{N}}^*} \eta$.

(i) Décrire $\boldsymbol{\mu}_{\mathrm{N}}^*$ à partir des $\boldsymbol{\mu}_{\mathrm{N}/d}$, pour d divisant N. En déduire que $\mathrm{S}^*(\mathrm{N}) = \sum_{d|\mathrm{N}} \mu(d)\mathrm{S}(\mathrm{N}/d)$, où $\mu : \mathbf{N} - \{0\} \to \{-1, 0, 1\}$ est la fonction de Moebius définie par $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et $\mu(n) = (-1)^r$ si n est le produit de r nombres premiers distincts.

(ii) Montrer que $\mathrm{S}^*(\mathrm{N}) \in \mathbf{Z}$, pour $\mathrm{N} \geqslant 1$.

(iii) Soit V une représentation de S_n, et soit $g \in \mathrm{S}_n$ d'ordre N. Montrer que l'ensemble des valeurs propres de $\rho_{\mathrm{V}}(g)$ (avec multiplicité) est stable par $\lambda \mapsto \lambda^k$, pour tout entier k premier à N. (On s'intéressera à la décomposition de g^k en cycles.)

(iv) En déduire que les caractères de S_n prennent des valeurs entières.

(v) Soit χ un caractère irréductible de S_n distinct du caractère trivial et de la signature. Montrer que $\chi(1) \neq 1$ et en déduire qu'il existe $g \in \mathrm{G}$ tel que $\chi(g) = 0$. (On calculera $\langle \chi, \chi \rangle$.)

Dans tous les exercices qui suivent, G est un groupe fini.

Exercice I.3.32. — On suppose que G *agit 2-transitivement* sur X (cela signifie que, pour tous couples (x, x') et (y, y') d'éléments de X avec $x \neq x'$ et $y \neq y'$, il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ et $g \cdot x' = y'$).

(i) Montrer que le stabilisateur G_y de $y \in \mathrm{X}$ agit transitivement sur $\mathrm{X} - \{y\}$.

(ii) Montrer que l'hyperplan $\mathrm{W} = \{\sum_{x\in\mathrm{X}} \lambda_x e_x,\ \sum_{x\in\mathrm{X}} \lambda_x = 0\}$ de V_{X} est une représentation irréductible de G. (Si $v = \sum_{x\in\mathrm{X}} \lambda_x e_x \in \mathrm{W}$, et si $y \in \mathrm{X}$ on pourra s'intéresser à $\frac{1}{|\mathrm{G}_y|} \sum_{g\in\mathrm{G}_y} g \cdot v$.)

(ii) Retrouver le résultat de l'ex. I.3.25.

Exercice I.3.33. — Si χ est le caractère d'une représentation de G, soit $\mathrm{K}_\chi = \{g \in \mathrm{G},\ \chi(g) = \chi(1)\}$.

(i) Montrer que K_χ est un sous-groupe distingué de G.

(ii) Montrer que G est simple si et seulement si $K_\chi = \{1\}$, pour tout $\chi \in \mathrm{Irr}(G) - \{1\}$. Comment peut-on lire la simplicité d'un groupe fini sur sa table des caractères ?

Exercice I.3.34. — Soit V une représentation *fidèle* de G (i.e. $\rho_V(g) \neq 1$ si $g \neq 1$).

(i) Montrer que $\chi_V(g) \neq \dim V$, si $g \neq 1$.

(ii) Soit W une représentation irréductible de G. Montrer que $\sum_{n=0}^{+\infty} \langle \chi_W, \chi_V^n \rangle \, T^n$ est une fraction rationnelle que l'on explicitera, mais n'est pas un polynôme.

(iii) En déduire que W apparaît dans la décomposition en représentations irréductibles d'une infinité de $\otimes^n V$.

Exercice I.3.35. — Soit $H \neq G$ un sous-groupe de G, et soit V la représentation de permutation associée à l'action de G sur G/H.

(i) Montrer que $V = \mathrm{Ind}_H^G \mathbf{1}$. En déduire que $\sum_{g \in G} \chi_V(g) = |G|$.

(ii) Montrer que V n'est pas irréductible ; en déduire que $\frac{1}{|G|} \sum_{g \in G} \chi_V(g)^2 \geqslant 2$. (On remarquera que χ_V est à valeurs réelles.)

(iii) Soit Y l'ensemble des $g \in G$ vérifiant $\chi_V(g) = 0$. Montrer que

$$\sum_{g \in G} (\chi_V(g) - 1)(\chi_V(g) - |G/H|) \leqslant |G/H| \cdot |Y|.$$

(iv) En déduire que $|Y| \geqslant |H|$.

(v) Soit X, avec $|X| \geqslant 2$, un ensemble sur lequel G agit *transitivement* (i.e., quels que soient $x, y \in X$, il existe $g \in G$, tel que $y = g \cdot x$). Montrer que la proportion des $g \in G$ agissant sans point fixe sur X est supérieure [10] ou égale à $1/|X|$.

Exercice I.3.36. — Soient G_1, G_2 deux groupes finis, et soit $G = G_1 \times G_2$.

(i) Montrer que, si V_1 et V_2 sont des représentations irréductibles de G_1 et G_2, alors $V_1 \boxtimes V_2$ (cf. rem. I.3.6) est une représentation irréductible de G.

(ii) Montrer que toute représentation irréductible de G est obtenue de cette manière.

Exercice I.3.37. — (i) Si $\sigma \in S_n$, soit M_σ la matrice de l'isomorphisme u_σ de $\mathbf{C}^n$, envoyant l'élément e_i de la base canonique sur $e_{\sigma(i)}$. Quelles sont, en fonction de la décomposition de σ en cycles, les valeurs propres de M_σ (avec multiplicité). En déduire que, si M_σ et M_τ sont semblables, alors σ et τ ont le même nombre de points fixes.

(ii) Montrer que la matrice T_G, définie par la table des caractères de G, est inversible.

(iii) Montrer que, si $C \in \mathrm{Conj}(G)$, alors $C^{-1} = \{g^{-1},\ g \in C\}$ appartient à Conj(G), et que, si $\chi \in \mathrm{Irr}(G)$, alors $\chi(C^{-1}) = \overline{\chi(C)}$.

(iv) Montrer que le nombre de classes de conjugaison symétriques de G (i.e. vérifiant $C = C^{-1}$) est égal au nombre de caractères irréductibles réels de G (i.e $\chi(C) \in \mathbf{R}$, pour tout $C \in \mathrm{Conj}(G)$).

10. En théorie algébrique des nombres, ce résultat de Jordan permet de montrer que si $P \in \mathbf{Z}[T]$, de degré $\geqslant 2$, est irréductible dans $\mathbf{Q}[T]$, alors il existe une infinité de nombres premiers p tels que P n'ait aucune solution dans $\mathbf{F}_p$.

CHAPITRE II

ESPACES DE BANACH

La théorie des espaces vectoriels normés complets (appelés « espaces de Banach » en raison du rôle joué par ce dernier dans sa mise en forme) est issue des travaux du 19-ième siècle sur les équations différentielles, les équations aux dérivées partielles ou les équations intégrales du type $u(x) + \int_a^b \mathrm{K}(x,y)u(y)\,dy = f(x)$, où u est une fonction inconnue. Il s'est écoulé une vingtaine d'années entre l'introduction par D. Hilbert (1906) de l'espace qui porte son nom (l'espace ℓ^2 des suites de carré sommable), la réalisation l'année suivante, par E. Fischer et F. Riesz, de ce que l'espace des fonctions de carré sommable lui était isomorphe, et la forme définitive de la théorie par l'école polonaise (S. Banach, H. Hahn, H. Steinhaus). En retour, cette théorie a permis de nombreuses avancées sur les problèmes qui l'ont motivée. Le problème de la classification des espaces de Banach est toujours d'actualité [1].

II.1. Espaces de Banach

Dans tout ce qui suit, $\mathbf{K}$ désigne soit le corps $\mathbf{R}$ des nombres réels [2], soit le corps $\mathbf{C}$ des nombres complexes, et « espace vectoriel » est une abréviation pour « espace vectoriel sur $\mathbf{K}$ ». Le lecteur est renvoyé au § 17 du Vocabulaire pour le vocabulaire et les propriétés élémentaires des espaces vectoriels normés.

1. Convergence normale, séries sommables

Soit $(\mathrm{E}, \|\ \|)$ un espace vectoriel normé. On rappelle que, si $x \in \mathrm{E}$ et si $r \in \mathbf{R}_+$, on

1. Un problème qui est resté ouvert pendant longtemps était de savoir si un endomorphisme continu d'un $\mathbf{C}$-espace de Banach possède toujours un sous-espace fermé invariant (c'est le cas en dimension finie $\geqslant 2$). Un contrexemple a été construit par P. Enflo vers 1981, et C. Read (1984) en a construit un dans l'espace ℓ^1 des suites sommables, mais on ne sait pas s'il existe des contrexemples dans ℓ^2 ou, plus généralement, dans des espaces réflexifs (isomorphes au dual de leur dual), ce que ℓ^1 n'est pas.

2. Ou, plus généralement, un corps K, complet pour une norme (cf. n° 17.1 du Vocabulaire). Le seul énoncé qui ne s'étend pas toujours est le th. de Hahn-Banach (th. II.1.29), que nous ne démontrerons pas.

note $\mathrm{B}(x,r)$ ou $\mathrm{B}_{\mathrm{E}}(x,r)$ (resp. $\mathrm{B}(x,r^-)$ ou $\mathrm{B}_{\mathrm{E}}(x,r^-)$) la boule fermée (resp. ouverte) de centre x et de rayon r.

Une série $\sum_{n\in\mathbf{N}} u_n$ d'éléments de E est *normalement convergente*, si $\sum_{n\in\mathbf{N}} \|u_n\| < +\infty$.

Un espace vectoriel normé $(\mathrm{E}, \|\ \|)$, qui est complet (pour la distance associée à la norme), est appelé un *espace de Banach*. D'après le n° 14.1 du Vocabulaire, $(\mathrm{E}, \|\ \|)$ est un espace de Banach si et seulement si toute série normalement convergente converge dans E. Comme un sous-espace fermé d'un espace complet est complet, un sous-espace vectoriel fermé d'un espace de Banach est un espace de Banach.

Les exemples les plus simples d'espaces de Banach sont les espaces de dimension finie, mais ceux-ci ont des propriétés très spéciales. On a en particulier les résultats classiques suivants (cf. n$^{\mathrm{os}}$ 17.4 et 17.6 du Vocabulaire).

Proposition II.1.1. — (i) *Si* V *est un espace vectoriel de dimension finie, alors toutes les normes sur* V *sont équivalentes et* V *est complet pour n'importe laquelle d'entre elles.*

(ii) *Soit* E *un espace de Banach. La boule unité fermée* $\mathrm{B}(0,1)$ *est compacte si et seulement si* E *est de dimension finie.*

Remarque II.1.2. — Insistons sur le fait que le (i) de la prop. II.1.1 devient *totalement faux en dimension infinie* : les normes sur un espace E de dimension infinie ne sont pas toutes équivalentes, et E peut être complet pour certaines d'entre elles, mais il y en a "beaucoup plus" pour lesquelles ce n'est pas le cas.

Un espace est dit *séparable* s'il contient un sous-ensemble dénombrable dense [3] (i.e. s'il est « pas trop gros »).

Exercice II.1.3. — (i) Montrer qu'un espace vectoriel de dimension finie est séparable.

(ii) Montrer qu'un sous-espace d'un espace séparable est un espace séparable.

Soit E un espace de Banach. Une série $\sum_{i\in\mathrm{I}} x_i$, avec I dénombrable, est dite *sommable* si elle vérifie le critère de Cauchy non ordonné suivant : pour tout $\varepsilon > 0$, il existe $\mathrm{I}(\varepsilon) \subset \mathrm{I}$ fini, tel que pour tout $\mathrm{J} \subset \mathrm{I}$ fini avec $\mathrm{J} \cap \mathrm{I}(\varepsilon) = \varnothing$, on ait $\| \sum_{i\in\mathrm{J}} x_i\| \leqslant \varepsilon$.

• Si I est fini, toute série $\sum_{i\in\mathrm{I}} x_i$ est sommable.

• Si I est infini, si $\sum_{i\in\mathrm{I}} x_i$ est sommable, alors pour toute bijection $n \mapsto i(n)$ de $\mathbf{N}$ sur I, les sommes partielles de la série $\sum_{n=0}^{+\infty} x_{i(n)}$ vérifient le critère de Cauchy usuel, et comme E est complet, la série converge et la limite ne dépend pas du choix de la bijection $n \mapsto i(n)$; c'est la somme de la série $\sum_{i\in\mathrm{I}} x_i$.

La sommabilité et la convergence normale sont des notions assez proches. L'exercice ci-dessous (dans lequel on s'intéresse aux séries $\sum_{i\in\mathrm{I}} x_i$, où I est un ensemble dénombrable infini) explore leurs liens.

3. La plupart des espaces de Banach de l'analyse fonctionnelle sont séparables ; une exception notable étant l'espace $\mathscr{C}_b(\mathbf{R})$ des fonctions continues bornées sur $\mathbf{R}$ (cf. Ex. II.1.7) ou l'espace ℓ^∞ des suites bornées.

Exercice II.1.4. — (i) Montrer qu'une série normalement convergente est sommable.

(ii) Montrer que dans $\mathbf{R}$ une série est sommable si et seulement si elle est absolument convergente.

(iii) En déduire que dans un espace vectoriel normé, de dimension finie sur $\mathbf{R}$ ou $\mathbf{C}$, une série est sommable si et seulement si elle est normalement convergente.

(iv) Soit I dénombrable (les espaces $\ell^2(\mathrm{I})$ et $\ell^\infty(\mathrm{I})$ sont définis ci-dessous) et, si $i \in \mathrm{I}$, soit e_i la suite $(e_{i,j})_{j\in\mathrm{I}}$ d'éléments de $\mathbf{C}$, définie par $e_{i,i} = 1$ et $e_{i,j} = 0$, si $i \neq j$.

(a) Montrer que $\sum_{i\in\mathrm{I}} a_i e_i$ est sommable dans $\ell^\infty(\mathrm{I})$ si et seulement si la suite $(a_i)_{i\in\mathrm{I}}$ tend vers 0 à l'infini (pour tout $\varepsilon > 0$, il existe $\mathrm{I}(\varepsilon) \subset \mathrm{I}$ fini tel que $|a_i| \leqslant \varepsilon$, si $i \notin \mathrm{I}(\varepsilon)$).

(b) Montrer que $\sum_{i\in\mathrm{I}} a_i e_i$ est sommable dans $\ell^2(\mathrm{I})$ si et seulement si $\sum_{i\in\mathrm{I}} |a_i|^2 < +\infty$.

(c) Quelle est la somme dans ces deux cas ?

2. Espaces de suites

Exemple II.1.5. — (i) On note ℓ^∞ l'ensemble des suites bornées $(x_n)_{n\in\mathbf{N}}$. Muni de la norme $\| \ \|_\infty$ définie par $\|(x_n)_{n\in\mathbf{N}}\|_\infty = \sup_{n\in\mathbf{N}} |x_n|$, l'espace ℓ^∞ est un espace de Banach. L'espace ℓ_0^∞, sous-espace de ℓ^∞ des suites tendant vers 0 quand n tend vers $+\infty$ est un sous-espace fermé de ℓ^∞, et donc aussi un Banach.

(ii) On note ℓ^1 l'ensemble des suites $(x_n)_{n\in\mathbf{N}}$, telles que $\sum_{n\in\mathbf{N}} |x_n| < +\infty$. Muni de la norme $\| \ \|_1$ définie par $\|(x_n)_{n\in\mathbf{N}}\|_1 = \sum_{n\in\mathbf{N}} |x_n|$, l'espace ℓ^1 est un espace de Banach.

(iii) On note ℓ^2 l'ensemble des suites $(x_n)_{n\in\mathbf{N}}$, telles que $\sum_{n\in\mathbf{N}} |x_n|^2 < +\infty$. Muni de la norme $\| \ \|_2$ définie par $\|(x_n)_{n\in\mathbf{N}}\|_2 = \left(\sum_{n\in\mathbf{N}} |x_n|^2\right)^{1/2}$, l'espace ℓ^2 est un espace de Banach [4].

(iv) Si I est un ensemble dénombrable infini, on définit de même les espaces $\ell^\infty(\mathrm{I})$, $\ell_0^\infty(\mathrm{I})$, $\ell^1(\mathrm{I})$ et $\ell^2(\mathrm{I})$; ce sont aussi des espaces de Banach.

Démonstration. — Le cas I dénombrable se déduit du cas de $\mathbf{N}$ en choisissant une bijection entre I et $\mathbf{N}$; il suffit donc de démontrer les (i), (ii) et (iii). Soit E un des espaces ℓ^∞, ℓ^1 ou ℓ^2, et soit $\| \ \|$ la norme correspondante. Pour prouver que E est un espace de Banach, il s'agit de vérifier que toute série normalement convergente d'éléments de E admet une limite dans E. Soit donc $(x^{(k)})_{k\in\mathbf{N}}$ une suite d'éléments de E vérifiant $\sum_{k\in\mathbf{N}} \|x^{(k)}\| < +\infty$. Chaque $x^{(k)}$ est une suite $(x_n^{(k)})_{n\in\mathbf{N}}$ d'éléments de $\mathbf{K}$, et dans les trois cas, $|x_n^{(k)}| \leqslant \|x^{(k)}\|$ pour tout $n \in \mathbf{N}$, ce qui fait que, quel que soit $n \in \mathbf{N}$, la série $\sum_{k\in\mathbf{N}} x_n^{(k)}$ est normalement convergente dans $\mathbf{K}$, et donc converge dans $\mathbf{K}$ (puisque $\mathbf{K}$ est complet) ; nous noterons y_n la somme de cette série et y la suite $(y_n)_{n\in\mathbf{N}}$. Pour conclure, il suffit de vérifier que $\|y\| \leqslant \sum_{k\in\mathbf{N}} \|x^{(k)}\|$: en effet, ceci prouve que $y \in \mathrm{E}$, que $\|y - \sum_{i\leqslant k} x^{(i)}\| \leqslant \sum_{i\geqslant k+1} \|x^{(i)}\|$ tend vers 0 quand $k \to +\infty$, puisque majoré par le reste d'une série convergente, et donc que y est somme de la série $\sum_{k\in\mathbf{N}} x^{(k)}$ dans E.

• Si $\mathrm{E} = \ell^\infty$, on a $|y_n| \leqslant \sum_{k\in\mathbf{N}} |x_n^{(k)}| \leqslant \sum_{k\in\mathbf{N}} \|x^{(k)}\|_\infty$, et donc $\|y\|_\infty \leqslant \sum_{k\in\mathbf{N}} \|x^{(k)}\|_\infty$. Pour la fermeture de ℓ_0^∞ dans ℓ^∞, cf. Vocabulaire, ex. 16.2.

4. Comme la norme $\| \ \|_2$ est définie par un produit scalaire, c'est même un espace de Hilbert.

• Si $\mathrm{E} = \ell^1$, on a $|y_n| \leqslant \sum_{k\in\mathbf{N}} |x_n^{(k)}|$, et donc

$$\|y\|_1 = \sum_{n\in\mathbf{N}} |y_n| \leqslant \sum_{n\in\mathbf{N}} \sum_{k\in\mathbf{N}} |x_n^{(k)}| = \sum_{k\in\mathbf{N}} \sum_{n\in\mathbf{N}} |x_n^{(k)}| = \sum_{k\in\mathbf{N}} \|x^{(k)}\|_1.$$

• Si $\mathrm{E} = \ell^2$, on a

$$\begin{aligned}\sum_{n\in\mathbf{N}} |y_n|^2 &\leqslant \sum_{n\in\mathbf{N}} \big(\sum_{k\in\mathbf{N}} |x_n^{(k)}|\big)^2 = \sum_{n\in\mathbf{N}} \sum_{k_1,k_2\in\mathbf{N}} |x_n^{(k_1)}|\,|x_n^{(k_2)}| \\ &= \sum_{k_1,k_2\in\mathbf{N}} \sum_{n\in\mathbf{N}} |x_n^{(k_1)}|\,|x_n^{(k_2)}| = \sum_{k_1,k_2\in\mathbf{N}} \big\langle |x^{(k_1)}|, |x^{(k_2)}| \big\rangle \\ &\leqslant \sum_{k_1,k_2\in\mathbf{N}} \|x^{(k_1)}\|_2\,\|x^{(k_2)}\|_2 = \big(\sum_{k\in\mathbf{N}} \|x^{(k)}\|_2\big)^2\end{aligned}$$

où l'on a utilisé le fait que l'on pouvait réordonner les termes comme on le voulait dans une série à termes positifs, la notation $|x^{(k)}|$ pour désigner la suite $(|x_n^{(k)}|)_{n\in\mathbf{N}}$, et l'inégalité de Cauchy-Schwarz (cf. n° 18 du Vocabulaire). On en déduit que $\|y\|_2 \leqslant \sum_{k\in\mathbf{N}} \|x^{(k)}\|_2$.

Ceci permet de conclure.

3. Espaces de fonctions continues

Si X est un espace topologique, on note $\mathscr{C}(\mathrm{X})$ l'espace des fonctions continues de X dans $\mathbf{C}$.

Exemple II.1.6. — (i) Si X est un espace métrique (ou plus généralement un espace topologique), on peut munir l'espace $\mathscr{C}_b(\mathrm{X})$ des fonctions continues bornées de X dans $\mathbf{C}$ de la norme $\|\ \|_\infty$ de la *convergence uniforme* définie par $\|\phi\|_\infty = \sup_{x\in\mathrm{X}} |\phi(x)|$. Alors $(\mathscr{C}_b(\mathrm{X}), \|\ \|_\infty)$ est un espace de Banach. En effet, la complétude de $\mathscr{C}_b(\mathrm{X})$ est une traduction de ce qu'une limite uniforme de fonctions continues est continue (cf. n° 16.2 du Vocabulaire).

(ii) On note $\mathscr{C}_c(\mathrm{X})$ l'espace des fonctions continues sur X, nulles en dehors d'un compact (le « c » en indice signifie « *à support compact* »). Comme une fonction continue sur un compact a une image compacte et donc bornée, on a $\mathscr{C}_c(\mathrm{X}) \subset \mathscr{C}_b(\mathrm{X})$, et cette inclusion est stricte sauf si X est compact auquel cas $\mathscr{C}_c(\mathrm{X}) = \mathscr{C}_b(\mathrm{X}) = \mathscr{C}(\mathrm{X})$. On note $\mathscr{C}_0(\mathrm{X})$ l'adhérence de $\mathscr{C}_c(\mathrm{X})$ dans $\mathscr{C}_b(\mathrm{X})$; c'est l'espace des fonctions continues sur X *tendant vers* 0 *à l'infini*.

(iii) Plus généralement, si W est un $\mathbf{K}$-espace vectoriel de dimension finie muni d'une norme $\|\ \|$, l'espace $\mathscr{C}_b(\mathrm{X}, \mathrm{W})$ des fonctions continues bornées de X dans W, muni de la norme $\|\ \|_\infty$ définie par $\|\phi\|_\infty = \sup_{x\in\mathrm{X}} \|\phi(x)\|$, est un espace de Banach. En effet, changer la norme sur W revient à changer la norme $\|\ \|_\infty$ sur $\mathscr{C}_b(\mathrm{X}, \mathrm{W})$ en une norme équivalente puisque toutes les normes sont équivalentes sur W ; on peut donc choisir une base $e_1, \ldots, e_n$ de W, et supposer que $\|\ \|$ est donnée par $\|x_1e_1 + \cdots + x_ne_n\| = \sup_{1\leqslant i\leqslant n} |x_i|$. Alors tout $\phi \in \mathscr{C}_b(\mathrm{X}, \mathrm{W})$ peut s'écrire, de manière unique, sous la forme $\phi = \sum_{i=1}^n \phi_i e_i$

avec $\phi_i \in \mathscr{C}_b(\mathrm{X}, \mathbf{K})$, et $\phi \mapsto (\phi_1, \dots, \phi_n)$ est une isométrie de $\mathscr{C}_b(\mathrm{X}, \mathrm{W})$ sur $(\mathscr{C}_b(\mathrm{X}, \mathbf{K}))^n$, qui est complet puisqu'un produit d'espaces complets est complet.

Exercice II.1.7. — Si $\lambda \in \mathbf{R}$, on note e_λ la fonction $t \mapsto e^{2i\pi\lambda t}$.
(i) Montrer que $e_\lambda \in \mathscr{C}_b(\mathbf{R})$, et que $\|e_\lambda - e_\mu\|_\infty = 2$ si $\lambda \neq \mu$.
(ii) En déduire que $\mathscr{C}_b(\mathbf{R})$ n'est pas séparable.

Théorème II.1.8. — (de Stone-Weierstrass, Stone (1948)) *Si* X *est un espace compact, et si $\mathscr{A}$ est une sous-algèbre de $\mathscr{C}(\mathrm{X})$ qui contient les fonctions constantes, sépare les points, et est stable par $f \mapsto \overline{f}$, alors $\mathscr{A}$ est dense dans $\mathscr{C}(\mathrm{X})$.*

Démonstration. — Avant de faire la démonstration de cet important théorème, explicitons la condition « $\mathscr{A}$ sépare les points » : elle signifie que, si $x \neq y$, on peut trouver $f \in \mathscr{A}$, avec $f(x) \neq f(y)$.

Maintenant, quitte à remplacer $\mathscr{A}$ par son adhérence dans $\mathscr{C}(\mathrm{X})$, qui est encore une algèbre vérifiant les conditions du théorème, on peut supposer que $\mathscr{A}$ est complète et on doit démontrer qu'alors $\mathscr{A} = \mathscr{C}(\mathrm{X})$.

Soit $\mathscr{A}_{\mathbf{R}} = \mathscr{A} \cap \mathscr{C}(\mathrm{X}, \mathbf{R})$. C'est une sous-algèbre fermée (et donc complète) de $\mathscr{C}(\mathrm{X}, \mathbf{R})$, ensemble des fonctions continues sur X, à valeurs dans $\mathbf{R}$, et la condition « $\mathscr{A}$ est stable par $f \mapsto \overline{f}$ » entraîne que $\mathscr{A}_{\mathbf{R}}$ sépare les points puisque $\mathscr{A}_{\mathbf{R}}$ contient $\mathrm{Re}(f) = \frac{1}{2}(f + \overline{f})$ et $\mathrm{Im}(f) = \frac{1}{2i}(f - \overline{f})$, si $f \in \mathscr{A}$. Comme $\mathscr{C}(\mathrm{X}) = \mathscr{C}(\mathrm{X}, \mathbf{R}) + i\mathscr{C}(\mathrm{X}, \mathbf{R})$, il suffit de prouver que $\mathscr{A}_{\mathbf{R}} = \mathscr{C}(\mathrm{X}, \mathbf{R})$. Nous aurons besoin du lemme suivant.

Lemme II.1.9. — *Il existe une suite $(\mathrm{P}_n(t))_{n\in\mathbf{N}}$ de polynômes à coefficients réels tendant vers $|t|$ uniformément sur $[-1, 1]$.*

Démonstration. — La formule de Taylor avec reste intégral

$$f(x) = f(0) + xf'(0) + \cdots + \frac{x^n}{n!}f^{(n)}(0) + \frac{x^{n+1}}{n!}\int_0^1 (1-t)^n f^{(n+1)}(tx)\,dt$$

permet de montrer que, si $\alpha > 0$, la série $\sum_{n=0}^{+\infty} \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}x^n$ tend vers $(1+x)^\alpha$ uniformément sur $x \in [-1, 1]$. En particulier, pour $\alpha = \frac{1}{2}$ et $x = t^2 - 1$, les sommes partielles de cette série fournissent une suite de polynômes tendant, uniformément sur $[-1, 1]$, vers $(1 + t^2 - 1)^{1/2} = |t|$.

Revenons à la démonstration du théorème.

• Si $f \in \mathscr{A}_{\mathbf{R}}$, il existe $a \in \mathbf{R}_+^*$ tel que f prenne ses valeurs dans $[-a, a]$. Mais alors $a\mathrm{P}_n(a^{-1}f)$ est une suite d'éléments de $\mathscr{A}_{\mathbf{R}}$ tendant uniformément vers $|f|$, et comme $\mathscr{A}_{\mathbf{R}}$ est complète, on en déduit que, si $f \in \mathscr{A}_{\mathbf{R}}$, alors $|f| \in \mathscr{A}_{\mathbf{R}}$.

• Maintenant, si $f, g \in \mathscr{A}_{\mathbf{R}}$, on déduit de ce qui précède, que $\sup(f, g) = \frac{f+g}{2} + \frac{|f-g|}{2}$ et $\inf(f, g) = \frac{f+g}{2} - \frac{|f-g|}{2}$ appartiennent toutes les deux à $\mathscr{A}_{\mathbf{R}}$.

• Soit alors $h \in \mathscr{C}(\mathrm{X}, \mathbf{R})$. Fixons $x \in \mathrm{X}$ et $\varepsilon > 0$. Comme $\mathscr{A}_{\mathbf{R}}$ sépare les points et contient les constantes, on peut trouver, quel que soit $y \in \mathrm{X}$, une fonction $f_y \in \mathscr{A}_{\mathbf{R}}$ vérifiant $f_y(x) = h(x)$ et $f_y(y) = h(y)$. Comme $h - f_y$ est continue, il existe un ouvert U_y

contenant y tel que $|h(z) - f_y(z)| < \varepsilon$, si $z \in \mathrm{U}_y$. Comme X est compact, et comme les U_y recouvrent X, on peut trouver un sous-ensemble fini Y de X tel que $\mathrm{X} = \cup_{y\in\mathrm{Y}}\mathrm{U}_y$. Alors $g_x = \inf_{y\in\mathrm{Y}} f_y$ est un élément de $\mathscr{A}_{\mathbf{R}}$, d'après le point précédent, et g_x vérifie $g_x(x) = h(x)$ et $g_x(z) \leqslant h(z) + \varepsilon$, quel que soit $z \in \mathrm{X}$, puisque z appartient à au moins l'un des U_y, avec $y \in \mathrm{Y}$.

• Comme $g_x(x) = h(x)$ et comme g_x est continu, il existe un ouvert V_x contenant x tel que $|g_x(z) - h(z)| \leqslant \varepsilon$, si $z \in \mathrm{V}_x$. Comme ci-dessus, on peut extraire du recouvrement de X par les V_x un sous-recouvrement $(\mathrm{V}_x)_{x\in\mathrm{X}'}$, avec X′ fini. Comme ci-dessus, la fonction $g = \sup_{x\in\mathrm{X}'} g_x$ appartient à $\mathscr{A}_{\mathbf{R}}$ et vérifie $g(z) \leqslant h(z) + \varepsilon$, pour tout z, puisque cette inégalité est vérifiée par tous les g_x, et $g(z) \geqslant h(z) - \varepsilon$ puisque z appartient à au moins l'un des U_x, avec $x \in \mathrm{X}'$.

On a donc construit, quel que soit $\varepsilon > 0$, un élément g de $\mathscr{A}_{\mathbf{R}}$ vérifiant $\|g - h\|_\infty \leqslant \varepsilon$, ce qui prouve que h est dans l'adhérence de $\mathscr{A}_{\mathbf{R}}$, et donc dans $\mathscr{A}_{\mathbf{R}}$. Ceci permet de conclure.

Exemple II.1.10. — (i) Si I est un intervalle compact de $\mathbf{R}$, alors les polynômes sont denses dans $\mathscr{C}(\mathrm{I})$ (Weierstrass 1885).

(ii) Plus généralement, si K est un compact de $\mathbf{R}^m$, les polynômes (en $x_1, \dots x_m$) [5] sont denses dans $\mathscr{C}(\mathrm{K})$.

(iii) Les *polynômes trigonométriques* (i.e. les fonctions de la forme $\sum_{k\in\mathrm{I}} a_k e^{2i\pi\, kt}$, où I décrit les sous-ensembles finis de $\mathbf{Z}$) sont denses dans l'espace $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ des fonctions continues, périodiques de période 1 (Weierstrass). Ils ne sont pas denses dans $\mathscr{C}([0,1])$ car un élément de l'adhérence doit vérifier $f(0) = f(1)$, les point 0 et 1 n'étant pas séparés par les polynômes trigonométriques.

Exercice II.1.11. — Soit $h : \mathbf{R} \to \mathbf{R}$ la fonction indicatrice de $\mathbf{Q}$.

(i) Construire une suite double $f_{n,k}$ de fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$ telle que, si n est fixé, alors la suite $f_{n,k}$ tend *simplement* (i.e. $f_{n,k}(x) \to g_n(x)$, quel que soit $x \in \mathbf{R}$) vers une fonction g_n quand k tend vers $+\infty$, et la suite g_n tend simplement vers h quand n tend vers $+\infty$. (En bref, h est limite simple de limites simples de fonctions continues).

(ii) Montrer que h n'est pas une limite simple de fonctions continues. (Si h_n est une suite de fonctions continues tendant simplement vers h, construire une suite extraite $h_{\varphi(n)}$ et une suite de segments emboités $[a_n, b_n]$ tels que l'image de $[a_n, b_n]$ par $h_{\varphi(n)}$ soit incluse dans $[\frac{1}{4}, \frac{3}{4}]$ et en tirer une contradiction.)

4. Équations différentielles linéaires

4.1. *Le théorème de Cauchy-Lipshitz*

Soit V un $\mathbf{K}$-espace vectoriel de dimension finie. On munit V d'une norme $\|\ \|$ et $\mathrm{End}(\mathrm{V})$ de la norme d'opérateur associée (cf. n° 17.3 du Vocabulaire ; c'est en particulier une norme de $\mathbf{K}$-espace vectoriel, et $\|u(v)\| \leqslant \|u\|\,\|v\|$, si $u \in \mathrm{End}(\mathrm{V})$ et $v \in \mathrm{V}$).

5. Attention au fait que, si D est le disque unité de $\mathbf{C}$, les polynômes en z ne sont pas denses dans $\mathscr{C}(\mathrm{D})$; en effet, un élément de l'adhérence est une fonction holomorphe, comme nous le verrons. Le problème vient de ce que les polynômes en z ne sont pas stables par $f \mapsto \overline{f}$.

Soient I un intervalle de $\mathbf{R}$ et $u : \mathrm{I} \to \mathrm{End}(\mathrm{V})$ une fonction continue. On cherche à résoudre le système différentiel $\phi' = u \cdot \phi$, i.e. décrire l'ensemble des $\phi : \mathrm{I} \to \mathrm{V}$, de classe $\mathscr{C}^1$, telles que $\phi'(t) = u(t) \cdot \phi(t)$, pour tout $t \in \mathrm{I}$.

Théorème II.1.12. — (Cauchy-Lipschitz) *L'ensemble $\mathscr{L}$ des solutions du système différentiel $\phi' = u \cdot \phi$ est un espace vectoriel de dimension* $\dim \mathrm{V}$ *et l'application $\phi \mapsto \phi(t)$ induit un isomorphisme de $\mathscr{L}$ sur* V *pour tout $t \in \mathrm{I}$. Autrement dit,*

- *si $t_0 \in \mathrm{I}$, alors pour tout $z \in \mathrm{V}$ il existe, sur* I *tout entier, une unique solution ϕ_z du système différentiel $\phi' = u \cdot \phi$, prenant la valeur z en t_0 ;*
- *si $t \in \mathrm{I}$, il existe $a(t) \in \mathrm{GL}(\mathrm{V})$ tel que $\phi_z(t) = a(t) \cdot z$, pour tout $z \in \mathrm{V}$ $(a(t_0) = \mathrm{id})$.*

Démonstration. — La linéarité de la dérivation et de $u(t) : \mathrm{V} \to \mathrm{V}$ implique que toute combinaison linéaire de solutions est encore une solution, et donc $\mathscr{L}$ est un espace vectoriel. Comme $\phi \mapsto \phi(t)$ est linéaire de manière évidente, il suffit de prouver le second énoncé (existence et unicité d'une solution prenant la valeur z en t_0) ; le reste s'en déduit.

Les conditions « ϕ de classe $\mathscr{C}^1$ », « $\phi' = u \cdot \phi$ » et « $\phi(t_0) = z$ » sont équivalentes à « ϕ continue » et « $\phi(t) = z + \int_{t_0}^t u(x) \cdot \phi(x)\, dx$ ». En effet, la continuité de ϕ entraîne la dérivabilité de $t \mapsto \int_{t_0}^t u(x)\phi(x)\, dx$ et la relation $\phi'(t) = u(t) \cdot \phi(t)$. En d'autres termes, ϕ vérifie les trois premières conditions si et seulement si elle est continue et est un point fixe de $\phi \mapsto \mathrm{F}(\phi)$, où $\mathrm{F} : \mathscr{C}(\mathrm{I}, \mathrm{V}) \to \mathscr{C}(\mathrm{I}, \mathrm{V})$ est définie par $(\mathrm{F}(\phi))(t) = z + \int_{t_0}^t u(x)\phi(x)\, dx$. Il suffit donc de prouver que F a un unique point fixe dans $\mathscr{C}(\mathrm{I}, \mathrm{V})$, et pour ce faire, il suffit de démontrer le même énoncé en remplaçant I par un intervalle compact arbitraire $\mathrm{J} \subset \mathrm{I}$ (on peut écrire I comme une réunion croissante d'intervalles compacts J_n, et l'unicité d'une solution $\phi_{z,n}$ sur J_n montre que la restriction à J_n de la solution $\phi_{z,n+1}$ sur J_{n+1} est égale à $\phi_{z,n}$, et donc que les $\phi_{z,n}$ se recollent pour donner une solution ϕ_z de l'équation $\phi' = u(t)\phi$ sur I tout entier ; cette solution vérifie $\phi_z(t_0) = z$ et c'est la seule car c'est le cas sur chacun des J_n). On note F^n la composée $\mathrm{F} \circ \cdots \circ \mathrm{F}$ de n copies de F.

Soit donc J un intervalle compact de I contenant t_0, et soit $\mathrm{A}_\mathrm{J} = \sup_{t \in \mathrm{J}} \|u(t)\|$. Si $\phi : \mathrm{J} \to \mathrm{V}$ est une fonction continue, on pose $\|\phi\|_\mathrm{J} = \sup_{t \in \mathrm{J}} \|\phi(t)\|$, ce qui fait de $\mathscr{C}(\mathrm{J}, \mathrm{V})$ un espace de Banach (cf. ex. II.1.6). On a

$$\|(\mathrm{F}(\phi_1))(t) - (\mathrm{F}(\phi_2))(t)\| \leqslant \Big| \int_{t_0}^t \|u(x)\| \, \|\phi_1(x) - \phi_2(x)\| \, dx \Big| \leqslant \mathrm{A}_\mathrm{J} \Big| \int_{t_0}^t \|\phi_1(x) - \phi_2(x)\| \, dx \Big|.$$

En majorant $\|\phi_1(x) - \phi_2(x)\|$ par $\|\phi_1 - \phi_2\|_\mathrm{J}$, pour tout $x \in \mathrm{J}$, cela nous fournit la majoration $\|(\mathrm{F}(\phi_1))(t) - (\mathrm{F}(\phi_2))(t)\| \leqslant \mathrm{A}_\mathrm{J} \|\phi_1 - \phi_2\|_\mathrm{J} |t - t_0|$, pour tout $t \in \mathrm{J}$. On peut alors réinjecter cette majoration dans l'inégalité ci-dessus et une petite récurrence nous permet de montrer que $\|(\mathrm{F}^n(\phi_1))(t) - (\mathrm{F}^n(\phi_2))(t)\| \leqslant \mathrm{A}_\mathrm{J}^n \|\phi_1 - \phi_2\|_\mathrm{J} \frac{|t-t_0|^n}{n!}$, pour tout $t \in \mathrm{J}$. Si $\mathrm{M}_\mathrm{J} = \sup_{t \in \mathrm{J}} |t - t_0|$, on en déduit que $\|\mathrm{F}^n(\phi_1) - \mathrm{F}^n(\phi_2)\|_\mathrm{J} \leqslant \frac{(\mathrm{A}_\mathrm{J}\mathrm{M}_\mathrm{J})^n}{n!} \|\phi_1 - \phi_2\|_\mathrm{J}$. Comme $\frac{(\mathrm{A}_\mathrm{J}\mathrm{M}_\mathrm{J})^n}{n!} \to 0$, cela prouve que F a au plus un point fixe (appliquer la majoration précédente à deux points fixes de F). On peut aussi appliquer la majoration précédente à $\phi_1 = \mathrm{F}(\phi)$ et $\phi_2 = \phi$, et comme $\sum_{n \in \mathbf{N}} \frac{(\mathrm{A}_\mathrm{J}\mathrm{M}_\mathrm{J})^n}{n!} < +\infty$, cela prouve que $\sum_{n \in \mathbf{N}} (\mathrm{F}^{n+1}(\phi) - \mathrm{F}^n(\phi))$ est

normalement convergente, et donc convergente puisque $\mathscr{C}(\mathrm{J},\mathrm{V})$ est complet. La suite des sommes partielles a donc une limite, et $\mathrm{F}^n(\phi)$ a une limite pour tout $\phi \in \mathscr{C}(\mathrm{J},\mathrm{V})$. Comme cette limite est un point fixe de F, cela permet de conclure.

Remarque II.1.13. — (i) Si I' est un sous-intervalle ouvert de I, il résulte du théorème que la restriction à I' induit un isomorphisme de l'espace des solutions sur I sur celui des solutions sur I' ; autrement dit toute solution sur I' se prolonge de manière unique en une solution sur I.

(ii) On a démontré en passant que l'on obtient la solution ϕ_z en itérant l'application $\phi \mapsto \mathrm{F}(\phi)$, en partant de n'importe quelle ϕ. Par exemple, l'équation différentielle $\phi' = \phi$ a une unique solution sur $\mathbf{R}$ prenant la valeur 1 en 0, et on obtient cette solution en itérant la fonctionnelle $\phi \mapsto 1 + \int_0^t \phi(x)\,dx$ à partir de n'importe quelle fonction ϕ ; si on part de $\phi = 0$, les fonctions que l'on obtient sont 1, $1+t$, …, $1 + t + \frac{t^2}{2} + \cdots + \frac{t^n}{n!}$, et la solution est donc $t \mapsto \sum_{n=0}^{+\infty} \frac{t^n}{n!} = e^t$.

(iii) Plus généralement, si $\mathrm{I} = \mathbf{R}$ et $t \mapsto u(t)$ est *constante*, la solution ϕ_z obtenue par ce procédé de point fixe est $\sum_{n=0}^{+\infty} \frac{t^n u^n}{n!} \cdot z$, où on a noté exponentiellement la composée de n fois le même endomorphisme. Si on définit *l'exponentielle* e^{φ} d'un endomorphisme φ par $e^{\varphi} = \sum_{n=0}^{+\infty} \frac{\varphi^n}{n!}$ (la convergence normale de la série résulte de ce que $\|\ \|$ est une norme d'algèbre sur $\mathrm{End}(\mathrm{V})$, et donc $\|u^n\| \leqslant \|u\|^n$) , la formule précédente s'écrit sous la forme $\phi_z = e^{tu} \cdot z$.

Le calcul de e^{tu} se fait en utilisant la décomposition de Dunford $u = \mathrm{D} + \mathrm{N}$ de u ou bien la mise sous forme de Jordan de la matrice de u dans une base bien choisie : si $e_1, \ldots, e_m$ est une base de V dans laquelle la matrice A de u est sous forme de Jordan, on a $\mathrm{A} = \mathrm{D} + \mathrm{N}$ où $\mathrm{D} = \mathrm{Diag}(\lambda_1, \ldots, \lambda_m)$ est diagonale, et N est triangulaire supérieure avec des 0 sur la diagonale et commute à D ; comme D et N commutent, on a $e^{tu} = e^{t\mathrm{D}} e^{t\mathrm{N}}$, et $e^{t\mathrm{D}} = \mathrm{Diag}(e^{\lambda_1 t}, \ldots, e^{\lambda_m t})$ et $e^{t\mathrm{N}} = \sum_{n=0}^{m-1} \frac{t^n \mathrm{N}^n}{n!}$ car $\mathrm{N}^m = 0$.

(iv) Soient I un intervalle de $\mathbf{R}$ et $f : \mathrm{V} \times \mathrm{I} \to \mathrm{V}$ lipschitzienne par rapport à u (i.e. si $\mathrm{J} \subset \mathrm{I}$ est un intervalle compact, il existe $\mathrm{C}(\mathrm{J})$ tel que $\|f(u_1,t) - f(u_2,t)\| \leqslant \mathrm{C}(\mathrm{J})\|u_1 - u_2\|$, pour tous $u_1, u_2 \in \mathrm{V}$ et $t \in \mathrm{J}$). La même démonstration prouve que l'équation différentielle $u' = f(u,t)$ admet une unique solution, sur I tout entier, vérifiant la condition initiale $u(t_0) = u_0$ quel que soit $u_0 \in \mathrm{V}$. Le résultat est faux si on supprime la condition « $f : \mathrm{V} \times \mathrm{I} \to \mathrm{V}$ lipschitzienne par rapport à u » : la solution de $u' = u^2$ valant 1 en 0 est $t \mapsto \frac{1}{1-t}$ qui explose en $t = 1$ et donc ne s'étend pas en une solution sur $\mathbf{R}$ tout entier.

4.2. *Wronskien et variation des constantes*

Le th. II.1.12 nous a fourni une fonction $a : \mathrm{I} \to \mathrm{GL}(\mathrm{V})$, telle que la solution ϕ_z du système différentiel $\phi' = u \cdot \phi$ prenant la valeur z en t_0 soit $a \cdot z$.

Proposition II.1.14. — (i) $a : \mathrm{I} \to \mathrm{GL}(\mathrm{V})$ *satisfait le système différentiel* $a' = ua$.

(ii) *Le déterminant* W *de* a (c'est le wronskien du système différentiel) *satisfait l'équa-*

tion différentielle $\mathrm{W}' = (\mathrm{Tr}(u))\mathrm{W}$*, et on a* $\mathrm{W}(t) = \exp\big(\int_{t_0}^t \mathrm{Tr}(u(t))\,dt\big)$*, pour tout* $t \in \mathrm{I}$ (formule de Liouville).

Démonstration. — Si $z \in \mathrm{V}$, alors $\phi_z = a \cdot z$, et donc $\phi'_z = a' \cdot z$. Comme par ailleurs $\phi'_z = u \cdot \phi_z$, on obtient $a' \cdot z = ua \cdot z$, pour tout $z \in \mathrm{V}$, et donc $a' = ua$, ce qui prouve le (i).

Pour prouver le (ii), choisissons une base $e_1, \dots, e_n$ de V. Comme le déterminant est n-linéaire, on a

$$\mathrm{W}'(t) = \big(\det_{e_1,\dots,e_n}(\phi_{e_1}(t), \dots, \phi_{e_n}(t)\big)' = \sum_{i=1}^n \det_{e_1,\dots,e_n}(\phi_{e_1}(t), \dots, \phi'_{e_i}(t), \dots, \phi_{e_n}(t))$$

Par ailleurs, $\phi'_{e_i}(t) = u(t) \cdot \phi_{e_i}(t)$, et comme

$$\sum_{i=1}^n \det_{e_1,\dots,e_n}(v_1, \dots, u \cdot v_i, \dots, v_n) = \mathrm{Tr}(u) \det_{e_1,\dots,e_n}(v_1, \dots, v_n), \tag{II.1.1}$$

on obtient l'équation différentielle annoncée $\mathrm{W}' = (\mathrm{Tr}(u))\mathrm{W}$, dont l'unique solution valant 1 en t_0 est $t \mapsto \exp\big(\int_{t_0}^t \mathrm{Tr}(u(t))\,dt\big)$. Ceci permet de conclure. (Pour vérifier la formule (II.1.1), on constate que les deux membres sont n-linéaires alternés en $(v_1, \dots, v_n)$, et donc il suffit de vérifier qu'ils coïncident sur une base bien choisie de V ; la base $e_1, \dots, e_n$ ne demande qu'à être utilisée, et comme $\det_{e_1,\dots,e_n}(e_1, \dots, u \cdot e_i, \dots, e_n) = u_{i,i}$ si $(u_{i,j})$ est la matrice de u dans cette base, on en déduit le résultat.)

Exercice II.1.15. — Montrer que $\det(\exp \mathrm{A}) = e^{\mathrm{Tr}\,\mathrm{A}}$ si $\mathrm{A} \in \mathbf{M}_n(\mathbf{C})$. (Commencer par A triangulaire.)

On s'intéresse maintenant à un système différentiel *avec second membre*, c'est-à-dire de la forme $\phi' - u \cdot \phi = v$ où $v : \mathrm{I} \to \mathrm{V}$ est continue. Si on dispose d'une solution particulière ϕ_0 de ce système, alors $\phi \mapsto \phi - \phi_0$ induit une bijection de l'ensemble des solutions du système avec second membre $\phi' - u \cdot \phi = v$ sur celui *sans second membre* $\phi' - u \cdot \phi = 0$. Résoudre un système avec second membre est donc équivalent à trouver une solution particulière et résoudre le système sans second membre.

Par ailleurs, si on sait résoudre le système sans second membre, on peut trouver une solution particulière du système avec second membre en utilisant la méthode de *variation des constantes*. La résolution du système sans second membre nous fournit une solution $a : \mathrm{I} \to \mathrm{GL}(\mathrm{V})$ du système différentiel $a' = ua$, et les solutions du système $\phi' = u \cdot \phi$ sont les $t \mapsto a(t) \cdot z$, pour $z \in \mathrm{V}$. La méthode de variation des constantes consiste à chercher une solution de $\phi' - u \cdot \phi = v$ sous la forme $\phi(t) = a(t) \cdot z(t)$. On a alors $\phi'(t) = a'(t) \cdot z(t) + a(t) \cdot z'(t)$, et donc $a'(t) \cdot z(t) + a(t) \cdot z'(t) - u(t)a(t) \cdot z(t) = v(t)$, et comme $a' = ua$, cette équation se simplifie en $z' = a^{-1} \cdot v$, qui se résoud par simple intégration.

4.3. *Équations différentielles d'ordre supérieur*

Corollaire II.1.16. — *Soit* $\mathrm{I} \subset \mathbf{R}$ *un intervalle ouvert. Si* $a_0, \dots, a_{n-1}$ *sont des fonctions continues de* I *dans* $\mathbf{K}$*, l'ensemble* $\mathscr{L}$ *des solutions sur* I *de l'équation différentielle* $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$ *est un espace vectoriel de dimension* n *et, pour tout* $t \in \mathrm{I}$*, l'application* $\phi \mapsto (\phi(t), \dots, \phi^{(n-1)}(t))$ *est un isomorphisme de* $\mathscr{L}$ *sur* $\mathbf{K}$*. Autrement dit,*

- *si* $t_0 \in \mathrm{I}$*, et si* $z = (z_0, \dots, z_{n-1}) \in \mathbf{K}^n$*, il existe, sur* I *tout entier, une unique solution* ϕ_z *de l'équation différentielle* $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$*, telle que* $\phi_z^{(i)}(t_0) = z_i$*, si* $0 \leqslant i \leqslant n-1$ *;*
- *si* $t \in \mathrm{I}$*, il existe* $\mathrm{A}(t) \in \mathbf{GL}_n(\mathbf{K})$ *tel que* ${}^{\mathrm{t}}(\phi_z(t), \phi_z'(t), \dots, \phi_z^{(n-1)}(t)) = \mathrm{A}(t){}^{\mathrm{t}}z$*.*

Démonstration. — Soit

$$\mathrm{U} = \begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \\ a_0 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix}.$$

Si $\Phi = {}^{\mathrm{t}}(\phi_0, \dots, \phi_{n-1})$ est une solution, sur I, du système différentiel $\Phi' = \mathrm{U}\Phi$, alors $\phi_0, \dots, \phi_{n-1}$ sont de classe $\mathscr{C}^1$ et $\phi_0' = \phi_1, \dots, \phi_{n-2}' = \phi_{n-1}$ et $\phi_{n-1}' = a_0\phi_0 + \cdots + a_{n-1}\phi_{n-1}$. Il s'ensuit que $\phi = \phi_0$ est de classe $\mathscr{C}^n$, que $\phi_i = \phi^{(i)}$ si $0 \leqslant i \leqslant n-1$, et que ϕ vérifie l'équation différentielle $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$. Réciproquement, si ϕ est une solution de cette équation, alors $\Phi = {}^{\mathrm{t}}(\phi, \dots, \phi^{(n-1)})$ est une solution du système différentiel $\Phi' = \mathrm{U}\Phi$. Autrement dit $\Phi \mapsto \phi_0$ est un isomorphisme de l'espace des solutions de $\Phi' = \mathrm{U}\Phi$ sur celui de $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$. L'énoncé est alors une simple traduction du th. II.1.12.

Remarque II.1.17. — (i) Une équation $\phi^{(n)} - a_{n-1}(t)\phi^{(n-1)} + \cdots - a_0(t)\phi = b(t)$, avec second membre, se résoud par la méthode de variation des constantes en revenant au système différentiel associé comme dans la démonstration du cor. II.1.16.

(ii) Si l'équation différentielle est à *coefficients constants*, les solutions sont les coefficients de la matrice $e^{t\mathrm{U}}$, où U est la matrice ci-dessus (et ne dépend pas de t puisqu'on a supposé les a_i constantes). Si $\lambda_1, \dots, \lambda_r$ sont les valeurs propres de U et si λ_i est de multiplicité d_i, il n'y a qu'un bloc de Jordan J_i (d'ordre d_i) pour chaque λ_i (cela résulte de l'ex. 10.4, et de ce qu'une matrice et sa transposée ont même polynôme minimal car $\mathrm{P}({}^{\mathrm{t}}\mathrm{A}) = {}^{\mathrm{t}}(\mathrm{P}(\mathrm{A}))$ si $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ et $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$). Or les coefficients de $\exp(t\mathrm{J}_i)$ sont de la forme $e^{\lambda_i t}\mathrm{P}_i(t)$, où $\mathrm{P}_i \in \mathbf{C}[\mathrm{X}]$ est de degré $\leqslant d_i - 1$. On en déduit que les $t \mapsto e^{\lambda_i t}t^j$, pour $1 \leqslant i \leqslant r$ et $0 \leqslant j \leqslant d_i - 1$, forment une base de l'espace des solutions de l'équation différentielle. Par exemple, si tous les a_i sont nuls, on retrouve le résultat selon lequel l'ensemble des ϕ dont la dérivée n-ième est identiquement nulle est l'espace des polynôme de degré $\leqslant n-1$.

5. Complétion d'espaces vectoriels normés

La manière la plus standard pour construire des espaces de Banach est de partir d'espaces vectoriels normés et de les compléter [6]. On renvoie au n° 14.3 du Vocabulaire pour tout ce qui a trait à la complétion d'un espace métrique. De manière générale, on a le résultat suivant.

Proposition II.1.18. — (i) *Si* $(\mathrm{E}, \| \ \|)$ *est un espace vectoriel normé, alors le complété* $\widehat{\mathrm{E}}$ *de* E (pour la distance associée à $\| \ \|$) *est un espace vectoriel. De plus,* $\| \ \|$ *s'étend par continuité en une norme sur* $\widehat{\mathrm{E}}$*, et* $(\widehat{\mathrm{E}}, \| \ \|)$ *est un espace de Banach.*

(ii) *Si* F *est un espace de Banach, et si* $u : \mathrm{E} \to \mathrm{F}$ *est linéaire continue, alors* u *admet un unique prolongement continu à* $\widehat{\mathrm{E}}$*, et ce prolongement est linéaire.*

Démonstration. — Le (i) est un petit exercice utilisant de manière répétée les résultats du n° 14.3 du Vocabulaire. Par exemple, pour montrer que l'addition $s : \mathrm{E} \times \mathrm{E} \to \mathrm{E}$ s'étend par continuité en une addition $s : \widehat{\mathrm{E}} \times \widehat{\mathrm{E}} \to \widehat{\mathrm{E}}$, on peut munir $\mathrm{E} \times \mathrm{E}$ de la norme $\|(x, y)\| = \sup(\|x\|, \|y\|)$. Alors $s : \mathrm{E} \times \mathrm{E} \to \mathrm{E} \subset \widehat{\mathrm{E}}$ est lipschitzienne de rapport 2, et donc s'étend par continuité à $\widehat{\mathrm{E}} \times \widehat{\mathrm{E}}$.

Pour le (ii), voir le n° 17.2 du Vocabulaire.

Exemple II.1.19. — Soit Ω un ouvert de $\mathbf{R}^m$.

(i) L'espace $\mathrm{L}^1(\Omega)$ défini au n° 1 du § III.2 est un espace de Banach dans lequel $\mathscr{C}_c(\Omega)$ est dense ; on peut donc aussi le définir comme le complété de $\mathscr{C}_c(\Omega)$ pour la norme $\| \ \|_1$ définie par $\|\phi\|_1 = \int_\Omega |\phi(x)|\, dx$.

(ii) De même, l'espace $\mathrm{L}^2(\Omega)$ défini au n° 2 du § III.2 peut aussi être défini comme le complété de $\mathscr{C}_c(\Omega)$ pour la norme $\| \ \|_2$ définie par $\|\phi\|_2 = \big(\int_\Omega |\phi(x)|^2\, dx \big)^{1/2}$.

(iii) Si $k \geqslant 1$, on définit l'*espace de Sobolev* $\mathrm{H}^k(\mathbf{R}^m)$ comme le complété de l'espace $\mathscr{C}^k_c(\mathbf{R}^m)$ des fonctions de classe $\mathscr{C}^k$ sur $\mathbf{R}^m$, nulles en dehors d'un compact, pour la norme $\| \ \|_{\mathrm{H}^k}$ définie par

$$\|\phi\|_{\mathrm{H}^k} = \Big(\sum_{|\alpha| \leqslant k} (\|\partial_\alpha \phi\|_2)^2 \Big)^{1/2} = \Big(\sum_{|\alpha| \leqslant k} \int_{\mathbf{R}^m} |\partial_\alpha \phi(x)|^2\, dx \Big)^{1/2},$$

6. Pour beaucoup de questions c'est très utile, car on obtient un espace dans lequel l'analyse devient plus facile ; en particulier, il est nettement plus aisé de démontrer des résultats d'existence dans un espace complet. Évidemment, le problème est qu'il est difficile de retrouver ses petits après complétion. Par exemple, il est impossible de montrer que deux nombres réels sont égaux ($\mathbf{R}$ est obtenu en complétant $\mathbf{Q}$) sauf si on sait par ailleurs que leur différence est un entier (à multiplication près par un nombre réel explicite). De même, il est nettement plus facile de démontrer l'existence de solutions d'équations différentielles dans un espace de Sobolev H^k, mais si ce qui nous intéresse sont des solutions de classe $\mathscr{C}^k$, il y a un travail supplémentaire pour vérifier que les solutions obtenues conviennent.

où, si $\boldsymbol{\ell} = (\ell_1, \dots, \ell_m) \in \mathbf{N}^m$, on a posé $|\boldsymbol{\ell}| = \sum_{j=1}^m \ell_j$, et noté $\partial_{\amalg}$ l'opérateur différentiel

$$\partial_{\amalg} = \Big(\frac{\partial}{\partial x_1}\Big)^{\ell_1} \cdots \Big(\frac{\partial}{\partial x_m}\Big)^{\ell_m}.$$

Par définition, si $\boldsymbol{\ell} = (\ell_1, \dots, \ell_m) \in \mathbf{N}^m$ vérifie $|\boldsymbol{\ell}| \leqslant k$, l'application linéaire

$$\partial_{\amalg} = \Big(\frac{\partial}{\partial x_1}\Big)^{\ell_1} \cdots \Big(\frac{\partial}{\partial x_m}\Big)^{\ell_m} : \mathscr{C}_c^k(\mathbf{R}^m) \to \mathscr{C}_c^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$$

est continue (et même 1-lipschitzienne) si on munit $\mathscr{C}_c^k(\mathbf{R}^m)$ de la norme $\| \ \|_{\mathrm{H}^k}$ et $\mathscr{C}_c^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$ de la norme $\| \ \|_{\mathrm{H}^{k-|\boldsymbol{\ell}|}}$. Elle s'étend donc, par continuité, en une application linéaire, encore notée $\partial_{\amalg}$ de $\mathrm{H}^k(\mathbf{R}^m)$ dans $\mathrm{H}^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$.

Proposition II.1.20. — *Si $k \in \mathbf{N}$, si $\boldsymbol{\ell} \in \mathbf{N}^m$ vérifie $|\boldsymbol{\ell}| \leqslant k$, si $\phi \in \mathscr{C}_c^k(\mathbf{R}^m)$, et si $f \in \mathrm{H}^k(\mathbf{R}^m)$, alors*[7]

$$\int_{\mathbf{R}^m} (\partial_{\amalg}\phi)\, f = (-1)^{|\boldsymbol{\ell}|} \int_{\mathbf{R}^m} (\partial_{\amalg} f)\, \phi.$$

Démonstration. — Les deux membres sont bien définis car $\partial_{\amalg}\phi$, f, $\partial_{\amalg} f$ et ϕ sont de carré sommable. On en déduit que

$$f \mapsto \mathrm{L}_\phi(f) = \int_{\mathbf{R}^m} (\partial_{\amalg}\phi)\, f - (-1)^{|\boldsymbol{\ell}|} \int_{\mathbf{R}^m} (\partial_{\amalg} f)\, \phi$$

est une forme linéaire sur $\mathrm{H}^k(\mathbf{R}^m)$, qui est continue car

$$|\mathrm{L}_\phi(f)| \leqslant \|f\|_2 \|\partial_{\amalg}\phi\|_2 + \|\partial_{\amalg} f\|_2 \|\phi\|_2 \leqslant (\|\partial_{\amalg}\phi\|_2 + \|\phi\|_2)\|f\|_{\mathrm{H}^k}.$$

Par ailleurs, une (suite d') intégrations par partie montre que $\mathrm{L}_\phi(f) = 0$ si $f \in \mathscr{C}_c^k(\mathbf{R}^m)$, et comme $\mathscr{C}_c^k(\mathbf{R}^m)$ est dense dans $\mathrm{H}^k(\mathbf{R}^m)$, cela implique que L_ϕ est identiquement nulle sur $\mathrm{H}^k(\mathbf{R}^m)$. Ceci permet de conclure.

6. Applications linéaires continues entre espaces de Banach

Théorème II.1.21. — (Banach-Steinhaus, 1927) *Soient* E *un espace de Banach,* F *un espace vectoriel normé, et $(u_n)_{n\in\mathbf{N}}$ une suite d'applications linéaires continues de* E *dans* F*. Alors, de deux choses l'une :*

- *soit la suite $(\|u_n\|)_{n\in\mathbf{N}}$ est bornée*[8]*, et donc $u_n(x)$ est bornée pour tout $x \in \mathrm{E}$,*
- *soit $\{x \in \mathrm{E},\ \sup_{n\in\mathbf{N}} \|u_n(x)\|_{\mathrm{F}} = +\infty\}$ est dense dans* E*.*

Démonstration. — Il s'agit de prouver que, si $(\|u_n\|)_{n\in\mathbf{N}}$ n'est pas bornée, et si on définit $\varphi : \mathrm{E} \to \mathbf{R}_+ \cup \{+\infty\}$ par $\varphi(x) = \sup_{n\in\mathbf{N}} \|u_n(x)\|_{\mathrm{F}}$, alors $\{x \in \mathrm{E},\ \varphi(x) = +\infty\}$ est dense. Pour cela, considérons, si $\mathrm{N} \in \mathbf{N}$, l'ensemble $\mathrm{U_N} = \{x \in \mathrm{E},\ \varphi(x) > \mathrm{N}\}$. On a $\mathrm{U_N} = \cup_{n\in\mathbf{N}}\{x \in \mathrm{E},\ \|u_n(x)\|_{\mathrm{F}} > \mathrm{N}\}$, et comme chaque u_n est continue, $\mathrm{U_N}$ est une

7. Autrement dit, $\partial^{\boldsymbol{\ell}} f$ est la dérivée $\boldsymbol{\ell}$-ième de f au sens des distributions.

8. $\|u_n\|$ est la norme d'opérateur de u_n. Rappelons qu'elle est définie par $\|u_n\| = \sup_{x\neq 0} \|x\|_{\mathrm{E}}^{-1} \|u_n(x)\|_{\mathrm{F}}$, cf. n° 17 du § 11.

réunion d'ouverts et donc est ouvert. Si U_N n'est pas dense, il existe $x_0 \in E$ et $r > 0$ tel que $\|u_n(x + x_0)\|_F \leqslant N$, quel que soient $x \in E$, avec $\|x\|_E < r$, et $n \in \mathbf{N}$. Mais alors $\|u_n(x)\|_F = \|u_n(x + x_0) - u_n(x_0)\|_F \leqslant 2N$, quel que soit $x \in E$, avec $\|x\|_E < r$, et quel que soit $n \in \mathbf{N}$. Autrement dit, on a $\|u_n\| \leqslant \frac{2N}{r}$, quel que soit $n \in \mathbf{N}$, contrairement à l'hypothèse. C'est donc que U_N est un ouvert dense, quel que soit $N \in \mathbf{N}$, et comme $\{x \in E,\ \varphi(x) = +\infty\} = \cap_{N\in\mathbf{N}} U_N$, le lemme de Baire (n° 14.2 du Vocabulaire) montre qu'il est dense dans E, ce que l'on cherchait à démontrer.

Remarque II.1.22. — D'après la démonstration, $\{x \in E,\ \sup_{n\in\mathbf{N}} \|u_n(x)\|_F = +\infty\}$ est une intersection dénombrable d'ouverts denses, si $\|u_n\|$ n'est pas bornée. Une intersection dénombrable d'ouverts est appelée un G_δ, et il résulte du lemme de Baire qu'un G_δ dense dans un espace de Banach E est non dénombrable (cf. ex. 14.3 du Vocabulaire).

Le théorème de Banach-Steinhaus admet comme corollaire le très utile résultat suivant, qui est un peu surprenant quand on pense à ce qui se passe pour une limite simple de fonctions continues [9].

Corollaire II.1.23. — *Si* E *est un espace de Banach, et si* F *un espace vectoriel, alors une limite simple d'applications linéaires continues de* E *dans* F *est une application linéaire continue de* E *dans* F.

Démonstration. — Soit $(u_n)_{n\in\mathbf{N}}$ une suite d'applications linéaires continues de E dans F telle que la suite $(u_n(x))_{n\in\mathbf{N}}$ ait une limite $u(x) \in F$, quel que soit $x \in E$. Si $x \in E$ et $\lambda \in \mathbf{K}$, on a $u(\lambda x) = \lim_{n\to+\infty} u_n(\lambda x) = \lim_{n\to+\infty} \lambda u_n(x) = \lambda \lim_{n\to+\infty} u_n(x) = \lambda u(x)$, et de même, $u(x+y) = u(x)+u(y)$, quels que soient $x, y \in E$, ce qui prouve que u est linéaire. Maintenant, le fait que la suite $(u_n(x))_{n\in\mathbf{N}}$ a une limite quel que soit $x \in E$, implique, d'après le théorème de Banach-Steinhaus, l'existence de $M \in \mathbf{R}_+$ tel que $\|u_n\| \leqslant M$ quel que soit $n \in \mathbf{N}$. On a donc $\|u_n(x)\|_F \leqslant M \cdot \|x\|_E$ quels que soient $n \in \mathbf{N}$ et $x \in E$. On en déduit, en passant à la limite, que $\|u(x)\|_F \leqslant M \cdot \|x\|_E$ quel que soit $x \in E$, et donc que u est continue, ce qui permet de conclure.

Théorème II.1.24. — (de l'image ouverte, Banach (1929)) *Si* E *et* F *sont deux espaces de Banach, et si* $u : E \to F$ *est une application linéaire continue surjective, alors il existe* $\rho > 0$ *tel que* $u(B_E(0, 1^-))$ *contienne* $B_F(0, \rho^-)$.

Démonstration. — Si $n \in \mathbf{N}$, soit A_n l'adhérence dans F de $u(B_E(0, n^-))$. Comme E est la réunion des $B_E(0, n^-)$, pour $n \in \mathbf{N}$, et comme u est supposée surjective, on a $\cup_{n\in\mathbf{N}} A_n = F$. Le lemme de Baire implique donc l'existence de n tel que A_n soit d'intérieur non vide.

9. Bien que Cauchy ait réussi à "démontrer", dans son *Cours d'analyse*, qu'une limite simple de fonctions continues est continue, on sait bien, à l'heure actuelle, qu'il n'en est rien, en général. Baire (1904) a démontré qu'*une fonction* $f : \mathbf{R}^n \to \mathbf{R}$ *est limite simple de fonctions continues si et seulement si la restriction de* f *à tout fermé non vide a au moins un point où elle est continue.* C'est à cette occasion qu'il a introduit son fameux lemme.

Ceci se traduit par l'existence de $x_0 \in \mathrm{B_E}(0, n^-)$ et de $r > 0$, tels que, si $\|y\|_\mathrm{F} < r$, alors quel que soit $\varepsilon > 0$, il existe $x \in \mathrm{B_E}(0, n^-)$, avec $\|u(x) - (u(x_0) + y)\|_\mathrm{F} < \varepsilon$. Comme $x - x_0 \in \mathrm{B_E}(0, 2n^-)$, quitte à faire une homothétie de rapport $\frac{1}{4n}$, on voit que l'on a démontré le résultat suivant (avec $\rho = \frac{r}{4n}$) : il existe $\rho > 0$ tel que, quel que soit $y \in \mathrm{B_F}(0, \rho^-)$ et quel que soit $\varepsilon > 0$, il existe $x \in \mathrm{B_E}(0, (\frac{1}{2})^-)$ avec $\|y - u(x)\|_\mathrm{F} < \varepsilon$.

Ce n'est pas tout à fait le résultat cherché, mais presque. Si $y \in \mathrm{B_F}(0, \rho^-)$, on peut construire par récurrence, en utilisant ce qui précède, une suite $(x_m)_{m\in\mathbf{N}}$ d'éléments de $\mathrm{B_E}(0, (\frac{1}{2})^-)$, et une suite $(y_m)_{m\in\mathbf{N}}$ d'éléments de $\mathrm{B_F}(0, \rho^-)$ vérifiant :

$$y_0 = y, \quad \|y_m - u(x_m)\|_\mathrm{F} < \frac{\rho}{2}, \quad \text{et} \quad y_{m+1} = 2(y_m - u(x_m)).$$

On a alors $y = u(x_0) + 2^{-1}u(x_1) + \cdots + 2^{-m}u(x_m) + 2^{-m-1}y_{m+1}$, et comme la série $\sum_{m=0}^{+\infty} 2^{-m}x_m$ converge dans E vers un élément x de $\mathrm{B_E}(0, 1^-)$, un passage à la limite montre que $y = u(x)$. Ceci démontre l'inclusion $\mathrm{B_F}(0, \rho^-) \subset u(\mathrm{B_E}(0, 1^-))$ que l'on cherchait à obtenir.

Remarque II.1.25. — Si $x \in \mathrm{E}$ et $r > 0$, alors $\mathrm{B_E}(x, r^-) = x + r\mathrm{B_E}(0, 1^-)$ et donc $u(\mathrm{B_E}(x, r^-)) = u(x) + ru(\mathrm{B_E}(0, 1^-))$. Le théorème ci-dessus montre donc que, si u est surjective, alors $u(\mathrm{B_E}(x, r^-))$ contient un voisinage ouvert de $u(x)$. On en déduit le fait que, si U est un ouvert de E, alors $u(\mathrm{U})$ est voisinage ouvert de $u(x)$, quel que soit $x \in \mathrm{U}$; autrement dit $u(\mathrm{U})$ est ouvert. Le théorème ci-dessus peut donc se reformuler sous la forme « l'image d'un ouvert par une application linéaire continue *surjective* entre deux espaces de Banach est un ouvert » ; c'est ce qui explique son nom.

Corollaire II.1.26. — *Si* E *et* F *sont deux espaces de Banach, et si* $u : \mathrm{E} \to \mathrm{F}$ *est une application linéaire continue bijective, alors* $u^{-1} : \mathrm{F} \to \mathrm{E}$ *est aussi continue.*

Démonstration. — Si U est un ouvert de E, alors $(u^{-1})^{-1}(\mathrm{U}) = u(\mathrm{U})$ est ouvert d'après la remarque ci-dessus. Ceci permet de conclure.

Exercice II.1.27. — (Théorème du graphe fermé)

Soient E et F deux espaces de Banach, et $u : \mathrm{E} \to \mathrm{F}$ une application linéaire. Soit $\mathrm{G} \subset \mathrm{E} \times \mathrm{F}$ le graphe de u (i.e. l'ensemble des couples $(x, u(x))$, pour $x \in \mathrm{E}$).

(i) Montrer que $\mathrm{E} \times \mathrm{F}$ muni de la norme $\|(x, y)\| = \sup(\|x\|_\mathrm{E}, \|y\|_\mathrm{F})$ est un espace de Banach et que les deux projections $p_\mathrm{E} : \mathrm{E} \times \mathrm{F} \to \mathrm{E}$ et $p_\mathrm{F} : \mathrm{E} \times \mathrm{F} \to \mathrm{F}$ sont continues.

(ii) Montrer que G est un sous-espace vectoriel de $\mathrm{E} \times \mathrm{F}$ et que, si G est fermé dans $\mathrm{E} \times \mathrm{F}$, alors u est continue. (On s'intéressera aux restrictions de p_E et p_F à G.)

(iii) Construire $f : \mathbf{R} \to \mathbf{R}$, non continue, avec un graphe fermé.

7. Le dual d'un espace de Banach

Si E est un espace vectoriel normé, on note E^* le *dual* de E, c'est-à-dire l'ensemble des formes linéaires continues sur E. Si $\Lambda : \mathrm{E} \to \mathbf{K}$ est une forme linéaire continue, on rappelle que l'on définit sa norme $\|\Lambda\|$ comme la borne inférieure de l'ensemble des $\mathrm{C} \in \mathbf{R}_+$ tels que $|\Lambda(x)| \leqslant \mathrm{C}\|x\|$ quel que soit $x \in \mathrm{E}$.

Théorème II.1.28. — *Si* E *est un espace vectoriel normé, alors* $(\mathrm{E}^*, \| \ \|)$ *est un espace de Banach.*

Démonstration. — Que $\| \ \|$ soit une norme d'espace vectoriel a déjà été démontré dans le n° 17.3 du Vocabulaire. Maintenant, soit Λ_n une suite d'éléments de E^* telle que $\sum_{n\in\mathbf{N}} \|\Lambda_n\| = \mathrm{C} < +\infty$. Si $x \in \mathrm{E}$, la série $\sum_{n\in\mathbf{N}} \Lambda_n(x)$ est alors absolument convergente, et la somme $\Lambda(x)$ vérifie $|\Lambda(x)| \leqslant \sum_{n\in\mathbf{N}} |\Lambda_n(x)| \leqslant \mathrm{C}\|x\|$. Comme par ailleurs, $x \mapsto \Lambda(x)$ est linéaire, la majoration ci-dessus montre que $x \mapsto \Lambda(x)$ est aussi continue. On en déduit que $\Lambda \in \mathrm{E}^*$ et que $\sum_{n\in\mathbf{N}} \Lambda_n = \Lambda$, ce qui prouve que E est complet.

Théorème II.1.29. — (Hahn-Banach, 1927) *Si* E *est un espace vectoriel normé, si* F *est un sous-espace vectoriel de* E*, et si f est une forme linéaire continue sur* F*, alors il existe* $\Lambda \in \mathrm{E}^*$ *dont la restriction à* F *est f et qui vérifie* $\|\Lambda\| = \|f\|$.

Le théorème de Hahn-Banach, que nous ne démontrerons pas (la démonstration utilise l'axiome du choix), a un certain nombre de conséquences intéressantes, dont le fait que $\mathrm{E}^* \neq 0$. On en trouvera d'autres dans les exercices suivants.

Exercice II.1.30. — Montrer que l'adhérence $\overline{\mathrm{F}}$ de F dans E est l'intersection des noyaux des formes linéaires, continues sur E, nulles sur F.

Exercice II.1.31. — (i) Montrer que, si $x_0 \in \mathrm{E}$, il existe $\Lambda \in \mathrm{E}^*$, avec $\|\Lambda\| = 1$ et $|\Lambda(x_0)| = \|x_0\|$.

(ii) Montrer que E^* sépare les points (si $x \neq y$, il existe $\Lambda \in \mathrm{E}^*$ tel que $\Lambda(x) \neq \Lambda(y)$.)

(iii) Montrer que l'application $\Lambda \mapsto \Lambda(x)$ est une forme linéaire continue sur E^* et induit une isométrie de E dans $(\mathrm{E}^*)^*$. (On dit qu'un espace de Banach E est *réflexif* si cette isométrie est bijective, et donc si E s'identifie au dual de son dual ; il peut arriver que $(\mathrm{E}^*)^*$ soit beaucoup plus gros que E, mais les espaces de Hilbert sont réflexifs d'après le théorème de Riesz (th. II.2.12)).

II.2. Espaces de Hilbert

Les espaces de Hilbert sont des espaces de Banach aux propriétés mathématiques particulièrement agréables : l'existence de bases hilbertiennes montre que tous ceux qu'on rencontre en pratique sont isomorphes, et l'existence de projecteurs orthogonaux permet très souvent de se ramener à la dimension finie. La nature étant bien faite, ce sont précisément ces espaces qui interviennent naturellement dans beaucoup de questions physiques (par exemple en mécanique quantique).

1. Espaces de Hilbert

Un *espace de Hilbert* est un espace préhilbertien (cf. § 18 du Vocabulaire) complet ; c'est donc un cas particulier d'espace de Banach.

Exemple II.2.1. — (i) Un espace de dimension finie muni d'un produit scalaire est un

espace de Hilbert.

(ii) Si E est un espace préhilbertien, son complété $\widehat{\mathrm{E}}$ est un espace de Hilbert (le produit scalaire s'étendant par continuité).

(iii) ℓ^2 et, plus généralement, $\ell^2(\mathrm{I})$ si I est dénombrable, sont des espaces de Hilbert.

(iv) Si Ω est un ouvert non vide de $\mathbf{R}^n$, alors $\mathrm{L}^2(\Omega)$ est un espace de Hilbert.

(v) Le complété $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ de $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ pour la norme $\| \ \|_2$ définie par $\|f\|_2 = \int_0^1 |f(t)|^2 \, dt$ est un espace de Hilbert (de produit scalaire $\langle f, g\rangle = \int_0^1 \overline{f(t)} g(t) \, dt$).

(vi) Les espaces de Sobolev $\mathrm{H}^k(\mathbf{R}^m)$ sont des espaces de Hilbert.

1.1. *Bases hilbertiennes*

Soit E un espace de Hilbert *séparable* [10] de dimension infinie. Une *base hilbertienne* [11] de E est une famille orthonormale dénombrable $(e_i)_{i\in\mathrm{I}}$ d'éléments de E telle que le sous-espace vectoriel de E engendré par les e_i, pour $i \in \mathrm{I}$, soit dense dans E.

Exemple II.2.2. — (i) Si I est un ensemble dénombrable, alors $\ell^2(\mathrm{I})$ possède une base hilbertienne naturelle, à savoir celle constituée des e_i, pour $i \in \mathrm{I}$, où e_i est la suite avec un 1 en i et des 0 partout ailleurs.

(ii) Les $e^{2i\pi nt}$, pour $n \in \mathbf{Z}$ forment une base hilbertienne de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$.

Démonstration. — (i) Que les e_i forment une famille orthonormale est immédiat. Maintenant, si $x = (x_i)_{i\in\mathrm{I}} \in \ell^2(\mathrm{I})$, et si $\mathrm{J} \subset \mathrm{I}$ est fini, alors $\|x - \sum_{j\in\mathrm{J}} x_j e_j\|_2^2 = \sum_{j\in\mathrm{I}-\mathrm{J}} |x_j|^2$. Comme $\sum_{j\in\mathrm{I}} |x_j|^2 < +\infty$, on peut rendre $\|x - \sum_{j\in\mathrm{J}} x_j e_j\|_2$ aussi petit que l'on veut en augmentant J, ce qui prouve que le sous-espace engendré par les e_i, pour $i \in \mathrm{I}$, est dense dans $\ell^2(\mathrm{I})$. On en déduit le (i).

(ii) Un calcul immédiat montre que les $e^{2i\pi nt}$ forment une famille orthonormale ; l'espace qu'elle engendre est l'espace des polynômes trigonométriques. Si $f \in \mathrm{L}^2(\mathbf{R}/\mathbf{Z})$, et si $\varepsilon > 0$, il existe, par définition de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$, une fonction continue g sur $\mathbf{R}/\mathbf{Z}$ avec $\|f - g\|_2 < \frac{\varepsilon}{2}$. Par ailleurs, l'espace des polynômes trigonométriques est dense dans $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ d'après le théorème de Stone-Weierstrass (cf. (iii) de l'ex. II.1.10) ; il existe donc P, polynôme trigonométrique, tel que $\|\mathrm{P} - g\|_\infty < \frac{\varepsilon}{2}$. Comme $\|h\|_2 \leqslant \|h\|_\infty$, si $h \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, on a $\|f - \mathrm{P}\|_2 < \varepsilon$, ce qui prouve que toute boule ouverte de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ contient un polynôme trigonométrique, et donc que l'espace engendré par les $e^{2i\pi nt}$, pour $n \in \mathbf{Z}$, est dense dans $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$. Ceci permet de conclure.

Proposition II.2.3. — *Un espace de Hilbert séparable admet des bases hilbertiennes.*

10. La théorie qui suit s'étend au cas des espaces de Hilbert non séparables, mais ceux-ci ne se rencontrent pas en pratique. La seule différence est qu'une base hilbertienne n'est plus de cardinal dénombrable, si E n'est pas séparable.

11. Une base hilbertienne est aussi souvent appelée une *base orthonormale*. On fera attention au fait qu'une base hilbertienne n'est, en général, pas une base au sens algébrique. Plus précisément, une base hilbertienne est une base algébrique si et seulement si on est en dimension finie, ce qui est rarement le cas en analyse fonctionnelle.

Démonstration. — Soient E un espace de Hilbert séparable et $A \subset E$ un sous-ensemble dénombrable dense. Pour construire une base hilbertienne à partir de A, on numérote les éléments de A, on élimine ceux qui se trouvent dans l'espace vectoriel engendré par les éléments précédents, ce qui nous fournit une base $(b_i)_{i\in I}$, avec $I \subset \mathbf{N}$, de l'espace vectoriel E' engendré par A. Enfin, on utilise le procédé d'orthonormalisation de Schmidt pour construire une famille orthonormale d'éléments de E engendrant le sous-espace E' ; cette famille est une base hilbertienne de E puisque E', qui contient A, est dense dans E.

1.2. *Projection orthogonale sur un sous-espace fermé*

Lemme II.2.4. — *Soit* E *un espace de Hilbert, et soit* $(e_i)_{i\in I}$ *une famille orthonormale dénombrable d'éléments de* E.

(i) *Si* $(x_i)_{i\in I}$ *est une famille d'éléments de* $\mathbf{C}$*, alors la série* $\sum_{i\in I} x_i e_i$ *est sommable si et seulement si* $(x_i)_{i\in I} \in \ell^2(I)$.

(ii) *Si* $(x_i)_{i\in I} \in \ell^2(I)$*, et si* $x \in E$ *est la somme de la série* $\sum_{i\in I} x_i e_i$*, alors* $\langle e_i, x\rangle = x_i$*, pour tout* $i \in I$*, et* $\|x\|^2 = \sum_{i\in I} |x_i|^2$.

Démonstration. — On a $\big\|\sum_{i\in J} x_i e_i\big\| = \big(\sum_{i\in J} |x_i|^2\big)^{1/2}$, pour tout $J \subset I$ fini, par orthonormalité de la famille $(e_i)_{i\in I}$. La sommabilité de $\sum_{i\in J} x_i e_i$ est donc équivalente à la condition $\sum_{i\in I} |x_i|^2 < +\infty$. On en déduit le (i).

Le (ii) est évident si I est fini. On peut donc supposer $I = \mathbf{N}$. Alors x est la limite de la suite de terme général $y_n = \sum_{j=0}^{n} x_j e_j$, et comme on a $\langle e_i, y_n\rangle = x_i$, pour tout $n \geqslant i$, et $\|y_n\|^2 = \sum_{j=0}^{n} |x_j|^2$, le (ii) s'en déduit par un passage à la limite, en utilisant la continuité de la norme et du produit scalaire.

Proposition II.2.5. — *Soit* F *un sous-espace vectoriel fermé de* E *muni d'une base hilbertienne* $(e_i)_{i\in I}$.

(i) *Si* $x \in E$*, alors* $(\langle e_i, x\rangle)_{i\in I} \in \ell^2(I)$.

(ii) *La série* $\sum_{i\in I} \langle e_i, x\rangle e_i$ *est sommable ; sa somme* $p_F(x)$ *appartient à* F*, et on a l'identité* $\|p_F(x)\|^2 = \sum_{i\in I} |\langle e_i, x\rangle|^2$.

(iii) $p_F : E \to F$ *est un projecteur, et* $p_F(x)$ *est l'unique élément de* F *tel que* $x - p_F(x)$ *soit orthogonal à* F *tout entier. De plus,* p_F *est* 1*-lipschitzien.*

Démonstration. — Si F est de dimension finie, le résultat est démontré dans le n° 18.2 du Vocabulaire. On peut donc supposer que $I = \mathbf{N}$. Notons F_i le sous-espace vectoriel de E engendré par les e_j, pour $j \leqslant i$. Alors $y_i = \sum_{j=0}^{i} \langle e_j, x\rangle e_j$ est la projection orthogonale de x sur F_i. En particulier, $\sum_{j=0}^{i} |\langle e_i, x\rangle|^2 = \|y_i\|^2 \leqslant \|x\|^2$, quel que soit $i \in \mathbf{N}$. On en déduit l'appartenance de $(\langle e_i, x\rangle)_{i\in\mathbf{N}}$ à ℓ^2, ce qui démontre le (i).

Le (ii) est une conséquence directe du lemme II.2.4, dont on déduit aussi que $x - p_F(x)$ est orthogonal à tous les e_i, et donc à F tout entier par linéarité et densité. Le reste du (iii) résulte de l'unicité de la projection orthogonale sur un sous-espace (pas forcément fermé, cf. Vocabulaire, n° 18.2). Ceci permet de conclure.

Théorème II.2.6. — *Si $(e_i)_{i\in \mathrm{I}}$ est une base hilbertienne de* E*, l'application $x \mapsto (\langle e_i, x\rangle)_{i\in \mathrm{I}}$ induit une isométrie*[12] *de* E *sur $\ell^2(\mathrm{I})$. Autrement dit,*

(a) *si $x \in \mathrm{E}$, alors $(\langle e_i, x\rangle)_{i\in \mathrm{I}} \in \ell^2(\mathrm{I})$ et $\sum_{i\in \mathrm{I}} |\langle e_i, x\rangle|^2 = \|x\|^2$* (identité de Bessel-Parseval) *;*

(b) *si $(x_i)_{i\in \mathrm{I}} \in \ell^2(\mathrm{I})$, alors $\sum_{i\in \mathrm{I}} x_i e_i$ converge dans* E *et sa somme x vérifie $\langle e_i, x\rangle = x_i$ quel que soit $i \in \mathrm{I}$.*

Démonstration. — Commençons par justifier le « Autrement dit » : le (a) peut se reformuler en disant que $x \mapsto (\langle e_i, x\rangle)_{i\in \mathrm{I}}$ est une isométrie de E sur un sous-espace de $\ell^2(\mathrm{I})$, tandis que le (b) montre que $\ell^2(\mathrm{I})$ est dans l'image de $x \mapsto (\langle e_i, x\rangle)_{i\in \mathrm{I}}$. Maintenant, le (a) résulte des (i) et (ii) de la prop. II.2.5 utilisée pour $\mathrm{F} = \mathrm{E}$, et le (b) suit du lemme II.2.4.

Si on spécialise le th. II.2.6 à la base hilbertienne de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ constituée des $e^{2i\pi\, nt}$, on obtient, en particulier, le résultat suivant.

Corollaire II.2.7. — *Si $f \in \mathrm{L}^2(\mathbf{R}/\mathbf{Z})$, soit $c_n(f)$ son n-ième coefficient de Fourier :*

$$c_n(f) = \langle e^{2i\pi\, nt}, f\rangle = \int_{\mathbf{R}/\mathbf{Z}} f(t)e^{-2i\pi\, nt}\, dt = \int_0^1 f(t)e^{-2i\pi\, nt}\, dt.$$

Alors $f = \sum_{n\in\mathbf{Z}} c_n(f)e^{2i\pi\, nt}$ dans[13] *$\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ et $\sum_{n\in\mathbf{Z}} |c_n(f)|^2 = (\|f\|_2)^2 = \int_0^1 |f(t)|^2\, dt$* (Bessel-Parseval).

Corollaire II.2.8. — (critère de totalité). *Si $(e_i)_{i\in \mathrm{I}}$ est une famille orthonormale dénombrable d'éléments de* E*, les conditions suivantes sont équivalentes :*

(i) *$(e_i)_{i\in \mathrm{I}}$ est une base hilbertienne de* E *;*

(ii) *l'ensemble des $x \in \mathrm{E}$, orthogonaux à tous les e_i, est réduit à $\{0\}$.*

Démonstration. — L'implication (i)⇒(ii) est une conséquence directe du (a) du th. II.2.6 Pour montrer (ii)⇒(i), introduisons l'espace vectoriel F, adhérence dans E de l'espace engendré par les e_i. Alors $(e_i)_{i\in \mathrm{I}}$ est une base hilbertienne de F, et la condition (ii) implique que l'on a $p_{\mathrm{F}}(x) = x$, pour tout $x \in \mathrm{E}$, et donc que $\mathrm{F} = \mathrm{E}$. Ceci permet de conclure.

2. Le théorème de projection sur un convexe

Rappelons que, si E est un espace vectoriel sur $\mathbf{K}$, un sous-ensemble C de E est *convexe* si C contient le segment $[x, y]$ quels que soient $x, y \in \mathrm{C}$. En particulier, si C est convexe,

12. Un sous-espace fermé de dimension infinie de ℓ^2 est un espace de Hilbert séparable, et donc, d'après le théorème, isomorphe à ℓ^2. T. Gowers a reçu la médaille Fields en 1998, en grande partie pour avoir démontré (1996) que ceci caractérise ℓ^2 : un espace de Banach séparable, qui est isomorphe à tous ses sous-espaces fermés de dimension infinie, est isomorphe à ℓ^2.

13. On prendra garde au fait que cette convergence dans $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ (convergence en moyenne quadratique) n'implique la convergence en aucun point ; de fait, rien n'empêche a priori que tout réarrangement de la série diverge en tout point sauf celui où on s'est débrouillé pour le faire converger.

et si $x, y \in \mathrm{C}$, alors le milieu $\frac{x+y}{2}$ de x et y appartient à C. Le théorème suivant joue un rôle fondamental en analyse fonctionnelle.

Théorème II.2.9. — *Soient* E *un espace de Hilbert et* $\mathrm{C} \neq \varnothing$ *un convexe fermé de* E.

(i) *Quel que soit* $x \in \mathrm{E}$*, il existe* $p_{\mathrm{C}}(x) \in \mathrm{C}$ *unique* (appelé la projection de x sur C) *tel que* $d(x, p_{\mathrm{C}}(x)) \leqslant d(x, y)$*, pour tout* $y \in \mathrm{C}$.

(ii) $p_{\mathrm{C}}(x)$ *est l'unique point* y *de* C *tel que, quel que soit* $z \in \mathrm{C}$*, l'angle* $(x - y, z - y)$ *soit obtus* (*i.e.* $\mathrm{Re}(\langle x - y, z - y\rangle) \leqslant 0$).

(iii) *L'application* $x \mapsto p_{\mathrm{C}}(x)$ *est* 1*-lipschitzienne.*

Démonstration. — Notons $d(x, \mathrm{C})$ la borne inférieure des $d(x, y)$, pour $y \in \mathrm{C}$. Si y_1, y_2 réalisent cette borne inférieure, et si $z = \frac{y_1+y_2}{2}$, alors $z \in \mathrm{C}$, et l'identité de la médiane nous donne

$$\|y_1 - y_2\|^2 = 2\|y_1 - x\|^2 + 2\|y_2 - x\|^2 - 4\|z - x\|^2 = 4(d(x, \mathrm{C})^2 - d(x, z)^2) \leqslant 0.$$

On a donc $y_1 = y_2$, d'où l'unicité de la projection.

Passons à l'existence [14]. Par définition de $d(x, \mathrm{C})$, il existe une suite $(y_n)_{n\in\mathbf{N}}$ d'éléments de C, telle que $d(x, y_n)$ tende vers $d(x, \mathrm{C})$ quand n tend vers $+\infty$. L'identité de la médiane se traduit, en notant $z_{n,m}$ le milieu de y_n et y_m, par

$$\begin{aligned}\|y_n - y_{n+p}\|^2 =& 2\|y_n - x\|^2 + 2\|y_{n+p} - x\|^2 - 4\|z_{n,n+p} - x\|^2\\ \leqslant& 2(\|y_n - x\|^2 + \|y_{n+p} - x\|^2 - 2d(x, \mathrm{C})^2).\end{aligned}$$

Comme par hypothèse, le membre de droite tend vers 0 quand $n \to +\infty$ et $p \in \mathbf{N}$, la suite $(y_n)_{n\in\mathbf{N}}$ est de Cauchy, et comme on a supposé C fermé dans un espace complet, elle converge vers un élément $p_{\mathrm{C}}(x)$ appartenant à C. Par continuité de la norme, on a $d(x, p_{\mathrm{C}}(x)) = \lim_{n\to+\infty} d(x, y_n) = d(x, \mathrm{C})$, ce qui démontre le (i).

Soit $z \in \mathrm{C}$. Si $0 < t < 1$, le point $y_t = (1 - t)p_{\mathrm{C}}(x) + tz$ appartient à C, et donc

$$\|p_{\mathrm{C}}(x) - x\|^2 \leqslant \|y_t - x\|^2 = \|p_{\mathrm{C}}(x) - x\|^2 + t^2\|z - p_{\mathrm{C}}(x)\|^2 + 2t\mathrm{Re}\langle p_{\mathrm{C}}(x) - x, z - p_{\mathrm{C}}(x)\rangle.$$

En faisant tendre t vers 0, on en déduit l'inégalité $\mathrm{Re}\langle x - p_{\mathrm{C}}(x), z - p_{\mathrm{C}}(x)\rangle \leqslant 0$. Réciproquement, si $\mathrm{Re}\langle x - y, z - y\rangle \leqslant 0$, alors

$$\|z - x\|^2 = \|y - x\|^2 + \|z - y\|^2 - 2\mathrm{Re}\langle x - y, z - y\rangle \geqslant \|y - x\|^2,$$

ce qui montre que, si $\mathrm{Re}\langle x - y, z - y\rangle \leqslant 0$ quel que soit $z \in \mathrm{C}$, alors y vérifie la propriété définissant $p_{\mathrm{C}}(x)$. On en déduit le (ii).

Enfin, si $x, y \in \mathrm{E}$, on a

$$\mathrm{Re}\langle x - p_{\mathrm{C}}(x), p_{\mathrm{C}}(y) - p_{\mathrm{C}}(x)\rangle \leqslant 0 \quad \text{et} \quad \mathrm{Re}\langle y - p_{\mathrm{C}}(y), p_{\mathrm{C}}(x) - p_{\mathrm{C}}(y)\rangle \leqslant 0.$$

On en déduit, en faisant la somme, l'inégalité

$$\mathrm{Re}\langle x - y, p_{\mathrm{C}}(y) - p_{\mathrm{C}}(x)\rangle \geqslant \mathrm{Re}\langle p_{\mathrm{C}}(y) - p_{\mathrm{C}}(x), p_{\mathrm{C}}(y) - p_{\mathrm{C}}(x)\rangle = \|p_{\mathrm{C}}(y) - p_{\mathrm{C}}(x)\|^2.$$

14. En dimension finie, un petit argument de compacité permettrait de la démontrer (exercice).

On conclut la démonstration du (iii) en utilisant l'inégalité de Cauchy-Schwarz, selon laquelle

$$\mathrm{Re}\langle x-y, p_{\mathrm{C}}(y)-p_{\mathrm{C}}(x)\rangle \leqslant |\langle x-y, p_{\mathrm{C}}(y)-p_{\mathrm{C}}(x)\rangle| \leqslant \|x-y\|\cdot\|p_{\mathrm{C}}(y)-p_{\mathrm{C}}(x)\|.$$

3. Le dual d'un espace de Hilbert

Dans ce n°, E est un space de Hilbert. Si $x \in \mathrm{E}$, on note Λ_x la forme linéaire définie par $\Lambda_x(y) = \langle x, y\rangle$.

Lemme II.2.10. — *Si $x \in \mathrm{E}$, la forme linéaire Λ_x est continue et $\|\Lambda_x\| = \|x\|$.*

Démonstration. — L'inégalité de Cauchy-Schwarz qui devient $|\Lambda_x(y)| \leqslant \|x\|\cdot\|y\|$, nous donne la continuité de Λ_x ainsi que l'inégalité $\|\Lambda_x\| \leqslant \|x\|$. L'inégalité $\|\Lambda_x\| \geqslant \|x\|$, se déduit de ce que $|\Lambda_x(x)| = \|x\|\cdot\|x\|$.

Proposition II.2.11. — *Soit* E *un espace de Hilbert séparable.*

(i) *Si* A *est une partie de* E, *alors* l'orthogonal $\mathrm{A}^\perp$ de A (i.e. l'ensemble des $x \in \mathrm{E}$ tels que $\langle x, a\rangle = 0$, quel que soit $a \in \mathrm{A}$) *est un sous-espace vectoriel fermé de* E.

(ii) *Si* F *est un sous-espace vectoriel fermé de* E, *et si $x \in \mathrm{E}$, alors $x - p_{\mathrm{F}}(x) \in \mathrm{F}^\perp$, et on a*[15] $\mathrm{E} = \mathrm{F} \oplus \mathrm{F}^\perp$ *et* $(\mathrm{F}^\perp)^\perp = \mathrm{F}$.

Démonstration. — (i) On a $\langle x, a\rangle = 0$ si et seulement si $\Lambda_a(x) = 0$, et comme Λ_a est continue, son noyau H_a est un hyperplan fermé de E, ce qui démontre le (i) puisque $\mathrm{A}^\perp = \cap_{a\in\mathrm{A}}\mathrm{H}_a$.

(ii) On a $x - p_{\mathrm{F}}(x) \in \mathrm{F}^\perp$ par définition. Maintenant, si $x \in \mathrm{F}\cap\mathrm{F}^\perp$, alors $\langle x, x\rangle = 0$, et donc $x = 0$; on en déduit que $\mathrm{F}\cap\mathrm{F}^\perp = \{0\}$. Par ailleurs, $x = (x - p_{\mathrm{F}}(x)) + p_{\mathrm{F}}(x)$, avec $x - p_{\mathrm{F}}(x) \in \mathrm{F}^\perp$ et $p_{\mathrm{F}}(x) \in \mathrm{F}$. On en déduit que $\mathrm{E} = \mathrm{F} + \mathrm{F}^\perp$ et donc que $\mathrm{E} = \mathrm{F} \oplus \mathrm{F}^\perp$. Enfin, l'unicité de la projection sur un convexe fermé montre que $p_{\mathrm{F}^\perp}(x) = x - p_{\mathrm{F}}(x)$, et donc que $x = p_{\mathrm{F}}(x) + p_{\mathrm{F}^\perp}(x)$. Comme on a aussi $x = p_{\mathrm{F}^\perp}(x) + p_{(\mathrm{F}^\perp)^\perp}(x)$, on en déduit que $p_{(\mathrm{F}^\perp)^\perp}(x) = p_{\mathrm{F}}(x)$, quel que soit $x \in \mathrm{E}$, et finalement que $(\mathrm{F}^\perp)^\perp = \mathrm{F}$.

Théorème II.2.12. — (Théorème de Riesz) *Si* E *est un espace de Hilbert séparable, alors l'application qui associe, à $x \in \mathrm{E}$, la forme linéaire Λ_x, définie par $\Lambda_x(y) = \langle x, y\rangle$, est une isométrie de* E *sur son dual* E^*. *Autrement dit :*

15. Il ressort de ce théorème que tout sous-espace vectoriel fermé d'un espace de Hilbert admet un supplémentaire fermé. Réciproquement, J. Lindenstrauss et L. Tzafriri (1971) ont démontré qu'un espace de Banach séparable ayant cette propriété est isomorphe à ℓ^2.

Une question ouverte concernant la classification des espaces de Banach séparables est de savoir si ℓ^2 est le seul pour lequel le groupe des isométries (applications linéaires bijectives, vérifiant $\|u(z)\| = \|z\|$, quel que soit z) agit transitivement sur la sphère unité (i.e. si, quels que soient x, y de norme 1, il existe une isométrie u, avec $u(x) = y$). En dimension finie, l'énoncé analogue est vrai : le groupe des isométries de E est compact car fermé et borné dans GL(E), et donc possède une mesure de Haar ce qui permet de construire un produit scalaire invariant par G en faisant la moyenne comme dans le th. I.2.6 ; l'hypothèse de transitivité montre que la boule unité est une homothétique de celle pour ce produit scalaire.

(i) *si* $x \in \mathrm{E}$*, la forme linéaire* Λ_x *est continue et* $\|\Lambda_x\| = \|x\|$ *;*

(ii) *si* $\Lambda : \mathrm{E} \to \mathbf{K}$ *est une forme linéaire continue, il existe* (un unique) $x \in \mathrm{E}$ *tel que* $\Lambda(y) = \langle x, y\rangle$ *quel que soit* $y \in \mathrm{E}$*.*

Démonstration. — Le (i) a déjà été démontré (c'est le contenu du lemme II.2.10). Passons à la démonstration du (ii) [16].

Première demonstration. Supposons Λ non nulle sinon il n'y a qu'à prendre $x = 0$. Soit H le noyau de Λ. C'est un hyperplan de E, qui est fermé puisque Λ est continue. Soit $h \in \mathrm{H}^\perp$, non nul. Comme $\mathrm{H} \cap \mathrm{H}^\perp = \{0\}$, et comme H est le noyau de Λ, on a $\Lambda(h) \neq 0$. Soit $y \in \mathrm{E}$ et soit $z = y - \frac{\Lambda(y)}{\Lambda(h)}h$. On a $\Lambda(z) = 0$, et donc $z \in \mathrm{H}$, ce qui implique $\langle h, z\rangle = 0$ et se traduit par $\langle h, y\rangle = \frac{\|h\|^2}{\Lambda(h)}\Lambda(y)$ quel que soit $y \in \mathrm{E}$. Autrement dit, si on pose $x = \frac{\overline{\Lambda}(h)}{\|h\|^2}\, h$, on a $\Lambda(y) = \Lambda_x(y)$ quel que soit $y \in \mathrm{E}$. Ceci permet de conclure.

Seconde demonstration. Comme E est supposé séparable, il est isométrique à ℓ^2, et on peut donc supposer que $\mathrm{E} = \ell^2$. On note e_n, pour $n \in \mathbf{N}$, la base hilbertienne standard de ℓ^2 (i.e. e_n est la suite dont tous les termes sont nuls sauf le n-ième qui est égal à 1), et on pose $a_n = \Lambda(e_n)$. Notons $\pi_n : \ell^2 \to \ell^2$, l'application $(y_i)_{i\in\mathbf{N}} \mapsto (z_i)_{i\in\mathbf{N}}$, avec $z_i = y_i$, si $i \leqslant n$, et $z_i = 0$, si $i > n$. Alors π_n est linéaire, continue car $\|\pi_n(y)\|_2 \leqslant \|y\|_2$, et on a $\pi_n(y) \to y$, pour tout $y \in \ell^2$. Soit $\Lambda_n = \Lambda \circ \pi_n$. Par linéarité, on a

$$\Lambda_n(y) = \Lambda\big(\sum\nolimits_{i\leqslant n} y_i e_i\big) = \sum\nolimits_{i\leqslant n} a_i y_i = \langle x^{(n)}, y\rangle,$$

où $x^{(n)} \in \ell^2$ est définie par $x_i^{(n)} = \overline{a_i}$, si $i \leqslant n$, et $x_i^{(n)} = 0$, si $i > n$. On déduit du (i) que $\|\Lambda_n\| = \|x^{(n)}\|_2$. Par ailleurs, si $y \in \ell^2$, on a $\Lambda_n(y) \to \Lambda(y)$, puisque $\pi_n(y) \to y$ et Λ est continue. Il résulte du th. de Banach-Steinhaus que $\|\Lambda_n\|$ est bornée et donc que $\|x^{(n)}\|_2$ est majorée. Ceci implique que $x = (\overline{a_n})_{n\in\mathbf{N}} \in \ell^2$. Par ailleurs, $y \mapsto \Lambda'(y) = \Lambda(y) - \langle x, y\rangle$ est une forme linéaire continue sur ℓ^2, nulle sur e_n pour tout n, et donc identiquement nulle puisque les e_n engendrent un sous-espace dense de ℓ^2. Ceci permet de conclure.

II.3. Exercices

1. Espaces de Banach

Exercice II.3.1. — Soient f continue et périodique de période 1 et α irrationnel. Montrer que

$$\lim_{\mathrm{N}\to+\infty} \frac{1}{\mathrm{N}} \sum_{n=1}^{\mathrm{N}} f(n\alpha) = \int_0^1 f(t)\, dt$$

(commencer par un polynôme trigonométrique).

Exercice II.3.2. — a) La forme linéaire $f \mapsto \int_{-\infty}^{\infty} f(t)dt = \mathrm{I}(f)$ sur $\mathscr{C}_c(\mathbf{R})$ s'étend-elle en une forme linéaire continue sur $\mathrm{L}^2(\mathbf{R})$?

16. C'est la partie non triviale du théorème et celle qui a les conséquences les plus spectaculaires en analyse fonctionnelle. On en déduit sans effort des tas de théorèmes d'existence.

b) Soit e_n la fonction valant $\frac{1}{n}$ sur $[0,n]$, et 0 ailleurs. Montrer que $e_n \in \mathrm{L}^2(\mathbf{R})$, et que la suite $(e_n)_{n\geqslant 1}$ tend vers 0 dans L^2. En déduire que le sous-espace $\{f \in \mathscr{C}_c(\mathbf{R}) : \mathrm{I}(f) = 0\}$ est dense dans $\mathrm{L}^2(\mathbf{R})$.

c) Relation entre a) et b) ?

Exercice II.3.3. — Soit $a = (a_n)_{n\in\mathbf{N}} \in \ell^\infty$ une suite bornée de nombres complexes.

(i) Montrer que, si $x = (x_n)_{n\in\mathbf{N}} \in \ell^2$, alors $(a_n x_n)_{n\in\mathbf{N}} \in \ell^2$, et que l'application linéaire $f : \ell^2 \to \ell^2$ ainsi définie est continue.

(ii) Montrer que, si f est surjective, il existe $\mathrm{C} > 0$ tel que $|a_n| \geqslant \mathrm{C}$, pour tout $n \in \mathbf{N}$. (On pourra commencer par montrer que f est injective.)

Exercice II.3.4. — (i) Montrer que, si $a = (a_n)_{n\in\mathbf{N}} \in \ell^\infty$, et si $b = (b_n)_{n\in\mathbf{N}} \in \ell^1$, alors la série $\sum_{n\in\mathbf{N}} a_n b_n$ converge. On note $\Lambda_a(b)$ la somme de la série.

(ii) Montrer que l'application $\Lambda_a : \ell^1 \to \mathbf{C}$ ainsi définie appartient à $(\ell^1)^*$, et que $\|\Lambda_a\| = \|a\|_\infty$.

(iii) Montrer que $a \mapsto \Lambda_a$ est une isométrie de ℓ^∞ sur $(\ell^1)^*$. (On pourra s'inspirer de la seconde démonstration du th. II.2.12.)

Exercice II.3.5. — Montrer qu'un espace de Banach possédant une famille génératrice dénombrable est de dimension finie. (Si $(e_n)_{n\in\mathbf{N}}$ est une telle famille, on pourra considérer le sous-espace F_n engendré par les e_i, pour $i \leqslant n$.)

Exercice II.3.6. — Soit I un intervalle de $\mathbf{R}$, et soit $(f_n)_{n\in\mathbf{N}}$ une suite de fonctions continues sur I tendant simplement vers une fonction f. Si $j \in \mathbf{N}$, soit

$$\mathrm{F}_{n,j} = \cap_{p\geqslant n}\{x \in \mathrm{I},\ |f_{n+p}(x) - f_n(x)| \leqslant 2^{-j}\}.$$

(i) Montrer que $\mathrm{F}_{n,j}$ est fermé et que $\cup_{n\in\mathbf{N}}\mathrm{F}_{n,j} = \mathrm{I}$.

(ii) Soient $\mathrm{U}_{n,j}$ l'intérieur de $\mathrm{F}_{n,j}$ et $\mathrm{U}_j = \cup_{n\in\mathbf{N}}\mathrm{U}_{n,j}$. Montrer que U_j est dense dans I.

(iii) Montrer que si $x \in \mathrm{U}_j$, il existe V_x ouvert contenant x tel que $|f(x) - f(y)| \leqslant 2^{2-j}$, si $y \in \mathrm{V}_x$. En déduire que f est continue en au moins un point de I.

2. Espaces de Hilbert

Exercice II.3.7. — Quelle est la valeur maximale de $\int_{-1}^1 xf(x)dx$ pour $f \in \mathrm{L}^2([-1,1])$ soumis aux conditions $\int_{-1}^1 f(x)dx = 0$ et $\int_{-1}^1 f(x)^2 = 1$.

Exercice II.3.8. — Soit $(a_n)_{n\in\mathbf{N}}$ une suite de nombres complexes telle que, quelle que soit $(b_n)_{n\in\mathbf{N}} \in \ell^2$, la série $\sum_{n=0}^{+\infty} a_n b_n$ converge. Montrer que $\sum_{n=0}^{+\infty} |a_n|^2 < +\infty$. (On pourra considérer la suite de formes linéaires $\Lambda_k : \ell^2 \to \mathbf{C}$, pour $k \in \mathbf{N}$, définie par $\Lambda_k((b_n)_{n\in\mathbf{N}}) = \sum_{n=0}^k a_n b_n$. Les nostalgiques des classes préparatoires pourront considérer la suite de terme général $b_n = \frac{\overline{a}_n}{\sum_{i=0}^n |a_i|^2}$.)

Exercice II.3.9. — Soit E un espace de Hilbert de dimension infinie.

(i) Montrer, en exhibant une suite sans valeur d'adhérence, que la boule unité de E n'est pas compacte.

(ii) Construire un sous-ensemble fermé F de E tel que 0 n'ait pas de projection sur F (c'est-à-dire tel qu'il n'existe pas d'élément de F de norme minimale).

Exercice II.3.10. — Soit $(\mathrm{E}, \|\ \|)$ un espace de Hilbert.

(i) Soient a, x, y des points de E vérifiant

$$\|x - a\|, \|y - a\| \leqslant r_2 \quad \text{et} \quad \|\frac{x+y}{2} - a\| \geqslant r_1.$$

Montrer que $\|x - y\| \leqslant 4(r_2^2 - r_1^2)$.

(ii) Soit $(\mathrm{C}_n)_{n\in\mathbf{N}}$ une suite décroissante de convexes fermés non vides. Vérifier que $\mathrm{C} = \cap_{n=0}^{+\infty}\mathrm{C}_n$ est un convexe fermé. Montrer que C est non vide si et seulement si $\sup_{n\in\mathbf{N}} d(0,\mathrm{C}_n) < +\infty$. On montrera en particulier que sous cette condition, si $x \in \mathrm{E}$, alors $\mathrm{P}_{\mathrm{C}_n}(x)$ tend vers $\mathrm{P}_{\mathrm{C}}(x)$.

(iii) Soit $\varphi : \mathrm{E} \to \mathbf{R}$ une fonction convexe (c'est-à-dire telle que $\varphi(tx+(1-t)y) \leqslant t\varphi(x)+(1-t)\varphi(y)$ quels que soient $t \in [0,1]$ et $x, y \in \mathrm{E}$) telle que $\lim_{\|x\|\to\infty} \varphi(x) = +\infty$. Montrer que φ est bornée inférieurement sur E et atteint son minimum.

Exercice II.3.11. — Soit E un espace de Hilbert et $(e_n)_{n\in\mathbf{N}}$ une famille orthonormale. Soit $(a_n)_{n\in\mathbf{N}}$ une suite de réels positifs. Montrer que $\mathrm{C} = \mathrm{B}(0,1) \cap \{\sum_{n=0}^{+\infty} x_n e_n \mid x_n \in [-a_n, a_n]\}$ est compact si et seulement si $\sum_{n=0}^{+\infty} a_n^2 < +\infty$.

Exercice II.3.12. — (Polynômes de Legendre) On note P_n le polynôme $\frac{d^n}{dx^n}(1-x^2)^n$. Montrer que les P_n forment une famille orthogonale dans $\mathrm{L}^2([-1,1])$, et que les $\mathrm{P}_n/\|\mathrm{P}_n\|_2$ forment une base hilbertienne de $\mathrm{L}^2([-1,1])$.

Exercice II.3.13. — Soit E un espace de Hilbert, et soit $\mathrm{A} : \mathrm{E} \to \mathrm{E}$, linéaire, vérifiant $\langle \mathrm{A}x, y\rangle = \langle x, \mathrm{A}y\rangle$, pour tous $x, y \in \mathrm{E}$. Montrer que A est continue. (On utilisera le résultat de l'ex. II.1.27.)

Exercice II.3.14. — Soit $\mathrm{L}^2([0,1])$ le complété de $\mathscr{C}([0,1])$ pour le produit scalaire $\langle f, g\rangle = \int_0^1 \overline{f(t)}g(t)\,dt$.

(i) Soient $\mathrm{X}_1, \ldots, \mathrm{X}_n$ des variables. Montrer que le déterminant de la matrice des $(\frac{1}{\mathrm{X}_i+\mathrm{X}_j})_{1\leqslant i,j\leqslant n}$ est

$$\Delta_n(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \frac{\prod_{i<j}(\mathrm{X}_i - \mathrm{X}_j)^2}{\prod_{i,j}(\mathrm{X}_i + \mathrm{X}_j)}.$$

(ii) Soit $1 \leqslant a_1 < a_2 < \ldots$ une suite d'entiers strictement croissante. Si $n \in \mathbf{N}$, notons $\mathrm{Vect}(x^{a_1}, \ldots, x^{a_n})$ le sous-espace de $\mathscr{C}([0,1])$ engendré par les x^{a_i}, pour $1 \leqslant i \leqslant n$. Montrer que, si $k \in \mathbf{N}$, alors

$$d(x^k, \mathrm{Vect}(x^{a_1}, \ldots, x^{a_n}))^2 = \frac{\Delta_{n+1}(k+\frac{1}{2}, a_1+\frac{1}{2}, \ldots, a_n+\frac{1}{2})}{\Delta_n(a_1+\frac{1}{2}, \ldots, a_n+\frac{1}{2})}.$$

(iii) Montrer que $\mathrm{Vect}(x^{a_i},\ i \in \mathbf{N})$ est dense dans $\mathrm{L}^2([0,1])$, si et seulement si $\sum_{n=1}^{+\infty} \frac{1}{a_i} = +\infty$.

Exercice II.3.15. — (i) Soit $\mathscr{C}_c([1,+\infty[)$ l'espace des $\phi : [1,+\infty[\to \mathbf{C}$, continues, à support compact. Montrer que $(f,g) \mapsto \langle f, g\rangle = \int_1^{+\infty} \overline{f(t)}g(t)\,\frac{dt}{t^2}$ est un produit scalaire sur $\mathscr{C}_c([1,+\infty[)$, pour lequel $\mathscr{C}_c([1,+\infty[)$ n'est pas complet.

(ii) On note E le complété de $\mathscr{C}_c([1,+\infty[)$ pour ce produit scalaire. Si n est un entier $\geqslant 2$, soit $\phi_n : [1,+\infty[\to \mathbf{C}$ la fonction définie par $\phi_n(t) = [\frac{t}{n}] - \frac{[t]}{n}$. Montrer que $\phi_n \in \mathrm{E}$.

(iii) Montrer que l'adhérence dans E de l'espace engendré par les ϕ_n, pour $n \geqslant 2$, contient l'espace des fonctions constantes sur $[1,+\infty[$. (Indication : consulter l'ex. VII.5.2.)

3. Séries de Fourier

Exercice II.3.16. — Soit f la fonction périodique de période 1 telle que l'on ait $f(x) = x$ si $x \in]-\frac{1}{2}, \frac{1}{2}]$. Calculer les coefficients de Fourier de f ; en déduire la valeur de $\sum_{n=1}^{+\infty} \frac{1}{n^2}$.

Si $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, et si $\mathrm{N} \in \mathbf{N}$, soit $\Lambda_{\mathrm{N}}(f) = \sum_{k=-\mathrm{N}}^{\mathrm{N}} c_k(f)$. Plus généralement, si $x \in \mathbf{R}/\mathbf{Z}$, soit $\Lambda_{\mathrm{N},x}(f) = \sum_{k=-\mathrm{N}}^{\mathrm{N}} c_k(f)e^{2i\pi\,kx}$. Notre but est d'étudier la convergence des sommes partielles symétriques $\Lambda_{\mathrm{N},x}(f)$ de la série de Fourier de f vers $f(x)$.

Comme question préliminaire, on montrera que Λ_{N} est une forme linéaire continue sur $\mathscr{C}(\mathbf{R}/\mathbf{Z})$, et on établira la formule $\Lambda_{\mathrm{N}}(f) = \int_0^1 \mathrm{S}_{\mathrm{N}}(t)f(t)\,dt$, où $\mathrm{S}_{\mathrm{N}}(t) = \frac{\sin(2\mathrm{N}+1)\pi t}{\sin \pi t}$.

Exercice II.3.17. — (i) Montrer que $\|\Lambda_N\| = \|S_N\|_1$.

(ii) Montrer que $\|\Lambda_N\|$ tend vers $+\infty$; en déduire que $\{f \in \mathscr{C}(\mathbf{R}/\mathbf{Z}),\ \sup_{N\in\mathbf{N}} |\Lambda_N(f)| = +\infty\}$ est un G_δ dense dans $\mathscr{C}(\mathbf{R}/\mathbf{Z})$.

(iii) Montrer que, si $r \in \mathbf{Q}$, l'ensemble des $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ tels que $\sup_{N\in\mathbf{N}} |\Lambda_{N,r}(f)| = +\infty$ est un G_δ dense dans $\mathscr{C}(\mathbf{R}/\mathbf{Z})$. En déduire qu'il existe un G_δ dense X de $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ tel que $\sup_{N\in\mathbf{N}} |\Lambda_{N,r}(f)| = +\infty$ quels que soient $f \in X$ et $r \in \mathbf{Q}$.

(iv) Montrer que, si $f \in X$, et si $M \in \mathbf{N}$, alors l'ensemble des $x \in \mathbf{R}/\mathbf{Z}$ tels que $\sup_{N\in\mathbf{N}} |\Lambda_{N,x}(f)| > M$ est un ouvert contenant $\mathbf{Q}/\mathbf{Z}$. En déduire que, si $f \in X$, il existe un G_δ dense Y_f de $\mathbf{R}/\mathbf{Z}$ tel que $\sup_{N\in\mathbf{N}} |\Lambda_{N,x}(f)| = +\infty$, quel que soit [17] $x \in Y_f$.

Exercice II.3.18. — Soit $L^1(\mathbf{R}/\mathbf{Z})$ le complété de $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ pour la norme $\|f\|_1 = \int_0^1 |f(t)|\,dt$.

(i) Montrer que, si $k \in \mathbf{Z}$, $f \mapsto c_k(f)$ s'étend par continuité à $L^1(\mathbf{R}/\mathbf{Z})$.

(ii) Montrer que, si $f \in L^1(\mathbf{R}/\mathbf{Z})$, alors $c_k(f) \to 0$ quand $|k| \to +\infty$.

(iii) On suppose f hölderienne d'exposant $\alpha > 0$ (i.e il existe $C > 0$ tel que $|f(x) - f(y)| \leqslant C|x-y|^\alpha$ quels que soient $x, y \in [0,1]$). Montrer que, si $x \in \mathbf{R}$, alors la suite de terme général $\sum_{k=-N}^{N} c_k(f)e^{2i\pi kx}$ tend vers $f(x)$.

II.4. Espaces de Banach p-adiques

1. Définition et exemples

Un espace de Banach p-adique est un espace de Banach sur [18] $\mathbf{Q}_p$, mais comme la norme sur $\mathbf{Q}_p$ est ultramétrique, il est naturel d'imposer à la norme de l'espace de l'être aussi, ce qui nous amène à la définition suivante.

Définition II.4.1. — Un *espace de Banach p-adique* est un $\mathbf{Q}_p$-espace vectoriel E muni d'une norme ultramétrique $\|\ \|$ (i.e. $\|x+y\| \leqslant \sup(\|x\|, \|y\|)$ et $\|\lambda x\| = |\lambda|_p\|x\|$, si $\lambda \in \mathbf{Q}_p$, $x, y \in E$) pour laquelle il est complet.

Remarque II.4.2. — (i) Si E est un espace de Banach p-adique, l'ultramétricité de la norme fait que sa boule unité $E^0 = \{x \in E,\ \|x\| \leqslant 1\}$ est un sous-groupe additif de E stable par multiplication par un élément de $\mathbf{Z}_p$ (i.e. c'est un sous-$\mathbf{Z}_p$-module du $\mathbf{Q}_p$-espace vectoriel E).

17. Autrement dit, il existe un sous-ensemble non dénombrable dense X de $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ tel que, si $f \in X$, alors la série de Fourier de f diverge en tout point d'un sous-ensemble non dénombrable dense de $\mathbf{R}/\mathbf{Z}$. Malgré ce résultat peu encourageant, Carleson (prix Abel 2006) a démontré en 1965 que, si $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ (et même si $f \in L^2(\mathbf{R}/\mathbf{Z})$), alors $\Lambda_{N,x}(f) \to f(x)$ pour presque tout x (au sens du chapitre suivant). Par contre, Kolmogorov (1926) a montré qu'il existe des éléments de $L^1(\mathbf{R}/\mathbf{Z})$ dont la transformée de Fourier diverge en tout point.

18. De la même manière que l'on peut considérer des espaces de Banach sur $\mathbf{R}$ ou $\mathbf{C}$, on pourrait remplacer $\mathbf{Q}_p$ par n'importe quel corps complet pour la norme p-adique comme, par exemple, une extension finie de $\mathbf{Q}_p$ ou le corps $\mathbf{C}_p$.

(ii) L'ultramétricité de la norme et la complétude de l'espace font qu'une série $\sum_{i\in \mathrm{I}} x_i$ converge dans E si et seulement si $x_i \to 0$ à l'infini [19].

Hypothèse II.4.3. — On dit que E vérifie l'hypothèse (N) si quel que soit $x \in \mathrm{E}$, il existe $\lambda \in \mathbf{Q}_p$ tel que $\|x\| = |\lambda|_p$.

Lemme II.4.4. — *Si* $(\mathrm{E}, \| \ \|)$ *est un espace de Banach p-adique, on peut trouver une norme* $\| \ \|_1$ *sur* E *qui est équivalente à* $\| \ \|$ *et qui vérifie l'hypothèse* (N).

Démonstration. — Si $x \in \mathrm{E}$, soit $v_p(x)$ l'élément de $\mathbf{R} \cup \{+\infty\}$ défini par $\|x\| = p^{-v_p(x)}$. et soit $\|x\|_1 = p^{-[v_p(x)]}$, où, si $v \in \mathbf{R}$, $[v]$ désigne la partie entière de v. Alors $\| \ \|_1$ est une norme ultramétrique sur E et on a de plus $\frac{1}{p}\|x\|_1 \leqslant \|x\| \leqslant \|x\|_1$.

Exemple II.4.5. — (i) Si I est un ensemble, soit $\ell^\infty(\mathrm{I})$ l'ensemble des suites bornées $(a_i)_{i\in \mathrm{I}}$ d'éléments de $\mathbf{Q}_p$. On munit $\ell^\infty(\mathrm{I})$ de la norme $\| \ \|_\infty$ définie par $\|(a_i)_{i\in \mathrm{I}}\|_\infty = \sup_{i\in \mathrm{I}} |a_i|_p$, ce qui en fait un espace de Banach p-adique.

(ii) Soit $\ell_0^\infty(\mathrm{I})$ le sous-espace de $\ell^\infty(\mathrm{I})$ des suites $(a_i)_{i\in \mathrm{I}}$ tendant vers 0 à l'infini. C'est un espace de Banach p-adique comme sous-espace fermé d'un espace de Banach p-adique. C'est aussi l'adhérence dans $\ell^\infty(\mathrm{I})$ de l'espace des suites n'ayant qu'un nombre fini de termes non nuls.

(iii) Si X est un espace topologique compact, l'espace $\mathscr{C}(\mathrm{X})$ des applications continues de X dans $\mathbf{Q}_p$ muni de la norme $\| \ \|_\infty$ définie par $\|\phi\|_\infty = \sup_{x\in \mathrm{X}} |\phi(x)|_p$ est un espace de Banach p-adique.

(iv) On trouvera d'autres exemples intéressants dans l'annexe D.

2. Bases orthonormales

La théorie des espaces de Banach p-adiques est très loin d'être aussi riche que son homologue archimédienne ; elle se rapproche plutôt de celle des espaces de Hilbert. En particulier, la notion suivante remplace celle de base hilbertienne dans un espace de Hilbert.

Définition II.4.6. — Soit E un espace de Banach p-adique. On dit qu'une famille bornée $(e_i)_{i\in \mathrm{I}}$ est une *base orthonormale* de E si $(a_i)_{i\in \mathrm{I}} \mapsto \sum_{i\in \mathrm{I}} a_i e_i$ est une isométrie de $\ell_0^\infty(\mathrm{I})$ sur E. On dit que c'est une *base de Banach* si cette application est un isomorphisme d'espaces de Banach p-adiques (une base orthonormale est donc une base de Banach).

Autrement dit, une famille $(e_i)_{i\in \mathrm{I}}$ est une base orthonormale de E si et seulement si

(i) tout élément x de E peut s'écrire de manière unique sous la forme d'une série convergente $x = \sum_{i\in \mathrm{I}} a_i e_i$, où les a_i sont des éléments de $\mathbf{Q}_p$ tendant vers 0 à l'infini.

(ii) $\|x\| = \sup_{i\in \mathrm{I}} |a_i|$

19. Une famille $(x_i)_{i\in \mathrm{I}}$ *tend vers* 0 *à l'infini* si $\{i, \ \|x_i\| \geqslant \varepsilon\}$ est fini, pour tout $\varepsilon > 0$ (il faudrait dire « tend vers 0 suivant le filtre des complémentaires des parties finies », mais c'est un peu lourd...).

C'est une base de Banach si elle est bornée et vérifie la condition (i), ce qui implique, d'après le théorème de l'image ouverte, la propriété suivante :

(ii') il existe une constante $C \geqslant 1$ telle que l'on ait

$$C^{-1} \sup_{i\in I} |a_i| \leqslant \|x\| \leqslant C \sup_{i\in I} |a_i|.$$

Exemple II.4.7. — (i) Si $i \in I$, soit $e_i = (e_{i,j})_{j\in I}$, avec $e_{i,i} = 1$ et $e_{i,j} = 0$ si $j \neq i$. Par définition, ou presque, les e_i, pour $i \in I$, forment une base orthonormale de $\ell_0^\infty(I)$.

(ii) Les $\binom{x}{n}$, pour $n \in \mathbf{N}$, forment une base orthonormale de $\mathscr{C}(\mathbf{Z}_p)$: c'est une simple traduction du théorème de Mahler (th. 20.4 et rem. 20.5).

Proposition II.4.8. — (i) *Tout espace de Banach p-adique possède des bases de Banach.*

(ii) *Un espace de Banach p-adique possède des bases orthonormales si et seulement si il vérifie l'hypothèse* (N). *De plus, sous cette hypothèse,* $(e_i)_{i\in I}$ *est une base orthonormale de* E *si et seulement si* $(\overline{e}_i)_{i\in I}$ *est une base algébrique du* $\mathbf{F}_p$*-espace vectoriel* $\overline{E} = E^0/pE^0$, *où* $E^0 = \{x \in E \mid \|x\| \leqslant 1\}$ *est la boule unité de* E.

Démonstration. — Le lemme II.4.4 implique que le (i) est une conséquence du (ii). Supposons donc que E vérifie l'hypothèse (N) et montrons que $(e_i)_{i\in I}$ est une base orthonormale de E si et seulement si $(\overline{e}_i)_{i\in I}$ est une base algébrique du $\mathbf{F}_p$-espace vectoriel $\overline{E}$.

Soit $(e_i)_{i\in I}$ une famille d'éléments de E^0 telle que la famille $(\overline{e}_i)_{i\in I}$ soit une base du $\mathbf{F}_p$-espace vectoriel $\overline{E}$. Soient $S = \{0, 1, \dots, p-1\}$ et $s : \mathbf{F}_p \to S$ l'inverse de la réduction modulo p. Si $x \in E^0$, on peut écrire son image $\overline{x}$ modulo p comme une somme finie $\sum_{i\in I} a_i\overline{e}_i$, où les a_i sont des éléments de $\mathbf{F}_p$ presque tous nuls. Soit $s(x) = \sum_{i\in I} s(a_i)e_i$. Par construction, on a $x - s(x) \in pE^0$.

Si $x \in E^0$, définissons par récurrence une suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de E^0 par $x_0 = x$ et $x_{n+1} = \frac{1}{p}(x_n - s(x_n))$. Alors $x = \sum_{n=0}^{k} p^n s(x_n) + p^{k+1}x_{k+1}$ quel que soit $k \in \mathbf{N}$, et donc $x = \sum_{n\in\mathbf{N}} p^n s(x_n)$. De plus, $s(x_n) = \sum_{i\in I} s_{n,i}e_i$, où les $s_{n,i}$ sont des éléments de S presque tous nuls, ce qui montre que si on pose $a_i = \sum_{n=0}^{+\infty} p^n s_{n,i}$, alors la suite des a_i tend vers 0 à l'infini ($|a_i|_p \leqslant p^{-k}$ si $s_{n,i} = 0$ pour $n \leqslant k-1$, ce qui est vérifié pour presque tout i). On a alors $x = \sum_{i\in I} a_i e_i$, ce qui prouve que l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i$ est une surjection de $\ell_0^\infty(I)$ sur E. Si $\mathbf{a} = (a_i)_{i\in I} \in \ell_0^\infty(I)$ vérifie $\|\mathbf{a}\|_\infty = 1$, il existe $i \in I$ tel que $a_i \notin p\mathbf{Z}_p$, et alors $\sum_{i\in I} a_i e_i \neq 0$ modulo p car les $\overline{e}_i$, pour $i \in I$, forment une base de $\overline{E}$. Ceci implique que $1 \geqslant \|\sum_{i\in I} a_i e_i\| > p^{-1}$, et comme on a supposé que E vérifie (N), on en déduit que $\|\sum_{i\in I} a_i e_i\| = 1$ et que l'application $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i$ est une isométrie de $\ell_0^\infty(I)$ sur E. Ceci prouve que si les $\overline{e}_i$, pour $i \in I$, forment une base de $\overline{E}$, alors les e_i, pour $i \in I$, forment une base orthonormale de E.

Supposons maintenant que les e_i, pour $i \in I$, forment une base orthonormale de E. Si $x \in \overline{E}$, on peut choisir $\tilde{x} \in E^0$ ayant pour image x modulo p. Comme $\|\tilde{x}\| \leqslant 1$, on peut écrire $\tilde{x}$, de manière unique, sous la forme $\tilde{x} = \sum_{i\in I} a_i e_i$, où $a_i \in \mathbf{Z}_p$ tend vers 0 à l'infini. Il en résulte que la réduction $\overline{a}_i$ modulo p de a_i est nulle sauf pour un nombre fini de i (on

a $\overline{a}_i \neq 0$ si et seulement si $|a_i|_p = 1$), et que $x = \sum_{i\in \mathrm{I}} \overline{a}_i \overline{e}_i$ est une combinaison linéaire des $\overline{e}_i$; les $\overline{e}_i$ forment donc une famille génératrice de $\overline{\mathrm{E}}$. Enfin, si $\sum_{i\in \mathrm{I}} a_i \overline{e}_i = 0$ dans $\overline{\mathrm{E}}$, et si $\tilde{a}_i \in \mathbf{Z}_p$ a pour image a_i modulo p, alors $x = \sum_{i\in \mathrm{I}} \tilde{a}_i e_i \in p\mathrm{E}^0$, et donc $\|x\| < 1$. Comme $\|x\| = \sup_{i\in \mathrm{I}} |\tilde{a}_i|_p$, cela implique $|\tilde{a}_i|_p < 1$, et donc $a_i = 0$, pour tout $i \in \mathrm{I}$. Il s'ensuit que les $\overline{e}_i$ forment une famille libre, et donc une base, de $\overline{\mathrm{E}}$.

Ceci permet de conclure.

3. Le dual d'un espace de Banach p-adique

Si E est un space de Banach p-adique, on note E^* son dual (i.e l'espace des formes linéaires continues de E dans $\mathbf{Q}_p$). Comme d'habitude, une forme linéaire $\Lambda : \mathrm{E} \to \mathbf{Q}_p$ est continue si et seulement si il existe $\mathrm{C} > 0$ tel que $|\Lambda(x)|_p \leqslant \mathrm{C}\|x\|$, pour tout $x \in \mathrm{E}$, et on définit la norme $\|\Lambda\|$ de Λ comme la borne inférieure des C vérifiant la condition ci-dessus ; c'est la norme d'opérateur de Λ et on a aussi $\|\Lambda\| = \sup_{x\in \mathrm{E}-\{0\}} \|x\|^{-1}|\Lambda(x)|_p$. Ceci munit E^* d'une norme ultramétrique (l'ultramétricité est une conséquence de celle de $|\ |_p$), et il résulte du th. II.1.28 que E^*, muni de cette norme, est complet ; c'est donc un espace de Banach p-adique.

Proposition II.4.9. — *Soit* I *un ensemble.*

(i) *Si* $\mathbf{b} = (b_i)_{i\in \mathrm{I}} \in \ell^\infty(\mathrm{I})$ *et si* $\mathbf{a} = (a_i)_{i\in \mathrm{I}} \in \ell_0^\infty(\mathrm{I})$, *la série* $\sum_{i\in \mathrm{I}} a_i b_i$ *converge dans* $\mathbf{Q}_p$.

(ii) *Si* $\Lambda_{\mathbf{b}}(\mathbf{a})$ *désigne la somme de la série* $\sum_{i\in \mathrm{I}} a_i b_i$, *l'application* $\mathbf{b} \mapsto \Lambda_{\mathbf{b}}$ *est une isométrie de* $\ell^\infty(\mathrm{I})$ *sur le dual de* $\ell_0^\infty(\mathrm{I})$.

Démonstration. — (i) La convergence de la série vient de ce que $a_i b_i$ tend vers 0 à l'infini puisque a_i tend vers 0 et b_i est bornée.

(ii) La linéarité de Λ_b et l'égalité $\|\Lambda_{\mathbf{b}}\| = \|\mathbf{b}\|_\infty$ sont immédiates. Il n'y a donc que la surjectivité de l'application $\mathbf{b} \mapsto \Lambda_{\mathbf{b}}$ à vérifier. Soit donc $\Lambda \in \ell_0^\infty(\mathrm{I})^*$. Comme Λ est continue, si on pose $b_i = \Lambda(\delta_i)$, on a $|b_i|_p \leqslant \|\Lambda\|$, ce qui prouve que $\mathbf{b} = (b_i)_{i\in \mathrm{I}} \in \ell^\infty(\mathrm{I})$. Mais alors $\Lambda - \Lambda_{\mathbf{b}}$ est nulle sur le sous-espace de $\ell_0^\infty(\mathrm{I})$ engendré par les δ_i, et comme celui-ci est dense dans $\ell_0^\infty(\mathrm{I})$ et $\Lambda - \Lambda_{\mathbf{b}}$ continue, cela implique $\Lambda = \Lambda_{\mathbf{b}}$. Ceci permet de conclure.

CHAPITRE III

INTÉGRATION

III.1. Intégrale de Lebesgue

L'intégrale de Lebesgue (1902-1904) est une extension (ou plutôt une complétion) de l'intégrale de Riemann [1] d'une extrême souplesse. Les espaces de fonctions intégrables deviennent complets [2], ce qui simplifie grandement les problèmes d'existence ou de convergence d'intégrales, et on dispose, grâce au théorème de convergence dominée de Lebesgue (th. III.1.32), d'un outil extrêmement puissant pour intervertir limites et intégrales. Tous les énoncés classiques de l'intégrale de Riemann (continuité et dérivabilité d'une intégrale dépendant d'un paramètre, théorème de Fubini) s'étendent avec des démonstrations souvent simplifiées. Il est toutefois toujours aussi difficile de calculer explicitement les intégrales dont on a montré l'existence, mais c'est un autre problème...

1. Dallages et fonctions en escalier

Soit $\mathbf{Z}[\frac{1}{2}]$ l'anneau des *nombres dyadiques* (i.e. des nombres rationnels dont le dénominateur est une puissance de 2). Une *dalle* de $\mathbf{R}^m$ est un sous-ensemble de $\mathbf{R}^m$ de la forme [3] $\prod_{j=1}^m [r_j, s_j[$, où $r_j < s_j$, pour $1 \leqslant j \leqslant m$, sont des nombres dyadiques. Un *dallage* est une réunion *finie* de dalles. Une *dalle élémentaire* (*de taille* 2^{-r}) est un ensemble de la forme $\mathrm{D}_{r,\mathbf{k}}$, où $r \in \mathbf{N}$, $\mathbf{k} = (k_1, \ldots, k_m) \in \mathbf{Z}^m$, et $\mathrm{D}_{r,\mathbf{k}} = \prod_{j=1}^m [\frac{k_j}{2^r}, \frac{k_j+1}{2^r}[$.

Lemme III.1.1. — (i) *Si* D_1 *et* D_2 *sont des dalles élémentaires* (pas forcément de même taille)*, alors soit* D_1 *et* D_2 *sont disjointes, soit l'une est incluse dans l'autre* [4].

(ii) *Si* $\mathbf{k} \in \mathbf{Z}^m$*, alors* $\mathrm{D}_{r,\mathbf{k}}$ *est la réunion disjointe des* $\mathrm{D}_{r+1,2\mathbf{k}+\mathbf{a}}$*, pour* $\mathbf{a} \in \{0,1\}^m$.

(iii) *Tout dallage est une réunion finie disjointe de dalles élémentaires de même taille.*

---

1. L'intégrale de Riemann date de 1854 ; elle généralise l'intégrale que Cauchy avait définie (cours à l'École Polytechnique de 1823) pour les fonctions (uniformément) continues (cf. ex. 16.5 du Vocabulaire).

2. Et on peut même, quitte à se passer de l'axiome du choix, imposer que toute fonction pas trop grosse (par exemple bornée sur un ensemble borné) soit intégrable (cf. note 14).

3. Le lecteur est invité à supposer $m = 1$ ou $m = 2$, et à faire des dessins ; cela rend les énoncés qui suivent parfaitement évidents.

4. Autrement dit, les dalles élémentaires se comportent comme des billes de mercure.

Démonstration. — Exercice.

On définit la *mesure* $\lambda(\mathrm{D}_{r,\mathbf{k}})$ d'une dalle élémentaire $\mathrm{D}_{r,\mathbf{k}}$ par la formule $\lambda(\mathrm{D}_{r,\mathbf{k}}) = 2^{-mr}$. Si D est un dallage quelconque, réunion disjointes des $\mathrm{D}_{r,\mathbf{k}_i}$, pour $i \in \mathrm{I}$ ensemble fini, on définit $\lambda(\mathrm{D})$ par $\lambda(\mathrm{D}) = \sum_{i\in\mathrm{I}} \lambda(\mathrm{D}_{r,\mathbf{k}_i})$. On vérifie que cela ne dépend pas du choix de la taille des dalles élémentaires choisies pour recouvrir D, en utilisant le (ii) du lemme précédent.

Si $r \in \mathbf{N}$, et si $\mathbf{k} \in \mathbf{Z}^m$, on note $e_{r,\mathbf{k}}$ la fonction caractéristique de $\mathrm{D}_{r,\mathbf{k}}$. Si $r \in \mathbf{N}$, on note $\mathrm{Esc}_r(\mathbf{R}^m)$, l'espace vectoriel des combinaisons linéaires des $e_{r,\mathbf{k}}$, pour $\mathbf{k} \in \mathbf{Z}^m$; c'est l'ensemble des *fonctions en escalier sur* $\mathbf{R}^m$*, constantes sur les dalles élémentaires de taille* 2^{-r}. Les $e_{r,\mathbf{k}}$, pour $\mathbf{k} \in \mathbf{Z}^m$, étant linéairement indépendantes (si $x \in \mathbf{R}^m$ il existe exactement un $\mathbf{k} \in \mathbf{Z}^n$ tel que $e_{r,\mathbf{k}}(x) \neq 0$), forment une base de $\mathrm{Esc}_r(\mathbf{R}^m)$.

Comme $e_{r,\mathbf{k}} = \sum_{\mathbf{a}\in\{0,1\}^m} e_{r+1,2\mathbf{k}+\mathbf{a}}$, on a $\mathrm{Esc}_r(\mathbf{R}^m) \subset \mathrm{Esc}_{r+1}(\mathbf{R}^m)$, si $r \in \mathbf{N}$. La réunion $\mathrm{Esc}(\mathbf{R}^m)$ des $\mathrm{Esc}_r(\mathbf{R}^m)$, pour $r \in \mathbf{N}$, est donc un espace vectoriel ; c'est l'espace vectoriel des *fonctions en escalier* sur $\mathbf{R}^m$. (On notera qu'une combinaison linéaire étant une somme finie, *une fonction en escalier est à support* [5] *compact.*)

Si $\mathrm{X} \subset \mathbf{R}^m$, on note $\mathrm{Esc}(\mathrm{X})$ l'ensemble des fonctions en escalier sur X ; il peut se voir comme l'ensemble des fonctions en escalier sur $\mathbf{R}^m$ qui sont nulles en dehors de X. Plus généralement, si $\mathrm{X} \subset \mathbf{R}^m$, et si $\mathrm{U} \subset \mathbf{C}$, on note $\mathrm{Esc}(\mathrm{X}, \mathrm{U})$ l'ensemble des fonctions, en escalier sur X, prenant leurs valeurs dans U. On a donc $\mathrm{Esc}(\mathrm{X}) = \mathrm{Esc}(\mathrm{X}, \mathbf{C})$.

Si $\phi \in \mathrm{Esc}(\mathbf{R}^m)$, il existe $r \in \mathbf{N}$ tel que l'on puisse écrire ϕ sous la forme $\phi = \sum_{i\in\mathrm{I}} \alpha_i e_{r,\mathbf{k}_\mathbf{i}}$, et on définit son intégrale $\int \phi$ par $\int \phi = \sum_{i\in\mathrm{I}} \alpha_i \lambda(\mathrm{D}_{r,\mathbf{k}_\mathbf{i}}) = 2^{-rm} \sum_{i\in\mathrm{I}} \alpha_i$. On vérifie, en utilisant la formule $e_{r,\mathbf{k}} = \sum_{\mathbf{a}\in\{0,1\}^m} e_{r+1,2\mathbf{k}+\mathbf{a}}$, que cela ne dépend pas du choix de r, et que l'on a défini de la sorte une forme linéaire sur $\mathrm{Esc}(\mathbf{R}^m)$. Suivant le contexte, l'intégrale de ϕ sera notée indifféremment

$$\int \phi = \int_{\mathbf{R}^m} \phi = \int_{\mathbf{R}^m} \phi \, d\lambda = \int_{\mathbf{R}^m} \phi(x)\, dx = \int_{\mathbf{R}^m} \phi(x)\, dx_1 \cdots dx_m.$$

Remarque III.1.2. — Si $\phi \in \mathscr{C}_c(\mathbf{R}^m)$ est une fonction continue à support compact, et si on note ϕ_r la fonction en escalier $\sum_{k\in\mathbf{Z}^m} \phi(\frac{\mathbf{k}}{2^r}) e_{r,\mathbf{k}}$ prenant la valeur $\phi(\frac{k_1}{2^r}, \ldots, \frac{k_m}{2^r})$ sur la dalle élémentaire $\prod_{j=1}^m [\frac{k_j}{2^r}, \frac{k_j+1}{2^r}[$, quel que soit $\mathbf{k} \in \mathbf{Z}^m$, alors $\phi_r \to \phi$ en norme $\| \ \|_\infty$ (i.e. uniformément [6]). Ceci permet de montrer que la suite $(\int \phi_r)_{r\in\mathbf{N}}$ converge, et on définit *l'intégrale de Riemann* $\int \phi$ comme la limite de cette suite. L'intégrale de Lebesgue va être définie de la même manière, mais en relachant [7] la condition de convergence uniforme, remplacée par la condition de *convergence simple presque partout.*

5. Le support de ϕ est l'adhérence de l'ensemble des x tels que $\phi(x) \neq 0$; c'est donc un fermé par définition.

6. C'est une conséquence de l'uniforme continuité d'une fonction continue sur un compact.

7. Comme la convergence uniforme implique la convergence simple presque partout définie plus loin, les intégrales de Riemann et de Lebesgue d'une fonction continue à support compact coïncident, et l'intégrale de Lebesgue est bien une extension de l'intégrale de Riemann.

2. Ensembles de mesure nulle

On définit la *mesure extérieure* $\lambda^+(\mathrm{A})$ d'un ensemble A comme la borne inférieure des $\sum_{n\in\mathbf{N}}\lambda(\mathrm{D}_n)$, où $(\mathrm{D}_n)_{n\in\mathbf{N}}$ décrit l'ensemble des suites de dalles de $\mathbf{R}^m$ telles que $\mathrm{A}\subset\cup_{n\in\mathbf{N}}\mathrm{D}_n$. En décomposant les dalles D_n en dalles élémentaires disjointes de taille décroissante avec n, et en éliminant les dalles élémentaires de D_n incluses dans un des D_i, pour $i\leqslant n-1$, on peut se ramener au cas où les D_n sont des dalles élémentaires disjointes [8].

Proposition III.1.3. — (i) *Si* $\mathrm{B}\subset\mathrm{A}$, *alors* $\lambda^+(\mathrm{B})\leqslant\lambda^+(\mathrm{A})$.

(ii) *Si* $\mathrm{A}_n\subset\mathbf{R}^m$, *pour* $n\in\mathbf{N}$, *alors* $\lambda^+(\cup_{n\in\mathbf{N}}\mathrm{A}_n)\leqslant\sum_{n\in\mathbf{N}}\lambda^+(\mathrm{A}_n)$.

Démonstration. — Le (i) est une évidence. Le (ii) est évident si $\sum_{n\in\mathbf{N}}\lambda^+(\mathrm{A}_n)=+\infty$. Dans le cas contraire, soit $\mathrm{A}=\cup_{n\in\mathbf{N}}\mathrm{A}_n$, et soit $\varepsilon>0$. Pour tout $n\in\mathbf{N}$, on peut trouver une suite $(\mathrm{D}_{n,k})_{k\in\mathbf{N}}$ de dallages de $\mathbf{R}^m$ tels que $\mathrm{A}_n\subset\cup_{k\in\mathbf{N}}\mathrm{D}_{n,k}$ et $\sum_{k\in\mathbf{N}}\lambda(\mathrm{D}_{n,k})\leqslant\lambda^+(\mathrm{A}_n)+2^{-1-n}\varepsilon$. Mais alors $\mathrm{A}\subset\cup_{k,n\in\mathbf{N}}\mathrm{D}_{n,k}$ et

$$\sum_{k,n\in\mathbf{N}}\lambda(\mathrm{D}_{n,k})\leqslant\sum_{n\in\mathbf{N}}(\lambda^+(\mathrm{A}_n)+2^{-1-n}\varepsilon)=\varepsilon+\sum_{n\in\mathbf{N}}\lambda^+(\mathrm{A}_n).$$

On en déduit que $\lambda^+(\mathrm{A})\leqslant\varepsilon+\sum_{n\in\mathbf{N}}\lambda^+(\mathrm{A}_n)$ quel que soit $\varepsilon>0$, ce qui permet de conclure.

On dit que A est *de mesure nulle* si $\lambda^+(\mathrm{A})=0$. En revenant à la définition, on voit que A est de mesure nulle si et seulement si, quel que soit $\varepsilon>0$, il existe une suite $(\mathrm{D}_n)_{n\in\mathbf{N}}$ de dallages de $\mathbf{R}^m$ tels que $\mathrm{A}\subset\cup_{n\in\mathbf{N}}\mathrm{D}_n$ et $\sum_{n\in\mathbf{N}}\lambda(\mathrm{D}_n)<\varepsilon$.

Proposition III.1.4. — (i) *Tout sous-ensemble d'un ensemble de mesure nulle est de mesure nulle.*

(ii) *Une réunion dénombrable d'ensembles de mesure nulle est de mesure nulle.*

Démonstration. — C'est une conséquence immédiate de la prop. III.1.3.

Exercice III.1.5. — Montrer que, si A est de mesure nulle dans $\mathbf{R}^n$, alors $\mathrm{A}\times\mathbf{R}^m$ est de mesure nulle dans $\mathbf{R}^{n+m}$.

Exercice III.1.6. — (i) Montrer que la diagonale dans $\mathbf{R}^2$ est de mesure nulle.

(ii) Montrer, plus généralement, que le graphe dans $\mathbf{R}^2$ d'une application continue $f:\mathbf{R}\to\mathbf{R}$ est de mesure nulle, et qu'un hyperplan est de mesure nulle dans $\mathbf{R}^m$.

(iii) L'image dans $\mathbf{R}^2$ de $[0,1]$ par une application continue est-elle nécessairement de mesure nulle ?

On dit qu'une propriété est *vraie presque partout*, ou bien est *vraie pour presque tout* $x\in\mathbf{R}^m$, ou encore *est vraie p.p.*, si l'ensemble des points ne la vérifiant pas est de mesure nulle. Par exemple, l'ensemble des rationnels étant dénombrable, presque tout réel est

8. Le résultat n'est pas sans rappeler la manière dont une image apparaît sur un ordinateur.

irrationnel. De même, presque tout [9] nombre complexe est transcendant. (Un nombre complexe est *algébrique* s'il est racine d'un polynôme unitaire à coefficients dans $\mathbf{Q}$. Un nombre complexe non algébrique est un *nombre transcendant*.)

Remarque III.1.7. — (i) Il ne faudrait pas croire qu'un sous-ensemble de $\mathbf{R}$ de mesure nulle est forcément dénombrable. Par exemple, fixons une bijection $n \mapsto r_n$ de $\mathbf{N}$ sur $\mathbf{Q}$, et soient $\mathrm{U}_k = \cup_{n\in\mathbf{N}}]r_n - 2^{-n-k}, r_n + 2^{-n-k}[$, si $k \in \mathbf{N}$, et $\mathrm{A} = \cap_{k\in\mathbf{N}}\mathrm{U}_k$. Alors A est de mesure nulle puisqu'il est inclus dans U_k, pour tout k, et que $\lambda^+(\mathrm{U}_k) \leqslant \sum_{n=0}^{+\infty} 2^{1-n-k} = 2^{2-k}$ peut être rendu arbitrairement petit. D'un autre côté, U_k est un ouvert dense pour tout k, et donc A est dense et non dénombrable d'après le lemme de Baire (cf. n° 14.2 du Vocabulaire). En particulier, A contient bien d'autres éléments que les rationnels, ce qui n'est pas totalement transparent sur sa construction.

(ii) Un ensemble de mesure nulle peut avoir des propriétés assez surprenantes. Par exemple, A. Besicovitch (1919) a construit des ensembles de mesure nulle de $\mathbf{R}^m$, pour $m \geqslant 2$, contenant un segment de longueur 1 dans toutes les directions [10].

Exercice III.1.8. — Montrer qu'une fonction continue, qui est nulle p.p., est identiquement nulle.

Théorème III.1.9. — (Borel-Cantelli) *Si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{R}_+$ telle que $\sum_{n\in\mathbf{N}} a_n < +\infty$, et si $(\mathrm{A}_n)_{n\in\mathbf{N}}$ est une suite de sous-ensembles de $\mathbf{R}^m$ vérifiant $\lambda^+(\mathrm{A}_n) \leqslant a_n$, pour tout $n \in \mathbf{N}$, alors presque tout $x \in \mathbf{R}^m$ n'appartient qu'à un nombre fini de A_n.*

Démonstration. — Il s'agit de prouver que l'ensemble A des $x \in \mathbf{R}$ appartenant à une infinité de A_n est de mesure nulle. Or $x \in \mathrm{A}$ si et seulement si, quel que soit $n \in \mathbf{N}$, il existe $p \geqslant n$ tel que $x \in \mathrm{A}_p$; autrement dit, on a $\mathrm{A} = \cap_{n\in\mathbf{N}}\big(\cup_{p\geqslant n}\mathrm{A}_p\big)$. On en déduit que $\lambda^+(\mathrm{A}) \leqslant \sum_{p\geqslant n}\lambda^+(\mathrm{A}_p)$, quel que soit $n \in \mathbf{N}$, et comme la série $\sum_{n\in\mathbf{N}}\lambda^+(\mathrm{A}_n)$ est supposée convergente, son reste tend vers 0, ce qui permet de conclure.

9. Au vu de ces résultats, il est raisonnable de penser qu'un nombre n'ayant pas de bonnes raisons d'être algébrique est transcendant. Démontrer qu'un nombre donné est transcendant ou même irrationnel est, en général, très difficile. Par exemple, il a fallu attendre 1979 pour que R. Apéry démontre que $\zeta(3)$ est irrationnel, et il n'y a aucun entier n impair $\geqslant 5$, pour lequel on sache prouver que $\zeta(n)$ est irrationnel. Le seul résultat dans cette direction est un résultat de T. Rivoal (2000) qui a démontré que $\zeta(n)$ est irrationnel pour une infinité de n impairs, et qu'au moins un des 9 nombres $\zeta(5), \cdots, \zeta(21)$ est irrationnel (amélioré depuis par W. Zudilin : au moins un des 4 nombres $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ est irrationnel).

10. Ces ensembles sont sources de contrexemples empoisonnants en analyse (par exemple pour la convergence des séries de Fourier en dimension $\geqslant 2$). Les analystes seraient plutôt contents si on arrivait à démontrer (problème de Kakeya) qu'un ensemble de Besicovitch n'est pas trop petit, et plus précisément qu'un *ensemble de Besicovitch* de $\mathbf{R}^m$ est de dimension de Minkowski m : la *dimension de Minkowski* d'un ensemble X, si elle existe, est la limite de $\frac{\log \mathrm{N}(\mathrm{X},k)}{\log k}$ quand $k \to +\infty$, où $\mathrm{N}(\mathrm{X}, k)$ est le nombre minimum de boules de rayon $\frac{1}{k}$ nécessaires pour recouvrir complètement X. Le meilleur résultat connu pour le moment est dû à N. Katz et T. Tao (2001) : la dimension de Minkowski d'un ensemble de Besicovitch de $\mathbf{R}^m$ est au moins $(2-\sqrt{2})(m-4)+3$, si $m > 4$.

Exercice III.1.10. — (i) Montrer que, si $\varepsilon > 0$ et $C > 0$, alors pour presque tout [11] nombre réel x, l'ensemble des couples d'entiers (p, q), tels que $|x - \frac{p}{q}| \leqslant Cq^{-2-\varepsilon}$, est fini.

(ii) Montrer que l'ensemble des nombres de Liouville est de mesure nulle, non dénombrable, et dense dans $\mathbf{R}$. (Un réel x est *de Liouville* [12] si ce n'est pas un nombre rationnel et si, quel que soit $n \in \mathbf{N}$, il existe un couple d'entiers (p, q), $q \geqslant 2$, tels que $|x - \frac{p}{q}| \leqslant q^{-n}$.)

3. Fonctions mesurables, ensembles mesurables

3.1. *Fonctions mesurables*

Une fonction $f : \mathbf{R}^m \to \mathbf{C}$ (resp. $f : \mathbf{R}^m \to \overline{\mathbf{R}}_+$) est dite *mesurable* si elle est limite p.p. d'une suite de fonctions en escalier. Autrement dit, f est mesurable s'il existe $A \subset \mathbf{R}^m$ de mesure nulle, et une suite $(f_n)_{n\in\mathbf{N}}$ d'éléments de $\mathrm{Esc}(\mathbf{R}^m)$ (resp. $\mathrm{Esc}(\mathbf{R}^m, \mathbf{R}_+)$) tels que $f_n(x) \to f(x)$, quel que soit $x \notin A$.

On note $\mathrm{Mes}(\mathbf{R}^m)$ l'ensemble des fonctions mesurables sur $\mathbf{R}^m$ à valeurs dans $\mathbf{C}$. Plus généralement, si $D \subset \mathbf{R}^m$ et $F \subset \mathbf{C}$ (ou $F \subset \overline{\mathbf{R}}_+$), on note $\mathrm{Mes}(D, F)$ l'ensemble des fonctions mesurables sur $\mathbf{R}^m$, qui sont nulles en dehors de D et qui prennent leurs valeurs dans F.

• Les fonctions constantes sont mesurables (la fonction λ est la limite de $\lambda \mathbf{1}_{D_N}$, où D_N est la dalle $[-N, N[^m$).

• $\mathrm{Mes}(\mathbf{R}^m)$ est une $\mathbf{C}$-algèbre (i.e. λf, $f + g$ et fg sont mesurables si $\lambda \in \mathbf{C}$, f, g mesurables). En effet, si $(f_n)_{n\in\mathbf{N}}$ et $(g_n)_{n\in\mathbf{N}}$ sont des suites d'élements de $\mathrm{Esc}(\mathbf{R}^m)$ tendant respectivement vers f et g en dehors de A_f et A_g, où A_f et A_g sont de mesure nulle, alors :

— $\lambda f_n \to \lambda f$ en dehors de A_f et donc λf est mesurable,

— $f_n + g_n \to f + g$ en dehors de $A_f \cup A_g$ (qui est de mesure nulle), et donc $f + g$ est mesurable,

— $f_n g_n \to fg$ en dehors de $A_f \cup A_g$, et donc fg est mesurable.

---

11. K. Roth (1955) a démontré, ce qui lui a valu la médaille Fields, que les nombres algébriques ont cette propriété (c'est évident pour les rationnels ou les nombres algébriques de degré 2 (si α est un nombre algébrique, le *degré* de α est le minimum des degrés des polynômes $P \in \mathbf{Q}[X]$ non nuls, avec $P(\alpha) = 0$), mais le cas général représente un tour de force). On ne sait pas démontrer que π vérifie cette propriété.

Dans le même genre d'idées, si x est un nombre réel non rationnel, on peut prendre son développement en fractions continues (il s'agit de la suite d'entiers $(a_n)_{n\in\mathbf{N}}$ définie par l'algorithme $x_0 = x$, $a_n = [x_n]$, $x_{n+1} = \frac{1}{x_n - a_n}$; les nombres rationnels $\frac{u_n}{v_n}$, obtenus en écrivant x en termes de $a_0, \cdots, a_{n-1}$ et x_n, et en remplaçant x_n par a_n dans l'expression, sont les meilleures approximations de x par des nombres rationnels). On montre facilement que, pour presque tout nombre réel x, la suite a_n n'est pas bornée, ce qui équivaut à la nullité de la borne inférieure de l'ensemble des $q\,|qx - p|$, pour $p, q \in \mathbf{Z}$, $q \geqslant 1$. Si x est algébrique de degré 2, la suite a_n devient périodique à partir d'un certain rang et donc est bornée. On est persuadé que si x est algébrique de degré $\geqslant 3$, alors la suite a_n n'est pas bornée, mais on ne sait le démontrer dans aucun cas.

12. Ces nombres, introduits par Liouville en 1844, sont les premiers nombres dont on ait montré la transcendance ; celle de e a été prouvée en 1873 (Hermite), et celle de π en 1882 (Lindemann).

• Si $f, g \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$, alors $\inf(f,g)$ et $\sup(f,g)$ sont mesurables. En effet, si $(f_n)_{n\in\mathbf{N}}$ et $(g_n)_{n\in\mathbf{N}}$ sont des suites d'élements de $\mathrm{Esc}(\mathbf{R}^m, \mathbf{R}_+)$ tendant respectivement vers f et g en dehors de A_f et A_g, où A_f et A_g sont de mesure nulle, alors $\inf(f_n, g_n)$ (resp. $\sup(f_n, g_n)$) tend vers $\inf(f,g)$ (resp. $\sup(f,g)$) en dehors de $\mathrm{A}_f \cup \mathrm{A}_g$.

• $f : \mathbf{R}^m \to \mathbf{C}$ est mesurable si et seulement si les fonctions [13] $\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ et $\mathrm{Re}^+(-if)$ sont mesurables : $f = \mathrm{Re}^+(f) - \mathrm{Re}^+(-f) - i\mathrm{Re}^+(if) + i\mathrm{Re}^+(-if)$, d'où l'implication « $\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ et $\mathrm{Re}^+(-if)$ mesurables » ⇒ « f mesurable ». L'implication réciproque résulte de ce que $\mathrm{Re}^+(g)$ est en escalier, si g est en escalier, et de ce que Re^+ est continue.

Exercice III.1.11. — (i) Montrer que $h(x,y) = f(x)g(y)$ est mesurable sur $\mathbf{R}^{n+m}$, si f est mesurable sur $\mathbf{R}^n$ et si g est mesurable sur $\mathbf{R}^m$.

(ii) Montrer qu'une fonction continue est mesurable.

Proposition III.1.12. — *Une limite simple p.p. de fonctions mesurables est mesurable.*

Démonstration. — Cette proposition est moins évidente qu'il n'y paraît (cf. ex. II.1.11). La démonstration sera faite au n° 4 du § III.4.

Exercice III.1.13. — (i) Montrer qu'une fonction est mesurable si et seulement si elle est limite simple p.p. d'une suite de fonctions continues.

(ii) En déduire qu'une limite simple p.p. de limites simples p.p. de fonctions continues est limite simple p.p. d'une suite de fonctions continues. Comparer avec l'exercice II.1.11.

3.2. *La tribu des ensembles mesurables*

• Un *sous-ensemble* X de $\mathbf{R}^m$ est *mesurable* si sa fonction caractéristique $\mathbf{1}_\mathrm{X}$ est une fonction mesurable [14]. En particulier :

— un ensemble de mesure nulle est mesurable (sa fonction caractéristique est la limite simple p.p. de la suite dont tous les termes sont la fonction nulle).

— si A et B sont mesurables, alors $\mathrm{A} \cap \mathrm{B}$ et $\mathrm{A} \cup \mathrm{B}$ sont mesurables [en effet, on a $\mathbf{1}_{\mathrm{A}\cap\mathrm{B}} = \inf(\mathbf{1}_\mathrm{A}, \mathbf{1}_\mathrm{B})$ et $\mathbf{1}_{\mathrm{A}\cup\mathrm{B}} = \sup(\mathbf{1}_\mathrm{A}, \mathbf{1}_\mathrm{B})$].

13. Si $z \in \mathbf{C}$, on note $\mathrm{Re}^+(z)$ le nombre réel $\sup(0, \mathrm{Re}(z))$; on a alors
$$z = \mathrm{Re}^+(z) - \mathrm{Re}^+(-z) + i\mathrm{Re}^+(-iz) - i\mathrm{Re}^+(iz).$$

14. S. Banach et A. Tarski (1924) ont construit un découpage d'une boule de rayon 1 dans $\mathbf{R}^3$ en un nombre fini de morceaux (5 morceaux suffisent), tel que si on réarrange ces morceaux (i.e. si on les bouge par des isométries de $\mathbf{R}^3$), on obtient deux boules de rayon 1 (*paradoxe de Banach-Tarski*). Ces morceaux ne sont pas mesurables, et la construction de Banach et Tarski utilise l'axiome du choix.

D'un autre côté, R. Solovay (1966) a démontré que, si on s'interdit l'axiome du choix non dénombrable, tout en gardant l'axiome du choix dénombrable, on peut, sans introduire de contradiction supplémentaire aux mathématiques, supposer que tout ensemble est mesurable. La leçon à retenir de ce résultat est, qu'en pratique, toutes les fonctions et tous les ensembles rencontrés en analyse sont mesurables et qu'il est inutile de passer son temps à vérifier qu'ils le sont ; le problème est différent en théorie des probabilités où un même événement peut être mesurable ou non mesurable suivant les conditions.

Exercice III.1.14. — Montrer que, si X est mesurable dans $\mathbf{R}^n$ et Y est mesurable dans $\mathbf{R}^m$, alors $\mathrm{X}\times\mathrm{Y}$ est mesurable dans $\mathbf{R}^{n+m}$.

• Si E est un ensemble, une *tribu* $\mathscr{A}$ sur E est un ensemble non vide de parties de E, stable par passage au complémentaire (si $\mathrm{A}\in\mathscr{A}$, alors $\mathrm{E}-\mathrm{A}\in\mathscr{A}$) et par réunion dénombrable (si I est dénombrable et si $(\mathrm{A}_i)_{i\in\mathrm{I}}$ sont des éléments de $\mathscr{A}$, alors $\cup_{i\in\mathrm{I}}\mathrm{A}_i\in\mathscr{A}$). Une tribu sur E contient toujours E et $\varnothing$ (si $\mathrm{A}\in\mathscr{A}$, alors $\mathrm{A}\cup(\mathrm{E}-\mathrm{A})\in\mathscr{A}$), et est aussi stable par intersection dénombrable puisque $\cap_{i\in\mathrm{I}}\mathrm{A}_i$ est le complémentaire de la réunion des complémentaires des A_i.

• Une intersection de tribus sur E est encore une tribu ce qui permet, si $\mathscr{B}$ est un ensemble non vide de parties de E, de définir la *tribu engendrée par* $\mathscr{B}$ comme l'intersection de toutes les tribus contenant $\mathscr{B}$.

• Si E est un espace topologique (par exemple $\mathrm{E}=\mathbf{R},\mathbf{R}^m,\overline{\mathbf{R}}_+...$), la *tribu borélienne* $\mathscr{B}or$ sur E est la tribu engendrée par les ouverts ou, ce qui revient au même, par les fermés. Un élément de la tribu borélienne est un *borélien* ; les ouverts et les fermés sont donc des boréliens, mais un borélien quelconque est assez difficile à décrire [15]. Parmi les sous-ensembles de $\mathscr{B}or$ mentionnons l'ensemble $\mathscr{G}_\delta$ des intersections dénombrables d'ouverts et l'ensemble $\mathscr{F}_\sigma$ des réunions dénombrables de fermés.

• La tribu borélienne de $\mathbf{R}^m$ est aussi la tribu engendrée par les dalles élémentaires. En effet, un ouvert de $\mathbf{R}^m$ est la réunion des dalles élémentaires qu'il contient et celles-ci sont en nombre dénombrable, ce qui prouve que les ouverts sont dans la tribu engendrée par les dalles élémentaires qui, de ce fait, contient $\mathscr{B}or$. Réciproquement, la dalle $\prod_{i=1}^m[\frac{k_i}{2^r},\frac{k_i+1}{2^r}[$ est l'intersection de l'ouvert $\prod_{i=1}^m]-\infty,\frac{k_i+1}{2^r}[$ et du fermé $\prod_{i=1}^m[\frac{k_i}{2^r},+\infty[$, et donc est un élément de $\mathscr{B}or$; il en résulte que $\mathscr{B}or$ contient toutes les dalles élémentaires et donc aussi la tribu qu'elles engendrent.

Exercice III.1.15. — Soit $(f_n)_{n\in\mathbf{N}}$ une suite de fonctions continues de $\mathbf{R}^m$ dans $\mathbf{C}$.

(i) Montrer que $\{x\in\mathbf{R}^m,\ f_n(x)\to 0\}$ est un borélien.

(ii) Montrer $\{x\in\mathbf{R}^m,\ f_n(x)$ a une limite$\}$ est un borélien (penser au critère de Cauchy).

On dit que A *et* B *ne diffèrent que par des ensembles de mesure nulle* si $\mathbf{1}_\mathrm{A}=\mathbf{1}_\mathrm{B}$ p.p., ce qui équivaut à ce que $\mathrm{A}-(\mathrm{A}\cap\mathrm{B})$ et $\mathrm{B}-(\mathrm{A}\cap\mathrm{B})$ sont de mesure nulle.

Théorème III.1.16. — (i) *Les ensembles mesurables forment une tribu sur* $\mathbf{R}^m$.

(ii) *La tribu des ensembles mesurables est la tribu engendrée par les boréliens et les ensembles de mesure nulle* [16]. *Plus précisément, les conditions suivantes sont équivalentes :*

- X *est mesurable,*
- *il existe* $\mathrm{G}\in\mathscr{G}_\delta$ *tel que* X *et* G *ne diffèrent que par des ensembles de mesure nulle,*
- *il existe* $\mathrm{F}\in\mathscr{F}_\sigma$ *tel que* X *et* F *ne diffèrent que par des ensembles de mesure nulle.*

Démonstration. — Si X est mesurable, alors son complémentaire l'est puisque sa fonction caractéristique est $1-\mathbf{1}_\mathrm{X}$ qui est mesurable comme combinaison linéaire de fonctions mesurables. Si les $(\mathrm{X}_i)_{i\in\mathbf{N}}$ sont mesurables, alors la fonction caractéristique de la réunion est la limite simple des fonctions $\sup_{i\leqslant n}\mathbf{1}_{\mathrm{X}_i}$, et donc est mesurable comme limite simple de fonctions mesurables.

15. Une description explicite est, de toute façon, parfaitement inutile pour les applications : la manière dont on démontre une propriété pour un borélien quelconque consiste à vérifier qu'elle est vraie par passage au complémentaire et par réunion dénombrable, et qu'elle est vrai pour les ouverts (ou toute autre famille d'éléments de $\mathscr{B}or$ engendrant $\mathscr{B}or$).

16. On peut montrer qu'il existe des ensembles mesurables qui ne sont pas des boréliens par un argument de cardinal : l'ensemble des boréliens a même cardinal que $\mathbf{R}$, alors que l'ensemble des mesurables, qui contient l'ensemble des parties de l'ensemble de Cantor, a un cardinal strictement plus grand.

On en déduit le (i). Pour démontrer le (ii) commençons par constater qu'un borélien est mesurable puisqu'une dalle élémentaire l'est et que la tribu engendrée par les dalles élémentaires est celle des boréliens. Comme un ensemble de mesure nulle l'est aussi, la tribu des mesurables contient la tribu engendrée par les boréliens et les ensembles de mesure nulle. Pour montrer l'inclusion réciproque, il suffit de montrer qu'un ensemble X mesurable admet l'une des descriptions du théorème. Si $(f_k)_{k\in\mathbf{N}}$ est une suite de fonctions en escalier tendant simplement vers $\mathbf{1}_{\mathrm{X}}$ en dehors de A, où A est de mesure nulle, on a aussi $\mathbf{1}_{\mathrm{X}_k} \to \mathbf{1}_{\mathrm{X}}$ en dehors de A, si X_k est le dallage des $x \in \mathbf{R}^m$ vérifiant $|f_k(x) - 1| \leqslant \frac{1}{2}$. Soit U_k l'intérieur de X_k. Comme $\mathrm{X}_k - \mathrm{U}_k$ est de mesure nulle puisqu'inclus dans une réunion finie de faces de dalles élémentaires, il existe un ensemble de mesure nulle A′ tel que $\mathbf{1}_{\mathrm{U}_k} \to \mathbf{1}_{\mathrm{X}}$ en dehors de A′. Il en résulte que $\mathbf{1}_{\mathrm{X}}(x) = \limsup \mathbf{1}_{\mathrm{U}_k}(x)$, si $x \notin \mathrm{A}'$, et donc que X ne diffère de $\mathrm{G} = \cap_{n\in\mathbf{N}} \cup_{k\geqslant n} \mathrm{U}_k$ que par des ensembles de mesure nulle, et comme $\cup_{k\geqslant n}\mathrm{U}_k$ est un ouvert, on a $\mathrm{G} \in \mathscr{G}_\delta$, ce qui fournit la première description cherchée. La seconde s'en déduisant en passant aux complémentaires, cela termine la démonstration.

3.3. *Fonctions mesurables et ensembles mesurables*

D'après la note 14, toute fonction et tout ensemble raisonnable sont mesurables (pour un ensemble déraisonnable, cf. ex. III.1.27), mais si on éprouve une réticence à utiliser ce métathéorème pour vérifier la mesurabilité d'une fonction, le résultat ci-dessous fournit un critère commode.

Proposition III.1.17. — *Les conditions suivantes sont équivalentes si* $f : \mathbf{R}^m \to \overline{\mathbf{R}}_+$ *:*

- f *est mesurable,*
- $f^{-1}(\mathrm{X})$ *est mesurable pour tout borélien* X *de* $\overline{\mathbf{R}}_+$*,*
- $f^{-1}([0, a[)$ *est mesurable pour tout* $a \in \mathbf{R}_+$*,*
- $f^{-1}([0, a])$ *est mesurable pour tout* $a \in \mathbf{R}_+$*.*

Démonstration. — L'équivalence entre les 3 derniers points résulte de ce que la tribu borélienne de $\overline{\mathbf{R}}_+$ est engendrée par les $[0, a[$ ou les $[0, a]$, pour $a \in \mathbf{R}_+$. Il suffit donc de prouver l'équivalence entre les premier et troisième points. Si $f^{-1}([0, a[)$ est mesurable pour tout $a \in \mathbf{R}_+$, alors $\mathrm{X}_{n,k} = f^{-1}([\frac{k}{2^n}, \frac{k+1}{2^n}[) = f^{-1}([0, \frac{k+1}{2^n}[) - f^{-1}([0, \frac{k}{2^n}[)$ l'est aussi, pour tous $n \in \mathbf{N}$ et $k \in \mathbf{N}$. Il s'ensuit que $f_n = \sum_{k\in\mathbf{N}} \frac{k}{2^n}\mathbf{1}_{\mathrm{X}_{n,k}}$ est mesurable, comme limite simple (i.e. série) de fonctions mesurables, et comme f_n tend simplement vers f, on en déduit la mesurabilité de f.

Réciproquement, soit f mesurable, et soit $(f_k)_{k\in\mathbf{N}}$ une suite d'éléments de $\mathrm{Esc}(\mathbf{R}^m, \mathbf{R}_+)$ tendant vers f en dehors de B, où B est de mesure nulle. Si $b \in \mathbf{R}_+$, soit $\mathrm{D}_{b,k} = f_k^{-1}([0, b[)$, et soient $\mathrm{X}_b = f^{-1}([0, b[)$ et $\mathrm{X}_b^+ = f^{-1}([0, b])$. Alors $\mathrm{D}_{b,k}$ est un dallage, et donc $\mathrm{Y}_b = \cap_{n\in\mathbf{N}} \cup_{k\geqslant n} \mathrm{D}_{b,k}$ est mesurable. Par ailleurs, si $x \in \mathrm{X}_b - \mathrm{B}$, alors $f(x) < b$, et donc $f_k(x) < b$, pour tout k assez grand, et donc $\mathrm{X}_b - \mathrm{B} \subset \mathrm{Y}_b$. De même, si $x \in \mathrm{Y}_b - \mathrm{B}$, alors $f_k(x) < b$, pour une infinité de k, et donc $f(x) \leqslant b$; autrement dit, $\mathrm{Y}_b - \mathrm{B} \subset \mathrm{X}_b^+$. Comme B est de mesure nulle, on en déduit l'existence de Y'_b, mesurable, ne différant de Y_b que par un ensemble de mesure nulle, tel que $\mathrm{X}_b \subset \mathrm{Y}'_b \subset \mathrm{X}_b^+$. On a alors $\mathrm{X}_a = \cup_{n\in\mathbf{N}}\mathrm{Y}'_{a_n}$, si a_n est une suite croissante de limite a, ce qui prouve que X_a est mesurable, en tant que réunion dénombrable d'ensembles mesurables. Ceci termine la démonstration.

4. Définition de l'intégrale de Lebesgue

Une fois qu'on a défini ce qu'était une fonction mesurable, on peut se demander comment la mesurer. Une mesure naturelle pour beaucoup de questions est fournie par l'intégrale de Lebesgue (et la mesure de Lebesgue). La présentation que nous avons choisie

est purement axiomatique [17] ; elle n'est pas sans rappeler le point de vue concernant les nombres réels adopté en classes préparatoires (où $\mathbf{R}$ est présenté comme un corps totalement ordonné dans lequel toute partie non vide admet une borne supérieure, le rôle joué par la propriété de la borne supérieure dans cette présentation de $\mathbf{R}$ étant tenu ici par le théorème de convergence monotone).

4.1. *Intégration des fonctions positives*

Théorème III.1.18. — *Il existe une unique application* $f \mapsto \int f$ *de* $\mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$ *dans* $\overline{\mathbf{R}}_+$ *vérifiant les propriétés* (i)–(v) *ci-dessous.*

(i) *Si* f *est en escalier, alors* $\int f$ *est la quantité précédemment définie.*

(ii) (linéarité) $\int (af + bg) = a \int f + b \int g$, *si* $a, b \in \mathbf{R}_+$, *et* $f, g \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$.

(iii) $\int f = 0$ *si et seulement si* $f = 0$ *p.p.*

(iv) *Si* $f \leqslant g$ *p.p., alors* $\int f \leqslant \int g$.

(v) (théorème de convergence monotone) *Si* (f_n) *est une suite croissante d'éléments de* $\mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$, *alors* $\lim_{n\to+\infty} \int f_n = \int \lim_{n\to+\infty} f_n$.

Remarque III.1.19. — (i) Les propriétés fondamentales sont la linéarité de l'intégration (propriété (ii)) et le théorème de convergence monotone (propriété (v)).

(ii) La propriété (iv) découle des (ii) et (iii) : en effet, on a $\int g + \int -\inf(0, g-f) = \int f + \int \sup(g-f, 0)$, où toutes les fonctions sont positives et $-\inf(0, g-f) = 0$ p.p. par hypothèse.

(iii) La propriété (i) est une normalisation qui définit une mesure bien particulière sur $\mathbf{R}^m$, à savoir la *mesure de Lebesgue*. Comme nous le verrons (th. III.3.8), cette propriété implique que la mesure de Lebesgue est invariante par translation. Réciproquement, si $f \to \int f$ est linéaire et invariante par translation [ce qui signifie que, pour tous $f \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$ et $a \in \mathbf{R}^m$, on a $\int \mathrm{T}_a(f) = \int f$, où $(\mathrm{T}_a(f))(t) = f(t+a)$], et si $\int e_{0,\mathbf{0}} = 1$, alors $\int e_{r,\mathbf{k}}$ ne dépend pas de $\mathbf{k}$, grâce à l'invariance par translation, et donc vaut 2^{-rm}, grâce à la normalisation $\int e_{0,\mathbf{0}} = 1$ (cela suit, par une récurrence sur r, de l'indépendance de $\int e_{r,\mathbf{k}}$ par rapport à $\mathbf{k}$ et de la formule $e_{r,\mathbf{k}} = \sum_{\mathbf{a}\in\{0,1\}^m} e_{r+1,\mathbf{k}+\mathbf{a}}$) ; la linéarité implique alors que $\int f$ vérifie la propriété (i). Autrement dit, on aurait pu remplacer [18] la propriété (i) par l'invariance par translation et la normalisation $\int e_{0,\mathbf{0}} = 1$.

17. Ceci a pour avantage de faire glisser sous le tapis certains points assez délicats sans diminuer la facilité d'utilisation de la théorie. Toutefois, dans le but d'atténuer le sentiment d'inconfort que ressent toujours un peu un esprit mathématicien à l'idée d'utiliser un résultat dont il n'a pas vu (et souvent oublié) une démonstration, nous avons inclus, au § III.4, une construction de l'intégrale satisfaisant les axiomes.

18. Ce procédé s'étend à tout groupe localement compact, ce qui inclut $\mathbf{R}^m$, les groupes finis, les groupes compacts, $\mathbf{Z}$, le groupe additif $\mathbf{Q}_p$, les groupes multiplicatifs $\mathbf{R}^*$, $\mathbf{C}^*$ ou $\mathbf{Q}_p^*$, ou plus généralement, si $d \geqslant 1$, les groupes $\mathbf{GL}_d(\mathbf{R})$, $\mathbf{GL}_d(\mathbf{C})$, $\mathbf{GL}_d(\mathbf{Q}_p)$ et leurs sous-groupes fermés... Un tel groupe possède, à multiplication près par une constante > 0, une unique mesure invariante à droite (resp. à gauche), ce qui

4.2. *Mesure de Lebesgue d'un ensemble*

Si $\mathrm{X} \subset \mathbf{R}^m$ est mesurable, *sa mesure de Lebesgue* est définie par $\lambda(\mathrm{X}) = \int \mathbf{1}_\mathrm{X} \in \overline{\mathbf{R}}_+$. La résultat suivant montre que la mesure de Lebesgue est dénombrablement additive et donc définit une mesure [19] sur $\mathbf{R}^m$ muni de la tribu des ensembles mesurables.

Proposition III.1.20. — *Si les* $(\mathrm{X}_i)_{i\in\mathrm{I}}$*, où* I *est dénombrable, sont des sous-ensembles mesurables de* $\mathbf{R}^m$ *deux à deux disjoints, alors*

$$\lambda(\cup_{i\in\mathrm{I}}\mathrm{X}_i) = \sum_{i\in\mathrm{I}} \lambda(\mathrm{X}_i).$$

Démonstration. — L'hypothèse selon laquelle les X_i sont deux à deux disjoints se traduit par $\mathbf{1}_{\cup_{i\in\mathrm{I}}\mathrm{X}_i} = \sum_{i\in\mathrm{I}} \mathbf{1}_{\mathrm{X}_i}$, et il n'y a plus qu'à numéroter les éléments de I et appliquer le théorème de convergence monotone (dans le cas I infini) à la suite des sommes partielles $\sum_{i\leqslant n} \mathbf{1}_{\mathrm{X}_i}$.

Proposition III.1.21. — *Soit* $f \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$.
(i) $\int f = 0$ *si et seulement si* $\lambda(\{t,\ f(t) \neq 0\}) = 0$.
(ii) *Si* $\int f < +\infty$*, alors* $\lambda(\{t,\ f(t) = +\infty\}) = 0$.

Démonstration. — Soit $\mathrm{A} = \{t,\ f(t) \neq 0\}$. Alors $\inf(f, \mathrm{N}) \leqslant \mathrm{N}\mathbf{1}_\mathrm{A}$ et $\int \inf(f, \mathrm{N}) \leqslant \mathrm{N}\lambda(\mathrm{A})$, pour tout $\mathrm{N} \in \mathbf{N}$. Comme $\inf(f, \mathrm{N})$ tend en croissant vers f, le th. de convergence monotone montre que $\int f = 0$ si $\lambda(\mathrm{A}) = 0$. Réciproquement, si $\int f = 0$, alors $\int \mathrm{N}f = \mathrm{N}\int f = 0$ pour tout N, et comme $\mathrm{N}f$ tend en croissant vers $+\infty\mathbf{1}_\mathrm{A}$, le th. de convergence monotone implique que $+\infty\lambda(\mathrm{A}) = 0$ et donc $\lambda(\mathrm{A}) = 0$. Ceci démontre le (i).

Pour démontrer le (ii), il suffit de remarquer que si $\mathrm{A} = \{t,\ f(t) = +\infty\}$, alors $f \geqslant \mathrm{M}\mathbf{1}_\mathrm{A}$ quel que soit $\mathrm{M} \in \mathbf{R}_+$, et donc $\mathrm{M}\lambda(\mathrm{A}) \leqslant \int f$ quel que soit $\mathrm{M} \in \mathbf{R}_+$.

Corollaire III.1.22. — X *est de mesure nulle si et seulement si* $\lambda(\mathrm{X}) = 0$.

Démonstration. — Si $\mathrm{X} \subset \mathbf{R}^m$ est mesurable, alors

$$\mathrm{X} \text{ est de mesure nulle} \iff \mathbf{1}_\mathrm{X} = 0 \text{ p.p.} \iff \int \mathbf{1}_\mathrm{X} = 0 \iff \lambda(\mathrm{X}) = 0.$$

La première équivalence est par définition, la seconde suit du (iii) du th. III.1.18, et la dernière résulte du (i) de la prop. III.1.21.

Le cor. III.1.22 est un cas particulier du résultat suivant, démontré au n° 2 du § III.4.

Théorème III.1.23. — *Si* X *est mesurable, alors* $\lambda(\mathrm{X}) = \lambda^+(\mathrm{X})$.

---

signifie que $\int \mathrm{T}^d_a(f) = \int f$ (resp. $\int \mathrm{T}^g_a(f) = \int f$), où $(\mathrm{T}^d_a(f))(x) = f(xa^{-1})$ et $(\mathrm{T}^g_a(f))(x) = f(ax)$; cette mesure est « la » *mesure de Haar* à droite (resp. à gauche).

19. Une *mesure* μ sur un ensemble de E muni d'une tribu $\mathscr{A}$ est une fonction $\mu : \mathscr{A} \to \overline{\mathbf{R}}_+$ vérifiant $\mu(\varnothing) = 0$ et $\mu(\cup_{i\in\mathrm{I}}\mathrm{X}_i) = \sum_{i\in\mathrm{I}} \mu(\mathrm{X}_i)$ pour toute famille dénombrable $(\mathrm{X}_i)_{i\in\mathrm{I}}$ d'éléments de $\mathscr{A}$ deux à deux disjoints.

Exercice III.1.24. — Soient $X_n \subset \mathbf{R}^m$ mesurables, pour $n \in \mathbf{N}$, et soient $B = \cup_{n\in\mathbf{N}} X_n$ et $C = \cap_{n\in\mathbf{N}} X_n$.
(i) Montrer que si la suite X_n est croissante, alors $\lambda(B) = \lim_{n\to+\infty} \lambda(X_n)$.
(ii) Montrer que si la suite X_n est décroissante et si $\lambda(X_0) < +\infty$, alors $\lambda(C) = \lim_{n\to+\infty} \lambda(X_n)$. Le résultat est-il toujours valable sans l'hypothèse $\lambda(X_0) < +\infty$?

Exercice III.1.25. — Soit $X \subset \mathbf{R}^m$ mesurable de mesure finie. Montrer que, quel que soit $\alpha \in [0,1]$, il existe $B \subset X$ mesurable tel que $\lambda(B) = \alpha\lambda(X)$. (On pourra s'intéresser à $f(t) = \lambda(X \cap [-t,t]^m)$.)

Exercice III.1.26. — (i) Montrer, en revenant à la définition, que $\lambda^+([0,1]) = 1$ (th. fondamental de la théorie de la mesure : il n'est pas si évident que $\lambda^+([0,1]) \neq 0$...).
(ii) Un *pavé* de $\mathbf{R}^m$ est un ensemble de la forme $\prod_{j=1}^m I_j$, où I_j est un intervalle de n'importe quel type (ouvert ou fermé à chacune des extrémités). Montrer que, si $P = \prod_{j=1}^m I_j$ est un pavé, sa mesure extérieure est donnée par $\lambda^+(P) = \prod_{j=1}^m \lambda(I_j)$, où $\lambda(I_j)$ est la longueur de l'intervalle I_j [i.e. si $a \leqslant b$ sont deux réels, alors $\lambda(]a,b[) = \lambda([a,b[) = \lambda(]a,b]) = \lambda([a,b]) = b-a$].

Exercice III.1.27. — Montrer que, si $S \subset [0,1]$ est un système de représentants de $\mathbf{R}/\mathbf{Q}$ (i.e. tout élément de $\mathbf{R}$ peut s'écrire de manière unique sous la forme $s+q$, avec $s \in S$ et $q \in \mathbf{Q}$), alors S n'est pas mesurable. Comparer avec la note 14.

4.3. *Intégration des fonctions sommables*

En découpant une fonction quelconque en partie réelle positive et négative et partie imaginaire positive et négative, cela permet de définir l'intégrale d'une fonction mesurable à valeurs dans $\mathbf{C}$. Toutefois, comme $+\infty-(+\infty)$ n'a pas de sens, on est forcé de restreindre l'ensemble des fonctions considérées.

Définition III.1.28. — (Intégrale de Lebesgue)
(i) $f \in \mathrm{Mes}(\mathbf{R}^m)$ est *sommable*, si $\int |f| < +\infty$. On note $\mathscr{L}^1(\mathbf{R}^m) \subset \mathrm{Mes}(\mathbf{R}^m)$ l'ensemble des fonctions sommables.
(ii) Si $f \in \mathscr{L}^1(\mathbf{R}^m)$, les fonctions $\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ et $\mathrm{Re}^+(-if)$ sont sommables puisque majorées par $|f|$, et on pose

$$\int f = \int \mathrm{Re}^+(f) - \int \mathrm{Re}^+(-f) + i\int \mathrm{Re}^+(-if) - i\int \mathrm{Re}^+(if).$$

Remarque III.1.29. — (i) L'intégrale $f \mapsto \int f$ est $\mathbf{C}$-linéaire : cela résulte formellement du (ii) du th. III.1.18. (Il est immédiat que $\int \lambda f = \lambda \int f$, si $\lambda \in \mathbf{R}$ ou si $\lambda = i$; le seul problème est donc de prouver que $\int f+g = \int f + \int g$. Après découpage en parties imaginaire et réelle, positive et négative, on est ramené à montrer que $\int f-g = \int f - \int g$, si f et g sont positives. Soient $A = \{x,\ f(x) \geqslant g(x)\}$ et $B = \{x,\ f(x) < g(x)\}$. Alors $\int f-g = \int (f-g)\mathbf{1}_A - \int (g-f)\mathbf{1}_B$ par définition. Comme $(f-g)\mathbf{1}_A + g\mathbf{1}_A = f\mathbf{1}_A$, on a $\int (f-g)\mathbf{1}_A + \int g\mathbf{1}_A = \int f\mathbf{1}_A$, et donc $\int (f-g)\mathbf{1}_A = \int f\mathbf{1}_A - \int g\mathbf{1}_A$. De même, $\int (g-f)\mathbf{1}_B = \int g\mathbf{1}_B - \int f\mathbf{1}_B$, et donc $\int (f-g)\mathbf{1}_A - \int (g-f)\mathbf{1}_B = \int f\mathbf{1}_A - \int g\mathbf{1}_A + \int f\mathbf{1}_B - \int g\mathbf{1}_B = \int f - \int g$ car $f = f\mathbf{1}_A + f\mathbf{1}_B$ et $g = g\mathbf{1}_A + g\mathbf{1}_B$.)

(ii) Si f est sommable, si $\int f = \rho e^{i\theta}$, et si h est définie par $f = |f|e^{ih}$ p.p., alors

$$\int |f| - |\int f| = \mathrm{Re}\big(\int |f| - |\int f|\big) = \mathrm{Re}\big(\int |f| - \int e^{-i\theta} f\big) = \mathrm{Re}\big(\int |f|(1 - e^{ih-i\theta})\big) \geqslant 0,$$

puisque la fonction $\mathrm{Re}(|f|(1-e^{ih-i\theta}))$ est positive. *En résumé,* $|\int f| \leqslant \int |f|$.

(iii) Si $\mathrm{X} \subset \mathbf{R}^m$ est mesurable, et si $\phi \in \mathscr{L}^1(\mathbf{R}^m)$, alors $\mathbf{1}_{\mathrm{X}}\phi \in \mathscr{L}^1(\mathbf{R}^m)$ car $|\mathbf{1}_{\mathrm{X}}\phi| \leqslant |\phi|$. On note $\int_{\mathrm{X}} \phi$, si $\phi \in \mathscr{L}^1(\mathbf{R}^m)$, l'intégrale $\int_{\mathbf{R}^m} \mathbf{1}_{\mathrm{X}}\phi$.

5. Les théorèmes de convergence monotone et de convergence dominée

Soit X un sous-ensemble mesurable de $\mathbf{R}^m$. On dit que $\phi : \mathrm{X} \to \mathbf{C}$ est mesurable si la fonction obtenue en prolongeant ϕ par 0 à $\mathbf{R}^m$ est mesurable. L'ensemble $\mathrm{Mes}(\mathrm{X})$ des fonctions mesurables sur X est donc naturellement un sous-espace de $\mathrm{Mes}(\mathbf{R}^m)$, et on définit $\mathscr{L}^1(\mathrm{X})$ comme l'intersection de $\mathrm{Mes}(\mathrm{X})$ avec $\mathscr{L}^1(\mathbf{R}^m)$.

L'application $\phi \to \mathbf{1}_{\mathrm{X}}\phi$ est une projection de $\mathscr{L}^1(\mathbf{R}^m)$ sur son sous-espace $\mathscr{L}^1(\mathrm{X})$.

Théorème III.1.30. — (de convergence monotone)

(i) *Si* $(f_n)_{n\in\mathbf{N}}$ *est une suite croissante d'éléments de* $\mathrm{Mes}(\mathrm{X}, \overline{\mathbf{R}}_+)$*, alors la limite est mesurable et* $\lim_{n\to+\infty} \int f_n = \int \lim_{n\to+\infty} f_n$.

(ii) *Si* $(u_n)_{n\in\mathbf{N}}$ *est une suite d'éléments de* $\mathrm{Mes}(\mathrm{X}, \overline{\mathbf{R}}_+)$*, alors la somme de la série est mesurable et* $\int \sum_{n\in\mathbf{N}} u_n = \sum_{n\in\mathbf{N}} \int u_n$ (Fubini pour les fonctions positives sur $\mathbf{N} \times \mathrm{X}$).

Démonstration. — Le (i) est immédiat (compte-tenu du théorème de convergence uniforme sur $\mathbf{R}^m$, cf. (v) du th. III.1.18). Le (ii) se déduit du (i) en considérant les sommes partielles.

Proposition III.1.31. — (Lemme de Fatou) *Si* $f_n \in \mathrm{Mes}(\mathrm{X}, \overline{\mathbf{R}}_+)$*, alors*

$$\int (\liminf f_n) \leqslant \liminf \int f_n.$$

Démonstration. — Soit $g_n = \inf_{k\geqslant n} f_k$. Alors g_n est mesurable comme limite simple de fonctions mesurables, et $g_n \to \liminf f_n$ en croissant, par définition de la limite inférieure. D'après le théorème de convergence monotone, on a donc $\int g_n \to \int \liminf f_n$. Par ailleurs, $\int g_n \leqslant \int f_n$ quel que soit n. On a donc

$$\int \liminf f_n = \lim \int g_n = \liminf \int g_n \leqslant \liminf \int f_n,$$

ce qu'il fallait démontrer.

Si $f \in \mathscr{L}^1(\mathrm{X})$, on définit sa (semi)-norme $\|f\|_1$ par $\|f\|_1 = \int |f|$. Il résulte du (iii) du th. III.1.18 que l'on a $\|f\|_1 = 0$ si et seulement si $f = 0$ p.p. On dit que f_k *tend vers* f *dans* $\mathscr{L}^1(\mathrm{X})$ (ou que f_k *tend vers* f *en moyenne*), si $\|f_k - f\|_1 \to 0$. Comme $\| \ \|_1$ est une semi-norme et pas une norme, la limite d'une suite n'est pas unique ; de fait si $f_k \to f$ dans $\mathscr{L}^1(\mathrm{X})$, alors $f_k \to g$ dans $\mathscr{L}^1(\mathrm{X})$ pour tout g tel que $g - f = 0$ p.p.

Il résulte du (ii) de la rem. III.1.29 que $|\int f| \leqslant \|f\|_1$, et donc que $f \mapsto \int f$ *est linéaire continue* (et même 1-lipschitzienne) *sur* $\mathscr{L}^1(\mathrm{X})$.

Théorème III.1.32. — (de convergence dominée)
Si $(f_n)_{n\in\mathbf{N}}$ est une suite d'éléments $\mathscr{L}^1(\mathrm{X})$ vérifiant :
• *il existe $g \in \mathscr{L}^1(\mathrm{X})$ telle que, quel que soit $n \in \mathbf{N}$, on a $|f_n| \leqslant g$ p.p.* (domination),
• *f_n converge simplement presque partout,*
alors la limite presque partout f de la suite $(f_n)_{n\in\mathbf{N}}$ appartient à $\mathscr{L}^1(\mathrm{X})$, et f_n tend vers f dans $\mathscr{L}^1(\mathrm{X})$; en particulier $\lim_{n\to+\infty}\int f_n = \int f$.

Démonstration. — f est mesurable comme limite simple p.p. de fonctions mesurables et sommable car $|f| \leqslant g$ p.p. (si $\mathrm{A}_n = \{x,\ |f_n| > g\}$, on a $|f| \leqslant g$, si $x \notin \mathrm{A} = \cup_{n\in\mathbf{N}}\mathrm{A}_n$, et comme A_n est de mesure nulle pour tout n, il en est de même de A). D'autre part, quitte à modifier g et les f_n sur un ensemble de mesure nulle, on peut supposer que l'on a $|f_n| \leqslant g$ partout. On a alors $|f_n - f| \leqslant 2g$, et on peut appliquer le lemme de Fatou à $h_n = 2g - |f_n - f|$. Comme $h_n \to 2g$, on obtient

$$\int 2g \leqslant \liminf \int 2g - |f_n - f| = \int 2g - \limsup \int |f_n - f|,$$

et comme $\int 2g$ est fini, on en tire $\limsup \int |f_n - f| \leqslant 0$, et donc $\int |f_n - f| \to 0$, puisque $\int |f_n - f| \geqslant 0$, quel que soit $n \in \mathbf{N}$. Ceci permet de conclure.

Exercice III.1.33. — Si $n \geqslant 1$, soient $f_n = n\mathbf{1}_{[0,1/n]}$ et $g_n = \frac{1}{n}\mathbf{1}_{[0,n]}$. Montrer que $f_n \to 0$ p.p et $g_n \to 0$ p.p., et que $\int f_n = \int g_n = 1$. Peut-on en déduire que $1 = 0$?

Exercice III.1.34. — (i) Montrer que $\Gamma(s) = \int_0^{+\infty} e^{-t}t^{s-1}\,dt$ est fini si $s > 0$.
(ii) Montrer que $\lim_{n\to\infty}\int_0^n \left(1 - \frac{t}{n}\right)^n t^{s-1}\,dt \to \Gamma(s)$ quand $n \to \infty$.
(iii) En déduire la formule $\Gamma(s) = \lim_{n\to\infty} \frac{n!\,n^s}{s(s+1)\cdots(s+n)}$ de Gauss.

Exercice III.1.35. — Soit $f : \mathbf{R}_+ \to \mathbf{R}_+$ décroissante et sommable. Montrer que $\lim_{t\to+\infty} tf(t) = 0$.

Exercice III.1.36. — Soient $f \in \mathscr{L}^1(\mathbf{R}^m)$ et A_n, pour $n \in \mathbf{N}$, des sous-ensembles mesurables de $\mathbf{R}^m$.
(i) Montrer que si A_n est croissante et $\cup_{n\in\mathbf{N}}\mathrm{A}_n = \mathbf{R}^m$, alors $\int_{\mathbf{R}^m} f = \lim_{n\to\infty}\int_{\mathrm{A}_n} f$.
(ii) Montrer que, si $\lambda(\mathrm{A}_n) \to 0$, alors $\int_{\mathrm{A}_n} f \to 0$. (Utiliser le th. de Borel-Cantelli ou le th. III.2.11.)

6. Premières applications

Le résultat qui suit est très utile pour calculer explicitement des intégrales en dimension 1 ; le théorème de Fubini dont il sera question plus loin permet de ramener le calcul d'intégrales en dimension quelconque à une suite d'intégrations en une variable (on n'est heureusement pas forcé de revenir à la définition !).

Théorème III.1.37. — (Théorème fondamental de l'analyse)
Si $f : [a,b] \to \mathbf{C}$ est continue, et si $\mathrm{F} : [a,b] \to \mathbf{C}$ est dérivable de dérivée f, alors $\int_{[a,b]} f = \mathrm{F}(b) - \mathrm{F}(a)$.

Démonstration. — Par linéarité, en considérant séparément Im(F) et Re(F), on peut se ramener au cas où F est à valeurs réelles. Si $n \in \mathbf{N}$, et si $i \in \{0, 1, \ldots, n\}$, soit $c_{n,i} = a + i\frac{b-a}{n}$, et soit $f_n : [a,b[\to \mathbf{R}$, la fonction valant $\frac{n}{b-a}\big(\mathrm{F}(c_{n,i+1}) - \mathrm{F}(c_{n,i})\big)$ sur $[c_{n,i}, c_{n,i+1}[$,

pour tout $i \in \{0, \dots, n-1\}$. Alors $\int f_n = \sum_{i=0}^{n-1} \big(\mathrm{F}(c_{n,i+1}) - \mathrm{F}(c_{n,i})\big) = \mathrm{F}(b) - \mathrm{F}(a)$, pour tout n. Le théorème des accroissements finis montre qu'il existe $u_{n,i} \in [c_{n,i}, c_{n,i+1}[$ tel que $f_n(t) = f(u_{n,i})$, si $t \in [c_{n,i}, c_{n,i+1}[$, et donc que $f_n(t) = f(u_n(t))$, avec $|t - u_n(t)| \leqslant \frac{b-a}{n}$. On en déduit que $|f_n| \leqslant \|f\|_\infty$ pour tout n et, f étant continue, que f_n tend simplement vers f sur $[a, b[$. On peut donc appliquer le théorème de convergence dominée pour intervertir limite et intégrale, ce qui nous donne $\int_{[a,b[} f = \mathrm{F}(b) - \mathrm{F}(a)$. Le résultat s'en déduit en remarquant que $\{b\}$ étant de mesure nulle, on a $\int_{[a,b[} f = \int_{[a,b]} f$.

Exercice III.1.38. — Soit $f : [a, b] \to \mathbf{C}$ dérivable. Montrer que f' est mesurable et que, si f' est bornée, alors $\int_a^b f' = f(b) - f(a)$.

Théorème III.1.39. — (convergence dominée pour les séries)
Soient I *un ensemble dénombrable et* $(a_{n,i})_{n\in\mathbf{N}, i\in\mathrm{I}}$ *des nombres complexes verifiant :*
- *il existe* $(b_i)_{i\in\mathrm{I}}$*, avec* $\sum_{i\in\mathrm{I}} |b_i| < +\infty$*, telle que* $|a_{n,i}| \leqslant b_i$ *pour tous* $n \in \mathbf{N}$ *et* $i \in \mathrm{I}$*,*
- $\lim_{n\to+\infty} a_{n,i}$ *existe pour tout* $i \in \mathrm{I}$*.*

Alors $\lim_{n\to+\infty} \sum_{i\in\mathrm{I}} a_{n,i} = \sum_{i\in\mathrm{I}} \lim_{n\to+\infty} a_{n,i}$.

Démonstration. — On peut supposer que $\mathrm{I} = \mathbf{N}$, et on transforme les séries en intégrales de fonctions « localement constantes » en associant à une suite $(u_n)_{n\in\mathbf{N}}$, la fonction valant u_n sur $[n, n+1[$ et 0 sur $\mathbf{R}_-^*$. L'énoncé se déduit alors du th. III.1.32 (en fait, on peut le démontrer directement, en se fatiguant un peu, cf. n° 15.3 du Vocabulaire).

III.2. Quelques espaces fonctionnels

1. L'espace $\mathrm{L}^1(\mathrm{X})$

Dans tout ce qui suit, X est un sous-ensemble mesurable de $\mathbf{R}^m$.

Théorème III.2.1. — (Fubini sur $\mathbf{N} \times \mathrm{X}$)
Soit $(u_n)_{n\in\mathbf{N}}$ *une suite d'éléments de* $\mathscr{L}^1(\mathrm{X})$ *telle que* $\sum_{n\in\mathbf{N}} \int |u_n| < +\infty$*.*
(i) *La série* $\sum_{n\in\mathbf{N}} u_n(t)$ *converge* (absolument) *p.p.*
(ii) *Si* $g = \sum_{n\in\mathbf{N}} u_n$ *p.p., alors* $g \in \mathscr{L}^1(\mathrm{X})$*, et la série de terme général* u_n *converge vers* g *dans* $\mathscr{L}^1(\mathrm{X})$ *; en particulier,* $\int_\mathrm{X} g = \sum_{n\in\mathbf{N}} \int_\mathrm{X} u_n$*.*

Démonstration. — Soit $h(t) = \sum_{n\in\mathbf{N}} |u_n(t)|$. D'après le théorème de convergence monotone, on a $\int_\mathrm{X} h = \sum_{n\in\mathbf{N}} \int |u_n|$, et l'hypothèse implique que $\int_\mathrm{X} h < +\infty$. La prop. III.1.21 permet d'en conclure que $\mathrm{A}_1 = \{t \in \mathrm{X},\ \sum_{n\in\mathbf{N}} |u_n(t)| = +\infty\}$ est de mesure nulle, et comme A_1 est précisément l'ensemble des $t \in \mathrm{X}$ tels que la série $\sum_{n\in\mathbf{N}} u_n(t)$ ne converge pas absolument, on en déduit le premier point.

Soit A_2 l'ensemble des points tels que $g(t) \neq \sum_{n\in\mathbf{N}} u_n(t)$. Alors A_2 est de mesure nulle par hypothèse, et donc $\mathrm{A} = \mathrm{A}_1 \cup \mathrm{A}_2$ est aussi de mesure nulle comme réunion de deux ensembles de mesure nulle. Soit S la fonction définie par $\mathrm{S}(t) = \sum_{n\in\mathbf{N}} u_n(t)$, si $t \notin \mathrm{A}$, et $\mathrm{S}(t) = 0$ si $t \in \mathrm{A}$. Si $\mathrm{N} \in \mathbf{N}$, soit $\mathrm{S}_\mathrm{N} = \sum_{n\leqslant\mathrm{N}} u_n$ la somme partielle de la série. On a

$S = g$ p.p., et pour démontrer le second point, il suffit de prouver que S est sommable et $\|S - S_N\|_1 \to 0$. Or $|S_N(t)| \leqslant h(t)$ quels que soient $t \notin A$ et $N \in \mathbf{N}$, et donc $|S(t)| \leqslant h(t)$, quel que soit $t \notin A$. On en déduit le fait que S est sommable. De plus, $|S_N - S| \leqslant 2h$ en dehors de A et $|S_N(t) - S(t)| \to 0$, si $t \notin A$. Comme A est de mesure nulle, on est dans les conditions d'application du théorème de convergence dominée ; on en déduit que $\int |S_N - S| \to 0$, ce qui permet de conclure.

Exercice III.2.2. — Soient $f \in \mathscr{L}^1(\mathbf{R})$ et $T \in \mathbf{R}_+^*$. Montrer que $f_T(x) = \sum_{n\in\mathbf{Z}} f(x + nT)$ converge presque partout et que f_T est sommable sur $[0, T]$.

Exercice III.2.3. — Soit $f : \mathbf{R} \to \mathbf{R}_+$ définie par $f(x) = |x|^{-1/2}$, si $0 < |x| < 1$, et $f(x) = 0$, sinon.

(i) Montrer que f est sommable.

(ii) Soit $n \mapsto r_n$ une bijection de $\mathbf{N}$ sur $\mathbf{Q}$. Montrer que $\sum_{n=0}^{+\infty} (\frac{-1}{2})^n f(x - r_n)$ converge absolument p.p., que la somme $F(x)$ est sommable, et calculer $\int_{\mathbf{R}} F(x)\,dx$. À quoi ressemble le graphe de F ?

Corollaire III.2.4. — *Si $(f_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathscr{L}^1(X)$ tendant vers f dans $\mathscr{L}^1(X)$, on peut extraire de la suite $(f_n)_{n\in\mathbf{N}}$ une sous-suite convergeant p.p. vers f.*

Démonstration. — Extrayons de $(f_n)_{n\in\mathbf{N}}$ une sous-suite $(g_n)_{n\in\mathbf{N}}$ telle que $\|f - g_n\|_1 \leqslant 2^{-n}$, pour tout $n \in \mathbf{N}$. Soit $u_n = g_n - g_{n-1}$, si $n \geqslant 1$, et $u_0 = g_0$. Alors $\sum_{n\in\mathbf{N}} \|u_n\|_1 < +\infty$, puisque $\|u_n\|_1 \leqslant \|g_n - f\|_1 + \|g_{n-1} - f\|_1 \leqslant 2^{1-n}$. D'après le th. III.2.1, la série $\sum_{n\in\mathbf{N}} u_n(x)$ converge presque partout, la limite presque partout g appartient à $\mathscr{L}^1(X)$, et $g_n = \sum_{i=0}^{n} u_i$ tend vers g dans $\mathscr{L}^1(X)$. Comme $g_n \to f$ dans $\mathscr{L}^1(X)$, on en déduit que $\|f - g\|_1 = 0$, ce qui implique que $f = g$ p.p., et que g_n tend vers f p.p., ce qui permet de conclure.

Exercice III.2.5. — Si $2^k \leqslant n < 2^{k+1}$, soit f_n la fonction caractéristique de $[\frac{n-2^k}{2^k}, \frac{n+1-2^k}{2^k}[$. Montrer que $f_n \to 0$ dans $\mathscr{L}^1([0, 1])$, mais que $f_n(x)$ ne tend vers 0 pour aucun $x \in [0, 1[$. Ce résultat n'est-il pas en contradiction avec le corollaire précédent ?

L'espace $\mathscr{L}^1(X)$ muni de la semi-norme $\| \ \|_1$ n'est pas séparé puisque deux fonctions différant d'une fonction nulle p.p. sont à distance nulle. On note $L^1(X)$ le séparé de $\mathscr{L}^1(X)$. Comme $\|f\|_1 = 0$ si et seulement si $f = 0$ p.p., $L^1(X)$ est le quotient de $\mathscr{L}^1(X)$ par le sous-espace Npp(X) des fonctions nulles presque partout ; on peut donc penser à $L^1(X)$ comme étant l'espace $\mathscr{L}^1(X)$ des fonctions sommables, en *considérant comme égales deux fonctions qui sont égales presque partout*[20].

Remarque III.2.6. — L'intégrale $f \mapsto \int f$ est bien définie sur $L^1(X)$ car $\int(f - g) = 0$ si $f = g$ p.p. De plus, $f \mapsto \int f$, qui est linéaire puisqu'elle l'est sur $\mathscr{L}^1(X)$, est continue car $|\int f| \leqslant \int |f| = \|f\|_1$.

20. Cette représentation mentale de $L^1(X)$ est probablement la plus facile d'utilisation ; il faut quand même faire attention qu'un élément de $L^1(X)$ a beau être défini presque partout, il n'a de valeur précise en aucun point puisqu'on peut modifier arbitrairement sa valeur sur un ensemble de mesure nulle. Autrement dit, on peut parler de $f(x)$, où x est pensé comme une variable (par exemple pour les changements de variable dans les intégrales, ou pour définir le produit d'une fonction de $L^1(X)$ et d'une fonction bornée), mais pas de $f(x_0)$.

Théorème III.2.7. — *L'espace* $\mathrm{L}^1(\mathrm{X})$ *est un espace de Banach.*

Démonstration. — On s'est débrouillé pour que $\| \ \|_1$ soit une norme sur $\mathrm{L}^1(\mathrm{X})$; il suffit donc de prouver que $\mathrm{L}^1(\mathrm{X})$ est complet, et pour cela, il suffit de vérifier que toute série normalement convergente est convergente, ce qui est précisément le contenu du th. III.2.1.

2. L'espace $\mathrm{L}^2(\mathrm{X})$

Si X est un sous-ensemble mesurable de $\mathbf{R}^m$, on note $\mathscr{L}^2(\mathrm{X})$ l'ensemble des $f : \mathrm{X} \to \mathbf{C}$ mesurables et *de carré sommable* (i.e. telles que $\int_{\mathrm{X}} |f(t)|^2\, dt < +\infty$). Il est immédiat que $\mathscr{L}^2(\mathrm{X})$ est stable par multiplication par un scalaire, et un peu moins qu'il est stable par addition, mais cela résulte de l'inégalité $|a+b|^2 \leqslant 2|a|^2 + 2|b|^2$, si $a, b \in \mathbf{C}$ dont on déduit que $\int_{\mathrm{X}} |f+g|^2 \leqslant (2\int_{\mathrm{X}} |f|^2 + 2\int_{\mathrm{X}} |g|^2)$, si $f, g \in \mathrm{Mes}(\mathrm{X})$. Autrement dit, $\mathscr{L}^2(\mathrm{X})$ est un espace vectoriel.

Maintenant, comme $|ab| \leqslant \frac{1}{2}(|a|^2 + |b|^2)$, si $a, b \in \mathbf{C}$, on en déduit que, si $f, g \in \mathscr{L}^2(\mathrm{X})$, alors $\overline{f}g \in \mathscr{L}^1(\mathrm{X})$, ce qui permet de définir $\langle f, g\rangle \in \mathbf{C}$ par $\langle f, g\rangle = \int_{\mathrm{X}} \overline{f}g$. L'application $\langle\ ,\ \rangle$ vérifie toutes les propriétés d'un produit scalaire, sauf celle d'être définie. On a :

$$\langle f, f\rangle = 0 \Longleftrightarrow \int_{\mathrm{X}} |f(t)|^2 = 0 \Longleftrightarrow f \in \mathrm{Npp}(\mathrm{X}).$$

Autrement dit, l'application $f \mapsto \|f\|_2 = \langle f, f\rangle^{1/2}$ définit une semi-norme hilbertienne sur $\mathscr{L}^2(\mathrm{X})$. On note $\mathrm{L}^2(\mathrm{X})$ l'espace séparé associé ; d'après ce qui précède, c'est le quotient de $\mathscr{L}^2(\mathrm{X})$ par $\mathrm{Npp}(\mathrm{X})$. Ceci permet, comme pour $\mathrm{L}^1(\mathrm{X})$, de penser à $\mathrm{L}^2(\mathrm{X})$ comme étant l'espace $\mathscr{L}^2(\mathrm{X})$ des fonctions de carré sommable, en considérant comme égales deux fonctions qui sont égales presque partout. Comme $\langle f, g\rangle = 0$, si f ou g est nulle p.p., la forme sesquilinéaire $\langle\ ,\ \rangle$ passe au quotient, et induit un produit scalaire sur $\mathrm{L}^2(\mathrm{X})$, étant donné qu'on a fait ce qu'il fallait pour la rendre définie.

Théorème III.2.8. — (Fischer-Riesz, 1907) *L'espace* $\mathrm{L}^2(\mathrm{X})$*, muni de la norme* $\| \ \|_2$ *définie par* $\|f\|_2 = \big(\int_{\mathrm{X}} |f|^2\big)^{1/2}$*, est un espace de Hilbert.*

Démonstration. — D'après la discussion précédant le théorème, il suffit de prouver que $\mathrm{L}^2(\mathrm{X})$ est complet, et pour cela, il suffit de prouver qu'une série normalement convergente a une limite. La démonstration, très analogue à celle du th. III.2.7, fait l'objet de l'exercice ci-dessous. La convergence dans $\mathrm{L}^2(\mathrm{X})$ est dite *en moyenne quadratique.*

Exercice III.2.9. — Soit $(u_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathscr{L}^2(\mathrm{X})$ telle que $\sum_{n\in\mathbf{N}} \|u_n\|_2 < +\infty$, et soit $h : \mathrm{X} \to \overline{\mathbf{R}}_+$ définie par $h(t) = (\sum_{n\in\mathbf{N}} |u_n(t)|)^2$.

(i) Montrer que $\int_{\mathrm{X}} h < +\infty$. En déduire qu'il existe $\mathrm{A} \subset \mathrm{X}$ de mesure nulle tel que, si $t \in \mathrm{X} - \mathrm{A}$, la série $\sum_{n\in\mathbf{N}} u_n(t)$ converge absolument.

(ii) On note $\mathrm{S}(t)$ la somme de la série $\sum_{n\in\mathbf{N}} u_n(t)$, si $t \notin \mathrm{A}$, et on prolonge S par 0 à A, et, si $\mathrm{N} \in \mathbf{N}$, on pose $\mathrm{S}_\mathrm{N}(t) = \sum_{n\leqslant\mathrm{N}} u_n(t)$. Montrer que $|\mathrm{S} - \mathrm{S}_\mathrm{N}|^2$ est majoré par $4h$, quel que soit $\mathrm{N} \in \mathbf{N}$.

(iii) Montrer que $\mathrm{S} \in \mathscr{L}^2(\mathrm{X})$ et que $\mathrm{S}_\mathrm{N} \to \mathrm{S}$ dans $\mathrm{L}^2(\mathrm{X})$.

(iv) Montrer que, si $f_n \to f$ dans $\mathscr{L}^2(\mathrm{X})$, on peut extraire de la suite $(f_n)_{n\in\mathbf{N}}$ une sous-suite convergeant p.p. vers f.

3. Convergence dans L^1 et L^2

Remarque III.2.10. — (i) Les espaces $L^1(X)$ et $L^2(X)$ n'ont a priori rien à voir. Toutefois, comme ils sont tous deux obtenus en prenant le quotient d'un sous-espace de Mes(X) par Npp(X), nous commettrons l'abus de notations de désigner par $L^1(X)+L^2(X)$ (resp. $L^1(X)\cap L^2(X)$) le quotient de $\mathscr{L}^1(X)+\mathscr{L}^2(X)$ (resp. $\mathscr{L}^1(X)\cap\mathscr{L}^2(X)$) par Npp(X). Autrement dit, nous verrons un élément de $L^1(X)\cap L^2(X)$ comme une fonction qui est à la fois sommable et de carré sommable, à addition près d'une fonction nulle presque partout.

(ii) Il n'y a d'inclusion dans aucun sens entre $L^1(\mathbf{R}^m)$ et $L^2(\mathbf{R}^m)$. Par contre, *si* X *est de mesure finie*, alors $L^2(X)\subset L^1(X)$. En effet, l'inégalité de Cauchy-Schwarz montre que, si f est de carré sommable sur X, alors

$$\int_X |f| \leqslant \Big(\int_X 1\Big)^{1/2}\Big(\int_X |f|^2\Big)^{1/2} < +\infty.$$

En fait, l'inégalité ci-dessus montre que l'inclusion ι de $L^2(X)$ dans $L^1(X)$ est continue, et que l'on a $\|\iota\| \leqslant \lambda(X)^{1/2}$.

Soit X un ouvert de $\mathbf{R}^m$. On rappelle que $\mathscr{C}_c(X)$, $\mathscr{C}_c^k(X)$ et $\mathscr{C}_c^\infty(X)$ désignent respectivement l'espace des fonctions continues (resp. de classe $\mathscr{C}^k$, resp. de classe $\mathscr{C}^\infty$) sur X, dont le support est compact. Comme une fonction continue, nulle p.p., est identiquement nulle, la projection naturelle de $\mathscr{L}^1(X)$ sur $L^1(X)$ induit une injection de chacun des espaces ci-dessus dans $L^1(X)$, ce qui permet de les considérer comme des sous-espaces de $L^1(X)$. Pour la même raison, Esc(X) est, de manière naturelle, un sous-espace de $L^1(X)$.

Une fonction générale de $L^1(X)$ ou $L^2(X)$ étant assez difficile à appréhender (ex. III.2.3), le très utile résultat suivant permet de démontrer des résultats sur $L^1(X)$ ou $L^2(X)$ en commençant par des fonctions simples et en utilisant des arguments de continuité pour traiter le cas général (cf. th. IV.2.7). Il montre que l'on aurait pu aussi définir $L^1(X)$ et $L^2(X)$ comme les complétés de $\mathscr{C}_c(X)$ (ou de Esc(X)) pour les normes $\|\ \|_1$ et $\|\ \|_2$.

Théorème III.2.11. — *Si* X *est un ouvert de* $\mathbf{R}^m$*, et si* E *est un des espaces* Esc(X)*,* $\mathscr{C}_c(X)$*,* $\mathscr{C}_c^k(X)$*, avec* $k\in\mathbf{N}$*, ou* $\mathscr{C}_c^\infty(X)$*, alors* E *est dense dans* $L^1(X)$ *et* $L^2(X)$*. De plus, si* $\phi\in L^1(X)\cap L^2(X)$*, il existe une suite d'éléments de* E *convergeant vers* ϕ*, à la fois dans* $L^1(X)$ *et dans* $L^2(X)$*.*

Démonstration. — Si D_n est la réunion des dalles élémentaires de taille 2^{-n} incluses dans $X\cap([-2^n,2^n[^m)$, alors X est la réunion croissante des dallages D_n, pour $n\in\mathbf{N}$. Soit F un des espaces $L^1(X)$, $L^2(X)$ ou $L^1(X)\cap L^2(X)$, et soit $\phi\in F$ [on munit $L^1(X)\cap L^2(X)$ de la norme $\sup(\|\ \|_1,\|\ \|_2)$]. Si $n\in\mathbf{N}$, soit ϕ_n la fonction valant $\phi(x)$, si $x\in D_n$ et $|\phi_n(x)|\leqslant n$, et valant 0 si $x\notin D_n$ ou si $|\phi(x)|>n$. Alors $\phi_n(x)\to\phi(x)$ quel que soit $x\in X$, et comme $|\phi_n|\leqslant|\phi|$ et $|\phi_n^2|\leqslant|\phi^2|$, cela implique que ϕ_n converge vers ϕ dans F, d'après le théorème de convergence dominée. On peut donc, si $j\in\mathbf{N}$, trouver n_j tel que $\|\phi-\phi_{n_j}\|_F\leqslant 2^{-j}$. Maintenant, comme ϕ_{n_j} est une fonction mesurable bornée à support

borné, il existe $f_j \in \mathrm{Esc}(\mathrm{D}_{n_j})$ tel que $\|f_j - \phi_{n_j}\|_\mathrm{F} \leqslant 2^{-j}$. On a donc $\|f_j - \phi\|_\mathrm{F} \leqslant 2^{1-j}$. On en déduit la densité de Esc(X) dans F, ce qui prouve le théorème pour $\mathrm{E} = \mathrm{Esc}(\mathrm{X})$. Le reste s'en déduit en utilisant l'existence de fonctions $\mathscr{C}^\infty$ sympathiques (cf. exercice ci-dessous).

Exercice III.2.12. — La fonction φ_0 définie par $\varphi_0(x) = 0$ si $x \leqslant 0$ et $\varphi_0(x) = e^{-1/x}$ si $x > 0$ est une fonction $\mathscr{C}^\infty$ sur $\mathbf{R}$ (la dérivée n-ième de φ_0 sur $\mathbf{R}_+^*$ est de la forme $e^{-1/x}\mathrm{P}_n(\frac{1}{x})$, où P_n est un polynôme ; elle tend donc vers 0 en 0^+, ce qui permet de la recoller avec la dérivée n-ième de φ_0 sur $\mathbf{R}_-^*$).

(i) A partir de φ_0, construire successivement des fonctions $\mathscr{C}^\infty$ sur $\mathbf{R}$:

• $\varphi_1 : \mathbf{R} \to [0,1]$, nulle en dehors de $[0,1]$, avec $\int_0^1 \varphi_1 = 1$;

• $\varphi_2 : \mathbf{R} \to [0,1]$, valant 0 si $x \leqslant 0$ et 1 ; si $x \geqslant 1$;

• $\varphi_\varepsilon : \mathbf{R} \to [0,1]$, pour $\varepsilon \in]0, \frac{1}{2}[$, nulle en dehors de $[0,1]$ et valant 1 sur $[\varepsilon, 1-\varepsilon]$.

(ii) Terminer la démonstration du théorème III.2.11.

Corollaire III.2.13. — *Si $f \in \mathrm{L}^1(\mathrm{X})$ vérifie $\int_\mathrm{X} \varphi f = 0$, pour tout $\varphi \in \mathscr{C}_c^\infty(\mathrm{X})$, alors $f = 0$.*

Démonstration. — Il résulte de la démonstration du th. III.2.11 que, si $g \in \mathrm{L}^1(\mathrm{X})$ est bornée, on peut trouver une suite $(g_n)_{n\in\mathbf{N}}$ d'éléments de $\mathscr{C}_c^\infty(\mathrm{X})$ tendant vers g dans $\mathrm{L}^1(\mathrm{X})$ et vérifiant de plus $\|g_n\|_\infty \leqslant \|g\|_\infty$, pour tout n. En outre, quitte à extraire une sous-suite, on peut s'arranger (cor. III.2.4) pour que $g_n \to g$ p.p.

Ce qui précède s'applique en particulier, si $\mathrm{Y} \subset \mathrm{X}$ est un ouvert de mesure finie, à la fonction g_Y définie par $g_\mathrm{Y}(x) = 0$, si $f(x) = 0$ ou $x \notin \mathrm{Y}$, et $g_\mathrm{Y}(x) = \overline{f}(x)/|f(x)|$, si $f(x) \neq 0$ et $x \in \mathrm{Y}$. La suite $g_n f$ tend alors vers $\mathbf{1}_\mathrm{Y}|f|$ p.p. et est majorée, pour tout n, par $\|g_\mathrm{Y}\|_\infty |f| = |f|$. On est donc sous les conditions d'application du th. de convergence dominée, ce qui permet de montrer que $\int g_n f \to \int_\mathrm{Y} |f|$. L'hypothèse $\int_\mathrm{X} \varphi f = 0$ pour tout $\varphi \in \mathscr{C}_c^\infty(\mathrm{X})$ entraîne donc $\int_\mathrm{Y} |f| = 0$, pour tout Y, et donc aussi $\int |f| = 0$ par le théorème de convergence monotone. Ceci permet de conclure.

4. Comparaison des différents modes de convergence

Soit X un ouvert de $\mathbf{R}^m$, et soient ϕ_n, pour $n \in \mathbf{N}$, et f des fonctions de X dans $\mathbf{C}$. Nous avons rencontré un certain nombre de notions de convergence de la suite $(\phi_n)_{n\in\mathbf{N}}$ vers f ; il n'est probablement pas inutile de récapituler les liens qu'ont ces divers modes de convergence.

• $\phi_n \to f$ uniformément $\Rightarrow$ $\phi_n \to f$ simplement $\Rightarrow$ $\phi_n \to f$ simplement p.p.

• $\phi_n \to f$ simplement p.p. et $(\phi_n)_{n\in\mathbf{N}}$ est dominée par une fonction sommable (resp. de carré sommable) $\Rightarrow$ $\phi_n \to f$ dans $\mathrm{L}^1(\mathrm{X})$ (resp. dans $\mathrm{L}^2(\mathrm{X})$).

• $\phi_n \to f$ dans $\mathrm{L}^1(\mathrm{X})$ ou $\mathrm{L}^2(\mathrm{X})$ $\Rightarrow$ il existe une sous-suite de $(\phi_n)_{n\in\mathbf{N}}$ tendant vers f p.p.

• Si $\lambda(\mathrm{X}) < +\infty$, alors $\phi_n \to f$ dans $\mathrm{L}^2(\mathrm{X}) \Rightarrow \phi_n \to f$ dans $\mathrm{L}^1(\mathrm{X})$.

Terminons ce n° par ce petit résultat qui sera utile plus tard.

Lemme III.2.14. — *Soit* X *un ouvert de* $\mathbf{R}^m$.

(i) *Soient* $\phi \in \mathrm{L}^1(\mathrm{X})$, *et* $g \in \mathscr{C}(\mathrm{X})$. *S'il existe une suite* $(\phi_j)_{j\in\mathbf{N}}$ *d'éléments de* $\mathrm{L}^1(\mathrm{X})$ *tendant vers* ϕ *dans* $\mathrm{L}^1(\mathrm{X})$, *telle que* $\phi_j(x) \to g(x)$ *p.p.* , *alors* $g \in \mathrm{L}^1(\mathrm{X})$ *et* $g = \phi$ *p.p.*

(ii) *On a le même résultat en remplaçant* $\mathrm{L}^1(\mathrm{X})$ *par* $\mathrm{L}^2(\mathrm{X})$.

Démonstration. — La démonstration est exactement la même dans les deux cas. Quitte à extraire une sous-suite de la suite $(\phi_j)_{j\in\mathbf{N}}$, on peut supposer (cf. cor. III.2.4 et (iv) de l'ex. III.2.9) que $\phi_j(x) \to \phi(x)$ p.p., ce qui permet de conclure.

5. Espaces L^p

Les espaces $\mathrm{L}^1(\mathrm{X})$ et $\mathrm{L}^2(\mathrm{X})$ vivent dans une famille $\mathrm{L}^p(\mathrm{X})$, pour $p \in [1, +\infty]$, d'espaces de Banach introduits par F. Riesz en 1910, obtenus comme séparés de sous-espaces $\mathscr{L}^p(\mathrm{X})$ de $\mathrm{Mes}(\mathrm{X})$ (de fait, dans tous les cas, on passe de $\mathscr{L}^p(\mathrm{X})$ à $\mathrm{L}^p(\mathrm{X})$ en quotientant par $\mathrm{Npp}(\mathrm{X})$). Les espaces $\mathscr{L}^p(\mathrm{X})$ sont définis comme suit.

• Si $1 \leqslant p < +\infty$, on définit $\mathscr{L}^p(\mathrm{X})$ comme le sous-espace de $\mathrm{Mes}(\mathrm{X})$ des f tels que $|f|^p$ soit sommable. *L'inégalité de Minkowski* $(\int |f+g|^p)^{1/p} \leqslant (\int |f|^p)^{1/p} + (\int |g|^p)^{1/p}$ permet de montrer que $\mathscr{L}^p(\mathrm{X})$ est un espace vectoriel et que $f \mapsto \|f\|_p = (\int |f|^p)^{1/p}$ est une semi-norme sur $\mathscr{L}^p(\mathrm{X})$.

• Si $p = +\infty$, on définit l'espace $\mathscr{L}^\infty(\mathrm{X})$ comme le sous-espace de $\mathrm{Mes}(\mathrm{X})$ des f qui sont *essentiellement bornées*, c'est-à-dire qu'il existe $\mathrm{A} \subset \mathrm{X}$ de mesure nulle et $\mathrm{M} \in \mathbf{R}_+$ tels que $|f(t)| \leqslant \mathrm{M}$, quel que soit $t \in \mathrm{X} - \mathrm{A}$. On note $\|f\|_\infty$ la *borne supérieur essentielle* de $|f|$, c'est-à-dire la borne inférieure de l'ensemble des $\mathrm{M} \in \mathbf{R}_+$, tels qu'il existe $\mathrm{A} \subset \mathrm{X}$ de mesure nulle tel que $|f(t)| \leqslant \mathrm{M}$, quel que soit $t \in \mathrm{X} - \mathrm{A}$. Alors $\| \ \|_\infty$ est une semi-norme sur $\mathscr{L}^\infty(\mathrm{X})$.

Si X est un ouvert de $\mathbf{R}^m$, et si $p < +\infty$, les fonctions en escalier sont denses dans $\mathrm{L}^p(\mathrm{X})$. Ce n'est plus le cas si $p = +\infty$, l'adhérence des fonctions en escalier étant l'ensemble des fonctions bornées tendant vers 0 à l'infini.

L'espace $\mathrm{L}^2(\mathrm{X})$ étant un espace de Hilbert, il est son propre dual d'après le théorème de Riesz. Dans le cas général, on note $q \in [1, +\infty]$ *l'exposant conjugué* de p, défini par $1/p + 1/q = 1$. *L'inégalité de Hölder* $\int |fg| \leqslant \|f\|_p \|g\|_q$ montre que si $g \in \mathrm{L}^q(\mathrm{X})$, alors $f \mapsto \int fg$ définit une forme linéaire Λ_g continue sur $\mathrm{L}^p(\mathrm{X})$, et que l'on a $\|\Lambda_g\| \leqslant \|g\|_q$ (le résultat est trivial si $p = 1$ ou $p = +\infty$). Si $p \neq +\infty$, on peut montrer qu'en fait $g \mapsto \Lambda_g$ est une isométrie [21] de $\mathrm{L}^q(\mathrm{X})$ sur le dual de l'espace de Banach $\mathrm{L}^p(\mathrm{X})$. Par contre, le dual de $\mathrm{L}^\infty(\mathbf{R}^m)$ est nettement plus gros que $\mathrm{L}^1(\mathbf{R}^m)$.

Exercice III.2.15. — (i) Montrer que $\mathrm{L}^1(\mathrm{X})$ et $\mathrm{L}^2(\mathrm{X})$ sont séparables, si $\mathrm{X} \subset \mathbf{R}^m$ est mesurable.

(ii) Montrer que $\mathrm{L}^\infty(\mathbf{R}^m)$ n'est pas séparable.

III.3. Intégrales multiples

1. Le théorème de Fubini

Une somme finie $\sum_{j,k} a_{j,k}$ peut se calculer en sommant d'abord sur j puis sur k ou en sommant d'abord sur k puis sur j. Le théorème de Fubini ci-dessous dit qu'il en est de

21. On remarquera que, si X est de mesure finie, les $\mathrm{L}^p(\mathrm{X})$ forment une famille décroissante d'espaces de Banach (on a $\mathrm{L}^p(\mathrm{X}) \subset \mathrm{L}^{p'}(\mathrm{X})$ si $p \geqslant p'$), alors que leurs duaux $\mathrm{L}^q(\mathrm{X})$ forment une famille croissante. Autrement dit, plus l'espace fonctionnel est petit, plus son dual est gros, ce qui est un peu étrange quand on pense au cas des espaces vectoriels de dimension finie, mais conduit à la construction des distributions pour laquelle L. Schwartz a obtenu la medaille Fields (1950).

même pour des intégrales (à condition que tout soit sommable).

Lemme III.3.1. — (Fubini pour les fonctions en escalier) *L'application* $f \mapsto \int_{\mathbf{R}^n} f$ (*resp.* $f \mapsto \int_{\mathbf{R}^m} f$) *est une application linéaire de* $\mathrm{Esc}(\mathbf{R}^{n+m})$ *dans* $\mathrm{Esc}(\mathbf{R}^m)$ (*resp.* $\mathrm{Esc}(\mathbf{R}^n)$)*, et on a*

$$\int_{\mathbf{R}^m} \Big|\int_{\mathbf{R}^n} f\Big| \leqslant \int_{\mathbf{R}^{n+m}} |f| \quad \text{et} \quad \int_{\mathbf{R}^n} \Big|\int_{\mathbf{R}^m} f\Big| \leqslant \int_{\mathbf{R}^{n+m}} |f|$$
$$\int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} f\Big) = \int_{\mathbf{R}^{n+m}} f = \int_{\mathbf{R}^n} \Big(\int_{\mathbf{R}^m} f\Big).$$

Démonstration. — La linéarité est une conséquence de la linéarité de l'intégrale. Maintenant, soit $r \in \mathbf{N}$, et soient $\mathbf{j} = (j_1, \dots, j_n) \in \mathbf{Z}^n$ et $\mathbf{k} = (k_1, \dots, k_m) \in \mathbf{Z}^m$. On note $(\mathbf{j}, \mathbf{k})$ l'élément $(j_1, \dots, j_n, k_1, \dots, k_m)$ de $\mathbf{Z}^{n+m}$. Un calcul immédiat montre alors que

$$\int_{\mathbf{R}^n} e_{r,(\mathbf{j},\mathbf{k})} = 2^{-rn} e_{r,\mathbf{k}}, \qquad \int_{\mathbf{R}^m} e_{r,(\mathbf{j},\mathbf{k})} = 2^{-rm} e_{r,\mathbf{j}},$$
$$\int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} e_{r,(\mathbf{j},\mathbf{k})}\Big) = 2^{-rn} \int_{\mathbf{R}^m} e_{r,\mathbf{k}} = 2^{-r(n+m)} = \int_{\mathbf{R}^{n+m}} e_{r,(\mathbf{j},\mathbf{k})} = \int_{\mathbf{R}^n} \Big(\int_{\mathbf{R}^m} e_{r,(\mathbf{j},\mathbf{k})}\Big).$$

Le résultat s'en déduit en décomposant f sous la forme $f = \sum_{(\mathbf{j},\mathbf{k})} a_{(\mathbf{j},\mathbf{k})} e_{r,(\mathbf{j},\mathbf{k})}$, pour r assez grand (la somme étant une somme finie).

Proposition III.3.2. — (Fubini dans L^1) *Il existe une unique application linéaire continue* $f \mapsto \int_{\mathbf{R}^n} f$ (*resp.* $f \mapsto \int_{\mathbf{R}^m} f$) *de* $\mathrm{L}^1(\mathbf{R}^{n+m})$ *dans* $\mathrm{L}^1(\mathbf{R}^m)$ (*resp.* $\mathrm{L}^1(\mathbf{R}^n)$) *coïncidant avec l'application du même nom sur* $\mathrm{Esc}(\mathbf{R}^{n+m})$*, et on a*

$$\int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} f\Big) = \int_{\mathbf{R}^{n+m}} f = \int_{\mathbf{R}^n} \Big(\int_{\mathbf{R}^m} f\Big).$$

Démonstration. — L'application linéaire $\int_{\mathbf{R}^n} : \mathrm{Esc}(\mathbf{R}^{n+m}) \to \mathrm{L}^1(\mathbf{R}^m)$ est, d'après le lemme III.3.1, uniformément continue (en fait 1-lipschitzienne) si on munit tous les espaces de la norme $\| \ \|_1$. Comme $\mathrm{L}^1(\mathbf{R}^m)$ est complet, et comme $\mathrm{Esc}(\mathbf{R}^{n+m})$ est dense dans $\mathrm{L}^1(\mathbf{R}^{n+m})$, l'application $\int_{\mathbf{R}^n} : \mathrm{Esc}(\mathbf{R}^{n+m}) \to \mathrm{L}^1(\mathbf{R}^m)$ s'étend (de manière unique) par continuité à $\mathrm{L}^1(\mathbf{R}^{n+m})$. De même, $\int_{\mathbf{R}^m} : \mathrm{Esc}(\mathbf{R}^{n+m}) \to \mathrm{L}^1(\mathbf{R}^n)$ s'étend par continuité à $\mathrm{L}^1(\mathbf{R}^{n+m})$. Enfin, les trois applications

$$f \mapsto \int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} f\Big), \quad f \mapsto \int_{\mathbf{R}^{n+m}} f, \quad f \mapsto \int_{\mathbf{R}^n} \Big(\int_{\mathbf{R}^m} f\Big)$$

sont continues sur $\mathrm{L}^1(\mathbf{R}^{n+m})$ et coïncident sur $\mathrm{Esc}(\mathbf{R}^{n+m})$. Comme cet espace est dense dans $\mathrm{L}^1(\mathbf{R}^{n+m})$, elles coïncident sur $\mathrm{L}^1(\mathbf{R}^{n+m})$ tout entier. Ceci permet de conclure.

On peut rendre la prop. III.3.2 plus concrète (et plus facilement utilisable pour le calcul d'intégrales multiples) sous la forme du (i) du théorème suivant.

Théorème III.3.3. — (Fubini)
(i) *Si* $f \in \mathscr{L}^1(\mathbf{R}^{n+m})$, *alors*
- $f(\cdot, y) \in \mathscr{L}^1(\mathbf{R}^n)$, *pour presque tout* $y \in \mathbf{R}^m$, *et* $y \mapsto \int_{\mathbf{R}^n} f(x,y)dx \in \mathscr{L}^1(\mathbf{R}^m)$,
- $f(x, \cdot) \in \mathscr{L}^1(\mathbf{R}^m)$, *pour presque tout* $x \in \mathbf{R}^n$, *et* $x \mapsto \int_{\mathbf{R}^m} f(x,y)dy \in \mathscr{L}^1(\mathbf{R}^n)$,

$$\int_{\mathbf{R}^m} \big(\int_{\mathbf{R}^n} f(x,y)\, dx\big)\, dy = \int_{\mathbf{R}^{n+m}} f(x,y)\ dx\, dy = \int_{\mathbf{R}^n} \big(\int_{\mathbf{R}^m} f(x,y)\, dy\big)\, dx.$$

(ii) *Si* $f : \mathbf{R}^{n+m} \to \overline{\mathbf{R}}_+$ *est mesurable, alors les fonctions*

$$y \mapsto \int_{\mathbf{R}^n} f(x,y)dx \quad \text{et} \quad x \mapsto \int_{\mathbf{R}^m} f(x,y)dy,$$

à valeurs dans $\overline{\mathbf{R}}_+$, *sont mesurables, et*

$$\int_{\mathbf{R}^m} \big(\int_{\mathbf{R}^n} f(x,y)\, dx\big)\, dy = \int_{\mathbf{R}^{n+m}} f(x,y)\ dx\, dy = \int_{\mathbf{R}^n} \big(\int_{\mathbf{R}^m} f(x,y)\, dy\big)\, dx.$$

Remarque III.3.4. — (i) Si $\mathrm{X} \subset \mathbf{R}^n$ et $\mathrm{Y} \subset \mathbf{R}^m$ sont mesurables, alors $\mathrm{X}\times\mathrm{Y}$ est mesurable dans $\mathbf{R}^{n+m}$, et on a un énoncé analogue à celui ci-dessus, en remplaçant $\mathbf{R}^n$ par X, $\mathbf{R}^m$ par Y et $\mathbf{R}^{n+m}$ par $\mathrm{X} \times \mathrm{Y}$. Il se déduit de celui sur $\mathbf{R}^{n+m}$ en écrivant une intégrale sur $\mathrm{X} \times \mathrm{Y}$ sous la forme $\int_{\mathbf{R}^{n+m}} \mathbf{1}_{\mathrm{X}\times\mathrm{Y}}\phi$.

(ii) Dans la pratique, on commence par utiliser le (ii) pour vérifier que $|f|$ est sommable, avant d'utiliser le (i) pour calculer des intégrales, intervertir les variables...

(iii) Le (i) s'utilise aussi comme un théorème de semi-existence : il affirme que si $f(x,y)$ est sommable, alors $\int f(x,y)\, dx$ converge pour presque tout y, et $\int f(x,y)\, dy$ converge pour presque tout x ; par contre on ne peut en déduire la convergence de ces intégrales pour aucun x ou y particulier.

Démonstration. — Soit $(f_k)_{k\in\mathbf{N}}$ une suite d'éléments de $\mathrm{Esc}(\mathbf{R}^{n+m})$, tendant vers f dans $\mathscr{L}^1(\mathbf{R}^{n+m})$, et telle que $\sum_{k\in\mathbf{N}} \|f_{k+1} - f_k\|_1 < +\infty$. Il résulte du lemme III.3.1 que la série $\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^n}(f_{k+1} - f_k)$ est à termes dans $\mathrm{Esc}(\mathbf{R}^m)$, converge normalement dans $\mathscr{L}^1(\mathbf{R}^m)$, et que, si on note $g \in \mathscr{L}^1(\mathbf{R}^m)$, la limite, alors $\int_{\mathbf{R}^m} g = \int_{\mathbf{R}^{n+m}} f$. Le problème est donc de montrer que, pour y en dehors d'un ensemble B de mesure nulle, la fonction $x \mapsto f(x,y)$ appartient à $\mathscr{L}^1(\mathbf{R}^n)$, et $g(y) = \int_{\mathbf{R}^n} f(x,y)\, dx$. Nous aurons besoin du lemme suivant.

Lemme III.3.5. — *Si* $\mathrm{A} \subset \mathbf{R}^{n+m}$ *est de mesure nulle, alors les ensembles* A_1 *et* A_2 *définis par*

$$\mathrm{A}_1 = \{x \in \mathbf{R}^n,\ \mathrm{A} \cap (\{x\} \times \mathbf{R}^m) \text{ n'est pas de mesure nulle,}\}$$
$$\mathrm{A}_2 = \{y \in \mathbf{R}^m,\ \mathrm{A} \cap (\mathbf{R}^n \times \{y\}) \text{ n'est pas de mesure nulle,}\}$$

sont de mesure nulle dans $\mathbf{R}^n$ *et* $\mathbf{R}^m$ *respectivement.*

Démonstration. — Par symétrie (entre n et m), il suffit de le prouver pour A_1. Soit $\varepsilon > 0$. Comme A est de mesure nulle, on peut trouver une suite $(\mathrm{D}_k)_{k\in\mathbf{N}}$ de dalles de $\mathbf{R}^n$, et une suite $(\mathrm{E}_k)_{k\in\mathbf{N}}$ de dalles de $\mathbf{R}^m$, telles que $\mathrm{A} \subset \cup_{k\in\mathbf{N}} \mathrm{D}_k \times \mathrm{E}_k$, et $\sum_{k\in\mathbf{N}} \lambda(\mathrm{D}_k)\lambda(\mathrm{E}_k) \leqslant \varepsilon$. Si $r \in \mathbf{N}$ et $j \in \mathbf{N}$, soit $\mathrm{B}_{\varepsilon,r,j}$ l'ensemble des $x \in \mathbf{R}^n$ tels que $\sum_{k\leqslant j,\, x\in\mathrm{D}_k} \lambda(\mathrm{E}_k) > 2^{-r}$; c'est un dallage de $\mathbf{R}^n$, et on a $2^{-r}\lambda(\mathrm{B}_{\varepsilon,r,j}) \leqslant \sum_{k\leqslant j} \lambda(\mathrm{D}_k)\lambda(\mathrm{E}_k) \leqslant \varepsilon$. De plus, la suite des $(\mathrm{B}_{\varepsilon,r,j})_{j\in\mathbf{N}}$ est une suite croissante de dallages finis, et donc $\lambda^+(\cup_{j\in\mathbf{N}} \mathrm{B}_{\varepsilon,r,j}) = \lim_{j\to+\infty} \lambda(\mathrm{B}_{\varepsilon,r,j}) \leqslant 2^r\varepsilon$. Or l'ensemble B_r des $x \in \mathbf{R}^n$ tel que $\lambda^+(\mathrm{A} \cap (\{x\} \times \mathbf{R}^m)) >$

2^{-r} est inclus dans $\cup_{j\in\mathbf{N}} \mathrm{B}_{\varepsilon,r,j}$, quel que soit $\varepsilon > 0$; c'est donc un ensemble de mesure nulle puisque de mesure extérieure $\leqslant 2^r\varepsilon$ quel que soit $\varepsilon > 0$. Enfin, $\mathrm{A}_1 = \cup_{r\in\mathbf{N}} \mathrm{B}_r$ est de mesure nulle, en tant que réunion dénombrable d'ensembles de mesures nulles.

Revenons à la démonstration du théorème de Fubini. Comme $\sum_{k\in\mathbf{N}} \|f_{k+1} - f_k\|_1 < +\infty$, il résulte du th. III.2.1, que la série $\sum_{k\in\mathbf{N}} f_{k+1}(x,y) - f_k(x,y)$ converge absolument vers $f(x,y)$ pour tout (x,y) en dehors d'un ensemble de mesure nulle A. Par ailleurs, d'après le lemme III.3.5, il existe un sous-ensemble de mesure nulle B_1 de $\mathbf{R}^m$ tel que, si $y \notin \mathrm{B}_1$, alors $\mathrm{A}\cap(\mathbf{R}^n \times \{y\})$ est de mesure nulle dans $\mathbf{R}^n$. Si $y \notin \mathrm{B}_1$, on a donc $f_k(x,y) \to f(x,y)$ pour x en dehors d'un ensemble de mesure nulle.

De même, comme $\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^n} (f_{k+1} - f_k)\,dx$ converge normalement dans $\mathscr{L}^1(\mathbf{R}^m)$ vers g, il existe $\mathrm{B}_2 \subset \mathbf{R}^m$ tel que, si $y \notin \mathrm{B}_2$, alors $\int_{\mathbf{R}^n} f_k(x,y)\,dx \to g(y)$.

Maintenant, en appliquant Fubini pour les fonctions en escalier à $u_k = |f_{k+1} - f_k|$, puis deux fois de suite le théorème de convergence monotone, on obtient :

$$\begin{aligned}\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^{n+m}} |u_k(x,y)|\,dx\,dy &= \sum_{k\in\mathbf{N}} \int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} |u_k(x,y)|\,dx\Big)\,dy \\ &= \int_{\mathbf{R}^m} \Big(\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^n} |u_k(x,y)|\,dx\Big)\,dy \\ &= \int_{\mathbf{R}^m} \Big(\int_{\mathbf{R}^n} \sum_{k\in\mathbf{N}} |u_k(x,y)|\,dx\Big)\,dy.\end{aligned}$$

Comme on a fait l'hypothèse que $\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^{n+m}} |u_k(x,y)|\,dx\,dy < +\infty$, l'ensemble B_3 des $y \in \mathbf{R}^m$ tels que $\int_{\mathbf{R}^n} \sum_{k\in\mathbf{N}} |u_k(x,y)|\,dx = +\infty$ est de mesure nulle. Si $y \notin \mathrm{B}_3$, la fonction $h_y(x) = \sum_{k\in\mathbf{N}} |u_k(x,y)|$ est donc sommable, et comme $f_k = \sum_{j=0}^{k-1} u_k$, on a $|f_k(x,y)| \leqslant h_y(x)$ quel que soit $k \in \mathbf{N}$.

Si $\mathrm{B} = \mathrm{B}_1 \cup \mathrm{B}_2 \cup \mathrm{B}_3$, et si $y \notin \mathrm{B}$, on est dans les conditions d'application du théorème de convergence dominée, et donc

$$g(y) = \lim_{k\to+\infty} \int_{\mathbf{R}^n} f_k(x,y)\,dx = \int_{\mathbf{R}^n} \big(\lim_{k\to+\infty} f_k(x,y)\big)\,dx = \int_{\mathbf{R}^n} f(x,y)\,dx.$$

Ceci permet de terminer la démonstration du (i).

Le (ii) est une conséquence du (i) sauf si $\int_{\mathbf{R}^{n+m}} f(x,y)\ dx\,dy = +\infty$. Mais, dans ce cas, il suffit de prendre une suite $(f_k)_{k\in\mathbf{N}}$ d'éléments de $\mathscr{L}^1(\mathbf{R}^{n+m})$ tendant vers f en croissant, de constater que les trois membres de l'identité dépendent de manière croissante de f, et d'utiliser le théorème de convergence monotone pour montrer que $\lim_{k\to+\infty} \int_{\mathbf{R}^{n+m}} f_k(x,y)\ dx\,dy = +\infty$, et en déduire que les trois membres sont égaux à $+\infty$. Ceci permet de conclure.

Exercice III.3.6. — Soit $f : \mathbf{R}_+ \times \mathbf{R}_+ \to \mathbf{R}$ définie par $f(x,y) = e^{x-y}$ si $x \leqslant y$, et $f(x,y) = -e^{y-x}$, si $y < x$. Calculer

$$\int_0^{+\infty} \Big(\int_0^{+\infty} f(x,y)\,dx\Big)\,dy \quad \text{et} \quad \int_0^{+\infty} \Big(\int_0^{+\infty} f(x,y)\,dy\Big)\,dx.$$

Peut-on en déduire que $-1 = 1$?

Exercice III.3.7. — (i) Soit $\mathrm{P} \in \mathbf{R}[\mathrm{X},\mathrm{Y}]$ non nul. Montrer que $\mathrm{X} = \{(x,y) \in \mathbf{R}^2,\ \mathrm{P}(x,y) = 0\}$ est de mesure nulle dans $\mathbf{R}^2$. (On pourra s'intéresser à $\int_{\mathbf{R}^2} \mathbf{1}_{\mathrm{X}}$.)

(ii) Soit $\mathrm{P} \in \mathbf{R}[\mathrm{X}_1,\ldots,\mathrm{X}_m]$ non nul. Montrer que $\{x \in \mathbf{R}^m,\ \mathrm{P}(x) = 0\}$ est de mesure nulle dans $\mathbf{R}^m$.

2. La formule du changement de variable

Théorème III.3.8. — (invariance par translation de la mesure de Lebesgue)
Si $v \in \mathbf{R}^m$, et si $\phi : \mathbf{R}^m \to \mathbf{C}$ est mesurable, alors $x \mapsto \phi(x+v)$ est mesurable, et on a

$$\int |\phi(x+v)|\,dx = \int |\phi(x)|\,dx \quad \textit{et, si } \phi \textit{ est sommable, } \int \phi(x+v)\,dx = \int \phi(x)\,dx.$$

Démonstration. — Notons T_v l'application $\phi \mapsto \mathrm{T}_v(\phi)$, définie par $(\mathrm{T}_v(\phi))(x) = \phi(x+v)$. Si D est une dalle, et si les coordonnées de v sont des nombres dyadiques, alors $\mathrm{D} - v = \{x - v,\ x \in \mathrm{D}\}$ est encore une dalle, et on a $\mathrm{T}_v(\mathbf{1}_\mathrm{D}) = \mathbf{1}_{\mathrm{D}-v}$; on en déduit, en découpant D et $\mathrm{D}-v$ en dalles élémentaires de même taille, que $\int \mathrm{T}_v(\mathbf{1}_\mathrm{D}) = \int \mathbf{1}_\mathrm{D}$. Dans le cas général, on prend une suite $(v_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{R}^m$ à coordonnées dyadiques tendant vers le vecteur v de la translation : la suite des $\mathbf{1}_{\mathrm{D}-v_n}$ tend simplement vers $\mathbf{1}_{\mathrm{D}-v}$ en dehors des faces, mais celles-ci sont de mesure nulle ((ii) de l'ex. III.1.6, par exemple), ce qui montre que $\mathbf{1}_{\mathrm{D}-v}$ est mesurable en tant que limite simple p.p. de fonctions mesurables, et permet d'utiliser le théorème de convergence dominée pour en déduire que $\int \mathrm{T}_v(\mathbf{1}_\mathrm{D}) = \int \mathbf{1}_\mathrm{D}$.

Par linéarité, on en déduit que $\mathrm{T}_v(\phi)$ est mesurable et $\int \mathrm{T}_v(\phi) = \int \phi$, si $\phi \in \mathrm{Esc}(\mathbf{R}^m)$. Le théorème s'en déduit en utilisant la densité de $\mathrm{Esc}(\mathbf{R}^m)$ dans $\mathrm{L}^1(\mathbf{R}^m)$ (et le théorème de convergence monotone pour traiter le cas $\int |\phi| = +\infty$).

Soit Ω un ouvert de $\mathbf{R}^m$, et soit $\varphi : \Omega \to \varphi(\Omega)$ un *difféomorphisme* de Ω sur un ouvert $\varphi(\Omega)$ de $\mathbf{R}^m$, c'est-à-dire une application bijective de classe $\mathscr{C}^1$ dont l'inverse est aussi de classe $\mathscr{C}^1$. L'application φ s'écrit, en coordonnées

$$\varphi(x) = \big(\varphi_1(x_1,\dots,x_m),\dots,\varphi_m(x_1,\dots,x_m)\big),$$

et la condition « φ est de classe $\mathscr{C}^1$ » se traduit par le fait que les dérivées partielles $\frac{\partial \varphi_i}{\partial x_j}$ sont continues sur Ω. On note $\mathrm{Jac}_\varphi(x) = (\frac{\partial \varphi_i}{\partial x_j}(x))_{1\leqslant i,j\leqslant m}$ la *matrice jacobienne* de f au point x. On définit le *jacobien* $\mathrm{J}_\varphi(x)$ de φ au point x comme le déterminant de $\mathrm{Jac}_\varphi(x)$; le fait que φ soit un difféomorphisme implique que $\mathrm{Jac}_\varphi(x)$ est inversible, et donc que $\mathrm{J}_\varphi(x) \neq 0$, pour tout $x \in \Omega$.

Théorème III.3.9. — *Si f est une fonction mesurable sur $\varphi(\Omega)$, alors f est sommable si et seulement si la fonction $x \mapsto f(\varphi(x)) \cdot \mathrm{J}_\varphi(x)$ est sommable sur Ω, et on a*

$$\int_{\varphi(\Omega)} f(y)\,dy = \int_\Omega f(\varphi(x)) \cdot |\mathrm{J}_\varphi(x)|\,dx.$$

Remarque III.3.10. — (i) En dimension 1, la matrice jacobienne de φ n'est autre que la dérivée φ' de φ, et on tombe sur la formule $\int_{\varphi(]a,b[)} f(y)\,dy = \int_{]a,b[} f(\varphi(x))|\varphi'(x)|\,dx$. Comme φ' ne s'annule pas sur $]a,b[$, il y a deux cas : soit $\varphi' > 0$ sur $]a,b[$ et alors $\varphi(]a,b[) =]\varphi(a),\varphi(b)[$, soit $\varphi' < 0$ sur $]a,b[$ et $\varphi(]a,b[) =]\varphi(b),\varphi(a)[$. Dans le premier cas, la formule devient $\int_{\varphi(a)}^{\varphi(b)} f(y)\,dy = \int_a^b f(\varphi(x))\varphi'(x)\,dx$, et dans le second, elle devient

$-\int_{\varphi(a)}^{\varphi(b)} f(y)\,dy = -\int_a^b f(\varphi(x))\varphi'(x)\,dx$; on retombe donc bien, dans les deux cas, sur la formule classique.

(ii) Une manière très pratique d'écrire la formule du changement de variable est d'expliciter formellement les éléments de volume dx et dy sous la forme $dx = |dx_1 \wedge \cdots \wedge dx_m|$ et $dy = |dy_1 \wedge \cdots \wedge dy_m|$. Comme $y_i = \varphi_i(x)$, on a $dy_i = \sum_{j=1}^m \frac{\partial \varphi_i}{\partial x_j}(x)\,dx_j$. Comme $\wedge$ est multilinéaire alternée, on a $\wedge_{i=1}^m \big(\sum_{j=1}^m a_{i,j}\,dx_j\big) = \det(a_{i,j}) \wedge_{j=1}^m dx_j$ (c'est une des manières de définir le déterminant de m vecteurs), ce qui nous donne

$$dy = \big|\wedge_{i=1}^m \big(\sum_{j=1}^m \frac{\partial \varphi_i}{\partial x_j}(x)\,dx_j\big)\big| = \big|\mathrm{J}_\varphi(x)\,dx_1 \wedge \cdots \wedge dx_m\big| = |\mathrm{J}_\varphi(x)|\,dx.$$

Démonstration. — Commençons par regarder ce qui se passe dans le cas $\Omega = \mathbf{R}^m$ et φ affine (i.e. de la forme $x \mapsto \mathrm{A}\cdot x + b$, avec $\mathrm{A} \in \mathbf{GL}_m(\mathbf{R})$, et $b \in \mathbf{R}^m$). Dans ce cas, la matrice jacobienne de φ est constante égale à A ; on a donc $\mathrm{J}_\varphi(x) = |\det \mathrm{A}|$ pour tout x.

Par ailleurs, si $r \in \mathbf{N}$ et si $\mathbf{k} \in \mathbf{Z}^m$, alors $\varphi(\mathrm{D}_{r,\mathbf{k}})$ est un translaté de $\varphi(\mathrm{D}_{r,\mathbf{0}})$ et donc a même volume. On en déduit l'existence de $\mathrm{C}(\mathrm{A}) \in \mathbf{R}_+^*$ tel que $\lambda(\varphi(\mathrm{D}_{r,\mathbf{k}})) = 2^{-r}\mathrm{C}(\mathrm{A})$, quels que soient $r \in \mathbf{N}$ et $\mathbf{k} \in \mathbf{Z}^m$. Par linéarité on a $\int_{\mathbf{R}^m} \phi(x)\,dx = \mathrm{C}(\mathrm{A}) \int_{\mathbf{R}^m} \phi(\mathrm{A}\cdot x + b)\,dx$, quel que soit $\phi \in \mathrm{Esc}(\mathbf{R}^m)$. Par continuité, cette égalité s'étend à $\mathrm{L}^1(\mathbf{R}^m)$. Pour conclure dans le cas affine, il reste à vérifier que $\mathrm{C}(\mathrm{A}) = |\det \mathrm{A}|$, ce qui constitue l'interprétation géométrique du déterminant [22], et fait l'objet de l'exercice III.3.11 ci-dessous.

On démontre le cas général en utilisant le fait que, plus on regarde de près autour d'un point x, plus φ ressemble à l'application affine $h \mapsto \varphi(x) + \mathrm{Jac}_\varphi(x)\cdot h$, et donc que quand r tend vers $+\infty$, l'image de $x + \mathrm{D}_{r,\mathbf{0}}$ ressemble de plus en plus au parallèlépipède $\varphi(x) + \mathrm{Jac}_\varphi(x)\cdot \mathrm{D}_{r,\mathbf{0}}$, dont le volume est $|\mathrm{J}_\varphi(x)|\lambda(\mathrm{D}_{r,\mathbf{0}})$.

De manière plus précise, on démontre, en utilisant la continuité uniforme de $x \mapsto \mathrm{Jac}_\varphi(x)$ (et de $x \mapsto \mathrm{Jac}_{\varphi^{-1}}(x)$), que si $\mathrm{K} \subset \Omega$ est compact, il existe une suite de fonctions $\varepsilon_{\mathrm{K},r} : \mathrm{K} \to \mathbf{R}_+$, pour r assez grand, tendant uniformément vers 0 sur K, telle que, quel que soit $x \in \mathrm{K}$, on ait

$$\varphi(x) + (1-\varepsilon_{\mathrm{K},r}(x))\mathrm{Jac}_\varphi(x)\cdot \mathrm{D}_{r,\mathbf{0}} \subset \varphi(x + \mathrm{D}_{r,\mathbf{0}}) \subset \varphi(x) + (1+\varepsilon_{\mathrm{K},r}(x))\mathrm{Jac}_\varphi(x)\cdot \mathrm{D}_{r,\mathbf{0}}.$$

On en déduit l'existence de $\varepsilon'_{\mathrm{K},r}$, tendant uniformément vers 0 sur K, telle que, quel que soit $x \in \mathrm{K}$, on ait $\lambda(\varphi(x + \mathrm{D}_{r,\mathbf{0}})) = (1+\varepsilon'_{\mathrm{K},r}(x))|\mathrm{J}_\varphi(x)|\lambda(x + \mathrm{D}_{r,\mathbf{0}})$. Maintenant, on peut écrire Ω comme une réunion croissante de dallages D_n dont l'adhérence est contenue dans Ω, et il suffit de prouver que la formule du théorème est valable pour une fonction en escalier f à support dans un des D_n, car ces fonctions forment un sous-espace dense dans $\mathscr{L}^1(\Omega)$. Par linéarité, on est ramené à prouver que $\lambda(\varphi(\mathrm{D})) = \int_{\mathrm{D}} |\mathrm{J}_\varphi(x)|\,dx$, si D est une dalle élémentaire dont l'adhérence K est incluse dans Ω. Si r est assez grand, D est la réunion disjointe des $\mathrm{D}_{r,\mathbf{k}}$ contenues dans D, et comme $\mathrm{D}_{r,\mathbf{k}} = \frac{\mathbf{k}}{2^r} + \mathrm{D}_{r,\mathbf{0}}$, on tire de la discussion ci-dessus l'identité

$$\lambda(\varphi(\mathrm{D})) = \sum_{\mathrm{D}_{r,\mathbf{k}} \subset \mathrm{D}} \lambda(\varphi(\frac{\mathbf{k}}{2^r} + \mathrm{D}_{r,\mathbf{0}})) = \sum_{\mathrm{D}_{r,\mathbf{k}} \subset \mathrm{D}} (1+\varepsilon'_{\mathrm{K},r}(\frac{\mathbf{k}}{2^r}))|\mathrm{J}_\varphi(\frac{\mathbf{k}}{2^r})|\lambda(\mathrm{D}_{r,\mathbf{k}}) = \int_{\mathrm{D}} \phi_r(x)\,dx,$$

où ϕ_r est la fonction en escalier sur D valant $(1+\varepsilon'_{\mathrm{K},r}(\frac{\mathbf{k}}{2^r}))|\mathrm{J}_\varphi(\frac{\mathbf{k}}{2^r})|$, sur $\mathrm{D}_{r,\mathbf{k}}$. Comme $\varepsilon'_{\mathrm{K},r}$, tend uniformément vers 0 sur K, ϕ_r tend uniformément vers $|\mathrm{J}_\varphi(x)|$ sur D. On en déduit le résultat.

22. Le volume du parallèlépipède supporté par des vecteurs $v_1, \ldots, v_m$ de $\mathbf{R}^m$ est égal à la valeur absolue du déterminant de ces vecteurs.

Exercice III.3.11. — (i) Prouver que $C(AB) = C(A)C(B)$, quels que soient $A, B \in \mathbf{GL}_m(\mathbf{R})$.

(ii) Montrer que $C(A) = |\det A|$ si A est une matrice diagonale ou une matrice de permutation (i.e. si $x \mapsto A \cdot x$ induit une permutation des vecteurs de la base canonique de $\mathbf{R}^m$).

(iii) Montrer que toute matrice unipotente supérieure ou inférieure (i.e. triangulaire avec des 1 sur la diagonale) peut s'écrire sous la forme $DUD^{-1}U^{-1}$, avec D diagonale, et U unipotente supérieure ou inférieure. En déduire que $C(A) = 1$ si U est unipotente inférieure ou supérieure.

(iv) En utilisant la méthode du pivot, montrer que $\mathbf{GL}_m(\mathbf{R})$ est engendré par les matrices diagonales, les unipotentes inférieures et supérieures et les matrices de permutation.

(v) En déduire que $C(A) = |\det A|$ quel que soit $A \in \mathbf{GL}_m(\mathbf{R})$.

3. L'intégrale de la gaussienne

Nous allons utiliser les résultats des deux précédents n$^{\text{os}}$ pour établir les formules

$$\int_{-\infty}^{+\infty} e^{-x^2} dx = \sqrt{\pi} \quad \text{et} \quad \int_{-\infty}^{+\infty} e^{-\pi x^2} dx = 1.$$

On passe de la première à la seconde par le changement de variable $x = \sqrt{\pi}\, u$; il suffit donc de démontrer la première formule. Pour cela, notons $I = \int_{-\infty}^{+\infty} e^{-x^2} dx$ l'intégrale à calculer, et posons $I_0 = \int_{\mathbf{R}^2} e^{-(x^2+y^2)}\, dx\, dy$.

• $e^{-(x^2+y^2)} = e^{-x^2} e^{-y^2}$ et, d'après le théorème de Fubini pour les fonctions positives,

$$I_0 = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-x^2} e^{-y^2} dx \Big)\, dy = \int_{\mathbf{R}} I\, e^{-y^2}\, dy = I^2.$$

• Soit Δ la demi-droite $]-\infty, 0] \times \{0\}$, et soit $\Omega' = \mathbf{R}^2 - \Delta$. Comme Δ est de mesure nulle, on a aussi $I_0 = \int_{\Omega'} e^{-(x^2+y^2)}\, dx\, dy$.

• Soit $\Omega = \mathbf{R}_+^* \times]-\pi, \pi[$. Alors φ défini par $\varphi(r, \theta) = (r\cos\theta, r\sin\theta)$ est un difféomorphisme de Ω sur Ω', et comme $dx = \cos\theta\, dr - r\sin\theta\, d\theta$ et $dy = \sin\theta\, dr + r\cos\theta\, d\theta$, la matrice jacobienne de φ est $\left(\begin{smallmatrix} \cos\theta & -r\sin\theta \\ \sin\theta & r\cos\theta \end{smallmatrix}\right)$, et son jacobien est $J_\varphi(r, \theta) = r\cos^2\theta + r\sin^2\theta = r$. La formule du changement de variable appliquée à $f(x, y) = e^{-(x^2+y^2)}$ nous donne :

$$I_0 = \int_\Omega e^{-(r^2\cos^2\theta + r^2\sin^2\theta)} |J_\varphi(r, \theta)|\, dr\, d\theta = \int_\Omega e^{-r^2} r\, dr\, d\theta.$$

• On utilise de nouveau le théorème de Fubini pour les fonctions positives :

$$I_0 = \int_{\mathbf{R}_+^* \times]-\pi, \pi[} e^{-r^2} r\, dr\, d\theta = \int_0^{+\infty} \Big(\int_{-\pi}^{\pi} e^{-r^2} r\, d\theta \Big)\, dr = 2\pi \int_0^{+\infty} e^{-r^2} r\, dr.$$

• Enfin, le changement de variable $r^2 = u$, et donc $r\, dr = \frac{1}{2} du$, nous donne :

$$I_0 = \pi \int_0^{+\infty} e^{-u}\, du = \pi [-e^{-u}]_0^{+\infty} = \pi.$$

Comme $I_0 = I^2$, cela permet de conclure.

4. Exercices

Exercice III.3.12. — (Convolution de deux fonctions sommables) Soient $f, g \in \mathscr{L}^1(\mathbf{R}^m)$.

(i) Montrer que $\int\int |f(x-y)g(y)| = \|f\|_1 \|g\|_1$.

(ii) En déduire que, pour presque tout x la fonction $y \mapsto f(x-y)g(y)$ est sommable et que $f*g$ définie p.p. par $f*g(x) = \int f(x-y)g(y)\,dy$ est elle-aussi sommable.

(iii) Montrer que, si $f_1 = f_2$ p.p. et $g_1 = g_2$ p.p., alors $f_1 * g_1 = f_2 * g_2$ p.p. (L'application $(f,g) \mapsto f*g$ passe donc au quotient et définit une application encore notée $(f,g) \mapsto f*g$ de $\mathrm{L}^1(\mathbf{R}^m) \times \mathrm{L}^1(\mathbf{R}^m)$ dans $\mathrm{L}^1(\mathbf{R}^m)$.)

(iv) Montrer que $(f,g) \mapsto f*g$ induit une application bilinéaire continue de $\mathrm{L}^1(\mathbf{R}^m) \times \mathrm{L}^1(\mathbf{R}^m)$ dans $\mathrm{L}^1(\mathbf{R}^m)$, et que l'on a $f*g = g*f$ et $f*(g*h) = (f*g)*h$, si $f, g, h \in \mathrm{L}^1(\mathbf{R}^m)$.

Exercice III.3.13. — Soit ϕ une fonction $\mathscr{C}^\infty$ sur $\mathbf{R}^m$, à support dans $[-1,1]^m$, à valeurs dans $\mathbf{R}_+$, et vérifiant $\int_{\mathbf{R}^m} \phi = 1$. Si $\varepsilon > 0$, soit ϕ_ε définie par $\phi_\varepsilon(x) = \varepsilon^{-m}\phi(\frac{x}{\varepsilon})$.

(i) Montrer que $\int_{\mathbf{R}^m} \phi_\varepsilon = 1$, et que ϕ_ε est à support dans $[-\varepsilon,\varepsilon]^m$.

(ii) Montrer que, si f est une fonction en escalier, alors $f * \phi_\varepsilon \to f$ p.p, quand $\varepsilon \to 0$.

(iii) Montrer que, si f est une fonction en escalier, alors $f * \phi_\varepsilon \to f$ dans $\mathrm{L}^1(\mathbf{R}^m)$, quand $\varepsilon \to 0$.

(iv) Montrer que, si $f \in \mathrm{L}^1(\mathbf{R}^m)$, alors $f * \phi_\varepsilon \to f$ dans $\mathrm{L}^1(\mathbf{R}^m)$, quand $\varepsilon \to 0$.

(v) Montrer que, si $f \in \mathrm{L}^1(\mathbf{R}^m) + \mathrm{L}^2(\mathbf{R}^m)$ vérifie $\int_{\mathbf{R}^m} \phi f = 0$, pour tout $\phi \in \mathscr{C}_c^\infty(\mathbf{R}^m)$, alors $f = 0$ p.p.

Exercice III.3.14. — Soient $f, g \in \mathrm{L}^2(\mathbf{R}^n)$.

(i) Montrer que $\|f*g\|_\infty \leqslant \|f\|_2 \, \|g\|_2$.

(ii) Montrer que $f*g$ est continue et tend vers 0 à l'infini. (Commencer par des fonctions en escalier.)

(iii) Montrer que si A et B sont deux sous-ensembles de $\mathbf{R}^n$ de mesure strictement positive, alors l'ensemble $\mathrm{A} + \mathrm{B}$ des $a+b$, pour $a \in \mathrm{A}$ et $b \in \mathrm{B}$, contient un ouvert.

(iv) Un fermé d'intérieur vide est-il forcément de mesure nulle ?

Exercice III.3.15. — (i) Établir la formule $\int_0^1 \int_0^1 \frac{dx\,dy}{1-x^2y^2} = \frac{3}{4}\zeta(2)$.

(ii) Soient $\Omega_1 = \{(u,v),\ u>0,\ v>0,\ u+v<\frac{\pi}{2}\}$ et $\Omega_2 = \{(x,y),\ 0<x,y<1\}$. Montrer que φ défini par $\varphi(u,v) = \left(\frac{\sin u}{\cos v}, \frac{\sin v}{\cos u}\right)$ induit un difféomorphisme de Ω_1 sur Ω_2.

(iii) En déduire la formule $\zeta(2) = \frac{\pi^2}{6}$.

Exercice III.3.16. — Soit $\mathrm{N} \in \mathbf{N} - \{0\}$, et soit $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$ l'application déduite de $z \mapsto z^\mathrm{N}$ de $\mathbf{C}$ dans $\mathbf{C}$, en identifiant $\mathbf{R}^2$ à $\mathbf{C}$. On rappelle par anticipation (cf. (i) de la rem. V.3.1) que le jacobien de φ en $z_0 \in \mathbf{C}$ est $|\mathrm{N} z_0^{\mathrm{N}-1}|^2$. Montrer que, si f est sommable sur $\mathbf{R}^2$, alors

$$\int_{\mathbf{R}^2} f(u,v)\,du\,dv = \mathrm{N} \int_{\mathbf{R}^2} f(\varphi(x,y))(x^2+y^2)^{\mathrm{N}-1}\,dx\,dy.$$

Exercice III.3.17. — (Volume [23] de la boule unité de $\mathbf{R}^m$)

Soit $m \geqslant 1$. On munit $\mathbf{R}^m$ de la norme euclidienne standard $\|\ \|$. Si $\rho \in \mathbf{R}_+$, soit $\mathrm{B}(\rho)$ la boule unité fermée de centre 0 et de rayon ρ. On note C_m le volume de $\mathrm{B}(1)$.

(i) Montrer que $\lambda(\mathrm{B}(\rho)) = \mathrm{C}_m \rho^m$, si $\rho \in \mathbf{R}_+$.

(ii) Soit $\phi_r = \sum_{k=1}^{2^r} (\frac{k}{2^r})^{1-m} \mathbf{1}_{\mathrm{B}(\frac{k}{2^r}) - \mathrm{B}(\frac{k-1}{2^r})}$. Montrer que $\int_{\mathbf{R}^m} \phi_r \to \int_{\mathrm{B}(1)} \|x\|^{1-m}\,dx$.

(iii) En déduire que $\int_{\mathrm{B}(1)} \|x\|^{1-m}\,dx = m\mathrm{C}_m$.

(iv) Montrer que, si $\phi \in \mathrm{Esc}(\mathbf{R}_+)$, alors $m\mathrm{C}_m \int_{\mathbf{R}_+} \phi(t)\,dt = \int_{\mathbf{R}^m} \|x\|^{1-m}\phi(\|x\|)\,dx$. En déduire que $\phi \in \mathrm{L}^1(\mathbf{R}_+)$ si et seulement si $\|x\|^{1-m}\phi(\|x\|) \in \mathrm{L}^1(\mathbf{R}^m)$, et que $m\mathrm{C}_m \int_{\mathbf{R}_+} \phi(t)\,dt = \int_{\mathbf{R}^m} \|x\|^{1-m}\phi(\|x\|)\,dx$, quel que soit $\phi \in \mathrm{L}^1(\mathbf{R}_+)$.

23. Pour $n = 3$, le résultat était connu du mathématicien indien Bhaskaracarya, vers 1150.

(v) Soit $s \in \mathbf{R}$. Montrer que $\int_{\|x\|\leqslant 1} \|x\|^s < +\infty$ si et seulement si $s > -m$ et que $\int_{\|x\|\geqslant 1} \|x\|^s < +\infty$ si et seulement si $s < -m$.

(vi) En appliquant ce qui précède à la fonction $t^{m-1}e^{-\pi t^2}$, et en utilisant la définition de $\pi = \mathrm{C}_2$, en déduire la valeur de $\int_{\mathbf{R}} e^{-\pi x^2}\, dx$, et montrer que $\mathrm{C}_m = \frac{\pi^{m/2}}{\Gamma(1+\frac{m}{2})}$.

III.4. Construction de l'intégrale de Lebesgue

Ce § est consacré à la démonstration des th. III.1.18 et III.1.23 et de la prop. III.1.12 sur lesquels repose toute la théorie. Commençons par remarquer que l'unicité n'a pas été utilisée pour déduire le théorème de convergence dominée du th. III.1.18. On en déduit que, si on peut définir l'intégrale, alors le résultat suivant doit être vrai.

Proposition III.4.1. — *Soient* D *un dallage et* $\mathrm{M} > 0$. *Soit* $h \in \mathrm{Mes}(\mathrm{D}, [0, \mathrm{M}])$ *et soit* $(h_n)_{n\in\mathbf{N}}$ *une suite d'éléments de* $\mathrm{Esc}(\mathrm{D}, [0, \mathrm{M}])$ *tendant vers* h *p.p. Alors* $\int h_n$ *a une limite qui ne dépend que de* h.

De plus, si ce résultat est vrai, les théorèmes de convergence dominée et de convergence monotone montrent que l'on doit définir l'intégrale de Lebesgue [24] de la manière suivante.

(L1) Si $f \in \mathrm{Mes}(\mathrm{D}, [0, \mathrm{M}])$, alors $\int f \in \mathbf{R}_+$ est la limite, quand $n \to +\infty$, de $\int f_n$, où $(f_n)_{n\in\mathbf{N}}$ est n'importe quelle suite d'éléments de $\mathrm{Esc}(\mathrm{D}, [0, \mathrm{M}])$ qui converge vers f p.p.

(L2) Si $f \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$, alors $\int f \in \overline{\mathbf{R}}_+$ est la limite, quand $\mathrm{N} \to +\infty$, de la suite croissante de terme général $\int_{\mathrm{D}_\mathrm{N}} \inf(f, \mathrm{N})$, où D_N est la dalle de sommets $(\pm\mathrm{N}, \ldots, \pm\mathrm{N})$.

On en déduit l'unicité d'une application $f \mapsto \int f$ satisfaisant aux conclusions du th. III.1.18. On est donc ramené à démontrer la prop. III.4.1, et à vérifier les th. III.1.18 et III.1.23 pour l'intégrale définie par les propriétés (L1) et (L2). La démonstration se fait en plusieurs étapes, la plus délicate étant la démonstration de la prop. III.4.1.

1. Le théorème de convergence dominée pour les fonctions en escalier bornées

Ce n° est consacré à la démonstration de la prop. III.4.1 sous la forme renforcée ci-dessous.

Dans tout ce qui suit, D est un dallage de $\mathbf{R}^m$, et $\mathrm{M} \in \mathbf{R}_+$.

---

24. La présentation choisie dans ce texte fait ressembler beaucoup l'intégrale de Lebesgue à celle de Riemann : on part des fonctions en escalier, on définit l'intégrale d'une fonction mesurable par passage à la limite, et enfin on définit la notion d'ensemble mesurable et de mesure d'un ensemble. L'approche originelle de Lebesgue était inverse. Son point de départ était le suivant : pour calculer l'aire d'une surface sous le graphe d'une fonction d'un intervalle $[a, b]$ dans $\mathbf{R}_+$, on peut soit découper verticalement (ce que fait Riemann), soit horizontalement (ce que fait Lebesgue). Comme le dit Lebesgue, pour calculer la quantité d'argent dans un tas contenant des pièces de différentes valeurs, l'intégrale de Riemann consiste à prendre chaque pièce à son tour et à ajouter sa valeur au total, alors que l'intégrale de Lebesgue consiste à commencer par trier les pièces et compter combien il y en a de chaque sorte. Évidemment, en découpant horizontalement, on tombe sur des ensembles nettement plus compliqués que verticalement comme un petit dessin le prouvera aisément. L'approche originelle de Lebesgue a l'avantage de s'étendre telle quelle à une théorie de la mesure valable dans un cadre très général (et indispensable en théorie des probabilités). Celle suivie dans ce texte permet d'éviter certains aspects un peu rébarbatifs de théorie des ensembles. Elle a l'inconvénient d'être limitée à des espaces ressemblant (au moins localement) à $\mathbf{R}^n$.

Proposition III.4.2. — *Soit* $h \in \mathrm{Mes}(\mathrm{D},[0,\mathrm{M}])$ *et soit* $(h_n)_{n\in\mathbf{N}}$ *une suite d'éléments de* $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$ *tendant vers* h *p.p. Alors* $\int h_n$ *a une limite notée* $\int h$ *qui ne dépend que de* h *et pas du choix de* $(h_n)_{n\in\mathbf{N}}$. *De plus,* $|h-h_n| \in \mathrm{Mes}(\mathrm{D},[0,\mathrm{M}])$, *et* $\int |h-h_n| \to 0$.

Remarque III.4.3. — (i) Comme $\int h_n \geqslant 0$, pour tout n, on a $\int h \geqslant 0$.

(ii) Si $h_n \to f$ p.p. et $h'_n \to g$ p.p., alors $h_n + h'_n \to f+g$ p.p. Il en résulte que $\int f+g = \int f + \int g$, si $f,g \in \mathrm{Mes}(\mathrm{D},[0,\mathrm{M}])$. En particulier, si $g \geqslant f$, alors $\int g = \int f + \int g - f \geqslant \int f$.

Lemme III.4.4. — *Si* A *est de mesure extérieure finie, alors, quel que soit* $\varepsilon > 0$, *il existe un ouvert* U *contenant* A *et tel que* $\lambda^+(\mathrm{U}) \leqslant \lambda^+(\mathrm{A}) + \varepsilon$.

Démonstration. — Si $\mathrm{D} = \prod_{j=1}^m [a_j, b_j[$ est une dalle, on peut, quel que soit $\eta > 0$, trouver un pavé ouvert $\mathrm{P} = \prod_{j=1}^m]a'_j, b_j[$ contenant D, tel que $\lambda^+(\mathrm{P}) \leqslant \lambda(\mathrm{D}) + \eta$. Soit alors $(\mathrm{D}_n)_{n\in\mathbf{N}}$ une suite de dalles élémentaires telle que $\mathrm{A} \subset \cup_{n\in\mathbf{N}} \mathrm{D}_n$, et $\lambda^+(\mathrm{A}) \leqslant \sum_{n\in\mathbf{N}} \lambda(\mathrm{D}_n) + \frac{\varepsilon}{2}$. D'après la discussion précédente, il existe P_n, pavé ouvert contenant D_n, tel que $\lambda^+(\mathrm{P}_n) \leqslant \lambda(\mathrm{D}_n) + \frac{\varepsilon}{2^{n+3}}$, et $\mathrm{U} = \cup_{n\in\mathbf{N}} \mathrm{P}_n$ répond aux exigences du lemme.

Lemme III.4.5. — *Si* $(\mathrm{X}_n)_{n\in\mathbf{N}}$ *est une suite décroissante de dallages telle que* $\cap_{n\in\mathbf{N}} \mathrm{X}_n$ *est de mesure nulle, alors* $\lim_{n\to+\infty} \lambda(\mathrm{X}_n) = 0$.

Démonstration. — Soit $\mathscr{L}$ la réunion des hyperplans de la forme $x_i = r$, pour $1 \leqslant i \leqslant m$ et $r \in \mathbf{Z}[\frac{1}{2}]$. Comme $\{1,\dots,m\} \times \mathbf{Z}[\frac{1}{2}]$ est dénombrable, $\mathscr{L}$ est de mesure nulle. Maintenant, si $n \in \mathbf{N}$, et si $\overline{\mathrm{X}}_n$ désigne l'adhérence de X_n, on a $\overline{\mathrm{X}}_n \subset \mathrm{X}_n \cup \mathscr{L}$, et donc

$$\cap_{n\in\mathbf{N}} \overline{\mathrm{X}}_n \subset \cap_{n\in\mathbf{N}} (\mathrm{X}_n \cup \mathscr{L}) \subset (\cap_{n\in\mathbf{N}} \mathrm{X}_n) \cup \mathscr{L};$$

on en déduit que $\cap_{n\in\mathbf{N}} \overline{\mathrm{X}}_n$ est de mesure nulle.

Soit alors $\varepsilon > 0$. Comme $\cap_{n\in\mathbf{N}} \overline{\mathrm{X}}_n$ est de mesure nulle, il existe un ouvert U_ε contenant $\cap_{n\in\mathbf{N}} \overline{\mathrm{X}}_n$, avec $\lambda^+(\mathrm{U}_\varepsilon) < \varepsilon$. Soit F_ε le complémentaire de U_ε dans $\overline{\mathrm{X}}_0$. On a $\mathrm{F}_\varepsilon \cap (\cap_{n\in\mathbf{N}} \overline{\mathrm{X}}_n) = \varnothing$, ce qui implique qu'il existe $n_0 \in \mathbf{N}$ tel que $\mathrm{F}_\varepsilon \cap (\cap_{n\leqslant n_0} \overline{\mathrm{X}}_n) = \varnothing$ car $\overline{\mathrm{X}}_0$ est compact et F_ε et les $\overline{\mathrm{X}}_n$ sont fermés dans $\overline{\mathrm{X}}_0$. Comme la suite $(\overline{\mathrm{X}}_n)_{n\in\mathbf{N}}$ est décroissante, on en déduit le fait que $\mathrm{F}_\varepsilon \cap \overline{\mathrm{X}}_{n_0} = \varnothing$, et donc que $\mathrm{X}_n \subset \overline{\mathrm{X}}_n \subset \mathrm{U}_\varepsilon$, quel que soit $n \geqslant n_0$. On a donc prouvé que, quel que soit $\varepsilon > 0$, il existe n_0, tel que $\lambda(\mathrm{X}_n) \leqslant \lambda^+(\mathrm{U}_\varepsilon) < \varepsilon$, si $n \geqslant n_0$. Ceci permet de conclure.

Lemme III.4.6. — *Si* $(h_n)_{n\in\mathbf{N}}$ *est une suite décroissante d'éléments de* $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$, *tendant vers* 0 *presque partout, alors* $\lim_{n\to+\infty} \int h_n = 0$.

Démonstration. — Si $\varepsilon > 0$, et si $n \in \mathbf{N}$, soit $\mathrm{X}_{n,\varepsilon} = \{x \in \mathrm{D},\ h_n(x) \geqslant \varepsilon\}$. Alors $(\mathrm{X}_{n,\varepsilon})_{n\in\mathbf{N}}$ est une suite décroissante de dallages, et $\cap_{n\in\mathbf{N}} \mathrm{X}_{n,\varepsilon}$ est de mesure nulle puisque h_n tend vers 0 presque partout. D'après le lemme III.4.5, ceci implique que $\lim_{n\to+\infty} \lambda(\mathrm{X}_{n,\varepsilon}) = 0$; et donc qu'il existe $n \in \mathbf{N}$ tel que $\lambda(\mathrm{X}_{n+p,\varepsilon}) \leqslant \varepsilon$, si $p \in \mathbf{N}$. Comme $h_{n+p}(x) \leqslant \mathrm{M}$, si $x \in \mathrm{X}_{n+p,\varepsilon}$, et $h_{n+p}(x) \leqslant \varepsilon$, si $x \notin \mathrm{X}_{n+p,\varepsilon}$, on a $\int h_{n+p} \leqslant \varepsilon(\lambda(\mathrm{D}) + \mathrm{M})$, quel que soit $p \in \mathbf{N}$. Ceci permet de conclure.

Lemme III.4.7. — *Si* $(h_n)_{n\in\mathbf{N}}$ *est une suite d'éléments de* $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$, *tendant vers* 0 *presque partout, telle que* $\sum_{n\in\mathbf{N}} \int |h_{n+1} - h_n| < +\infty$, *alors* $\lim_{n\to+\infty} \int h_n = 0$.

Démonstration. — Supposons le contraire. Il existe alors $\mathrm{C} > 0$ et une infinité de $n \in \mathbf{N}$ tels que $\int h_n \geqslant \mathrm{C}$. Quitte à extraire une sous-suite de la suite h_n, on peut donc supposer que $\int h_n \geqslant \mathrm{C}$ quel que soit $n \in \mathbf{N}$ (cela ne change pas la condition $\sum_{n\in\mathbf{N}} \int |h_{n+1} - h_n| < +\infty$ car, si $\varphi : \mathbf{N} \to \mathbf{N}$ est strictement croissante, on a $|h_{\varphi(n+1)} - h_{\varphi(n)}| \leqslant \sum_{k=\varphi(n)}^{\varphi(n+1)-1} |h_{k+1} - h_k|$). Comme la série $\sum_{n\in\mathbf{N}} \int |h_{n+1} - h_n|$ converge, on peut, quitte à rempacer n par $n + n_0$, supposer de plus que $\sum_{k\in\mathbf{N}} \int |h_{k+1} - h_k| \leqslant \frac{\mathrm{C}}{2}$. Soit alors

$g_n = \inf_{k\leqslant n} h_k$. Par construction, g_n est une suite décroissante d'éléments de $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$, qui tend vers 0 presque partout car $g_n \leqslant h_n$. D'après le lemme III.4.6, cela implique $\lim_{n\to+\infty}\int g_n = 0$. Par ailleurs, on a $g_n(x) \geqslant h_0(x) - \sum_{k=0}^{n-1} |h_{k+1}(x) - h_k(x)|$ (avec égalité si et seulement si la suite $(h_n(x))_{n\in\mathbf{N}}$ est décroissante). On en déduit que $\int g_n \geqslant \int h_0 - \sum_{k=0}^{n-1}\int |h_{k+1} - h_k| \geqslant \mathrm{C} - \frac{\mathrm{C}}{2}$, quel que soit $n \in \mathbf{N}$. D'où une contradiction qui permet de conclure.

Passons à la démonstration de la prop. III.4.2. Si $n \leqslant p$, soient

$$f_{n,p} = \inf_{n\leqslant k\leqslant p} h_k \quad \text{et} \quad g_{n,p} = \sup_{n\leqslant k\leqslant p} h_k.$$

Alors, quand n est fixé, $f_{n,p}$ (resp. $g_{n,p}$) est une suite décroissante (resp. croissante) d'éléments de $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$, alors que quand p est fixé $f_{n,p}$ (resp. $g_{n,p}$) est croissante (resp. décroissante). En particulier, si n est fixé, la suite $\int f_{n,p}$ (resp. $\int g_{n,p}$) est une suite décroissante (resp. croissante) d'éléments de $[0,\mathrm{M}\lambda(\mathrm{D})]$; elle admet donc une limite et est de Cauchy. On peut donc trouver $\varphi_0(n) \geqslant n$ tel que, quels que soient $p_1, p_2 \geqslant \varphi_0(n)$, on ait

$$\Big|\int f_{n,p_1} - \int f_{n,p_2}\Big| \leqslant 2^{-n} \quad \text{et} \quad \Big|\int g_{n,p_1} - \int g_{n,p_2}\Big| \leqslant 2^{-n}.$$

On note a_n la limite, quand p tend vers $+\infty$ de la suite croissante $\int g_{n,p} - f_{n,p}$, et on choisit $\varphi : \mathbf{N}\to\mathbf{N}$, avec $\varphi(n) \geqslant \varphi_0(n)$, et $\int u_n \geqslant \frac{1}{2}a_n$, où $u_n = g_{n,\varphi(n)} - f_{n,\varphi(n)}$. Par construction, $u_n \in \mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$, et $u_n \to 0$ p.p. car h_n a une limite p.p.

Si $n \in \mathbf{N}$, et si $p \geqslant \varphi(n)$,

$$\int |g_{n+1,\varphi(n+1)} - g_{n,\varphi(n)}| \leqslant \int |g_{n+1,\varphi(n+1)} - g_{n+1,p}| + \int |g_{n+1,p} - g_{n,p}| + \int |g_{n,p} - g_{n,\varphi(n)}|.$$

Maintenant, par hypothèse, on a

$$\int |g_{n+1,\varphi(n+1)} - g_{n+1,p}| + \int |g_{n,p} - g_{n,\varphi(n)}| \leqslant 2^{-n-1} + 2^{-n} \leqslant 2^{1-n},$$

et comme la suite $(g_{n,p})_{n\leqslant p}$ est décroissante, on a $|g_{n+1,p} - g_{n,p}| = g_{n,p} - g_{n+1,p}$. On en déduit, quel que soit $p \geqslant \max_{n\leqslant \mathrm{N}} \varphi(n)$, la majoration

$$\sum_{n=0}^{\mathrm{N}-1}\int |g_{n+1,\varphi(n+1)} - g_{n,\varphi(n)}| \leqslant \sum_{n=0}^{\mathrm{N}-1}\big(2^{1-n} + \int g_{n,p} - g_{n+1,p}\big) \leqslant 4 + \int g_{0,p} - g_{\mathrm{N},p} \leqslant 4 + \mathrm{M}\lambda(\mathrm{D}),$$

la dernière inégalité venant de ce que $g_{0,p} - g_{\mathrm{N},p} \in \mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$. On montre de même que

$$\sum_{n=0}^{\mathrm{N}-1}\int |f_{n+1,\varphi(n+1)} - f_{n,\varphi(n)}| \leqslant 4 + \mathrm{M}\lambda(\mathrm{D}).$$

On en déduit que

$$\sum_{n=0}^{+\infty}\int |u_n - u_{n+1}| \leqslant \sum_{n=0}^{+\infty}\Big(\int |f_{n+1,\varphi(n+1)} - f_{n,\varphi(n)}| + |g_{n+1,\varphi(n+1)} - g_{n,\varphi(n)}|\Big) \leqslant 8 + 2\mathrm{M}\lambda(\mathrm{D}) < +\infty,$$

ce qui permet d'utiliser le lemme III.4.7 pour montrer que $\int u_n \to 0$ et donc que $a_n \to 0$. Or on a

$$a_n = \sup_{p\geqslant n}\Big(\Big(\int \sup_{n\leqslant k\leqslant p} h_k\Big) - \Big(\int \inf_{n\leqslant k\leqslant p} h_k\Big)\Big) \geqslant \Big(\sup_{k\geqslant n}\int h_k\Big) - \Big(\inf_{k\geqslant n}\int h_k\Big).$$

On en déduit que les limites inférieure et supérieure de la suite $(\int h_n)_{n\in\mathbf{N}}$ sont égales et donc que $(\int h_n)_{n\in\mathbf{N}}$ a une limite.

Maintenant, si on part de suites $(h_n)_{n\in\mathbf{N}}$ et $(h'_n)_{n\in\mathbf{N}}$ d'éléments de $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$ convergeant p.p. vers h, on peut fabriquer une troisième suite $(h''_n)_{n\in\mathbf{N}}$ d'éléments de $\mathrm{Esc}(\mathrm{D},[0,\mathrm{M}])$ convergeant p.p.

vers h, en posant $h''_{2n} = h_n$ et $h''_{2n+1} = h'_n$, si $n \in \mathbf{N}$. L'existence de la limite de $\int h''_n$ quand n tend vers $+\infty$ implique l'égalité de $\lim_{n\to+\infty} \int h_n$ et $\lim_{n\to+\infty} \int h'_n$, ce qui prouve que la limite ne dépend que de h et pas de la suite $(h_n)_{n\in\mathbf{N}}$.

Ce qui précède s'applique à $f_n = \inf_{k\geqslant n} h_k = \lim_{p\to+\infty} f_{n,p}$ et $g_n = \sup_{k\geqslant n} h_k = \lim_{p\to+\infty} g_{n,p}$ qui sont des éléments de $\mathrm{Mes}(\mathrm{D}, [0, \mathrm{M}])$ par construction. On a donc $\int g_n - f_n = \lim_{p\to+\infty} \int g_{n,p} - f_{n,p} = a_n$, et $a_n \to 0$. Comme par ailleurs, $f_n \leqslant h_n \leqslant g_n$, et $f_n \leqslant h \leqslant g_n$ p.p, ce qui implique $|h - h_n| \leqslant g_n - f_n$ p.p., on a $\int |h - h_n| \leqslant a_n$, et donc $\int |h - h_n| \to 0$.

Ceci termine la démonstration de la proposition.

2. Mesure et mesure extérieure des ensembles mesurables

Ce n° est consacré à la démonstration du th. III.1.23, selon lequel $\lambda(\mathrm{A}) = \lambda^+(\mathrm{A})$ pour tout ensemble mesurable A. Si A est mesurable, et si $\mathrm{A_N} = \mathrm{A} \cap [-\mathrm{N}, \mathrm{N}[^m$, alors $\lambda(\mathrm{A}) = \lim_{n\to+\infty} \lambda(\mathrm{A_N})$ par définition. Par ailleurs, on déduit des (i) et (ii) de la prop. III.1.3, que $\lambda^+(\mathrm{A}) = \sup_{\mathrm{N}\in\mathbf{N}} \lambda^+(\mathrm{A_N})$. Il suffit donc de prouver que $\lambda(\mathrm{A_N}) = \lambda^+(\mathrm{A_N})$ pour tout N pour prouver que $\lambda(\mathrm{A}) = \lambda^+(\mathrm{A})$. Autrement dit, on peut supposer que A est borné.

Dans le reste de ce n°, on fixe un dallage D de $\mathbf{R}^m$, et tous les ensembles considérés sont inclus dans D. On dit que $\mathrm{A} \subset \mathrm{D}$ est *dallable* s'il existe une suite $(\mathrm{D}_n)_{n\in\mathbf{N}}$ de dalles élémentaires disjointes telles que $\mathrm{A} = \coprod_{n\in\mathbf{N}} \mathrm{D}_n$; une telle décomposition de A est une *décomposition en dalles élémentaires.*

Lemme III.4.8. — *Si* $(\mathrm{A}_n)_{n\in\mathbf{N}}$ *est une suite de sous-ensembles dallables de* D*, alors* $\mathrm{A} = \cup_{n\in\mathbf{N}} \mathrm{A}_n$ *est dallable.*

Démonstration. — Écrivons chaque A_n comme une réunion disjointe dénombrable de dalles élémentaires $\mathrm{D}_{n,i}$, pour $i \in \mathrm{I}_n$. Si $x \in \mathrm{A}$, soit D_x la plus grande dalle élémentaire contenant x parmi les $\mathrm{D}_{n,i}$, pour $n \in \mathbf{N}$ et $i \in \mathrm{I}_n$ (l'existence de D_x vient de ce que les dalles élémentaires se comportent comme des billes de mercure). Soit $\mathrm{J} \subset \cup_{n\in\mathbf{N}} \big(\{n\} \times \mathrm{I}_n\big)$ l'ensemble des (n, i) tels qu'il existe $x \in \mathrm{A}$ avec $\mathrm{D}_x = \mathrm{D}_{n,i}$. Alors A est la réunion disjointe des $\mathrm{D}_{n,i}$, pour $(n, i) \in \mathrm{J}$, et donc A est dallable.

Lemme III.4.9. — (i) *Si* $\mathrm{A} \subset \mathrm{D}$ *est dallable, alors* A *est mesurable et* $\lambda^+(\mathrm{A}) = \lambda(\mathrm{A}) = \sum_{n\in\mathbf{N}} \lambda(\mathrm{D}_n)$*, pour toute décomposition* $\mathrm{A} = \coprod_{n\in\mathbf{N}} \mathrm{D}_n$ *de* A *en dalles élémentaires.*

(ii) *Si* $\mathrm{A} \subset \mathrm{D}$*, alors* $\lambda^+(\mathrm{A}) = \inf \lambda(\mathrm{B})$*, où* B *décrit l'ensemble des ensembles dallables, avec* $\mathrm{A} \subset \mathrm{B} \subset \mathrm{D}$*.*

Démonstration. — Si $n \in \mathbf{N}$, soit $f_n = \sum_{i\leqslant n} \mathbf{1}_{\mathrm{D}_i}$. Alors $(f_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathrm{Esc}(\mathrm{D}, [0, 1])$ tendant vers $\mathbf{1}_\mathrm{A}$ en tout point, et donc $\int f_n = \sum_{i\leqslant n} \lambda(\mathrm{D}_i)$ tend vers $\int \mathbf{1}_\mathrm{D} = \lambda(\mathrm{D})$, d'après la prop. III.4.2. On en déduit que A est mesurable et que $\lambda(\mathrm{A}) = \sum_{n\in\mathbf{N}} \lambda(\mathrm{D}_n)$. Le (ii) s'en déduit en revenant à la définition de $\lambda^+(\mathrm{A})$, et l'égalité $\lambda^+(\mathrm{A}) = \lambda(\mathrm{A})$ du (i) est alors une conséquence immédiate du (ii).

Lemme III.4.10. — *Si* $f \in \mathrm{Mes}(\mathrm{D}, \mathbf{R}_+)$*, et si* $\mathrm{M} \in \mathbf{R}_+$*, alors* $\int f \geqslant \mathrm{M}\lambda^+(\{x,\ f(x) > \mathrm{M}\})$*.*

Démonstration. — Le cas $\mathrm{M} = 0$ étant évident, on se ramène au cas $\mathrm{M} = 1$ en multipliant f par M^{-1}, et quitte à remplacer f par $\inf(f, 2)$, on peut supposer f à valeurs dans $[0, 2]$. Soit $(h_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathrm{Esc}(\mathrm{D}, [0, 2])$ tendant vers f p.p. On a $\int |f - h_n| \to 0$ d'après la prop. III.4.2, et quitte à extraire une sous-suite de la suite h_n, on peut supposer que $\int |f - h_n| \leqslant 2^{-2-n}$. Soit $\mathrm{A} = \{x,\ f(x) > 1\}$ et, si $n \in \mathbf{N}$, soit $\mathrm{A}_n = \{x,\ h_n(x) > 1\}$. Alors A_n est un dallage, et il existe $\mathrm{B} \subset \mathrm{A}$ de mesure nulle tel que $\mathrm{A} - \mathrm{B} \subset \cup_{n\geqslant\mathrm{N}} \mathrm{A}_n$ pour tout $\mathrm{N} \in \mathbf{N}$. Comme $\cup_{n\geqslant\mathrm{N}} \mathrm{A}_n$ est dallable (lemme III.4.8), le (ii) du lemme III.4.9 nous fournit la minoration $\lambda(\cup_{n\geqslant\mathrm{N}} \mathrm{A}_n) \geqslant \lambda^+(\mathrm{A} - \mathrm{B}) = \lambda^+(\mathrm{A})$, pour tout $\mathrm{N} \in \mathbf{N}$, et comme $\sup_{n\geqslant\mathrm{N}} h_n \geqslant \mathbf{1}_{\cup_{n\geqslant\mathrm{N}} \mathrm{A}_n}$, on a aussi $\int \sup_{n\geqslant\mathrm{N}} h_n \geqslant \lambda^+(\mathrm{A})$, pour tout $\mathrm{N} \in \mathbf{N}$.

Par ailleurs, il résulte de la prop. III.4.2 que $\int \sup_{n\geqslant \mathrm{N}} h_n$ est la limite de $\int \sup_{k\geqslant n\geqslant \mathrm{N}} h_n$ quand $k \to +\infty$, et comme

$$\sup_{k\geqslant n\geqslant \mathrm{N}} h_n \leqslant h_{\mathrm{N}} + |h_{\mathrm{N}+1} - h_{\mathrm{N}}| + \cdots + |h_k - h_{k+1}| \text{ et } \int |h_{n+1} - h_n| \leqslant \int |h_{n+1} - h| + \int |h - h_n| \leqslant 2^{-1-n},$$

on obtient $\int \sup_{n\geqslant \mathrm{N}} h_n \leqslant 2^{-\mathrm{N}} + \int h_{\mathrm{N}}$, et donc $\lambda^+(\mathrm{A}) \leqslant 2^{-\mathrm{N}} + \int h_{\mathrm{N}}$, pour tout N. Enfin, comme $\int h_{\mathrm{N}} \to \int f$, un passage à la limite fournit la minoration $\lambda^+(\mathrm{A}) \leqslant \int f$ voulue, ce qui permet de conclure.

Revenons à la démonstration du th. III.1.23. Si B est un ensemble dallable contenant A, on a $\lambda(\mathrm{A}) \leqslant \lambda(\mathrm{B})$ puisque $\mathbf{1}_{\mathrm{A}} \leqslant \mathbf{1}_{\mathrm{B}}$. En prenant la borne inférieure sur tous les B dallables contenant A, on obtient $\lambda(\mathrm{A}) \leqslant \lambda^+(\mathrm{A})$, d'après le (ii) du lemme III.4.9.

L'inégalité $\lambda^+(\mathrm{A}) \leqslant \lambda(\mathrm{A})$ s'obtient en appliquant le lemme III.4.10 à $f = (1+\varepsilon)\mathbf{1}_{\mathrm{A}}$ et $\mathrm{M} = 1$, et en faisant tendre ε vers 0.

Ceci permet de conclure.

3. Le théorème de convergence monotone pour les fonctions bornées à support compact

Lemme III.4.11. — *Si $(h_n)_{n\in\mathbf{N}}$ est une suite d'éléments de* $\mathrm{Mes}(\mathbf{R}^m, \mathbf{R}_+)$ *tendant simplement p.p. vers h, et si $\int h_n \to 0$, alors $h = 0$ p.p.*

Démonstration. — h est la limite p.p. de toute suite extraite de la suite $(h_n)_{n\in\mathbf{N}}$, ce qui permet, quitte à extraire une sous-suite, de supposer que l'on a $\int h_n \leqslant 2^{-n}$ quel que soit $n \in \mathbf{N}$. Pour montrer que $h = 0$ p.p., il suffit de montrer que, quel que soit $j \in \mathbf{N}$, l'ensemble X_j des x tels que $h(x) > 2^{-j}$ est de mesure nulle. Il résulte du lemme III.4.10 que $\lambda^+(\{x,\ h_n(x) > 2^{-j}\}) \leqslant 2^j \int h_n \leqslant 2^{j-n}$. Comme $\sum 2^{j-n} < +\infty$, l'ensemble des x tels que $h_n(x) > 2^{-j}$ pour une infinité de $n \in \mathbf{N}$ est de mesure nulle d'après le théorème de Borel-Cantelli, et comme X_j est inclus dans cet ensemble (à l'ensemble près des x tels que $h_n(x) \not\to h(x)$, qui est de mesure nulle), cela permet de conclure.

Lemme III.4.12. — *Si $(g_n)_{n\in\mathbf{N}}$ est une suite d'éléments de* $\mathrm{Esc}(\mathbf{R}^m)$*, telle que $\sum_{n\in\mathbf{N}} \int |g_n| < +\infty$, alors la série $\sum_{n\in\mathbf{N}} g_n(x)$ converge absolument p.p.*

Démonstration. — Soit $\mathrm{C} = \sum_{n\in\mathbf{N}} \int |g_n|$. Si $\mathrm{M} \in \mathbf{R}_+$, soit $\mathrm{X}_{\mathrm{M},n}$ l'ensemble des $x \in \mathbf{R}^m$ tel que $\sum_{k\leqslant n} |g_k(x)| \geqslant \mathrm{M}$. Alors $\mathrm{X}_{\mathrm{M},n}$ est une suite croissante de dallages, et on a

$$\mathrm{M}\lambda(\mathrm{X}_{\mathrm{M},n}) \leqslant \int_{\mathrm{X}_{\mathrm{M},n}} \sum_{k\leqslant n} |g_k| \leqslant \int \sum_{k\leqslant n} |g_k| = \sum_{k\leqslant n} \int |g_k| \leqslant \mathrm{C},$$

quel que soit $n \in \mathbf{N}$. On en déduit que $\lambda^+(\cup_{n\in\mathbf{N}} \mathrm{X}_{\mathrm{M},n}) \leqslant \mathrm{M}^{-1}\mathrm{C}$, et comme l'ensemble A des $x \in \mathbf{R}^m$ tels que $\sum_{n\in\mathbf{N}} |g_n(x)| = +\infty$ est l'intersection des $\mathrm{X}_{\mathrm{M},n}$, pour $\mathrm{M} \in \mathbf{R}_+$, on a $\lambda^+(\mathrm{A}) \leqslant \mathrm{M}^{-1}\mathrm{C}$ quel que soit $\mathrm{M} \in \mathbf{R}_+$. Ceci implique que A est de mesure nulle, et permet de conclure.

Lemme III.4.13. — *Si $(h_k)_{k\in\mathbf{N}}$ est une suite croissante d'éléments de* $\mathrm{Mes}(\mathrm{D}, [0, \mathrm{M}])$*, alors la limite h de la suite $(h_k)_{k\in\mathbf{N}}$ est mesurable, et $\int h = \lim \int h_k = \sup \int h_k$.*

Démonstration. — La suite $\int h_k$ est croissante et majorée par $\mathrm{M}\lambda(\mathrm{D})$; elle admet donc une limite ℓ finie, et, quitte à extraire une sous-suite, on peut supposer que $\ell - \int h_k \leqslant 2^{-k}$, quel que soit $k \in \mathbf{N}$.

Maintenant, comme h_k est supposée mesurable, il existe une suite de fonctions en escalier $f_{k,\ell}$ tendant vers h_k p.p. Comme h_k est à support dans D et à valeurs dans $[0, \mathrm{M}]$, on peut, quitte à remplacer $f_{k,\ell}$ par la fonction valant 0 si $x \notin \mathrm{D}$, ou si $\mathrm{Re}(f_{k,\ell}(x)) \leqslant 0$, valant $\mathrm{Re}(f_{k,\ell}(x))$ si $\mathrm{Re}(f_{k,\ell}(x)) \in [0, \mathrm{M}]$ et $x \in \mathrm{D}$, et valant M si $\mathrm{Re}(f_{k,\ell}(x)) \geqslant \mathrm{M}$ et $x \in \mathrm{D}$, supposer que $f_{k,\ell} \in \mathrm{Esc}(\mathrm{D}, [0, \mathrm{M}])$. D'après la prop. III.4.2,

$\lim_{\ell\to+\infty}\int|h_k-f_{k,\ell}|=0$; il existe donc $\ell(k)$ tel que, si on pose $f_k=f_{k,\ell(k)}$, alors $\int|f_k-h_k|\leqslant 2^{-k}$. On a donc

$$\int|f_{k+1}-f_k|\leqslant\int|f_{k+1}-h_{k+1}|+\int|h_{k+1}-h_k|+\int|h_k-f_k|\leqslant 3\cdot 2^{-k},$$

et comme $\sum_{k\in\mathbf{N}}3\cdot 2^{-k}<+\infty$, le lemme III.4.12 montre que $f_k(x)$ a une limite simple $f(x)$ p.p. La fonction f est alors mesurable comme limite simple p.p. de fonctions en escalier, et $\int f_k\to\int f$ d'après la prop. III.4.2. Comme $\int f_k$ et $\int h_k$ ont même limite, il suffit, pour terminer la démonstration, de prouver que $f=h$ p.p. Or $f-h$ est la limite p.p. de f_k-h_k et $\int|f_k-h_k|\to 0$ par construction, ce qui permet d'utiliser le lemme III.4.11 pour conclure.

4. Limites simples p.p. de fonctions mesurables

Le but de ce n° est de démontrer la prop. III.1.12 selon laquelle une limite simple p.p. de fonctions mesurables est mesurable. Comme $f:\mathbf{R}^m\to\mathbf{C}$ est mesurable si et seulement si les fonctions $\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ et $\mathrm{Re}^+(-if)$ sont mesurables, et comme une fonction positive est mesurable si et seulement si elle est limite simple p.p. de fonctions en escalier positives, on peut supposer que toutes les fonctions considérées sont positives.

Lemme III.4.14. — *Soit f une fonction positive sur $\mathbf{R}^m$, et si $j\in\mathbf{N}$, soit D_j le dallage de sommets $(\pm 2^j,\dots,\pm 2^j)$.*

(i) *Si $\mathbf{1}_{\mathrm{D}_j}f$ est mesurable pour tout $j\in\mathbf{N}$, alors f est mesurable.*

(ii) *Si $\mathbf{1}_{\mathrm{D}_j}\inf(f,\mathrm{N})$ est mesurable pour tous $j,\mathrm{N}\in\mathbf{N}$, alors f est mesurable.*

Démonstration. — (i) Soit $(f_{j,k})_{k\in\mathbf{N}}$, si $j\in\mathbf{N}$, une suite de fonctions en escalier tendant vers $\mathbf{1}_{\mathrm{D}_j}f$ p.p. Soit g_k la fonction en escalier, nulle en dehors de D_k et égale à $f_{j,k}$ sur $\mathrm{D}_j-\mathrm{D}_{j-1}$, si $j\leqslant k$. On a donc $g_k(x)=f_{j,k}(x)$ si $x\in\mathrm{D}_j-\mathrm{D}_{j-1}$ et $k\geqslant j$, ce qui permet de prouver que g_k tend vers f p.p. On en déduit le (i).

(ii) Pour démontrer le (ii), compte tenu du (i), on peut supposer que f est à support dans D_j, et donc que $\mathbf{1}_{\mathrm{D}_j}\inf(f,\mathrm{N})=\inf(f,\mathrm{N})$. Soit $(f_{\mathrm{N},k})_{k\in\mathbf{N}}$, si $\mathrm{N}\in\mathbf{N}$, une suite de fonctions en escalier tendant vers $\inf(f,\mathrm{N})$ p.p. Soit g_k la fonction en escalier valant $f_{1,k}$ si $f_{1,k}<1$, $f_{2,k}$ si $f_{1,k}=1$ et $f_{2,k}<2$, $f_{3,k}$ si $f_{1,k}=1$, $f_{2,k}=2$ et $f_{3,k}<3$, …, et valant k si $f_{i,k}=i$ quel que soit $i\leqslant k$. Soit A_N l'ensemble des points tels que $f_{\mathrm{N},k}$ ne tende pas vers $\inf(f,\mathrm{N})$, et soit $\mathrm{A}=\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{A}_\mathrm{N}$. Alors A est un ensemble de mesure nulle comme réunion dénombrable d'ensembles de mesure nulle, et si $x\notin\mathrm{A}$, on a $g_k(x)=f_{i,k}(x)$, si k est assez grand et $f(x)\in]i-1,i[$, et $g_k(x)\in\{f_{i,k}(x),f_{i-1,k}(x)\}$, si k est assez grand et $f(x)=i$. On en déduit que $g_k(x)$ tend vers $f(x)$ si $x\notin\mathrm{A}$, ce qui permet de conclure.

Passons à la démonstration de la prop. III.1.12. Soit donc (ϕ_k) une suite de fonctions mesurables positives ayant une limite ϕ p.p. Pour montrer que ϕ est mesurable, il suffit, d'après le lemme III.4.14, de montrer que $\mathbf{1}_{\mathrm{D}_j}(\sup(\phi,\mathrm{N}))$ est mesurable, quels que soient $j,\mathrm{N}\in\mathbf{N}$. Comme $\mathbf{1}_{\mathrm{D}_j}(\sup(\phi,\mathrm{N}))$ est la limite p.p. de $\mathbf{1}_{\mathrm{D}_j}(\sup(\phi_k,\mathrm{N}))$, on peut supposer que ϕ et les ϕ_k sont à support dans D_j et à valeurs dans $[0,\mathrm{N}]$.

Or on a démontré (lemme III.4.13) qu'une suite croissante d'éléments h_n de $\mathrm{Mes}(\mathrm{D}_j,[0,\mathrm{N}])$ est mesurable ; il en est de même pour une suite décroissante comme on le voit en remplaçant h_n par $\mathrm{N}-h_n$. Comme $\phi_k\to\phi$ p.p., ϕ est aussi la limite inférieure de ϕ_k et donc est mesurable en tant que limite p.p. de la suite croissante $g_k=\inf_{\ell\geqslant k}\phi_\ell$, où chaque g_k est mesurable comme limite de la suite décroissante $g_{k,n}=\inf_{k\leqslant\ell\leqslant n}\phi_\ell$. Ceci permet de conclure.

5. Le théorème de convergence monotone et ses conséquences

Théorème III.4.15. — *Si $(f_n)_{n\in\mathbf{N}}$ est une suite croissante de fonctions mesurables positives sur $\mathbf{R}^m$, alors* $\lim_{n\to+\infty}\int f_n = \int \lim_{n\to+\infty} f_n$.

Démonstration. — Notons f la limite de la suite f_n ; c'est un élément de $\mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$. Si $n, \mathrm{N} \in \mathbf{N}$, soit $a_{n,\mathrm{N}} = \int_{\mathrm{D_N}} \inf(f_n, \mathrm{N})$. Par définition, on a $\int f_n = \lim_{\mathrm{N}\to+\infty} a_{n,\mathrm{N}}$, et donc $\int f_n = \sup_{\mathrm{N}\in\mathbf{N}} a_{n,\mathrm{N}}$ puisque la suite est croissante. Par ailleurs, comme $f_n \to f$ p.p., cela implique que $\inf(f_n, \mathrm{N}) \to \inf(f, \mathrm{N})$ p.p. sur $\mathrm{D_N}$, et comme la suite $\inf(f_n, \mathrm{N})$ est croissante, il résulte du lemme III.4.13 que $\int_{\mathrm{D_N}} \inf(f, \mathrm{N}) = \sup_{n\in\mathbf{N}} a_{n,\mathrm{N}}$. On a donc

$$\int f = \sup_{\mathrm{N}\in\mathbf{N}} (\sup_{n\in\mathbf{N}} a_{n,\mathrm{N}}) = \sup_{(n,\mathrm{N})\in\mathbf{N}\times\mathbf{N}} a_{n,\mathrm{N}} = \sup_{n\in\mathbf{N}} (\sup_{\mathrm{N}\in\mathbf{N}} a_{n,\mathrm{N}}) = \sup_{n\in\mathbf{N}} \int f_n,$$

et comme la suite $(\int f_n)_{n\in\mathbf{N}}$ est croissante, on a aussi $\sup_{n\in\mathbf{N}} \int f_n = \lim_{n\to+\infty} \int f_n$, ce qui permet de conclure.

On peut maintenant prouver que l'intégrale que l'on a construite satisfait les propriété (i)-(v) du th. III.1.18, ce qui terminera la preuve de l'existence de l'intégrale de Lebesgue.

- On vient de prouver la propriété (v).
- La (i) est incluse dans la construction.
- Si $f, g \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$, alors

$$\inf(f+g, \mathrm{N}) \leqslant \inf(f, \mathrm{N}) + \inf(g, \mathrm{N}) \leqslant \inf(f+g, 2\mathrm{N}),$$

et donc

$$\mathbf{1}_{\mathrm{D_N}} \inf(f+g, \mathrm{N}) \leqslant \mathbf{1}_{\mathrm{D_N}} \inf(f, \mathrm{N}) + \mathbf{1}_{\mathrm{D_N}} \inf(g, \mathrm{N}) \leqslant \mathbf{1}_{\mathrm{D_{2N}}} \inf(f+g, 2\mathrm{N}).$$

On en déduit, en faisant tendre N vers $+\infty$, et en utilisant le théorème de convergence monotone, les inégalités $\int(f+g) \leqslant \int f + \int g \leqslant \int(f+g)$, ce qui prouve que $\int(f+g) = \int f + \int g$. Par récurrence, on en déduit que $\int nf = n\int f$, si $n \in \mathbf{N}$, puis $\int af = a\int f$, si $a \in \mathbf{Q}_+$, et finalement, en utilisant la croissance de $a \mapsto \int af$, que $\int af = a\int f$, si $a \in \mathbf{R}_+$. On en déduit la linéarité de l'intégration (propriété (ii)).

- On sait que, si le théorème de convergence monotone (propriété (v) démontrée ci-dessus) est vérifié, alors la propriété (iii) est un cas particulier du th. III.1.23 (cf. cor. III.1.22), démontré au n° 2.
- On a remarqué (cf. (ii) de la rem. III.1.19) que la (iv) pouvait se déduire des (ii) et (iii).

Ceci permet de conclure.

CHAPITRE IV

TRANSFORMÉE DE FOURIER

La représentation d'une fonction périodique comme somme d'une série de Fourier est un outil très efficace pour la résolution de certaines équations aux dérivées partielles (la transformée de Fourier et cette représentation des fonctions périodiques ont d'ailleurs été introduites par Fourier en 1811 dans un mémoire consacré à l'équation de la chaleur). La formule d'inversion de Fourier (démontrée par Cauchy (1815) et Poisson (1816) dans des mémoires consacrés à l'équation de Laplace), qui permet d'écrire une fonction raisonnable sur $\mathbf{R}^m$ comme somme continue de caractères linéaires unitaires [1] continus, rend le même genre de services pour des équations aux dérivées partielles sur $\mathbf{R}^m$. Cette « boite à outils » de Fourier s'adapte à tout groupe commutatif localement compact : il s'agit de décomposer une fonction sur un tel groupe comme une « somme » de caractères [2]. Nous l'avons déjà rencontrée dans le cadre des groupes finis (n° 5 du § I.2) ; les séries de Fourier correspondent au groupe $\mathbf{R}/\mathbf{Z}$; nous la rencontrerons de nouveau pour $\mathbf{R}_+^*$ (sous le nom de transformée de Mellin, cf. rem. VII.2.5), pour $\mathbf{Q}_p$ et pour le groupe des adèles de $\mathbf{Q}$ (cf. n° 2 du § G.2).

IV.1. Intégrales dépendant d'un paramètre

De nombreuses fonctions sont définies comme intégrales de fonctions plus simples [3], et le théorème de convergence dominée permet, bien souvent, de démontrer leur continuité et leur dérivabilité.

Théorème IV.1.1. — (Continuité d'une intégrale dépendant d'un paramètre) *Soit* X *un espace métrique, et soit* $x_0 \in \mathrm{X}$. *Soit* $f : \mathrm{X} \times \mathbf{R}^m \to \mathbf{C}$ *vérifiant :*

- *la fonction* $t \mapsto f(x,t)$ *est mesurable, quel que soit* $x \in \mathrm{X}$ *;*
- *pour presque tout* $t \in \mathbf{R}^m$, *la fonction* $x \mapsto f(x,t)$ *est continue en* x_0 *;*

1. Un caractère linéaire de $\mathbf{R}^m$ est une fonction $\chi : \mathbf{R}^m \to \mathbf{C}^*$ vérifiant $\chi(x+y) = \chi(x)\chi(y)$, quels que soient $x, y \in \mathbf{R}^m$; un tel caractère est unitaire si $|\chi(x)| = 1$, quel que soit $x \in \mathbf{R}^m$.

2. En probabilité, la transformée de Fourier est connue sous le nom de *fonction caractéristique*.

3. C'est par exemple le cas de la fonction Γ d'Euler définie par $\Gamma(s) = \int_{\mathbf{R}_+} e^{-t} t^s \frac{dt}{t}$, ou de la transformée de Fourier $\hat{f}$ d'une fonction sommable f définie (en une variable) par $\hat{f}(x) = \int_{\mathbf{R}} e^{-2i\pi xt} f(t)\, dt$.

• *il existe* $h \in \mathscr{L}^1(\mathbf{R}^m)$ *tel que, quel que soit* $x \in \mathrm{X}$*, on ait* $|f(x,t)| \leqslant h(t)$ *p.p.*
Alors, si $x \in \mathrm{X}$*, l'intégrale* $\int_{\mathbf{R}^m} f(x,t)\,dt$ *est bien définie et la fonction* $\mathrm{F} : \mathrm{X} \to \mathbf{C}$ *définie par* $\mathrm{F}(x) = \int_{\mathbf{R}^m} f(x,t)\,dt$ *est continue en* x_0*.*

Démonstration. — La fonction $t \mapsto f(x,t)$ appartient à $\mathscr{L}^1$, quel que soit $x \in \mathrm{X}$, puisqu'on l'a supposée mesurable et majorée en module par un élément de $\mathscr{L}^1(\mathbf{R}^m)$. La fonction F est donc bien définie. Pour montrer que F est continue en x_0, il suffit (car X est un espace métrique) de prouver que pour toute suite $(y_n)_{n\in\mathbf{N}}$ convergeant vers x_0, la suite $(\mathrm{F}(y_n))_{n\in\mathbf{N}}$ tend vers $\mathrm{F}(x_0)$, c'est-à-dire

$$\lim_{n\to+\infty} \int_{\mathbf{R}^m} f(y_n,t)\,dt = \int_{\mathbf{R}^m} f(x_0,t)\,dt.$$

Posons $g_n(t) = f(y_n,t)$, et $g(t) = g(x_0,t)$. On a alors
• $\lim_{n\to+\infty} g_n(t) = g(t)$ p.p., car $x \mapsto f(x,t)$ est continue en x_0, pour presque tout t ;
• $|g_n(t)| \leqslant h(t)$ p.p. et h est sommable (et indépendante de n).
On est donc dans les conditions d'application du théorème de convergence dominée, et $\lim_{n\to+\infty} \int_{\mathbf{R}^m} g_n(t)\,dt = \int_{\mathbf{R}^m} g(t)\,dt$, ce qui permet de conclure.

Théorème IV.1.2. — (de dérivation sous le signe somme) *Soient* I *un intervalle de* $\mathbf{R}$ *et* $f : \mathrm{I} \times \mathbf{R}^m \to \mathbf{C}$ *vérifiant :*
• $t \mapsto f(x,t)$ *est sommable, quel que soit* $x \in \mathrm{I}$ *;*
• *il existe un ensemble de mesure nulle* $\mathrm{A} \subset \mathbf{R}^m$ *et* $h : \mathbf{R}^m \to \mathbf{R}_+$ *sommable, tels que* $\frac{\partial f}{\partial x}(x,t)$ *existe en tout point de* $\mathbf{R}^m - \mathrm{A}$ *et* $|\frac{\partial f}{\partial x}(x,t)| \leqslant h(t)$*, pour tous*[4] $x \in \mathrm{I}$ *et* $t \notin \mathrm{A}$*.*
Alors la fonction F *définie sur* I *par* $\mathrm{F}(x) = \int_{\mathbf{R}^m} f(x,t)\,dt$ *est dérivable et, quel que soit* $x \in \mathrm{I}$*, on a*

$$\mathrm{F}'(x) = \int_{\mathbf{R}^m} \frac{\partial f}{\partial x}(x,t)\,dt.$$

Démonstration. — Quitte à remplacer f par la fonction valant $f(x,t)$, si $t \notin \mathrm{A}$, et valant 0, si $t \in \mathrm{A}$, ce qui ne change pas la valeur des intégrales, on peut supposer que $\mathrm{A} = \varnothing$.

Fixons $x \in \mathrm{I}$. Soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathrm{I} - \{x\}$ tendant vers x quand n tend vers $+\infty$. Soit $g(t) = \frac{\partial f}{\partial x}(x,t)$, et si $n \in \mathbf{N}$, soit $g_n(t) = \frac{f(x_n,t)-f(x,t)}{x_n-x}$. Alors g_n tend vers g simplement, et d'après le théorème des accroissement finis, on a

$$|g_n(t)| \leqslant \sup_{0\leqslant\theta\leqslant1} \Big|\frac{\partial f}{\partial x}(x+\theta(x_n-x),t)\Big| \leqslant h(t),$$

4. La dérivabilité étant une propriété locale, pour démontrer la dérivabilité sur un intervalle I, il suffit de la démontrer sur une suite d'intervalles dont la réunion est I. En d'autre termes, on n'a pas vraiment besoin d'une majoration sur I tout entier, mais sur une suite d'intervalles dont la réunion est I. Cette remarque s'applique aussi au cor. IV.1.3 pour lequel on peut aussi commencer par diminuer Ω.

quel que soit $t \in \mathbf{R}^m$. On est donc dans les conditions d'application du théorème de convergence dominée, et $\lim_{n\to+\infty} \int_{\mathbf{R}^m} g_n = \int_{\mathbf{R}^m} g$. Autrement dit, on a

$$\lim_{n\to+\infty} \frac{\mathrm{F}(x_n) - \mathrm{F}(x)}{x_n - x} = \int_{\mathbf{R}^m} \frac{\partial f}{\partial x}(x,t)\, dt,$$

pour toute suite $(x_n)_{n\in\mathbf{N}}$ d'éléments de $\mathrm{I} - \{x\}$ tendant vers x quand n tend vers $+\infty$. On en déduit le résultat.

Si $\boldsymbol{\ell} = (\ell_1, \dots, \ell_n) \in \mathbf{N}^n$, on pose $|\boldsymbol{\ell}| = \ell_1 + \cdots + \ell_n$, et $\partial_{\amalg} = (\frac{\partial}{\partial x_1})^{k_1} \cdots (\frac{\partial}{\partial x_n})^{k_n}$.

Corollaire IV.1.3. — *Soient Ω un ouvert de $\mathbf{R}^n$, $k \in \mathbf{N}$ et $f : \Omega \times \mathbf{R}^m \to \mathbf{C}$ vérifiant :*

- *$t \mapsto f(x,t)$ est sommable, quel que soit $x \in \Omega$;*
- *il existe un ensemble de mesure nulle $\mathrm{A} \subset \mathbf{R}^m$ et $h : \mathbf{R}^m \to \mathbf{R}_+$ sommable, tels que, si $t \in \mathbf{R}^m - \mathrm{A}$, la fonction $x \mapsto f(x,t)$ est de classe $\mathscr{C}^k$ sur Ω, et $|\partial_{\amalg} f(x,t)| \leqslant h(t)$, quels que soient $x \in \Omega$, $\boldsymbol{\ell} \in \mathbf{N}^n$, avec $|\boldsymbol{\ell}| \leqslant k$, et $t \notin \mathrm{A}$.*

Alors la fonction F définie sur Ω par $\mathrm{F}(x) = \int_{\mathbf{R}^m} f(x,t)\, dt$ est de classe $\mathscr{C}^k$ et, quels que soient $\boldsymbol{\ell} \in \mathbf{N}^n$, avec $|\boldsymbol{\ell}| \leqslant k$, et $x \in \Omega$, on a

$$\partial_{\amalg} \mathrm{F}(x) = \int_{\mathbf{R}^m} \partial_{\amalg} f(x,t)\, dt.$$

Démonstration. — Cela se déduit du théorème de dérivation sous le signe somme par une récurrence immédiate.

Exercice IV.1.4. — Soit $\mathrm{I} =]0,1[$, et soit $f : \mathrm{I} \times \mathbf{R} \to \mathbf{R}$ définie par $f(x,t) = 0$ si $t \leqslant 0$ ou si $t \geqslant x$, et $f(x,t) = 1$ si $0 < t < x$. Calculer explicitement $\mathrm{F}(x) = \int_{\mathbf{R}} f(x,t)\, dt$ et $\mathrm{F}'(x)$. Peut-on en déduire $1 = 0$?

Exercice IV.1.5. — (Fonction Γ d'Euler)

(i) Montrer que l'intégrale $\Gamma(s) = \int_0^{+\infty} e^{-t} t^s \frac{dt}{t}$ est bien définie si $s \in \mathbf{R}_+^*$.

(ii) Montrer que Γ est de classe $\mathscr{C}^\infty$ sur $\mathbf{R}_+^*$ et tend vers $+\infty$ en $s = 0$.

(iii) Montrer que $\Gamma(s+1) = s\Gamma(s)$ si $s > 0$; en déduire que $\Gamma(n+1) = n!$, si $n \in \mathbf{N}$.

(iv) *Formule de Stirling (1730)* : montrer que $\Gamma(s+1) \sim (\frac{s}{e})^s \sqrt{2\pi s}$ au voisinage de $+\infty$. Faire le changement de variable $t = s + u\sqrt{s}$ (méthode de Laplace), et montrer que

$$-u\sqrt{s} + s\log(1 + \frac{u}{\sqrt{s}}) \leqslant \begin{cases} -\frac{u^2}{2} & \text{si } -\sqrt{s} < u \leqslant 0, \\ -u + \log(1+u) & \text{si } u \geqslant 0 \text{ et } s \geqslant 1. \end{cases}$$

(v) En déduire la *formule de Gauss* : $\frac{1}{\Gamma(s)} = \lim_{n\to+\infty} \frac{s(s+1)\cdots(s+n)}{n!\, n^s}$, si $s \in \mathbf{R}_+^*$.

Exercice IV.1.6. — Soit $\mathrm{B}(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1} dx$. Montrer que $\mathrm{B}(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$, si $s > 0$ et $t > 0$. (On écrira $\Gamma(s+t)\mathrm{B}(s,t)$ comme une intégrale double.)

Exercice IV.1.7. — Soient $f \in \mathscr{L}^1(\mathbf{R}^m)$ et $g \in \mathscr{C}_c^k(\mathbf{R}^m)$, où $k \in \mathbf{N} \cup \{\infty\}$. Montrer que la convolée $x \mapsto f * g(x) = \int f(x-y) g(y)\, dy$ est de classe $\mathscr{C}^k$ sur $\mathbf{R}^m$.

Exercice IV.1.8. — (i) Montrer que l'intégrale $\int_0^{+\infty} \frac{\sin t}{t}\, dt$ est semi-convergente (c'est-à-dire que $\frac{\sin t}{t}$ est sommable sur $[0, \mathrm{T}]$, pour tout T, et que $\int_0^{\mathrm{T}} \frac{\sin t}{t}\, dt$ a une limite quand $\mathrm{T} \to +\infty$).

(ii) Si $\lambda \geqslant 0$, soit $\mathrm{F}(\lambda) = \int_0^{+\infty} e^{-\lambda t} \frac{\sin t}{t}\, dt$. Montrer que F est de classe $\mathscr{C}^1$ sur $\mathbf{R}_+^*$ et calculer $\mathrm{F}'(\lambda)$.

(iii) Montrer que F tend vers 0 en $+\infty$; en déduire $\mathrm{F}(\lambda)$, pour $\lambda > 0$.

(iv) Montrer que F est continue en 0 ; en déduire la valeur de $\int_0^{+\infty} \frac{\sin t}{t}\, dt$.

Exercice IV.1.9. — (Fonction de Bessel) Soit $\nu \in \mathbf{C}$.

(i) Montrer que $y \mapsto \mathrm{K}_\nu(y) = \frac{1}{2}\int_0^{+\infty} e^{-y(t+t^{-1})/2} t^\nu \frac{dt}{t}$ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+^*$.

(ii) Montrer que $\mathrm{K}_\nu(y) \sim \sqrt{\frac{2\pi}{y}} e^{-y}$ au voisinage de $y = +\infty$. (On pourra couper l'intégrale en 1 pour se ramener à une intégrale sur $[1, +\infty[$, et faire le changement de variable $t = 1 + \frac{y}{\sqrt{x}}$.)

IV.2. Transformée de Fourier dans L^1

1. Caractères linéaires de R et $\mathbf{R}^m$

Si $x = (x_1, \dots, x_m)$ et $t = (t_1, \dots, t_n)$ sont deux éléments de $\mathbf{R}^m$, on note $x \cdot t$ leur produit scalaire $\sum_{i=1}^m x_i t_i$; on a $x \cdot t = t \cdot x$. Rappelons que, si $\mathrm{A} \in \mathbf{M}_m(\mathbf{R})$, on note ${}^{\mathrm{t}}\mathrm{A}$ la matrice transposée de A. On a alors ${}^{\mathrm{t}}\mathrm{A}x \cdot t = x \cdot \mathrm{A}t$ pour tous $x, t \in \mathbf{R}^m$.

Proposition IV.2.1. — (i) *Les caractères linéaires continus de* $\mathbf{R}$ *sont les* $t \mapsto e^{\lambda t}$*, pour* $\lambda \in \mathbf{C}$*, et les caractères linéaires unitaires continus sont les* $t \mapsto e^{2i\pi\, xt}$*, pour* $x \in \mathbf{R}$*.*

(ii) *Les caractères linéaires unitaires continus de* $\mathbf{R}^m$ *sont les* $t \mapsto e^{2i\pi\, x\cdot t}$*, pour* $x \in \mathbf{R}^m$*.*

Démonstration. — Soit $\chi : \mathbf{R} \to \mathbf{C}^*$ un caractère linéaire continu. On a en particulier $\chi(0) = 1$, et la continuité implique l'existence de $j \in \mathbf{N}$ tel que $|\chi(t) - 1| \leqslant \frac{1}{2}$, si $|t| \leqslant 2^{-j}$. Notons $\log : \mathbf{C}^* \to \{x + iy,\ -\pi < y \leqslant \pi\}$ le logarithme complexe. Comme $\mathrm{B}(1, \frac{1}{2})$ est incluse dans le secteur angulaire $|\arg(z)| \leqslant \frac{\pi}{4}$, l'application $g = \log \circ \chi : \mathrm{B}(1, \frac{1}{2}) \to \mathbf{C}$ est à valeur dans la bande $\{x + iy,\ |y| \leqslant \frac{\pi}{4}\}$. Maintenant, $\log(z_1 z_2) - \log z_1 - \log z_2 \in 2i\pi$, pour tous $z_1, z_2 \in \mathbf{C}^*$, et comme $\chi(t_1 + t_2) = \chi(t_1)\chi(t_2)$, on a $g(t_1 + t_2) = g(t_1) + g(t_2)$ si t_1, t_2 et $t_1 + t_2$ appartiennent à $\mathrm{B}(1, \frac{1}{2})$. On en déduit, par récurrence sur n, que $g(2^{-j-n}) = 2^{-n} g(2^{-j})$, pour tout $n \in \mathbf{N}$, et, par récurrence sur k, que $g(k2^{-j-n}) = kg(2^{-j-n})$, si $k \in \{-2^n, \dots, 2^n\}$. On a donc $g(r2^{-j}) = rg(2^{-j})$, si r est un nombre dyadique dans l'intervalle $[-1, 1]$, et comme g est continue, on en déduit que $g(t) = \lambda t$, avec $\lambda = 2^j g(2^{-j})$, pour tout $t \in [-2^{-j}, 2^{-j}]$. Par définition de g, cela implique que $\chi(t) = e^{\lambda t}$ pour tout $t \in [-2^{-j}, 2^{-j}]$. Enfin, si $t \in \mathbf{R}$, il existe $n \in \mathbf{N}$ tel que $t/n \in [-2^{-j}, 2^{-j}]$, et comme $\chi(t) = \chi(t/n)^n$, on a $\chi(t) = e^{\lambda t}$ pour tout $t \in \mathbf{R}$.

Maintenant, si χ est unitaire, on doit avoir $\lambda t \in i\mathbf{R}$, pour tout $t \in \mathbf{R}$, et il existe donc $x \in \mathbf{R}$ tel que $\lambda = 2i\pi\, x$. On en déduit le (i).

Si $\chi : \mathbf{R}^m \to \mathbf{C}^*$ est un caractère linéaire unitaire continu, alors sa restriction à $\mathbf{R}e_j$ définit un caractère linéaire unitaire continu de $\mathbf{R}$, pour tout $j \in \{1, \dots, m\}$. Il existe donc $x_j \in \mathbf{R}$ tel que $\chi(t_j e_j) = e^{2i\pi\, x_j t_j}$. Or $t = \sum_{j=1}^m t_j e_j$, et donc $\chi(t) = \prod_{j=1}^m \chi(t_j e_j) = e^{2i\pi\, x\cdot t}$, avec $x = (x_1, \dots, x_m)$. Ceci permet de conclure.

2. Définition et premières propriétés

Si $f \in \mathscr{L}^1(\mathbf{R}^m)$, on a $|e^{-2i\pi\, x\cdot t} f(t)| = |f(t)|$ quels que soient $x, t \in \mathbf{R}^m$; l'intégrale $\int_{\mathbf{R}^m} e^{-2i\pi\, x\cdot t} f(t)\, dt$ est donc bien définie pour toute valeur de $x \in \mathbf{R}^m$.

On appelle *transformée de Fourier* de f la fonction $\hat{f}$ définie, pour $x \in \mathbf{R}^m$, par

$$\hat{f}(x) = \int_{\mathbf{R}^m} e^{-2i\pi\, x\cdot t} f(t)\, dt.$$

Elle ne dépend que de la classe de f dans $\mathrm{L}^1(\mathbf{R}^m)$, ce qui permet de définir la transformée de Fourier d'un élément de $\mathrm{L}^1(\mathbf{R}^m)$ par la même formule. On note souvent, pour des raisons typographiques, $\mathscr{F}f$ au lieu de $\hat{f}$, la transformée de Fourier de f, et on définit $\overline{\mathscr{F}}f$ par $\overline{\mathscr{F}}f(x) = \hat{f}(-x)$.

Exemple IV.2.2. — La transformée de Fourier de $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$ est $\alpha(x) = \frac{\sin \pi x}{\pi x}$, comme le montre un calcul immédiat.

Soit $f \in \mathrm{L}^1(\mathbf{R}^m)$. Des changements de variable immédiats montrent que :

• $\mathscr{F}(f(at))(x) = |a|^{-m}\hat{f}(a^{-1}x)$, si $a \in \mathbf{R}^*$; *la transformée de Fourier tranforme une dilatation en dilatation de rapport inverse* ;

• $\mathscr{F}\big(f(t+b)\big)(x) = e^{2i\pi\, b\cdot x}\hat{f}(x)$ et $\mathscr{F}\big(e^{2i\pi\, c\cdot t}f(t)\big)(x) = \hat{f}(x-c)$, si $b, c \in \mathbf{R}^m$; *la transformée de Fourier échange les translations et les multiplications par un caractère.*

Exercice IV.2.3. — Montrer plus généralement que, si $f \in \mathrm{L}^1(\mathbf{R}^m)$, si $\mathrm{A} \in \mathbf{GL}_m(\mathbf{R})$, si $b, c \in \mathbf{R}^m$, et si $g(t) = e^{2i\pi\, c\cdot t} f(\mathrm{A}t + b)$, alors $\hat{g}(x) = |\det \mathrm{A}|^{-1} e^{2i\pi\, {}^t\mathrm{A}^{-1}(x-c)\cdot b}\hat{f}({}^t\mathrm{A}^{-1}(x-c))$.

Exercice IV.2.4. — Soit f une fonction continue bornée et sommable sur $\mathbf{R}$, et soit $x_0 \in \mathbf{R}$. Montrer que, quand λ tend vers 0^+, la fonction

$$\mathrm{F}(\lambda) = \int_{-\infty}^{+\infty} e^{2i\pi\, x_0 y - \lambda|y|}\hat{f}(y)dy$$

tend vers une limite que l'on calculera. En déduire que si $\hat{f}$ est identiquement nulle, alors f est identiquement nulle.

Exercice IV.2.5. — Soit $f \in \mathrm{L}^1(\mathbf{R})$. Montrer que $\lim_{\mathrm{T}\to+\infty} \mathrm{T}^{-1}\int_{-\mathrm{T}}^{\mathrm{T}} |\hat{f}(x)|^2\, dx = 0$.

3. Le théorème de Riemann-Lebesgue

On rappelle que $\mathscr{C}_0(\mathbf{R}^m)$ désigne l'espace des fonctions continues sur $\mathbf{R}^m$, tendant vers 0 à l'infini.

Proposition IV.2.6. — (i) *Si $r \in \mathbf{N}$, et si $\mathbf{k} \in \mathbf{Z}^m$, alors*

$$\hat{e}_{r,\mathbf{k}}(x) = 2^{-rm}\prod_{j=1}^{m}\big(e^{-2^{1-r}i\pi(k_j+\frac{1}{2})x_j}\alpha(2^{-r}x_j)\big).$$

(ii) *Si f est une fonction en escalier, alors $\hat{f} \in \mathscr{C}_0(\mathbf{R}^m)$.*

Démonstration. — Le (i) est une conséquence de la formule

$$e_{r,\mathbf{k}}(t) = \prod_{j=1}^{m}\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}(2^r t_j - k_j - \frac{1}{2}),$$

de la formule de l'exemple IV.2.2, et des formules pour les dilatations-translations. Le (ii) est une conséquence du (i), de ce que les $e_{r,\mathbf{k}}$ forment une famille génératrice de $\mathrm{Esc}(\mathbf{R}^m)$, et de ce que α est une fonction continue sur $\mathbf{R}$, tendant vers 0 à l'infini.

Théorème IV.2.7. — (Riemann-Lebesgue) *L'application $f \mapsto \hat{f}$ est une application linéaire* 1*-lipschtzienne de* $\mathrm{L}^1(\mathbf{R}^m)$ *dans* $\mathscr{C}_0(\mathbf{R}^m)$*. Autrement dit, si $f \in \mathrm{L}^1(\mathbf{R}^m)$, alors $\hat{f}$ est une fonction continue sur $\mathbf{R}^m$, tendant vers* 0 *à l'infini, et on a $\|\hat{f}\|_\infty \leqslant \|f\|_1$.*

Démonstration. — La linéarité de $f \mapsto \hat{f}$ résulte de la linéarité de l'intégration, et l'inégalité $\|\hat{f}\|_\infty \leqslant \|f\|_1$ résulte de la majoration

$$\Big| \int_{\mathbf{R}^m} e^{-2i\pi\, x\cdot t} f(t)\, dt \Big| \leqslant \int_{\mathbf{R}^m} |e^{-2i\pi\, x\cdot t} f(t)|\, dt = \int_{\mathbf{R}^m} |f(t)|\, dt = \|f\|_1.$$

Maintenant, si f est une fonction en escalier, la prop. IV.2.6, montre que $\hat{f} \in \mathscr{C}_0(\mathbf{R}^m)$. Comme les fonctions en escalier sont denses dans $\mathrm{L}^1(\mathbf{R}^m)$, comme $f \mapsto \hat{f}$ est linéaire continue de $\mathrm{L}^1(\mathbf{R}^m)$ dans l'espace $\mathscr{B}(\mathbf{R}^m)$ des fonctions bornées sur $\mathbf{R}^m$ (muni de la norme $\| \ \|_\infty$) dans lequel $\mathscr{C}_0(\mathbf{R}^m)$ est fermé, on en déduit que $\hat{f} \in \mathscr{C}_0(\mathbf{R}^m)$ quel que soit $f \in \mathrm{L}^1(\mathbf{R}^m)$ [on peut rendre cet argument moins abstrait en considérant une suite f_n de fonctions en escalier tendant vers f dans $\mathrm{L}^1(\mathbf{R}^m)$; alors $\hat{f}_n \to \hat{f}$ uniformément, et on conclut en utilisant le fait qu'une limite uniforme de fonctions continues tendant vers 0 à l'infini est encore une fonction continue tendant vers 0 à l'infini (cf. ex. 16.4 du Vocabulaire)]. Ceci permet de conclure.

4. Transformée de Fourier et dérivation

Une des propriétés fondamentales de la transformée de Fourier est d'échanger la régularité et la décroissance à l'infini (i.e. plus une fonction est régulière, plus sa transformée de Fourier est petite à l'infini, et réciproquement, plus une fonction est petite à l'infinie et plus sa transformée de Fourier est régulière), ainsi que dérivations et multiplications par des polynômes, ce qui, combiné avec la formule d'inversion de Fourier (prop. IV.3.25), facilite grandement l'étude de certaines équations aux dérivées partielles [5]. On a en particulier le résultat suivant.

Théorème IV.2.8. — (i) *Si $f \in \mathscr{C}^k(\mathbf{R}^m)$ a toutes ses dérivées partielles d'ordre $\leqslant k$ sommables, alors $(1+\|x\|^2)^{k/2}\hat{f}(x)$ tend vers* 0 *à l'infini, et $\mathscr{F}(\partial_{\mathbf{L}} f) = (2i\pi x)_{\mathbf{L}}\hat{f}$ si $\boldsymbol{\ell} \in \mathbf{N}^m$*

5. Soit $\mathrm{P} = \sum_{\boldsymbol{\ell}} a_{\boldsymbol{\ell}} \mathrm{X}^{\boldsymbol{\ell}} \in \mathbf{C}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$, et soit $\mathrm{P}(\partial)$ l'opérateur différentiel $\sum_{\boldsymbol{\ell}} a_{\boldsymbol{\ell}} \partial^{\boldsymbol{\ell}}$. Si on cherche à résoudre l'équation aux dérivées partielles $\mathrm{P}(\partial)u = \phi$, où ϕ est donnée, et supposée suffisamment sympathique, on peut appliquer formellement la transformée de Fourier aux deux membres, pour obtenir $\mathrm{P}(2i\pi\, x)\hat{u}(x) = \hat{\phi}(x)$. En appliquant la formule d'inversion de Fourier, cela nous donne $u = \overline{\mathscr{F}}\big(\frac{\hat{\phi}(x)}{\mathrm{P}(2i\pi\, x)}\big)$. Ce qui précède est un jeu d'écriture purement formel, mais donne des résultats utilisables dans de nombreux cas provenant de problèmes physiques. Cette méthode de résolution d'équations aux dérivées partielles acquiert une efficacité maximale dans le cadre de la théorie des distributions.

vérifie[6] $|\boldsymbol{\ell}| \leqslant k$.

(ii) *Si* $(1+\|t\|^2)^{k/2} f(t)$ *est sommable,* $\hat{f}$ *est de classe* $\mathscr{C}^k$, *et* $\partial_{\boldsymbol{\ell}} \hat{f}(x) = (-2i\pi)^{|\boldsymbol{\ell}|} \mathscr{F}(t_{\boldsymbol{\ell}} f)$, *si* $|\boldsymbol{\ell}| \leqslant k$.

Démonstration. — Si $f \in \mathscr{C}_c^k(\mathbf{R}^m)$, la formule $\mathscr{F}(\partial_{\boldsymbol{\ell}} f) = (2i\pi x)_{\boldsymbol{\ell}} \hat{f}$ s'obtient en intégrant par partie (on intègre $\partial_{\boldsymbol{\ell}} f$ et on dérive $e^{-2i\pi\, x\cdot t}$). Par exemple, si $f \in \mathscr{C}_c^1(\mathbf{R}^2)$, on déduit du théorème de Fubini, que

$$\widehat{\partial_1 f}(x_1, x_2) = \int_{\mathbf{R}^2} e^{-2i\pi(x_1 t_1 + x_2 t_2)} \frac{\partial f}{\partial t_1}(t_1, t_2)\, dt_1\, dt_2 = \int_{\mathbf{R}} e^{-2i\pi x_2 t_2} \Big(\int_{\mathbf{R}} e^{-2i\pi x_1 t_1} \frac{\partial f}{\partial t_1}(t_1, t_2)\, dt_1 \Big)\, dt_2.$$

Une intégration par partie dans l'intégrale entre parenthèses nous donne

$$\int_{\mathbf{R}} e^{-2i\pi x_1 t_1} \frac{\partial f}{\partial t_1}(t_1, t_2)\, dt_1 = \big[e^{-2i\pi x_1 t_1} f(t_1, t_2) \big]_{t_1=-\infty}^{+\infty} + 2i\pi\, x_1 \int_{\mathbf{R}} e^{-2i\pi x_1 t_1} f(t_1, t_2)\, dt_1,$$

et comme f est à support compact, le premier terme du second membre est nul. On réinjecte alors le second terme dans l'intégrale double, et on réutilise le théorème de Fubini, pour obtenir

$$\begin{aligned} \widehat{\partial_1 f}(x_1, x_2) &= \int_{\mathbf{R}} e^{-2i\pi x_2 t_2} \Big(2i\pi\, x_1 \int_{\mathbf{R}} e^{-2i\pi x_1 t_1} f(t_1, t_2)\, dt_1 \Big)\, dt_2 \\ &= 2i\pi\, x_1 \int_{\mathbf{R}^2} e^{-2i\pi(x_1 t_1 + x_2 t_2)} f(t_1, t_2)\, dt_1\, dt_2 = 2i\pi x_1\, \hat{f}(x_1, x_2). \end{aligned}$$

Le cas général se traite, par récurrence, de la même manière.

Pour traiter le cas f général, choisissons $\phi \in \mathscr{C}_c^k(\mathbf{R}^m)$ valant 1 sur $[-1, 1]^m$, et définissons f_j par $f_j(x) = f(x)\phi(2^{-j}x)$, si $j \in \mathbf{N}$. Alors $f_j \in \mathscr{C}_c^k(\mathbf{R}^m)$ et un petit calcul utilisant la formule de Leibnitz pour la dérivée d'un produit montre que $\partial_{\boldsymbol{\ell}} f_j$ tend simplement vers $\partial_{\boldsymbol{\ell}} f$ et que $\partial_{\boldsymbol{\ell}} f_j$ est majorée par une somme de dérivées $\mathbf{k}$-ièmes de f, avec $|\mathbf{k}| \leqslant |\boldsymbol{\ell}|$, ce qui implique que $\partial_{\boldsymbol{\ell}} f_j$ tend vers $\partial_{\boldsymbol{\ell}} f$ dans $\mathrm{L}^1(\mathbf{R}^m)$. Ceci permet de déduire l'identité $\mathscr{F}(\partial_{\boldsymbol{\ell}} f) = (2i\pi x)_{\boldsymbol{\ell}} \hat{f}$ par passage à la limite (en utilisant la continuité de $\phi \mapsto \hat{\phi}(x)$ qui découle de la continuité de $\phi \mapsto \hat{\phi}$ de $\mathrm{L}^1(\mathbf{R}^m)$ dans $\mathscr{C}_0(\mathbf{R}^m)$). On en déduit le (i) car $\mathscr{F}(\partial_{\boldsymbol{\ell}} f)$ tendant vers 0 à l'infini quel que soit $\boldsymbol{\ell} \in \mathbf{N}^m$ vérifiant $|\boldsymbol{\ell}| \leqslant k$, il en est de même de $|x|_{\boldsymbol{\ell}} \hat{f}$, et donc aussi de $|(1 + \|x\|^2)^{k/2} \hat{f}(x)|$ car $(1 + \|x\|^2)^{k/2} \leqslant (1 + \sum_{j=1}^m |x_j|)^k$.

Le (ii) est, quant à lui, une simple application du théorème de dérivation sous le signe somme, une fois que l'on a remarqué que $\partial_{\boldsymbol{\ell}} \big(e^{-2i\pi\, x\cdot t} \big) = (-2i\pi t)_{\boldsymbol{\ell}} e^{-2i\pi\, x\cdot t}$.

IV.3. Formules d'inversion

1. Séries de Fourier

Une fonction $f : \mathbf{R} \to \mathbf{C}$ est *périodique de période* 1, si $f(x+1) = f(x)$, pour tout $x \in \mathbf{R}$. On a alors $f(x + n) = f(x)$ pour tous $x \in \mathbf{R}$ et $n \in \mathbf{Z}$, et donc f est périodique de période $\mathbf{Z}$.

6. On rappelle que $(2i\pi\, x)^{\boldsymbol{\ell}} = \prod_{j=1}^m (2i\pi\, x_j)^{\ell_j}$, si $x = (x_1, \ldots, x_m)$ et $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_m)$.

On peut aussi (et c'est souvent nettement plus agréable) voir une fonction périodique de période 1 comme une fonction de $\mathbf{T} = \mathbf{R}/\mathbf{Z}$ dans $\mathbf{C}$. Le passage d'un point de vue à l'autre se fait de la manière suivante, en notant $\pi : \mathbf{R} \to \mathbf{T}$ l'application envoyant $x \in \mathbf{R}$ sur sa classe modulo $\mathbf{Z}$: si f est une fonction sur $\mathbf{T}$, alors $f \circ \pi : \mathbf{R} \to \mathbf{C}$ est une fonction périodique de période 1, et réciproquement, si $g : \mathbf{R} \to \mathbf{C}$ est périodique de période 1, alors il existe $f : \mathbf{T} \to \mathbf{C}$ unique, telle que $g = f \circ \pi$.

$\mathbf{T}$ est muni de la topologie quotient, ce qui signifie que $f : \mathbf{T} \to \mathbf{C}$ est continue si et seulement si $f \circ \pi : \mathbf{R} \to \mathbf{C}$ est continue. L'espace $\mathscr{C}(\mathbf{T})$ des fonctions continues sur $\mathbf{T}$ s'identifie donc à l'espace des fonctions continues sur $\mathbf{R}$, périodiques de période 1.

$\mathbf{T}$ est un groupe (quotient du groupe commutatif $(\mathbf{R}, +)$ par son sous-groupe $\mathbf{Z}$), et, par construction, $\pi : \mathbf{R} \to \mathbf{T}$ est un morphisme de groupes dont le noyau est $\mathbf{Z}$. Si $n \in \mathbf{Z}$, alors $t \mapsto e^{2i\pi\, nt}$ est un caractère continu de $\mathbf{R}$ dont le noyau contient $\mathbf{Z}$, et donc est un caractère continu de $\mathbf{T}$ en vertu de notre identification entre les fonctions périodiques de période 1 et les fonctions sur $\mathbf{T}$. On note χ_n le caractère $t \mapsto e^{2i\pi\, nt}$ de $\mathbf{T}$, si $n \in \mathbf{N}$.

Proposition IV.3.1. — *Les caractères linéaires continus de* $\mathbf{T}$ *sont les* χ_n*, pour* $n \in \mathbf{Z}$*.*

Démonstration. — Si $\chi : \mathbf{T} \to \mathbf{C}^*$ est un caractère linéaire continu, alors $\psi = \chi \circ \pi$ est un caractère continue de $\mathbf{R}$, périodique de période 1. D'après la prop. IV.2.1 , il existe $\lambda \in \mathbf{C}$ tel que $\psi(t) = e^{\lambda t}$, pour tout $t \in \mathbf{R}$. La périodicité de ψ équivaut alors à $\psi(1) = \psi(0) = 1$, ce qui montre que λ doit être de la forme $2i\pi\, n$, avec $n \in \mathbf{Z}$. Ceci permet de conclure.

Si $a \in \mathbf{R}$, tout élément t de $\mathbf{R}$ peut s'écrire de manière unique sous la forme $t = x + n$, avec $x \in [a, a+1[$ et $n \in \mathbf{Z}$. Autrement dit, l'intervalle $[a, a+1[$ est un système de représentants de $\mathbf{R}$ modulo $\mathbf{Z}$, pour tout $a \in \mathbf{R}$. On en déduit que l'application ι_a, qui à une fonction f sur $\mathbf{T}$ associe sa restriction (plus précisément, la restriction de $f \circ \pi$) à $[a, a+1[$, est un isomorphisme de l'espace des fonctions sur $\mathbf{T}$ sur celui des fonctions sur $[a, a+1[$. On va utiliser ces isomorphismes pour définir un certain nombre d'espaces de fonctions sur $\mathbf{T}$.

On vérifie facilement, en utilisant l'invariance de l'intégrale de Lebesgue par translation, que les définitions suivantes, pour $f : \mathbf{T} \to \mathbf{C}$, ne dépendent pas du choix de $a \in \mathbf{R}$:

f est dite nulle p.p., si $\iota_a(f)$ est nulle p.p.,

f est dite sommable, si $\iota_a(f)$ est sommable ; si f est sommable, on définit $\int_{\mathbf{T}} f$ par $\int_{\mathbf{T}} f = \int_a^{a+1} f(t)\, dt$, et $\|f\|_1$ par $\|f\|_1 = \int_{\mathbf{T}} |f|$.

f est dite de carré sommable, si $\iota_a(f)$ est de carré sommable ; si f est de carré sommable, on pose $\|f\|_2 = (\int_{\mathbf{T}} |f|^2)^{1/2}$, et si f, g sont de carrés sommables, on définit leur produit scalaire $\langle f, g\rangle$ par la formule $\langle f, g\rangle = \int_{\mathbf{T}} \overline{f}\, g$.

On note, $\mathscr{L}^1(\mathbf{T})$ (resp. $\mathscr{L}^2(\mathbf{T})$) l'espace des fonctions sommables (resp. de carré sommable), et $\mathrm{L}^1(\mathbf{T})$ (resp. $\mathrm{L}^2(\mathbf{T})$) son quotient par l'espace des fonctions nulles p.p. Par définition, ces espaces sont isométriques (via ι_a) aux espaces $\mathscr{L}^1([a, a+1[)$, $\mathscr{L}^2([a, a+1[)$,

$\mathrm{L}^1([a,a+1[)$ et $\mathrm{L}^2([a,a+1[)$ respectivement. Comme $[a,a+1[$ est de volume fini, on a $\mathrm{L}^2(\mathbf{T}) \subset \mathrm{L}^1(\mathbf{T})$.

On définit $\mathrm{Esc}(\mathbf{T})$ comme l'image inverse de $\mathrm{Esc}([0,1[)$ par ι_0 ; si $r \in \mathbf{N}$, et si $k \in \{0,\dots,2^r-1\}$, on note encore $e_{r,k}$ la fonction sur $\mathbf{T}$ dont l'image par ι_0 est $e_{r,k}$. Les $e_{r,k}$, pour $r \in \mathbf{N}$ et $k \in \{0,\dots,2^r-1\}$ forment une famille génératrice de $\mathrm{Esc}(\mathbf{T})$. De plus, $\mathrm{Esc}(\mathbf{T})$ est dense dans $\mathrm{L}^1(\mathbf{T})$ et $\mathrm{L}^2(\mathbf{T})$: en effet, $\mathrm{Esc}(]0,1[)$ est dense dans $\mathrm{L}^1(]0,1[)$ et $\mathrm{L}^2(]0,1[)$ (cf. th. III.2.11).

Soit $\mathrm{Trig}(\mathbf{T})$ l'espace des polynômes trigonométriques (i.e. des combinaisons linéaires des χ_n, pour $n \in \mathbf{Z}$).

Théorème IV.3.2. — (i) $\mathrm{Trig}(\mathbf{T})$ *est dense dans* $\mathrm{L}^2(\mathbf{T})$.

(ii) *Les* χ_n*, pour* $n \in \mathbf{Z}$*, forment une base hilbertienne de* $\mathrm{L}^2(\mathbf{T})$.

Démonstration. — On a

$$\langle \chi_n, \chi_m \rangle = \int_a^{a+1} e^{2i\pi(m-n)t}\,dt = \begin{cases} 1 & \text{si } m=n, \\ \left[\frac{1}{2i\pi(m-n)} e^{2i\pi(m-n)t}\right]_a^{a+1} = 0 & \text{si } m \neq n. \end{cases}$$

Les χ_n forment donc une famille orthonormale, et le (ii) est une conséquence du (i), puisque les χ_n engendrent $\mathrm{Trig}(\mathbf{T})$. La manière standard (cf. ex. II.2.2) pour démontrer la densité de $\mathrm{Trig}(\mathbf{T})$ dans $\mathrm{L}^2(\mathbf{T})$ est de passer par sa densité dans $\mathscr{C}(\mathbf{T})$ (cas particulier du théorème de Stone-Weierstrass). Nous proposons ci-dessous une autre approche, via les fonctions en escalier.

Soit F l'adhérence de $\mathrm{Trig}(\mathbf{T})$ dans $\mathrm{L}^2(\mathbf{T})$. Le lemme IV.3.3 ci-dessous montre que $\phi_0 \in \mathrm{F}$, où $\phi_0 \in \mathrm{L}^2(\mathbf{T})$ est définie par $\phi_0(t) = t$, si $t \in [\frac{-1}{2}, \frac{1}{2}[$. Nous allons en déduire que F contient $\mathrm{Esc}(\mathbf{T})$, ce qui permettra de conclure, cet espace étant dense dans $\mathrm{L}^2(\mathbf{T})$.

Soit $\mathrm{T}_a : \mathrm{L}^2(\mathbf{T}) \to \mathrm{L}^2(\mathbf{T})$ définie par $(\mathrm{T}_a(\phi))(t) = \phi(t+a)$. Alors T_a est une isométrie grâce à l'invariance par translation de l'intégration ; en particulier, T_a est continue. Comme $\mathrm{Trig}(\mathbf{T})$ est stable par T_a, il en est de même de F [si $\phi \in \mathrm{F}$, et si $(f_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathrm{Trig}(\mathbf{T})$ tendant vers ϕ dans $\mathrm{L}^2(\mathbf{T})$, alors $(\mathrm{T}_a(f_n))_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathrm{Trig}(\mathbf{T})$ tendant vers $\mathrm{T}_a(\phi)$ dans $\mathrm{L}^2(\mathbf{T})$]. Maintenant, si $r \in \mathbf{N}$, et si $k \in \{0,\dots,2^r-1\}$, on a $e_{r,k} = 2^{-r} - \mathrm{T}_{-\frac{1}{2}-\frac{k}{2^r}}(\phi_0) + \mathrm{T}_{-\frac{1}{2}-\frac{k+1}{2^r}}(\phi_0)$, comme le montre un petit calcul ; on déduit donc de l'appartenance de ϕ_0 et des constantes à F, celle de $e_{r,k}$, pour tous $r \in \mathbf{N}$ et $k \in \{0,\dots,2^r-1\}$. Les $e_{r,k}$ formant une famille génératrice de $\mathrm{Esc}(\mathbf{T})$, cela implique $\mathrm{Esc}(\mathbf{T}) \subset \mathrm{F}$, ce que l'on cherchait à démontrer.

Lemme IV.3.3. — (i) *Si* $t \in]\frac{-1}{2}, \frac{1}{2}[$*, et si* $z = e^{2i\pi t}$*, alors* $\sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{2i\pi n}(z^n - \overline{z}^n) = t$.

(ii) *La série* $\sum_{n\neq 0} \frac{(-1)^{n-1}}{2i\pi n} e^{2i\pi nt}$ *tend vers* ϕ_0 *dans* $\mathrm{L}^2(\mathbf{T})$.

Démonstration. — Si $|a| = 1$ et $a \neq -1$, on a

$$\sum_{n=1}^{\mathrm{N}} \frac{(-1)^{n-1}}{2i\pi\, n} a^n = \frac{a}{2i\pi} \int_0^1 \sum_{n=1}^{\mathrm{N}} (-ua)^{n-1}\,du = \frac{a}{2i\pi} \int_0^1 \frac{1-(-ua)^{\mathrm{N}}}{1+ua}\,du.$$

Comme $|a| = 1$, la suite de fonctions $\frac{1-(-ua)^N}{1+ua}$, pour $N \in \mathbf{N}$, tend simplement vers $\frac{1}{1+ua}$, sur $[0,1[$, et est majorée en module par $\frac{2}{|1+ua|}$, qui est sommable, puisque $a \neq -1$. On peut donc utiliser le théorème de convergence dominée pour intervertir limite et intégrale. On en déduit que la série qui nous intéresse converge vers :

$$\frac{z}{2i\pi}\int_0^1 \frac{du}{1+uz} - \frac{\overline{z}}{2i\pi}\int_0^1 \frac{du}{1+u\overline{z}} = \frac{1}{\pi}\int_0^1 \frac{\sin 2\pi t}{(u+\cos 2\pi t)^2+\sin^2 2\pi t}\,du$$
$$= \frac{1}{\pi}\big[\operatorname{arctg}\frac{u+\cos 2\pi t}{\sin 2\pi t}\big]_0^1 = \frac{1}{\pi}\big(\operatorname{arctg}(\operatorname{cotg}\pi t) - \operatorname{arctg}(\operatorname{cotg} 2\pi t)\big) = t,$$

car $\operatorname{arctg}(\operatorname{cotg} x)$ est égal à $\frac{\pi}{2} - x$, si $0 < x < \pi$ et à $\frac{-\pi}{2} - x$, si $-\pi < x < 0$. Ceci démontre le (i). Maintenant, $\sum_{n\neq 0} \frac{1}{4\pi^2 n^2} < +\infty$, et comme les χ_n forment une famille orthonormale, la série $\sum_{n\neq 0} \frac{(-1)^{n-1}}{2i\pi n}\chi_n$ est, d'après le lemme II.2.4, sommable dans $\mathrm{L}^2(\mathbf{T})$. On note f sa somme. On peut alors extraire (cf. ex. III.2.9) une sous-suite tendant p.p. vers f de la suite de ses sommes partielles. Or le (i) montre que toute sous-suite de ses sommes partielles tend simplement vers ϕ_0 en dehors de $\frac{1}{2}$. On en déduit que $f = \phi_0$ p.p., et donc que la série tend vers ϕ_0 dans $\mathrm{L}^2(\mathbf{T})$. Ceci permet de conclure.

Si $f \in \mathrm{L}^1(\mathbf{T})$, on note $c_n(f) = \langle \chi_n, f\rangle = \int_0^1 e^{-2i\pi nt} f(t)\,dt$ son n-ième *coefficient de Fourier*.

Corollaire IV.3.4. — *Si $f \in \mathrm{L}^2(\mathbf{T})$, alors $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ est sommable, de somme f, dans $\mathrm{L}^2(\mathbf{T})$, et $\|f\|_2 = \big(\sum_{n\in\mathbf{Z}} |c_n(f)|^2\big)^{1/2}$.*

Démonstration. — C'est une simple application du th. II.2.6.

Exercice IV.3.5. — Calculer de deux manières $\|\phi_0\|_2$. En déduire la formule $\zeta(2) = \frac{\pi^2}{6}$.

Proposition IV.3.6. — *Si $f \in \mathscr{C}(\mathbf{T})$, et si $\sum_{n\in\mathbf{Z}} |c_n(f)| < +\infty$, alors $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ tend uniformément vers f. En particulier, $f(t) = \sum_{n\in\mathbf{Z}} c_n(f)e^{2i\pi nt}$, pour tout t.*

Démonstration. — La série $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ converge normalement dans $\mathscr{C}(\mathbf{T})$ (muni de $\|\ \|_\infty$), et la somme g est donc une fonction continue. De plus, comme $\|h\|_2 \leqslant \|h\|_\infty$, la série $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ converge vers g aussi dans $\mathrm{L}^2(\mathbf{T})$. Par ailleurs, il résulte du cor. IV.3.4 que la série converge aussi vers f dans $\mathrm{L}^2(\mathbf{T})$, et donc que $f = g$ dans $\mathrm{L}^2(\mathbf{T})$. Ceci se traduit par $\int_0^1 |f(t) - g(t)|^2\,dt = 0$ et, f et g étant continues, cela implique que $f - g$ est identiquement nulle. Ceci permet de conclure.

Remarque IV.3.7. — La condition $\sum_{n\in\mathbf{Z}} |c_n(f)| < +\infty$ est en particulier vérifiée si f est de classe $\mathscr{C}^1$. En effet, si $n \neq 0$, une intégration par partie nous donne

$$c_n(f) = \int_0^1 f(t)e^{-2i\pi nt}\,dt = \frac{1}{2i\pi n}\int_0^1 f'(t)e^{-2i\pi nt}\,dt = \frac{1}{2i\pi n}c_n(f'),$$

et comme $\big(\sum_{n\neq 0}|c_n(f')|^2\big)^{1/2}\leqslant\|f'\|_2$, on a

$$\sum_{n\neq 0}\big|\frac{1}{2i\pi\, n}c_n(f')\big|\leqslant\big(\sum_{n\neq 0}\frac{1}{4\pi^2n^2}\big)^{1/2}\big(\sum_{n\neq 0}|c_n(f')|^2\big)^{1/2}<+\infty.$$

Remarque IV.3.8. — Comme $\mathrm{L}^2([a,a+1[)$ est isométrique à $\mathrm{L}^2(\mathbf{T})$, les χ_n, pour $n\in\mathbf{N}$, forment aussi une base hilbertienne de $\mathrm{L}^2([a,a+1[)$ et donc aussi de $\mathrm{L}^2(]a,a+1[)$ ou $\mathrm{L}^2([a,a+1])$ puisque $[a,a+1[$, $]a,a+1[$ et $[a,a+1]$ ne diffèrent que par des ensembles de mesure nulles. Il est très facile d'en déduire une base hilbertienne de $\mathrm{L}^2(\mathrm{I})$, pour tout intervalle I de longueur finie.

2. Séries de Fourier multidimensionnelles

L'étude des séries de Fourier en dimension m se ramène de manière assez formelle [7] à celle des séries de Fourier en dimension 1.

2.1. *Le cas du réseau* $\mathbf{Z}^m$

Une fonction $f:\mathbf{R}^m\to\mathbf{C}$ est *périodique de période* $\mathbf{Z}^m$, si $f(x+\omega)=f(x)$, pour tous $x\in\mathbf{R}^m$ et $\omega\in\mathbf{Z}^m$. Pour que ceci soit le cas, il suffit que l'on ait $f(x+e_j)=f(x)$, pour tout $x\in\mathbf{R}^m$, et tout $j\in\{1,\dots,m\}$, où $e_1,\dots,e_m$ est la base canonique de $\mathbf{R}^m$.

Comme en dimension 1, on voit une fonction périodique de période $\mathbf{Z}^m$ comme une fonction du groupe $\mathbf{T}^m=(\mathbf{R}/\mathbf{Z})^m=\mathbf{R}^m/\mathbf{Z}^m$ dans $\mathbf{C}$, et l'espace $\mathscr{C}(\mathbf{T}^m)$ des fonctions continues sur $\mathbf{T}^m$ s'identifie à l'espace des fonctions continues sur $\mathbf{R}^m$, périodiques de période $\mathbf{Z}^m$.

Si $\mathbf{n}=(n_1,\dots,n_m)\in\mathbf{Z}^m$, on note $\chi_{\mathbf{n}}$ le caractère de $\mathbf{T}^m$ défini par $\chi_{\mathbf{n}}(t)=e^{2i\pi\,\mathbf{n}\cdot t}$.

Proposition IV.3.9. — *Les caractères linéaires continus de* $\mathbf{T}^m$ *sont les* $\chi_{\mathbf{n}}$, *pour* $\mathbf{n}\in\mathbf{Z}^m$.

Démonstration. — Si $\chi:\mathbf{T}^m\to\mathbf{C}^*$ est un caractère linéaire continu, la restriction de χ à $\mathbf{R}e_j$ est un caractère linéaire continu, périodique de période $\mathbf{Z}$, et donc, d'après la prop. IV.3.1, de la forme $t_j\mapsto e^{2i\pi\,n_jt_j}$. Comme $t=\sum_{j=1}^m t_je_j$, et comme χ est un caractère, on a $\chi(t)=\prod_{j=1}^m e^{2i\pi\,n_jt_j}=e^{2i\pi\,\mathbf{n}\cdot t}$, où $\mathbf{n}=(n_1,\dots,n_m)$. Ceci permet de conclure.

Comme en dimension 1, si $a=(a_1,\dots,a_m)\in\mathbf{R}^m$, et si $\mathrm{X}_a=\prod_{j=1}^m[a_j,a_j+1[$, l'application ι_a, qui à une fonction f sur $\mathbf{T}^m$ associe la restriction de f à X_a, est un isomorphisme

7. On peut s'amuser à formaliser le lemme IV.3.11 et son utilisation à grands coups de produits tensoriels et de produits tensoriels complétés. On a vu (ex. I.3.3) que l'espace des fonctions sur $\mathrm{I}\times\mathrm{J}$ est le produit tensoriel des espaces de fonctions sur I et J, si I et J sont finis. Si I et J ne sont pas finis, la situation est plus compliquée, mais certains sous-espaces de fonctions sur $\mathrm{I}\times\mathrm{J}$ sont encore des produits tensoriels d'espaces de fonctions sur I et J. C'est par exemple le cas des polynômes trigonométriques sur $\mathbf{R}^m/\mathbf{Z}^m$ qui sont le produit tensoriel de m copies des polynômes trigonométriques sur $\mathbf{R}/\mathbf{Z}$. L'espace $\mathrm{L}^2(\mathbf{R}^m/\mathbf{Z}^m)$ est, quant-à-lui, obtenu en complétant le produit tensoriel de m copies de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$. Ce procédé de réduction à la dimension est 1 est extrêmement efficace pour beaucoup de questions.

de l'espace des fonctions sur $\mathbf{T}^m$ sur celui des fonctions sur X_a. Ceci permet de définir, comme en dimension 1 :

— des espaces $\mathrm{L}^1(\mathbf{T}^m) \cong \mathrm{L}^1(\mathrm{X}_a)$ et $\mathrm{L}^2(\mathbf{T}^m) \cong \mathrm{L}^2(\mathrm{X}_a)$,

— une intégrale $f \mapsto \int_{\mathbf{T}^m} f = \int_{\mathrm{X}_a} f$ sur $\mathrm{L}^1(\mathbf{T}^m)$,

— une norme $\|f\|_1 = \int_{\mathbf{T}^m} |f|$ sur $\mathrm{L}^1(\mathbf{T}^m)$,

— un produit scalaire $(f,g) \mapsto \langle f,g\rangle = \int_{\mathbf{T}^m} \overline{f}\, g$ sur $\mathrm{L}^2(\mathbf{T}^m)$, et la norme $\|f\|_2 = \langle f,f\rangle^{1/2}$ qui va avec.

L'invariance de l'intégrale de Lebesgue par translation implique que ce qu'on obtient ne dépend pas du choix de $a \in \mathbf{R}^m$ (cf. lemme IV.3.16 pour un énoncé plus général).

On définit $\mathrm{Esc}(\mathbf{T}^m)$ comme l'image inverse de $\mathrm{Esc}([0,1[^m)$ par ι_0 ; si $r \in \mathbf{N}$, et si $\mathbf{k} \in \{0,\dots,2^r-1\}^m$, on note encore $e_{r,\mathbf{k}}$ la fonction sur $\mathbf{T}^m$ dont l'image par ι_0 est $e_{r,\mathbf{k}}$. Les $e_{r,\mathbf{k}}$, pour $r \in \mathbf{N}$ et $\mathbf{k} \in \{0,\dots,2^r-1\}^m$ forment une famille génératrice de $\mathrm{Esc}(\mathbf{T}^m)$.

Soit $\mathrm{Trig}(\mathbf{T}^m)$ l'espace des polynômes trigonométriques sur $\mathbf{T}^m$ (i.e. des combinaisons linéaires des $\chi_{\mathbf{n}}$, pour $\mathbf{n} \in \mathbf{Z}^m$).

Si $f \in \mathrm{L}^1(\mathbf{T}^m)$, on définit ses *coefficients de Fourier* $c_{\mathbf{n}}(f)$, pour $\mathbf{n} \in \mathbf{Z}^m$, par la formule $c_{\mathbf{n}}(f) = \langle \chi_{\mathbf{n}}, f\rangle = \int_{[0,1[^m} e^{-2i\pi\,\mathbf{n}\cdot t} f(t)\,dt$.

Théorème IV.3.10. — (i) $\mathrm{Trig}(\mathbf{T}^m)$ *est dense dans dans* $\mathrm{L}^2(\mathbf{T}^m)$.

(ii) *Les* $\chi_{\mathbf{n}}$*, pour* $\mathbf{n} \in \mathbf{Z}^m$ *forment une base hilbertienne de* $\mathrm{L}^2(\mathbf{T}^m)$.

(iii) *Si* $f \in \mathrm{L}^2(\mathbf{T}^m)$*, alors* $f = \sum_{\mathbf{n}\in\mathbf{Z}^m} c_{\mathbf{n}}(f)\chi_{\mathbf{n}}$ *dans* $\mathrm{L}^2(\mathbf{T}^m)$.

(iv) *Si* $f \in \mathscr{C}(\mathbf{T}^m)$*, et si* $\sum_{\mathbf{n}\in\mathbf{Z}^m} |c_{\mathbf{n}}(f)| < +\infty$*, alors* $f = \sum_{\mathbf{n}\in\mathbf{Z}^m} c_{\mathbf{n}}(f)\chi_{\mathbf{n}}$ *dans* $\mathscr{C}(\mathbf{T}^m)$*, et en particulier,* $f(t) = \sum_{\mathbf{n}\in\mathbf{Z}^m} c_{\mathbf{n}}(f)e^{2i\pi\,\mathbf{n}\cdot t}$ *pour tout* t.

Démonstration. — Nous allons déduire cet énoncé de l'énoncé analogue en dimension 1. Si $\phi_1,\dots,\phi_m$ sont des fonctions de $\mathbf{R}$ dans $\mathbf{C}$, on note $\phi_1 \otimes \cdots \otimes \phi_m$ ou, de manière plus compacte, $\otimes_i \phi_i$, la fonction de $\mathbf{R}^m$ dans $\mathbf{C}$ définie par

$$(\otimes_i \phi_i)(t) = \phi_1 \otimes \cdots \otimes \phi_m(t) = \prod_{i=1}^{m} \phi_i(t_i), \quad \text{si } t = (t_1,\dots,t_m).$$

Par exemple,

$$\chi_{\mathbf{n}} = \otimes_i \chi_{n_i}, \quad \text{si } \mathbf{n} = (n_1,\dots,n_m) \in \mathbf{Z}^m,$$
$$e_{r,\mathbf{k}} = \otimes_i e_{r,k_i}, \quad \text{si } r \in \mathbf{N}, \text{ et si } \mathbf{k} = (k_1,\dots,k_m) \in \mathbf{Z}^m.$$

Lemme IV.3.11. — (i) *Si* $\phi_i = \psi_i$ *p.p., pour tout* i*, alors* $\otimes_i \phi_i = \otimes_i \psi_i$ *p.p.*

(ii) *Si* $\phi_i \in \mathscr{L}^1(\mathbf{T})$ *pour tout* i*, alors* $\otimes_i \phi_i \in \mathscr{L}^1(\mathbf{T}^m)$*, et on a* $\|\otimes_i \phi_i\|_1 = \prod_i \|\phi_i\|_1$.

(iii) *Si* $\phi_i \in \mathscr{L}^2(\mathbf{T})$ *pour tout* i*, alors* $\otimes_i \phi_i \in \mathscr{L}^2(\mathbf{T}^m)$*, et on a* $\|\otimes_i \phi_i\|_2 = \prod_i \|\phi_i\|_2$.

Démonstration. — Soit $\mathrm{A}_i \subset \mathbf{R}$ (resp. $\mathrm{A} \subset \mathbf{R}^m$) l'ensemble des x tels que $\phi_i(x) \neq \psi_i(x)$ (resp. $\otimes_i \phi_i(x) \neq \otimes_i \psi_i(x)$). Alors A est inclus dans la réunion des $\mathrm{A}_i \times \prod_{j\neq i} \mathbf{R}$, qui sont tous de mesure nulle dans $\mathbf{R}^m$, puisque A_i est de mesure nulle dans $\mathbf{R}$ par hypothèse. Cela démontre le (i).

Les (ii) et (iii) sont des conséquences immédiates du théorème de Fubini.

Revenons à la démonstration du th. IV.3.10. Le (i) du lemme précédent montre que l'application $(\phi_1, \dots, \phi_m) \mapsto \otimes_i \phi_i$ passe au quotient (des deux côtés à la fois) modulo les fonctions nulles p.p. Comme cette application est linéaire en chacune des ϕ_i, les (ii) et (iii) montre que l'on obtient ainsi des applications multilinéaires continues $\mathrm{L}^1(\mathbf{T})^m \to \mathrm{L}^1(\mathbf{T}^m)$ et $\mathrm{L}^2(\mathbf{T})^m \to \mathrm{L}^2(\mathbf{T}^m)$.

Pour montrer que $\mathrm{Trig}(\mathbf{T}^m)$ est dense dans $\mathrm{L}^2(\mathbf{T}^m)$, il suffit de montrer que son adhérence contient $\mathrm{Esc}(\mathbf{T}^m)$, et, par linéarité, il suffit de vérifier qu'elle contient les $e_{r,\mathbf{k}}$, pour $r \geqslant 1$ et $\mathbf{k} \in \{0, \dots, 2^r - 1\}^m$. Pour cela, on écrit $e_{r,\mathbf{k}}$ sous la forme $e_{r,\mathbf{k}} = \otimes_i e_{r,k_i}$, et on choisit, pour chaque i, une suite $\mathrm{P}_{i,n}$ d'éléments de $\mathrm{Trig}(\mathbf{T})$ tendant vers e_{r,k_i} dans $\mathrm{L}^2(\mathbf{T})$. Il résulte de la continuité de $(\phi_1, \dots, \phi_m) \mapsto \otimes_i \phi_i$ que $\mathrm{P}_n = \otimes_i \mathrm{P}_{i,n}$ tend vers $e_{r,\mathbf{k}}$ dans $\mathrm{L}^2(\mathbf{T}^m)$, et comme $\mathrm{P}_n \in \mathrm{Trig}(\mathbf{T}^m)$, on en déduit le (i).

On déduit du théorème de Fubini que $\langle \chi_{\mathbf{n}}, \chi_{\boldsymbol{\ell}} \rangle = \prod_{i=1}^m \langle \chi_{n_i}, \chi_{\ell_i} \rangle$, si $\mathbf{n} = (n_1, \dots, n_m)$ et $\boldsymbol{\ell} = (\ell_1, \dots, \ell_m)$, ce qui permet de déduire l'orthonormalité de la famille des $\chi_{\mathbf{n}}$, pour $\mathbf{n} \in \mathbf{Z}^m$, de celle des χ_n, pour $n \in \mathbf{Z}$; le (ii) est donc une conséquence du (i).

Le (iii) est alors une application du th. II.2.6, et le (iv) se déduit du (iii) comme dans la démonstration de la prop. IV.3.6.

Ceci permet de conclure. □

Exercice IV.3.12. — Montrer que, si $k > \frac{m}{2}$, et si f est périodique de période $\mathbf{Z}^m$ et de classe $\mathscr{C}^k$, alors $f(t) = \sum_{\mathbf{n} \in \mathbf{Z}^m} c_{\mathbf{n}}(f) e^{2i\pi\, \mathbf{n} \cdot t}$, pour tout t.

2.2. *Le cas d'un réseau quelconque*

Un *réseau* Λ de $\mathbf{R}^m$ est un sous-groupe de $\mathbf{R}^m$ de la forme $\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_m$, où $(v_1, \dots, v_m)$ est une base de $\mathbf{R}^m$. On dit alors que $(v_1, \dots, v_m)$ est une base de Λ (sous-entendu sur $\mathbf{Z}$). L'exemple le plus simple est le réseau $\mathbf{Z}^m$ dont une base est la base canonique de $\mathbf{R}^m$.

Le *réseau dual* Λ^* de Λ, est l'ensemble des $x \in \mathbf{R}^m$ tels que $x \cdot \omega \in \mathbf{Z}$, pour tout $\omega \in \Lambda$. Le réseau dual de $\mathbf{Z}^m$ est $\mathbf{Z}^m$ de manière évidente. Le cas général est décrit par le lemme suivant.

Lemme IV.3.13. — *Soit $(v_1, \dots, v_m)$ une base de Λ, soit A la matrice dont la j-ième colonne est le vecteur v_j. Alors $\Lambda^* = {}^{\mathrm{t}}\mathrm{A}^{-1}\mathbf{Z}^m$.*

Démonstration. — Le fait que $(v_1, \dots, v_m)$ soit une base de Λ se traduit par $\Lambda = \mathrm{A}\,\mathbf{Z}^m = \{\mathrm{A}\mathbf{n},\ \mathbf{n} \in \mathbf{Z}^m\}$. Or $x \cdot \mathrm{A}\mathbf{n} = {}^{\mathrm{t}}\mathrm{A}x \cdot \mathbf{n}$. Comme le réseau dual de $\mathbf{Z}^m$ est $\mathbf{Z}^m$, on en déduit que $x \in \Lambda^*$, si et seulement si ${}^{\mathrm{t}}\mathrm{A}x \in \mathbf{Z}^m$; autrement dit, on a $\Lambda^* = {}^{\mathrm{t}}\mathrm{A}^{-1}\mathbf{Z}^m$.

Une fonction $f : \mathbf{R}^m \to \mathbf{C}$ est *périodique de période* Λ, si $f(x + \omega) = f(x)$, pour tous $x \in \mathbf{R}^m$ et $\omega \in \Lambda$. Pour que ceci soit le cas, il suffit que l'on ait $f(x + v_j) = f(x)$, pour tout $x \in \mathbf{R}^m$, et tout $j \in \{1, \dots, m\}$, si $(v_1, \dots, v_m)$ est une base Λ.

Comme d'habitude, on voit une fonction périodique de période Λ comme une fonction du groupe $\mathbf{T}(\Lambda) = \mathbf{R}^m/\Lambda$ dans $\mathbf{C}$, et l'espace $\mathscr{C}(\mathbf{T}(\Lambda))$ des fonctions continues sur $\mathbf{T}(\Lambda)$ s'identifie à l'espace des fonctions continues sur $\mathbf{R}^m$, périodiques de période Λ.

Si $\omega \in \Lambda^*$, alors $t \mapsto e^{2i\pi\,\omega\cdot t}$ est un caractère de $\mathbf{R}^m$ dont le noyau contient Λ ; c'est donc un caractère de $\mathbf{T}(\Lambda)$; nous le noterons χ_ω.

Lemme IV.3.14. — *Les caractères linéaires continus de* $\mathbf{T}(\Lambda)$ *sont les* χ_ω*, pour* $\omega \in \Lambda^*$.

Démonstration. — Un caractère de $\mathbf{T}(\Lambda)$ est de la forme $e^{2i\pi\,x\cdot t}$, avec $x \in \mathbf{R}^m$, trivial sur Λ, ce qui équivaut à $x \cdot \omega \in \mathbf{Z}$, pour tout $\omega \in \Lambda$. On en déduit le résultat.

Si Λ est un réseau de $\mathbf{R}^m$, un *domaine fondamental* de $\mathbf{R}^m$ modulo Λ, est un ensemble mesurable $\mathrm{X} \subset \mathbf{R}^m$ tel que tout élément x de $\mathbf{R}^m$ puisse s'écrire de manière unique sous la forme $\omega + a$, avec $a \in \mathrm{X}$ et $\omega \in \Lambda$. Par exemple, si $(v_1, \dots, v_m)$ est une base Λ, alors $\{t_1v_1 + \cdots + t_mv_m,\ 0 \leqslant t_i < 1,\ \text{pour tout } i\}$ est un domaine fondamental modulo Λ.

Soit X un domaine fondamental de $\mathbf{R}^m$ modulo Λ. On note $\mathrm{Vol}(\Lambda)$ la mesure de Lebesgue de X. Le lemme IV.3.16 ci-dessous montre que ceci ne dépend pas du choix de X ; on a donc $\mathrm{Vol}(\Lambda) = |\det(v_1, \dots, v_m)|$, si $(v_1, \dots, v_m)$ est une base de Λ ; en particulier, $\mathrm{Vol}(\mathbf{Z}^m) = 1$.

L'application ι_X, qui à une fonction f sur $\mathbf{T}(\Lambda)$ associe la restriction de f à X, est un isomorphisme de l'espace des fonctions sur $\mathbf{T}(\Lambda)$ sur celui des fonctions sur X. Ceci permet de définir, comme d'habitude,

— des espaces $\mathrm{L}^1(\mathbf{T}(\Lambda)) \cong \mathrm{L}^1(\mathrm{X})$ et $\mathrm{L}^2(\mathbf{T}(\Lambda)) \cong \mathrm{L}^2(\mathrm{X})$,

— une intégrale $f \mapsto \int_{\mathbf{T}(\Lambda)} f = \int_\mathrm{X} f$ sur $\mathrm{L}^1(\mathbf{T}(\Lambda))$,

— une norme $\|f\|_1 = \frac{1}{\mathrm{Vol}(\Lambda)} \int_{\mathbf{T}(\Lambda)} |f|$ sur $\mathrm{L}^1(\mathbf{T}(\Lambda))$,

— un produit scalaire $(f, g) \mapsto \langle f, g\rangle = \frac{1}{\mathrm{Vol}(\Lambda)} \int_{\mathbf{T}(\Lambda)} \overline{f}\, g$ sur $\mathrm{L}^2(\mathbf{T}(\Lambda))$, et la norme $\|f\|_2 = \langle f, f\rangle^{1/2}$ qui va avec.

Le lemme IV.3.16 ci-dessous montre que ce qu'on obtient ne dépend pas du choix de X.

Si $f \in \mathrm{L}^1(\mathbf{T}(\Lambda))$, on définit ses *coefficients de Fourier* $c_\omega(f)$, pour $\omega \in \Lambda^*$, par la formule $c_\omega(f) = \langle \chi_\omega, f\rangle = \frac{1}{\mathrm{Vol}(\Lambda)} \int_\mathrm{X} e^{-2i\pi\,\omega\cdot t} f(t)\, dt$, où X est un domaine fondamental modulo Λ.

Théorème IV.3.15. — (i) *Les* χ_ω*, pour* $\omega \in \Lambda^*$*, forment une base hilbertienne de* $\mathrm{L}^2(\mathbf{T}(\Lambda))$.

(ii) *Si* $f \in \mathrm{L}^2(\mathbf{T}(\Lambda))$*, alors* $f = \sum_{\omega\in\Lambda^*} c_\omega(f)\chi_\omega$ *dans* $\mathrm{L}^2(\mathbf{T}(\Lambda))$.

(iii) *Si* $f \in \mathscr{C}(\mathbf{T}(\Lambda))$*, et si* $\sum_{\omega\in\Lambda^*} |c_\omega(f)| < +\infty$*, alors* $f = \sum_{\omega\in\Lambda^*} c_\omega(f)\chi_\omega$ *dans* $\mathscr{C}(\mathbf{T}(\Lambda))$ *; en particulier,* $f(t) = \sum_{\omega\in\Lambda^*} c_\omega(f) e^{2i\pi\,\omega\cdot t}$ *pour tout* t.

Démonstration. — Soit $(v_1, \dots, v_d)$ une base de Λ, et soit A la matrice dont la j-ième colonne est v_j. Alors $\mathrm{A} \cdot \mathbf{Z}^m = \Lambda$, ce qui fait que $\phi \mapsto \phi \circ \mathrm{A}$ transforme une fonction périodique de période Λ en une fonction périodique de période $\mathbf{Z}^m$. De plus, le facteur $\frac{1}{\mathrm{Vol}(\Lambda)} = \frac{1}{|\det \mathrm{A}|}$ dans la définition du produit scalaire sur $\mathrm{L}^2(\mathbf{T}(\Lambda))$ fait que $\phi \mapsto \phi \circ \mathrm{A}$ est une isométrie de $\mathrm{L}^2(\mathbf{T}(\Lambda))$ sur $\mathrm{L}^2(\mathbf{T}^m)$. Ceci permet, en remarquant que $\chi_\omega(\mathrm{A}t) = \chi_\mathbf{n}(t)$

si $\omega = {}^{\mathrm{t}}\mathrm{A}^{-1}\mathbf{n} \in \Lambda^*$ (cf. lemme IV.3.13), de déduire le théorème ci-dessus du résultat pour $\mathbf{Z}^m$.

Lemme IV.3.16. — *Si $f : \mathbf{T}(\Lambda) \to \mathbf{R}_+$ est mesurable, alors $\int_{\mathrm{X}} f$ ne dépend pas du choix du domaine fondamental* X *modulo* Λ.

Démonstration. — Le fait pour X d'être un domaine fondamental modulo Λ peut se réécrire sous la forme $\sum_{\omega\in\Lambda} \mathbf{1}_{\omega+\mathrm{X}} = 1$, où $\omega + \mathrm{X} = \{\omega + a,\ a \in \mathrm{X}\}$.

Soient $\mathrm{X}_1, \mathrm{X}_2$ des domaines fondamentaux modulo Λ. En utilisant successivement :
– l'identité $1 = \sum_{\omega\in\Lambda} \mathbf{1}_{\omega+\mathrm{X}_2}$,
– le théorème de convergence monotone pour échanger somme et intégrale,
– le changement de variable $x = \omega + t$ et l'invariance de f par ce changement de variable,
– de nouveau le théorème de convergence monotone,
– l'identité $\sum_{\omega\in\Lambda} \mathbf{1}_{-\omega+\mathrm{X}_1} = 1$,
on obtient

$$\begin{aligned}\int_{\mathrm{X}_1} f = \int \mathbf{1}_{\mathrm{X}_1} f = \int \big(\sum_{\omega\in\Lambda} \mathbf{1}_{\omega+\mathrm{X}_2}\big)\mathbf{1}_{\mathrm{X}_1} f = \sum_{\omega\in\Lambda} \int \mathbf{1}_{\omega+\mathrm{X}_2}\mathbf{1}_{\mathrm{X}_1} f \\ = \sum_{\omega\in\Lambda} \int \mathbf{1}_{\mathrm{X}_2}\mathbf{1}_{-\omega+\mathrm{X}_1} f = \int \big(\sum_{\omega\in\Lambda} \mathbf{1}_{-\omega+\mathrm{X}_1}\big)\mathbf{1}_{\mathrm{X}_2} f = \int \mathbf{1}_{\mathrm{X}_2} f = \int_{\mathrm{X}_2} f,\end{aligned}$$

ce qui permet de conclure.

3. La formule de Poisson

On note $\mathscr{S}(\mathbf{R}^m)$ *l'espace de Schwartz* des fonctions de classe $\mathscr{C}^\infty$ sur $\mathbf{R}^m$, qui sont *à décroissance rapide à l'infini* ainsi que toutes leur dérivées. (g est *à décroissance rapide à l'infini*, si $(1+\|t\|^2)^{\mathrm{N}} g(t)$ est bornée sur $\mathbf{R}^m$, quel que soit $\mathrm{N} \in \mathbf{N}$.) On déduit du th. IV.2.8 le résultat suivant.

Corollaire IV.3.17. — *L'image de $\mathscr{S}(\mathbf{R}^m)$ par la transformée de Fourier est incluse dans $\mathscr{S}(\mathbf{R}^m)$.*

Théorème IV.3.18. — (Formule de Poisson, 1816) *Si $f \in \mathscr{S}(\mathbf{R})$ ou, plus généralement, si f est de classe $\mathscr{C}^1$, et si f et f' sont des $\mathrm{O}(|t|^{-2})$ au voisinage de $\pm\infty$, alors*

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{n\in\mathbf{Z}} \hat{f}(n).$$

Démonstration. — Soit $\mathrm{F}(t) = \sum_{n\in\mathbf{Z}} f(n+t)$. La série converge pour tout t grâce à l'hypothèse $f = \mathrm{O}(|t|^{-2})$, et la fonction F est périodique de période 1. De plus, sur $[0,1]$, la série des $f'(n+t)$ converge normalement, grâce à l'hypothèse $f' = \mathrm{O}(|t|^{-2})$, ce qui implique que $\mathrm{F} \in \mathscr{C}^1(\mathbf{T})$. On en déduit, en utilisant la rem. IV.3.7, que F est somme de

sa série de Fourier en tout point. Or, si $k \in \mathbf{Z}$, on a (l'interversion de l'intégrale et de la série ci-dessous est justifiée par la convergence uniforme sur $[0,1]$) :

$$c_k(\mathrm{F}) = \int_0^1 e^{-2i\pi\, kt}\mathrm{F}(t)\, dt = \int_0^1 e^{-2i\pi\, kt}\big(\sum_{n\in\mathbf{Z}} f(n+t)\big)\, dt = \sum_{n\in\mathbf{Z}} \int_0^1 e^{-2i\pi\, kt} f(n+t)\, dt$$
$$= \sum_{n\in\mathbf{Z}} \int_n^{n+1} e^{-2i\pi\, kt} f(t)\, dt = \int_{-\infty}^{+\infty} e^{-2i\pi\, kt} f(t)\, dt = \hat{f}(k).$$

On en déduit la formule du théorème en comparant la série donnant $\mathrm{F}(0)$ avec la série de Fourier de F en 0.

On démontre de même, en dimension quelconque, le résultat suivant.

Théorème IV.3.19. — (Formule de Poisson dans $\mathbf{R}^m$) *Si $f \in \mathscr{S}(\mathbf{R}^m)$, et si Λ est un réseau de $\mathbf{R}^m$, alors*

$$\sum_{\omega\in\Lambda} f(\omega) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\omega\in\Lambda^*} \hat{f}(\omega).$$

Exercice IV.3.20. — Comparer ce que donnent la formule du th. IV.3.18 et celle du th. IV.3.19 pour évaluer $\sum_{n\in\mathbf{Z}} f(\lambda n)$, avec $\lambda \in \mathbf{R}^*$.

4. La formule d'inversion de Fourier dans $\mathscr{S}$

Théorème IV.3.21. — *Si $\varphi \in \mathscr{S}(\mathbf{R}^m)$, alors $\overline{\mathscr{F}}\mathscr{F}\varphi = \varphi$ et $\mathscr{F}\overline{\mathscr{F}}\varphi = \varphi$.*

Remarque IV.3.22. — Comme $\overline{\mathscr{F}}\varphi(x) = \mathscr{F}\varphi(-x)$, on peut réécrire l'égalité $\overline{\mathscr{F}}\mathscr{F}\varphi = \varphi$ sous la forme $(\mathscr{F}\circ\mathscr{F}\varphi)(x) = \varphi(-x)$ ou encore $\widehat{\widehat{\varphi}}(x) = \varphi(-x)$.

Démonstration. — Comme on passe de $\mathscr{F}$ à $\overline{\mathscr{F}}$ en changeant x en $-x$, il suffit de démontrer une des deux formules ; nous démontrerons la première. Soient $u \in \mathbf{R}^m$ et $r \in \mathbf{N}$. Si on applique la formule de Poisson à la fonction $f(t) = \varphi(u + 2^r t)$ et au réseau $\Lambda = \mathbf{Z}^m$ (et donc $\Lambda^* = \mathbf{Z}^m$), on obtient la formule suivante (où l'on a utilisé l'identité $\hat{f}(x) = 2^{-rm} e^{2i\pi u\cdot 2^{-r}x}\hat{\varphi}(2^{-r}x)$, conséquence des formules pour les dilations-translations) :

$$\sum_{\mathbf{k}\in\mathbf{Z}^m} \varphi(u + 2^r\mathbf{k}) = 2^{-rm} \sum_{\mathbf{k}\in\mathbf{Z}^m} e^{2i\pi u\cdot 2^{-r}\mathbf{k}}\hat{\varphi}(2^{-r}\mathbf{k}).$$

Nous allons montrer que, quand $r \to +\infty$, le membre de gauche tend vers $\varphi(u)$ et le membre de droite vers $\overline{\mathscr{F}}\hat{\varphi}(u)$, ce qui permettra de conclure.

• On commence par remarquer que, comme φ tend vers 0 à l'infini, on a $\varphi(u+2^r\mathbf{k}) \to 0$ si $\mathbf{k} \neq 0$, et $\varphi(u + 2^r\mathbf{k}) = \varphi(u)$ si $\mathbf{k} = 0$; pour prouver que le membre de gauche tend vers $\varphi(u)$, il n'y a donc qu'à justifier l'interversion de la somme et de la limite. La décroissance rapide de φ à l'infini implique en particulier l'existence de C tel que $|\varphi(t)| \leqslant \mathrm{C}(1+\|t\|^2)^{-(m+1)/2}$ pour tout $t \in \mathbf{R}^m$. Or $\sum_{\mathbf{k}\in\mathbf{Z}^m}(1+a\|\mathbf{k}\|^2)^{-(m+1)/2} < +\infty$ pour tout $a > 0$ (cf. n° 15.2 du Vocabulaire), et, si $2^r \geqslant 2\|u\|$, on a $\|u + 2^r\mathbf{k}\| \geqslant a\,\|\mathbf{k}\|$, avec $a = \|u\|$, pour tout $\mathbf{k} \in \mathbf{Z}^m$. La série de terme général $\mathrm{C}(1 + a\|\mathbf{k}\|^2)^{-(m+1)/2}$ est donc un

majorant sommable, pour tout r assez grand, de la série de terme général $\varphi(u+2^r\mathbf{k})$. On conclut en utilisant le théorème de convergence dominée pour les séries.

• Passons à l'étude de la série dans le membre de droite. Le procédé habituel transformant une somme en intégrale d'une fonction en escalier montre que cette série est égale à $\int \psi_r$, où ψ_r est la fonction définie par

$$\psi_r = \sum_{\mathbf{k}\in\mathbf{Z}^m} \psi(2^{-r}\mathbf{k})e_{r,\mathbf{k}}, \quad \text{et } \psi(x) = e^{2i\pi u\cdot x}\hat{\varphi}(x).$$

Maintenant, si $t=(t_1,\dots,t_m)$, alors $\psi_r(t)=\psi(t^{(r)})$, où $t_i^{(r)} = 2^{-r}[2^r t_i] \in [t_i-2^{-r}, t_i]$. En particulier, $t^{(r)}\to t$, et ψ étant continue, on a $\psi_r(t)\to\psi(t)$, pour tout $t\in\mathbf{R}^m$. De plus, si $\mathrm{C}(t)$ désigne le cube $\prod_{i=1}^m [t_i-1,t_i]$, on a $t^{(r)}\in\mathrm{C}(t)$, pour tout $r\in\mathbf{N}$. La fonction ψ_r est donc majorée, pour tout $r\in\mathbf{N}$, par g, où $g(t)=\sup_{u\in\mathrm{C}(t)}|\psi(t)| = \sup_{u\in\mathrm{C}(t)}|\hat{\varphi}(t)|$. Enfin, comme $\hat{\varphi}$ est à décroissance rapide à l'infini, il en est de même de g qui est, de ce fait, sommable, ce qui permet d'utiliser le théorème de convergence dominée pour en déduire que $\int\psi_r\to\int\psi$. Comme $\int\psi = \overline{\mathscr{F}}\hat{\varphi}(u)$, cela permet de conclure.

Corollaire IV.3.23. — *$\mathscr{F}$ et $\overline{\mathscr{F}}$ sont des isomorphismes de $\mathscr{S}(\mathbf{R}^m)$ dans $\mathscr{S}(\mathbf{R}^m)$, inverses*[8] *l'un de l'autre.*

5. Formules d'inversion dans L^1

Proposition IV.3.24. — *Si $f,g\in\mathrm{L}^1(\mathbf{R}^m)$, alors*

$$\int_{\mathbf{R}^m} g\ \mathscr{F}f = \int_{\mathbf{R}^m} f\ \mathscr{F}g \quad \text{et} \quad \int_{\mathbf{R}^m} g\ \overline{\mathscr{F}}f = \int_{\mathbf{R}^m} f\ \overline{\mathscr{F}}g.$$

Démonstration. — Remarquons que les deux membres sont bien définis car $\hat{f}$ et $\hat{g}$ sont bornées puisqu'éléments de $\mathscr{C}_0(\mathbf{R}^m)$. Soit $h(x,t)=g(x)f(t)e^{-2i\pi\, x\cdot t}$. Alors h est sommable sur $\mathbf{R}^m\times\mathbf{R}^m$, car d'après le théorème de Fubini pour les fonctions positives, on a

$$\begin{aligned}\int_{\mathbf{R}^m\times\mathbf{R}^m} |h(x,t)|\,dx\,dt &= \int_{\mathbf{R}^m\times\mathbf{R}^m} |f(t)||g(x)|\,dx\,dt = \int_{\mathbf{R}^m}\Big(\int_{\mathbf{R}^m}|f(t)||g(x)|\,dx\Big)\,dt\\ &= \int_{\mathbf{R}^m}\|g\|_1|f(t)|\,dt = \|g\|_1\|f\|_1 < +\infty.\end{aligned}$$

Une application immédiate du théorème de Fubini montre alors que les deux membres sont égaux à $\int_{\mathbf{R}^m\times\mathbf{R}^m} h(x,t)\,dx\,dt$, ce qui permet de conclure.

Proposition IV.3.25. — *Si $h\in\mathrm{L}^1(\mathbf{R}^m)$ a une transformée de Fourier sommable, alors $\overline{\mathscr{F}}\mathscr{F}h = h$ p.p.*

8. Ce résultat, combiné avec la formule de la prop. IV.3.24, est à la base de la définition de la transformée de Fourier d'une distribution.

Démonstration. — Soit $\varphi \in \mathscr{C}_c^\infty(\mathbf{R}^m)$. Alors $\mathscr{F}\overline{\mathscr{F}}\varphi = \varphi$ d'après le th. IV.3.21. Par ailleurs, en appliquant la prop. IV.3.24 successivement à $f = \mathscr{F}h$ et $g = \varphi$, puis à $f = h$ et $g = \overline{\mathscr{F}}\varphi$ (ce qui est licite car h et $\mathscr{F}h$ sont dans $\mathrm{L}^1(\mathbf{R}^m)$ par hypothèse, et φ et $\overline{\mathscr{F}}\varphi$ sont dans $\mathscr{S}(\mathbf{R}^m)$ qui est inclus dans $\mathrm{L}^1(\mathbf{R}^m)$), on obtient :

$$\int_{\mathbf{R}^m} \overline{\mathscr{F}}\mathscr{F}h\ \varphi = \int_{\mathbf{R}^m} \mathscr{F}h\ \overline{\mathscr{F}}\varphi = \int_{\mathbf{R}^m} h\ \mathscr{F}\overline{\mathscr{F}}\varphi = \int_{\mathbf{R}^m} h\ \varphi.$$

La fonction $\overline{\mathscr{F}}\mathscr{F}h$ n'est pas a priori dans $\mathrm{L}^1(\mathbf{R}^m)$ mais, comme elle est continue, sa restriction à tout ouvert borné X est dans $\mathrm{L}^1(\mathrm{X})$. Or $\int_{\mathrm{X}}(\overline{\mathscr{F}}\mathscr{F}h - h)\,\varphi = 0$ pour tout $\varphi \in \mathscr{C}_c^\infty(\mathrm{X})$, d'après ce qui précède, et le cor. III.2.13 permet d'en déduire la nullité (presque partout) de $\overline{\mathscr{F}}\mathscr{F}h - h$, sur tout ouvert borné X. Ceci permet de conclure.

On trouvera une autre démonstration sous forme d'exercice (utilisant la convolution introduite dans les ex. III.3.12 et III.3.13) ci-dessous, et encore une autre en passant par la transformée de Fourier dans L^2 au n° 3 du § IV.4.

Exercice IV.3.26. — (Formule d'inversion)

(i) Soit $h : \mathbf{R} \to \mathbf{R}$ définie par $h(t) = e^{-|t|}$, et, si $\varepsilon > 0$, soit $h_\varepsilon(t) = h(\varepsilon t)$. Soit $\delta(x) = \hat{h}(-x)$.

(a) Calculer $\delta(x)$ et vérifier que $\int_{\mathbf{R}} \delta = 1$ et que $\hat{h}_\varepsilon(-x) = \delta_\varepsilon(x)$, avec $\delta_\varepsilon(x) = \frac{1}{\varepsilon}\delta(x/\varepsilon)$.

(b) Soit $f \in \mathrm{L}^1(\mathbf{R})$. Montrer que $\|f * \delta_\varepsilon - f\|_{\mathrm{L}^1} \to_{\varepsilon\to 0} 0$. (Commencer par f en escalier.)

(c) En déduire qu'il existe une suite $(\varepsilon_n)_{n\in\mathbf{N}}$, tendant vers 0, telle que $f * \delta_{\varepsilon_n}(x) \to f(x)$ pour presque tout $x \in \mathbf{R}$.

(d) Montrer que $(f * \delta_\varepsilon)(x) = \int_{\mathbf{R}} h(\varepsilon t)\hat{f}(t)e^{2i\pi\, tx}\, dt$.

(ii) On suppose de plus que $\hat{f} \in \mathrm{L}^1(\mathbf{R})$. On pose $g(x) = \int_{\mathbf{R}} \hat{f}(t)e^{2i\pi\, tx}\, dt$. Vérifier que g est continue, bornée, que $\int_{\mathbf{R}} h(\varepsilon t)\hat{f}(t)e^{2i\pi\, tx}\ dt \to g(x)$, quand $\varepsilon \to 0$, quel que soit $x \in \mathbf{R}$. En déduire que $f(x) = g(x)$, pour presque tout $x \in \mathbf{R}$.

6. Exercices

Exercice IV.3.27. — Soit $f : \mathbf{R} \to \mathbf{C}$ définie par $f(t) = \frac{1}{(t+i)^3}$.

(i) Montrer que $\hat{f}$ est définie, de classe $\mathscr{C}^1$, et que $|t^{\mathrm{N}}\hat{f}(t)| \to 0$ quand $|t| \to +\infty$, pour tout $\mathrm{N} \in \mathbf{N}$.

(ii) Soit $g : \mathbf{R} \to \mathbf{C}$ définie par $g(t) = e^{-2\pi t}$, si $t > 0$, et $g(t) = 0$, si $t \leqslant 0$. Calculer $\hat{g}$; en déduire la transformée de Fourier de $h(t) = t^2 g(t)$, puis $\hat{f}$.

(iii) Montrer que la série $\sum_{n\in\mathbf{Z}} \frac{1}{(n+i)^3}$ est absolument convergente, et calculer sa somme.

Exercice IV.3.28. — (i) Montrer que, si $\phi \in \mathscr{C}_c^\infty$, l'équation différentielle $u'' - u = \phi$ a une unique solution dans $\mathscr{S}(\mathbf{R})$. Cette solution est-elle toujours à support compact ?

(ii) À quelle condition portant sur $\hat{\phi}$, l'équation différentielle $u'' + u = \phi$ a-t-elle une solution dans $\mathscr{S}(\mathbf{R})$? Si solution il y a, est-elle toujours à support compact ?

Exercice IV.3.29. — Soit $f : \mathbf{R} \to \mathbf{R}$ définie par $f(t) = e^{-\pi t^2}$.

(i) Montrer que $\hat{f}$ est $\mathscr{C}^\infty$ sur $\mathbf{R}$, et vérifie l'équation différentielle $\hat{f}'(x) = -2\pi x\hat{f}(x)$. En déduire, en utilisant la formule $\int_{\mathbf{R}} e^{-\pi t^2}\, dt = 1$, que $\hat{f}(x) = e^{-\pi x^2}$.

(ii) Si $u \in \mathbf{R}_+^*$, calculer la transformée de Fourier de f_u définie par $f_u(t) = e^{-\pi u t^2}$.

(iii) Si $u \in \mathbf{R}_+^*$, et si $\mathrm{F}(u) = \sum_{n\in\mathbf{Z}} e^{-\pi n^2 u}$, montrer que $\mathrm{F}(u) = \frac{1}{\sqrt{u}}\mathrm{F}(\frac{1}{u})$.

Exercice IV.3.30. — Si $\lambda > 0$, soit $\phi_\lambda(t) = e^{-\pi\lambda|t|}\,\frac{\sin \pi t}{\pi t}$.

(i) Montrer que $\lambda \mapsto \hat{\phi}_\lambda(x)$ est dérivable sur $\mathbf{R}_+^*$, si $x \in \mathbf{R}$, et calculer sa dérivée. En déduire $\hat{\phi}_\lambda(x)$.

(ii) Remarquer que $\frac{\sin \pi t}{\pi t}$ est la transformée de Fourier de $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$, et retrouver directement le (i).

IV.4. Transformée de Fourier dans L^2

Si $\phi \in \mathrm{L}^2(\mathbf{R}^m)$ n'est pas sommable, l'intégrale $\int_{\mathbf{R}^m} e^{-2i\pi\, xt}\phi(t)\,dt$ ne converge pour aucune valeur de x. Malgré ce petit problème, on peut définir la transformée de Fourier d'un élément de $\mathrm{L}^2(\mathbf{R}^m)$, par un passage à la limite, et ce qu'on obtient fournit une théorie ayant des propriétés nettement plus agréables que dans $\mathrm{L}^1(\mathbf{R}^m)$. Il y a des tas de manières d'arriver au résultat. Nous avons choisi de privilégier les fonctions en escalier jusqu'au bout. On trouvera une autre approche dans le problème H.6.

1. Transformée de Fourier des fonctions en escalier

Commençons par quelques calculs en dimension 1.

Lemme IV.4.1. — (i) *Si $\lambda > 0$, la transformée de Fourier de $e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}$ est*

$$\frac{1}{\pi}\big(\mathrm{arctg}(\frac{2x+1}{\lambda}) - \mathrm{arctg}(\frac{2x-1}{\lambda})\big).$$

(ii) *La transformée de Fourier de $\frac{\sin^2 \pi t}{(\pi t)^2}$ est $\frac{1}{2}(|x+1| + |x-1| - 2|x|)$.*

Démonstration. — (i) On cherche à calculer $\int_{\mathbf{R}} e^{-2i\pi\, xt}e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}dt$. Or $\frac{\sin \pi t}{\pi t}$ est la transformée de Fourier de $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$, alors que la transformée de Fourier de $e^{-2i\pi\, xt}e^{-\pi\lambda|t|}$ est

$$\begin{aligned} y \mapsto \int_{\mathbf{R}} e^{-2i\pi\,(x+y)t}e^{-\pi\lambda|t|}\,dt &= \int_0^{+\infty} e^{-\pi t(\lambda+2i(x+y))} + e^{-\pi t(\lambda-2i(x+y))}\,dt \\ &= \frac{1}{\pi}\big(\frac{1}{\lambda+2i(x+y)} + \frac{1}{\lambda-2i(x+y)}\big) = \frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}. \end{aligned}$$

Il résulte donc de la prop. IV.3.24 que $\int_{\mathbf{R}} e^{-2i\pi\, xt}e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t} = \int_{\frac{-1}{2}}^{\frac{1}{2}} \frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}\,dy$. On conclut en utilisant le fait que la primitive de $\frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}$ est $\frac{1}{\pi}\mathrm{arctg}(\frac{2(x+y)}{\lambda})$.

(ii) Nous allons plutôt calculer la transformée de Fourier de $e^{-\pi\lambda|t|}\frac{\sin^2 \pi t}{(\pi t)^2}$, pour $\lambda > 0$, et en déduire le résultat en faisant tendre λ vers 0. Si $x \in \mathbf{R}$, et $\lambda \geqslant 0$, soit

$$\mathrm{G}_x(\lambda) = \int_{\mathbf{R}} g_x(\lambda, t)\,dt, \quad \text{avec } g_x(\lambda,t) = e^{-2i\pi\, xt}e^{-\pi\lambda|t|}\frac{\sin^2 \pi t}{(\pi t)^2}.$$

Comme la fonction $\frac{\sin^2 \pi t}{(\pi t)^2}$ est un majorant sommable de $g_x(\lambda, t)$ pour tout $\lambda \geqslant 0$, et comme $\lambda \mapsto g_x(\lambda, t)$ est continu sur $\mathbf{R}_+$, pour tout $t \geqslant 0$, le théorème de continuité d'une intégrale dépendant d'un paramètre montre que G_x est continue sur $\mathbf{R}_+$. La quantité $\mathrm{G}_x(0)$ qui nous intéresse est donc la limite, quand $\lambda \to 0$, de $\mathrm{G}_x(\lambda)$.

On va utiliser la prop. IV.3.24, avec $f = \mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$ et $g = e^{-2i\pi xt}e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}$, puisque $\mathrm{G}_x(\lambda) = \int_{\mathbf{R}} \hat{f}g$. En utilisant le (i), on obtient $\mathrm{G}_x(\lambda) = \int_{\mathbf{R}} f\hat{g} = \frac{1}{\pi}\int_{-1/2}^{1/2} h_x(\lambda, y)\, dy$, avec

$$h_x(\lambda, y) = \big(\mathrm{arctg}(\frac{2(x+y)+1}{\lambda}) - \mathrm{arctg}(\frac{2(x+y)-1}{\lambda})\big).$$

Maintenant, $|h_x(\lambda, y)|$ est majoré par π quel que soit $\lambda > 0$, et comme $\mathrm{arctg}(\frac{a}{\lambda})$ tend vers $\mathrm{sign}(a)\frac{\pi}{2}$, quand $\lambda \to 0^+$, on obtient, en utilisant le théorème de continuité d'une intégrale dépendant d'un paramètre,

$$\mathrm{G}_x(0) = \frac{1}{2}\int_{-1/2}^{1/2} (\mathrm{sign}(2(x+y)+1) - \mathrm{sign}(2(x+y)-1))\, dy.$$

On conclut en utilisant la formule $\int_{-1/2}^{1/2} \mathrm{sign}(2y+a)\, dy = |\frac{a+1}{2}| - |\frac{a-1}{2}|$.

Proposition IV.4.2. — *Soit $m \geqslant 1$.*

(i) *Si $r \in \mathbf{N}$, et si $\mathbf{k} \in \mathbf{Z}^m$, alors $\hat{e}_{r,\mathbf{k}} \in \mathrm{L}^2(\mathbf{R}^m)$.*

(ii) *Si $\mathbf{k}, \mathbf{k}' \in \mathbf{Z}^m$, alors*

$$\langle \hat{e}_{r,\mathbf{k}}, \hat{e}_{r,\mathbf{k}'}\rangle = \begin{cases} 0 & \text{si } \mathbf{k} \neq \mathbf{k}' \\ 2^{-rm} & \text{si } \mathbf{k} = \mathbf{k}' \end{cases} = \langle e_{r,\mathbf{k}}, e_{r,\mathbf{k}'}\rangle.$$

(iii) *L'application $\phi \mapsto \hat{\phi}$ induit une isométrie de* $\mathrm{Esc}(\mathbf{R}^m)$*, muni de la norme $\|\ \|_2$, sur un sous-espace de* $\mathrm{L}^2(\mathbf{R}^m)$.

Démonstration. — Le (i) est une conséquence du fait que $\alpha(t) = \frac{\sin \pi t}{\pi t}$ est de carré sommable dans $\mathbf{R}$, et de la formule de la prop. IV.2.6 exprimant $\hat{e}_{r,\mathbf{k}}$ en terme de α.

Un calcul immédiat montre que $\langle e_{r,\mathbf{k}}, e_{r,\mathbf{k}'}\rangle$ est nul si $\mathbf{k} \neq \mathbf{k}'$, et vaut 2^{-rm} si $\mathbf{k} = \mathbf{k}'$. Par ailleurs, en partant de la formule

$$\hat{e}_{r,\mathbf{k}}(x) = \prod_{j=1}^{m} \big(2^{-r}e^{-2^{1-r}i\pi(k_j+\frac{1}{2})x_j}\alpha(2^{-r}x_j)\big)$$

de la prop. IV.2.6, on obtient (après une application immédiate du théorème de Fubini),

$$\begin{aligned}\langle \hat{e}_{r,\mathbf{k}}, \hat{e}_{r,\mathbf{k}'}\rangle =& 2^{-2rm}\prod_{j=1}^{m}\big(\int_{\mathbf{R}} e^{-2^{1-r}i\pi(k'_j-k_j)x_j}\alpha(2^{-r}x_j)^2\, dx_j\big) \\ =& 2^{-rm}\prod_{j=1}^{m}\big(\int_{\mathbf{R}} e^{-2i\pi(k'_j-k_j)u_j}\alpha(u_j)^2\, du_j\big).\end{aligned}$$

On reconnaît dans la parenthèse la transformée de Fourier de $\alpha^2(t) = \frac{\sin^2 \pi t}{(\pi t)^2}$, ce qui permet d'utiliser le (ii) du lemme IV.4.1 pour montrer que $\int_{\mathbf{R}} e^{-2i\pi(k'_j-k_j)u_j}\alpha(u_j)^2\, du_j$ est nul si $k_j \neq k'_j$, et vaut 1 si $k_j = k'_j$. On en déduit le (ii).

Enfin, le (iii) suit (car les $e_{r,\mathbf{k}}$, pour $\mathbf{k} \in \mathbf{Z}^m$, forment une base de $\mathrm{Esc}_r(\mathbf{R}^m)$) du (ii) et de ce que $\mathrm{Esc}(\mathbf{R}^m)$ est la réunion des $\mathrm{Esc}_r(\mathbf{R}^m)$, pour $r \in \mathbf{N}$.

2. Définition de la transformée de Fourier dans L^2

Théorème IV.4.3. — (Plancherel, 1910) *$\mathscr{F} : \mathrm{Esc}(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ se prolonge par continuité en une isométrie de $L^2(\mathbf{R}^m)$ sur $L^2(\mathbf{R}^m)$ dont l'inverse est $\phi \mapsto \overline{\mathscr{F}}\phi$, avec*[9] *$\overline{\mathscr{F}}\phi(x) = \mathscr{F}\phi(-x)$. Autrement dit :*

(i) *$\langle \mathscr{F}\phi_1, \mathscr{F}\phi_2 \rangle = \langle \phi_1, \phi_2 \rangle$, si $\phi_1, \phi_2 \in L^2(\mathbf{R}^m)$ ($\mathscr{F}$ est une isométrie),*

(ii) *$\mathscr{F}(\mathscr{F}\phi)(x) = \phi(-x)$, si $\phi \in L^2(\mathbf{R}^m)$* (formule d'inversion de Fourier dans L^2).

De plus, les formules du n° IV.2.2, pour les dilatations, translations et multiplications par un caractère, sont encore valables dans $L^2(\mathbf{R}^m)$, et si $\phi \in L^1(\mathbf{R}^m) \cap L^2(\mathbf{R}^m)$, les deux définitions de $\mathscr{F}\phi$ coïncident.

Démonstration. — Il résulte du (iii) de la prop. IV.4.2 et de la densité de $\mathrm{Esc}(\mathbf{R}^m)$ dans $L^2(\mathbf{R}^m)$, que $\mathscr{F}$ peut se prolonger par continuité, de manière unique, en une isométrie de $L^2(\mathbf{R}^m)$ sur un sous-espace[10] de $L^2(\mathbf{R}^m)$. De plus, les formules pour les dilatations, translations et multiplications par un caractère s'étendent à $L^2(\mathbf{R}^m)$ par continuité.

Maintenant, si $\phi \in L^1(\mathbf{R}^m) \cap L^2(\mathbf{R}^m)$, notons (provisoirement) $\mathscr{F}_1\phi$ (resp. $\mathscr{F}_2\phi$) la transformée de Fourier de ϕ dans $L^1(\mathbf{R}^m)$ (resp. $L^2(\mathbf{R}^m)$). Soit $(f_j)_{j\in\mathbf{N}}$ une suite d'éléments de $\mathrm{Esc}(\mathbf{R}^m)$ convergeant vers ϕ à la fois dans $L^1(\mathbf{R}^m)$ et dans $L^2(\mathbf{R}^m)$ (cf. th. III.2.11). Alors $\mathscr{F}_1 f_j = \mathscr{F}_2 f_j$ tend uniformément vers la fonction continue $\mathscr{F}_1\phi$ et en norme $\| \ \|_2$ vers $\mathscr{F}_2\phi$. D'après le lemme III.2.14, cela implique $\mathscr{F}_1\phi \in L^2(\mathbf{R}^m)$ et $\mathscr{F}_1\phi = \mathscr{F}_2\phi$ p.p.

Pour conclure, il suffit donc de prouver l'on a $\mathscr{F} \circ \mathscr{F} = s$, où $s : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ est l'application déduite de celle sur $\mathscr{L}^2(\mathbf{R}^m)$ définie par $s(\phi)(x) = \phi(-x)$. En effet ceci prouve à la fois la surjectivité et le fait que $\overline{\mathscr{F}}$ est l'inverse de $\mathscr{F}$. Par continuité des applications $\mathscr{F}\circ\mathscr{F}$ et s, il suffit de vérifier qu'elles coïncident sur $\mathrm{Esc}(\mathbf{R}^m)$, qui est un sous-espace dense, et par linéarité, il suffit de le prouver pour une famille génératrice de $\mathrm{Esc}(\mathbf{R}^m)$, par exemple la famille des $\mathbf{e}_{r,\mathbf{k}}$, pour $r \in \mathbf{N}$, et $\mathbf{k} \in \mathbf{Z}^m$. Enfin, comme les $\mathbf{e}_{r,\mathbf{k}}$ sont obtenues par translation et dilatation à partir de la fonction $\beta_m(t) = \prod_{j=1}^m \mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}(t_j)$, il suffit de prouver que $\mathscr{F}(\mathscr{F}\beta_m)(t) = \beta_m(-t)$ dans $L^2(\mathbf{R}^m)$. Or on a $(\mathscr{F}\beta_m)(x) = \prod_{j=1}^m \frac{\sin \pi x_j}{\pi x_j}$, et on est ramené à calculer la transformée de Fourier de $\prod_{j=1}^m \frac{\sin \pi x_j}{\pi x_j}$. Les arguments étant les mêmes pour $m = 1$ que pour m quelconque, nous ne traiterons que le cas $m = 1$, ce qui a pour avantage de raccourcir un peu les expressions.

On doit donc calculer la transformée de Fourier de $\alpha(t) = \frac{\sin \pi t}{\pi t}$. Comme α n'est pas sommable, on ne peut pas utiliser l'expression $\hat{\alpha}(x) = \int_{\mathbf{R}} e^{-2i\pi\, xt}\alpha(t)\, dt$ pour faire le calcul. Pour contourner le problème, constatons que $\alpha_\lambda(t) = e^{-\pi\lambda|t|}\alpha(t)$ tend vers α dans $L^2(\mathbf{R}^m)$, quand λ tend vers 0, car $|\alpha_\lambda|$ est majoré, pour tout $\lambda \geqslant 0$, par $|\alpha|$ qui est de carré sommable, et $\alpha_\lambda(t)$ tend vers $\alpha(t)$ quand λ tend vers 0, pour tout $t \in \mathbf{R}$. Par continuité

9. Écrire $\phi(x)$ est un abus de notation ; pour être correct, il vaudrait mieux écrire $\overline{\mathscr{F}} = \mathscr{F} \circ s$, où $s : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ est l'application déduite, par passage au quotient, de l'application s sur $\mathscr{L}^2(\mathbf{R}^m)$, définie par $s(\phi)(x) = \phi(-x)$.

10. Comme on est en dimension infinie, l'injectivité n'implique pas, a priori, la surjectivité.

de $\mathscr{F}$, on en déduit que $\mathscr{F}\alpha_\lambda$ tend vers $\mathscr{F}\alpha$ dans L^2 quand λ tend vers 0. Or on a calculé $\mathscr{F}\alpha_\lambda$ (cf. IV.4.1), et il est apparent sur la formule que $\mathscr{F}\alpha_\lambda(x)$ tend vers $\mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}(x)$, quand λ tend vers 0, pour tout $x \neq \pm\frac{1}{2}$. On en déduit que $\mathscr{F}\alpha = \mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}$ p.p., ce qui permet de conclure.

Remarque IV.4.4. — On a été confronté, au cours de la démonstration, au problème du calcul de la transformée de Fourier d'une fonction ϕ, de carré sommable, mais non sommable. On s'en est sorti par un passage à la limite, en multipliant ϕ par $e^{-\pi\lambda(|t_1|+\cdots+|t_m|)}$, et en faisant tendre λ vers 0. Une autre manière de procéder est de prendre une suite croissante $(\mathrm{X_N})_{\mathrm{N}\in\mathbf{N}}$ d'ensembles bornés dont la réunion est $\mathbf{R}^m$, et d'écrire $\mathscr{F}\phi$ comme la limite de $\mathscr{F}(\mathbf{1}_{\mathrm{X_N}}\phi)$ quand N tend vers $+\infty$ (en effet, $\mathbf{1}_{\mathrm{X_N}}\phi$ tend vers ϕ dans $\mathrm{L}^2(\mathbf{R}^m)$ d'après le théorème de convergence dominée, et $\mathbf{1}_{\mathrm{X_N}}\phi$ est sommable puisque de carré sommable et à support borné).

Corollaire IV.4.5. — *Si $f, g \in \mathrm{L}^2(\mathbf{R}^m)$, alors $\int_{\mathbf{R}^m} g\hat{f} = \int_{\mathbf{R}^m} f\hat{g}$.*

Démonstration. — Posons $\phi_1 = \overline{\mathscr{F}f}$, et $\phi_2 = g$. On a $\mathscr{F}\phi_1 = \overline{f}$, et donc

$$\int_{\mathbf{R}^m} g\hat{f} = \langle\phi_1, \phi_2\rangle = \langle\mathscr{F}\phi_1, \mathscr{F}\phi_2\rangle = \int_{\mathbf{R}^m} f\hat{g},$$

ce qu'il fallait démontrer.

3. Comparaison des transformées de Fourier dans L^1 et L^2

Proposition IV.4.6. — *Si $f_1 \in \mathrm{L}^1(\mathbf{R}^m)$ et $f_2 \in \mathrm{L}^2(\mathbf{R}^m)$ ont même transformée de Fourier, alors $f_1 = f_2$.*

Démonstration. — Si $\phi \in \mathscr{C}_c^\infty(\mathbf{R}^m)$, alors $\overline{\mathscr{F}}\phi \in \mathrm{L}^1(\mathbf{R}^m) \cap \mathrm{L}^2(\mathbf{R}^m)$ d'après le cor. IV.3.23 ; en particulier, $\mathscr{F}(\overline{\mathscr{F}}\phi) = \phi$. Comme f et g ont même transformée de Fourier, on déduit de la prop. IV.3.24 et du cor. IV.4.5, utilisés pour $g = \overline{\mathscr{F}}\phi$, que $\int_{\mathbf{R}^m} f_1\phi = \int_{\mathbf{R}^m} f_2\phi$. D'après l'exercice III.3.13, ceci implique $f_1 = f_2$.

Proposition IV.4.7. — (Formule d'inversion de Fourier dans L^1) *Si $\phi \in \mathrm{L}^1(\mathbf{R}^m)$ a une transformée de Fourier sommable, alors $\phi = \overline{\mathscr{F}}\hat{\phi}$.*

Démonstration. — Par hypothèse, $\hat{\phi} \in \mathrm{L}^1(\mathbf{R}^m)$. Par ailleurs, on sait que $\hat{\phi}$ est bornée puisque $\phi \in \mathrm{L}^1(\mathbf{R}^m)$. Donc $|\hat{\phi}|^2 \leqslant \|\hat{\phi}\|_\infty \cdot |\hat{\phi}|$, et $\hat{\phi} \in \mathrm{L}^2(\mathbf{R}^m)$, ce qui fait que $\overline{\mathscr{F}}\hat{\phi}$ est un élément de $\mathrm{L}^2(\mathbf{R}^m)$ ayant même transformée de Fourier que ϕ (grâce à la formule d'inversion de Fourier dans $\mathrm{L}^2(\mathbf{R}^m)$). La prop. IV.4.6 permet de conclure.

4. Dérivation

Théorème IV.4.8. — (i) *Si $f \in \mathrm{H}^k(\mathbf{R}^m)$, alors $(1+\|x\|^2)^{k/2}\hat{f}(x)$ est de carré sommable, $\mathscr{F}(\partial_{\mathbf{l}}f) = (2i\pi x)_{\mathbf{l}}\hat{f}$ si $\boldsymbol{\ell} \in \mathbf{N}^m$ vérifie $|\boldsymbol{\ell}| \leqslant k$, et $\|(1+\|x\|^2)^{k/2}\hat{f}\|_2 \leqslant (1+\frac{m}{2\pi})^k\|f\|_{\mathrm{H}^k}$.*

(ii) *Réciproquement, si $(1+\|t\|^2)^{k/2}f(t)$ est de carré sommable, alors $\hat{f} \in \mathrm{H}^k(\mathbf{R}^m)$, on a $\partial_{\mathbf{l}}\hat{f}(x) = (-2i\pi)^{|\mathbf{l}|}\mathscr{F}(t_{\mathbf{l}}f)$, si $|\boldsymbol{\ell}| \leqslant k$, et $\|\hat{f}\|_{\mathrm{H}^k} \leqslant (2\pi)^k\|(1+\|t\|^2)^{k/2}f\|_2$.*

Remarque IV.4.9. — (i) Le (i) s'applique en particulier à une fonction de classe $\mathscr{C}^k$ dont toutes les dérivées partielles d'ordre $\leqslant k$ sont de carré sommable.

(ii) On déduit du théorème une définition « par Fourier » de l'espace de Sobolev $H^k(\mathbf{R}^m)$. C'est l'ensemble des $f \in L^2(\mathbf{R}^m)$ tel que $(1+\|x\|^2)^{k/2}\hat{f} \in L^2(\mathbf{R}^m)$. On peut étendre cette définition à $k \in \mathbf{R}_+$, et parler de l'espace de Sobolev $H^s(\mathbf{R}^m)$, pour $s \in \mathbf{R}_+$ (et même pour $s \in \mathbf{R}$ en supprimant la condition $f \in L^2(\mathbf{R}^m)$, mais on tombe alors sur un espace de distributions).

Démonstration. — On sait déjà que $\mathscr{F}(\partial_\alpha f) = (2i\pi x)_\alpha \hat{f}$, si $f \in \mathscr{C}^k_c(\mathbf{R}^m)$. Maintenant, $\mathscr{F}\circ\partial_\alpha \colon H^k(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ est continue, comme composée de $\partial_\alpha \colon H^k(\mathbf{R}^m) \to H^{k-|\alpha|}(\mathbf{R}^m)$, qui est continue d'après le n° 5 du § II.2, de l'inclusion de $H^{k-|\alpha|}(\mathbf{R}^m)$ dans $L^2(\mathbf{R}^m)$ qui est 1-lipschitzienne, et de $\mathscr{F} : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ qui est une isométrie. Comme $\mathscr{C}^k_c(\mathbf{R}^m)$ est dense dans $H^k(\mathbf{R}^m)$ par construction, cela permet d'en déduire que $\mathscr{F}(\partial_\alpha f) = (2i\pi x)_\alpha \hat{f}$, quel que soit $f \in H^k(\mathbf{R}^m)$. En utilisant le fait que $\mathscr{F} : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ est une isométrie, on obtient alors (en développant $(1+\sum_{j=1}^m |x_j|)^k$ sous la forme $\sum_{|\alpha|\leqslant k} a_\alpha |x|^\alpha$),

$$\|(1+\|x\|^2)^{k/2}\hat{f}\|_2 \leqslant \|(1+\sum_{j=1}^m |x_j|)^k \hat{f}\|_2 \leqslant \sum_{|\alpha|\leqslant k} a_\alpha \|x^\alpha \hat{f}\|_2 = \sum_{|\alpha|\leqslant k} a_\alpha (2\pi)^{-|\alpha|}\|\partial_\alpha f\|_2 \,.$$

On conclut la démonstration du (i) en majorant chaque $\|\partial_\alpha f\|_2$ par $\|f\|_{H^k}$, et en remarquant que $\sum_{|\alpha|\leqslant k} a_\alpha (2\pi)^{-|\alpha|} = (1+\frac{m}{2\pi})^k$.

Passons à la démonstration du (ii). Soit E l'ensemble des f tels que $(1+\|t\|^2)^{k/2} f$ soit de carré sommable. On munit E de la norme $\|\ \|_E$ définie par $\|f\|_E = \|(1+\|t\|^2)^{k/2} f\|_2$. Par définition, l'application $f \mapsto (1+\|t\|^2)^{k/2} f$ induit une isométrie de E sur $L^2(\mathbf{R}^m)$, ce qui fait que E est un espace de Hilbert.

Maintenant, si f est de la forme $(1+\|t\|^2)^{-k/2} g$, où g est une fonction en escalier, alors $(1+\|t\|^2)^{k/2} f$ est sommable, et il résulte du (ii) du théorème IV.2.8, que $\hat{f}$ est de classe $\mathscr{C}^k$, et que $\partial_\alpha \hat{f} = (-2i\pi)^{|\alpha|}\mathscr{F}(t_\alpha f)$, si $|\alpha| \leqslant k$. En utilisant le fait que $\mathscr{F} : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ est une isométrie, on obtient alors

$$\|\hat{f}\|_{H^k} = \sup_{|\alpha|\leqslant k} \|\partial_\alpha \hat{f}\|_2 = \sup_{|\alpha|\leqslant k} (2\pi)^{|\alpha|}\|t_\alpha f\|_2 \leqslant (2\pi)^k \|(1+\|t\|^2)^{k/2} f\|_2 = (2\pi)^k \|f\|_E.$$

Autrement dit, $f \mapsto \hat{f}$ est une application $(2\pi)^k$-lipschitzienne de $(1+\|t\|^2)^{-k/2}\mathrm{Esc}(\mathbf{R}^m)$ muni de la norme $\|\ \|_E$ dans $H^k(\mathbf{R}^m)$ muni de la norme $\|\ \|_{H^k}$. Comme $\mathrm{Esc}(\mathbf{R}^m)$ est dense dans $L^2(\mathbf{R}^m)$, l'espace $(1+\|t\|^2)^{-k/2}\mathrm{Esc}(\mathbf{R}^m)$ est dense dans E, et comme $H^k(\mathbf{R}^m)$ est complet, on en déduit que $f \mapsto \hat{f}$ induit une application $(2\pi)^k$-lipschitzienne de E dans H^k. Autrement dit, si $(1+\|t\|^2)^{k/2} f$ est de carré sommable, alors $\hat{f} \in H^k(\mathbf{R}^m)$ et $\|\hat{f}\|_{H^k} \leqslant (2\pi)^k \|(1+\|t\|^2)^{k/2} f\|_2$.

Il reste à prouver que l'on a $\partial_\alpha \hat{f} = (-2i\pi)^{|\alpha|}\mathscr{F}(t_\alpha f)$, quel que soit $f \in E$, sachant que que c'est vrai pour f dans un sous-espace dense. Or $\partial_\alpha \circ \mathscr{F} : E \to L^2(\mathbf{R}^m)$ est continue, puisque l'on vient de prouver que $\mathscr{F} : E \to H^k(\mathbf{R}^m)$ est continue et que

$\partial_{\amalg} : \mathrm{H}^k(\mathbf{R}^m) \to \mathrm{H}^{k-1}_{\amalg}(\mathbf{R}^m) \subset \mathrm{L}^2(\mathbf{R}^m)$ est continue. De même, $f \mapsto t_{\amalg} f$ est continue (et même 1-lipschitzienne) de E dans $\mathrm{L}^2(\mathbf{R}^m)$, et donc $f \mapsto (-2i\pi)^{1}_{\amalg}\mathscr{F}(t_{\amalg} f)$ est continue de E dans $\mathrm{L}^2(\mathbf{R}^m)$. On a deux applications continues coïncidant sur un sous-espace dense ; elles sont donc égales, ce qui permet de conclure.

CHAPITRE V

FONCTIONS HOLOMORPHES

Une fonction holomorphe sur un ouvert Ω est une fonction de Ω dans $\mathbf{C}$ qui est $\mathscr{C}^\infty$ au sens complexe et somme de sa série de Taylor autour de chaque point. Ces fonctions jouissent de propriétés de rigidité absolument remarquables et qui peuvent sembler miraculeuses si on se réfère à ce que l'on connaît des fonctions d'une variable réelle. Une des premières surprises que l'on rencontre est qu'une fonction est holomorphe si et seulement si elle est de classe $\mathscr{C}^1$ (au sens complexe) ! Ceci est une des nombreuses conséquences de la formule intégrale de Cauchy (th. V.4.6). Cette formule et ses conséquences immédiates (rem. V.4.9, th. V.5.1, V.5.4 et V.5.7), couplées avec le principe du maximum (th. V.3.11), le théorème des zéros isolés (th. V.3.3) et la formule des résidus de Cauchy du chapitre suivant, permettent d'attaquer une variété de problèmes assez spectaculaire. Parmi ceux-ci, mentionnons le théorème fondamental de l'algèbre (ex. V.3.13, cor. V.4.15 ou ex. VI.3.21), le théorème des 4 carrés de Lagrange (ex. VII.6.9), la loi de réciprocité quadratique (ex. VI.3.28), l'irrationnalité de $\zeta(3)$ (prob. H.12) ou encore le théorème des nombres premiers auquel l'annexe A est consacrée.

V.1. Fonctions holomorphes et fonctions analytiques complexes

1. Séries entières

Soit K un corps. Une *série entière* (*ou série formelle*) *à coefficients dans* K est une expression du type $\sum_{n=0}^{+\infty} a_n \mathrm{T}^n$, où les a_n sont des éléments de K. L'ensemble K[[T]] des séries entières à coefficients dans K contient l'anneau K[T] des polynômes à coefficients dans K, et on munit K[[T]] d'une structure d'anneau étendant celle de K[T] en posant

$$\Big(\sum_{n=0}^{+\infty} a_n \mathrm{T}^n\Big)+\Big(\sum_{n=0}^{+\infty} b_n \mathrm{T}^n\Big) = \sum_{n=0}^{+\infty}(a_n+b_n)\mathrm{T}^n, \quad \Big(\sum_{n=0}^{+\infty} a_n \mathrm{T}^n\Big)\Big(\sum_{n=0}^{+\infty} b_n \mathrm{T}^n\Big) = \sum_{n=0}^{+\infty}\Big(\sum_{k=0}^{n} a_k b_{n-k}\Big)\,\mathrm{T}^n.$$

On définit la *valuation* $v_{\mathrm{T}}(\mathrm{F})$ de $\mathrm{F} = \sum_{n\in\mathbf{N}} a_n \mathrm{T}^n$ comme étant le plus petit élément de l'ensemble des $n \in \mathbf{N}$ vérifiant $a_n \neq 0$, si $\mathrm{F} \neq 0$, et comme étant $+\infty$, si $\mathrm{F} = 0$. On a $v_{\mathrm{T}}(\mathrm{FG}) = v_{\mathrm{T}}(\mathrm{F}) + v_{\mathrm{T}}(\mathrm{G})$, et $v_{\mathrm{T}}(\mathrm{F}+\mathrm{G}) \geqslant \inf(v_{\mathrm{T}}(\mathrm{F}), v_{\mathrm{T}}(\mathrm{G}))$. En définissant $|\ |_{\mathrm{T}}$,

par $|\mathrm{F}|_{\mathrm{T}} = e^{-v_{\mathrm{T}}(\mathrm{F})}$, cela se traduit par $|\mathrm{FG}|_{\mathrm{T}} = |\mathrm{F}|_{\mathrm{T}}|\mathrm{G}|_{\mathrm{T}}$ et $|\mathrm{F}+\mathrm{G}|_{\mathrm{T}} \leqslant \sup(|\mathrm{F}|_{\mathrm{T}}, |\mathrm{G}|_{\mathrm{T}})$. Cette dernière inégalité (*ultramétrique*), plus forte que l'inégalité triangulaire, montre que $d(\mathrm{F},\mathrm{G}) = |\mathrm{F}-\mathrm{G}|_{\mathrm{T}}$ est une distance sur $\mathrm{K}[[\mathrm{T}]]$. On vérifie facilement, que $\mathrm{K}[[\mathrm{T}]]$ est complet pour cette distance, qu'une série $\sum_{n\in\mathbf{N}} \mathrm{F}_n$ converge, si et seulement si $|\mathrm{F}_n|_{\mathrm{T}} \to 0$ (ce qui équivaut à $v_{\mathrm{T}}(\mathrm{F}_n) \to +\infty$), et que $\mathrm{K}[\mathrm{T}]$ est dense dans $\mathrm{K}[[\mathrm{T}]]$, ce qui prouve que $\mathrm{K}[[\mathrm{T}]]$ est le complété de $\mathrm{K}[\mathrm{T}]$ pour la (distance associée à la) valuation v_{T}. Ceci fournit une construction topologique [1] de $\mathrm{K}[[\mathrm{T}]]$ à partir de $\mathrm{K}[\mathrm{T}]$.

Si $\mathrm{F} = \sum_{n=0}^{+\infty} a_n \mathrm{T}^n \in \mathrm{K}[[\mathrm{T}]]$, soit $\mathrm{F}' = \sum_{n=1}^{+\infty} n a_n \mathrm{T}^{n-1}$ la dérivée de F. On définit par récurrence la dérivée k-ième $\mathrm{F}^{(k)}$ comme la dérivée de $\mathrm{F}^{(k-1)}$, en posant $\mathrm{F}^{(0)} = \mathrm{F}$, et donc $\mathrm{F}^{(1)} = \mathrm{F}'$. La dérivée seconde $\mathrm{F}^{(2)}$ est souvent aussi notée F''. Un calcul immédiat montre que $\frac{1}{k!}\mathrm{F}^{(k)} = \sum_{n=0}^{+\infty} \binom{n+k}{k} \mathrm{T}^n$.

Exercice V.1.1. — (i) Montrer que, si $\mathrm{F},\mathrm{G} \in \mathrm{K}[[\mathrm{T}]]$, alors $(\mathrm{FG})' = \mathrm{F}'\mathrm{G} + \mathrm{FG}'$.

(ii) Montrer que, si $(\mathrm{F}_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathrm{K}[[\mathrm{T}]]$ telle que $\sum_{n\in\mathbf{N}} \mathrm{F}_n$ converge dans $\mathrm{K}[[\mathrm{T}]]$, et si F est la somme de la série, alors la série $\sum_{n\in\mathbf{N}} \mathrm{F}'_n$ converge dans $\mathrm{K}[[\mathrm{T}]]$, et on a $\mathrm{F}' = \sum_{n\in\mathbf{N}} \mathrm{F}'_n$.

(iii) Montrer que, si $\mathrm{F} = \sum_{n\in\mathbf{N}} a_n \mathrm{T}^n \in \mathrm{K}[[\mathrm{T}]]$, et si $\mathrm{G} \in \mathrm{TK}[[\mathrm{T}]]$, alors $\sum_{n\in\mathbf{N}} a_n \mathrm{G}^n$ converge dans $\mathrm{K}[[\mathrm{T}]]$, et la limite $\mathrm{F}\circ\mathrm{G}$ vérifie $(\mathrm{F}\circ\mathrm{G})' = (\mathrm{F}'\circ\mathrm{G})\,\mathrm{G}'$.

Exercice V.1.2. — Soit $(u_n)_{n\in\mathbf{N}} \in \mathbf{C}^{\mathbf{N}}$ vérifiant la relation de récurrence $u_{n+2} - 3u_{n+1} + 2u_n = 1$, pour tout $n \in \mathbf{N}$, et soit $\mathrm{F} = \sum_{n\in\mathbf{N}} u_n \mathrm{T}^n \in \mathbf{C}[[\mathrm{T}]]$. Calculer $(1-3\mathrm{T}+2\mathrm{T}^2)\mathrm{F}(\mathrm{T})$ en fonction de u_0 et u_1. En déduire une formule générale pour u_n.

On ne s'intéressera, par la suite, qu'au cas $\mathrm{K} = \mathbf{C}$, mais les exemples qui suivent ont un sens sur un corps K de caractéristique 0 quelconque.

Exemple V.1.3. — • *La série exponentielle.* Si $\lambda \in \mathbf{C}$, on note $\exp(\lambda\mathrm{T})$ la série formelle $\sum_{n=0}^{+\infty} \frac{\lambda^n}{n!}\mathrm{T}^n$. C'est la solution formelle de l'équation différentielle $\mathrm{F}' = \lambda\mathrm{F}$ dont le terme constant est 1, et on a $\exp(\lambda\mathrm{T})\exp(\mu\mathrm{T}) = \exp((\lambda+\mu)\mathrm{T})$.

• *Les séries puissances.* Si $\alpha \in \mathbf{N}$, alors $(1+\mathrm{T})^\alpha = \sum_{n=0}^{+\infty} \binom{\alpha}{n}\mathrm{T}^n$, d'après la formule du binôme, et l'annulation de $\binom{\alpha}{n}$, pour $n > \alpha$. Par analogie, on définit $(1+\mathrm{T})^\alpha$, pour $\alpha \in \mathbf{C}$, comme la série entière $\sum_{n=0}^{+\infty} \binom{\alpha}{n}\mathrm{T}^n$. Si $\alpha,\beta \in \mathbf{N}$, on a

$$\sum_{n=0}^{+\infty} \Big(\sum_{k=0}^{n} \tbinom{\alpha}{k}\tbinom{\beta}{n-k} \Big) \mathrm{T}^n = (1+\mathrm{T})^\alpha (1+\mathrm{T})^\beta = (1+\mathrm{T})^{\alpha+\beta} = \sum_{n=0}^{+\infty} \tbinom{\alpha+\beta}{n} \mathrm{T}^n,$$

ce qui se traduit par le fait que les polynômes en 2 variables $\binom{\mathrm{X}+\mathrm{Y}}{n}$ et $\sum_{k=0}^{n} \binom{\mathrm{X}}{k}\binom{\mathrm{Y}}{n-k}$

1. On obtient une construction algébrique en remarquant que $\mathrm{F} \in \mathrm{K}[[\mathrm{T}]]$ est déterminée si on connaît ses n premiers coefficients, quel que soit $n \in \mathbf{N}$. Autrement dit F est déterminée par ses images F_n dans $\mathrm{K}[\mathrm{T}]/(\mathrm{T}^n)$, pour $n \in \mathbf{N}$, et l'application $\mathrm{F} \mapsto (\mathrm{F}_n)_{n\in\mathbf{N}}$ permet d'identifier $\mathrm{K}[[\mathrm{T}]]$ à la *limite projective* $\varprojlim \mathrm{K}[\mathrm{T}]/(\mathrm{T}^n)$ des $\mathrm{K}[\mathrm{T}]/(\mathrm{T}^n)$, ensemble des suites $(\mathrm{F}_n)_{n\in\mathbf{N}}$, où $\mathrm{F}_n \in \mathrm{K}[\mathrm{T}]/(\mathrm{T}^n)$, et $\mathrm{F}_{n+1} \in \mathrm{K}[\mathrm{T}]/(\mathrm{T}^{n+1})$ a pour image F_n modulo T^n, quel que soit $n \in \mathbf{N}$. On remarquera l'analogie avec la construction des nombres p-adiques.

prennent les mêmes valeurs sur $\mathbf{N}\times\mathbf{N}$. Par suite, ils sont égaux, ce qui permet de démontrer que $(1+\mathrm{T})^\alpha(1+\mathrm{T})^\beta=(1+\mathrm{T})^{\alpha+\beta}$ quels que soient $\alpha,\beta\in\mathbf{C}$.

La dérivée de $(1+\mathrm{T})^\alpha$ est $\sum_{n=0}^{+\infty}(n+1)\binom{\alpha}{n+1}\mathrm{T}^n=\alpha(1+\mathrm{T})^{\alpha-1}$, car $(n+1)\binom{\alpha}{n+1}=\alpha\binom{\alpha-1}{n}$.

• *La série du logarithme.* On définit $\log(1+\mathrm{T})$ comme la série $\sum_{n=1}^{+\infty}\frac{(-1)^{n-1}}{n}\mathrm{T}^n$. Sa dérivée est $\sum_{n=0}^{+\infty}(-1)^n\mathrm{T}^n=\frac{1}{1+\mathrm{T}}$.

Exercice V.1.4. — (i) Montrer que $\log(\exp(\lambda\mathrm{T}))=\lambda\mathrm{T}$ dans $\mathbf{C}[[\mathrm{T}]]$.

(ii) Montrer que $(1+\mathrm{T})^\alpha=\exp(\alpha\log(1+\mathrm{T}))$ dans $\mathbf{C}[[\mathrm{T}]]$. (On pourra appliquer l'opérateur $(1+\mathrm{T})\frac{d}{d\mathrm{T}}$ aux deux membres.)

Exercice V.1.5. — (i) Si $\alpha\in\mathbf{C}$, résoudre l'équation différentielle $(1+\mathrm{T})\mathrm{F}'=\alpha\mathrm{F}$ dans $\mathbf{C}[[\mathrm{T}]]$, avec la condition $\mathrm{F}(0)=1$ (i.e. $\mathrm{F}=1+a_1\mathrm{T}+\cdots$).

(ii) Résoudre l'équation différentielle $\mathrm{T}^2\mathrm{F}'+\mathrm{TF}+\mathrm{F}=1$ dans $\mathbf{Q}[[\mathrm{T}]]$.

2. Rayon de convergence d'une série entière

Si $z_0\in\mathbf{C}$ et si $r>0$, on note $\mathrm{D}(z_0,r)$ le *disque fermé* de centre z_0 et de rayon r (i.e. l'ensemble des $z\in\mathbf{C}$ vérifiant $|z-z_0|\leqslant r$), et $\mathrm{D}(z_0,r^-)$ le *disque ouvert* de centre z_0 et de rayon r (i.e. l'ensemble des $z\in\mathbf{C}$ vérifiant $|z-z_0|<r$).

Rappelons (n° 15.4 du Vocabulaire) que, si $\mathrm{F}=\sum_{n=0}^{+\infty}a_n\mathrm{T}^n\in\mathbf{C}[[\mathrm{T}]]$, il existe un unique $\rho(\mathrm{F})\in\overline{\mathbf{R}}_+$, appelé *rayon de convergence* de F, tel que, si $|z|<\rho$, la série $\sum_{n=0}^{+\infty}a_nz^n$ soit normalement convergente, et si $|z|>\rho(\mathrm{F})$, la suite a_nz^n ne soit pas bornée (et donc la série soit divergente). On a par ailleurs $\rho(\mathrm{F})^{-1}=\limsup|a_n|^{1/n}$.

Si $z\in\mathrm{D}(0,\rho(\mathrm{F})^-)$, on note $\mathrm{F}(z)$ la somme de la série $\sum_{n=0}^{+\infty}a_nz^n$. La vérification du résultat suivant est laissée au lecteur.

Lemme V.1.6. — *Si* $\mathrm{F},\mathrm{G}\in\mathbf{C}[[\mathrm{T}]]$, *alors*

$$\rho(\mathrm{F}+\mathrm{G})\geqslant\inf(\rho(\mathrm{F}),\rho(\mathrm{G}))\quad\text{et}\quad\rho(\mathrm{FG})\geqslant\inf(\rho(\mathrm{F}),\rho(\mathrm{G})),$$

et on a

$$(\mathrm{F}+\mathrm{G})(z)=\mathrm{F}(z)+\mathrm{G}(z)\quad\text{et}\quad(\mathrm{FG})(z)=\mathrm{F}(z)\mathrm{G}(z),\quad\textit{si }|z|<\inf(\rho(\mathrm{F}),\rho(\mathrm{G})).$$

Exemple V.1.7. — • Si $\lambda\in\mathbf{C}$, alors $\rho(\exp(\lambda\mathrm{T}))=+\infty$.

• $\rho(\log(1+\mathrm{T}))=1$, et $\rho((1+\mathrm{T})^\alpha)=1$, si $\alpha\notin\mathbf{N}$ (sinon on a affaire à un polynôme dont le rayon de convergence est infini). En effet, si $\alpha\in\mathbf{C}-\mathbf{N}$, alors $|\binom{\alpha}{n+1}/\binom{\alpha}{n}|=|\frac{\alpha-n}{n+1}|\to1$, et donc $|\binom{\alpha}{n}|^{1/n}\to1$ (version multiplicative de la moyenne de Césaro).

• La série [2] $\sum_{n=0}^{+\infty}(-1)^nn!\mathrm{T}^n$ a un rayon de convergence nul.

Remarque V.1.8. — Comme $(1+\mathrm{T})^\alpha(1+\mathrm{T})^\beta=(1+\mathrm{T})^{\alpha+\beta}$ dans $\mathbf{C}[[\mathrm{T}]]$, et comme les trois séries entières ci-dessus ont un rayon de convergence $\geqslant1$, on a $(1+z)^\alpha(1+z)^\beta=(1+z)^{\alpha+\beta}$

2. C'est la série de Taylor en 0 de la fonction $f(x)=\int_0^{+\infty}\frac{e^{-t}}{1+tx}\,dt$, qui est $\mathscr{C}^\infty$ sur $\mathbf{R}_+$, ce qui faisait dire à Euler que $\sum_{n=0}^{+\infty}(-1)^nn!=\int_0^{+\infty}\frac{e^{-t}}{1+t}\,dt$. On remarquera quand même que f satisfaît l'équation différentielle $x^2f'+xf+f=1$ de l'ex. V.1.5

quels que soient $z \in \mathrm{D}(0,1^-)$, et $\alpha, \beta \in \mathbf{C}$. En particulier, si $m \in \mathbf{N}-\{0\}$, alors $(1+z)^{1/m}$ est une racine m-ième de $1+z$, quel que soit $z \in \mathrm{D}(0,1^-)$.

Exercice V.1.9. — Soit $\alpha \in \mathbf{R}-\mathbf{N}$ [3].

(i) Exprimer $\binom{\alpha}{n}$ en termes de la fonction Γ.

(ii) En déduire qu'il existe $\mathrm{C}(\alpha) \in \mathbf{C}$ tel que $\binom{\alpha}{n} \sim \mathrm{C}(\alpha)(-1)^n n^{-1-\alpha}$. (On utilisera la formule de Stirling (ex. IV.1.5).)

Proposition V.1.10. — (i) *Si* $\mathrm{F} = \sum_{n=0}^{+\infty} a_n \mathrm{T}^n \in \mathbf{C}[[\mathrm{T}]]$, *alors* $\rho(\mathrm{F}^{(k)}) \geqslant \rho(\mathrm{F})$, *quel que soit* $k \in \mathbf{N}$, *et si* $|z_0| + |z-z_0| < \rho(\mathrm{F})$, *alors*

$$\mathrm{F}(z) = \sum_{k=0}^{+\infty} \Big(\sum_{n=0}^{+\infty} \binom{n+k}{k} a_{n+k} z_0^n \Big) (z-z_0)^k = \sum_{k=0}^{+\infty} \frac{\mathrm{F}^{(k)}(z_0)}{k!} (z-z_0)^k.$$

(ii) *Si* $|z_0| < \rho(\mathrm{F})$, *alors* $\lim_{z \to z_0} \frac{\mathrm{F}(z)-\mathrm{F}(z_0)}{z-z_0} = \mathrm{F}'(z_0)$.

Démonstration. — Si $|z_0| + |z-z_0| < \rho(\mathrm{F})$, on a

$$\begin{aligned} \sum_{k=0}^{+\infty} \Big(\sum_{n=0}^{+\infty} \binom{n+k}{k} |a_{n+k} z_0^n| \Big) |z-z_0|^k &= \sum_{m=0}^{+\infty} \sum_{n+k=m} \binom{m}{k} |a_m| |z_0^n| |z-z_0|^k \\ &= \sum_{m=0}^{+\infty} |a_m| (|z_0| + |z-z_0|)^m < +\infty, \end{aligned}$$

ce qui montre que la série double de la proposition est absolument convergente. En fixant k, on en déduit que $\mathrm{F}^{(k)}$ converge si $|z_0| < \rho(\mathrm{F})$, et donc $\rho(\mathrm{F}^{(k)}) \geqslant \rho(\mathrm{F})$. De plus, on peut réordonner les termes comme on veut, et commencer par sommer sur $n+k=m$, puis sommer sur $m \in \mathbf{N}$. La somme pour $n+k=m$ étant $\sum_{n+k=m} \binom{m}{n} a_m z_0^k (z-z_0)^n = a_m z^m$, cela démontre le (i).

Le (i) permet, en faisant le changement de variables $z = z_0 + h$, de supposer que $z_0 = 0$ pour démontrer le (ii). Or on a

$$\Big| \frac{\mathrm{F}(h)-\mathrm{F}(0)}{h} - \mathrm{F}'(0) \Big| = \Big| h \sum_{n=2}^{+\infty} a_n h^{n-2} \Big| \leqslant |h| \Big(\sum_{n=2}^{+\infty} |a_n| (\rho(\mathrm{F})/2)^{n-2} \Big), \quad \text{si } |h| < \rho(\mathrm{F})/2,$$

et comme $\sum_{n=2}^{+\infty} |a_n| (\rho(\mathrm{F})/2)^{n-2} < +\infty$, on en déduit que $\frac{\mathrm{F}(h)-\mathrm{F}(0)}{h} - \mathrm{F}'(0)$ tend vers 0 quand $h \to 0$, ce qui permet de conclure.

Remarque V.1.11. — On peut reformuler le (ii) de la proposition précédente en disant que, si $\mathrm{F} \in \mathbf{C}[[\mathrm{T}]]$ est de rayon de convergence non nul, alors F est *dérivable au sens complexe* dans $\mathrm{D}(0, \rho(\mathrm{F})^-)$, et que la dérivée au sens complexe de F est F'. Une récurrence immédiate permet donc de montrer que F est de classe $\mathscr{C}^\infty$ au sens complexe sur $\mathrm{D}(0, \rho(\mathrm{F})^-)$, et que la dérivée k-ième au sens complexe de F est la fonction associée à la série entière $\mathrm{F}^{(k)}$.

3. Les résultats de cet exercice s'étendent à $\alpha \in \mathbf{C}-\mathbf{N}$, une fois que l'on dispose de la fonction Γ dans le plan complexe (cf. th. VII.2.1 et prop. VII.2.9).

V.2. Exemples de fonctions holomorphes

1. Définition

Soient Ω un ouvert de $\mathbf{C}$, et $f : \Omega \to \mathbf{C}$. Si $z_0 \in \Omega$, si $r > 0$, et si $\mathrm{D}(z_0, r^-) \subset \Omega$, on dit que f est *développable en série entière sur* $\mathrm{D}(z_0, r^-)$, s'il existe $\mathrm{F} \in \mathbf{C}[[\mathrm{T}]]$, de rayon de convergence $\geqslant r$, telle que $f(z) = \mathrm{F}(z - z_0)$, pour tout $z \in \mathrm{D}(z_0, r^-)$. Il résulte du (i) de la prop. V.1.10 que si f est développable en série entière sur $\mathrm{D}(z_0, r^-)$, et si $\mathrm{D}(z_1, r_1^-) \subset \mathrm{D}(z_0, r^-)$, alors f est développable en série entière sur $\mathrm{D}(z_1, r_1^-)$.

On dit que f est *développable en série entière autour de* z_0 s'il existe $r > 0$ tel que f soit développable en série entière sur $\mathrm{D}(z_0, r^-)$, et on dit que f est *analytique sur* Ω ou encore que f est *holomorphe sur* Ω, si f est développable en série entière autour de tout point de Ω. Il résulte de la rem. V.1.11 qu'une fonction analytique sur Ω est de classe $\mathscr{C}^\infty$ au sens complexe sur Ω.

Exemple V.2.1. — (i) Un polynôme est une fonction holomorphe sur $\mathbf{C}$.

(ii) $z \mapsto \exp(\lambda z)$ est holomorphe sur $\mathbf{C}$, pour tout $\lambda \in \mathbf{C}$; sa dérivée est $z \mapsto \lambda \exp(\lambda z)$.

(iii) $z \mapsto \frac{1}{z}$ est holomorphe sur $\mathbf{C} - \{0\}$; sa dérivée est $z \mapsto \frac{-1}{z^2}$.

(iv) $z \mapsto \log(1+z)$ et $z \mapsto (1+z)^s$, si $s \in \mathbf{C}$, définies à partir des séries formelles de l'ex. V.1.3, sont holomorphes sur $\mathrm{D}(0, 1^-)$; leurs dérivées sont respectivement $z \mapsto \frac{1}{1+z}$ et $z \mapsto s(1+z)^{s-1}$.

(v) Si f et g sont holomorphes sur Ω, alors $f + g$ et fg sont holomorphes sur Ω ; leurs dérivées sont respectivement $f' + g'$ et $f'g + fg'$.

(vi) Si $f : \Omega_1 \to \Omega_2$ et $g : \Omega_2 \to \mathbf{C}$ sont holomorphes, alors $g \circ f$ est holomorphe sur Ω_1 ; sa dérivée est $(g' \circ f)f'$.

(vii) Si $f : \Omega_1 \to \Omega_2$ est holomorphe bijective, sa réciproque $f^{-1} : \Omega_2 \to \Omega_1$ est holomorphe.

(viii) Une fonction rationnelle est holomorphe sur l'ouvert complémentaire de ses pôles.

Démonstration. — Le (i) est évident. Le (ii) et le (iv) suivent de l'exemple V.1.7. Le (iii) se démontre en constatant que $\frac{1}{z} = \sum_{n=0}^{+\infty} \frac{(z_0 - z)^n}{z_0^{n+1}}$, si $|z - z_0| < |z_0|$. Le (v) résulte du lemme V.1.6. Le (vi) et (vii) pourraient se démontrer directement, mais nous attendrons d'en savoir plus pour en donner une démonstration élégante (cf. cor. V.4.8). Enfin, le (viii) se déduit des (i), (iii), (v) et (vi).

Exercice V.2.2. — (i) Montrer que $z \mapsto \sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$ et $z \mapsto \cos z = \frac{1}{2}(e^{iz} + e^{-iz})$ sont holomorphes sur $\mathbf{C}$, et que $z \mapsto \operatorname{cotg} \pi z = \frac{\cos \pi z}{\sin \pi z}$ est holomorphe sur $\mathbf{C} - \mathbf{Z}$.

(ii) Montrer que $z \mapsto |z|^2$ est $\mathscr{C}^\infty$ au sens réel sur $\mathbf{C} \cong \mathbf{R}^2$, mais n'est pas holomorphe.

2. Logarithme et fonctions puissances

Soit $\alpha \in \mathbf{R}$. L'application $z \mapsto e^z$ est holomorphe et est une bijection de la bande $\{z,\ \alpha < \mathrm{Im}(z) < \alpha + 2\pi\}$, sur $\mathbf{C}$ privé de la demi-droite $\mathbf{R}_+ e^{i\alpha}$ d'argument α (ou $\alpha + 2\pi$,

ce qui revient au même). La bijection réciproque

$$\log_\alpha : \mathbf{C} - \mathbf{R}_+ e^{i\alpha} \to \{z,\ \alpha < \mathrm{Im}(z) < \alpha + 2\pi\}.$$

est donc une fonction holomorphe, d'après le (vii) de l'ex. V.2.1.

Comme $\exp(\log_\alpha(z)) = z$ sur $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$, on obtient, en dérivant cette relation, que la dérivée de $\log_\alpha$ sur $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$ est $\frac{1}{z}$, et donc que $\log_\alpha$ vérifie les propriétés que l'on est en droit d'attendre d'une fonction logarithme. Le seul problème est qu'*on ne peut pas définir le logarithme comme une fonction holomorphe sur* $\mathbf{C}^*$ *tout entier*, à cause de la discontinuité le long de la demi-droite $\mathbf{R}_+ e^{i\alpha}$ (les limites « à gauche » et « à droite » diffèrent de $2i\pi$, le long de cette demi-droite). Ce problème [4] est dans la nature des choses : le logarithme est une fonction holomorphe *multivaluée* sur $\mathbf{C}^*$, et chacune des fonctions $\log_\alpha$ ci-dessus correspond au choix d'une détermination du logarithme, holomorphe dans un ouvert aussi grand que possible. La *détermination principale du logarithme* est la fonction $\log_{-\pi}$; c'est donc la détermination du logarithme, définie sur $\mathbf{C}$ privé de la demi-droite réelle négative $\mathbf{R}_-$, et qui vaut 0 en 1 ; ses valeurs ont une partie imaginaire dans l'intervalle $]-\pi, \pi[$. Dans la pratique, on ne met pas le α en indice, ce qui demande de *faire attention à ce que signifie exactement* $\log z$ dans la situation que l'on considère ; les valeurs possibles de $\log z$ étant les $2i\pi\, k + \log_{-\pi} z$, pour $k \in \mathbf{Z}$.

Exercice V.2.3. — Soit log la détermination principale du logarithme.

(i) Montrer que $\log z = \log|z| + i \arg z$, où $\arg z \in]-\pi, \pi[$ est l'argument principal de z.

(ii) Soient $z_1, z_2 \in \mathbf{C} - \mathbf{R}_-$, tels que $z_1 z_2 \in \mathbf{C} - \mathbf{R}_-$. Déterminer, suivant les cas, la valeur de $\log(z_1 z_2) - \log z_1 - \log z_2$.

Exercice V.2.4. — Soient $\mathrm{A} < \mathrm{B}$ deux réels, et $a = e^{\mathrm{A}}$ et $b = e^{\mathrm{B}}$. On note $\Omega(\mathrm{A}, \mathrm{B})$ la bande horizontale $\{z \in \mathbf{C},\ \mathrm{A} < \mathrm{Im}(z) < \mathrm{B}\}$ et $\mathrm{C}(a, b)$ la couronne $\{z \in \mathbf{C},\ a < |z| < b\}$. Soit $f : \Omega(\mathrm{A}, \mathrm{B}) \to \mathbf{C}$, périodique de période 1.

(i) Montrer qu'il existe une unique $\tilde{f} : \mathrm{C}(a, b) \to \mathbf{C}$, telle que $f(z) = \tilde{f}(e^{2i\pi z})$, pour tout $z \in \Omega(\mathrm{A}, \mathrm{B})$.

(ii) Montrer que $\tilde{f}$ est holomorphe sur $\mathrm{C}(a, b)$ si et seulement si f l'est sur $\Omega(\mathrm{A}, \mathrm{B})$.

Si $s \in \mathbf{C}^*$, on définit z^s par la formule $z^s = \exp(s \log z)$. Comme la fonction $\log z$ est multivaluée, il en est de même de z^s, et il faut donc bien faire attention au choix que l'on a fait de $\log z$. Si a est une valeur possible de z^s, les autres sont les $e^{2i\pi k s} a$, pour $k \in \mathbf{Z}$. En particulier, on peut se débrouiller, par un choix convenable de la détermination de $\log z$, pour que z^s soit holomorphe dans $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$, mais, *si* $s \notin \mathbf{Z}$, *la fonction* z^s *ne peut pas se prolonger en une fonction holomorphe sur* $\mathbf{C}^*$. Même si on prend la détermination principale du logarithme, il n'est pas toujours vrai que $z_1^s z_2^s = (z_1 z_2)^s$. Par contre, la

4. Il a fortement perturbé nos ancêtres. Bernoulli et Leibnitz se sont battus (épistolairement), en 1712-1713, sur la valeur de $\log(-1)$, l'un soutenant que $\log(-1) = 0$ car $2\log(-1) = \log(-1)^2 = \log 1 = 0$, et l'autre que $\log(-1)$ devait être imaginaire car $\log(-1) = -2 - \frac{2^2}{2} - \frac{2^3}{3} \cdots$ ne converge pas... Il a fallu attendre 1749 pour qu'Euler explique qu'un nombre complexe a une infinité de logarithmes. Le lecteur trouvera dans les exercices corrigés H.1.11, H.1.13 et dans la démonstration du th. VII.3.7, des exemples d'utilisation du logarithme complexe.

fonction $s \mapsto z^s$ est, elle, holomorphe sur $\mathbf{C}$ tout entier, et on a $z^{s_1+s_2} = z^{s_1}z^{s_2}$ (si on ne s'amuse pas à changer la valeur de $\log z$). En particulier, si $m \in \mathbf{N} - \{0\}$, alors $z^{1/m}$ est une racine m-ième de z, quelle que soit la détermination du logarithme choisie.

Remarque V.2.5. — On verra plus loin (prop. V.4.10 et ex. V.4.12) que les restrictions de $z \mapsto \log(1+z)$ et $z \mapsto (1+z)^s$, si $s \in \mathbf{C}$, coïncident avec les fonctions du (iv) de l'ex. V.2.1, si on choisit la détermination principale du logarithme.

Exercice V.2.6. — (i) Soit $\Omega = \mathbf{C} - [0,1]$. Montrer qu'il existe deux fonctions f, holomorphes sur Ω, dont le carré est $z \mapsto z(z-1)$.

(ii) Soient $a_1, \ldots, a_{2n}$, des éléments distincts de $\mathbf{C}$. Montrer qu'il existe une permutation σ de $1, \ldots, 2n$ telle que les segments $[a_{\sigma(2i-1)}, a_{\sigma(2i)}]$, pour $1 \leqslant i \leqslant n$ soient disjoints, et que si Ω est l'ouvert complémentaire de ces segments, il existe deux fonctions f, holomorphes sur Ω, dont le carré est $z \mapsto \prod_{i=1}^{2n}(z-a_i)$.

V.3. Premières propriétés des fonctions holomorphes

1. Relations de Cauchy-Riemann

Remarque V.3.1. — (i) On peut aussi considérer une fonction holomorphe f comme une fonction, à valeurs complexes, des variables $x = \mathrm{Re}(z)$ et $y = \mathrm{Im}(z)$. En notant P et Q les parties réelle et imaginaire de f, cela permet de voir f comme une fonction de classe $\mathscr{C}^1$ (et même de classe $\mathscr{C}^\infty$) d'un ouvert de $\mathbf{R}^2$ dans $\mathbf{R}^2$. La dérivabilité de f au sens complexe en z_0 s'exprime alors par le fait que la différentielle de f en z_0 est une similitude, ce qui se traduit par les *relations de Cauchy-Riemann*

$$\frac{\partial \mathrm{P}}{\partial x}(z_0) = \frac{\partial \mathrm{Q}}{\partial y}(z_0) = \mathrm{Re}(f'(z_0)) \quad \text{et} \quad \frac{\partial \mathrm{P}}{\partial y}(z_0) = -\frac{\partial \mathrm{Q}}{\partial x}(z_0) = -\mathrm{Im}(f'(z_0))$$

entre les dérivées partielles des parties réelle et imaginaire de f en z_0. Le jacobien de f en z_0 est alors $|f'(z_0)|^2$; en particulier, sa nullité est équivalente à celle de $f'(z_0)$.

(ii) Comme les similitudes ont comme propriété de conserver les angles de vecteurs (mais pas les longueurs), *une fonction holomorphe* f hérite de cette propriété, et donc *conserve les angles*, ce qui signifie, par exemple, qu'elle transforme deux courbes se coupant à angle droit en z_0 en deux courbes se coupant à angle droit en $f(z_0)$, si $f'(z_0) \neq 0$.

(iii) Réciproquement, soit $f : \Omega \to \mathbf{C}$ une fonction, de classe $\mathscr{C}^1$ en tant que fonction de x et y. Soient $\frac{\partial}{\partial z}$ et $\frac{\partial}{\partial \overline{z}}$, les opérateurs différentiels définis par

$$\frac{\partial}{\partial z} = \frac{1}{2}\Big(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\Big) \quad \text{et} \quad \frac{\partial}{\partial \overline{z}} = \frac{1}{2}\Big(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\Big).$$

Ces notations sont justifiées par les formules

$$\frac{\partial}{\partial z}z = 1, \quad \frac{\partial}{\partial z}\overline{z} = 0 \quad \text{et} \quad \frac{\partial}{\partial \overline{z}}z = 0, \quad \frac{\partial}{\partial \overline{z}}\overline{z} = 1.$$

On en déduit que l'on a $f(z_0+h) = f(z_0) + \frac{\partial f}{\partial z}(z_0)\cdot h + \frac{\partial f}{\partial \overline{z}}(z_0)\cdot \overline{h} + o(|h|)$ au voisinage de $h = 0$. La différentielle de f est une similitude, si et seulement si $\frac{\partial f}{\partial \overline{z}}(z_0) = 0$, et donc

f est dérivable au sens complexe en z_0, si et seulement si $\frac{\partial f}{\partial \overline{z}}(z_0) = 0$. Ceci permet de voir une fonction de classe $\mathscr{C}^1$ au sens complexe, comme une fonction qui « ne dépend que de z et pas de $\overline{z}$ » [5], et explique un peu le miracle de la prop. V.4.7.

Exercice V.3.2. — (i) Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ de degré $\geqslant 2$. Montrer que, si P ne s'annule pas dans $\mathbf{C}$, alors $1/\mathrm{P}$ et ses dérivées partielles par rapport à x et y sont de carrés sommables sur $\mathbf{C} \cong \mathbf{R}^2$. En déduire que la transformée de Fourier de $1/\mathrm{P}$ (vu comme fonction de x et y) est identiquement nulle, puis que $\mathbf{C}$ est algébriquement clos.

(ii) Adapter l'argument ci-dessus pour n'utiliser que la transformée de Fourier dans $\mathrm{L}^1(\mathbf{C})$.

2. Théorème des zéros isolés et unicité du prolongement analytique

Si f est analytique sur Ω, et si $z_0 \in \Omega$, on définit *l'ordre du zéro* $v_{z_0}(f) \in \mathbf{N} \cup \{+\infty\}$ *de* f *en* z_0 comme la valuation $v_{\mathrm{T}}(\mathrm{F})$ de la série entière F telle que $f(z) = \mathrm{F}(z - z_0)$. Si cet ordre est $+\infty$, c'est que la fonction f est identiquement nulle dans un voisinage de z_0 (i.e. il existe $r > 0$ tel que $f(z) = 0$ si $z \in \mathrm{D}(z_0, r^-)$). Si cet ordre est fini, égal à k, on peut factoriser F sous la forme $\mathrm{F} = \mathrm{T}^k\mathrm{G}$, avec $\mathrm{G}(0) \neq 0$. Par continuité, $\mathrm{G}(z - z_0)$ ne s'annule pas dans un voisinage de z_0, ce qui prouve que z_0 est le seul zéro de f dans ce voisinage.

Théorème V.3.3. — (des zéros isolés) *Soit Ω un ouvert connexe de $\mathbf{C}$. Si f est une fonction holomorphe sur Ω qui n'est pas identiquement nulle, et si $z_0 \in \Omega$ est un zéro de f, alors il existe $r > 0$ tel que z_0 soit le seul zéro de f sur $\mathrm{D}(z_0, r)$.*

Démonstration. — D'après la discussion précédant le théorème, z_0 est un zéro non isolé si et seulement si $v_{z_0}(f) = +\infty$. L'ensemble des zéros non isolés est donc fermé car c'est l'intersection des fermés $\{z,\ f^{(n)}(z) = 0\}$, pour $n \in \mathbf{N}$, et ouvert car si $f^{(n)}(z_0) = 0$ pour tout n, alors f est identiquement nulle dans $\mathrm{D}(z_0, r^-)$, si f est développable en série entière dans $\mathrm{D}(z_0, r^-)$. Comme Ω est supposé connexe, on en déduit que l'ensemble des zéros non isolés est soit Ω (auquel cas f est identiquement nulle), soit l'ensemble vide. Ceci permet de conclure.

Exercice V.3.4. — Soit $f : \Omega \to \mathbf{C}$ holomorphe, et soient $x_0 \in \Omega$ et $r > 0$ tel que $\mathrm{D}(x_0, r) \subset \Omega$. On suppose que $f(x_0) \neq 0$; montrer que f n'a qu'un nombre fini de zéros dans $\mathrm{D}(x_0, r)$.

Exercice V.3.5. — Soit f holomorphe sur $\mathbf{C}$ vérifiant $f(\frac{1}{n}) = \frac{1}{n^2}$, pour tout $n \in \mathbf{N} - \{0\}$. Montrer que $f(z) = z^2$ pour tout $z \in \mathbf{C}$.

Exercice V.3.6. — Peut-on trouver une fonction $\mathscr{C}^\infty$, non identiquement nulle, à support compact dans $\mathbf{R}$, dont la transformée de Fourier soit à support compact ?

5. Ceci ne doit pas être pris littéralement vu que $\overline{z}$ et z ne sont pas indépendants, mais se comprend bien si on regarde un polynôme en $x = \frac{1}{2}(z + \overline{z})$ et $y = \frac{1}{2i}(z - \overline{z})$ comme un polynôme en z et $\overline{z}$: on voit que $\mathrm{P}(x, y)$ définit une fonction holomorphe si et seulement si le polynôme $\mathrm{Q}(z, \overline{z}) = \mathrm{P}(\frac{1}{2}(z+\overline{z}), \frac{1}{2i}(z-\overline{z}))$ n'a pas de terme en $\overline{z}$.

Corollaire V.3.7. — (Unicité du prolongement analytique) *Soient $\Omega \subset \Omega'$ deux ouverts non vides de $\mathbf{C}$. Si Ω' est connexe, et si f et g sont deux fonctions analytiques sur Ω' ayant la même restriction à Ω, alors $f = g$ sur Ω' tout entier.*

Démonstration. — Il suffit d'appliquer le théorème des zéros isolés à $f - g$.

Remarque V.3.8. — Soit f une fonction holomorphe sur un ouvert Ω de $\mathbf{C}$, et soit Ω' un ouvert connexe de $\mathbf{C}$ contenant Ω. Il est, en général, impossible de trouver une fonction holomorphe g sur Ω' dont la restriction à Ω soit f. Dans le cas où c'est possible, le corollaire précédent montre que g est unique ; elle est appelée *le prolongement analytique de f à Ω'*.

On prendra garde au problème suivant. Si Ω_1 et Ω_2 sont deux ouverts connexes, contenant Ω, sur lesquels f admet des prolongements analytiques f_1 et f_2, on ne peut pas en conclure, en général, que $f_1 = f_2$ sur $\Omega_1 \cap \Omega_2$ (le problème étant que $\Omega_1 \cap \Omega_2$ n'a aucune raison d'être connexe). Le logarithme fournit un exemple de ce phénomène. Évidemment, si f admet un prolongement analytique à $\mathbf{C}$ tout entier, ce prolongement analytique est véritablement unique.

Exemple V.3.9. — La fonction analytique f définie sur $\mathrm{D}(0,1^-)$ par $f(z) = \sum_{n=0}^{+\infty} z^n$ admet un prolongement analytique à $\mathbf{C} - \{1\}$: en effet, elle coïncide [6], sur $\mathrm{D}(0,1^-)$, avec $\frac{1}{1-z}$ qui est holomorphe sur $\mathbf{C} - \{1\}$. Cet exemple n'est qu'à moitié convaincant car on est parti de la fonction $\frac{1}{1-z}$ qui est visiblement holomorphe sur $\mathbf{C} - \{1\}$, mais on verra des exemples moins banals plus tard (ex. V.5.9, th. VII.3.4 et VII.4.4, ou prob. H.10 par exemple).

Exercice V.3.10. — Montrer que $f(z) = \sum_{n=0}^{+\infty} z^{n!}$ est holomorphe sur $\mathrm{D}(0,1^-)$, mais n'a de prolongement analytique à aucun [7] ouvert connexe contenant strictement $\mathrm{D}(0,1^-)$. Quid de $\sum_{n=0}^{+\infty} \frac{z^{n!}}{n!}$?

---

6. On a donc envie d'écrire $1+2+4+8+\cdots = -1$, ce qu'Euler aurait fait sans aucun scrupule. Dans la même veine, on a (ex. VII.3.6)

$$1+1+1+1+\cdots = \zeta(0) = \frac{-1}{2}, \quad 1+2+3+4+\cdots = \zeta(-1) = \frac{-1}{12}, \quad 1+4+9+16+\cdots = \zeta(-2) = 0, \cdots$$

Manipuler des séries divergentes est amusant mais demande un certain doigté. Par exemple, il ne faut pas confondre $\sum_{n=0}^{+\infty} 1 = 1 + \zeta(0) = \frac{1}{2}$ avec $\sum_{n=1}^{+\infty} 1 = \zeta(0) = -\frac{1}{2}$. Les physiciens ont acquis une dextérité certaine en la matière ; les mathématiciens ont plus de complexes depuis que Cauchy a déclaré, dans son *Cours d'analyse* à l'École polytechnique, paru en 1821 : « *Je me suis vu forcé d'admettre plusieurs propositions qui paraitront peut-être un peu dures au premier abord. Par exemple (...) qu'une série divergente n'a pas de somme.* »

7. On peut montrer, mais c'est nettement plus difficile, que si $\sum_{n=0}^{+\infty} a_n z^n$, avec $a_n \in \mathbf{Z}$ pour tout n, a pour rayon de convergence 1, et s'il existe un ouvert connexe contenant strictement $\mathrm{D}(0,1^-)$ sur lequel f admet un prolongement analytique, alors f est une fraction rationnelle de la forme $\frac{\mathrm{P}(z)}{(1-z^{\mathrm{N}})^k}$, où P est un polynôme à coefficients dans $\mathbf{Z}$ (th. de Pólya-Carlson (1921)), cf. prob. H.13 pour un ancêtre de ce résultat.

3. Principe du maximum

Théorème V.3.11. — (Principe du maximum) *Si Ω est un ouvert connexe de $\mathbf{C}$, si $z_0 \in \Omega$, si f holomorphe sur Ω, et si $|f|$ admet un maximum local en z_0, alors f est constante sur Ω.*

Démonstration. — Si f n'est pas constante sur Ω, la fonction $f - f(z_0)$ n'est pas identiquement nulle sur Ω, et Ω étant connexe, le développement en série entière de $f - f(z_0)$ autour de z_0 n'est pas identiquement nul. Il existe donc $k \in \mathbf{N} - \{0\}$ et $\alpha \in \mathbf{C^*}$ tels que $f(z) = f(z_0) + \alpha \cdot (z - z_0)^k + (z - z_0)^k \varepsilon_0(z)$, avec $\lim_{z \to z_0} \varepsilon_0(z) = 0$.

• Si $f(z_0) = 0$, alors z_0 est un zéro isolé de f, et $|f(z)| > |f(z_0)|$, quel que soit z dans un voisinage de z_0 ; en particulier, $|f|$ n'admet pas de maximum local en z_0.

• Si $f(z_0) \neq 0$, soit β avec $\beta^k = \alpha^{-1} f(z_0)$. On a alors $f(z_0 + t\beta) = f(z_0)(1 + t^k + t^k \varepsilon_1(t))$, avec $\lim_{t \to 0} \varepsilon_1(t) = 0$. Ceci implique que $|f(z_0 + t\beta)| > |f(z_0)|$, si $t > 0$ est assez petit, et donc que $|f|$ n'admet pas de maximum local en z_0.

Ceci permet de conclure.

Remarque V.3.12. — Le principe du maximum est souvent utilisé sous la forme : *une fonction holomorphe atteint son maximum au bord.* Autrement dit, si K est un compact et si f est holomorphe sur un ouvert contenant K, alors le maximum de $|f|$ sur K est atteint sur la frontière de K.

Exercice V.3.13. — Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ non constant. Montrer que, si P ne s'annule pas sur $\mathbf{C}$, alors $|1/\mathrm{P}|$ atteint son maximum en un point de $\mathbf{C}$. En déduire que $\mathbf{C}$ est algébriquement clos.

Exercice V.3.14. — Soient $a < b \in \mathbf{R}$, et soit f une fonction holomorphe dans un voisinage ouvert de la bande verticale $\mathrm{B} = \{z \in \mathbf{C},\ a \leqslant \mathrm{Re}(z) \leqslant b\}$. On suppose f bornée sur les droites $\mathrm{Re}(z) = a$ et $\mathrm{Re}(z) = b$.

(i) Montrer que, s'il existe $\mathrm{C} > 0$ et $c > 0$ tels que $|f(z)| \leqslant \mathrm{C}e^{c|\mathrm{Im}(z)|}$, quel que soit $z \in \mathrm{B}$, alors f est bornée sur B. (On considérera la fonction $e^{\varepsilon z^2} f(z)$.)

(ii) Montrer de même que, s'il existe $\mathrm{C} > 0$, $c > 0$, et $\mathrm{N} \in \mathbf{N}$ tels que $|f(z)| \leqslant \mathrm{C}e^{c|\mathrm{Im}(z)|^{\mathrm{N}}}$, quel que soit $z \in \mathrm{B}$, alors f est bornée sur B.

(iii) Construire une fonction holomorphe sur $\mathbf{C}$, bornée sur chacune des droites $\mathrm{Re}(z) = a$ et $\mathrm{Re}(z) = b$, et non bornée sur B (penser à des exponentielles d'exponentielles).

Exercice V.3.15. — (Lemme de Schwarz) Soit $\mathrm{D} = \{z \in \mathbf{C},\ |z| < 1\}$, et soit f holomorphe de D dans D vérifiant $f(0) = 0$.

(i) Montrer que $|f(z)| \leqslant |z|$, quel que soit $z \in \mathrm{D}$. (Considérer $z \mapsto g(z) = \frac{f(z)}{z}$.)

(ii) Montrer que, si $|f'(0)| = 1$, alors $f(z) = f'(0)z$ quel que soit $z \in \mathrm{D}$.

(iii) Montrer que si f est une bijection holomorphe de D dans D, et si $f(0) = 0$, alors il existe $\theta \in [0, \pi]$ tel que $f(z) = e^{2i\theta} z$, quel que soit $z \in \mathrm{D}$.

(iv) Montrer que si f n'est pas bijective, alors pour tout compact K de D, il existe $c_{\mathrm{K}} < 1$ tel que $|f(z)| \leqslant c_{\mathrm{K}}|z|$, pour tout $z \in \mathrm{K}$.

(v) Soit $f^{\circ n} = f \circ f \circ \cdots \circ f$ (n fois). Montrer que, si f n'est pas bijective, alors $f^{\circ n}$ tend uniformément vers 0 sur tout compact de D.

Exercice V.3.16. — Soit $\mathscr{H} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$ le demi-plan de Poincaré.

(i) Vérifer que, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{R})$, alors $\gamma \cdot z = \frac{az+b}{cz+d} \in \mathscr{H}$, et que l'on a $\gamma_1\gamma_2 \cdot z = \gamma_1 \cdot (\gamma_2 \cdot z)$.

(ii) En déduire que $\gamma \mapsto \varphi_\gamma$, où φ_γ est la transformation $z \mapsto \gamma \cdot z$, est un morphisme de groupes de $\mathbf{SL}_2(\mathbf{R})$ dans le groupe $\mathrm{Aut}(\mathscr{H})$ des bijections holomorphes de $\mathscr{H}$.

(iii) Montrer que, si $z \in \mathscr{H}$, il existe $\gamma \in \mathbf{SL}_2(\mathbf{R})$, avec $z = \gamma \cdot i$. En déduire que, si $\varphi \in \mathrm{Aut}(\mathscr{H})$, alors il existe $\gamma \in \mathbf{SL}_2(\mathbf{R})$ tel que i soit un point fixe de $\varphi_\gamma \circ \varphi$.

(iv) Soit $h(z) = \frac{i-z}{i+z}$. Montrer que h est une bijection holomorphe de $\mathscr{H}$ dans D dont la réciproque h^{-1} est donnée par la formule $h^{-1}(z) = i\frac{1-z}{1+z}$.

(v) Montrer, en utilisant le lemme de Schwarz (ex. V.3.15), que si $\varphi \in \mathrm{Aut}(\mathscr{H})$ fixe i, alors il existe $\theta \in [0, \pi]$ tel que $\varphi(z) = \frac{z\cos\theta + \sin\theta}{-z\sin\theta + \cos\theta}$. (On considèrera $\psi = h \circ \varphi \circ h^{-1}$.)

(vi) Montrer que $\gamma \mapsto \varphi_\gamma$ induit une surjection de $\mathbf{SL}_2(\mathbf{R})$ sur $\mathrm{Aut}(\mathscr{H})$; en déduire que $\mathrm{Aut}(\mathscr{H})$ est isomorphe à $\mathbf{SL}_2(\mathbf{R})/\{\pm 1\}$.

V.4. La formule intégrale de Cauchy et ses conséquences

1. Généralités sur les chemins

Un *chemin* γ (sous-entendu $\mathscr{C}^1$ par morceaux) dans un ouvert Ω de $\mathbf{C}$ est une application $\gamma : [a, b] \to \Omega$, continue et $\mathscr{C}^1$ par morceaux, d'un intervalle compact $[a, b]$ de $\mathbf{R}$ dans Ω. Le point $\gamma(a)$ est *l'origine* de γ et $\gamma(b)$ en est *l'extrémité*. On dit que γ est un *lacet* si son origine et son extrémité coïncident. Si $t \in [a, b]$ est un point où les dérivées à droite et à gauche de γ sont distinctes, on dit que $\gamma(t)$ est un *point anguleux de* γ. Par hypothèse, γ n'a qu'un nombre fini de points anguleux.

Si $\gamma(t) = x(t) + iy(t)$, on définit la *longueur* $\lg(\gamma)$ de γ par la formule

$$\lg(\gamma) = \int_a^b \sqrt{x'(t)^2 + y'(t)^2}\, dt = \int_a^b |\gamma'(t)|\, dt.$$

La longueur est invariante par *reparamètrage* (un reparamètrage de γ est un chemin de la forme $\gamma_1 = \gamma \circ \varphi$, où $\varphi : [a_1, b_1] \to [a, b]$ est une bijection croissante de classe $\mathscr{C}^1$). En effet, on a

$$\begin{aligned}\lg(\gamma_1) &= \int_{a_1}^{b_1} \sqrt{(x \circ \varphi)'(t)^2 + (y \circ \varphi)'(t)^2}\, dt = \int_{a_1}^{b_1} \sqrt{(x' \circ \varphi)(t)^2\varphi'(t)^2 + (y' \circ \varphi)(t)^2\varphi'(t)^2}\, dt \\ &= \int_{a_1}^{b_1} \sqrt{(x' \circ \varphi)(t)^2 + (y' \circ \varphi)(t)^2}\varphi'(t)\, dt = \int_a^b \sqrt{x'(s)^2 + y'(s)^2}\, ds = \lg(\gamma).\end{aligned}$$

Si $\gamma : [a, b] \to \Omega$ est un chemin, on définit le *chemin opposé* $\gamma^{\mathrm{opp}} : [a, b] \to \Omega$ de γ, par $\gamma^{\mathrm{opp}}(t) = \gamma(a + b - t)$.

Si $\gamma_1 : [a_1, b_1] \to \Omega$ et $\gamma_2 : [a_2, b_2] \to \Omega$ sont deux chemins, on dit que γ_1 et γ_2 sont *composables* si l'origine de γ_2 coïncide avec l'extrémité de γ_1, et on définit le chemin $\gamma_1 \cdot \gamma_2 : [a_1, b_2 - a_2 + b_1] \to \Omega$, *composé de* γ_1 *et* γ_2, en posant $\gamma_1 \cdot \gamma_2(t) = \gamma_1(t)$, si $t \in [a_1, b_1]$ et $\gamma_1 \cdot \gamma_2(t) = \gamma_2(t + a_2 - b_1)$, si $t \in [b_1, b_2 - a_2 + b_1]$.

Exemple V.4.1. — (chemins standard)

• Si $z_0 \in \mathbf{C}$ et $r > 0$, on note $\mathrm{C}(z_0, r) : [0, 1] \to \mathbf{C}$ le chemin $t \mapsto z_0 + re^{2i\pi t}$; c'est le *cercle de centre* z_0 *et de rayon* r *parcouru dans le sens direct*. Sa longueur est $2\pi r$.

• Si $a, b \in \mathbf{C}$, on note $[a,b] : [0,1] \to \mathbf{C}$ le chemin $t \mapsto a + t(b-a)$; c'est le *segment d'origine a et d'extrémité b*. Sa longueur est $|b-a|$.

2. Intégration le long d'un chemin

On identifie $\mathbf{C}$ à $\mathbf{R}^2$, en écrivant z sous la forme $z = x+iy$. Une 1-*forme* sur un ouvert Ω de $\mathbf{C}$ est une expression [8] du type $\mathrm{P}\,dx + \mathrm{Q}\,dy$, où P, Q sont des fonctions continues sur Ω. Si f est une fonction de classe $\mathscr{C}^1$ sur Ω, la différentielle df de f peut être vue comme une 1-forme : on a $df = \frac{\partial f}{\partial x}\,dx + \frac{\partial f}{\partial y}\,dy$.

Si $\omega = \mathrm{P}\,dx + \mathrm{Q}\,dy$ est une 1-forme sur Ω, et si $\gamma : [a,b] \to \Omega$ est un chemin dans Ω, on définit l'intégrale $\int_\gamma \omega$ par la formule

$$\int_\gamma \omega = \int_a^b \mathrm{P}(\gamma(t))d(x(\gamma(t))) + \mathrm{Q}(\gamma(t))d(y(\gamma(t))) = \int_a^b \mathrm{P}(\gamma(t))(x\circ\gamma)'(t) + \mathrm{Q}(\gamma(t))(y\circ\gamma)'(t))\,dt.$$

Dans l'intégrale ci-dessus, $(x\circ\gamma)'(t)$ et $(y\circ\gamma)'(t)$ sont bien définis sauf aux points anguleux, mais comme ceux-ci sont en nombre fini, cela n'affecte pas l'intégrale.

Théorème V.4.2. — (i) *$\int_\gamma \omega$ est invariante par reparamètrage : si $\varphi : [a_1, b_1] \to [a,b]$ une bijection croissante de classe $\mathscr{C}^1$, et si $\gamma_1 = \gamma \circ \varphi$, alors $\int_{\gamma_1} \omega = \int_\gamma \omega$.*

(ii) *$\int_{\gamma^{\mathrm{opp}}} \omega = -\int_\gamma \omega$.*

(iii) *Si γ_1 et γ_2 sont composables, alors $\int_{\gamma_1\cdot\gamma_2} \omega = \int_{\gamma_1} \omega + \int_{\gamma_2} \omega$.*

(iv) *Si $\omega = df$, alors $\int_\gamma \omega = f(\gamma(b)) - f(\gamma(a))$.*

Démonstration. — Le (i) résulte du calcul suivant :

$$\begin{aligned}\int_{\gamma_1} \omega &= \int_{a_1}^{b_1} \big(\mathrm{P}(\gamma\circ\varphi(t))(x\circ\gamma\circ\varphi)'(t) + \mathrm{Q}(\gamma\circ\varphi(t))(y\circ\gamma\circ\varphi)'(t)\big)\,dt \\ &= \int_{\varphi(a_1)}^{\varphi(b_1)} \big(\mathrm{P}(\gamma(s))(x\circ\gamma)'(s) + \mathrm{Q}(\gamma(s))(y\circ\gamma)'(s)\big)\,ds = \int_\gamma \omega.\end{aligned}$$

8. Plus généralement, si Ω est un ouvert de $\mathbf{R}^n$, et si $p \leqslant n$, une *p-forme* sur Ω est une expression du type

$$\omega = \sum_{i_1<i_2<\cdots<i_p} f_{i_1,\ldots,i_p} dx_{i_1} \wedge \cdots \wedge dx_{i_p},$$

où les $f_{i_1,\ldots,i_p}$ sont des fonctions continues sur Ω. (Une 0-forme est juste, par convention, une fonction continue sur Ω.) On voit aussi souvent une p-forme ω sur Ω comme une fonction $x \mapsto \omega_x$, continue sur Ω, à valeurs dans les formes p-linéaires alternées : si $u_1, \ldots, u_p$ sont p vecteurs de $\mathbf{R}^n$, avec $u_i = (u_{i,1}, \ldots, u_{i,n})$, et si $x \in \Omega$, alors (cf. ex. 6.1 du Vocabulaire) :

$$\omega_x(u_1, \ldots, u_p) = \sum_{i_1<i_2<\cdots<i_p} f_{i_1,\ldots,i_p}(x) \sum_{\sigma\in \mathrm{S}_p} \mathrm{sign}(\sigma) u_{1,i_{\sigma(1)}} \cdots u_{p,i_{\sigma(p)}}.$$

Ces objets jouent un rôle très important en géométrie différentielle. L'exemple de base est la 1-forme df, si f est de classe $\mathscr{C}^1$ sur Ω. Sa valeur en x est la forme linéaire $u \mapsto \lim_{t\to 0} \frac{f(x+tu)-f(x)}{t} = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(x)\,u_i$.

Le (ii) suit, via le changement de variable $t \mapsto a+b-t$, de ce que les bornes d'intégration sont échangées.

Le (iii) est immédiat.

Le (iv) résulte du calcul suivant :

$$\begin{aligned}\int_\gamma df &= \int_a^b \big(\frac{\partial f}{\partial x}(\gamma(t))(x\circ\gamma)'(t) + \frac{\partial f}{\partial y}(\gamma(t))(y\circ\gamma)'(t)\big)\,dt \\ &= \int_a^b (f\circ\gamma)'(t)\,dt = f(\gamma(b)) - f(\gamma(a)).\end{aligned}$$

On note dz la différentielle $dx + i\,dy$. Si f est une fonction continue sur Ω, la 1-forme $f(z)dz$ n'est donc autre que $f(x+iy)\,dx + if(x+iy)\,dy$. Si $\gamma : [a,b] \to \Omega$ est un chemin $\mathscr{C}^1$ par morceaux, alors

$$\int_\gamma f(z)\,dz = \int_a^b f(\gamma(t))\big((x\circ\gamma)'(t) + i(y\circ\gamma)'(t)\big)\,dt = \int_a^b f(\gamma(t))\gamma'(t)\,dt.$$

La très utile majoration du lemme suivant est immédiate, puisque $\lg(\gamma) = \int_a^b |\gamma'(t)|\,dt$.

Lemme V.4.3. — $|\int_\gamma f(z)\,dz| \leqslant \lg(\gamma)\cdot \sup_{z\in\gamma([a,b])} |f(z)|$.

Exemple V.4.4. — (Intégration sur les chemins standard)

(i) Si $z_0 \in \mathbf{C}$ et $r > 0$, alors $\int_{\mathrm{C}(z_0,r)} f(z)\,dz = 2i\pi r \int_0^1 f(z_0 + re^{2i\pi t})e^{2i\pi t}\,dt$.

(ii) Si $a, b \in \mathbf{C}$, alors $\int_{[a,b]} f(z)\,dz = (b-a)\int_0^1 f(a+t(b-a))\,dt$.

Exercice V.4.5. — Soient Ω_1, Ω_2 des ouverts de $\mathbf{C}$, $f : \Omega_1 \to \mathbf{C}$ continue et $\varphi : \Omega_2 \to \Omega_1$ holomorphe. Montrer que si $\gamma : [a,b] \to \Omega_2$ est un chemin, alors $\int_\gamma (f\circ\varphi)\varphi'(z)\,dz = \int_{\varphi\circ\gamma} f(z)\,dz$.

3. La formule de Cauchy

Théorème V.4.6. — (Formule intégrale de Cauchy, 1825) *Soit f de classe $\mathscr{C}^1$ au sens complexe sur Ω, ouvert de $\mathbf{C}$, et soient $z_0 \in \Omega$ et $r > 0$, tels que $\mathrm{D}(z_0, r) \subset \Omega$. Alors, pour tout $z \in \mathrm{D}(z_0, r^-)$, on a*

$$f(z) = \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\,dw.$$

Démonstration. — Si $w \in \mathrm{C}(r_0, r)$ et $z \in \mathrm{D}(z_0, r^-)$, on a $|z - z_0| < |w - z_0|$, et donc $\frac{1}{w-z} = \sum_{n=0}^{+\infty} \frac{(z-z_0)^n}{(w-z_0)^{n+1}}$. Comme la convergence de la série est uniforme sur le cercle, on peut intervertir somme et intégrale, ce qui nous donne, en posant $w = z_0 + re^{2i\pi\,t}$,

$$\int_{\mathrm{C}(z_0,r)} \frac{dw}{w-z} = \sum_{n=0}^{+\infty} \int_{\mathrm{C}(z_0,r)} \frac{(z-z_0)^n}{(w-z_0)^{n+1}}\,dw = \sum_{n=0}^{+\infty} \int_0^1 \frac{(z-z_0)^n}{(re^{2i\pi\,t})^{n+1}}\,2i\pi\,r\,e^{2i\pi\,t}\,dt,$$

et comme tous les termes de la série sont nuls sauf celui pour $n = 0$ qui vaut $2i\pi$, on obtient $\int_{\mathrm{C}(z_0,r)} \frac{dw}{w-z} = 2i\pi$. On en tire l'identité

$$\Big(\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\,dw\Big) - f(z) = \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)-f(z)}{w-z}\,dw.$$

Maintenant, $\frac{f(w)-f(z)}{w-z} = \int_0^1 f'(w+u(z-w))\,du$, et

$$\int_{\mathrm{C}(z_0,r)} \int_0^1 f'(w+u(z-w))\,du\,dw = \int_0^1 \int_0^1 f'\big((1-u)(z_0+re^{2i\pi t})+uz\big)\,du\,2i\pi\,re^{2i\pi t}\,dt.$$

La fonction $(t,u) \mapsto f'\big((1-u)(z_0+re^{2i\pi t})+uz\big)\,2i\pi\,re^{2i\pi t}$ est sommable car continue sur le compact $[0,1]^2$; on peut donc utiliser le th. de Fubini pour intervertir les variables. Or

$$\int_0^1 f'\big((1-u)(z_0+re^{2i\pi t})+uz\big)2i\pi\,re^{2i\pi t}\,dt = \Big[\frac{1}{1-u} f\big((1-u)(z_0+re^{2i\pi t})+uz\big)\Big]_{t=0}^{t=1} = 0,$$

pour tout $u \neq 1$. On en déduit la nullité de l'intégrale double et le résultat.

4. Holomorphie des fonctions dérivables au sens complexe

Le th. V.4.6 a des conséquences totalement surprenantes pour quelqu'un de familier avec la théorie des fonctions d'une variable réelle [(9)]. La prop. V.4.7 ci-dessous en est un premier exemple, puisqu'elle montre qu'une fonction de classe $\mathscr{C}^1$ au sens complexe est en fait holomorphe (et donc, a fortiori, de classe $\mathscr{C}^\infty$). Le (i) de la rem. V.4.9 et le th. V.5.1 fournissent d'autres exemples de phénomènes un peu miraculeux.

Proposition V.4.7. — *Si f vérifie la formule de Cauchy, et si on définit $a_n \in \mathbf{C}$, pour $n \in \mathbf{N}$, par*

$$a_n = \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{(w-z_0)^{n+1}}\,dw,$$

la série $\mathrm{F}(\mathrm{T}) = \sum_{n=0}^{+\infty} a_n \mathrm{T}^n$ a un rayon de convergence $\geqslant r$, et on a $f(z) = \mathrm{F}(z-z_0)$ quel que soit $z \in \mathrm{D}(z_0, r^-)$.

---

9. • La fonction $\varphi_0(x) = e^{-x^{-2}}$, prolongée par continuité en 0, est $\mathscr{C}^\infty$ sur $\mathbf{R}$, mais n'est pas développable en série entière autour de 0, puisque toutes ses dérivées sont nulles en 0 et $\varphi_0(x) > 0$ si $x \neq 0$.

• La fonction $\frac{1}{x^2+1}$ est analytique sur $\mathbf{R}$, mais n'est pas développable en série entière sur $]-(1+\varepsilon), 1+\varepsilon[$, si $\varepsilon > 0$, car le développement de Taylor $\sum_{n=0}^{+\infty}(-x^2)^n$ en 0 a un rayon de convergence égal à 1.

• Il existe des fonctions continues sur $\mathbf{R}$ n'ayant de dérivée en aucun point (Weierstrass, 1875) ; en prenant la primitive d'une telle fonction cela montre qu'il existe des fonctions de classe $\mathscr{C}^1$ sur $\mathbf{R}$ qui ne sont pas de classe $\mathscr{C}^2$ et donc, a fortiori, pas analytiques sur $\mathbf{R}$.

D'un autre côté, la théorie des fonctions holomorphes a été développée avant la théorie des fonctions d'une variable réelle, et c'est les pathologies de cette dernière qui ont beaucoup surpris les mathématiciens du 19-ième siècle (et un peu ceux du 20-ième). Par exemple, H. Poincaré a eu quelques ennuis avec les fonctions $\mathscr{C}^\infty$ qui ne sont pas somme de leur série de Taylor...

Démonstration. — Soit $\mathrm{M} = \sup_{w\in \mathrm{C}(z_0,r)} |f(w)|$ (M est fini car f est continue sur le compact $\mathrm{C}(z_0,r)$). On a alors

$$|a_n| \leqslant \frac{1}{2\pi}\lg(\mathrm{C}(z_0,r)) \cdot \big(\sup_{w\in \mathrm{C}(z_0,r)} \big|\frac{f(w)}{(w-z_0)^{n+1}}\big|\big) \leqslant \mathrm{M}r^{-n}.$$

On en déduit que $\rho(\mathrm{F}) \geqslant r$. De plus, si $|z-z_0|<r$, alors

$$\begin{aligned}\sum_{n=0}^{+\infty} a_n(z-z_0)^n =& \frac{1}{2i\pi}\sum_{n=0}^{+\infty}\int_{\mathrm{C}(z_0,r)} \frac{(z-z_0)^n f(w)}{(w-z_0)^{n+1}}\,dw \\ =& \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \sum_{n=0}^{+\infty} \frac{(z-z_0)^n f(w)}{(w-z_0)^{n+1}}\,dw = \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\,dw.\end{aligned}$$

On conclut en utilisant la formule intégrale de Cauchy. (Pour justifier l'échange des signes $\int$ et $\sum$ ci-dessus, on peut, par exemple, faire appel au théorème de convergence dominée en majorant $|\sum_{n=0}^{\mathrm{N}} \frac{(z-z_0)^n f(w)}{(w-z_0)^{n+1}}|$ sur $\mathrm{C}(z_0,r)$ par $\mathrm{M}\sum_{n=0}^{+\infty} \frac{|z-z_0|^n}{r^{n+1}} = \frac{\mathrm{M}}{r-|z-z_0|}$.)

Corollaire V.4.8. — (i) *Si f est holomorphe et ne s'annule pas sur Ω, alors $1/f$ est holomorphe sur Ω ; sa dérivée est $\frac{-f'}{f^2}$.*

(ii) *Si $f : \Omega_1 \to \Omega_2$ est holomorphe et si $g : \Omega_2 \to \mathbf{C}$ est holomorphe, alors $g\circ f : \Omega_1 \to \mathbf{C}$ est holomorphe ; sa dérivée est $(g'\circ f)\,f'$.*

(iii) *Si $f : \Omega_1 \to \Omega_2$ est holomorphe bijective, si sa réciproque $f^{-1} : \Omega_2 \to \Omega_1$ est continue et si f' ne annule pas*[10] *dans Ω, alors f^{-1} est holomorphe ; sa dérivée est $\frac{1}{f'\circ f^{-1}}$.*

Démonstration. — Il suffit de recopier la démonstration du cas réel pour montrer que $1/f$ (resp. $g\circ f$, resp. f^{-1}) est $\mathscr{C}^1$ au sens complexe sur Ω (resp. sur Ω_1, resp. sur Ω_2) ; la prop. V.4.7 permet d'en déduire l'holomorphie de $1/f$ (resp. $g\circ f$, resp. f^{-1}). (On aurait aussi pu démontrer directement que $1/f$ (resp. $g\circ f$, resp. f^{-1}) est développable en série entière autour de chaque point, mais ça aurait été nettement plus fatigant.)

5. Rayon de convergence et inégalités de Cauchy pour les dérivées

Remarque V.4.9. — (i) La formule $f(z) = \mathrm{F}(z-z_0)$ montre que les a_n sont les coefficients du développement de Taylor de f en z_0. Autrement dit, *une fonction f, holomorphe sur un ouvert Ω, est somme de sa série de Taylor en z_0 sur tout disque ouvert $\mathrm{D}(z_0,r^-)$ contenu dans Ω*. De plus, si $\mathrm{D}(z_0,r)\subset\Omega$, alors

$$\frac{1}{n!}f^{(n)}(z_0) = \frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{(w-z_0)^{n+1}}\,dw.$$

10. Ces deux hypothèses sont en fait inutiles (cf. rem. V.6.3, deuxième point).

(ii) Dans le cas $n = 0$, on obtient la formule $f(z_0) = \frac{1}{2\pi}\int_0^{2\pi} f(z_0 + re^{i\theta})\,d\theta$, qui montre que f vérifie la *propriété de la moyenne* : $f(z_0)$ est la moyenne de $f(z)$ sur tout cercle de centre z_0 dont le disque correspondant est inclus dans Ω.

(iii) Dans le cas général, on en déduit la majoration (appelée *inégalité de Cauchy*)

$$|\frac{1}{n!}f^{(n)}(z_0)| \leqslant r^{-n} \sup_{w\in \mathrm{C}(z_0,r)} |f(z)| = r^{-n} \sup_{\theta\in[0,2\pi]} |f(z_0 + re^{i\theta})|.$$

(iv) Plus généralement, si $\mathrm{K} \subset \Omega$ est un compact, si U est un ouvert [11] contenant K, et dont l'adhérence $\overline{\mathrm{U}}$ est un compact contenu dans Ω, alors, quel que soit $n \in \mathbf{N}$, il existe $\mathrm{M} = \mathrm{M}(n, \mathrm{K}, \mathrm{U})$, tel que

$$\sup_{z\in \mathrm{K}} |f^{(n)}(z)| \leqslant \mathrm{M} \sup_{z\in\overline{\mathrm{U}}} |f(z)|.$$

En effet, si $r \leqslant d(\mathrm{K}, \Omega - \mathrm{U})$, alors $\mathrm{C}(z, r) \subset \overline{\mathrm{U}} \subset \Omega$ quel que soit $z \in \mathrm{K}$, et le (i) montre que $\mathrm{M} = n!r^{-n}$ convient.

Proposition V.4.10. — *Soit* log *la détermination principale du logarithme. Alors on a* $\log(1 + z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} z^n$, *si* $|z| < 1$.

Démonstration. — Soit $f(z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} z^n$. C'est une fonction holomorphe sur $\mathrm{D}(0, 1^-)$ dont la dérivée est $\sum_{n=1}^{+\infty}(-1)^{n-1}z^{n-1} = \frac{1}{1+z}$. Par ailleurs, $\log(1 + z)$ est aussi holomorphe sur $\mathrm{D}(0, 1^-)$, de dérivée $\frac{1}{1+z}$. La fonction $g(z) = f(z) - \log(1 + z)$ est, d'après le (i) de la rem. V.4.9, somme de sa série de Taylor en 0 sur tout $\mathrm{D}(0, 1^-)$, et comme sa dérivée est nulle, elle est constante sur $\mathrm{D}(0, 1^-)$. On conclut en remarquant que $g(0) = 0$.

Exercice V.4.11. — (i) Montrer que $\mathrm{tg} = \frac{\sin}{\cos}$ est somme de sa série de Taylor en 0 sur $]\frac{-\pi}{2}, \frac{\pi}{2}[$.
(ii) Quel est le rayon de convergence de la série de Taylor en 0 de $\frac{\mathrm{tg}\, z}{z^2+1}$?
(iii) Quel est le rayon de convergence de la série de Taylor en 0 de $\frac{\sin \pi z}{z^2-1}$?

Exercice V.4.12. — (i) Soit $s \in \mathbf{C}$. On définit $(1 + z)^s$ par $(1 + z)^s = \exp(s \log(1 + z))$, où log est la détermination principale du logarithme. Montrer que $(1 + z)^s = \sum_{n=0}^{+\infty} \binom{s}{n} z^n$, si $|z| < 1$.
(ii) Existe-t-il une fonction f holomorphe sur $\mathrm{D}(0, 1^-)$ telle que $f(z)^2 = z$, pour tout $z \in \mathrm{D}(0, 1^-)$?

Exercice V.4.13. — Déduire le principe du maximum de la propriété de la moyenne.

Corollaire V.4.14. — (Liouville, 1844) *Si f est une fonction holomorphe sur $\mathbf{C}$ tout entier, et si f est bornée, alors f est constante.*

Démonstration. — Par hypothèse, il existe $\mathrm{M} > 0$ tel que $|f(z)| \leqslant \mathrm{M}$, quel que soit $z \in \mathbf{C}$. On déduit de l'inégalité de Cauchy que, si $n \in \mathbf{N}$, alors $|\frac{1}{n!}f^{(n)}(0)| \leqslant r^{-n}\mathrm{M}$, quel que soit $r > 0$. En faisant tendre r vers $+\infty$, on en déduit que $f^{(n)}(0) = 0$, si $n \geqslant 1$. Or f étant

11. Un tel ouvert existe toujours : comme K est compact, on a $\delta = d(\mathrm{K}, \mathbf{C} - \Omega) > 0$, et si $0 < \delta' < \delta$, il suffit de prendre $\mathrm{U} = \{z \in \mathbf{C},\ d(z, \mathrm{K}) < \delta'\}$ qui est ouvert car $z \mapsto d(z, \mathrm{K})$ est continue, et dont l'adhérence $\overline{\mathrm{U}} = \{z \in \mathbf{C},\ d(z, \mathrm{K}) \leqslant \delta'\}$ est contenue dans Ω car $\delta' < \delta$, et est compacte car fermée et bornée puisque K est borné.

holomorphe sur $\mathbf{C}$ tout entier, est somme de sa série de Taylor en 0 en tout point de $\mathbf{C}$ et donc $f(z) = f(0)$, pour tout $z \in \mathbf{C}$. Ceci permet de conclure.

Corollaire V.4.15. — (th. de d'Alembert-Gauss, 1799) $\mathbf{C}$ *est algébriquement clos.*

Démonstration. — Soit $\mathrm{P} \in \mathbf{C}[\mathrm{T}]$ ne s'annulant pas sur $\mathbf{C}$. Alors $f = 1/\mathrm{P}$ est une fonction holomorphe. De plus f est bornée sur $\mathbf{C}$ car elle a une limite quand $|z| \to +\infty$, et est continue. On déduit du théorème de Liouville que f est constante, et donc que P est de degré 0. En prenant la contraposée, cela montre que, si $\deg \mathrm{P} \geqslant 1$, alors P a un zéro dans $\mathbf{C}$, ce qui permet de conclure.

Exercice V.4.16. — Soit f une fonction holomorphe sur $\mathbf{C}$ tout entier. On suppose qu'il existe $\mathrm{N} \in \mathbf{N}$ et $\mathrm{C} > 0$ tels que $|f(z)| \leqslant \mathrm{C}|z|^{\mathrm{N}}$, pour tout $z \in \mathbf{C}$. Montrer que f est un polynôme.

V.5. Construction de fonctions holomorphes

1. Séries de fonctions holomorphes

Soit Ω un ouvert de $\mathbf{C}$. Rappelons qu'une suite de fonctions $(f_n)_{n\in\mathbf{N}}$ *converge uniformément sur tout compact* vers f, si pour tout compact $\mathrm{K} \subset \Omega$, et tout $\varepsilon > 0$, il existe $\mathrm{N}(\mathrm{K}, \varepsilon)$, tel que $|f_n(z) - f(z)| < \varepsilon$, si $z \in \mathrm{K}$ et $n \geqslant \mathrm{N}(\mathrm{K}, \varepsilon)$. Une série $\sum_{n\in\mathbf{N}} u_n$ *converge uniformément sur tout compact*, si la suite de ses sommes partielles le fait ; elle *converge normalement sur tout compact*, si pour tout compact $\mathrm{K} \subset \Omega$, on a $\sum_{n\in\mathbf{N}} \|u_n\|_{\mathrm{K}} < +\infty$, où $\|u_n\|_{\mathrm{K}} = \sup_{z\in\mathrm{K}} |u_n(z)|$ est la norme de u_n pour la convergence uniforme sur K.

La convergence normale sur tout compact implique la convergence uniforme sur tout compact qui implique la convergence simple.

Théorème V.5.1. — *Soit Ω un ouvert de $\mathbf{C}$.*

(i) *Si $(f_n)_{n\in\mathbf{N}}$ est une suite de fonctions holomorphes sur Ω convergeant uniformément sur tout compact de Ω, alors la limite f de la suite f_n est holomorphe sur Ω et, pour tout k, la suite $(f_n^{(k)})_{n\in\mathbf{N}}$ converge uniformément vers $f^{(k)}$ sur tout compact de Ω.*

(ii) *Si $(u_n)_{n\in\mathbf{N}}$ est une suite de fonctions holomorphes sur Ω telle que la série $\sum_{n\in\mathbf{N}} u_n$ converge uniformément (resp. normalement) sur tout compact de Ω, alors la somme f de la série est holomorphe sur Ω et, pour tout k, la série $\sum_{n\in\mathbf{N}} u_n^{(k)}$ converge uniformément (resp. normalement) vers $f^{(k)}$ sur tout compact de Ω.*

Démonstration. — Le (i) se déduit du (ii), et pour montrer le (ii), il suffit de prouver que f est holomorphe, le reste s'en déduisant en utilisant le (iv) de la remarque V.4.9 ci-dessus.

Soit $z_0 \in \Omega$, et soit $r > 0$ tel que $\mathrm{D}(z_0, r) \subset \Omega$. Alors, d'après la formule de Cauchy, on a, pour tout $z \in \mathrm{K}$,

$$f(z) = \sum_{n\in\mathbf{N}} u_n(z) = \frac{1}{2i\pi} \sum_{n\in\mathbf{N}} \int_{\mathrm{C}(z_0,r)} \frac{u_n(w)}{w-z}\, dw$$
$$= \frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r)} \sum_{n\in\mathbf{N}} \frac{u_n(w)}{w-z}\, dw = \frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\, dw,$$

l'interversion des signes $\int$ et $\sum$ ci-dessus étant justifiée par la convergence uniforme (resp. normale) de la série $\sum_{n\in\mathbf{N}} u_n(z)$ sur le compact $\mathrm{C}(z_0, r)$. La prop. V.4.7 permet d'en déduire l'holomorphie de f dans $\mathrm{D}(z_0, r^-)$, ce qui permet de conclure.

Exercice V.5.2. — Soient Ω un ouvert de $\mathbf{C}$ et $(f_n)_{n\in\mathbf{N}}$ une suite de fonctions holomorphes sur Ω tendant simplement vers f. Montrer que, si pour tout compact K de Ω, il existe $\mathrm{M_K} > 0$ tel que $|f_n(z)| \leqslant \mathrm{M_K}$, pour tout $n \in \mathbf{N}$ et $z \in \mathrm{K}$, alors f est holomorphe.

Exercice V.5.3. — (i) Montrer que la série $\sum_{n=\mathrm{N}+1}^{+\infty} \left(\frac{1}{z+n} + \frac{1}{z-n}\right)$ est uniformément convergente sur $\mathrm{D}(0, (\mathrm{N}+\frac{1}{2})^-)$. En déduire que $z \mapsto \mathrm{F}(z) = \frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{z+n} + \frac{1}{z-n}\right)$ est holomorphe sur $\mathbf{C} - \mathbf{Z}$.

(ii) Montrer que $\mathrm{G}(z) = \mathrm{F}(z) - \pi \operatorname{cotg} \pi z$ est impaire et périodique de période 1.

(iii) Montrer que G se prolonge par continuité en une fonction holomorphe sur $\mathbf{C}$.

(iv) Montrer que G est bornée sur $\mathbf{C}$; en déduire que $\frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{z+n} + \frac{1}{z-n}\right) = \pi \operatorname{cotg} \pi z$, si $z \in \mathbf{C} - \mathbf{Z}$.

(v) Soit $\sum_{n=0}^{+\infty} \mathrm{B}_n \frac{t^n}{n!}$ le développement de Taylor de $\frac{t}{e^t-1}$ en $t = 0$, et, si k est un entier $\geqslant 1$, soit $\zeta(2k) = \sum_{n=1}^{+\infty} \frac{1}{n^{2k}}$. Montrer que

$$\zeta(2k) = -\frac{1}{2}\mathrm{B}_{2k} \frac{(2i\pi)^{2k}}{(2k)!}.$$

En déduire que $\pi^{-2k}\zeta(2k)$ est un nombre rationnel (Euler, 1734).

2. Produits infinis de fonctions holomorphes

Soit I un ensemble dénombrable, et soit $(u_i)_{i\in\mathrm{I}}$ une suite de nombres complexes. On dit que le *produit* $\prod_{i\in\mathrm{I}} u_i$ est *convergent* si $\sum_{i\in\mathrm{I}} |u_i - 1| < +\infty$. Si $u_i = 0$, pour tout $i \in \mathrm{I}$, la condition précédente équivaut à $\sum_{i\in\mathrm{I}} |\log u_i| < +\infty$, où $\log : \mathbf{C}^* \to \mathbf{C}$ désigne la détermination du logarithme dont la partie imaginaire appartient à $]-\pi, \pi]$ (en particulier $\log z = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n}(z-1)^n$, si $|z-1| < 1$, et $\lim_{z\to 1} \frac{\log z}{z-1} = 1$). Si I est fini, le produit est convergent et sa valeur est le produit au sens usuel. Si I est infini, et si $n \mapsto i(n)$ est une bijection de $\mathbf{N}$ sur I, alors $x_n = \prod_{k\leqslant n} u_{i(k)}$ est une suite convergente dont la limite ne dépend pas de la bijection de $\mathbf{N}$ sur I choisie, et qui est, par définition, la valeur du produit infini. En effet :

• s'il existe i tel que $u_i = 0$, alors $x_n = 0$, pour tout n assez grand, et la valeur du produit est 0 ;

• si $u_i \neq 0$, pour tout i, on a $x_n = \exp\left(\sum_{k\leqslant n} \log u_{i(k)}\right)$, et comme $\sum_{i\in\mathrm{I}} |\log u_i| < +\infty$, la série $\sum_{n\in\mathbf{N}} \log u_{i(n)}$ converge, et $\prod_{i\in\mathrm{I}} x_i = \exp\left(\sum_{n\in\mathbf{N}} \log u_{i(n)}\right) = \exp\left(\sum_{i\in\mathrm{I}} \log u_i\right)$.

En particulier, *un produit convergent est nul si et seulement si un des termes du produit est nul.*

Théorème V.5.4. — *Soit Ω un ouvert de $\mathbf{C}$, soit $(u_n)_{n\in\mathbf{N}}$ une suite de fonctions holomorphes sur $\mathbf{C}$ telle que la série $\sum_{n\in\mathbf{N}} u_n$ converge normalement sur tout compact de Ω, et soit $f_n = \prod_{k=0}^{n}(1+u_k)$, si $n \in \mathbf{N}$.*

(i) *La suite f_n converge uniformément sur tout compact* (on dit que le produit infini $\prod_{n\in\mathbf{N}}(1+u_n)$ converge uniformément sur tout compact)*, et la limite f de la suite f_n est une fonction holomorphe sur Ω.*

(ii) *Si Ω est connexe, et si aucune des u_n est identiquement -1 sur Ω, alors $f(z) = 0$ si et seulement si il existe $n \in \mathbf{N}$ tel que $1+u_n(z) = 0$, et on a $v_z(f) = \sum_{n\in\mathbf{N}} v_z(1+u_n)$, quel que soit $z \in \Omega$. De plus, la série $\sum_{n=0}^{+\infty} \frac{u_n'}{1+u_n}$ converge normalement sur tout compact de Ω sur lequel f ne s'annule pas, et*

$$\frac{f'(z)}{f(z)} = \sum_{n=0}^{+\infty} \frac{u_n'(z)}{1+u_n(z)}, \quad \text{si } f(z) \neq 0.$$

Démonstration. — Si K est un compact de Ω, soit $\mathrm{C}(\mathrm{K}) = \exp(\sum_{n\in\mathbf{N}} \|u_n\|_{\mathrm{K}})$; c'est une quantité finie, par hypothèse. Si $n \in \mathbf{N}$ et si $z \in \mathrm{K}$, on a alors

$$\begin{aligned}\Big|\prod_{k=0}^{n+1}(1+u_k(z)) - \prod_{k=0}^{n}(1+u_k(z))\Big| &= |u_{n+1}(z)| \cdot \Big|\prod_{k=0}^{n}(1+u_k(z))\Big| \\ &\leqslant \|u_{n+1}\|_{\mathrm{K}} \prod_{k=0}^{n}(1+\|u_k\|_{\mathrm{K}}) \leqslant \mathrm{C}(\mathrm{K})\|u_{n+1}\|_{\mathrm{K}}.\end{aligned}$$

On en déduit, grâce à la convergence de $\sum_{n\in\mathbf{N}} \|u_n\|_{\mathrm{K}}$, la convergence uniforme du produit sur K. La limite f est donc holomorphe sur Ω d'après le th. V.5.1.

Maintenant, si $z_0 \in \Omega$, on peut choisir $r > 0$ tel que $\mathrm{K} = \mathrm{D}(z_0, r) \subset \Omega$, et $\mathrm{N} \in \mathbf{N}$ tel que $\|u_n\|_{\mathrm{K}} \leqslant \frac{1}{2}$, si $n > \mathrm{N}$. En particulier, $1+u_n$ ne s'annule pas sur K et, pour tout $z \in \mathrm{K} = \mathrm{D}(z_0, r)$, on a $|1+u_n(z)| \geqslant 1 - \|u_n\|_{\mathrm{K}} \geqslant e^{-2\|u_n\|_{\mathrm{K}}}$. Soit $g_{\mathrm{N}} = \prod_{n\geqslant \mathrm{N}+1}(1+u_n)$. On déduit de ce qui précède la minoration $|g_{\mathrm{N}}(z)| \geqslant \exp\big(-2\sum_{n=\mathrm{N}+1}^{+\infty} \|u_n\|_{\mathrm{K}}\big)$, ce qui permet de prouver que g_{N} ne s'annule pas sur K. On en déduit que

$$v_{z_0}(f) = v_{z_0}\big(g_{\mathrm{N}} \prod_{n=0}^{\mathrm{N}}(1+u_n)\big) = \sum_{n=0}^{\mathrm{N}} v_{z_0}(1+u_n) = \sum_{n=0}^{+\infty} v_{z_0}(1+u_n).$$

La convergence normale de la série des u_n implique alors, d'après le (ii) du th. V.5.1, celle de la série des u_n'. Comme $|1+u_n(z)| \geqslant \frac{1}{2}$, si $z \in \mathrm{K}$ et $n \geqslant \mathrm{N}$, on en déduit la convergence normale de la série des $\frac{u_n'}{1+u_n}$. De même, la convergence uniforme sur K de f_n vers f entraîne celle de f_n' vers f' ((i) du th. V.5.1). On en déduit que $\frac{f_n'(z)}{f_n(z)}$ tend vers $\frac{f'(z)}{f(z)}$, si $f(z) \neq 0$. Or $\frac{f_n'}{f_n} = \sum_{k=0}^{n} \frac{u_k'}{1+u_k}$ (cela suit, par récurrence de ce que $(v_1v_2)' = v_1'v_2 + v_1v_2'$), et donc $\frac{f'(z)}{f(z)} = \sum_{n=0}^{+\infty} \frac{u_n'(z)}{1+u_n(z)}$, si $f(z) \neq 0$. Ceci permet de conclure.

Exercice V.5.5. — Reprendre la démonstration du théorème en utilisant la série des $\log u_n$ (attention au fait que $\log u_n$ n'est pas forcément holomorphe sur Ω tout entier).

Exercice V.5.6. — Montrer que $\prod_{n\geqslant 1}\left(1-\frac{z^2}{n^2}\right)$ est uniformément convergent sur tout compact de $\mathbf{C}$, et que sa valeur est $\frac{\sin \pi z}{\pi z}$. (On utilisera les résultats de l'ex. V.5.3 ; cf. ex. H.1.10 pour une autre méthode.)

3. Fonctions holomorphes définies par une intégrale

Théorème V.5.7. — *Soit* X *un sous-ensemble mesurable de* $\mathbf{R}^m$*, et soit* Ω *un ouvert de* $\mathbf{C}$*. Soit* $\mathrm{F}:\Omega\times \mathrm{X}\to\mathbf{C}$*. On suppose que :*

- $z\mapsto \mathrm{F}(z,t)$ *est holomorphe sur* Ω*, quel que soit* $t\in \mathrm{X}$ *;*
- $t\mapsto \mathrm{F}(z,t)$ *est mesurable quel que soit* $z_0\in\Omega$*, et il existe* $r_{z_0}>0$ *et* $g_{z_0}\in\mathscr{L}^1(\mathrm{X})$ *tels que* $\mathrm{D}(z_0,r_{z_0})\subset\Omega$ *et* $|\mathrm{F}(z,t)|\leqslant g_{z_0}(t)$*, pour tous* $z\in\mathrm{D}(z_0,r_{z_0})$ *et* $t\in\mathrm{X}$*.*

Alors la fonction $f:\Omega\to\mathbf{C}$ *définie par* $f(z)=\int_{\mathrm{X}}\mathrm{F}(z,t)\,dt$ *est holomorphe sur* Ω*. De plus, si* $k\in\mathbf{N}$*, alors* $\left(\frac{\partial}{\partial z}\right)^k f(z)=\int_{\mathrm{X}}\left(\frac{\partial}{\partial z}\right)^k\mathrm{F}(z,t)\,dt$*.*

Démonstration. — L'holomorphie étant une propriété locale, il suffit de prouver que, quel que soit $z_0\in\Omega$, il existe $r>0$ tel que f soit holomorphe sur $\mathrm{D}(z_0,r^-)$. Fixons donc z_0, et soit $r=r_{z_0}$. Comme $z\mapsto\mathrm{F}(z,t)$ est holomorphe, quel que soit $t\in\mathrm{X}$, on tire de la formule de Cauchy l'identité

$$f(z)=\frac{1}{2i\pi}\int_{\mathrm{X}}\Big(\int_{\mathrm{C}(z_0,r)}\frac{\mathrm{F}(w,t)}{w-z}\,dw\Big)dt,\quad \text{si } z\in\mathrm{D}(z_0,r^-).$$

Or on a $|\frac{\mathrm{F}(w,t)}{w-z}|\leqslant\frac{g_{z_0}(t)}{r-|z-z_0|}$, si $(w,t)\in(\mathrm{C}(z_0,r)\times\mathrm{X})$. Comme g_{z_0} est sommable sur X, la fonction $|\frac{\mathrm{F}(w,t)}{w-z}|$ est sommable sur $\mathrm{C}(z_0,r)\times\mathrm{X}$, ce qui permet d'utiliser le théorème de Fubini pour permuter les deux intégrations. On obtient

$$f(z)=\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)}\Big(\int_{\mathrm{X}}\frac{\mathrm{F}(w,t)}{w-z}\,dt\Big)dw=\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)}\frac{f(w)}{w-z}\,dw,\quad \text{si } z\in\mathrm{D}(z_0,r^-).$$

La prop. V.4.7 permet d'en déduire l'holomorphie de f sur $\mathrm{D}(z_0,r^-)$.

Maintenant, on a $\frac{1}{k!}f^{(k)}(z_0)=\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)}\frac{f(w)}{(w-z_0)^{k+1}}\,dw$ d'après le (i) de la rem. V.4.9. En majorant $|\frac{\mathrm{F}(w,t)}{(w-z_0)^{n+1}}|$ par $r^{-k-1}g_{z_0}(t)$ qui est sommable sur $\mathrm{C}(z_0,r)\times\mathrm{X}$, ce qui permet d'utiliser Fubini dans l'autre sens, on obtient

$$\frac{1}{k!}f^{(k)}(z_0)=\int_{\mathrm{X}}\Big(\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)}\frac{\mathrm{F}(w,t)}{(w-z_0)^{k+1}}\,dw\Big)\,dt=\int_{\mathrm{X}}\frac{1}{k!}\Big(\frac{\partial}{\partial z}\Big)^k\mathrm{F}(z_0,t)\,dt.$$

Ceci permet de conclure.

Corollaire V.5.8. — *Soient* Ω *et* D *deux ouverts de* $\mathbf{C}$*. Si* f *est continue sur* $\Omega\times\mathrm{D}$*, et si* $z\mapsto f(z,w)$ *est holomorphe sur* Ω *pour tout* $w\in\mathrm{D}$*, alors* $z\mapsto\int_\gamma f(z,w)\,dw$ *est holomorphe sur* Ω*, quel que soit le chemin* $\mathscr{C}^1$ *par morceaux* γ *inclus dans* D*.*

Démonstration. — On a $\int_\gamma f(z,w)\,dw=\int_0^1 f(z,\gamma(t))\gamma'(t)\,dt$. Soit alors $z_0\in\Omega$. On peut trouver $r>0$ tel que $\mathrm{D}(z_0,r)\subset\Omega$. La fonction continue $(z,t)\mapsto|f(z,\gamma(t))|$ est majorée sur le compact $\mathrm{D}(z_0,r)\times[0,1]$, et donc $f(z,\gamma(t))\gamma'(t)$ admet un majorant du type $\mathrm{M}\,|\gamma'(t)|$

sur $\mathrm{D}(z_0,r)\times[0,1]$. Comme $\int_0^1|\gamma'(t)|\,dt<+\infty$, on est dans les conditions d'application du th. V.5.7, ce qui permet de conclure.

Exercice V.5.9. — (La fonction Γ dans le plan complexe).

(i) Montrer que $\mathrm{F}(z)=\int_0^{+\infty}e^{-t}t^z\,\frac{dt}{t}$ converge si $\mathrm{Re}(z)>0$, et que $z\mapsto\mathrm{F}(z)$ est holomorphe sur le demi-plan $\mathrm{Re}(z)>0$.

(ii) Montrer que, quel que soit $n\in\mathbf{N}$, on a $\mathrm{F}(z)=\frac{\mathrm{F}(z+n+1)}{z(z+1)\cdots(z+n)}$, si $\mathrm{Re}(z)>0$. En déduire qu'il existe une unique fonction Γ, holomorphe sur $\mathbf{C}-(-\mathbf{N})$, avec des pôles simples aux entiers négatifs, telle que $\Gamma(z)=\mathrm{F}(z)$ si $\mathrm{Re}(z)>0$.

(iii) Montrer que $\mathrm{F}(z)$ est bornée dans toute bande verticale $0<a\leqslant\mathrm{Re}(z)\leqslant b<+\infty$; en déduire que Γ est à décroissance rapide à l'infini dans toute bande verticale de largeur finie, c'est-à-dire que, quels que soient $a<b\in\mathbf{R}$ et $\mathrm{N}\in\mathbf{N}$, il existe $\mathrm{C}(a,b,\mathrm{N})$ tel que l'on ait

$$|\Gamma(z)|\leqslant\mathrm{C}(a,b,\mathrm{N})|\mathrm{Im}(z)|^{-\mathrm{N}},\quad\text{si } a\leqslant\mathrm{Re}(z)\leqslant b\text{ et }|\mathrm{Im}(z)|\geqslant 1.$$

V.6. Inversion globale et image ouverte

1. Le théorème d'inversion locale holomorphe

Soient Ω_1,Ω_2 deux ouverts de $\mathbf{C}$. Une application $\varphi:\Omega_1\to\Omega_2$ est *biholomorphe*, si elle est bijective et si φ et φ^{-1} sont holomorphe. (On verra plus tard (rem. V.6.3) qu'il suffit que φ soit injective et holomorphe pour qu'elle soit biholomorphe.)

Théorème V.6.1. — (inversion locale pour les fonctions holomorphes) *Soient Ω un ouvert de $\mathbf{C}$, f holomorphe sur Ω, et $z_0\in\Omega$. Si $f'(z_0)\neq 0$, il existe un voisinage ouvert* U *de z_0 dans Ω et un voisinage ouvert* V *de $f(z_0)$ dans $\mathbf{C}$ tels que f soit biholomorphe de* U *sur* V.

Démonstration. — Commençons par supposer que $z_0=0$, $f(z_0)=0$ et $f'(z_0)=1$; nous allons construire l'application réciproque g de f par une méthode du point fixe (cf. n° 14.2 du Vocabulaire) en partant du fait que g est point fixe de $\varphi\mapsto\varphi-f\circ\varphi+\mathrm{id}$.

Il existe $\alpha\in\mathbf{C}$ tel que $f(z)=z+\alpha z^2+\mathrm{O}(|z|^3)$, ce qui fait que

$$h(u,v)=f(u-v)-f(u)+v=\alpha(v^2-2uv)+\mathrm{O}((|u|+|v|)^3).$$

Soit $r_0<\frac{1}{2}\rho(f)$. On déduit du développement limité ci-dessus, l'existence de $\mathrm{C}>0$, tel que l'on ait $|h(u,v)|<\mathrm{C}|u|\cdot|v|$ si $|v|\leqslant|u|\leqslant r_0$. Comme $f(z)-z=\mathrm{O}(|z|^2)$, on peut, quitte à diminuer r_0, imposer de plus que $|f(z)-z|\leqslant\frac{1}{4}|z|$ si $|z|\leqslant r_0$, et on peut aussi imposer $r_0\leqslant\frac{1}{2\mathrm{C}}$.

Soit $r=\frac{2}{3}r_0$. On construit, par récurrence, deux suites de fonctions $(g_n)_{n\geqslant1}$ et $(u_n)_{n\geqslant1}$, en posant $g_1(z)=z$; $u_n(z)=f(g_n(z))-z$; $g_{n+1}(z)=g_n(z)-u_n(z)$. Nous allons montrer que g_n et u_n sont holomorphes sur $\mathrm{D}(0,r^-)$, et que

$$(\frac{1}{2}+\frac{1}{2^n})|z|\leqslant|g_n(z)|\leqslant(\frac{3}{2}-\frac{1}{2^n})|z|\quad\text{et}\quad|u_n(z)|\leqslant\frac{1}{2^{n+1}}|z|,\ \text{quel que soit } z\in\mathrm{D}(0,r^-).$$

Le résultat est évident pour $n=1$ puisque $g_1(z)=z$ et $u_1(z)=f(z)-z$. Si la propriété est vérifiée pour n, alors l'encadrement de $|g_{n+1}(z)|$ est une conséquence immédiate de l'encadrement pour $|g_n(z)|$ et de la

majoration pour $|u_n(z)|$. Par ailleurs, comme $|g_{n+1}(z)| \leqslant \frac{3}{2}|z| < r_0 < \rho(f)$, la fonction $z \mapsto f(g_{n+1}(z))$ est bien définie et holomorphe sur $\mathrm{D}(0, r^-)$, et donc u_{n+1} est holomorphe sur $\mathrm{D}(0, r^-)$. Maintenant,

$$u_{n+1}(z) = f(g_n(z) - u_n(z)) - z = h(g_n(z), u_n(z)) + f(g_n(z)) - u_n(z) - z = h(g_n(z), u_n(z)).$$

Comme $|u_n(z)| \leqslant \frac{1}{2^{n+1}}|z| \leqslant (\frac{1}{2} + \frac{1}{2^n})|z| \leqslant |g_n(z)|$, on a

$$|u_{n+1}(z)| \leqslant |h(g_n(z), u_n(z))| \leqslant \mathrm{C}|g_n(z)|\,|u_n(z)| \leqslant \frac{3\mathrm{C}|z|}{2} \cdot \frac{|z|}{2^{n+1}} \leqslant \mathrm{C}r_0 \frac{|z|}{2^{n+1}} \leqslant \frac{|z|}{2^{n+2}}.$$

Ceci montre que l'hypothèse de récurrence est vérifiée au rang $n+1$.

On déduit de la majoration $|g_{n+1}(z) - g_n(z)| = |u_n(z)| \leqslant \frac{r}{2^{n+1}}$ la convergence uniforme de la suite g_n sur $\mathrm{D}(0, r^-)$. La limite est donc une fonction holomorphe sur $\mathrm{D}(0, r^-)$ qui vérifie $g(z) = g(z) - (f(g(z)) - z)$. Autrement dit, on a construit une fonction holomorphe g sur $\mathrm{D}(0, r^-)$ telle que $f(g(z)) = z$ si $z \in \mathrm{D}(0, r^-)$.

Dans le cas général, on peut appliquer ce qui précède à $\mathrm{F}(z) = f'(z_0)^{-1}(f(z + z_0) - f(z_0))$ (et donc $f(z) = f'(z_0)(\mathrm{F}(z - z_0) + f(z_0))$. On en déduit l'existence de $r_0 > 0$, et de G holomorphe sur $\mathrm{D}(0, r_0^-)$, tels que $\mathrm{F}(\mathrm{G}(z)) = z$, si $z \in \mathrm{D}(0, r_0^-)$. Si on définit g sur $\mathrm{D}(f(z_0), r^-)$, où $r = |f'(z_0)|r_0$, par la formule $g(z) = z_0 + \mathrm{G}(f'(z_0)^{-1}(z - f(z_0)))$, un calcul immédiat montre que $f(g(z)) = z$, si $z \in \mathrm{D}(f(z_0), r^-)$. Autrement, dit, on peut trouver un voisinage ouvert V_0 de $f(z_0)$ et g holomorphe sur V_0 tels que $f \circ g = \mathrm{id}$ sur V_0. Ceci implique en particulier que g est injective sur V_0. De plus, on a $f'(g(z))g'(z) = 1$, si $z \in \mathrm{V}_0$, et donc $g'(f(z_0)) \neq 0$. En appliquant ce qui précède à g au lieu de f, on en déduit l'existence d'un voisinage ouvert U de z_0 (inclus dans Ω), et de $h : \mathrm{U} \to \mathrm{V}_0$ holomorphe, tels que $g \circ h = \mathrm{id}$ sur U. Soit $\mathrm{V} = h(\mathrm{U})$. Comme $g \circ h = \mathrm{id}$ sur U, on a $g(\mathrm{V}) = \mathrm{U}$, et comme g est injective sur V_0, on a $\mathrm{V} = g^{-1}(\mathrm{U})$, ce qui prouve que V est un ouvert (dans V_0 et donc aussi dans $\mathbf{C}$ puisque V_0 est ouvert dans $\mathbf{C}$) qui contient $z_0 = h(f(z_0))$. Enfin, on a $f = f \circ (g \circ h) = (f \circ g) \circ h = h$ sur U, et $f \circ g = \mathrm{id}$ sur V (puisque $\mathrm{V} \subset \mathrm{V}_0$) et $g \circ f = g \circ h = \mathrm{id}$ sur U. En résumé, f induit une bijection holomorphe de U sur V dont l'inverse g est aussi holomorphe. Ceci permet de conclure.

2. Structure locale des fonctions holomorphes

Théorème V.6.2. — *Soient Ω un ouvert connexe de $\mathbf{C}$ et f une fonction holomorphe non constante sur Ω. Si $z_0 \in \Omega$, et si $m = v_{z_0}(f - f(z_0))$, il existe un voisinage ouvert* U *de z_0 dans Ω, un réel $r > 0$ et $\varphi : \mathrm{U} \to \mathrm{D}(0, r^-)$ biholomorphe, avec $\varphi(z_0) = 0$, telle que $f(z) = f(z_0) + \varphi(z)^m$, quel que soit $z \in \mathrm{U}$.*

Démonstration. — Par définition de m, on a, dans un voisinage U_0 de z_0,

$$f(z) - f(z_0) = (z - z_0)^m(a_m + a_{m+1}(z - z_0) + \cdots),$$

avec $a_m \neq 0$. Soit $\alpha \in \mathbf{C}^*$ une racine m-ième de a_m, et soit

$$g = \frac{f(z) - f(z_0)}{a_m(z - z_0)^m} = 1 + b_1(z - z_0) + \cdots .$$

La fonction g est holomorphe dans U_0, et comme elle vaut 1 en z_0, il existe un voisinage ouvert U_1 de z_0 tel que $g(z) \in \mathrm{D}(1, 1^-)$ si $z \in \mathrm{U}_1$. Mais alors la fonction $h = g^{1/m}$ est holomorphe sur U_1 et vérifie $h^m = g$ (cf. rem. V.1.8). Ceci montre que, si on pose $\varphi(z) = \alpha\,(z - z_0)h(z)$, alors φ est holomorphe sur U_1, et on a $f(z) = f(z_0) + \varphi(z)^m$ quel que soit $z \in \mathrm{U}_1$. Enfin, comme $\varphi'(z_0) = \alpha \neq 0$, le théorème d'inversion locale holomorphe montre qu'il existe un voisinage ouvert U de z_0 dans U_1 et $r > 0$ tels que φ induise une bijection biholomorphe de U sur $\mathrm{D}(0, r^-)$.

Remarque V.6.3. — Si $m \geqslant 1$, l'application $z \mapsto z^m$ induit une surjection de $\mathrm{D}(0, r^-)$, sur $\mathrm{D}(0, (r^m)^-)$, et tout point de $\mathrm{D}(0, (r^m)^-) - \{0\}$ a exactement m antécédents. On en déduit (grâce au th. V.6.2), les résultats suivants.

• *Si Ω est un ouvert connexe de $\mathbf{C}$, et si f est holomorphe non constante sur Ω, alors $f(\Omega)$ est un ouvert* (*théorème de l'application ouverte*). En effet, en reprenant les notations du théorème, on voit que si $z_0 \in \Omega$, alors il existe $r > 0$ tel que $f(\Omega)$ contienne $\mathrm{D}(f(z_0), (r^m)^-)$. Ceci fournit un raffinement du principe du maximum.

• *Si Ω est un ouvert de $\mathbf{C}$, et si f est holomorphe injective sur Ω, alors f est biholomorphe de Ω sur $f(\Omega)$* (*inversion globale*). En effet, si f est injective, on doit avoir $m = 1$ dans les notations du théorème [12], et f' ne s'annule pas sur Ω. On déduit du théorème d'inversion locale que f^{-1} est holomorphe au voisinage de tout point de l'ouvert $f(\Omega)$.

Exercice V.6.4. — Montrer qu'il n'existe pas de fonction holomorphe $f : \mathrm{D}(0, 1^-) \to \mathbf{C}$ qui soit bijective.

12. Si $m \geqslant 2$, et si $0 < |u - f(z_0)| < r^m$, alors u a m antécédents par f dans U, à savoir les images réciproques par φ des m racines m-ièmes de $u - f(z_0)$.

CHAPITRE VI

LA FORMULE DE CAUCHY ET CELLE DES RÉSIDUS (DE CAUCHY)

Le lecteur a déjà pu apprécier la puissance de la formule de Cauchy pour l'étude des fonctions holomorphes. La formule des résidus, qui en est une extension, est à la fois un outil pratique permettant de calculer sans douleur certaines intégrales, et un outil théorique extrêmement souple dont nous verrons certaines utilisations au chap. VII et dans l'annexe A. Par ailleurs, les idées qu'elle met en oeuvre sont le point de départ de constructions plus générales permettant d'associer des invariants aux variétés de dimension quelconque. Par exemple, on peut utiliser (les idées intervenant dans) la formule des résidus, pour démontrer qu'un ouvert de $\mathbf{R}^2$ n'est pas homéomorphe à un ouvert de $\mathbf{R}^n$, si $n \neq 2$. Démontrer, ce qui est vital si on veut pouvoir parler de dimension d'un point de vue topologique, qu'un ouvert de $\mathbf{R}^n$ n'est pas homéomorphe à un ouvert de $\mathbf{R}^m$, si $n \neq m$, peut se faire en généralisant (grandement) ces idées.

VI.1. Homotopie de lacets et formule de Cauchy

1. Vocabulaire de topologie algébrique

Soient X et Y deux espaces topologiques et $f : \mathrm{X} \to \mathrm{Y}$ et $g : \mathrm{X} \to \mathrm{Y}$ deux applications continues. On dit que f et g sont *homotopes* si « on peut passer continûment de f à g ». De manière précise, f et g sont homotopes, s'il existe $u : [0,1] \times \mathrm{X} \to \mathrm{Y}$ continue, telle que $u(0,x) = f(x)$ et $u(1,x) = g(x)$, quel que soit $x \in \mathrm{X}$. Si on note $f_t : \mathrm{X} \to \mathrm{Y}$ l'application $x \mapsto f_t(x) = u(t,x)$, alors f_t est continue, pour tout $t \in [0,1]$, et $t \mapsto f_t$ est une application continue de $[0,1]$ dans l'espace des applications continues de X dans Y (muni de la topologie de la convergence simple), qui connecte $f = f_0$ à $g = f_1$.

Un ouvert Ω de $\mathbf{C}$ est *contractile* s'il est *homotope à un point*, c'est-à-dire, s'il existe $z_0 \in \Omega$ tel que $\mathrm{id} : \Omega \to \Omega$ est homotope, dans Ω, à l'application constante $z \mapsto z_0$, quel que soit $z \in \Omega$. Autrement dit, Ω est contractile, s'il existe $z_0 \in \Omega$ et $u : [0,1] \times \Omega \to \Omega$, continue, telle que $u(0,z) = z$ et $u(1,z) = z_0$, quel que soit $z \in \Omega$.

Un ouvert Ω est *étoilé* s'il existe $z_0 \in \Omega$ tel que, quel que soit $z \in \Omega$, le segment $[z_0, z]$ est inclus dans Ω. En particulier, un ouvert convexe est étoilé ; $\mathbf{C}$ privé d'une demi-droite Y est

étoilé (on peut prendre pour z_0 n'importe quel élément de l'autre demi-droite de la droite contenant Y). Un ouvert étoilé est contractile : il suffit de poser $u(t,z) = z(1-t) + tz_0$; la condition selon laquelle $[z_0, z] \subset \Omega$ fait que u est bien à valeurs dans Ω.

Si Ω est un ouvert de $\mathbf{C}$, une *homotopie de lacets dans* Ω de $\gamma_0 : (\mathbf{R}/\mathbf{Z}) \to \Omega$ sur $\gamma_1 : (\mathbf{R}/\mathbf{Z}) \to \Omega$ est une application continue $u : [0,1] \times (\mathbf{R}/\mathbf{Z}) \to \Omega$, vérifiant $u(0,t) = \gamma_0(t)$ et $u(1,t) = \gamma_1(t)$; on peut aussi voir u comme une application continue $u : [0,1] \times [0,1] \to \Omega$ telle que $u(s,0) = u(s,1)$, quel que soit $s \in [0,1]$. On dit qu'un lacet $\gamma : (\mathbf{R}/\mathbf{Z}) \to \Omega$ est *contractile dans* Ω, s'il existe une homotopie de lacets de γ sur un lacet constant. Si Ω est contractile [1], alors tout lacet est contractile dans Ω.

2. Un cas particulier de la formule de Stokes

Soient $\mathrm{A} = (0,0)$, $\mathrm{B} = (1,0)$, $\mathrm{C} = (1,1)$ et $\mathrm{D} = (0,1)$ les sommets du carré $[0,1]^2$. On note $\partial([0,1]^2)$ le bord orienté du carré $[0,1]^2$; c'est la réunion des segments $[\mathrm{A},\mathrm{B}]$, $[\mathrm{B},\mathrm{C}]$, $[\mathrm{C},\mathrm{D}]$ et $[\mathrm{D},\mathrm{A}]$.

Proposition VI.1.1. — *Si* $\omega = \mathrm{P}\,ds + \mathrm{Q}\,dt$ *est une* 1*-forme sur* $[0,1]^2$*, avec* P *et* Q *de classe* $\mathscr{C}^1$*, alors* [2]

$$\int_{\partial([0,1]^2)} \omega = \int_{[0,1]^2} \Big(-\frac{\partial \mathrm{P}}{\partial t} + \frac{\partial \mathrm{Q}}{\partial s} \Big)\, ds\, dt.$$

Démonstration. — En revenant à la définition d'une intégrale curviligne, on obtient

$$\int_{[\mathrm{A},\mathrm{B}]} \omega = \int_0^1 \mathrm{P}(s,0)\, ds, \quad \int_{[\mathrm{C},\mathrm{D}]} \omega = \int_0^1 \mathrm{P}(1-v,1)\, dv = -\int_0^1 \mathrm{P}(s,1)\, ds,$$
$$\int_{[\mathrm{B},\mathrm{C}]} \omega = \int_0^1 \mathrm{Q}(1,t)\, dt, \quad \int_{[\mathrm{D},\mathrm{A}]} \omega = \int_0^1 \mathrm{Q}(0,1-v)\, dv = -\int_0^1 \mathrm{Q}(0,t)\, dt.$$

1. Plus généralement, un espace topologique connexe X est *simplement connexe*, si tout lacet dans X est contractile. D'après un célèbre théorème énoncé par B. Riemann (1851) et vraiment démontré par P. Koebe en 1914, (le *théorème de représentation conforme de Riemann*), un ouvert simplement connexe de $\mathbf{C}$, non égal à $\mathbf{C}$, est biholomorphe au disque unité $\mathrm{D} = \mathrm{D}(0,1^-)$. En particulier, cela permet de montrer que tout ouvert U simplement connexe de $\mathbf{R}^2$ est difféomorphe à $\mathbf{R}^2$ (i.e. il existe une bijection de classe $\mathscr{C}^1$ de U sur $\mathbf{R}^2$ dont la réciproque est aussi de classe $\mathscr{C}^1$). Comme une fonction holomorphe préserve les angles, on voit que l'on peut transformer (l'intérieur d') un cercle en (l'intérieur d') un triangle en conservant les angles...

2. La formule qui suit est un cas particulier de la *formule de Stokes* $\int_\Omega d\omega = \int_{\partial\Omega} \omega$, qui est une des formules mathématiques les plus esthétiques, et aussi une des plus utiles. Dans la formule de Stokes, ω est une p-forme sur un compact K de dimension $p+1$, $d\omega$ est sa différentielle, Ω est l'intérieur de K et $\partial\Omega$ est la frontière orientée de Ω (et donc aussi celle de K). Donner un sens précis à ce qui précède demande un peu de travail (en particulier définir une orientation sur la frontière, ce qui n'est pas toujours possible). Si $p = 0$, la formule de Stokes est « le théorème fondamental de l'analyse » $\int_a^b df = f(b) - f(a)$, et si $p = 1$ et si Ω est de dimension 2, la formule de Stokes est aussi connue sous le nom de *théorème de Green* (on a alors $d(\mathrm{P}\,dx + \mathrm{Q}\,dy) = d\mathrm{P} \wedge dx + d\mathrm{Q} \wedge dy = \big(-\frac{\partial \mathrm{P}}{\partial y} + \frac{\partial \mathrm{Q}}{\partial x} \big)\, dx \wedge dy$, en tenant compte de ce que $\wedge$ est bilinéaire alterné ; on retombe donc bien sur la formule de la proposition).

Ceci nous donne

$$\begin{aligned}\int_{\partial([0,1]^2)}\omega &= \int_0^1 (\mathrm{P}(s,0)-\mathrm{P}(s,1))\,ds + \int_0^1 (\mathrm{Q}(1,t)-\mathrm{Q}(0,t))\,dt\\ &= -\int_0^1 \Big(\int_0^1 \frac{\partial \mathrm{P}}{\partial t}(s,t)\,dt\Big)ds + \int_0^1 \Big(\int_0^1 \frac{\partial \mathrm{Q}}{\partial s}(s,t)\,ds\Big)dt\\ &= \int_{[0,1]^2} \Big(-\frac{\partial \mathrm{P}}{\partial t}+\frac{\partial \mathrm{Q}}{\partial s}\Big)dsdt.\end{aligned}$$

Si Ω est un ouvert de $\mathbf{C}$, si $u : [0,1]^2 \to \Omega$ est une application de classe $\mathscr{C}^1$, et si $f : \Omega \to \mathbf{C}$ est de classe $\mathscr{C}^1$, on définit la 1-forme $u^*(f(z)\,dz)$ sur $[0,1]^2$, par la formule :

$$u^*(f(z)\,dz) = f(u(s,t))\,d(u(s,t)) = f(u(s,t))\Big(\frac{\partial u}{\partial s}(s,t)\,ds + \frac{\partial u}{\partial t}(s,t)\,dt\Big).$$

Lemme VI.1.2. — *Soit Ω un ouvert de $\mathbf{C}$. Si $f : \Omega \to \mathbf{C}$ est une fonction de classe $\mathscr{C}^1$ au sens complexe, si $u : [0,1]^2 \to \Omega$ est une application de classe $\mathscr{C}^2$, et si on pose $u^*(f(z)\,dz) = \mathrm{P}(s,t)\,ds + \mathrm{Q}(s,t)\,dt$, alors $-\frac{\partial \mathrm{P}}{\partial t} + \frac{\partial \mathrm{Q}}{\partial s} = 0$.*

Démonstration. — Comme f est holomorphe [3], on a

$$f(u(s+h,t)) = f(u(s,t)+h\frac{\partial u}{\partial s}(s,t)+o(h)) = f(u(s,t)) + f'(u(s,t))\Big(\frac{\partial u}{\partial s}(s,t)h\Big) + o(h).$$

On en déduit que (avec le même argument pour $\frac{\partial}{\partial t}$)

$$\frac{\partial(f\circ u)}{\partial s} = \frac{\partial u}{\partial s}\cdot f'\circ u \quad \text{et} \quad \frac{\partial(f\circ u)}{\partial t} = \frac{\partial u}{\partial t}\cdot f'\circ u.$$

Comme $\mathrm{P} = \frac{\partial u}{\partial s}\cdot f\circ u$ et $\mathrm{Q} = \frac{\partial u}{\partial t}\cdot f\circ u$, on obtient

$$\begin{aligned}-\frac{\partial \mathrm{P}}{\partial t}+\frac{\partial \mathrm{Q}}{\partial s} &= -\frac{\partial^2 u}{\partial t\partial s}\cdot f\circ u - \frac{\partial u}{\partial s}\frac{\partial u}{\partial t}\cdot f'\circ u + \frac{\partial^2 u}{\partial s\partial t}\cdot f\circ u - \frac{\partial u}{\partial t}\frac{\partial u}{\partial s}\cdot f'\circ u\\ &= \Big(-\frac{\partial^2 u}{\partial t\partial s}+\frac{\partial^2 u}{\partial s\partial t}\Big)\,f\circ u = 0.\end{aligned}$$

Théorème VI.1.3. — *Soient Ω un ouvert de $\mathbf{C}$ et f une fonction de classe $\mathscr{C}^1$ au sens complexe sur Ω. Si γ_0, γ_1 sont deux lacets homotopes dans Ω, alors*

$$\int_{\gamma_0} f(z)\,dz = \int_{\gamma_1} f(z)\,dz.$$

Remarque VI.1.4. — Si γ est un lacet constant, on a $\int_\gamma \omega = 0$ quelle que soit la 1-forme ω.

3. Une démonstration plus savante, mais plus naturelle, consisterait à remarquer que l'on a d'une part $(-\frac{\partial \mathrm{P}}{\partial t}+\frac{\partial \mathrm{Q}}{\partial s})\,ds\wedge dt = d(u^*(f(z)\,dz))$, et d'autre part que $d(u^*(f(z)dz)) = u^*(d(f(z)\,dz))$, et $\frac{\partial f}{\partial \overline{z}} = 0$, puisque f est holomorphe, et donc $d(f(z)\,dz) = \frac{\partial f}{\partial \overline{z}}\,d\overline{z}\wedge dz = 0$.

On en déduit, si $\omega = f(z)\,dz$, avec f holomorphe sur Ω, les résultats suivants.

(i) *Si γ est un lacet contractile dans Ω, alors $\int_\gamma f(z)\,dz = 0$.*

(ii) *Si Ω est contractile* (en particulier, si Ω est étoilé), *alors $\int_\gamma f(z)\,dz = 0$, quel que soit le lacet γ dans Ω.*

Démonstration. — Commençons par supposer qu'il existe, dans Ω, une homotopie de lacets, de classe $\mathscr{C}^2$, de γ_0 sur γ_1. Autrement dit, il existe $u : [0,1]^2 \to \Omega$ de classe $\mathscr{C}^2$, telle que $u(0,t) = \gamma_0(t)$, $u(1,t) = \gamma_1(t)$, et $u(s,0) = u(s,1)$ quel que soit $s \in [0,1]$. Notons ω la 1-forme $f(z)\,dz$. Écrivons $u^*\omega$, sous la forme $\mathrm{P}\,ds + \mathrm{Q}\,dt$. D'après le lemme VI.1.2, on a $-\frac{\partial \mathrm{P}}{\partial t} + \frac{\partial \mathrm{Q}}{\partial s} = 0$. On déduit donc de la proposition VI.1.1, la nullité de $\int_{\partial([0,1]^2)} u^*\omega$. En notant, $\mathrm{A} = (0,0)$, $\mathrm{B} = (1,0)$, $\mathrm{C} = (1,1)$ et $\mathrm{D} = (0,1)$ les sommets du carré $[0,1]^2$, on voit que

$$\int_{[\mathrm{B,C}]} u^*\omega = \int_0^1 \mathrm{Q}(1,t)\,dt = \int_0^1 f(u(1,t))\frac{\partial u}{\partial t}(1,t)\,dt = \int_0^1 f(\gamma_1(t))\gamma_1'(t)\,dt = \int_{\gamma_1} f(z)\,dz.$$

De même, $\int_{[\mathrm{D,A}]} u^*\omega = -\int_{\gamma_0} f(z)\,dz$. Par ailleurs, on a $\int_{[\mathrm{A,B}]} u^*\omega + \int_{[\mathrm{C,D}]} u^*\omega = 0$, puisque $u(s,0) = u(s,1)$, quel que soit $s \in [0,1]$. On obtient donc

$$0 = \int_{\partial([0,1]^2)} u^*\omega = \int_{[\mathrm{A,B}]} u^*\omega + \int_{[\mathrm{B,C}]} u^*\omega + \int_{[\mathrm{C,D}]} u^*\omega + \int_{[\mathrm{D,A}]} u^*\omega = \int_{\gamma_1} f(z)\,dz - \int_{\gamma_0} f(z)\,dz,$$

ce qui permet de conclure dans le cas particulier où γ_0 et γ_1 sont homotopes dans Ω par une homotopie de classe $\mathscr{C}^2$.

Passons au cas général. Les chemins γ_0 et γ_1 sont $\mathscr{C}^1$ par morceaux, et on dispose de $u : [0,1]^2 \to \Omega$, continue, telle que $u(0,t) = \gamma_0(t)$, $u(1,t) = \gamma_1(t)$, et $u(s,0) = u(s,1)$ quel que soit $s \in [0,1]$. L'idée est d'approximer u par des fonctions u_ε de classe $\mathscr{C}^2$, en régularisant (cf. ex. IV.1.7) comme dans l'ex. IV.3.26, et de passer à la limite. La mise en œuvre de cette stratégie demande de prendre un peu de précautions pour s'assurer que les approximations construites sont des homotopies de lacets et ne sortent pas de Ω.

On note $[x]$ la partie entière de $x \in \mathbf{R}$. Soit $\tilde{u} : [-1,2]^2 \to \Omega$ définie par

$$\tilde{u}(s,t) = \begin{cases} u(0, t-[t]), & \text{si } s \leqslant 0, \\ u(s, t-[t]), & \text{si } 0 \leqslant s \leqslant 1, \\ u(1, t-[t]), & \text{si } s \geqslant 1. \end{cases}$$

Par construction, $\tilde{u}$ est continue, coïncide avec u sur $[0,1]^2$, est la restriction d'une fonction périodique (en t) de période 1, et son image coïncide avec celle de u. Comme $[-1,2]^2$ est compact, son image K par $\tilde{u}$ est compacte, et la distance $d(\mathrm{K}, \mathbf{C} - \Omega)$ de K au fermé $\mathbf{C} - \Omega$ est > 0. Il existe donc $\delta > 0$ tel que Ω contienne $\mathrm{K}_\delta = \{z \in \mathbf{C},\ d(z,\mathrm{K}) \leqslant \delta\}$. Maintenant, si $\varepsilon > 0$, soit

$$\delta(\varepsilon) = \sup_{(s',t',s,t)\in[-1,2]^4,\ |s'-s|\leqslant\varepsilon,\ |t'-t|\leqslant\varepsilon} |\tilde{u}(s',t') - \tilde{u}(s,t)|.$$

Comme $[-1,2]^2$ est compact, $\tilde{u}$ est uniformément continue sur $[-1,2]^2$, ce qui se traduit par $\delta(\varepsilon) \to 0$ quand $\varepsilon \to 0$. On choisit $\varepsilon_0 \leqslant \frac{1}{2}$, tel que $\delta(\varepsilon) \leqslant \delta$, si $\varepsilon \leqslant \varepsilon_0$. Enfin, on choisit $\varphi : \mathbf{R} \to \mathbf{R}_+$, de classe $\mathscr{C}^2$, nulle en dehors de $[-1,1]$, avec $\int_{\mathbf{R}} \varphi = 1$, et on définit φ_ε, par $\varphi_\varepsilon(x) = \varepsilon^{-1}\varphi(\varepsilon^{-1}x)$, ce qui fait de φ_ε une fonction positive de classe $\mathscr{C}^2$ sur $\mathbf{R}$, nulle en dehors de $[-\varepsilon,\varepsilon]$, avec $\int_{\mathbf{R}} \varphi_\varepsilon = 1$.

On note $\varphi_\varepsilon^{[2]} : \mathbf{R}^2 \to \mathbf{R}_+$ la fonction définie par $\varphi_\varepsilon^{[2]}(s,t) = \varphi_\varepsilon(s)\varphi_\varepsilon(t)$. Si $\varepsilon \leqslant \varepsilon_0$, soit u_ε la restriction de $\tilde{u} * \varphi_\varepsilon^{[2]}$ à $[-\frac{1}{2}, \frac{3}{2}]$. On a donc

$$u_\varepsilon(s,t) = \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \tilde{u}(x,y)\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)\,dy\,dx.$$

Comme $|\tilde{u}(x,y) - \tilde{u}(s,t)| \leqslant \delta(\varepsilon)$, si $x \in [s-\varepsilon, s+\varepsilon]$ et $y \in [t-\varepsilon, t+\varepsilon]$, on obtient

$$\begin{aligned} |u_\varepsilon(s,t) - \tilde{u}(s,t)| &= \Big| \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} (\tilde{u}(x,y) - \tilde{u}(s,t))\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)\,dy\,dx \Big| \\ &\leqslant \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} |\tilde{u}(x,y) - \tilde{u}(s,t)|\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)\,dy\,dx \\ &\leqslant \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \delta(\varepsilon)\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y) = \delta(\varepsilon), \end{aligned}$$

ce qui montre à la fois que u_ε est à valeurs dans $\mathrm{K}_\delta \subset \Omega$, si $\varepsilon \leqslant \varepsilon_0$, et que u_ε tend uniformément vers $\tilde{u}$ sur $[\frac{-1}{2}, \frac{3}{2}]^2$ quand ε tend vers 0.

Par ailleurs, comme $\varphi_\varepsilon^{[2]}$ est de classe $\mathscr{C}^2$ sur $\mathbf{R}^2$ et à support compact, il en est de même de $\tilde{u} * \varphi_\varepsilon^{[2]}$, et comme $\tilde{u}(s,t+1) = \tilde{u}(s,t)$, si $s \in [-1,2]$, et $t \in [-2,0]$, on a $u_\varepsilon(s,t+1) = u_\varepsilon(s,t)$, si $\varepsilon \leqslant \frac{1}{2}$, si $s \in [\frac{-1}{2}, \frac{3}{2}]$, et si $t \in [\frac{-1}{2}, \frac{1}{2}]$. Ceci s'applique en particulier à $t = 0$; on en déduit que $\gamma_{s,\varepsilon} = u_\varepsilon(s,\cdot)$, est un lacet de $[0,1]$ dans Ω, pour tout $s \in [\frac{-1}{2}, \frac{3}{2}]$, et tout $\varepsilon \leqslant \varepsilon_0$. En résumé, on a prouvé que, si $\varepsilon \leqslant \varepsilon_0$, u_ε est une homotopie de lacets dans Ω, de classe $\mathscr{C}^2$. On en déduit que $\int_{\gamma_{s,\varepsilon}} f(z)\,dz$ ne dépend pas de $s \in [\frac{-1}{2}, \frac{3}{2}]$. En particulier, on a

$$\int_{\gamma_{-1/2,\varepsilon}} f(z)\,dz = \int_{\gamma_{3/2,\varepsilon}} f(z)\,dz, \quad \text{quel que soit } \varepsilon \leqslant \varepsilon_0.$$

Or, par construction, $\tilde{u}(s,t) = \gamma_0(t)$, si $s \leqslant 0$. On en déduit que

$$\gamma_{-1/2,\varepsilon}(t) = \int_{-1/2-\varepsilon}^{-1/2+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \gamma_0(t)\varphi_\varepsilon(-\frac{1}{2} - x)\varphi_\varepsilon(t-y)\,dx\,dy = \int_{t-\varepsilon}^{t+\varepsilon} \gamma_0(t)\varphi_\varepsilon(t-y)\,dy = (\gamma_0 * \varphi_\varepsilon)(t),$$

et donc que $\gamma'_{-1/2,\varepsilon} = \gamma'_0 * \varphi_\varepsilon$. On a déjà montré que $\gamma_{-1/2,\varepsilon}(t) = u_\varepsilon(\frac{-1}{2}, t)$ tend vers $\tilde{u}(\frac{-1}{2}, t) = \gamma_0(t)$; les mêmes arguments montrent que $\gamma'_{-1/2,\varepsilon}(t) \to \gamma'_0(t)$, si t n'est pas un point anguleux de γ_0. Enfin, si $t \in [0,1]$, on a

$$|f(\gamma_{-1/2,\varepsilon}(t))\gamma'_{-1/2,\varepsilon}(t)| \leqslant \sup_{z \in \mathrm{K}_\delta} |f(z)| \cdot \sup_{t \in [0,1]} |\gamma'_0(t)|,$$

ce qui permet de déduire du théorème de convergence dominée que, quand $\varepsilon \to 0$,

$$\int_{\gamma_{-1/2,\varepsilon}} f(z)\,dz = \int_0^1 f(\gamma_{-1/2,\varepsilon}(t))\gamma'_{-1/2,\varepsilon}(t)\,dt \to \int_0^1 f(\gamma_0(t))\gamma'_0(t)\,dt = \int_{\gamma_0} f(z)\,dz.$$

On montre de même que $\int_{\gamma_{3/2,\varepsilon}} f(z)\,dz \to \int_{\gamma_1} f(z)\,dz$, et un passage à la limite permet d'en conclure que $\int_{\gamma_0} f(z)\,dz = \int_{\gamma_1} f(z)\,dz$. Ceci termine la démonstration du théorème.

3. Seconde démonstration de la formule de Cauchy

Reprenons les notations du th. V.4.6. Si $\varepsilon \in]0, r - |z - z_0|[$, soit

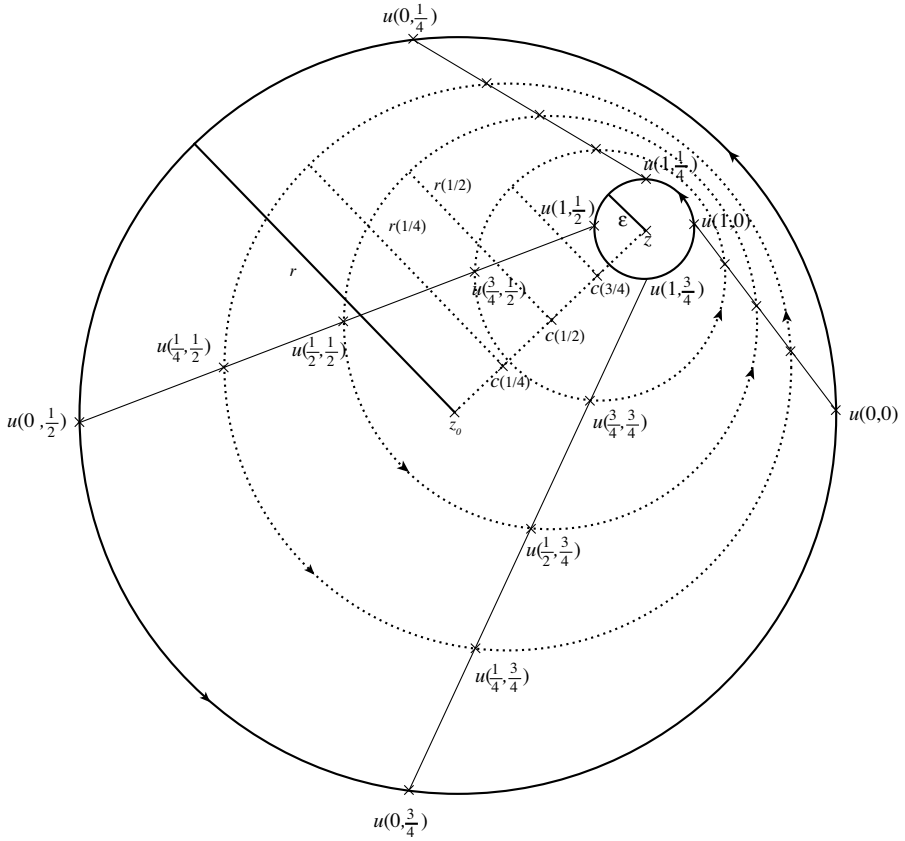
$$u(s,t) = (1-s)(z_0 + re^{2i\pi t}) + s(z + \varepsilon e^{2i\pi t}) = (1-s)z_0 + sz + ((1-s)r + s\varepsilon)e^{2i\pi t}.$$

Alors $\gamma_s(t) = u(s,t)$ est le cercle de centre $c(s) = (1-s)z_0 + sz$ et de rayon $r(s) = (1-s)r + s\varepsilon$, parcouru dans le sens direct. On a donc $\gamma_0 = \mathrm{C}(z_0, r)$ et $\gamma_1 = \mathrm{C}(z, \varepsilon)$. Par

ailleurs, on a $u(s,0) = u(s,1)$ quel que soit $s \in [0,1]$, et

$$|u(s,t) - z| \geqslant |r(s) - |c(s) - z|| = s\varepsilon + (1-s)(r - |z - z_0|) \geqslant \varepsilon,$$
$$|u(s,t) - z_0| \leqslant |c(s) - z_0| + r(s) = r - s(r - |z - z_0| - \varepsilon) \leqslant r,$$

ce qui prouve que u est une homotopie de lacets dans $\mathrm{D}(z_0,r) - \mathrm{D}(z,\varepsilon^-) \subset \Omega - \{z\}$, de $\mathrm{C}(z_0,r)$ sur $\mathrm{C}(z,\varepsilon)$.



L'homotopie de $C(z_0,r)$ sur $C(z,\varepsilon)$

Comme $\frac{f(w)}{w-z}$ est de classe $\mathscr{C}^1$ au sens complexe (en w) sur $\Omega - \{z\}$, on déduit du th. VI.1.3, que

$$\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\,dw = \frac{1}{2i\pi}\int_{\mathrm{C}(z,\varepsilon)} \frac{f(w)}{w-z}\,dw, \quad \text{quel que soit } \varepsilon > 0.$$

Or $\mathrm{C}(\varepsilon,r)$ est le chemin $t \mapsto z + \varepsilon e^{2i\pi t}$, et donc $\frac{1}{2i\pi}\int_{\mathrm{C}(z,\varepsilon)} \frac{f(w)}{w-z}\,dw = \int_0^1 f(z + \varepsilon e^{2i\pi t})\,dt$ tend vers $\int_0^1 f(z)\,dt = f(z)$ quand ε tend vers 0 (continuité d'une intégrale dépendant d'un paramètre, f étant continue en z puisque holomorphe dans un voisinage de z). En passant à la limite, on en déduit la formule $\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f(w)}{w-z}\,dw = f(z)$ que l'on cherchait à établir.

VI.2. Indice d'un lacet par rapport à un point

1. Primitives

Soit Ω un ouvert connexe de $\mathbf{C}$. Si f est holomorphe sur Ω, on dit que $\mathrm{F} : \Omega \to \mathbf{C}$ est une *primitive* de f, si F est holomorphe sur Ω et si $\mathrm{F}' = f$. Si $\gamma : [a,b] \to \Omega$ est un chemin de classe $\mathscr{C}^1$, alors $(\mathrm{F} \circ \gamma)'(t) = f(\gamma(t))\gamma'(t)$, quel que soit $t \in [a,b]$.

Une fonction holomorphe admet toujours *localement* une primitive. En effet, si f est holomorphe sur $\mathrm{D}(z_0, r^-)$, on a $f(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(z_0)}{n!}(z-z_0)^n$, d'après le (i) de la rem. V.4.9, et f admet la fonction F, définie par $\mathrm{F}(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(z_0)}{(n+1)!}(z-z_0)^{n+1}$, comme primitive sur $\mathrm{D}(z_0, r^-)$. Par contre, une fonction holomorphe sur un ouvert Ω quelconque n'admet pas toujours une primitive sur tout Ω.

Proposition VI.2.1. — *Soit Ω un ouvert connexe de $\mathbf{C}$. Si f est holomorphe sur Ω, les conditions suivantes sont équivalentes :*

(i) *f admet une primitive* F *sur Ω ;*

(ii) *$\int_\gamma f(z)\,dz = 0$, pour tout lacet γ, de classe $\mathscr{C}^1$ par morceaux, contenu dans Ω.*

Démonstration. — Si f admet une primitive F sur Ω, alors $f(z)\,dz = d\mathrm{F}$. On en déduit, en utilisant le (iv) du th. V.4.2, que $\int_\gamma f(z)\,dz = \mathrm{F}(\gamma(b)) - \mathrm{F}(\gamma(a))$, si $\gamma : [a,b] \to \Omega$ est $\mathscr{C}^1$. En particulier, si γ est un lacet, $\int_\gamma f(z)\,dz = 0$, puisque $\gamma(b) = \gamma(a)$. D'où l'implication (i)⇒(ii). Passons à la démonstration de la réciproque. Fixons $a \in \Omega$. Si γ_1 et γ_2 sont deux chemins [4] $\mathscr{C}^1$ par morceaux dans Ω, d'extrémités a et b, on obtient un lacet γ en composant γ_1 avec l'opposé de γ_2 ; on a donc $\int_{\gamma_1} f(z)\,dz - \int_{\gamma_2} f(z)\,dz = \int_\gamma f(z)\,dz = 0$, par hypothèse. Ceci permet de définir $\mathrm{F} : \Omega \to \mathbf{C}$, par $\mathrm{F}(b) = \int_\gamma f(z)\,dz$, où γ est n'importe quel chemin $\mathscr{C}^1$ par morceaux dans Ω, d'extrémités a et b.

Il suffit de prouver que F est dérivable au sens complexe, et qu'en tout point de Ω sa dérivée est $f(z_0)$, car la prop. V.4.7 montre qu'alors F est holomorphe. Soit donc $z_0 \in \Omega$, et soit $r > 0$ tel que $\mathrm{D}(z_0, r^-) \subset \Omega$. Si on fixe un chemin γ_0 joignant a à z_0 dans Ω, et si $b \in \mathrm{D}(z_0, r^-)$, on fabrique un chemin γ_b joignant a à b dans Ω, en rajoutant le segment $[z_0, b]$ au chemin γ_0. On a alors

$$\frac{\mathrm{F}(b) - \mathrm{F}(z_0)}{b - z_0} = \frac{1}{b - z_0}\Big(\int_{\gamma_0} f(z)\,dz + \int_{[z_0,b]} f(z)\,dz - \mathrm{F}(z_0)\Big) = \int_0^1 f(z_0 + t(b - z_0))\,dt,$$

et la continuité de f en z_0 permet de montrer (par exemple en utilisant le théorème de continuité d'une intégrale dépendant d'un paramètre), que $\frac{\mathrm{F}(b)-\mathrm{F}(z_0)}{b-z_0} \to f(z_0)$ quand $b \to z_0$. Ceci permet de conclure.

4. On déduit de la démonstration de ce qu'un ouvert connexe de $\mathbf{R}^n$ est connexe par arcs qu'un tel ouvert est aussi connexe par lignes brisées (réunion finie de segments de droite), et donc aussi par chemins $\mathscr{C}^1$ par morceaux.

Remarque VI.2.2. — (i) D'après le (ii) de la rem. VI.1.4, la condition (ii) est automatiquement vérifiée si Ω est un ouvert étoilé ou, plus généralement, contractile. Il en résulte qu'*une fonction holomorphe sur un ouvert contractile possède une primitive.*

(ii) Si $a \in \mathbf{C}$, et si $0 < \mathrm{R}_1 < \mathrm{R}_2$, la fonction $1/(z-a)$ est holomorphe sur la couronne $\mathrm{C}(a, \mathrm{R}_1, \mathrm{R}_2)$, mais $\int_{\mathrm{C}(a,r)} \frac{dz}{z-a} = 2i\pi \neq 0$ si $\mathrm{R}_1 < r < \mathrm{R}_2$. La fonction $1/(z-a)$ n'admet donc pas de primitive sur la couronne $\mathrm{C}(a, \mathrm{R}_1, \mathrm{R}_2)$ et cette couronne n'est pas contractile.

Proposition VI.2.3. — (logarithme d'une fonction holomorphe)
Soit Ω un ouvert contractile de $\mathbf{C}$, et soit f holomorphe sur Ω ne s'annulant pas sur Ω. Alors il existe g holomorphe sur Ω, telle que $f = e^g$, et on a $g' = \frac{f'}{f}$.

Démonstration. — Comme Ω est contractile, et comme $\frac{f'}{f}$ est holomorphe sur Ω, il existe, d'après le (i) de la rem. VI.2.2, h holomorphe sur Ω telle que $h' = \frac{f'}{f}$. Soit $z_0 \in \Omega$. Quitte à rajouter une constante à h, on peut supposer que $e^{h(z_0)} = f(z_0)$. Mais alors $(e^{-h}f)' = -h'e^{-h}f + e^{-h}f' = 0$, et donc $e^{-h}f$ est constante sur Ω, et comme elle vaut 1 en z_0, on a $f = e^h$ sur Ω. Si g est une autre fonction holomorphe sur Ω vérifiant $e^g = f$, on a $e^{g-h} = 1$, et donc $g - h$ est holomorphe et à valeurs dans $2i\pi\mathbf{Z}$. Comme Ω est connexe, $g - h$ est constante et $g' = \frac{f'}{f}$.

Exercice VI.2.4. — (Théorème de Morera) Soient $z_0 \in \mathbf{C}$ et $r > 0$.
(i) Montrer que, si f est holomorphe sur $\mathrm{D}(z_0, r^-)$, alors

$$\int_{[a,b]} f(z)\,dz + \int_{[b,c]} f(z)\,dz + \int_{[c,a]} f(z)\,dz = 0 \quad \text{quels que soient } a, b, c \in \mathrm{D}(z_0, r^-). \tag{VI.2.1}$$

(ii) Soit $f : \mathrm{D}(z_0, r^-) \to \mathbf{C}$ continue, et vérifiant la propriété (VI.2.1). Soit $\mathrm{F}(z) = \int_{[z_0,z]} f(z)\,dz$. Montrer que $\frac{1}{h}(\mathrm{F}(z+h) - \mathrm{F}(z))$ tend vers $f(z)$, quand h tend vers 0. En déduire que F et f sont holomorphes.
(iii) Soit Ω un ouvert de $\mathbf{C}$. Montrer que $f : \Omega \to \mathbf{C}$ est holomorphe si et seulement si f est continue et $\int_{[a,b]} f(z)\,dz + \int_{[b,c]} f(z)\,dz + \int_{[c,a]} f(z)\,dz = 0$ quels que soient $a, b, c \in \Omega$ tels que le triangle plein (i.e. avec son intérieur) de sommets a, b et c soit inclus dans Ω.

2. Nombre de tours d'un lacet autour d'un point

Soit $z_0 \in \mathbf{C}$, et soit γ un lacet ne passant pas par z_0. Notre but est de définir mathématiquement le nombre de tours que fait γ autour de z_0.

2.1. *Définition*

Lemme VI.2.5. — *Soit $\gamma : [a,b] \to \mathbf{C} - \{z_0\}$ un chemin $\mathscr{C}^1$ par morceaux. Si $t \in [a,b]$, soit γ_t la restriction de γ à $[a,t]$, et soit $f(t) = \int_{\gamma_t} \frac{dz}{z-z_0}$. Alors $e^{-f(t)}(\gamma(t) - z_0)$ est constante sur $[a,b]$.*

Démonstration. — Par définition, on a $f(t) = \int_0^t \frac{\gamma'(u)}{\gamma(u)-z_0}\,du$, et donc $f'(t) = \frac{\gamma'(t)}{\gamma(t)-z_0}$, si t

n'est pas un point anguleux de γ. La dérivée de $t \mapsto g(t) = e^{-f(t)}(\gamma(t) - z_0)$ est donc

$$-f'(t)e^{-f(t)}(\gamma(t) - z_0) + e^{-f(t)}\gamma'(t) = e^{-f(t)}(-\frac{\gamma'(t)}{\gamma(t) - z_0}(\gamma(t) - z_0) + \gamma'(t)) = 0,$$

et g est constante par morceaux ; comme elle est continue cela permet de conclure.

Corollaire VI.2.6. — *Si $\gamma : [a, b] \to \mathbf{C}$ est un lacet $\mathscr{C}^1$ par morceaux, ne rencontrant pas z_0, alors $\mathrm{I}(\gamma, z_0) = \frac{1}{2i\pi}\int_\gamma \frac{dz}{z-z_0}$ est un entier.*

Démonstration. — En reprenant les notations du lemme, on voit que $e^{f(b)} = e^{f(a)}\frac{\gamma(b)-z_0}{\gamma(a)-z_0}$, et, comme γ est un lacet, que $\exp(\int_\gamma \frac{dz}{z-z_0}) = e^{f(b)} = e^{f(a)} = 1$, ce qui permet de conclure.

L'entier $\mathrm{I}(\gamma, z_0)$ défini ci-dessus est *l'indice de γ par rapport à z_0*. Par exemple, si γ est le chemin $\mathrm{C}(a, r)$, et si $|z_0 - a| < r$, la formule de Cauchy utilisée pour la fonction constante 1, montre que $\mathrm{I}(\mathrm{C}(a, r), z_0) = 1$. Par contre, si $|z_0 - a| > r$, le cercle $\mathrm{C}(z_0, r)$ est homotope à $\{a\}$ dans $\mathbf{C} - \{z_0\}$, et comme $\frac{1}{z-z_0}$ est holomorphe sur $\mathbf{C} - \{z_0\}$, on a $\mathrm{I}(\mathrm{C}(a, r), z_0) = 0$. Autrement dit, si z_0 est à l'intérieur du cercle parcouru dans le sens direct, l'indice du cercle par rapport à z_0 est 1, alors que si z_0 est à l'extérieur, cet indice est 0, ce qui est en accord avec l'idée selon laquelle $\mathrm{I}(\gamma, z_0)$ représente le nombre de tours que fait γ autour de z_0. On fera attention au fait que, *si le cercle est parcouru dans le sens rétrograde, son indice par rapport à un point à l'intérieur est -1.*

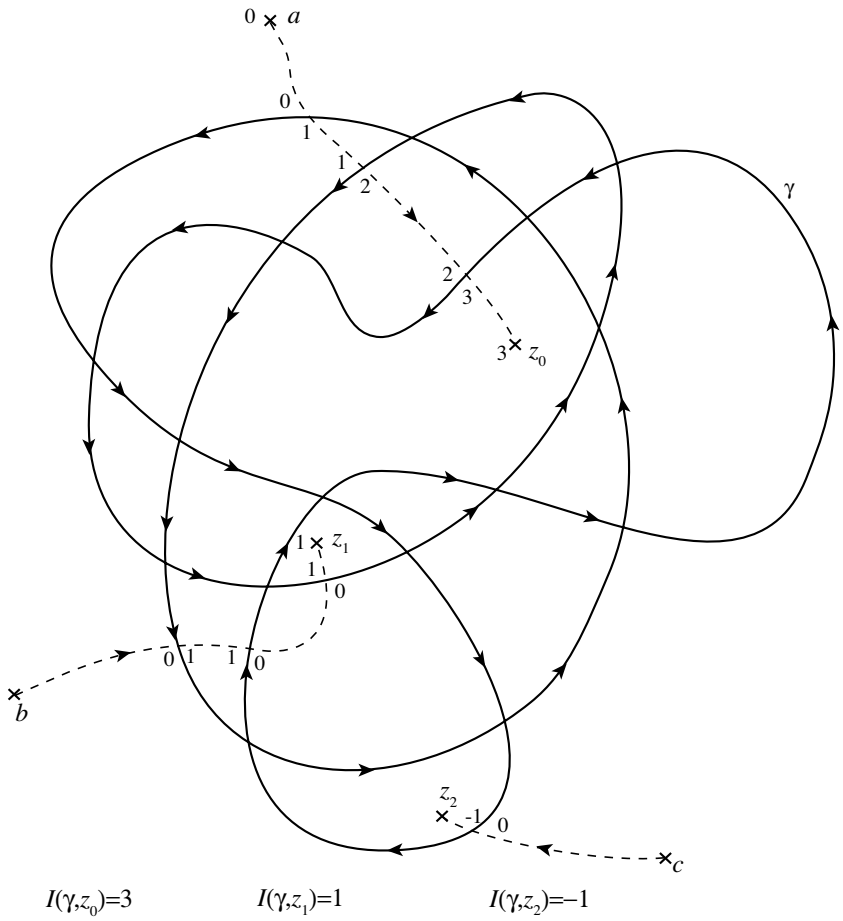
2.2. *Détermination visuelle de l'indice d'un lacet par rapport à un point*

Dans les situations considérées dans ce cours, les lacets sont sans point double (et sont constitués de segments de droite et d'arcs de cercle), et un théorème de Jordan affirme qu'un tel lacet découpe le plan en deux régions, l'une à l'intérieur du lacet et l'autre à l'extérieur du lacet, auquel cas on se retrouve dans le même cas de figure que pour le cercle. Dans le cas général, déterminer sur un dessin l'indice d'un lacet par rapport à un chemin peut donner le tournis, mais la prop. VI.2.7 ci-dessous fournit un procédé permettant un calcul en regardant toujours droit devant soi.

La recette est la suivante. On choisit un point $a \in \mathbf{C}$ assez grand pour que que $\gamma \subset \mathrm{D}(0, |a|^-)$, et on trace un chemin u allant de a à z_0. Alors $\mathrm{I}(\gamma, z_0) = n_g - n_d$, où n_g (resp. n_d) est le nombre de points d'intersections de u et γ, où γ arrive de la gauche [5] (resp. de la droite), quand on va de a à z_0.

Soit γ un lacet dans $\mathbf{C}$. Comme γ est compact (en tant qu'image d'un intervalle compact par une application continue), son complémentaire est ouvert, et chacune des composantes connexes du complémentaire est un ouvert. D'autre part, si R est assez grand, γ est inclus dans $\mathrm{D}(0, \mathrm{R})$, et comme $\mathbf{C} - \mathrm{D}(0, \mathrm{R})$ est connexe, une (et une seule) des composantes connexes de $\mathbf{C} - \gamma$ contient $\mathbf{C} - \mathrm{D}(0, \mathrm{R})$, pour R assez grand. Cette composante connexe est *la composante connexe de l'infini.*

5. Pour que ceci ait un sens, il vaut mieux prendre quelques précautions ; par exemple, imposer que u et γ ne s'intersectent qu'en des points simples non anguleux de γ, et que les tangentes à γ et à u en un point d'intersection ne soient pas colinéaires.



Proposition VI.2.7. — *Soit γ un lacet $\mathscr{C}^1$ par morceaux.*

(i) *$z \mapsto \mathrm{I}(\gamma, z)$ est constant sur chacune des composantes connexes de $\mathbf{C} - \gamma$.*

(ii) *$\mathrm{I}(\gamma, z) = 0$ si z est dans la composante connexe de l'infini de $\mathbf{C} - \gamma$.*

(iii) *Soit $t \mapsto \gamma(t)$, $t \in [a, b]$ un paramètrage de γ, $\mathscr{C}^1$ par morceaux, et soit $t_0 \in]a, b[$ tel que $\gamma(t_0)$ soit un point simple de γ, et $\gamma'(t_0) \neq 0$. Si $h \in \mathbf{C}$ vérifie $\mathrm{Im}(h) > 0$, et si $\varepsilon > 0$ est assez petit, alors*

- *$\gamma(t_0) + \varepsilon h \gamma'(t_0)$ et $\gamma(t_0) - \varepsilon h \gamma'(t_0)$ n'appartiennent pas à γ,*
- *$\mathrm{I}(\gamma, \gamma(t_0) + \varepsilon h \gamma'(t_0)) - \mathrm{I}(\gamma, \gamma(t_0) - \varepsilon h \gamma'(t_0)) = 1$.*

Démonstration. — Le théorème de continuité d'une intégrale dépendant d'un paramètre montre que $z_0 \mapsto \mathrm{I}(\gamma, z_0)$ est continue sur $\mathbf{C} - \gamma$, et comme $\mathrm{I}(\gamma, z_0)$ est à valeurs dans $\mathbf{Z}$, qui est discret, cela démontre le (i).

Si $\gamma \subset \mathrm{D}(0, \mathrm{R})$, et si $|z_0| > \mathrm{R}$, alors γ est homotope à un point dans $\mathbf{C} - \{z_0\}$ (et même dans $\mathrm{D}(0, \mathrm{R})$, puisque $\mathrm{D}(0, \mathrm{R})$ est contractile), et comme $\frac{1}{z - z_0}$ est holomorphe sur $\mathbf{C} - \{z_0\}$, on a $\int_\gamma \frac{dz}{z - z_0} = 0$. On en déduit le (ii) pour $|z_0| > \mathrm{R}$, et le (i) permet de terminer la démonstration du (ii).

Passons à la démonstration du (iii). Choisissons $h \in \mathbf{C}$, avec $\mathrm{Im}(h) > 0$. On a donc $0 < \arg(h) < \pi$. Quitte à faire une translation sur la variable, on peut supposer $t_0 = 0$, et quitte à transformer la situation par la similitude $z \mapsto \gamma'(t_0)^{-1}(z - \gamma(t_0))$, on peut supposer que $\gamma(t_0) = 0$, et $\gamma'(t_0) = 1$, ce qui permet de simplifier un peu les formules. On a alors $\lim_{t \to 0} t^{-1}\gamma(t) = 1$, ce qui implique qu'il existe $\delta > 0$ tel que, quel que soit $t \in [-\delta, \delta] - \{0\}$,

- $|\arg(t^{-1}\gamma(t))| < \frac{1}{2}\inf(\arg(h), \pi - (\arg(h))$,
- $|t^{-1}\gamma(t) - 1| \leqslant 1/2$.

Par ailleurs, comme $0 = \gamma(0)$ est un point simple de γ, il existe $\eta > 0$ tel que $d(0, \gamma(t)) \geqslant \eta$, si $t \in [a, b] -]-\delta, \delta[$. On en déduit que, si $0 < \varepsilon < |h|^{-1}\eta$, alors $\pm\varepsilon h$ n'est pas de la forme $\gamma(t)$, avec $t \in [a, b] -]-\delta, \delta[$. Par ailleurs, $\pm\varepsilon h$ n'est pas non plus de la forme $\gamma(t)$, avec $t \in [-\delta, \delta]$, puisque $\pm\varepsilon h \neq 0$ et $\arg(\frac{\pm\varepsilon h}{\gamma(t)}) \neq 0$, si $t \in [-\delta, \delta] - \{0\}$, d'après le choix de δ. En résumé, si $0 < \varepsilon < |h|^{-1}\eta$, alors $\pm\varepsilon h$ n'appartient pas à γ.

Maintenant, on a $\mathrm{I}(\gamma, \varepsilon h) - \mathrm{I}(\gamma, -\varepsilon h) = \mathrm{I}_1(\varepsilon) + \mathrm{I}_2(\varepsilon)$, où l'on a posé

$$\mathrm{I}_1(\varepsilon) = \frac{1}{2i\pi}\int_{\gamma([a,-\delta])\cup\gamma([\delta,b])} \frac{dz}{z-\varepsilon h} - \frac{dz}{z+\varepsilon h} \quad \text{et} \quad \mathrm{I}_2(\varepsilon) = \frac{1}{2i\pi}\int_{\gamma([-\delta,\delta])} \frac{dz}{z-\varepsilon h} - \frac{dz}{z+\varepsilon h}.$$

On a $\lim_{\varepsilon\to 0^+} \mathrm{I}_1(\varepsilon) = 0$, puisque $\frac{1}{z-\varepsilon h} - \frac{1}{z+\varepsilon h}$ tend vers 0 et est majoré en module par $\frac{2}{\eta-\varepsilon|h|}$. Comme $\mathrm{I}(\gamma, \varepsilon h) - \mathrm{I}(\gamma, -\varepsilon h) \in \mathbf{Z}$, il suffit donc, pour montrer que $\mathrm{I}(\gamma, \varepsilon h) - \mathrm{I}(\gamma, -\varepsilon h) = 1$, si $\varepsilon > 0$ est assez petit, de prouver que $\lim_{\varepsilon\to 0^+} \mathrm{I}_2(\varepsilon) = 1$. Pour cela, écrivons $2i\pi\,\mathrm{I}_2(\varepsilon)$ sous la forme

$$2i\pi\,\mathrm{I}_2(\varepsilon) = \int_{\gamma([-\delta,\delta])} \frac{2\varepsilon h}{z^2 - \varepsilon^2 h^2} dz = \int_{-\delta}^{\delta} \frac{2\varepsilon h\,\gamma'(t)}{\gamma(t)^2 - \varepsilon^2 h^2}\, dt = \int_{-\delta/\varepsilon}^{\delta/\varepsilon} \frac{2h\,\gamma'(\varepsilon t)}{\varepsilon^{-2}\gamma(\varepsilon t)^2 - h^2}\, dt.$$

L'expression sous l'intégrale tend vers $\frac{2h}{t^2-h^2}$ quand ε tend vers 0 et $t \in \mathbf{R}$. Par ailleurs, d'après le choix de δ, il existe $c > 0$ tel que $2\pi - c > \arg(h^2\gamma(u)^{-2}) > c$, si $u \in [-\delta, \delta]$; on en déduit l'existence de $\mathrm{C} > 0$ (avec $\mathrm{C} = 1$, si $\cos c \leqslant 0$, et $\mathrm{C} = |\sin c|$, si $\cos c \geqslant 0$) tel que $|\lambda\gamma(t)^2 - \mu h^2| \geqslant \mathrm{C}\sup(|\lambda\gamma(t)^2|, |\mu h^2|)$, quels que soient $\mu, \lambda \in \mathbf{R}_+$. Comme $|\gamma(u)| \geqslant \frac{1}{2}|u|$, et comme il existe $\mathrm{M} \geqslant 0$ tel que $|\gamma'(u)| \leqslant \mathrm{M}$, si $u \in [-\delta, \delta]$, on peut majorer, en module, $\frac{2h\,\gamma'(\varepsilon t)}{\varepsilon^{-2}\gamma(\varepsilon t)^2 - h^2}$ sur $[-\delta/\varepsilon, \delta/\varepsilon]$, par $\frac{2|h|\mathrm{M}}{\mathrm{C}\sup(t^2/4, |h|^2)}$, qui est une fonction sommable sur $\mathbf{R}$, indépendante de ε. On obtient donc, via le théorème de continuité d'une intégrale dépendant d'un paramètre,

$$\lim_{\varepsilon\to 0^+} 2i\pi\,\mathrm{I}_2(\varepsilon) = \int_{-\infty}^{+\infty} \frac{2h}{t^2 - h^2} dt.$$

Enfin, en posant $h = \sigma + i\tau$, avec $\tau > 0$ par hypothèse, cette dernière intégrale devient.

$$\begin{aligned}\int_{-\infty}^{+\infty} \frac{dt}{t-h} - \frac{dt}{t+h} &= \int_{-\infty}^{+\infty} \frac{(t-\sigma)+i\tau}{(t-\sigma)^2+\tau^2} - \frac{(t+\sigma)-i\tau}{(t+\sigma)^2+\tau^2} dt \\ &= \Big[\frac{1}{2}\log\frac{(t-\sigma)^2+\tau^2}{(t+\sigma)^2+\tau^2}\Big]_{-\infty}^{+\infty} + i\Big[\operatorname{artg}\frac{t-\sigma}{\tau} + \operatorname{artg}\frac{t+\sigma}{\tau}\Big]_{-\infty}^{+\infty} = 2i\pi,\end{aligned}$$

ce qui permet de conclure. (On peut fabriquer (exercice) une démonstration de ce que $\mathrm{I}_2(\varepsilon) \to 1$ en remarquant qu'au voisinage de 0, γ est le graphe d'une fonction, ce qui permet d'écrire $2i\pi\,\mathrm{I}_2(\varepsilon)$ comme l'intégrale de $\frac{dz}{z}$ sur un contour C_ε ressemblant à un parallélogramme de sommets $\pm\delta \pm \varepsilon h$, privé des cotés verticaux (dont la longueur tend vers 0). La formule des résidus (th. VI.3.13) montre que l'intégrale sur C_ε est égale à $2i\pi$. On évite de cette manière les majorations ci-dessus.)

VI.3. La formule des résidus de Cauchy

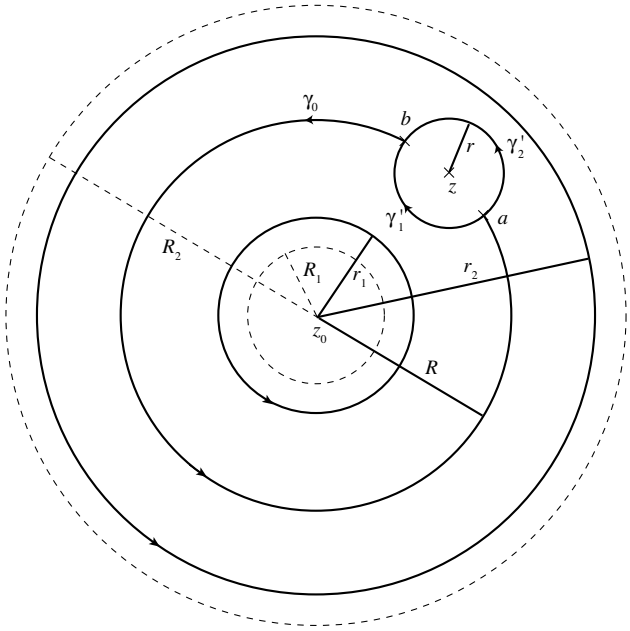
1. Fonctions holomorphes sur une couronne

Si $z_0 \in \mathbf{C}$ et si $0 \leqslant \mathrm{R}_1, < \mathrm{R}_2$, on note $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$ la *couronne ouverte* des $z \in \mathbf{C}$, avec $\mathrm{R}_1 < |z - z_0| < \mathrm{R}_2$. Si $\mathrm{R}_1 = 0$, on obtient le *disque épointé* ouvert de centre z_0 et de rayon R_2 (i.e. $\mathrm{D}(z_0, \mathrm{R}_2^-) - \{z_0\}$).

Lemme VI.3.1. — *Si f est holomorphe sur la couronne $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$, si $z \in \mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$, et si $\mathrm{R}_1 < r_1 < |z - z_0| < r_2 < \mathrm{R}_2$, alors*

$$f(z) = \frac{1}{2i\pi} \int_{\mathrm{C}(z_0, r_2)} \frac{f(w)}{w - z}\, dw - \frac{1}{2i\pi} \int_{\mathrm{C}(z_0, r_1)} \frac{f(w)}{w - z}\, dw.$$

Démonstration. — Le lecteur est invité à suivre les arguments qui suivent [6]sur un dessin.



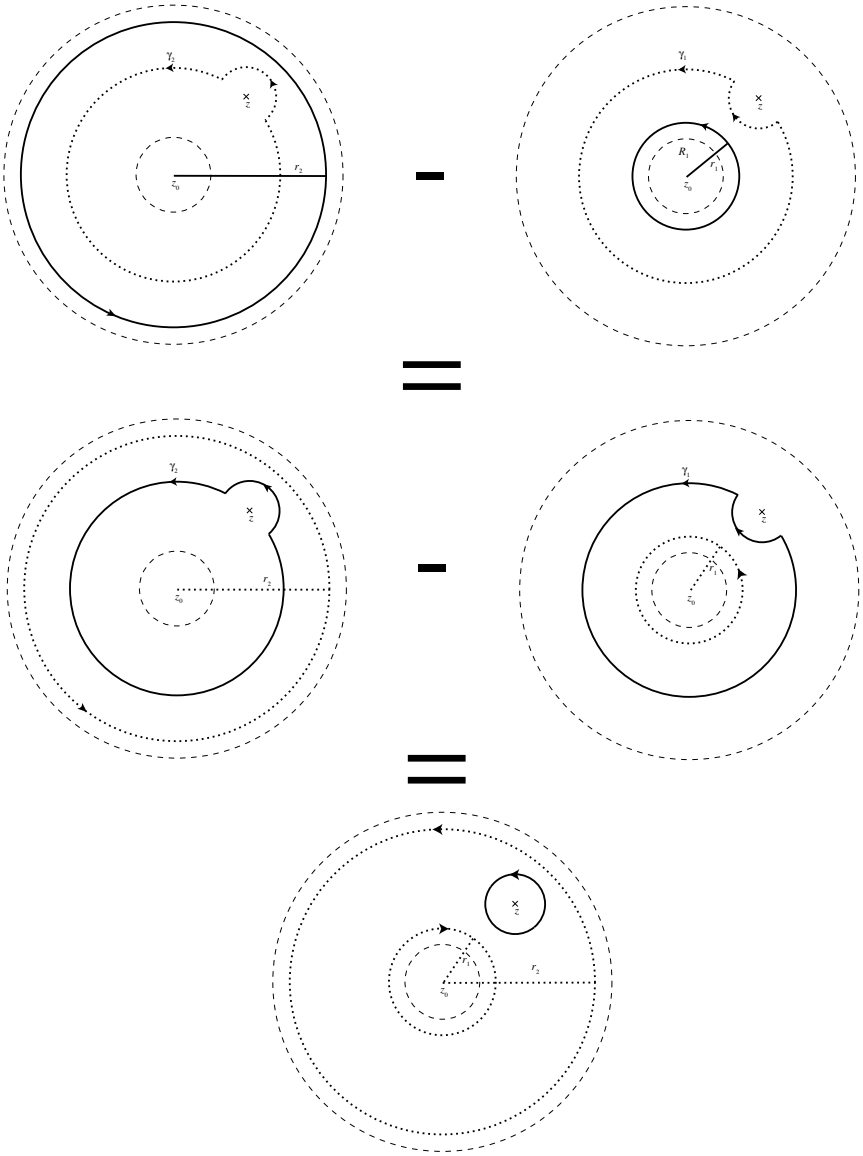
Soit $r < \inf(r_2 - |z - z_0|, |z - z_0| - r_1)$ de telle sorte que $\mathrm{D}(z, r) \subset \mathrm{C}(z_0, r_1, r_2)$. Soit $\mathrm{R} \in]|z - z_0| - r, |z - z_0| + r[$ de telle sorte que les cercles $\mathrm{C}(z_0, \mathrm{R})$ et $\mathrm{C}(z, r)$ s'intersectent en deux points a et b. Soit γ_0 l'arc du cercle $\mathrm{C}(z_0, \mathrm{R})$ à l'extérieur de $\mathrm{D}(z, r)$, parcouru dans le sens direct ; quitte à échanger les noms de a et b, c'est un chemin allant de b à a. Soit γ_1' (resp. γ_2') l'arc du cercle $\mathrm{C}(z, r)$ à l'intérieur (resp. l'extérieur) de $\mathrm{D}(z_0, \mathrm{R})$, parcouru dans le sens rétrograde (resp. direct) ; c'est un chemin allant de a à b. Si $i \in \{1, 2\}$, soit γ_i le lacet dans $\mathrm{C}(z_0, r_1, r_2) - \{z\}$ obtenu en composant γ_0, avec γ_i' ; c'est un lacet homotope [7]

6. Il peut aussi préférer utiliser la forme générale de la formule de Stokes, dont on déduit directement que $\int_{\mathrm{C}(z_0, r_i)} \frac{f(w)}{w-z}\, dw = \int_{\gamma_i} \frac{f(w)}{w-z}\, dw$, car f est holomorphe sur l'ouvert délimité par $\mathrm{C}(z_0, r_i)$ et γ_i.

7. C'est parfaitement évident sur un dessin, mais on peut aussi écrire une formule d'homotopie explicite. Par exemple, pour aller de γ_2 à $\mathrm{C}(z_0, r_2)$, on paramètre γ_0 par $\gamma_0(t) = z_0 + \mathrm{R}e^{2i\pi(t-\beta)}$, où β est choisit pour que $\gamma_0(t) = b$, et $t \in [0, \alpha]$, avec $\alpha < 1$ vérifiant $\gamma_0(\alpha) = a$, puis on paramètre γ_2' sous la forme $\gamma_2'(t) = z + re^{2i\pi(\lambda t + \mu)}$, avec $t \in [\alpha, 1]$, ce qui nous fournit un paramètrage $t \mapsto \gamma_2(t)$, avec $t \in [0, 1]$, de γ_2. Enfin, on paramètre $\mathrm{C}(z_0, r_2)$ sous la forme $t \mapsto \delta(t) = z_0 + r_2 e^{2i\pi(t-\beta)}$, avec $t \in [0, 1]$, et on fabrique une homotopie $u(s, t)$ de γ_2 sur $\mathrm{C}(z_0, r_2)$, en posant $u(s, t) = (1 - s)\gamma_2(t) + s\delta(t)$. Il reste à vérifier que cette homotopie a bien lieu dans $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2) - \{z\}$, ce qui est évident sur un dessin (on s'est débrouillé pour que l'angle entre $\gamma_2(t) - z_0$ et $\delta(t) - z_0$ soit petit, et $u(s, t)$ parcourt le segment $[\gamma_2(t), \delta(t)]$ quand s varie de 0 à 1).

dans $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2) - \{z\}$ à $\mathrm{C}(z_0, r_i)$. On a donc

$$\begin{aligned}\int_{\mathrm{C}(z_0,r_2)} \frac{f(w)}{w-z}\,dw - \int_{\mathrm{C}(z_0,r_1)} \frac{f(w)}{w-z}\,dw &= \int_{\gamma_2} \frac{f(w)}{w-z}\,dw - \int_{\gamma_1} \frac{f(w)}{w-z}\,dw \\ &= \int_{\gamma_2'} \frac{f(w)}{w-z}\,dw - \int_{\gamma_1'} \frac{f(w)}{w-z}\,dw = \int_{\mathrm{C}(z,r)} \frac{f(w)}{w-z}\,dw.\end{aligned}$$



On conclut en utilisant la formule de Cauchy pour f, qui est holomorphe sur $\mathrm{D}(z, r^-)$.

Corollaire VI.3.2. — *Si f est holomorphe sur $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$, il existe une unique suite $(a_n)_{n\in\mathbf{Z}}$ d'éléments de $\mathbf{C}$ vérifiant*

(i) $\sum_{n=0}^{+\infty} a_n z^n$ *converge si* $|z| < \mathrm{R}_2$ *et* $\sum_{n=-\infty}^{-1} a_n z^n$ *converge si* $|z|^{-1} < \mathrm{R}_1^{-1}$;
(ii) $f(z)$ *est somme de la série* (de Laurent) $\sum_{n\in\mathbf{Z}} a_n(z-z_0)^n$, *si* $z \in \mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$.
De plus, quels que soient $r \in]\mathrm{R}_1, \mathrm{R}_2[$ *et* $n \in \mathbf{Z}$, *on a*

$$a_n = \frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r)} (w-z_0)^{-n-1} f(w)\, dw.$$

Démonstration. — Si $r, r' \in]\mathrm{R}_1, \mathrm{R}_2[$, les cercles $\mathrm{C}(z_0, r)$ et $\mathrm{C}(z_0, r')$ sont homotopes dans $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$. Comme $(z-z_0)^{-n-1} f(z)$ est holomorphe dans $\mathrm{C}(z_0, \mathrm{R}_1, \mathrm{R}_2)$, cela permet de montrer que $\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} (z-z_0)^{-n-1} f(z)\, dz$ ne dépend pas du choix de $r \in]\mathrm{R}_1, \mathrm{R}_2[$; notons le a_n. Maintenant, d'après le lemme VI.3.1, si $\mathrm{R}_1 < r_1 < |z-z_0| < r_2 < \mathrm{R}_2$, on a

$$f(z) = \frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r_2)} \frac{f(w)}{w-z}\, dw - \frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r_1)} \frac{f(w)}{w-z}\, dw.$$

Par ailleurs,

$$\frac{1}{w-z} = \begin{cases} \sum_{n=0}^{+\infty} \frac{(z-z_0)^n}{(w-z_0)^{n+1}}, & \text{si } |w-z_0| = r_2, \\ -\sum_{n=0}^{+\infty} \frac{(w-z_0)^n}{(z-z_0)^{n+1}} = -\sum_{n=-\infty}^{-1} \frac{(z-z_0)^n}{(w-z_0)^{n+1}}, & \text{si } |w-z_0| = r_1. \end{cases}$$

On en déduit, en reportant les développements ci-dessus dans l'intégrale comme dans la démonstration de la prop. V.4.7, la convergence normale (pour la norme uniforme) de la série $\sum_{n\in\mathbf{Z}} a_n(z-z_0)^n$ vers $f(z)$ sur la couronne $r_1 < |z-z_0| < r_2$. On conclut en faisant tendre r_1 vers R_1 et r_2 vers R_2.

Exercice VI.3.3. — Soit f holomorphe sur $\mathbf{C}^*$. Montrer qu'il existe une suite $(a_n)_{n\in\mathbf{Z}}$ d'éléments de $\mathbf{C}$ telle que l'on ait $f(z) = \sum_{n\in\mathbf{Z}} a_n z^n$, pour tout $z \in \mathbf{C}^*$.

Exercice VI.3.4. — Soit $\mathscr{H} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$ le demi-plan de Poincaré, et soit $f : \mathscr{H} \to \mathbf{C}$ une fonction holomorphe, périodique de période 1.

(i) Montrer qu'il existe $\tilde{f} : \mathrm{D}(0, 1^-) - \{0\} \to \mathbf{C}$, holomorphe, telle que $f(z) = \tilde{f}(e^{2i\pi z})$.

(ii) En déduire qu'il existe des $a_n(f) \in \mathbf{C}$, pour $n \in \mathbf{Z}$, tels que $f(z) = \sum_{n\in\mathbf{Z}} a_n(f) e^{2i\pi nz}$, quel que soit $z \in \mathscr{H}$, la série étant normalement convergente sur toute bande horizontale $a \leqslant \mathrm{Im}(z) \leqslant b$, avec $0 < a < b < +\infty$.

(iii) Montrer que $a_n(f) = \int_{[i\mathrm{T}, 1+i\mathrm{T}]} e^{-2i\pi z} f(z) dz$, pour tout $\mathrm{T} > 0$ (on pourra utiliser l'ex. V.4.5).

2. Fonctions holomorphes sur un disque épointé ; résidus

Soient Ω un ouvert de $\mathbf{C}$, $z_0 \in \Omega$, et f holomorphe sur $\Omega - \{z_0\}$. Soit $r > 0$ tel que $\mathrm{D}(z_0, r^-) \subset \Omega$. La fonction f est donc holomorphe sur le disque épointé $\mathrm{D}(z_0, r^-) - \{z_0\}$ qui peut aussi être vu comme la couronne $\mathrm{C}(z_0, 0, r)$. On peut donc lui appliquer les résultats du n° 1, et on en déduit l'existence d'une suite $(a_n)_{n\in\mathbf{Z}}$ de nombres complexes vérifiant les propriétés suivantes :

- la série $g(z) = \sum_{n=0}^{+\infty} a_n(z-z_0)^n$ converge sur $\mathrm{D}(z_0, r^-)$;
- la série $h(z) = \sum_{n\leqslant -1} a_n(z-z_0)^n$ converge, et définit une fonction holomorphe, sur $\mathbf{C} - \{z_0\}$;
- $f(z) = \sum_{n\in\mathbf{Z}} a_n(z-z_0)^n$, quel que soit $z \in \mathrm{D}(z_0, r^-) - \{z_0\}$.

La série $h(z)$ est la *partie singulière* de f en z_0, et le coefficient a_{-1} de $(z-z_0)^{-1}$ est *le résidu* $\mathrm{Res}(f, z_0)$ *de* f *en* z_0.

On dit que f est *holomorphe* [8] *en* z_0, si $h = 0$. Plus généralement, on dit que f est *méromorphe* en z_0, s'il existe $k \in \mathbf{Z}$, avec $a_n = 0$, si $n \leqslant k$. Si k est un entier $\geqslant 1$, on dit que f *a un pôle d'ordre* k en z_0, si $a_{-k} \neq 0$ et $a_n = 0$, quel que soit $n < -k$ [9]. On dit que f *a une singularité essentielle en* z_0 si elle n'est pas méromorphe en z_0.

On peut reformuler les définitions ci-dessus en terme de *la valuation* $v_{z_0}(f)$ de f en z_0 définie par

$$v_{z_0}(f) = \inf_{n\in\mathbf{Z},\ a_n\neq 0} \in \mathbf{Z} \cup \{\pm\infty\}.$$

On a alors :

- $v_{z_0}(f) = -\infty \iff f$ a une singularité essentielle en z_0 ;
- $v_{z_0}(f) > -\infty \iff f$ est méromorphe en z_0 ;
- $v_{z_0}(f) = -k$, $k \in \mathbf{N} - \{0\} \iff f$ a un pôle d'ordre k en z_0 ;
- $v_{z_0}(f) \geqslant 0 \iff f$ est holomorphe en z_0 ;
- $v_{z_0}(f) = 0 \iff f$ est holomorphe et ne s'annule pas en z_0 ;
- $v_{z_0}(f) = k$, $k \in \mathbf{N} \iff f$ a un zéro d'ordre k en z_0 ;
- $v_{z_0}(f) = +\infty \iff f$ est nulle dans la composante connexe de z_0 dans Ω.

Dans les équivalences précédentes, la seule qui ne soit pas une reformulation de la définition est la dernière, qui est une reformulation du théorème des zéros isolés (th. V.3.3).

Si Ω est un ouvert de $\mathbf{C}$, on dit que $f : \Omega \to \mathbf{C}$ est *méromorphe* sur Ω, si f est méromorphe en tout point de Ω.

Pour un certain nombre d'applications, il est important de savoir calculer explicitement le résidu $\mathrm{Res}(f, z_0)$ de f en z_0. L'exercice ci-dessous fournit quelques recettes [10].

Exercice VI.3.5. — Soient Ω un ouvert de $\mathbf{C}$ et $z_0 \in \Omega$.

(i) Si f est holomorphe en z_0, alors $\mathrm{Res}(f, z_0) = 0$.

(ii) Si $f = \frac{g}{h}$, où g et h sont holomorphes sur Ω, si $g(z_0) \neq 0$, et si h a un zéro simple en z_0, alors $\mathrm{Res}(f, z_0) = \frac{g(z_0)}{h'(z_0)}$.

(iii) Si f a un pôle simple en z_0, et si g est holomorphe en z_0, alors $\mathrm{Res}(gf, z_0) = g(z_0)\mathrm{Res}(f, z_0)$.

(iv) Si $k \geqslant 1$, et $f = (z-z_0)^{-k}g$, où g est holomorphe sur Ω, alors $\mathrm{Res}(f, z_0) = \frac{g^{(k-1)}(z_0)}{(k-1)!}$.

---

8. C'est un abus de langage, mais cela veut dire que la fonction f peut se prolonger par continuité en z_0, et que la fonction obtenue est holomorphe sur $\mathrm{D}(z_0, r^-)$.

9. Une fonction est donc méromorphe en z_0 si et seulement si elle est holomorphe ou a un pôle d'ordre fini.

10. Si f a une singularité essentielle, il est en général impossible de trouver une expression « finie » du résidu. C'est une des raisons qui fait que certaines intégrales résistent à la méthode des résidus (cf. exercices du n° 4).

(v) Si f est méromorphe sur Ω, alors $\frac{f'}{f}$ est méromorphe sur Ω, avec des pôles simples aux pôles et zéros de f, et on a

$$\mathrm{Res}(\frac{f'}{f}, z_0) = v_{z_0}(f), \quad \text{quel que soit } z_0 \in \Omega.$$

Exercice VI.3.6. — Soit $\lambda \in \mathbf{R}_+^*$. Calculer $\mathrm{Res}(\frac{1}{z^2+\lambda^2} e^{1/z}, 0)$.

Exercice VI.3.7. — Montrer que f est méromorphe sur Ω, si et seulement si tout point z_0 de Ω a un voisinage [11] ouvert U sur lequel f peut s'écrire sous la forme $f = \frac{g}{h}$, avec g et h holomorphes sur U.

Exercice VI.3.8. — Soit $f : \Omega \to \mathbf{C}$ méromorphe.

(i) Montrer que les pôles de f sont isolés (si a est un pôle, il existe $r > 0$ tel que a soit le seul pôle de f dans $\mathrm{D}(a, r^-)$).

(ii) Montrer que f n'a qu'un nombre fini de pôles dans $\mathrm{D}(x_0, r)$, si $\mathrm{D}(x_0, r) \subset \Omega$.

Exercice VI.3.9. — (i) Montrer qu'une fonction méromorphe bornée à l'infini (il existe M et R tels que $|f(z)| \leqslant \mathrm{M}$, si $|z| \geqslant \mathrm{R}$) est une fraction rationnelle. (Commencer par prouver que f n'a qu'un nombre fini de pôles.)

(ii) Montrer qu'une fonction méromorphe tendant vers l'infini à l'infini est une fraction rationnelle.

Exercice VI.3.10. — Soit $(x_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathbf{C}^*$ tendant vers l'infini, et soit $(k_n)_{n\in\mathbf{N}}$ une suite d'éléments de $\mathbf{N}$.

(i) Montrer qu'il existe $a_n \in \mathbf{N}$ tel que, si $|z| < \frac{|x_n|}{2}$, alors

$$\left| \left((1 - \frac{z}{x_n}) e^{\frac{z}{x_n} + \frac{z^2}{2x_n^2} + \cdots + \frac{z^{a_n}}{a_n x_n^{a_n}}} \right)^{k_n} - 1 \right| \leqslant 2^{-n}.$$

(ii) Construire une fonction holomorphe sur $\mathbf{C}$ dont les zéros sont les x_n avec multiplicité k_n.

(iii) Montrer que toute fonction méromorphe sur $\mathbf{C}$ est quotient de deux fonctions holomorphes sur $\mathbf{C}$.

(iv) Montrer, en adaptant la méthode, que toute fonction méromorphe sur $\mathrm{D}(0, 1^-)$ est quotient de deux fonctions holomorphes sur $\mathrm{D}(0, 1^-)$.

Exercice VI.3.11. — Soient $\mathrm{R} > 0$ et f holomorphe sur $\mathrm{D}(z_0, \mathrm{R}^-) - \{z_0\}$. Montrer que :

(i) f est holomorphe en z_0, si et seulement si f est bornée dans $\mathrm{D}(z_0, r) - \{z_0\}$, quel que soit $r \in]0, \mathrm{R}[$ (on pourra s'intéresser à $\frac{1}{2i\pi} \int_{\mathrm{C}(z_0,r)} (z - z_0)^{-1-n} f(z)\, dz$) ;

(ii) f est méromorphe non holomorphe en z_0 si et seulement si $|f(z)| \to +\infty$ quand $z \to z_0$;

(iii) f a une singularité essentielle en z_0 si et seulement si l'image de $\mathrm{D}(z_0, r^-) - \{z_0\}$ par f est dense [12] dans $\mathbf{C}$, quel que soit $r \in]0, \mathrm{R}[$.

Exercice VI.3.12. — (i) Soit $f : \mathbf{C} \to \mathbf{C}$ holomorphe. Montrer, en utilisant l'exercice précédent, que si f n'est pas un polynôme, alors $f(\mathbf{C} - \mathrm{D}(0, n))$ est un ouvert dense de $\mathbf{C}$, quel que soit $n \in \mathbf{N}$. En déduire que f n'est pas injective.

(ii) Montrer que si $f : \mathbf{C} \to \mathbf{C}$ est holomorphe bijective, alors il existe $a \in \mathbf{C}^*$ et $b \in \mathbf{C}$ tels que $f(z) = az + b$, quel que soit $z \in \mathbf{C}$.

---

11. On peut montrer que l'on peut écrire $f = \frac{g}{h}$, avec g et h holomorphes sur Ω tout entier, mais c'est loin d'être évident si Ω est un ouvert quelconque.

12. Le « grand théorème de Picard » affirme qu'en fait l'image de $\mathrm{D}(z_0, r^-) - \{z_0\}$ par f contient $\mathbf{C}$ à au plus un point près (l'exemple de $e^{1/z}$ montre que ce résultat est optimum). La démonstration repose sur des techniques un peu plus sophistiquées que celles introduites dans ce cours.

3. La formule des résidus

Théorème VI.3.13. — *Soient Ω un ouvert de $\mathbf{C}$, F un ensemble fini de points de Ω, f une fonction holomorphe sur $\Omega - \mathrm{F}$, et γ un lacet de Ω, contractile dans Ω, et ne rencontrant pas F. Alors*

$$\int_\gamma f(z)\,dz = 2i\pi \sum_{a\in \mathrm{F}} \mathrm{I}(\gamma, a)\mathrm{Res}(f, a).$$

Démonstration. — Si $a \in \mathrm{F}$, et si $r_a > 0$ est tel que $\mathrm{D}(a, r_a^-)$ est inclus dans Ω et ne contient aucun autre point de F, alors il existe une suite $(c_{a,n})_{n\in\mathbf{Z}}$ d'éléments de $\mathbf{C}$, telle que $f(z) = \sum_{n\in\mathbf{Z}} c_{a,n}(z-a)^n$, si $z \in \mathrm{D}(a, r_a^-)$. De plus, la série $\sum_{n\leqslant -2} c_{a,n}(z-a)^n$ définit une fonction holomorphe g_a dans $\mathbf{C} - \{a\}$, et g_a admet $\mathrm{G}_a(z) = \sum_{n\leqslant -2} c_{a,n}\frac{(z-a)^{n+1}}{n+1}$ comme primitive sur $\mathbf{C} - \{a\}$. Soit alors $h = f - \sum_{a\in\mathrm{F}}(g_a + \frac{c_{a,-1}}{z-a})$. Par construction, h est holomorphe sur $\Omega - \mathrm{F}$, et a une singularité fictive en tous les points de F ; elle se prolonge donc, par continuité, en une fonction holomorphe sur Ω tout entier. On a alors

- $\int_\gamma f(z)\,dz = \int_\gamma h(z)\,dz + \sum_{a\in\mathrm{F}} \int_\gamma g_a(z)\,dz + \sum_{a\in\mathrm{F}} c_{a,-1}\int_\gamma \frac{dz}{z-a}$;
- $\int_\gamma h(z)\,dz = 0$ puisque h est holomorphe dans Ω et γ est contractile dans Ω ;
- $\int_\gamma g_a(z)\,dz = 0$, si $a \in \mathrm{F}$, puisque g_a a une primitive sur $\Omega - \{a\}$ qui contient γ ;
- $c_{a,-1} = \mathrm{Res}(f, a)$ et $\int_\gamma \frac{dz}{z-a} = 2i\pi\,\mathrm{I}(\gamma, a)$, par définition.

Ceci permet de conclure.

La formule des résidus permet de localiser les zéros d'une fonction holomorphe.

Corollaire VI.3.14. — *Soit $\Omega \subset \mathbf{C}$ un ouvert, et soient $z_0 \in \Omega$ et $r > 0$ tels que $\mathrm{D}(z_0, r) \subset \Omega$. Soit f holomorphe sur Ω. Si $\mathrm{C}(z_0, r)$ ne contient aucun zéro de f, alors le nombre de zéros de f dans $\mathrm{D}(z_0, r^-)$, comptés avec multiplicité, est égal à $\frac{1}{2i\pi}\int_{\mathrm{C}(z_0,r)} \frac{f'(z)}{f(z)}\,dz$.*

Démonstration. — On sait (cf. (v) de l'ex. VI.3.5) que $\frac{f'(z)}{f(z)}$ est méromorphe sur Ω, avec des pôles simples aux zéros de f, le résidu en chacun de ces pôles étant l'ordre du zéro de f. La formule des résidus permet de conclure.

4. Exercices

Exercice VI.3.15. — Soit f définie sur $\mathbf{R}$ par $f(t) = e^{-\pi t^2}$. Rappel : $\int_{\mathbf{R}} e^{-\pi t^2}\,dt = 1$.

(i) Montrer que f se prolonge analytiquement en une fonction (encore notée f) holomorphe sur $\mathbf{C}$.

(ii) Si $a \in \mathbf{R}$ et $\mathrm{R} \in \mathbf{R}_+$, soit $\gamma_{a,\mathrm{R}}$ le lacet composé des segments $[-\mathrm{R}, \mathrm{R}]$, $[\mathrm{R}, \mathrm{R}+ai]$, $[\mathrm{R}+ai, -\mathrm{R}+ai]$ et $[-\mathrm{R}+ai, -\mathrm{R}]$. Que vaut $\int_{\gamma_{a,\mathrm{R}}} f(z)\,dz$?

(iii) En déduire, en faisant tendre R vers $+\infty$, que $\hat{f}(a) = e^{-\pi a^2}$.

Exercice VI.3.16. — Calculer les intégrales suivantes par la méthode des résidus :

(a) $\int_{\mathbf{R}} \frac{dx}{(x^2+1)(x^2+4)(x^2+9)}$ et $\int_{\mathbf{R}} \frac{dx}{(x+i)(x-i)(x-2i)\cdots(x-ni)}$. (On prendra un lacet γ formé du segment $[-\mathrm{R}, \mathrm{R}]$ et d'un demi-cercle convenable.)

(b) $\lim_{\mathrm{R}\to+\infty} \int_{-\mathrm{R}}^{\mathrm{R}} \frac{x^3}{(x^2+1)(x^2+x+1)}dx$.

(c) $\int_0^{+\infty} \frac{x^a}{x^b+1}\,dx$, avec $a, b \in \mathbf{N}$ et $b \geqslant a+2$. (On prendra un lacet γ formé du segment $[0, \mathrm{R}]$, d'un arc de cercle convenable, et d'un segment $[\mathrm{R}e^{i\alpha}, 0]$, avec α bien choisi.)

Exercice VI.3.17. — (transformée de Fourier de fonctions rationnelles)

(i) Calculer $\int_{\mathbf{R}} \frac{e^{-2i\pi\, t\xi}}{t^2+1}\,dt$ et $\int_{\mathbf{R}} \frac{e^{-2i\pi\, t\xi}}{(t+i)^2}\,dt$ par la méthode des résidus. (On prendra un lacet γ formé du segment $[-\mathrm{R}, \mathrm{R}]$ et d'un demi-cercle convenable [13])

(ii) Calculer de même $\lim_{\mathrm{R}\to+\infty} \int_{-\mathrm{R}}^{\mathrm{R}} \frac{t\, e^{-2i\pi\, t\xi}}{t^2+t+1}\,dt$.

Exercice VI.3.18. — Soit $\gamma_{\varepsilon,\mathrm{R}}$ le lacet composé du segment $[\varepsilon, \mathrm{R}]$, du demi-cercle $\mathrm{C}^+(0, \mathrm{R}) : [0, \pi] \to \mathbf{C}$, donné par $t \mapsto \mathrm{R}e^{it}$, du segment $[-\mathrm{R}, -\varepsilon]$, et demi-cercle $\mathrm{C}^+(0, \varepsilon)^{\mathrm{opp}}$, donné par $t \mapsto \varepsilon e^{i(\pi-t)}$. (Faire un dessin.)

(i) Calculer $\int_{\gamma_{\varepsilon,\mathrm{R}}} \frac{e^{iz}}{z}\,dz$ via la formule des résidus.

(ii) Montrer que $\int_{\mathrm{C}^+(0,\mathrm{R})} \frac{e^{iz}}{z}\,dz \to 0$ quand $\mathrm{R} \to +\infty$.

(iii) Calculer la limite de $\int_{\mathrm{C}^+(0,\varepsilon)^{\mathrm{opp}}} \frac{e^{iz}}{z}\,dz$ quand $\varepsilon \to 0$.

(iv) En déduire que $\int_0^{+\infty} \frac{\sin x}{x}\,dx = \frac{\pi}{2}$.

Exercice VI.3.19. — Nous nous proposons de démontrer que $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$, pour tout $s \notin \mathbf{Z}$ (formule des compléments [14]), où Γ est la fonction holomorphe sur $\mathbf{C} - (-\mathbf{N})$ de l'exercice V.5.9.

(i) Soit s dans la bande $-1 < \mathrm{Re}(s) < 0$. (On peut adapter ce qui suit pour calculer les intégrales du type $\int_0^{+\infty} f(t)t^s\,dt$, où f est une fraction rationnelle). Si $r > 0$, on note $\mathrm{C}^+(0, r)$ le quart de cercle $\theta \mapsto re^{i\theta}$, pour $\theta \in [0, \frac{\pi}{2}]$ et $\mathrm{C}^-(0, r)$ les 3 quarts de cercle $\theta \mapsto re^{i\theta}$, pour $\theta \in [\frac{\pi}{2}, 2\pi]$. Si $0 < \varepsilon < \mathrm{R}$, soit $\gamma^+_{\varepsilon,\mathrm{R}}$ le lacet obtenu en composant $\mathrm{C}^+(0, \mathrm{R})$, $[i\mathrm{R}, i\varepsilon]$, $\mathrm{C}^+(0, \varepsilon)^{\mathrm{opp}}$ et $[\varepsilon, \mathrm{R}]$ (faire un dessin !), et soit $\gamma^-_{\varepsilon,\mathrm{R}}$ le lacet obtenu en composant $[i\varepsilon, i\mathrm{R}]$, $\mathrm{C}^-(0, \mathrm{R})$, $[\mathrm{R}, \varepsilon]$ et $\mathrm{C}^-(0, \varepsilon)^{\mathrm{opp}}$.

(a) Calculer $\int_{\gamma^+_{\varepsilon,\mathrm{R}}} \frac{(-z)^s}{z+1}\,dz$ et $\int_{\gamma^-_{\varepsilon,\mathrm{R}}} \frac{(-z)^s}{z+1}\,dz$ en utilisant la formule des résidus, avec $\log(-z) \in \mathbf{R}$, si $z \in \mathbf{R}^*_-$. (Attention à la détermination du logarithme !).

(b) Montrer que les intégrales sur les portions de cercle tendent vers 0 quand $\varepsilon \to 0$ et $\mathrm{R} \to +\infty$.

(c) En déduire la valeur de $\int_0^{+\infty} \frac{y^s}{y+1}\,dy$, si $-1 < \mathrm{Re}(s) < 0$.

(ii) Soit $\mathrm{B}(s,t) = \int_0^1 x^{s-1}(1-x)^{t-1}dx$. Montrer que $\mathrm{B}(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$, si $\mathrm{Re}(s) > 0$ et $\mathrm{Re}(t) > 0$. (On écrira $\Gamma(s+t)\mathrm{B}(s,t)$ comme une intégrale double.)

(iii) Démontrer la formule des compléments (on utilisera la formule $\mathrm{B}(s,t) = \int_0^{+\infty} \frac{y^{s-1}}{(1+y)^{s+t}} dy$ obtenue en faisant le changement de variable $y = \frac{x}{x-1}$).

Exercice VI.3.20. — Calculer $\int_0^{+\infty} \frac{\log t}{(t+1)(t+2)}\,dt$ par la méthode des résidus. (On intègrera $\frac{(\log z)^2}{(z+1)(z+2)}\,dz$ sur les contours de l'ex. VI.3.19.)

Exercice VI.3.21. — Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ unitaire de degré n. Calculer

$$\lim_{\mathrm{R}\to+\infty} \frac{1}{2i\pi} \int_{\mathrm{C}(0,\mathrm{R})} \frac{\mathrm{P}'(z)}{\mathrm{P}(z)}\,dz.$$

En déduire que $\mathbf{C}$ est algébriquement clos.

Exercice VI.3.22. — Soit Ω un ouvert connexe de $\mathbf{C}$, Soit f une fonction holomorphe non identiquement nulle sur Ω, et soit f_n une suite de fonctions holomorphes tendant vers f uniformément sur tout compact de Ω.

13. Une manière de voir que l'on a pris le bon demi-cercle est de vérifier que ce qu'on obtient tend vers 0 quand $|\xi| \to +\infty$; il faut aussi faire attention à l'indice du lacet par rapport aux pôles...

14. D'autres démonstrations se trouvent dans les ex. VII.2.2 et H.1.11.

(i) Soient $z_0 \in \Omega$ et $r > 0$ tels que $\mathrm{D}(z_0, r) \subset \Omega$. On suppose que $\mathrm{C}(z_0, r)$ ne contient aucun zéro de f. Montrer qu'il existe $\mathrm{N}(z_0, r)$ tel que, si $n \geqslant \mathrm{N}(z_0, r)$, alors f et f_n ont le même nombre de zéros, comptés avec multiplicité, dans $\mathrm{D}(z_0, r^-)$.

(ii) Montrer que, si f_n est injective sur Ω, pour tout n assez grand, il en est de même de f.

Exercice VI.3.23. — (Théorème de Rouché et applications).

Soient $\mathrm{R} > 0$, $\mathrm{D} = \mathrm{D}(0, \mathrm{R})$ et $\mathrm{C} = \partial\mathrm{D} = \mathrm{C}(0, \mathrm{R})$. Soient Ω un ouvert contenant D, f holomorphe sur Ω, ne s'annulant pas sur C, et g holomorphe sur Ω, telle que $|f(z) - g(z)| < |f(z)|$, si $z \in \mathrm{C}$.

(i) Montrer qu'il existe $\Omega' \subset \Omega$ ouvert contenant C et h holomorphe sur Ω' tels que $\frac{g}{f} = e^h$ sur Ω'. Que vaut h' ?

(ii) Montrer que f et g ont le même nombre de zéros (comptés avec multiplicité) dans D (théorème de Rouché). Le résultat n'est-il valable que pour un disque ?

(iii) Soit G holomorphe sur Ω telle que $|\mathrm{G}(z)| < \mathrm{R}$, si $z \in \mathrm{C}$. Montrer que $\mathrm{G}(\mathrm{D}) \subset \mathrm{D}$ et que G a un unique point fixe dans D.

(iv) Montrer que toutes les solutions de $z \sin z = 1$ sont réelles.

Exercice VI.3.24. — Soit Γ la fonction méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples en les entiers négatifs, définie par $\Gamma(z) = \int_0^{+\infty} e^{-t} t^z \, \frac{dt}{t}$, si $\mathrm{Re}(z) > 0$. On rappelle (cf. ex. V.5.9) que l'on a $\Gamma(z) = \frac{\Gamma(z+n+1)}{z(z+1)\cdots(z+n)}$, quel que soit $n \in \mathbf{N}$.

(i) Montrer que $\lim_{z \to -n}(z+n)\Gamma(z) = \frac{(-1)^n}{n!}$.

(ii) Montrer que, si $x > 0$, et si $c \notin -\mathbf{N}$, alors $\mathrm{I}_c(x) = \int_{c-i\infty}^{c+i\infty} x^{-z}\Gamma(z)\, dz$ converge.

(iii) Si $n \in \mathbf{N}$, calculer $\mathrm{I}_1(x) - \mathrm{I}_{\frac{1}{2}-n}(x)$ par la méthode des résidus.

(iv) Montrer que $\mathrm{I}_{\frac{1}{2}-n}(x) \to 0$. En déduire que $\frac{1}{2i\pi}\int_{1-i\infty}^{1+i\infty} x^{-z}\Gamma(z)\, dz = e^{-x}$.

(v) Retrouver le résultat en utilisant la transformée de Fourier.

Exercice VI.3.25. — Si $\mathrm{N} \in \mathbf{N}$, soit C_N le carré de sommets $(2\mathrm{N}+1)\pi(\pm 1 \pm i)$ parcouru dans le sens direct, et soit $\mathrm{I}_\mathrm{N} = \int_{\mathrm{C}_\mathrm{N}} \frac{dz}{z^2(e^z-1)}$.

(i) Calculer I_N en utilisant la formule des résidus.

(ii) Montrer que $\mathrm{I}_\mathrm{N} \to 0$ quand $\mathrm{N} \to +\infty$.

(iii) En déduire la formule $\zeta(2) = \frac{\pi^2}{6}$.

(iv) Soient B_n, pour $n \in \mathbf{N}$, définis par $\frac{z}{e^z-1} = \sum_{n=0}^{+\infty} \mathrm{B}_n \frac{z^n}{n!}$. Adapter ce qui précède pour calculer $\zeta(2k)$, pour $k \in \mathbf{N} - \{0\}$, en fonction des B_n. En déduire que $\pi^{-2k}\zeta(2k) \in \mathbf{Q}$.

Exercice VI.3.26. — Calculer l'intégrale de $\frac{\pi \mathrm{cotg}\, \pi z}{(z^2+1)^2}$ sur le carré de sommets $(\mathrm{N}+\frac{1}{2})(\pm 1 \pm i)$. En déduire la valeur de $\sum_{n \in \mathbf{Z}} \frac{1}{(n^2+1)^2}$.

Exercice VI.3.27. — (transformée de Fourier de $\frac{1}{\mathrm{ch}\, \pi t}$)

Calculer $\int_\mathbf{R} e^{2i\pi\, t\xi} \frac{e^{\pi t}}{e^{2\pi t}+1}\, dt$ de deux manières : d'une part en intégrant $e^{2i\pi\, z\xi} \frac{e^{\pi z}}{e^{2\pi z}+1}\, dz$ sur un rectangle convenable, en faisant tendre les sommets vers l'infini, d'autre part en écrivant $\frac{e^{\pi t}}{e^{2\pi t}+1}$ comme une série en $e^{\pi t}$ ou $e^{-\pi t}$ suivant que t est négatif ou positif. Comparer avec l'ex. V.5.3.

Exercice VI.3.28. — (intégrale de la gaussienne et loi de réciprocité quadratique)

Cet exercice fournit une démonstration de la formule $\int_\mathbf{R} e^{-\pi t^2}\, dt = 1$ par la méthode des résidus, et une démonstration de la loi de réciprocité quadratique.

(i) On note I l'intégrale $\int_\mathbf{R} e^{-\pi t^2}\, dt$ et, si $a \in \mathbf{N} - \{0\}$, on pose $\mathrm{G}(a) = \sum_{k \in \mathbf{Z}/a\mathbf{Z}} e^{2i\pi \frac{k^2}{a}}$.

(a) Montrer que $z \mapsto \mathrm{F}(z) = \int_\mathbf{R} e^{-\pi t^2} e^{-2i\pi\, tz}$ est holomorphe sur $\mathbf{C}$.

(b) Calculer $\mathrm{F}(iy)$, si $y \in \mathbf{R}$; en déduire que $\mathrm{F}(z) = \mathrm{I}\, e^{-\pi z^2}$, pour tout $z \in \mathbf{C}$.

(c) Soit $\Phi_a(z) = \sum_{k=0}^{2a-1} e^{-2\pi a z^2} e^{2\pi\, k\omega z}$, où $\omega = \frac{1+i}{\sqrt{2}}$. Montrer que $\int_{\mathbf{R}} \Phi_a(t)\, dt = \frac{\mathrm{I}}{\sqrt{8a}}\mathrm{G}(4a)$. (On commencera par montrer que $\int_{\mathbf{R}} e^{-2\pi a t^2} e^{2\pi k\omega t}\, dt = \frac{\mathrm{I}}{\sqrt{2a}} e^{2i\pi \frac{k^2}{4a}}$.)

(ii) Si $a \in \mathbf{N} - \{0\}$, soit $\Psi_a(z) = \frac{e^{-2\pi a z^2}}{e^{2i\pi \frac{z}{\omega}} - 1}$.

(a) Vérifier que $\Psi_a(z-\omega) - \Psi_a(z) = \Phi_a(z)$.

(b) Calculer $\int_{\mathbf{R}} \Psi_a(t - \frac{\omega}{2})\, dt - \int_{\mathbf{R}} \Psi_a(t + \frac{\omega}{2})\, dt$ par la méthode des résidus.

(c) En déduire que $\frac{\mathrm{I}}{\sqrt{8a}}\mathrm{G}(4a) = \omega$, puis que $\mathrm{I} = 1$.

(iii) Si p est un nombre premier, et si $(n,p) = 1$, on définit le symbole de Legendre $\left(\frac{n}{p}\right)$ par $\left(\frac{n}{p}\right) = 1$ ou -1, suivant que n est ou n'est pas un carré dans $\mathbf{F}_p$. On pose aussi $\mathrm{G}_n(p) = \sum_{k\in\mathbf{F}_p} e^{2i\pi \frac{nk^2}{p}}$. On rappelle que, si a et b sont premiers entre eux, alors $(x,y) \mapsto bx+ay$ induit une bijection $(\mathbf{Z}/a\mathbf{Z})\times(\mathbf{Z}/b\mathbf{Z}) \cong \mathbf{Z}/ab\mathbf{Z}$.

(a) Relier $\mathrm{G}(4a)$ et $\mathrm{G}(a)$ si a est impair ; en déduire que $\mathrm{G}(a) = \sqrt{a}$, si $a \equiv 1 \bmod 4$ et $\mathrm{G}(a) = i\sqrt{a}$, si $a \equiv 3 \bmod 4$ (formule due à Gauss).

(b) Montrer que $\sum_{m\in\mathbf{F}_p} e^{2i\pi \frac{m}{p}} = 0$; en déduire que $\mathrm{G}_n(p) = \left(\frac{n}{p}\right)\mathrm{G}(p)$, si $(n,p) = 1$.

(c) Soient $p \neq q$ deux nombres premiers impairs. Montrer que $\mathrm{G}(pq) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\mathrm{G}(p)\mathrm{G}(q)$; en déduire la loi de réciprocité quadratique $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.

CHAPITRE VII

SÉRIES DE DIRICHLET

Une série de Dirichlet générale est une expression de la forme $\sum_{n=1}^{+\infty} a_n e^{-\lambda_n s}$, où les a_n sont des nombres complexes, et les λ_n sont des nombres complexes dont la partie réelle tend vers $+\infty$. (Si $\lambda_n = n-1$ pour tout n, on retombe, modulo le changement de variable $e^{-s} = z$, sur le cas des séries entières (avec une indexation bizarre), ce qui permet de voir les séries de Dirichlet générales comme une généralisation des séries entières.) Dans ce chapitre, nous ne nous intéresserons qu'au cas où $\lambda_n = \log n$, pour tout n, qui est le cas originellement considéré par Dirichlet, mais le cas général intervient naturellement quand, par exemple, on essaie de définir le déterminant d'un opérateur en dimension infinie, ce qui a de multiples applications en physique [1] et en mathématiques. Comme illustration de ce procédé « de zêta-régularisation », mentionnons la formule

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots = \sqrt{2\pi},$$

équivalente à $-\sum_{n=1}^{+\infty} \log n = -\frac{1}{2}\log 2\pi$, dans laquelle le membre de gauche s'interprète comme la dérivée en 0 de la fonction ζ définie par $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$, si $\mathrm{Re}(s) > 1$, et prolongée analytiquement [2] à $\mathbf{C} - \{1\}$.

VII.1. Séries de Dirichlet

1. Abscisse de convergence absolue

On appelle *série de Dirichlet* une série de la forme $\mathrm{L}(\mathbf{a}, s) = \sum_{n=1}^{+\infty} a_n\, n^{-s}$, où $s \in \mathbf{C}$ et $\mathbf{a} = (a_n)_{n\geqslant 1}$ est une suite de nombres complexes (et $n^{-s} = \exp(-s\log n)$, où $\log n \in \mathbf{R}_+$). Une série de Dirichlet peut ne converger pour aucune valeur de s, mais si elle converge pour s_0, on a en particulier, $a_n n^{-s_0} \to 0$, et donc $|a_n| = o(n^{\mathrm{Re}(s_0)})$. Réciproquement,

1. Les fréquences d'une membrane vibrante sont les valeurs propres du laplacien sur l'ouvert de $\mathbf{C}$ représentant cette membrane. La *fonction zêta du laplacien* $\zeta_\Delta(s) = \sum \lambda^{-s}$, où la somme porte sur les valeurs propres non nulles, encode des relations entre ces fréquences et la géométrie de la surface. Le déterminant du laplacien est $\exp(-\zeta'_\Delta(0))$; il intervient par exemple dans des questions de renormalisation.

2. L'existence de ce prolongement analytique fait l'objet du th. VII.3.4, et une démonstration de la formule $\zeta'(0) = -\frac{1}{2}\log 2\pi$ est proposée dans l'ex. VII.3.9.

si $|a_n| = \mathrm{O}(n^\alpha)$, pour un certain $\alpha \in \mathbf{R}$, alors $\sum_{n=1}^{+\infty} a_n\, n^{-s}$ converge normalement sur tout demi-plan de la forme $\mathrm{Re}(s) > \alpha + 1 + \delta$, avec $\delta > 0$; elle définit donc une fonction holomorphe sur le demi-plan $\mathrm{Re}(s) > \alpha+1$. De même, si $\sum_{n=1}^{+\infty} a_n\, n^{-s}$ converge absolument pour $s = s_0$, alors elle converge normalement sur le demi-plan $\mathrm{Re}(s - s_0) \geqslant 0$, puisque $|a_n\, n^{-s}| \leqslant |a_n\, n^{-s_0}|$ sur ce demi-plan ; elle définit donc une fonction holomorphe sur le demi-plan ouvert $\mathrm{Re}(s - s_0) > 0$, qui se prolonge par continuité au demi-plan fermé $\mathrm{Re}(s - s_0) \geqslant 0$.

La discussion précédente amène naturellement à définir les éléments suivants de $\overline{\mathbf{R}}$:

- $\sigma_{\mathrm{conv}} = \inf\{\mathrm{Re}(s),\ \mathrm{L}(\mathbf{a}, s) \text{ converge}\}$ *abscisse de convergence* ;
- $\sigma_{\mathrm{abs}} = \inf\{\mathrm{Re}(s),\ \mathrm{L}(\mathbf{a}, s) \text{ converge absolument}\}$ *abscisse de convergence absolue* ;
- $\sigma_{\mathrm{hol}} = \inf\{\sigma \in \mathbf{R},\ \mathrm{L}(\mathbf{a}, s) \text{ admet un prolongement holomorphe sur } \mathrm{Re}(s) > \sigma\}$.
- $\tau = \inf\{\alpha \in \mathbf{R},\ a_n = \mathrm{O}(n^\alpha)\}$.

Le nombre τ n'a pas de signification particulière, mais des quantités précédentes, c'est la plus facile à calculer ; de plus la discussion ci-dessus nous fournit les encadrements :

$$\tau \leqslant \sigma_{\mathrm{conv}} \leqslant \sigma_{\mathrm{abs}} \leqslant \tau + 1.$$

Par ailleurs, contrairement au cas des séries entières (cf. (i) de la rem. V.4.9), on n'a pas forcément $\sigma_{\mathrm{hol}} = \sigma_{\mathrm{abs}}$, comme le montre l'exemple des fonctions L de Dirichlet (th. VII.4.4). Pour beaucoup de séries de Dirichlet issues de la théorie des nombres ou de la physique théorique, on conjecture que $\sigma_{\mathrm{hol}} = -\infty$ (i.e. il existe un prolongement analytique à tout le plan complexe), mais ceci est un petit miracle indiquant des symétries cachées qui restent fort mystérieuses.

On suppose dans tout ce qui suit que les séries de Dirichlet que l'on considère convergent quelque part (i.e. $\sigma_{\mathrm{abs}} \neq +\infty$), le cas contraire n'ayant qu'un intérêt limité... On peut alors retrouver les a_n à partir de la fonction $\mathrm{L}(\mathbf{a}, s)$ (en effet, $a_1 = \lim_{s\to+\infty} \mathrm{L}(\mathbf{a}, s)$, $a_2 = \lim_{s\to+\infty} 2^s(\mathrm{L}(\mathbf{a}, s) - a_1)$, etc.).

On remarquera que le produit de deux séries de Dirichlet $\mathrm{L}(\mathbf{a}, s)\mathrm{L}(\mathbf{b}, s)$ est encore une série de Dirichlet $\mathrm{L}(\mathbf{c}, s) = \sum_{n\geqslant 1} \frac{c_n}{n^s}$, où $c_n = \sum_{d|n} a_d b_{n/d}$. Cette formule, qui fait intervenir la factorisation des entiers, est largement responsable de l'intérêt des séries de Dirichlet pour des questions d'arithmétique.

Théorème VII.1.1. — (Landau) *Soit* $\mathrm{L}(\mathbf{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ *une série de Dirichlet à coefficients positifs* (i.e. $a_n \in \mathbf{R}_+$, quel que soit $n \geqslant 1$). *Alors* σ_{abs} *n'a aucun voisinage dans* $\mathbf{C}$ *sur lequel* $\mathrm{L}(\mathbf{a}, s)$ *admet un prolongement analytique* [3].

Corollaire VII.1.2. — *Si* $\mathrm{L}(\mathbf{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ *est une série de Dirichlet à coefficients positifs, alors* $\sigma_{\mathrm{hol}} = \sigma_{\mathrm{abs}}$.

3. Il arrive que $\mathrm{L}(\mathbf{a}, s)$ admette un prolongement méromorphe comme le montre le cas de la fonction zêta de Riemann (cf. th. VII.3.4), mais alors σ_{abs} est un pôle de ce prolongement.

Démonstration. — Le corollaire est immédiat. Passons à la démontration du théorème. Posons $\sigma = \sigma_{\text{abs}}$, et supposons, par l'absurde, qu'il existe $\varepsilon > 0$ tel que $\mathrm{L}(\mathbf{a}, s)$ admette un prolongement analytique au disque $\mathrm{D}(\sigma, 3\varepsilon^-)$. Alors $\mathrm{L}(\mathbf{a}, s)$ est holomorphe sur l'ouvert Ω réunion de $\mathrm{D}(\sigma, 3\varepsilon^-)$ et du demi-plan $\mathrm{Re}(s) > \sigma$. Comme Ω contient $\mathrm{D}(\sigma + \varepsilon, 3\varepsilon^-)$, $\mathrm{L}(\mathbf{a}, s)$ est somme de sa série de Taylor en $\sigma + \varepsilon$ sur ce disque, et en particulier, on a $\mathrm{L}(\mathbf{a}, \sigma - \varepsilon) = \sum_{k=0}^{+\infty} \frac{\mathrm{L}^{(k)}(\mathbf{a}, \sigma+\varepsilon)}{k!}(-2\varepsilon)^k$. Par ailleurs, comme $\sigma + \varepsilon$ est dans le demi-plan de convergence de $\mathrm{L}(\mathbf{a}, s)$, on peut, d'après le th. V.5.1, calculer $\mathrm{L}^{(k)}(\mathbf{a}, \sigma + \varepsilon)$ en dérivant terme à terme la série de Dirichlet. On obtient donc

$$\mathrm{L}(\mathbf{a}, \sigma - \varepsilon) = \sum_{k=0}^{+\infty} \mathrm{L}^{(k)}(\mathbf{a}, \sigma + \varepsilon)\frac{(-2\varepsilon)^k}{k!} = \sum_{k=0}^{+\infty} \Big(\sum_{n=1}^{+\infty} \frac{a_n(-\log n)^k}{n^{\sigma+\varepsilon}} \Big) \frac{(-2\varepsilon)^k}{k!}.$$

En faisant rentrer le $\frac{(-2\varepsilon)^k}{k!}$ à l'intérieur de la parenthèse, on obtient une série double *à termes positifs*, ce qui permet d'échanger l'ordre des sommations, et d'obtenir :

$$\mathrm{L}(\mathbf{a}, \sigma - \varepsilon) = \sum_{n=1}^{+\infty} \frac{a_n}{n^{\sigma+\varepsilon}} \Big(\sum_{k=0}^{+\infty} \frac{(2\varepsilon \log n)^k}{k!} \Big) = \sum_{n=1}^{+\infty} \frac{a_n}{n^{\sigma+\varepsilon}} n^{2\varepsilon} = \sum_{n=1}^{+\infty} \frac{a_n}{n^{\sigma-\varepsilon}}.$$

On en déduit que $\mathrm{L}(\mathbf{a}, s)$ converge en $\sigma - \varepsilon$, ce qui est contraire à la définition de σ. Ceci permet de conclure.

2. Demi-plan de convergence d'une série de Dirichlet

Contrairement au cas des séries entières, on a, en général [4], $\sigma_{\text{conv}} \neq \sigma_{\text{abs}}$, et la détermination de σ_{conv} peut cacher des difficultés redoutables... D'autre part, d'après le cor. VII.1.6 ci-dessous, on a $\sigma_{\text{hol}} \leqslant \sigma_{\text{conv}}$, et le cas des fonctions L de Dirichlet (th. VII.4.4) montre que, contrairement au cas des séries entières, on n'a pas toujours égalité. La quantité σ_{hol} est très souvent extrêmement difficile à calculer. Une grande partie du programme de Langlands (cf. annexe G) est destinée à prouver que pour beaucoup de séries de Dirichlet issues de la théorie des nombres, on a $\sigma_{\text{hol}} = -\infty$.

L'étude de la convergence des séries de Dirichlet repose sur le lemme suivant.

4. Supposons par exemple que $a_n \in \{\pm 1\}$, pour tout $n \geqslant 1$. On a alors $\sigma_{\text{abs}} = 1$. Pour étudier σ_{conv}, on peut utiliser la formule sommatoire d'Abel : on pose $\mathrm{A}_n = \sum_{k=1}^{n} a_k$ de telle sorte que

$$\sum_{n=1}^{\mathrm{N}} \frac{a_n}{n^s} = \frac{\mathrm{A_N}}{(\mathrm{N}+1)^s} + \sum_{n=1}^{\mathrm{N}} \mathrm{A}_n(n^{-s} - (n+1)^{-s}) = \frac{\mathrm{A_N}}{(\mathrm{N}+1)^s} + \sum_{n=1}^{\mathrm{N}} \frac{\mathrm{A}_n}{n^{s+1}}\big(n\big(1 - \big(1 + \frac{1}{n}\big)^{-s}\big)\big).$$

On en déduit le fait que, si $\mathrm{A}_n = \mathrm{O}(n^\alpha)$, avec $\alpha < 1$, alors $\sigma_{\text{conv}} \leqslant \alpha$. Or Hausdorff (1913) a démontré que, presque sûrement (en considérant les a_n comme des variables aléatoires indépendantes à valeurs dans $\{\pm 1\}$ muni de l'équiprobabilité), $\mathrm{A}_n = \mathrm{O}(n^{1/2+\varepsilon})$, quel que soit $\varepsilon > 0$, et donc $\sigma_{\text{conv}} \leqslant 1/2$ presque sûrement (et $1/2$ est sûrement différent de 1).

Lemme VII.1.3. — *Soient $\alpha, \beta \in \mathbf{R}$, avec $0 < \alpha < \beta$. Soit $z = x + iy$, avec $x, y \in \mathbf{R}$, et $x > 0$. Alors*

$$|e^{-\alpha z} - e^{-\beta z}| \leqslant \big|\frac{z}{x}\big|(e^{-\alpha x} - e^{-\beta x}).$$

Démonstration. — On a $e^{-\alpha z} - e^{-\beta z} = z\int_\alpha^\beta e^{-tz}\,dt$, et donc

$$|e^{-\alpha z} - e^{-\beta z}| \leqslant |z|\int_\alpha^\beta e^{-tx}\,dt = \big|\frac{z}{x}\big|(e^{-\alpha x} - e^{-\beta x}).$$

En appliquant ce lemme à $\alpha = \log n$, $\beta = \log(n+1)$ et $z = s - s_0$, on obtient :

Corollaire VII.1.4. — *Si $n \geqslant 1$, et si $\mathrm{Re}(s - s_0) > 0$, alors*

$$|n^{-(s-s_0)} - (n+1)^{-(s-s_0)}| \leqslant \frac{|s - s_0|}{\mathrm{Re}(s - s_0)}(n^{-\mathrm{Re}(s-s_0)} - (n+1)^{-\mathrm{Re}(s-s_0)}).$$

Théorème VII.1.5. — *Soient $\mathrm{L}(\mathbf{a}, s) = \sum_{n=1}^{+\infty} a_n\, n^{-s}$ une série de Dirichlet, et $s_0 \in \mathbf{C}$.*

(i) *Si la suite des sommes partielles $\mathrm{A}_n(s_0) = \sum_{k=1}^{n} a_k\, k^{-s_0}$ est bornée, alors $\mathrm{L}(\mathbf{a}, s)$ converge uniformément dans tout compact du demi-plan $\mathrm{Re}(s - s_0) > 0$.*

(ii) *Si la série $\sum_{n=1}^{+\infty} a_n\, n^{-s_0}$ converge, alors $\mathrm{L}(\mathbf{a}, s)$ converge uniformément dans tout secteur angulaire $|\arg(s - s_0)| \leqslant \alpha < \frac{\pi}{2}$ du demi-plan $\mathrm{Re}(s - s_0) \geqslant 0$.*

Démonstration. — La démonstration est la même dans les deux cas et repose sur *la formule sommatoire d'Abel*. Si $p, q \in \mathbf{N}$ vérifient $p \leqslant q$, soit

$$\mathrm{M}_{p,q} = \sup_{p \leqslant n \leqslant q} |\mathrm{B}_{n,p}|, \quad \text{avec } \mathrm{B}_{n,p} = \mathrm{A}_n(s_0) - \mathrm{A}_{p-1}(s_0)$$

(et $\mathrm{A}_0(s_0) = 0$, puisqu'une somme vide est nulle par convention). On a

$$\begin{aligned}\sum_{n=p}^{q} a_n\, n^{-s} =& \sum_{n=p}^{q} (\mathrm{B}_{n,p} - \mathrm{B}_{n-1,p}) n^{-(s-s_0)} \\ =& \mathrm{B}_{q,p} q^{-(s-s_0)} + \sum_{n=p}^{q-1} \mathrm{B}_{n,p}(n^{-(s-s_0)} - (n+1)^{-(s-s_0)}).\end{aligned}$$

Si $\mathrm{Re}(s - s_0) > 0$, en utilisant la majoration du cor. VII.1.4, l'inégalité $1 \leqslant \frac{|s-s_0|}{\mathrm{Re}(s-s_0)}$, et la définition de $\mathrm{M}_{p,q}$, on en déduit la majoration

$$\begin{aligned}\Big|\sum_{n=p}^{q} a_n\, n^{-s}\Big| \leqslant& \mathrm{M}_{p,q}\Big(q^{-\mathrm{Re}(s-s_0)} + \frac{|s - s_0|}{\mathrm{Re}(s - s_0)} \sum_{n=p}^{q-1} (n^{-\mathrm{Re}(s-s_0)} - (n+1)^{-\mathrm{Re}(s-s_0)})\Big) \\ \leqslant& \mathrm{M}_{p,q} \frac{|s - s_0|}{\mathrm{Re}(s - s_0)} p^{-\mathrm{Re}(s-s_0)}.\end{aligned}$$

Maintenant, si $|\mathrm{A}_n(s_0)| \leqslant \mathrm{M}$, quel que soit $n \in \mathbf{N}$, on a $\mathrm{M}_{p,q} \leqslant 2\mathrm{M}$ quels que soient $p \leqslant q$. Par ailleurs, si K est un compact du demi-plan $\mathrm{Re}(s - s_0) > 0$, alors il existe $a > 0$ et $b > 0$ tels que $|s - s_0| \leqslant a$ et $\mathrm{Re}(s - s_0) \geqslant b$, quel que soit $s \in \mathrm{K}$. On a donc

$\big|\sum_{n=p}^{q} a_n\, n^{-s}\big| \leqslant 2\mathrm{M}ab^{-1}p^{-b}$, si $s \in \mathrm{K}$, ce qui prouve que la série $\sum_{n\geqslant 1} a_n\, n^{-s}$ satisfait au critère de Cauchy uniforme sur K. On en déduit le (i).

Pour démontrer le (ii), il suffit de constater que l'hypothèse selon laquelle $\sum_{n\geqslant 1} a_n\, n^{-s_0}$ converge est équivalente à $\mathrm{M}_{p,q} \to 0$, quand $p \to +\infty$, d'après le critère de Cauchy. Comme $\frac{|s-s_0|}{\mathrm{Re}(s-s_0)}$ est majoré par $\mathrm{tg}\,\alpha$ sur le secteur angulaire $|\arg(s-s_0)| \leqslant \alpha < \frac{\pi}{2}$ du demi-plan $\mathrm{Re}(s-s_0) \geqslant 0$, et comme $p^{-\mathrm{Re}(s-s_0)} \leqslant 1$ sur le demi-plan, on en déduit que la série $\sum_{n\geqslant 1} a_n\, n^{-s}$ satisfait au critère de Cauchy uniforme sur le secteur angulaire, ce qui démontre le (ii).

Corollaire VII.1.6. — *Soient* $\mathrm{L}(\mathbf{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ *une série de Dirichlet, et* $\sigma_{\mathrm{conv}} \in \overline{\mathbf{R}}$ *l'abscisse de convergence de* $\mathrm{L}(\mathbf{a}, s)$. *Alors* $\mathrm{L}(\mathbf{a}, s)$ *converge en tout* s *du demi-plan* $\mathrm{Re}(s) > \sigma_{\mathrm{conv}}$ *et définit une fonction holomorphe sur ce demi-plan, et donc* $\sigma_{\mathrm{hol}} \leqslant \sigma_{\mathrm{conv}}$.

Démonstration. — Par définition de σ_{conv}, pour tout $\varepsilon > 0$, il existe $s_\varepsilon \in \mathbf{C}$, tel que $\mathrm{L}(\mathbf{a}, s_\varepsilon)$ soit convergente et $\mathrm{Re}(s_\varepsilon) \leqslant \sigma_{\mathrm{conv}} + \varepsilon$. D'après le th. VII.1.5, la série $\mathrm{L}(\mathbf{a}, s)$ converge pour tout s du demi-plan $\mathrm{Re}(s) > \sigma_{\mathrm{conv}} + \varepsilon$, car ce demi-plan est une réunion de secteurs angulaires de sommet s_ε, et comme ceci est vrai pour tout $\varepsilon > 0$, cela prouve que $\mathrm{L}(\mathbf{a}, s)$ converge en tout s du demi-plan $\mathrm{Re}(s) > \sigma_{\mathrm{conv}}$. L'holomorphie de $\mathrm{L}(\mathbf{a}, s)$ sur ce demi-plan résulte de ce qu'une fonction qui est limite uniforme sur tout compact de fonctions holomorphes est elle-même holomorphe (th. V.5.1).

VII.2. Séries de Dirichlet et transformée de Mellin

1. La fonction Γ dans le plan complexe

La fonction Γ d'Euler a été définie (cf. ex. IV.1.5) sur $\mathbf{R}_+^*$ par la formule $\Gamma(x) = \int_0^{+\infty} e^{-t} t^x \frac{dt}{t}$. Nous nous proposons de l'étendre en une fonction méromorphe sur $\mathbf{C}$ tout entier. On trouvera une autre approche dans l'ex. V.5.9 ; l'approche ci-dessous montre directement que Γ ne s'annule pas, ce qui peut aussi se déduire de la formule des compléments (ex. VI.3.19).

On rappelle que la *constante d'Euler* γ est la limite de $-\log n + \sum_{k=1}^{n} \frac{1}{k}$, quand $n \to +\infty$.

Théorème VII.2.1. — (i) *Le produit*

$$f(z) = z\, e^{\gamma z} \prod_{k=1}^{+\infty} \Big(\big(1 + \frac{z}{k}\big) e^{-z/k} \Big)$$

est uniformément convergent sur tout compact de $\mathbf{C}$, *et coïncide avec* $\frac{1}{\Gamma}$ *sur* $\mathbf{R}_+^*$.

(ii) *La* fonction Γ complexe *définie par* $\Gamma(z) = \frac{1}{f(z)}$ *est méromorphe sur* $\mathbf{C}$, *holomorphe en dehors de pôles simples aux entiers négatifs, de résidu* $\frac{(-1)^n}{n!}$ *en* $-n$, *si* $n \in \mathbf{N}$. *De plus, on a* $\Gamma(z+1) = z\Gamma(z)$, *quel que soit* $z \in \mathbf{C} - (-\mathbf{N})$.

Démonstration. — La fonction $h(z) = z^{-2}((1+z)e^{-z} - 1)$ est holomorphe sur $\mathbf{C}$, et donc est bornée sur tout compact. En particulier, il existe M tel que $|(1+z)e^{-z} - 1| \leqslant \mathrm{M}|z^2|$, si $|z| \leqslant 1$. Maintenant, si K est compact, il existe R(K) tel que $|z| \leqslant \mathrm{R(K)}$, quel que soit $z \in \mathrm{K}$, et on a $\big|\big(1+\frac{z}{k}\big)e^{-z/k} - 1\big| \leqslant \frac{\mathrm{M\,R(K)}^2}{k^2}$, si $k \geqslant \mathrm{R(K)}$ et $z \in \mathrm{K}$. On en déduit la convergence uniforme du produit sur K, et le th. V.5.4 montre que f est une fonction holomorphe sur $\mathbf{C}$ avec des zéros simples en 0 et les $-k$, pour $k \in \mathbf{N} - \{0\}$. En passant à l'inverse, cela montre que Γ est méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples aux entiers négatifs.

Maintenant, si $x \in \mathbf{R}_+^*$, on a, d'après la formule de Gauss (cf. ex. IV.1.5),

$$\begin{aligned}\frac{1}{\Gamma(x)} &= \lim_{n\to+\infty} \frac{x(x+1)\cdots(x+n)}{n!\,n^x} = x \lim_{n\to+\infty} e^{-x\log n} \prod_{k=1}^{n} \big(1+\frac{x}{k}\big) \\ &= xe^{\gamma x}\Big(\lim_{n\to+\infty} e^{-(1+\cdots+1/n)x} \prod_{k=1}^{n} \big(1+\frac{x}{k}\big)\Big) = x\,e^{\gamma x} \lim_{n\to+\infty} \prod_{k=1}^{n} \Big(\big(1+\frac{x}{k}\big)e^{-x/k}\Big),\end{aligned}$$

ce qui permet de montrer que f coïncide avec $\frac{1}{\Gamma}$ sur $\mathbf{R}_+^*$.

Enfin, les fonctions $z \mapsto \Gamma(z+1)$ et $z \mapsto z\Gamma(z)$ sont holomorphes sur $\mathbf{C} - (-\mathbf{N})$, et coïncident sur $\mathbf{R}_+^*$; elle coïncident donc sur $\mathbf{C} - (-\mathbf{N})$, d'après le th. des zéros isolés. Comme $\Gamma(1) = 1$, cela permet de montrer que $\lim_{z\to-n}(z+n)\Gamma(z) = \frac{(-1)^n}{n!}$, par récurrence sur n. Ceci termine la démonstration du théorème.

Exercice VII.2.2. — (i) Établir la *formule des compléments* $\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$ (on prendra la *dérivée logarithmique* [5] des deux membres, et on utilisera l'ex. V.5.3). En déduire une démonstration de l'identité $\int_{-\infty}^{+\infty} e^{-\pi t^2}\,dt = 1$.

(ii) Établir de même la *formule de multiplication* : si $p \in \mathbf{N} - \{0\}$, et si $z \in \mathbf{C} - (-\mathbf{N})$, alors

$$\prod_{j=0}^{p-1} \Gamma\big(\frac{z+j}{p}\big) = (2\pi)^{(p-1)/2} p^{-z+1/2} \Gamma(z).$$

2. Une formule intégrale pour les séries de Dirichlet

Le changement de variable [6] $u = \lambda t$ montre que, si $\lambda \in \mathbf{R}_+^*$, et si $\mathrm{Re}(s) > 0$, alors

$$\frac{1}{\lambda^s} = \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-\lambda t} t^s\,\frac{dt}{t}.$$

Cette simple remarque va se révèler extrêmement utile pour étudier le prolongement analytique de certaines séries de Dirichlet.

Soit $\mathrm{L}(\mathbf{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ une série de Dirichlet convergeant quelque part.

---

5. La dérivée logarithmique d'une fonction f est la fonction $\frac{f'}{f}$; c'est la dérivée de $\log f$.

6. Une raison pour faire apparaître la mesure $\frac{dt}{t}$ est qu'elle est invariante par ce type de changement de variable de même que dt est invariante par un changement de variable $u = t + a$. Autrement dit, $\frac{dt}{t}$ est une mesure de Haar sur $\mathbf{R}_+^*$.

Lemme VII.2.3. — (i) *La série entière* $\mathrm{F}_{\mathbf{a}}(z) = \sum_{n=1}^{+\infty} a_n z^n$ *est de rayon de convergence au moins* 1.

(ii) $f_{\mathbf{a}}(t) = \mathrm{F}_{\mathbf{a}}(e^{-t})$ *est* $\mathscr{C}^\infty$ *sur* $\mathbf{R}_+^*$ *et à décroissance rapide à l'infini, ainsi que toutes ses dérivées.*

Démonstration. — Il existe $\tau \in \mathbf{R}$ tel que $a_n = \mathrm{O}(n^\tau)$; on en déduit le (i) et le fait que $\mathrm{F}_{\mathbf{a}}(z) = \mathrm{O}(|z|)$ au voisinage de 0. Ceci implique que $f_{\mathbf{a}}$ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+^*$ et $\mathrm{O}(e^{-t})$ au voisinage de $+\infty$ (et donc à décroissance rapide, ce qui, pour une fonction $f : \mathbf{R}_+ \to \mathbf{C}$, signifie, rappelons-le, que $t^{\mathrm{N}} f(t)$ est bornée quand $t \to +\infty$, pour tout $\mathrm{N} \in \mathbf{N}$). Pour passer au cas d'une dérivée d'ordre quelconque de $f_{\mathbf{a}}$, il suffit de constater que $f_{\mathbf{a}}^{(k)} = f_{\mathbf{a}^{(k)}}$, où $\mathbf{a}^{(k)} = ((-n)^k a_n)_{n\in\mathbf{N}}$.

Lemme VII.2.4. — *Si* $\mathrm{Re}(s) > \sup(\sigma_{\mathrm{abs}}, 0)$*, la fonction* $f_{\mathbf{a}}(t)t^{s-1}$ *est sommable sur* $\mathbf{R}_+^*$*, et on a*

$$\mathrm{L}(\mathbf{a}, s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} f_{\mathbf{a}}(t) t^s \, \frac{dt}{t}.$$

Démonstration. — Si $\mathrm{Re}(s) = \sigma > \sup(\sigma_{\mathrm{abs}}, 0)$, on a

$$\begin{aligned}\int_0^{+\infty} |f_{\mathbf{a}}(t)t^{s-1}| \, dt &\leqslant \int_0^{+\infty} \Big(\sum_{n=1}^{+\infty} |a_n| e^{-nt}\Big) t^\sigma \, \frac{dt}{t} \\ &= \sum_{n=1}^{+\infty} |a_n| \int_0^{+\infty} e^{-nt} t^\sigma \, \frac{dt}{t} = \Gamma(\sigma) \sum_{n=1}^{+\infty} \frac{|a_n|}{n^\sigma} < +\infty,\end{aligned}$$

ce qui prouve que $f_{\mathbf{a}}(t)t^{s-1}$ est sommable sur $\mathbf{R}_+^*$ et que la série $\sum_{n=1}^{+\infty} a_n e^{-nt} t^{s-1}$ converge dans $\mathrm{L}^1(\mathbf{R}_+^*)$ vers $f_{\mathbf{a}}(t)t^{s-1}$. On a donc

$$\int_0^{+\infty} f_{\mathbf{a}}(t) t^{s-1} dt = \sum_{n=1}^{+\infty} \int_0^{+\infty} a_n e^{-nt} t^{s-1} \, dt = \sum_{n=1}^{+\infty} a_n \frac{\Gamma(s)}{n^s}.$$

Ceci permet de conclure.

Remarque VII.2.5. — (i) Si $f : \mathbf{R}_+^* \to \mathbf{C}$, la fonction $s \mapsto \mathrm{Mel}(f, s) = \int_0^{+\infty} f(t) t^s \, \frac{dt}{t}$ est la *transformée de Mellin* de f. Le changement de variable $t = e^u$ montre que, sur une droite verticale $\mathrm{Re}(s) = \sigma$, la transformée de Mellin coïncide, à homothétie près, avec la transformée de Fourier de $f(e^u)e^{\sigma u}$, ce qui permet de déduire un grand nombre de ses propriétés de celles de la transformée de Fourier.

(ii) La fonction $f_{\mathbf{a}}(t) = \sum_{n=1}^{+\infty} a_n e^{-nt}$ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+^*$, mais n'a aucune raison, a priori, d'être très sympathique en 0. De fait, les propriétés de prolongement analytique de la série de Dirichlet $\sum_{n=1}^{+\infty} \frac{a_n}{n^s}$ sont étroitement liées à la régularité de $f_{\mathbf{a}}$ en 0. La prop. VII.2.6 ci-dessous donne une illustration de ce phénomène.

3. Prolongement analytique de séries de Dirichlet

Proposition VII.2.6. — *Soit f une fonction $\mathscr{C}^\infty$ sur $\mathbf{R}_+$, à décroissance rapide à l'infini ainsi que toutes ses dérivées.*

(i) *La fonction* $\mathrm{M}(f,s)=\frac{1}{\Gamma(s)}\int_0^{+\infty} f(t)t^s\frac{dt}{t}$, *définie pour* $\mathrm{Re}(s)>0$, *admet un prolongement holomorphe à* $\mathbf{C}$ *tout entier*[7]

(ii) *Si* $k\in\mathbf{N}$, *alors* $\mathrm{M}(f,-k)=(-1)^k f^{(k)}(0)$.

Démonstration. — Sur la bande $b>\mathrm{Re}(s)>a>0$, on a $|f(t)t^{s-1}|\leqslant|f(t)\sup(t^{a-1},t^{b-1})|$. Or $\int_0^{+\infty}|f(t)\sup(t^{a-1},t^{b-1})|dt<+\infty$, grâce à la décroissance rapide de f à l'infini, et à l'hypothèse $a>0$ pour ce qui se passe au voisinage de 0. On est sous les conditions d'application du th. V.5.7, ce qui permet de montrer que $\mathrm{M}(f,s)$ est holomorphe sur le demi-plan $\mathrm{Re}(s)>0$.

Par ailleurs, une intégration par partie nous donne $\mathrm{M}(f,s)=-\mathrm{M}(f',s+1)$, si $\mathrm{Re}(s)>0$. On a donc, plus généralement, $\mathrm{M}(f,s)=(-1)^n\mathrm{M}(f^{(n)},s+n)$, si $\mathrm{Re}(s)>0$ et $n\in\mathbf{N}$. En appliquant ce qui précède à $f^{(n)}$, au lieu de f, on en déduit que $(-1)^n\mathrm{M}(f^{(n)},s+n)$ est holomorphe sur le demi-plan $\mathrm{Re}(s)>-n$. Comme cette fonction coïncide avec $\mathrm{M}(f,s)$ sur le demi-plan $\mathrm{Re}(s)>0$, cela prouve que $\mathrm{M}(f,s)$ admet un prolongement holomorphe au demi-plan $\mathrm{Re}(s)>-n$, et comme ceci est vrai quel que soit $n\in\mathbf{N}$, cela permet de démontrer le (i).

Le (ii) résulte de ce que $\mathrm{M}(f,-k)=(-1)^{k+1}\mathrm{M}(f^{(k+1)},1)$ est aussi égal à

$$(-1)^{k+1}\int_0^{+\infty} f^{(k+1)}(t)\,dt=(-1)^{k+1}[f^{(k)}]_0^{+\infty}=(-1)^k f^{(k)}(0).$$

Corollaire VII.2.7. — *Si $f_{\mathbf{a}}$ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+$, alors $\mathrm{L}(\mathbf{a},s)$ admet un prolongement holomorphe à $\mathbf{C}$ tout entier. De plus, si $k\in\mathbf{N}$, on a $\mathrm{L}(\mathbf{a},-k)=(-1)^k f_{\mathbf{a}}^{(k)}(0)$.*

Démonstration. — C'est une conséquence directe du lemme VII.2.4 et de la prop. VII.2.6 puisque $f_{\mathbf{a}}$ est à décroissance rapide à l'infini, ainsi que toutes ses dérivées (lemme VII.2.3).

Remarque VII.2.8. — La formule $\mathrm{L}(\mathbf{a},-k)=(-1)^k f_{\mathbf{a}}^{(k)}(0)$ montre que l'on obtient la même valeur pour la somme de la série divergente $\sum_{n\geqslant 1}a_n n^k$, en prenant la valeur de $\mathrm{L}(\mathbf{a},s)$ en $-k$ ou la limite quand $x\to 1^-$ de $\sum_{n=1}^{+\infty}a_n n^k x^n$.

4. Croissance dans une bande verticale

La prop. VII.2.11 ci-dessous montre que le prolongement analytique d'une série de Dirichlet a un comportement raisonnable dans une bande verticale ; ceci nous sera utile plus tard (lemme A.3.1). Sa démonstration repose sur la formule de Stirling.

7. La distribution $f\mapsto\mathrm{M}(f,s)$ que ceci permet de définir, est une *partie finie de Hadamard*. Le (ii) montre que si $k\in\mathbf{N}$, alors $\mathrm{M}(\ ,-k)$ est la dérivée k-ième de la masse de Dirac en 0.

Proposition VII.2.9. — *Sur tout secteur angulaire de la forme* $|\arg(z)| < \alpha$, *où* $\alpha < \pi$, *on a les développement suivants au voisinage de* $|z| = \infty$ *:*

(i) $\frac{\Gamma'(z)}{\Gamma(z)} = \log z - \frac{1}{2z} + \mathrm{O}(\frac{1}{z^2})$ *;*

(ii) $\log\Gamma(z) = z\log z - z + \frac{1}{2}(\log(2\pi) - \log z) + \mathrm{O}(\frac{1}{z})$, *où* $\log\Gamma(z) = \int_{[1,z]} \frac{\Gamma'(w)}{\Gamma(w)} dw$ *est le logarithme de* $\Gamma(z)$, *holomorphe dans le secteur angulaire, prenant la valeur* 0 *en* $z = 1$. (formule de Stirling complexe).

Démonstration. — On part de la formule $\frac{\Gamma'(z)}{\Gamma(z)} = -\gamma - \frac{1}{z} + \sum_{k=1}^{+\infty} (\frac{1}{k} - \frac{1}{z+k})$, qui découle (th. V.5.4) de la définition de $\frac{1}{\Gamma}$ comme un produit convergent. Si $z \notin \mathbf{R}_-$, on peut réécrire cette formule sous la forme (où $[t]$ désigne la partie entière de t et $\{t\} = t - [t]$, sa partie fractionnaire)

$$\begin{aligned}\frac{\Gamma'(z)}{\Gamma(z)} &= -\gamma - \frac{1}{z} + \int_1^{+\infty} (\frac{1}{[t]} - \frac{1}{z+[t]})\, dt \\ &= -\gamma - \frac{1}{z} + \int_1^{+\infty} (\frac{1}{[t]} - \frac{1}{t} - \frac{1}{z+[t]} + \frac{1}{z+t})\, dt + \int_1^{+\infty} (\frac{1}{t} - \frac{1}{z+t})\, dt \\ &= -\gamma - \frac{1}{z} + \int_1^{+\infty} \frac{\{t\}}{t[t]}\, dt - \int_1^{+\infty} \frac{\{t\}}{(z+t)(z+[t])}\, dt + \big[\log\frac{t}{z+t}\big]_1^{+\infty}.\end{aligned}$$

Maintenant, $\big[\log\frac{t}{z+t}\big]_1^{+\infty} = \log(z+1) = \log z + \frac{1}{z} + \mathrm{O}(\frac{1}{z^2})$ et $\mathrm{C} = \int_1^{+\infty} \frac{\{t\}}{t[t]}\, dt$ est une constante. Enfin, on peut écrire $\int_1^{+\infty} \frac{\{t\}}{(z+t)(z+[t])}\, dt$ sous la forme

$$\begin{aligned}\int_1^{+\infty} \frac{\{t\}}{(z+t)(z+[t])}\, dt &= \int_1^{+\infty} \frac{\{t\}}{(z+t)^2}\, dt + \int_1^{+\infty} \frac{\{t\}^2}{(z+t)^2(z+[t])}\, dt \\ &= \frac{1}{2(z+1)} + \int_1^{+\infty} \frac{\{t\} - 1/2}{(z+t)^2}\, dt + \int_1^{+\infty} \frac{\{t\}^2}{(z+t)^2(z+[t])}\, dt,\end{aligned}$$

et une intégration par parties nous donne

$$\int_1^{+\infty} \frac{\{t\} - 1/2}{(z+t)^2}\, dt = \big[\frac{\{t\}^2 - \{t\}}{2(z+t)^2}\big]_1^{+\infty} + \int_1^{+\infty} \frac{\{t\}^2 - \{t\}}{(z+t)^3}\, dt = \int_1^{+\infty} \frac{\{t\}^2 - \{t\}}{(z+t)^3}\, dt.$$

En utilisant la minoration

$$|z+u|^2 \geqslant \frac{1+\cos\alpha}{2}(|z|+u)^2, \quad \text{si } u \in \mathbf{R}_+ \text{ et } |\arg(z)| \leqslant \alpha,$$

cela permet de majorer en module les quantités $\int_1^{+\infty} \frac{\{t\}^2}{(z+t)^2(z+[t])}\, dt$ et $\int_1^{+\infty} \frac{\{t\}^2 - \{t\}}{(z+t)^3}\, dt$ par $\int_1^2 \frac{1}{(|z|-2)^3}\, dt + \int_2^{+\infty} (\frac{2}{1+\cos\alpha})^{3/2} \frac{1}{(|z|+t-1)^3}\, dt$. On en déduit que ces deux intégrales sont des $\mathrm{O}(\frac{1}{z^2})$ et comme il en est de même de $\frac{1}{2(z+1)} - \frac{1}{2z}$, on obtient finalement :

$$\frac{\Gamma'(z)}{\Gamma(z)} = \log z + \mathrm{C} - \gamma - \frac{1}{2z} + \mathrm{H}(z),$$

où H est holomorphe dans le secteur angulaire $|\arg(z)| < \alpha$ et y vérifie $|\mathrm{H}(z)| \leqslant \frac{\mathrm{A}}{|z|^2}$, si $|z| \geqslant 1$, pour une certaine constante $\mathrm{A} > 0$. On en déduit, en intégrant, que

$$\log\Gamma(z) = \big[w\log w - w + (\mathrm{C} - \gamma)w - \frac{1}{2}\log w\big]_1^z + \int_1^z \mathrm{H}(w)\, dw.$$

Maintenant, si $z = re^{i\theta}$, on peut écrire $\int_1^z$ sous la forme $\int_1^{\mathrm{R}} + \int_{\mathrm{R}}^{\mathrm{R}e^{i\theta}} + \int_{\mathrm{R}e^{i\theta}}^{re^{i\theta}}$, et quand R tend vers $+\infty$, $\int_1^{\mathrm{R}} \mathrm{H}(w)dw$ tend vers une constante ; $\int_{\mathrm{R}}^{\mathrm{R}e^{i\theta}} \mathrm{H}(w)dw \to 0$ car $|\mathrm{H}(w)| \leqslant \frac{\mathrm{A}}{\mathrm{R}^2}$ et la longueur de l'arc de cercle est $\theta\mathrm{R}$, et $\big|\int_{\mathrm{R}e^{i\theta}}^{re^{i\theta}} \mathrm{H}(w)dw\big| \leqslant \int_r^{\mathrm{R}} \frac{\mathrm{A}}{u^2}\, du \leqslant \frac{\mathrm{A}}{r} = \frac{\mathrm{A}}{|z|}$. D'où l'existence de $\mathrm{C}' \in \mathbf{C}$, tel que l'on ait

$\log\Gamma(z) = z\log z - z + (\mathrm{C}-\gamma)z - \frac{1}{2}\log z + \mathrm{C}' + \mathrm{O}(\frac{1}{z})$ au voisinage de l'infini. La formule de Stirling réelle :

$$\log(\Gamma(x+1)) = x\log x - x + \frac{1}{2}\log(2\pi x) + o(1), \quad \text{au voisinage de } +\infty$$

permet alors d'en déduire que $\mathrm{C}-\gamma = 0$ et $\mathrm{C}' = \frac{1}{2}\log 2\pi$, ce qui permet de conclure.

Corollaire VII.2.10. — *Quand $|\tau|$ tend vers $+\infty$, on a*

$$|\Gamma(\sigma+i\tau)| = \sqrt{2\pi}|\tau|^{\sigma-\frac{1}{2}}e^{-\pi|\tau|/2}(1+\mathrm{O}(\frac{1}{\tau})),$$

uniformément dans toute bande verticale de largeur finie.

Démonstration. — Si $s = \sigma + i\tau$, et $a \leqslant \sigma \leqslant b$, où $a, b \in \mathbf{R}$ sont fixés, alors

$$\log s = \log i\tau + \frac{\sigma}{i\tau} + \mathrm{O}(\frac{1}{\tau^2}) = \log|\tau| + \frac{i\pi}{2}\cdot\frac{\tau}{|\tau|} + \frac{\sigma}{i\tau} + \mathrm{O}(\frac{1}{\tau^2}).$$

En utilisant le (ii) de la prop. VII.2.9 et la formule ci-dessus, on en déduit que

$$\mathrm{Re}(\log\Gamma(\sigma+i\tau)) = \sigma\log|\tau| - \frac{\pi|\tau|}{2} + \sigma - \sigma - \frac{1}{2}\log|\tau| + \frac{1}{2}\log 2\pi + \mathrm{O}(\frac{1}{\tau}).$$

Ceci permet de conclure.

Proposition VII.2.11. — *Soit f une fonction $\mathscr{C}^\infty$ sur $\mathbf{R}_+$, à décroissance rapide à l'infini ainsi que toutes ses dérivées. Si $a \leqslant b$ sont deux réels, alors pour tout $k \in \mathbf{N}$, il existe $\mathrm{C}_{a,b,k}(f)$ tel que*

$$|\mathrm{M}(f,s)| \leqslant \mathrm{C}_{a,b,k}(f)(1+|\tau|)^{-k}e^{\frac{\pi}{2}|\tau|}, \text{ si } s = \sigma+i\tau \text{ et } a \leqslant \sigma \leqslant b.$$

Démonstration. — Choisissons $n \in \mathbf{N}$ tel que $n + a > k + \frac{1}{2}$. Si $s = \sigma + i\tau$, avec $a \leqslant \sigma \leqslant b$, alors

$$|\mathrm{M}(f,s)| \leqslant \frac{1}{|\Gamma(s+n)|}\int_0^{+\infty}|f^{(n)}(t)|t^{\sigma+n}\frac{dt}{t} \leqslant \frac{\mathrm{C}_n}{|\Gamma(s+n)|},$$

où $\mathrm{C}_n = \int_0^{+\infty}|f^{(n)}(t)|\sup(t^{a+n}, t^{b+n})\frac{dt}{t}$. Par ailleurs, d'après le cor. VII.2.10, il existe $\mathrm{T} > 0$ tel que, si $s = \sigma + i\tau$, alors

$$|\Gamma(s+n)|^{-1} \leqslant \frac{2}{\sqrt{2\pi}}(1+|\tau|)^{\frac{1}{2}-\sigma-n}e^{\frac{\pi}{2}|\tau|} \leqslant \frac{2}{\sqrt{2\pi}}(1+|\tau|)^{-k}e^{\frac{\pi}{2}|\tau|}, \quad \text{si } |\tau| \geqslant \mathrm{T} \text{ et } a \leqslant \sigma \leqslant b.$$

Donc $(1+|\tau|)^k e^{-\frac{\pi}{2}|\tau|}|\mathrm{M}(f,s)|$ est bornée sur $\{s = \sigma+i\tau,\ |\tau| \geqslant \mathrm{T},\ a \leqslant \sigma \leqslant b\}$, et comme elle est continue sur la bande $a \leqslant \mathrm{Re}(s) \leqslant b$, elle est aussi bornée sur la bande toute entière. Ceci permet de conclure.

VII.3. La fonction zêta de Riemann

1. Séries de Dirichlet attachées à des fonctions multiplicatives

On note $\mathscr{P}$ l'ensemble des nombres premiers.

Une fonction $n \mapsto a(n)$ de $\mathbf{N}-\{0\}$ dans $\mathbf{C}$ est *multiplicative*, si $a(1)=1$, et si $a(nm)=a(n)a(m)$ pour tous n et m *premiers entre eux*; elle est *strictement multiplicative*, si $a(1)=1$, et $a(nm)=a(n)a(m)$, quels que soient $m,n \geqslant 1$. On remarquera qu'une fonction strictement multiplicative est déterminée par les $a(p)$, pour $p \in \mathscr{P}$ puisque, si $n=\prod_{i\in \mathrm{I}} p_i^{k_i}$ est la décomposition de n en facteurs premiers, on a $a(n)=\prod_{i\in \mathrm{I}} a(p_i)^{k_i}$. Par contre, pour une fonction multiplicative, on a besoin de connaître les $a(p^k)$, pour $p \in \mathscr{P}$ et $k \geqslant 1$. On a alors $a(n)=\prod_{i\in \mathrm{I}} a(p_i^{k_i})$

Proposition VII.3.1. — *Si $n \mapsto a(n)$ est multiplicative, et si $\mathrm{L}(a,s)=\sum_{n\geqslant 1}\frac{a(n)}{n^s}$ converge quelque part, alors pour tout s dans le demi-plan $\mathrm{Re}(s)>\sigma_{\mathrm{abs}}$, on a :*

(i) $1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots$ *est absolument convergent quel que soit $p \in \mathscr{P}$;*

(ii) *le produit $\prod_{p\in\mathscr{P}}(1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots)$ converge uniformément sur tout demi-plan $\mathrm{Re}(s)>c>\sigma_{\mathrm{abs}}$, et sa valeur est $\mathrm{L}(a,s)$.*

Démonstration. — Soit $c>\sigma_{\mathrm{abs}}$. Si $\mathrm{Re}(s)>c$, alors

$$\sum_{p\in\mathscr{P}} \big|\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots\big| \leqslant \sum_{p\in\mathscr{P}} \big(\big|\frac{a(p)}{p^s}\big|+\big|\frac{a(p^2)}{p^{2s}}\big|+\cdots\big) \leqslant \sum_{n=2}^{+\infty}\frac{|a(n)|}{n^c}<+\infty.$$

On en déduit le (i) et, en utilisant le th. V.5.4 (ou plutôt la démonstration du (i) de ce théorème), la convergence uniforme du produit sur $\mathrm{Re}(s)>c$.

Si $\mathrm{X}\in\mathbf{R}_+$, soit $\mathscr{P}(\mathrm{X})$ l'ensemble des nombres premiers $\leqslant \mathrm{X}$, et soit $\mathrm{I}(\mathrm{X})$ l'ensemble des entiers dont tous les diviseurs premiers sont dans $\mathscr{P}(\mathrm{X})$. Si $k\in\mathbf{N}$, soit $\mathrm{I}(\mathrm{X},k)$ l'ensemble des entiers de la forme $\prod_{p\in\mathscr{P}(\mathrm{X})} p^{k_p}$, avec $0\leqslant k_p\leqslant k$. L'ensemble $\mathrm{I}(\mathrm{X},k)$ est donc un ensemble fini. Par ailleurs, la multiplicativité de $n\mapsto a(n)$ fait que

$$\prod_{p\in\mathscr{P}(\mathrm{X})}(1+\frac{a(p)}{p^s}+\cdots+\frac{a(p^k)}{p^{ks}})=\sum_{n\in\mathrm{I}(\mathrm{X},k)}\frac{a(n)}{n^s}.$$

Comme toutes les séries qui interviennent sont majorées, en valeur absolue, par la série sommable $\sum_{n\geqslant 1}\big|\frac{a(n)}{n^s}\big|$, le théorème de convergence dominée pour les séries montre, en faisant tendre k vers $+\infty$, que

$$\prod_{p\in\mathscr{P}(\mathrm{X})}(1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots)=\sum_{n\in\mathrm{I}(\mathrm{X})}\frac{a(n)}{n^s},$$

puis, en faisant tendre X vers $+\infty$, que

$$\prod_{p\in\mathscr{P}}(1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots)=\sum_{n\geqslant 1}\frac{a(n)}{n^s},$$

ce que l'on cherchait à établir.

Remarque VII.3.2. — (i) Le facteur $1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots$ du produit est *le facteur d'Euler en p* de la fonction $\mathrm{L}(a,s)$, et la formule $\mathrm{L}(a,s)=\prod_{p\in\mathscr{P}}(1+\frac{a(p)}{p^s}+\frac{a(p^2)}{p^{2s}}+\cdots)$ est la *décomposition de* $\mathrm{L}(a,s)$ *en produit de facteurs d'Euler* (ou en *produit eulérien*).

(ii) Si a est strictement multiplicative, les facteurs d'Euler sont donnés par des séries géométriques et on a $\mathrm{L}(a,s)=\prod_{p\in\mathscr{P}}\frac{1}{1-a(p)p^{-s}}$.

2. Prolongement analytique de la fonction ζ

La série de Dirichlet $\mathrm{L}(\mathbf{1},s)=\sum_{n\geqslant 1}\frac{1}{n^s}$ admet 1 comme abscisse de convergence absolue (et comme abscisse de convergence puisqu'elle est à coefficients positifs (cor. VII.1.2)). De plus $n\mapsto 1$ est on ne peut plus strictement multiplicative ; on déduit donc de la théorie générale le résultat suivant (dû à Euler, 1737).

Proposition VII.3.3. — *Si* $\mathrm{Re}(s)>1$, *alors* $\sum_{n\geqslant 1}\frac{1}{n^s}=\prod_{p\in\mathscr{P}}\frac{1}{1-p^{-s}}$, *et le produit est uniformément convergent sur tout demi-plan* $\mathrm{Re}(s)>c>1$.

Théorème VII.3.4. — *Il existe une unique fonction, notée* ζ (fonction zêta de Riemann), *vérifiant :*

• ζ *est méromorphe sur* $\mathbf{C}$ *tout entier, holomorphe en dehors d'un pôle simple en* $s=1$, *de résidu* 1 ;

• $\zeta(s)=\mathrm{L}(\mathbf{1},s)$, *si* $\mathrm{Re}(s)>1$.

Démonstration. — L'unicité est une conséquence de l'unicité du prolongement analytique (cor. V.3.7). Si $f_{\mathbf{1}}(t)=\sum_{n=1}^{+\infty}e^{-nt}=\frac{1}{e^t-1}$ et si $g(t)=tf_{\mathbf{1}}(t)$, on déduit du lemme VII.2.4 que, quel que soit s, avec $\mathrm{Re}(s)>1$,

$$\mathrm{L}(\mathbf{1},s)=\frac{1}{\Gamma(s)}\int_0^{+\infty}f_{\mathbf{1}}(t)t^s\frac{dt}{t}=\frac{1}{(s-1)\Gamma(s-1)}\int_0^{+\infty}tf_{\mathbf{1}}(t)t^{s-1}\frac{dt}{t}=\frac{1}{s-1}\mathrm{M}(g,s-1).$$

Comme $g(t)$ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+^*$, holomorphe au voisinage de 0 (et donc $\mathscr{C}^\infty$ sur $\mathbf{R}_+$), et à décroissance rapide à l'infini ainsi que toutes ses dérivées, la prop. VII.2.6 s'applique. On en déduit que $\mathrm{M}(g,s)$ a un prolongement analytique à $\mathbf{C}$ tout entier, avec $\mathrm{M}(g,0)=g(0)=1$. Le résultat s'en déduit.

Remarque VII.3.5. — Si s est réel >1, on a $\log\zeta(s)=-\sum_{p\in\mathscr{P}}\log(1-p^{-s})$ d'après la prop. VII.3.3. Or $-\log(1-p^{-s})\sim p^{-s}$, et l'existence d'un pôle de ζ en $s=1$ se traduit par le fait que $\lim_{s\to 1^+}\sum_{p\in\mathscr{P}}p^{-s}=+\infty$. Il en résulte que la somme des inverses des nombres premiers diverge (résultat dû à Euler (1737)) ; en particulier, ceci prouve que l'ensemble des nombres premiers est infini (résultat remontant à l'antiquité), mais en dit un peu plus sur leur répartition que la preuve des grecs.

Exercice VII.3.6. — Soit $\sum_{n=0}^{+\infty} \mathrm{B}_n \frac{t^n}{n!}$ le développement de Taylor [8] de $g(t) = \frac{t}{e^t-1}$ en 0.

(i) Calculer $g(t) - g(-t)$. En déduire $\mathrm{B}_{2k+1} = 0$, si $k \geqslant 1$.

(ii) Montrer que $\zeta(-n) = (-1)^n \frac{\mathrm{B}_{n+1}}{n+1}$, si $n \in \mathbf{N}$. En déduire que ζ prend des valeurs rationnelles aux entiers [9] négatifs, et a des zéros en les entiers pairs < 0.

(iii) Montrer que $g(z) - \frac{2i\pi}{z-2i\pi} + \frac{2i\pi}{z+2i\pi}$ est holomorphe sur $\mathrm{D}(0, (4\pi)^-)$. En déduire des équivalents de $\frac{\mathrm{B}_{2n}}{(2n)!}$ et de $\zeta(1-2n)$ quand $n \to +\infty$.

3. Équation fonctionnelle de la fonction zêta

Théorème VII.3.7. — (Riemann, 1858) *La fonction ζ vérifie l'équation fonctionnelle* [10]

$$\zeta(s) = 2 \cdot (2\pi)^{s-1} \cdot \Gamma(1-s) \cdot \sin\frac{\pi s}{2} \cdot \zeta(1-s).$$

Remarque VII.3.8. — (i) Soit $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$. Modulo les formules (ex. VII.2.2)

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}, \quad \Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{s+1}{2}\Big) = 2^{1-s}\Gamma\Big(\frac{1}{2}\Big)\Gamma(s), \quad \text{et} \quad \Gamma\Big(\frac{1}{2}\Big) = \sqrt{\pi},$$

on peut déduire de l'équation fonctionnelle de ζ que ξ vérifie l'équation fonctionnelle

$$\xi(s) = \xi(1-s).$$

(ii) L'équation fonctionnelle de la fonction ξ peut s'établir directement (cf. ex. VII.6.6), mais la démonstration ci-dessous a l'avantage de se généraliser plus facilement aux fonctions L de Dirichlet. De plus, c'est sous la forme du th. VII.3.7 que nous utiliserons l'équation fonctionnelle de ζ dans la démonstration du théorème des nombres premiers (annexe A).

Démonstration. — Si $c > 0$, soit γ_c le contour obtenu en composant la demi-droite $(+\infty, c]$ suivi du carré C_c de sommets $c(\pm 1 \pm i)$ parcouru dans le sens direct et de la demi-droite $[c, +\infty)$. Soit

$$\mathrm{F}_c(s) = \frac{1}{2i\pi}\int_{\gamma_c} f_{\mathbf{1}}(z)(-z)^s \frac{dz}{z},$$

8. Les B_n sont des nombres rationnels, appelés nombres de Bernoulli, et qu'on retrouve dans toutes les branches des mathématiques. On a en particulier

$$\mathrm{B}_0 = 1, \quad \mathrm{B}_1 = \frac{-1}{2}, \quad \mathrm{B}_2 = \frac{1}{6}, \quad \mathrm{B}_3 = 0, \quad \mathrm{B}_4 = \frac{-1}{30}, \quad \ldots, \quad \mathrm{B}_{12} = \frac{-691}{2730}, \ldots$$

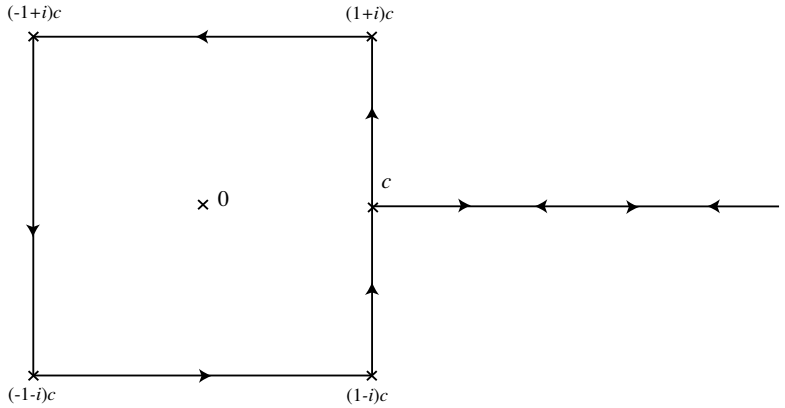
Un test presque infaillible pour savoir si une suite de nombres a un rapport avec les nombres de Bernoulli est de regarder si 691 apparaît dans les premiers termes de cette suite.

9. Les valeurs aux entiers de la fonction zêta, ou plus généralement des fonctions L de la géométrie arithmétique, recellent une quantité impressionante d'informations arithmétiques. Kummer fut l'un des premiers à exploiter cette information, ce qui lui a permis de montrer (1852) que, si p est un nombre premier $\geqslant 3$ ne divisant pas le numérateur de $\zeta(-1)$, $\zeta(-3)$, …, $\zeta(2-p)$, alors l'équation $a^p + b^p = c^p$ n'a pas de solution en nombres entiers avec $abc \neq 0$ (i.e. le théorème de Fermat est vrai pour un tel p (dit *régulier*)). Jusqu'à 100, les seuls nombres premiers irréguliers sont 37, 59 et 67.

10. Cette équation fonctionnelle avait été conjecturée par Euler (1749) qui se basait sur ses calculs de ζ en les entiers.

où $f_{\mathbf{1}}(z) = \frac{1}{e^z - 1}$, et $(-z)^s = \exp(s \log(-z))$, la détermination du logarithme choisie étant celle dont la partie imaginaire est comprise entre $-\pi$ et π ; en particulier, $(-z)^s = e^{-i\pi s} z^s$ de $+\infty$ à c et $(-z)^s = e^{i\pi s} z^s$ de c à $+\infty$ (après avoir parcouru le carré).

La démonstration consiste à utiliser la formule des résidus pour évaluer $\mathrm{F}_d(s) - \mathrm{F}_c(s)$, ce qui fait apparaître la fonction $\zeta(1-s)$. La fonction $\zeta(s)$ s'obtient en faisant tendre c vers 0, et un passage à la limite quand $c \to +\infty$ donne le lien cherché entre $\zeta(s)$ et $\zeta(1-s)$.



le chemin γ_c

• *Calcul de* $\mathrm{F}_d(s) - \mathrm{F}_c(s)$. (Un peu plus de familiarité avec les fonctions holomorphes permettrait de se passer de la cuisine peu ragoûtante qui suit et de démontrer directement que $\mathrm{F}_d(s) - \mathrm{F}_c(s)$ est la somme des résidus de la fonction $f_{\mathbf{1}}(z)\frac{(-z)^s}{z}$ (qui est méromorphe sur $\mathbf{C} - [0, +\infty)$) en les points à l'intérieur du chemin $\gamma_{c,d}$ composé de C_d, $[d, c]$, C_c parcouru en sens opposé, et $[c, d]$.)

Les chemins sur lesquels on intègre ne sont pas vraiment contenus dans un ouvert sur lequel la fonction qu'on intègre est méromorphe ; pour se ramener à ce cas, on va être forcé de tout découper en morceaux.

On note g_s^+ (resp. g_s^-) la fonction $g_s^+(z) = f_{\mathbf{1}}(z)\frac{(-z)^s}{z}$ sur l'ouvert Ω^+ (resp. Ω^-) obtenu en enlevant la demi-droite $[0, -i\infty)$ (resp. $[0, +i\infty)$) à $\mathbf{C}$, la détermination de $\log(-z)$ étant celle prenant des valeurs réelles sur la demi-droite $[0, -\infty)$. Les fonctions g_s^+ et g_s^- sont méromorphes sur Ω^+ et Ω^- respectivement, et coïncident sur le demi-plan $\mathrm{Re}(s) < 0$; par contre, sur le demi-plan $\mathrm{Re}(s) > 0$, on a $g_s^-(z) = e^{2i\pi s} g_s^+(z)$.

On note C_c^+ (resp. C_c^-) le morceau de C_c contenu dans le demi-plan $\mathrm{Im}(s) \geqslant 0$ (resp. $\mathrm{Im}(s) \leqslant 0$). On a donc $\mathrm{C}_c^+ = [c, (1+i)c] \cdot [(1+i)c, (-1+i)c] \cdot [(-1+i)c, -c]$, et $\mathrm{C}_c^- = [-c, (-1-i)c] \cdot [(-1-i)c, (1-i)c] \cdot [(1-i)c, c]$. Soit γ_c^+ (resp. γ_c^-) le chemin composé de $(+\infty, c]$ et C_c^+ (resp. de C_c^- et $[c, +\infty)$), et soient $\mathrm{F}_c^+(s) = \frac{1}{2i\pi}\int_{\gamma_c^+} g_s^+(z)\,dz$ et $\mathrm{F}_c^-(s) = \frac{1}{2i\pi}\int_{\gamma_c^-} g_s^+(z)\,dz$, de telle sorte que $\mathrm{F}_c(s) = \mathrm{F}_c^+(s) + \mathrm{F}_c^-(s)$.

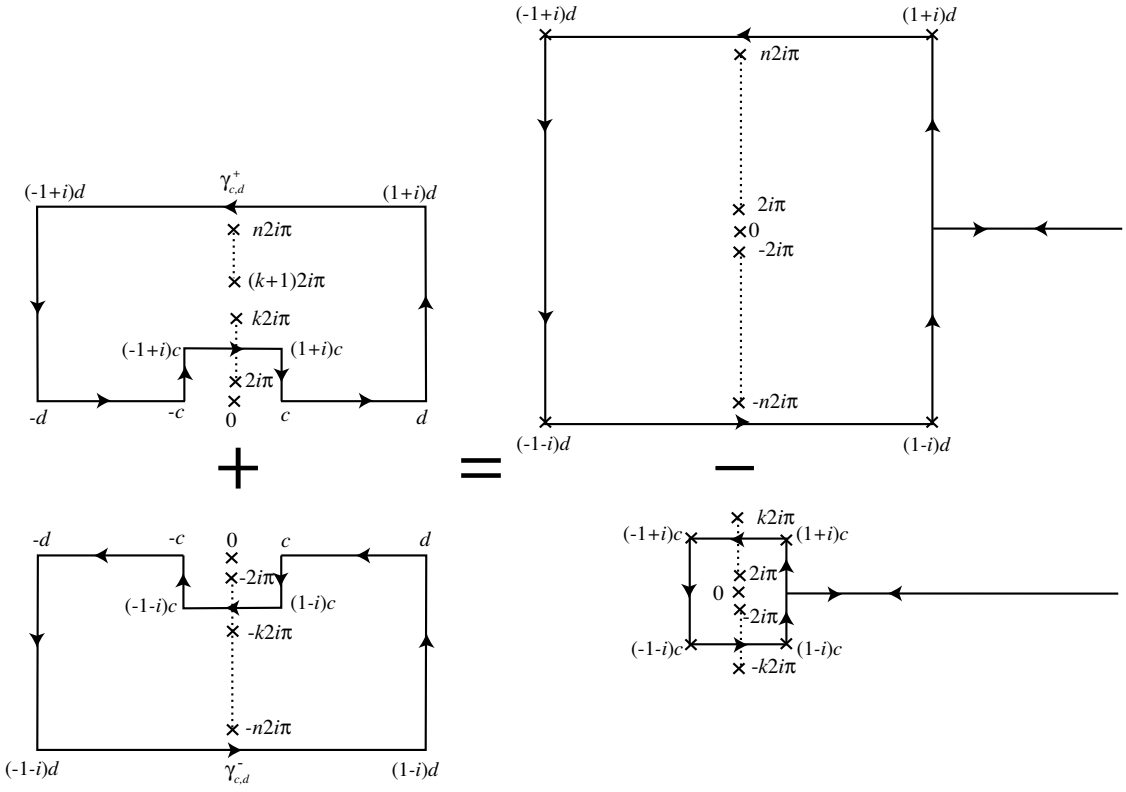
Si $c < d$, soient $\gamma_{c,d}^+$ le lacet $\mathrm{C}_d^+ \cdot [-d, -c] \cdot (\mathrm{C}_c^+)^{\mathrm{opp}} \cdot [c, d]$ et $\gamma_{c,d}^+$ le lacet $\mathrm{C}_d^- \cdot [d, c] \cdot (\mathrm{C}_c^-)^{\mathrm{opp}} \cdot [-c, -d]$, où $(\mathrm{C}_c^+)^{\mathrm{opp}}$ et $(\mathrm{C}_c^-)^{\mathrm{opp}}$ désignent les chemins C_c^+ et C_c^- parcourus dans le sens opposé. On a

$$\mathrm{F}_d^+(s) - \mathrm{F}_c^+(s) = \frac{1}{2i\pi}\int_{\gamma_{c,d}^+} g_s^+(z)\,dz - \frac{1}{2i\pi}\int_{[-d,-c]} g_s^+(z)\,dz$$

$$\mathrm{F}_d^-(s) - \mathrm{F}_c^-(s) = \frac{1}{2i\pi}\int_{\gamma_{c,d}^-} g_s^-(z)\,dz - \frac{1}{2i\pi}\int_{[-c,-d]} g_s^-(z)\,dz,$$

comme on peut le voir sur le dessin ci-dessus. Comme $g_s^+(z) = g_s^-(z)$ sur $[-c,-d]$, l'intégrale sur $[-c,-d]$ disparaît quand on fait la somme des deux égalités ci-dessus, et on obtient

$$\mathrm{F}_d(s) - \mathrm{F}_c(s) = \frac{1}{2i\pi}\int_{\gamma_{c,d}^+} g_s^-(z)\,dz + \frac{1}{2i\pi}\int_{\gamma_{c,d}^-} g_s^+(z)\,dz.$$



$$\int_{\gamma_d} - \int_{\gamma_c} = \int_{\gamma_{c,d}^+} + \int_{\gamma_{c,d}^-}$$

Le membre de droite peut se calculer grâce à la formule des résidus. La fonction g_s^+ est méromorphe sur Ω^+, avec des pôles simples aux $2i\pi k$, pour $k \in \mathbf{N} - \{0\}$, et comme $e^z - 1$ a une dérivée égale à 1 en $2i\pi k$, on a $\mathrm{Res}(g_s^+, 2i\pi k) = \frac{(-2i\pi k)^s}{2i\pi k} = -(2k\pi)^{s-1}e^{-i\pi\frac{s-1}{2}}$. De même, g_s^- est méromorphe sur Ω^-, avec des pôles simples aux $-2i\pi k$, pour $k \in \mathbf{N} - \{0\}$, et on a $\mathrm{Res}(g_s^-, -2i\pi k) = \frac{(2i\pi k)^s}{-2i\pi k} = -(2k\pi)^{s-1}e^{i\pi\frac{s-1}{2}}$. Par ailleurs, l'indice de $\gamma_{c,d}^+$ par rapport à $2i\pi k$ est 1, si $c < 2k < d$, et 0 sinon ; l'indice de $\gamma_{c,d}^-$ par rapport à $-2i\pi k$ est 1, si $c < 2k < d$, et 0 sinon. On obtient donc, en utilisant la formule des résidus,

$$\mathrm{F}_d(s) - \mathrm{F}_c(s) = -\sum_{c<2k\pi<d} 2\cos\pi\frac{s-1}{2}\cdot(2k\pi)^{s-1}.$$

• *Une majoration pour* $|(-z)^s|$. On a $|(-z)^s| = e^{\mathrm{Re}(s\log(-z))} = |z|^{\mathrm{Re}(s)}e^{-\mathrm{Im}(s)\arg(-z)}$. Comme $\arg(-z)$ varie entre $-\pi$ et π sur les domaines considérés, cela montre que, si s est fixé, il existe une constante $c(s)$ telle que $|(-z)^s| \leqslant c(s)|z|^{\mathrm{Re}(s)}$, pour tout z.

• *Lien entre* F_π *et* $\zeta(s)$. La formule obtenue pour $\mathrm{F}_d(s) - \mathrm{F}_c(s)$ montre, en particulier, que F_c ne dépend pas de c dans l'intervalle $]0, 2\pi[$, et donc que $\mathrm{F}_\pi(s) = \lim_{c\to 0^+} \mathrm{F}_c(s)$. Or la majoration ci-dessus pour $|(-z)^s|$ implique que, quand c tend vers 0, l'intégrale sur C_c tend vers 0, si $\mathrm{Re}(s) > 1$. On obtient donc, en passant à la limite si $\mathrm{Re}(s) > 1$,

$$\mathrm{F}_\pi(s) = \frac{1}{2i\pi}\Big(e^{-i\pi s}\int_{+\infty}^{0}\frac{1}{e^t-1}t^s\frac{dt}{t} + e^{i\pi s}\int_0^{+\infty}\frac{1}{e^t-1}t^s\frac{dt}{t}\Big) = \frac{\sin\pi s}{\pi}\cdot\Gamma(s)\cdot\zeta(s).$$

• *Lien entre* F_π *et* $\zeta(1-s)$. On a $|\frac{1}{e^z-1}| \leqslant \frac{1}{1-e^{-(2\mathrm{N}+1)\pi}} \leqslant \frac{1}{2}$ sur le carré $\mathrm{C}_{(2\mathrm{N}+1)\pi}$ (sur un bord vertical, on minore $|e^z-1|$ par $||e^z|-1|$, et on remarque que e^z est réel négatif sur les deux bords horizontaux). On en déduit, en utilisant la majoration $|(-z)^s| \leqslant c(s)|z|^{\mathrm{Re}(s)}$, que, si $\mathrm{Re}(s) < 0$, alors $\mathrm{F}_{(2\mathrm{N}+1)\pi}(s) \to 0$ quand $\mathrm{N} \to +\infty$. En utilisant la formule ci-dessus pour $\mathrm{F}_d(s) - \mathrm{F}_c(s)$, avec $d = (2\mathrm{N}+1)\pi$ et $c = \pi$, et en passant à la limite quand $\mathrm{N} \to +\infty$, on obtient

$$\mathrm{F}_\pi(s) = 2\cdot\cos(\pi\frac{s-1}{2})\cdot(2\pi)^{s-1}\cdot\zeta(1-s) \quad \text{si } \mathrm{Re}(s) < 0.$$

• *Holomorphie de* F_π. On a $\mathrm{F}_\pi(s) = \frac{1}{2i\pi}\big(\int_{\mathrm{C}_\pi}\frac{(-z)^s}{e^z-1}\frac{dz}{z} + (e^{i\pi s} - e^{-i\pi s})\int_\pi^{+\infty}\frac{t^s}{e^t-1}\frac{dt}{t}\big)$. Sur un demi-plan $\mathrm{Re}(s) > a$, on a $|t^s| \leqslant t^a$, si $t \in [\pi, +\infty[$, et comme $\frac{t^{a-1}}{e^t-1}$ est sommable sur $[\pi, +\infty[$, on déduit du th. V.5.7 que $\int_\pi^{+\infty}\frac{t^s}{e^t-1}\frac{dt}{t}$ est holomorphe en s, sur tout demi-plan de la forme $\mathrm{Re}(s) > a$, et donc aussi sur $\mathbf{C}$ tout entier. Pour prouver que F_π est holomorphe sur $\mathbf{C}$, il suffit donc de vérifier que $\int_{\mathrm{C}_\pi}\frac{(-z)^s}{e^z-1}\frac{dz}{z}$ l'est, ce qui résulte du cor. V.5.8.

• *Conclusion.* Comme F_π, Γ, sin, cos et ζ sont méromorphes sur $\mathbf{C}$ tout entier, on en déduit, en utilisant le th. des zéros isolés, que

$$\sin\pi s\cdot\Gamma(s)\cdot\zeta(s) = \pi\,\mathrm{F}_\pi(s) = \cos\pi\frac{s-1}{2}\cdot(2\pi)^s\cdot\zeta(1-s),$$

pour tout s qui n'est pas un pôle d'une des fonctions ci-dessus. En utilisant la formule $\sin\pi s = -\sin\pi(s-1) = -2\sin\pi\frac{s-1}{2}\cdot\cos\pi\frac{s-1}{2}$, on peut réécrire cette équation fonctionnelle sous la forme

$$\zeta(1-s) = -2(2\pi)^{-s}\cdot\sin\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot\zeta(s),$$

et on obtient l'équation fonctionnelle du théorème en appliquant l'équation fonctionnelle ci-dessus à $1-s$ au lieu de s.

Exercice VII.3.9. — On note γ la constante d'Euler comme dans le th. VII.2.1.

(i) Montrer que $\Gamma'(1) = -\gamma$.

(ii) Montrer que $\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{+\infty}\int_n^{n+1}\big(\frac{1}{n^s} - \frac{1}{t^s}\big)\,dt$, si $\mathrm{Re}(s) > 1$. En déduire $\lim_{s\to 1}\zeta(s) - \frac{1}{s-1} = \gamma$, puis $\frac{\zeta'(0)}{\zeta(0)} = \log 2\pi$ et $\zeta'(0) = -\frac{1}{2}\log 2\pi$.

4. Les zéros de la fonction ζ

Le thèorème VII.3.7 permet une bonne localisation des zéros de la fonction ζ dans le plan complexe.

Corollaire VII.3.10. — *Les seuls zéros de la fonction ζ qui ne sont pas dans la bande verticale $0 \leqslant \mathrm{Re}(s) \leqslant 1$ sont des zéros simples aux entiers pairs < 0.*

Démonstration. — $\zeta(s)$ est donnée (prop. VII.3.3) par le produit absolument convergent $\prod_{p\in\mathscr{P}} \frac{1}{1-p^{-s}}$ sur le demi-plan $\mathrm{Re}(s) > 1$. Comme aucun des termes du produit ne s'annule sur ce demi-plan, la fonction ζ ne s'annule pas sur le demi-plan $\mathrm{Re}(s) > 1$. D'autre part, si $\mathrm{Re}(s) < 0$, on a $\Gamma(1-s) \neq 0$, et, d'après ce qui précède, $\zeta(1-s) \neq 0$. L'équation fonctionnelle du th. VII.3.7 montre donc que les zéros de ζ sur le demi-plan $\mathrm{Re}(s) < 0$ sont les mêmes que ceux de $\sin\frac{\pi s}{2}$. Ceci permet de conclure.

On appelle *zéros triviaux* les zéros aux entiers pairs < 0. La *bande critique* est la bande verticale $0 \leqslant \mathrm{Re}(s) \leqslant 1$; c'est un monde mystérieux, où il est difficile de voir clair. Riemann, à qui on doit la démonstration ci-dessus de l'équation fonctionnelle de la fonction ζ a, le premier (en 1858), dans un mémoire qui est un des grands classiques des mathématiques, montré comment la répartition des zéros dans cette bande critique est reliée à la répartition des nombres premiers (cf. annexe A). Ce mémoire contient aussi *l'hypothèse de Riemann*, toujours non résolue à ce jour, et dont la tête est mise à prix pour un million de dollar, selon laquelle *tous les zéros de ζ dans la bande critique sont sur la droite* $\mathrm{Re}(s) = \frac{1}{2}$.

VII.4. Fonctions L de Dirichlet

1. Caractères de Dirichlet et Fonctions L de Dirichlet

Si D est un entier, un *caractère de Dirichlet modulo* D est un morphisme de groupes $\chi : (\mathbf{Z}/\mathrm{D}\mathbf{Z})^* \to \mathbf{C}^*$. L'image d'un caractère de Dirichlet est un sous-groupe fini de $\mathbf{C}^*$, et donc est incluse dans le groupe des racines de l'unité. On note $\mathbf{1}_\mathrm{D}$ le *caractère trivial*, défini par $\mathbf{1}_\mathrm{D}(a) = 1$, quel que soit $a \in (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$.

Si χ est un caractère de Dirichlet modulo D, on considère aussi souvent χ comme une fonction périodique sur $\mathbf{Z}$ de période D, en composant χ avec la projection naturelle de $\mathbf{Z}$ sur $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, et en étendant χ par 0 sur les entiers non premiers à D. La fonction $\chi \mapsto \chi(n)$ est alors strictement multiplicative : en effet, si m et n sont premiers à D, alors $\chi(mn) = \chi(m)\chi(n)$ par multiplicativité de la réduction modulo D et celle de χ, tandis que si m ou n n'est pas premier à D, alors mn non plus, et on a $\chi(mn) = 0 = \chi(m)\chi(n)$. La *fonction* L *de Dirichlet* attachée à χ est alors la série de Dirichlet $\mathrm{L}(\chi, s) = \sum_{n\geqslant 1} \frac{\chi(n)}{n^s}$. Comme $|\chi(n)| = 1$, si $(n, \mathrm{D}) = 1$, l'abscisse de convergence absolue de $\mathrm{L}(\chi, s)$ est 1, et on a la proposition suivante.

Proposition VII.4.1. — *Soit χ un caractère de Dirichlet modulo* D.

(i) *Si* $\mathrm{Re}(s) > 1$, *alors* $\mathrm{L}(\chi, s) = \prod_{p\in\mathscr{P}} \frac{1}{1-\chi(p)p^{-s}}$, *et le produit est uniformément convergent sur tout demi-plan de la forme* $\mathrm{Re}(s) > c > 1$.

(ii) *Si* $\chi \neq \mathbf{1}_{\mathrm{D}}$, *l'abscisse de convergence de* $\mathrm{L}(\chi, s)$ *est* 0.

Démonstration. — Le (i) suit juste de la théorie générale (cf. prop. VII.3.1). Maintenant, si $\chi \neq \mathbf{1}_{\mathrm{D}}$, il existe $a \in (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$, tel que $\chi(a) \neq 1$. On a alors

$$\chi(a) \sum_{x\in(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*} \chi(x) = \sum_{x\in(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*} \chi(ax) = \sum_{x\in(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*} \chi(x),$$

puisque $x \mapsto ax$ est une bijection de $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$. On en déduit $\sum_{x\in(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*} \chi(x) = 0$, et donc $\sum_{n=k\mathrm{D}+1}^{(k+1)\mathrm{D}} \chi(n) = 0$ (on aurait pu aussi utiliser l'orthogonalité des caractères χ et $\mathbf{1}_{\mathrm{D}}$ de $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$). Ceci implique que la suite des sommes partielles $\sum_{k=1}^{n} \chi(k)$ est bornée (par D en valeur absolue), et permet d'utiliser le (i) du th. VII.1.5 pour démontrer le (ii).

2. Conducteur et sommes de Gauss

Si D' est un diviseur de D et χ est un caractère de Dirichlet modulo D', on peut aussi voir χ comme un caractère de Dirichlet modulo D en composant χ avec la projection $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^* \to (\mathbf{Z}/\mathrm{D}'\mathbf{Z})^*$. On dit que χ est *primitif*, si on ne peut pas trouver de diviseur D' de D, distinct de D, tel que χ provienne d'un caractère modulo D'. On dit que χ *est de conducteur* D, si c'est un caractère de Dirichlet modulo D qui est primitif. Si χ est de conducteur D et si N est un multiple de D, on note χ_{N} le caractère modulo N obtenu en composant χ avec la projection $(\mathbf{Z}/\mathrm{N}\mathbf{Z})^* \to (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$.

Lemme VII.4.2. — *On a* $\mathrm{L}(\chi_{\mathrm{N}}, s) = \mathrm{L}(\chi, s) \prod_{p|\mathrm{N}} (1 - \chi(p)p^{-s})$.

Démonstration. — Il suffit d'utiliser la décomposition en produit de facteurs d'Euler.

Comme $1-\chi(p)p^{-s}$ est une fonction holomorphe sur $\mathbf{C}$ ayant tous ses zéros sur la droite $\mathrm{Re}(s) = 0$, on voit que l'étude des propriétés analytiques des fonctions L de Dirichlet se ramène à celle des fonctions L associées aux caractères primitifs.

Si χ est un caractère de Dirichlet modulo D, on note $\overline{\chi}$ le caractère de Dirichlet modulo D défini par $\overline{\chi}(n) = \overline{\chi(n)}$ si $n \in (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$. Comme $\chi(n)$ est une racine de l'unité, on a aussi $\overline{\chi}(n) = \chi(n)^{-1}$.

Si D est un entier, si χ est un caractère de Dirichlet de conducteur D et si $n \in \mathbf{Z}$, on définit la somme de Gauss tordue $\mathrm{G}(\chi, n)$ par la formule

$$\mathrm{G}(\chi, n) = \sum_{a \bmod \mathrm{D}} \chi(a) e^{2i\pi \frac{na}{\mathrm{D}}},$$

et on pose $\mathrm{G}(\chi) = \mathrm{G}(\chi, 1)$.

Lemme VII.4.3. — *Si* $n \in \mathbf{N}$, *alors* $\mathrm{G}(\chi, n) = \overline{\chi}(n)\mathrm{G}(\chi)$

Démonstration. — Si $(n, \mathrm{D}) = 1$, alors n est inversible dans $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$, ce qui permet d'écrire

$$\mathrm{G}(\chi, n) = \sum_{a \bmod \mathrm{D}} \chi(a) e^{2i\pi \frac{na}{\mathrm{D}}} = \overline{\chi}(n) \sum_{an \bmod \mathrm{D}} \chi(an) e^{2i\pi \frac{na}{\mathrm{D}}} = \overline{\chi}(n)\mathrm{G}(\chi).$$

Si $(n, \mathrm{D}) = d > 1$, on peut écrire $\mathrm{D} = d\mathrm{D}'$ et $n = dn'$. Comme χ est de conducteur D, il existe $b \equiv 1 \bmod \mathrm{D}/d$ tel que $\chi(b) \neq 1$ (sinon χ serait de conducteur divisant D′). On a alors

$$e^{2i\pi \frac{nab}{\mathrm{D}}} = e^{2i\pi \frac{na}{\mathrm{D}}} e^{2i\pi \frac{n(b-1)a}{\mathrm{D}}} = e^{2i\pi \frac{na}{\mathrm{D}}},$$

puisque n est divisible par d et $b-1$ par D/d. On en déduit que

$$\chi(b)\mathrm{G}(\chi, n) = \sum_{a \bmod \mathrm{D}} \chi(ab) e^{2i\pi \frac{nab}{\mathrm{D}}} = \sum_{a \bmod \mathrm{D}} \chi(a) e^{2i\pi \frac{na}{\mathrm{D}}} = \mathrm{G}(\chi, n),$$

et donc, comme $\chi(b) \neq 1$, que $\mathrm{G}(\chi, n) = 0 = \overline{\chi}(n)\mathrm{G}(\chi)$. Ceci permet de conclure.

Théorème VII.4.4. — *Si χ est un caractère de Dirichlet de conducteur $\mathrm{D} \neq 1$, alors $\mathrm{L}(\chi, s)$ admet un prolongement analytique à $\mathbf{C}$ tout entier. De plus, $\mathrm{L}(\chi, s) = \mathrm{M}(f_\chi, s)$, où $f_\chi : \mathbf{R}_+ \to \mathbf{C}$ est donnée par la formule*

$$f_\chi(t) = \frac{1}{\mathrm{G}(\overline{\chi})} \sum_{b=1}^{\mathrm{D}-1} \frac{\overline{\chi}(b)}{e^{-\frac{2i\pi b}{\mathrm{D}}} e^t - 1}.$$

Démonstration. — Il résulte du lemme VII.2.4, que $\mathrm{L}(\chi, s) = \mathrm{M}(f, s)$, où f est définie par $f(t) = \sum_{n=1}^{+\infty} \chi(n) e^{-nt}$. Si on utilise l'identité [11] $\chi(n) = \frac{\mathrm{G}(\overline{\chi}, n)}{\mathrm{G}(\overline{\chi})}$ du lemme VII.4.3, on obtient

$$f(t) = \sum_{n=1}^{+\infty} \Big(\frac{1}{\mathrm{G}(\overline{\chi})} \sum_{b \bmod \mathrm{D}} \overline{\chi}(b) e^{2i\pi \frac{nb}{\mathrm{D}}} \Big) e^{-nt} = \frac{1}{\mathrm{G}(\overline{\chi})} \sum_{b=1}^{\mathrm{D}-1} \frac{\overline{\chi}(b)}{e^{-\frac{2i\pi b}{\mathrm{D}}} e^t - 1} = f_\chi(t).$$

(La dernière égalité venant de ce que $\chi(n) = 0$ si n est un multiple de D, ce qui fait que 0 mod D ne contribue pas à la somme). Maintenant, f_χ est à décroissance rapide à l'infini ainsi que toutes ses dérivées, et $e^{2i\pi \frac{nb}{\mathrm{D}}} \neq 1$, si $1 \leqslant b \leqslant \mathrm{D} - 1$, ce qui fait que f_χ est $\mathscr{C}^\infty$ sur $\mathbf{R}_+$. On conclut en utilisant la prop. VII.2.6.

3. Le théorème de la progression arithmétique

Proposition VII.4.5. — *$\mathrm{F}(s) = \prod_{\chi \in \mathrm{Dir}(\mathrm{D})} \mathrm{L}(\chi, s)$ est une série de Dirichlet à coefficients dans $\mathbf{N}$.*

Démonstration. — D'après le (i) de la prop. VII.4.1, si $\chi \in \mathrm{Dir}(\mathrm{D})$ et si $\mathrm{Re}(s) > 1$, alors $\mathrm{L}(\chi, s)$ est le produit (convergent) des $(1 - \chi(p)p^{-s})^{-1}$ pour p premier ne divisant pas D.

11. On a quand même besoin de vérifier que $\mathrm{G}(\overline{\chi}) \neq 0$ (cf. ex. VII.4.10).

On obtient donc

$$\mathrm{F}(s) = \prod_{p\nmid \mathrm{D}} \Big(\prod_{\chi\in \mathrm{Dir(D)}} (1-\chi(p)p^{-s})^{-1}\Big).$$

Maintenant, l'application $p \mapsto \chi(p)$ est un morphisme du groupe $\mathrm{Dir(D)}$ dans $\mathbf{C}^*$; son image est un sous-groupe fini de $\mathbf{C}^*$, et donc de la forme $\boldsymbol{\mu}_{d(p)}$, et son noyau est un sous-groupe H_p de $\mathrm{Dir(D)}$ dont on note $h(p)$ le cardinal. Si $\eta \in \boldsymbol{\mu}_{d(p)}$, il existe $h(p)$ éléments χ de $\mathrm{Dir(D)}$ tels que $\chi(p) = \eta$ (si χ_0 en est un, l'application $\chi' \mapsto \chi_0\chi'$ induit une bijection de H_p sur l'ensemble de ces χ). Il en résulte que

$$\prod_{\chi\in \mathrm{Dir(D)}} (1-\chi(p)p^{-s}) = \Big(\prod_{\eta\in\boldsymbol{\mu}_{d(p)}} (1-\eta\, p^{-s})\Big)^{h(p)},$$

et comme $\prod_{\eta\in\boldsymbol{\mu}_{d(p)}}(1-\eta \mathrm{X}) = 1-\mathrm{X}^{d(p)}$, on obtient

$$\mathrm{F}(s) = \prod_{p\nmid \mathrm{D}} \Big(\frac{1}{1-p^{-d(p)s}}\Big)^{h(p)}.$$

Le résultat suit de ce que $\frac{1}{1-p^{-d(p)s}} = 1 + p^{-d(p)s} + p^{-2d(p)s} + \cdots$ est une série de Dirichlet à coefficients dans $\mathbf{N}$, et un produit de séries de Dirichlet à coefficients dans $\mathbf{N}$ est une série de Dirichlet à coefficients dans $\mathbf{N}$.

Théorème VII.4.6. — (i) $\mathrm{L}(\mathbf{1}_\mathrm{D}, s)$ *a un pôle simple en* $s = 1$, *de résidu* $\frac{\varphi(\mathrm{D})}{\mathrm{D}}$.
(ii) *Si* $\chi \in \mathrm{Dir(D)} - \{\mathbf{1}_\mathrm{D}\}$, *alors* $\mathrm{L}(\chi, 1) \neq 0$.

Démonstration. — Compte-tenu de ce que ζ a un pôle simple en $s = 1$, de résidu 1 (th. VII.3.4), le (i) résulte des formules $\mathrm{L}(\mathbf{1}_\mathrm{D}, s) = \zeta(s)\prod_{p|\mathrm{D}}(1-p^{-s})$ (cf. lemme VII.4.2) et $\prod_{p|\mathrm{D}}(1-\frac{1}{p}) = \frac{\varphi(\mathrm{D})}{\mathrm{D}}$ (ex. 2.9 du Vocabulaire).

Maintenant, s'il existe $\chi \in \mathrm{Dir(D)} - \{\mathbf{1}_\mathrm{D}\}$, avec $\mathrm{L}(\chi, 1) = 0$, le zéro de $\mathrm{L}(\chi, s)$ compense le pôle simple de $\mathrm{L}(\mathbf{1}_\mathrm{D}, s)$; il s'ensuit que $\mathrm{F}(s) = \prod_{\chi\in\mathrm{Dir(D)}} \mathrm{L}(\chi, s)$ est holomorphe sur $\mathbf{C}$ tout entier. Comme $\mathrm{F}(s)$ est, d'après la prop. VII.4.5, une série de Dirichlet $\sum_{n\geqslant 1} a_n n^{-s}$ à coefficients dans $\mathbf{N}$ (et donc positifs), il résulte du th. de Landau (th. VII.1.1) que la série $\sum_{n\geqslant 1} a_n n^{-s}$ converge pour tout $s \in \mathbf{C}$ et donc, en particulier, pour $s = 0$. Comme les a_n appartiennent à $\mathbf{N}$, cela implique que seul un nombre fini d'entre eux sont non nuls, ce qui est clairement absurde (par exemple parce que le coefficient de $p^{-d(p)s}$ est $h(p)$ et qu'il y a une infinité de nombres premiers).

On en déduit le (ii), ce qui termine la démonstration.

Théorème VII.4.7. — (Dirichlet, 1837) *Si* $(a, \mathrm{D}) = 1$, *il y a une infinité de nombres premiers de la forme* $a + n\mathrm{D}$, *avec* $n \in \mathbf{N}$.

Démonstration. — Soit $\phi_a : (\mathbf{Z}/\mathrm{D}\mathbf{Z})^* \to \mathbf{C}$ la fonction valant 1 en a et 0 ailleurs. Il s'agit de prouver que $\{p,\ \phi_a(p) = 1\}$ est infini et, pour ce faire, nous allons prouver que $\lim_{s\to 1^+} \mathrm{F}_a(s) = +\infty$, où $\mathrm{F}_a(s) = \sum_p \phi_a(p)p^{-s}$; ceci montrera non seulement que l'ensemble des p de la forme $a + n\mathrm{D}$ est infini, mais aussi que ces nombres premiers sont

assez denses dans les entiers puisque la somme de leurs inverses diverge [cette stratégie est inspirée de la démonstration d'Euler de l'existence d'une infinité de nombres premiers (rem. VII.3.5)].

Il résulte de la prop. I.2.26 que, si $p \nmid \mathrm{D}$, alors $\phi_a(p) = \frac{1}{\varphi(\mathrm{D})} \sum_{\chi \in \mathrm{Dir}(\mathrm{D})} \overline{\chi}(a)\chi(p)$, et donc

$$\mathrm{F}_a(s) = \frac{1}{\varphi(\mathrm{D})} \sum_{\chi \in \mathrm{Dir}(\mathrm{D})} \overline{\chi}(a) \sum_{p \nmid \mathrm{D}} \chi(p) p^{-s}, \quad \text{si } s \text{ est réel} > 1.$$

Maintenant, $|\chi(p)p^{-s}| \leqslant \frac{1}{2}$, si $p \in \mathscr{P}$ et $s > 1$, et comme

$$|z + \log(1-z)| \leqslant \frac{|z|^2}{2} + \frac{|z|^3}{3} + \cdots \leqslant \frac{1}{2} \frac{|z|^2}{1-|z|} \leqslant |z|^2, \quad \text{si } |z| \leqslant \frac{1}{2},$$

il en résulte que

$$\Big| \sum_{p \nmid \mathrm{D}} \big(\chi(p)p^{-s} + \log(1 - \chi(p)p^{-s}) \big) \Big| \leqslant \sum_{p \nmid \mathrm{D}} p^{-2s} \leqslant \zeta(2), \quad \text{si } s > 1.$$

La fonction $-\sum_{p \nmid \mathrm{D}} \log(1 - \chi(p)p^{-s})$ est continue sur $]1, +\infty]$ comme restriction d'une fonction holomorphe, et son exponentielle est $\mathrm{L}(\chi, s)$ d'après le (i) de la prop. VII.4.1 ; il est donc justifié de la noter $\log \mathrm{L}(\chi, s)$. Il résulte alors de la majoration ci-dessus que $\mathrm{F}_a(s) - \frac{1}{\varphi(\mathrm{D})} \sum_{\chi \in \mathrm{Dir}(\mathrm{D})} \overline{\chi}(a) \log \mathrm{L}(\chi, s)$ reste bornée quand $s \to 1^+$. Or le (ii) du th. VII.4.6 et la continuité de $\log \mathrm{L}(\chi, s)$ pour $s > 1$ impliquent que la somme $\sum_{\chi \neq \mathbf{1}_\mathrm{D}} \overline{\chi}(a) \log \mathrm{L}(\chi, s)$ admet une limite finie en 1^+, tandis que $\log \mathrm{L}(\mathbf{1}_\mathrm{D}, s)$ tend vers $+\infty$ en 1^+ d'après le (i) du th. VII.4.6, et donc $\mathrm{F}_a(s) \to +\infty$ en 1^+, puisque $\mathbf{1}_\mathrm{D}(a) = 1$, ce que l'on cherchait à démontrer. (En utilisant toute la force du (i) du th. VII.4.6, on montre plus précisément que $\lim_{s \to 1^+} \frac{\mathrm{F}_a(s)}{\log(s-1)} = \frac{1}{\varphi(\mathrm{D})}$.)

4. Équation fonctionnelle des fonctions L de Dirichlet

Théorème VII.4.8. — *Si χ est un caractère de Dirichlet de conducteur $\mathrm{D} \neq 1$, alors $\mathrm{L}(\chi, s)$ vérifie l'équation fonctionnelle*

$$\mathrm{L}(\chi, s) = \begin{cases} 2 \cdot \mathrm{G}(\chi) \cdot \mathrm{D}^{-s} \cdot (2\pi)^{s-1} \cdot \Gamma(1-s) \cdot \sin \frac{\pi s}{2} \cdot \mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = 1, \\ -2i \cdot \mathrm{G}(\chi) \cdot \mathrm{D}^{-s} \cdot (2\pi)^{s-1} \cdot \Gamma(1-s) \cdot \cos \frac{\pi s}{2} \cdot \mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = -1. \end{cases}$$

Démonstration. — La démonstration est très semblable à celle de l'équation fonctionnelle de la fonction ζ, et nous reprenons les notations de cette dernière en indiquant les points où l'argument diffère. Soit $\mathrm{F}_c(\chi, s) = \frac{1}{2i\pi} \int_{\gamma_c} f_\chi(z)(-z)^s \frac{dz}{z}$, où f_χ est la fonction définie dans le th. VII.4.4. Comme $f_\chi(z)$ est à décroissance rapide à l'infini, la fonction $\mathrm{F}_c(\chi, s)$ est holomorphe sur $\mathbf{C}$ pour tout c qui n'est pas de la forme $\frac{2\pi b}{\mathrm{D}} + 2\pi k$, avec $k \in \mathbf{N}$ et $b \leqslant \mathrm{D}$ premier à D (pour éviter les pôles de f_χ). Comme f_χ n'a pas de pôle à l'intérieur du carré de sommets $\frac{2\pi}{\mathrm{D}}(\pm 1 \pm i)$, on a $\mathrm{F}_c(\chi, s) = \mathrm{F}_{\pi/\mathrm{D}}(\chi, s)$, quel que soit $c \in]0, \frac{2\pi}{\mathrm{D}}[$. En

faisant tendre c vers 0, on en déduit, si $\mathrm{Re}(s) > 1$, la formule

$$\mathrm{F}_{\pi/\mathrm{D}}(\chi, s) = \frac{1}{2i\pi}\Big(e^{-i\pi s}\int_{+\infty}^{0} f_\chi(t)t^s\,\frac{dt}{t} + e^{i\pi s}\int_0^{+\infty} f_\chi(t)t^s\,\frac{dt}{t}\Big) = \frac{\sin\pi s}{\pi}\cdot\Gamma(s)\cdot\mathrm{L}(\chi, s).$$

Maintenant, quand N tend vers $+\infty$, la fonction $\mathrm{F}_{\mathrm{N}\pi}(\chi, s)$ tend vers 0 quand $\mathrm{Re}(s) < 0$. La différence entre $\mathrm{F}_{\pi/\mathrm{D}}(s)$ et $\mathrm{F}_{\mathrm{N}\pi}(s)$ peut se calculer grâce au théorème des résidus. La fonction $f_\chi(z)\frac{(-z)^s}{z}$ a des pôles en les $z = \pm\frac{2i\pi k}{\mathrm{D}}$, avec $1 \leqslant k \leqslant \mathrm{ND}-1$ dans le contour délimité par la différence entre $\gamma_{\mathrm{N}\pi}$ et $\gamma_{\pi/\mathrm{D}}$. Si $1 \leqslant k \leqslant \mathrm{ND}-1$, on a

$$\mathrm{Res}\big(f_\chi(z)\frac{(-z)^s}{z}, \frac{2i\pi k}{\mathrm{D}}\big) = \frac{\overline{\chi}(k)}{\mathrm{G}(\overline{\chi})}\frac{(-2i\pi k/\mathrm{D})^s}{(2i\pi k/\mathrm{D})} = -\frac{\overline{\chi}(k)}{\mathrm{G}(\overline{\chi})}\cdot\big(\frac{2\pi k}{\mathrm{D}}\big)^{s-1}e^{-i\pi\frac{s-1}{2}}$$
$$\mathrm{Res}\big(f_\chi(z)\frac{(-z)^s}{z}, \frac{-2i\pi k}{\mathrm{D}}\big) = \frac{\overline{\chi}(-k)}{\mathrm{G}(\overline{\chi})}\frac{(2i\pi k/\mathrm{D})^s}{(-2i\pi k/\mathrm{D})} = -\frac{\overline{\chi}(-k)}{\mathrm{G}(\overline{\chi})}\cdot\big(\frac{2\pi k}{\mathrm{D}}\big)^{s-1}e^{i\pi\frac{s-1}{2}}$$

On obtient donc

$$\mathrm{F}_{\mathrm{N}\pi}(\chi, s) - \mathrm{F}_{\pi/\mathrm{D}}(\chi, s) = \frac{-1}{\mathrm{G}(\overline{\chi})}\sum_{k=1}^{\mathrm{ND}-1}\big(\frac{2\pi k}{\mathrm{D}}\big)^{s-1}\big(\overline{\chi}(k)e^{-i\pi\frac{s-1}{2}} + \overline{\chi}(-k)e^{i\pi\frac{s-1}{2}}\big).$$

En faisant tendre N vers $+\infty$, on en déduit, si $\mathrm{Re}(s) < 0$, les formules

$$\mathrm{F}_{\pi/\mathrm{D}}(\chi, s) = \frac{1}{\mathrm{G}(\overline{\chi})}\begin{cases}\big(\frac{2\pi}{\mathrm{D}}\big)^{s-1}\cdot\big(2\cos\pi\frac{s-1}{2}\big)\cdot\mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = 1,\\ \big(\frac{2\pi}{\mathrm{D}}\big)^{s-1}\cdot\big(-2i\sin\pi\frac{s-1}{2}\big)\cdot\mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = -1.\end{cases}$$

On en tire l'équation fonctionnelle

$$\sin\pi s\cdot\Gamma(s)\cdot\mathrm{L}(\chi, s) = \frac{1}{\mathrm{G}(\overline{\chi})}\begin{cases}(2\pi)^s\cdot\mathrm{D}^{1-s}\cdot\cos\pi\frac{s-1}{2}\cdot\mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = 1,\\ -i(2\pi)^s\cdot\mathrm{D}^{1-s}\cdot\sin\pi\frac{s-1}{2}\cdot\mathrm{L}(\overline{\chi}, 1-s) & \text{si } \chi(-1) = -1,\end{cases}$$

qui peut aussi se mettre sous la forme

$$\mathrm{L}(\overline{\chi}, 1-s) = \begin{cases}2\mathrm{G}(\overline{\chi})\cdot(2\pi)^{-s}\cdot\mathrm{D}^{s-1}\cdot\sin\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot\mathrm{L}(\chi, s) & \text{si } \chi(-1) = 1,\\ -2i\mathrm{G}(\overline{\chi})\cdot(2\pi)^{-s}\cdot\mathrm{D}^{s-1}\cdot\cos\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot\mathrm{L}(\chi, s) & \text{si } \chi(-1) = -1.\end{cases}$$

L'équation fonctionnelle du théorème s'obtient en appliquant l'équation fonctionnelle ci-dessus à $\overline{\chi}$ au lieu de χ et $1-s$ au lieu de s.

Remarque VII.4.9. — (i) Si χ est un caractère de Dirichlet de conducteur $\mathrm{D} \neq 1$, posons

$$w(\chi) = \begin{cases}\frac{\mathrm{G}(\chi)}{\sqrt{\mathrm{D}}} & \text{si } \chi(-1) = 1,\\ \frac{\mathrm{G}(\chi)}{i\sqrt{\mathrm{D}}} & \text{si } \chi(-1) = -1,\end{cases}$$
$$\Lambda(\chi, s) = \begin{cases}\Gamma(\frac{s}{2})\cdot\big(\frac{\mathrm{D}}{\pi}\big)^{s/2}\cdot\mathrm{L}(\chi, s) & \text{si } \chi(-1) = 1,\\ \Gamma(\frac{s+1}{2})\cdot\big(\frac{\mathrm{D}}{\pi}\big)^{(s+1)/2}\cdot\mathrm{L}(\chi, s) & \text{si } \chi(-1) = -1.\end{cases}$$

Un petit calcul permet de déduire de l'équation fonctionnelle de $\mathrm{L}(\chi, s)$ que $\Lambda(\chi, s)$ vérifie

l'équation fonctionnelle

$$\Lambda(\chi, s) = w(\chi)\Lambda(\overline{\chi}, 1-s).$$

(ii) La fonction $\mathrm{L}(\chi, s)$ est holomorphe sur $\mathbf{C}$ tout entier et ne s'annule pas sur le demi-plan $\mathrm{Re}(s) > 1$ sur lequel elle est donnée (prop. VII.4.1) par un produit absolument convergent dont aucun des termes ne s'annule. Elle ne s'annule pas non plus sur la droite $\mathrm{Re}(s) = 1$ (cf. ex. A.4.4), ce qui est nettement plus profond. L'équation fonctionnelle du th. VII.4.8 montre donc que, en dehors de la bande $0 < \mathrm{Re}(s) < 1$, les seuls zéros de $\mathrm{L}(\chi, s)$ sont des zéros (dit triviaux) aux entiers négatifs pairs (resp. impairs), si $\chi(-1) = 1$ (resp. $\chi(-1) = -1$). On conjecture (*hypothèse de Riemann généralisée*, GRH en abréviation anglaise) que tous les zéros de $\mathrm{L}(\chi, s)$ dans la bande $0 < \mathrm{Re}(s) < 1$ se trouvent sur la droite $\mathrm{Re}(s) = \frac{1}{2}$. Ceci aurait des implications profondes sur la répartition des nombres premiers entre les différentes progressions arithmétiques [12].

Exercice VII.4.10. — Soit χ un caractère de conducteur $\mathrm{D} \neq 1$. Montrer que :

$$\overline{\mathrm{G}(\chi)} = \chi(-1)\mathrm{G}(\overline{\chi}),\ \mathrm{G}(\chi)\mathrm{G}(\overline{\chi}) = \chi(-1)\mathrm{D} \ \text{ et } \ |w(\chi)| = 1.$$

Exercice VII.4.11. — On s'intéresse au nombre $r(n)$ de manière d'écrire un entier n comme une somme de deux carrés : $r(n) = |\{(x,y) \in \mathbf{Z}^2,\ x^2+y^2 = n\}|$. Soit $\mathrm{A} = \mathbf{Z}[i]$, et si $a = x+iy$, soit [13] $\mathrm{N}(a) = x^2+y^2$. D'après l'ex. 4.4, on dispose des résultats suivants :

- $\mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$, pour tous $a, b, \in \mathrm{A}$;
- tout élément a de $\mathrm{A}-\{0\}$ admet une unique factorisation $a = u(1+i)^{k_2} \prod_{p\equiv 1 \bmod 4} q_{p,1}^{k_{p,1}} q_{p,2}^{k_{p,2}} \prod_{p\equiv 3 \bmod 4} p^{k_p}$,

où $u \in \{1, -1, i, -i\}$, les k_p et les $k_{p,i}$ sont des entiers $\geqslant 0$, et $\mathrm{N}(q_{p,1}) = \mathrm{N}(q_{p,2}) = p$.

(i) Montrer que

$$\sum_{n\geqslant 1} \frac{r(n)}{n^s} = \sum_{a\in \mathrm{A}-\{0\}} \frac{1}{\mathrm{N}(a)^s} = 4\,\frac{1}{1-2^{-s}} \prod_{p\equiv 1 \bmod 4} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv 3 \bmod 4} \frac{1}{1-p^{-2s}} \quad \text{si } \mathrm{Re}(s) > 1.$$

$$r(n) = \begin{cases} 0, & \text{si } v_p(n) \text{ est impair pour au moins un } p \text{ de la forme } 4n+3, \\ 4 \prod_{p\equiv 1 \bmod 4} (v_p(n)+1), & \text{si } v_p(n) \text{ est pair pour tout } p \text{ de la forme } 4n+3. \end{cases}$$

(ii) Soit $\chi : (\mathbf{Z}/4\mathbf{Z})^* \to \{\pm 1\}$ le caractère de Dirichlet défini par $\chi(1) = 1$ et $\chi(-1) = -1$. Montrer que $\sum_{n\geqslant 1} \frac{r(n)}{n^s} = 4\zeta(s)\mathrm{L}(\chi, s)$; en déduire que $r(n) = 4\sum_{d|n} \chi(d)$.

---

12. En particulier, sur la taille du plus petit nombre premier dans une progression arithmétique, ce qui intervient naturellement dans beaucoup de questions ; par exemple en cryptographie.

13. On a $\mathrm{N}(a) = |\mathrm{A}/a|$ (voir plus loin), ce qui fait que la fonction $\sum_{a\in \mathrm{A}-\{0\}} \frac{1}{\mathrm{N}(a)^s}$ est, à un facteur $4 = |\mathrm{A}^*|$ près, la fonction $\zeta_{\mathrm{A}}(s)$ apparaissant dans l'introduction de l'annexe G. Si on identifie $\mathbf{C}$ à $\mathbf{R}^2$ via $z = x + iy \mapsto (x, y)$, alors A et aA deviennent des réseaux : A devient le réseau $\mathbf{Z}^2$ dont le volume est 1 et, si $a = x + iy$, alors aA est le réseau de base $a = (x, y)$ et $ia = (-y, x)$ dont le volume est le déterminant de a et ia, c'est-à-dire, $x^2+y^2 = \mathrm{N}(a)$. Par ailleurs, $(\mathbf{C}/a\mathrm{A})/(\mathrm{A}/a\mathrm{A}) = \mathbf{C}/\mathrm{A}$. Autrement dit, si D est un domaine fondamental de $\mathbf{C}$ modulo A et si S est un système de représentants de $\mathrm{A}/a\mathrm{A}$, alors les $s + \mathrm{D}$, pour $s \in \mathrm{S}$, sont disjoints deux à deux et leur réunion est un domaine fondamental de $\mathbf{C}/a\mathrm{A}$. Comme $\mathrm{Vol}(\Lambda)$ est le volume d'un domaine fondamental modulo Λ, pour tout réseau Λ, on en déduit que $|\mathrm{Vol}(a\mathrm{A})| = |\mathrm{A}/a\mathrm{A}| \cdot \mathrm{Vol}(\mathrm{A})$, et donc $\mathrm{N}(a) = |\mathrm{A}/a\mathrm{A}|$.

VII.5. Autres exemples

1. La fonction de Moebius

Soit μ la *fonction de Moebius*. Elle est définie par $\mu(n) = 0$ si n est divisible par le carré d'au moins un nombre premier, et $\mu(n) = (-1)^r$, si $n = p_1 \cdots p_r$, où les p_i sont des nombres premiers distincts. C'est une fonction multiplicative, et on a

$$\zeta(s)^{-1} = \prod_{p\in\mathscr{P}} (1 - p^{-s}) = \sum_{n\in\mathbf{N}} \mu(n) n^{-s} = \mathrm{L}(\mu, s).$$

On en déduit que $\mathrm{L}(\mu, s)$ a un prolongement méromorphe à tout le plan complexe. Il est facile de voir que son abscisse de convergence absolue σ_{abs} est 1, mais son abscisse de convergence σ_{conv} est inconnue. On conjecture que $\sigma_{\mathrm{conv}} = \frac{1}{2}$, mais c'est équivalent à l'hypothèse de Riemann (cf. n° 2 du § A.5).

Exercice VII.5.1. — (Formule d'inversion de Moebius)

(i) Montrer que $\sum_{d|n} \mu(d) = 0$, si $n \geqslant 2$.

(ii) Soit $\mathrm{F} : [0, +\infty[\to \mathbf{C}$, vérifiant $\mathrm{F}(x) = 0$, si $x < 1$, et soit $\mathrm{G} : [0, +\infty[\to \mathbf{C}$ définie par $\mathrm{G}(x) = \sum_{n=1}^{+\infty} \mathrm{F}(\frac{x}{n})$. Montrer que $\mathrm{G}(x) = 0$, si $x < 1$, et que $\mathrm{F}(x) = \sum_{n=1}^{+\infty} \mu(n)\mathrm{G}(\frac{x}{n})$.

(iii) Montrer que $\sum_{n=1}^{+\infty} \mu(n)[\frac{x}{n}] = 1$, si $x \geqslant 1$.

Exercice VII.5.2. — (Critère de Báez-Duarte)

Soit E l'espace de Hilbert, séparé de l'espace $\mathscr{L}^2([1, +\infty[, \frac{dt}{t^2})$ des $\phi : [1, +\infty[\to \mathbf{C}$ telles que $t \mapsto t^{-1}\phi(t)$ soit de carré sommable, muni du produit scalaire $\langle f, g\rangle = \int_0^{+\infty} \overline{f(t)} g(t) \frac{dt}{t^2}$.

(i) Vérifier que $t \mapsto t^{1-s}$ appartient à E, si $\mathrm{Re}(s) > \frac{1}{2}$, et qu'il en est de même de ϕ_n, définie par $\phi_n(t) = [\frac{t}{n}] - \frac{[t]}{n}$, si n est un entier $\geqslant 2$.

(ii) Montrer que $\int_1^{+\infty} \{t\} t^{-s-1}\, dt = \frac{1}{s-1} - \frac{\zeta(s)}{s}$, si $\mathrm{Re}(s) > 1$.

(iii) Montrer que $s \mapsto \int_1^{+\infty} \{t\} t^{-s-1}\, dt$ est holomorphe sur le demi-plan $\mathrm{Re}(s) > 0$. En déduire que $\int_0^{+\infty} \{t\} t^{-s-1}\, dt = -\frac{\zeta(s)}{s}$, si $0 < \mathrm{Re}(s) < 1$.

(iv) Montrer que $\langle t^{1-s}, \phi_n\rangle = \left(\frac{1}{n^s} - \frac{1}{n}\right) \frac{\zeta(s)}{s}$, si $n \geqslant 2$, et si $\mathrm{Re}(s) > \frac{1}{2}$.

(v) En déduire que si l'adhérence dans E du sous-espace engendré par les ϕ_n, pour $n \geqslant 2$, contient les fonctions constantes sur $[1, +\infty[$, alors l'hypothèse de Riemann est vraie [14].

2. La fonction τ de Ramanujan

La *fonction τ de Ramanujan*. Elle est définie par l'identité

$$q \prod_{n=1}^{+\infty} (1 - q^n)^{24} = \sum_{n=1}^{+\infty} \tau(n) q^n.$$

S. Ramanujan a fait deux conjectures à son sujet. La première, démontrée peu après par L. Mordell (1917),

14. On peut montrer, mais c'est plus difficile, que si l'hypothèse de Riemann est vraie, alors l'adhérence dans E du sous-espace engendré par les ϕ_n, pour $n \geqslant 2$, contient les fonctions constantes sur $[1, +\infty[$. Il s'agit d'une variante, due à Báez-Duarte (2003), du critère de Nyman-Beurling (1955). Il est à noter que la question (iii) de l'ex. VII.5.1 et la formule $\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} = \zeta(1)^{-1} = 0$, permettent de montrer que $\sum_{n=1}^{+\infty} \frac{\mu(n)}{n} \phi_n(t) = -1$, si $t \geqslant 1$, mais la série ne converge probablement pas dans E. La convergence de la série $\sum_{n=1}^{+\infty} \frac{\mu(n)}{n}$ est plus délicate qu'il n'y paraît ; elle est plus ou moins équivalente à la non annulation de la fonction ζ sur la droite $\mathrm{Re}(s) = 1$.

peut s'énoncer sous la forme

$$\mathrm{L}(\tau, s) = \prod_{p \in \mathscr{P}} \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}}.$$

En particulier, τ est une fonction multiplicative ! Sa démonstration repose sur le fait que, si $q = e^{2i\pi z}$, alors $z \mapsto \Delta(z) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$ est une forme modulaire de poids 12 pour $\mathbf{SL}_2(\mathbf{Z})$ (cf. ex. VII.6.3 et VII.6.11).

La seconde conjecture de Ramanujan affirme que *les pôles du facteur d'Euler en p de la fonction* $\mathrm{L}(\tau, s)$ *sont tous sur la droite* $\mathrm{Re}(s) = \frac{11}{2}$. Elle peut aussi s'énoncer sous la forme $|\tau(p)| \leqslant 2p^{11/2}$, si $p \in \mathscr{P}$. Il a fallu attendre 1973 pour que P. Deligne démontre la conjecture de Ramanujan (généralisée sous le nom de *conjecture de Ramanujan-Petersson* aux formes modulaires quelconques) comme conséquence de sa démonstration (qui lui a valu la médaille Fields en 1978) de *l'hypothèse de Riemann pour les variétés sur les corps finis*, conjecturée par A. Weil vers la fin des années 1940. La démonstration de Deligne est l'aboutissement d'un énorme programme mis sur pied par A. Grothendieck entre 1958 et 1964, et qui a totalement révolutionné la géométrie algébrique.

D'après le résultat de Deligne, $\tau'(p) = \frac{\tau(p)}{2\,p^{11/2}} \in [-1, 1]$, et la question se pose de savoir comment les $\tau'(p)$ se répartissent dans cet intervalle. La réponse est fournie par la conjecture de Sato-Tate, qui date de 1960 et vient d'être démontrée (en 2009), par M. Harris et R. Taylor (avec l'aide de L. Clozel, N. Sheperd-Barron, T. Barnet-Lamb, D. Geraghty...). Dans le cas particulier de la fonction τ de Ramanujan cette conjecture affirme que les $\tau'(p)$ sont équirépartis dans $[-1, 1]$ par rapport à la mesure $\frac{2\sqrt{1-t^2}}{\pi}\,dt$; autrement dit, si $-1 \leqslant a \leqslant b \leqslant 1$,

$$\lim_{x\to+\infty} \frac{|\{p \leqslant x,\ a \leqslant \tau'(p) \leqslant b\}|}{|\{p \leqslant x\}|} = \frac{2}{\pi}\int_a^b \sqrt{1-t^2}\,dt.$$

VII.6. Formes modulaires

Les exercices qui suivent explorent certaines propriétés des formes modulaires, qui possèdent tellement de symétries qu'elles ne devraient pas exister, mais se retrouvent, un peu inexplicablement, jouer un rôle dans les questions les plus variées (cf. note 2 du chap. I, ou note 1 de l'annexe C, par exemple). Ils sont l'occasion d'utiliser les résultats des chapitres précédents en démontrant une série de jolis résultats comme le théorème des 4 carrés (le problème H.11 offre une voie différente pour démontrer beaucoup des résultats qui suivent [15]).

Soit $\mathscr{H} = \{z,\ \mathrm{Im}(z) > 0\}$ le demi-plan de Poincaré. On rappelle (ex. VI.3.4) que si $f : \mathscr{H} \to \mathbf{C}$ est holomorphe et périodique de période 1, alors il existe une suite $(a_n(f))_{n\in\mathbf{Z}}$ de nombres complexes telle que l'on ait $f(z) = \sum_{n\in\mathbf{Z}} a_n(f)e^{2i\pi nz}$, quel que soit $z \in \mathscr{H}$. Il est d'usage de poser $e^{2i\pi z} = q$ et d'appeler *q-développement* de f la série $\sum_{n\in\mathbf{Z}} a_n(f)\,q^n$. On définit alors $v_\infty(f) \in \mathbf{Z}\cup\{\pm\infty\}$ comme l'inf. de l'ensemble des n tels que $a_n(f) \neq 0$ (en particulier, $v_\infty(f) = +\infty$ si et seulement si $f = 0$).

Si $k \in \mathbf{Z}$, une *fonction modulaire de poids k* est une fonction holomorphe f sur $\mathscr{H}$, et qui vérifie :

- $f(z+1) = f(z)$, quel que soit $z \in \mathscr{H}$,
- $f(z) = z^{-k}f(-1/z)$, quel que soit $z \in \mathscr{H}$,
- $v_\infty(f) > -\infty$.

Si $v_\infty(f) \geqslant 0$, on dit que f est une *forme modulaire de poids k*, et si $v_\infty(f) > 0$, on dit que f est parabolique (ou cuspidale).

15. Il est conseillé de commencer par les prob. H.8 et H.11 avant de s'attaquer à la série d'exercices qui suit : les méthodes sont assez semblables et les problèmes sont corrigés.

Soit Ω l'ouvert $\{z \in \mathscr{H},\ |z| > 1 \text{ et } -\frac{1}{2} < \mathrm{Re}(z) < \frac{1}{2}\}$. Si $a, b \in \mathscr{H}$ vérifient $|a| = |b| = 1$, et si C^+ est le demi-cercle de centre 0 et rayon 1 contenu dans $\mathscr{H}$, on note $\mathrm{A}(a,b)$ l'arc de C^+ allant de a à b. Soit $\alpha = e^{i\pi/3}$. Le bord $\partial\Omega$ de Ω est alors la réunion des demi-droites verticales $[\alpha, \alpha + i\infty)$ et $[\alpha^2, \alpha^2 + i\infty)$, et de l'arc de cercle $\mathrm{A}(\alpha^2, \alpha)$. On note D la réunion de Ω, de la demi-droite $[\alpha, \alpha + i\infty)$ et de l'arc de cercle $\mathrm{A}(i, \alpha)$.

Exercice VII.6.1. — (formule $\frac{k}{12}$) Soit f une forme modulaire de poids k non nulle. Le but de cet exercice est de prouver la formule suivante.

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\alpha(f) + \sum_{z \in \mathrm{D} - \{i,\alpha\}} v_z(f) = \frac{k}{12}.$$

(i) On suppose que f ne s'annule pas sur $\partial\Omega$. Si $\mathrm{T} \geqslant 2$, soit γ_T le lacet composé des segments $[\alpha, \alpha + i\mathrm{T}]$, $[\alpha + i\mathrm{T}, \alpha^2 + i\mathrm{T}]$, $[\alpha^2 + i\mathrm{T}, \alpha^2]$, et de l'arc de cercle $\mathrm{A}(\alpha^2, \alpha)$. On note $\frac{df}{f}$ la 1-forme [16] $\frac{f'(z)}{f(z)}\,dz$.

- Montrer que $\frac{1}{2i\pi}\int_{[\alpha+i\mathrm{T}, \alpha^2+i\mathrm{T}]} \frac{df}{f}$ tend vers $-v_\infty(f)$ quand $\mathrm{T} \to +\infty$.
- Montrer que $\int_{[\alpha, \alpha+i\mathrm{T}]} \frac{df}{f} + \int_{[\alpha^2+i\mathrm{T}, \alpha^2]} \frac{df}{f} = 0$.
- Montrer que $\int_{\mathrm{A}(\alpha^2, i)} \frac{df}{f} = -\int_{\mathrm{A}(i,\alpha)} \left(\frac{df}{f} + \frac{k}{z}\,dz\right)$. En déduire que $\frac{1}{2i\pi}\int_{\mathrm{A}(\alpha^2,\alpha)} \frac{df}{f} = \frac{k}{12}$.
- Montrer que $v_\infty(f) + \sum_{z \in \Omega} v_z(f) = \frac{k}{12}$.

(ii) Montrer que, si on ne suppose pas que f ne s'annule pas sur $\partial\Omega$, alors

$$v_\infty(f) + \sum_{z \in \Omega} v_z(f) + \frac{1}{2}\sum_{z \in \partial\Omega - \{\alpha, \alpha^2\}} v_z(f) + \frac{1}{6}(v_\alpha(f) + v_{\alpha^2}(f)) = \frac{k}{12}.$$

(Si f s'annule en $z \in \partial\Omega$, modifier le chemin γ_T au voisinage de z en le remplaçant par un arc de cercle, à l'intérieur de Ω, de centre z et de rayon tendant vers 0.)

(iii) Conclure.

La « formule $\frac{k}{12}$ » a beaucoup de conséquences intéressantes. En voici quelques-unes ; d'autres se trouvent dans les ex. VII.6.8 et VII.6.10.

Exercice VII.6.2. — (Dimension des espaces de formes modulaires [17])

(i) Montrer qu'une forme modulaire de poids 0 est constante.

(ii) Montrer qu'il n'y a pas [18] de forme modulaire de poids 2 ou de poids impair.

(iii) Montrer que l'ensemble M_k des formes modulaires de poids k est un espace vectoriel et que $f \mapsto (a_n(f))_{0 \leqslant n \leqslant \frac{k}{12}}$ est une application linéaire injective de M_k dans $\mathbf{C}^{d(k)}$, avec $d(k) = 1 + [\frac{k}{12}]$. En déduire que M_k est de dimension finie et que $\dim \mathrm{M}_k \leqslant 1 + [\frac{k}{12}]$.

Exercice VII.6.3. — (fonction L d'une forme modulaire)

Soit $\mathrm{Y} = \{z \in \mathbf{C},\ \mathrm{Im}(z) \geqslant \frac{1}{2},\ |\mathrm{Re}(z)| \leqslant \frac{1}{2}\}$. Soit $f = \sum_{n=1}^{+\infty} a_n q^n$ une forme modulaire parabolique de poids $2k$, et soit $\mathrm{F}(z) = \mathrm{Im}(z)^k |f(z)|$.

(i) Montrer qu'il existe $\mathrm{M} > 0$ tel que $|\mathrm{F}(z)| \leqslant \mathrm{M}$, quel que soit $z \in \mathrm{Y}$.

(ii) Montrer que $\mathrm{F}(z+1) = \mathrm{F}(z)$ et $\mathrm{F}(-1/z) = \mathrm{F}(z)$.

(iii) Montrer que, si $|\mathrm{Re}(z_0)| \leqslant \frac{1}{2}$ et si $0 < \mathrm{Im}(z_0) \leqslant \frac{1}{2}$, alors il existe z_1 vérifiant $|\mathrm{Re}(z_1)| \leqslant \frac{1}{2}$, $\mathrm{Im}(z_1) \geqslant 2\mathrm{Im}(z_0)$, et $\mathrm{F}(z_1) = \mathrm{F}(z_0)$. En déduire que $\mathrm{F}(z) \leqslant \mathrm{M}$, quel que soit z vérifiant $|\mathrm{Re}(z)| \leqslant \frac{1}{2}$.

---

16. On remarquera que $\frac{h'}{h} = \frac{f'}{f} + \frac{g'}{g}$ si $h = fg$ et que $\frac{h'}{h} = \left(\frac{f'}{f} \circ \varphi\right)\varphi'$ si $h = f \circ \varphi$, et on aura à utiliser l'ex. V.4.5 pour faire les calculs.

17. Le lecteur trouvera des compléments dans l'ex. VII.6.12.

18. Ce résultat intervient de manière cruciale dans la démonstration de Wiles du théorème de Fermat.

(iv) Montrer que $a_n = \int_{-1/2}^{1/2} f(x+\frac{i}{n}) e^{-2i\pi(nx+i)}\,dx$. En déduire que $|a_n| \leqslant e^{2\pi} \mathrm{M}\, n^k$.

(v) Soit $\mathrm{L}(f,s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$. Montrer que $\mathrm{L}(f,s)$ a une abscisse de convergence finie, possède un prolongement analytique à $\mathbf{C}$ tout entier, que $\mathrm{L}(f,-n)=0$, si $n \in \mathbf{N}$, et que $\Lambda(f,s) = \frac{\Gamma(s)}{(2\pi)^s}\mathrm{L}(f,s)$ vérifie l'équation fonctionnelle $\Lambda(f,s) = (-1)^k \Lambda(f, 2k-s)$. (On s'intéressera à $\int_0^{+\infty} f(iy) y^s \,\frac{dy}{y}$.)

L'exercice suivant montre que l'on n'est pas en train de faire la théorie de l'ensemble vide (dont les éléments ont, comme chacun sait, beaucoup de propriétés mirifiques...).

Exercice VII.6.4. — (Séries d'Eisenstein)

(i) Montrer que $|mz+n| \geqslant \inf(y, \frac{y}{|z|}) \sup(|m|,|n|)$, si $z = x+iy \in \mathscr{H}$ et $m, n \in \mathbf{Z}$.

(ii) Montrer que, si $k \geqslant 3$, la série $\sum_{(m,n)\in\mathbf{Z}^2-(0,0)} \frac{1}{(mz+n)^k}$ converge uniformément sur tout compact de $\mathscr{H}$.

(iii) Si $z \in \mathscr{H}$, soit $\mathrm{G}_k(z) = \frac{\Gamma(k)}{2\,(-2i\pi)^k} \sum_{(m,n)\in\mathbf{Z}^2-(0,0)} \frac{1}{(mz+n)^k}$. Montrer que G_k est une fonction holomorphe sur $\mathscr{H}$ et que

$$\mathrm{G}_k\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^k \mathrm{G}_k(z), \quad \text{quel que soit } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z}).$$

(iv) Montrer que, si k est impair, alors $\mathrm{G}_k = 0$, et que si k est pair, G_k est une forme modulaire de poids k non nulle.

Exercice VII.6.5. — (q-développement des séries d'Eisenstein)

Le but de cet exercice est de prouver que, si k est un entier pair $\geqslant 3$, le q-développement de G_k est donné par la formule suivante [19] :

$$\mathrm{G}_k = \frac{\Gamma(k)}{(-2i\pi)^k}\zeta(k) + \sum_{n=1}^{+\infty} \sigma_{k-1}(n)\, q^n, \quad \text{où } \sigma_{k-1}(n) = \sum_{d|n,\, d\geqslant 1} d^{k-1}.$$

Soit k un entier $\geqslant 2$.

(i) Montrer que la série $\sum_{n\in\mathbf{Z}} \frac{1}{(z+n)^k}$ converge uniformément sur tout compact de $\mathscr{H}$. En déduire que sa somme $\mathrm{A}_k(z)$ est une fonction holomorphe sur $\mathscr{H}$.

(ii) Montrer que A_k est périodique de période 1. Déduire du (i) que $x \mapsto \mathrm{A}_k(x+iy)$ est somme de sa série de Fourier $\sum_{n\in\mathbf{Z}} a_n(y) e^{2i\pi\, nx}$ pour tout $x \in \mathbf{R}$.

(iii) Calculer $a_n(y)$ par la formule des résidus.

(iv) En déduire que $\frac{\Gamma(k)}{(-2i\pi)^k}\mathrm{A}_k(z) = \sum_{n\geqslant 1} n^{k-1} e^{2i\pi\, nz}$.

(v) Montrer que $\mathrm{G}_k(z) = \frac{\Gamma(k)}{(-2i\pi)^k}\big(\zeta(k) + \sum_{m\geqslant 1} \mathrm{A}_k(mz)\big)$, et en déduire le résultat.

Exercice VII.6.6. — (La fonction thêta de Jacobi)

(i) Montrer que $\theta(z) = \sum_{n\in\mathbf{Z}} e^{i\pi n^2 z}$ converge normalement sur tout compact de $\mathscr{H}$. En déduire que θ est holomorphe sur $\mathscr{H}$.

(ii) Montrer, en utilisant le fait que la transformée de Fourier de $e^{-\pi t^2}$ est $e^{-\pi x^2}$ (cf. ex. IV.3.29), que $\theta(iu) = \frac{1}{\sqrt{u}}\theta(\frac{i}{u})$, si $u \in \mathbf{R}_+^*$.

(iii) En déduire que l'on a $\theta(z) = \sqrt{\frac{i}{z}}\theta(\frac{-1}{z})$, si $z \in \mathscr{H}$ (où $\sqrt{z}$ est la racine carrée de z holomorphe sur $\mathbf{C} - \mathbf{R}_-$, et valant 1 en 1).

19. On remarquera que tous les termes de ce q-développement sont visiblement, à l'exception du terme constant, des nombres rationnels. On peut utiliser ceci pour (modulo un certain travail) en déduire qu'il en est de même du terme constant, ce qui permet de donner une démonstration du résultat d'Euler sur les valeurs aux entiers pairs de la fonction zêta.

(iv) On pose $\xi(s) = \frac{\Gamma(s/2)}{\pi^{s/2}}\zeta(s)$, où ζ est la fonction zêta de Riemann. Montrer que, si $\mathrm{Re}(s) > 1$, alors $\xi(s) = \frac{1}{2}\int_0^{+\infty}(\theta(iy)-1)y^{s/2}\,\frac{dy}{y}$.

(v) En déduire que, si $\mathrm{Re}(s) > 1$, alors

$$\xi(s) = -\frac{1}{s} + \frac{1}{s-1} + \frac{1}{2}\int_1^{+\infty}(\theta(iy)-1)(y^{s/2} + y^{(1-s)/2})\,\frac{dy}{y},$$

puis que ξ admet un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples en $s = 0$ et $s = 1$, et vérifie l'équation fonctionnelle $\xi(s) = \xi(1-s)$.

(vi) Montrer que $\xi(s) = \mathrm{O}(\frac{1}{\mathrm{Im}(s)})$ dans toute bande verticale de largeur finie.

Exercice VII.6.7. — (La série d'Eisenstein de poids 2)

Soit G_2 la fonction holomorphe sur $\mathscr{H}$, périodique de période 1, dont le q-développement est [20]

$$\mathrm{G}_2 = \frac{-1}{24} + \sum_{n=1}^{+\infty}\sigma(n)\,q^n, \quad \text{où } \sigma(n) = \sum_{d|n,\,d\geqslant 1} d.$$

Nous allons montrer [21] que G_2 est presque modulaire ; plus précisément, G_2 vérifie l'équation fonctionnelle $z^{-2}\mathrm{G}_2(-1/z) = \mathrm{G}_2(z) - \frac{1}{4i\pi\, z}$.

On rappelle (ex. VI.3.24) que $\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\Gamma(s)y^{-s} = e^{-y}$, si $y \in \mathbf{R}_+^*$ et $c > 0$, l'intégrale étant absolument convergente.

(i) Montrer que, si $\mathrm{L}(\mathbf{a}, s) = \sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ a une abscisse de convergence finie, alors $\mathrm{F}_{\mathbf{a}}(z) = \sum_{n=1}^{+\infty} a_n e^{2i\pi\, nz}$ est holomorphe sur $\mathbf{C}$, et si $c > \sup(0, \sigma_{\mathrm{abs}})$, alors

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{\Gamma(s)}{(2\pi)^s}\mathrm{L}(\mathbf{a}, s)y^{-s}\,ds = \mathrm{F}_{\mathbf{a}}(iy), \quad \text{si } y \in \mathbf{R}_+^*.$$

(ii) Soit $\sigma(n) = \sum_{d|n,\,d\geqslant 1} d$. Montrer que $\mathrm{L}(\sigma, s) = \zeta(s)\zeta(s-1)$.

(iii) Soit $\mathrm{H}(s) = \frac{\Gamma(s)}{(2\pi)^s}\zeta(s)\zeta(s-1)$. Montrer que $\mathrm{H}(s) = \frac{s-1}{4\pi}\xi(s)\xi(s-1)$. En déduire que $\mathrm{H}(2-s) = -\mathrm{H}(s)$, que $\mathrm{H}(s)$ tend vers 0 à l'infini dans toute bande verticale de largeur finie, et que H est holomorphe sur $\mathbf{C}$ en dehors de pôles simples en 0, 1 et 2 de résidus respectifs $\frac{1}{24}$, $\frac{-1}{4\pi}$ et $\frac{1}{24}$, (On pourra utiliser les formules $\zeta(0) = \frac{-1}{2}$, $\zeta(-1) = \frac{-1}{12}$ et $\zeta(2) = \frac{\pi^2}{6}$.)

(iv) Montrer que, si $y > 0$, alors $\mathrm{G}_2(iy) + y^{-2}\mathrm{G}_2(i/y) = \frac{1}{24} - \frac{1}{4\pi\, y} + \frac{1}{24y^2}$. (On intégrera $\mathrm{H}(s)y^{-s}$ sur le rectangle de sommets $3 - i\mathrm{T}$, $3 + i\mathrm{T}$, $-1 + i\mathrm{T}$ et $-1 - i\mathrm{T}$.)

(v) Conclure.

Exercice VII.6.8. — Cet exercice est un préliminaire pour le théorème des 4 carrés. Son but est de démontrer que si $(a_n)_{n\geqslant 2}$ est une suite de nombres complexes vérifiant :

- il existe $c \in \mathbf{N}$ tel que $a_n = \mathrm{O}(n^c)$,
- $\mathrm{F}(z) = \sum_{n=2}^{+\infty} a_n e^{i\pi\, nz}$ vérifie l'équation fonctionnelle $z^{-4}\mathrm{F}(-1/z) = \mathrm{F}(z)$, si $z \in \mathscr{H}$,

alors $a_n = 0$ pour tout $n \geqslant 2$.

(i) Montrer que $\mathrm{F}(z) = \mathrm{O}(e^{-2\pi\mathrm{Im}(z)})$ dans $\mathrm{Y} = \{z \in \mathbf{C},\ |\mathrm{Re}(z)| \leqslant 1,\ \mathrm{Im}(z) \geqslant 1\}$.

---

20. Si on reprend l'exercice VII.6.5, et qu'on utilise la formule $\zeta(2) = \frac{\pi^2}{6}$, on voit que $\mathrm{G}_2(z)$ est la somme des $\frac{\Gamma(2)}{(-2i\pi)^2(mz+n)^2}$ en sommant d'abord sur n puis sur m.

21. La méthode de l'exercice consiste à déduire une équation fonctionnelle reliant $\varphi(-1/z)$ et $\varphi(z)$, à partir d'une équation fonctionnelle reliant $\Lambda(2-s)$ et $\Lambda(s)$, où $\Lambda(s) = \int_0^{+\infty}\varphi(iy)y^s\,\frac{dy}{y}$. Cette méthode a beaucoup d'autres applications. On peut par exemple montrer que la fonction dont le q-développement est celui de G_k est une forme modulaire, sans passer par la construction de G_k et le calcul de son q-développement. Une autre méthode est proposée dans le prob. H.11.

(ii) Montrer que $\mathrm{F}(1-1/z) = \mathrm{O}(\mathrm{Im}(z)^{c+1})$ dans Y.

(iii) Soit k un entier pair. Si $f : \mathscr{H} \to \mathbf{C}$ est une fonction, et si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{R})$, on définit $f_{|_k}\gamma : \mathscr{H} \to \mathbf{C}$ par la formule $f_{|_k}\gamma(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$. Vérifier que ceci est bien défini et que $(f_{|_k}\gamma_1)_{|_k}\gamma_2 = f_{|_k}\gamma_1\gamma_2$, pour tous $\gamma_1, \gamma_2 \in \mathbf{SL}_2(\mathbf{R})$.

(iv) Soient $\mathrm{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathrm{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $\mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Vérifier que $\mathrm{S}^2 = (\mathrm{TS})^3 = -\mathrm{I}$; en déduire que pour toute fonction $f : \mathscr{H} \to \mathbf{C}$, on a $f_{|_k}\mathrm{S}^2 = f_{|_k}(\mathrm{TS})^3 = f$.

(v) Montrer que $\mathrm{F}_{|_4}\mathrm{TS} = \mathrm{F}_{|_4}\mathrm{TST}$. (On pourra s'intéresser à $\mathrm{F}_{|_4}\mathrm{T}^2\mathrm{STSTS}^2$ et calculer $\mathrm{F}_{|_4}\mathrm{S}$ et $\mathrm{F}_{|_4}\mathrm{T}^2$.)

(vi) En déduire [22] que $\mathrm{F}_{|_4}(\mathrm{TS})^2 = \mathrm{F}_{|_4}\mathrm{T}$ et que, si $\mathrm{G} = \mathrm{F} \cdot \mathrm{F}_{|_4}\mathrm{TS} \cdot \mathrm{F}_{|_4}(\mathrm{TS})^2$, alors $\mathrm{G}_{|_{12}}\mathrm{S} = \mathrm{G}_{|_{12}}\mathrm{T} = \mathrm{G}$ et $\mathrm{G} = \mathrm{O}(\mathrm{Im}(y)^{c+1-4}e^{-4\pi\mathrm{Im}(y)})$ dans Y.

(vii) En déduire que G est une forme modulaire de poids 12, que $v_\infty(\mathrm{G}) \geqslant 2$, et conclure.

Exercice VII.6.9. — (Sommes de 4 carrés)

Le but de cet exercice est de démontrer la formule suivante (C. Jacobi, 1829), dont on déduit une forme effective du théorème de Lagrange (1770) : *tout nombre entier positif est somme* [23] *d'au plus* 4 *carrés de nombres entiers*,

$$|\{(a,b,c,d) \in \mathbf{Z}^4,\ a^2+b^2+c^2+d^2 = n\}| = 8 \sum_{d|n,\ 4\nmid d} d.$$

On note $r(n)$ la quantité $|\{(a,b,c,d) \in \mathbf{Z}^4,\ a^2+b^2+c^2+d^2 = n\}|$; autrement dit $r(n)$ est le nombre de décompositions de n en somme de quatre carrés. On note $\theta = \sum_{n\in\mathbf{Z}} e^{i\pi n^2 z}$ la fonction thêta de Jacobi de l'ex. VII.6.6.

(i) Montrer que $\sum_{n=0}^{+\infty} r(n)e^{i\pi nz} = \theta(z)^4$.

(ii) Soit $\mathrm{F}(z) = \theta(z)^4 - 8(\mathrm{G}_2(\frac{z}{2}) - 4\mathrm{G}_2(2z))$. Montrer que $\mathrm{F}_{|_2}\mathrm{S} = -\mathrm{F}$ et $\mathrm{F}_{|_2}\mathrm{T}^2 = \mathrm{F}$. (On utilisera l'ex. VII.6.7.)

(iii) Montrer que $r(n) \leqslant (1+2\sqrt{n})^4$ et $\sigma(n) \leqslant \frac{n(n+1)}{2}$. En déduire que, si $\mathrm{F}(z) = \sum_{n=1}^{+\infty} a_n e^{i\pi nz}$, alors $a_n = \mathrm{O}(n^2)$.

(iv) En déduire, en utilisant l'ex. VII.6.8, que $\theta^4(z) = 8(\mathrm{G}_2(\frac{z}{2}) - 4\mathrm{G}_2(2z))$, et conclure.

On a en particulier (car $\zeta(4) = \frac{\pi^4}{90}$ et $\zeta(6) = \frac{\pi^6}{3^3\cdot 5\cdot 7}$, cf. ex. V.5.3)

$$\mathrm{G}_4 = \frac{1}{240} + \sum_{n\geqslant 1} \sigma_3(n)q^n \quad \text{et} \quad \mathrm{G}_6 = \frac{-1}{504} + \sum_{n\geqslant 1} \sigma_5(n)q^n.$$

On définit alors la *forme discrimant* Δ et l'*invariant modulaire* [24] j par

$$\Delta = \frac{1}{1728}\big((240\mathrm{G}_4)^3 - (504\mathrm{G}_6)^2\big) \quad \text{et} \quad j = \frac{(240\mathrm{G}_4)^3}{\Delta}.$$

22. Ces calculs cachent les résultats suivants. Le sous-groupe de $\mathbf{SL}_2(\mathbf{R})$ engendré par S et T est $\mathbf{SL}_2(\mathbf{Z})$, et celui engendré par S et T^2 est le sous-groupe Γ de $\mathbf{SL}_2(\mathbf{Z})$ des matrices dont l'image dans $\mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})$ est I ou S. Comme $|\mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})| = 6$, l'indice de Γ dans $\mathbf{SL}_2(\mathbf{Z})$ est 3, et I, TS, $(\mathrm{TS})^2$ forment un système de représentants de $\Gamma\backslash\mathbf{SL}_2(\mathbf{Z})$.

23. Ce résultat a été énoncé par Bachet de Méziriac en 1624 et généralisé par Fermat en 1638, sous la forme : tout nombre entier est somme de 3 nombres triangulaires, 4 carrés, 5 nombres pentagonaux, 6 nombres hexagonaux etc. (un nombre k-gonal est de la forme $\frac{n((k-2)n-(k-4))}{2}$, avec $n \geqslant 1$), mais on n'a aucune trace de démonstration. L'énoncé général a été démontré par Cauchy en 1815.

24. le q-développement $j = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$ recèle des trésors (cf. chap. I, note 2).

Exercice VII.6.10. — (La forme modulaire Δ et l'invariant modulaire j)

(i) Montrer que Δ est une forme parabolique non nulle de poids 12 et, en utilisant la « formule $\frac{k}{12}$ », que Δ ne s'annule pas sur D ou sur $\overline{\Omega}$.

(ii) Montrer que j induit une bijection de D sur $\mathbf{C}$.

(iii) Montrer que le seul zéro de G_4 dans D est α et le seul zéro de G_6 dans D est i.

(iv) Montrer que, si $\Delta(z) = 0$, alors $\Delta(z+n) = 0$ quel que soit $n \in \mathbf{Z}$ et $\Delta(-1/z) = 0$. En déduire que si $\Delta(z_0) = 0$, et si $|\mathrm{Re}(z_0)| \leqslant \frac{1}{2}$ et $|z_0| < 1$, alors il existe $z_1 \in \mathscr{H}$, vérifiant $\Delta(z_1) = 0$, $\mathrm{Im}(z_1) > \mathrm{Im}(z_0)$ et $|\mathrm{Re}(z_1)| \leqslant \frac{1}{2}$.

(v) Montrer que Δ ne s'annule pas sur $\mathscr{H}$, et que j est une fonction modulaire de poids 0.

Exercice VII.6.11. — (La formule de Jacobi pour Δ)

Soit $\mathrm{F}(q) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$. Notre but est de prouver que $\Delta(z) = \mathrm{F}(e^{2i\pi z})$. On utilisera pleinement le résultat de l'ex. VII.6.7.

(i) Soit $f(z) = \log(\mathrm{F}(e^{2i\pi z}))$. Montrer que $\frac{1}{2i\pi}f'(z) = -24\mathrm{G}_2(z)$.

(ii) Soit $g(z) = f(-1/z) - 12\log z$. Montrer que $g'(z) = f'(z)$.

(iii) En déduire que, si on pose $\mathrm{H}(z) = \mathrm{F}(e^{2i\pi z})$, alors $\frac{z^{-12}\mathrm{H}(-1/z)}{\mathrm{H}(z)}$ est constante sur $\mathscr{H}$, puis que H est une forme modulaire de poids 12.

(iv) Conclure.

Exercice VII.6.12. — (complément de l'ex. VII.6.2)

(i) Montrer que $\dim \mathrm{M}_k = 1$, si $k \in \{0,4,6,8,10\}$ (utiliser l'ex. VII.6.5 et la formule $\frac{k}{12}$).

(ii) Montrer que $\Delta^{-1}f \in \mathrm{M}_{k-12}$, si $f = \sum_{n\in\mathbf{N}} a_n q^n \in \mathrm{M}_k$ et $a_0 = 0$.

(iii) En déduire que $\dim \mathrm{M}_k = 1 + [\frac{k}{12}]$, si $k \equiv 0,4,6,8,10 \bmod 12$ et $\dim \mathrm{M}_k = [\frac{k}{12}]$, si $k \equiv 2 \bmod 12$.

APPENDICE A

LE THÉORÈME DES NOMBRES PREMIERS

A.1. Introduction

Ce chapitre est consacré à la démonstration du *théorème des nombres premiers* et du *théorème de la progression arithmétique*. On sait depuis les grecs qu'il existe une infinité de nombres premiers [(1)]. Leur répartition n'a cessé depuis de fasciner les mathématiciens. Voici, par exemple, ce qu'écrivait Euler en 1747 : « *Les mathématiciens ont tâché jusqu'ici en vain à découvrir un ordre quelconque dans la progression des nombres premiers, et on a lieu de croire, que c'est un mystère auquel l'esprit humain ne saurait jamais pénétrer. Pour s'en convaincre, on n'a qu'à jeter les yeux sur les tables des nombres premiers, que quelques personnes se sont donné la peine de continuer au-delà de cent-mille : et on s'apercevra d'abord qu'il n'y règne aucun ordre ni règle. Cette circonstance est d'autant plus surprenante, que l'arithmétique nous fournit des règles sûres, par le moyen desquelles on est en état de continuer la progression de ces nombres aussi loin que l'on souhaite, sans pourtant nous y laisser apercevoir la moindre marque d'un ordre quelconque.* ».

Le même Euler a, entre autres :

• démontré que $\sum_{k=1}^{n} \frac{1}{k}$ diverge comme $\log n$, (et même que $-\log n + \sum_{k=1}^{n} \frac{1}{k}$ tend vers une limite γ appelée depuis « constante d'Euler »),

• factorisé $\sum_{n\in\mathbf{N}} \frac{1}{n}$ sous la forme $\prod_{p\in\mathscr{P}}(1 + \frac{1}{p} + \frac{1}{p^2} \cdots)$,

• remarqué que le logarithme du produit était $\sum \frac{1}{p}$ à une somme convergente près.

Ceci lui a fourni, en 1737, une nouvelle démonstration de l'existence d'une infinité de nombres premiers (puisque la somme de leurs inverses diverge). De plus, en partant de la formule $\sum \frac{1}{p} \sim \log(\sum_n \frac{1}{n})$, il en avait déduit que $\sum_{p\leqslant x} \frac{1}{p} \sim \log\log x$. Maintenant, si Δx est petit devant x, les nombres premiers entre x et $x+\Delta x$ sont tous de taille x. Si on note $\pi(x)$ le nombre de nombres premiers $\leqslant x$, on a donc $\log\log(x + \Delta x) - \log\log x \sim \frac{\pi(x+\Delta x)-\pi(x)}{x}$. Comme la dérivée de $\log\log x$ est $\frac{1}{x\log x}$, on en « déduit » que la densité des nombres

1. Il n'est toutefois pas si facile d'en produire explicitement ; le plus grand nombre premier connu à ce jour est le nombre premier de Mersenne $2^{43112609} - 1$, découvert en août 2008 ; il a plus de 10^7 chiffres en écriture décimale.

premiers autour de x est de l'ordre de $\frac{1}{\log x}$, et donc que [2] $\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. Il a fallu attendre plus d'un siècle pour que ce résultat soit rigoureusement [3] démontré, ce qui fut fait en 1896 par J. Hadamard et de la Vallée Poussin indépendamment.

Théorème A.1.1. — (des nombres premiers) $\pi(x) \sim \frac{x}{\log x}$.

Les démonstrations de J. Hadamard et C. de la Vallée Poussin reposent sur la stratégie suggérée par B. Riemann, utilisant le lien entre les zéros de la fonction ζ et la répartition des nombres premiers. L'ingrédient fondamental est la non existence de zéros de la fonction ζ sur la droite $\mathrm{Re}(s) = 1$, où la convergence du produit eulérien cesse, ce qui ne permet pas de conclure quoi que ce soit de la non annulation de chacun de ses facteurs. De fait, le théorème des nombres premiers est équivalent (cf. ex. A.4.6) à la non annulation de ζ sur la droite $\mathrm{Re}(s) = 1$. Cette équivalence a longtemps fait penser qu'une démonstration « élémentaire » (i.e. n'utilisant pas la variable complexe) du théorème des nombres premiers était impossible mais, en 1948, P. Erdös et A. Selberg ont obtenu une telle démonstration, ce qui a valu à A. Selberg la médaille Fields en 1950.

Si P est un polynôme, et s'il n'y a aucune obstruction arithmétique à ce que les valeurs de P aux entiers puissent être des nombres premiers [4], on peut partir du principe que $\mathrm{P}(n)$ a autant de chance d'être premier qu'un nombre de même taille pris au hasard, soit $\frac{1}{\log \mathrm{P}(n)} \sim \frac{1}{\deg \mathrm{P}} \cdot \frac{1}{\log n}$. C'est ce genre d'heuristique, convenablement modifiée pour tenir compte de la probabilité qu'un entier de la forme $\mathrm{P}(n)$ soit divisible par p si $p \in \mathscr{P}$, qui mène à la conjecture de Bateman et Horn ci-dessous.

Soient $\mathrm{P}_1, \cdots, \mathrm{P}_k$ des polynômes distincts, à coefficients entiers, irréductibles dans $\mathbf{Q}[\mathrm{X}]$, dont le coefficient dominant est > 0, et soit $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_k$. Si $p \in \mathscr{P}$, on note $\mathrm{N}_p(\mathrm{P})$ le nombre de solutions de l'équation $\mathrm{P}(x) = 0$ dans le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, et on définit une constante [5] $\mathrm{C}(\mathrm{P}) = \prod_{p \in \mathscr{P}} \big(\big(1 - \frac{1}{p}\big)^{-k} \big(1 - \frac{\mathrm{N}_p(\mathrm{P})}{p}\big)\big)$.

2. La fonction Li est *le logarithme intégral* ; au voisinage de l'infini, on a $\mathrm{Li}(x) \sim \frac{x}{\log x}$ (faire une intégration par partie, en intégrant 1 et en dérivant $\frac{1}{\log t}$). On peut donc reformuler le théorème des nombres premiers sous la forme plus parlante $\pi(x) \sim \frac{x}{\log x}$; c'est sous cette forme que nous le démontrerons, mais $\mathrm{Li}(x)$ est une bien meilleure approximation (cf. prop. A.5.1) de $\pi(x)$ que $\frac{x}{\log x}$.

3. Le lecteur pourra vérifier que, si $\mathrm{M} = \cup_{k \geqslant 1} [2^{2^k}, 2^{2^k+1}[$, alors $\sum_{n \in \mathbf{N} \cap \mathrm{M},\, n \leqslant x} \frac{1}{n} \sim \log\log x$, mais que $\frac{|\{n \in \mathbf{N} \cap \mathrm{M},\, n \leqslant x\}|}{x/\log x}$ n'a pas de limite.

4. Par exemple $12n + 9$, $n(n^2 + 1)$ ou $n(n-1) + 2$ ne peuvent prendre qu'un nombre fini de valeurs premières pour des raisons évidentes.

5. Le produit définissant $\mathrm{C}(\mathrm{P})$ n'est pas convergent ; on définit sa valeur comme la limite quand $x \to +\infty$ des produits partiels $\prod_{p \leqslant x}$. L'existence de cette limite n'est pas du tout évidente, mais la preuve montre, en outre, que $\mathrm{C}(\mathrm{P}) \neq 0$ si $\mathrm{N}_p(\mathrm{P}) \neq p$ pour tout $p \in \mathscr{P}$. Ceci traduit le fait que le nombre de solutions modulo p de l'équation $\mathrm{P}(x) = 0$, pour $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ sans racine double, est, en moyenne, le nombre de facteurs de la décomposition de P en produit de facteurs irréductibles dans $\mathbf{Z}[\mathrm{X}]$.

Conjecture A.1.2. — (Bateman-Horn, 1962) *Si* $\mathrm{C(P)} \neq 0$*, alors l'ensemble des* $n \in \mathbf{N}$ *tels que* $\mathrm{P}_1(n), \ldots, \mathrm{P}_k(n)$ *soient simultanément premiers est infini, et on a*

$$|\{n \leqslant x,\ \mathrm{P}_1(n) \in \mathscr{P}, \ldots, \mathrm{P}_k(n) \in \mathscr{P}\}| \sim \frac{\mathrm{C(P)}}{\deg \mathrm{P}_1 \cdots \deg \mathrm{P}_k} \cdot \frac{x}{(\log x)^k}.$$

Le théorème des nombres premiers correspond au cas $k = 1$, $\mathrm{P} = \mathrm{X}$ de la conjecture. Le seul autre résultat que l'on ait confirmant cette conjecture est celui où $k = 1$, et $\mathrm{P} = \mathrm{P}_1$ est de degré 1. Dans ce cas, P est de la forme $\mathrm{D}x + a$, où $\mathrm{D} \geqslant 2$, et a est premier à D, sinon il existe un nombre premier p pour lequel $\mathrm{D}x + a$ est identiquement nul modulo p, et $\mathrm{C(P)} = 0$. Si $p \mid \mathrm{D}$, alors $\mathrm{N}_p(\mathrm{P}) = 0$, et si $p \nmid \mathrm{D}$, alors $\mathrm{N}_p(\mathrm{P}) = 1$. La constante C(P) de la conjecture de Bateman et Horn est donc

$$\prod_{p|\mathrm{D}} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|\mathrm{D}} \frac{p}{p-1} = \prod_{p|\mathrm{D}} \frac{p^{v_p(\mathrm{D})}}{(p-1)p^{v_p(\mathrm{D})-1}} = \frac{\mathrm{D}}{\varphi(\mathrm{D})},$$

où $\varphi(\mathrm{D}) = |(\mathbf{Z}/\mathrm{D}\mathbf{Z})^*|$ est la fonction indicatrice d'Euler. La conjecture de Bateman et Horn est donc, dans ce cas, conséquence du résultat suivant (appliqué à $\mathrm{D}x$ au lieu de x).

Théorème A.1.3. — (de la progression arithmétique) *Si* $\mathrm{D} \geqslant 2$*, si* a *est premier à* D*, et si* $\pi(\mathrm{D}, a, x) = |\{p \in \mathscr{P},\ p \equiv a \bmod \mathrm{D},\ p \leqslant x\}|$*, alors* $\pi(\mathrm{D}, a, x) \sim \frac{1}{\varphi(\mathrm{D})} \cdot \frac{x}{\log x}$

On peut paraphraser ce théorème en disant que les nombres premiers s'équirépartissent dans les progressions arithmétiques dans lesquelles ils peuvent exister. Sous la forme du théorème, le résultat est dû à de la Vallée Poussin, mais n'est qu'une petite extension du théorème des nombres premiers, si on utilise les idées de Dirichlet (1837) qui avait déjà démontré (th. VII.4.7) un résultat d'équirépartion des nombres premiers dans les progressions arithmétiques (nettement moins fin, mais quand même spectaculaire : démontrer, à la main, l'existence d'une infinité de nombres premiers de la forme $7n + 3$ (par exemple), n'est pas si facile...). La démonstration du th. A.1.3 suit celle du théorème des nombres premiers, en utilisant toutes les fonctions L de Dirichlet (que celui-ci avait précisément introduites pour démontrer son théorème), au lieu de la seule fonction ζ. Nous l'avons transformée en une série d'exercices.

Le théorème de la progression arithmétique est aussi le seul cas où on sache prouver l'existence d'une infinité de n tel que $\mathrm{P}_1(n), \ldots, \mathrm{P}_k(n)$ soient simultanément premiers (ici $k = 1$). Par exemple, on ne sait pas démontrer l'existence d'une infinité de $p \in \mathscr{P}$ tels que $p + 2$ soit premier (problème des *nombres premiers jumeaux*[6] ; il correspond à

6. Il a fallu attendre 2005 pour que D. Goldston et C. Yildirim démontrent que $\liminf \frac{p_{n+1}-p_n}{\log n} = 0$, si p_n désigne le n-ième nombre premier, ce qui constitue un pas encourageant en direction du problème des nombres premiers jumeaux. (La division par $\log n$ se justifie par le fait que p_n est de l'ordre de $n \log n$ et l'écart moyen entre $p_{n+1} - p_n$ est $\log n$.). Chen J. R. a démontré (1975) qu'il existait une infinité de nombres premiers p tels que $p+2$ soit presque premier (i.e. produit d'au plus deux nombres premiers). En 2013, Zhang Y., inspiré par le résultat de Goldston et Yildirim, a prouvé qu'il existe une infinité d'entiers a tels que n et $n+a$ soient simultanément premiers pour une infinité de n, et qu'il existe un tel $a < 7 \cdot 10^7$

$k = 2$, $\mathrm{P}_1 = \mathrm{X}$, $\mathrm{P}_2 = \mathrm{X} + 2$). De même, on ne sait pas démontrer qu'il existe une infinité de nombres premiers de la forme $n^2 + 1$ [7].

La situation est nettement meilleure si on se permet de rajouter une variable : des techniques venant des systèmes dynamiques ont permis récemment des progrès spectaculaires.

• En 2004, B. Green et T. Tao ont démontré qu'il existait des progressions arithmétiques de longueur arbitraire dans l'ensemble des nombres premiers, ce qui joua un rôle certain dans l'attribution de la médaille Fields à T. Tao en 2006 [8]. Autrement dit, si $k \in \mathbf{N}$, il existe une infinité de $(n_1, n_2) \in \mathbf{N}^2$, avec $n_2 \geqslant 1$, tels que $n_1, n_1 + n_2, \ldots, n_1 + kn_2 \in \mathscr{P}$.

• En 2006, T. Tao et T. Ziegler ont démontré que si $\mathrm{P}_1, \ldots, \mathrm{P}_k \in \mathbf{Z}[\mathrm{X}]$ vérifient la condition $\mathrm{P}_1(0) = \cdots = \mathrm{P}_k(0) = 0$, il existe une infinité de $(n_1, n_2) \in \mathbf{N}^2$, avec $n_2 \geqslant 1$, tels que $n_2 + \mathrm{P}_1(n_1), \ldots, n_2 + \mathrm{P}_k(n_1)$ soient des nombres premiers.

• En 2010, B. Green, T. Tao et T. Ziegler ont montré que si $\mathrm{L}_1, \ldots, \mathrm{L}_k$ sont des formes affines (i.e. $\mathrm{L}_i = \mathrm{L}'_i + a_i$, où L'_i est une forme linéaire et a_i une constante) sur $\mathbf{R}^d$ ($d \geqslant 2$), à coefficients entiers, telles que les L'_i soient deux à deux linéairement indépendantes (pour éviter par exemple $\mathrm{L}_1(n) = n_1 + n_2$ et $\mathrm{L}_2(n) = n_1 + n_2 + 2$ qui inclurait le problème des nombres premiers jumeaux), et si

◇ $\{n \in \mathbf{N}^d,\ \mathrm{L}'_1(n) > 0, \ldots, \mathrm{L}'_k(n) > 0\}$ est non vide,

◇ $\{n \in \mathbf{N}^d,\ \mathrm{L}_1(n) \cdots \mathrm{L}_k(n)$ non divisible par $p\}$ est non vide pour tout $p \in \mathscr{P}$,

alors il existe une infinité de $n = (n_1, \ldots, n_d) \in \mathbf{N}^d$ tels que $\mathrm{L}_1(n), \ldots, \mathrm{L}_k(n)$ soient des nombres premiers. Plus précisément, si $\mathrm{P} = \mathrm{L}_1 \cdots \mathrm{L}_k$, et si $\mathrm{N}_p(\mathrm{P})$ est le nombre de solutions de $\mathrm{P}(x) = 0$ dans $\mathbf{F}_p^d$, alors

$$|\{n \in \mathbf{N}^d,\ \sup_{1 \leqslant i \leqslant d} n_i \leqslant x,\ \mathrm{L}_1(n), \ldots, \mathrm{L}_k(n) \in \mathscr{P}\}| \sim \mathrm{C}_\infty \prod_{p \in \mathscr{P}} \Big(\big(1 - \tfrac{1}{p}\big)^{-k} \big(1 - \tfrac{\mathrm{N}_p(\mathrm{P})}{p^d}\big) \Big) \cdot \frac{x^d}{(\log x)^k},$$

(borne descendue à 5000 peu après par une armée de mathématiciens regroupant leurs efforts, mais la méthode ne fournit aucun a explicite).

7. On sait, depuis Fermat (lettre à Mersenne de Noël 1640), que tout nombre premier de la forme $4k + 1$ est somme de deux carrés ; on en déduit qu'il existe une infinité de nombres premiers de la forme $n^2 + m^2$, avec $n, m \in \mathbf{N}$. Il a fallu attendre 1998 pour que J. Friedlander et H. Iwaniec démontrent l'existence d'une infinité de nombres premiers de la forme $n^2 + m^4$; on est encore loin de $n^2 + 1$, bien qu'Iwaniec ait démontré (en 1978) qu'il y a une infinité de n tels que $n^2 + 1$ soit presque premier...

8. P. Erdös avait espéré que l'on pourrait démontrer ce résultat en utilisant juste la divergence de la somme des inverses des nombres premiers (il offrait 3000 dollar pour une solution selon ces lignes). Malgré les efforts de pas mal de gens réputés pour leur astuce (dont Roth, Gowers, Bourgain et Tao, médaillés Fields tous les quatre), on ne sait toujours pas démontrer (ou infirmer...) que si $\mathrm{X} \subset \mathbf{N} - \{0\}$ ne contient pas de progression arithmétique de longueur 3 (i.e. il n'existe pas $a, b, c \in \mathrm{X}$ distincts, tels que $a + c = 2b$), alors $\sum_{n \in \mathrm{X}} \frac{1}{n} < +\infty$. Le meilleur résultat dans cette direction est un résultat de J. Bourgain (1999) selon lequel $|\{n \in \mathrm{X},\ n \leqslant \mathrm{N}\}| = \mathrm{O}(\frac{\mathrm{N}\sqrt{\log\log \mathrm{N}}}{\sqrt{\log \mathrm{N}}})$ (qu'il a amélioré en 2007 avec $(\log \mathrm{N})^{2/3}$ au lieu de $\sqrt{\log \mathrm{N}}$, mais il faudrait pouvoir remplacer $2/3$ par $1 + \delta$, avec $\delta > 0$).

où C_∞ est le volume du convexe déterminé par $0 \leqslant t_i \leqslant 1$ et $\mathrm{L}'_i(t) \geqslant 0$ (C_∞ est la proportion de $n \in \mathbf{N}^d$ tels que $\mathrm{L}_i(n) \geqslant 0$, pour tout i), et $\prod_{p\in\mathscr{P}} \big(\big(1-\frac{1}{p}\big)^{-k}\big(1-\frac{\mathrm{N}_p(\mathrm{P})}{p^d}\big)\big)$ est un produit convergent, contrairement au cas de la conj. A.1.2.

A.2. Les fonctions ψ et ψ_1

1. Théorème des nombres premiers et comportement de ψ_1 en $+\infty$

Si $(a_n)_{n\geqslant 1}$ est une suite de nombres complexes, l'étude de $\sum_{n\leqslant x} a_n$ est étroitement liée à celle de la série de Dirichlet $\sum_{n\geqslant 1} a_n n^{-s}$ comme le montre le cor. A.2.5 ci-dessous. Pour évaluer $\pi(x)$, on est donc naturellement amené à considérer la série de Dirichlet $\sum_{p\in\mathscr{P}} p^{-s}$, qui n'est pas très éloignée de la fonction $-\log\zeta(s)$, et comme elle a des propriétés nettement moins agréables que cette dernière, cela nous conduit à introduire les fonctions auxiliaires suivantes.

• La *fonction* Λ *de von Mangolt* définie par $\sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$. Si $\mathrm{Re}(s) > 1$, on a $\zeta(s) = \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-s}}$, d'après la prop. VII.3.3, et donc (th. V.5.4),

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p\in\mathscr{P}} \frac{p^{-s}\log p}{1-p^{-s}} = \sum_{p\in\mathscr{P}} \sum_{\nu=1}^{+\infty} \frac{\log p}{p^{\nu s}}, \quad \text{si } \mathrm{Re}(s) > 1.$$

On en déduit que $\Lambda(n) = 0$, si n n'est pas une puissance d'un nombre premier, et $\Lambda(n) = \log p$, si $n = p^\nu$, et $\nu \geqslant 1$.

• La fonction ψ définie par $\psi(x) = \sum_{n\leqslant x} \Lambda(n)$.

• La fonction ψ_1 définie par $\psi_1(x) = \int_0^x \psi(t)\,dt$.

Lemme A.2.1. — *Les énoncés suivants sont équivalents au voisinage de* $+\infty$.

(i) $\pi(x) \sim \frac{x}{\log x}$.

(ii) $\psi(x) \sim x$.

(iii) $\psi_1(x) \sim \frac{1}{2}x^2$.

Démonstration. — Par définition, $\psi(x) = \sum_{p^\nu\leqslant x} \log p$. Or, $p^\nu \leqslant x$ implique en particulier $\nu \leqslant \frac{\log x}{\log 2}$, et $\nu \geqslant 2$ implique $p \leqslant \sqrt{x}$. On en déduit l'encadrement

$$\sum_{p\leqslant x} \log p \leqslant \psi(x) \leqslant \sum_{p\leqslant x} \log p + (\sqrt{x}\,\log x)/\log 2 \leqslant \pi(x)\log x + (\sqrt{x}\,\log x)/\log 2.$$

Par ailleurs, si $\beta < 1$, et $x^\beta \leqslant p$, on a $\log p \geqslant \beta \log x$. On en déduit que

$$\sum_{p\leqslant x} \log p \geqslant \beta \log x((\pi(x) - \pi(x^\beta)),$$

et comme $\pi(x^\beta) \leqslant x^\beta$, on obtient, quel que soit $\beta < 1$, l'encadrement

$$\beta(\pi(x)\log x - x^\beta \log x) \leqslant \psi(x) \leqslant \pi(x)\log x + (\sqrt{x}\,\log x)/\log 2.$$

On en déduit l'équivalence entre (i) et (ii).

L'implication (ii)⇒(iii) est immédiate par intégration. Pour démontrer la réciproque, constatons que ψ est une fonction croissante, et donc que

$$\frac{\psi_1(x)-\psi_1((1-\varepsilon)x)}{\varepsilon x}\leqslant\psi(x)\leqslant\frac{\psi_1((1+\varepsilon)x)-\psi_1(x)}{\varepsilon x},$$

quel que soit $\varepsilon>0$. Maintenant, si $\psi_1(x)=\frac{1}{2}x^2+x^2\eta(x)$, avec $\lim_{x\to+\infty}\eta(x)=0$, on obtient, en divisant l'encadrement ci-dessus par x, l'encadrement suivant :

$$1-\frac{\varepsilon}{2}+\frac{\eta(x)-(1-\varepsilon)^2\eta((1-\varepsilon)x)}{\varepsilon}\leqslant\frac{\psi(x)}{x}\leqslant1+\frac{\varepsilon}{2}+\frac{(1+\varepsilon)^2\eta((1+\varepsilon)x)-\eta(x)}{\varepsilon}.$$

En faisant tendre x vers $+\infty$, on en déduit que $\liminf\frac{\psi(x)}{x}\geqslant1-\frac{\varepsilon}{2}$ et $\limsup\frac{\psi(x)}{x}\leqslant1+\frac{\varepsilon}{2}$. Comme ceci est vrai pour tout $\varepsilon>0$, cela prouve que $\psi(x)\sim x$, ce qui permet de conclure.

Exercice A.2.2. — Si $\mathrm{D}\geqslant2$, si a est premier à D, et si $x\geqslant1$, soient

$$\psi(\mathrm{D},a,x)=\sum_{n\leqslant x,\,n\equiv a\bmod \mathrm{D}}\Lambda(n)\quad\text{et}\quad\psi_1(\mathrm{D},a,x)=\int_0^x\psi(\mathrm{D},a,t)\,dt.$$

Montrer que les deux énoncés suivants sont équivalents au théorème de la progression arithmétique : « $\varphi(\mathrm{D})\psi(\mathrm{D},a,x)\sim x$ » et « $\varphi(\mathrm{D})\psi_1(\mathrm{D},a,x)\sim\frac{x^2}{2}$ ».

Exercice A.2.3. — Montrer que le théorème des nombres premier équivaut à $\mathrm{ppcm}(1,\dots,n)=e^{n+o(n)}$.

2. Une formule intégrale pour ψ_1

Lemme A.2.4. — *Si $c>0$ et $x>0$, alors*

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{x^{s+1}}{s(s+1)}\,ds=\begin{cases}0 & \text{si } x<1,\\ x-1 & \text{si } x\geqslant1.\end{cases}$$

Démonstration. — C'est un calcul de résidus parfaitement standard. La fonction $\frac{x^{s+1}}{s(s+1)}$ est méromorphe sur $\mathbf{C}$, holomorphe en dehors de deux pôles simples en $s=0$ et $s=-1$, de résidus respectifs $\mathrm{Res}(\frac{x^{s+1}}{s(s+1)},0)=x$ et $\mathrm{Res}(\frac{x^{s+1}}{s(s+1)},-1)=-1$.

• Si $x\geqslant1$, on intègre sur le lacet γ_{T} constitué du segment $[c-i\mathrm{T},c+i\mathrm{T}]$, et de $\mathrm{C}^+(\mathrm{T})$, arc de cercle $c+\mathrm{T}e^{i\theta}$, avec θ variant de $\frac{\pi}{2}$ à $\frac{3\pi}{2}$. Si $\mathrm{T}>c+1$, le lacet γ_{T} a pour indice 1 par rapport aux deux points 0 et -1. On déduit de la formule des résidus que $\frac{1}{2i\pi}\int_{\gamma_{\mathrm{T}}}\frac{x^{s+1}}{s(s+1)}\,ds=x-1$, si $\mathrm{T}>c+1$. Par ailleurs, sur $\mathrm{C}^+(\mathrm{T})$, on a $|x^{s+1}|\leqslant x^{c+1}$ et $|\frac{1}{s(s+1)}|\leqslant\frac{1}{(\mathrm{T}-c)(\mathrm{T}-c-1)}$. Donc $\int_{\mathrm{C}^+(\mathrm{T})}\frac{x^{s+1}}{s(s+1)}\,ds\to0$ quand $\mathrm{T}\to+\infty$, et

$$\begin{aligned}\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{x^{s+1}}{s(s+1)}\,ds&=\lim_{\mathrm{T}\to+\infty}\frac{1}{2i\pi}\int_{[c-i\mathrm{T},c+i\mathrm{T}]}\frac{x^{s+1}}{s(s+1)}\,ds\\&=x-1-\lim_{\mathrm{T}\to+\infty}\int_{\mathrm{C}^+(\mathrm{T})}\frac{x^{s+1}}{s(s+1)}\,ds=x-1.\end{aligned}$$

• Si $x<1$, on intègre sur le lacet γ_{T} constitué du segment $[c-i\mathrm{T},c+i\mathrm{T}]$, et de $\mathrm{C}^-(\mathrm{T})$, arc de cercle $c+\mathrm{T}e^{i\theta}$, avec θ variant de $\frac{\pi}{2}$ à $\frac{-\pi}{2}$. Dans ce cas γ_{T} a pour indice 0 par rapport

aux deux points 0 et -1, et la formule des résidus nous donne $\frac{1}{2i\pi}\int_{\gamma_T}\frac{x^{s+1}}{s(s+1)}\,ds = 0$, quel que soit $T > 0$. Le reste de l'argument est le même que ci-dessus.

Corollaire A.2.5. — *Soit* $L(\mathbf{a}, s) = \sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ *une série de Dirichlet d'abscisse de convergence absolue* $\sigma_{abs} \neq +\infty$. *Alors, si* $c > \sup(0, \sigma_{abs})$ *et* $x > 0$, *on a*

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{L(\mathbf{a}, s)x^{s+1}}{s(s+1)}\,ds = \int_0^x \Big(\sum_{n\leqslant t} a_n\Big)\,dt.$$

Démonstration. — Par hypothèse, la série $\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ converge normalement sur la droite $c + i\mathbf{R}$, et comme la fonction $\frac{1}{s(s+1)}$ est sommable sur cette droite, on peut échanger somme et intégrale. Par ailleurs, on a

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{1}{n^s}\frac{x^{s+1}}{s(s+1)}\,ds = \begin{cases} 0 & \text{si } x < n, \\ n(\frac{x}{n} - 1) = x - n & \text{si } x \geqslant n. \end{cases}$$

On en déduit que

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{L(\mathbf{a}, s)x^{s+1}}{s(s+1)}\,ds = \sum_{n\leqslant x} a_n(x-n) = \int_0^x \Big(\sum_{n\leqslant t} a_n\Big)\,dt,$$

ce qui permet de conclure.

Corollaire A.2.6. — *Si* $c > 1$, *et si* $x > 1$, *alors* $\psi_1(x) = -\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{\zeta'(s)}{\zeta(s)}\frac{x^{s+1}}{s(s+1)}\,ds$.

Exercice A.2.7. — Si $D \geqslant 2$, notons Dir(D) l'ensemble des caractères de Dirichlet modulo D. On utilisera le résultat suivant démontré dans le n° 5 du § I.2 :

$$\textit{Si } a \textit{ est premier à } D\textit{, alors } \sum_{\chi\in \mathrm{Dir}(D)} \overline{\chi(a)}\chi(n) = \begin{cases} \varphi(D) & \text{si } n \equiv a \bmod D, \\ 0 & \text{sinon.} \end{cases}$$

Établir, si $c > 1$ et $x > 1$, la formule

$$\varphi(D)\,\psi_1(D, a, x) = \frac{1}{2i\pi}\sum_{\chi\in \mathrm{Dir}(D)} \overline{\chi(a)}\int_{c-i\infty}^{c+i\infty}\frac{-L'(\chi, s)}{L(\chi, s)}\frac{x^{s+1}}{s(s+1)}\,ds.$$

A.3. Formules explicites

La formule du cor. A.2.6 est, en elle-même, assez peu utile en ce qui concerne la démonstration du théorème des nombres premiers. La seule information qu'on puisse en tirer est, semble-t-il, en majorant brutalement ce qu'on intègre, l'existence, pour tout $c > 1$, d'une constante $C(c)$ telle que $\psi_1(x) \leqslant C(c)x^{1+c}$, ce qui était évident dès le départ. Pour obtenir des résultats plus fins, on va déplacer la ligne d'intégration vers la gauche [9] (de manière à diminuer le c). La traversée de la bande critique est un peu périlleuse à cause de

9. On va envoyer la ligne d'intégration vers $-\infty$, ce qui induit des complications un peu inutiles si on ne s'intéresse qu'au th. des nombres premiers, mais permet d'établir un lien direct entre la répartition des nombres premiers et les zéros de la fonction ζ de Riemann (en appliquant le th. A.3.3 à $L = \zeta$) ; la

la présence des zéros de ζ qui entraîne l'existence de nombreux pôles pour la fonction $\frac{\zeta'}{\zeta}$, ce qui fait que la fonction $\frac{\zeta'}{\zeta}$ est loin d'être assez petite pour qu'on puisse se dispenser de prendre des précautions en se déplaçant. On va donc être forcé de majorer cette fonction $\frac{\zeta'}{\zeta}$ dans la bande critique, et le miracle des fonctions holomorphes (lemmes A.3.6, A.3.9 et A.3.10) fait que la connaissance de la fonction ζ des deux côtés de la bande critique permet de contrôler un peu ce qui se passe à l'intérieur (on maîtrise bien la fonction ζ dans le demi-plan $\mathrm{Re}(s) < 0$ grâce à l'équation fonctionnelle et à la formule de Stirling).

1. Énoncé du résultat

Afin de pouvoir appliquer les résultats de ce § aux fonctions L de Dirichlet, nous allons partir d'une fonction L méromorphe sur $\mathbf{C}$, holomorphe en dehors d'un pôle simple éventuel en $s = 1$, et qui vérifie les conditions (L1)–(L3) ci-dessous, ce qui est le cas de ζ (d'après le lemme A.3.1) et des fonctions L de Dirichlet :

(L1) Si $a > 1$, il existe $c(a)$, tel que, si $\mathrm{Re}(s) \geqslant a$, on ait

$$|\mathrm{L}(s)| \leqslant c(a), \quad |\mathrm{L}(s)^{-1}| \leqslant c(a), \quad \Big|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\Big| \leqslant c(a).$$

En particulier, L ne s'annule pas sur le demi-plan $\mathrm{Re}(s) > 1$.

(L2) Il existe $\mathrm{A} \in \mathbf{C}^*$, $\mathrm{B} \in \mathbf{R}_+^*$ et $c \in [0, 2[$ tels que L vérifie l'équation fonctionnelle

$$\mathrm{L}(s) = \mathrm{A} \cdot \mathrm{B}^s \cdot \Gamma(1-s) \cdot \sin\frac{\pi(s-c)}{2} \cdot \overline{\mathrm{L}}(1-s), \quad \text{où } \overline{\mathrm{L}} \text{ est définie par } \overline{\mathrm{L}}(s) = \overline{\mathrm{L}(\overline{s})}.$$

(L3) Quels que soient $a \leqslant b$ réels, il existe $\mathrm{C}(a,b) > 0$ et $c(a,b) > 0$ tels que, si $a \leqslant \sigma \leqslant b$ et $|\tau| \geqslant 1$, alors

$$|\mathrm{L}(\sigma + i\tau)| \leqslant \mathrm{C}(a,b) e^{c(a,b)|\tau|}.$$

Lemme A.3.1. — *La fonction ζ vérifie les propriétés (L1)–(L3).*

Démonstration. — Si $\mathrm{Re}(s) > a$, on a

$$|\zeta(s)| = \prod_{p\in\mathscr{P}} \frac{1}{|1-p^{-s}|} \leqslant \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-\mathrm{Re}(s)}} \leqslant \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-a}} \leqslant \zeta(a),$$

$$|\zeta(s)^{-1}| = \prod_{p\in\mathscr{P}} |1-p^{-s}| \leqslant \prod_{p\in\mathscr{P}} (1+p^{-a}) \leqslant \frac{\zeta(a)}{\zeta(2a)},$$

$$\Big|\frac{\zeta'(s)}{\zeta(s)}\Big| \leqslant \sum_{n\in\mathbf{N}} \Lambda(n)|n^{-s}| \leqslant \sum_{n\in\mathbf{N}} \Lambda(n)\, n^{-a} = \frac{\zeta'(a)}{\zeta(a)},$$

ce qui montre que ζ vérifie (L1), avec $c(a) = \sup(\zeta(a), \frac{\zeta'(a)}{\zeta(a)})$. Les propriétés (L2) et (L3) sont nettement plus délicates mais ont déjà été démontrées (la propriété (L2) fait l'objet

démonstration du th. A.3.3 mélange de jolis résultats et des majorations un peu pénibles ; il est conseillé de lire le § A.4 pour voir comment le th. A.3.3 est utilisé avant de s'attaquer à sa démonstration.

du th. VII.3.7, et la prop. VII.2.11 (allié à la formule $\zeta(s) = \frac{1}{s-1}\mathrm{M}(\frac{t}{e^t-1}, s-1)$ de la démonstration du th. VII.3.4) montre que l'on peut prendre $c(a,b) = \frac{\pi}{2}$).

Exercice A.3.2. — (i) Montrer que $\mathrm{L}(\chi, s)$ vérifie les propriétés (L1)–(L3), si χ est primitif.

(ii) Montrer que, si χ est primitif de conducteur divisant D, si $c > 1$, et si $x > 1$, alors

$$\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\Big(\frac{\mathrm{L}'(\chi_{\mathrm{D}},s)}{\mathrm{L}(\chi_{\mathrm{D}},s)} - \frac{\mathrm{L}'(\chi,s)}{\mathrm{L}(\chi,s)}\Big)\frac{x^{s+1}}{s(s+1)}\,ds = \sum_{p|\mathrm{D}}\sum_{\nu\leqslant\frac{\log x}{\log p}}\chi(\nu)(x-p^\nu).$$

En déduire que $\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\big(\frac{\mathrm{L}'(\chi_{\mathrm{D}},s)}{\mathrm{L}(\chi_{\mathrm{D}},s)} - \frac{\mathrm{L}'(\chi,s)}{\mathrm{L}(\chi,s)}\big)\frac{x^{s+1}}{s(s+1)}\,ds$ est un $\mathrm{O}(x\log x)$.

Soit donc L une fonction méromorphe sur $\mathbf{C}$, holomorphe en dehors d'un pôle simple éventuel (ce pôle simple éventuel pouvant en fait être un zéro) en $s = 1$, et vérifiant les propriétés (L1)-(L3). Si $x > 1$, on note F_x la fonction $\mathrm{F}_x(s) = -\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\frac{x^{s+1}}{s(s+1)}$. C'est une fonction méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles en 0, -1, éventuellement en 1, et en les zéros de L. Comme L ne s'annule pas sur $\mathrm{Re}(s) > 0$ et vérifie l'équation fonctionnelle de la propriété (L2), les seuls zéros de L en dehors de la bande $0 \leqslant \mathrm{Re}(s) \leqslant 1$ (bande critique) sont les $c - 2k$, pour $k \in \mathbf{N} - \{0\}$, ce qui peut inclure -1. On note $\mathrm{Y}(\mathrm{L})$ l'ensemble des zéros dans la bande critique, distincts de 0 et 1.

Soient $a_0 = x^{-1}\mathrm{Res}(\mathrm{F}_x, 0)$ et $a_{-1} = \mathrm{Res}(\mathrm{F}_x, -1)$ [10]. Le résultat que nous avons en vue est la « formule explicite » suivante (dans laquelle $v_z(\mathrm{L}) \in \mathbf{Z}$ désigne la valuation (i.e. l'ordre du zéro) de L au point z).

Théorème A.3.3. — (i) *La série* $\sum_{\rho\in\mathrm{Y}(\mathrm{L})}\frac{v_\rho(\mathrm{L})}{\rho(\rho+1)}$ *est absolument convergente.*

(ii) *Si* $x > 1$, *alors* $\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\frac{-\mathrm{L}'(s)}{\mathrm{L}(s)}\frac{x^{s+1}}{s(s+1)}\,ds$ *est aussi égal à*

$$-v_1(\mathrm{L})\frac{x^2}{2} + a_0 x + a_{-1} - \sum_{\rho\in\mathrm{Y}(\mathrm{L})}\frac{v_\rho(\mathrm{L})x^{\rho+1}}{\rho(\rho+1)} - \sum_{k\geqslant 1,\, c-2k\neq -1}\frac{x^{1+c-2k}}{(2k-c)(2k-c-1)},$$

les deux séries ci-dessus étant absolument convergentes.

La démonstration va demander un peu de préparation, mais on peut tout de même remarquer que l'expression finale peut se réécrire sous la forme plus compacte [11]

$$\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\frac{-\mathrm{L}'(s)}{\mathrm{L}(s)}\frac{x^{s+1}}{s(s+1)}\,ds = \sum_{\mathrm{Re}(\rho)<2}\mathrm{Res}(\mathrm{F}_x,\rho),$$

l'expression du théorème étant obtenue en explicitant le résidu de F_x en tous ses pôles (qui sont simples sauf peut-être 0 et -1). De plus, comme $|x^{\rho+1}| \leqslant x^3$, si $\mathrm{Re}(\rho) < 2$,

10. Si 0 n'est pas un zéro de L, alors $a_0 = \frac{-\mathrm{L}'(0)}{\mathrm{L}(0)}$. Si 0 est un zéro de L, alors 0 est un pôle double de F, et a_0 est de la forme $a_{0,0} + a_{0,1}\log x$.

Si $c \neq 1$, alors -1 est un pôle simple de F, et $a_{-1} = \frac{\mathrm{L}'(1)}{\mathrm{L}(1)}$. Si $c = 1$, alors -1 est un pôle double de F, et a_{-1} est de la forme $a_{-1,0} + a_{-1,1}\log x$.

11. Formellement, cette formule n'est autre que la formule des résidus si on considère la droite $\mathrm{Re}(s) = 2$ comme un lacet entourant le demi-plan $\mathrm{Re}(s) < 2$.

la convergence des séries suit juste de la convergence absolue des séries $\sum_{\rho\in \mathrm{Y(L)}} \frac{v_\rho(\mathrm{L})}{\rho(\rho+1)}$ et $\sum_{k\geqslant 1} \frac{1}{(2k-c)(2k-c-1)}$. Il suffit donc de démontrer le (i) et la forme compacte ci-dessus.

2. Les fonctions L et $\frac{\mathrm{L}'}{\mathrm{L}}$ en dehors de la bande critique

Lemme A.3.4. — *Si $a<0$, la fonction $(s-a+1)^{a-\frac{3}{2}}(s-1)\mathrm{L}(s)$ est bornée sur la droite $\mathrm{Re}(s)=a$.*

Démonstration. — Sur la droite $\mathrm{Re}(s)=a$, la fonction $\mathrm{F}(s)=(s-a+1)^{a-\frac{3}{2}}(s-1)\mathrm{L}(s)$ est continue. Par ailleurs, si $t\in\mathbf{R}$, on a

$$\mathrm{L}(a+it)=\mathrm{A}\,\mathrm{B}^{a+it}\sin(\frac{\pi(a-c+it)}{2})\Gamma(1-a-it)\overline{\mathrm{L}}(1-a-it).$$

Or $\mathrm{A}\,\mathrm{B}^{a+it}\overline{\mathrm{L}}(1-a-it)$ est bornée pour $t\in\mathbf{R}$, et $e^{-\pi|t|/2}|\sin\frac{\pi(a-c+it)}{2}|$ tend vers $\frac{1}{2}$ quand $|t|$ tend vers $+\infty$, ce qui permet de déduire du cor. VII.2.10 que

$$|\sin(\frac{\pi(a-c+it)}{2})\Gamma(1-a-it)|\,|t|^{-\frac{1}{2}+a}$$

est borné quand $|t|$ tend vers $+\infty$. Donc $|\mathrm{F}(a+it)|=|(it+1)^{a-\frac{3}{2}}(a+it-1)\mathrm{L}(a+it)|$ est borné quand $|t|$ tend vers $+\infty$, et comme $\mathrm{F}(a+it)$ est continue sur $\mathbf{R}$, elle est bornée sur $\mathbf{R}$. Ceci permet de conclure.

Lemme A.3.5. — *Soit $(t_n^+)_{n\geqslant 2}$ (resp. $(t_n^-)_{n\geqslant 2}$) une suite de réels vérifiant $n\leqslant t_n^+\leqslant n+1$ (resp. $-n-1\leqslant t_n^-\leqslant -n$). Soient $b_n^+=-1+it_n^+$ (resp. $b_n^-=-1+it_n^-$) et $c_n^+=c+1-2n+it_n^+$ (resp. $c_n^-=c+1-2n+it_n^-$). Alors il existe $\mathrm{C}>0$ tels que, $|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}|\leqslant \mathrm{C}+\log n$, quels que soient $n\geqslant 2$ et $s\in[b_n^+,c_n^+]\cup[c_n^+,c_n^-]\cup[c_n^-,b_n^-]$.*

Démonstration. — On part de l'équation fonctionnelle (L2) dont on déduit l'identité

$$\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}=\log\mathrm{B}+\frac{i\pi}{2}\cdot\frac{e^{i\pi(s-c)/2}+e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2}-e^{-i\pi(s-c)/2}}-\frac{\Gamma'(1-s)}{\Gamma(1-s)}-\frac{\overline{\mathrm{L}}'(1-s)}{\overline{\mathrm{L}}(1-s)}.$$

Maintenant, quand s décrit $[b_n^+,c_n^+]\cup[c_n^+,c_n^-]\cup[c_n^-,b_n^-]$, on a $\mathrm{Re}(1-s)\geqslant 2$.

- Or $|\frac{\overline{\mathrm{L}}'(1-s)}{\overline{\mathrm{L}}(1-s)}|\leqslant c(2)$, si $\mathrm{Re}(1-s)\geqslant 2$, d'après la propriété (L1).
- D'après la prop. VII.2.9, il existe $\mathrm{C}_1>0$ tel que $|\frac{\Gamma'(1-s)}{\Gamma(1-s)}-\log(1-s)|\leqslant \mathrm{C}_1$, si $\mathrm{Re}(1-s)\geqslant 2$. On en déduit, si $s\in[b_n^+,c_n^+]\cup[c_n^+,c_n^-]\cup[c_n^-,b_n^-]$, que

$$|\frac{\Gamma'(1-s)}{\Gamma(1-s)}|\leqslant \pi+\mathrm{C}_1+\log|1-s|\leqslant \pi+\mathrm{C}_1+\log\sqrt{(2n-c)^2+(n+1)^2}\leqslant \pi+\mathrm{C}_1+\log 3+\log n.$$

- Si s appartient à $[b_n^+,c_n^+]$ ou $[c_n^-,b_n^-]$, on a $|\mathrm{Im}(s)|\geqslant n$, et donc

$$|\frac{e^{i\pi(s-c)/2}+e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2}-e^{-i\pi(s-c)/2}}|\leqslant\frac{e^{\pi n/2}+e^{-\pi n/2}}{e^{\pi n/2}-e^{-\pi n/2}}\leqslant\frac{1+e^{-\pi}}{1-e^{-\pi}}.$$

Si $s \in [c_n^+, c_n^-]$, et si $s = c + 1 - 2n + it$, alors

$$\Big|\frac{e^{i\pi(s-c)/2} + e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2} - e^{-i\pi(s-c)/2}}\Big| = \Big|\frac{e^{-\pi t/2} - e^{\pi t/2}}{e^{-\pi t/2} + e^{\pi t/2}}\Big| \leqslant 1 \leqslant \frac{1+e^{-\pi}}{1-e^{-\pi}}.$$

On en déduit l'inégalité $|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}| \leqslant \log \mathrm{B} + c(2) + \pi + \mathrm{C}_1 + \log 3 + \frac{\pi}{2}\frac{1+e^{-\pi}}{1-e^{-\pi}} + \log n$, si $s \in [b_n^+, c_n^+] \cup [c_n^+, c_n^-] \cup [c_n^-, b_n^-]$. Ceci permet de conclure.

3. La fonction L dans la bande critique

Lemme A.3.6. — *Soit* F *une fonction holomorphe sur un ouvert contenant la bande* $a \leqslant \mathrm{Re}(s) \leqslant b$. *On suppose que* $|\mathrm{F}(s)| \leqslant \mathrm{M}$ *sur les droites* $\mathrm{Re}(s) = a$ *et* $\mathrm{Re}(s) = b$, *et qu'il existe* $c, \mathrm{C} > 0$ *tels que* $|\mathrm{F}(\sigma + i\tau)| \leqslant \mathrm{C}\, e^{c|\tau|}$, *si* $a \leqslant \sigma \leqslant b$ *et* $|\tau| \geqslant 1$. *Alors* $|\mathrm{F}(s)| \leqslant \mathrm{M}$ *sur la bande toute entière.*

Démonstration. — Si $\varepsilon > 0$, alors $\mathrm{F}(s)e^{\varepsilon s^2}$ tend vers 0 quand s tend vers l'infini dans cette bande, puisque $\mathrm{Re}(\varepsilon s^2) \sim -\varepsilon \mathrm{Im}(s)^2$ tend vers $-\infty$ beaucoup plus vite que $c|\mathrm{Im}(s)|$. Le principe du maximum (rem. V.3.12) permet d'en déduire que, si T est assez grand, le maximum de $|\mathrm{F}(s)e^{\varepsilon s^2}|$ sur le rectangle de sommets $a \pm i\mathrm{T}$ et $b \pm i\mathrm{T}$ est atteint sur un des segments verticaux, et donc que le maximum de $|\mathrm{F}(s)e^{\varepsilon s^2}|$ dans la bande est atteint sur la droite $\mathrm{Re}(s) = a$ ou sur la droite $\mathrm{Re}(s) = b$. On en déduit que $|\mathrm{F}(s)e^{\varepsilon s^2}| \leqslant \mathrm{M} \sup(e^{\varepsilon a^2}, e^{\varepsilon b^2})$, quels que soient $\varepsilon > 0$, et s dans la bande $a \leqslant \mathrm{Re}(s) \leqslant b$. En faisant tendre ε vers 0, cela montre que $|\mathrm{F}|$ est majorée par M sur la bande, ce que l'on cherchait à démontrer.

Lemme A.3.7. — *Si* $a < 0$, *la fonction* $(s - a + 1)^{a-\frac{3}{2}}(s-1)\mathrm{L}(s)$ *est bornée sur le demi-plan* $\mathrm{Re}(s) \geqslant a$.

Démonstration. — Comme $\frac{3}{2} - a \geqslant 1$ et comme L est bornée sur le demi-plan $\mathrm{Re}(s) \geqslant 1 - a$, la fonction $\mathrm{F}(s) = (s - a + 1)^{a-\frac{3}{2}}(s-1)\mathrm{L}(s)$ est bornée sur le demi-plan $\mathrm{Re}(s) \geqslant 1 - a$ (et donc en particulier sur la droite $\mathrm{Re}(s) = 1 - a$). Par ailleurs, la fonction F est bornée sur la droite $\mathrm{Re}(s) = a$, d'après le lemme A.3.4. Enfin, la fonction F est holomorphe dans la bande $a \leqslant \mathrm{Re}(s) \leqslant 1 - a$ et la propriété (L3) montre que F vérifie les hypothèses du lemme A.3.6 (avec $b = 1 - a$ et c n'importe quel réel $> c(a, 1-a)$). On en déduit le résultat.

Lemme A.3.8. — *Il existe* $\mathrm{C}_1 > 0$ *tel que* $\sup_{s \in \mathrm{D}(2+it,12)} \big|\frac{\mathrm{L}(s)}{\mathrm{L}(2+it)}\big| \leqslant \mathrm{C}_1 |t|^{21/2}$, *si* $t \in \mathbf{R}$ *et* $|t| \geqslant 15$.

Démonstration. — On déduit du lemme A.3.7 (avec $a = -10$) l'existence d'une constante C_1' telle que

$$|\mathrm{L}(s)| \leqslant \mathrm{C}_1' \frac{|s+11|^{23/2}}{|s-1|}, \quad \text{si } \mathrm{Re}(s) \geqslant -10.$$

Maintenant, si $s \in \mathrm{D}(2+it, 12)$, on a $|s+11| \leqslant |t|+25$, et $|s-1| \geqslant |s|-1 \geqslant |t|-13$. Comme de plus, $|\mathrm{L}(2+it)^{-1}| \leqslant c(2)$, d'après la propriété (L1), on obtient, si $|t| > 13$,

$$\sup_{s\in \mathrm{D}(2+it,12)} \Big|\frac{\mathrm{L}(s)}{\mathrm{L}(2+it)}\Big| \leqslant c(2)\mathrm{C}_1' \, \frac{(|t|+25)^{23/2}}{|t|-13}.$$

Le résultat s'en déduit sans problème.

4. La fonction $\frac{\mathrm{L}'}{\mathrm{L}}$ dans la bande critique

Lemme A.3.9. — (Borel-Carathéodory) *Soient Ω un ouvert de $\mathbf{C}$, $\mathrm{R} > 0$ tel que $\mathrm{D}(0,\mathrm{R}) \subset \Omega$, et f holomorphe sur Ω, avec $f(0) = 0$. Si $\mathrm{A} = \sup_{|s|=\mathrm{R}} \mathrm{Re}(f(s))$, alors*

$$\Big|\frac{f^{(k)}(s)}{k!}\Big| \leqslant \frac{4\mathrm{AR}}{(\mathrm{R}-|s|)^{k+1}}, \quad \textit{quels que soient } k \in \mathbf{N} \textit{ et } s \in \mathrm{D}(0,\mathrm{R}^-).$$

Démonstration. — On a $\mathrm{F}(s) = \sum_{n=1}^{+\infty} a_n s^n$ sur $\mathrm{D}(0,\mathrm{R})$. En écrivant a_n sous la forme $|a_n|e^{i\theta_n}$, on obtient $\mathrm{Re}(f(\mathrm{R}e^{i\theta})) = \sum_{m=1}^{+\infty} |a_m|\mathrm{R}^m \cos(m\theta+\theta_m)$ et

$$\int_0^{2\pi} (1+\cos(n\theta+\theta_n))\mathrm{Re}(f(\mathrm{R}e^{i\theta}))\,d\theta$$
$$= \sum_{m=1}^{+\infty} |a_m|\mathrm{R}^m \int_0^{2\pi} (1+\cos(n\theta+\theta_n))\cos(m\theta+\theta_m)\,d\theta = \pi|a_n|\mathrm{R}^n.$$

Comme $0 \leqslant 1+\cos(n\theta+\theta_n) \leqslant 2$, on en tire la majoration $\pi|a_n|\mathrm{R}^n \leqslant 4\pi\mathrm{A}$ et donc $|a_n| \leqslant 4\mathrm{AR}^{-n}$. (En particulier, $\mathrm{A} \geqslant 0$.) Maintenant, si $|s| < \mathrm{R}$, on a

$$\Big|\frac{f^{(k)}(s)}{k!}\Big| = \Big|\sum_{n=0}^{+\infty} \binom{n+k}{k} a_{n+k} s^n\Big| \leqslant 4\mathrm{A}\sum_{n=0}^{+\infty} \binom{n+k}{k} \frac{|s|^n}{\mathrm{R}^{n+k}} = \frac{4\mathrm{AR}}{(\mathrm{R}-|s|)^{k+1}}.$$

Ceci permet de conclure.

Lemme A.3.10. — *Soient Ω un ouvert de $\mathbf{C}$, $\mathrm{R} > 0$ tel que $\mathrm{D}(0,3\mathrm{R}) \subset \Omega$, et f holomorphe sur Ω, avec $f(0) = 1$. Soit $\mathrm{M} = \sup_{s\in\mathrm{D}(0,3\mathrm{R})} |f(s)|$, et soit Y l'ensemble des zéros de f dans $\mathrm{D}(0,\mathrm{R})$. Alors :*

$$\sum_{\rho\in\mathrm{Y}} v_\rho(f) \leqslant \frac{\log \mathrm{M}}{\log 2} \quad \text{et} \quad \Big|\frac{f'(s)}{f(s)} - \sum_{\rho\in\mathrm{Y}} \frac{v_\rho(f)}{s-\rho}\Big| \leqslant \frac{4\mathrm{R}\log \mathrm{M}}{(\mathrm{R}-|s|)^2}, \textit{ quel que soit } s \in \mathrm{D}(0,\mathrm{R}^-).$$

Démonstration. — Soit $g(s) = f(s)\prod_{\rho\in\mathrm{Y}}(1-s/\rho)^{-v_\rho(f)}$. Par construction, g ne s'annule pas sur $\mathrm{D}(0,\mathrm{R})$, et $g(0) = 1$; il existe donc (cf. prop. VI.2.3) un ouvert $\Omega' \subset \Omega$ contenant $\mathrm{D}(0,\mathrm{R})$ et h holomorphe sur Ω', avec $h(0) = 0$, tels que $g = e^h$ sur Ω'. Soit $\mathrm{N} = \sum_{\rho\in\mathrm{Y}} v_\rho(f)$. Comme $|1-s/\rho| \geqslant 2$, si $|s| = 3\mathrm{R}$, on a $|g(s)| \leqslant 2^{-\mathrm{N}}\mathrm{M}$, si $|s| = 3\mathrm{R}$. Par le principe du maximum (rem. V.3.12) cela implique que $1 = |g(1)| \leqslant 2^{-\mathrm{N}}\mathrm{M}$, et donc que $\mathrm{N} \leqslant \frac{\log \mathrm{M}}{\log 2}$. Enfin, on a $|g(s)| \leqslant \mathrm{M}$, si $|s| = 3\mathrm{R}$ et donc, d'après le principe du maximum,

$\sup_{|s|=\mathrm{R}} |g(s)| \leqslant \mathrm{M}$ et $\sup_{|s|=\mathrm{R}} \mathrm{Re}(h(s)) \leqslant \log \mathrm{M}$. Le lemme A.3.9 permet d'en déduire que $|h'(s)| \leqslant \frac{4\mathrm{R}\log \mathrm{M}}{(\mathrm{R}-|s|)^2}$, si $|s| < \mathrm{R}$, et comme $h'(s) = \frac{f'(s)}{f(s)} - \sum_{\rho\in\mathrm{Y}} \frac{v_\rho(f)}{s-\rho}$, cela permet de conclure.

Si $n \in \mathbf{N}$, notons Z_n l'ensemble des zéros de L dans le disque $\mathrm{D}(2+in, 4)$.

Corollaire A.3.11. — *Il existe des constantes* C_2, C_3, *telles que, si* $|n|$ *est assez grand :*
(i) $\sum_{\rho\in\mathrm{Z}_n} v_\rho(\mathrm{L}) \leqslant \mathrm{C}_2 \log|n|$;
(ii) $\left|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\right| \leqslant \mathrm{C}_3 \log|n| + \mathrm{C}_2 \log|n| (\inf_{\rho\in\mathrm{Z}_n} |s-\rho|)^{-1}$, *si* $s \in \mathrm{D}(2+in, \sqrt{10})$.

Démonstration. — On applique le lemme A.3.10 à $f(s) = \frac{\mathrm{L}(s+(2+in))}{\mathrm{L}(2+in)}$, et $\mathrm{R} = 4$; dans les notations de ce lemme, on peut prendre $\mathrm{M} = \mathrm{C}_1|n|^{21/2}$, d'après le lemme A.3.8. On en déduit que

$$\sum_{\rho\in\mathrm{Z}_n} v_\rho(\mathrm{L}) \leqslant \frac{\frac{21}{2}\log n + \log \mathrm{C}_1}{\log 2} \quad \text{et} \quad \left|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\right| \leqslant \frac{16(\frac{21}{2}\log n + \log \mathrm{C}_1)}{4-\sqrt{10}} + \sum_{\rho\in\mathrm{Z}_n} \frac{v_\rho(\mathrm{L})}{|s-\rho|},$$

si $|s-(2+in)| \leqslant \sqrt{10}$. Le résultat s'en déduit.

Corollaire A.3.12. — *Il existe* $\mathrm{C}_4 > 0$, *tel que, si* $n \in \mathbf{N}$ *est assez grand, il existe* $t_n^+ \in [n, n+1]$ *et* $t_n^- \in [-n-1, -n]$, *tels que*

$$\sup_{s\in[2+it_n^+, -1+it_n^+]} \left|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\right| \leqslant \mathrm{C}_4(\log n)^2 \quad \text{et} \quad \sup_{s\in[-1+it_n^-, 2+it_n^-]} \left|\frac{\mathrm{L}'(s)}{\mathrm{L}(s)}\right| \leqslant \mathrm{C}_4(\log n)^2.$$

Démonstration. — Comme $|\mathrm{Z}_n| \leqslant \mathrm{C}_2 \log n$, les segments $]\mathrm{Im}(\rho) - \frac{1}{2\mathrm{C}_2\log n}, \mathrm{Im}(\rho) + \frac{1}{2\mathrm{C}_2\log n}[$, pour $\rho \in \mathrm{Z}_n$ ne recouvrent pas complètement $[n, n+1]$, puisque leur réunion est un ouvert de longueur $\leqslant 1$. Il existe donc t_n^+ tel que $|\mathrm{Im}(\rho) - t_n^+| \geqslant \frac{1}{2\mathrm{C}_2\log n}$, quel que soit $\rho \in \mathrm{Z}_n$. On a alors $\inf_{\rho\in\mathrm{Z}_n} |s-\rho| \geqslant \inf_{\rho\in\mathrm{Z}_n} |\mathrm{Im}(s-\rho)| \geqslant \frac{1}{2\mathrm{C}_2\log n}$, quel que soit $s \in [2+it_n^+, -1+it_n^+]$. De même il existe $t_n^- \in [-n-1, -n]$ tel que $\inf_{\rho\in\mathrm{Z}_{-n}} |s-\rho| \geqslant \frac{1}{2\mathrm{C}_2\log n}$, quel que soit $s \in [-1+it_n^-, 2+it_n^-]$. Le (ii) du lemme A.3.11 permet de conclure (avec $\mathrm{C}_4 = 2\mathrm{C}_2^2 + 1$ par exemple).

5. Conclusion

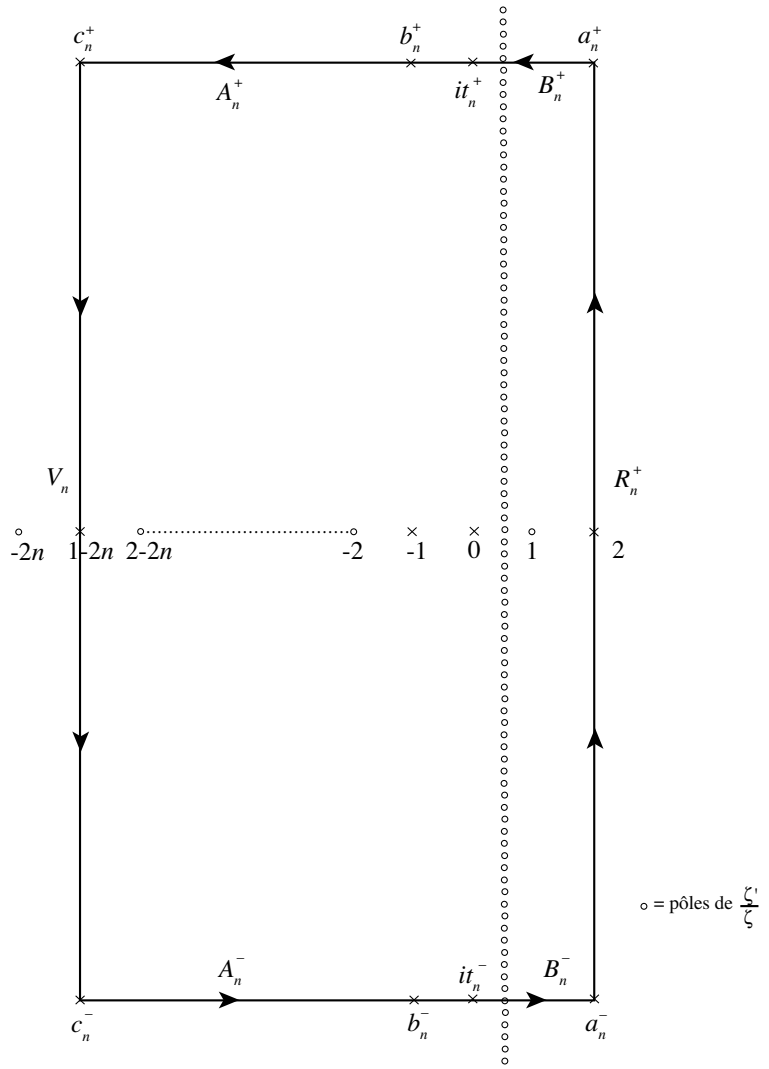
Passons à la démonstration du th. A.3.3. Pour prouver la convergence absolue de la série $\sum_{\rho\in\mathrm{Y}(\mathrm{L})} \frac{v_\rho(\mathrm{L})}{\rho(\rho+1)}$, constatons que l'ensemble Z'_n des éléments de $\mathrm{Y}(\mathrm{L})$ dont la partie imaginaire est comprise entre n et $n+1$ est inclus dans le disque $\mathrm{D}(2+in, 4)$, et donc est un sous-ensemble de Z_n. Comme $\sum_{\rho\in\mathrm{Z}_n} v_\rho(\mathrm{L}) \leqslant \mathrm{C}_2 \log|n|$, si n est assez grand, on déduit la convergence absolue de $\sum_{\rho\in\mathrm{Y}(\mathrm{L})} \frac{v_\rho(\mathrm{L})}{\rho(\rho+1)}$ de celle de $\sum_{n=1}^{+\infty} \frac{\log n}{n^2}$.

Maintenant, choisissons, pour tout n assez grand, des réels t_n^+ et t_n^- vérifiant les conclusions du cor. A.3.12. Soient a_n^+, b_n^+, c_n^+ les points $2+it_n^+$, $-1+it_n^+$, $c+1-2n+it_n^+$, et a_n^-, b_n^-, c_n^- les points $2+it_n^-$, $-1+it_n^-$, $c+1-2n+it_n^-$. On note :

- V_n le segment vertical $[c_n^+, c_n^-]$,
- A_n^+ et A_n^- les segments horizontaux $[b_n^+, c_n^+]$ et $[c_n^-, b_n^-]$,

- B_n^+ et B_n^- les segments horizontaux $[a_n^+, b_n^+]$ et $[b_n^-, a_n^-]$,
- R_n^- le chemin composé $\mathrm{B}_n^+ \cdot \mathrm{A}_n^+ \cdot \mathrm{V}_n \cdot \mathrm{A}_n^- \cdot \mathrm{B}_n^-$,
- R_n^+ le segment vertical $[a_n^-, a_n^+]$.

Alors $\mathrm{R}_n = \mathrm{R}_n^+ \cdot \mathrm{R}_n^-$ est le rectangle de sommets a_n^-, a_n^+, c_n^+ et c_n^- parcouru dans le sens direct. On note Y_n l'ensemble des pôles de F_x se trouvant à l'intérieur du rectangle R_n.



Le chemin R_n dans le cas de ζ

La formule des résidus nous donne alors

$$\int_{\mathrm{R}_n} \mathrm{F}_x(s)\, ds = \sum_{\rho \in \mathrm{Y}_n} \mathrm{Res}(\mathrm{F}_x, \rho).$$

Maintenant, $\int_{\mathrm{R}_n} \mathrm{F}_x(s)\, ds = \int_{\mathrm{R}_n^+} \mathrm{F}_x(s)\, ds + \int_{\mathrm{B}_n^+} \mathrm{F}_x(s)\, ds + \int_{\mathrm{A}_n^+ \cdot \mathrm{V}_n \cdot \mathrm{A}_n^-} \mathrm{F}_x(s)\, ds + \int_{\mathrm{B}_n^-} \mathrm{F}_x(s)\, ds$.

• $\int_{\mathrm{R}_n^+} \mathrm{F}_x(s)\,ds$ tend vers $\int_{2-i\infty}^{2+i\infty} \frac{-\mathrm{L}'(s)}{\mathrm{L}(s)} \frac{x^{s+1}}{s(s+1)}\,ds$.

• Sur B_n^+ et B_n^-, $\mathrm{F}_x(s)$ est, d'après le cor. A.3.12, majorée en valeur absolue, si $x \geqslant 1$, par $\mathrm{C}_4(\log n)^2 \frac{x^3}{|\mathrm{Im}(s)|\cdot|\mathrm{Im}(s+1)|} \leqslant \frac{x^3 \mathrm{C}_4(\log n)^2}{n^2}$. Donc $\int_{\mathrm{B}_n^+} \mathrm{F}_x(s)\,ds$ et $\int_{\mathrm{B}_n^-} \mathrm{F}_x(s)\,ds$ sont majorés en valeur absolue par $3\frac{x^3 \mathrm{C}_4(\log n)^2}{n^2}$ et tendent vers 0 quand n tend vers $+\infty$.

• Sur $\mathrm{A}_n^+ \cdot \mathrm{V}_n \cdot \mathrm{A}_n^-$, $\mathrm{F}_x(s)$ est, d'après le lemme A.3.5, majorée en valeur absolue, si $x \geqslant 1$, par $(\mathrm{C}_0 + \log n)\frac{x^3}{|s(s+1)|} \leqslant (\mathrm{C}_0 + \log n)\frac{x^3}{n^2}$, et comme la longueur de $\mathrm{A}_n^+ \cdot \mathrm{V}_n \cdot \mathrm{A}_n^-$ est $2(2n-2) + t_n^+ - t_n^- \leqslant 6n - 2$, on en déduit que $\int_{\mathrm{A}_n^+ \cdot \mathrm{V}_n \cdot \mathrm{A}_n^-} \mathrm{F}_x(s)\,ds$ tend vers 0 quand n tend vers $+\infty$.

On en déduit le théorème en faisant tendre n vers $+\infty$, et en remarquant que l'ensemble des pôles de F_x est la réunion croissante des Y_n, et donc que $\sum_{\rho\in\mathrm{Y}_n} \mathrm{Res}(\mathrm{F}_x, \rho)$ tend vers $\sum_{\mathrm{Re}(\rho)<2} \mathrm{Res}(\mathrm{F}_x, \rho)$.

Exercice A.3.13. — On note $\mathscr{N}(\mathrm{T})$ le nombre de zéros s de la fonction ζ dans la bande critique, vérifiant $0 \leqslant \mathrm{Im}(s) \leqslant \mathrm{T}$. Montrer que $\mathscr{N}(\mathrm{T}) = \frac{\mathrm{T}}{2\pi}\log\frac{\mathrm{T}}{2\pi} - \frac{\mathrm{T}}{2\pi} + \mathrm{O}(\log \mathrm{T})$. (Considérer la partie imaginaire de l'intégrale de $\frac{\xi'(s)}{\xi(s)}\,ds$ sur le rectangle de sommets $2+i$, a_n^+, b_n^+ et $-1+i$, où $\xi(s) = \frac{\Gamma(s/2)}{\pi^{s/2}}\zeta(s)$, et utiliser l'équation fonctionnelle satisfaite par ξ (rem. VII.3.8 ou ex. VII.6.6), la formule de Stirling dans le plan complexe (prop. VII.2.9) et le lemme A.3.10.)

A.4. Démonstration du théorème des nombres premiers

1. Non annulation sur la droite $\mathrm{Re}(s) = 1$

Lemme A.4.1. — *Si $\alpha, \beta \in \mathbf{C}$, et si $|z| < \inf(1, |\alpha|^{-1}, |\beta|^{-1}, |\alpha\beta|^{-1})$, alors*

$$\frac{1-\alpha\beta z^2}{(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)} = \sum_{n=0}^{+\infty}(1+\alpha+\cdots+\alpha^n)(1+\beta+\cdots+\beta^n)z^n.$$

Démonstration. — Si on multiplie par $(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)$ les deux membres de l'identité à démontrer, on obtient des séries du type $\sum_{n=0}^{+\infty} \mathrm{P}_n(\alpha,\beta)z^n$ et $\sum_{n=0}^{+\infty} \mathrm{Q}_n(\alpha,\beta)z^n$, où les P_n et Q_n sont des polynômes (en deux variables). On est ramené à prouver que $\mathrm{P}_n = \mathrm{Q}_n$ pour tout n. Or pour prouver que $\mathrm{P}_n = \mathrm{Q}_n$, il suffit de prouver que $\mathrm{P}_n = \mathrm{Q}_n$ sur un ouvert, le reste s'en déduisant par prolongement analytique. On peut donc se restreindre au cas où 1, α, β et $\alpha\beta$ sont tous distincts. Dans ce cas, la fraction rationnelle $\mathrm{F}(z) = \frac{1-\alpha\beta z^2}{(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)}$ n'a que des pôles simples, ce qui rend sa décomposition en

éléments simples particulièrement facile à calculer. Soient

$$\begin{aligned}
a_1 &= \lim_{z\to 1}(1-z)\mathrm{F}(z) = \frac{1-\alpha\beta}{(1-\alpha)(1-\beta)(1-\alpha\beta)} = \frac{1}{(1-\alpha)(1-\beta)}\,,\\
a_\alpha &= \lim_{z\to \alpha^{-1}}(1-\alpha z)\mathrm{F}(z) = \frac{1-\alpha^{-1}\beta}{(1-\alpha^{-1})(1-\alpha^{-1}\beta)(1-\beta)} = -\frac{\alpha}{(1-\alpha)(1-\beta)}\,,\\
a_\beta &= \lim_{z\to \beta^{-1}}(1-\beta z)\mathrm{F}(z) = \frac{1-\alpha\beta^{-1}}{(1-\beta^{-1})(1-\alpha\beta^{-1})(1-\alpha)} = -\frac{\beta}{(1-\alpha)(1-\beta)}\,,\\
a_{\alpha\beta} &= \lim_{z\to \alpha^{-1}\beta^{-1}}(1-\alpha\beta z)\mathrm{F}(z) = \frac{1-\alpha^{-1}\beta^{-1}}{(1-\alpha^{-1}\beta^{-1})(1-\beta^{-1})(1-\alpha^{-1})} = \frac{\alpha\beta}{(1-\alpha)(1-\beta)}\,.
\end{aligned}$$

Alors

$$\begin{aligned}
\mathrm{F}(z) =& \frac{a_1}{1-z} + \frac{a_\alpha}{1-\alpha z} + \frac{a_\beta}{1-\beta z} + \frac{a_{\alpha\beta}}{1-\alpha\beta z}\\
=& \frac{1}{(1-\alpha)(1-\beta)}\Big(\frac{1}{1-z} - \frac{\alpha}{1-\alpha z} - \frac{\beta}{1-\beta z} + \frac{\alpha\beta}{1-\alpha\beta z}\Big)\\
=& \frac{1}{(1-\alpha)(1-\beta)}\sum_{n=0}^{+\infty}\big(1-\alpha^{n+1}-\beta^{n+1}+(\alpha\beta)^{n+1}\big)z^n\\
=& \sum_{n=0}^{+\infty}\frac{(1-\alpha^{n+1})(1-\beta^{n+1})}{(1-\alpha)(1-\beta)}z^n = \sum_{n=0}^{+\infty}(1+\alpha+\cdots+\alpha^n)(1+\beta+\cdots+\beta^n)z^n.
\end{aligned}$$

Proposition A.4.2. — *Si $t\in\mathbf{R}$, alors $\mathrm{F}(s)=\zeta(2s)^{-1}\zeta(s)^2\zeta(s+it)\zeta(s-it)$ est une série de Dirichlet à coefficients positifs.*

Démonstration. — En utilisant la factorisation de ζ en facteurs d'Euler, on obtient

$$\mathrm{F}(s) = \prod_{p\in\mathscr{P}}\frac{(1-p^{-2s})}{(1-p^{-s})^2(1-p^{-s-it})(1-p^{-s+it})}.$$

On peut alors utiliser le lemme A.4.1 avec $z=p^{-s}$, $\alpha=p^{it}$ et $\beta=p^{-it}$ pour obtenir la formule

$$\mathrm{F}(s) = \prod_{p\in\mathscr{P}}\Big(\sum_{k=1}^{+\infty}|1+p^{it}+\cdots+p^{ikt}|^2p^{-ks}\Big)\,,$$

ce qui permet de conclure.

Théorème A.4.3. — *La fonction ζ ne s'annule pas sur la droite* $\mathrm{Re}(s)=1$.

Démonstration. — Supposons, par l'absurde qu'il existe $t\in\mathbf{R}$, avec $\zeta(1+it)=0$. On a alors $\zeta(1-it)=\overline{\zeta(1+it)}=0$. La fonction $\zeta(s+it)\zeta(s-it)$ a donc un zéro double en $s=1$, ce qui fait que $\mathrm{F}(s)=\zeta(2s)^{-1}\zeta(s)^2\zeta(s+it)\zeta(s-it)$ est holomorphe en $s=1$, le zéro double contrebalançant le pôle double de $\zeta(s)^2$. De même, les zéros de $\zeta(s)$ en $1+it$ et $1-it$ contrebalancent les pôles de $\zeta(s+it)$ en $1-it$ et $\zeta(s-it)$ en $1+it$. On en déduit que $\mathrm{F}(s)$ est holomorphe dans le demi-plan $\mathrm{Re}(s)>\frac{1}{2}$. De plus, comme $\zeta(2s)^{-1}$

est holomorphe au voisinage de $s = \frac{1}{2}$, et comme F est à coefficients positifs, il résulte du théorème de Landau (th. VII.1.1) que l'abscisse de convergence absolue de F est $< \frac{1}{2}$. On aboutit à une contradiction car, d'une part $\mathrm{F}(\frac{1}{2}) = 0$ puisque $\zeta(2s)^{-1} = 0$, et d'autre part $\mathrm{F}(\frac{1}{2}) > 0$ comme somme d'une série à termes positifs non tous nuls. Ceci permet de conclure.

Exercice A.4.4. — Soit χ un caractère de Dirichlet de conducteur D.

(i) Montrer que $\zeta_{\mathrm{D}}(2s)^{-1}\zeta_{\mathrm{D}}(s)^2\mathrm{L}(\chi, s+it)\mathrm{L}(\overline{\chi}, s-it)$ est une série de Dirichlet à coefficients positifs (ζ_{D} désigne la fonction ζ privée de ses facteurs d'Euler en les p divisant D, i.e. $\zeta_{\mathrm{D}}(s) = \prod_{p\in\mathscr{P},\, p\nmid \mathrm{D}} \frac{1}{1-p^{-s}}$).

(ii) En déduire que $\mathrm{L}(\chi, s)$ ne s'annule pas sur la droite $\mathrm{Re}(s) = 1$.

2. Conclusion

D'après le lemme A.2.1, pour démontrer le théorème des nombres premiers, il suffit de prouver que $\psi_1(x) \sim \frac{x^2}{2}$. Maintenant, comme ζ vérifie les propriétés (L1)–(L3) (cf. lemme A.3.1), le cor. A.2.6 et le th. A.3.3 nous fournissent la formule explicite

$$\psi_1(x) = \frac{x^2}{2} - \frac{\zeta'(0)}{\zeta(0)}x + \frac{\zeta'(-1)}{\zeta(-1)} - \sum_{\rho\in\mathrm{Y}(\zeta)} \frac{v_\rho(\zeta)x^{\rho+1}}{\rho(\rho+1)} - \sum_{r=1}^{+\infty} \frac{x^{1-2r}}{2r(2r-1)}.$$

Il en résulte que « $\psi_1(x) \sim \frac{x^2}{2}$ » est équivalent à « $\lim_{x\to+\infty} \sum_{\rho\in\mathrm{Y}(\zeta)} \frac{x^{\rho-1}}{\rho(\rho+1)} = 0$ ». Comme ζ ne s'annule pas sur la droite $\mathrm{Re}(s) = 1$, on a $\mathrm{Re}(\rho-1) < 0$, et donc $\lim_{x\to+\infty} \frac{x^{\rho-1}}{\rho(\rho+1)} = 0$, quel que soit $\rho \in \mathrm{Y}(\zeta)$. Comme de plus $|\frac{v_\rho(\zeta)x^{\rho-1}}{\rho(\rho+1)}| \leqslant |\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$, et comme la somme des $|\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$ est convergente, on peut utiliser le théorème de convergence dominée pour les séries pour intervertir sommes et limites, ce qui permet de conclure.

Exercice A.4.5. — Adapter les arguments ci-dessus pour démontrer le théorème de la progression arithmétique.

Exercice A.4.6. — On se propose de montrer, en partant de la formule explicite ci-dessus, et en utilisant la convergence absolue de la série $\sum_{\rho\in\mathrm{Y}(\zeta)} \frac{v_\rho(\zeta)}{\rho(\rho+1)}$, que le théorème des nombres premiers implique la non annulation de ζ sur la droite $\mathrm{Re}(s) = 1$. On numérote les zéros de ζ sur la droite $\mathrm{Re}(s) = 1$ sous la forme $\rho = 1 + i\tau_n$, avec $n \in \mathrm{I}$, I sous-ensemble de $\mathbf{N}$, et on pose $a_n = \frac{v_{1+i\tau_n}(\zeta)}{(1+i\tau_n)(2+i\tau_n)}$.

(i) Montrer que, si $\psi_1(x) \sim \frac{x^2}{2}$, alors $\lim_{x\to+\infty} \sum_{n\in\mathrm{I}} a_n x^{i\tau_n} = 0$.

(ii) En déduire que $\lim_{\mathrm{U}\to+\infty} \frac{1}{\mathrm{U}} \int_0^{\mathrm{U}} |f(u)|^2\, du = 0$, où $f(u) = \sum_{n\in\mathrm{I}} a_n e^{i\tau(n)u}$.

(iii) Exprimer $\lim_{\mathrm{U}\to+\infty} \frac{1}{\mathrm{U}} \int_0^{\mathrm{U}} |f(u)|^2\, du = 0$ en fonction des a_n.

(iv) Conclure.

A.5. Compléments

1. L'hypothèse de Riemann et ses conséquences

Si on suppose que l'hypothèse de Riemann est vraie, tous les ρ apparaissant dans la démonstration ci-dessus ont une partie réelle égale à $\frac{1}{2}$, ce qui permet de majorer $|\frac{v_\rho(\zeta)x^{\rho+1}}{\rho(\rho+1)}|$

par $x^{3/2}|\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$, et comme la série $\sum_{\rho\in\mathrm{Y}(\zeta)}\frac{v_\rho(\zeta)}{\rho(\rho+1)}$ est absolument convergente, on en déduit que $\psi_1(x)=\frac{1}{2}x^2+\mathrm{O}(x^{3/2})$.

On peut montrer, via l'encadrement $\psi_1(x)-\psi_1(x-1)\leqslant\psi(x)\leqslant\psi_1(x+1)-\psi_1(x)$ et la formule explicite pour $\psi_1(x)$, que l'on a $\psi(x)=x+\mathrm{O}(x^{1/2}(\log x)^2)$.

Enfin, en utilisant l'exercice A.5.2 ci-dessous, on en déduit le résultat suivant, qui montre que l'hypothèse de Riemann a des implications profondes sur la répartition des nombres premiers.

Proposition A.5.1. — *Si l'hypothèse de Riemann est vraie, alors*

$$\pi(x)=\int_2^x\frac{1}{\log t}\,dt+\mathrm{O}(x^{1/2}\log x).$$

Exercice A.5.2. — On suppose l'hypothèse de Riemann vraie, ce que l'on utilisera sous la forme $\psi(x)=x+\mathrm{O}(x^{1/2}(\log x)^2)$. Soient $\mathrm{A}(x)=\sum_{p\leqslant x}\log p$ et $\mathrm{B}(x)=\mathrm{A}(x)-x$.

(i) Montrer que $\psi(x)-\mathrm{A}(x)=\mathrm{O}(x^{1/2}\log x)$; en déduire qu'il existe $\mathrm{C}>0$ tel que $\mathrm{B}(x)\leqslant\mathrm{C}\,x^{1/2}(\log x)^2$, si $x\geqslant 2$.

(ii) Montrer que $\pi(x)=\sum_{2\leqslant n\leqslant x}\frac{\mathrm{A}(n)-\mathrm{A}(n-1)}{\log n}$.

(iii) En déduire que

$$\pi(x)=\Big(\sum_{2\leqslant n\leqslant x}\frac{1}{\log n}\Big)+\frac{\mathrm{B}([x])}{\log([x]+1)}+\Big(\sum_{n=2}^{[x]}\mathrm{B}(n)\big(\frac{1}{\log n}-\frac{1}{\log(n+1)}\big)\Big).$$

(iv) Conclure.

Remarque A.5.3. — De la Vallée Poussin a montré qu'il existe $c>0$ tel que ζ ne s'annule pas sur $\{s=\sigma+it,\ \sigma\geqslant 1-\frac{c}{\log(1+|t|)}\}$. En déplaçant la ligne d'intégration sur le contour de cette région, cela permet de préciser le terme d'erreur dans le th. des nombres premiers : il existe $a>0$ tel que $\pi(x)=\int_2^x\frac{1}{\log t}\,dt+\mathrm{O}(x\exp(-a\sqrt{\log x}))$.

2. L'hypothèse de Riemann et la fonction M de Mertens

On rappelle que l'on note μ la fonction de Moebius définie par

$$\sum_{n=1}^{+\infty}\frac{\mu(n)}{n^s}=\zeta(s)^{-1}=\prod_{p\in\mathscr{P}}(1-p^{-s}),$$

si $\mathrm{Re}(s)>0$. On a donc $\mu(n)=0$ si n est divisible par le carré d'un nombre premier et $\mu(n)=(-1)^r$, si $n=p_1\cdots p_r$, où les p_i sont des nombres premiers distincts. La *fonction* M *de Mertens* est définie par $\mathrm{M}(x)=\sum_{n\leqslant x}\mu(n)$, et F. Mertens a conjecturé que $|\mathrm{M}(x)|\leqslant\sqrt{x}$, si $x>1$. Cette conjecture, si elle avait le bon goût d'être vraie, impliquerait l'hypothèse de Riemann. En effet, la formule de sommation d'Abel nous donne

$$\zeta(s)^{-1}=\sum_{n=1}^{+\infty}\mathrm{M}(n)(n^{-s}-(n+1)^{-s}),$$

et l'hypothèse $|\mathrm{M}(n)| \leqslant \sqrt{n}$ implique que la série est absolument convergente pour $\mathrm{Re}(s) > \frac{1}{2}$, et donc que ζ ne s'annule pas pour $\mathrm{Re}(s) > \frac{1}{2}$.

On ne connaît aucun contrexemple explicite à la conjecture de Mertens, mais celle-ci n'est pas très raisonnable à cause de la *loi du logarithme itéré* (Khinchine 1924), selon laquelle, si $a_n \in \{\pm 1\}$ et $\mathrm{A}_n = \sum_{k=1}^{n} a_n$, alors presque sûrement

$$\limsup \frac{\mathrm{A}_n}{\sqrt{2n \log\log n}} = 1 \quad \text{et} \quad \liminf \frac{\mathrm{A}_n}{\sqrt{2n \log\log n}} = -1.$$

De fait, A. Odlyzko et H. te Riele ont démontré en 1985 que la conjecture de Mertens est fausse et on sait qu'il existe des contrexemples plus petits que $3,21 \cdot 10^{64}$. Par contre, la même loi du logarithme itéré ou le résultat de Hausdorff mentionné dans la note 4 du chap. VII rendent l'hypothèse de Riemann plus que plausible. D'un autre côté, le résultat de Odlyzko et te Riele relativise quelque peu les confirmations numériques de l'hypothèse de Riemann (on a vérifié que les 10^{13} premiers zéros de la fonction ζ dans la bande critique sont effectivement sur la droite $\mathrm{Re}(s) = \frac{1}{2}$).

3. L'hypothèse de Lindelöf

C'est une conjecture impliquée par l'hypothèse de Riemann, mais qui est a priori plus faible. Elle est équivalente à un des énoncés suivants (il faut travailler pas mal pour démontrer l'équivalence de ces énoncés).

- On a $|\zeta(\frac{1}{2} + it)| = \mathrm{O}(t^{\varepsilon})$ au voisinage de $+\infty$, quel que soit $\varepsilon > 0$.
- Si $\sigma > \frac{1}{2}$, et si $\mathscr{N}(\sigma, \mathrm{T})$ est le nombre de zéros de la fonction ζ vérifiant $\mathrm{Re}(s) \geqslant \sigma$ et $0 \leqslant \mathrm{Im}(s) \leqslant \mathrm{T}$, alors $\mathscr{N}(\sigma, \mathrm{T}+1) - \mathscr{N}(\sigma, \mathrm{T}) = o(\log \mathrm{T})$ quand $\mathrm{T} \to +\infty$.
- $\sum_{n \leqslant t} n^{-(\frac{1}{2} + 2i\pi\, t)} = \mathrm{O}(t^{\varepsilon})$, au voisinage de $+\infty$, quel que soit $\varepsilon > 0$.

Le deuxième de ces énoncés, que l'on peut comparer avec l'ex. A.3.13, est une conséquence de l'hypothèse de Riemann qui peut s'énoncer sous la forme $\mathscr{N}(\sigma, \mathrm{T}) = 0$, quels que soient $\sigma > \frac{1}{2}$ et $\mathrm{T} \geqslant 0$. Le troisième ne fait intervenir que des sommes finies et donc a l'air parfaitement innocent.

Contrairement à l'hypothèse de Riemann, il y a des progrès à intervalles réguliers concernant l'hypothèse de Lindelöf. Par exemple, G. Kolesnik a prouvé en 1982 que

$$\zeta(1/2 + it) = \mathrm{O}(t^{1/6 - 1/216 + \varepsilon}), \quad \text{quel que soit } \varepsilon > 0.$$

F. Bombieri et H. Iwaniec ont démontré en 1986 que

$$\zeta(1/2 + it) = \mathrm{O}(t^{1/6 - 1/28 + \varepsilon}), \quad \text{quel que soit } \varepsilon > 0.$$

APPENDICE B

VOLUME DE $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$

Cet appendice est consacré au calcul du volume de $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ (voir plus loin pour la signification exacte de cette notion), résultat dû à Siegel (1945). Ce calcul se fait par récurrence sur n en utilisant astucieusement la formule de Poisson selon une idée de Weil (1946). Le résultat (th. B.1.4) est à rapprocher de la formule (prop. B.1.1) pour le cardinal du groupe $\mathbf{SL}_n(\mathbf{F}_p)$: convenablement réinterprétée, cette formule dit que le volume du groupe $\mathbf{SL}_n(\mathbf{Z}_p)$ est $\prod_{k=2}^{n}\left(1-\frac{1}{p^k}\right)$, et la formule pour le volume de $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ donne lieu à une *formule du produit* [1]

$$\mathrm{Vol}(\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z}))\cdot\prod_{p\in\mathscr{P}}\mathrm{Vol}(\mathbf{SL}_n(\mathbf{Z}_p))=1.$$

Il s'agit là d'un cas particulier de formules très générales (dont certaines, comme la conjecture de Bloch-Kato mentionnée dans l'introduction, sont largement conjecturales), indiquant des liens profonds et encore assez mystérieux entre les mondes réels et p-adiques.

B.1. Volume d'objets arithmétiques

1. Résultats

Proposition B.1.1. — *Si* K *est un corps fini de cardinal* q*, et si* $n\geqslant 2$*, alors*

$$|\mathbf{SL}_n(\mathrm{K})|=q^{n-1}\prod_{k=2}^{n}(q^n-q^{n-k})=q^{n^2-1}\prod_{k=2}^{n}\left(1-\frac{1}{q^k}\right).$$

Démonstration. — L'application $g\mapsto \det g$, de $\mathbf{GL}_n(\mathrm{K})$ dans K^*, est un morphisme surjectif de groupes dont le noyau est $\mathbf{SL}_n(\mathrm{K})$. Comme $|\mathrm{K}^*|=q-1$, on en déduit que $|\mathbf{SL}_n(\mathrm{K})|=\frac{1}{q-1}|\mathbf{GL}_n(\mathrm{K})|$.

Par ailleurs, si $g\in\mathbf{GL}_n(\mathrm{K})$, les n vecteurs colonnes de g forment une base de K^n et on obtient de la sorte une bijection de $\mathbf{GL}_n(\mathrm{K})$ sur l'ensemble des bases de K^n. Comme

1. Si $\mathbf{A}$ désigne l'anneau des adèles de $\mathbf{Q}$ (cf. n° 1 du § G.2), cette formule peut se réécrire sous la forme plus frappante $\mathrm{Vol}(\mathbf{SL}_n(\mathbf{A})/\mathbf{SL}_n(\mathbf{Q}))=1$.

une base de K^n est constituée d'un premier vecteur e_1 non nul ($q^n - 1$ choix), d'un second e_2 n'appartenant pas à la droite engendrée par e_1 ($q^n - q$ choix), d'un troisième e_3 n'appartenant pas au plan engendré par e_1 et e_2 ($q^n - q^2$ choix)..., il y a au total $(q^n - 1)\cdots(q^n - q^{n-1})$ bases de K^n.

On en déduit le résultat.

Soit $n \geqslant 2$. Si $\mathrm{A} \in \mathbf{M}_n(\mathbf{R})$, et si $1 \leqslant \alpha, \beta \leqslant n$, on définit (cf. alinéa 7.6.2 du Vocabulaire) le *cofacteur* $\mathrm{M}_{\alpha,\beta}(\mathrm{A})$ comme $(-1)^{\alpha+\beta}$ fois le déterminant de la matrice $(n-1)\times(n-1)$ obtenue en retirant la α-ième ligne et la β-ième colonne. En développant $\det \mathrm{A}$ par rapport à la α-ième ligne, on obtient

$$\det \mathrm{A} = \sum_{\beta=1}^{n} x_{\alpha,\beta}\mathrm{M}_{\alpha,\beta}(\mathrm{A}).$$

Pour alléger les notations, on note G le groupe $\mathbf{SL}_n(\mathbf{R})$ et Γ son sous-groupe $\mathbf{SL}_n(\mathbf{Z})$.

Si $1 \leqslant \alpha, \beta \leqslant n$, on note $\mathrm{I}(\alpha,\beta)$ l'ensemble $\{1,\dots,n\}^2 - \{(\alpha,\beta)\}$ et $\mathrm{E}_{\alpha,\beta} = \mathbf{R}^{\mathrm{I}(\alpha,\beta)}$ le $\mathbf{R}$-espace vectoriel de dimension $m = n^2 - 1$ des $(x_{i,j})_{(i,j)\in\mathrm{I}(\alpha,\beta)}$. On note $\pi_{\alpha,\beta} : \mathbf{M}_n(\mathbf{R}) \to \mathrm{E}_{\alpha,\beta}$ l'application linéaire envoyant $(a_{i,j})_{1\leqslant i,j\leqslant n}$ sur $(a_{i,j})_{(i,j)\neq(\alpha,\beta)}$. Comme $\mathrm{M}_{\alpha,\beta}$ ne fait pas intervenir $x_{\alpha,\beta}$, on peut ausi voir $\mathrm{M}_{\alpha,\beta}$ comme une fonction sur $\mathrm{E}_{\alpha,\beta}$, et on note $\Omega_{\alpha,\beta}$ l'ouvert de $\mathrm{E}_{\alpha,\beta}$ défini par la condition $\mathrm{M}_{\alpha,\beta} \neq 0$. Si $x \in \Omega_{\alpha,\beta}$, la formule ci-dessus pour $\det \mathrm{A}$ montre qu'il existe $\iota_{\alpha,\beta}(x) \in \mathrm{G}$ unique vérifiant $\pi_{\alpha,\beta}(\iota_{\alpha,\beta}(x)) = x$.

On dit que $\phi : \mathrm{G} \to \mathbf{R}^+$ est mesurable si $\phi \circ \iota_{n,n}$ est mesurable sur $\Omega_{n,n}$, et on définit $\int_{\mathrm{G}} \phi(g)\, dg$ par la formule $\int_{\mathrm{G}} \phi(g)\, dg = \int_{\Omega_{n,n}} \phi \circ \iota_{n,n} \frac{dx}{|\mathrm{M}_{n,n}|}$.

Proposition B.1.2. — *Si $\phi : \mathrm{G} \to \overline{\mathbf{R}}_+$ est mesurable, alors pour tout $\gamma \in \mathrm{G}$, on a $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\mathrm{G}} \phi(g)\, dg = \int_{\mathrm{G}} \phi(\gamma g)\, dg$. Autrement dit, dg est une mesure de Haar* (i.e. invariante) *à droite et à gauche sur* G.

Remarque B.1.3. — Le rôle privilégié joué par le couple (n,n) peut sembler surprenant, mais les calculs effectués (cf. n° 2 du § B.2) pour prouver que dg est invariante par multiplication par une matrice de permutation montrent que $\int_{\mathrm{G}} \phi(g)\, dg = \int_{\Omega_{\alpha,\beta}} \phi \circ \iota_{\alpha,\beta} \frac{dx}{|\mathrm{M}_{\alpha,\beta}|}$, pour n'importe quel couple (α,β), et donc que la situation est, en fait, parfaitement symétrique.

Si $\phi : \mathrm{G} \to \mathbf{R}_+$ est invariante à droite par Γ (i.e. si $\phi(g\gamma) = \phi(g)$ pour tous $g \in \mathrm{G}$ et $\gamma \in \Gamma$), alors $\int_{\mathrm{D}} \phi\, dg$ ne dépend pas du choix d'un domaine fondamental D de G/Γ (cf. lemme B.1.5). On note $\int_{\mathrm{G}/\Gamma} \phi\, dg$ cette quantité.

On définit le volume de $\mathrm{G}/\Gamma = \mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ par la formule $\mathrm{Vol}(\mathrm{G}/\Gamma) = \int_{\mathrm{G}/\Gamma} dg$.

Théorème B.1.4. — *Si $n \geqslant 2$, le volume de $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ est fini et donné par la formule*

$$\mathrm{Vol}(\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})) = \prod_{k=2}^{n} \zeta(k).$$

2. Intégration sur un quotient

Le lemme B.1.5 ci-dessous est une généralisation directe de ce que nous avons fait au n° 2 du § IV.3 (cf. lemme IV.3.16) pour définir l'intégration sur $\mathbf{R}^n/\Lambda$, où Λ est un réseau de $\mathbf{R}^n$. On peut l'appliquer à G car l'intégration sur G est définie comme l'intégration sur $\Omega_{n,n}$, ce qui fait qu'elle vérifie bien les conditions ci-dessous. Le lemme B.1.6 et son corollaire sont, quant à eux, des versions du th. de Fubini sur $\mathbf{N} \times \mathrm{X}$.

Soit G un groupe muni d'une mesure de Haar à droite (notée dg) : on dispose des objets suivants.

• L'espace $\mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$ des fonctions mesurables positives sur G, qui est stable par combinaisons linéaires à coefficients positifs, par $(f,g) \mapsto \inf(f,g)$ et $(f,g) \mapsto \sup(f,g)$, et par limite simple.

• Une intégration $\phi \mapsto \int_{\mathrm{G}} \phi\, dg$ de $\mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$ dans $\overline{\mathbf{R}}_+$,

— qui est linéaire : $\int_{\mathrm{G}} (\lambda_1\phi_1 + \lambda_2\phi_2)\, dg = \lambda_1 \int_{\mathrm{G}} \phi_1\, dg + \lambda_2 \int_{\mathrm{G}} \phi_2\, dg$, quels que soient $\phi_1, \phi_2 \in \mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$ et $\lambda_1, \lambda_2 \geqslant 0$,

— vérifie le théorème de convergence monotone : $\int_{\mathrm{G}} \sum_{i\in\mathrm{I}} \phi_i\, dg = \sum_{i\in\mathrm{I}} \int_{\mathrm{G}} \phi_i\, dg$, si I est dénombrable et les ϕ_i appartiennent à $\mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$,

— est invariante par translation à droite : $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\mathrm{G}} \phi(g)\, dg$, quels que soient $\phi \in \mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$ et $\gamma \in \Gamma$.

• L'espace $\mathscr{L}^1(\mathrm{G})$ des fonctions sommables (i.e. des $\phi : \mathrm{G} \to \mathbf{C}$ telles que $\mathrm{Re}^+(i^k\phi)$ appartienne à $\mathrm{Mes}(\mathrm{G}, \overline{\mathbf{R}}_+)$ et vérifie $\int_{\mathrm{G}} \mathrm{Re}^+(i^k\phi) < +\infty$, si $k \in \{0,1,2,3\}$) et d'une intégration $\phi \mapsto \int_{\mathrm{G}} \phi\, dg$ de $\mathscr{L}^1(\mathrm{G})$ dans $\mathbf{C}$, définie par $\int_{\mathrm{G}} \phi\, dg = \sum_{i=0}^{3} i^{-k} \int_{\mathrm{G}} \mathrm{Re}^+(i^k\phi)\, dg$, qui est linéaire, invariante par translation à droite, et vérifie le théorème de convergence dominée.

• Les notions d'ensemble mesurable, d'ensemble de mesure nulle, de fonctions nulle p.p. définies de la manière habituelle : $\mathrm{X} \subset \mathrm{G}$ *est mesurable* si sa fonction caractéristique l'est, il est *de mesure nulle* s'il est mesurable et si $\int_{\mathrm{X}} dg$ (défini comme étant $\int_{\mathrm{G}} \mathbf{1}_{\mathrm{X}}\, dg$) est nul, et ϕ *est nulle p.p.* si $\{g,\ \phi(g) \neq 0\}$ est de mesure nulle ; on a $\int_{\mathrm{G}} \phi\, dg = 0$ si ϕ est nulle p.p.

Soit Γ un sous-groupe dénombrable de G. Un *domaine fondamental* D de G/Γ est un sous-ensemble mesurable de G tel que l'on puisse écrire tout élément de G de manière unique sous la forme $g = g_0\gamma$, avec $g_0 \in \mathrm{D}$ et $\gamma \in \Gamma$. Ceci peut aussi se réécrire sous la forme $\sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}\gamma}(g) = 1$, pour tout $g \in \mathrm{G}$, où $\mathrm{D}\gamma = \{g_0\gamma,\ g_0 \in \mathrm{D}\}$. Plus généralement, un sous-ensemble mesurable D de G est *presque un domaine fondamental de* G/Γ si $g \mapsto \sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}\gamma}(g) = 1$ p.p.

On dit qu'une fonction ϕ sur G est *invariante à droite* par Γ si $\phi(g\gamma) = \phi(g)$ pour tous $g \in \mathrm{G}$ et $\gamma \in \Gamma$.

Lemme B.1.5. — *Si* $\phi : \mathrm{G} \to \overline{\mathbf{R}}_+$ *est mesurable et invariante à droite par* Γ*, alors* $\int_{\mathrm{D}} \phi\, dg$ *ne dépend pas de* D*, si* D *est presque un domaine fondamental de* G/Γ*.*

Démonstration. — Soient $\mathrm{D}_1, \mathrm{D}_2$ deux sous-ensembles de G qui sont presque des domaines fondamentaux de G/Γ. En utilisant successivement :

– l'identité $1 = \sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}_2\gamma}$ p.p.,

– le théorème de convergence monotone pour échanger somme et intégrale,

– le changement de variable $h = g\gamma$ et l'invariance de ϕ et dg par ce changement de variable,

– de nouveau le théorème de convergence monotone,

– l'identité $\sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}_1\gamma^{-1}} = 1$ p.p.,

on obtient

$$\begin{aligned}\int_{\mathrm{D}_1} \phi = \int_{\mathrm{G}} \mathbf{1}_{\mathrm{D}_1}\phi = \int_{\mathrm{G}} \big(\sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}_2\gamma}\big)\mathbf{1}_{\mathrm{D}_1}\phi = \sum_{\gamma\in\Gamma} \int_{\mathrm{G}} \mathbf{1}_{\mathrm{D}_2\gamma}\mathbf{1}_{\mathrm{D}_1}\phi \\ = \sum_{\gamma\in\Gamma} \int_{\mathrm{G}} \mathbf{1}_{\mathrm{D}_2}\mathbf{1}_{\mathrm{D}_1\gamma^{-1}}\phi = \int_{\mathrm{G}} \big(\sum_{\gamma\in\Gamma} \mathbf{1}_{\mathrm{D}_1\gamma^{-1}}\big)\mathbf{1}_{\mathrm{D}_2}\phi = \int_{\mathrm{G}} \mathbf{1}_{\mathrm{D}_2}\phi = \int_{\mathrm{D}_2} \phi,\end{aligned}$$

ce qui permet de conclure.

Si $\phi : \mathrm{G} \to \overline{\mathbf{R}}_+$ est mesurable et invariante à droite par Γ, on note $\int_{\mathrm{G}/\Gamma} \phi\, dg$ la quantité $\int_{\mathrm{D}} \phi\, dg$, où D est presque un domaine fondamental de G/Γ. Si $\phi : \mathrm{G} \to \mathbf{C}$ est invariante à droite par Γ, on dit que ϕ *est sommable sur* G/Γ, si les fonctions $\mathrm{Re}^+(i^k\phi)$ sont mesurables et vérifient $\int_{\mathrm{G}/\Gamma} \mathrm{Re}^+(i^k\phi) < +\infty$, si $k \in \{0,1,2,3\}$; on pose alors $\int_{\mathrm{G}/\Gamma} \phi\, dg = \sum_{i=0}^{3} i^{-k} \int_{\mathrm{G}/\Gamma} \mathrm{Re}^+(i^k\phi)\, dg$.

Lemme B.1.6. — *Soient $\Gamma_1 \subset \Gamma_2$ deux sous-groupes dénombrables de* G*, et $\phi : \mathrm{G} \to \overline{\mathbf{R}}_+$ une fonction mesurable, invariante à droite par Γ_1.*

(i) *Si $g \in \mathrm{G}$, alors $\sum_{s\in\mathrm{S}} \phi(gs) \in \overline{\mathbf{R}}_+$ ne dépend pas du choix du système* S *de représentants de Γ_2/Γ_1 dans Γ_2.*

(ii) *La fonction $\int_{\Gamma_2/\Gamma_1} \phi$ ainsi définie est invariante à droite par Γ_2.*

(iii) $\int_{\mathrm{G}/\Gamma_1} \phi\, dg = \int_{\mathrm{G}/\Gamma_2} \big(\int_{\Gamma_2/\Gamma_1} \phi\big)\, dg$.

Démonstration. — Si $\mathrm{S}_1, \mathrm{S}_2$ sont deux systèmes de représentants de Γ_2/Γ_1, il existe une (unique) bijection $\alpha : \mathrm{S}_1 \to \mathrm{S}_2$ telle que $\theta(s_1) = \alpha(s_1)^{-1}s_1 \in \Gamma_1$. On a alors

$$\sum_{s_1\in\mathrm{S}_1} \phi(gs_1) = \sum_{s_1\in\mathrm{S}_1} \phi(g\alpha(s_1)\theta(s_1)) = \sum_{s_1\in\mathrm{S}_1} \phi(g\alpha(s_1)) = \sum_{s_2\in\alpha(\mathrm{S}_1)} \phi(gs_2) = \sum_{s_2\in\mathrm{S}_2} \phi(gs_2),$$

ce qui démontre le (i).

Maintenant, si $\gamma \in \Gamma_2$ et si S_1 est un système de représentants de Γ_2/Γ_1, il en est de même de $\mathrm{S}_2 = \{\gamma s_1,\ s_1 \in \mathrm{S}_1\}$ (en effet, si $s_1, s_1' \in \mathrm{S}_1$ et s'il existe $\gamma_1 \in \Gamma_1$ tel que $\gamma s_1' = \gamma s_1\gamma_1$, alors $s_1' = s_1\gamma_1$, et donc $s_1' = s_1$, ce qui prouve que $\mathrm{S}_2 \to \Gamma_2/\Gamma_1$ est injective ; si $\gamma' \in \Gamma_2$, il existe $s_1 \in \mathrm{S}_1$ tel que $\gamma^{-1}\gamma' \in s_1\Gamma_1$, et donc $\gamma' \in \gamma s_1\Gamma_1$, ce qui prouve que

$S_2 \to \Gamma_2/\Gamma_1$ est surjective). Il en résulte que

$$\big(\int_{\Gamma_2/\Gamma_1} \phi\big)(g\gamma) = \sum_{s_1 \in S_1} \phi(g\gamma s_1) = \sum_{s_2 \in S_2} \phi(g s_2) = \big(\int_{\Gamma_2/\Gamma_1} \phi\big)(g),$$

ce qui démontre le (ii).

Passons à la démonstration du (iii). Soient D un domaine fondamental de G/Γ_2 et S un système de représentants de Γ_2/Γ_1. Par définition, le membre de droite est égal à $\int_D \sum_{s\in S} \phi(gs)\, dg$, et comme dg est invariante par translation à droite par un élément de G, il est aussi égal à $\int_\Delta \phi\, dg$, où Δ est la réunion disjointe (car $S \subset \Gamma_2$) des Ds, pour $s \in S$. Pour conclure, il suffit donc de prouver que Δ est un domaine fondamental de G/Γ_1. Or

$$\sum_{\gamma_1 \in \Gamma_1} \mathbf{1}_\Delta(g\gamma_1) = \sum_{\gamma_1 \in \Gamma_1} \sum_{s \in S} \mathbf{1}_D(gs\gamma_1),$$

et comme S est un système de représentants de Γ_2/Γ_1, l'ensemble $\{s\gamma_1,\ s \in S,\ \gamma_1 \in \Gamma_1\}$ est égal à Γ_2. On a donc $\sum_{\gamma_1\in\Gamma_1} \sum_{s\in S} \mathbf{1}_D(gs\gamma_1) = \sum_{\gamma_2\in\Gamma_2} \mathbf{1}_D(g\gamma_2)$, et comme D est un domaine fondamental de G/Γ_2, cette dernière quantité est égale à 1, pour tout $g \in G$.

Ceci permet de conclure.

Corollaire B.1.7. — *Soit $\phi : G \to \mathbf{C}$ une fonction invariante à droite par Γ_1, et sommable sur G/Γ_1.*

(i) *La série $\sum_{s\in S} \phi(gs)$ converge absolument p.p., et sa somme ne dépend pas du choix du système S de représentants de Γ_2/Γ_1 dans Γ_2.*

(ii) *La fonction $\int_{\Gamma_2/\Gamma_1} \phi$ ainsi définie p.p. est invariante à droite par Γ_2 et sommable sur G/Γ_2.*

(iii) $\int_{G/\Gamma_1} \phi\, dg = \int_{G/\Gamma_2} \big(\int_{\Gamma_2/\Gamma_1} \phi\big)\, dg$.

Démonstration. — Le (iii) du lemme B.1.6 montre que $\int_{G/\Gamma_2} \big(\int_{\Gamma_2/\Gamma_1} |\phi|\big)\, dg < +\infty$, et donc que $\int_{\Gamma_2/\Gamma_1} |\phi| < +\infty$ p.p., ce qui permet de démontrer la convergence absolue p.p. de la série $\sum_{s\in S} \phi(gs)$. Le reste s'en déduit en reprenant les calculs faits pour démontrer le lemme B.1.6 et en utilisant le fait que l'on peut réarranger comme on veut une série absolument convergente (pour démontrer les (i) et (ii)), et le théorème de convergence dominée (pour démontrer le (iii)).

3. Un dévissage du groupe $\mathbf{SL}_n(\mathbf{R})$

Soit $n \geqslant 2$. On note :

- G' le groupe $\mathbf{SL}_{n-1}(\mathbf{R})$,
- Γ' le sous-groupe $\mathbf{SL}_{n-1}(\mathbf{Z})$ de G',
- c (resp. c') le volume de G/Γ (resp. G'/Γ') ; si $n = 2$, alors $c' = 1$.

On cherche à prouver que $c = \zeta(n)c'$. Le cor. B.1.10 fait apparaître c' dans une intégrale sur G/Γ. Pour relier c et c', on est amené à dévisser le groupe G de manière à faire apparaître G'. De manière un peu plus précise, on montre que G est presque égal à

$\mathrm{W} \times \mathrm{V} \times \mathrm{G}'$, où W et V sont des $\mathbf{R}$-espaces vectoriels naturellement isomorphes à $\mathbf{R}^n$ et $\mathbf{R}^{n-1}$ respectivement, et pour cela, on est conduit à introduire les objets suivants.

• Soit W l'espace des vecteurs colonnes à n lignes. L'application envoyant $w \in \mathrm{W}$ sur le n-uplet de ses coordonnées $(w_1, \dots, w_n)$ induit un isomorphisme naturel de W sur $\mathbf{R}^n$; on note W_* l'ouvert complémentaire de l'hyperplan d'équation $w_1 = 0$. Si $w \in \mathrm{W}_*$ a pour coordonnées $w_1, \dots, w_n$, on note $\alpha(w)$ la matrice diagonale $(n-1) \times (n-1)$ dont tous les coefficients diagonaux sont des 1 sauf le dernier, qui est égal à w_1^{-1}, et on note $\iota_{\mathrm{W}}(w)$ la matrice par blocs $\left(\begin{smallmatrix} w_1 & 0 \\ w' & \alpha(w) \end{smallmatrix}\right)$, où w' est le vecteur colonne de coordonnées $w_2, \dots, w_n$. Comme $\det \alpha(w) = w_1^{-1}$, on a $\det \iota_{\mathrm{W}}(w) = 1$, et donc $\iota_{\mathrm{W}}(w) \in \mathrm{G}$.

• Soit V l'espace des vecteurs lignes à $n-1$ colonnes. L'application envoyant $v \in \mathrm{V}$ sur le $n-1$-uplet de ses coordonnées $(v_1, \dots, v_{n-1})$ induit un isomorphisme naturel de V sur $\mathbf{R}^{n-1}$. On note ι_{V} l'application envoyant le vecteur ligne $v \in \mathrm{V}$ sur la matrice par blocs $\left(\begin{smallmatrix} 1 & v \\ 0 & 1_{n-1} \end{smallmatrix}\right)$. Un calcul immédiat montre que ι_{V} est un morphisme de groupes de V dans G (i.e. $\iota_{\mathrm{V}}(v_1 + v_2) = \iota_{\mathrm{V}}(v_1)\iota_{\mathrm{V}}(v_2)$).

• On note $\iota_{\mathrm{G}'} : \mathrm{G}' \to \mathrm{G}$ le morphisme de groupes envoyant $g' \in \mathrm{G}'$ sur la matrice par blocs $\left(\begin{smallmatrix} 1 & 0 \\ 0 & g' \end{smallmatrix}\right)$.

• Soit $\mathrm{H} \subset \mathrm{G}$ l'ensemble des $g \in \mathrm{G}$ dont les coefficients de la première colonne sont $1, 0, \dots, 0$. Si $h = \left(\begin{smallmatrix} 1 & v \\ 0 & g' \end{smallmatrix}\right)$, on définit $\pi_{\mathrm{V}}(h) \in \mathrm{V}$ et $\pi_{\mathrm{G}'}(h) \in \mathrm{G}'$ par $\pi_{\mathrm{V}}(h) = v$ et $\pi_{\mathrm{G}'}(h) = g'$. On a alors $h = \iota_{\mathrm{G}'}(\pi_{\mathrm{G}'}(h))\iota_{\mathrm{V}}(\pi_{\mathrm{V}}(h))$ et ceci est l'unique écriture de h sous la forme $h = \iota_{\mathrm{G}'}(g')\iota_{\mathrm{V}}(v)$, avec $g' \in \mathrm{G}'$ et $v \in \mathrm{V}$. De plus, $\pi_{\mathrm{G}'} : \mathrm{H} \to \mathrm{G}'$ est un morphisme de groupes et on a $\pi_{\mathrm{V}}(h_1 h_2) = \pi_{\mathrm{V}}(h_1)\pi_{\mathrm{G}'}(h_2) + \pi_{\mathrm{V}}(h_2)$, comme on le voit sur la formule $\left(\begin{smallmatrix} 1 & v_1 \\ 0 & g_1' \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & v_2 \\ 0 & g_2' \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & v_1 g_2' + v_2 \\ 0 & g_1' g_2' \end{smallmatrix}\right)$.

• Soit $\pi_{\mathrm{W}} : \mathrm{G} \to \mathrm{W}$ l'application envoyant g sur sa première colonne. L'image de G par π_{W} est $\mathrm{W} - \{0\}$ et on a $\pi_{\mathrm{W}} \circ \iota_{\mathrm{W}} = \mathrm{id}$ sur W_*. De plus, $\pi_{\mathrm{W}}(g_1) = \pi_{\mathrm{W}}(g_2)$ si et seulement si il existe $h \in \mathrm{H}$ tel que $g_2 = g_1 h$: en effet, si $e_1, \dots, e_n$ est la base canonique de $\mathrm{W} \cong \mathbf{R}^n$, alors $\pi_{\mathrm{W}}(g_1) = \pi_{\mathrm{W}}(g_2)$ équivaut à $g_1(e_1) = g_2(e_1)$, et donc à $g_1^{-1} g_2(e_1) = e_1$, ou encore à $g_1^{-1} g_2 \in \mathrm{H}$.

Si $(w, v, g') \in \mathrm{W}_* \times \mathrm{V} \times \mathrm{G}'$, soit $\varphi(w, v, g') = \iota_{\mathrm{W}}(w)\iota_{\mathrm{G}'}(g')\iota_{\mathrm{V}}(v)$. Alors $\varphi(w, v, g')$ est la matrice par blocs $\left(\begin{smallmatrix} w_1 & w_1 v \\ w' & w' v + \alpha(w) g' \end{smallmatrix}\right)$. Comme $\iota_{\mathrm{V}}(v)\iota_{\mathrm{G}'}(g') \in \mathrm{H}$, cela implique que $\pi_{\mathrm{W}}(\varphi(w, v, g')) = \pi_{\mathrm{W}}(\iota_{\mathrm{W}}(w)) = w$. Réciproquement, si $\pi_{\mathrm{W}}(g) \in \mathrm{W}_*$, il existe un unique triplet $(w, v, g') \in \mathrm{W}_* \times \mathrm{V} \times \mathrm{G}'$ tel que $g = \varphi(w, v, g')$. Plus précisément,

$$w = \pi_{\mathrm{W}}(g) \text{ et } v = \pi_{\mathrm{V}}(h),\ g' = \pi_{\mathrm{G}'}(h),\ \text{où } h = (\iota_{\mathrm{W}}(\pi_{\mathrm{W}}(g)))^{-1} g.$$

En résumé, φ induit une bijection de $\mathrm{W}_* \times \mathrm{V} \times \mathrm{G}'$ (qui est presque égal à $\mathrm{W} \times \mathrm{V} \times \mathrm{G}'$) sur l'ensemble $\mathrm{G}_* = \pi_{\mathrm{W}}^{-1}(\mathrm{W}_*)$ des $g \in \mathrm{G}$ dont le premier coefficient est non nul (cet ensemble est presque égal à G).

La formule du changement de variable fournit, après un calcul sans grand mystère, mais un peu désagréable à rédiger (cf. n° 3 du § B.2), le résultat suivant, où dw (resp. dv) est la

mesure de Lebesgue $dw_1 \cdots dw_n$ (resp. $dv_1 \cdots dv_{n-1}$) sur W (resp. V) et dg' est la mesure sur $\mathrm{G}' = \mathbf{SL}_{n-1}(\mathbf{R})$ de la prop. B.1.2 (en remplaçant n par $n-1$).

Lemme B.1.8. — *Si $\phi : \mathrm{G} \to \mathbf{R}_+$ est mesurable, alors*

$$\int_{\mathrm{G}} \phi \, dg = \int_{\mathrm{W}_* \times \mathbf{R}^{n-1} \times \mathrm{G}'} \phi \circ \varphi \; dw \, dv \, dg'.$$

4. Intégration sur $\mathbf{R}^n$ et sur $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$

On note Λ le sous-groupe de V des vecteurs à coordonnées dans $\mathbf{Z}$; c'est un réseau de V. On note Θ l'ensemble des éléments de H à coordonnées entières. C'est un sous-groupe de H, et c'est aussi l'ensemble des $h \in \mathrm{H}$ tels que $\pi_{\mathrm{V}}(h) \in \Lambda$ et $\pi_{\mathrm{G}'}(h) \in \Gamma'$.

Soient D' et D'' des domaines fondamentaux de G'/Γ' et V/Λ respectivement. On a $\int_{\mathrm{D}''} dv = 1$ (on peut prendre $\mathrm{D}'' = [0,1[^{n-1}$) et $\int_{\mathrm{D}'} dg' = c'$ par définition de c'.

Lemme B.1.9. — *Soit $\phi : \mathbf{R}^n \to \overline{\mathbf{R}}_+$ une fonction mesurable, invariante à droite par Θ. Alors*

$$\int_{\varphi(\mathrm{W}_* \times \mathrm{D}'' \times \mathrm{D}')} \phi \, dg = \int_{\mathrm{G}/\Gamma} \Big(\int_{\Gamma/\Theta} \phi \Big) \, dg.$$

Démonstration. — D'après le lemme B.1.6, le membre de droite est égal à $\int_{\mathrm{G}/\Theta} \phi \, dg$, et il suffit donc de vérifier que $\Delta_0 = \varphi(\mathrm{W}_* \times \mathrm{D}'' \times \mathrm{D}')$ est presque un domaine fondamental de G/Θ. On va montrer, plus précisément, que Δ_0 est un domaine fondamental de G_*/Θ.

Il s'agit donc de prouver que tout élément g de G_* peut s'écrire, de manière unique, sous la forme $g = \iota_{\mathrm{W}}(w_0)\iota_{\mathrm{G}'}(g'_0)\iota_{\mathrm{V}}(v_0)\theta$, avec $w_0 \in \mathrm{W}_*$, $g'_0 \in \mathrm{D}'$, $v_0 \in \mathrm{D}''$ et $\theta \in \Theta$. En appliquant π_{W} à l'égalité ci-dessus, on voit que l'on doit avoir $w_0 = \pi_{\mathrm{W}}(g)$, et on peut alors écrire g sous la forme $\iota_{\mathrm{W}}(w_0)h$, avec $h \in \mathrm{H}$. Comme D' est un domaine fondamental de G'/Γ', il existe $g'_0 \in \mathrm{D}'$ et $\gamma \in \Gamma'$, uniques, tels que $\pi_{\mathrm{G}'}(h) = g'_0\gamma$. On a alors $h = \iota_{\mathrm{G}'}(g'_0)\iota_v(v)\iota_{\mathrm{G}'}(\gamma)$, où $v \in \mathrm{V}$ est déterminé de manière unique. Comme D'' est un domaine fondamental de V/Λ, il existe $v_0 \in \mathrm{D}''$ et $\nu \in \Lambda$, uniques, tels que $v = v_0 + \nu$. On a alors $g = \iota_{\mathrm{W}}(w_0)\iota_{\mathrm{G}'}(g'_0)\iota_{\mathrm{V}}(v_0)\theta$, avec $\theta = \iota_{\mathrm{V}}(\nu)\iota_{\mathrm{G}'}(\gamma) \in \Theta$. Ceci prouve l'existence d'une décomposition de g sous la forme souhaitée. L'unicité se démontre en reprenant les arguments ci-dessus et en utilisant l'unicité des décompositions à chacune des étapes.

Corollaire B.1.10. — (i) *Si $\phi : \mathrm{W} \to \overline{\mathbf{R}}_+$ est mesurable, alors*

$$c' \int_{\mathrm{W}} \phi \, dw = \int_{\mathrm{G}/\Gamma} \Big(\int_{\Gamma/\Theta} \phi \circ \pi_{\mathrm{W}} \Big) \, dg.$$

(ii) *Si $\phi : \mathrm{W} \to \overline{\mathbf{R}}_+$ est sommable, alors $\int_{\Gamma/\Theta} \phi \circ \pi_{\mathrm{W}}$ est sommable sur G/Γ et*

$$c' \int_{\mathrm{W}} \phi \, dw = \int_{\mathrm{G}/\Gamma} \Big(\int_{\Gamma/\Theta} \phi \circ \pi_{\mathrm{W}} \Big) \, dg.$$

Démonstration. — Le (ii) se déduit formellement du (i). Comme $\phi \circ \pi_{\mathrm{W}}$ est invariante à droite par H, et donc par Θ, le membre de droite est, d'après le lemme B.1.9, égal à $\int_{\varphi(\mathrm{W}_* \times \mathrm{D}' \times \mathrm{D}'')} \phi \circ \pi_{\mathrm{W}}\, dg$. Le lemme B.1.8 permet alors d'écrire cette dernière quantité sous la forme $\int_{\mathrm{W}_* \times \mathrm{D}' \times \mathrm{D}''} \phi \circ \pi_{\mathrm{W}} \circ \varphi\; dw\, dv\, dx'$. Comme $\pi_{\mathrm{W}} \circ \varphi(w, v, x') = w$, on peut écrire cette intégrale triple sous la forme du produit de $\int_{\mathrm{W}} \phi\, dw$, $\int_{\mathrm{D}''} dv = 1$ et $\int_{\mathrm{D}'} dx' = c'$, ce qui permet de conclure.

5. Apparition de $\zeta(n)$ et fin du calcul

Si $g \in \mathrm{G}$, les colonnes de g forment une base de W sur $\mathbf{R}$; le sous-groupe Λ_g qu'elles engendrent est donc un réseau de W. De plus, comme $\det g = 1$, le réseau Λ_g est de volume 1.

Réciproquement, si Λ est un réseau de W de volume 1, et si $v_1, \ldots, v_n$ est une base de Λ sur $\mathbf{Z}$, orientée (i.e. $\det(v_1, \ldots, v_n) > 0$), alors la matrice g dont les colonnes sont $v_1, \ldots, v_n$ est un élément de G tel que $\Lambda_g = \Lambda$; il en résulte que $g \mapsto \Lambda_g$ induit une surjection de G sur l'ensemble des réseaux de W de volume 1.

Maintenant, $\Lambda_{g_1} = \Lambda_{g_2}$ si et seulement si on peut écrire les colonnes de g_2 (resp. g_1) comme des combinaisons linéaires à coefficients entiers des colonnes de g_1 (resp. g_2). Traduit en termes matriciels cela équivaut à l'existence de matrices $\mathrm{A}, \mathrm{B} \in \mathbf{M}_n(\mathbf{Z})$ telles que $g_2 = g_1\mathrm{A}$ et $g_1 = g_2\mathrm{B}$. Alors $\mathrm{B} = \mathrm{A}^{-1}$ et, $\mathrm{A} \in \Gamma$ puisque g_1 et g_2 ont pour déterminant 1. Il résulte de cette discussion que l'application $g \mapsto \Lambda_g$ induit une bijection de G/Γ sur l'ensemble des réseaux de volume 1 de $\mathbf{R}^n$ (autrement dit, G/Γ *peut être vu comme l'ensemble des réseaux de* $\mathrm{W} \cong \mathbf{R}^n$ *de volume* 1).

Si Λ est un réseau de W, un élément λ non nul de Λ est dit *primitif* si on ne peut pas l'écrire sous la forme $a \cdot \lambda'$, avec $a \in \mathbf{N}$ et $\lambda' \in \Lambda$. Si $v_1, \ldots, v_n$ est une base de Λ sur $\mathbf{Z}$, et si $\lambda = a_1 v_1 + \cdots + a_n v_n$, alors λ est primitif si et seulement si les a_i sont premiers entre eux dans leur ensemble. Dans le cas général, si $a = \mathrm{pgcd}(a_1, \ldots, a_n)$, alors $\lambda = a\lambda'$ où λ' est primitif. Il en résulte que, si l'on note Λ' l'ensemble des éléments primitifs de Λ, alors $\Lambda - \{0\}$ est la réunion disjointes des $a\Lambda'$, pour $a \in \mathbf{N} - \{0\}$.

Maintenant, si $\gamma \in \Gamma$, alors $\pi_{\mathrm{W}}(g\gamma)$ est une combinaison linéaire, à coefficients entiers *premiers entre eux* des colonnes de g ; c'est donc un élément primitif du réseau Λ_g. Par ailleurs, il résulte de l'ex. 10.16 (appliqué à la transposée des matrices considérées) que si $\mathrm{pgcd}(a_1, \ldots, a_n) = 1$, alors il existe $\gamma \in \Gamma$ dont la première ligne est $(a_1, \ldots, a_n)$. Il en résulte que l'application $\gamma \mapsto \pi_{\mathrm{W}}(g\gamma)$ induit une surjection de Γ sur l'ensemble Λ'_g des éléments primitifs de Λ_g, et donc une bijection de Γ/Θ sur Λ'_g (car $\Theta = \Gamma \cap \mathrm{H}$ et $\pi_{\mathrm{W}}(g_1) = \pi_{\mathrm{W}}(g_2)$ si et seulement si $g_1^{-1} g_2 \in \mathrm{H}$).

La discussion précédente permet de réécrire le cor. B.1.10 sous la forme

$$c' \int_{\mathrm{W}} \phi(w) dw = \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda'_g} \phi(\lambda) \Big) dg.$$

Le facteur $\zeta(n)$ apparaît quand on passe de Λ'_g à Λ_g. Pour effectuer ce passage, on utilise la formule de changement de variable (pour $a \in \mathbf{R}_+^*$),

$$\int_{\mathrm{W}} \phi(aw)dw = a^{-n} \int_{\mathrm{W}} \phi(w)dw,$$

ce qui nous donne, en sommant sur $a \in \mathbf{N} - \{0\}$,

$$\begin{aligned}\zeta(n)c' \int_{\mathrm{W}} \phi(w)dw &= c' \sum_{a=1}^{+\infty} \int_{\mathrm{W}} \phi(aw)dw \\ &= \sum_{a=1}^{+\infty} \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda'_g} \phi(a\lambda) \Big) dg = \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda_g - \{0\}} \phi(\lambda) \Big) dg.\end{aligned}$$

D'après le lemme de Minkowski (th. B.1.12), un convexe de W, de volume $\geqslant 2^n$, symétrique par rapport à l'origine, contient un élément non nul de tout réseau de W de volume 1. Si on prend pour ϕ la fonction caractéristique d'un tel convexe, alors $\sum_{\lambda \in \Lambda_g - \{0\}} \phi(\lambda) \geqslant 1$ quel que soit $g \in \mathrm{G}$; on en déduit l'inégalité $c = \int_{\mathrm{G}/\Gamma} dg \leqslant 2^n \zeta(n) c'$; en particulier, c est fini.

Maintenant, si ϕ est une fonction de Schwartz sur $\mathrm{W} \cong \mathbf{R}^n$, et si $\widehat{\phi}$ désigne la transformée de Fourier de ϕ, on dispose de la formule de Poisson (th. IV.3.19, où l'on pose $g^* = {}^t g^{-1}$ (cf. lemme IV.3.13) ; le volume de Λ_g n'apparaît pas car il est égal à 1) :

$$\sum_{\lambda \in \Lambda_g} \phi(\lambda) = \sum_{\lambda \in \Lambda_{g^*}} \widehat{\phi}(\lambda).$$

Ceci nous donne, en utilisant le fait que $\widehat{\phi}(0) = \int_{\mathrm{W}} \phi(w)\, dw$, puis en utilisant la formule de Poisson, et enfin en appliquant la première identité [(2)] à $\widehat{\phi}$ au lieu de ϕ,

$$\begin{aligned}\zeta(n)c'\widehat{\phi}(0) + c\,\phi(0) &= \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda_g} \phi(\lambda) \Big) dg \\ &= \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda_{g^*}} \widehat{\phi}(\lambda) \Big) dg = \zeta(n)c'\widehat{\widehat{\phi}}(0) + c\,\widehat{\phi}(0).\end{aligned}$$

2. Cela demande de vérifier que $\int_{\mathrm{G}/\Gamma} \phi(g^*)\, dg = \int_{\mathrm{G}/\Gamma} (\phi(g))\, dg$. Pour cela, notons $\varphi : \mathrm{G} \to \mathrm{G}$ le difféomorphisme $g \mapsto \varphi(g) = g^*$; notons que $\varphi(hg) = \varphi(h)\varphi(g)$, pour tous $g, h \in \mathrm{G}$. La formule du changement de variable nous fournit une fonction continue $\mathrm{J} : \mathrm{G} \to \mathbf{R}_+^*$ telle que $\int_{\mathrm{G}} \phi\, dg = \int_{\mathrm{G}} (\phi \circ \varphi)\, \mathrm{J}\, dg$. Si $h \in \mathrm{G}$, l'invariance de dg par translation à gauche nous donne

$$\int_{\mathrm{G}} \phi(\varphi(hg))\mathrm{J}(hg)\, dg = \int_{\mathrm{G}} \phi(\varphi(g))\mathrm{J}(g)\, dg = \int_{\mathrm{G}} \phi(g)\, dg = \int_{\mathrm{G}} \phi(\varphi(h)g)\, dg = \int_{\mathrm{G}} \phi(\varphi(h)\varphi(g))\mathrm{J}(g)\, dg,$$

pour tout $h \in \mathrm{G}$ et toute ϕ sommable. Comme $\varphi(hg) = \varphi(h)\varphi(g)$, il s'ensuit que $\mathrm{J}(hg) = \mathrm{J}(g)$ pour tous $h, g \in \mathrm{G}$, et donc J est constante. Comme $\varphi \circ \varphi = \mathrm{id}$, on en déduit que $\mathrm{J}^2 = 1$, et donc que $\int_{\mathrm{G}} \phi(g^*)\, dg = \int_{\mathrm{G}} (\phi(g))\, dg$, pour toute ϕ sommable sur G. Pour conclure, il suffit de remarquer que $\varphi(\Gamma) = \Gamma$ et $\varphi(g\gamma) = \varphi(g)\varphi(\gamma)$ si $g \in \mathrm{G}$ et $\gamma \in \Gamma$, ce qui fait que φ transforme un domaine fondamental de G/Γ en un domaine fondamental de G/Γ.

Cette formule étant valable quel que soit ϕ, la formule d'inversion de Fourier $\widehat{\widehat{\phi}}(0) = \phi(0)$ nous permet d'obtenir l'égalité

$$c = \zeta(n)c'$$

que l'on cherchait à démontrer.

Remarque B.1.11. — Comme $\zeta(n)c' = c = \mathrm{Vol}(\mathrm{G}/\Gamma)$, on a démontré en passant la formule

$$\int_{\mathrm{W}} \phi(w)dw = \frac{1}{\mathrm{Vol}(\mathrm{G}/\Gamma)} \int_{\mathrm{G}/\Gamma} \Big(\sum_{\lambda \in \Lambda_g - \{0\}} \phi(\lambda) \Big) dg.$$

Autrement dit, *l'intégrale sur* $\mathbf{R}^n$ *d'une fonction* ϕ *est la moyenne sur l'ensemble des réseaux de volume* 1 *de la somme des valeurs de* ϕ *en les points non nuls du réseau.*

6. Le lemme de Minkowski

Le résultat qui suit est d'une utilité assez incroyable en théorie des nombres.

Théorème B.1.12. — (Lemme de Minkowski) *Soit* $\mathrm{K} \subset \mathbf{R}^m$ *un convexe compact, symétrique par rapport à l'origine. Si* $\mathrm{Vol}(\mathrm{K}) \geqslant 2^m$*, alors* K *contient un point de* $\mathbf{Z}^m$ *distinct de l'origine.*

Démonstration. — Supposons le contraire. Si $\mathbf{n} \in \mathbf{Z}^m$, soit $\mathrm{X}_{\mathbf{n}} = \{\mathbf{n} + \frac{v}{2},\ v \in \mathrm{K}\}$. Alors $\mathrm{X}_{\mathbf{n}_1}$ et $\mathrm{X}_{\mathbf{n}_2}$ sont disjoints si $\mathbf{n}_1 \neq \mathbf{n}_2$: en effet, sinon il existe $v_1, v_2 \in \mathrm{K}$ tels que $\mathbf{n}_1 + \frac{v_1}{2} = \mathbf{n}_2 + \frac{v_2}{2}$, ce qui peut se réécrire sous la forme $\frac{1}{2}(v_2 - v_1) = \mathbf{n}_1 - \mathbf{n}_2$, et $-v_1 \in \mathrm{K}$ puisque K est symétrique par rapport à l'origine, ce qui fait que $\mathbf{n}_1 - \mathbf{n}_2 \in \mathrm{K}$ puisque K est convexe. Il en résulte que le volume de la réunion $\mathrm{K_N}$ des $\mathrm{X}_{\mathbf{n}}$, pour $\mathbf{n} = (n_1, \ldots, n_m)$ vérifiant $\sup |n_i| \leqslant \mathrm{N}$, est égal à $(2\mathrm{N}+1)^m \frac{\mathrm{Vol}(\mathrm{K})}{2^m}$, puisque chacun des $\mathrm{X}_{\mathbf{n}}$ a pour volume $\frac{\mathrm{Vol}(\mathrm{K})}{2^m}$, qu'il y a $(2\mathrm{N}+1)^m$ tels $\mathrm{X}_{\mathbf{n}}$, et que les $\mathrm{X}_{\mathbf{n}}$ sont disjoints deux à deux. Par ailleurs, K étant compact, il existe $\mathrm{C} > 0$ tel que K soit inclus dans $[-2\mathrm{C}, 2\mathrm{C}]^m$. Ceci implique que $\mathrm{K_N} \subset [-\mathrm{N} - \mathrm{C}, \mathrm{N} + \mathrm{C}]^m$, et donc que $\mathrm{Vol}(\mathrm{K_N}) \leqslant (2\mathrm{N} + 2\mathrm{C})^m$, pour tout $\mathrm{N} \in \mathbf{N}$.

• Si $\mathrm{Vol}(\mathrm{K}) > 2^m$, on obtient, si N est assez grand, une contradiction avec la formule $\mathrm{Vol}(\mathrm{K_N}) = (2\mathrm{N}+1)^m \frac{\mathrm{Vol}(\mathrm{K})}{2^m}$, ce qui permet de conclure dans ce cas.

• Si $\mathrm{Vol}(\mathrm{K}) = 2^m$, il suffit d'appliquer ce qui précède à l'homothétique $\lambda\mathrm{K}$ de K, pour $\lambda > 1$ suffisamment petit (en effet, comme K est compact, la distance de K à $\mathbf{Z}^m - \{(0, \ldots, 0)\}$ est strictement positive, et donc $\lambda\mathrm{K}$ ne contient aucun élément de $\mathbf{Z}^m - \{(0, \ldots, 0)\}$, si $\lambda > 1$ est assez petit).

Ceci permet de conclure.

B.2. La mesure de Haar de $\mathbf{SL}_n(\mathbf{R})$

Nous allons vérifier que la mesure dg de la prop. B.1.2 est bien une mesure de Haar à droite et à gauche. L'invariance à gauche de dg se déduit de son invariance à droite en passant à la transposée. Il suffit donc de vérifier son invariance à droite et, comme

l'ensemble des $\gamma \in \mathrm{G}$ vérifiant $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\mathrm{G}} \phi(g)\, dg$, pour tout $\phi : \mathrm{G} \to \mathrm{R}_+$, est un sous-groupe de G, il suffit de vérifier que c'est le cas pour un ensemble de γ engendrant G. Le lemme B.2.4 ci-dessous fournit un système de générateurs particulièrement sympathiques.

1. Transvections et structure du groupe $\mathbf{SL}_n(\mathrm{K})$

Soit K un corps commutatif. Une *transvection* T est un élément de $\mathbf{M}_n(\mathrm{K})$ avec des 1 sur la diagonale, et un unique coefficient non nul en dehors de la diagonale. Si ce coefficient est celui de la i-ième ligne et de la j-ième colonne (avec $i \neq j$), alors $\mathrm{T} = 1 + \lambda \mathrm{N}_{i,j}$, où $\mathrm{N}_{i,j}$ est la matrice dont tous les coefficients sont nuls sauf celui de la i-ième ligne et de la j-ième colonne, qui est égal à 1. Comme $\mathrm{N}_{i,j}^2 = 0$, on a $\mathrm{T}^{-1} = 1 - \lambda \mathrm{N}_{i,j}$, et donc l'inverse d'une transvection est une transvection. Le déterminant d'une transvection est égal à 1 puisqu'une transvection est triangulaire supérieure ou inférieure, avec des 1 sur la diagonale ; c'est donc un élément de $\mathbf{SL}_n(\mathrm{K})$. Le résultat suivant, selon lequel tout élément de $\mathbf{SL}_n(\mathrm{K})$ est un produit d'un nombre fini de transvections, est très utile pour toutes sortes de questions.

Théorème B.2.1. — *Si $n \geqslant 2$, les transvections engendrent $\mathbf{SL}_n(\mathrm{K})$.*

Démonstration. — La démonstration se fait par récurrence sur n. Pour $n = 2$, cela résulte du lemme suivant.

Lemme B.2.2. — *Si* K *est un corps, et si* $\mathrm{A} \in \mathbf{SL}_2(\mathrm{K})$, *il existe* $t, x, y, z \in \mathrm{K}$ *tels que l'on ait* $\mathrm{A} = \left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$.

Démonstration. — On part de la formule $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1+xy & x+z+xyz \\ y & 1+yz \end{smallmatrix}\right)$. On en déduit que si $\mathrm{A} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathrm{K})$ vérifie $c \neq 0$, alors A est le produit des 3 matrices ci-dessus, avec $y = c$, $x = c^{-1}(a-1)$ et $z = c^{-1}(d-1)$ et on peut prendre $t = 0$. Si $c = 0$, il suffit de multiplier A par une matrice de la forme $\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ -t & 1 \end{smallmatrix}\right)$, pour obtenir une nouvelle matrice qui peut s'écrire comme produit de 3 matrices comme ci-dessus. Ceci permet de conclure.

Lemme B.2.3. — *Soit $n \geqslant 3$.*

(i) *Une matrice de la forme*

$$\mathrm{V}(\lambda_1, \ldots, \lambda_{n-1}) = \begin{pmatrix} 1 & 0 & 0 & \lambda_1 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & \lambda_{n-1} \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{ou} \quad \mathrm{H}(\lambda_1, \ldots, \lambda_{n-1}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \lambda_1 & \ldots & \lambda_{n-1} & 1 \end{pmatrix}$$

est un produit de transvections.

(ii) *Une matrice diagonale* $\mathrm{Diag}(1, \ldots, 1, \lambda, \lambda^{-1})$, *avec* $\lambda \in \mathrm{K}^*$, *est un produit de transvections.*

Démonstration. — Le (i) se démontre en constatant que

$$\mathrm{V}(\lambda_1,\dots,\lambda_{n-1})=\prod_{i=1}^{n-1}(1+\lambda_i \mathrm{N}_{i,n}) \quad \text{et} \quad \mathrm{H}(\lambda_1,\dots,\lambda_{n-1})=\prod_{i=1}^{n-1}(1+\lambda_i \mathrm{N}_{n,i}).$$

Le (ii) se démontre en écrivant, ce qui est possible d'après le lemme B.2.2, la matrice $\left(\begin{smallmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{smallmatrix}\right)$ comme un produit de transvections dans $\mathbf{SL}_2(\mathrm{K})$, et en complétant toutes les matrices ainsi obtenue par des 1 sur la diagonale et des 0 ailleurs pour en faire des éléments de $\mathbf{SL}_n(\mathrm{K})$.

Revenons à la démonstration du théorème. On suppose le résultat vérifié pour $n-1$, et on cherche à le prouver pour n. Pour cela, il suffit de montrer qu'en partant d'une matrice quelconque M de $\mathbf{SL}_n(\mathrm{K})$, et en la multipliant à droite par des transvections $\mathrm{T}_1,\dots,\mathrm{T}_m$ bien choisies, on peut obtenir une matrice qui est un produit de transvections $\mathrm{T}'_1\cdots\mathrm{T}'_r$: en effet, on a alors $\mathrm{M}=\mathrm{T}'_1\cdots\mathrm{T}'_r\mathrm{T}_m^{-1}\cdots\mathrm{T}_1^{-1}$, et les T_i^{-1} étant des transvections cela fournit une écriture de M sous la forme voulue.

Comme M est inversible, ses colonnes $w_1,\dots,w_n$ forment une famille génératrice de K^n, et il existe $\lambda_1,\dots,\lambda_n\in\mathrm{K}$ tels que $\lambda_1w_1+\cdots+\lambda_nw_n={}^{\mathrm{t}}(0,\dots,0,1)$. Il y a deux cas :

• $\lambda_1=\cdots=\lambda_{n-1}=0$, auquel cas M est, par blocs, de la forme $\left(\begin{smallmatrix}\mathrm{P}_1 & 0\\ v_1 & \lambda\end{smallmatrix}\right)$, où $\mathrm{P}_1\in\mathbf{GL}_{n-1}(\mathrm{K})$, $\lambda\in\mathrm{K}^*$ et $v_1\in\mathrm{K}^{n-1}$ (et 0 désigne le vecteur colonne à $n-1$ lignes dont toutes les coordonnées sont nulles). Multiplier à droite M par $\mathrm{Diag}(1,\dots,1,\lambda,\lambda^{-1})$ qui, d'après le lemme B.2.3, est aussi un produit de transvections, fournit une matrice (par blocs) M_2 de la forme $\left(\begin{smallmatrix}\mathrm{P}_2 & 0\\ v & 1\end{smallmatrix}\right)$, où $\mathrm{P}_2\in\mathbf{SL}_{n-1}(\mathrm{K})$ (car le déterminant de M_2 est égal à 1) et $v\in\mathrm{K}^{n-1}$.

• Il existe $i\leqslant n-1$ tel que $\lambda_i\neq 0$. Multiplier M à droite par $(1+\frac{\lambda_n-1}{\lambda_i}\mathrm{N}_{n,i})\mathrm{V}(\lambda_1,\dots,\lambda_{n-1})$ qui, d'après le lemme B.2.3, est un produit de transvections, fournit une matrice M_2 dont la dernière colonne est $v=\lambda_1w_1+\cdots+\lambda_i(w_i+\frac{\lambda_n-1}{\lambda_i}w_n)+\lambda_{n-1}w_{n-1}+w_n={}^{\mathrm{t}}(0,\dots,0,1)$, et donc est de la forme $\left(\begin{smallmatrix}\mathrm{P}_2 & 0\\ v & 1\end{smallmatrix}\right)$ comme ci-dessus.

Maintenant, si on note v_i la i-ième ligne de P_2, les v_i forment une base de K^{n-1} et il existe $\lambda_1,\dots,\lambda_{n-1}\in\mathrm{K}$ (uniques) tels que $v+\lambda_1v_1+\cdots+\lambda_{n-1}v_{n-1}=0$. Multiplier à gauche M_2 par $\mathrm{H}(\lambda_1,\dots,\lambda_{n-1})$ qui, d'après le lemme B.2.3, est un produit de transvections, fournit donc une matrice (par blocs) M_3 de la forme $\left(\begin{smallmatrix}\mathrm{P}_3 & 0\\ 0 & 1\end{smallmatrix}\right)$, où $\mathrm{P}_3=\mathrm{P}_2\in\mathbf{SL}_{n-1}(\mathrm{K})$.

Il ne reste plus qu'à appliquer l'hypothèse de récurrence pour écrire P_3 comme un produit de transvections dans $\mathbf{SL}_{n-1}(\mathrm{K})$, et compléter toutes les matrices ainsi obtenues par un 1 sur la diagonale et des 0 ailleurs pour en faire des éléments de $\mathbf{SL}_n(\mathrm{K})$. On obtient de cette manière une écriture de M_3 comme un produit de transvections, ce qui permet de conclure.

Notons $e_1,\dots,e_n$ la base canonique de K^n. Soit W l'ensemble des matrices des endomorphismes w de $\mathbf{R}^n$ tels qu'il existe une permutation $\sigma\in\mathrm{S}_n$ et $\varepsilon_1,\dots,\varepsilon_n\in\{\pm1\}$ tels que $w(e_i)=\varepsilon_ie_{\sigma(i)}$. Alors W est un groupe et le déterminant d'un élément de w est ±1. On note W^+ l'intersection de W et $\mathbf{SL}_n(\mathrm{K})$.

Un élément de w permute les axes de coordonnées $\mathrm{K}e_i$, pour $i \in \{1, \ldots, n\}$, ce qui nous fournit un morphisme surjectif de W sur S_n dont le noyau est le groupe des matrices diagonales dont les coefficients diagonaux sont des 1 ou des -1. La restriction de ce morphisme à W^+ est encore surjective : si $\sigma \in \mathrm{S}_n$ est de signature $\varepsilon \in \{\pm 1\}$, alors la matrice de l'application linéaire envoyant e_1 sur $\varepsilon e_{\sigma(1)}$ et e_i sur $e_{\sigma(i)}$, si $i \neq 1$, est un élément de W^+ dont l'image dans S_n est σ.

Lemme B.2.4. — $\mathbf{SL}_n(\mathrm{K})$ *est engendré par* W^+ *et les* $1 + \lambda \mathrm{N}_{1,2}$*, pour* $\lambda \in \mathrm{K}$.

Démonstration. — Soient $i \neq j$ deux éléments de $\{1, \ldots, n\}$ et $\sigma \in \mathrm{S}_n$ tel que $\sigma(1) = i$ et $\sigma(2) = j$. Soit $w \in \mathrm{W}^+$ dont l'image dans S_n est σ de telle sorte qu'il existe $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ tels que $w(e_1) = \varepsilon_1 e_i$ et $w(e_2) = \varepsilon_2 e_j$. Notons $u_{i,j}$ l'endomorphisme de K^n dont la matrice est $\mathrm{N}_{i,j}$; on a donc $u_{i,j}(e_j) = e_i$ et $u_{i,j}(e_k) = 0$, si $k \neq j$. On en déduit que $wu_{1,2}w^{-1}(e_k) = 0$ si $k \neq j$ car $w^{-1}(e_k) = \pm e_{\sigma^{-1}(k)}$ et $\sigma^{-1}(k) \neq 2$, et $wu_{1,2}w^{-1}(e_j) = \varepsilon_1\varepsilon_2 e_i$. Il en résulte que $w\mathrm{N}_{1,2}w^{-1} = \varepsilon_1\varepsilon_2\mathrm{N}_{i,j}$ et $w(1 + \lambda\mathrm{N}_{1,2})w^{-1} = 1 + \varepsilon_1\varepsilon_2\lambda\mathrm{N}_{i,j}$. Il s'ensuit que le sous-groupe de $\mathbf{SL}_n(\mathrm{K})$ engendré par W^+ et les $1 + \lambda\mathrm{N}_{1,2}$, pour $\lambda \in \mathrm{K}$, contient toutes les transvections et comme celles-ci engendrent $\mathbf{SL}_n(\mathrm{K})$, cela permet de conclure.

2. Invariance de dg par translation

D'après le lemme B.2.4, pour prouver que dg est invariante à droite, on peut se contenter de vérifier que $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\mathrm{G}} \phi(g)\, dg$ pour tout $\phi : \mathrm{G} \to \mathbf{R}_+$, pour $\gamma \in \mathrm{W}^+$, et pour $\gamma = 1 + \lambda\mathrm{N}_{1,2}$.

• Si $\gamma \in \mathrm{W}^+$, on peut l'écrire sous la forme $\mathrm{Diag}(\varepsilon_i)\mathrm{A}_\sigma$, où les ε_i sont des éléments de $\{\pm 1\}$, $\sigma \in \mathrm{S}_n$ et A_σ est la matrice $(a_{i,j})_{1 \leqslant i,j \leqslant n}$, avec $a_{i,j} = 0$ si $i \neq \sigma(j)$ et $a_{\sigma(i),i} = 1$. Multiplier à droite une matrice par $\mathrm{Diag}(\varepsilon_i)$ revient à multiplier la i-ème colonne par ε_i, et multiplier à droite une matrice par A_σ revient à permuter les colonnes : la i-ième colonne de BA_σ est la $\sigma(i)$-ième colonne de B. On en déduit que $\mathrm{M}_{n,n}(\mathrm{B}\gamma) = \pm\mathrm{M}_{n,\sigma(n)}(\mathrm{B})$.

Soit $\Omega_n = \cap_{i=1}^n \Omega_{n,i}$. D'après le lemme B.2.5 ci-dessous, $\Omega_{n,n} - \Omega_n$ est de mesure nulle et donc $\int_{\mathrm{G}} \phi(g)\, dg = \int_{\Omega_n} \phi \circ \iota_{n,n}\, dx$. Par ailleurs, $g \mapsto g\gamma$ induit une bijection de $\iota_{n,i}(\Omega_{n,i})$ sur $\iota_{n,\sigma(i)}(\Omega_{n,\sigma(i)})$, et donc $\varphi(x) = \pi_{n,n}(\iota_{n,n}(x)\gamma)$ est un difféomorphisme de Ω_n sur Ω_n, le difféomorphisme inverse étant $\psi(x) = \pi_{n,n}(\iota_{n,n}(x)\gamma^{-1})$. On a alors

$$\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\Omega_n} \widetilde{\phi}(\varphi(x)) \left|\frac{\wedge_{(i,j)\neq(n,n)} dx_{i,j}}{\mathrm{M}_{n,n}(x)}\right| = \int_{\Omega_n} \widetilde{\phi}(x) \left|\frac{\wedge_{(i,j)\neq(n,n)} (d\psi(x))_{i,j}}{\mathrm{M}_{n,n}(\psi(x))}\right|.$$

Or

$$\frac{\wedge_{(i,j)\neq(n,n)} (d\psi(x))_{i,j}}{\mathrm{M}_{n,n}(\psi(x))} = \pm\frac{\wedge_{(i,j)\neq(n,n)} dx_{i,\sigma(j)}}{\mathrm{M}_{n,\sigma(n)}(x)},$$

et la relation (on l'obtient en différenciant la relation $\det \mathrm{A} = 1$, et en utilisant le fait que $\det \mathrm{A}$ est linéaire en $x_{\alpha,\beta}$ avec comme coefficient le cofacteur correspondant)

$$dx_{n,n} = \frac{-1}{\mathrm{M}_{n,n}(x)} \sum_{(\alpha,\beta)\neq(n,n)} \mathrm{M}_{\alpha,\beta}(x)\, dx_{\alpha,\beta}$$

montre que

$$\frac{\wedge_{(i,j)\neq(n,n)} dx_{i,\sigma(j)}}{\mathrm{M}_{n,\sigma(n)}(x)} = \pm \frac{\wedge_{(i,j)\neq(n,n)} dx_{i,j}}{\mathrm{M}_{n,n}(x)},$$

et donc que $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\Omega_n} \widetilde{\phi}(x) \left| \frac{\wedge_{(i,j)\neq(n,n)} dx_{i,j}}{\mathrm{M}_{n,n}(x)} \right| = \int_{\mathrm{G}} \phi(g)\, dg$.

• Si $\gamma = 1 + \lambda \mathrm{N}_{1,2}$, les colonnes de $\mathrm{B}\gamma$ sont les mêmes que celles de B sauf la seconde qui est obtenue en rajoutant λ fois la première colonne de B à la seconde. Il s'ensuit que $\varphi(x) = \pi_{n,n}(\iota_{n,n}(x)\gamma)$ est un difféomorphisme de $\Omega_{n,n}$ sur $\Omega_{n,n}$ d'inverse $\psi(x) = \pi_{n,n}(\iota_{n,n}(x)\gamma^{-1})$, et que l'on a $\mathrm{M}_{n,n}(\psi(x)) = \mathrm{M}_{n,n}(x)$ et $\wedge_{(i,j)\neq(n,n)}(d\psi(x))_{i,j} = \wedge_{(i,j)\neq(n,n)} dx_{i,j}$. On en déduit l'égalité $\int_{\mathrm{G}} \phi(g\gamma)\, dg = \int_{\mathrm{G}} \phi(g)\, dg$ qui permet de conclure.

Lemme B.2.5. — *Si* $\mathrm{P} \in \mathbf{R}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ *est non nul, et si* $\mathrm{Z} = \{x \in \mathbf{R}^m,\ \mathrm{P}(x) = 0\}$, *alors* Z *est de mesure nulle.*

Démonstration. — La démonstration se fait par récurrence sur m, le résultat étant immédiat pour $m = 1$ puisqu'un polynôme non nul n'a qu'un nombre fini de zéros. Supposons donc $m \geqslant 2$, et écrivons P(X) sous la forme $\sum_{i=0}^{d} \mathrm{Q}_i(\mathrm{X})\mathrm{X}_n^i$, avec $\mathrm{Q}_i \in \mathbf{R}[\mathrm{X}_1, \ldots, \mathrm{X}_{m-1}]$, et $\mathrm{Q}_d \neq 0$. L'ensemble $\mathrm{Y} = \{y \in \mathbf{R}^{m-1},\ \mathrm{Q}_d(y) = 0\}$ est alors de mesure nulle d'après l'hypothèse de récurrence, et si $y \notin \mathrm{Y}$, la fonction $x_n \mapsto \mathbf{1}_{\mathrm{Z}}(y, x_n)$ est nulle p.p. puisqu'un polynôme non nul n'a qu'un nombre fini de zéros. Il en résulte que $\lambda(\mathrm{Z})$, qui est égal à

$$\int_{\mathrm{Y}\times\mathbf{R}} \mathbf{1}_{\mathrm{Z}} + \int_{(\mathbf{R}^{m-1}-\mathrm{Y})\times\mathbf{R}} \mathbf{1}_{\mathrm{Z}} = \int_{\mathbf{R}} \Big(\int_{\mathrm{Y}} \mathbf{1}_{\mathrm{Z}}(y, x_n)\, dy \Big)\, dx_n + \int_{\mathbf{R}^{m-1}-\mathrm{Y}} \Big(\int_{\mathbf{R}} \mathbf{1}_{\mathrm{Z}}(y, x_n)\, dx_n \Big)\, dy,$$

est nul puisque $\int_{\mathrm{Y}} \mathbf{1}_{\mathrm{Z}}(y, x_n)\, dy \leqslant \lambda(\mathrm{Y}) = 0$, et que $\int_{\mathbf{R}} \mathbf{1}_{\mathrm{Z}}(y, x_n)\, dx_n = 0$ pour tout $y \in \mathbf{R}^{m-1} - \mathrm{Y}$. Ceci permet de conclure.

3. De $\mathbf{SL}_{n-1}(\mathbf{R})$ à $\mathbf{SL}_n(\mathbf{R})$

Ce n° est consacré à la démonstration de la formule du changement de variable du lemme B.1.8. Notons $\Omega'_{n-1,n-1}$ l'ouvert de $\mathbf{R}^{(n-1)^2-1}$ défini par la non annulation du cofacteur $\mathrm{M}'_{n-1,n-1}$ obtenu en retirant la $(n-1)$-ième ligne et la $(n-1)$-ième colonne d'une matrice $(n-1)\times(n-1)$. Par définition de $\int_{\mathrm{G}'}$, le membre de droite de l'identité à vérifier est aussi égal à $\int_{\mathrm{U}\times\mathbf{R}^{n-1}\times\Omega'_{n-1,n-1}} \phi \circ \varphi \circ \iota' \frac{dw\, dv\, dg'}{|\mathrm{M}'_{n-1,n-1}|}$, où $\iota'(w, v, x') = (w, v, g')$ et $g' = \iota'_{n-1,n-1}(x')$ est l'unique élément de G′ s'envoyant sur x' en retirant la coordonnée sur la $(n-1)$-ième ligne et la $(n-1)$-ième colonne.

Maintenant $\tilde{\varphi} = \pi_{n,n} \circ \varphi \circ \iota'$, induit un difféomorphisme de $\mathrm{U} \times \mathbf{R}^{n-1} \times \Omega'_{n-1,n-1}$ sur l'ouvert $\mathrm{X} = \{x \in \Omega_{n,n},\ x_{1,1} \neq 0\}$ de $\mathrm{E}_{n,n}$, d'inverse $x \mapsto (w(x), v(x), g'(x))$, avec

$$w(x) = \pi_{\mathrm{W}} \circ \iota_{n,n}(x),\ v(x) = \pi_{\mathrm{V}}(h(x)) \text{ et } g'(x) = \pi_{\mathrm{G}'}(h(x)),\ \text{où } h(x) = \iota_{\mathrm{W}}(w(x))^{-1} \iota_{n,n}(x).$$

Or $\Omega_{n,n} - \mathrm{X}$ est de mesure nulle puisque inclus dans un hyperplan ; il en résulte que $\int_{\mathrm{G}} \phi\, dg$ est aussi égal à $\int_{\mathrm{X}} \phi \circ \iota_{n,n} \frac{dx}{|\mathrm{M}_{n,n}|}$. La formule du changement de variable montre que cette dernière quantité est aussi égale à $\int_{\mathrm{U}\times\mathbf{R}^{n-1}\times\Omega'_{n-1,n-1}} \phi \circ \iota_{n,n} \circ \tilde{\varphi} \frac{\mathrm{J}_{\tilde{\varphi}}\, dw\, dv\, dg'}{|\mathrm{M}_{n,n} \circ \tilde{\varphi}|}$, et comme

$\iota_{n,n} \circ \tilde{\varphi} = \iota_{n,n} \circ \pi_{n,n} \circ \varphi \circ \iota' = \varphi \circ \iota'$, puisque $\iota_{n,n} \circ \pi_{n,n}$ est l'identité sur $\pi_{n,n}^{-1}(\Omega_{n,n})$, le lemme B.2.6 ci-dessous permet de conclure.

Lemme B.2.6. — (i) $\mathrm{M}_{n,n}(\tilde{\varphi}(w,v,x')) = w_1 \mathrm{M}'_{n-1,n-1}(x')$.
(ii) $|\mathrm{J}_{\tilde{\varphi}}(w,v,x')| = |w_1|$.

Démonstration. — Soient w'' le vecteur colonne de coordonnées $w_2, \dots, w_{n-1}$, v'' le vecteur ligne de coordonnées $v_1, \dots, v_{n-2}$ et g'' la matrice $(n-2) \times (n-2)$ obtenue en retirant la dernière ligne et la dernière colonne de $\iota'_{n-1,n-1}(x')$. Alors $\mathrm{M}_{n,n}(\tilde{\varphi}(w,v,x'))$ est le déterminant de la matrice par blocs $\left(\begin{smallmatrix} w_1 & w_1 v'' \\ w'' & w''v''+g'' \end{smallmatrix}\right)$. On ne ne change pas ce déterminant en retirant v_i fois la première colonne à la $(i+1)$-ième, et ce déterminant est donc aussi celui de $\left(\begin{smallmatrix} w_1 & 0 \\ w'' & g'' \end{smallmatrix}\right)$, c'est-à-dire $w_1 \det g''$. Comme $\det g'' = \mathrm{M}'_{n-1,n-1}(x')$, par définition, cela démontre le (i).

Pour démontrer le (ii), on part de la formule

$$\bigwedge_{(i,j)\neq(n,n)} d(\tilde{\varphi}(w,v,x')_{i,j}) = \pm \mathrm{J}_{\tilde{\varphi}}(w,v,x') \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} dv_j \bigwedge_{(i,j)\neq(n-1,n-1)} dx'_{i,j}.$$

Comme $\tilde{\varphi}(w,v,x') = \left(\begin{smallmatrix} w_1 & w_1 v \\ w' & w'v+\alpha(w)\iota'_{n-1,n-1}(x') \end{smallmatrix}\right)$, on a

- $d(\tilde{\varphi}(w,v,x')_{i,1}) = dw_i$, si $1 \leqslant i \leqslant n$
- $d(\tilde{\varphi}(w,v,x')_{1,j}) = w_1 dv_{j-1} +$ terme en dw_1, si $1 \leqslant j \leqslant n-1$,
- $d(\tilde{\varphi}(w,v,x')_{i,j}) = dx'_{i-1,j-1} +$ combinaison linéaire des dw_i et des dv_j, si $2 \leqslant i \leqslant n-1$ et $2 \leqslant j \leqslant n$,
- $d(\tilde{\varphi}(w,v,x')_{n,j}) = w_1^{-1} dx'_{n-1,j-1} +$ combinaison linéaire des dw_i et des dv_j, si $2 \leqslant j \leqslant n-1$.

Il en résulte, en utilisant le fait que $\wedge$ est multilinéaire alterné, que

$$\begin{aligned}\bigwedge_{(i,j)\neq(n,n)} d(\tilde{\varphi}(w,v,x')_{i,j}) &= \pm \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} (w_1 dv_j) \bigwedge_{1\leqslant i\leqslant n-2,\ 1\leqslant j\leqslant n-1} dx'_{i,j} \bigwedge_{1\leqslant j\leqslant n-2} (w_1^{-1} dx'_{n-1,j}) \\ &= \pm\, w_1 \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} dv_j \bigwedge_{(i,j)\neq(n-1,n-1)} dx'_{i,j}.\end{aligned}$$

Ceci permet de conclure.

APPENDICE C

GROUPES FINIS ET REPRÉSENTATIONS : EXEMPLES

Cette annexe vise à illustrer l'intérêt de l'induction pour l'étude des représentations d'un groupe fini. On s'intéresse à trois séries de groupes : les groupes de cardinal une puissance de p, le groupe symétrique S_n dont les représentations jouent un rôle important en physique théorique, et le groupe $\mathbf{GL}_2(\mathbf{F})$, où $\mathbf{F}$ est un corps fini. Ce dernier cas permet de passer en revue les principaux résultats de la théorie exposée au chap. I.

C.1. p-Groupes

1. Généralités sur les p-groupes

Soit p un nombre premier. Un *p-groupe* est un groupe d'ordre une puissance de p.

Proposition C.1.1. — (i) *Si* $\mathrm{G} \neq \{1\}$ *est un p-groupe, le centre de* G *est non trivial.*

(ii) *Si* G *est un p-groupe non commutatif, alors* G *contient un sous-groupe commutatif distingué contenant strictement le centre de* G.

Démonstration. — (i) On fait agir G sur lui même par conjugaison. Les orbites sont alors les classes de conjugaison et le centre Z est l'ensemble des $c \in \mathrm{G}$ dont la classe de conjugaison est réduite à un point. On sait que Z contient l'élément neutre, et notre problème est de montrer qu'il existe d'autres classes de conjugaison réduites à un point. Maintenant, si O est une classe de conjugaison, et si $x \in \mathrm{O}$, alors $\mathrm{O} = \mathrm{G}/\mathrm{Z}_x$, où Z_x est l'ensemble des éléments de G commutant à x ; on a alors $|\mathrm{O}| = \frac{|\mathrm{G}|}{|\mathrm{Z}_x|}$, ce qui prouve que $|\mathrm{O}|$ est une puissance de p ; en particulier, $|\mathrm{O}|$ est divisible par p sauf si $|\mathrm{O}| = 1$. Comme $|\mathrm{G}|$ est divisible par p, et est aussi la somme des cardinaux des orbites, on en déduit que l'ensemble des orbites réduites à un point a un cardinal divisible par p. Autrement dit, $|\mathrm{Z}|$ est divisible par p, et comme $|\mathrm{Z}| \geqslant 1$, on a $|\mathrm{Z}| \geqslant p$, ce qui démontre le (i).

(ii) Supposons maintenant G non commutatif (et donc $\mathrm{G} \neq \mathrm{Z}$), et soit $\mathrm{H} = \mathrm{G}/\mathrm{Z}$. Alors H est un p-groupe, et son centre Y est non trivial. Soit y un élément du centre de H distinct de l'élément neutre, soit $\langle y \rangle$ le sous-groupe de Y engendré par y, et soit A l'image inverse de $\langle y \rangle$ dans G. Comme $\langle y \rangle$ est distingué (car central) dans H, cela implique que A

est un sous-groupe distingué de G, et comme A contient strictement Z, il suffit de vérifier que A est commutatif. Soit a l'ordre de y, et soit $\tilde{y} \in \mathrm{A}$ ayant pour image y dans H. Alors les éléments de $\langle y \rangle$ sont les y^i, avec $0 \leqslant i \leqslant a-1$, et tout élément de A peut s'écrire sous la forme $\tilde{y}^i z$, avec $0 \leqslant i \leqslant a-1$ et $z \in \mathrm{Z}$. Si $x_1 = \tilde{y}^{i_1} z_1$ et $x_2 = \tilde{y}^{i_2} z_2$, on a, en tenant compte du fait que les éléments de Z commutent à tout,

$$x_1 x_2 = \tilde{y}^{i_1} z_1 \tilde{y}^{i_2} z_2 = \tilde{y}^{i_1} \tilde{y}^{i_2} z_1 z_2 = \tilde{y}^{i_1+i_2} z_2 z_1 = \tilde{y}^{i_2} z_2 \tilde{y}^{i_1} z_1 = x_2 x_1,$$

ce qui permet de conclure.

2. Représentations des p-groupes

Remarque C.1.2. — Soit G un groupe fini. Si A est un sous-groupe distingué de G, si W est une représentation de A, et si $g \in \mathrm{G}$, on peut fabriquer une représentation W^g de A en posant $\rho_{\mathrm{W}^g}(a) = \rho_{\mathrm{W}}(g^{-1}ag)$, ce qui a un sens puisque $g^{-1}ag \in \mathrm{A}$ si $a \in \mathrm{A}$ et $g \in \mathrm{G}$, par définition d'un sous-groupe distingué. Il est immédiat que W^g est irréductible si et seulement si W l'est, et on obtient de la sorte une action $(g, \chi) \mapsto \chi^g$ de G sur $\mathrm{Irr}(\mathrm{A})$. [Si $\chi \in \mathrm{Irr}(\mathrm{A})$ est un caractère irréductible, on a $\chi^g(a) = \chi(g^{-1}ag)$.]

Proposition C.1.3. — *Soit* G *un groupe fini, et soit* A *un sous-groupe distingué de* G*. Si* V *est une représentation irréductible de* G *dont la restriction* $\mathrm{Res}^{\mathrm{A}}_{\mathrm{G}} \mathrm{V}$ *à* A *n'est pas isotypique, il existe un sous-groupe* H *de* G *contenant* A *et strictement inclus dans* G*, et une représentation irréductible* W *de* H*, tels que* $\mathrm{V} = \mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}$*.*

Démonstration. — Décomposons $\mathrm{Res}^{\mathrm{A}}_{\mathrm{G}} \mathrm{V}$ en la somme directe $\oplus_{\chi \in \mathrm{X}} \mathrm{V}_\chi$, avec $\mathrm{X} \subset \mathrm{Irr}(\mathrm{A})$, de ses composantes isotypiques. Par hypothèse, on a $|\mathrm{X}| \geqslant 2$. Si $\chi \in \mathrm{X}$, si $g \in \mathrm{G}$, et si $a \in \mathrm{A}$, on a $a \cdot (g \cdot \mathrm{V}_\chi) = g \cdot (g^{-1}ag \cdot \mathrm{V}_\chi)$, ce qui prouve que $g \cdot \mathrm{V}_\chi$ est stable par a, et que $\rho_{g \cdot \mathrm{V}_\chi}(a) = \rho_{\mathrm{V}_\chi}(g^{-1}ag)$. On en déduit que g envoie la composante isotypique V_χ sur la composante isotypique V_{χ^g}, et donc permute les éléments de X.

Soit $\chi_0 \in \mathrm{X}$, et soient W la composante isotypique de $\mathrm{Res}^{\mathrm{A}}_{\mathrm{G}} \mathrm{V}$ correspondant à χ_0, et $\mathrm{H} \subset \mathrm{G}$ le stabilisateur de χ_0. Alors W est stable par H et peut donc être considérée comme une représentation de H. Maintenant $\sum_{g \in \mathrm{G}} g \cdot \mathrm{W} = \oplus_{g \in \mathrm{G/H}} \mathrm{V}_{\chi_0^g}$ est stable par G, et donc est égal à V puisqu'on a supposé V irréductible. On en déduit que $\mathrm{X} = \mathrm{G/H}$, et donc que $\mathrm{H} \neq \mathrm{G}$, et que V et $\mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}$ ont même dimension $|\mathrm{X}| \cdot \dim \mathrm{W}$. Par ailleurs, $\mathrm{Hom}_{\mathrm{H}}(\mathrm{W}, \mathrm{V})$ est non nul, et donc $\mathrm{Hom}_{\mathrm{G}}(\mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}, \mathrm{V})$ est aussi non nul (ex. I.3.17). Comme V est irréductible, et comme $\mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}$ et V ont même dimension, tout élément non nul de $\mathrm{Hom}_{\mathrm{G}}(\mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}, \mathrm{V})$ induit un isomorphisme de $\mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \mathrm{W}$ sur V. Ceci permet de conclure.

Proposition C.1.4. — *Si* G *est un p-groupe, et si* V *est une représentation irréductible de* G*, il existe un sous-groupe* H *de* G *et un caractère linéaire* $\chi \in \widehat{\mathrm{H}}$*, tels que* $\mathrm{V} = \mathrm{Ind}^{\mathrm{G}}_{\mathrm{H}} \chi$*.*

Démonstration. — La démonstration se fait par récurrence sur $|\mathrm{G}|$. Si G est commutatif, alors toute représentation irréductible est de dimension 1, et il n'y a rien à démontrer. Supposons donc G non commutatif, et soit V une représentation irréductible de G.

• Si le noyau N de ρ_{V} est non trivial, alors ρ_{V} se factorise à travers $\mathrm{G}' = \mathrm{G}/\mathrm{N}$, et on peut appliquer l'hypothèse de récurrence à G' : il existe $\mathrm{H}' \subset \mathrm{G}'$ et $\chi \in \widehat{\mathrm{H}}'$ tel que $\mathrm{V} = \mathrm{Ind}_{\mathrm{H}'}^{\mathrm{G}'}\chi$, en tant que représentation de G'. Si H est l'image inverse de H' dans G, on peut voir χ comme un élément de $\widehat{\mathrm{H}}$ en composant avec la projection $\mathrm{H} \to \mathrm{H}'$, et on a $\mathrm{V} = \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\chi$, ce qui permet de conclure dans ce cas.

• Si le noyau de ρ_{V} est trivial, considérons un sous-groupe commutatif A de G, distingué, et non contenu dans le centre de G (cf. (ii) de la prop. C.1.1). En particulier, il existe $a \in \mathrm{A}$ et $g \in \mathrm{G}$, avec $ag \neq ga$, et comme le noyau de ρ_{V} est trivial, on a $\rho_{\mathrm{V}}(a)\rho_{\mathrm{V}}(g) \neq \rho_{\mathrm{V}}(g)\rho_{\mathrm{V}}(a)$. Ceci implique que $\rho_{\mathrm{V}}(a)$ n'est pas une homothétie et, A étant commutatif, que $\mathrm{Res}_{\mathrm{G}}^{\mathrm{A}}\,\mathrm{V}$ n'est pas isotypique. On en déduit, en utilisant la prop. C.1.3, l'existence d'un sous-groupe H de G, contenant A et distinct de G, et d'une représentation irréductible W de H, tels que $\mathrm{V} = \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{W}$. L'hypothèse de récurrence appliquée à H nous fournit un sous-groupe H' de H et $\chi \in \widehat{\mathrm{H}}'$, tels que $\mathrm{W} = \mathrm{Ind}_{\mathrm{H}'}^{\mathrm{H}}\chi$. On conclut en remarquant que

$$\mathrm{V} = \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\mathrm{Ind}_{\mathrm{H}'}^{\mathrm{H}}\chi) = \mathrm{Ind}_{\mathrm{H}'}^{\mathrm{G}}\chi.$$

Exercice C.1.5. — Soient p un nombre premier et G un groupe non commutatif d'ordre p^3. Montrer que G a p^2 représentations irréductibles de dimension 1 et $p-1$ de dimension p.

C.2. Représentations du groupe symétrique S_n

La théorie des représentations de S_n fait intervenir une combinatoire assez amusante, qui est loin d'être triviale. Nous nous contenterons de décrire les résultats, et de renvoyer le lecteur à des ouvrages plus spécialisés (comme le livre de Fulton et Harris cité dans l'introduction) pour les démonstrations (qu'il peut aussi voir comme une série de défis...).

1. Partitions de n et représentations de S_n

Soit n un entier $\geqslant 1$. Une *partition* $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_r)$ de n est une décomposition de n sous la forme $n = \ell_1 + \cdots + \ell_r$, avec $\ell_1 \geqslant \ell_2 \geqslant \cdots \geqslant \ell_r \geqslant 1$. Le nombre de partitions [1] de n est traditionnellement noté $p(n)$. Par exemple, les partitions de 1, 2, 3, 4, 5 et 6 sont données par

1. L'étude de la fonction $p(n)$ a donné lieu à de nombreux travaux ; la plupart ont pour point de départ la formule

$$\sum_{n=1}^{+\infty} p(n)\mathrm{T}^n = \prod_{\ell=1}^{+\infty} \frac{1}{1-\mathrm{T}^\ell},$$

qui se démontre en remarquant que $\frac{1}{1-\mathrm{T}^\ell} = \sum_{i=0}^{+\infty} \mathrm{T}^{i\ell}$, et en développant brutalement le second membre. Cette formule fait intervenir l'inverse de *la fonction η de Dedekind* définie par $\eta(q) = q^{1/24}\prod_{\ell=1}^{+\infty}(1-q^\ell)$, avec $q = e^{2i\pi z}$ et z variant dans le demi-plan de Poincaré. En utilisant les propriétés de la fonction η, qui se trouve être une forme modulaire de poids $\frac{1}{2}$ (prob. H.11), on peut par exemple obtenir l'équivalent asymptotique $p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}$, ce qui montre que $p(n)$ croît assez vite avec n.

1	4	5	6
	$3+1$	$4+1$	$5+1$
2	$2+2$	$3+2$	$4+2$
$1+1$	$2+1+1$	$3+1+1$	$4+1+1$
	$1+1+1+1$	$2+2+1$	$3+3$
3		$2+1+1+1$	$3+2+1$
$2+1$		$1+1+1+1+1$	$3+1+1+1$
$1+1+1$			$2+2+2$
			$2+2+1+1$
			$2+1+1+1+1$
			$1+1+1+1+1+1$

et on a $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ et $p(6) = 11$.

On munit l'ensemble des partitions de n de l'*ordre lexicographique* qui est défini par : $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_r) > \mathbf{k} = (k_1, \ldots, k_s)$ si et seulement si $\ell_i > k_i$, si i est le plus petit indice tel que $\ell_i \neq k_i$. Les partitions de 1 2, 3, 4, 5 et 6 données ci-dessus sont rangées en ordre décroissant pour l'ordre lexicographique. (C'est le meilleur moyen pour ne pas en oublier.)

Il y a une bijection naturelle $\boldsymbol{\ell} \mapsto \mathrm{C}_{\amalg\amalg}$ entre les partitions de n et les classes de conjugaison de S_n : si $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_r)$, alors $\mathrm{C}_{\amalg\amalg}$ est la classe de conjugaison de S_n constituée des permutations σ dont la décomposition en cycles est $(\ell_1, \ldots, \ell_r)$ (ce qui, rappelons-le, signifie que σ est le produit de r cycles $\tau_1, \ldots, \tau_r$ de longueurs respectives $\ell_1, \ldots, \ell_r$, et dont les supports sont disjoints).

De manière remarquable, il y a aussi une bijection naturelle entre les partitions de n et les représentations irréductibles de S_n. Si $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_s)$ est une partition de n, soit $\mathrm{S}_{\boldsymbol{\lambda}} \cong \mathrm{S}_{\lambda_1} \times \cdots \times \mathrm{S}_{\lambda_s}$ le sous-groupe de S_n constitué des permutations laissant globalement stable chacun des sous-ensembles

$$\{1, \ldots, \lambda_1\},\ \{\lambda_1 + 1, \ldots, \lambda_1 + \lambda_2\}, \ldots,\ \{\lambda_1 + \cdots + \lambda_{s-1} + 1, \ldots, \lambda_1 + \cdots + \lambda_s\}$$

de $\{1, \ldots, n\}$, et soit $\mathrm{U}_{\boldsymbol{\lambda}} = \mathrm{Ind}_{\mathrm{S}_{\boldsymbol{\lambda}}}^{\mathrm{S}_n} \mathbf{1}$. Par exemple :

- Si $\boldsymbol{\lambda} = (n)$, alors $\mathrm{U}_{\boldsymbol{\lambda}}$ est la représentation triviale.
- Si $\boldsymbol{\lambda} = (n-1, 1)$, alors $\mathrm{U}_{\boldsymbol{\lambda}}$ est la représentation standard de S_n sur $\mathbf{C}^n$ obtenue en permutant les éléments de la base canonique ; elle se décompose sous la forme $\mathbf{1} \oplus \mathrm{V}_{(n-1,1)}$, où $\mathbf{1}$ est la droite de $\mathbf{C}^n$ engendrée par $(1, \ldots, 1)$ et $\mathrm{V}_{(n-1,1)}$ est l'hyperplan d'équation $\sum_{i=1}^n x_i = 0$.
- Si $\boldsymbol{\lambda} = (1, \ldots, 1)$, on a $\mathrm{S}_{\boldsymbol{\lambda}} = \{1\}$, et donc $\mathrm{U}_{(1,\ldots,1)}$ est la représentation régulière de S_n.

Comme le montre déjà l'exemple de $\mathrm{U}_{(n-1,1)}$, la représentation $\mathrm{U}_{\boldsymbol{\lambda}}$ n'est pas irréductible, mais sa décomposition en représentations irréductibles fait apparaître une unique représentation irréductible $\mathrm{V}_{\boldsymbol{\lambda}}$ qui n'apparaît pas déjà dans les $\mathrm{U}_{\boldsymbol{\mu}}$, pour $\boldsymbol{\mu} > \boldsymbol{\lambda}$. On peut d'ailleurs donner une construction directe de $\mathrm{V}_{\boldsymbol{\lambda}}$ (voir plus loin).

2. Diagrammes de Young et représentations de S_n

Si $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_r)$ est une partition de n, on note $\mathrm{Y}_{\boldsymbol{\lambda}}$ le *diagramme de Young attaché à* $\boldsymbol{\lambda}$: c'est le sous-ensemble du carré $n \times n$ obtenu en prenant les λ_1 premières cases de la $1^{\text{ère}}$ ligne, les λ_2 premières cases de la $2^{\text{ème}}$ ligne, ..., les λ_r premières cases de la r-ième ligne. Si $\boldsymbol{\lambda}^* = (\lambda_1^*, \dots, \lambda_s^*)$ est la partition de n *conjuguée de* $\boldsymbol{\lambda}$, obtenue en définissant λ_i^* comme le nombre de λ_j qui sont $\geqslant i$ (et donc $\lambda_1^* = r$, et $s = \lambda_1$), alors $\mathrm{Y}_{\boldsymbol{\lambda}}$ est aussi obtenu en prenant les λ_1^* premières cases de la $1^{\text{ère}}$ colonne, les λ_2^* premières cases de la $2^{\text{ème}}$ colonne,... En particulier, les diagrammes de Young de $\boldsymbol{\lambda}$ et $\boldsymbol{\lambda}^*$ sont symétriques par rapport à la diagonale.

La représentation $\mathrm{V}_{\boldsymbol{\lambda}}$ admet la construction directe suivante : on remplit le diagramme de Young associé à $\boldsymbol{\lambda}$ avec les nombres de 1 à n (on obtient de la sorte un *tableau de Young*). Ceci permet de définir deux sous-groupes A et B de S_n, en prenant pour A (resp. pour B) l'ensemble des permutations de $\{1, \dots, n\}$ qui préserve globalement chaque ligne (resp. chaque colonne). Alors $\mathrm{V}_{\boldsymbol{\lambda}}$ est la sous-représentation de la représentation régulière $\oplus_{\sigma \in \mathrm{S}_n} \mathbf{C} e_\sigma$ de S_n engendrée par le vecteur $\sum_{a \in \mathrm{A},\, b \in \mathrm{B}} \mathrm{sign}(b) e_{ab}$. Le sous-espace engendré par $\sum_{a \in \mathrm{A},\, b \in \mathrm{B}} \mathrm{sign}(b) e_{ab}$ dépend du tableau de Young, mais il est facile de voir que, à isomorphisme près, la représentation obtenue n'en dépend pas ; elle ne dépend que de la partition $\boldsymbol{\lambda}$.

Par exemple, si $\boldsymbol{\lambda} = (1, \dots, 1)$, on a $\mathrm{A} = \{1\}$ et $\mathrm{B} = \mathrm{S}_n$. La représentation $\mathrm{V}_{\boldsymbol{\lambda}}$ est engendrée par $v = \sum_{\sigma \in \mathrm{S}_n} \mathrm{sign}(\sigma) e_\sigma$, et comme $g \cdot v = \mathrm{sign}(g)\, v$, si $g \in \mathrm{S}_n$ (ne pas oublier que $\mathrm{sign}(g) \in \{\pm 1\}$), cette représentation est la représentation de dimension 1 correspondant au caractère linéaire sign de S_n. Plus généralement, il est facile, sur la construction ci-dessus, de voir que $\mathrm{V}_{\boldsymbol{\lambda}^*} = \mathrm{V}_{\boldsymbol{\lambda}} \otimes \mathrm{sign}$.

La dimension de $\mathrm{V}_{\boldsymbol{\lambda}}$ est donnée par la *formule des équerres*. Si a est une case du diagramme de Young de $\boldsymbol{\lambda}$, l'équerre E_a de sommet a, est la réunion des cases se trouvant à droite, sur la même ligne que a, ou en dessous, sur la même colonne que a (en incluant a) ; la longueur $\lg(\mathrm{E}_a)$ est le nombre de ses éléments. On a alors

$$\dim \mathrm{V}_{\boldsymbol{\lambda}} = \frac{n!}{\prod_{a \in \mathrm{Y}_{\boldsymbol{\lambda}}} \lg(\mathrm{E}_a)}.$$

Exercice C.2.1. — Calculer les dimensions des représentations irréductibles de S_3, S_4 et S_5, et comparer les résultats avec les ex. I.3.23, I.3.26 et I.3.27.

3. Caractères de S_n

Les caractères de $\mathrm{U}_{\boldsymbol{\lambda}}$ et $\mathrm{V}_{\boldsymbol{\lambda}}$ ont des expressions compactes assez miraculeuses : si $\boldsymbol{\ell} = (\ell_1, \dots, \ell_r)$, et si $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_s)$, alors

$$\chi_{\mathrm{U}_{\boldsymbol{\lambda}}}(\mathrm{C}_{\boldsymbol{\ell}}) = \text{coefficient de } \mathrm{X}_n^{\lambda_1} \cdots \mathrm{X}_n^{\lambda_n} \text{ dans } \mathrm{P}_{\boldsymbol{\ell}},$$
$$\chi_{\mathrm{V}_{\boldsymbol{\lambda}}}(\mathrm{C}_{\boldsymbol{\ell}}) = \text{coefficient de } \mathrm{X}_1^{\lambda_1 + n - 1} \cdots \mathrm{X}_n^{\lambda_n} \text{ dans } \mathrm{P}_{\boldsymbol{\ell}} \cdot \prod_{i < j \leqslant n} (\mathrm{X}_i - \mathrm{X}_j),$$

où $P_{II}(X_1,\dots,X_n) = (X_1^{\ell_1}+\cdots+X_n^{\ell_1})\cdots(X_1^{\ell_r}+\cdots+X_n^{\ell_r})$, et où on a posé $\lambda_i = 0$ si $s+1 \leqslant i \leqslant n$.

La formule pour $\chi_{U_{\boldsymbol{\lambda}}}$ est assez facile à établir car $U_{\boldsymbol{\lambda}}$ est une représentation induite, ce qui permet d'utiliser le th. I.3.13. Le passage de $U_{\boldsymbol{\lambda}}$ à $V_{\boldsymbol{\lambda}}$ utilise la combinatoire des polynômes de Schur.

Si $\boldsymbol{\mu} = (\mu_1,\dots,\mu_s)$ est une partition de n, on note encore $\boldsymbol{\mu}$ la famille $(\mu_1,\dots,\mu_n)$, avec $\mu_i = 0$ si $s+1 \leqslant i \leqslant n$. On définit le *polynôme de Schur* $\mathrm{Sch}_{\boldsymbol{\mu}}$ par

$$\mathrm{Sch}_{\boldsymbol{\mu}}(X_1,\dots,X_n) = \frac{\det\begin{pmatrix} X_1^{\mu_1+n-1} & \dots & X_n^{\mu_n+n-1} \\ \vdots & X_j^{\mu_j+n-i} & \vdots \\ X_1^{\mu_1} & \dots & X_n^{\mu_n} \end{pmatrix}}{\det\begin{pmatrix} X_1^{n-1} & \dots & X_n^{n-1} \\ \vdots & X_j^{n-i} & \vdots \\ 1 & \dots & 1 \end{pmatrix}}$$

Si $\boldsymbol{\lambda} = (\lambda_1,\dots,\lambda_r)$ est une autre partition de n, on définit le *nombre de Kostka* $K_{\boldsymbol{\mu},\boldsymbol{\lambda}}$ comme le coefficient de $X_1^{\lambda_1}\cdots X_r^{\lambda_r}$ dans $\mathrm{Sch}_{\boldsymbol{\mu}}(X_1,\dots,X_n)$.

On a $U_{\boldsymbol{\lambda}} = \sum_{\boldsymbol{\mu}} K_{\boldsymbol{\mu},\boldsymbol{\lambda}} V_{\boldsymbol{\mu}}$, et $K_{\boldsymbol{\mu},\boldsymbol{\lambda}} = 0$, si $\boldsymbol{\mu} < \boldsymbol{\lambda}$, $K_{\boldsymbol{\lambda},\boldsymbol{\lambda}} = 1$. C'est comme ça que l'on vérifie que $V_{\boldsymbol{\lambda}}$ n'apparaît pas dans les $U_{\boldsymbol{\mu}}$, pour $\boldsymbol{\mu} > \boldsymbol{\lambda}$. Comme de plus $U_{(1,\dots,1)}$ est la représentation régulière, on déduit du cor. I.2.23, et de la formule ci-dessus, que $\dim V_{\boldsymbol{\mu}} = K_{\boldsymbol{\mu},(1,\dots,1)}$.

Le nombre $K_{\boldsymbol{\mu},\boldsymbol{\lambda}}$ a aussi une interprétation combinatoire : c'est le nombre de manières de remplir le diagramme de Young de $\boldsymbol{\lambda}$ avec λ_1 fois le nombre 1, λ_2 fois le nombre 2,..., λ_r fois le nombre r, de telle sorte que chaque ligne soit croissante (au sens large) et chaque colonne soit strictement croissante.

En utilisant la formule ci-dessus pour la dimension de $V_{\boldsymbol{\mu}}$, on en déduit que $\dim V_{\boldsymbol{\mu}}$ est le nombre de tableaux de Young pour la partition $\boldsymbol{\mu}$ dans lesquels les lignes et les colonnes sont croissantes ; un tel tableau de Young est dit *standard*[2]. Il n'est pas totalement évident de prouver, combinatoirement, que ceci coïncide avec la formule des équerres.

C.3. Représentations de $\mathbf{GL}_2(\mathbf{F})$

1. Le groupe $\mathbf{GL}_2(\mathbf{F})$

Soit $\mathbf{F}$ un corps fini de cardinal q. Il existe alors un nombre premier p tel que l'on ait $p = 0$ dans $\mathbf{F}$, ce qui fait que $\mathbf{F}$ est un $\mathbf{F}_p$-espace vectoriel de dimension finie (avec $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$), et donc que q est une puissance de p.

2. C. Schensted (1961) a établi une bijection entre les paires de tableaux de Young standard de même forme et les permutations, ce qui fournit une démonstration combinatoire de la formule de Burnside ((ii) du cor. I.2.23) dans le cas de S_n (modulo la formule des équerres).

Soit $\mathrm{G} = \mathbf{GL}_2(\mathbf{F})$ le groupe des matrices 2×2, à coefficients dans $\mathbf{F}$, de déterminant non nul. Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{M}_2(\mathbf{F})$, alors $g \in \mathrm{G}$, si et seulement si les vecteurs colonnes de la matrice sont linéairement indépendants sur $\mathbf{F}$, ce qui signifie que le premier vecteur est non nul et que le second n'est pas dans la droite engendrée par le premier. On en déduit que $|\mathbf{GL}_2(\mathbf{F})| = (q^2-1)(q^2-q)$.

Le corps $\mathbf{F}$ a une unique extension $\mathbf{K}$ de degré 2 (cf. n° 8.7 du vocabulaire). Si $p \neq 2$, on choisit $\Delta \in \mathbf{F}^*$ qui n'est pas un carré [3] dans $\mathbf{F}^*$, et une racine carrée δ de Δ dans $\mathbf{K}$. On peut alors associer à $z = x + \delta y$ la matrice $\mathrm{C}_z = \left(\begin{smallmatrix} x & \Delta y \\ y & x \end{smallmatrix}\right)$ de la multiplication par z dans la base $1, \delta$ de $\mathbf{K}$ sur $\mathbf{F}$ [4]. La conjugaison par $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ envoie C_z, avec $z = x + \delta y$, sur $\mathrm{C}_{\overline{z}}$, avec $\overline{z} = x - \delta y$, comme le montre un calcul immédiat.

2. Construction de représentations de $\mathbf{GL}_2(\mathbf{F})$

On cherche à faire la liste des représentations irréductibles de G. Le théorème de Brauer (th. I.3.20) montre que l'on peut les obtenir à partir d'induites de caractères linéaires de sous-groupes. Par ailleurs, comme les dimensions des représentations irréductibles ont tendance à être assez petites, on a intérêt à induire à partir des sous-groupes les plus gros possibles. Toutes les représentations ci-dessous sont obtenues avec ces considérations en tête.

• *Représentations de dimension* 1. Si $\eta \in \widehat{\mathbf{F}^*}$ est un caractère linéaire de $\mathbf{F}^*$, on fabrique un caractère linéaire $\eta \circ \det$ de G en composant avec le déterminant.

• *La steinberg et ses tordues.* On note $\mathbf{P}^1(\mathbf{F})$ l'ensemble des droites vectorielles de $\mathbf{F}^2$; c'est un ensemble à $q+1$ éléments sur lequel G agit. Il lui correspond donc une représentation de permutation $\mathrm{V}_{\mathbf{P}^1(\mathbf{F})} = \oplus_{x \in \mathbf{P}^1(\mathbf{F})} \mathbf{C} e_x$, qui n'est pas irréductible puisque la droite engendrée par $\sum_{x \in \mathbf{P}^1(\mathbf{F})} e_x$ est fixe par G. On note St la représentation de G sur l'hyperplan $\{\sum_{x \in \mathbf{P}^1(\mathbf{F})} \lambda_x e_x,\ \sum_{x \in \mathbf{P}^1(\mathbf{F})} \lambda_x = 0\}$; c'est une représentation de dimension q.

Plus généralement, si $\eta \in \widehat{\mathbf{F}^*}$, on peut considérer la représentation $\mathrm{St} \otimes (\eta \circ \det)$ obtenue en tordant l'action de G sur St par le caractère linéaire $\eta \circ \det$.

• *La série principale.* Soit B le *sous-groupe de Borel* de G ; c'est l'ensemble des matrices triangulaires supérieures inversibles. Si $\eta_1, \eta_2 \in \widehat{\mathbf{F}^*}$ sont deux caractères linéaires de $\mathbf{F}^*$, on note $\eta_1 \otimes \eta_2$ le caractère linéaire de B défini par

$$(\eta_1 \otimes \eta_2)\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \eta_1(a)\eta_2(d).$$

Si $\eta_1 \neq \eta_2$, la représentation $\mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}} \eta_1 \otimes \eta_2$ est dite *de la série principale.* [5]

3. Si $p = 2$, il faut modifier un peu ce qui suit, car un polynôme de la forme $\mathrm{X}^2 - \Delta$ n'est jamais irréductible. On choisit $\Delta \in \mathbf{F}$ qui n'est pas dans l'image de $x \mapsto x^2 + x$, et $\delta \in \mathbf{K}$ vérifiant $\delta^2 + \delta = \Delta$. On peut alors associer à $z = x + \delta y$ la matrice $\mathrm{C}_z = \left(\begin{smallmatrix} x & \Delta y \\ y & x+y \end{smallmatrix}\right)$ de la multiplication par z dans la base $1, \delta$ de $\mathbf{K}$ sur $\mathbf{F}$. La conjugaison par $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ envoie C_z, avec $z = x + \delta y$, sur $\mathrm{C}_{\overline{z}}$, avec $\overline{z} = x + (\delta + 1)y$.

4. On remarquera la similarité avec la représentation matricielle des nombres complexes.

5. Le lecteur pourra vérifier que $\mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}} \eta \otimes \eta = \mathrm{V}_{\mathbf{P}^1(\mathbf{F})} \otimes (\eta \circ \det)$, ce qui explique que l'on ne s'intéresse pas au cas $\eta_1 = \eta_2$.

• *Autres représentations.* Comme nous le verrons, les représentations précédentes sont irréductibles, mais ne suffisent pas à remplir la liste des représentations irréductibles de G. Les représentations qui suivent ne sont pas irréductibles (on induit à partir d'un sous-groupe trop petit), mais contiennent les représentations qui nous manquent.

– Soit $\mathrm{C} \subset \mathrm{G}$ l'image de $\mathbf{K}^*$ par l'application $z \mapsto \mathrm{C}_z$. C'est un sous-groupe [6] de G de cardinal q^2-1. Si $\eta \in \widehat{\mathbf{K}^*}$, on peut aussi considérer η comme un caractère de C, en utilisant l'isomorphisme $z \mapsto \mathrm{C}_z$ de $\mathbf{K}^*$ sur C, et nous aurons à considérer la représentation $\mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \eta$.

– Soit $\mathrm{ZU} \subset \mathrm{B}$ le sous-groupe des matrices ayant une seule valeur propre (Z est là pour désigner le centre, qui est l'ensemble des matrices d'homothéties de rapport non nul, et U est le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale ; une telle matrice est unipotente). On fixe un caractère linéaire non trivial $\psi \in \widehat{\mathbf{F}}$ de $\mathbf{F}$, et si $\eta \in \widehat{\mathbf{F}^*}$ est un caractère linéaire de $\mathbf{F}^*$, on note $\eta \otimes \psi$ le caractère linéaire de ZU défini par

$$(\eta \otimes \psi)\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) = \eta(a)\psi(a^{-1}b).$$

Nous aurons à considérer la représentation $\mathrm{Ind}_{\mathrm{ZU}}^{\mathrm{G}} \eta \otimes \psi$. En fait, le cas qui nous intéressera est celui où on part d'un élément η de $\widehat{\mathbf{K}^*}$, que l'on restreint à $\mathbf{F}^*$ (nous nous permettrons de garder le même nom pour la restriction).

3. Les classes de conjugaison de $\mathbf{GL}_2(\mathbf{F})$

Comme $\mathbf{F}$ a une unique extension de degré 2, la classification, à conjugaison près par une matrice inversible, des matrices 2×2 à coefficients dans $\mathbf{F}$, est identique à ce qui se passe sur $\mathbf{R}$. Il y a quatre types distincts :

• type I : A est scalaire, et donc de la forme $a_x = \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$, avec $x \in \mathbf{F}$;

• type II : A a une unique valeur propre $x \in \mathbf{F}$, mais n'est pas diagonalisable ; elle est alors conjuguée à $b_x = \left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)$;

• type III : A a deux valeurs propres $x \neq y$ dans $\mathbf{F}$, et donc est conjuguée à $b_{x,y} = \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$, et donc aussi à $b_{y,x}$;

• type IV : A n'a pas de valeurs propres dans $\mathbf{F}$, et donc a deux valeurs propres $z \neq \overline{z}$ dans $\mathbf{K}$, et A est conjuguée à c_z et $c_{\overline{z}}$.

Comme on s'intéresse aux classes de conjugaison de G, il faut ne garder que les matrices inversibles dans l'énumération ci-dessus. On aboutit à la liste de paramètres de la fig. 1.

6. Un tel sous-groupe est un *sous-groupe de Cartan non déployé*, un sous-groupe de Cartan déployé étant un sous-groupe conjugué au sous-groupe des matrices diagonales.

	description	**cardinal**
$\mathrm{E_I}$	$\mathbf{F}^*$	$q-1$
$\mathrm{E_{II}}$	$\mathbf{F}^*$	$q-1$
$\mathrm{E_{III}}$	$\{(x,y)\in\mathbf{F}^*\times\mathbf{F}^*,\ x\neq y\}/(x,y)\sim(y,x)$	$\frac{1}{2}(q-1)(q-2)$
$\mathrm{E_{IV}}$	$\{z\in\mathbf{K}^*,\ \overline{z}\neq z\}/\overline{z}\sim z$	$\frac{1}{2}q(q-1)$

FIGURE 1. Paramètres des classes de conjugaison de $\mathbf{GL}_2(\mathbf{F})$

Proposition C.3.1. — *La liste des classes de conjugaison de* $\mathbf{GL}_2(\mathbf{F})$ *est celle de la figure 2*

type	**nombre**	**classe**	**représentant**	**cardinal**
I	$q-1$	a_x, $x\in\mathrm{E_I}$	$\mathrm{A}_x=\left(\begin{smallmatrix}x&0\\0&x\end{smallmatrix}\right)$	1
II	$q-1$	b_x, $x\in\mathrm{E_{II}}$	$\mathrm{B}_x=\left(\begin{smallmatrix}x&1\\0&x\end{smallmatrix}\right)$	q^2-1
III	$\frac{(q-1)(q-2)}{2}$	$b_{x,y}$, $(x,y)\in\mathrm{E_{III}}$	$\mathrm{B}_{x,y}=\left(\begin{smallmatrix}x&0\\0&y\end{smallmatrix}\right)$	$q(q+1)$
IV	$\frac{q^2-q}{2}$	c_z, $z=x+\delta y\in\mathrm{E_{IV}}$	$\mathrm{C}_z=\left(\begin{smallmatrix}x&\Delta y\\y&x\end{smallmatrix}\right)$	q^2-q

FIGURE 2. Classes de conjugaison de $\mathbf{GL}_2(\mathbf{F})$

Démonstration. — La seule chose qui ne suive pas directement de la discussion précédant la proposition, est la détermination du cardinal de chacune des classes. De manière générale, si G est un groupe, et $x\in\mathrm{G}$, la classe de conjugaison de x est l'orbite O_x de x sous l'action de G par conjugaison intérieure ($g\cdot x=gxg^{-1}$) ; si Z_x est le centralisateur de x dans G (i.e. est l'ensemble des éléments de G commutant à x), on a $\mathrm{O}_x=\mathrm{G}/\mathrm{Z}_x$, et donc $|\mathrm{O}_x|=\frac{|\mathrm{G}|}{|\mathrm{Z}_x|}$. On est donc ramené au problème de déterminer l'ensemble des matrices inversibles commutant à une matrice donnée. Or, si $\mathrm{A}\in\mathbf{M}_2(\mathbf{F})$, l'ensemble des matrices $\mathrm{M}\in\mathbf{M}_2(\mathbf{F})$ qui commutent à A sont :

- $\mathbf{M}_2(\mathbf{F})$ tout entier, si A est scalaire.
- le sous-espace vectoriel engendré par $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ et A, si A n'est pas scalaire [7].

On déduit de cette discussion les résultats suivants :

- Tout commute à A_x et donc il y a un seul élément dans a_x.
- Les matrices commutant à B_x sont de la forme $\left(\begin{smallmatrix}a&b\\0&a\end{smallmatrix}\right)$, avec $a,b\in\mathbf{F}$, et une telle matrice est inversible si et seulement si $a\neq 0$. Le centralisateur de B_x est donc de cardinal $q(q-1)$ et le nombre d'éléments de b_x est $\frac{(q^2-1)(q^2-q)}{q(q-1)}=q^2-1$.

7. Un calcul brutal montre que l'espace des solutions est de dimension 2 si A n'est pas scalaire, et comme 1 et A commutent à A, et sont linéairement indépendantes, cela permet de conclure. Cet argument est raisonnable en dimension 2, mais pour déterminer le commutant d'une matrice en dimension quelconque, il vaut mieux utiliser le point de vue du n° 10.2 du § 10.

• si $x \neq y$, les matrices commutant à $\mathrm{B}_{x,y}$ sont de la forme $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$, avec $a, b \in \mathbf{F}$, et une telle matrice est inversible si et seulement si $a \neq 0$ et $b \neq 0$. Le centralisateur de $\mathrm{B}_{x,y}$ est donc de cardinal $(q-1)^2$ et le nombre d'éléments de $b_{x,y}$ est $\frac{(q^2-1)(q^2-q)}{(q-1)^2} = q(q+1)$.

• si $z \in \mathbf{K} - \mathbf{F}$, les matrices commutant à C_z sont de la forme $\mathrm{C}_{z'}$, avec $z' \in \mathbf{K}$, et une telle matrice est inversible si et seulement si $z' \neq 0$. Le centralisateur de C_z est donc de cardinal $q^2 - 1$ et le nombre d'éléments de c_z est $\frac{(q^2-1)(q^2-q)}{q^2-1} = q(q-1)$.

Ceci permet de conclure.

4. La table des caractères de $\mathbf{GL}_2(\mathbf{F})$

On suppose dorénavant que q n'est pas une puissance de 2 (il y a des petites modifications (cf. note 3) à faire dans le cas $p = 2$; nous les laissons en exercice). Les caractères de G se paramètrent de manière parallèle aux classes de conjugaison de G. Il y a aussi 4 types paramètrés par les ensembles $\mathrm{E}^*_{\mathrm{I}}$, $\mathrm{E}^*_{\mathrm{II}}$, $\mathrm{E}^*_{\mathrm{III}}$ et $\mathrm{E}^*_{\mathrm{IV}}$ de la figure 3.

	description	**cardinal**
$\mathrm{E}^*_{\mathrm{I}}$	$\widehat{\mathbf{F}^*}$	$q-1$
$\mathrm{E}^*_{\mathrm{II}}$	$\widehat{\mathbf{F}^*}$	$q-1$
$\mathrm{E}^*_{\mathrm{III}}$	$\{(\eta_1, \eta_2) \in \widehat{\mathbf{F}^*} \times \widehat{\mathbf{F}^*},\ \eta_1 \neq \eta_2\}/(\eta_1, \eta_2) \sim (\eta_2, \eta_1)$	$\frac{1}{2}(q-1)(q-2)$
$\mathrm{E}^*_{\mathrm{IV}}$	$\{\eta \in \widehat{\mathbf{K}^*},\ \eta^* \neq \eta\}/\eta^* \sim \eta$	$\frac{1}{2}q(q-1)$

FIGURE 3. Paramètres des caractères de $\mathbf{GL}_2(\mathbf{F})$

Dans le tableau ci-dessus, on a noté η^* le caractère linéaire $z \mapsto \eta(\overline{z})$, si $\eta \in \widehat{\mathbf{K}^*}$.

type	I	II	III	IV
nombre	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q(q-1)}{2}$
caractère	α_η, $\eta \in \mathrm{E}^*_{\mathrm{I}}$	β_η, $\eta \in \mathrm{E}^*_{\mathrm{II}}$	β_{η_1,η_2}, $(\eta_1, \eta_2) \in \mathrm{E}^*_{\mathrm{III}}$	γ_η, $\eta \in \mathrm{E}^*_{\mathrm{IV}}$
dimension	1	q	$q+1$	$q-1$
a_x	$\eta(x)^2$	$q\eta(x)^2$	$(q+1)\eta_1\eta_2(x)$	$(q-1)\eta(x)$
b_x	$\eta(x)^2$	0	$\eta_1\eta_2(x)$	$-\eta(x)$
$b_{x,y}$	$\eta(xy)$	$\eta(xy)$	$\eta_1(x)\eta_2(y) + \eta_1(y)\eta_2(x)$	0
c_z	$\eta(z\,\overline{z})$	$-\eta(z\,\overline{z})$	0	$-(\eta(z) + \eta^*(z))$

FIGURE 4. Table des caractères de $\mathbf{GL}_2(\mathbf{F})$

Théorème C.3.2. — *La table des caractères de* $\mathbf{GL}_2(\mathbf{F})$ *est celle donnée par la figure 4.*

Démonstration. — On note X l'ensemble des fonctions centrales apparaissant dans le tableau (i.e. de la forme α_η, β_η, β_{η_1,η_2} ou γ_η). Comme il y a autant de paramètres pour les éléments de X que pour les classes de conjugaison de G, il suffit de vérifier que les χ correspondant à deux paramètres distincts sont différents (lemme C.3.6) et que $\chi \in \mathrm{Irr}(\mathrm{G})$, si $\chi \in \mathrm{X}$. Pour vérifier ce deuxième point, il suffit, d'après l'ex. I.2.22, de vérifier que

- $\chi(1) \geqslant 0$ (ce qui est évident),
- $\langle \chi, \chi \rangle = 1$ (ce qui fait l'objet du lemme C.3.5),
- $\chi \in \mathrm{R}_{\mathbf{Z}}(\mathrm{G})$ (ce qui fait l'objet du lemme C.3.4).

Remarque C.3.3. — (i) Remplacer le couple (η_1, η_2) par (η_2, η_1) ne change rien dans la colonne du type III, ce qui montre que l'on peut effectivement passer au quotient par la relation d'équivalence $(\eta_1, \eta_2) \sim (\eta_2, \eta_1)$.

(ii) De même, remplacer η par η^* ne change rien dans la colonne du type IV (car $\eta^*(x) = \eta(x)$, si $x \in \mathbf{F}^*$), ce qui montre que l'on peut effectivement passer au quotient par la relation d'équivalence $\eta \sim \eta^*$.

5. Démonstrations

Lemme C.3.4. — (i) *Si* $\eta \in \widehat{\mathbf{F}^*}$, *alors* $\alpha_\eta = \eta \circ \det$.

(ii) *Si* $\eta \in \widehat{\mathbf{F}^*}$, *alors* β_η *est le caractère de* $\mathrm{St} \otimes (\eta \circ \det)$.

(iii) *Si* $(\eta_1, \eta_2) \in \mathrm{E}_{\mathrm{III}}$, *alors* β_{η_1,η_2} *est le caractère de* $\mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}} \eta_1 \otimes \eta_2$.

(iv) *Si* $\eta \in \mathrm{E}_{\mathrm{IV}}$, *alors* $\gamma_\eta = \mathrm{Ind}_{\mathrm{ZU}}^{\mathrm{G}} \eta \otimes \psi - \mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \eta$.

Démonstration. — Le (i) est immédiat. Pour démontrer le reste, nous noterons (e_1, e_2) la base canonique de $\mathbf{F}^2$.

• Pour démontrer le (ii), il faut commencer par calculer le caractère χ_{St} de St. Pour ce faire, on commence par calculer le caractère $\chi_{\mathbf{P}^1(\mathbf{F})}$ de la représentation de permutation $\mathrm{V}_{\mathbf{P}^1(\mathbf{F})}$, et on est ramené (alinéa 2.3 du § I.1) à calculer le nombre de points fixes de l'action de $g \in \mathrm{G}$ sur $\mathbf{P}^1(\mathbf{F})$. Comme les points fixes sont exactement les droites propres de $\mathbf{F}^2$ sous l'action de g, on voit que le nombre de points fixes de A_x est $q+1$, celui de B_x est 1 (la droite $\mathbf{F}e_1$), celui de $\mathrm{B}_{x,y}$ est 2 (les droites $\mathbf{F}e_1$ et $\mathbf{F}e_2$) et celui de C_z est 0. Comme $\mathrm{V}_{\mathbf{P}^1(\mathbf{F})} = \mathrm{St} \oplus \mathbf{1}$, on a $\chi_{\mathrm{St}} = \chi_{\mathbf{P}^1(\mathbf{F})} - 1$, et donc $\chi_{\mathrm{St}}(\mathrm{A}_x) = q$, $\chi_{\mathrm{St}}(\mathrm{B}_x) = 0$, $\chi_{\mathrm{St}}(\mathrm{B}_{x,y}) = 1$ et $\chi_{\mathrm{St}}(\mathrm{C}_z) = -1$. Le (ii) s'en déduit en tordant par le caractère $\eta \circ \det$.

• Passons au (iii). Soit $\chi = \mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}} \eta_1 \otimes \eta_2$, avec $\eta_1, \eta_2 \in \widehat{\mathbf{F}^*}$. Pour calculer χ, on part de la formule du th. I.3.13

$$\chi(g) = \frac{1}{|\mathrm{B}|} \sum_{s \in \mathrm{G},\, sgs^{-1} \in \mathrm{B}} \eta_1 \otimes \eta_2(sgs^{-1}).$$

◇ Comme A_x est dans le centre de G qui est inclus dans B, on a $s\mathrm{A}_x s^{-1} \in \mathrm{B}$ et $\eta_1 \otimes \eta_2(s\mathrm{A}_x s^{-1}) = \eta_1\eta_2(x)$, quel que soit $s \in \mathrm{G}$. On en déduit que

$$\chi(\mathrm{A}_x) = \frac{|\mathrm{G}|}{|\mathrm{B}|} \eta_1\eta_2(x) = (q+1)\eta_1\eta_2(x).$$

$\diamond$ On a $s\mathrm{B}_x s^{-1} \in \mathrm{B}$ si et seulement si $s\mathrm{B}_x s^{-1}(e_1) \in \mathbf{F}e_1$, et donc si et seulement si $\mathrm{B}_x(s^{-1}(e_1)) \in \mathbf{F}s^{-1}(e_1)$. Comme $\mathbf{F}e_1$ est la seule droite propre de B_x, cela équivaut à $s^{-1}(e_1) \in \mathbf{F}e_1$ et donc à $s \in \mathrm{B}$. Comme $\eta_1 \otimes \eta_2(s\mathrm{B}_x s^{-1}) = \eta_1\eta_2(x)$, si $s \in \mathrm{B}$, on obtient

$$\chi(\mathrm{B}_x) = \frac{1}{|\mathrm{B}|}\sum_{s\in\mathrm{B}} \eta_1\eta_2(x) = \eta_1\eta_2(x).$$

$\diamond$ On montre de même que $s\mathrm{B}_{x,y}s^{-1} \in \mathrm{B}$, si et seulement si $\mathrm{B}_{x,y}(s^{-1}(e_1)) \in \mathbf{F}s^{-1}(e_1)$, et donc si et seulement si $s^{-1}(e_1) \in \mathbf{F}e_1$ ou $s^{-1}(e_1) \in \mathbf{F}e_2$. Le premier cas équivaut à $s \in \mathrm{B}$ comme ci-dessus, et on a $\eta_1 \otimes \eta_2(s\mathrm{B}_{x,y}s^{-1}) = \eta_1(x)\eta_2(y)$; le second équivaut à $s \in \mathrm{B}w$, où $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, et on a $\eta_1 \otimes \eta_2(s\mathrm{B}_{x,y}s^{-1}) = \eta_1(y)\eta_2(x)$. On obtient donc

$$\chi(\mathrm{B}_{x,y}) = \frac{1}{|\mathrm{B}|}\Big(\sum_{s\in\mathrm{B}} \eta_1(x)\eta_2(y) + \sum_{s\in\mathrm{B}w} \eta_1(y)\eta_2(x)\Big) = \eta_1(x)\eta_2(y) + \eta_1(y)\eta_2(x).$$

$\diamond$ Si $z \in \mathbf{K}^* - \mathbf{F}^*$, il n'existe aucun $s \in \mathrm{G}$ tel que $s\mathrm{C}_z s^{-1} \in \mathrm{B}$, et donc $\chi(\mathrm{C}_z) = 0$.

• Finalement, venons-en au (iv). Soit $\eta \in \widehat{\mathbf{K}^*}$, soient χ_1 et χ_2 les caractères de $\mathrm{Ind}_{\mathrm{ZU}}^{\mathrm{G}} \eta\otimes\psi$ et $\mathrm{Ind}_{\mathrm{C}}^{\mathrm{G}} \eta$, et soit $\chi = \chi_1 - \chi_2$. D'après le th. I.3.13,

$$\chi_1(g) = \frac{1}{|\mathrm{ZU}|}\sum_{s\in\mathrm{G},\, sgs^{-1}\in\mathrm{ZU}} \eta\otimes\psi(sgs^{-1}) \quad \text{et} \quad \chi_2(g) = \frac{1}{|\mathrm{C}|}\sum_{s\in\mathrm{G},\, sgs^{-1}\in\mathrm{C}} \eta(sgs^{-1}).$$

$\diamond$ Comme $\mathrm{A}_x \in \mathrm{ZU}$ et $\mathrm{A}_x \in \mathrm{C}$, on a, comme ci-dessus,

$$\chi_1(\mathrm{A}_x) = \frac{|\mathrm{G}|}{|\mathrm{ZU}|}\eta(x) = (q^2-1)\eta(x) \quad \text{et} \quad \chi_2(\mathrm{A}_x) = \frac{|\mathrm{G}|}{|\mathrm{C}|}\eta(x) = (q^2-q)\eta(x),$$

et donc $\chi(\mathrm{A}_x) = (q-1)\eta(x)$.

$\diamond$ $\chi_1(\mathrm{B}_{x,y}) = 0$ et $\chi_1(\mathrm{C}_z) = 0$ car aucun élément de ZU n'est conjugué à $\mathrm{B}_{x,y}$ ou C_z.

$\diamond$ $\chi_2(\mathrm{B}_{x,y}) = 0$ et $\chi_2(\mathrm{B}_x) = 0$ car aucun élément de C n'est conjugué à $\mathrm{B}_{x,y}$ ou B_x.

$\diamond$ On a $\mathrm{ZU} \subset \mathrm{B}$. Or on a vu plus haut que $s\mathrm{B}_x s^{-1} \in \mathrm{B}$ implique $s \in \mathrm{B}$. De plus, comme B_x a une seule valeur propre, il en est de même de $s\mathrm{B}_x s^{-1}$, et donc $s\mathrm{B}_x s^{-1} \in \mathrm{ZU}$ si et seulement si $s \in \mathrm{B}$. Maintenant, on a

$$\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right)\left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \delta \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} \alpha x & \alpha+\beta x \\ 0 & \delta x \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha^{-1} & -\beta\alpha^{-1}\delta^{-1} \\ 0 & \delta^{-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & \alpha\delta^{-1} \\ 0 & x \end{smallmatrix}\right).$$

On en déduit que

$$\chi_1(\mathrm{B}_x) = \frac{1}{|\mathrm{ZU}|}\sum_{\alpha,\delta\in\mathbf{F}^*,\, \beta\in\mathbf{F}} \eta(x)\psi(\alpha\delta^{-1}) = \frac{\eta(x)}{q-1}\sum_{\alpha,\delta\in\mathbf{F}^*} \psi(\alpha\delta^{-1}).$$

En faisant le changement de variable $\alpha' = \alpha\delta^{-1}$, $\delta' = \delta$, et en utilisant le fait que $\sum_{\alpha'\in\mathbf{F}} \psi(\alpha') = 0$ puisque l'on a supposé ψ non trivial (orthogonalité des caractères ψ et $\mathbf{1}$ du groupe $\mathbf{F}$), on obtient finalement

$$\chi_1(\mathrm{B}_x) = \eta(x)(-\psi(0)) = -\eta(x) \quad \text{et} \quad \chi(\mathrm{B}_x) = -\eta(x).$$

$\diamond$ Si $s\mathrm{C}_z s^{-1} \in \mathrm{C}$, alors $s\mathrm{C}_z s^{-1}$ est égal à C_z ou $\mathrm{C}_{\overline{z}}$ (le polynôme caractéristique de C_z est égal à $\mathrm{X}^2 - (z+\overline{z})\mathrm{X} + z\overline{z}$, et donc celui de $s\mathrm{C}_z s^{-1}$ aussi). Si $s\mathrm{C}_z s^{-1} = \mathrm{C}_z$, alors s est

dans le centralisateur de C_z qui, comme on l'a vu (dém. de la prop. C.3.1), est égal à C ; si $s\mathrm{C}_z s^{-1} = \mathrm{C}_{\overline{z}}$, alors $s\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\mathrm{C}_{\overline{z}}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)s^{-1} = \mathrm{C}_{\overline{z}}$, et donc $s\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ est dans le centralisateur de $\mathrm{C}_{\overline{z}}$, et $s \in \mathrm{C}\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$. On en déduit que

$$\chi_2(\mathrm{C}_z) = \frac{1}{|\mathrm{C}|}\Big(\sum_{s\in\mathrm{C}} \eta(z) + \sum_{s\in\mathrm{C}} \eta(\overline{z})\Big) = \eta(z) + \eta^*(z) \quad \text{et} \quad \chi(\mathrm{C}_z) = -(\eta(z) + \eta^*(z)).$$

Ceci permet de conclure

Lemme C.3.5. — *Si $\chi \in \mathrm{X}$, alors $\langle \chi, \chi\rangle = 1$.*

Démonstration. — Si ϕ est une fonction centrale sur G, il résulte de la table des classes de conjugaison, que

$$\begin{aligned}|\mathrm{G}|\langle\phi,\phi\rangle = {} & \sum_{x\in\mathbf{F}^*} |\phi(a_x)|^2 + (q^2-1)\sum_{x\in\mathbf{F}^*} |\phi(b_x)|^2 \\ & + q(q+1)\sum_{\substack{(x,y)\in(\mathbf{F}^*)^2,\ x\neq y\\ \mathrm{mod}\,(x,y)\mapsto(y,x)}} |\phi(b_{x,y})|^2 + q(q-1)\sum_{\substack{z\in\mathbf{K}^*-\mathbf{F}^*\\ \mathrm{mod}\, z\mapsto\overline{z}}} |\phi(c_z)|^2\end{aligned}$$

Il nous faut vérifier que $|\mathrm{G}|\langle\phi,\phi\rangle = |\mathrm{G}| = (q^2-1)(q^2-q)$, si ϕ est un des caractères apparaissant dans la table 4.

• Pour un caractère du type $\eta\circ\det$, il n'y a rien à faire puisque l'on a affaire au caractère d'une représentation de dimension 1 qui est automatiquement irréductible.

• On remarque que, si ϕ est le caractère de la représentation $\mathrm{St}\otimes(\eta\circ\det)$, les contributions des classes $b_{x,y}$ et c_z sont les mêmes que pour $\eta\circ\det$. Il suffit donc de vérifier que $\sum_{x\in\mathbf{F}^*}|\phi(a_x)|^2 + (q^2-1)\sum_{x\in\mathbf{F}^*}|\phi(b_x)|^2$ a la même valeur que dans le cas $\phi = \eta\circ\det$, ce qui est immédiat, les deux sommes valant $(q-1)q^2$.

• Dans le cas où $\phi = \beta_{\eta_1,\eta_2}$, avec $\eta_1,\eta_2 \in \widehat{\mathbf{F}^*}$ et $\eta_1 \neq \eta_2$, la somme à évaluer devient

$$(q-1)(q+1)^2 + (q-1)(q^2-1) + q(q+1)\sum_{\substack{(x,y)\in(\mathbf{F}^*)^2,\ x\neq y\\ \mathrm{mod}\,(x,y)\mapsto(y,x)}} |\eta_1(x)\eta_2(y) + \eta_2(x)\eta_1(y)|^2.$$

Comme $\overline{\eta}(a) = \eta(a)^{-1} = \eta(a^{-1})$, on peut écrire $|\eta_1(x)\eta_2(y) + \eta_2(x)\eta_1(y)|^2$ sous la forme

$$2 + \eta_1(x)\eta_2(y)\overline{\eta_2(x)\eta_1(y)} + \overline{\eta_1(x)\eta_2(y)}\eta_2(x)\eta_1(y) = 2 + (\eta_1/\eta_2)(x/y) + (\eta_2/\eta_1)(y/x).$$

Ceci permet de mettre $\sum|\eta_1(x)\eta_2(y) + \eta_2(x)\eta_1(y)|^2$ sous la forme

$$(q-1)(q-2) + \sum_{(x,y)\in(\mathbf{F}^*)^2,\ x\neq y} (\eta_1/\eta_2)(x/y) = (q-1)(q-2) + \sum_{(x,y)\in(\mathbf{F}^*)^2} (\eta_1/\eta_2)(x/y) - (q-1).$$

Maintenant, comme $\eta_1 \neq \eta_2$, on a $\sum_{(x,y)\in(\mathbf{F}^*)^2}(\eta_1/\eta_2)(x/y) = 0$. La somme à évaluer est donc, finalement, égale à

$$(q-1)(q+1)^2 + (q-1)(q^2-1) + q(q+1)(q-1)(q-3) = (q^2-1)(q+1+q-1+q(q-3)) = (q^2-1)(q^2-q),$$

ce que l'on voulait.

• Dans le cas où $\phi = \gamma_\eta$, avec $\eta \in \widehat{\mathbf{K}^*}$ et $\eta \neq \eta^*$, la somme à évaluer est

$$(q-1)(q-1)^2 + (q-1)(q^2-1) + q(q-1) \sum_{z \in \mathbf{K}^* - \mathbf{F}^*, \bmod z \mapsto \overline{z}} |\eta(z) + \eta^*(z)|^2.$$

Les mêmes calculs que ci-dessus (en utilisant le fait que $\eta^*(z) = \eta(\overline{z})$) permettent de mettre $\sum_{z \in \mathbf{K}^* - \mathbf{F}^*, \bmod z \mapsto \overline{z}} |\eta(z) + \eta^*(z)|^2$ sous la forme

$$q(q-1) + \sum_{z \in \mathbf{K}^* - \mathbf{F}^*} (\eta/\eta^*)(z) = q(q-1) + \sum_{z \in \mathbf{K}^*} (\eta/\eta^*)(z) - (q-1),$$

et comme ci-dessus $\sum_{z \in \mathbf{K}^*} (\eta/\eta^*)(z) = 0$ puisque $\eta \neq \eta^*$. La somme à évaluer est donc, finalement, égale à

$$\begin{aligned}(q-1)(q-1)^2 + (q-1)(q^2-1) + q(q-1)(q-1)^2 &= (q-1)^2(q-1+q+1+q(q-1)) \\ &= (q-1)^2(q^2+q) = (q^2-1)(q^2-q),\end{aligned}$$

ce que l'on voulait.

Lemme C.3.6. — *Si χ et χ' sont deux éléments de* X *tels que $\chi = \chi'$, alors les paramètres de χ et χ' sont égaux.*

Démonstration. — Si $\chi = \chi'$, on a en particulier $\chi(1) = \chi'(1)$, ce qui implique que χ et χ' sont de même type.

• Dans les cas des types I et II, il suffit de regarder la valeur en les $b_{x,y}$, pour prouver que les paramètres de χ et χ' sont les mêmes.

• Pour traiter le cas du type III, associons à un couple (δ_1, δ_2) d'éléments $\widehat{\mathbf{F}^*}$, le caractère linéaire $\delta_1 \otimes \delta_2$ de $\mathbf{F}^* \times \mathbf{F}^*$ défini par $(\delta_1 \otimes \delta_2)(x,y) = \delta_1(x)\delta_2(y)$. Si (η_1, η_2) et (η_1', η_2') sont deux éléments de $\mathrm{E_{III}}$ tels que $\beta_{\eta_1,\eta_2} = \beta_{\eta_1',\eta_2'}$, on voit, en regardant ce que cela signifie sur les $b_{x,y}$ et les b_x, que les caractères linéaires $\eta_1 \otimes \eta_2$, $\eta_2 \otimes \eta_1$, $\eta_1' \otimes \eta_2'$ et $\eta_2' \otimes \eta_1'$ sont liés par la relation

$$\eta_1 \otimes \eta_2 + \eta_2 \otimes \eta_1 = \eta_1' \otimes \eta_2' + \eta_2' \otimes \eta_1'.$$

En utilisant l'orthogonalité des caractères, cela prouve que $\eta_1 \otimes \eta_2$ est égal à un des deux caractères $\eta_1' \otimes \eta_2'$ ou $\eta_2' \otimes \eta_1'$, et donc que les éléments (η_1, η_2) et (η_1', η_2') de $\mathrm{E_{III}}$ sont égaux.

• Le cas du type IV se traite de la même manière. Si η_1 et η_2 sont deux éléments de $\mathrm{E_{IV}}$ tels que $\gamma_{\eta_1} = \gamma_{\eta_2}$, alors en regardant ce que cela signifie sur les c_z et les b_x, on voit que l'on a $\eta_1 + \eta_1^* = \eta_2 + \eta_2^*$ sur $\mathbf{K}^*$. On en déduit, en utilisant l'orthogonalité des caractères, que η_1 est égal à η_2 ou à η_2^*, et donc que η_1 et η_2 sont égaux dans $\mathrm{E_{IV}}$.

Ceci permet de conclure.

APPENDICE D

FONCTIONS D'UNE VARIABLE p-ADIQUE

Dans cet appendice, on décrit ce que deviennent un certain nombre de notions classiques dans le monde p-adique (fonctions de classe $\mathscr{C}^k$, fonctions analytiques, intégration...). On termine par une application arithmétique (indépendante du reste) aux congruences découvertes par Kummer entre les valeurs de la fonction ζ aux entiers négatifs (cf. ex. VII.3.6).

D.1. Analyses fonctionnelles réelle et p-adique

Ce § est consacré à une comparaison entre l'analyse fonctionnelle classique sur $\mathbf{R}/\mathbf{Z}$ (i.e. l'étude des propriétés du développement de Fourier des fonctions périodiques) et l'analyse fonctionnelle p-adique sur $\mathbf{Z}_p$ (développement de Mahler). Les résultats sont remarquablement semblables, mais les énoncés p-adiques sont souvent, grâce à l'ultramétricité de la norme p-adique, un peu plus agréables.

Dans ce qui suit, on note $c_k(\phi)$, pour $k \in \mathbf{Z}$, les coefficients de Fourier d'une fonction sur $\mathbf{R}/\mathbf{Z}$ (à valeurs dans $\mathbf{C}$) et $a_n(\phi)$, pour $n \in \mathbf{N}$, les coefficients de Mahler d'une fonction sur $\mathbf{Z}_p$ (à valeurs dans $\mathbf{Q}_p$).

Commençons par les fonctions continues. En p-adique, on dispose du th. de Mahler (th. 20.4) dont nous rappelons l'énoncé.

Théorème D.1.1. — (Mahler, 1958) *Si $\phi \in \mathscr{C}(\mathbf{Z}_p)$, alors*
(i) $\lim_{n\to+\infty} a_n(\phi) = 0$,
(ii) *ϕ est la somme de la série $\sum_{n\in\mathbf{N}} a_n(\phi)\binom{x}{n}$ dans $\mathscr{C}(\mathbf{Z}_p)$; en particulier, pour tout $x \in \mathbf{Z}_p$, on a $\sum_{n\in\mathbf{N}} a_n(\phi)\binom{x}{n} = \phi(x)$.*
(iii) *Réciproquement, si $(a_n)_{n\in\mathbf{N}}$ tend vers 0 en $+\infty$, alors $\sum_{n\in\mathbf{N}} a_n\binom{x}{n}$ converge dans $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ vers une fonction continue dont les coefficients de Mahler sont les a_n.*

En réel, la situation est nettement moins claire. (Pour avoir un énoncé propre, il faut considérer l'espace de Hilbert $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$ au lieu de $\mathscr{C}(\mathbf{R}/\mathbf{Z})$, cf. cor. II.2.7.)

Théorème D.1.2. — (i) *Si $\phi \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, alors $c_k(\phi) \to 0$ quand $|k| \to +\infty$.*

(ii) *Si* $\sum_{k\in\mathbf{Z}}|a_k(\phi)|<+\infty$, *alors* $\sum_{k\in\mathbf{Z}}c_k(\phi)e^{2i\pi kx}\to\phi$ *dans* $\mathscr{C}(\mathbf{R}/\mathbf{Z})$. *En particulier, pour tout* $x\in\mathbf{R}/\mathbf{Z}$, *on a* $\sum_{k\in\mathbf{Z}}c_k(\phi)e^{2i\pi kx}=\phi(x)$.

(iii) *Si* $\phi\in\mathscr{C}(\mathbf{R}/\mathbf{Z})$, *la suite des somme partielles* $\sum_{k=-n}^{n}c_k(\phi)e^{2i\pi kx}$ *converge vers* $\phi(x)$ *p.p., mais il existe* $\phi\in\mathscr{C}(\mathbf{R}/\mathbf{Z})$ *tel que cette suite ne soit pas bornée* (et donc ne tende pas vers $\phi(x)$) *pour* x *dans un sous-ensemble non dénombrable dense de* $\mathbf{R}/\mathbf{Z}$.

(iv) *Il existe des suites* $(c_k)_{k\in\mathbf{Z}}$, *avec* $c_k\to 0$ *quand* $|k|\to+\infty$, *qui ne sont pas la suite des coefficients de Fourier d'une fonction continue.*

Démonstration. — Le (i) est une conséquence du fait que $\sum_{k\in\mathbf{Z}}|c_k(\phi)|^2=\int_0^1|\phi(t)|^2\,dt$ (cf. cor. II.2.7), le (ii) fait l'objet de la prop. IV.3.6, la convergence p.p. de la série de Fourier d'une fonction continue est un résultat difficile de Carleson (1965), le reste du (iii) et le (iv) peuvent se démontrer en utilisant le lemme de Baire (cf. ex. II.3.17 et prob. H.5).

Les énoncés deviennent parfaitement identiques quand on augmente la régularité des fonctions considérées. Rappelons qu'une suite de terme général u_k (à valeurs dans un corps muni d'une norme $\|\ \|$) est :

- *à décroissance rapide*, si $k^{\mathrm{N}}\|u_k\|\to 0$ quand $|k|\to+\infty$, pour tout $\mathrm{N}\in\mathbf{N}$.
- *à décroissance exponentielle* s'il existe $r>1$ tel que $r^{|k|}\|u_k\|\to 0$ quand $|k|\to+\infty$.

Théorème D.1.3. — (i) $\phi\in\mathscr{C}(\mathbf{R}/\mathbf{Z})$ *est de classe* $\mathscr{C}^\infty$ *si et seulement si la suite de ses coefficients de Fourier est à décroissance rapide.*

(ii) $\phi\in\mathscr{C}(\mathbf{R}/\mathbf{Z})$ *est analytique si et seulement si la suite de ses coefficients de Fourier est à décroissance exponentielle.*

Démonstration. — Le (i) se démontre en utilisant la relation entre les coefficients de Fourier d'une fonction et ceux de ses dérivées (cf. rem. IV.3.7). Le (ii) fait l'objet du prob. H.9.

En p-adique on a le résultat suivant dont la démonstration du (i) (resp. du (ii)) fait l'objet du § D.2 (resp. du § D.3).

Théorème D.1.4. — (i) $\phi\in\mathscr{C}(\mathbf{Z}_p)$ *est uniformément de classe* $\mathscr{C}^\infty$ *si et seulement si la suite de ses coefficients de Mahler est à décroissance rapide.*

(ii) $\phi\in\mathscr{C}(\mathbf{Z}_p)$ *est localement analytique si et seulement si la suite de ses coefficients de Mahler est à décroissance exponentielle.*

D.2. Fonctions k-fois uniformément dérivables

1. Fonctions de classe $\mathscr{C}^k$ et fonctions de classe $\mathscr{C}^k_u$

Une fonction $\phi:\mathbf{Z}_p\to\mathbf{Q}_p$ est *dérivable en* $x_0\in\mathbf{Z}_p$, si la quantité $\frac{\phi(x_0+h)-\phi(x_0)}{h}$ admet une limite quand h tend vers 0. La limite est alors notée $\phi'(x_0)$. Une fonction est *dérivable à l'ordre* 1 si elle est dérivable en tout $x_0\in\mathbf{Z}_p$; une fonction dérivable à l'ordre 1 est en particulier continue. Plus généralement, on définit par récurrence sur k la notion de

fonction dérivable à l'ordre k : ϕ est *dérivable à l'ordre k* si elle est dérivable à l'ordre $k-1$, et si sa dérivée $(k-1)$-ième $\phi^{(k-1)}$ est dérivable à l'ordre 1.

On dit que ϕ est *de classe $\mathscr{C}^k$* si elle est dérivable à l'ordre k et si sa dérivée k-ième est continue. La notion de fonction de classe $\mathscr{C}^k$ ne se comporte pas très bien en p-adique, et on préfère la remplacer par celle fonction *uniformément de classe $\mathscr{C}^k$* (de classe $\mathscr{C}^k_u$ pour faire court) : une fonction ϕ sur $\mathbf{Z}_p$ est *de classe $\mathscr{C}^k_u$* si les fonctions $\phi^{[i]}(x, h_1, \dots, h_i)$, définies sur $\mathbf{Z}_p \times (\mathbf{Z}_p - \{0\})^i$ (pour $0 \leqslant i \leqslant k$), par récurrence, grâce à la formule $\phi^{[0]}(x) = \phi(x)$ et

$$\phi^{[i]}(x, h_1, \dots, h_i) = \frac{1}{h_i}(\phi^{[i-1]}(x + h_i, h_1, \dots, h_{i-1}) - \phi^{[i-1]}(x, h_1, \dots, h_{i-1})),$$

se prolongent en des fonctions continues sur $\mathbf{Z}_p^{i+1}$. Une fonction de classe $\mathscr{C}^k_u$ est de classe $\mathscr{C}^k$, de dérivée i-ème donnée par $\phi^{(i)}(x) = \phi^{[i]}(x, 0, \dots, 0)$.

Remarque D.2.1. — (i) Sur $\mathbf{R}$, les notions de classe $\mathscr{C}^k_u$ et de classe $\mathscr{C}^k$ coïncident car

$$\phi^{[i]}(x, h_1, \dots, h_i) = \int_{[0,1]^i} \phi^{(i)}(x + t_1 h_1 + \cdots + t_i h_i)\, dt_1 \dots dt_i.$$

(ii) Sur $\mathbf{Z}_p$, l'exemple suivant montre qu'il n'en est rien. L'écriture en base p permet d'écrire tout élément x de $\mathbf{Z}_p$, de manière unique, sous la forme $\sum_{n=0}^{+\infty} p^n a_n(x)$, avec $a_n(x) \in \{0, \dots, p-1\}$, ce qui permet de définir une fonction $\phi : \mathbf{Z}_p \to \mathbf{Z}_p$ grâce à la formule $\phi(x) = \sum_{n=0}^{+\infty} p^{2n} a_n(x)$. On a alors $|\phi(x) - \phi(y)|_p = |x - y|_p^2$ pour tous $x, y \in \mathbf{Z}_p$ (en effet, $|x - y|_p = p^{-k}$, où k est le plus petit entier vérifiant $a_k(x) \neq a_k(y)$), ce qui montre que ϕ est dérivable, de dérivée nulle, en tout point (elle est donc aussi de classe $\mathscr{C}^\infty$), bien que ϕ ne soit constante dans le voisinage d'aucun point. Par ailleurs, si $(x, h_1, h_2) = (0, p^n, p^n)$, alors $\phi^{[2]}(x, h_1, h_2) = 0$, et si $(x, h_1, h_2) = ((p-1)p^n, p^n, p^n)$, alors $\phi^{[2]}(x, h_1, h_2) = p - p^2$, ce qui montre que $\phi^{[2]}$ ne peut pas se prolonger par continuité en $(0, 0, 0)$.

On munit $\mathscr{C}^k_u(\mathbf{Z}_p)$ de la norme naturelle $\| \ \|_{\mathscr{C}^k_u}$ définie par

$$\|\phi\|_{\mathscr{C}^k_u} = \sup_{0 \leqslant i \leqslant k} \ \sup_{(x, h_1, \dots, h_i) \in \mathbf{Z}_p^{i+1}} |\phi^{[i]}(x, h_1, \dots, h_i)|_p.$$

Alors $\mathscr{C}^k_u(\mathbf{Z}_p)$ est complet puisqu'une limite uniforme de fonctions continues est continue, et donc est un espace de Banach p-adique.

Théorème D.2.2. — (Barsky, 1973)

(i) *$\phi \in \mathscr{C}^k_u$ si et seulement si la suite de terme général $n^k |a_n(\phi)|_p$ tend vers 0 et la norme $\sup_n (n+1)^k |a_n(\phi)|_p$ est équivalente à $\|\phi\|_{\mathscr{C}^k_u}$.*

(ii) *ϕ est de classe $\mathscr{C}^\infty_u$ si et seulement si la suite de ses coefficients de Mahler est à décroissance rapide.*

Démonstration. — Une fonction étant de classe $\mathscr{C}^\infty_u$ si et seulement si elle est de classe $\mathscr{C}^k_u$, pour tout $k \in \mathbf{N}$, le (ii) est une conséquence du (i). Le (i), quant-à-lui est une conséquence

des lemmes D.2.7 et D.2.6 ci-dessous (le lemme D.2.6 permet de montrer que la suite $n \mapsto (n+1)^k p^{-\mathrm{L}(n,k)}$ est bornée et le lemme D.2.7 que $\|\phi\|_{\mathscr{C}^k_u} = \sup_{n\in\mathbf{N}} p^{\mathrm{L}(n,k)}|a_n(\phi)|_p$).

2. Fonctions continues sur $\mathbf{Z}_p^m$

Pour pouvoir étudier les coefficients de Mahler des fonctions de classe $\mathscr{C}^k_u$, on a besoin d'une description des fonctions continues sur $\mathbf{Z}_p^m$ (c'est assez naturel, au vu de la définition d'une fonction de classe $\mathscr{C}^k_u$). Le résultat suivant montre comment obtenir une base orthonormale des fonctions continues sur $\mathbf{Z}_p^m$ à partir d'une base orthonormale des fonctions continues sur $\mathbf{Z}_p$. La situation est tout-à-fait analogue [1] à la description d'une base orthonormale de $\mathrm{L}^2((\mathbf{R}/\mathbf{Z})^m)$ en fonction d'une base orthonormale de $\mathrm{L}^2(\mathbf{R}/\mathbf{Z})$. Le lecteur est invité à comparer l'enoncé ci-dessous et sa démonstration avec ceux du th. IV.3.10.

Proposition D.2.3. — *Si $m \geqslant 1$, les $\phi_{k_1,\dots,k_m} = \binom{x_1}{k_1}\cdots\binom{x_m}{k_m}$, pour $(k_1,\dots,k_m) \in \mathbf{N}^m$, forment une base orthonormale de $\mathscr{C}(\mathbf{Z}_p^m)$.*

Démonstration. — Il suffit de prouver que leurs réductions modulo p forment une base de $\mathscr{C}(\mathbf{Z}_p^m, \mathbf{F}_p)$, sur $\mathbf{F}_p$. Pour montrer qu'ils forment une famille libre, on peut utiliser le fait que les $\phi_k = \binom{x}{k}$, pour $k \in \mathbf{N}$, forment une famille libre modulo p, puisque les $\binom{x}{k}$, pour $k \in \mathbf{N}$, forment une base orthonormale de $\mathscr{C}(\mathbf{Z}_p)$. La liberté se déduit alors, par une récurrence immédiate, du lemme suivant (appliqué à $\mathrm{K} = \mathbf{F}_p$, $\mathrm{X} = \mathbf{Z}_p$ et $\mathrm{Y} = \mathbf{Z}_p^{m-1}$).

Lemme D.2.4. — *Si K est un corps, si X et Y sont des ensembles, et si $(f_i)_{i\in\mathrm{I}}$ et $(g_j)_{j\in\mathrm{J}}$ sont des familles libres déléments de K^{X} et K^{Y} respectivement, alors $(f_i \otimes g_j)_{(i,j)\in\mathrm{I}\times\mathrm{J}}$, où $f_i \otimes g_j(x,y) = f_i(x)g_j(y)$, est une famille libre dans $\mathrm{K}^{\mathrm{X}\times\mathrm{Y}}$.*

Démonstration. — Si $\sum \lambda_{i,j}\, f_i \otimes g_j$ est une combinaison linéaire (seul un nombre fini de $\lambda_{i,j}$ sont non nuls) identiquement nulle sur $\mathrm{X}\times\mathrm{Y}$, alors pour tout $y \in \mathrm{Y}$, on a $\sum_{j\in\mathrm{J}} \big(\sum_{i\in\mathrm{I}} \lambda_{i,j} f_i(x)\big) g_j(y) = 0$. Les g_j formant une famille libre ceci implique que, pour tout $j \in \mathrm{J}$, on a $\sum_{i\in\mathrm{I}} \lambda_{i,j} f_i(x) = 0$, quel que soit $x \in \mathrm{X}$. Comme les f_i forment une famille libre, cela implique que les $\lambda_{i,j}$ sont tous nuls, ce qui permet de conclure.

Revenons à la démonstration de la proposition. Il reste à vérifier que les $\phi_{k_1,\dots,k_m}$ forment une famille génératrice. Soit donc $\phi : \mathbf{Z}_p^m \to \mathbf{F}_p$ continue. La topologie sur $\mathbf{F}_p$ est la topologie discrète que l'on peut définir par la distance triviale ($d(x,y) = 1$, si $x \neq y$), et comme $\mathbf{Z}_p^m$ est compact, en tant que produit de compacts, ϕ est uniformément continue. Ceci se traduit, en particulier, par l'existence de $\mathrm{N} \in \mathbf{N}$ tel que $\sup_{1\leqslant i\leqslant m} |x_i - y_i|_p \leqslant p^{-\mathrm{N}}$ implique $d(\phi(x),\phi(y)) < 1$ (i.e. $\phi(x) = \phi(y)$) ; autrement dit, ϕ est constante sur $x + p^{\mathrm{N}}\mathbf{Z}_p^m$, pour tout $x \in \mathbf{Z}_p$; on peut donc l'écrire sous la forme

$$\phi = \sum_{0\leqslant r_1,\dots,r_m\leqslant p^{\mathrm{N}}-1} \lambda_{r_1,\dots,r_m} \mathbf{1}_{(r_1+p^{\mathrm{N}}\mathbf{Z}_p)\times\cdots\times(r_m+p^{\mathrm{N}}\mathbf{Z}_p)}.$$

1. Dans les deux cas, l'espace de fonctions en plusieurs variables est un produit tensoriel complété de copies de l'espace de fonctions en une variable.

Or $\mathbf{1}_{(r_1+p^{\mathrm{N}}\mathbf{Z}_p)\times\cdots\times(r_m+p^{\mathrm{N}}\mathbf{Z}_p)}(x) = \prod_{i=1}^m \mathbf{1}_{r_i+p^{\mathrm{N}}\mathbf{Z}_p}(x_i)$ et $\mathbf{1}_{r_i+p^{\mathrm{N}}\mathbf{Z}_p}$ peut s'exprimer comme une combinaison linéaire des ϕ_k, d'après le th. de Mahler. Il n'y a plus qu'à développer l'expression obtenue pour aboutir à une écriture de ϕ comme combinaison linéaire des $\phi_{k_1,\ldots,k_m}$.

Ceci permet de conclure.

Remarque D.2.5. — (i) Il résulte de la proposition que tout $\phi \in \mathscr{C}(\mathbf{Z}_p^m)$ peut s'écrire, de manière unique, sous la forme $\phi = \sum_{\mathbf{k}=(k_1,\ldots,k_m)\in\mathbf{N}^m} a_{\mathbf{k}}(\phi)\binom{x_1}{k_1}\cdots\binom{x_m}{k_m}$, où $a_{\mathbf{k}}(\phi) \to 0$ à l'infini, et que, de plus, $\|\phi\|_\infty = \sup_{\mathbf{k}\in\mathbf{N}^m} |a_{\mathbf{k}}(\phi)|_p$. Réciproquement, si $a_{\mathbf{k}} \to 0$ à l'infini, alors $\sum_{\mathbf{k}=(k_1,\ldots,k_m)\in\mathbf{N}^m} a_{\mathbf{k}}\binom{x_1}{k_1}\cdots\binom{x_m}{k_m}$ est une fonction continue sur $\mathbf{Z}_p^m$ dont les coefficients de Mahler sont les $a_{\mathbf{k}}$, pour $\mathbf{k} \in \mathbf{N}^m$.

(ii) Si $\mathbf{n} = (n_1, \ldots, n_m) \in \mathbf{N}^m$, alors $\binom{n_1}{k_1}\cdots\binom{n_m}{k_m} \in \mathbf{N}$ et est nul sauf pour un nombre fini de $\mathbf{k}$. Il en résulte que les valeurs de ϕ sur $\mathbf{N}^m$ sont des combinaisons linéaires à coefficients entiers des $a_{\mathbf{k}}(\phi)$, pour $\mathbf{k} \in \mathbf{N}$. Réciproquement, on peut, comme en dimension 1, définir les coefficients de Mahler $a_{\mathbf{k}}(\phi)$, à partir des valeurs de ϕ aux entiers. On définit l'opérateur de « dérivée partielle discrète » $\partial_i^{[1]}$ par

$$\partial_i^{[1]}\phi(x_1, \ldots, x_m) = \phi(x_1, \ldots, x_i + 1, \ldots, x_m) - \phi(x_1, \ldots, x_i, \ldots, x_m),$$

et on note $\partial_i^{[k]}$ le composé de k copies de $\partial_i^{[1]}$. Alors $a_{\mathbf{k}}(\phi) = \partial_1^{[k_1]}\cdots\partial_m^{[k_m]}\phi(0, \ldots, 0)$, ce qui montre que $a_{\mathbf{k}}(\phi)$ est une combinaison linéaire, à coefficients entiers, des $\phi(\mathbf{n})$, pour $\mathbf{n} \in \mathbf{N}^m$.

3. Coefficients de Mahler des fonctions de classe $\mathscr{C}_u^k$

Soit $\mathrm{L}(n,k) = \max\{v_p(n_1) + \cdots + v_p(n_i) \mid i \leqslant k,\ n_1 + \cdots + n_i \leqslant n,\ n_j \geqslant 1\}$.

Lemme D.2.6. — *Il existe* $\mathrm{C}_k > 0$ *tel que* $k\frac{\log n}{\log p} - \mathrm{C}_k \leqslant \mathrm{L}(n,k) \leqslant k\frac{\log n}{\log p}$.

Démonstration. — Si $n_i \leqslant n$, alors $v_p(n_i) \leqslant \frac{\log n}{\log p}$, et donc $\mathrm{L}(n,k) \leqslant k\frac{\log n}{\log p}$. D'autre part, si $k \leqslant p^r$ et $u = [\frac{\log n}{\log p}]$, on peut prendre $(n_1, \ldots, n_k) = (p^{u-r}, \ldots, p^{u-r})$ ce qui implique $\mathrm{L}(n,k) \geqslant k(\frac{\log n}{\log p} - 1 - r)$ et permet de conclure.

Lemme D.2.7. — *Les* $p^{\mathrm{L}(n,k)}\binom{x}{n}$ *forment une base de Banach de* $\mathscr{C}_u^k(\mathbf{Z}_p)$.

Démonstration. — Soit $g_{\mathrm{T}}(x) = (1+\mathrm{T})^x$. On a $g_{\mathrm{T}}(x) = \sum_{n\in\mathbf{N}} \mathrm{P}_n(x)\mathrm{T}^n$, où $\mathrm{P}_n(x) = \binom{x}{n}\mathrm{T}^n$. Donc

$$\sum_{n\in\mathbf{N}} \mathrm{P}_n^{[i]}(x, h_1, \ldots, h_k) = g_{\mathrm{T}}^{[i]}(x, h_1, \ldots, h_k) = (1+\mathrm{T})^x \prod_{j=1}^{i} \frac{(1+\mathrm{T})^{h_j} - 1}{h_j}.$$

En identifiant les termes de degré n en T, et en utilisant l'identité $\frac{1}{h}\binom{h}{n} = \frac{1}{n}\binom{h-1}{n-1}$, on obtient la formule

$$\mathrm{P}_n^{[i]}(x, h_1, \ldots, h_i) = \sum_{\substack{n_0+n_1+\cdots+n_i=n \\ n_1,\ldots,n_i\geqslant 1}} \frac{1}{n_1\cdots n_i}\binom{x}{n_0}\binom{h_1-1}{n_1-1}\cdots\binom{h_i-1}{n_i-1}.$$

Soit $\phi \in \mathscr{C}_u^k(\mathbf{Z}_p)$ et soit $g_i(x, h_1, \dots, h_i) = \phi^{[i]}(x, h_1 + 1, \dots, h_i + 1)$. Comme $\phi(x) = \sum_{n\in\mathbf{N}} a_n(\phi)\mathrm{P}_n(x)$, pour tout $x \in \mathbf{Z}_p$, on déduit de la formule ci-dessus que

$$g_i(x, h_1, \dots, h_i) = \sum_{n\in\mathbf{N}} \Big(\sum_{\substack{n_0+n_1+\cdots+n_i=n \\ n_1,\dots,n_i\geqslant 1}} \frac{a_n(\phi)}{n_1\cdots n_i} \binom{x}{n_0}\binom{h_1}{n_1-1}\cdots\binom{h_i}{n_i-1}\Big),$$

et que les coefficients de Mahler de g_i sont donnés par

$$a_{n_0,n_1-1\dots,n_i-1}(g_i) = \frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}.$$

Si $i \leqslant k$, comme g_i se prolonge en une fonction continue sur $\mathbf{Z}_p^{i+1}$ puisque $\phi \in \mathscr{C}_u^k(\mathbf{Z}_p)$, le théorème de Mahler à $i+1$ variables (prop. D.2.3) montre que la suite de terme général $\frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}$ tend vers 0 quand $(n_0, \dots, n_i)$ tend vers l'infini.

Réciproquement, si cette suite tend vers 0, alors la série

$$\sum_{n_0=0}^{+\infty}\sum_{n_1=1}^{+\infty}\cdots\sum_{n_i=1}^{+\infty} \frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}\binom{x}{n_0}\binom{h_1}{n_1-1}\cdots\binom{h_i}{n_i-1}$$

définit une fonction continue sur $\mathbf{Z}_p^{i+1}$ qui coïncide avec g_i sur $\mathbf{N}^{i+1}$, au vu du lien entre les coefficients de Mahler d'une fonction et ses valeurs aux entiers (rem. D.2.5). Comme $\mathbf{N}^{i+1}$ est dense dans $\mathbf{Z}_p \times (\mathbf{Z}_p - \{-1\})^i$, cela prouve que :

- la fonction ci-dessus est égale à g_i sur $\mathbf{Z}_p \times (\mathbf{Z}_p - \{-1\})^i$,
- g_i, et donc aussi $\phi^{[i]}$, se prolonge par continuité à $\mathbf{Z}_p^{i+1}$,
- $\|\phi^{[i]}\|_\infty = \|g_i\|_\infty = \sup_{n_0,\dots,n_i} \frac{1}{|n_1\cdots n_i|_p}|a_{n_0+\cdots+n_i}(\phi)|_p$.

En résumé, $\phi \in \mathscr{C}_u^k(\mathbf{Z}_p)$ si et seulement si $\frac{a_n(\phi)}{n_1\cdots n_i}$ tend vers 0 quand $n = n_0+n_1+\cdots+n_i$ tend vers $+\infty$ et

$$\|\phi\|_{\mathscr{C}_u^k} = \sup_{i\leqslant k}\sup_{n\in\mathbf{N}}\Big(\sup_{\substack{n_0+n_1+\cdots+n_i=n \\ n_1,\dots,n_i\geqslant 1}} \frac{|a_n(\phi)|_p}{|n_1\cdots n_i|_p}\Big) = \sup_{n\in\mathbf{N}} p^{\mathrm{L}(n,k)}|a_n(\phi)|_p.$$

On en déduit le résultat.

D.3. Fonctions localement analytiques sur $\mathbf{Z}_p$

1. Fonctions analytiques

Le lecteur est invité à comparer l'énoncé suivant, et sa démonstration, avec la prop. V.1.10.

Proposition D.3.1. — *Soit* $\mathrm{F} = \sum_{n=0}^{+\infty} a_n \mathrm{T}^n \in \mathbf{Q}_p[[\mathrm{T}]]$, *avec* $a_n \to 0$ *quand* $n \to +\infty$.

(i) F *et toutes ses dérivées convergent sur* $\mathbf{Z}_p$.

(ii) *Si* $z, z_0 \in \mathbf{Z}_p$, *alors* $\mathrm{F}(z) = \sum_{k=0}^{+\infty} \frac{\mathrm{F}^{(k)}(z_0)}{k!}(z - z_0)^k$, *où* $\mathrm{F}^{(k)}(z_0)$ *désigne la somme de la série* $\mathrm{F}^{(k)}$ *en* z_0.

(iii) *La fonction* $z \mapsto \mathrm{F}(z)$ *est de classe* $\mathscr{C}^\infty$ *sur* $\mathbf{Z}_p$ *et sa dérivée* k*-ième en* z_0 *est la valeur de la série* $\mathrm{F}^{(k)}$ *en* z_0.

(iv) *Si* $z_0 \in \mathbf{Z}_p$, *alors* $\frac{\mathrm{F}^{(k)}(z_0)}{k!} \to 0$ *et* $\sup_{k\in\mathbf{N}} \left|\frac{\mathrm{F}^{(k)}(z_0)}{k!}\right|_p = \sup_{n\in\mathbf{N}} |a_n|_p$.

Démonstration. — On a $\frac{\mathrm{F}^{(k)}(\mathrm{T})}{k!} = \sum_{n=0}^{+\infty} \binom{n+k}{k} a_{n+k}\mathrm{T}^k$. Or $\left|\binom{n+k}{k}\right|_p \leqslant 1$, puisque $\binom{n+k}{k} \in \mathbf{N}$, et donc $\binom{n+k}{k} a_{n+k} z^k \to 0$, si $z \in \mathbf{Z}_p$ (i.e. si $|z|_p \leqslant 1$). On en déduit, grâce à l'ultramétricité de $|\ |_p$, la convergence de la série de $\frac{\mathrm{F}^{(k)}}{k!}$ sur $\mathbf{Z}_p$, ce qui démontre le (i).

Maintenant, si $z, z_0 \in \mathbf{Z}_p$, on a

$$\mathrm{F}(z) = \sum_{n=0}^{+\infty} a_n \big(z_0 + (z - z_0)\big)^n = \sum_{n=0}^{+\infty} a_n \Big(\sum_{k=0}^{n} \binom{n}{k} z_0^{n-k} (z - z_0)^k \Big).$$

Or la suite double $a_n \binom{n}{k} z_0^k (z - z_0)^{n-k}$ tend vers 0 à l'infini, ce qui permet, grâce à l'ultramétricité de $|\ |_p$, de réordonner la série comme on veut ; on en déduit le (ii) en posant $n = m + k$, ce qui nous donne

$$\mathrm{F}(z) = \sum_{k=0}^{+\infty} \Big(\sum_{m=0}^{+\infty} \binom{m+k}{k} a_{m+k} z_0^m \Big) (z - z_0)^k = \sum_{k=0}^{+\infty} \frac{\mathrm{F}^{(k)}(z_0)}{k!} (z - z_0)^k.$$

Le (ii) permet, en faisant le changement de variable $z = z_0 + h$, de supposer que $z_0 = 0$ pour démontrer le (iii). On a

$$\Big|\frac{\mathrm{F}(h) - \mathrm{F}(0)}{h} - \mathrm{F}'(0)\Big|_p = \Big|h \sum_{n=2}^{+\infty} a_n h^{n-2}\Big|_p \leqslant |h|_p \sup_{n\in\mathbf{N}} |a_n|_p, \quad \text{si } h \in \mathbf{Z}_p,$$

et donc $\frac{\mathrm{F}(h)-\mathrm{F}(0)}{h} - \mathrm{F}'(0)$ tend vers 0 quand $h \to 0$, ce qui montre que $z \mapsto \mathrm{F}(z)$ est dérivable en 0 et que sa dérivée en 0 est $\mathrm{F}'(0)$. On en déduit que $z \mapsto \mathrm{F}(z)$ est dérivable sur $\mathbf{Z}_p$ et que sa dérivée en z_0 est la somme de la série F' en z_0. Une récurrence immédiate permet d'en déduire le (iii).

Enfin, $\left|\frac{\mathrm{F}^{(k)}(z_0)}{k!}\right|_p \leqslant \sup_{n\in\mathbf{N}} \left|\binom{n+k}{k} a_{n+k} z_0^k\right|_p \leqslant \sup_{n\geqslant k} |a_n|_p$, si $z_0 \in \mathbf{Z}_p$, et donc $\frac{\mathrm{F}^{(k)}(z_0)}{k!} \to 0$ puisque $a_n \to 0$, et $\sup_{k\in\mathbf{N}} \left|\frac{\mathrm{F}^{(k)}(z_0)}{k!}\right|_p \leqslant \sup_{n\in\mathbf{N}} |a_n|_p$. Pour démontrer l'inégalité inverse, il suffit d'appliquer ce qui précède à $\mathrm{G}(z) = \sum_{k=0}^{+\infty} \frac{\mathrm{F}^{(k)}(z_0)}{k!} z^k$: on a $a_n = \frac{\mathrm{F}^{(k)}(0)}{k!} = \frac{\mathrm{G}^{(k)}(-z_0)}{k!}$.

On dit que $\phi : \mathbf{Z}_p \to \mathbf{Q}_p$ est *analytique* s'il existe $\mathrm{F} = \sum_{n\in\mathbf{N}} b_n \mathrm{T}^n \in \mathbf{Q}_p[[\mathrm{T}]]$, avec $b_n \to 0$, telle que $\phi(x) = \mathrm{F}(x)$ pour tout $x \in \mathbf{Z}_p$. Il résulte de la prop. D.3.1 que ϕ est alors $\mathscr{C}^\infty$ sur $\mathbf{Z}_p$ et que $b_n = \frac{\phi^{(n)}(0)}{n!}$; en particulier, b_n est déterminé par ϕ, ce qui permet de le noter $b_n(\phi)$.

On munit l'espace $\mathrm{An}(\mathbf{Z}_p)$ des fonctions analytiques sur $\mathbf{Z}_p$ de la norme $\|\ \|_{\mathrm{An}}$ définie par $\|\phi\|_{\mathrm{An}} = \sup_{n\in\mathbf{N}} |b_n(\phi)|_p$. D'après la prop. D.3.1, on a aussi $\|\phi\|_{\mathrm{An}} = \sup_{n\in\mathbf{N}} \left|\frac{\phi^{(n)}(x)}{n!}\right|_p$, pour tout $x \in \mathbf{Z}_p$. De plus, il est clair que $\phi \mapsto (b_n(\phi))_{n\in\mathbf{N}}$ est une isométrie de $\mathrm{An}(\mathbf{Z}_p)$ sur $\ell_0^\infty(\mathbf{N})$; on en déduit que $\mathrm{An}(\mathbf{Z}_p)$ est un espace de Banach p-adique dont les x^n, pour $n \in \mathbf{N}$, forment une base orthonormale.

2. Fonctions localement analytiques

On dit que $\phi : \mathbf{Z}_p \to \mathbf{Q}_p$ est *localement analytique*[2], si pour tout $a \in \mathbf{Z}_p$, il existe $h(a) \in \mathbf{N}$ tel que $x \mapsto \phi(a + p^{h(a)}x)$ soit analytique sur $\mathbf{Z}_p$. D'après la prop. D.3.1, si $x \mapsto \phi(a+p^{h(a)}x)$ est analytique sur $\mathbf{Z}_p$, il en est de même de $x \mapsto \phi(b+p^{h(a)}x)$, pour tout $b \in a+p^{h(a)}\mathbf{Z}_p$. Maintenant, comme $\mathbf{Z}_p$ est compact, on peut extraire un sous-recouvrement fini du recouvrement de $\mathbf{Z}_p$ par les ouverts $a + p^{h(a)}\mathbf{Z}_p$. Si on note h le minimum des $h(a)$ apparaissant dans ce sous-recouvrement fini, alors $x \mapsto \phi(b + p^h x)$ est analytique sur $\mathbf{Z}_p$, pour tout $b \in \mathbf{Z}_p$; autrement dit, $h(a)$ peut être choisi indépendamment de $a \in \mathbf{Z}_p$.

Notons $\mathrm{LA}(\mathbf{Z}_p)$ l'espace des fonctions localement analytiques sur $\mathbf{Z}_p$ et, si $h \in \mathbf{N}$, soit $\mathrm{LA}_h(\mathbf{Z}_p)$ l'espace des fonctions $\phi : \mathbf{Z}_p \to \mathbf{Q}_p$ telles que $x \mapsto \phi(a + p^h x)$ est analytique sur $\mathbf{Z}_p$, pour tout $a \in \mathbf{Z}_p$. Alors $\mathrm{LA}_h(\mathbf{Z}_p) \subset \mathrm{LA}_{h+1}(\mathbf{Z}_p)$, et la discussion ci-dessus montre que $\mathrm{LA}(\mathbf{Z}_p) = \cup_{h\in\mathbf{N}}\mathrm{LA}_h(\mathbf{Z}_p)$.

Soit S un système de représentants de $\mathbf{Z}_p$ modulo p^h. On peut alors écrire toute fonction $\phi : \mathbf{Z}_p \to \mathbf{Q}_p$, de manière unique, sous la forme $\sum_{j\in\mathrm{S}} \mathbf{1}_{j+p^h\mathbf{Z}_p}\phi_j\big(\frac{x-j}{p^h}\big)$, où les ϕ_j sont des fonctions de $\mathbf{Z}_p$ dans $\mathbf{Q}_p$ (de manière explicite, ϕ_j est la restriction à $\mathbf{Z}_p$ de $x \mapsto \phi(j+p^h x)$). Ceci permet de munir $\mathrm{LA}_h(\mathbf{Z}_p)$ d'une norme $\| \ \|_{\mathrm{LA}_h}$ en posant $\|\phi\|_{\mathrm{LA}_h} = \sup_{j\in\mathrm{S}} \|\phi_j\|_{\mathrm{An}}$, et la prop. D.3.1 montre que ceci ne dépend pas du choix de S (dans la suite, on prendra $\mathrm{S} = \{-1, \dots, -p^h\}$). Par construction, l'application $\phi \mapsto (\phi_j)_{j\in\mathrm{S}}$ est une isométrie de $\mathrm{LA}_h(\mathbf{Z}_p)$ sur $\mathrm{An}(\mathbf{Z}_p)^{p^h}$, ce qui prouve que $\mathrm{LA}_h(\mathbf{Z}_p)$, muni de la norme $\| \ \|_{\mathrm{LA}_h}$, est un espace de Banach p-adique.

Théorème D.3.2. — (Amice, 1964)

(i) *Les* $[\frac{n}{p^h}]!\binom{x}{n}$*, pour* $n \in \mathbf{N}$*, forment une base orthonormale de* $\mathrm{LA}_h(\mathbf{Z}_p)$*.*

(ii) $\phi \in \mathrm{LA}(\mathbf{Z}_p)$ *si et seulement si la suite de ses coefficients de Mahler est à décroissance exponentielle.*

Démonstration. — Le (ii) est une conséquence du (i). En effet, si $\phi \in \mathrm{LA}(\mathbf{Z}_p)$, il existe $h \in \mathbf{N}$ tel que $\phi \in \mathrm{LA}_h(\mathbf{Z}_p)$, puisque $\mathrm{LA}(\mathbf{Z}_p) = \cup_{h\in\mathbf{N}}\mathrm{LA}_h(\mathbf{Z}_p)$. D'après le (i), cela implique que $\phi = \sum_{n\in\mathbf{N}} b_n[\frac{n}{p^h}]!\binom{x}{n}$, où $b_n \to 0$. On a alors $a_n(\phi) = b_n[\frac{n}{p^h}]!$; il existe donc $\mathrm{C} > 0$ tel que $|a_n(\phi)|_p \leqslant \mathrm{C}\big|[\frac{n}{p^h}]!\big|_p$.

Or, d'après l'ex. 1.4 du Vocabulaire, on a $v_p(m!) = \frac{m-\mathrm{S}(m)}{p-1}$, où $\mathrm{S}(m)$ est la somme des chiffres de m dans son écriture en base p. Comme m a au plus $\frac{\log m}{\log p}$ chiffres non nuls et comme ces chiffres sont $\leqslant p-1$, on obtient les encadrements

$$\frac{m}{p-1} - \frac{\log m}{\log p} \leqslant v_p(m!) \leqslant \frac{m}{p-1} \quad \text{et} \quad p^{-m/(p-1)} \leqslant |m!|_p \leqslant m\,p^{-m/(p-1)}.$$

2. Bien que la définition soit identique à celle d'une fonction analytique ou holomorphe sur $\mathbf{C}$, on ne les appelle pas comme ça car ces fonctions ne vérifient pas l'unicité du prolongement analytique.

En appliquant ceci à $m = [\frac{n}{p^h}]$, on en déduit la majoration

$$\big|[\frac{n}{p^h}]!\big|_p \leqslant n\,\mathrm{C}_h r_h^n, \text{ où } r_h = p^{-1/(p-1)p^h} \text{ et } \mathrm{C}_h = \frac{p^{1/(p-1)}}{p^h},$$

et la décroissance exponentielle de $a_n(\phi)$.

Réciproquement, si $r^n|a_n(\phi)|_p \to 0$, avec $r > 1$, il existe $h \in \mathbf{N}$ tel que $r_h > r^{-1}$, et alors $([\frac{n}{p^h}]!)^{-1}a_n(\phi) \to 0$, ce qui implique que $\phi \in \mathrm{LA}_h(\mathbf{Z}_p)$.

3. Bases orthonormales d'espaces de fonctions localement analytiques

On a démontré que le (i) du th. D.3.2 impliquait le (ii). Pour démontrer le (i), écrivons $n \in \mathbf{N}$ sous la forme $n = (m(n)+1)p^h - i(n)$, avec $i(n) \in \{1, \dots, p^h\}$ et $m(n) \in \mathbf{N}$ (une telle écriture est unique). On note alors e_n la fonction $x \mapsto \mathbf{1}_{n+p^h\mathbf{Z}_p}(x)(\frac{x+i(n)}{p^h})^{m(n)}$, et g_n le polynôme $[\frac{n}{p^h}]!\binom{x}{n}$. Notre but est de prouver que les g_n, pour $n \in \mathbf{N}$, forment une base orthormale de $\mathrm{LA}_h(\mathbf{Z}_p)$. Pour cela, nous allons prouver que :

- les e_n, pour $n \in \mathbf{N}$, forment une base orthormale de $\mathrm{LA}_h(\mathbf{Z}_p)$ (lemme D.3.3),
- g_n appartient à la boule unité B_h de $\mathrm{LA}_h(\mathbf{Z}_p)$,
- la matrice exprimant les réductions $\overline{g}_n$, pour $n \leqslant (m+1)p^h - 1$, en fonction des $\overline{e}_n$, pour $n \leqslant (m+1)p^h - 1$, est une matrice inversible, pour tout $m \in \mathbf{N}$ (ces deux derniers points sont une conséquence du lemme D.3.4, comme il est expliqué juste avant la démonstration dudit lemme).

D'après la prop. II.4.8, le premier point implique que les $\overline{e}_n$, pour $n \in \mathbf{N}$, forment une base algébrique de $\mathrm{B}_h/p\mathrm{B}_h$ sur $\mathbf{F}_p$. Le dernier implique alors qu'il en est de même des $\overline{g}_n$, pour $n \in \mathbf{N}$, ce qui, d'après la prop. II.4.8, implique que les g_n, pour $n \in \mathbf{N}$, forment une base orthormale de $\mathrm{LA}_h(\mathbf{Z}_p)$, ce que l'on veut démontrer.

Lemme D.3.3. — *Les e_n pour $n \in \mathbf{N}$ forment une base orthonormale de $\mathrm{LA}_h(\mathbf{Z}_p)$. Plus précisément, si $\phi \in \mathrm{LA}_h(\mathbf{Z}_p)$ et si $\phi_i(x) = \phi(-i + p^h x)$, alors*

- *ϕ_i est analytique sur $\mathbf{Z}_p$ et donc $\phi_i(x) = \sum_{m\in\mathbf{N}} \alpha_{i,m}x^m$, où $\alpha_{i,m} \to 0$,*
- *$\phi = \sum_{i=1}^{p^h}\sum_{m\in\mathbf{N}} \alpha_{i,m}e_{(m+1)p^h-i} = \sum_{n\in\mathbf{N}} \alpha_{i(n),m(n)}e_n$,*
- *$\|\phi\|_{\mathrm{LA}_h} = \sup_{n\in\mathbf{N}} |\alpha_{i(n),m(n)}|_p$.*

Démonstration. — Cela résulte de l'identité $\phi(x) = \sum_{i=1}^{p^h} \mathbf{1}_{-i+p^h\mathbf{Z}_p}(x)\phi_i\big(\frac{x+i}{p^h}\big)$ et de ce que $\|\phi\|_{\mathrm{LA}_h} = \sup_{1\leqslant i\leqslant p^h} \|\phi_i\|_{\mathrm{An}}$.

Si $j \in \{1, \dots, p^h\}$, soit $g_{n,j}$ le polynôme défini par $g_{n,j}(x) = g_n(-j + p^h x)$. On a donc

$$g_{n,j}(x) = [\frac{n}{p^h}]!\frac{1}{n!}\prod_{k=0}^{n-1}(-j-k+p^h x).$$

Lemme D.3.4. — (i) *$g_{n,j}$ est à coefficients dans $\mathbf{Z}_p$.*

(ii) *Sa réduction $\overline{g}_{n,j}$ modulo p vérifie :*

- *$\overline{g}_{n,j} = 0$ si $j > i(n)$,*

- $\deg(\overline{g}_{n,j}) = m(n)$ *si* $j = i(n)$,
- $\deg(\overline{g}_{n,j}) \leqslant m(n)$ *si* $j < i(n)$.

Ce lemme permet de terminer la démonstration du th. D.3.2. En effet, le (i) implique que g_n appartient à la boule unité de $\mathrm{LA}_h(\mathbf{Z}_p)$. Le (ii) se traduit par l'existence d'éléments $\alpha_{j,m} \in \mathbf{F}_p$, pour $m \leqslant m(n)$, nuls si $j > i(n)$, tels que $\overline{g}_{n,j} = \sum_{m=0}^{m(n)} \alpha_{j,m} x^m$. D'après le lemme D.3.3, on a alors $\overline{g}_n = \sum_{m(k)\leqslant m(n)} \alpha_{i(k),m(k)} \overline{e}_k$. Maintenant, si $n \leqslant (m+1)p^h - 1$, alors $m(k) \leqslant m(n)$ implique que $k \leqslant (m+1)p^h - 1$. Il en résulte que les $\overline{g}_n$, pour $n \leqslant (m+1)p^h - 1$, s'expriment en termes des $\overline{e}_k$, pour $k \leqslant (m+1)p^h - 1$. On note M_m la matrice ainsi obtenue. Le (ii) du lemme implique alors que si on découpe la matrice M_m en blocs de taille $p^h \times p^h$, on obtient une matrice triangulaire supérieure par blocs et chacun des blocs diagonaux est triangulaire inférieur avec des éléments inversibles sur la diagonale (cette inversibilité résulte de ce que $\deg(\overline{g}_{n,j}) = m(n)$ si $j = i(n)$). La matrice M_m est donc inversible, ce qui montre que le lemme D.3.4 fournit les points manquant pour démontrer le th. D.3.2.

4. Démonstration du lemme D.3.4

Soit $\mathrm{K}_{n,j} = \{k \leqslant n-1,\ v_p(j+k) \geqslant h\}$. L'application $k \mapsto j+k$ induisant une bijection de $\mathrm{K}_{n,j}$ sur l'ensemble des entiers de $[j, j+n-1] = [0, j+n-1] - [0, j-1]$ qui sont divisibles par p^h, on a $|\mathrm{K}_{n,j}| = [\frac{j+n-1}{p^h}] - [\frac{j-1}{p^h}]$, et donc $|\mathrm{K}_{n,j}| = m(n)+1$ si $j > i(n)$ et $|\mathrm{K}_{n,j}| = m(n)$ si $j \leqslant i(n)$.

On a $g_{n,j} = c_{n,j} f_{n,j}$, où $c_{n,j} \in \mathbf{Q}^*$ et $f_{n,j} = \prod_{k\in \mathrm{K}_{n,j}} \left(x - \frac{j+k}{p^h}\right) \prod_{k\notin \mathrm{K}_{n,j}} \left(1 - \frac{p^h x}{j+k}\right)$ est un polynôme à coefficients dans $\mathbf{Z}_p$ dont la réduction $\overline{f}_{n,j}$ modulo p est $\prod_{k\in \mathrm{K}_{n,j}} (x - \beta_k)$, où $\beta_k \in \mathbf{F}_p$ est la réduction modulo p de $\frac{j+k}{p^h}$. Comme le degré de $\overline{f}_{n,j}$ est le cardinal de $\mathrm{K}_{n,j}$, le lemme est équivalent aux résultats suivants :

- $v_p(c_{n,j}) \geqslant 0$, pour tout j,
- $v_p(c_{n,j}) = 0$, si $j = i(n)$,
- $v_p(c_{n,j}) > 0$, si $j > i(n)$.

On obtient la relation $c_{n,j} \prod_{k\in \mathrm{K}_{n,j}} \left(\frac{-j-k}{p^h}\right) = [\frac{n}{p^h}]! \frac{1}{n!} \prod_{k=0}^{n-1}(-j-k)$ en identifiant les termes constants. On a donc

$$c_{n,j} = [\frac{n}{p^h}]! \frac{1}{n!} \prod_{k\in \mathrm{K}_{n,j}} p^h \prod_{k\notin \mathrm{K}_{n,j}} (-j-k).$$

$$v_p(c_{n,j}) = v_p([\frac{n}{p^h}]!) - v_p(n!) + \sum_{0\leqslant k\leqslant n-1} \inf(v_p(j+k), h).$$

En utilisant l'identité $v_p(n!) - v_p([\frac{n}{p^h}]!) = \sum_{\ell=1}^{h} \left[\frac{n}{p^\ell}\right]$ (cf. ex. 1.4 du Vocabulaire), et

$$\sum_{k=0}^{n-1} \inf(v_p(j+k), h) = \sum_{\ell=1}^{h} \left|\{k \leqslant n-1,\ v_p(j+k) \geqslant \ell\}\right| = \sum_{\ell=1}^{h} \Big([\frac{n+j-1}{p^\ell}] - [\frac{j-1}{p^\ell}]\Big),$$

on en déduit la formule

$$v_p(c_{n,j}) = \sum_{\ell=1}^{h} \Big([\frac{n+j-1}{p^\ell}] - [\frac{j-1}{p^\ell}] - [\frac{n}{p^\ell}] \Big).$$

Comme $[x+y] \geqslant [x]+[y]$, chacun des termes de la somme est $\geqslant 0$, et donc $v_p(c_{n,j}) \geqslant 0$, ce qui démontre le premier point.

Pour démontrer le second, on utilise la formule $-[\frac{-a}{b}] = [\frac{a-1}{b}] + 1$, valable quels que soient $a \in \mathbf{Z}$ et $b \in \mathbf{N} - \{0\}$, ce qui nous donne

$$\begin{aligned} v_p(c_{n,i(n)}) &= \sum_{\ell=1}^{h} \Big([\frac{m(n)p^h - 1}{p^\ell}] - [\frac{i(n)-1}{p^\ell}] - [\frac{m(n)p^h - i(n)}{p^\ell}] \Big) \\ &= \sum_{\ell=1}^{h} \Big((m(n)p^{h-\ell} - 1) + \big(1 + [\frac{-i(n)}{p^\ell}]\big) - \big(m(n)p^{h-\ell} + [\frac{-i(n)}{p^\ell}]\big) \Big) = 0. \end{aligned}$$

Enfin, pour démontrer le troisième, constatons que $[\frac{n+j-1}{p^h}] - [\frac{j-1}{p^h}] - [\frac{n}{p^h}] = 1$, si $j > i(n)$, et donc $v_p(c_{n,j}) \geqslant 1$.

Ceci permet de conclure.

D.4. La fonction zêta p-adique

Kummer, dans son travail sur le th. de Fermat (cf. note 9 du chap. VII), a découvert des congruences modulo p^n entre les valeurs aux entiers négatifs de la fonction zêta (cf. ex. D.4.9), ce qui, quand on y pense, est assez intrigant : la fonction ζ est définie par une série ne convergeant pas en les entiers négatifs ; on la prolonge analytiquement (l'existence d'un tel prolongement est déjà un peu miraculeux), et on découvre que les valeurs aux entiers négatifs sont des nombres rationnels et, cerise sur le gâteau, que ces nombres rationnels ont des propriétés p-adiques remarquables, pour tout nombre premier p...

Les congruences de Kummer ont été réinterprétées par Kubota et Leopoldt (1964) comme une propriété de continuité p-adique de la fonction $n \mapsto \zeta(-n)$, ce qui les a menés à la construction de la fonction zêta p-adique.

Théorème D.4.1. — *Si $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, il existe une unique fonction $\zeta_{p,i}$, continue sur $\mathbf{Z}_p$ (resp. $\mathbf{Z}_p - \{1\}$) si $i \neq 1$ (resp. si $i = 1$), telle que $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ si $n \in \mathbf{N}$ vérifie $-n \equiv i$ modulo $p-1$.*

Remarque D.4.2. — (i) Comme nous le verrons, la continuité de $n \mapsto \zeta(-n)$ est une conséquence de celle de $n \mapsto x^n$, si $x \in \mathbf{Z}_p^*$.

(ii) Si $i \in \{1, \dots, p-1\}$, l'ensemble des $-n \equiv i$, avec $n \in \mathbf{N}$, est l'image de $\mathbf{N}$ par $x \mapsto i - (p-1)(x+1)$, et comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$ et $p-1 \in \mathbf{Z}_p^*$, cet ensemble est dense dans $\mathbf{Z}_p$. On en déduit l'unicité de $\zeta_{p,i}$; par contre son existence n'est pas du tout automatique et relève un peu du miracle. La fonction $\zeta_{p,i}$ est appelée la i-ème branche

de la *fonction zêta p-adique*. Si i est pair et $p \neq 2$, alors $\zeta_{p,i}$ est identiquement nulle car $\zeta(-n) = 0$ si $n \geqslant 2$ est pair.

(iii) Les zéros de la fonction ζ p-adique (contrairement à ceux de la fonction ζ de Riemann...) sont bien compris : ils faisaient l'objet de la « conjecture principale » qui a été démontrée par Mazur et Wiles (1984).

1. Intégration p-adique

Une *mesure* μ *sur* $\mathbf{Z}_p$ est une forme linéaire continue sur $\mathscr{C}(\mathbf{Z}_p)$. On écrira $\mu(\phi)$ sous la forme plus parlante $\int_{\mathbf{Z}_p} \phi(x)\mu(x)$ ou simplement sous la forme $\int_{\mathbf{Z}_p} \phi\,\mu$.

Si μ est une mesure sur $\mathbf{Z}_p$, on note $\|\mu\|_\infty$ la norme de μ en tant qu'opérateur, c'est-à-dire le sup. de $|\int_{\mathbf{Z}_p} \phi\mu|_p$, avec $\|\phi\|_\infty \leqslant 1$.

• On note $\mu(a + p^n\mathbf{Z}_p)$ la mesure de $a + p^n\mathbf{Z}_p$ (i.e. l'intégrale $\int_{\mathbf{Z}_p} \mathbf{1}_{a+p^n\mathbf{Z}_p}\mu$).

• Comme $a + p^n\mathbf{Z}_p$ est la réunion disjointe des $a + jp^n + p^{n+1}\mathbf{Z}_p$ pour $0 \leqslant j \leqslant p-1$, on a $\mu(a + p^n\mathbf{Z}_p) = \sum_{j=0}^{p-1} \mu(a + jp^n + p^{n+1}\mathbf{Z}_p)$.

• Comme $\|\mathbf{1}_{a+p^n\mathbf{Z}_p}\|_\infty = 1$, les $\mu(a + p^n\mathbf{Z}_p)$ sont bornés (on a $|\mu(a + p^n\mathbf{Z}_p)| \leqslant \|\mu\|_\infty$).

Si on utilise le fait que $\phi \in \mathscr{C}(\mathbf{Z}_p)$ est la limite dans $\mathscr{C}(\mathbf{Z}_p)$ de $\sum_{a=0}^{p^n-1} \phi(a)\mathbf{1}_{a+p^n\mathbf{Z}_p}$ (cf. solution du (v) de l'ex. 20.6 du Vocabulaire) et la continuité de μ, on obtient

$$\int_{\mathbf{Z}_p} \phi\,\mu = \lim_{n\to+\infty} \sum_{a=0}^{p^n-1} \phi(a)\mu(a + p^n\mathbf{Z}_p),$$

formule qui ressemble beaucoup à une somme de Riemann.

Remarque D.4.3. — (i) Réciproquement, si on se donne une famille $\mu(a + p^n\mathbf{Z}_p)$, pour $a \in \mathbf{Z}_p$ et $n \in \mathbf{N}$, d'éléments de $\mathbf{Q}_p$ vérifiant les conditions :

• $\mu(a + p^n\mathbf{Z}_p) = \mu(b + p^n\mathbf{Z}_p)$ si $v_p(a - b) \geqslant n$,

• $\mu(a + p^n\mathbf{Z}_p) = \sum_{j=0}^{p-1} \mu(a + jp^n + p^{n+1}\mathbf{Z}_p)$,

• il existe $\mathrm{C} \in \mathbf{R}$ tel que $|\mu(a + p^n\mathbf{Z}_p)| \leqslant \mathrm{C}$ quels que soient $a \in \mathbf{Z}_p$ et $n \in \mathbf{N}$,

alors les deux premières permettent d'étendre μ en une forme linéaire sur l'espace $\mathrm{LC}(\mathbf{Z}_p)$ des fonctions localement constantes sur $\mathbf{Z}_p$, et la troisième implique que $|\mu(\phi)|_p \leqslant \mathrm{C}\|\phi\|_\infty$, ce qui permet (cf. n° 17.2 du Vocabulaire) d'étendre μ, par continuité, à $\mathscr{C}(\mathbf{Z}_p)$.

(ii) Il n'y a pas de mesure de Haar en p-adique et donc aucun moyen canonique d'associer une mesure à une fonction. En effet, une mesure μ, qui est invariante par translation sur $\mathbf{Z}_p$, doit vérifier $\mu(a + p^n\mathbf{Z}_p) = \frac{1}{p^n}\mu(\mathbf{Z}_p)$, et donc $|\mu(a + p^n\mathbf{Z}_p)|_p = p^n|\mu(\mathbf{Z}_p)|_p$, quels que soient $a \in \mathbf{Z}_p$ et $n \in \mathbf{N}$. Ceci n'est possible que si $\mu(\mathbf{Z}_p) = 0$ (et donc si $\mu = 0$) car les $\mu(a+p^n\mathbf{Z}_p)$ doivent être bornés en norme par $\|\mu\|_\infty$.

A une mesure, on associe la série formelle $\mathscr{A}_\mu(\mathrm{T}) = \sum_{n=0}^{+\infty} \mathrm{T}^n \int_{\mathbf{Z}_p} \binom{x}{n}\mu(x)$ appelée *transformée d'Amice* de μ. C'est un analogue p-adique de la transformée de Fourier : on a formellement $\mathscr{A}_\mu(\mathrm{T}) = \int_{\mathbf{Z}_p} (1+\mathrm{T})^x\mu(x)$ puisque $(1+\mathrm{T})^x = \sum_{n=0}^{+\infty} \binom{x}{n}\mathrm{T}^n$, et on peut voir T

comme un analogue p-adique de $e^{2i\pi}-1$ (qui a le mauvais goût d'être nul dans le monde réel bien que $e^{2i\pi x}$ ne soit pas toujours égal à 1...).

Théorème D.4.4. — *L'application $\mu \mapsto \mathscr{A}_\mu$ est une isométrie de l'espace des mesures muni de $\| \|_\infty$ sur l'espace des séries formelles à coefficients bornés muni de la norme du sup. des normes des coefficients.*

Démonstration. — Comme les $\binom{x}{n}$ forment une base orthonormale de $\mathscr{C}(\mathbf{Z}_p)$, le résultat est un cas particulier de la prop. II.4.9. De manière explicite, l'application réciproque associe à $\sum_{n\in\mathbf{N}} b_n \mathrm{T}^n$, où $(b_n)_{n\in\mathbf{N}}$ est bornée, la mesure μ définie par $\mu(\phi)=\sum_{n=0}^{+\infty} b_n a_n(\phi)$ si ϕ est une fonction continue sur $\mathbf{Z}_p$.

Si $z\in\mathbf{C}_p$ vérifie $|z-1|_p>0$, alors $(z-1)^n\to 0$, et la série $\phi_z(x)=\sum_{n=0}^{+\infty}\binom{x}{n}(z-1)^n$ converge uniformément et définit une fonction continue $x\mapsto\phi_z(x)$ sur $\mathbf{Z}_p$, à valeurs dans $\mathbf{C}_p$ (si $z\in\mathbf{Q}_p$, cette fonction est à valeurs dans $\mathbf{Q}_p$). D'autre part, si $k\in\mathbf{N}$, on a $\phi_z(k)=z^k$, ce qui nous permet de noter de manière plus parlante $x\mapsto z^x$ la fonction $x\mapsto\phi_z(x)$. On a $z^{x+y}=z^x z^y$ quels que soient $x,y\in\mathbf{Z}_p$ car cette formule est vraie si $x,y\in\mathbf{N}$, et $\mathbf{N}^2$ est dense dans $\mathbf{Z}_p^2$.

Ceci s'applique en particulier à $z\in\boldsymbol{\mu}_{p^n}$ (cf. ex. 20.3). On a alors $z^{x+p^n k}=z^x$ quel que soit $k\in\mathbf{N}$ et donc $z^x=z^y$, si $y\in x+p^n\mathbf{Z}_p$, ce qui fait que la fonction $x\mapsto z^x$ est localement constante.

Si μ est une mesure sur $\mathbf{Z}_p$, on peut étendre μ en une forme $\mathbf{C}_p$-linéaire continue sur l'espace $\mathscr{C}(\mathbf{Z}_p,\mathbf{C}_p)$ des fonctions continues sur $\mathbf{Z}_p$, à valeurs dans $\mathbf{C}_p$, grâce à la formule $\int_{\mathbf{Z}_p}\phi\,\mu=\lim_{n\to+\infty}\sum_{a=0}^{p^n-1}\phi(a)\mu(a+p^n\mathbf{Z}_p)$ (la convergence se démontre en utilisant la continuité uniforme de ϕ, comme dans le cas d'une fonction à valeurs dans $\mathbf{Q}_p$). Le lemme suivant montre que l'identité $\mathscr{A}_\mu(\mathrm{T})=\int_{\mathbf{Z}_p}(1+\mathrm{T})^x\mu(x)$ n'est pas que formelle.

Lemme D.4.5. — *Si $|z|_p<1$, alors $\int_{\mathbf{Z}_p}(1+z)^x\mu(x)=\mathscr{A}_\mu(z)$*

Démonstration. — La suite de fonctions $x\mapsto\sum_{n=0}^{\mathrm{N}}\binom{x}{n}z^n$ converge uniformément sur $\mathbf{Z}_p$ vers $x\mapsto(1+z)^x$ (le reste est plus petit en norme $\|\ \|_\infty$ que $|z|_p^{n+1}$) ; on peut donc échanger intégration et somme, d'où le résultat.

Corollaire D.4.6. — *Si $i\in\mathbf{Z}_p$ et $n\in\mathbf{N}$, alors $\mu(i+p^n\mathbf{Z}_p)=\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-i}\mathscr{A}_\mu(\eta-1)$.*

Démonstration. — On a

$$\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^x=\begin{cases}p^n & \text{si } x\in p^n\mathbf{Z}_p,\\ 0 & \text{sinon,}\end{cases}$$

et la fonction caractéristique de $i+p^n\mathbf{Z}_p$ est donc $\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{x-i}$. On peut donc utiliser le lemme D.4.5 pour conclure.

2. La mesure μ_a

Dans tout ce qui suit, a est un entier $\geqslant 2$, premier à p. On peut appliquer la proposition VII.2.6 à la fonction

$$f_a(t) = \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1},$$

qui est $\mathscr{C}^\infty$ sur $\mathbf{R}_+$ (on s'est débrouillé pour supprimer le pôle en 0), et à décroissance rapide à l'infini ainsi que toutes ses dérivées. Comme

$$\frac{1}{\Gamma(s)} \int_0^{+\infty} f_a(t) t^s \, \frac{dt}{t} = \frac{1 - a^{1-s}}{\Gamma(s)} \int_0^{+\infty} \frac{1}{e^t - 1} t^s \, \frac{dt}{t} = (1 - a^{1-s})\zeta(s), \quad \text{si } \mathrm{Re}(s) > 1,$$

on obtient la formule suivante pour les valeurs de $\zeta(s)$ aux entiers négatifs.

Lemme D.4.7. — *Si $n \in \mathbf{N}$, alors $(1 - a^{1+n})\zeta(-n) = (-1)^n f_a^{(n)}(0)$.*

Proposition D.4.8. — *Il existe une* (unique) *mesure μ_a sur $\mathbf{Z}_p$ telle que, pour tout $n \in \mathbf{N}$, on ait $\int_{\mathbf{Z}_p} x^n \mu_a = (-1)^n (1 - a^{1+n})\zeta(-n)$.*

Démonstration. — L'unicité de μ_a vient de ce que la connaissance de $\int_{\mathbf{Z}_p} x^n \mu_a$, pour tout $n \in \mathbf{N}$, équivaut à celle de $\int_{\mathbf{Z}_p} \binom{x}{n} \mu_a$, pour tout $n \in \mathbf{N}$, et donc à la transformée d'Amice de μ_a ; or celle-ci détermine μ_a d'après le th. D.4.4.

Soit $\mathrm{F}_a(\mathrm{T}) = \frac{1}{\mathrm{T}} - \frac{a}{(1+\mathrm{T})^a - 1}$, de sorte que $\mathrm{F}_a(e^t - 1) = f_a(t)$ (comme série formelle en t). On peut écrire $(1 + \mathrm{T})^a - 1$ sous la forme $a\mathrm{T}(1 + \mathrm{T}g(\mathrm{T}))$, où $g(\mathrm{T}) = \sum_{n \geqslant 2} \frac{1}{a}\binom{a}{n}\mathrm{T}^{n-2}$ appartient à $\mathbf{Z}_p[\mathrm{T}]$ car a est inversible dans $\mathbf{Z}_p$, puisque premier à p. Il en résulte que

$$\mathrm{F}_a(\mathrm{T}) = \frac{1}{\mathrm{T}} - \frac{a}{(1 + \mathrm{T})^a - 1} = \sum_{n=1}^{+\infty} (-\mathrm{T})^{n-1} g^n \in \mathbf{Z}_p[[\mathrm{T}]],$$

et donc que F_a est la transformée d'Amice d'une mesure μ_a puisque F_a est à coefficients bornés car entiers. Maintenant, $\int_{\mathbf{Z}_p} x^n \mu_a$ est la dérivée n-ième en $t = 0$ de la série formelle $\mathscr{L}(t) = \int_{\mathbf{Z}_p} e^{tx} \, \mu_a$. Or $e^{tx} = (1 + (e^t - 1))^x$, et donc $\mathscr{L}(t) = \mathrm{F}_a(e^t - 1) = f_a(t)$. On déduit donc du lemme D.4.7 que $\int_{\mathbf{Z}_p} x^n \mu_a = (-1)^n (1 - a^{1+n})\zeta(-n)$, ce qui permet de conclure.

Exercice D.4.9. — Montrer que $(1 - a^{1+n_1})\zeta(-n_1) \equiv (1 - a^{1+n_2})\zeta(-n_2) \bmod p^k$, si $n_1, n_2 \geqslant k$, et si $n_1 \equiv n_2 \bmod (p-1)p^{k-1}$. (On montrera que $\|x^{n_1} - x^{n_2}\|_\infty \leqslant p^{-k}$ et $\|\mu_a\|_\infty \leqslant 1$.)

3. Continuité de la fonction $n \mapsto x^n$

Si $x \in \mathbf{Z}_p$, il n'existe pas toujours de fonction continue $s \mapsto x^s$ prenant la valeur x^n en $s = n$ pour tout $n \in \mathbf{N}$, mais on dispose d'une fonction multivaluée, dont les branches sont indexées par $\mathbf{Z}/(p-1)\mathbf{Z}$, qui joue le rôle de x^s (cf. prop. D.4.13).

Lemme D.4.10. — *Si $a, b \in \mathbf{Z}_p$, et si $|a - b|_p \leqslant p^{-1}$, alors $|a^p - b^p|_p \leqslant p^{-1}|a - b|_p$.*

Démonstration. — $a^p - b^p = p(a-b)\sum_{i=0}^{p-1} \frac{1}{p}\binom{p}{i}(a-b)^{p-i-1}$, et tous les termes de la somme appartiennent à $\mathbf{Z}_p$ grâce à l'hypothèse $|a-b|_p \leqslant p^{-1}$ et à la divisibilité de $\binom{p}{i}$ par p, si $1 \leqslant i \leqslant p-1$ (ex. 1.4 du Vocabulaire). Cela permet de conclure.

Proposition D.4.11. — (i) *Si $a \in \mathbf{Z}_p$, la suite $(a^{p^n})_{n\in\mathbf{N}}$ a une limite $\omega(a) \in \mathbf{Z}_p$ vérifiant $|a-\omega(a)|_p \leqslant p^{-1}$.*

(ii) *On a $\omega(a) = 0$ si $a \in p\mathbf{Z}_p$, et $\omega(a) \in \boldsymbol{\mu}_{p-1}$ si $a \in \mathbf{Z}_p^*$.*

(iii) *$\omega(ab) = \omega(a)\omega(b)$, pour tous $a, b \in \mathbf{Z}_p$.*

Démonstration. — Si $a \in \mathbf{N}$, on a $|a^p - a|_p \leqslant p^{-1}$ d'après le petit th. de Fermat. Comme $\mathbf{N}$ est dense dans $\mathbf{Z}_p$, cette inégalité est vraie pour tout $a \in \mathbf{Z}_p$, par continuité de $a \mapsto |a^p - a|_p$. Le lemme D.4.10 permet donc d'en déduire, par récurrence sur n, que $|u_{n+1} - u_n|_p \leqslant p^{-n}$, où l'on a posé $u_n = a^{p^n}$. Il en résulte que u_n a une limite $\omega(a)$ puisque $u_{n+1} - u_n \to 0$, et que $a - \omega(a) = \sum_{n=0}^{+\infty}(u_n - u_{n+1})$ a une norme $\leqslant \sup_{n\in\mathbf{N}} |u_n - u_{n+1}|_p \leqslant p^{-1}$. D'où le (i).

Maintenant, $\omega(a)^p = \omega(a)$ car $\omega(a)^p$ est limite de la suite $(a^{p^{n+1}})_{n\in\mathbf{N}}$.

• Si $a \in p\mathbf{Z}_p$, alors $|a^{p^n}|_p \leqslant p^{-p^n}$, et donc $a^{p^n} \to 0$ et $\omega(a) = 0$.

• si $a \in \mathbf{Z}_p^*$, alors $\omega(a) \neq 0$ puisque $|a|_p = 1$ et $|a - \omega(a)|_p \leqslant p^{-1}$. Comme $\omega(a)^p = \omega(a)$, on a $\omega(a)^{p-1} = 1$, ce qui démontre le (ii).

Enfin, $\omega(ab) = \lim(ab)^{p^n} = \lim a^{p^n} b^{p^n} = (\lim a^{p^n})(\lim b^{p^n}) = \omega(a)\omega(b)$.

Remarque D.4.12. — (i) Il résulte de la proposition précédente que $\omega : \mathbf{Z}_p^* \to \boldsymbol{\mu}_{p-1}$ est un caractère linéaire ; c'est le *caractère de Teichmüller*.

(ii) Si $x \in \mathbf{Z}_p^*$, on pose $\langle x\rangle = \omega(x)^{-1}x$. On a $|\langle x\rangle - 1|_p \leqslant p^{-1}$ puisque $|x - \omega(x)|_p \leqslant p^{-1}$.

Proposition D.4.13. — (i) *Si $s \in \mathbf{Z}_p$ et $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, la suite de terme général x^n, pour $n \in \mathbf{N}$, $n \equiv i \bmod p-1$, a une limite* (on note $x^{s,i}$ cette limite).

(ii) *On a $x^{s,i} = 0$ si $x \in p\mathbf{Z}_p$, et $x^{s,i} = \omega(x)^i\langle x\rangle^s$, si $x \in \mathbf{Z}_p^*$.*

(iii) *$x^{n,i} = x^n$ si $n \in \mathbf{Z}$ est congru à i modulo $p-1$, et si $x \in \mathbf{Z}_p^*$.*

Démonstration. — • Si $x \in 1 + p\mathbf{Z}_p$, la fonction $s \mapsto x^s = \sum_{n=0}^{+\infty}\binom{s}{n}(x-1)^n$ est, comme nous l'avons déjà vu, une fonction continue qui vaut x^n, si $n \in \mathbf{N}$. D'où l'existence de $x^{s,i} = x^s$.

• Si $x \in p\mathbf{Z}_p$, la suite de terme général x^n tend vers 0 quand n tend vers $+\infty$.

• Si $x \in \mathbf{Z}_p^*$, on peut écrire x sous la forme $\omega(x)\langle x\rangle$ et x^n sous la forme $\omega(x)^n\langle x\rangle^n$. Comme $\langle x\rangle \in 1 + p\mathbf{Z}_p$, la fonction $n \mapsto \langle x\rangle^n$ se prolonge par continuité et $\omega(x)$ étant une racine $(p-1)$-ième de l'unité, la fonction $n \mapsto \omega(x)^n$ est périodique de période $p-1$. Ceci fait que, si on fixe $i \in \{0, 1, \ldots, p-1\}$ et si $x \in \mathbf{Z}_p^*$, la fonction $x \mapsto x^n$ de $i + (p-1)\mathbf{N}$ dans $\mathbf{Z}_p$ se prolonge par continuité en une fonction continue sur $\mathbf{Z}_p$.

On en déduit les (i) et (ii). Le (iii) résulte de ce que $\langle x\rangle^n = x^n\omega(x)^n$ si $n \in \mathbf{Z}$ et $\omega(x)^n = \omega(x)^i$ si $n \equiv i \bmod p-1$ et $x \in \mathbf{Z}_p^*$.

Lemme D.4.14. — *Si μ est une mesure sur $\mathbf{Z}_p$, et si $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, alors $s \mapsto \int_{\mathbf{Z}_p} x^{s,i}\,\mu$ est continue sur $\mathbf{Z}_p$.*

Démonstration. — On a $x^{s,i} = \sum_{n=0}^{+\infty} \binom{s}{n} \big(\mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle - 1)^n\big)$, et comme $\big|\binom{s}{n}\big|_p \leqslant 1$, si $s \in \mathbf{Z}_p$ et $\|\mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle - 1)^n\|_\infty \leqslant p^{-n}$, cette série converge dans $\mathscr{C}(\mathbf{Z}_p)$, ce qui permet d'intervertir série et intégrale, et d'obtenir $\int_{\mathbf{Z}_p} x^{s,i}\,\mu = \sum_{n=0}^{+\infty} a_n \binom{s}{n}$, avec $a_n = \int_{\mathbf{Z}_p} \mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle - 1)^n\,\mu$. On a alors $|a_n|_p \leqslant p^{-n}\|\mu\|_\infty$, et donc $a_n \to 0$, ce qui permet de conclure. (La majoration $|a_n|_p \leqslant p^{-n}\|\mu\|_\infty$ montre qu'en fait $s \mapsto \int_{\mathbf{Z}_p} x^{s,i}\,\mu$ est analytique si $p \geqslant 3$ (si $p = 2$, cette fonction est analytique sur $2\mathbf{Z}_2$ et sur $1 + 2\mathbf{Z}_2$).)

4. Restriction de μ_a à $\mathbf{Z}_p^*$

Si U est un ouvert compact de $\mathbf{Z}_p$, et si μ est une mesure sur $\mathbf{Z}_p$, on note $\mathrm{Res}_{\mathrm{U}}\mu$ la restriction de μ à U : c'est la mesure définie par $\int_{\mathbf{Z}_p} \phi\,\mathrm{Res}_{\mathrm{U}}\mu = \int_{\mathbf{Z}_p} \mathbf{1}_{\mathrm{U}}\phi\,\mu$ (que l'on note aussi $\int_{\mathrm{U}} \phi\,\mu$). Le cor. D.4.18 ci-dessous [3] montre que restreindre μ_a à $\mathbf{Z}_p^*$ fait sortir un facteur d'Euler en p. Il est rare que le lien entre une mesure et sa restriction à $\mathbf{Z}_p^*$ soit aussi simple.

Lemme D.4.15. — *Soit c un entier $\geqslant 1$, et soit $i \in \{0, 1, \dots, c-1\}$.*

(i) $\lim_{z\to 0} \frac{(1+z)^i}{(1+z)^c-1} - \frac{1}{cz} = \frac{i}{c} - \frac{c-1}{2c}$.

(ii) $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}} \frac{\eta^{-i}}{\eta-1} = \frac{i}{c} - \frac{c-1}{2c}$.

(iii) *Si $(a, c) = 1$, alors* $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}} \frac{\eta^{-i}}{\eta^a-1} = \frac{[a^{-1}i]}{c} - \frac{c-1}{2c}$, *où $[a^{-1}i] \in \{0, 1, \dots, c-1\}$ est le représentant de $a^{-1}i \in \mathbf{Z}/c\mathbf{Z}$.*

Démonstration. — On a $\frac{(1+z)^i}{(1+z)^c-1} = \frac{1+iz+\cdots}{cz(1+\frac{c-1}{2}z+\cdots)} = \frac{1}{cz}(1 + iz - \frac{c-1}{2}z + \cdots)$, d'où le (i).

On a $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}} \frac{\eta^{-i}}{\eta-1} = \lim_{z\to 0} \frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c} \frac{\eta^{-i}}{(1+z)\eta-1} - \frac{1}{cz}$ et $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c} \frac{\eta^{-i}}{(1+z)\eta-1} = \frac{(1+z)^i}{(1+z)^c-1}$ (cela résulte de ce que $\lim_{z\to\eta^{-1}-1}((1+z)\eta - 1)\frac{(1+z)^i}{(1+z)^c-1} = \frac{\eta^{-i}\eta}{c(\eta^{-1})^{c-1}} = \eta^{-i}$, si $\eta \in \boldsymbol{\mu}_c$). Le (ii) est donc une conséquence du (i).

Enfin, $\eta \mapsto \eta^a$ est une bijection de $\boldsymbol{\mu}_c$ car $(a, c) = 1$, et on a $\eta^{-i} = (\eta^a)^{-[a^{-1}i]}$, si $\eta \in \boldsymbol{\mu}_c$, ce qui permet de déduire le (iii) du (ii).

Si $b \in \mathbf{Q}_p$ a pour écriture $\sum_{i=-k}^{+\infty} p^i b_i$ en base p (les b_i appartiennent à $\{0, \dots, p-1\}$), on note $\{b\}$ l'élément $\sum_{i=-k}^{-1} p^i b_i$ de $\mathbf{Q}$: c'est l'unique élément de $\mathbf{Z}[\frac{1}{p}] \cap [0, 1[$ tel que $b - \{b\} \in \mathbf{Z}_p$. On a $\{b\} = \{b'\}$ si et seulement si $b - b' \in \mathbf{Z}_p$.

Lemme D.4.16. — $\mu_a(i + p^n\mathbf{Z}_p) = \big\{\frac{i}{p^n}\big\} - a\big\{\frac{a^{-1}i}{p^n}\big\} + \frac{a-1}{2}$, *pour tous $i \in \mathbf{Z}_p$ et $n \in \mathbf{N}$.*

Démonstration. — Quitte à remplacer i par un représentant mod p^n, on peut supposer $i \in \{0, 1, \dots, p^n - 1\}$. On a, d'après le cor. D.4.6,

$$\mu_a(i + p^n\mathbf{Z}_p) = \frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}} \eta^{-i}\mathscr{A}_{\mu_a}(\eta - 1) = \frac{1}{p^n}\mathscr{A}_{\mu_a}(0) + \frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}} \Big(\frac{\eta^{-i}}{\eta-1} - a\frac{\eta^{-i}}{\eta^a-1}\Big).$$

3. La démonstration proposée est assez pataude mais elle permet de ne pas sortir de $\mathbf{Q}_p$; l'ex. D.4.19 en suggère une plus élégante.

Il résulte du (i) du lemme D.4.15 que $\mathscr{A}_{\mu_a}(0) = \frac{1-a}{2}$, et du (ii) et (iii) du même lemme que $\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}}\frac{\eta^{-i}}{\eta-1} = \frac{i}{p^n} - \frac{p^n-1}{2p^n}$ et $\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}}\frac{\eta^{-i}}{\eta^a-1} = \frac{[a^{-1}i]}{p^n} - \frac{p^n-1}{2p^n}$. On conclut en remarquant que $\big\{\frac{a^{-1}i}{p^n}\big\} = \frac{[a^{-1}i]}{p^n}$.

Lemme D.4.17. — *On a $\int_{p\mathbf{Z}_p}\phi\big(\frac{x}{p}\big)\,\mu_a = \int_{\mathbf{Z}_p}\phi\,\mu_a$, pour tout $\phi\in\mathscr{C}(\mathbf{Z}_p)$.*

Démonstration. — Si $\phi\in\mathscr{C}(\mathbf{Z}_p)$, soit $[p]\cdot\phi$ la fonction définie par $([p]\cdot\phi)(x) = \phi\big(\frac{x}{p}\big)$, si $x\in p\mathbf{Z}_p$, et $([p]\cdot\phi)(x) = 0$, si $x\in\mathbf{Z}_p^*$. Alors $[p]\cdot\phi\in\mathscr{C}(\mathbf{Z}_p)$ et $[p]:\mathscr{C}(\mathbf{Z}_p)\to\mathscr{C}(\mathbf{Z}_p)$ est linéaire, et continue puisque $\|[p]\cdot\phi\|_\infty \leqslant \|\phi\|_\infty$. Il s'ensuit que $\lambda = \mu_a\circ([p]-1)$ est une mesure sur $\mathbf{Z}_p$. Maintenant, si $i\in\mathbf{Z}_p$ et $n\in\mathbf{N}$, on a $[p]\cdot\mathbf{1}_{i+p^n\mathbf{Z}_p} = \mathbf{1}_{pi+p^{n+1}\mathbf{Z}_p}$ car $\frac{x}{p}\in i+p^n\mathbf{Z}_p$ équivaut à $x\in pi+p^{n+1}\mathbf{Z}_p$. On a donc, d'après le lemme D.4.16,

$$\begin{aligned}\int_{\mathbf{Z}_p}\mathbf{1}_{i+p^n\mathbf{Z}_p}\lambda &= \mu_a(i+p^n\mathbf{Z}_p) - \mu_a(pi+p^{n+1}\mathbf{Z}_p)\\ &= \big(\big\{\frac{i}{p^n}\big\} - a\big\{\frac{a^{-1}i}{p^n}\big\} + \frac{a-1}{2}\big) - \big(\big\{\frac{pi}{p^{n+1}}\big\} - a\big\{\frac{a^{-1}pi}{p^{n+1}}\big\} + \frac{a-1}{2}\big) = 0.\end{aligned}$$

Il s'ensuit, par linéarité, que λ est identiquement nulle sur $\mathrm{LC}(\mathbf{Z}_p)$, et donc aussi sur $\mathscr{C}(\mathbf{Z}_p)$, puisque $\mathrm{LC}(\mathbf{Z}_p)$ est dense dans $\mathscr{C}(\mathbf{Z}_p)$ et que λ est continue. On en déduit le résultat car $\int_{\mathbf{Z}_p}\phi\,\lambda = \int_{p\mathbf{Z}_p}\phi\big(\frac{x}{p}\big)\,\mu_a - \int_{\mathbf{Z}_p}\phi\,\mu_a$.

Corollaire D.4.18. — *Si $n\in\mathbf{N}$, alors $\int_{\mathbf{Z}_p^*}x^n\mu_a = (-1)^n(1-a^{n+1})(1-p^n)\zeta(-n)$.*

Démonstration. — $\int_{\mathbf{Z}_p^*}x^n\mu_a = \int_{\mathbf{Z}_p}x^n\mu_a - \int_{p\mathbf{Z}_p}x^n\mu_a$ et $\int_{p\mathbf{Z}_p}x^n\mu_a = p^n\int_{p\mathbf{Z}_p}\big(\frac{x}{p}\big)^n\mu_a = p^n\int_{\mathbf{Z}_p}x^n\mu_a$, d'après le lemme D.4.17. Ceci permet de déduire le résultat de la prop. D.4.8.

Exercice D.4.19. — (i) Établir la formule $\mathbf{1}_{\mathbf{Z}_p^*}(x) = 1 - \frac{1}{p}\sum_{\eta\in\boldsymbol{\mu}_p}\eta^x$.

(ii) En déduire que la transformée d'Amice de $\mathrm{Res}_{\mathbf{Z}_p^*}\mu$ est $\mathscr{A}_\mu(\mathrm{T}) - \frac{1}{p}\sum_{\eta\in\boldsymbol{\mu}_p}\mathscr{A}_\mu((1+\mathrm{T})\eta-1)$, si μ est une mesure sur $\mathbf{Z}_p$.

(iii) Montrer que la transformée d'Amice de $\mathrm{Res}_{\mathbf{Z}_p^*}\mu_a$ est $\mathscr{A}_{\mu_a} - \mathscr{A}_{\mu_a}((1+\mathrm{T})^p-1)$ et retrouver le résultat du cor. D.4.18.

5. Construction de la fonction zêta p-adique

Passons à la démonstration du th. D.4.1. Si $i\in\mathbf{Z}/(p-1)\mathbf{Z}$ et si $a\in\mathbf{Z}_p^*$, définissons une fonction $g_{a,i}$ sur $\mathbf{Z}_p$ par

$$g_{a,i}(s) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}}\int_{\mathbf{Z}_p^*}\omega(x)^{-i}\langle x\rangle^{-s}\mu_a(x).$$

Cette fonction est continue en dehors des zéros de $s\mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$, d'après le lemme D.4.14. Par ailleurs, si $-n\equiv i\ [p-1]$, on a $\omega(a)^{1-i} = \omega(a)^{1+n}$ et $\omega(x)^{-i} = \omega(x)^n$

si $x \in \mathbf{Z}_p^*$ et donc, d'après le cor. D.4.18,

$$g_{a,i}(-n) = \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}} \int_{\mathbf{Z}_p^*} \omega(x)^n \langle x\rangle^n \mu_a(x) = \frac{1}{1-a^{1+n}} \int_{\mathbf{Z}_p^*} x^n \mu_a(x)$$
$$= (-1)^n(1-p^n)\zeta(-n)$$

Pour conclure, il suffit donc de trouver un a tel que $s \mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ ne s'annule pas si $i \neq 1$ et ne s'annule qu'en $s=1$, si $i=1$.

• L'image de $1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ dans $\mathbf{F}_p$ est celle de $1-a^{1-i}$. Maintenant, si $i \neq 1$, on peut choisir un représentant de i dans $\mathbf{Z}$ appartenant à $\{2,\dots,p-1\}$, ce qui fait que l'équation $x^{1-i}=1$ a moins de $p-2$ solutions dans $\mathbf{F}_p$ si $i \neq 1$. Il existe donc $a \in \mathbf{N}$ tel que l'image de $1-a^{1-i}$ dans $\mathbf{F}_p$ soit non nulle, et pour un tel a, la fonction $s \mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ ne s'annule pas.

• Si $u \in 1+p\mathbf{Z}_p$, et si $x \in \mathbf{Z}_p - \{0\}$ vérifie $u^x = 1$, alors $u^{ax}=1$, pour tout $a \in \mathbf{N}$, et donc aussi, par densité de $\mathbf{N}$ dans $\mathbf{Z}_p$ et continuité de $a \mapsto u^{ax}$, pour tout $a \in \mathbf{Z}_p$. Si $v_p(x)=k$, et si $a = p^k x^{-1}$, on a $a \in \mathbf{Z}_p$, et donc $u^{p^k}=1$, ce qui montre que la fonction $u \mapsto u^x - 1$ ne s'annule pas si u n'est pas une racine de l'unité d'ordre une puissance de p. On peut donc prendre pour a n'importe quel élément de $\mathbf{N}$ tel que $\langle a\rangle$ ne soit pas une racine de l'unité (par exemple $a=1+2p$), et alors $s \mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ ne s'annule qu'en $s=1$, si $i=1$.

APPENDICE E

IRRATIONALITÉ D'UNE INFINITÉ DE $\zeta(2n+1)$

Cet appendice est consacré au résultat de Rivoal (2000) mentionné dans la note 9 du chap. III selon lequel il existe une infinité de $n \geqslant 1$ tels que $\zeta(2n+1)$ est irrationnel. On va en fait démontrer un résultat plus fort (cf. (i) du th. E.1.1 ci-dessous).

E.1. Indépendance linéaire de nombres réels

Si les v_i, pour $i \in \mathrm{I}$, sont des réels, on note $\mathrm{Vect}(v_i,\ i \in \mathrm{I})$ le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{R}$ engendré par les v_i, et on note $\dim_{\mathbf{Q}} \mathrm{Vect}(v_i,\ i \in \mathrm{I})$ sa dimension. Par exemple, v est irrationnel si et seulement si $\dim_{\mathbf{Q}} \mathrm{Vect}(1, v) = 2$.

Théorème E.1.1. — (i) $\dim_{\mathbf{Q}} \mathrm{Vect}(\zeta(2n+1),\ n \geqslant 1) = +\infty$.
(ii) $\dim_{\mathbf{Q}} \mathrm{Vect}(\zeta(2n),\ n \geqslant 1) = +\infty$.

Remarque E.1.2. — (i) Le (ii) permet de redémontrer la transcendance de π due à Lindemann (1882). En effet, comme $\zeta(2n) \in \mathbf{Q}\,\pi^{2n}$ (cf. ex. V.5.3), le (ii) est équivalent à n'importe lequel des énoncés suivants :
- $\dim_{\mathbf{Q}} \mathrm{Vect}(\pi^{2n},\ n \geqslant 1) = +\infty$.
- π est transcendant.
- 1 et les π^{2n}, pour $n \geqslant 1$, sont linéairement indépendants sur $\mathbf{Q}$.
- 1 et les $\zeta(2n)$, pour $n \geqslant 1$, sont linéairement indépendants sur $\mathbf{Q}$.

(ii) On conjecture que 1 et les $\zeta(n)$, pour $n \geqslant 2$, sont linéairement indépendants sur $\mathbf{Q}$, mais on est loin de savoir démontrer un tel énoncé : en particulier, on ne sait pas prouver que $\zeta(5)$ est irrationnel ; l'irrationalité de $\zeta(3)$ (prob. H.12) remonte à 1979 (Apéry).

1. Le critère de Nesterenko

Pour démontrer que deux nombres v_1, v_2 sont linéairement indépendants sur $\mathbf{Q}$, il suffit de produire deux suites d'entiers $(a_{n,i})_{n\in\mathbf{N}}$, pour $i = 1, 2$, telles que $a_{n,1}v_1 + a_{n,2}v_2 \neq 0$, pour n assez grand, et $\lim_{n\to+\infty} a_{n,1}v_1 + a_{n,2}v_2 = 0$ (en effet, si $v_2 = \frac{c}{d}v_1$, avec $d \in \mathbf{N} - \{0\}$ et $c \in \mathbf{Z}$, alors $|a_1v_1 + a_2v_2| = \left|\frac{da_1+ca_2}{d}\right| |v_1| \geqslant \frac{1}{d}|v_1|$, si $a_1, a_2 \in \mathbf{Z}$ et $a_1v_1 + a_2v_2 \neq 0$). Dans le cas général, on dispose du critère suivant, dû à Nesterenko.

Théorème E.1.3 (Critère de Nesterenko). — *Soient* $v_1, \dots, v_b \in \mathbf{R}$. *On suppose qu'il existe* $\mathrm{B} > 1$, $\mathrm{A} > 1$ *et des combinaisons linéaires* $\mathrm{L}_n = a_{n,1}v_1 + \cdots + a_{n,b}v_b$, *pour* $n \in \mathbf{N}$, *à coefficients entiers, vérifiant* :
(i) $\sum_{1 \leqslant j \leqslant b} |a_{n,j}| \leqslant \mathrm{B}^{n+o(n)}$;
(ii) $|a_{n,1}v_1 + \cdots + a_{n,b}v_b| = \mathrm{A}^{-n+o(n)}$.
Alors $\dim_{\mathbf{Q}} \mathrm{Vect}(v_1, \dots, v_b) \geqslant 1 + \frac{\log \mathrm{A}}{\log \mathrm{B}}$.

Dans le cas qui nous intéresse, on dispose d'une machine (cf. prop. E.2.1 ci-dessous) à fabriquer des relations linéaires à coefficients rationnels entre les $\zeta(n)$, $n \geqslant 2$, en partant de fonctions rationnelles n'ayant des pôles qu'aux entiers $\leqslant 0$; le problème est alors de bien choisir ces fonctions rationnelles pour que les combinaisons linéaires ainsi obtenues permettent d'utiliser le critère de Nesterenko.

Démonstration. — Quitte à diviser $v_1, \dots, v_b$ par v_1, on peut supposer que $v_1 = 1$. Soit $1 = w_0, w_1, \dots, w_r$ une base de $\mathrm{Vect}(v_1, \dots, v_b)$ sur $\mathbf{Q}$. On peut exprimer les v_i dans cette base et multiplier tout par le ppcm des dénominateurs des coordonnées des v_i ; les L_n deviennent alors des combinaisons linéaires de $w_0, \dots, w_r$, à coefficients entiers, vérifiant les mêmes estimées que dans l'énoncé (avec de nouveaux $o(n)$, différant des $o(n)$ initiaux par l'addition de constantes). On s'est donc ramené à prouver l'énoncé suivant :

Si $1 = w_0, \dots, w_r$ sont linéairement indépendants sur $\mathbf{Q}$, et s'il existe $\mathrm{B} > 1$, $\mathrm{A} > 1$ et des formes linéaires $\mathrm{L}_n(x_0, \dots, x_r) = a_{n,0}x_0 + \cdots + a_{n,r}x_r$, à coefficients entiers, telles que $\sum_{j=0}^{r} |a_{n,j}| \leqslant \mathrm{B}^{n+o(n)}$ et $\Lambda_n = |\mathrm{L}_n(w_0, \dots, w_r)|^{-1} = \mathrm{A}^{n+o(n)}$, alors $\frac{\log \mathrm{A}}{\log \mathrm{B}} \leqslant r$.

Soit $\mathrm{C}_n = \{(x_0, \dots, x_r) \in \mathbf{R}^{r+1},\ |x_0| \leqslant \Lambda_n \text{ et } |x_0 w_i - w_0| \leqslant \Lambda_n^{-1/r},\ \text{si } 1 \leqslant i \leqslant r\}$. Alors C_n est un parallèlépipède fermé de $\mathbf{R}^{r+1}$, de volume $(2\Lambda_n)\prod_{i=1}^{r}(2\Lambda_n^{-1/r}) = 2^{r+1}$. Il s'ensuit que C_n est un compact convexe symétrique de volume 2^{r+1}, et le lemme de Minkowski (th. B.1.12) assure l'existence de $(x_0(n), \dots, x_r(n)) \in \mathbf{Z}^{r+1}$ appartenant à $\mathrm{C}_n - \{0\}$.

Si $n \gg 0$, soit $k(n)$ le plus grand entier tel que $|x_0(n)|\Lambda_{k(n)}^{-1} \leqslant \frac{1}{2}$. L'hypothèse selon laquelle $\Lambda_n = \mathrm{A}^{n+o(n)}$ implique que $k(n) = \frac{\log |x_0(n)|}{\log \mathrm{A}} + o(\log |x_0(n)|)$, et donc :
- $k(n) \leqslant \frac{\log \Lambda_n}{\log \mathrm{A}} + o(\log \Lambda_n) = n + o(n)$,
- $\Lambda_{k(n)} = |x_0(n)|^{1+o(1)}$ et $|x_0(n)\mathrm{L}_{k(n)}(w_0, \dots, w_r)| = |x_0(n)|^{o(1)} = \Lambda_n^{o(1)} = \mathrm{A}^{o(n)}$.

Maintenant, $\sum_{i=0}^{r} a_{k(n),i}x_i(n) = x_0(n)\mathrm{L}_{k(n)}(w_0, \dots, w_r) + \sum_{i=0}^{r} a_{k(n),i}(x_i(n) - x_0(n)w_i)$. Or le membre de gauche est un entier et $|x_0(n)\mathrm{L}_{k(n)}(w_0, \dots, w_r)| \leqslant \frac{1}{2}$ par construction. Il s'ensuit que $\big|\sum_{i=0}^{r} a_{k(n),i}(x_i(n) - x_0(n)w_i)\big| \geqslant |x_0(n)\mathrm{L}_{k(n)}(w_0, \dots, w_r)| = \mathrm{A}^{o(n)}$. Le membre de gauche est majoré par $\big(\sum_{i=0}^{r} |a_{k(n),i}|\big)\Lambda_n^{-1/r} \leqslant \mathrm{B}^{k(n)+o(k(n))}\mathrm{A}^{-n/r+o(n)}$, et comme $k(n) \leqslant n + o(n)$, on a $\mathrm{B}^{k(n)+o(k(n))} \leqslant \mathrm{B}^{n+o(n)}$. On obtient donc $\mathrm{B}^{n+o(n)}\mathrm{A}^{-n/r+o(n)} \geqslant \mathrm{A}^{o(n)}$, ce qui nous donne $\mathrm{B}\mathrm{A}^{-1/r} \geqslant 1$ et $r \geqslant \frac{\log \mathrm{A}}{\log \mathrm{B}}$, ce que l'on voulait [1].

1. Cette démonstration est due à Fischler et Zudilin (2010) ; elle est nettement plus simple que la démonstration originale de Nesterenko.

E.2. Transcendance de π et indépendance linéaire des $\zeta(n)$

1. Génération de combinaisons linéaires entre les $\zeta(n)$

Soit $a \in \mathbf{N}$, et soit $\mathrm{F} \in \mathbf{Q}(\mathrm{X})$, de degré $\leqslant -2$, n'ayant des pôles qu'aux entiers $\leqslant 0$, ces pôles étant d'ordre $\leqslant a$. Soient $\alpha_{j,k}$, pour $j \geqslant 0$, $1 \leqslant k \leqslant a$ et α_k pour $1 \leqslant k \leqslant a$, les rationnels définis via la décomposition en éléments simples de F(X) par

$$\mathrm{F}(\mathrm{X}) = \sum_{j=0}^{+\infty} \sum_{k=1}^{a} \frac{\alpha_{j,k}}{(\mathrm{X}+j)^k} \quad \text{et} \quad \alpha_k = \sum_{j=0}^{+\infty} \alpha_{j,k}.$$

Remarquons que l'on a $\alpha_{j,k} = 0$ sauf pour un nombre fini de couples (j,k) et donc que les séries ci-dessus sont en fait des sommes finies et, d'autre part, que $\alpha_1 = 0$ car on a supposé F de degré $\leqslant -2$.

Proposition E.2.1. — *La série $\sum_{m=1}^{+\infty} \mathrm{F}(m)$ converge absolument, et on a*

$$\sum_{m=1}^{+\infty} \mathrm{F}(m) = \sum_{k=2}^{a} \alpha_k \zeta(k) - \sum_{k=1}^{a} \sum_{j=0}^{+\infty} \alpha_{j,k} \Big(\sum_{u=1}^{j} \frac{1}{u^k} \Big).$$

Démonstration. — La convergence absolue découle de l'hypothèse $\deg \mathrm{F} \leqslant -2$. Si $\mathrm{N} \in \mathbf{N}$ est tel que $\alpha_{j,k} = 0$ si $j \geqslant \mathrm{N}+1$, on a

$$\sum_{m=1}^{\mathrm{M}} \sum_{j=0}^{\mathrm{N}} \frac{\alpha_{j,1}}{m+j} = \Big(\sum_{j=0}^{\mathrm{N}} \alpha_{j,1} \Big) \Big(\sum_{u=1}^{\mathrm{N+M}} \frac{1}{u} \Big) - \sum_{j=0}^{\mathrm{N}} \alpha_{j,1} \Big(\sum_{u=1}^{j} \frac{1}{u} + \sum_{u=\mathrm{M}+j+1}^{\mathrm{N+M}} \frac{1}{u} \Big),$$

et comme $\sum_{j=0}^{\mathrm{N}} \alpha_{j,1} = 0$, on obtient, en faisant tendre M vers $+\infty$,

$$\sum_{m=1}^{+\infty} \sum_{j=0}^{\mathrm{N}} \frac{\alpha_{j,1}}{m+j} = -\sum_{j=0}^{\mathrm{N}} \alpha_{j,1} \Big(\sum_{u=1}^{j} \frac{1}{u} \Big).$$

D'autre part, on a

$$\begin{aligned} \sum_{m=1}^{+\infty} \sum_{j=0}^{\mathrm{N}} \sum_{k=2}^{a} \frac{\alpha_{j,k}}{(m+j)^k} &= \sum_{k=2}^{a} \sum_{j=0}^{\mathrm{N}} \sum_{u=j+1}^{+\infty} \frac{\alpha_{j,k}}{u^k} = \sum_{k=2}^{a} \sum_{j=0}^{\mathrm{N}} \alpha_{j,k} \Big(\zeta(k) - \sum_{u=1}^{j} \frac{1}{u^k} \Big) \\ &= \sum_{k=2}^{a} \alpha_k \zeta(k) - \sum_{k=2}^{a} \sum_{j=0}^{\mathrm{N}} \alpha_{j,k} \Big(\sum_{u=1}^{j} \frac{1}{u^k} \Big), \end{aligned}$$

et il n'y a plus qu'à faire la somme des deux expressions ci-dessus pour conclure.

2. Un choix judicieux de fonction rationnelle

Soient $a, r \in \mathbf{N}$ vérifiant $2r \leqslant a$ et $r \geqslant 1$. (On cherche des combinaisons linéaires à coefficients entiers entre 1 et les $\zeta(k)$, $k \leqslant a$, et r est un paramètre que l'on ajustera de

manière à ce que ces combinaisons linéaires soient les plus petites possibles.) Soit

$$\begin{aligned}\mathrm{F}_n(\mathrm{X}) &= (n!)^{a-2r}\frac{(\mathrm{X}-rn)(\mathrm{X}-rn+1)\cdots(\mathrm{X}+(r+1)n)}{(\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n))^{a+1}}\\ &= (n!)^{a-2r}\frac{(\mathrm{X}-rn)\cdots(\mathrm{X}-1)(\mathrm{X}+n+1)\cdots(\mathrm{X}+(r+1)n)}{(\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n))^{a}}.\end{aligned}$$

Soient aussi $\alpha_{j,k}^{(n)}$, pour $0\leqslant j\leqslant n$, $1\leqslant k\leqslant a$ et $\alpha_k^{(n)}$ pour $1\leqslant k\leqslant a$, les rationnels définis via la décomposition en éléments simples de $\mathrm{F}_n(\mathrm{X})$ par

$$\mathrm{F}_n(\mathrm{X})=\sum_{j=0}^{n}\sum_{k=1}^{a}\frac{\alpha_{j,k}^{(n)}}{(\mathrm{X}+j)^k}\quad\text{et}\quad\alpha_k^{(n)}=\sum_{j=0}^{n}\alpha_{j,k}^{(n)}.$$

Cette fraction rationnelle a un certain nombre de propriétés intéressantes.

• F_n est de degré $(2r+1)n+1-(n+1)(a+1)=(2r-a)n-a\leqslant -a\leqslant -2$ et a des pôles d'ordre a en $0,-1,\ldots,-n$; la série $\mathrm{S}_n=\sum_{m=1}^{+\infty}\mathrm{F}_n(m)$ converge donc absolument et on a

$$\mathrm{S}_n=\beta^{(n)}+\sum_{k=2}^{a}\alpha_k^{(n)}\zeta(k)\quad\text{avec }\beta^{(n)}=-\sum_{k=1}^{a}\sum_{j=0}^{n}\alpha_{j,k}^{(n)}\Big(\sum_{u=1}^{j}\frac{1}{u^k}\Big).$$

• $\mathrm{F}_n(1)=\cdots=\mathrm{F}_n(rn)=0$, ce qui montre que la somme définissant S_n ne commence qu'à $m=rn+1$ [i.e. $\mathrm{S}_n=\sum_{m=0}^{+\infty}\mathrm{F}_n(rn+m+1)$] et assure que S_n est petit.

• $\mathrm{F}_n(m)\geqslant 0$ si $m\geqslant 1$, ce qui assure que S_n est non nul.

• F_n vérifie l'équation fonctionnelle $\mathrm{F}_n(-n-\mathrm{X})=(-1)^{(n+1)a}\mathrm{F}_n(\mathrm{X})$, ce qui nous fournit les relations $\alpha_{n-j,k}^{(n)}=(-1)^{k+(n+1)a}\alpha_{j,k}^{(n)}$, si $1\leqslant k\leqslant a$ et $0\leqslant j\leqslant n$; ces relations impliquent que $\alpha_k^{(n)}=0$ si $k+(n+1)a$ est impair, ce qui est le point crucial pour arriver à séparer les valeurs aux entiers pairs des valeurs aux entiers impairs. (Pour ne garder que les valeurs aux entiers pairs, il suffit de prendre a pair, et pour ne garder que les valeurs aux entiers impairs, il suffit de prendre a impair et n pair.)

Pour pouvoir appliquer le critère de Nesterenko (cf. n° 5), il s'agit alors d'évaluer précisément S_n (cf. n° 4), majorer les coefficients $\alpha_k^{(n)}$ et le p.p.c.m. de leurs dénominateurs (cf. n° 3) car on a besoin de combinaisons linéaires à coefficients *entiers*.

3. Propriétés archimédiennes et arithmétiques des $\alpha_k^{(n)}$

Notons d_n le p.p.c.m. de $1,2,\ldots,n$.

Proposition E.2.2. — *Si $1\leqslant k\leqslant a$ et $0\leqslant j\leqslant n$, alors*

$$d_n^{a-k}\alpha_{k,j}^{(n)}\in\mathbf{Z}\quad\text{et}\quad|\alpha_{k,j}^{(n)}|\leqslant(2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n}.$$

Corollaire E.2.3. — (i) *$d_n^a\beta^{(n)}\in\mathbf{Z}$ et $d_n^{a-k}\alpha_k^{(n)}\in\mathbf{Z}$ si $n\in\mathbf{N}$ et $k\in\{2,\ldots,a\}$.*

(ii) *Si $\delta>2^a(r+1)^{2r+2}$, alors $|\beta^{(n)}|=\mathrm{O}(\delta^n)$ et $|\alpha_k^{(n)}|=\mathrm{O}(\delta^n)$, pour tout $k\in\{2,\ldots,a\}$.*

Démonstration. — (i) L'appartenance de $d_n^{a-k}\alpha_k^{(n)} = \sum_{j=0}^n d_n^{a-k}\alpha_{k,j}^{(n)}$ à $\mathbf{Z}$ est immédiate ; celle de $d_n^a\beta^{(n)} = -\sum_{k=1}^a \big(\sum_{j=0}^n d_n^{a-k}\alpha_{k,j}^{(n)}\big(\sum_{u=1}^j \frac{d_n^k}{u^k}\big)\big)$ résulte de ce que tous les termes du membre de droite sont entiers puisque $u \leqslant j \leqslant n$ implique $u \mid d_n$.

(ii) La proposition implique que $|\alpha_k^{(n)}| \leqslant (n+1)(2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n} = \mathrm{O}(\delta^n)$, pour tout $\delta > 2^a(r+1)^{2r+2}$. Par ailleurs, on a la majoration $\sum_{u=1}^j \frac{1}{u^k} \leqslant j \leqslant n$, et donc $|\beta^{(n)}| \leqslant a(n+1)n(2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n} = \mathrm{O}(\delta^n)$, pour tout $\delta > 2^a(r+1)^{2r+2}$.

On en déduit le corollaire.

Pour démontrer la proposition E.2.2, écrivons $\mathrm{F}_n(\mathrm{X})$ sous la forme :

$$\mathrm{F}_n(\mathrm{X}) = \prod_{i=1}^a \frac{n!\,\mathrm{P}_i(\mathrm{X})}{\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n)},$$

où $\mathrm{P}_i(\mathrm{X})$ est le polynôme défini par ($\binom{\mathrm{X}}{n}$ est le polynôme binomial $\frac{\mathrm{X}(\mathrm{X}-1)\cdots(\mathrm{X}-n+1)}{n!}$)

$$\mathrm{P}_i(\mathrm{X}) = \begin{cases} \binom{\mathrm{X}-1-(i-1)n}{n} & \text{si } 1 \leqslant i \leqslant r, \\ \binom{\mathrm{X}+(i-r+1)n}{n} & \text{si } r+1 \leqslant i \leqslant 2r, \\ 1 & \text{si } 2r+1 \leqslant i \leqslant a. \end{cases}$$

Nous aurons besoin d'un certain nombre de résultats préparatoires.

Lemme E.2.4. — *Soit $\mathrm{Q} \in \mathbf{Q}[\mathrm{X}]$, de degré $\leqslant n$, prenant des valeurs entières aux entiers et soient $(\beta_j(\mathrm{Q}))_{0\leqslant j\leqslant n}$ les rationnels définis par la décomposition en éléments simples de la fraction rationnelle*

$$\mathrm{F}(\mathrm{X}) = \frac{n!\,\mathrm{Q}(\mathrm{X})}{\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n)} = \sum_{j=0}^n \frac{\beta_j(\mathrm{Q})}{\mathrm{X}+j}$$

et $\mathrm{B}(\mathrm{Q}) = \sup_{0\leqslant j\leqslant n}|\beta_j(\mathrm{Q})|$. Alors $\beta_j \in \mathbf{Z}$ quel que soit $j \in \{0,\dots,n\}$ et $\mathrm{B}(\mathrm{Q}) \leqslant 2^n \sup_{0\leqslant j\leqslant n}|\mathrm{Q}(-j)|$.

Démonstration. — On a

$$\beta_j(\mathrm{Q}) = \lim_{\mathrm{X}\to -j}(\mathrm{X}+j)\mathrm{F}(\mathrm{X}) = (-1)^j\binom{n}{j}\mathrm{Q}(-j).$$

Lemme E.2.5. — *Soient Q_i pour $1 \leqslant i \leqslant a$ des polynômes de degrés $\leqslant n$ prenant des valeurs entières aux entiers. Soient $\alpha_{j,k}$ pour $0 \leqslant j \leqslant n$ et $1 \leqslant k \leqslant a$, définis grâce à la décomposition en élément simples de*

$$\mathrm{F}(\mathrm{X}) = \prod_{i=1}^a \frac{n!\,\mathrm{Q}_i(\mathrm{X})}{\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n)} = \sum_{j=0}^n\sum_{k=1}^a \frac{\alpha_{j,k}}{(\mathrm{X}+j)^k}.$$

Alors $d_n^{a-k}\alpha_{j,k} \in \mathbf{Z}$ et $|\alpha_{j,k}| \leqslant (2n)^{a-1}(a-1)!\prod_{i=1}^a \mathrm{B}(\mathrm{Q}_i)$, quels que soient $0 \leqslant j \leqslant n$ et $1 \leqslant k \leqslant a$.

Démonstration. — La démonstration se fait par récurrence sur a, le cas $a = 1$ étant contenu dans le lemme E.2.4. Si $a \geqslant 2$, l'hypothèse de récurrence permet d'écrire

$$\prod_{i=1}^{a-1} \frac{n!\,\mathrm{Q}_i(\mathrm{X})}{\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n)} = \sum_{j=0}^{n}\sum_{k=1}^{a-1} \frac{\gamma_{j,k}}{(\mathrm{X}+j)^k}\,,$$

avec $d_n^{a-1-k}\gamma_{j,k} \in \mathbf{Z}$ et $|\gamma_{j,k}| \leqslant (2n)^{a-2}(a-2)!\prod_{i=1}^{a-1}\mathrm{B}(\mathrm{Q}_i)$.

Maintenant, si $j_1 \neq j_2$, on a

$$\frac{1}{(\mathrm{X}+j_1)(\mathrm{X}+j_2)^\ell} = \frac{1}{(j_2-j_1)^\ell(\mathrm{X}+j_1)} - \sum_{k=1}^{\ell} \frac{1}{(j_2-j_1)^{\ell+1-k}(\mathrm{X}+j_2)^k}.$$

On en déduit la formule

$$\alpha_{j,k} = \begin{cases} \beta_j(\mathrm{P}_a)\gamma_{j,k-1} - \sum_{\ell\geqslant k}\sum_{j'\neq j}\frac{\beta_{j'}(\mathrm{P}_a)\gamma_{j,\ell}}{(j-j')^{\ell+1-k}} & \text{si } k \geqslant 2, \\ \sum_{\ell\geqslant 1}\sum_{j'\neq j}\frac{\beta_j(\mathrm{P}_a)\gamma_{j',\ell}-\beta_{j'}(\mathrm{P}_a)\gamma_{j,\ell}}{(j-j')^\ell} & \text{si } k = 1. \end{cases}$$

La somme dans le membre de droite comporte au plus $2n(a-1)$ termes et chacun de ces termes est de valeur absolue $\leqslant \mathrm{B}(\mathrm{P}_a)(2n)^{a-2}(a-2)!\prod_{i=1}^{a-2}\mathrm{B}(\mathrm{P}_i)$; on en tire la majoration voulue pour $|\alpha_{j,k}|$.

Enfin, on a

$$d_n^{a-k}\frac{\beta_{j'}(\mathrm{P}_a)\gamma_{j,\ell}}{(j-j')^{\ell+1-k}} = d_n^{a-1-\ell}\gamma_{j,\ell}\cdot\frac{d_n^{\ell+1-k}}{(j-j')^{\ell+1-k}}\cdot\beta_{j'}(\mathrm{P}_a) \in \mathbf{Z}$$

et

$$d_n^{a-k}\gamma_{j,k-1} = d_n^{a-1-(k-1)}\gamma_{j,k-1} \in \mathbf{Z},$$

et tous les termes intervenant dans le calcul de $\alpha_{j,k}$ sont entiers ; il en est donc de même de $\alpha_{j,k}$, ce qui termine la démonstration.

Lemme E.2.6. — *Si $1 \leqslant i \leqslant a$, alors P_i est de degré $\leqslant n$ et prend des valeurs entières aux entiers. De plus, on a*

$$\mathrm{B}(\mathrm{P}_i) \leqslant \begin{cases} 2^n\frac{((i+1)n)!}{(in)!n!} & \textit{si } 1 \leqslant i \leqslant r, \\ 2^n\frac{((i-r+1)n)!}{((i-r)n)!n!} & \textit{si } r+1 \leqslant i \leqslant 2r, \\ 2^n & \textit{si } 2r+1 \leqslant i \leqslant a. \end{cases}$$

Démonstration. — Les $\binom{\mathrm{X}}{n}$ prenant des valeurs entières aux entiers (cf. § 1.1 du Vocabulaire), il en est de même des P_i. La majoration de $\mathrm{B}(\mathrm{P}_i)$, quant à elle, s'obtient en en majorant le coefficient binomial $\binom{n}{j}$ par 2^n et en constatant que le maximum de $|\mathrm{P}_i(-j)|$ pour $0 \leqslant j \leqslant n$ est atteint en $j = 0$ (resp. $j = n$) si $1 \leqslant i \leqslant r$ (resp. $r+1 \leqslant i \leqslant 2r$).

La proposition E.2.2 est une conséquence des lemmes E.2.6 et E.2.5 et de la majoration

$$\prod_{i=1}^{a}\mathrm{B}(\mathrm{P}_i) \leqslant 2^{na}\Big(\frac{((r+1)n)!}{(n!)^{r+1}}\Big)^2 \leqslant 2^{na}(r+1)^{2(r+1)n},$$

la première inégalité s'obtenant en multipliant les majorations du lemme E.2.6 et la seconde en utilisant la majoration des coefficients multinomiaux (si $m_1 + \cdots + m_c = m$, alors $\frac{m!}{m_1!\cdots m_c!}$ est le coefficient de $x_1^{m_1}\cdots x_c^{m_c}$ dans le développement de $(x_1 + \cdots + x_c)^m$ et donc est $\leqslant c^m$ (poser $x_1 = \cdots = x_c = 1$) : ce coefficient est le nombre de partitions de $\{1, \ldots, m\}$ en c ensembles, le premier ayant m_1 éléments correspondant aux positions des facteurs x_1, le second m_2... ; or S_m permute ces partitions et $\sigma \in \mathrm{S}_m$ laisse fixe une partition si et seulement si elle laisse stable chacun des ensembles de la partition ; on en déduit que le stabilisateur G_p d'une telle partition p est de cardinal $m_1!\cdots m_c!$ et que le nombre de ces partitions est $\frac{|\mathrm{S}_m|}{|\mathrm{G}_p|} = \frac{m!}{m_1!\cdots m_c!}$).

4. Évaluation de S_n

Une expression de S_n sous forme d'une intégrale (prop. E.2.9) va nous permettre d'étudier le comportement asymptotique de S_n : on obtient le résultat suivant.

Proposition E.2.7. — (i) *Il existe* $\mathrm{A}_0 > 0$ *tel que* $\lim_{n\to+\infty} \mathrm{S}_n^{1/n} = \mathrm{A}_0$.
(ii) *On a* $\mathrm{A}_0 \leqslant (2r+1)^{2r+1} r^{2r-a}$.

Lemme E.2.8. — *Si* $a, b \in \mathbf{N}$, *alors* $\int_0^1 x^a(1-x)^b\,dx = \frac{a!\ b!}{(a+b+1)!}$.

Démonstration. — C'est un cas particulier de la formule $\int_0^1 x^{s-1}(1-x)^{t-1}\,dx = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$ d'Euler. (On peut aussi utiliser la formule $\int_0^1 x^a(1-x)^b\,dx = \frac{b}{a+1}\int_0^1 x^{a+1}(1-x)^{b-1}\,dx$.)

Proposition E.2.9. — *On a*

$$\mathrm{S}_n = \frac{((2r+1)n+1)!}{(n!)^{2r+1}} \int_{[0,1]^{a+1}} \frac{\prod_{\ell=1}^{a+1} x_\ell^{nr}(1-x_\ell)^n\,dx_\ell}{(1-x_1\cdots x_{a+1})^{(2r+1)n+2}}.$$

Démonstration. — Si $k \geqslant 1$ et $|x| < 1$, on a $(1-x)^{-k} = \sum_{m=0}^{+\infty} \binom{m+k-1}{k-1} x^m$. Comme toutes les fonctions considérées sont positives, on peut intervertir somme et intégrale pour obtenir

$$\begin{aligned}\int_{[0,1]^{a+1}} \frac{\prod_{\ell=1}^{a+1}\bigl(x_\ell^{nr}(1-x_\ell)^n\,dx_\ell\bigr)}{(1-x_1\cdots x_{a+1})^k} &= \sum_{m=0}^{+\infty}\binom{m+k-1}{k-1}\Bigl(\int_0^1 x^{rn+m}(1-x)^n\,dx\Bigr)^{a+1}\\ &= \sum_{m=0}^{+\infty}\frac{(m+1)\cdots(m+k-1)}{(k-1)!}\Bigl(\frac{(rn+m)!n!}{((r+1)n+m+1)!}\Bigr)^{a+1}.\end{aligned}$$

Pour $k = (2r+1)n+2$, on a

$$\frac{((2r+1)n+1)!}{(n!)^{2r+1}}\frac{(m+1)\cdots(m+k-1)}{(k-1)!}\Bigl(\frac{(rn+m)!n!}{((r+1)n+m+1)!}\Bigr)^{a+1} = \mathrm{F}_n(rn+m+1).$$

On en tire le résultat car $\mathrm{F}_n(m) = 0$ si $1 \leqslant m \leqslant rn$.

Lemme E.2.10. — *On a*

$$\lim_{n\to+\infty}\Bigl(\frac{((2r+1)n+1)!}{(n!)^{2r+1}}\Bigr)^{1/n} = (2r+1)^{2r+1}.$$

Démonstration. — C'est une conséquence du comportement asymptotique de $n!$ donné par la formule de Stirling : $n! = n^n e^{-n}\sqrt{2\pi n}(1+\mathrm{O}(\frac{1}{n}))$, cf. prop. VII.2.9.

Lemme E.2.11. — *Soient* $\mathrm{K} \subset \mathbf{R}^{a+1}$ *compact,* f *une fonction continue, positive sur* K, *et* $g \in \mathrm{L}^1(\mathrm{K})$ *une fonction positive dont l'intégrale sur tout ouvert de* K *est non nulle. Alors* $\lim_{n\to+\infty} |\int_{\mathrm{K}} f^n g\,dx|^{1/n} = \sup_{x\in\mathrm{K}} f(x)$.

Démonstration. — Soient $\mathrm{M} = \sup_{x\in\mathrm{K}} f(x)$ et $\mathrm{I}_n = \int_{\mathrm{K}} f^n\, g\, dx$.

• $\mathrm{I}_n \leqslant \mathrm{M}^n \int_{\mathrm{K}} g\,dx$, et donc $\mathrm{I}_n^{1/n} \leqslant (1+\varepsilon)\mathrm{M}$, pour tout $n \gg 0$, si $\varepsilon > 0$.

• f atteint son maximum M en un point $u \in \mathrm{K}$, et pour tout $\varepsilon > 0$, il existe un ouvert U de K, contenant u, tel que $f(x) \geqslant \mathrm{M}-\varepsilon$, pour tout $x \in \mathrm{U}$. Alors $\mathrm{I}_n \geqslant (\mathrm{M}-\varepsilon)^n \int_{\mathrm{U}} g\ dx$, et comme $\int_{\mathrm{U}} g\,dx > 0$, on a $\mathrm{I}_n^{1/n} \geqslant (1-\varepsilon)(\mathrm{M}-\varepsilon)$, pour tout $n \gg 0$.

Il s'ensuit que $\mathrm{I}_n^{1/n} \to \mathrm{M}$ quand $n \to +\infty$, ce que l'on cherchait à démontrer.

Passons à la démonstration de la prop. E.2.7. Le lemme E.2.10 et le lemme E.2.11 utilisé pour $\mathrm{K} = [0,1]^{a+1}$, $f(x) = \frac{\prod_{\ell=1}^{a+1} x_\ell^r(1-x_\ell)}{(1-x_1\cdots x_{a+1})^{2r+1}}$ et $g(x) = \frac{1}{(1-x_1\cdots x_{a+1})^2}$, montrent que

$$\lim_{n\to+\infty} \mathrm{S}_n^{1/n} = \mathrm{A}_0, \quad \text{avec } \mathrm{A}_0 = (2r+1)^{2r+1} \sup_{x\in[0,1]^{a+1}} f(x).$$

D'autre part, on a $1-x_1\cdots x_{a+1} \geqslant 1-x_\ell$ pour tout $\ell \in \{1,\dots,a+1\}$. On a donc aussi $1-x_1\cdots x_{a+1} \geqslant \prod_{\ell=1}^{a+1}(1-x_\ell)^{1/(a+1)}$, d'où la majoration $f(x) \leqslant \prod_{\ell=1}^{a+1}\big(x_\ell^r(1-x_\ell)^{\frac{a-2r}{a+1}}\big)$. Le maximum de $x \to x^r(1-x)^{\frac{a-2r}{a+1}}$ sur $[0,1]$ est atteint en $\rho = \big(1+\frac{a-2r}{r(a+1)}\big)^{-1}$; le maximum de f sur $[0,1]^{a+1}$ est donc $\leqslant \rho^{r(a+1)}(1-\rho)^{a-2r} \leqslant (1-\rho)^{a-2r}$, et on termine la démonstration de la proposition E.2.7 grâce à la majoration

$$1-\rho = 1 - \frac{1}{1+\frac{a-2r}{r(a+1)}} = \frac{\frac{a-2r}{r(a+1)}}{1+\frac{a-2r}{r(a+1)}} \leqslant \frac{a-2r}{r(a+1)} \leqslant \frac{1}{r}.$$

5. Utilisation du critère de Nesterenko

5.1. *Le plus petit commun multiple des n premiers entiers*

Pour appliquer le critère de Nesterenko, nous aurons besoin d'estimer la taille de d_n.

Proposition E.2.12. — *Il existe* $\gamma > 1$ *tel que l'on ait* $d_n = \mathrm{O}(\gamma^n)$.

Démonstration. — Les seuls nombres premiers divisant d_n sont ceux $\leqslant n$, et si $p^v | b \leqslant n$, alors $v \leqslant \big[\frac{\log n}{\log p}\big]$, et donc $v_p(d_n) = \big[\frac{\log n}{\log p}\big]$. Il en résulte que

$$\log d_n \leqslant \sum_{p\leqslant n} \big[\frac{\log n}{\log p}\big] \log p \leqslant \pi(n)\log n,$$

où $\pi(n) = |\{p \in \mathscr{P},\ p \leqslant n\}|$. Le th. des nombres premiers ($\pi(n) \sim \frac{n}{\log n}$) implique que $\log d_n \leqslant \alpha n$, pour tout $n \gg 0$, si $\alpha > 1$; on peut donc prendre $\gamma > e$ quelconque. (On peut montrer (exercice) que $\gamma > 4$ convient en utilisant le fait que le produit des nombres

premiers compris entre $m+1$ et $2m$ divise $\binom{2m}{m} \leqslant 2^{2m}$, ce qui permet de se passer du th. des nombres premiers.)

5.2. *Minoration de la dimension du* $\mathbf{Q}$*-espace vectoriel engendré par les* $\zeta(2j+1)$

Nos efforts sont récompensés par la proposition suivante qui fournit une minoration non triviale de la dimension du $\mathbf{Q}$-espace vectoriel engendré par les valeurs de la fonction zêta aux entiers pairs ou impairs.

Proposition E.2.13. — *Soit $a \geqslant 3$ un entier impair. Soit $\delta_{\mathrm{pair}}(a)$ (resp. $\delta_{\mathrm{impair}}(a)$) la dimension du sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{R}$ engendré par 1 et les $\zeta(k)$, k pair (resp. k impair), $2 \leqslant k \leqslant a$. Alors, quel que soit $r \leqslant \frac{a}{2}$, les dimensions $\delta_{\mathrm{pair}}(a)$ et $\delta_{\mathrm{impair}}(a)$ sont minorées par*

$$1 + \frac{(a-2r)\log r - a\log\gamma - (2r+1)\log(2r+1)}{a\log 2\gamma + (2r+2)\log(r+1)}.$$

Remarque E.2.14. — En prenant $r = \frac{a}{(\log a)^2} + \mathrm{O}(1)$, on voit que $\delta_{\mathrm{pair}}(a)$ et $\delta_{\mathrm{impair}}(a)$ sont minorées par $1 + \frac{\log a}{\log 2\gamma} + o(1)$; en particulier, $\delta_{\mathrm{pair}}(a)$ et $\delta_{\mathrm{impair}}(a)$ tendent vers $+\infty$, ce qui termine la démonstration du théorème E.1.1 (modulo la démonstration de la proposition).

Démonstration. — La démonstration pour $\delta_{\mathrm{pair}}(a)$ est la même (en un peu plus simple) que la démonstration pour $\delta_{\mathrm{impair}}(a)$; nous ne traiterons donc que le cas de $\delta_{\mathrm{impair}}(a)$.

Soit D_n un multiple de d_n tel que $\mathrm{D}_n = \gamma^{n+o(n)}$, où γ vérifie les conclusions de la prop. E.2.12. Soit $b = \frac{a+1}{2}$. Soient $v_1 = 1$, et $v_j = \zeta(2j-1)$ si $2 \leqslant j \leqslant b$. Soient $a_{n,1} = \mathrm{D}_{2n+1}^a \beta^{(2n+1)}$ et $a_{n,j} = \mathrm{D}_{2n+1}^a \alpha_{2j-1}^{(2n+1)}$ si $2 \leqslant j \leqslant b$. D'après la prop. E.2.3, les $a_{n,j}$ sont des entiers, et la conjonction de la prop. E.2.12 et du (ii) du cor. E.2.3 montre que

$$\sup_{1\leqslant j\leqslant b} |a_{n,j}| = \mathrm{O}(\mathrm{B}^n), \quad \text{et donc} \sum_{1\leqslant j\leqslant b} |a_{n,j}| \leqslant \mathrm{B}^{n+o(n)} \text{ pour tout } \mathrm{B} > \left(\gamma^a 2^a (r+1)^{2r+2}\right)^2.$$

D'autre part, a étant impair, on a $a_{n,1}v_1 + \cdots + a_{n,b}v_b = \mathrm{D}_{2n+1}^a \mathrm{S}_{2n+1}$ puisque $\alpha_k^{(2n+1)} = 0$ si k est pair. La conjonction des prop. E.2.7 et E.2.12 montre qu'il existe $\mathrm{A} > 0$ tel que

$$|a_{n,1}v_1 + \cdots + a_{n,b}v_b| = \mathrm{A}^{-n+o(n)} \quad \text{avec } \mathrm{A} \geqslant \left(\gamma^a (2r+1)^{2r+1} r^{2r-a}\right)^2.$$

Le critère de Nesterenko (th. E.1.3) permet de conclure.

APPENDICE F

LE PROBLÈME DES NOMBRES CONGRUENTS

Ce chapitre est une introduction à la conjecture de Birch et Swinnerton-Dyer (un des problèmes à un million de dollar), à travers le problème des nombres congruents qui est probablement le plus vieux problème non résolu à ce jour.

F.1. Courbes elliptiques et nombres congruents

1. Introduction

Définition F.1.1. — Un entier D, *sans facteur carré* (divisible par le carré d'aucun nombre premier), est *congruent*, s'il existe un triangle rectangle de cotés rationnels dont l'aire est D ; autrement dit, si et seulement s'il existe $a, b, c \in \mathbf{Q}$ avec $a^2 + b^2 = c^2$ et $\mathrm{D} = \frac{ab}{2}$.

Pour étudier les nombres congruents, on peut commencer par étudier l'ensemble des triangles rectangles à côtés rationnels, c'est-à-dire résoudre l'équation $a^2 + b^2 = c^2$ en nombres rationnels. On pose $u = \frac{a}{c}$ et $v = \frac{b}{c}$, et on est ramené à trouver les points rationnels sur le cercle $u^2 + v^2 = 1$ avec $u > 0$ et $v > 0$. Pour cela, on note t la pente de la droite joignant (u, v) à $(-1, 0)$, dont l'équation est donc $v = t(u + 1)$; on a $t \in \mathbf{Q}$ et $(u, v) = (\frac{1-t^2}{t^2+1}, \frac{2t}{t^2+1})$. En conclusion, $a, b, c \in \mathbf{Q}$ sont les côtés d'un triangle rectangle si et seulement s'il existe $t \in \mathbf{Q}$, $0 < t < 1$, tel que $a = \frac{1-t^2}{t^2+1}c$ et $b = \frac{2t}{t^2+1}c$. En posant $x = -t$ et $y = \frac{t^2+1}{c}$, ce qui précède permet presque [1] de démontrer le résultat suivant qui permet

1. La relation $\mathrm{D} = \frac{ab}{2}$ devient $\mathrm{D} = \frac{x^3-x}{y^2}$, et la condition $0 < t < 1$ équivaut à $-1 < x < 0$. On a donc démontré que D est congruent si et seulement si l'équation $\mathrm{D}y^2 = x^3 - x$ a une solution dans $\mathbf{Q}^2$ avec $-1 < x < 0$. La courbe $\mathrm{C_D}(\mathbf{R}) = \{(x, y) \in \mathbf{R}^2,\ \mathrm{D}y^2 = x^3 - x\}$ a deux composantes connexes : un ovale dans la région $-1 \leqslant x \leqslant 0$, et une courbe avec une direction asymptotique verticale dans la région $x \geqslant 1$. L'application qui, à $\mathrm{P} = (x, y) \in \mathrm{C_D}(\mathbf{R})$, associe $\mathrm{P}' = (x', y')$, intersection de la droite $(\mathrm{P}, (-1, 0))$ avec $\mathrm{C_D}$, échange les deux composantes connexes comme le montre un petit dessin (ou un calcul explicite), et envoie $\mathrm{C_D}(\mathbf{Q})$ dans lui-même comme il est expliqué au § 2 (ou comme le montre un calcul explicite). Ceci permet de montrer que l'existence d'une solution dans $\mathbf{Q}^2$ avec $-1 < x < 0$ est équivalente à celle d'une solution dans $\mathbf{Q}^2$ avec $x > 1$. On en déduit la proposition.

de rattacher le problème des nombres congruents à celui de la résolution des équations diophantiennes (cf. § F.2).

Proposition F.1.2. — *Si* D *est un entier positif sans facteur carré, alors les conditions suivantes sont équivalentes :*

(i) D *est congruent*

(ii) *L'équation* $\mathrm{D}y^2 = x^3 - x$ *a une solution dans* $\mathbf{Q}^2$ *avec* $y \neq 0$.

Déterminer si un entier est congruent ou pas, est un problème très ancien et très difficile. On a par exemple le résultat suivant « conjecturé » par Fibonacci (1175-1240).

Théorème F.1.3 (Fermat (1601-1665))**.** — 1 *n'est pas un nombre congruent.*

C'est une des nombreuses utilisations que Fermat a trouvées pour sa méthode de « la descente infinie [2] ». Remarquons que si a, b, c sont des entiers non nuls vérifiant $a^4 - b^4 = c^4$, et si $x = \frac{a^2}{b^2}$, $y = \frac{ac^2}{b^3}$, alors $y = x^3 - x$. Le fait que 1 n'est pas congruent implique donc le théorème de Fermat [3] pour l'exposant 4.

Exemple F.1.4 (Zagier). — L'entier 157 est congruent, mais le triangle (a, b, c) le plus simple d'aire 157 est

$$a = \frac{6803298487826435051217540}{411340519227716149383203}, \qquad b = \frac{411340519227716149383203}{21666555693714761309610},$$
$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Cet exemple montre que la chasse aux triangles rectangles à côtés rationnels d'aire D risque d'être un peu acrobatique... Le résultat suivant de Tunnell (1983) n'en est que plus remarquable.

Théorème F.1.5. — *Soit* D *un entier impair sans facteur carré. Si* D *est congruent, alors*

$$|\{x, y, z \in \mathbf{Z},\ 2x^2 + y^2 + 8z^2 = \mathrm{D}\}| = 2 \cdot |\{x, y, z \in \mathbf{Z},\ 2x^2 + y^2 + 32z^2 = \mathrm{D}\}|. \qquad (*)$$

Réciproquement, si D *vérifie* $(*)$*, et si* (une forme faible de) *la conjecture de Birch et Swinnerton-Dyer est vraie, alors* D *est congruent.*

Il y a un résultat similaire pour D pair. Comme il est très facile [4] de décider si D vérifie ou non $(*)$, cela fournit un critère effectif permettant de décider qu'un nombre donné est non congruent, ou (sous Birch et Swinnerton-Dyer) congruent, et ce, sans exhiber de triangle rectangle d'aire D. Un entier congru à 5 ou 7 modulo 8 vérifie $(*)$ car les deux ensembles sont vides, mais on ne sait pas montrer que cela implique que D est congruent...

2. Cette méthode fait l'objet du prob. H.14 ; en spécialisant ce problème au cas $\mathrm{D} = 1$, on obtient une démonstration du résultat de Fermat (on n'a besoin que des parties III et IV).

3. Il semble que Fermat se soit légèrement laissé emporté par son enthousiasme devant cette découverte...

4. Le lecteur pourra s'en convaincre en en déduisant le th. F.1.3.

Comme le lecteur le constatera, la démonstration de ce théorème emprunte des chemins très détournés (ce qui en fait le charme) ; on peut légitimement se demander si une preuve plus directe ne serait pas possible, maintenant qu'on connaît la réponse.

2. Arithmétique des courbes elliptiques

Si C est une conique, on peut étudier l'ensemble $C(\mathbf{Q})$, des points de C à coordonnées rationnelles, comme on l'a fait pour le cercle. On trouve un point $P \in C(\mathbf{Q})$ sur la conique et on paramêtre les points de la conique par la pente d'une droite variable passant par P. Cette stratégie ne marche plus pour une courbe C donnée par une équation de degré 3 (comme la courbe C_D d'équation $Dy^2 = x^3 - x$) car, si on coupe par une droite passant par un point de $C(\mathbf{Q})$, et qu'on élimine y entre les deux équations, on obtient une équation de degré 3 en x dont on sait seulement qu'une des solutions est rationnelle ; les deux autres vivent donc, en général, dans une extension quadratique de $\mathbf{Q}$, mais pas dans $\mathbf{Q}$. Par contre, si on prend une droite passant par deux points rationnels de C ou tangente à un point rationnel de C, alors on obtient une équation dont deux des solutions (ou une solution double) sont rationnelles ; comme la somme des racines est aussi rationnelle, cela montre que cette droite recoupe C en un point rationnel.

Une *courbe elliptique* E sur un corps [5] K est une courbe d'équation $y^2 = P(x)$, avec $P \in K[X]$, de degré 3, sans racine double [6] On note $E(K)$ l'ensemble des solutions dans K^2 de $y^2 = P(x)$, et $\overline{E}(K) = E(K) \cup \{\infty\}$, avec la convention qu'une droite passe par ∞ si et seulement si elle est verticale [7]. On munit $\overline{E}(K)$ d'une loi de composition + qui en fait un groupe commutatif [8] avec ∞ comme élément neutre et $P + Q + R = \infty$ si et seulement si (P, Q, R) sont alignés (avec les conventions évidentes si deux ou trois des points sont confondus ; en particulier, P est d'ordre 2 si et seulement si ∞ appartient à la tangente à E en P, c'est-à-dire si et seulement si $y = 0$; de même, P est d'ordre 3 si et seulement si la tangente en P à E a un contact d'ordre 3).

5. Si K est de caractéristique 2, il faut aussi permettre des équations du type $y^2 + y = P(x)$.

6. Ceci se traduit par la non nullité du discriminant $\Delta(P)$ de P (cf. alinéa 9.2.1 du Vocabulaire).

7. Cette définition de $\overline{E}(K)$ est parfaitement artificielle. Une définition naturelle demande de travailler dans le plan projectif $\mathbf{P}^2$, espace des droites de l'espace vectoriel de dimension 3. Celui-ci peut être vu comme la réunion du plan affine et d'une droite (projective) à l'infini dont les points correspondent aux directions de droites du plan affine ; notre ∞ est le point de cette droite à l'infini correspondant à la direction verticale.

8. L'associativité n'est pas une évidence. Elle peut se vérifier par un calcul explicite assez pénible (mais on peut demander l'aide d'un ordinateur...). Une solution plus élégante consiste, si K est un sous-corps de $\mathbf{C}$, à passer par les fonctions elliptiques (cf. prob. H.8), ce qui permet de montrer que $\overline{E}(\mathbf{C})$ est isomorphe, en tant que groupe, à $\mathbf{C}/\Lambda$, où Λ est un réseau de $\mathbf{C}$ (pour pouvoir utiliser les résultats du prob. H.8, il faut savoir que si le discriminant de $X^3 - aX - b$ est non nul, il existe un réseau Λ de $\mathbf{C}$ tel que $g_2(\Lambda) = a$ et $g_3(\Lambda) = b$; cela se démontre en utilisant la surjectivité de l'invariant modulaire j (ex. VII.6.7) et l'homogénéité de g_2 et g_3 qui permet d'exprimer g_2 et g_3 en fonction de G_4 et G_6). Dans le cas général, il y a une jolie démonstration passant par la géométrie projective.

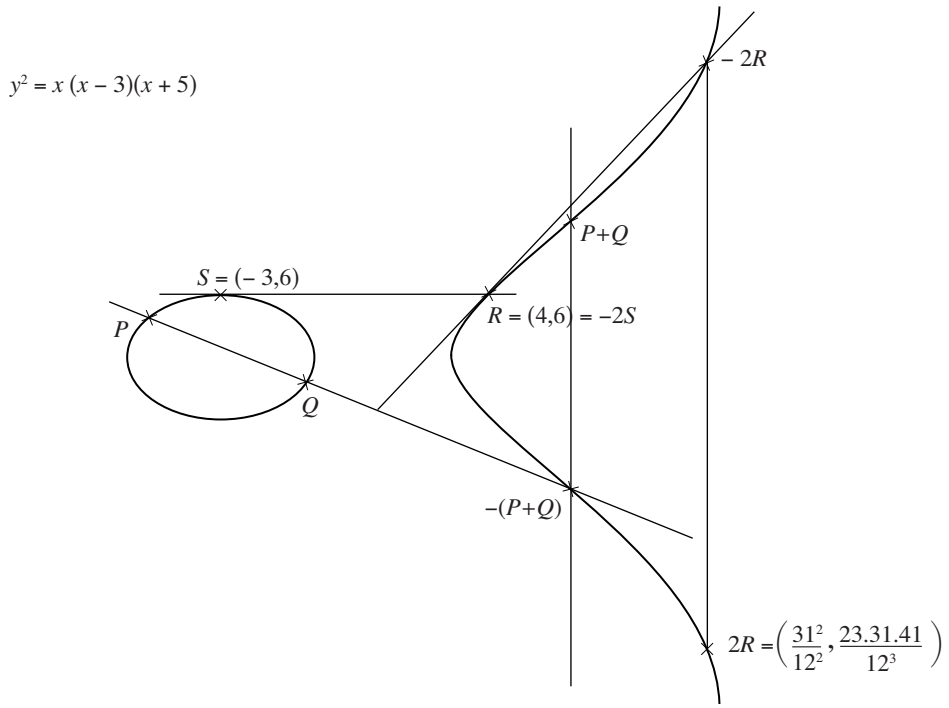


FIGURE 1. Addition sur la courbe elliptique d'équation $\mathrm{Y}^2 = \mathrm{X}(\mathrm{X}-3)(\mathrm{X}+5)$.

Théorème F.1.6. — *Si* E *est une courbe elliptique sur* $\mathbf{Q}$*, le groupe* $\overline{\mathrm{E}}(\mathbf{Q})$ *est engendré par un nombre fini d'éléments ; il est donc isomorphe à* $\overline{\mathrm{E}}(\mathbf{Q})_{\mathrm{tors}} \oplus \mathbf{Z}^{r(\mathrm{E})}$*, où* $\overline{\mathrm{E}}(\mathbf{Q})_{\mathrm{tors}}$*, sous-groupe des points d'ordre fini*[9]*, est un groupe fini, et* $r(\mathrm{E}) \in \mathbf{N}$*.*

Ce résultat, conjecturé par Poincaré vers 1900, a été démontré par Mordell en 1922 en adaptant la méthode de la descente infinie[10] de Fermat ; c'est un cas particulier du célèbre théorème de Mordell-Weil. Le groupe $\overline{\mathrm{E}}(\mathbf{Q})_{\mathrm{tors}}$ se calcule très facilement ; par contre la détermination du *rang* $r(\mathrm{E})$ et des générateurs de $\mathbf{Z}^{r(\mathrm{E})}$ est très délicate. À ce jour, il n'y a pas d'algorithme dont on peut prouver qu'il va permettre de les déterminer, ce qui ne nous arrange pas en ce qui concerne le problème des nombres congruents, mais la conjecture de Birch et Swinnerton-Dyer, dont il sera question plus loin, fournirait un tel algorithme si elle était démontrée.

Exemple F.1.7. — On note $\mathrm{C_D}$ la courbe elliptique d'équation $\mathrm{D}y^2 = x^3 - x$. Alors $\mathrm{Q}_1 = (-1,0)$, $\mathrm{Q}_2 = (0,0)$ et $\mathrm{Q}_3 = (1,0)$ sont d'ordre 2, et $\overline{\mathrm{C}}_{\mathrm{D}}(\mathbf{Q})_{\mathrm{tors}} = \{\infty, \mathrm{Q}_1, \mathrm{Q}_2, \mathrm{Q}_3\}$. En conséquence, D est congruent si et seulement si $r(\mathrm{C_D}) \geqslant 1$.

9. Si K est un sous-corps de C, et si $\overline{\mathrm{E}}(\mathbf{C}) \cong \mathbf{C}/\Lambda$, alors le sous-groupe des points de n-torsion de $\overline{\mathrm{E}}(\mathrm{K})$ s'identifie à un sous-groupe de $\frac{1}{n}\Lambda/\Lambda \cong (\mathbf{Z}/n\mathbf{Z})^2$; en particulier il est de cardinal $\leqslant n^2$.

10. Le cas particulier de $\mathrm{C_D}$ fait l'objet du problème H.14.

3. L'heuristique de Birch et Swinnerton-Dyer

Si p est un nombre premier, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est un corps. Si $r = \frac{a}{b} \in \mathbf{Q}$ et p ne divise pas b, on peut voir r comme un élément de $\mathbf{F}_p$ en réduisant a et b modulo p (i.e. en prenant le quotient des images de a et b dans $\mathbf{F}_p$, ce qui ne dépend pas des choix de a et b). En particulier, si E est une courbe elliptique sur $\mathbf{Q}$ d'équation $y^2 = \mathrm{P}(x)$, on peut aussi considérer E comme une courbe elliptique sur $\mathbf{F}_p$ pour tous les *bons* nombres premiers (ceux ne divisant ni les dénominateurs des coefficients de P, ni le numérateur de son discriminant (note 6)).

Si E est une courbe elliptique [11] sur $\mathbf{F}_p$, on a trivialement, $|\overline{\mathrm{E}}(\mathbf{F}_p)| \leqslant 2p+1$, mais on dispose du résultat plus précis suivant.

Théorème F.1.8 (Hasse, 1933)**.** — *Si* E *est une courbe elliptique sur* $\mathbf{F}_p$*, et si on pose* $a_p = p + 1 - |\overline{\mathrm{E}}(\mathbf{F}_p)|$*, alors* $|a_p| \leqslant 2\sqrt{p}$

L'idée de Birch et Swinnerton-Dyer (1960-1965), est que, si $r(\mathrm{E}) \geqslant 1$, alors il devrait y avoir en moyenne plus de points dans $\mathrm{E}(\mathbf{F}_p)$ que si $r(\mathrm{E}) = 0$, à cause de la réduction modulo p des éléments de $\mathrm{E}(\mathbf{Q})$. Comme ce nombre de points est a peu près p d'après le théorème de Hasse, le produit $\prod_p \frac{p}{|\overline{\mathrm{E}}(\mathbf{F}_p)|}$ devrait avoir des chance de diverger (d'être nul), si $r(\mathrm{E}) \geqslant 1$, et de converger, si $r(\mathrm{E}) = 0$. Comme le produit n'est pas convergent au sens usuel, nous allons devoir passer par les fonctions holomorphes pour donner corps à cette heuristique.

4. Fonction L d'une courbe elliptique

Soit E une courbe elliptique sur $\mathbf{Q}$. Si p est un bon nombre premier, soit a_p l'entier défini par $a_p = 1 + p - |\overline{\mathrm{E}}(\mathbf{F}_p)|$. On définit la [12] fonction $\mathrm{L}(\mathrm{E}, s)$, et des entiers a_n, pour $n \in \mathbf{N} - \{0\}$, par

$$\mathrm{L}(\mathrm{E}, s) = \prod_{p \text{ bon}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

Il est facile de voir que le produit converge pour $\mathrm{Re}(s) > 2$, et même $\mathrm{Re}(s) > \frac{3}{2}$ si on utilise la majoration $|a_p| \leqslant 2\sqrt{p}$ de Hasse, et définit une fonction holomorphe sur ce demi-plan.

11. On peut aussi considérer des courbes elliptiques sur $\mathbf{Z}/\mathrm{D}\mathbf{Z}$, où D n'est pas premier, ou sur $\mathbf{F}_q$. Ceci est utilisé pour factoriser des grands nombres, prouver la primalité de grands nombres (de plus de 1000 chiffres), ou pour fabriquer des signatures plus sures, à taille égale, que celles fournies par $\mathbf{F}_q^*$.

12. Cette fonction n'est pas celle qui est habituellement considérée ; elle en diffère par la multiplication par des facteurs en les mauvais p, mais comme ceux-ci ne s'annulent pas en $s = 1$, cela ne change rien en ce qui concerne la conjecture de Birch et Swinnerton-Dyer. La bonne fonction $\mathrm{L}(\mathrm{E}, s)$ a une équation fonctionnelle plus sympathique que celle considérée dans cet article : il existe $\varepsilon \in \{\pm 1\}$ et $\mathrm{N} \in \mathbf{N}$ tel que, si $\Lambda(\mathrm{E}, s) = \frac{\Gamma(s)}{(2\pi)^s}\mathrm{N}^{s/2}\mathrm{L}(\mathrm{E}, s)$, alors $\Lambda(\mathrm{E}, 2-s) = \varepsilon\Lambda(\mathrm{E}, s)$; en particulier, si $\varepsilon = -1$, alors $r_\infty(\mathrm{E})$ est impair et $\mathrm{L}(\mathrm{E}, 1) = 0$.

Théorème F.1.9. — *La fonction* $\mathrm{L}(\mathrm{E}, s)$ *admet un prolongement analytique à* $\mathbf{C}$ *tout entier.*

Ce résultat a été conjecturé par Hasse vers 1935 ; c'est un cas particulier de la conjecture de Hasse-Weil. Le premier résultat dans sa direction est celui, dû à Weil (1952), de la famille [13] des courbes $\mathrm{C_D}$. Shimura (1958), inspiré par des travaux d'Eichler (1954), a démontré de nombreux cas de cette conjecture en utilisant la théorie des formes modulaires dont il sera question plus loin. Le pas le plus important a été accompli par Wiles en 1994, dans sa quête de la démonstration du théorème de Fermat, qui a démontré cette conjecture dans le cas où E est d'équation $y^2 = \mathrm{P}(x)$ et P a toutes ses racines dans $\mathbf{Q}$. Le cas général a finalement été résolu par Breuil, Conrad, Diamond et Taylor en 1999.

La quantité $\prod_{p \text{ bon}} \frac{p}{|\overline{\mathrm{E}}(\mathbf{F}_p)|}$ apparaissant dans l'heuristique de Birch et Swinnerton-Dyer est, au moins formellement, égale à $\mathrm{L}(\mathrm{E}, 1)$, et leur heuristique devient :

Conjecture F.1.10 (Birch et Swinnerton-Dyer (forme faible))
« $r(\mathrm{E}) \geqslant 1$ » *si et seulement si* « $\mathrm{L}(\mathrm{E}, 1) = 0$ ».

On peut préciser cet énoncé [14]. Notons $r_\infty(\mathrm{E})$ l'ordre du zéro en $s = 1$ de $\mathrm{L}(\mathrm{E}, s)$. La conjecture de Birch et Swinnerton-Dyer prend alors la forme suivante.

Conjecture F.1.11. — (Birch et Swinnerton-Dyer) *On a l'égalité* $r(\mathrm{E}) = r_\infty(\mathrm{E})$.

---

13. Dans ce cas, on définit $\delta : \mathbf{Z}[i] \to \{0, 1, i, -1, -i\}$ par

$$\begin{cases} \delta(\omega) = 0 & \text{si } \omega \text{ est divisible par } 1+i \text{ dans } \mathbf{Z}[i], \\ \omega\delta(\omega) - 1 \text{ est divisible par } (1+i)^3 & \text{sinon.} \end{cases}$$

On a alors

$$\mathrm{L}(\mathrm{C}_1, s) = \frac{1}{4} \sum_{\omega \in \mathbf{Z}[i] - \{0\}} \frac{\omega\delta(\omega)}{|\omega|^{2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

Le cas D général se déduit facilement du cas $\mathrm{D} = 1$: on a $\mathrm{L}(\mathrm{C_D}, s) = \sum_{n=1}^{+\infty} \chi_\mathrm{D}(n) a_n n^{-s}$, où $\chi_\mathrm{D} : \mathbf{Z} \to \{-1, 0, 1\}$ est le symbole de Legendre modulo D. Ce symbole de Legendre est caractérisé par les propriétés suivantes : $\chi_\mathrm{D}(n + 4\mathrm{D}) = \chi_\mathrm{D}(n)$, $\chi_\mathrm{D}(n) = 0$ si $(\mathrm{D}, n) \neq 1$, et

$$\chi_\mathrm{D}(nm) = \chi_\mathrm{D}(n)\chi_\mathrm{D}(m), \quad \chi_\mathrm{D}(p) = \begin{cases} 1 & \text{si D est un carré dans } \mathbf{F}_p^*, \\ -1 & \text{si D n'est pas un carré dans } \mathbf{F}_p^*. \end{cases}$$

L'existence de χ_D est une conséquence de la loi de réciprocité quadratique conjecturée par Euler en 1783 et démontrée par Gauss en 1801.

14. En fait, Birch et Swinnerton-Dyer avaient été plus optimistes et avaient conjecturé que

$$\prod_{p \text{ bon}, \ p \leqslant x} \frac{p}{|\overline{\mathrm{E}}(\mathbf{F}_p)|} \sim \mathrm{C}(\log x)^{-r(\mathrm{E})}.$$

Goldfeld (1982) a prouvé que, si c'est le cas, alors $r_\infty(\mathrm{E}) = r(\mathrm{E})$, la fonction $\mathrm{L}(\mathrm{E}, s)$ vérifie l'hypothèse de Riemann (i.e. elle ne s'annule pas pour $\mathrm{Re}(s) > 1$), mais, de manière surprenante, que l'on a $\mathrm{C} = \frac{\mathrm{L}(\mathrm{E},1)}{\sqrt{2}}$ au lieu de $\mathrm{C} = \mathrm{L}(\mathrm{E}, 1)$, si $r(\mathrm{E}) = 0$.

C'est sous cette forme que le problème vaut un million de dollar. Il y a en fait une forme plus précise [15] de cette conjecture (donnant une formule pour $\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}(\mathrm{E},s)$), et plus générale ($\mathbf{Q}$ peut être remplacé par une extension finie, ou même par des corps de caractéristique p, extensions finies du corps $\mathbf{F}_p(\mathrm{T})$).

Les résultats sont peu nombreux ; ce sont les suivants.

• Coates et Wiles (1977) ont démontré que, si $\mathrm{E}=\mathrm{C_D}$ (ou si E est une courbe elliptique sur $\mathbf{Q}$ à multiplication complexe [16]), alors « $\mathrm{L}(\mathrm{E},1)\neq 0$ » ⇒ « $r(\mathrm{E})=0$ ».

• Gross et Zagier (1983) ont donné une formule explicite [17] pour $\mathrm{L}'(\mathrm{E},1)$ en termes de certains points rationnels sur E, dits « de Heegner », et qui sont construits de manière purement analytique (ce sont ces points qui permettent d'amuser la galerie en exhibant des triangles rectangles à côtés rationnels avec un nombre astronomique de chiffres). Comme conséquence, ils obtiennent l'implication : « $r_\infty(\mathrm{E})=1$ » ⇒ « $r(\mathrm{E})\geqslant 1$ ».

• Kolyvagin (1989) a démontré, en utilisant ces points de Heegner, l'implication suivante « $r_\infty(\mathrm{E})\leqslant 1$ » ⇒ « $r(\mathrm{E})=r_\infty(\mathrm{E})$ ».

C'est tout ! On est dans la situation paradoxale où plus il est censé y avoir de points rationnels ($r_\infty(\mathrm{E})\geqslant 2$), moins on sait en construire... Mentionnons quand-même, qu'en général, le rang $r(\mathrm{E})$ est égal à 0 ou 1, mais il y a tout lieu de croire que $r(\mathrm{E})$ peut prendre des valeurs arbitrairement grandes. Le record actuel est détenu par Elkies (2006) avec une courbe vérifiant $r(\mathrm{E})\geqslant 28$; Bhargava et Shankar ont démontré (2011) que le rang moyen est $\leqslant 0,98$ (il s'agit de la moyenne, quand $\mathrm{M}\to+\infty$, des rangs des courbes elliptiques $y^2=x^3+\mathrm{A}x+\mathrm{B}$, avec $\sup(\mathrm{B}^2,\mathrm{A}^3)\leqslant \mathrm{M}$).

5. La stratégie de Tunnell

Le théorème de Coates-Wiles mentionné ci-dessus fournit un critère pour que D ne soit pas congruent : il suffit que $\mathrm{L}(\mathrm{C_D},1)\neq 0$. Réciproquement, si la conjecture de Birch et Swinnerton-Dyer est vraie (même sous sa forme faible), alors la nullité de $\mathrm{L}(\mathrm{C_D},1)$ implique que D est congruent. C'est le point de départ de la démonstration du théorème de Tunnell. Le problème est donc de calculer $\mathrm{L}(\mathrm{C_D},1)$ et de décider si ce nombre est

15. Celle-ci prend la forme $\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}(\mathrm{E},s)=|Ш(\mathrm{E})|\cdot \mathrm{R}_\infty(\mathrm{E})\cdot\Omega_\infty(\mathrm{E})\cdot\prod_{p\text{ mauvais}} c_p$, où c_p est un nombre rationnel explicite, $\Omega_\infty(\mathrm{E})$ est la période réelle de E (donnée par $\Omega_\infty(\mathrm{E})=2\int_\alpha^{+\infty}\frac{dx}{\sqrt{\mathrm{P}(x)}}$, si E est d'équation $y^2=\mathrm{P}(x)$ et α est la plus grande racine réelle de P), $\mathrm{R}_\infty(\mathrm{E})$ est un « régulateur » mesurant la taille des générateurs de $\overline{\mathrm{E}}(\mathbf{Q})$, et $Ш(\mathrm{E})$, le *groupe de Tate-Shafarevich* de E, est un groupe mystérieux, *conjecturalement* fini.

16. Si $(x,y)\in \mathrm{C_D}(\mathbf{C})$, alors $(-x,iy)\in \mathrm{C_D}(\mathbf{C})$. Si Λ est le réseau de $\mathbf{C}$ correspondant à $\overline{\mathrm{C}}_\mathrm{D}(\mathbf{C})$ (cf. note 8), la remarque précédente se traduit par le fait que $i\Lambda=\Lambda$. On dit qu'une courbe elliptique E définie sur un sous-corps de $\mathbf{C}$ *a de la multiplication complexe* si, Λ étant le réseau de $\mathbf{C}$ qui lui correspond, il existe $\tau\in\mathbf{C}-\mathbf{R}$ tel que $\tau\Lambda\subset\Lambda$ (c'est donc le cas de $\mathrm{C_D}$, avec $\tau=i$) ; un tel τ est alors racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbf{Z}$.

17. La démonstration de cette formule occupe une centaine de pages...

nul ou pas. Il y a deux problèmes sérieux qui se posent : le produit définissant $\mathrm{L}(\mathrm{C}_\mathrm{D}, 1)$ converge beaucoup trop lentement (s'il converge..., cf. note 14) pour qu'on puisse l'utiliser pour le calcul de $\mathrm{L}(\mathrm{C}_\mathrm{D}, 1)$, et de toute façon, il est impossible de prouver qu'un nombre réel est nul en le calculant de manière approchée, sauf si on sait par ailleurs qu'il s'agit d'un entier. La solution que Tunnell apporte à ces deux problèmes est particulièrement élégante.

On note $\mathscr{H} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$ le demi-plan de Poincaré. On pose $q = e^{2i\pi z}$, et on définit $\Theta : \mathscr{H} \to \mathbf{C}$ par

$$\Theta(z) = \sum_{n \in \mathbf{Z}} q^{n^2}.$$

Le résultat que démontre Tunnell est alors le suivant.

Théorème F.1.12. — (Tunnell) *Soit* $\Omega = \int_1^{+\infty} \frac{dx}{\sqrt{x^3 - x}}$, *et soit* $\sum_{n=0}^{+\infty} b_n q^n$ *le développement de*

$$\Theta(z) \cdot \Theta(2z) \cdot (2\Theta(32z) - \Theta(8z)),$$

alors, si D *est impair* (il y a une formule similaire pour les entiers pairs) *sans facteur carré,*

$$\mathrm{L}(\mathrm{C}_\mathrm{D}, 1) = \frac{\Omega}{16\sqrt{\mathrm{D}}} \cdot b_\mathrm{D}^2.$$

Comme b_D est la différence des deux termes apparaissant dans la condition $(*)$ du th. F.1.5, cela explique comment ledit théorème peut se déduire du théorème de Coates-Wiles. La démonstration du théorème F.1.12 repose sur la théorie des formes modulaires dont il est question au § suivant.

6. Formes modulaires

Si f est holomorphe sur $\mathscr{H}$ et vérifie $f(z+1) = f(z)$, alors f a un développement de Fourier (q-développement, cf. ex. VI.3.4) :

$$f(z) = \sum_{n \in \mathbf{Z}} a_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

On dit que f est à croissance lente à l'infini si $a_n = 0$ pour tout $n < 0$ et s'il existe $\mathrm{C} \in \mathbf{R}$ tel que $a_n = \mathrm{O}(n^\mathrm{C})$.

Si N est un entier, on note $\Gamma_0(\mathrm{N})$ le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ des $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec c divisible par N. On note $\mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Définition F.1.13. — Si $k \in \frac{1}{2}\mathbf{N}$ et $j : \Gamma_0(\mathrm{N}) \to \{\text{racines de l'unité}\}$ vérifie $j(\mathrm{T}) = 1$, l'espace $\mathrm{M}_k(\Gamma_0(\mathrm{N}), j)$ des formes modulaires de poids k et type j pour $\Gamma_0(\mathrm{N})$ est l'espace des fonctions f, holomorphes sur $\mathscr{H}$, vérifiant

$$f\Big(\frac{az+b}{cz+d}\Big) = j\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(cz+d)^k f(z), \quad \text{quels que soient } z \in \mathscr{H} \text{ et } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathrm{N}),$$

et qui sont à croissance lente à l'infini.

Remarque F.1.14. — (i) Il n'est pas du tout clair que de telles formes existent ; et de fait, il faut choisir correctement la fonction j pour $\mathrm{M}_k(\Gamma_0(\mathrm{N}), j)$ soit non nul.

(ii) $\mathrm{M}_k(\Gamma_0(\mathrm{N}), j)$ est un $\mathbf{C}$-espace vectoriel de dimension finie $\leqslant 1 + \frac{\mathrm{N}k}{12}\prod_{p|\mathrm{N}}(1+\frac{1}{p})$.

(iii) Les formes modulaires ont un don d'ubiquité assez remarquable. On les rencontre en théorie des nombres, en combinatoire ou en physique théorique, bien que ce soient des objets définis de manière purement analytique.

Pour un aperçu de la théorie des formes modulaires pour $\mathbf{SL}_2(\mathbf{Z})$, le lecteur est invité à se reporter aux exercices VII.6.1-VII.6.11 du chap. VII.

• La fonction $\theta(z) = \Theta(\frac{z}{2})$ est étudiée dans l'ex. VII.6.6, et les résultats de cet exercice montrent que Θ est une forme modulaire de poids $\frac{1}{2}$ pour $\Gamma_0(4)$ et un j un peu compliqué.

• Si k est un entier pair $\geqslant 3$, la série d'Eisenstein $\mathrm{G}_k(z) = \frac{(k-1)!}{2\cdot(2i\pi)^k}\sum'_{m,n}\frac{1}{(mz+n)^k}$ fait l'objet des ex. VII.6.4 et VII.6.5 ; elle appartient à $\mathrm{M}_k(\mathbf{SL}_2(\mathbf{Z}), 1)$, et son q-développement est donné par $\mathrm{G}_k = \frac{(k-1)!\zeta(k)}{(2i\pi)^k} + \sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n$, où $\sigma_t(n) = \sum_{d|n,\, d\geqslant 1} d^t$, si $t \in \mathbf{C}$ et $n \in \mathbf{N} - \{0\}$.

• La fonction $\mathrm{G}_2 = \frac{\zeta(2)}{(2i\pi)^2} + \sum_{n=1}^{+\infty}\sigma_1(n)q^n$ est étudiée dans l'ex. VII.6.7. Elle n'est pas modulaire, mais presque, et $4\mathrm{G}_2(4z) - \mathrm{G}_2(z)$ est modulaire.

Comme échauffement pour le théorème de Tunnell, mentionnons (cf. ex. VII.6.9) l'identité de Jacobi (1829) : $4\mathrm{G}_2(4z) - \mathrm{G}_2(z) = \frac{3\zeta(2)}{(2i\pi)^2}\Theta^4$, qui se démontre en constatant que les deux membres appartiennent à $\mathrm{M}_2(\Gamma_0(4), 1)$ qui est de dimension 2, et que la différence est divisible par q^2. On en tire, en comparant les q-développements, une forme effective du théorème des 4 carrés de Lagrange (1770).

$$|\{(a,b,c,d) \in \mathbf{Z}^4,\ a^2+b^2+c^2+d^2 = n\}| = 8\sum_{d|n,\, 4\nmid d} d.$$

7. Courbes elliptiques et formes modulaires

Théorème F.1.15. — *Si* E *est une courbe elliptique définie sur* $\mathbf{Q}$ *et* $\mathrm{L}(\mathrm{E}, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$, *alors* $f = \sum_{n=1}^{+\infty} a_n q^n \in \mathrm{M}_2(\mathrm{N}_\mathrm{E}, 1)$, *où* N_E *est un entier explicite ne dépendant que des* p *mauvais.*

Autrement dit, *une courbe elliptique définie sur* $\mathbf{Q}$ *est modulaire.* Ce résultat, conjecturé de manière vague par Taniyama en 1956, et précisé par Weil en 1966 suite aux travaux de Shimura sus-mentionnés, est celui que démontrent Wiles [18] (dans un cas particulier)

18. Si $a^p + b^p = c^p$ est un contre-exemple au théorème de Fermat, on peut considérer la courbe elliptique introduite par Hellegouarch et Frey, d'équation $y^2 = x(x-a^p)(x+b^p)$. Wiles montre que cette courbe est modulaire, ce qui est en contradiction avec la « conjecture ε » de Serre (1984) démontrée par Ribet (1988). La « conjecture ε » décrit les congruences que l'on peut attendre entre formes modulaires. Dans le cas qui nous intéresse, cette conjecture prédit une congruence modulo p entre le q-développement de la forme modulaire attachée à la courbe elliptique $y^2 = x(x-a^p)(x+b^p)$, et celui de $g \in \mathrm{M}_2(\Gamma_0(2), 1)$, ce qui n'est pas possible car cet espace est de dimension 1, et la divisibilité par p du terme constant du q-développement de g entraine celle de tous les termes du q-développement.

et Breuil-Conrad-Diamond-Taylor. Le prolongement analytique de $\mathrm{L}(\mathrm{E}, s)$ s'en déduit en utilisant la formule (cf. ex. VII.6.3)

$$\mathrm{L}(\mathrm{E}, s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{+\infty} f(iy) y^s \frac{dy}{y},$$

ce qui permet d'utiliser les propriétés analytiques de f pour étudier $\mathrm{L}(\mathrm{E}, s)$. C'est un cas particulier de la philosophie de Langlands sur les fonctions L arithmétiques (elle devraient provenir de *formes automorphes*, généralisations des formes modulaires, et donc avoir des tas de propriétés mirifiques). Dans le cas de la courbe $\mathrm{C_D}$, la forme modulaire que l'on obtient est une combinaison linéaire de fonctions thêta.

La modularité d'une courbe elliptique E en fournit une description analytique en termes du demi-plan de Poincaré. Ceci est à la base de la construction des points de Heegner (ce sont les images [19] des points $\tau \in \mathscr{H}$ solutions d'une équation du second degré à coefficients dans $\mathbf{Q}$) qui, comme nous l'avons déjà mentionné, jouent un rôle essentiel dans la démonstration du résultat de Kolyvagin ($r(\mathrm{E}) = r_\infty(\mathrm{E})$ si $r_\infty(\mathrm{E}) \leqslant 1$) ; ce résultat n'est donc devenu valable pour toutes les courbes elliptiques sur $\mathbf{Q}$ que depuis les travaux de Wiles et Breuil-Conrad-Diamond-Taylor.

Une autre application de la modularité des courbes elliptiques est le résultat suivant qui permet, modulo un calcul numérique, de déterminer la valeur de $\mathrm{L}(\mathrm{E}, 1)$, ce qui fournit, modulo la conjecture de Birch et Swinnerton-Dyer (sous sa forme faible), un algorithme pour décider de l'existence de solutions en nombres rationnels pour une équation $y^2 = \mathrm{P}(x)$, avec P de degré 3.

Corollaire F.1.16. — (Manin-Drinfeld, 1973) *Si* E *est d'équation* $y^2 = \mathrm{P}(x)$*, et si* α *est la plus grande racine réelle de* P*, alors*

$$\Big(\int_\alpha^{+\infty} \frac{dx}{\sqrt{\mathrm{P}(x)}} \Big)^{-1} \mathrm{L}(\mathrm{E}, 1)$$

est un nombre rationnel de dénominateur explicite.

Le point de départ de la démonstration du théorème F.1.12 est un théorème de Waldspurger (1979). Si $f = \sum_{n=1}^{+\infty} a_n q^n \in \mathrm{M}_{2k}(\Gamma_0(\mathrm{N}), 1)$, k entier, si D est sans facteur carré et premier à N, et si χ_D est le caractère de Legendre (cf. note 13), on peut montrer que $f \otimes \chi_\mathrm{D}$, défini par $f \otimes \chi_\mathrm{D} = \sum \chi_\mathrm{D}(n) a_n q^n$, est un élément de $\mathrm{M}_{2k}(\Gamma_0(\mathrm{ND}^2), 1)$. Le théorème de Waldspurger dit, de manière vague, que les $\mathrm{L}(f \otimes \chi_\mathrm{D}, k)$ sont, quand D varie, les carrés de coefficients de Fourier de formes modulaires de poids $k + \frac{1}{2}$ pour $\Gamma_0(\mathrm{N}')$, avec N' explicite. « Il n'y a plus qu'à » exhiber une base de l'espace de ces formes modulaires et calculer quelques coefficients pour obtenir une identité valable pour tout D.

19. La théorie de la multiplication complexe (note 16) permet de déterminer le corps de définition de ces points ; ce sont, d'après un théorème de Schneider (1937), les seuls éléments de $\mathscr{H}$, algébriques sur $\mathbf{Q}$, qui fournissent des points algébriques de E.

F.2. Équations diophantiennes

1. Généralités

1.1. *Exemples.* — Traditionnellement, une *équation diophantienne* est une équation polynomiale P (en une ou plusieurs variables) à coefficients entiers (comme $X^2 = 2$, $DY^2 = X^3 - X$, $X^n + Y^n = Z^n$, $X^2 + Y^2 + Z^2 = 8n + 7$, etc.), et on s'intéresse à l'ensemble $V_P(\mathbf{Z})$ des solutions en nombres entiers ou à celui $V_P(\mathbf{Q})$ des solutions en nombres rationnels. Plus généralement, on peut considérer une équation polynomiale P à coefficients dans un anneau A, et, pour toute A algèbre B (i.e. tout anneau B muni d'un morphisme d'anneaux de A dans B), s'intéresser à l'ensemble $V_P(B)$ des solutions [20] dans B.

Résoudre l'équation diophantienne P demande de décrire l'ensemble $V_P(\mathbf{Z})$ ou $V_P(\mathbf{Q})$, mais on peut se demander, plus modestement, de pouvoir décider si $V_P(\mathbf{Z})$ ou $V_P(\mathbf{Q})$ est vide ou pas. Il s'agit de problèmes, en général très difficiles, qui ont joué un très grand rôle dans le développement des mathématiques.

• Les grecs ont été fort traumatisés par la découverte que $V_P(\mathbf{Q}) = \varnothing$, si P est l'équation polynomiale $X^2 = 2$ (irrationalité de $\sqrt{2}$).

• L'étude de l'équation $X^2 - DY^2 = 1$ (Pell-Fermat) ou celle, en fonction de n, du cardinal de $V_P(\mathbf{Z})$, si P est l'équation $X^2 + DY^2 = n$, ou, plus généralement, de l'équation $a_1X_1^2 + \cdots + a_dX_d^2 = n$, ont donné naissance à la théorie algébrique des nombres et à celles des formes quadratiques ou des fractions continues, et ont contribué fortement au développement de celle des formes modulaires.

• L'équation $X^n + Y^n = Z^n$ a fait couler beaucoup d'encre et donné naissance à un nombre impressionnant de théories mathématiques pendant plus de 350 ans.

• Euler avait conjecturé (1769), influencé par le th. de Fermat, que $X^4 + Y^4 + Z^4 = 1$ n'a pas de solutions en nombres rationnels autres que les évidentes $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ et $(0, 0, \pm 1)$, ce qui a été infirmé par Elkies (1988), qui a trouvé (avec l'aide d'un ordinateur) la relation $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$, et l'a utilisée pour montrer que les points rationnels sont denses dans les points réels (on peut difficilement faire plus faux comme conjecture...).

1.2. *Le dixième problème de Hilbert.* — En fait, le problème de la résolution des équations diophantiennes est encore nettement plus fondamental que ce que la liste d'exemples ci-dessus laisserait penser. Ceci avait été bien vu par Hilbert dont la série de 23 problèmes rassemblés pour le congrès international des mathématiciens de 1900, en comportait un (le 10-ième) demandant de produire un algorithme permettant de décider si une équation diophantienne a, ou non, des solutions en nombres entiers.

• Il est très facile de produire un tel algorithme en une variable (nous laissons au lecteur le plaisir de le faire).

20. Par exemple, si P est l'équation $X^2 + Y^2 + Z^2 = 8n + 7$, on constate à la main que $V_P(\mathbf{Z}/8\mathbf{Z}) = \varnothing$, les carrés de $\mathbf{Z}/8\mathbf{Z}$ étant 0, 1 et 4 ; cela permet de prouver que P n'a pas de solutions en nombres entiers.

• L'existence d'un tel algorithme en deux variables a été prouvée par Baker (1969), ce qui lui a valu la médaille Fields en 1970. Ce que fournit Baker, c'est une borne pour la taille des solutions, et l'algorithme consiste alors à explorer toutes les possibilités jusqu'à cette borne.

• Ce problème fut finalement résolu par Matiyasevich en 1970, qui prouva qu'un tel algorithme ne peut pas exister, au grand soulagement des arithméticiens qui voyaient d'un mauvais œil l'idée qu'un ordinateur puisse les mettre au chômage. En poussant plus loin les méthodes de Matiyasevich, on peut en fait ramener tout problème mathématique, de manière parfaitement algorithmique, au problème de savoir si une certaine équation diophantienne a des solutions ou pas (le projet de Hilbert n'aurait pas mis que les arithméticiens au chômage...). On peut aussi construire des polynômes explicites pour lesquels on peut décider arbitrairement de l'existence ou de la non existence de solutions en nombres entiers, sans rajouter de contradiction dans les mathématiques... C'est un peu ennuyeux, car cela veut dire qu'on n'est jamais sûr que le problème auquel on s'attaque n'est pas de ce type.

• Le théorème de Matiyasevich n'exclut pas, a priori, l'existence d'un algorithme pour décider si un polynôme (en plusieurs variables) a des solutions rationnelles [21] ou pas. Il n'exclut pas non plus qu'il existe un tel algorithme pour les équations diophantiennes en 3 variables. Les courbes elliptiques constituent le premier test non trivial dans cette direction, la conjecture de Birch et Swinnerton-Dyer fournissant un tel algorithme (cor. F.1.16), si elle est vraie...

1.3. *L'équation* $Y^2 - Y = X^5 - X$. — Un bon marqueur des progrès effectués est fourni par l'équation diophantienne P donnée par $Y^2 - Y = X^5 - X$:

• On sait depuis 1929, grâce à un résultat de Siegel concernant les points entiers des courbes algébriques, que $V_P(\mathbf{Z})$ est un ensemble fini.

• Le résultat de Baker mentionné ci-dessus permet de montrer que si $(X, Y) \in V_P(\mathbf{Z})$, alors $\sup(|X|, |Y|) \leqslant \exp(\exp(\exp 5^{1250}))$; « l'algorithme » de Baker n'est donc pas très utilisable en pratique...

• On sait depuis 1983, grâce à un résultat de Faltings démontrant la conjecture de Mordell (cf. n° suivant), que $V_P(\mathbf{Q})$ est un ensemble fini.

• L'augmentation de la puissance des ordinateurs a rendu envisageable une recherche des solutions en nombres entiers (cela demande quand même de réduire grandement les bornes fournies par Baker et de cibler intelligemment les solutions éventuelles, par exemple

21. On peut ramener le problème de décrire l'ensemble $V_P(\mathbf{Q})$ à celui de $V_Q(\mathbf{Z})$ en rajoutant une variable (qui est le ppcm des dénominateurs des solutions) : par exemple, l'équation $DY^2 = X^3 - X$ devient $Dcb^2 = a^3 - ac^2$, en posant $X = \frac{a}{c}$, $Y = \frac{b}{c}$ et en multipliant le tout par c^3. L'équation ainsi obtenue est d'un type bien particulier : elle est *homogène* ce qui fait que si (a, b, c) est une solution, il en est de même de (na, nb, nc), pour tout $n \in \mathbf{Z}$; il suffit donc de considérer les solutions où a, b, c sont premiers entre eux dans leur ensemble.

en utilisant des méthodes p-adiques). Le résultat complet a finalement été obtenu par Bugeaud, Mignotte, Siksek, Stoll et Tengely en 2008 :

$$\mathrm{V_P}(\mathbf{Z}) = \big(\{-1,0,1\}\times\{0,1\}\big) \cup \big\{\big(2,\frac{1\pm 11}{2}\big),\big(3,\frac{1\pm 31}{2}\big),\big(30,\frac{1\pm 9859}{2}\big)\big\}.$$

• On ne sait toujours pas calculer $\mathrm{V_P}(\mathbf{Q})$...

2. La topologie des solutions complexes gouverne l'arithmétique !

2.1. *Le genre d'une surface de Riemann.* — Si $\mathrm{P} \in \mathbf{C}[\mathrm{X},\mathrm{Y}]$ est non nul, l'ensemble $\mathrm{V_P}(\mathbf{C})$ des solutions dans $\mathbf{C}^2$ de l'équation $\mathrm{P}(\mathrm{X},\mathrm{Y}) = 0$ est une courbe complexe et peut aussi être vu comme une surface réelle puisque $\mathbf{C}$ est de dimension 2 sur $\mathbf{R}$; c'est ce qu'on appelle une *surface de Riemann*.

Si P est l'équation $\mathrm{X}+\mathrm{Y}=0$, alors $(\mathrm{X},\mathrm{Y}) \mapsto \mathrm{X}$ induit un homéomorphisme de $\mathrm{V_P}(\mathbf{C})$ sur $\mathbf{C}$ (d'inverse $z \mapsto (z,-z)$). Le plan complexe $\mathbf{C}$ se compactifie naturellement en rajoutant un point à l'infini (noté ∞), et on obtient de la sorte une sphère dite *sphère de Riemann* ; autrement dit, $\mathrm{V_P}(\mathbf{C})$ est homéomorphe à une sphère S moins un point ∞ : la projection stéréographique à partir de ∞ fournit un homéomorphisme de $\mathrm{S}-\{\infty\}$ sur le plan.

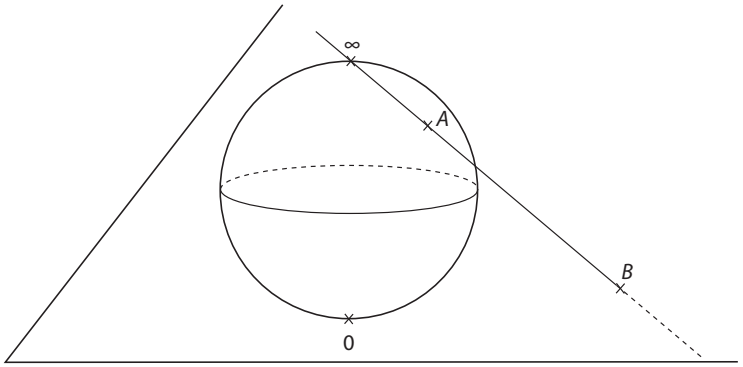


FIGURE 2. Le plan est une sphère moins un point.

De même, si P est l'équation $\mathrm{XY}=1$, alors $(\mathrm{X},\mathrm{Y}) \mapsto \mathrm{X}$ induit un homéomorphisme de $\mathrm{V_P}(\mathbf{C})$ sur $\mathbf{C}^*$ que l'on peut voir comme la sphère privée de deux points (0 et ∞).

De manière générale, si P est l'équation $\mathrm{Q}(\mathrm{X},\mathrm{Y})=0$, où $\mathrm{Q} \in \mathbf{C}[\mathrm{X},\mathrm{Y}]$ est irréductible (i.e. ne peut pas se factoriser sous la forme $\mathrm{Q}=\mathrm{Q_1Q_2}$, où $\mathrm{Q_1},\mathrm{Q_2}$ sont non constants), alors $\mathrm{V_P}(\mathbf{C})$, privé d'un nombre fini de points *singuliers*[22] est homéomorphe à un tore

22. Par exemple, si P est l'équation $\mathrm{Y}^2 = \mathrm{X}^2(\mathrm{X}+1)$, il y a deux branches qui passent par le point $(0,0)$, l'une tangente a $\mathrm{Y}=\mathrm{X}$ et l'autre à $\mathrm{Y}=-\mathrm{X}$. La surface $\mathrm{V_P}(\mathbf{C})$ est alors une sphère privée du point ∞, dont deux des points se retrouvent attachés en $(0,0)$ ce qui crée la singularité. Quand on enlève $(0,0)$, on obtient une sphère privée de 3 points (∞ et les deux points qui étaient collés ensemble).

avec un nombre fini de trous, auquel on a retiré un nombre fini de points. Le nombre de trous est appelé le *genre* (noté g) de $\mathrm{V_P}(\mathbf{C})$.

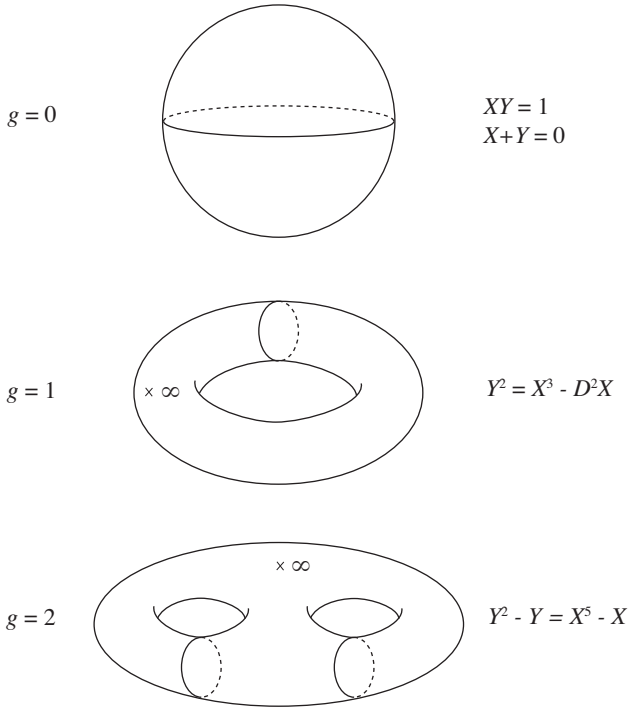


FIGURE 3. Surfaces de Riemann de genres 0, 1 et 2.

- Si P est $\mathrm{X} + \mathrm{Y} = 0$ ou $\mathrm{XY} = 1$, alors $g = 0$.
- Si P est l'équation $\mathrm{Y}^2 - \mathrm{Y} = \mathrm{X}^5 - \mathrm{X}$, alors $g = 2$.

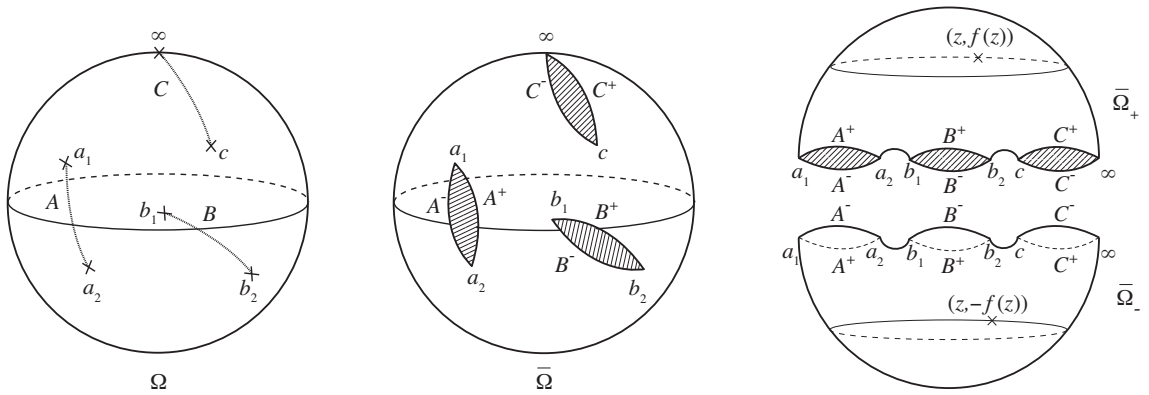


FIGURE 4. Construction de la surface de Riemann de la fonction $\sqrt{z^5 - z - \frac{1}{4}}$.

Expliquons pourquoi la surface de Riemann $V_P(\mathbf{C})$ définie par l'équation $Y^2 - Y = X^5 - X$ est un tore à deux trous auquel on a retiré un point. On fait le changement de variable $Y = T + \frac{1}{2}$ de manière à se ramener à l'équation $T^2 = X^5 - X - \frac{1}{4}$, ce qui ne change pas la forme de $V_P(\mathbf{C})$. Alors $V_P(\mathbf{C})$ est l'ensemble des couples $(z, \pm\sqrt{z^5 - z - \frac{1}{4}})$, pour $z \in \mathbf{C}$. Le problème de cette description est que la fonction $z \mapsto \sqrt{z^5 - z - \frac{1}{4}}$ est multivaluée sur $\mathbf{C}$ (quand on tourne autour d'un des zéros a_1, a_2, b_1, b_2, c du polynôme $z^5 - z - \frac{1}{4}$ ou de ∞, cette racine carrée change de signe), et donc qu'il faut faire attention à la signification qu'on lui donne.

Pour remédier à ce problème on effectue des coupures dans le plan complexe. On choisit [23] des chemins A, B, C disjoints sur la sphère de Riemann $\mathbf{C} \cup \{\infty\}$, d'extrémités respectives a_1, a_2 (pour A), b_1, b_2 (pour B) et c, ∞ (pour C) qui ne se recoupent pas (i.e. qui ne comportent pas de boucles), et on note Ω l'ouvert de $\mathbf{C}$ complémentaire de ces chemins. Sur Ω, le polynôme $z^5 - z - \frac{1}{4}$ a une racine carrée holomorphe que l'on note $z \mapsto f(z)$. De plus, si z appartient à A, B ou C et n'est pas un zéro de $z^5 - z - \frac{1}{4}$, alors $f(z)$ admet deux limites opposées, racines carrées de $z^5 - z - \frac{1}{4}$, suivant que l'on s'approche de z par « en-dessous » du chemin ou par « au-dessus ». Pour tenir compte de ce phénomène, on dédouble chacun des points z des chemins A, B, C, à l'exception des extrémités, en deux points z^+, z^-, un peu comme si on ouvrait une fermeture éclair le long de ces chemins. Ceci nous fournit deux chemins A^+, A^- joignant a_1 et a_2, deux chemins B^+, B^- joignant b_1 et b_2 et deux chemins C^+, C^- joignant c et ∞. La réunion $\overline{\Omega}$ de Ω et des chemins $A^+, A^-, B^+, B^-, C^+, C^-$ est alors un compact (on a rajouté un bord à l'ouvert Ω), et f se prolonge par continuité à Ω (c'était le but de l'opération), en une fonction encore notée f qui vérifie $f(z^-) = -f(z^+)$ si $z \in A, B, C$ (avec la convention que $z^+ = z^- = z$ si z est une extrémité, et $f(\infty) = \infty$).

Soient maintenant $\overline{\Omega}_+ = \{(z, f(z)),\ z \in \overline{\Omega}\}$ et $\overline{\Omega}_- = \{(z, -f(z)),\ z \in \overline{\Omega}\}$. Alors $\overline{\Omega}_+$ et $\overline{\Omega}_-$ sont deux sous-ensembles de $V_P(\mathbf{C}) \cup \{\infty\}$, homéomorphes à $\overline{\Omega}$, et qui recouvrent $V_P(\mathbf{C}) \cup \{\infty\}$. Pour obtenir $V_P(\mathbf{C}) \cup \{\infty\}$, il suffit alors de recoller [24] $\overline{\Omega}_+$ et $\overline{\Omega}_-$ le long des chemins que l'on a dédoublés pour construire $\overline{\Omega}$.

• Si P est l'équation $DY^2 = (X - a)(X - b)(X - c)$ d'une courbe elliptique, alors $g = 1$.

Cela se justifie par les mêmes arguments que pour $Y^2 - Y = X^5 - X$ en faisant des coupures joignant a à b et c à ∞ sur la sphère de Riemann. On peut aussi remarquer que le changement de variable $X = 2T + \frac{a+b+c}{3}$ et $Y = \sqrt{\frac{2}{D}}Z$ transforme l'équation en $Z^2 = 4T^3 - BT - C$, et on peut utiliser les résultats du prob. H.8, selon lesquels $V_P(\mathbf{C})$ est homéomorphe à $\mathbf{C}/\Lambda$ moins un point, où Λ est un réseau de $\mathbf{C}$. Le choix d'une base de Λ sur $\mathbf{Z}$ fournit un homéomorphisme de $\mathbf{C}/\Lambda$ sur $(\mathbf{R}/\mathbf{Z}) \times (\mathbf{R}/\mathbf{Z})$, c'est-à-dire sur un produit de deux cercles, ce qui peut se matérialiser en faisant tourner un des cercles autour d'un axe passant par le centre de l'autre, et on obtient de la sorte un tore à un trou, comme annoncé.

23. Nous laissons le lecteur se persuader du fait que c'est possible

24. Si $z \in A, B, C$ n'est pas une extrémité, les deux points $(z, \pm\sqrt{z^5 - z - \frac{1}{4}})$ apparaissent à la fois dans $\overline{\Omega}_+$ et $\overline{\Omega}_-$. Pour obtenir $V_P(\mathbf{C}) \cup \{\infty\}$, il faut donc recoller $\overline{\Omega}_+$ et $\overline{\Omega}_-$ en identifiant les points $(z^+, f(z^+)) \in \overline{\Omega}_+$ avec $(z^-, f(z^+)) \in \overline{\Omega}_-$ et les points $(z^-, -f(z^+)) \in \overline{\Omega}_+$ avec $(z^+, -f(z^+)) \in \overline{\Omega}_-$ (on recolle A^+, B^+, C^+ sur $\overline{\Omega}_+$ avec A^-, B^-, C^- sur $\overline{\Omega}_-$ et A^-, B^-, C^- sur $\overline{\Omega}_+$ avec A^+, B^+, C^+ sur $\overline{\Omega}_-$; pour ce faire, il faut, dans la figure, passer de $\overline{\Omega}_+$ à $\overline{\Omega}_-$ par une rotation par rapport à un axe horizontal et pas par une symétrie par rapport à un plan horizontal).

• Il y a une formule algébrique permettant de calculer g ; par exemple, $g = \frac{(n-1)(-2)}{2}$ pour l'équation de Fermat $\mathrm{X}^n + \mathrm{Y}^n = 1$. La formule générale fait intervenir les points singuliers de la courbe (la courbe de Fermat n'en a pas, ce qui explique que la formule soit particulièrement simple).

2.2. *Genre et solutions rationnelles.* — Le comportement des solutions est très différent suivant que le genre est 0, 1 ou $\geqslant 2$.

• Si $g = 0$, et si $\mathrm{V_P}(\mathbf{Q})$ contient au moins un point non singulier, il existe $\mathrm{C} \geqslant 0$ et $t > 0$ tels que

$$\big|\big\{a, b, c \in \mathbf{Z}, c \geqslant 1 \ \sup(|a|, |b|, |c|) \leqslant x, \ (a, b, c) = 1, \ \mathrm{Q}\big(\frac{a}{c}, \frac{b}{c}\big)\big\}\big| \sim \mathrm{C}x^t.$$

Il y a donc beaucoup de solutions rationnelles s'il y en a au moins une (non singulière).

• Si $g = 1$, il existe $\mathrm{C} \geqslant 0$ et $r \in \mathbf{N}$ tels que

$$\big|\big\{a, b, c \in \mathbf{Z}, c \geqslant 1 \ \sup(|a|, |b|, |c|) \leqslant x, \ (a, b, c) = 1, \ \mathrm{Q}\big(\frac{a}{c}, \frac{b}{c}\big)\big\}\big| \sim \mathrm{C}(\log x)^{r/2}.$$

En particulier, si $r \geqslant 1$, il y a une infinité de solutions rationnelles, mais celles-ci sont assez clairsemées. Une courbe elliptique est de genre 1, et le r précédent n'est autre que le rang de la courbe elliptique (cf. th. F.1.6).

• Si $g \geqslant 2$, alors $\mathrm{V_P}(\mathbf{Q})$ est fini. Ce résultat, conjecturé par Mordell (1922), a finalement été démontré par Faltings (1983), ce qui lui a valu la médaille Fields en 1986.

APPENDICE G

INTRODUCTION AU PROGRAMME DE LANGLANDS

Un titre plus honnête pour ce chapitre, qui contient beaucoup d'énoncés magnifiques, mais peu de démonstrations [1], serait « Introduction à l'existence du programme de Langlands », une vraie introduction au programme de Langlands pouvant difficilement se faire avant le M2.

On peut faire remonter les thèmes menant au programme de Langlands à la *loi de réciprocité quadratique* conjecturée par Euler (1783) et démontrée par Gauss (1801). Le problème est, étant donné un nombre premier ℓ ou, plus généralement, un entier $d \in \mathbf{Z}$ divisible par le carré d'aucun nombre premier, de décrire l'ensemble des nombres premiers p tels que d soit un carré dans $\mathbf{F}_p$. De manière équivalente, il s'agit de déterminer le nombre de zéros dans $\mathbf{F}_p$ du polynôme $\mathrm{X}^2 - d$. La surprise est que la réponse ne dépend que de la classe de p modulo D, avec $\mathrm{D} = d$ si $d \equiv 1 \bmod 4$, et modulo $\mathrm{D} = 4d$ si $d \equiv 2, 3 \bmod 4$. Plus précisément, il existe un caractère de Dirichlet χ_{D} de conducteur D et à valeurs dans $\{\pm 1\}$ tel que le nombre de zéros de $\mathrm{X}^2 - d$ dans $\mathbf{F}_p$ soit égal à $1 + \chi_{\mathrm{D}}(p)$.

Du point de vue qui va nous intéresser dans ce chapitre, cette loi de réciprocité peut s'encoder dans une identité multiplicative entre fonctions L. On note P_{D} le polynôme $\mathrm{X}^2 - \mathrm{X} + \frac{1-d}{4}$, si $d \equiv 1 \bmod 4$, et $\mathrm{X}^2 - d$, si $d \equiv 2, 3 \bmod 4$. Dans tous les cas, ce polynôme est à coefficients entiers, son discriminant est D, et ses racines sont $\frac{1 \pm \sqrt{d}}{2}$ ou $\pm\sqrt{d}$ suivant la congruence de d modulo 4. On note A_{D} l'anneau $\mathbf{Z}[\mathrm{X}]/(\mathrm{P}_{\mathrm{D}})$. On a donc $\mathrm{A}_{\mathrm{D}} = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, si $d \equiv 1 \bmod 4$, et $\mathrm{A}_{\mathrm{D}} = \mathbf{Z}[\sqrt{d}]$, si $d \equiv 2, 3 \bmod 4$. On définit la fonction $\zeta_{\mathrm{A}_{\mathrm{D}}}(s)$ par la formule $\zeta_{\mathrm{A}_{\mathrm{D}}}(s) = \sum_{\mathfrak{n}} \frac{1}{|\mathrm{A}_{\mathrm{D}}/\mathfrak{n}|^s}$, où $\mathfrak{n}$ décrit l'ensemble des idéaux de A_{D} tels que l'anneau $\mathrm{A}_{\mathrm{D}}/\mathfrak{n}$ soit un anneau fini [2]. Un peu de théorie algébrique des nombres permet

1. Les seules démonstrations, outre celles esquissées en notes de bas de page, se trouvent dans le § G.2 où l'on étend aux adèles la transformée de Fourier du chap. IV et la transformée de Mellin du § VII.2, qui en est l'analogue multiplicatif. Comme le lecteur le constatera, la plupart des difficultés sont concentrées sur les nombres réels, les nombres p-adiques se comportant plutôt comme des groupes finis.

2. On remarquera que si on remplace A_{D} par $\mathbf{Z}$ dans la définition précédente, on tombe sur la fonction zêta de Riemann.

de montrer que la série de Dirichlet $\zeta_{\mathrm{A_D}}(s)$ converge pour $\mathrm{Re}(s) > 1$, et que la loi de réciprocité quadratique est équivalente à la factorisation $\zeta_{\mathrm{A_D}}(s) = \zeta(s)\mathrm{L}(\chi_{\mathrm{D}}, s)$.

Par exemple, si $d = -1$ (et donc $\mathrm{D} = -4$ et $\mathrm{A_D} = \mathbf{Z}[i]$), le caractère χ_{D} est donné par $\chi_{\mathrm{D}}(n) = 1$ si $n \equiv 1 \bmod 4$, et $\chi_{\mathrm{D}}(n) = -1$ si $n \equiv 3 \bmod 4$. On en déduit la relation [3]

$$\frac{1}{4}\sum_{\substack{(n,m)\in\mathbf{Z}^2\\(n,m)\neq(0,0)}}\frac{1}{(n^2+m^2)^s} = \zeta(s)\mathrm{L}(\chi_4,s) = \frac{1}{1-2^{-s}}\prod_{p\equiv 1 \bmod 4}\frac{1}{(1-p^{-s})^2}\prod_{p\equiv 3 \bmod 4}\frac{1}{1-p^{-2s}},$$

et en identifiant les termes en p^{-s} des deux côtés, on retrouve le résultat de Fermat selon lequel *un nombre premier impair est somme de deux carrés si et seulement si il est de la forme* $4n+1$.

La définition de $\zeta_{\mathrm{A_D}}$ se généralise à tout anneau $\mathrm{A} = \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_d]/(\mathrm{P}_1, \ldots, \mathrm{P}_r)$, où $\mathrm{P}_1, \ldots, \mathrm{P}_r$ sont des polynômes en $\mathrm{X}_1, \ldots, \mathrm{X}_d$ à coefficients dans $\mathbf{Z}$, ce qui permet d'associer à un tel anneau une *fonction zêta de Hasse-Weil* $\zeta_{\mathrm{A}}(s) = \sum_{\mathfrak{n}} \frac{1}{|\mathrm{A}/\mathfrak{n}|^s}$ comme ci-dessus. Comme un anneau fini de cardinal n est de manière unique un produit d'anneaux de cardinaux $p^{v_p(n)}$ (lemme des restes chinois), la fonction $\zeta_{\mathrm{A}}(s)$ admet une décomposition en produit de facteurs d'Euler $\zeta_{\mathrm{A}}(s) = \prod_{p\in\mathscr{P}} \zeta_{\mathrm{A},p}(s)$, et A. Weil a conjecturé en 1949 que $\zeta_{\mathrm{A},p}(s)$ est une fonction rationnelle de p^{-s} ce qui fut démontré par B. Dwork en 1959. Weil a aussi conjecturé que cette fonction rationnelle a une factorisation sous une forme indépendante de p, et ne dépendant que de la géométrie de l'espace des solutions $\mathrm{P}_1(z_1, \ldots, z_d) = \cdots = \mathrm{P}_r(z_1, \ldots, z_d)$ dans $\mathbf{C}^d$, ce qui fut démontré par A. Grothendieck [4] comme aboutissement d'un énorme programme ayant totalement révolutionné la géométrie algébrique. A la factorisation des facteurs d'Euler correspond une factorisation de la fonction ζ_{A} en fonctions L, et l'un des buts principaux du programme de Langlands est de comprendre chacune de ces fonctions L en vue, en particulier, de démontrer la *conjecture de Hasse-Weil* selon laquelle les fonctions zêta de Hasse-Weil possèdent un prolongement méromorphe à tout le plan complexe.

L'exemple le plus célèbre est probablement $\mathrm{A} = \mathbf{Z}[\mathrm{X}, \mathrm{Y}]/(\mathrm{Y}^2 - \mathrm{X}^3 - \alpha\mathrm{X}^2 - \beta\mathrm{X} - \gamma)$, avec $\alpha, \beta, \gamma \in \mathbf{Z}$. Dans ce cas, A. Wiles (1994, dans le cas « semi-stable ») et C. Breuil, B. Conrad, F. Diamond et R. Taylor (1999, dans le cas général) ont démontré, ce qui avait été conjecturé de manière vague par Y. Taniyama en 1956, et précisé par A. Weil en 1966, qu'il existe une forme modulaire primitive f (cf. n° 4.1 du § G.1) telle que $\zeta_{\mathrm{A}}(s) = \frac{\zeta(s-1)}{\mathrm{L}(f,s)}$, à multiplication près par un nombre fini de facteurs d'Euler innocents. Ceci a permis à A. Wiles, en utilisant des résultats antérieurs de K. Ribet (1988), d'en déduire la non

3. L'anneau $\mathbf{Z}[i]$ est principal, et si $n + mi \in \mathbf{Z}[i]$ est non nul, l'anneau $\mathbf{Z}[i]/(n+mi)$ est fini de cardinal $n^2 + m^2$; le facteur $\frac{1}{4}$ s'explique par le fait que α, $-\alpha$, $i\alpha$ et $-i\alpha$ engendrent le même idéal, si $\alpha = n + mi \in \mathbf{Z}[i] - \{0\}$.

4. Cela lui a valu une médaille Fields en 1966 ; P. Deligne en a obtenu une en 1978 pour avoir démontré la dernière des conjectures de Weil, *l'hypothèse de Riemann sur les corps finis*, selon laquelle les zéros et les pôles de $\zeta_{\mathrm{A},p}(s)$ se répartissent sur un nombre fini de droites verticales explicites.

existence d'un A de la forme ci-dessus avec $X^3 + \alpha X^2 + \beta X + \gamma = X(X - a^p)(X + b^p)$, où $a^p + b^p = c^p$ est un contrexemple au théorème de Fermat, et donc de démontrer le théorème de Fermat.

G.1. La conjecture d'Artin

1. Le groupe $\mathscr{G}_{\mathbf{Q}}$

Rappelons (cf. n$^{\text{os}}$ 8.2 et 8.3 du Vocabulaire) que $x \in \mathbf{C}$ est *algébrique* s'il existe $P \in \mathbf{Q}[X]$, non nul, tel que $P(x) = 0$. De manière équivalente, $x \in \mathbf{C}$ est algébrique si et seulement si la sous-$\mathbf{Q}$-algèbre $\mathbf{Q}[x]$ de $\mathbf{C}$ engendrée par x est de dimension finie sur $\mathbf{Q}$; c'est alors un sous-corps de $\mathbf{C}$. Ceci permet de montrer que, si x et y sont algébriques, alors $x+y$ et xy sont algébriques. On en déduit que l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est un sous-corps de $\mathbf{C}$.

On note $\mathscr{G}_{\mathbf{Q}}$ l'ensemble des *automorphismes de corps de* $\overline{\mathbf{Q}}$, c'est-à-dire l'ensemble des permutations σ de $\overline{\mathbf{Q}}$ telles que l'on ait

$$\sigma(x + y) = \sigma(x) + \sigma(y) \text{ et } \sigma(xy) = \sigma(x)\sigma(y), \quad \text{quels que soient } x, y \in \overline{\mathbf{Q}}.$$

Muni de la composition, $\mathscr{G}_{\mathbf{Q}}$ est un sous-groupe du groupe des permutations de $\overline{\mathbf{Q}}$; c'est même un sous-groupe du groupe des automorphismes $\mathbf{Q}$-linéaires [5] de $\overline{\mathbf{Q}}$.

Le groupe $\mathscr{G}_{\mathbf{Q}}$ est un groupe gigantesque et extrêmement mystérieux, mais dont la compréhension serait cruciale pour beaucoup de problèmes. Le simple fait qu'il existe est déjà très utile.

• Le seul élément de $\mathscr{G}_{\mathbf{Q}}$ que l'on sache décrire est la conjugaison complexe, que nous noterons frob_∞. On a $(\text{frob}_\infty)^2 = 1$, et Artin (1924) a démontré que tout élément d'ordre fini de $\mathscr{G}_{\mathbf{Q}}$ est conjugué à 1 ou frob_∞, et donc est d'ordre 1 ou 2.

• Si $P \in \mathbf{Q}[X]$ est irréductible de degré n, et si $\alpha_1, \ldots, \alpha_n \in \overline{\mathbf{Q}}$ sont les racines de P, alors quel que soient $i, j \in \{1, \ldots, n\}$, il existe [6] $\sigma_{i,j} \in \mathscr{G}_{\mathbf{Q}}$, avec $\sigma_{i,j}(\alpha_i) = \alpha_j$, ce qui montre qu'il y a bien d'autres éléments que frob_∞ dans $\mathscr{G}_{\mathbf{Q}}$.

• Si H est un sous-groupe de $\mathscr{G}_{\mathbf{Q}}$, alors l'ensemble $\overline{\mathbf{Q}}^{\mathrm{H}}$ des éléments de $\overline{\mathbf{Q}}$ fixes par H est un sous-corps de $\overline{\mathbf{Q}}$. Réciproquement, si K est un sous-corps de $\overline{\mathbf{Q}}$, l'ensemble $\mathscr{G}_{\mathrm{K}}$ des $\sigma \in \mathscr{G}_{\mathbf{Q}}$ fixant tous les éléments de K est un sous-groupe fermé [7] de $\mathscr{G}_{\mathbf{Q}}$. On obtient de la

5. On commence par montrer que $\sigma(1) = 1$, puis que $\sigma(n) = n$, quel que soit $n \in \mathbf{Z}$, et finalement que σ induit l'identité sur $\mathbf{Q}$.

6. C'est une conséquence de la théorie de Galois.

7. On met sur $\mathscr{G}_{\mathbf{Q}}$ la *topologie de Krull* qui, par définition, est la plus faible rendant continue l'action de $\mathscr{G}_{\mathbf{Q}}$ sur $\overline{\mathbf{Q}}$ muni de la topologie discrète. Ceci signifie que, si $\sigma_0 \in \mathscr{G}_{\mathbf{Q}}$, et si $\alpha \in \overline{\mathbf{Q}}$, l'ensemble $\mathrm{U}_\alpha(\sigma_0) = \{\sigma \in \mathscr{G}_{\mathbf{Q}},\ \sigma(\alpha) = \sigma_0(\alpha)\}$ est un ouvert de $\mathscr{G}_{\mathbf{Q}}$, et les $\mathrm{U}_\alpha(\sigma_0)$, pour $\sigma_0 \in \mathscr{G}_{\mathbf{Q}}$ et $\alpha \in \overline{\mathbf{Q}}$ forment une base d'ouverts de $\mathscr{G}_{\mathbf{Q}}$. En particulier, tout ouvert de $\mathscr{G}_{\mathbf{Q}}$ contenant 1 contient $\mathrm{U}_\alpha(1)$, pour un certain $\alpha \in \overline{\mathbf{Q}}$, et donc contient un sous-groupe d'indice fini.

sorte [8] une bijection entre les *corps de nombres* (i.e. les sous-corps de $\overline{\mathbf{Q}}$ dont la dimension sur $\mathbf{Q}$ est finie), et les sous-groupes fermés d'indice [9] fini de $\mathscr{G}_{\mathbf{Q}}$, et on a $\overline{\mathbf{Q}}^{\mathscr{G}_{\mathrm{K}}} = \mathrm{K}$ si K est un corps de nombres, et $\mathscr{G}_{\overline{\mathbf{Q}}^{\mathrm{H}}} = \mathrm{H}$ si H est un sous-groupe fermé d'indice fini de $\mathscr{G}_{\mathbf{Q}}$.

• On conjecture que $\mathscr{G}_{\mathbf{Q}}$ est tellement compliqué que tout groupe fini G est un quotient [10] de $\mathscr{G}_{\mathbf{Q}}$ (problème inverse de Galois). On sait montrer [11] que c'est vrai pour tout groupe d'ordre impair (I. Shafarevich, 1954), pour S_n et A_n quel que soit n, pour le monstre... ; je ne pense pas qu'on sache le démontrer pour $\mathbf{SL}_3(\mathbf{F}_9)$ par exemple ($\mathbf{F}_9$ est le corps à 9 éléments), bien qu'il soit beaucoup plus petit que le monstre.

2. Représentations de $\mathscr{G}_{\mathbf{Q}}$

Comme nous l'avons mentionné au chap. I, on n'a de prise sur $\mathscr{G}_{\mathbf{Q}}$ qu'à travers ses représentations. Nous ne nous intéresserons qu'aux représentations complexes ; celles-ci jouent un rôle fondamental mais sont, pour des raisons topologiques [12], un peu trop rigides pour beaucoup d'applications, et on est aussi amené à considérer des représentations de $\mathscr{G}_{\mathbf{Q}}$ sur d'autres corps (et mêmes sur des anneaux) que $\mathbf{C}$, comme le corps $\mathbf{Q}_p$ des nombres p-adiques. Comme il est expliqué dans la note 12, si V est une représentation complexe de $\mathscr{G}_{\mathbf{Q}}$, alors $\mathscr{G}_{\mathbf{Q}}$ agit à travers un groupe fini, ce qui permet d'utiliser les résultats du chap. I. De plus, tous les calculs à effectuer pour expliciter les objets apparaissant dans

8. C'est encore une conséquence de la théorie de Galois.

9. Rappelons que, si $\mathrm{H} \subset \mathrm{G}$ sont des groupes, l'indice $[\mathrm{G} : \mathrm{H}]$ de H dans G est le cardinal de G/H.

10. Si c'est vrai, alors $\mathrm{G} \times \cdots \times \mathrm{G}$ est aussi un quotient de $\mathscr{G}_{\mathbf{Q}}$ et donc G est un quotient de $\mathscr{G}_{\mathbf{Q}}$ d'une infinité de manières différentes.

11. Pour montrer un énoncé de ce type, on peut procéder de la manière suivante. Si $\mathrm{P} \in \mathbf{Q}[\mathrm{X}]$, si $\alpha \in \overline{\mathbf{Q}}$ vérifie $\mathrm{P}(\alpha) = 0$, et si $\sigma \in \mathscr{G}_{\mathbf{Q}}$, alors $0 = \sigma(\mathrm{P}(\alpha)) = \mathrm{P}(\sigma(\alpha))$ (car σ fixe les coefficients de P). On obtient de la sorte un morphisme de groupes de $\mathscr{G}_{\mathbf{Q}}$ dans le groupe des permutations des racines de P. La description de l'image $\mathrm{Gal}_{\mathrm{P}}$ (qui, par construction, est un quotient de $\mathscr{G}_{\mathbf{Q}}$) fait l'objet de la théorie de Galois. Si P est irréductible de degré n, alors $\mathrm{Gal}_{\mathrm{P}}$ est un sous-groupe de S_n, en général égal à S_n ; il faut pas mal d'astuce pour construire des polynômes irréductibles P tels que $\mathrm{Gal}_{\mathrm{P}}$ ne soit pas un groupe symétrique. Par exemple, la construction d'un polynôme P tel que $\mathrm{Gal}_{\mathrm{P}}$ soit le monstre utilise un mélange de géométrie complexe, de topologie algébrique, de théorie des groupes finis, de géométrie algébrique et de théorie des nombres.

12. Si $\rho : \mathscr{G}_{\mathbf{Q}} \to \mathbf{GL}_n(\mathbf{C})$ est un morphisme continu de groupes, on a $\rho(1) = 1$, et la continuité de ρ implique (cf. note 7) qu'il existe un sous-groupe H d'indice fini de $\mathscr{G}_{\mathbf{Q}}$ tel que, si $g \in \mathrm{H}$, alors $\rho(g) - 1$ a toutes ses coordonnées $a_{i,j}$ vérifiant $|a_{i,j}| \leqslant \frac{1}{2n}$. En appliquant ceci à g^k, on en déduit que $|\mathrm{Tr}(\rho(g)^k) - n| \leqslant \frac{1}{2}$ quel que soit $k \in \mathbf{Z}$, et il n'est pas très difficile d'en conclure que ceci implique que toutes les valeurs propres de $\rho(g)$ sont égales à 1, puis que $\rho(g) = 1$. En conclusion, le noyau de ρ contient un sous-groupe d'indice fini, et donc $\rho(\mathscr{G}_{\mathbf{Q}})$ est un groupe fini. En particulier, chaque représentation complexe de $\mathscr{G}_{\mathbf{Q}}$ ne fournit de renseignements que sur une toute petite partie de $\mathscr{G}_{\mathbf{Q}}$. La situation est nettement plus favorable sur $\mathbf{Q}_p$, et la définition naturelle des fonctions L apparaissant dans la factorisation de la fonction zêta de Hasse-Weil ζ_{A} de $\mathrm{A} = \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_d]/(\mathrm{P}_1, \ldots, \mathrm{P}_r)$ utilise des représentations de $\mathscr{G}_{\mathbf{Q}}$ que Grothendieck a associées à la variété d'équation $\mathrm{P}_1 = \cdots = \mathrm{P}_r = 0$.

la conjecture d'Artin du n° 3 se font dans le corps de nombres K, fixé par le noyau de ρ_V, ce qui explique qu'ils soient faisables bien qu'on ne maîtrise pas du tout $\mathscr{G}_{\mathbf{Q}}$.

Si $P \in \mathbf{Q}[X]$, alors $\mathscr{G}_{\mathbf{Q}}$ permute les racines de P, ce qui nous fournit une représentation de permutation V_P de $\mathscr{G}_{\mathbf{Q}}$. On peut montrer que toute $\mathbf{C}$-représentation irréductible de $\mathscr{G}_{\mathbf{Q}}$ apparaît comme une composante irréductible d'une représentation V_P, mais essayer de comprendre $\mathscr{G}_{\mathbf{Q}}$ en énumérant les éléments P de $\mathbf{Q}[X]$, et en décomposant les V_P en composantes irréductibles est à peu près aussi efficace que d'espérer tomber sur une démonstration de l'hypothèse de Riemann en faisant la liste de toutes les propositions logiques. Il y a quand même deux exemples de représentations intéressantes de $\mathscr{G}_{\mathbf{Q}}$ que l'on peut obtenir de cette manière.

• *Racines carrées.* Si $d \in \mathbf{Q}^*$ n'est pas un carré dans $\mathbf{Q}$, alors $\sqrt{d} \notin \mathbf{Q}$, et si $\sigma \in \mathscr{G}_{\mathbf{Q}}$, il existe $\eta_d(\sigma) \in \{\pm 1\}$ tel que $\sigma(\sqrt{d}) = \eta_d(\sigma)\sqrt{d}$, et il est facile de vérifier que $\sigma \mapsto \eta_d(\sigma)$ est un caractère linéaire de $\mathscr{G}_{\mathbf{Q}}$.

• *Racines de l'unité.* Soient D un entier $\geqslant 3$ et $\alpha = e^{2i\pi/D}$. Alors $\alpha^D = 1$ et $\alpha^d \neq 1$ pour tout diviseur strict d de D. Maintenant, si $\sigma \in \mathscr{G}_{\mathbf{Q}}$, alors $\sigma(\alpha)^D = \sigma(\alpha^D) = 1$ et $\sigma(\alpha)^d = \sigma(\alpha^d) \neq 1$, pour tout diviseur strict de D. D'où l'existence de $\chi_{\mathrm{cycl},D}(\sigma) \in (\mathbf{Z}/D\mathbf{Z})^*$ tel que $\sigma(\alpha) = e^{2i\pi\chi_{\mathrm{cycl},D}(\sigma)/D} = \alpha^{\chi_{\mathrm{cycl},D}(\sigma)}$. On a alors $\sigma(\alpha^n) = \alpha^{n\chi_{\mathrm{cycl},D}(\sigma)}$, quel que soit $n \in \mathbf{Z}$; on en déduit que $\chi_{\mathrm{cycl},D} : \mathscr{G}_{\mathbf{Q}} \to (\mathbf{Z}/D\mathbf{Z})^*$ est un morphisme de groupes [13]. Ceci permet d'associer une représentation continue ρ_χ de $\mathscr{G}_{\mathbf{Q}}$, de dimension 1, à tout caractère de Dirichlet primitif : si χ est un tel caractère, et si D est son conducteur, alors $\rho_\chi = \chi \circ \chi_{\mathrm{cycl},D}$ est un morphisme de groupes de $\mathscr{G}_{\mathbf{Q}}$ dans $\mathbf{C}^*$.

Théorème G.1.1. — (Kronecker-Weber) *Toute représentation de dimension* 1 *de* $\mathscr{G}_{\mathbf{Q}}$ *est de la forme* ρ_χ*, où* χ *est un caractère de Dirichlet primitif.*

Ce théorème a été énoncé par Kronecker (1853), mais il a fallu attendre 1886 pour une démonstration (presque) juste (par Weber).

Au vu du théorème de Kronecker-Weber, on peut se demander ce qui se passe si on considère les représentations de dimension 1 de $\mathscr{G}_K$, où K est un corps de nombres, ou bien si on considère les représentations de dimension n de $\mathscr{G}_{\mathbf{Q}}$, avec n fixé, ou encore si on mélange les deux problèmes et on considère les représentations de dimension n de $\mathscr{G}_K$, où K est un corps de nombres et n est fixé. La description des représentations de dimension 1 de $\mathscr{G}_K$ est ce qu'on appelle la *théorie du corps de classes* (qui a occupé les arithméticiens pendant une bonne trentaine d'années au début du 20-ième siècle).

La dimension $n \geqslant 2$ a longtemps été considérée comme sans espoir.

13. C'est le *caractère cyclotomique.*

3. Fonctions L d'Artin

Soit $\mathscr{P}$ l'ensemble des nombres premiers. Si $p \in \mathscr{P}$, on note $|\ |_p$ la norme p-adique sur $\mathbf{Q}$, et on choisit [14] une extension de $|\ |_p$ en une norme sur $\overline{\mathbf{Q}}$. On note alors $\mathscr{G}_{\mathbf{Q}_p}$ l'ensemble des $\sigma \in \mathscr{G}_{\mathbf{Q}}$ qui sont des isométries pour $|\ |_p$. On note I_p le sous-groupe de $\mathscr{G}_{\mathbf{Q}_p}$ des σ tels que $\sigma(e^{2i\pi/\mathrm{D}}) = e^{2i\pi/\mathrm{D}}$, quel que soit D premier à p. On dit qu'un élément σ de $\mathscr{G}_{\mathbf{Q}_p}$ est un frobenius en p, si $\sigma(e^{2i\pi/\mathrm{D}}) = e^{2i\pi p/\mathrm{D}}$, quel que soit D premier à p. Par définition de I_p, deux frobenius en p ne diffèrent que par un élément de I_p. On choisit un frobenius frob_p en p.

Soit V une représentation de $\mathscr{G}_{\mathbf{Q}}$ de dimension n. Si p est un nombre premier, on note $\mathrm{V}^{\mathrm{I}_p}$ le sous-espace de V fixe par I_p. On démontre [15] que l'on a $\mathrm{V}^{\mathrm{I}_p} = \mathrm{V}$ pour presque tout [16] p. L'action de frob_p sur $\mathrm{V}^{\mathrm{I}_p}$ ne dépend alors pas du choix de frob_p, et $\mathrm{E}_p(\mathrm{V},\mathrm{T}) = \det(1-\mathrm{T}\rho_{\mathrm{V}^{\mathrm{I}_p}}(\mathrm{frob}_p))$ ne dépend ni du choix de frob_p, ni de celui de l'extension de $|\ |_p$ à $\overline{\mathbf{Q}}$. C'est un polynôme de degré $\dim \mathrm{V}^{\mathrm{I}_p}$, et donc $\mathrm{E}_p(\mathrm{V},\mathrm{T})$ est un polynôme de degré n pour presque tout p. On définit alors la fonction L d'Artin $\mathrm{L}(\mathrm{V},s)$ attachée à V par le produit eulérien

$$\mathrm{L}(\mathrm{V},s) = \prod_{p\in\mathscr{P}} \mathrm{E}_p(\mathrm{V},p^{-s})^{-1}.$$

Exemple G.1.2. — (i) Si $\mathrm{V} = \mathbf{1}$ est la représentation triviale, alors $\mathrm{V}^{\mathrm{I}_p} = \mathrm{V}$ et on a $\mathrm{E}_p(\mathrm{V},\mathrm{T}) = 1-\mathrm{T}$, quel que soit p. On a donc $\mathrm{L}(\mathbf{1},s) = \prod_{p\in\mathscr{P}}(1-p^{-s})^{-1} = \zeta(s)$.

(ii) Plus généralement, si χ est un caractère de Dirichlet primitif, on a $\mathrm{L}(\rho_\chi,s) = \mathrm{L}(\chi,s)$.

(iii) Soit $d \in \mathbf{Z}$ divisible par le carré d'aucun nombre premier, et soient D et χ_{D} le caractère de Dirichlet modulo D à valeurs dans $\{\pm 1\}$ apparaissant dans l'introduction. La loi de réciprocité quadratique de l'introduction peut se reformuler comme une égalité $\mathrm{L}(\eta_d,s) = \mathrm{L}(\chi_{\mathrm{D}},s)$ entre une fonction L d'Artin et une fonction L de Dirichlet.

(iv) Si V_1 et V_2 sont deux représentations de $\mathscr{G}_{\mathbf{Q}}$, et si $\mathrm{V} = \mathrm{V}_1 \oplus \mathrm{V}_2$, alors on a $\mathrm{L}(\mathrm{V},s) = \mathrm{L}(\mathrm{V}_1,s)\mathrm{L}(\mathrm{V}_2,s)$. Par exemple, la représentation $\mathrm{V} = \mathrm{Ind}_{\mathscr{G}_{\mathbf{Q}[\sqrt{d}]}}^{\mathscr{G}_{\mathbf{Q}}} \mathbf{1}$, se décompose sous la forme $\mathrm{V} = \mathbf{1} \oplus \eta_d$, et l'identité $\zeta_{\mathrm{A}_{\mathrm{D}}}(s) = \zeta(s)\mathrm{L}(\chi_{\mathrm{D}},s)$ de l'introduction est une traduction de l'identité $\mathrm{L}(\mathrm{V},s) = \mathrm{L}(\mathbf{1},s)\mathrm{L}(\eta_d,s)$.

Le *degré d'une fonction* L *d'Artin* est la dimension de la représentation de $\mathscr{G}_{\mathbf{Q}}$ sous-jacente ; c'est aussi le degré de presque tous les facteurs d'Euler. D'après le théorème

14. Pour construire une telle norme, il suffit de choisir un isomorphisme de $\overline{\mathbf{Q}}$ sur la clôture intégrale de $\mathbf{Q}$ dans $\overline{\mathbf{Q}}_p$ (cf. alinéa 20.4.5 du Vocabulaire, ainsi que les n$^{\mathrm{os}}$ 8.3 et 8.8 du Vocabulaire pour le fait que la clôture intégrale de $\mathbf{Q}$ dans $\overline{\mathbf{Q}}_p$ est effectivement isomorphe à $\overline{\mathbf{Q}}$). On démontre, par des techniques de théorie algébrique des nombres, que si on a deux extensions $|\ |_{p,1}$ et $|\ |_{p,2}$ de $|\ |_p$ à $\overline{\mathbf{Q}}$, alors il existe $\sigma \in \mathscr{G}_{\mathbf{Q}}$ tel que $|x|_{p,2} = |\sigma(x)|_{p,1}$, quel que soit $x \in \overline{\mathbf{Q}}$, ce qui explique que ce qui suit ne dépend pas du choix de cette extension.

15. C'est encore un résultat de théorie algébrique des nombres.

16. L'expression « pour presque tout p » signifie « à l'exception d'un nombre fini de p ».

de Kronecker-Weber, les fonctions L de Dirichlet (en incluant la fonction zêta) décrivent l'ensemble des fonctions L d'Artin de degré 1. Il résulte des th. VII.3.4 et VII.4.4, que :

Théorème G.1.3. — *Une fonction* L *d'Artin de degré* 1 *possède un prolongement méromorphe à* $\mathbf{C}$ *tout entier, holomorphe en dehors d'un pôle simple en* $s = 1$, *si* $\mathrm{L} = \zeta$.

Conjecture G.1.4. — (Artin, 1923) *Si* V *est irréductible de dimension* $\geqslant 2$, *alors* $\mathrm{L}(\mathrm{V}, s)$ *a un prolongement holomorphe à* $\mathbf{C}$ *tout entier.*

Cette conjecture est très loin d'être démontrée, mais il y a eu récemment des progrès spectaculaires en dimension 2.

La théorie du corps de classes permet (cf. th. G.1.8 et G.1.9) de prouver que, si K est un corps de nombres, et si χ est un caractère linéaire de $\mathscr{G}_{\mathrm{K}}$, alors $\mathrm{L}(\mathrm{Ind}_{\mathscr{G}_{\mathrm{K}}}^{\mathscr{G}_{\mathbf{Q}}}\chi, s)$ est une fonction holomorphe sur $\mathbf{C}$, sauf si si $\chi = \mathbf{1}$ où elle est holomorphe en dehors d'un pôle simple en $s = 1$.

Artin lui-même a démontré, en utilisant ce résultat et la théorie des représentations des groupes finis (plus précisément le th. I.3.19 dont c'était la motivation principale [17]) qu'une puissance de $\mathrm{L}(\mathrm{V}, s)$ a un prolongement méromorphe à $\mathbf{C}$ tout entier. Si on utilise le th. de Brauer (th. I.3.20) au lieu du th. d'Artin, on peut montrer (et c'était la motivation principale de Brauer) que $\mathrm{L}(\mathrm{V}, s)$ a un prolongement méromorphe à $\mathbf{C}$ tout entier.

R. Langlands (1967) a proposé un gigantesque programme dont un des buts est la démonstration de la conjecture d'Artin.

4. Fonctions L de degré 2

4.1. *Représentations impaires et formes modulaires*

Soit D un entier, et soit $\Gamma_0(\mathrm{D})$ l'ensemble des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ à coefficients dans $\mathbf{Z}$, vérifiant $ad - bc = 1$ et $c \equiv 0$ modulo D. C'est le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$, image inverse du groupe des matrice triangulaires supérieures dans $\mathbf{SL}_2(\mathbf{Z}/\mathrm{D}\mathbf{Z})$.

Si $k \geqslant 1$ est un entier, et si χ est un caractère de Dirichlet modulo D, une forme quasi-modulaire f de poids k, niveau [18] D et caractère χ est une fonction holomorphe sur $\mathscr{H}$, telle que $f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$ quel que soit $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathrm{D})$. Une forme

17. Soit H le noyau de ρ_{V}, et soit $\mathrm{G} = \mathscr{G}_{\mathbf{Q}}/\mathrm{H}$; c'est un groupe fini, et V peut être considérée comme une représentation de G. D'après le th. I.3.19, il existe $d_{\mathrm{V}} \in \mathbf{N}$, une famille $(\mathrm{C}_i, \chi_i, n_i)$, pour $i \in \mathrm{I}$, où C_i est un sous-groupe (cyclique) de G, χ_i est un caractère linéaire de C_i, et $n_i \in \mathbf{Z}$, telle que $\chi_{\mathrm{V}} = \sum_{i\in\mathrm{I}} n_i \mathrm{Ind}_{\mathrm{C}_i}^{\mathrm{G}}\chi_i$. Soit alors K_i le corps de nombres tel que $\mathscr{G}_{\mathrm{K}_i}$ soit l'image réciproque de C_i dans $\mathscr{G}_{\mathbf{Q}}$. On peut considérer χ_i comme un caractère linéaire de $\mathscr{G}_{\mathrm{K}_i}$, et on déduit du (iv) de l'exemple G.1.2, la relation

$$\mathrm{L}(\mathrm{V}, s)^{d_{\mathrm{V}}} = \prod_{i\in\mathrm{I}} \mathrm{L}(\mathrm{Ind}_{\mathscr{G}_{\mathrm{K}_i}}^{\mathscr{G}_{\mathbf{Q}}}\chi_i, s)^{n_i}.$$

18. Si $\mathrm{D} = 1$, on a $\Gamma_0(\mathrm{D}) = \mathbf{SL}_2(\mathbf{Z})$ et $\chi = 1$. Comme $\mathbf{SL}_2(\mathbf{Z})$ est engendré par $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, la condition de quasi-modularité est équivalente aux conditions $f(z+1) = f(z)$ et $z^{-k}f(-1/z) = f(z)$ utilisée dans les exercices du § VII.5.

quasi-modulaire est en particulier périodique de période 1, et donc a un développement de Fourier (*q-développement*) du type

$$f(z) = \sum_{n\in\mathbf{Z}} a_n(f) q^n, \quad \text{avec } q = e^{2i\pi z}.$$

On dit que f est une *forme modulaire parabolique* (ou cuspidale) de poids k, niveau D et caractère χ si elle est quasi-modulaire, et si elle est *à décroissance rapide à l'infini*, ce qui signifie que $\mathrm{Im}(z)^{\mathrm{N}}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ est bornée sur le demi-plan $\mathrm{Im}(z) \geqslant 1$, quels que soient [19] $\mathrm{N} \in \mathbf{N}$ et $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z})$. On note $\mathrm{S}_k(\mathrm{D},\chi)$ l'espace de ces formes.

Si $f \in \mathrm{S}_k(\mathrm{D},\chi)$, on a en particulier $a_n(f) = 0$, si $n \leqslant 0$ à cause de la condition de décroissance à l'infini, et on démontre comme dans l'ex. VII.6.3 que $a_n(f) = \mathrm{O}(n^{k/2})$, ce qui permet d'associer à f une fonction L définie par

$$\mathrm{L}(f,s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^{+\infty} f(iy) y^s \frac{dy}{y} = \sum_{n=1}^{+\infty} \frac{a_n(f)}{n^s}.$$

Un petit calcul montre que $f \mapsto f_{|_k} w$, où $f_{|_k} w$ est définie par $(f_{|_k} w)(z) = z^{-k} f(-1/\mathrm{D}z)$, envoie $\mathrm{S}_k(\mathrm{D},\chi)$ dans $\mathrm{S}_k(\mathrm{D},\overline{\chi})$. Ceci permet, en coupant, comme dans les ex. VII.6.3, VII.6.6, l'intégrale ci-dessus en $\sqrt{\mathrm{D}}$, de démontrer que $\mathrm{L}(f,s)$ a un prolongement holomorphe à $\mathbf{C}$ tout entier et vérifie une équation fonctionnelle reliant s et $k-s$. On dit que f est *primitive*, si $\mathrm{L}(f,s)$ admet :

• un développement en produit de facteurs d'Euler

$$\mathrm{L}(f,s) = \prod_{p|\mathrm{D}} \frac{1}{1-a_p(f)p^{-s}} \prod_{p\nmid\mathrm{D}} \frac{1}{1-a_p(f)p^{-s}+\chi(p)p^{k-1-2s}},$$

• une équation fonctionnelle du type $\Lambda(f,k-s) = w\Lambda(f^*,s)$, où $f^*(z) = \overline{f(-\overline{z})}$, w est un nombre complexe de module 1, et

$$\Lambda(f,s) = \frac{\Gamma(s)}{(2\pi)^s} \mathrm{D}^{s/2} \mathrm{L}(f,s).$$

L'existence de formes modulaires primitives relève du miracle, mais Atkin et Lehner ont démontré que les $f(\frac{az+b}{d})$, où f décrit les formes primitives de poids k, et a, b, d les entiers ($a \neq 0$ et $d \neq 0$) forment une famille génératrice de l'espace vectoriel engendré par les formes paraboliques de poids k de tout niveau.

Théorème G.1.5. — *Si $\rho : \mathscr{G}_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{C})$ est une représentation irréductible impaire* [20]*, alors il existe une forme modulaire primitive f, de poids 1, telle que $\mathrm{L}(f,s) = \mathrm{L}(\rho,s)$. En particulier, la conjecture d'Artin est vérifiée pour une telle représentation.*

19. Comme $f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$, si $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathrm{D})$, il suffit de vérifier ceci pour un système de représentants de $\Gamma_0(\mathrm{D})\backslash\mathbf{SL}_2(\mathbf{Z})$, qui est un ensemble fini.

20. Cela signifie que $\rho(\mathrm{frob}_\infty) \neq \pm 1$ et donc que $\det\rho(\mathrm{frob}_\infty) = -1$, ce qui est, de loin, le cas le plus fréquent. Si $\det\rho(\mathrm{frob}_\infty) = 1$, la représentation ρ est dite *paire*.

Ce théorème est tout récent ; il a été annoncé en janvier 2007, et l'article a été complété en octobre 2008. Le cas où l'image [21] de ρ dans $\mathbf{PGL}_2(\mathbf{C})$ est un groupe diédral remonte aux années 30, et résulte des travaux de Artin et Hecke. L'un des premiers succès du programme de Langlands a été de démontrer un tel résultat dans le cas où l'image n'est pas A_5 (Langlands (1980) et Tunnell (1981)). Ceci couvre en particulier le cas où l'image de ρ dans $\mathbf{GL}_2(\mathbf{C})$ est le groupe [22] $\mathbf{GL}_2(\mathbf{F}_3)$, qui a servi de point de départ à Wiles pour démontrer le théorème de Fermat. Les méthodes de Wiles ont été transformées en une machine très efficace, par des mathématiciens de toute la planète, pour passer d'un point à un autre dans l'ensemble des représentations de dimension 2 de $\mathscr{G}_{\mathbf{Q}}$. La touche finale vient d'être apportée [23] par Kisin (australien, en poste à Havard), Khare (indien, en poste à Los Angeles) et Wintenberger (Strasbourg). Un des points amusants de la démonstration est qu'elle passe par une récurrence sur l'ensemble des nombres premiers.

4.2. *Un exemple*

Comme on l'a déjà remarqué, si $\mathrm{P} = \mathrm{X}^d + \alpha_{d-1}\mathrm{X}^{d-1} + \cdots + \alpha_0 \in \mathbf{Z}[\mathrm{X}]$, alors $\mathscr{G}_{\mathbf{Q}}$ permute les racines de P ; on note V_{P} la représentation de permutation de $\mathscr{G}_{\mathbf{Q}}$ qui s'en déduit. Comme toute représentation de permutation, V_{P} peut se décomposer sous la forme $\mathrm{V}_{\mathrm{P}} = \mathbf{1} + \rho_{\mathrm{P}}$, où $\mathbf{1}$ est la représentation triviale. Cette décomposition donne lieu à une factorisation $\mathrm{L}(\mathrm{V}_{\mathrm{P}}, s) = \zeta(s)\mathrm{L}(\rho_{\mathrm{P}}, s)$.

Si p est un nombre premier, on note $\mathrm{N}_p(\mathrm{P})$ le nombre de racines de P dans $\mathbf{F}_p$.

• Si $\mathrm{P} = \mathrm{X}^2 + \mathrm{X} + 6$, le discriminant de P est -23 et la loi de réciprocité quadratique nous fournit un caractère de Dirichlet $\chi_{23} : (\mathbf{Z}/23\mathbf{Z})^* \to \{\pm 1\}$ tel que $\mathrm{N}_p(\mathrm{P}) = 1 + \chi_{23}(p)$, pour tout p (pour $p = 23$, on a $\chi_{23}(p) = 0$ par convention, et il y a une racine double dans $\mathbf{F}_{23}$). Alors $\mathrm{L}(\rho_{\mathrm{P}}, s) = \mathrm{L}(\chi_{23}, s)$ est sans mystère.

• Si $\mathrm{P} = \mathrm{X}^3 - \mathrm{X} - 1$, le discriminant est une puissance de 23, et il y a une racine double dans $\mathbf{F}_{23}$. On a $\mathrm{L}(\rho_{\mathrm{P}}, s) = \prod_{p \in \mathscr{P}} \frac{1}{1-(\mathrm{N}_p(\mathrm{P})-1)p^{-s}+\chi_{23}(p)p^{-2s}}$ (la présence de χ_{23} trahit le fait que $\mathbf{Q}(\sqrt{-23})$ est un sous-corps du corps engendré par les racines de P). On définit des a_n, pour $n \geqslant 1$, en écrivant $\mathrm{L}(\rho_{\mathrm{P}}, s)$ comme une série de Dirichlet $\sum_{n \geqslant 1} a_n\, n^{-s}$ (on a donc $a_p = \mathrm{N}_p(\mathrm{P}) - 1$ si p est premier, et la série $\sum_{n \geqslant 1} a_n\, n^{-s}$ encode le comportement de

21. L'image de ρ dans $\mathbf{GL}_2(\mathbf{C})$ peut être arbitrairement grande car on peut toujours tordre une représentation par un caractère linéaire attaché à un caractère de Dirichlet. Par contre, si on regarde l'image de ρ dans le quotient $\mathbf{PGL}_2(\mathbf{C})$ de $\mathbf{GL}_2(\mathbf{C})$ par le sous-groupe des homothéties, on tue ce degré de liberté, et l'image de ρ est soit de type diédral (groupe des symétries d'un polygone régulier), soit isomorphe à A_4, S_4 ou A_5. Le cas le plus difficile est celui de A_5 car ce groupe est simple contrairement aux autres groupes de la liste qui se dévissent en une suite de groupes commutatifs.

22. Les représentations du type IV dans la figure 4 de l'annexe C sont de dimension 2 pour $\mathbf{GL}_2(\mathbf{F}_3)$.

23. Ils obtiennent ce résultat en démontrant une conjecture plus fine et plus générale de J-P. Serre (1984) qui a servi de fil conducteur pour tous les résultats du sujet postérieurs à ceux de Langlands et Tunnell, dont la démonstration du théorème de Fermat.

P modulo p quand p varie). Le th. G.1.5 pour $\mathrm{L}(\rho_{\mathrm{P}}, s)$ résulte des identités

$$\sum_{n\geqslant 1} a_n q^n = \frac{1}{2}\Big(\sum_{x,y\in\mathbf{Z}} q^{x^2+xy+6y^2} - \sum_{x,y\in\mathbf{Z}} q^{2x^2+xy+3y^2}\Big) = q\prod_{k\geqslant 1}(1-q^k)(1-q^{23k})$$

La première de ces identités se démontre grâce à la théorie du corps de classes qui permet d'écrire ρ_{P} comme l'induite d'un caractère linéaire de $\mathscr{G}_{\mathbf{Q}(\sqrt{-23})}$. La seconde se démontre par des techniques similaires à celles employées dans le prob. H.11 pour prouver que $q^{1/24}\prod_{k\geqslant 1}(1-q^k) = \sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$, le point étant que les deux membres sont des formes modulaires de poids 1 (si $q = e^{2i\pi z}$, le membre de droite est $\eta(z)\eta(23z)$, où η est la fonction êta de Dedekind et le membre de gauche s'exprime en termes de la fonction θ de Jacobi).

4.3. *Représentations paires et formes de Maass*

Les formes de Maass sont des objets beaucoup plus récents que les formes modulaires puisqu'elles n'ont été introduites, par H. Maass, qu'en 1949.

Une *forme de Maass* f de niveau D, caractère χ et valeur propre $\lambda \in \mathbf{C}$ est une fonction $\mathscr{C}^\infty$ sur $\mathscr{H}$ (vu comme un ouvert de $\mathbf{R}^2$) et vérifiant les conditions suivantes :

(i) $f(\frac{az+b}{cz+d}) = \chi(d)f(z)$, quel que soit $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_0(\mathrm{D})$;

(ii) $\Delta f = \lambda f$, où $\Delta = -y^2\big(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\big)$ est le laplacien hyperbolique.

(iii) f est à décroissance rapide à l'infini.

Une telle forme a un développement de Fourier du type [24]

$$f(z) = \sum_{n\in\mathbf{Z}-\{0\}} a_n(f)\,\sqrt{y}\,\mathrm{K}_\nu(2\pi|n|y)e^{2i\pi nx},$$

où $\frac{1}{4} - \nu^2 = \lambda$ et $\mathrm{K}_\nu(y) = \frac{1}{2}\int_0^{+\infty} e^{-y(t+t^{-1})/2}t^\nu\frac{dt}{t}$ est une *fonction de Bessel* (cf. ex. IV.1.9 et prob. H.10) dont une des vertus est de vérifier, si $\mathrm{Re}(s) > |\mathrm{Re}(\nu)|$,

$$\int_0^{+\infty} \mathrm{K}_\nu(y)y^s\frac{dy}{y} = 2^{s-2}\Gamma\big(\frac{s+\nu}{2}\big)\Gamma\big(\frac{s-\nu}{2}\big).$$

On dit que f est *paire* si $f(-\overline{z}) = f(z)$ et *impaire* si $f(-\overline{z}) = -f(z)$; toute forme de Maass peut s'écrire comme somme d'une forme paire et d'une forme impaire. On attache une fonction L à une forme de Maass f par la formule $\mathrm{L}(f,s) = \sum_{n=1}^{+\infty}\frac{a_n(f)}{n^s}$, et on a :

$$\int_0^{+\infty} f(iy)y^{s-1/2}\frac{dy}{y} = \pi^{-s}\Gamma\big(\frac{s+\nu}{2}\big)\Gamma\big(\frac{s-\nu}{2}\big)\mathrm{L}(f,s), \quad \text{si } f \text{ est paire,}$$

$$\int_0^{+\infty} \frac{1}{4i\pi}\frac{\partial f}{\partial x}(iy)y^{s+1/2}\frac{dy}{y} = \pi^{-s}\Gamma\big(\frac{s+1+\nu}{2}\big)\Gamma\big(\frac{s+1-\nu}{2}\big)\mathrm{L}(f,s), \quad \text{si } f \text{ est impaire.}$$

24. L'équation aux dérivées partielles satisfaite par f se traduit en une équation différentielle du second ordre pour les coefficients de Fourier, et une seule des solutions (a multiplication près par une constante) n'explose pas à l'infini.

On dit qu'une forme de Maass f est primitive, si sa fonction L possède :
• un développement en produit de facteurs d'Euler

$$\mathrm{L}(f,s)=\prod_{p|\mathrm{D}}\frac{1}{1-a_p(f)p^{-s}}\prod_{p\nmid\mathrm{D}}\frac{1}{1-a_p(f)p^{-s}+\chi(p)p^{k-1-2s}},$$

• une équation fonctionnelle du type $\Lambda(f,k-s)=w\Lambda(f^*,s)$, où $f^*(z)=\overline{f(-\overline{z})}$, w est un nombre complexe de module 1, $c=0$ ou 1 suivant que f est paire ou impaire, et

$$\Lambda(f,s)=\pi^{-s}\Gamma\Big(\frac{s+c+\nu}{2}\Big)\Gamma\Big(\frac{s+c-\nu}{2}\Big)\mathrm{D}^{s/2}\,\mathrm{L}(f,s).$$

Conjecture G.1.6. — *Si $\rho:\mathscr{G}_{\mathbf{Q}}\to\mathbf{GL}_2(\mathbf{C})$ est une représentation irréductible paire, il existe une forme de Maass primitive f, de valeur propre $\frac{1}{4}$, telle que $\mathrm{L}(f,s)=\mathrm{L}(\rho,s)$.*

Cet énoncé impliquerait la conjecture d'Artin pour une telle représentation. On sait le démontrer, grâce aux travaux de Langlands et J. Tunnell sus-mentionnés, si l'image de ρ dans $\mathbf{PGL}_2(\mathbf{C})$ n'est pas A_5.

5. La théorie du corps de classes

Soit F un corps de nombres [25]. L'ensemble $\mathscr{O}_{\mathrm{F}}$ des $x\in\mathrm{F}$ annulés par un polynôme unitaire $\mathrm{P}\in\mathbf{Z}[\mathrm{X}]$ (dépendant de x) est un sous-anneau de F appelé *anneau des entiers*. Par exemple, si $d\in\mathbf{Z}$ n'est divisible par le carré d'aucun nombre premier, l'anneau des entiers $\mathbf{Q}(\sqrt{d})$ est l'anneau A_{D} de l'introduction.

Un tel anneau n'est pas forcément principal [26], mais tout idéal $\mathfrak{n}$ non nul de $\mathscr{O}_{\mathrm{F}}$ peut s'écrire de manière unique sous la forme [27] $\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_r^{n_r}$, où les $\mathfrak{p}_i$ sont des idéaux premiers distincts [28]. Deux idéaux $\mathfrak{a}$, $\mathfrak{b}$ de $\mathscr{O}_{\mathrm{F}}$ sont premiers entre eux (ce qui, pour un anneau quelconque, signifie que $\mathfrak{a}+\mathfrak{b}=\mathscr{O}_{\mathrm{F}}$), si et seulement si il n'y a pas d'idéal premier de $\mathscr{O}_{\mathrm{F}}$ apparaissant à la fois dans la décomposition de $\mathfrak{a}$ et $\mathfrak{b}$ en idéaux premiers.

On peut généraliser les notions de caractère de Dirichlet et de fonction L de Dirichlet aux corps de nombres. Si $\mathfrak{f}$ est un idéal de $\mathscr{O}_{\mathrm{F}}$, on note $\mathrm{I}_{\mathfrak{f}}$ l'ensemble des idéaux de $\mathscr{O}_{\mathrm{F}}$ premiers à $\mathfrak{f}$. Un *caractère de Hecke* χ (d'ordre fini) modulo $\mathfrak{f}$ est une fonction multiplicative

25. Tous les énoncés qui suivent sont des résultats de base de théorie algébrique des nombres, ce qui ne signifie pas, loin de là, qu'ils sont faciles à établir.

26. Contrairement à ce qu'espéraient Lamé et Cauchy qui se sont disputés, en 1847, la paternité d'une démonstration du th. de Fermat en découlant jusqu'à ce que Kummer mette tout le monde d'accord en fournissant un contrexemple.

27. Un anneau ayant cette propriété est un *anneau de Dedekind*.

28. Si I et J sont deux idéaux d'un anneau A, le produit IJ de I et J est l'idéal de A engendré par les éléments de la forme ab, avec $a\in\mathrm{I}$ et $b\in\mathrm{J}$. Par exemple, si I et J sont principaux engendrés par α et β, alors IJ est l'idéal principal engendré par $\alpha\beta$. Par ailleurs, un idéal $\mathfrak{p}$ est premier si la condition $ab\in\mathfrak{p}$ implique $a\in\mathfrak{p}$ ou $b\in\mathfrak{p}$.

$\chi : \mathrm{I}_{\mathfrak{f}} \to \mathbf{C}^*$, telle que, si $\alpha \in \mathscr{O}_{\mathrm{F}}$ est positif[29], et si $\alpha - 1 \in \mathfrak{f}$, alors $\chi(\mathfrak{n}) = 1$, si $\mathfrak{n}$ est l'idéal principal engendré par α. La *fonction* L *de Hecke* attachée à un caractère de Hecke χ (d'ordre fini) modulo $\mathfrak{f}$ est alors définie par

$$\mathrm{L}(\chi, s) = \sum_{\mathfrak{n} \in \mathrm{I}_{\mathfrak{f}}} \frac{\chi(\mathfrak{n})}{\mathrm{N}(\mathfrak{n})^s}, \quad \text{où } \mathrm{N}(\mathfrak{n}) = |\mathscr{O}_{\mathrm{F}}/\mathfrak{n}|.$$

Comme χ est multiplicatif et comme $\mathfrak{n} \mapsto \mathrm{N}(\mathfrak{n})$ est aussi multiplicatif, les mêmes arguments que pour les fonctions L de Dirichlet montrent que l'on a une décomposition en produit de facteurs d'Euler

$$\mathrm{L}(\chi, s) = \prod_{\mathfrak{p} \in \mathscr{P}_{\mathrm{F}}} \frac{1}{1 - \chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}} = \prod_{p \in \mathscr{P}} \Big(\prod_{\mathfrak{p}|(p)} \frac{1}{1 - \chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}} \Big),$$

et comme $\prod_{\mathfrak{p}|(p)} \mathrm{N}(\mathfrak{p}) = p^{[\mathrm{F}:\mathbf{Q}]}$ pour presque tout p, le facteur $\prod_{\mathfrak{p}|(p)} \big(1 - \chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}\big)$ est un polynôme de degré $[\mathrm{F} : \mathbf{Q}]$ en p^{-s}, sauf pour un nombre fini de p.

Ce qui précède s'applique en particulier au caractère trivial envoyant tout idéal $\mathfrak{n}$ de $\mathscr{O}_{\mathrm{F}}$ sur 1. La fonction L de Hecke associée $\zeta_{\mathrm{F}}(s) = \sum_{\mathfrak{n}} \frac{1}{\mathrm{N}(\mathfrak{n})^s}$ avait été considérée longtemps auparavant par Dedekind ; c'est la *fonction zêta de Dedekind de* F.

Exemple G.1.7. — (i) Si $\mathrm{F} = \mathbf{Q}$, on retombe sur la fonction zêta de Riemann.

(ii) Si $\mathrm{F} = \mathbf{Q}[\sqrt{d}]$, on retombe sur la fonction $\zeta_{\mathrm{A_D}}$ de l'introduction.

Théorème G.1.8. — (Hecke, 1920) *Si χ est un caractère de Hecke primitif, alors* $\mathrm{L}(\chi, s)$ *admet un prolongement méromorphe à* $\mathbf{C}$ *tout entier, holomorphe en dehors d'un pôle simple en $s = 1$ si χ est le caractère trivial.*

La situation est donc exactement la même pour un corps de nombres quelconque que pour $\mathbf{Q}$. La démonstration du théorème de Hecke repose sur les mêmes idées que celles utilisées dans l'ex. VII.6.6 pour démontrer l'existence d'un prolongement méromorphe pour la fonction zêta de Riemann. La présence d'unités dans $\mathscr{O}_{\mathrm{F}}$ rend toutefois les arguments un peu plus délicats.

Le théorème principal de la théorie du corps de classes est alors le suivant.

Théorème G.1.9. — *Si ρ est une représentation de dimension* 1 *de $\mathscr{G}_{\mathrm{F}}$, alors il existe un caractère de Hecke χ de* F*, d'ordre fini, tel que* $\mathrm{L}(\mathrm{Ind}_{\mathscr{G}_{\mathrm{F}}}^{\mathscr{G}_{\mathbf{Q}}} \rho, s) = \mathrm{L}(\chi, s)$.

Le théorème de Kronecker-Weber est déjà un théorème profond, mais sa démonstration est grandement facilitée par l'existence des racines de l'unité qui donne une construction systématique des *extensions abéliennes de* $\mathbf{Q}$ (ce sont les corps de nombres fixés par le noyau d'un caractère linéaire de $\mathscr{G}_{\mathbf{Q}}$). Dans le cas d'un corps de nombres général, on ne

29. Cela signifie que $\sigma(\alpha) > 0$ si $\sigma \in \mathscr{G}_{\mathbf{Q}}$ et $\sigma(\alpha)$ est réel ; il n'y a pas de condition si $\sigma(\alpha)$ n'est pas un nombre réel.

connaît pas de tel procédé pour construire ces extensions [30], ce qui explique, en grande partie, qu'on ait mis tant de temps à démontrer le théorème ci-dessus (il a déjà fallu beaucoup de temps pour arriver à concevoir son énoncé). L'histoire a commencé dans la fin des années 1880 avec Kronecker et Weber, s'est continuée avec Hilbert [31] autour de 1900, et le théorème ci-dessus date de la fin des années 1920, avec des contributions essentielles de Furtwängler, Takagi, Artin et Hasse [32]. Grâce aux efforts de tous ces mathématiciens et de ceux des trois décennies suivantes, on a maintenant une théorie puissante, parfaitement bien comprise, aux énoncés compacts, et qui peut très bien s'utiliser comme une boite noire. Elle fait régulièrement l'objet de cours fondamentaux de M2.

G.2. Le théorème de Kronecker-Weber revisité

Chevalley s'est demandé s'il existait un groupe naturel, construit directement à partir de $\mathbf{Q}$ (resp. de F, où F est un corps de nombres), dont les représentations de dimension 1 seraient exactement les caractères de Dirichlet (resp. les caractères de Hecke d'ordre fini de F) primitifs. Cela l'a mené à la construction (1940) du groupe des idèles [33] esquissée ci-dessous. Nous allons aller à l'envers de l'ordre historique (les adèles sont nés, de la main d'Artin et Whaples, 5 ans plus tard que les idèles (sous le nom fort peu poétique de "valuation vectors")), mais ce sont toujours les idées simples qui viennent en dernier [34]. Les adèles sont construits en considérant simultanément tous les complétés de $\mathbf{Q}$ (resp. d'un corps de nombres F), et Tate a montré dans sa thèse (1950), sous la direction d'Artin, comment l'analyse de Fourier sur les adèles permet de démontrer naturellement toutes les propriétés analytiques des fonctions L de Dirichlet (resp. de Hecke) rencontrées au chap. VII (resp. mentionnées au n° 5 du § G.1).

1. Adèles

1.1. *Le théorème d'Ostrowski*

En dehors de la norme usuelle que nous noterons $|\ |_\infty$, on peut définir, pour chaque nombre premier p, une norme p-adique $|\ |_p$ sur $\mathbf{Q}$. Rappelons que celle-ci est définie (cf. alinéa 20.4 du § 1) par la formule $|\frac{a}{b}|_p = p^{-v_p(a)+v_p(b)}$, si $a, b \in \mathbf{Z} - \{0\}$, et $v_p(n)$ est le plus grand entier v tel que p^v divise n.

30. C'est un des derniers problèmes (généralisant le "liebster Jugendtraum" de Kronecker) énoncés par Hilbert en 1900 qu'on ne sait toujours pas résoudre.

31. Trois des problèmes de Hilbert (les 9-ième, 11-ième et 12-ième) sont reliés à la question.

32. L'école allemande a joué un rôle absolument primordial dans le sujet, et tous les articles de l'époque (y compris ceux du mathématicien japonais Takagi) sont en allemand.

33. Le mot "idèle" vient du mot "idéal" (dans tous les sens du terme...) ; il a donné naissance 20 ans plus tard au mot "adèle", et Roubaud a fait d'Adèle et Idèle des jumelles dans "La belle Hortense".

34. Comme le dit Weil : " Pour franchir toutes ces étapes, un bon étudiant ne met guère plus de jours à présent qu'il n'y a fallu d'années à l'époque..."

Théorème G.2.1. — (Ostrowski, 1918) *Une norme non triviale sur* $\mathbf{Q}$ *est équivalente à la norme usuelle* $|\ |_\infty$ *ou à la norme p-adique* $|\ |_p$ *pour un unique nombre premier* p.

Démonstration. — Commençons par supposer qu'il existe $k \in \mathbf{N}$ tel que $\|k\| > 1$. Comme $\|1\| = 1$, l'inégalité triangulaire implique $\|k\| \leqslant k$ et il existe $\alpha \in]0,1]$ tel que l'on ait $\|k\| = k^\alpha$. Soit $m \in \mathbf{N}$. On peut écrire m en base k sous la forme $m = \sum_{i=0}^{n} a_i k^i$ avec $a_i \in \{0, 1, \ldots, k-1\}$ et $a_n \neq 0$ de telle sorte que l'on a $m \geqslant k^n$. Comme $\|a_i\| \leqslant a_i \leqslant k-1$ et $\|k^i\| = \|k\|^i$, on obtient la majoration

$$\|m\| \leqslant (k-1)\sum_{i=1}^{n} k^{i\alpha} = \frac{k-1}{k^\alpha - 1}(k^{(n+1)\alpha} - 1) \leqslant \frac{k^\alpha(k-1)}{k^\alpha - 1} k^{n\alpha} \leqslant \mathrm{C}m^\alpha,$$

où $\mathrm{C} = \frac{k^\alpha(k-1)}{k^\alpha - 1}$ est indépendant de m. On peut appliquer cette inégalité à m^n, ce qui nous donne $\|m\|^n \leqslant \mathrm{C}m^{n\alpha}$ et, prenant la racine n-ième de cette égalité et passant à la limite, l'inégalité $\|m\| \leqslant m^\alpha$. En échangeant les rôles de k et m, on en déduit que cette inégalité est une égalité, si $\|m\| > 1$.

Maintenant, si $m \in \mathbf{N} - \{0\}$ est quelconque, il existe $n \in \mathbf{N}$ tel que l'on ait $\|k^n m\| > 1$. On a alors $\|m\| = \|k^n\|^{-1}\|k^n m\| = k^{-\alpha n}(k^n m)^\alpha = m^\alpha$, ce qui montre que l'on a égalité quel que soit $m \in \mathbf{N}$ puis, utilisant la multiplicativité de la norme et le fait que $\|-1\| = 1$, que $\|x\| = |x|_\infty^\alpha$ quel que soit $x \in \mathbf{Q}$. On en déduit que s'il existe $k \in \mathbf{N}$ tel que $\|k\| > 1$, alors $\|\ \|$ est équivalente à la norme usuelle.

Dans le cas contraire, on a $\|\ell\| \leqslant 1$ pour tout nombre premier ℓ. Comme on a supposé $\|\ \|$ non triviale, il existe au moins un nombre premier p tel que $\|p\| < 1$. Si il en existe un autre q, alors quel que soit $n \in \mathbf{N}$, on peut, d'après le théorème de Bézout, trouver $u_n, v_n \in \mathbf{Z}$ tels que l'on ait $u_n p^n + v_n q^n = 1$. On obtient donc

$$1 = \|1\| = \|u_n p^n + v_n q^n\| \leqslant \|u_n\| \cdot \|p\|^n + \|v_n\| \cdot \|q\|^n \leqslant \|p\|^n + \|q\|^n,$$

ce qui est impossible pour n assez grand. Il existe donc un et un seul nombre premier p tel que $\|p\| < 1$ et $\|\ \|$ est équivalente à la norme p-adique. Ceci termine la démonstration.

Le résultat suivant est une conséquence immédiate de l'unicité de la décomposition d'un entier en produit de facteurs premiers, mais est très important ; c'est ce qui justifie la normalisation utilisée pour $|\ |_p$.

Théorème G.2.2. — (Formule du produit) *Si* $x \in \mathbf{Q}^*$, *alors*

$$|x|_\infty \cdot \prod_{p \text{ premier}} |x|_p = 1.$$

1.2. *L'anneau des adèles de* $\mathbf{Q}$

On renvoie à l'alinéa 20.4 du § 1 pour ce qui concerne la construction des nombres p-adiques et leurs propriétés élémentaires.

Soit $\mathscr{V} = \{\infty\} \cup \mathscr{P}$. Les éléments de $\mathscr{V}$ sont les *places* de $\mathbf{Q}$. La place ∞ est la *place à l'infini* et les $p \in \mathscr{P}$ sont les *places finies*. Si $v \in \mathscr{V}$, on note $\mathbf{Q}_v$ le complété de $\mathbf{Q}$ correspondant ; on a donc $\mathbf{Q}_\infty = \mathbf{R}$.

D'après le théorème d'Ostrowski, les complétés de $\mathbf{Q}$ sont exactement les $\mathbf{Q}_v$, pour $v \in \mathscr{V}$. Il est donc naturel [35] d'essayer de considérer tous ces complétés ensemble. On peut plonger $\mathbf{Q}$ diagonalement dans $\prod_{v \in \mathscr{V}} \mathbf{Q}_v$, c'est-à-dire en envoyant $a \in \mathbf{Q}$ sur $(x_v)_{v \in \mathscr{V}}$,

35. C'est naturel, mais il s'est écoulé plus de 50 ans entre la construction des nombres p-adiques par K. Hensel et les constructions qui vont suivre.

avec $x_v = a$, quel que soit $v \in \mathscr{V}$. On a alors $x_p \in \mathbf{Z}_p$ sauf si p divise le dénominateur de a, ce qui montre que l'image de $\mathbf{Q}$ est incluse dans le sous-anneau de $\prod_{v\in\mathscr{V}} \mathbf{Q}_v$ des $x = (x_\infty, \dots, x_p, \dots)$, avec $x_p \in \mathbf{Z}_p$ pour presque tout p. Cet anneau est l'*anneau des adèles* $\mathbf{A}$ de $\mathbf{Q}$; c'est le *produit restreint* des $\mathbf{Q}_v$ relativement aux $\mathbf{Z}_p$, pour $p \in \mathscr{P}$. On note souvent $(x_\infty, x^{]\infty[})$ un élément x de $\mathbf{A}$, et $x^{]\infty[}$ est la partie finie (i.e. en dehors de ∞) de x. Si $v \in \mathscr{V}$, on peut identifier $\mathbf{Q}_v$ au sous-anneau de $\mathbf{A}$ des x dont toutes les composantes sont nulles sauf la composante en v.

On munit $\mathbf{A}$ de la *topologie du produit restreint* obtenue en prenant comme base d'ouverts les $\prod_{v\in\mathrm{S}} \mathrm{U}_v \times \prod_{p\notin\mathrm{S}} \mathbf{Z}_p$, où S décrit les parties finies de $\mathscr{V}$ contenant ∞, et U_v, pour $v \in \mathrm{S}$, décrit les ouverts de $\mathbf{Q}_v$. Les propositions G.2.3 et G.2.4 ci-dessous montrent que $\mathbf{Q}$ est discret dans $\mathbf{A}$, mais n'est pas loin d'être dense.

Proposition G.2.3. — (i) *Tout élément x de $\mathbf{A}$ peut s'écrire de manière unique sous la forme $x = \alpha + y$, avec $\alpha \in \mathbf{Q}$ et $y \in [0,1[\times\widehat{\mathbf{Z}}$, où $\widehat{\mathbf{Z}} = \prod_{p\in\mathscr{P}} \mathbf{Z}_p$.*

(ii) *$\mathbf{Q}$ est discret dans $\mathbf{A}$ et $\mathbf{A}/\mathbf{Q}$ est compact.*

Démonstration. — (i) Commençons par démontrer qu'une telle écriture, si elle existe, est unique. Si $\alpha_1 + y_1 = \alpha_2 + y_2$, avec $\alpha_1, \alpha_2 \in \mathbf{Q}$ et $y_1, y_2 \in [0,1[\times\widehat{\mathbf{Z}}$, alors en particulier, on a $\alpha_2 - \alpha_1 \in \mathbf{Z}_p$ quel que soit $p \in \mathscr{P}$, et donc $\alpha_2 - \alpha_1 \in \mathbf{Z}$. Mais alors $\alpha_1 + y_{1,\infty} = \alpha_2 + y_{2,\infty}$ implique, puisque $y_{1,\infty}, y_{2,\infty} \in [0,1[$, que $\alpha_2 = \alpha_1$, et donc aussi que $y_2 = y_1$. D'où l'unicité.

Passons à l'existence. Soit S un sous-ensemble fini de $\mathscr{P}$ tel que $x_p \in \mathbf{Z}_p$, si $p \notin \mathrm{S}$. Comme $\mathbf{Z}[\frac{1}{p}]$ est dense dans $\mathbf{Q}_p$ d'après l'alinéa 20.4.3 du Vocabulaire, il existe, pour tout $p \in \mathrm{S}$, un élément α_p de $\mathbf{Z}[\frac{1}{p}]$ tel que $x_p - \alpha_p \in \mathbf{Z}_p$. Mais alors $x' = x - \sum_{p\in\mathrm{S}} \alpha_p \in \mathbf{R} \times \widehat{\mathbf{Z}}$, et il suffit de poser $\alpha = [x'_\infty] + \sum_{p\in\mathrm{S}} \alpha_p$ et $y = x' - [x'_\infty]$ (où $[x'_\infty]$ est la partie entière de la composante x'_∞ en ∞ de x') pour obtenir une décomposition de x sous la forme souhaitée. Ceci termine la démonstration du (i).

Que $\mathbf{Q}$ soit discret résulte de ce que, si $x \in \mathbf{A}$, le voisinage ouvert $x + (]-\frac{1}{2}, \frac{1}{2}[\times\widehat{\mathbf{Z}})$ de x contient au plus un élément de $\mathbf{Q}$, vu que la différence de deux de ses éléments est dans $]-1,1[\times\widehat{\mathbf{Z}}$ qui ne contient que 0 comme élément de $\mathbf{Q}$.

Soient $x_1, x_2 \in \mathbf{A}/\mathbf{Q}$, distincts, et soit $\tilde{x}_i = (x_{i,v})$, si $i = 1, 2$, le représentant de x_i dans $[0,1[\times\widehat{\mathbf{Z}}$. Si $|x_{1,\infty} - x_{2,\infty}| > 0$, soient $\delta = \min(|x_{1,\infty} - x_{2,\infty}|, 1 - |x_{1,\infty} - x_{2,\infty}|)$, et $\mathrm{U}_{i,\infty} = \left]x_{i,\infty} - \frac{1}{3}\delta, x_{i,\infty} + \frac{1}{3}\delta\right[$ et $\mathrm{U}_i = \mathrm{U}_{i,\infty} \times \widehat{\mathbf{Z}}$, de telle sorte que U_i est un ouvert de $\mathbf{A}$ contenant $\tilde{x}_i$. Soit $\mathrm{V} = \{a - b,\ a \in \mathrm{U}_1,\ b \in \mathrm{U}_2\}$. Par construction, V est contenu dans $]\frac{1}{3}\delta, 1 - \frac{1}{3}\delta[\times\widehat{\mathbf{Z}}$; son intersection avec $\mathbf{Q}$ est donc incluse dans $]\frac{1}{3}\delta, 1 - \frac{1}{3}\delta[\cap\mathbf{Z} = \varnothing$, et donc V ne contient aucun élément de $\mathbf{Q}$. Il s'ensuit que $\{a + q_1,\ a \in \mathrm{U}_1\}$ et $\{b + q_2,\ b \in \mathrm{U}_2\}$ sont disjoints pour tous $q_1, q_2 \in \mathbf{Q}$, et donc que les images de U_1 et U_2 dans $\mathbf{A}/\mathbf{Q}$ sont des ouverts disjoints contenant x_1 et x_2 respectivement.

Si $x_{1,\infty} = x_{2,\infty} = c$, il existe p premier et $n \in \mathbf{N}$ tels que les réductions modulo p^n de $x_{1,p}$ et $x_{2,p}$ modulo p^n soient distinctes. On note U_i l'ouvert $]c - \frac{1}{2}, c + \frac{1}{2}[\times(x_{i,p} + p^n\mathbf{Z}_p) \times \prod_{\ell\in\mathscr{P}-\{p\}} \mathbf{Z}_\ell$, et $\mathrm{V} = \{a - b,\ a \in \mathrm{U}_1,\ b \in \mathrm{U}_2\}$. Alors V est contenu dans $]-1,1[\times((x_{1,p} - x_{2,p}) + p^n\mathbf{Z}_p) \times \prod_{\ell\in\mathscr{P}-\{p\}} \mathbf{Z}_\ell$ et donc ne contient aucun élément de $\mathbf{Q}$ (un élément q de $\mathrm{V} \cap \mathbf{Q}$ appartient à $(\mathbf{R} \times \widehat{\mathbf{Z}}) \cap \mathbf{Q} = \mathbf{Z}$, vérifie $|q| < 1$, et donc $q = 0$, ce qui est incompatible avec son appartenance à $(x_{1,p} - x_{2,p}) + p^n\mathbf{Z}_p$). Comme ci-dessus cela nous fournit des ouverts disjoints de $\mathbf{A}/\mathbf{Q}$ contenant x_1 et x_2 respectivement.

On en déduit le fait que $\mathbf{A}/\mathbf{Q}$ est séparé. Enfin, la restriction de la projection de $\mathbf{A}$ sur $\mathbf{A}/\mathbf{Q}$ à $[0,1] \times \widehat{\mathbf{Z}}$ est surjective. Comme $[0,1] \times \widehat{\mathbf{Z}}$ est compact en tant que produit de compacts (et même en

tant que produit dénombrable de compacts métriques), et que $\mathbf{A}/\mathbf{Q}$ est séparé, cela prouve que $\mathbf{A}/\mathbf{Q}$ est compact, en tant qu'image d'un compact par une application continue.

Si $\mathrm{S} = \{p_1, \dots, p_s\}$ est un sous-ensemble fini de $\mathscr{P}$, on note $\mathbf{Z}[\mathrm{S}^{-1}]$ le sous-anneau $\mathbf{Z}[\frac{1}{p_1}, \dots, \frac{1}{p_s}]$ de $\mathbf{Q}$ obtenu en rendant $p_1, \dots, p_s$ inversibles.

Proposition G.2.4. — *Si $\mathrm{S} \subset \mathscr{P}$ est fini, alors $\mathbf{Z}[\mathrm{S}^{-1}]$ est dense dans $\prod_{p\in\mathrm{S}} \mathbf{Q}_p$.*

Démonstration. — Comme les p_i^n sont premiers entre eux deux à deux, il existe, d'après le théorème des restes chinois, $a_{i,n} \in \mathbf{Z}$ congru à 1 modulo p_i^n, et à 0 modulo p_j^n, pour tout $j \in \mathrm{S} - \{i\}$. Si maintenant $y_i \in \mathbf{Q}_{p_i}$, on peut trouver $x_{i,n} \in \mathbf{Z}[\frac{1}{p_i}]$ tel que $|x_{i,n} - y_i| \leqslant p_i^{-n}$ car $\mathbf{Z}[\frac{1}{p_i}]$ est dense dans $\mathbf{Q}_{p_i}$ d'après l'alinéa 20.4.3 du Vocabulaire. En posant $x_n = \sum_{j=1}^{s} a_{j,n}x_{j,n}$, cela fournit une suite d'éléments de $\mathbf{Z}[\mathrm{S}^{-1}]$ vérifiant

$$\begin{aligned}|x_n - y_i|_{p_i} &= \big|a_{i,n}x_{i,n} - y_i + \sum_{j\neq i} a_{j,n}x_{j,n}\big|_{p_i} = \big|a_{i,n}(x_{i,n} - y_i) + (a_{i,n} - 1)y_i + \sum_{j\neq i} a_{j,n}x_{j,n}\big|_{p_i} \\ &\leqslant \sup\big(|a_{i,n}|_{p_i}|(x_{i,n} - y_i)|_{p_i}, |(a_{i,n} - 1)|_{p_i}|y_i|_{p_i}, \sup_{j\neq i} |a_{j,n}|_{p_i}|x_{j,n}|_{p_i}\big).\end{aligned}$$

Maintenant, on a $|x_{j,n}|_{p_i} \leqslant 1$, si $j \neq i$, et comme $|(x_{i,n} - y_i)|_{p_i}$, $|(a_{i,n} - 1)|_{p_i}$ et $|a_{j,n}|_{p_i}$, si $j \neq i$, sont tous $\leqslant p_i^{-n}$, on voit que x_n tend vers $(y_1, \dots, y_s)$ dans $\prod_{p\in\mathrm{S}} \mathbf{Q}_p$. Ceci permet de conclure.

1.3. *Le groupe des idèles de* $\mathbf{Q}$

Le *groupe des idèles* $\mathbf{A}^*$ de $\mathbf{Q}$ est le groupe des éléments inversibles de l'anneau $\mathbf{A}$; c'est donc l'ensemble des $(x_v)_{v\in\mathscr{V}}$, avec $x_v \in \mathbf{Q}_v^*$, et $x_p \in \mathbf{Z}_p^*$ pour presque tout p. Autrement dit, $\mathbf{A}^*$ est le produit restreint des $\mathbf{Q}_v^*$ relativement aux $\mathbf{Z}_p^*$, pour $p \in \mathscr{P}$, et on le munit de la topologie du produit restreint dont une base d'ouverts est constituée des $\prod_{v\in\mathrm{S}} \mathrm{U}_v \times \prod_{p\notin\mathrm{S}} \mathbf{Z}_p^*$, où S décrit les parties finies de $\mathscr{V}$ contenant ∞, et U_v les ouverts de $\mathbf{Q}_v^*$, si $v \in \mathrm{S}$.

Si $\beta \in \mathbf{Q}^*$, on a $\beta \in \mathbf{Z}_p^*$ sauf si p divise le dénominateur ou le numérateur de β, ce qui prouve que l'élément $(\beta, \beta, \dots)$ de $\prod_{v\in\mathscr{V}} \mathbf{Q}_v$ appartient à $\mathbf{A}^*$, et permet d'identifier $\mathbf{Q}^*$ à un sous-groupe de $\mathbf{A}^*$. Si $v \in \mathscr{V}$, on peut identifier $\mathbf{Q}_v^*$ au sous-groupe de $\mathbf{A}$ des x dont toutes les composantes sont égales à 1 sauf la composante en v.

Si $x = (x_v)_{v\in\mathscr{V}} \in \mathbf{A}^*$, on a $|x_p|_p = 1$ pour presque tout p, ce qui permet de définir $|x|_{\mathbf{A}}$ par $|x|_{\mathbf{A}} = \prod_{v\in\mathscr{V}} |x_v|_v$. Il résulte de la formule du produit (th. G.2.2) que $|\beta|_{\mathbf{A}} = 1$, quel que soit $\beta \in \mathbf{Q}^*$.

Lemme G.2.5. — (i) *Tout élément x de $\mathbf{A}^*$ peut s'écrire de manière unique sous la forme $x = \beta\, b_\infty\, b^{]\infty[}$, avec $\beta \in \mathbf{Q}^*$, $b_\infty \in \mathbf{R}_+^*$, et $b^{]\infty[} \in \widehat{\mathbf{Z}}^*$, où $\widehat{\mathbf{Z}}^* = \prod_{p\in\mathscr{P}} \mathbf{Z}_p^*$.*

(ii) $\mathbf{A}^*/\mathbf{Q}^* \cong \mathbf{R}_+^* \times \widehat{\mathbf{Z}}^*$.

Démonstration. — On peut et doit poser $\beta = \mathrm{sign}(x_\infty) \prod_{p\in\mathscr{P}} p^{v_p(x_p)}$, et alors $b = \beta^{-1}x$ vérifie les conditions $b_\infty \in \mathbf{R}_+$ et $b^{]\infty[} \in \prod_{p\in\mathscr{P}} \mathbf{Z}_p^*$. On en déduit le (i), et le (ii) en est une conséquence immédiate.

2. La formule de Poisson adélique

2.1. *Transformée de Fourier sur* $\mathbf{Q}_p$

Si $p \in \mathscr{P}$, on note $\mathscr{S}(\mathbf{Q}_p)$ l'espace (de Schwartz) des fonctions à valeurs dans $\mathbf{C}$, localement constantes, à support compact dans $\mathbf{Q}_p$. Soit $\phi \in \mathscr{S}(\mathbf{Q}_p)$. Comme ϕ est à support compact (et donc borné), il existe $m \in \mathbf{Z}$ tel que $\phi(x) = 0$ si $|x|_p > p^{-m}$; autrement dit, il existe $m \in \mathbf{Z}$ tel que $\phi(x) = 0$ si $x \notin p^m\mathbf{Z}_p$. Par ailleurs, comme ϕ est localement constante, il existe pour tout $x \in p^m\mathbf{Z}_p$, un entier $n_x \in \mathbf{N}$ tel que ϕ soit constante sur $\mathrm{B}(x, p^{-n_x}) = x + p^{n_x}\mathbf{Z}_p$. Comme $p^m\mathbf{Z}_p$ est compact, on peut extraire un recouvrement fini du recouvrement de $p^m\mathbf{Z}_p$ par les $x + p^{n_x}\mathbf{Z}_p$. En notant n le minimum des n_x intervenant dans le sous-recouvrement fini, on voit qu'il existe $n \in \mathbf{N}$ tel que ϕ soit constante sur $x + p^n\mathbf{Z}_p$, quel que soit $x \in p^m\mathbf{Z}_p$. En notant $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ la fonction caractéristique de $a + p^n\mathbf{Z}_p$, et en utilisant la densité de $\mathbf{Z}[\frac{1}{p}]$ dans $\mathbf{Q}_p$, on en déduit le résultat suivant.

Proposition G.2.6. — *$\mathscr{S}(\mathbf{Q}_p)$ est le $\mathbf{C}$-espace vectoriel engendré par les $\mathbf{1}_{a+p^n\mathbf{Z}_p}$, pour $a \in \mathbf{Z}[\frac{1}{p}]$ et $n \in \mathbf{N}$. De plus, les relations entre les $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ sont engendrées par les relations suivantes :*

- $\mathbf{1}_{a+p^n\mathbf{Z}_p} = \mathbf{1}_{b+p^n\mathbf{Z}_p}$, *si* $b \in a + p^n\mathbf{Z}$,
- $\mathbf{1}_{a+p^n\mathbf{Z}_p} = \sum_{i=0}^{p-1} \mathbf{1}_{a+ip^n+p^{n+1}\mathbf{Z}_p}$,

la seconde traduisant le fait qu'il y a p possibilités pour le reste de la division par p^{n+1}, si on connaît le reste de la division par p^n.

Si $\phi \in \mathscr{S}(\mathbf{Q}_p)$, on définit $\int_{\mathbf{Q}_p} \phi(x)\,dx$ par linéarité, en posant $\int_{\mathbf{Q}_p} \mathbf{1}_{a+p^n\mathbf{Z}_p}(x)\,dx = p^{-n}$, quels que soient $a \in \mathbf{Z}[\frac{1}{p}]$ et $n \in \mathbf{N}$, ce qui revient à demander que $\mathbf{Z}_p$ ait mesure 1 et que l'intégration soit invariante par translation (i.e. soit une mesure de Haar). Que ce soit possible suit du fait que les seules relations entre les $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ sont celles ci-dessus.

Si $x \in \mathbf{Q}_p$, il existe $\xi \in \mathbf{Z}[\frac{1}{p}]$ tel que $x - \xi \in \mathbf{Z}_p$ (c'est une conséquence de la densité de $\mathbf{Z}[\frac{1}{p}]$ dans $\mathbf{Q}_p$), et ξ est bien déterminé à addition près d'un élément de $\mathbf{Z}[\frac{1}{p}] \cap \mathbf{Z}_p = \mathbf{Z}$. On en déduit que $e^{2i\pi\,\xi}$ ne dépend que de x, et pas du choix de ξ, ce qui nous autorise à le noter $e^{2i\pi\,x}$. Il est alors immédiat que $x \mapsto e^{2i\pi\,x}$ est un caractère linéaire de $\mathbf{Q}_p$ ($e^{2i\pi(x+y)} = e^{2i\pi\,x}e^{2i\pi\,y}$), localement constant (constant sur $a + \mathbf{Z}_p$, pour tout $a \in \mathbf{Q}_p$).

On définit alors la *transformée de Fourier* $\hat{\phi} = \mathscr{F}_p\phi$ de $\phi \in \mathscr{S}(\mathbf{Q}_p)$ par la formule

$$\hat{\phi}(y) = \int_{\mathbf{Q}_p} \phi(x)e^{2i\pi\,xy}\,dx,$$

ce qui a un sens car $x \mapsto \phi(x)e^{2i\pi\,xy}$ a même support que ϕ et est localement constante comme produit de deux fonctions localement constantes.

Exemple G.2.7. — (i) La transformée de Fourier de $\mathbf{1}_{\mathbf{Z}_p}$ est $\mathbf{1}_{\mathbf{Z}_p}$. En effet, si $y \in \mathbf{Z}_p$, on a $e^{2i\pi xy} = 1$ quel que soit $x \in \mathbf{Z}_p$, et donc $\int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x)e^{2i\pi\,xy}\,dx = \int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x)\,dx = 1$. Par

contre, si $v_p(y) = -n < 0$, le caractère linéaire $x \mapsto e^{2i\pi xy}$ de $\mathbf{Z}_p$ est non trivial et constant modulo $p^n\mathbf{Z}_p$; on a donc

$$\int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x) e^{2i\pi xy}\, dx = \int_{\mathbf{Q}_p} \sum_{a\in\mathbf{Z}_p/p^n\mathbf{Z}_p} e^{2i\pi ya}\mathbf{1}_{a+p^n\mathbf{Z}_p}(x)\, dx = p^{-n} \sum_{a\in\mathbf{Z}_p/p^n\mathbf{Z}_p} e^{2i\pi ya} = 0,$$

d'après l'orthogonalité des caractères linéaires d'un groupe fini, puisque $a \mapsto e^{2i\pi ya}$ est un caractère linéaire non trivial de $\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$.

(ii) Les mêmes calculs montrent que, si ϕ est constante modulo $p^n\mathbf{Z}_p$, et à support dans $p^{-m}\mathbf{Z}_p$, alors $\hat{\phi}$ est constante modulo $p^m\mathbf{Z}_p$, et à support dans $p^{-n}\mathbf{Z}_p$.

(iii) Soit $\chi : (\mathbf{Z}/p^n\mathbf{Z})^* \to \mathbf{C}^*$ un caractère de Dirichlet de conducteur p^n, avec $n \geqslant 1$. En utilisant l'isomorphisme $\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$, on peut associer à χ une fonction ϕ_χ, à support dans $\mathbf{Z}_p$ (et même dans $\mathbf{Z}_p^*$), constante modulo $p^n\mathbf{Z}_p$, en posant $\phi_\chi(x) = 0$ si $x \in p\mathbf{Z}_p$, et $\phi_\chi(x) = \chi(\overline{x})$, si $x \in \mathbf{Z}_p^*$ et $\overline{x}$ est l'image de x modulo $p^n\mathbf{Z}_p$. Alors la transformée de Fourier de ϕ_χ est donnée par la formule

$$\hat{\phi}_\chi(y) = \frac{\mathrm{G}(\chi)}{p^n}\phi_{\overline{\chi}}(p^n y), \quad \text{où } \mathrm{G}(\chi) = \sum_{a\in(\mathbf{Z}/p^n\mathbf{Z})^*} \chi(a) e^{2i\pi\,\frac{a}{p^n}}$$

est la somme de Gauss introduite au n° 2 du § VII.4. En effet, ϕ_χ étant constante modulo $p^n\mathbf{Z}_p$, la fonction $\hat{\phi}_\chi$ est nulle en dehors de $p^{-n}\mathbf{Z}_p$, et si $v_p(y) \geqslant -n$, la formule à vérifier est équivalente à celle du lemme VII.4.3.

La transformée de Fourier sur $\mathbf{Q}_p$ vérifie les mêmes propriétés que sur $\mathbf{R}$ en ce qui concerne les dilatations, translations... De manière précise, on a le résultat suivant.

Proposition G.2.8. — (i) *Si $a \in \mathbf{Q}_p^*$ et $b, c \in \mathbf{Q}_p$, alors*

$$\mathscr{F}_p(\phi(ax))(y) = |a|_p^{-1}\hat{\phi}(a^{-1}y),$$
$$\mathscr{F}_p(\phi(x+b))(y) = e^{-2i\pi by}\hat{\phi}(y), \quad \text{et} \quad \mathscr{F}_p(e^{2i\pi cx}\phi(x))(y) = \hat{\phi}(y+c).$$

(ii) $(\mathscr{F}_p \circ \mathscr{F}_p\phi)(x) = \phi(-x)$ (formule d'inversion de Fourier).

Démonstration. — Si $a \in \mathbf{Q}_p^*$ et $b, c \in \mathbf{Q}_p$, soit $u_{a,b,c} : \mathscr{S}(\mathbf{Q}_p) \to \mathscr{S}(\mathbf{Q}_p)$ l'application définie par $(u_{a,b,c}\phi)(x) = e^{2i\pi cx}\phi(ax+b)$. Un changement de variable immédiat dans l'intégrale définissant $\mathscr{F}_p \circ u_{a,b,c}$ montre que

$$\mathscr{F}_p \circ u_{a,b,c} = |a|_p^{-1} e^{-2i\pi\,\frac{bc}{a}} u_{a^{-1},a^{-1}c,-a^{-1}b} \circ \mathscr{F}_p.$$

On en déduit le (i). En appliquant le (i) deux fois, on montre que $\mathscr{F}_p \circ \mathscr{F}_p \circ u_{a,b,c} = u_{a,-b,-c} \circ \mathscr{F}_p \circ \mathscr{F}_p$. Soit Y le sous-espace de $\mathscr{S}(\mathbf{Q}_p)$ des ϕ tels que $\mathscr{F}_p \circ \mathscr{F}_p\phi = u_{-1,0,0}\phi$. Comme $u_{a,-b,-c} \circ u_{-1,0,0} = u_{-1,0,0} \circ u_{a,b,c}$, on voit que Y est stable par les $u_{a,b,c}$. Par ailleurs, Y contient $\mathbf{1}_{\mathbf{Z}_p}$, et $u_{p^{-n},-p^{-n}a,0}\mathbf{1}_{\mathbf{Z}_p} = \mathbf{1}_{a+p^n\mathbf{Z}_p}$; on en déduit que Y contient les $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ pour $a \in \mathbf{Q}_p$ et $n \in \mathbf{Z}$, et donc $\mathrm{Y} = \mathscr{S}(\mathbf{Q}_p)$. Ceci permet de conclure.

2.2. *Transformée de Fourier adélique*

Soit $\mathscr{S}(\mathbf{A})$ l'espace de Schwartz de $\mathbf{A}$. C'est l'ensemble des combinaisons linéaires des fonctions de la forme $\phi(x) = \prod_{v\in\mathrm{S}} \phi_v(x_v) \prod_{p\notin\mathrm{S}} \mathbf{1}_{\mathbf{Z}_p}(x_p)$, où S décrit les parties finies de $\mathscr{V}$ contenant ∞, et $\phi_v \in \mathscr{S}(\mathbf{Q}_v)$, si $v \in \mathrm{S}$. Une telle fonction sera aussi notée $\otimes_{v\in\mathscr{V}}\phi_v$, étant

sous-entendu que $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$ pour presque tout $p \in \mathscr{P}$.

Comme les $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ engendrent $\mathscr{S}(\mathbf{Q}_p)$, on voit que $\mathscr{S}(\mathbf{A})$ est aussi engendré par des fonctions de la forme

$$\phi_\infty(x_\infty)\prod_{p\in \mathrm{S}}\mathbf{1}_{a_p+p^{n_p}\mathbf{Z}_p}(x_p)\prod_{p\notin \mathrm{S}}\mathbf{1}_{\mathbf{Z}_p}(x_p) = \phi_\infty(x_\infty)\mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}}(x^{]\infty[}),$$

où $\mathrm{N} = \prod_{p\in \mathrm{S}} p^{n_p}$ et a est un élément de $\mathbf{Z}[\mathrm{S}^{-1}]$ tel que $a - a_p \in \mathbf{Z}_p$, quel que soit $p \in \mathrm{S}$ (l'existence d'un tel a est garantie par le lemme G.2.4). De plus, les relations entre ces générateurs sont engendrées par les relations (en notant plus simplement $\phi_\infty \otimes \mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}}$ l'élément de $\mathscr{S}(\mathbf{A})$ apparaissant dans le membre de droite ci-dessus) :

- $\phi_\infty \otimes \mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}} = \phi_\infty \otimes \mathbf{1}_{b+\mathrm{N}\widehat{\mathbf{Z}}}$, si $a - b \in \mathrm{N}\mathbf{Z}$,
- $\phi_\infty \otimes \mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}} = \sum_{i=0}^{\mathrm{M}-1} \phi_\infty \otimes \mathbf{1}_{a+i\mathrm{N}+\mathrm{NM}\widehat{\mathbf{Z}}}$, si $a \in \mathbf{Q}$, $\mathrm{M}, \mathrm{N} \in \mathbf{N} - \{0\}$.

Si $\phi \in \mathscr{S}(\mathbf{A})$, on définit $\int_{\mathbf{A}} \phi\, dx$ par linéarité en imposant que $\int_{\mathbf{A}} \phi_\infty \otimes \mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}}\, dx = \frac{1}{\mathrm{N}}\int_{\mathbf{R}} \phi_\infty(x_\infty)\, dx_\infty$, ce qui revient à demander que la mesure de $[0,1[\times\widehat{\mathbf{Z}}$ soit 1, et que l'intégration sur $\mathbf{A}$ soit invariante par translation. On remarquera que si $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, alors $\int_{\mathbf{A}} \phi\, dx = \prod_{v\in\mathscr{V}} \int_{\mathbf{Q}_v} \phi_v(x_v)\, dx_v$, et presque tous les termes du produit valent 1.

Si $x = (x_v)_{v\in\mathscr{V}} \in \mathbf{A}$, on définit $e^{2i\pi\, x}$ par $e^{2i\pi\, x} = e^{-2i\pi\, x_\infty}\prod_{p\in\mathscr{P}} e^{2i\pi\, x_p}$, et presque tous les termes du produit sont égaux à 1. Il est immédiat sur la formule que l'on a $e^{2i\pi(x+y)} = e^{2i\pi\, x}e^{2i\pi\, y}$, si $x, y \in \mathbf{A}$. De plus, on vérifie sans peine que $e^{2i\pi(x+\nu)} = e^{2i\pi\, x}$, si $\nu \in \mathbf{Z}$ ou si ν est de la forme $\frac{1}{p^n}$, avec $p \in \mathscr{P}$ et $n \in \mathbf{N}$. Comme tout élément de $\mathbf{Q}$ peut s'écrire comme une somme d'éléments de ce type (décomposition en éléments simples), on en déduit que $x \mapsto e^{2i\pi\, x}$ *est périodique de période* $\mathbf{Q}$.

On définit la *transformée de Fourier adélique* $\hat{\phi} = \mathscr{F}_{\mathbf{A}}\phi$ de $\phi \in \mathscr{S}(\mathbf{A})$ par la formule $\hat{\phi}(y) = \int_{\mathbf{A}} \phi(x)e^{2i\pi\, xy}\, dx$. Il est clair que si $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, alors $\mathscr{F}_{\mathbf{A}}\phi = \otimes_{v\in\mathscr{V}}\mathscr{F}_v\phi_v$, (ce qui a un sens puisque, pour presque tout p, on a $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$ et donc $\mathscr{F}_p\phi_p = \mathbf{1}_{\mathbf{Z}_p}$).

On déduit des formules locales (i.e. sur $\mathbf{R}$ et sur $\mathbf{Q}_p$) d'inversion de Fourier et des formules locales pour les dilatations, que

$$(\mathscr{F}_{\mathbf{A}} \circ \mathscr{F}_{\mathbf{A}}\phi)(y) = \phi(-y), \quad \text{et} \quad \mathscr{F}_{\mathbf{A}}(\phi(bx))(y) = |b|_{\mathbf{A}}^{-1}\hat{\phi}(b^{-1}y), \text{ si } b \in \mathbf{A}^*.$$

Théorème G.2.9. — (Formule de Poisson) *Soit $\phi \in \mathscr{S}(\mathbf{A})$. Alors*

(i) $\sum_{\alpha\in\mathbf{Q}} \phi(\alpha) = \sum_{\alpha\in\mathbf{Q}} \hat{\phi}(\alpha)$.

(ii) *Plus généralement, si $b \in \mathbf{A}^*$, alors $\sum_{\alpha\in\mathbf{Q}} \phi(\alpha b) = |b|_{\mathbf{A}}^{-1}\sum_{\alpha\in\mathbf{Q}} \hat{\phi}(\alpha b^{-1})$.*

Démonstration. — Par linéarité, on peut supposer que $\phi = \phi_\infty \otimes \mathbf{1}_{a+\mathrm{N}\widehat{\mathbf{Z}}}$, avec $a \in \mathbf{Q}$, et $\mathrm{N} \in \mathbf{N}$. Dans ce cas, $\hat{\phi}(y) = \mathrm{N}^{-1}\hat{\phi}(y_\infty)e^{2i\pi\, ay^{]\infty[}}\mathbf{1}_{\mathrm{N}^{-1}\widehat{\mathbf{Z}}}$, et on est ramené à prouver l'identité

$$\sum_{\alpha\in a+\mathrm{N}\mathbf{Z}} \phi_\infty(\alpha) = \frac{1}{\mathrm{N}}\sum_{\alpha\in\mathrm{N}^{-1}\mathbf{Z}} e^{2i\pi a\alpha}\hat{\phi}_\infty(\alpha),$$

ce qui résulte de la formule de Poisson classique (th. IV.3.18) appliquée à la fonction $f : \mathbf{R} \to \mathbf{C}$, définie par $f(x) = \phi_\infty(\mathrm{N}x + a)$, dont la transformée de Fourier est $\hat{f}(y) = \frac{1}{\mathrm{N}}e^{2i\pi\,\frac{ay}{\mathrm{N}}}\hat{\phi}_\infty(\frac{y}{\mathrm{N}})$.

Le (ii) résulte de ce que la transformée de Fourier de $x \mapsto \phi_b(x) = \phi(bx)$ est $\hat{\phi}_b(y) = |b|_{\mathbf{A}}^{-1}\hat{\phi}(b^{-1}y)$.

3. Transformée de Mellin adélique et fonctions L

3.1. *Intégration sur* $\mathbf{Q}_p^*$

Soit $\mathscr{L}_0(\mathbf{Q}_p^*)$ l'ensemble des $\phi : \mathbf{Q}_p^* \to \mathbf{C}$, localement constantes et à support compact dans $\mathbf{Q}_p^*$ (autrement dit, $\mathscr{L}_0(\mathbf{Q}_p^*)$ est le sous-espace de $\mathscr{S}(\mathbf{Q}_p)$ des ϕ vérifiant $\phi(0) = 0$). Si $\phi \in \mathscr{L}_0(\mathbf{Q}_p^*)$, on définit $\int_{\mathbf{Q}_p^*} \phi(x)\, d^*x$ par la formule

$$\int_{\mathbf{Q}_p^*} \phi(x)\, d^*x = \frac{p}{p-1} \int_{\mathbf{Q}_p} \phi(x)\, |x|_p^{-1}\, dx,$$

ce qui revient à demander que la mesure de $\mathbf{Z}_p^*$ soit 1 et que l'intégration sur $\mathbf{Q}_p^*$ soit invariante par $x \mapsto bx$, si $b \in \mathbf{Q}_p^*$.

Soit $\mathscr{L}(\mathbf{Q}_p^*)$ l'ensemble des $\phi : \mathbf{Q}_p^* \to \mathbf{C}$, à support compact dans $\mathbf{Q}_p$, dont la restriction à $p^n\mathbf{Z}_p^* = \{x,\ |x|_p = p^{-n}\}$ appartient, quel que soit $n \in \mathbf{Z}$, à $\mathscr{L}_0(\mathbf{Q}_p^*)$, et qui sont *sommables*, ce qui signifie que $\sum_{n\in\mathbf{Z}} \int_{p^n\mathbf{Z}_p^*} |\phi(x)|\, d^*x < +\infty$. Si $\phi \in \mathscr{L}(\mathbf{Q}_p^*)$, on définit $\int_{\mathbf{Q}_p^*} \phi(x)\, d^*x$ par la formule

$$\int_{\mathbf{Q}_p^*} \phi(x)\, d^*x = \sum_{n\in\mathbf{Z}} \int_{p^n\mathbf{Z}_p^*} \phi(x)\, d^*x.$$

3.2. *Intégration sur le groupe des idèles*

Soit $\mathscr{L}(\mathbf{R}^*)$ l'ensemble des $\phi : \mathbf{R}^* \to \mathbf{C}^*$ à décroissance rapide à l'infini et telles que $\int_{\mathbf{R}^*} |\phi(t)|\, d^*t < +\infty$, où l'on a posé $d^*t = \frac{dt}{|t|}$. La mesure d^*t est invariante par le changement de variable $t \mapsto bt$, si $b \in \mathbf{R}^*$.

Soit $\mathscr{L}_0(\mathbf{A}^*)$ l'espace engendré par les fonctions de la forme $\phi(x) = \prod_{v\in\mathscr{V}} \phi_v(x_v)$, où $\phi_\infty \in \mathscr{L}(\mathbf{R}^*)$, $\phi_p \in \mathscr{L}_0(\mathbf{Q}_p^*)$ et $\phi_p = \mathbf{1}_{\mathbf{Z}_p^*}$ pour presque tout p. On notera une fonction de ce type sous la forme $\otimes_{v\in\mathscr{V}} \phi_v$, ce qui sous-entend que $\phi_p = \mathbf{1}_{\mathbf{Z}_p^*}$ pour presque tout p. Si $\phi \in \mathscr{L}_0(\mathbf{A}^*)$, on définit $\int_{\mathbf{A}^*} \phi(x)\, d^*x$ par linéarité en imposant que

$$\int_{\mathbf{A}^*} \otimes_{v\in\mathscr{V}} \phi_v\, d^*x = \prod_{v\in\mathscr{V}} \Big(\int_{\mathbf{Q}_v^*} \phi_v(x_v)\, d^*x_v \Big),$$

où presque tous les termes du produit sont égaux à 1. Cela revient à demander que la mesure de $[1, a[\times\widehat{\mathbf{Z}}^*$ soit $\log a$ et que d^*x soit invariante par $x \mapsto bx$, si $b \in \mathbf{A}^*$.

On note $\mathscr{L}(\mathbf{A}^*)$ l'espace des fonctions dont la restriction à $\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*$ appartient à $\mathscr{L}_0(\mathbf{A}^*)$, quel que soit $\beta \in \mathbf{Q}^*$, et qui sont *sommables*, i.e. $\sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)|\, d^*x < +\infty$. Si $\phi \in \mathscr{L}(\mathbf{A}^*)$, on définit $\int_{\mathbf{A}^*} \phi(x)\, d^*x$ par la formule

$$\int_{\mathbf{A}^*} \phi(x)\, d^*x = \sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} \phi(x)\, d^*x.$$

Proposition G.2.10. — *Soit $\phi_v \in \mathscr{L}(\mathbf{Q}_v^*)$, pour $v \in \mathscr{V}$, vérifiant :*

- *$\phi_p = 1$ sur $\mathbf{Z}_p^*$ pour presque tout p,*
- *$\prod_{v\in\mathscr{V}} \big(\int_{\mathbf{Q}_v^*} |\phi_v(x_v)|\, d^*x_v \big) < +\infty$.*

Alors $\phi : \mathbf{A}^* \to \mathbf{C}$ *définie par* $\phi(x) = \prod_{v\in\mathscr{V}} \phi_v(x_v)$ *est un élément de* $\mathscr{L}(\mathbf{A}^*)$, *et* $\int_{\mathbf{A}^*} \phi(x)\, d^*x = \prod_{v\in\mathscr{V}} \big(\int_{\mathbf{Q}_v^*} \phi_v(x_v)\, d^*x_v\big)$.

Démonstration. — Si $\beta \in \mathbf{Q}^*$, la restriction de ϕ à $\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*$ est le produit de $\mathbf{1}_{\mathbf{R}^*_{\mathrm{sign}(\beta)}}\phi_\infty$ et des $\mathbf{1}_{p^{v_p(\beta)}\mathbf{Z}_p^*}\phi_p$, et comme $v_p(\beta) = 0$ pour presque tout p, et $\phi_p = 1$ sur $\mathbf{Z}_p^*$ pour presque tout p, cette restriction est visiblement élément de $\mathscr{L}_0(\mathbf{A}^*)$.

Le reste se démontre comme la prop. VII.3.1. Soit $\mathscr{P}(\mathrm{X})$ l'ensemble des nombres premiers $\leqslant \mathrm{X}$, $\mathrm{I}(\mathrm{X})$ l'ensemble des $\beta \in \mathbf{Q}^*$, positifs ou négatifs, dont la décomposition en facteurs premiers ne fait intervenir que des éléments de $\mathscr{P}(\mathrm{X})$ et, si $k \in \mathbf{N}$, soit $\mathrm{I}(\mathrm{X},k)$ l'ensemble fini des $\beta \in \mathrm{I}(\mathrm{X})$ tels que $-k \leqslant v_p(\beta) \leqslant k$, si $p \in \mathscr{P}(\mathrm{X})$. En notant $\mathrm{C}_p(-k,k)$ la couronne $\{x \in \mathbf{Q}_p,\ p^{-k} \leqslant |x_p| \leqslant p^k\}$, on obtient :

$$\sum_{\beta\in\mathrm{I}(\mathrm{X},k)} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)|\, d^*x = \int_{\mathbf{R}^*\times\prod_{p\leqslant \mathrm{X}} \mathrm{C}_p(-k,k)\times\prod_{p>\mathrm{X}}\mathbf{Z}_p^*} |\phi(x)|\, d^*x.$$

Or $\phi(x) = \prod_{v\in\mathscr{V}} \phi_v(x_v)$, ce qui permet de mettre le membre de droite sous la forme

$$\Big(\int_{\mathbf{R}^*} |\phi_\infty(x_\infty)|\, d^*x_\infty\Big) \prod_{p\leqslant \mathrm{X}} \Big(\int_{\mathrm{C}_p(-k,k)} |\phi_p(x_p)|\, d^*x_p\Big),$$

si X est assez grand pour que $\phi_p = 1$ sur $\mathbf{Z}_p^*$, pour tout $p > \mathrm{X}$. En faisant tendre k vers $+\infty$, on en déduit

$$\sum_{\beta\in\mathrm{I}(\mathrm{X})} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)|\, d^*x = \Big(\int_{\mathbf{R}^*} |\phi_\infty(x_\infty)|\, d^*x_\infty\Big) \prod_{p\leqslant \mathrm{X}} \Big(\int_{\mathbf{Q}_p^*} |\phi_p(x_p)|\, d^*x_p\Big),$$

et en faisant tendre X vers $+\infty$, on obtient

$$\sum_{\beta\in\mathbf{Q}_+^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)|\, d^*x = \prod_{v\in\mathscr{V}} \Big(\int_{\mathbf{Q}_v^*} |\phi_v(x_v)|\, d^*x_v\Big) < +\infty,$$

et donc ϕ est sommable. En particulier la série $\sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} \phi(x)\, d^*x$ est absolument convergente, ce qui permet, en reprenant les calculs ci-dessus sans les valeurs absolues, de démontrer la formule $\int_{\mathbf{A}^*} \phi(x)\, d^*x = \prod_{v\in\mathscr{V}} \big(\int_{\mathbf{Q}_v^*} \phi_v(x_v)\, d^*x_v\big)$, que l'on cherchait à obtenir.

3.3. *Transformée de Mellin sur* $\mathbf{Q}_p$

Lemme G.2.11. — *Si* χ *est un caractère linéaire continu de* $\mathbf{Q}_p^*$, *il existe* $n \in \mathbf{N} - \{0\}$ *tel que* $\chi = 1$ *sur* $1 + p^n\mathbf{Z}_p$.

Démonstration. — Comme χ est continu, il existe $n > 0$ tel que $|\chi(x) - 1| \leqslant 1/2$, si $|x-1|_p \leqslant p^{-n}$. Or $\mathrm{B}(1,p^{-n}) = 1+p^{n_p}\mathbf{Z}_p$, est un sous-groupe d'indice fini de $\mathbf{Z}_p^*$ (c'est l'image réciproque de $1 \in (\mathbf{Z}/p^n\mathbf{Z})^*$ par la projection naturelle $\mathbf{Z}_p^* \to (\mathbf{Z}_p/p^n\mathbf{Z}_p)^* = (\mathbf{Z}/p^n\mathbf{Z})^*$). Comme χ est un morphisme de groupes, l'image de $1 + p^n\mathbf{Z}_p$ est un sous-groupe de $\mathbf{C}^*$ inclus dans le disque $\mathrm{D}(1,1/2)$; on en déduit que cette image est réduite à $\{1\}$, ce qui permet de conclure.

On dit que χ est *non ramifié* si $\chi = 1$ sur $\mathbf{Z}_p^*$. Si χ est ramifié, on note $n(\chi)$ le plus petit entier n tel que $\chi = 1$ sur $1 + p^n\mathbf{Z}_p$; alors $p^{n(\chi)}$ est le *conducteur de* χ.

Si G est un groupe, un caractère linéaire $\chi : \mathrm{G} \to \mathbf{C}^*$ est *unitaire* si $|\chi(g)| = 1$, quel que soit $g \in \mathrm{G}$. On a alors $\chi(g^{-1}) = \overline{\chi}(g)$, pour tout $g \in \mathrm{G}$.

Proposition G.2.12. — *Soit* $\chi : \mathbf{Q}_p^* \to \mathbf{C}^*$ *un caractère linéaire unitaire continu.*

(i) *Si* $\phi \in \mathscr{S}(\mathbf{Q}_p)$, *alors* $x \mapsto \phi(x)\chi(x)|x|_p^s \in \mathscr{L}(\mathbf{Q}_p^*)$, *si* $\mathrm{Re}(s) > 0$.

Si $\mathrm{Re}(s) > 0$, *soit* $\mathrm{M}_p(\phi,\chi,s) = \int_{\mathbf{Q}_p^*} \phi(x)\chi(x)|x|_p^s\, d^*x$ *la transformée de Mellin de* ϕ.

(ii) $\mathrm{M}_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)=\frac{1}{1-\chi(p)p^{-s}}$, *si* χ *est non ramifié, et* $\mathrm{M}_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)=0$, *si* χ *est ramifié.*

(iii) *Dans le cas général,* $\mathrm{M}_p(\phi,\chi,s)$ *est un polynôme en* p^s *et* p^{-s} *si* χ *est ramifié, et de la forme* $\frac{\phi(0)}{1-\chi(p)p^{-s}}+\mathrm{R}(s)$, *où* $\mathrm{R}(s)$ *est un polynôme en* p^s *et* p^{-s}, *si* χ *est non ramifié.*

Démonstration. — On écrit ϕ sous la forme $\phi(0)\mathbf{1}_{\mathbf{Z}_p}+\psi$, où $\psi\in\mathscr{L}_0(\mathbf{Q}_p^*)$. Il existe alors $n\in\mathbf{N}$ tel que $\psi\chi$ soit constant modulo $p^n\mathbf{Z}_p$, ce qui permet de l'écrire sous la forme $\sum_{a\in\mathrm{I}}\lambda_a\mathbf{1}_{a+p^n\mathbf{Z}_p}$. On a alors $\mathrm{M}_p(\psi,\chi,s)=\sum_{a\in\mathrm{I}}\lambda_a\frac{p^{1-n}}{p-1}|a|_p^{s-1}$, et comme $|a|_p\in p^{\mathbf{Z}}$, cela montre que $\mathrm{M}_p(\psi,\chi,s)$ est un polynôme en p^s et p^{-s}.

Maintenant, on a $\int_{p^n\mathbf{Z}_p^*}||x|_p^s|\,d^*x=p^{-n\mathrm{Re}(s)}$. On en déduit que $x\mapsto\mathbf{1}_{\mathbf{Z}_p}(x)\chi(x)|x|_p^s$ est sommable si $\mathrm{Re}(s)>0$. De plus,

$$\begin{aligned}\mathrm{M}_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)&=\sum_{n=0}^{+\infty}\int_{p^n\mathbf{Z}_p^*}\chi(x)|x|_p^s\,d^*x=\sum_{n=0}^{+\infty}\int_{\mathbf{Z}_p^*}\chi(p^nx)|p^nx|_p^s\,d^*x\\&=\sum_{n=0}^{+\infty}\chi(p)^np^{-ns}\int_{\mathbf{Z}_p^*}\chi(x)\,d^*x=\frac{1}{1-\chi(p)p^{-s}}\int_{\mathbf{Z}_p^*}\chi(x)\,d^*x,\end{aligned}$$

et le résultat suit de ce que $\int_{\mathbf{Z}_p^*}\chi(x)\,d^*x=1$ si $\chi=1$ sur $\mathbf{Z}_p^*$ et est nul si χ n'est pas trivial sur $\mathbf{Z}_p^*$, puisqu'il se factorise alors à travers le groupe fini $(\mathbf{Z}/p^{n(\chi)}\mathbf{Z})^*$, et que la somme des valeurs d'un caractère linéaire non trivial d'un groupe fini est nulle (orthogonalité des caractères linéaires).

3.4. *La transformée de Mellin adélique*

Proposition G.2.13. — *Soit* χ *un caractère continu de* $\mathbf{A}^*$, *et si* $v\in\mathscr{V}$, *soit* χ_v *la restriction de* χ *à* $\mathbf{Q}_v^*$. *Alors, pour presque tout* $p\in\mathscr{P}$, *on a* $\chi_p=1$ *sur* $\mathbf{Z}_p^*$, *et, si* $x\in\mathbf{A}^*$, $\chi(x)=\prod_{v\in\mathscr{V}}\chi_v(x_v)$.

Démonstration. — Comme χ est continu sur $\mathbf{A}^*$, il est continu sur $\widehat{\mathbf{Z}}^*=\prod_{p\in\mathscr{P}}\mathbf{Z}_p^*$, et par définition de la topologie produit, il existe $\mathrm{S}\subset\mathscr{P}$ fini et, si $p\in\mathrm{S}$, $n_p\in\mathbf{N}-\{0\}$, tels que $|\chi(x)-1|\leqslant 1/2$, si $x\in\mathrm{U}=\prod_{p\in\mathrm{S}}(1+p^{n_p}\mathbf{Z}_p)\prod_{p\notin\mathrm{S}}\mathbf{Z}_p^*$. Or U est un sous-groupe de $\widehat{\mathbf{Z}}^*$, et donc son image par χ est un sous-groupe de $\mathbf{C}^*$ inclus dans le disque $\mathrm{D}(1,1/2)$; on en déduit que cette image est réduite à $\{1\}$. En particulier, on a $\chi_p=1$ sur $\mathbf{Z}_p^*$ pour tout $p\notin\mathrm{S}$.

Maintenant, si $x\in\mathbf{A}^*$, on a $\chi_v(x_v)=1$ pour presque tout v, ce qui fait que $\chi'(x)=\prod_{v\in\mathscr{V}}\chi_v(x_v)$ est bien défini, et que χ' est un caractère linéaire continu de $\mathbf{A}^*$. On conclut en remarquant que χ' et χ coïncident sur le sous-groupe des idèles dont presque toutes les composantes sont égales à 1, et en utilisant la densité de ce sous-groupe dans $\mathbf{A}^*$. (Si U est un ouvert de $\mathbf{A}^*$, il contient un ouvert de la forme $\prod_{v\in\mathrm{S}}\mathrm{U}_v\times\prod_{p\notin\mathrm{S}}\mathbf{Z}_p^*$, et donc contient des éléments dont toutes les composantes en dehors de S sont égales à 1.)

Si $\phi\in\mathscr{L}(\mathbf{R}^*)$, et si χ est un caractère linéaire unitaire continu de $\mathbf{R}^*$, la *transformée de Mellin* $\mathrm{M}_\infty(\phi,\chi,s)$ de ϕ est la fonction $s\mapsto\int_{\mathbf{R}^*}\phi(t)\chi(t)|t|^s\,d^*t$, qui est holomorphe dans le demi-plan $\mathrm{Re}(s)>0$, comme le montre le th. V.5.7.

Proposition G.2.14. — *Soit* χ *un caractère unitaire continu de* $\mathbf{A}^*$ *et, si* $v\in\mathscr{V}$, *soit* χ_v *la restriction de* χ *à* $\mathbf{Q}_v^*$.

(i) *Si* $\phi\in\mathscr{S}(\mathbf{A})$, *alors* $x\mapsto\phi(x)\chi(x)|x|_{\mathbf{A}}^s\in\mathscr{L}(\mathbf{A}^*)$, *si* $\mathrm{Re}(s)>1$.

(ii) *La transformée de Mellin* $\mathrm{M}_{\mathbf{A}}(\phi,\chi,s)=\int_{\mathbf{A}^*}\phi(x)\chi(x)|x|_{\mathbf{A}}^s\,d^*x$ *de* ϕ *est holomorphe sur le demi-plan* $\mathrm{Re}(s)>1$.

(iii) *Si* $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, *et si* $\mathrm{Re}(s) > 1$, *alors* $\mathrm{M}_{\mathbf{A}}(\phi,\chi,s) = \prod_{v\in\mathscr{V}} \mathrm{M}_v(\phi_v,\chi_v,s)$.

Démonstration. — Commençons par supposer que $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, où $\phi_v \in \mathscr{S}(\mathbf{Q}_v)$, et $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$, pour presque tout p. Soit $\psi_v = \phi_v\chi_v|x_v|^s$. Il résulte de la prop. G.2.12 que, si $\mathrm{Re}(s) > 0$, alors $\psi_v \in \mathscr{L}(\mathbf{Q}_v)$ quel que soit $v \in \mathscr{V}$, et que $\int_{\mathbf{Q}_p^*} |\psi_p|\, d^*x_p = \frac{1}{1-p^{-\mathrm{Re}(s)}}$ pour presque tout p. Comme le produit des $\frac{1}{1-p^{-\mathrm{Re}(s)}}$ est convergent pour $\mathrm{Re}(s) > 1$, et comme $\psi_p = 1$ sur $\mathbf{Z}_p^*$ pour presque tout p, d'après la prop. G.2.13, on est dans les conditions d'application de la prop. G.2.10. On en déduit que $\prod_{v\in\mathscr{V}} \psi_v = \phi(x)\chi(x)|x|_{\mathbf{A}}^s \in \mathscr{L}(\mathbf{A}^*)$, si $\mathrm{Re}(s) > 1$, et que

$$\mathrm{M}_{\mathbf{A}}(\phi,\chi,s) = \prod_{v\in\mathscr{V}} \int_{\mathbf{Q}_v^*} \psi_v(x_v)\, d^*x_v = \prod_{v\in\mathscr{V}} \mathrm{M}_v(\phi_v,\chi_v,s).$$

Comme chacune des $\mathrm{M}_v(\phi_v,\chi_v,s)$ est holomorphe sur $\mathrm{Re}(s) > 0$, et comme le produit est absolument convergent sur tout demi-plan $\mathrm{Re}(s) > c$, si $c > 1$, on en déduit (th. V.5.4) l'holomorphie de $\mathrm{M}_{\mathbf{A}}(\phi,\chi,s)$ sur le demi-plan $\mathrm{Re}(s) > 1$. Ceci termine la démonstration dans le cas où ϕ est un produit. Les (i) et (ii) dans le cas général s'en déduisent par linéarité. Ceci permet de conclure.

3.5. *Le théorème de Tate*

Le théorème de Tate ci-dessous permet de prolonger analytiquement les transformées de Mellin de fonctions adéliques. Sa démonstration repose sur la formule de Poisson adélique et constitue une vaste généralisation de la méthode de l'ex. VII.6.6 pour prolonger analytiquement la fonction ζ de Riemann.

Soit χ un caractère unitaire continu de $\mathbf{A}^*$, et soit χ_v, si $v \in \mathscr{V}$, la restriction de χ à $\mathbf{Q}_v^*$. Soit $\mathrm{S}(\chi)$, l'ensemble des p tels que χ_p soit ramifié. D'après la prop. G.2.13 ci-dessus, cet ensemble est fini. On définit le *conducteur* $\mathrm{D}(\chi)$ de χ par la formule $\mathrm{D}(\chi) = \prod_{p\in\mathrm{S}(\chi)} p^{n(\chi_p)}$.

Par ailleurs, la restriction de χ_∞ à $\mathbf{R}_+^*$ est unitaire continue ; il existe donc $t(\chi) \in \mathbf{R}$ tel que $\chi_\infty(x) = x^{it(\chi)}$, si $x \in \mathbf{R}_+^*$.

Théorème G.2.15. — (Tate, 1950) *Si* $\phi \in \mathscr{S}(\mathbf{A})$, *et si* $\chi : \mathbf{A}^* \to \mathbf{C}^*$ *est un caractère linéaire unitaire continu, trivial sur* $\mathbf{Q}^*$, *alors* $\mathrm{M}_{\mathbf{A}}(\phi,\chi,s)$ *admet un prolongement méromorphe à* $\mathbf{C}$ *tout entier, holomorphe en dehors de pôles simples en* $s = -it(\chi)$ *et* $s = 1 - it(\chi)$, *si* $\mathrm{D}(\chi) = 1$, *de résidus respectifs* $-\phi(0)$ *et* $\hat{\phi}(0)$, *et vérifie l'équation fonctionnelle* $\mathrm{M}_{\mathbf{A}}(\phi,\chi,s) = \mathrm{M}_{\mathbf{A}}(\hat{\phi},\overline{\chi},1-s)$.

Démonstration. — Si $\mathrm{Re}(s) > 1$, on a

$$\mathrm{M}_{\mathbf{A}}(\phi,\chi,s) = \int_{\mathbf{A}^*} \phi(x)\chi(x)|x|_{\mathbf{A}}^s\, d^*x = \sum_{\beta\in\mathbf{Q}^*} \int_{\beta\cdot\mathbf{R}_+^*\cdot\widehat{\mathbf{Z}}^*} \phi(x)\chi(x)|x|_{\mathbf{A}}^s\, d^*x$$

Or d^*x et $\chi(x)|x|_{\mathbf{A}}^s$ sont invariants par $x \mapsto \beta\, x$, ce qui permet de réécrire l'expression précédente sous la forme

$$\sum_{\beta\in\mathbf{Q}^*} \int_0^{+\infty} \int_{\widehat{\mathbf{Z}}^*} \phi(\beta x)\chi(x)|x|_{\mathbf{A}}^s\, d^*x = \int_0^{+\infty} \int_{\widehat{\mathbf{Z}}^*} \Big(\sum_{\beta\in\mathbf{Q}^*} \phi(\beta x)\Big)\, \chi(x)|x|_{\mathbf{A}}^s\, d^*x,$$

l'échange des signes $\sum$ et $\int$ étant justifié par la sommabilité de $\phi(x)\chi(x)|x|_{\mathbf{A}}^s$ sur $\mathbf{A}^*$.

Maintenant, comme $\mathbf{Q}^* = \mathbf{Q} - \{0\}$, la formule de Poisson adélique (th. G.2.9) permet d'écrire $\sum_{\beta\in\mathbf{Q}^*}\phi(\beta x)$ sous la forme

$$-\phi(0)+\sum_{\beta\in\mathbf{Q}}\phi(\beta x) = -\phi(0)+|x|_{\mathbf{A}}^{-1}\sum_{\beta\in\mathbf{Q}}\hat{\phi}(\beta x^{-1}) = \hat{\phi}(0)|x|_{\mathbf{A}}^{-1}-\phi(0)+|x|_{\mathbf{A}}^{-1}\sum_{\beta\in\mathbf{Q}^*}\hat{\phi}(\beta x^{-1}).$$

On peut alors couper l'intégrale $\int_0^{+\infty}$ en $\int_0^1+\int_1^{+\infty}$, remplacer $\sum_{\beta\in\mathbf{Q}^*}\phi(\beta x)$ par l'expression ci-dessus dans $\int_0^1$, faire le changement de variable $x\mapsto x^{-1}$ dans $\int_0^1$, et utiliser l'identité $\chi(x^{-1})=\overline{\chi}(x)$ car χ est unitaire. Comme

$$\int_0^1\int_{\widehat{\mathbf{Z}}^*}|x|_{\mathbf{A}}^u\chi(x)d^*x = \Big(\int_0^1 x_\infty^{u+it(\chi)}\frac{dx_\infty}{x_\infty}\Big)\Big(\prod_{p\in\mathscr{P}}\int_{\mathbf{Z}_p^*}\chi_p(x_p)\,d^*x_p\Big) = \begin{cases}0 & \text{si } \mathrm{D}(\chi)\neq 1,\\ \frac{1}{u+it(\chi)} & \text{si } \mathrm{D}(\chi)=1,\end{cases}$$

(si $p|\mathrm{D}(\chi)$, alors $\int_{\mathbf{Z}_p^*}\chi_p(x_p)\,d^*x_p=0$), on obtient

$$\mathrm{M}_{\mathbf{A}}(\phi,\chi,s)=\int_1^{+\infty}\int_{\widehat{\mathbf{Z}}^*}\sum_{\beta\in\mathbf{Q}^*}\big(\phi(\beta x)\chi(x)|x|_{\mathbf{A}}^s+\hat{\phi}(\beta x)\overline{\chi}(x)|x|_{\mathbf{A}}^{1-s}\big)\,d^*x,$$

si $\mathrm{D}(\chi)\neq 1$, auquel il faut rajouter $-\frac{\phi(0)}{s+it(\chi)}-\frac{\hat{\phi}(0)}{1-s-it(\chi)}$, si $\mathrm{D}(\chi)=1$. On en déduit le théorème car $\sum_{\beta\in\mathbf{Q}^*}\big(\phi(\beta x)\chi(x)|x|^s+\hat{\phi}(\beta x)\overline{\chi}(x)|x|^{1-s}\big)$ est sommable pour toute valeur de s, et définit une fonction holomorphe de s sur $\mathbf{C}$ tout entier, et la formule $\hat{\hat{\phi}}(x)=\phi(-x)$ montre que ce qu'on obtient ne change pas si on remplace simultanément ϕ par $\hat{\phi}$, χ par $\overline{\chi}$ et s par $1-s$ (on a $t(\overline{\chi})=-t(\chi)$).

4. Application aux fonctions L de Dirichlet

Le th. G.2.15 permet de redémontrer l'existence de prolongements analytiques et d'équations fonctionnelles pour les fonctions L de Dirichlet. En ce qui concerne les fonctions L de Dirichlet, le gain n'est pas flagrant, mais les calculs adéliques ne sont pas plus compliqués pour les fonctions L de Hecke, et dans ce cas, le gain par rapport à la méthode originelle de Hecke devient très appréciable.

4.1. *La fonction zêta de Riemann.* — Le résultat suivant a déjà été démontré, et la démonstration proposée ci-dessous n'est qu'une traduction adélique de celle de l'ex. VII.6.6.

Proposition G.2.16. — *Soit $\xi(s)=\frac{\Gamma(s/2)}{\pi^{s/2}}\zeta(s)$. Alors $\xi(s)$ a un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples en $s=0$ et $s=1$, de résidus respectifs -1 et 1, et vérifie l'équation fonctionnelle $\xi(1-s)=\xi(s)$.*

Démonstration. — Soit $\phi=\otimes_v\phi_v\in\mathscr{S}(\mathbf{A})$, avec $\phi_\infty(t)=e^{-\pi t^2}$, et $\phi_p=\mathbf{1}_{\mathbf{Z}_p}$, quel que soit $p\in\mathbf{Z}_p$. On a $\hat{\phi}_v=\phi_v$, quel que soit v, et donc $\hat{\phi}=\phi$. De plus $\phi(0)=\hat{\phi}(0)=1$. Il résulte donc du th. G.2.15 que $\mathrm{M}_{\mathbf{A}}(\phi,\mathbf{1},s)$ admet un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples en $s=0$ et $s=1$, de résidus respectifs -1 et 1, et vérifie l'équation fonctionnelle $\mathrm{M}_{\mathbf{A}}(\phi,\mathbf{1},1-s)=\mathrm{M}_{\mathbf{A}}(\phi,\mathbf{1},s)$.

Par ailleurs, on a $\mathrm{M}_{\mathbf{A}}(\phi,\mathbf{1},s)=\prod_{v\in\mathscr{V}}\mathrm{M}_v(\phi_v,\mathbf{1},s)$, si $\mathrm{Re}(s)>1$, d'après le (iii) de la prop. G.2.14. Or $\mathrm{M}_p(\phi_p,\mathbf{1},s)=\frac{1}{1-p^{-s}}$, si $p\in\mathscr{P}$, d'après le (ii) de la prop. G.2.12, et donc $\prod_{p\in\mathscr{P}}\mathrm{M}_p(\phi_p,\mathbf{1},s)=\zeta(s)$. Enfin,

$$\mathrm{M}_\infty(\phi_\infty,\mathbf{1},s)=\mathrm{M}_\infty(e^{-\pi t^2},\mathbf{1},s)=\int_{\mathbf{R}^*}e^{-\pi\,t^2}t^s\,\frac{dt}{|t|}=\int_0^{+\infty}e^{-\pi\,u}u^{s/2}\,\frac{du}{u}=\frac{\Gamma(s/2)}{\pi^{s/2}}.$$

On en déduit que $\xi(s)=\mathrm{M}_{\mathbf{A}}(\phi,\mathbf{1},s)$, ce qui permet de conclure.

4.2. *Fonctions* L *de caractères de* $\mathbf{A}^*$

Soit χ un caractère linéaire unitaire continu de $\mathbf{A}^*$, trivial sur $\mathbf{Q}^*$, dont le conducteur $\mathrm{D}(\chi)$ est différent de 1, et soit χ_v la restriction de χ à $\mathbf{Q}_v^*$, si $v\in\mathscr{V}$.

Comme χ est unitaire, on a soit $\chi_\infty(x_\infty)=|x_\infty|^{it(\chi)}$, soit $\chi_\infty(x_\infty)=\mathrm{sign}(x_\infty)|x_\infty|^{it(\chi)}$. Dans le premier cas, on dit que χ est *pair*, dans le second, qu'il est *impair*. On pose :

$$w_\infty(\chi)=\begin{cases}1 & \text{si } \chi \text{ pair},\\ -i & \text{si } \chi \text{ impair},\end{cases}\qquad c(\chi)=\begin{cases}0 & \text{si } \chi \text{ pair},\\ 1 & \text{si } \chi \text{ impair}.\end{cases}$$

On définit $\varepsilon(\chi,s)$ par la formule $\varepsilon(\chi,s)=\prod_v\varepsilon_v(\chi,s)$, avec

$$\varepsilon_v(\chi,s)=\begin{cases}w_\infty(\chi) & \text{si } v=\infty,\\ w_p(\chi)p^{-n(\chi_p)s} & \text{si } p\in\mathscr{P},\end{cases},\quad \text{où } w_p(\chi)=\begin{cases}1 & \text{si } p\nmid \mathrm{D}(\chi),\\ \chi_p(p^{n(\chi_p)})\mathrm{G}(\overline{\chi}_p) & \text{si } p\mid \mathrm{D}(\chi).\end{cases}$$

On a donc $\varepsilon(\chi,s)=\big(\prod_v w_v(\chi)\big)\mathrm{D}(\chi)^{-s}$. (La somme de Gauss $\mathrm{G}(\overline{\chi}_p)$ est la somme de Gauss du caractère de Dirichlet de conducteur $p^{n(\chi_p)}$ obtenu en utilisant l'isomorphisme $(\mathbf{Z}_p/p^{n(\chi_p)}\mathbf{Z}_p)^*\cong(\mathbf{Z}/p^{n(\chi_p)}\mathbf{Z})^*$.)

Enfin, on définit la fonction L de χ par $\mathrm{L}(\chi,s)=\prod_{p\nmid \mathrm{D}(\chi)}\frac{1}{1-\chi_p(p)p^{-s}}$, si $\mathrm{Re}(s)>1$.

Proposition G.2.17. — *La fonction* $\Lambda(\chi,s)=\frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}}\mathrm{L}(\chi,s)$ *admet un prolongement holomorphe à* $\mathbf{C}$*, et vérifie l'équation fonctionnelle* $\Lambda(\chi,s)=\varepsilon(\chi,s)\Lambda(\overline{\chi},1-s)$.

Démonstration. — Soit $\phi=\otimes_v\phi_v$, on l'on a posé

- $\phi_\infty(t)=e^{-\pi\,t^2}$, si χ est pair, et $\phi_\infty(t)=t\,e^{-\pi\,t^2}$, si χ est impair,
- $\phi_p=\mathbf{1}_{\mathbf{Z}_p}$, si $p\nmid \mathrm{D}(\chi)$,
- $\phi_p=\mathbf{1}_{\mathbf{Z}_p^*}\overline{\chi}_p$, si $p\mid \mathrm{D}(\chi)$.

Nous allons calculer les facteurs $\mathrm{M}_v(\phi_v,\chi_v,s)$ et $\mathrm{M}_v(\hat{\phi}_v,\overline{\chi}_v,1-s)$, pour tout v.

• On a $\hat{\phi}_\infty=w_\infty(\chi)\phi_\infty$. En effet, si χ est pair, ceci est équivalent au fait que la transformée de Fourier de $e^{-\pi t^2}$ est $e^{-\pi x^2}$. Si χ est impair, ceci équivaut au fait que la transformée de Fourier de $te^{-\pi t^2}$ est $-ixe^{-\pi x^2}$, ce qui peut se vérifier en remarquant que $-2\pi te^{-\pi t^2}$ est la dérivée de $e^{-\pi t^2}$ et donc sa dérivée est $2i\pi x$ fois la transformée de Fourier de $e^{-\pi t^2}$. On en déduit que

$$\mathrm{M}_\infty(\phi_\infty,\chi_\infty,s)=\frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}}\quad\text{et}\quad\mathrm{M}_\infty(\hat{\phi}_\infty,\overline{\chi}_\infty,s)=w_\infty(\chi)\frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}},$$

par un petit calcul analogue à celui que l'on a fait pour déterminer $\mathrm{M}_\infty(e^{-\pi t^2},\mathbf{1},s)$.

• Si $p \nmid \mathrm{D}(\chi)$, on a $\hat{\phi}_p = \mathbf{1}_{\mathbf{Z}_p}$, et donc, d'après le (ii) de la prop. G.2.12, si $\mathrm{Re}(s) > 0$,

$$\mathrm{M}_p(\phi_p, \chi_p, s) = \frac{1}{1-\chi_p(p)p^{-s}} \quad \text{et} \quad \mathrm{M}_p(\hat{\phi}_p, \overline{\chi}_p, s) = \frac{1}{1-\overline{\chi}_p(p)p^{-s}}.$$

• Si $p \mid \mathrm{D}(\chi)$, on a $\mathrm{M}_p(\phi_p, \chi_p, s) = 1$, comme le montre un calcul immédiat. Par ailleurs, on a $\hat{\phi}_p(x) = \frac{\mathrm{G}(\overline{\chi}_p)}{p^{n(\chi_p)}}\chi_p(p^{n(\chi_p)}x)\mathbf{1}_{p^{-n(\chi_p)}\mathbf{Z}_p^*}(x)$, d'après le (iii) de l'ex. G.2.7, et donc

$$\begin{aligned}\mathrm{M}_p(\hat{\phi}_p, \overline{\chi}_p, 1-s) &= \frac{\mathrm{G}(\overline{\chi}_p)}{p^{n(\chi_p)}}\int_{p^{-n(\chi_p)}\mathbf{Z}_p^*} \chi_p(p^{n(\chi_p)}x)\overline{\chi}_p(x)|x|_p^{1-s}\, d^*x \\ &= \frac{\mathrm{G}(\overline{\chi}_p)}{p^{n(\chi_p)}}\chi_p(p^{n(\chi_p)})p^{n(\chi_p)(1-s)}\int_{p^{-n(\chi_p)}\mathbf{Z}_p^*} d^*x = w_p(\chi)p^{-n(\chi_p)(s)}.\end{aligned}$$

On a donc, si $\mathrm{Re}(s) > 1$,

$$\mathrm{M}_{\mathbf{A}}(\phi, \chi, s) = \prod_{v\in\mathscr{V}} \mathrm{M}_v(\phi_v, \chi_v, s) = \frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}} \prod_{p\nmid \mathrm{D}(\chi)} \frac{1}{1-\chi_p(p)p^{-s}} = \Lambda(\chi, s).$$

De même, si $\mathrm{Re}(s) < 0$, alors $\mathrm{M}_{\mathbf{A}}(\hat{\phi}, \overline{\chi}, 1-s) = \prod_{v\in\mathscr{V}} \mathrm{M}_v(\hat{\phi}_v, \overline{\chi}_v, 1-s)$ est aussi égal à

$$w_\infty(\chi)\frac{\Gamma((1-s+it(\chi)+c(\chi))/2)}{\pi^{(1-s+it(\chi)+c(\chi))/2}}\Big(\prod_{p\mid \mathrm{D}(\chi)} w_p(\chi)p^{-n(\chi_p)(s)}\Big)\prod_{p\nmid \mathrm{D}(\chi)} \frac{1}{1-\overline{\chi}_p(p)p^{-(1-s)}},$$

c'est-à-dire à $\varepsilon(\chi, s)\Lambda(\overline{\chi}, 1-s)$. Le résultat suit donc du th. G.2.15, en utilisant le fait que $\phi(0) = \hat{\phi}(0) = 0$ car $\phi_p(0) = \hat{\phi}_p(0) = 0$, si $p \mid \mathrm{D}(\chi)$.

4.3. *Caractères de Dirichlet et caractères linéaires continus des idèles*

A un caractère de Dirichlet χ de conducteur D, on peut associer, grâce au lemme G.2.5, un caractère linéaire $\chi_{\mathbf{A}}$ de $\mathbf{A}^*$, continu, d'ordre fini (et donc unitaire), par la formule $\chi_{\mathbf{A}}(x) = \chi(\pi_{\mathrm{D}}(b^{]\infty[}))^{-1}$, si $x = \beta b_\infty b^{]\infty[}$, où $\beta \in \mathbf{Q}^*$, $b_\infty \in \mathbf{R}_+^*$, $b^{]\infty[} \in \widehat{\mathbf{Z}}^*$, et où l'on note $\pi_{\mathrm{D}} : \widehat{\mathbf{Z}}^* \to (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$ la projection naturelle [36]. On remarquera que $\chi_{\mathbf{A}}$ est trivial sur $\mathbf{Q}^*$ par construction.

Lemme G.2.18. — $\mathrm{L}(\chi_{\mathbf{A}}, s) = \mathrm{L}(\chi, s)$.

Démonstration. — On note χ_p la restriction de $\chi_{\mathbf{A}}$ à $\mathbf{Q}_p^*$, et il s'agit de vérifier que si $p \nmid \mathrm{D}$, alors $\chi(p) = \chi_p(p)$. Soit x (resp. y) l'idèle dont toutes les composantes sont 1 (resp. p^{-1}) sauf la composante en p qui est égale à p (resp. 1). On a alors $\chi_p(p) = \chi_{\mathbf{A}}(x)$ par définition, et comme $x = py$, on a $\chi_p(p) = \chi(\pi_{\mathrm{D}}(y^{]\infty[}))^{-1}$. Or $y^{]\infty[}$ a toutes ses composantes en les ℓ divisant D égales à p^{-1} ; on en déduit que $\pi_{\mathrm{D}}(y^{]\infty[}) = p^{-1}$, et donc que $\chi_p(p) = \chi(p^{-1})^{-1} = \chi(p)$, ce qui permet de conclure.

36. On envoie $\mathbf{Z}_p^*$ sur 1, si $p \nmid \mathrm{D}$, et $\mathbf{Z}_p^*$ sur $(\mathbf{Z}_p/p^{v_p(\mathrm{D})}\mathbf{Z}_p)^* = (\mathbf{Z}/p^{v_p(\mathrm{D})}\mathbf{Z})^*$, si $p \mid \mathrm{D}$, et on utilise l'isomorphisme $(\mathbf{Z}/\mathrm{D}\mathbf{Z})^* = \prod_{p\mid \mathrm{D}}(\mathbf{Z}/p^{v_p(\mathrm{D})}\mathbf{Z})^*$ fourni par le théorème des restes chinois.

On déduit de ce lemme, et de la prop. G.2.17, une démonstration adélique de l'existence d'un prolongement analytique et d'une équation fonctionnelle pour $\mathrm{L}(\chi, s)$. Par ailleurs, ce lemme permet aussi de reformuler le théorème de Kronecker-Weber sous la forme suivante.

Théorème G.2.19. — *Si ρ est une représentation de dimension 1 de $\mathscr{G}_{\mathbf{Q}}$, il existe un caractère linéaire unitaire continu $\chi(\rho)$ de $\mathbf{A}^* = \mathbf{GL}_1(\mathbf{A})$, trivial sur $\mathbf{Q}^* = \mathbf{GL}_1(\mathbf{Q})$, tel que $\mathrm{L}(\rho, s) = \mathrm{L}(\chi(\rho), s)$.*

G.3. Le programme de Langlands

Le programme de Langlands consiste à remplacer 1 par n dans l'énoncé du th. G.2.19 ci-dessus. (C'est plus facile à dire qu'à faire...)

1. Représentations automorphes

Notons G le groupe $\mathbf{GL}_n$, et donc $\mathrm{G}(\mathbf{A})$, $\mathrm{G}(\mathbf{Q})$, $\mathrm{G}(\mathbf{R})$, $\mathrm{G}(\mathbf{Q}_p)$ et $\mathrm{G}(\mathbf{Z}_p)$ désignent respectivement les groupes $\mathbf{GL}_n(\mathbf{A})$, $\mathbf{GL}_n(\mathbf{Q})$, $\mathbf{GL}_n(\mathbf{R})$, $\mathbf{GL}_n(\mathbf{Q}_p)$ et $\mathbf{GL}_n(\mathbf{Z}_p)$. Alors $\mathrm{G}(\mathbf{A})$ est le produit restreint des $\mathrm{G}(\mathbf{Q}_v)$, pour $v \in \mathscr{V}$, relativement aux $\mathrm{G}(\mathbf{Z}_p)$, pour $p \in \mathscr{P}$; autrement dit, un élément x de $\mathrm{G}(\mathbf{A})$ est de la forme $(x_v)_{v\in\mathscr{V}}$, avec $x_v \in \mathrm{G}(\mathbf{Q}_v)$, et $x_p \in \mathrm{G}(\mathbf{Z}_p)$ pour presque tout p. On écrit aussi x sous la forme $(x_\infty, x^{]\infty[})$, où $x^{]\infty[} = (x_p)_{p\in\mathscr{P}}$ est la partie de x en dehors de ∞. Comme d'habitude, $\mathrm{G}(\mathbf{Q}_v)$ s'identifie à un sous-groupe de $\mathrm{G}(\mathbf{A})$, si $v \in \mathscr{V}$.

Soit $\mathscr{A}_0(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))$ le $\mathbf{C}$-espace vectoriel des *formes automorphes*[37] cuspidales pour $\mathrm{G}(\mathbf{A})$, c'est-à-dire des fonctions $\phi : \mathrm{G}(\mathbf{A}) \to \mathbf{C}$ vérifiant :

(i) $\phi(\gamma x) = \phi(x)$ quels que soient $\gamma \in \mathrm{G}(\mathbf{Q})$ et $x \in \mathrm{G}(\mathbf{A})$,

(ii) il existe K_ϕ d'indice fini dans $\prod_{p\in\mathscr{P}} \mathrm{G}(\mathbf{Z}_p)$ tel que $\phi(xh) = \phi(x)$ quels que soient $x \in \mathrm{G}(\mathbf{A})$ et $h \in \mathrm{K}_\phi$, et les $\phi(xh)$, pour[38] $h \in \mathbf{O}_n(\mathbf{R})$, engendrent un espace de dimension finie,

(iii) il existe un caractère linéaire unitaire continu χ de $\mathbf{A}^*$, trivial sur $\mathbf{Q}^*$, tel que $\phi(\mathrm{A}_z x) = \phi(x\mathrm{A}_z) = \chi(z)\phi(x)$, si A_z est la matrice de l'homothétie de rapport $z \in \mathbf{A}^*$,

(iv) Si $x^{]\infty[}$ est fixé, $\phi(x_\infty, x^{]\infty[})$ est une fonction de classe $\mathscr{C}^\infty$ des coordonnées de x_∞, vecteur propre de tous les opérateurs différentiels commutant à l'action de $\mathrm{G}(\mathbf{R})$.

(v) ϕ est à décroissance rapide à l'infini (en un sens que nous ne préciserons pas).

On fait agir $g \in \mathrm{G}(\mathbf{A})$ sur les fonctions $\phi : \mathrm{G}(\mathbf{A}) \to \mathbf{C}$ par translation à droite sur la variable, c'est-à-dire par $g \cdot \phi(x) = \phi(xg)$. L'espace $\mathscr{A}_0(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))$ n'est pas stable par

37. L'automorphie traduit la condition (i) qui est la plus subtile des conditions (i)-(v) ci-dessus, et la cuspidalité correspond à la condition (v).

38. Le groupe $\mathbf{O}_n(\mathbf{R})$ est le groupe des isométries de $\mathbf{R}^n$; c'est un sous-groupe compact de $\mathrm{G}(\mathbf{R})$, et il est maximal pour cette propriété, de la même manière que $\mathrm{G}(\mathbf{Z}_p)$ est un sous-groupe compact de $\mathrm{G}(\mathbf{Q}_p)$, et est maximal pour cette propriété.

l'action de $\mathrm{G}(\mathbf{A})$, mais presque [39], et nous allons un peu tricher en prétendant qu'il l'est (cf. note 39 pour un énoncé correct), et donc que $\mathscr{A}_0(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))$ est une représentation de $\mathrm{G}(\mathbf{A})$. Alors $\mathscr{A}_0(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))$ se décompose en somme directe de représentations irréductibles (ses composantes irréductibles sont les *représentations automorphes cuspidales*). Le théorème ci-dessous représente un travail certain (dû, pour $n = 2$, à Jacquet et Langlands (1969), et pour $n \geqslant 3$, à Godement et Jacquet (1972)). La démonstration de l'existence et du prolongement analytique des fonctions L automorphes a fortement été inspirée par la méthode introduite par Tate pour étudier les fonctions L de Hecke.

Théorème G.3.1. — *Soit* Π *une représentation automorphe cuspidale de degré* n*. Alors*

(i) Π *admet une factorisation* [40] *sous la forme* $\Pi = \otimes'_{v\in\mathscr{V}}\Pi_v$*, où* Π_v *est une représentation irréductible* (de dimension infinie) *de* $\mathrm{G}(\mathbf{Q}_v)$*.*

(ii) Π *admet une fonction* L *se factorisant sous la forme* [41] $\mathrm{L}(\Pi, s) = \prod_{v\in\mathscr{V}}\mathrm{L}(\Pi_v, s)$*, où* $\mathrm{L}(\Pi_\infty, s)$ *est un produit de fonctions* Γ *qui ne dépend que de* Π_∞*, et* $\mathrm{L}(\Pi_p, s) = \frac{1}{\mathrm{E}_p(p^{-s})}$*, où* $\mathrm{E}_p(\mathrm{X})$ *est un polynôme de degré* $\leqslant n$ *et de degré* n *pour presque tout* p*, dont le terme constant est* 1*, et qui ne dépend que de* Π_p*.*

(iii) $\mathrm{L}(\Pi, s)$ *admet un prolongement holomorphe à tout le plan complexe, et admet une*

---

39. Il est stable par $\mathrm{G}(\mathbf{A}^{]\infty[})$, par $\mathbf{O}_n(\mathbf{R})$, mais pas par $\mathrm{G}(\mathbf{R})$ à cause de la condition (iii) imposant que les $\phi(xh)$, pour $h \in \mathbf{O}_n(\mathbf{R})$, engendrent un espace de dimension finie. Par contre, il est stable par l'*action infinitésimale* de $\mathrm{G}(\mathbf{R})$, c'est-à-dire par les opérateurs différentiels ∂_A, pour $\mathrm{A} \in \mathbf{M}_n(\mathbf{R})$, avec $\partial_\mathrm{A}\phi(x) = \lim_{t\to 0} t^{-1}(\phi(xe^{t\mathrm{A}}) - \phi(x))$, et $e^{t\mathrm{A}} = \sum_{n=0}^{+\infty}\frac{t^n\mathrm{A}^n}{n!} \in \mathrm{G}(\mathbf{R})$ est l'exponentielle de la matrice $t\mathrm{A}$. Il y a des conditions de compatibilité évidentes que doivent satisfaire les actions de $\mathbf{O}_n(\mathbf{R})$ et $\mathbf{M}_n(\mathbf{R})$ car $e^{t\mathrm{A}} \in \mathbf{O}_n(\mathbf{R})$ si (et seulement si) A est antisymétrique. Dans ce qui suit, nous commettrons l'abus d'appeler représentation de $\mathrm{G}(\mathbf{R})$ (resp. de $\mathrm{G}(\mathbf{A})$) un $\mathbf{C}$-espace vectoriel muni d'actions de $\mathbf{O}_n(\mathbf{R})$ et $\mathbf{M}_n(\mathbf{R})$ vérifiant les relations de compatibilité évoquées ci-dessus.

40. Le groupe $\mathrm{G}_\mathbf{A}$ est essentiellement un produit. Or on a vu, dans le cas des groupes finis, que si $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2$, alors toute représentation irréductible de G se factorise sous la forme $\mathrm{V}_1 \otimes \mathrm{V}_2$ où V_i est une représentation irréductible de G_i, si $i = 1, 2$. Il est donc naturel de penser qu'une représentation irréductible de $\mathrm{G}_\mathbf{A}$ va aussi admettre une factorisation, et c'est ce que prétend le (i) du th. G.3.1.

D'un autre côté, il n'est pas très raisonnable de faire le produit tensoriel d'une infinité d'espaces vectoriels, et le produit tensoriel du théorème est un *produit tensoriel restreint*. (On a déjà vu des exemples de cette notion : $\mathscr{S}(\mathbf{A})$ est le produit tensoriel restreint des $\mathscr{S}(\mathbf{Q}_v)$, pour $v \in \mathscr{V}$, relativement aux fonctions $\mathbf{1}_{\mathbf{Z}_p}$, pour $p \in \mathscr{P}$; de même, $\mathscr{L}_0(\mathbf{A}^*)$ est le produit tensoriel restreint de $\mathscr{L}(\mathbf{R}^*)$ et des $\mathscr{L}_0(\mathbf{Q}_p^*)$, pour $p \in \mathscr{P}$, relativement aux fonctions $\mathbf{1}_{\mathbf{Z}_p^*}$, pour $p \in \mathscr{P}$.) De manière précise, pour tout p tel que le polynôme E_p du (ii) du théorème soit de degré n, la représentation Π_p possède un vecteur privilégié x_p (bien déterminé à multiplication près par un élément de $\mathbf{C}^*$, mais cette indétermination est sans importance) qui est fixe par $\mathrm{G}(\mathbf{Z}_p)$. Alors le produit tensoriel restreint $\otimes_{v\in\mathscr{V}}\Pi_v$ relativement aux vecteurs x_p est engendré par des éléments de la forme $\otimes_{v\in\mathscr{V}} y_v$, avec $y_p = x_p$ pour presque tout p. On remarquera que $g \in \mathrm{G}_\mathbf{A}$ agit naturellement sur un élément de ce type par la formule $g \cdot (\otimes_{v\in\mathscr{V}} y_v) = \otimes_{v\in\mathscr{V}}(g_v \cdot y_v)$, comme dans le cas du produit tensoriel de représentations de deux groupes, le point étant que $g_p \in \mathrm{G}(\mathbf{Z}_p)$ pour presque tout p et donc que $g_p \cdot y_p = x_p$, pour presque tout p.

41. Ces *fonctions* L *automorphes* sont de vastes généralisations des fonctions L de Dirichlet.

équation fonctionnelle du type $\mathrm{L}(\Pi, s) = \varepsilon(s)\mathrm{L}(\Pi^\vee, 1-s)$*, où* $\Pi^\vee$ *est une autre représentation automorphe cuspidale* (contragrédiente de Π)*, et* $\varepsilon(s)$ *est de la forme* $\mathrm{A}\cdot\mathrm{B}^s$*, avec* $\mathrm{A}\in\mathbf{C}^*$ *et* $\mathrm{B}\in\mathbf{R}_+^*$.

Conjecture G.3.2. — (Langlands, 1968) *Si* ρ *est une représentation irréductible de dimension* n *de* $\mathscr{G}_{\mathbf{Q}}$*, il existe une représentation automorphe cuspidale de degré* n *telle que* $\mathrm{L}(\rho, s) = \mathrm{L}(\Pi(\rho), s)$.

Au vu du théorème ci-dessus, cette conjecture implique la conjecture d'Artin, mais va en fait bien au-delà. Ce n'est qu'un petit bout de l'édifice dont Langlands conjecture l'existence.

Nous montrerons comment transformer une forme modulaire primitive ou une forme de Maass primitive en une représentation automorphe cuspidale de $\mathbf{GL}_2(\mathbf{A})$ dans le n° 2, ce qui permet de voir les représentations automorphes cuspidales comme une vaste généralisation des formes modulaires (ou de Maass) primitives. Notons qu'en degré $\geqslant 3$, il ne semble pas forcément y avoir d'équivalents des formes modulaires ou de Maass, et le recours au langage des représentations devient difficilement contournable.

2. Des formes modulaires aux représentations automorphes

2.1. *Préliminaires*

Si $\mathrm{D}\in\mathbf{N}$, soit K^{D} le sous-groupe de $\mathbf{GL}_2(\widehat{\mathbf{Z}}) = \prod_{p\in\mathscr{P}}\mathbf{GL}_2(\mathbf{Z}_p)$ des $h = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$, avec $c\in \mathrm{D}\widehat{\mathbf{Z}}$. Si χ est un caractère de Dirichlet modulo D, on fabrique un caractère linéaire $\tilde{\chi}$ de K^{D}, en posant $\tilde{\chi}(h) = \chi(\overline{d})$, où l'on a noté $\overline{d}$ l'image de d dans $(\widehat{\mathbf{Z}}/\mathrm{D}\widehat{\mathbf{Z}})^* = (\mathbf{Z}/\mathrm{D}\mathbf{Z})^*$. On a alors $\tilde{\chi}(\gamma) = \chi(d)$, si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_0(\mathrm{D})$.

Proposition G.3.3. — (i) *Tout élément de* $\mathbf{GL}_2(\mathbf{A})$ *peut s'écrire sous la forme* $\gamma g_\infty \kappa$*, avec* $\gamma\in\mathbf{GL}_2(\mathbf{Q})$*,* $g_\infty\in\mathbf{GL}_2(\mathbf{R})^+ = \{g\in\mathbf{GL}_2(\mathbf{R}),\ \det g > 0\}$*, et* $\kappa\in\mathrm{K}^{\mathrm{D}}$.

(ii) *Cette écriture est unique à multiplication près de* γ *à droite par* $\alpha\in\Gamma_0(\mathrm{D})$ *et de* g_∞ *et* κ *à gauche par* α^{-1}.

Démonstration. — Cf. alinéa 2.3.

2.2. *La forme automorphe associée à une forme modulaire*

Soit $f\in\mathrm{S}_k(\mathrm{D},\chi)$. On peut utiliser la décomposition de $\mathbf{GL}_2(\mathbf{A})$ ci-dessus pour attacher à f une fonction ϕ_f sur $\mathbf{GL}_2(\mathbf{A})$, grâce à la formule,

$$\phi_f(x) = \tilde{\chi}(h)^{-1}\Big(\frac{(a_\infty d_\infty - b_\infty c_\infty)^{1/2}}{c_\infty i + d_\infty}\Big)^k f\Big(\frac{a_\infty i + b_\infty}{c_\infty i + d_\infty}\Big),\quad \text{si } x = \gamma g_\infty h \text{ et } g_\infty = \left(\begin{smallmatrix} a_\infty & b_\infty \\ c_\infty & d_\infty\end{smallmatrix}\right).$$

Le (ii) de la prop. G.3.3 et le fait que $(cz+d)^{-k}f\big(\frac{az+b}{cz+d}\big) = \chi(d)f(z)$, si $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\in\Gamma_0(\mathrm{D})$, montrent que ceci ne dépend pas de la décomposition de x choisie. Il n'est pas très difficile de vérifier que ϕ_f est une forme automorphe cuspidale.

On procède de même avec une forme de Maass f, de caractère χ et valeur propre λ pour $\Gamma_0(\mathrm{D})$, en définissant ϕ_f par la formule $\phi_f(x) = \tilde{\chi}(h)^{-1} f(g_\infty)$.

Dans les deux cas, on note Π_f le sous-espace de $\mathscr{A}_0(\mathbf{GL}_2(\mathbf{Q})\backslash\mathbf{GL}_2(\mathbf{A}))$ engendré par ϕ_f sous l'action de $\mathbf{GL}_2(\mathbf{A})$. Le théorème ci-dessous peut être considéré comme le point de départ du programme de Langlands.

Théorème G.3.4. — (i) *Si f est primitive, alors Π_f est une représentation automorphe cuspidale de degré 2, et donc admet une factorisation sous la forme $\Pi_f = \otimes_{v\in\mathscr{V}}\Pi_{f,v}$.*

(ii) *Si f est de niveau D, et si p ne divise pas D, la représentation $\Pi_{f,p}$ est complètement décrite par le facteur d'Euler $\mathrm{E}_p(f,s)$ en p de la fonction $\mathrm{L}(f,s)$, et $\mathrm{L}(\Pi_{f,p},s) = \mathrm{E}_p(f,s)^{-1}$.*

Pour préciser le (ii), factorisons le facteur d'Euler $\mathrm{E}_p(f,s)$ sous la forme

$$\begin{cases} \mathrm{E}_p(f, s+\frac{k-1}{2}) = (1-\alpha_p p^{-s})(1-\beta_p p^{-s}) & \text{si } f \text{ est une forme modulaire de poids } k, \\ \mathrm{E}_p(f,s) = (1-\alpha_p p^{-s})(1-\beta_p p^{-s}) & \text{si } f \text{ est une forme de Maass.} \end{cases}$$

Ceci permet de définir deux caractères μ_1, μ_2 de $\mathbf{Q}_p^*$ par la formule $\mu_1(x) = \alpha_p^{-v_p(x)}$ et $\mu_2(x) = \beta_p^{-v_p(x)}$. La représentation $\Pi_{f,p}$ est alors la représentation $\mathrm{I}(\mu_1,\mu_2)$ obtenue en faisant agir $\mathbf{GL}_2(\mathbf{Q}_p)$, par translation à droite sur la variable, sur l'espace des fonctions ϕ localement constantes sur $\mathbf{GL}_2(\mathbf{Q}_p)$ telles que

$$\phi\big(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)x\big) = \mu_1(a)\mu_2(d)\big|\frac{a}{d}\big|^{1/2}\phi(x), \quad \text{si } a,d \in \mathbf{Q}_p^*,\ b \in \mathbf{Q}_p, \text{ et } x \in \mathbf{GL}_2(\mathbf{Q}_p).$$

La construction ci-dessus n'est pas sans rappeler la construction des représentations induites pour les groupes finis (cf. n° 2 du § C.3) et, si on note B le sous-groupe de Borel de $\mathbf{GL}_2(\mathbf{Q}_p)$, (i.e. le sous-groupe des matrices triangulaires supérieures), alors $\mathrm{I}(\mu_1,\mu_2)$ est *l'induite localement constante* à G du caractère linéaire $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto \mu_1(a)\mu_2(d)\big|\frac{a}{d}\big|^{1/2}$ de B.

La représentation $\Pi_{f,p}$, pour p divisant D, est plus subtile à décrire. Sa description rentre dans le cadre de la *correspondance de Langlands locale* (cf. n° 3).

2.3. *La décomposition de* $\mathbf{GL}_2(\mathbf{A})$

Lemme G.3.5. — *Si* S *est un sous-ensemble fini de $\mathscr{P}$, alors $\mathbf{SL}_2(\mathbf{Z}[\mathrm{S}^{-1}])$ est dense dans $\prod_{p\in\mathrm{S}}\mathbf{SL}_2(\mathbf{Q}_p)$.*

Démonstration. — Soit $\mathrm{A} = (\mathrm{A}_p)_{p\in\mathrm{S}} \in \prod_{p\in\mathrm{S}}\mathbf{SL}_2(\mathbf{Q}_p)$. D'après le lemme B.2.2, on peut écrire A_p sous la forme $\mathrm{A}_p = \left(\begin{smallmatrix} 1 & 0 \\ t_p & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & x_p \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ y_p & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & z_p \\ 0 & 1 \end{smallmatrix}\right)$, avec $t_p, x_p, y_p, z_p \in \mathbf{Q}_p$. Comme $\mathbf{Z}[\mathrm{S}^{-1}]$ est dense dans $\prod_{p\in\mathrm{S}}\mathbf{Q}_p$, on peut trouver des suites $(t'_n)_{n\in\mathbf{N}}$, $(x'_n)_{n\in\mathbf{N}}$, $(y'_n)_{n\in\mathbf{N}}$ et $(z'_n)_{n\in\mathbf{N}}$ d'éléments de $\mathbf{Z}[\mathrm{S}^{-1}]$ tendant respectivement vers t_p, x_p, y_p et t_p, pour tout $p \in \mathrm{S}$. Si on pose $\mathrm{A}'_n = \left(\begin{smallmatrix} 1 & 0 \\ t'_n & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & x'_n \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ y'_n & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & z'_n \\ 0 & 1 \end{smallmatrix}\right)$, alors $(\mathrm{A}'_n)_{n\in\mathbf{N}}$ est une suite d'éléments de $\mathbf{SL}_2(\mathbf{Z}[\mathrm{S}^{-1}])$ tendant vers A dans $\prod_{p\in\mathrm{S}}\mathbf{SL}_2(\mathbf{Q}_p)$. Ceci permet de conclure.

Venons-en à la démonstration de la prop. G.3.3. Soit $g \in \mathbf{GL}_2(\mathbf{A})$. Comme $\det g \in \mathbf{A}^*$, on peut écrire $\det g$ de manière unique sous la forme βb, où $b = (b_\infty, b^{]\infty[})$, avec $\beta \in \mathbf{Q}^*$,

$b_\infty \in \mathbf{R}_+^*$ et $b^{]\infty[} \in \prod_{p\in\mathscr{P}} \mathbf{Z}_p^*$. Mais alors $h = \left(\begin{smallmatrix}\beta^{-1} & 0\\ 0 & 1\end{smallmatrix}\right) g \left(\begin{smallmatrix}b^{-1} & 0\\ 0 & 1\end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{A})$. Soit S le sous-ensemble de $\mathscr{P}$ constitué des p divisant D et des p tels que $h_p \notin \mathbf{SL}_2(\mathbf{Z}_p)$. D'après le lemme G.3.5, on peut trouver $\gamma_0 \in \mathbf{SL}_2(\mathbf{Z}[\mathrm{S}^{-1}])$ aussi proche que l'on veut de $(h_p)_{p\in\mathrm{S}}$; en particulier, on peut trouver $\gamma_0 \in \mathbf{SL}_2(\mathbf{Z}[\mathrm{S}^{-1}])$ tel que $\gamma_0^{-1}h_p = \left(\begin{smallmatrix}a_p & b_p\\ c_p & d_p\end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbf{Z}_p)$ quel que soit $p \in \mathrm{S}$, et vérifie $v_p(c_p) \geqslant v_p(\mathrm{D})$, quel que soit p divisant D. Alors $\gamma = \left(\begin{smallmatrix}\beta & 0\\ 0 & 1\end{smallmatrix}\right)\gamma_0$, $g_\infty = \gamma_0^{-1}h_\infty \left(\begin{smallmatrix}b_\infty & 0\\ 0 & 1\end{smallmatrix}\right)$ et $\kappa = \gamma_0^{-1}h^{]\infty[}\left(\begin{smallmatrix}b^{]\infty[} & 0\\ 0 & 1\end{smallmatrix}\right)$ fournissent une décomposition de g ayant les propriétés voulues. Ceci démontre le (i).

Le (ii) suit juste du fait qu'un élément $\gamma = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ dans l'intersection de $\mathbf{GL}_2(\mathbf{Q})$ et de $\mathbf{GL}_2(\mathbf{R})^+\mathrm{K}^{\mathrm{D}}$ est à coefficients dans $\mathbf{Z}$ ainsi que son inverse, de déterminant positif, et vérifie $v_p(c) \geqslant v_p(\mathrm{D})$ quel que soit $p \in \mathscr{P}$. Autrement dit, c'est un élément de $\Gamma_0(\mathrm{D})$.

3. Quelques autres aspects du programme de Langlands

Le programme de Langlands a plusieurs autres facettes. En particulier, on peut remplacer $\mathbf{Q}$ par un corps de nombres F dans tout ce qu'on a fait ; l'anneau des adèles de F étant construit de la même manière, à partir de tous les complétés F_v de F.

• *La correspondance de Langlands locale.* Il s'agit d'une correspondance entre les représentations irréductibles de dimension n de $\mathscr{G}_{\mathbf{Q}_p}$ et certaines représentations irréductibles (les représentations cuspidales) de $\mathbf{GL}_n(\mathbf{Q}_p)$. Cette correspondance a finalement été établie, en toute généralité [42], par M. Harris (Paris 7) et R. Taylor (Harvard) en 1999, et simplifiée par G. Henniart (Orsay), toujours en 1999. Ceci fournit une description indirecte fort utile du groupe $\mathscr{G}_{\mathbf{Q}_p}$.

• *La correspondance de Langlands pour les corps de fonctions.* Fixons un nombre premier p. On peut considérer, au lieu de $\mathbf{Q}$ et des corps de nombres, les extensions finies K du corps $\mathbf{F}_p(\mathrm{X})$ des fractions rationnelles à coefficients dans $\mathbf{F}_p$. L'anneau des adèles de K est défini à partir des complétés de $\mathbf{F}_p(\mathrm{X})$ pour les différentes normes que l'on peut mettre sur $\mathbf{F}_p(\mathrm{X})$; une différence avec le cas des corps de nombres est que ces complétés se ressemblent beaucoup : ils sont tous de la forme $\mathbf{F}_q((\mathrm{T}))$, corps des fractions de l'anneau des séries formelles à coefficients dans $\mathbf{F}_q$, où $\mathbf{F}_q$ est le corps fini à q éléments et q est une puissance de p. Dans ce cadre, la correspondance de Langlands a été établie par L. Lafforgue (I.H.E.S., Bures sur Yvette) en 1999, ce qui lui a valu la médaille Fields (2002). La démonstration utilise, entre autres, de puissants outils de géométrie algébrique introduits par A. Grothendieck dans les années 60 ; le cas $n = 2$ avait été établi par V. Drinfeld (médaillé Fields en 1990) dans les années 70, et la démonstration de L. Lafforgue est une vaste généralisation de celle de V. Drinfeld.

• *La fonctorialité de Langlands.* Du côté galoisien, on dispose de tas de constructions donnant de nouvelles représentations à partir de représentations connues. Par exemple, si $\mathrm{F} \subset \mathrm{K}$ sont deux corps de nombres, et si ρ est une représentation de $\mathscr{G}_{\mathrm{F}}$ (resp. de $\mathscr{G}_{\mathrm{K}}$),

42. De la même manière que l'on peut considérer un corps de nombres au lieu de $\mathbf{Q}$, on peut considérer un complété F_v d'un corps de nombres au lieu de $\mathbf{Q}_p$.

on peut considérer la restriction (resp. l'induction) de ρ à $\mathscr{G}_{\mathrm{K}}$ (resp. à $\mathscr{G}_{\mathrm{F}}$). Toutes ces constructions devraient avoir des analogues du côté automorphe, mais on est encore bien loin de comprendre vraiment ce qui se passe même si, en 2008, Ngô B.C. (maintenant à Chicago) a achevé la démonstration du « lemme fondamental » énoncé 20 ans plus tôt par R. Langlands et D. Shelstad (« lemme » parce que cela semblait une petite identité combinatoire et « fondamental » car l'absence de démonstration bloquait tout progrès ultérieur), ce qui lui a valu la médaille Fields en 2010. La démonstration repose sur un échaffaudage assez impressionnant de théories et de réductions dues à M. Goreski, R. MacPherson, R. Kottwitz, G. Laumon et J.-L. Waldspurger (entre autres).

• *La correspondance de Langlands géométrique* (qui semble beaucoup intéresser l'armée américaine). Elle ne fait pas partie du programme initial de Langlands : c'est une extension [due à l'école russe autour de V. Drinfeld et A. Beilinson (maintenant à Chicago tous les deux)] dont la motivation vient de la physique mathématique en lien avec la théorie des cordes. Il s'agit d'une correspondance pour les corps de fonctions où on remplace le corps fini $\mathbf{F}_p$ par le corps $\mathbf{C}$ des nombres complexes.

APPENDICE H

PROBLÈMES CORRIGÉS

Les exercices et problèmes qui suivent portent sur le contenu des chapitres I à VII.

— Les exercices H.1.1, H.1.2, H.1.3 et les problèmes H.2, H.3 et H.4 ont pour but l'établissement de la table des caractères d'un groupe fini [il s'agit respectivement de S_3, S_4, $\left\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\right\} \subset \mathbf{GL}_2(\mathbf{F}_q)$, A_5, $\mathbf{GL}_2(\mathbf{F}_3)$ et $\mathbf{GL}_3(\mathbf{F}_2)$]. La difficulté va en croissant, mais les techniques sont assez similaires d'un problème à l'autre ; les 3 problèmes sont conçus pour passer en revue les principaux énoncés du chap. I.

— Le prob. H.5, qui explore les propriétés des coefficients de Fourier des fonctions continues, et le début du prob. H.6 utilisent le contenu du chap. II ; le reste du prob. H.6, consacré à la tranformée de Fourier dans L^2, et le prob. H.7, qui explore les liens importants entre la transformée de Fourier et la convolution, mettent en action les résultats des chap. III et IV.

— Les ex. H.1.8 (calcul de $\int_0^{+\infty} \frac{dt}{1+t^n}$), H.1.9, H.1.10 (formule $\sin \pi z = \pi z \prod_{n\geqslant 1} \left(1 - \frac{z^2}{n^2}\right)$ d'Euler), H.1.11 (formule $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$ des compléments), H.1.12, H.1.13 (th. de Rouché), H.1.14, et les prob. H.9 (coefficients de Fourier des fonctions analytiques, en écho au prob. H.5 et à l'annexe D), H.8 (fonctions elliptiques), H.12 (irrationalité de $\zeta(3)$) et H.13 utilisent des techniques diverses et variées de fonctions holomorphes. En particulier, le prob. H.8 utilise une panoplie à peu près complète des résultats des chap. V et VI.

— Les ex. H.1.4, H.1.5, H.1.6 et H.1.7 donnent plusieurs manières de calculer des transformées de Fourier de fonctions rationnelles (équations différentielles ou méthode des résidus) ou autre, et les ex. H.1.6 et H.1.7 donnent des exemples d'utilisation de la formule de Poisson. Ce sont de bons entrainements pour les prob. H.10 (prolongement analytique de séries du type $s \mapsto \sum_{n\in\mathbf{Z}} \frac{1}{P(n)^s}$, où P est un polynôme) et H.11 (formule $q^{1/24}\prod_{n\geqslant 1}(1-q^n) = \sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$ d'Euler, et plein d'autres jolies formules) qui sont destinés à faire utiliser le maximum d'énoncés des chap. IV à VI.

— Le prob. H.14 n'a pas vraiment de rapport avec le cours : c'est l'épreuve de 6 heures du concours d'entrée 2003 de l'École Normale ; il est là en rapport avec l'annexe F.

H.1. Exercices d'examen

1. Énoncés

1.1. *Représentations des groupes*

Exercice H.1.1. — Soit S_3 le groupe des permutations de $\{1,2,3\}$. On note e, s et t les trois classes de conjugaison de S_3, où e est la classe de conjugaison de l'identité, s celle des transpositions et t celle des 3-cycles.

(i) Montrer (sans les construire) que S_3 a deux représentations irréductibles de dimension 1 et une de dimension 2.

(ii) On note χ_1 le caractère de la représentation triviale $\mathbf{1}$, χ_2 celui de la signature ε qui est l'autre représentation de dimension 1, et θ celui de la représentation W de dimension 2. De quelle représentation $\psi = \chi_1 + \chi_2 + 2\theta$ est-il le caractère ? Compléter la table

	e	s	t
χ_1			
χ_2			
$\chi_1 + \chi_2 + 2\theta$			
θ			

(iii) On fait agir S_3 sur lui-même par congugaison intérieure ($g \cdot x = gxg^{-1}$), et on note V la représentation de permutation associée et χ son caractère. Calculer χ. En déduire les multiplicités de $\mathbf{1}$, ε et W dans la décomposition de V.

Exercice H.1.2. — On se propose d'établir la table des caractères du groupe S_4 des permutations de $\{1,2,3,4\}$. Comme les partitions de 4 sont 4, 3+1, 2+2, 2+1+1 et 1+1+1+1, le groupe S_4 a 5 classes de conjugaison : la classe C_1 de l'élément neutre 1 (1 élément), celle C_2 des transpositions (6 éléments), celle $\mathrm{C}_{2,2}$ des produits de deux transpositions de supports disjoints (3 éléments), celle C_3 des 3-cycles (8 éléments), celle C_4 des 4-cycles (6 éléments).

		$\mathbf{1}$	ε	θ	χ_1	χ_2
1	C_1	1	1	2	3	3
6	C_2	1	-1	0	1	-1
3	$\mathrm{C}_{2,2}$	1	1	2	-1	-1
8	C_3	1	1	-1	0	0
6	C_4	1	-1	0	-1	1

FIGURE 1. Table des caractères de S_4

(i) Soit V la représentation de permutation associée à l'action de S_4 sur $\{1,2,3,4\}$.

(a) Calculer χ_V et $\langle \chi_V, \chi_V \rangle$; en déduire que V est la somme directe $V_1 \oplus V_2$ de deux représentations irréductibles V_1, V_2 non isomorphes.

(b) Déterminer les sous-espaces V_1 et V_2 de V et montrer, en revenant à la définition, que ce sont des représentations irréductibles de S_4.

(c) Calculer les caractères de V_1 et V_2 ; quelles colonnes de la table cela permet-il de remplir ?

(ii) Quelle est la seconde représentation de dimension 1 ? Comment peut-on obtenir la seconde de dimension 3 (pourquoi est-elle irréductible et différente de celle déjà construite ?).

(iii) Comment peut-on compléter la table des caractères de S_4 ?

Exercice H.1.3. — Soit K un corps, et soit $G \subset \mathbf{GL}_2(K)$ le sous-groupe des $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, avec $a \in K^*$ et $b \in K$. On fait agir [1] G sur K par la formule $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot x = ax + b$.

(i) Calculer $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. En déduire que les classes de conjugaison de G sont $C_1 = \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$, $N = \left\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right),\ b \in K - \{0\}\right\}$ et les $D_a = \left\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right),\ b \in K\right\}$, pour $a \in K^* - \{1\}$.

(ii) On suppose à partir de maintenant que K est fini, de cardinal q, et donc que $|G| = q(q-1)$ et $|\mathrm{Conj}(G)| = q$. On note V la représentation de permutation de G associée à l'action de G sur K et W l'hyperplan de V défini par $W = \{\sum_{x \in K} \lambda_x e_x,\ \sum_{x \in K} \lambda_x = 0\}$. Montrer que W est une sous-représentation de V.

(iii) Calculer χ_W ; en déduire que W est irréductible.

(iv) Quelles sont les dimensions des autres représentations irréductibles de G ?

(v) Comment peut-on construire un caractère linéaire de G à partir d'un caractère linéaire de K^* ? En déduire que si $K = \mathbf{F}_5$ (où $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$), la table des caractères de G est la suivante.

	$\mathbf{1}$	η	η^2	η^3	χ_W
C_1	1	1	1	1	4
N	1	1	1	1	-1
D_2	1	i	-1	$-i$	0
D_4	1	-1	1	-1	0
D_3	1	$-i$	-1	i	0

FIGURE 2. Table des caractères de G, si $K = \mathbf{F}_5$

(vi) On suppose [2] $q = 4$. Établir la table des caractères de G. Cette table vous rappelle-t-elle quelque chose ? Pouvez-vous expliquer cette coïncidence ?

1.2. *Transformée de Fourier et méthode des résidus*

Exercice H.1.4. — Soit $f : \mathbf{R} \to \mathbf{C}$ définie par $f(t) = \frac{1}{(t+i)^3}$.

1. On a $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot x = x$ et $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot x\right) = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot (cx+d) = a(cx+d)+b = acx+(ad+b) = \left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right) \cdot x$, et comme $\left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)$, cela montre que l'on a bien affaire à une action de groupe.

2. On a alors $K = \mathbf{F}_2[X]/(X^2 + X + 1)$, mais il n'est pas nécessaire de savoir comment est construit K pour répondre à la question.

(i) Montrer que $\hat{f}$ est bien définie, est de classe $\mathscr{C}^1$, et que $|t^{\mathrm{N}}\hat{f}(t)| \to 0$ quand $|t| \to +\infty$, pour tout $\mathrm{N} \in \mathbf{N}$.

(ii) Soit $g : \mathbf{R} \to \mathbf{C}$ définie par $g(t) = e^{-2\pi t}$, si $t > 0$, et $g(t) = 0$, si $t \leqslant 0$. Calculer $\hat{g}$; en déduire la transformée de Fourier de $h(t) = t^2 g(t)$, puis $\hat{f}$.

(iii) Retrouver le résultat par la méthode des résidus. (On intégrera $\mathrm{F}_t(z) = \frac{e^{-2i\pi tz}}{(z+i)^3}$ sur un contour bien choisi.)

Exercice H.1.5. — (i) Montrer que l'on a $\int_{\mathbf{R}} \hat{f}(x)(\phi''(x) + a\phi(x))\,dx = \int_{\mathbf{R}} (a - 4\pi^2 t^2) f(t)\hat{\phi}(t)\,dt$, si $a \in \mathbf{C}$, $f \in \mathrm{L}^1(\mathbf{R})$ et $\phi \in \mathscr{C}_c^\infty(\mathbf{R})$. (On s'intéressera à la transformée de Fourier de $\phi'' + a\phi$.)

(ii) On suppose dorénavant que $f(t) = \frac{1}{t^2+2i}$. Montrer qu'il existe $a \in \mathbf{C}$ tel que l'on ait $\int_{\mathbf{R}} \hat{f}(x)(\phi''(x) + a\phi(x))\,dx = -4\pi^2\phi(0)$, pour tout $\phi \in \mathscr{C}_c^\infty(\mathbf{R})$.

(iii) Montrer, en utilisant la méthode des résidus, que $\hat{f}(u) = \frac{\pi}{1+i} e^{-2\pi(1+i)|u|}$.

(iv) Retrouver le (ii) à partir de cette expression.

Exercice H.1.6. — Soit $\Omega = \{z \in \mathbf{C},\ \mathrm{Re}(z) > 0\}$.

(i) Soit $\alpha = a + ib \in \Omega$, et soit γ_{R}, si $\mathrm{R} > 0$, le lacet constitué des segments $[0, \mathrm{R}]$, $[\mathrm{R}, \frac{\alpha \mathrm{R}}{a}]$ et $[\frac{\alpha \mathrm{R}}{a}, 0]$. Que vaut $\int_{\gamma_{\mathrm{R}}} z^n e^{-z}\,dz$, si $n \in \mathbf{N}$? En déduire que $\int_0^{+\infty} t^n e^{-\alpha t}\,dt = \frac{n!}{\alpha^{n+1}}$.

(ii) Si $\lambda \in \mathbf{R}_+^*$, soit $f_\lambda : \mathbf{R} \to \mathbf{C}$ la fonction définie par $f_\lambda(t) = 0$, si $t \leqslant 0$, et $f_\lambda(t) = te^{-\lambda t}$, si $t \geqslant 0$. Calculer $\hat{f}_\lambda(x)$, si $x \in \mathbf{R}$.

(iii) On remarque que $x \mapsto x\hat{f}_\lambda(x)$ n'est pas sommable. Pouvait-on le savoir sans calculer $\hat{f}_\lambda$? (On distinguera les cas $\hat{f}_\lambda$ non sommable et $\hat{f}_\lambda$ sommable.)

(iv) Établir la formule $\sum_{n\in\mathbf{Z}} \frac{1}{(\lambda+2i\pi n)^2} = \frac{e^\lambda}{(e^\lambda-1)^2}$, pour tout $\lambda \in \mathbf{R}_+^*$.

(v) Comment pourrait-on obtenir une formule analogue pour $\sum_{n\in\mathbf{Z}} \frac{(-1)^n}{(\lambda+2i\pi n)^2}$?

(vi) Montrer que $\sum_{n\in\mathbf{Z}} \frac{1}{(z+2i\pi n)^2}$ converge pour tout $z \notin 2i\pi\mathbf{Z}$ et que sa somme vaut $\frac{e^z}{(e^z-1)^2}$.

Exercice H.1.7. — Si $z \in \mathbf{C}$, on pose $\mathrm{ch}\, z = \frac{e^z+e^{-z}}{2}$ et $\mathrm{sh}\, z = \frac{e^z-e^{-z}}{2}$. On aura à utiliser la minoration $\left|\mathrm{ch}\,(x+iy)\right| \geqslant \frac{e^{|x|}-e^{-|x|}}{2}$.

(i) Montrer que $z \mapsto \mathrm{ch}\,\pi z$ est holomorphe. Quelle est sa dérivée ; quels sont ses zéros ?

(ii) Si $u \in \mathbf{R}$, on note f_u la fonction $z \mapsto e^{-2i\pi uz} \frac{1}{\mathrm{ch}\,\pi z}$. Calculer $\mathrm{I}(\mathrm{R}) = \int_{\gamma_{\mathrm{R}}} f_u(z)\,dz$, où γ_{R} est le lacet formé des segments $[-\mathrm{R}, \mathrm{R}]$, $[\mathrm{R}, \mathrm{R}+i]$, $[\mathrm{R}+i, -\mathrm{R}+i]$ et $[-\mathrm{R}+i, -\mathrm{R}]$.

(iii) En déduire que la transformée de Fourier de $t \mapsto g_y(t) = \frac{1}{\mathrm{ch}\,\pi yt}$ est $x \mapsto \frac{1}{y} \frac{1}{\mathrm{ch}(\pi x/y)}$, si $y > 0$. (On commencera par considérer le cas $y = 1$.)

(iv) Si $a \in \mathbf{R}$, on note Ω_a le demi-plan $\mathrm{Re}(z) > a$. Montrer que la série $\sum_{n\in\mathbf{Z}} \frac{1}{\mathrm{ch}\, n\pi z}$ converge pour tout $z \in \Omega_0$, et que la fonction $z \mapsto \mathrm{F}(z)$ ainsi définie vérifie l'équation fonctionnelle $\mathrm{F}(\frac{1}{z}) = z\mathrm{F}(z)$, pour tout $z \in \Omega_0$. (On commencera par traiter le cas z réel.)

Exercice H.1.8. — Soit n entier $\geqslant 2$, et soit $\theta \in [0, \pi]$ pas de la forme $\frac{(2k+1)\pi}{n}$, avec $k \in \mathbf{N}$. Si $\mathrm{R} > 1$, soient $\mathrm{I}_1(\mathrm{R})$, $\mathrm{I}_2(\mathrm{R})$ et $\mathrm{I}_3(\mathrm{R})$ les intégrales de $\frac{dz}{1+z^n}$ sur le segment $[0, \mathrm{R}]$, l'arc de cercle de centre 0 allant de R à $e^{i\theta}\mathrm{R}$, et le segment $[e^{i\theta}\mathrm{R}, 0]$. (Faire un dessin.)

(i) Calculer $\mathrm{I}_1(\mathrm{R}) + \mathrm{I}_2(\mathrm{R}) + \mathrm{I}_3(\mathrm{R})$.

(ii) Quelles sont les limites, quand $\mathrm{R} \to +\infty$, de $\mathrm{I}_1(\mathrm{R})$, $\mathrm{I}_2(\mathrm{R})$ et $\mathrm{I}_3(\mathrm{R})$.

(iii) En déduire, en choisissant judicieusement θ, la valeur de $\int_0^{+\infty} \frac{dt}{1+t^n}$.

1.3. *Fonctions holomorphes*

Exercice H.1.9. — (i) Montrer que $\mathrm{tg} = \frac{\sin}{\cos}$ est somme de sa série de Taylor en 0 sur $]\frac{-\pi}{2}, \frac{\pi}{2}[$.

(ii) Quel est le rayon de convergence de la série de Taylor en 0 de $\frac{\sin \pi z}{z-1}$?

Exercice H.1.10. — Si $z \in \mathbf{C}$, on pose $\sin z = \frac{e^{iz}-e^{-iz}}{2i}$. On a $|\sin z| \geqslant 1$, si $z = (k+\frac{1}{2})\pi + iy$, avec $k \in \mathbf{Z}$, ou si $z = x+iy$, avec $|y| \geqslant \frac{\pi}{2}$ (dans ce cas, on a même $|\sin z| \geqslant \frac{1}{2}(e^{\pi/2} - e^{-\pi/2})$).

(i) Montrer que le produit $\prod_{n\geqslant 1}\left(1-\frac{z^2}{n^2}\right)$ converge pour tout $z \in \mathbf{C}$, et que la fonction $z \mapsto \mathrm{F}(z)$ ainsi définie est holomorphe sur $\mathbf{C}$.

(ii) Montrer que $\mathrm{G}(z) = \frac{\pi z}{\sin \pi z}\mathrm{F}(z)$ est paire, holomorphe sur $\mathbf{C}$, et ne s'annule pas.

(iii) En déduire qu'il existe une suite $(a_n)_{n\geqslant 1}$ d'éléments de $\mathbf{C}$, telle que :

- la série $\sum_{n\geqslant 1} a_n z^n$ converge pour tout $z \in \mathbf{C}$,
- la fonction $z \mapsto g(z)$ ainsi définie vérifie $e^{g(z)} = \mathrm{G}(z)$, pour tout $z \in \mathbf{C}$.

(iv) Si N est un entier $\geqslant 1$, on note $\mathrm{C_N}$ le maximum de $|\mathrm{G}(z)|$ sur le carré de sommets $\pm(\mathrm{N}+\frac{1}{2}) \pm i(\mathrm{N}+\frac{1}{2})$ (i.e. $\{x+iy,\ -(\mathrm{N}+\frac{1}{2}) \leqslant x, y \leqslant \mathrm{N}+\frac{1}{2}\}$, et on pose $\mathrm{R_N} = \sqrt{2}(\mathrm{N}+\frac{1}{2})$. Montrer que $\mathrm{C_N} \leqslant \pi \mathrm{R_N}(\mathrm{R_N^2}+1)^{\mathrm{N}} e^{\sum_{n\geqslant \mathrm{N}+1} \mathrm{R_N^2}/n^2}$. En déduire que $\mathrm{N}^{-k}\log \mathrm{C_N} \to 0$, si $k \geqslant 2$.

(v) En déduire que $a_n = 0$, si $n \geqslant 2$. (On écrira a_n sous la forme $|a_n|e^{i\alpha_n}$, avec $\alpha_n \in [0, 2\pi[$, on calculera $\mathrm{I}_n(r) = \int_0^{2\pi}(1+\cos(n\theta+\alpha_n))\mathrm{Re}(g(re^{i\theta}))\,d\theta$, et on cherchera à majorer $\mathrm{I}_n(r)$.)

(vi) Montrer que $\mathrm{F}(z) = \frac{\sin \pi z}{\pi z}$, pour tout $z \in \mathbf{C}$.

Exercice H.1.11. — On rappelle que la fonction Γ est méromorphe dans $\mathbf{C}$, holomorphe en dehors de pôles simples en les $-n$, pour $n \in \mathbf{N}$, est bornée dans toute bande $0 < a \leqslant \mathrm{Re}(s) \leqslant b$, vérifie l'équation fonctionnelle $\Gamma(s+1) = s\Gamma(s)$, pour tout $s \notin -\mathbf{N}$, et que $\Gamma(1) = 1$.

(i) Montrer que $s \mapsto \mathrm{F}(s) = \sin \pi s\ \Gamma(s)\Gamma(1-s)$ est holomorphe sur $\mathbf{C}$, périodique de période 1.

(ii) En déduire qu'il existe f, holomorphe sur $\mathbf{C^*}$, telle que $\mathrm{F}(s) = f(e^{2i\pi s})$, pour tout $s \in \mathbf{C}$.

(iii) Montrer qu'il existe des $a_n \in \mathbf{C}$, pour $n \in \mathbf{Z}$ tels que $f(z) = \sum_{n\in\mathbf{Z}} a_n z^n$, pour tout $z \in \mathbf{C^*}$, et que, pour tout $\mathrm{T} \in \mathbf{R}$, l'on a $a_n = \int_{[i\mathrm{T}, 1+i\mathrm{T}]} e^{-2i\pi s}\mathrm{F}(s)ds$.

(iv) Montrer que $s \mapsto e^{-\pi|\mathrm{Im}(s)|}\mathrm{F}(s)$ est bornée sur $\mathbf{C}$. (On se ramènera à un ensemble de la forme $1 \leqslant \mathrm{Re}(s) \leqslant 2$ et $|\mathrm{Im}(s)| \geqslant 1$.)

(v) En déduire la formule des compléments $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$, pour tout $s \notin \mathbf{Z}$.

Exercice H.1.12. — Si g est méromorphe sur $\mathbf{C}$, et si $\mathrm{N} \in \mathbf{N}$, on dit que $g = \mathrm{O}(y^{\mathrm{N}})$ s'il existe $\mathrm{C}, \mathrm{M} \in \mathbf{R}$ tels que $|g(x+iy)| \leqslant \mathrm{C}|y|^{\mathrm{N}}$, si $|y| \geqslant \mathrm{M}$.

(i) Montrer que si g est $\mathrm{O}(y^{\mathrm{N}})$, alors g' est $\mathrm{O}(y^{\mathrm{N}-1})$.

(ii) Soit f une fonction méromorphe sur $\mathbf{C}$, impaire, périodique de période 1, holomorphe en dehors de pôles simples de résidu 1 en les entiers, et $\mathrm{O}(y^{\mathrm{N}})$. Montrer que $f^2 + f'$ est constante.

Exercice H.1.13. — Soient $\mathrm{D} = \mathrm{D}(0,1)$ et $\mathrm{C} = \partial\mathrm{D}$ le cercle de centre 0 et de rayon 1. Soient Ω un ouvert contenant D, f holomorphe sur Ω, ne s'annulant pas sur C, et g holomorphe sur Ω, telle que $|f(z) - g(z)| < |f(z)|$, si $z \in \mathrm{C}$.

(i) Montrer qu'il existe $\Omega' \subset \Omega$ ouvert contenant C et h holomorphe sur Ω' tels que $\frac{g}{f} = e^h$ sur Ω'. Que vaut h' ?

(ii) Montrer que f et g ont le même nombre de zéros (comptés avec multiplicité) dans D.

(iii) Soit G holomorphe sur Ω telle que $|\mathrm{G}(z)| < 1$, si $z \in \mathrm{C}$. Montrer que $\mathrm{G}(\mathrm{D}) \subset \mathrm{D}$ et que G a un unique point fixe dans D.

Exercice H.1.14. — (i) Soit $x \in \mathbf{R}_+^*$. Montrer que la série $\sum_{n\in\mathbf{N}} \frac{1}{(n+x)^s}$ converge si $\mathrm{Re}(s) > 1$, et que la somme $\mathrm{F}(x,s)$ de cette série est holomorphe en s sur le demi-plan $\mathrm{Re}(s) > 1$.

(ii) Établir la formule $\mathrm{F}(x,s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{e^{-tx}}{1-e^{-t}} t^{s-1}\, dt$, si $\mathrm{Re}(s) > 1$.

(iii) Montrer que $\mathrm{F}(x,s)$ admet un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors d'un pôle simple de résidu 1 en $s = 1$.

2. Corrigés

Exercice H.1.1. (i) Comme S_3 a trois classes de conjugaison, il a aussi 3 représentations irréductibles W_1, W_2 et W_3, et comme $(\dim \mathrm{W}_1)^2 + (\dim \mathrm{W}_2)^2 + (\dim \mathrm{W}_3)^2 = 6$ d'après la formule de Burnside, la seule possibilité est que deux des dimensions valent 1 et la troisième 2.

(ii) $\psi = \chi_1 + \chi_2 + 2\theta$ est le caractère de la représentation régulière d'après le (i) du cor. I.2.23 ; on a donc $\psi(e) = 6$, $\psi(s) = 0$ et $\psi(t) = 0$, d'après la formule générale pour le caractère de la représentation régulière (alinéa 2.3 du § I.1). Ceci nous fournit la table

	e	s	t
χ_1	1	1	1
χ_2	1	-1	1
$\chi_1 + \chi_2 + 2\theta$	6	0	0
θ	2	0	-1

(iii) Comme V est une représentation de permutation, $\chi(g)$ est le nombre de points fixes de g (alinéa 2.3 du § I.1), c'est-à-dire le nombre d'éléments h de S_3 tels que $ghg^{-1} = h$, ou encore le nombre d'éléments de S_3 commutant avec g. On a donc $\chi(g) = |\mathrm{Z}_g| = |\mathrm{S}_3| \cdot |\mathrm{C}_g|^{-1}$. On en déduit que $\chi(e) = 6$, $\chi(s) = 2$ et $\chi(t) = 3$.

Si W' est une représentation irréductible, alors la multiplicité de W' dans V est $\langle \chi_{\mathrm{W}'}, \chi \rangle$ d'après le cor. I.2.18. Comme

$\langle \chi_1, \chi \rangle = \frac{1}{6}(6 + 3 \cdot (1 \cdot 2) + 2 \cdot (1 \cdot 3)) = 3$,
$\langle \chi_2, \chi \rangle = \frac{1}{6}(6 + 3 \cdot (-1 \cdot 2) + 2 \cdot (1 \cdot 3)) = 1$
$\langle \theta, \chi \rangle = \frac{1}{6}(2 \cdot 6 + 3 \cdot (0 \cdot 2) + 2 \cdot (-1 \cdot 3)) = 1$,
on a $\mathrm{V} = 3 \cdot \mathbf{1} \oplus \varepsilon \oplus \mathrm{W}$.

Exercice H.1.2. (i) (a) Comme V est une représentation de permutation, $\chi_{\mathrm{V}}(\sigma)$ est le nombre de points fixes de σ agissant sur $\{1,2,3,4\}$ (alinéa 2.3 du § I.1). On a donc $\chi_{\mathrm{V}}(\mathrm{C}_1) = 4$, $\chi_{\mathrm{V}}(\mathrm{C}_2) = 2$, $\chi_{\mathrm{V}}(\mathrm{C}_{2,2}) = 0$, $\chi_{\mathrm{V}}(\mathrm{C}_3) = 1$ et $\chi_{\mathrm{V}}(\mathrm{C}_4) = 0$.

Le produit scalaire $\langle \chi_{\mathrm{V}}, \chi_{\mathrm{V}} \rangle$ est égal à $\frac{1}{24}(4^2 + 6 \cdot 2^2 + 3 \cdot 0^2 + 8 \cdot 1^2 + 6 \cdot 0^2) = 2$. Si $\mathrm{V} = \oplus_{\mathrm{W}\in\mathrm{Irr}(\mathrm{S}_4)} m_{\mathrm{W}} \mathrm{W}$, ce produit scalaire est aussi égal à $\sum_{\mathrm{W}\in\mathrm{Irr}(\mathrm{S}_4)} m_{\mathrm{W}}^2$ puisque les χ_{W} forment une famille orthonormale (th. I.2.14), et comme la seule écriture de 2 comme somme de deux carrés est $1^2 + 1^2$, on en déduit que $m_{\mathrm{W}} = 1$ pour exactement deux $\mathrm{W} \in \mathrm{Irr}(\mathrm{S}_4)$, et $m_{\mathrm{W}} = 0$ pour les autres, ce qui permet de conclure.

(b) La droite V_1 engendrée par $e_1 + \cdots + e_4$ et l'hyperplan V_2 d'équation $x_1 + \cdots + x_4$ sont stables par S_4. Comme V_1 est de dimension 1, elle est automatiquement irréductible.

Soit $x = (x_1, x_2, x_3, x_4) \in \mathrm{V}_2$ non nul. Il s'agit de prouver que le sous-espace vectoriel U_x de V_2 engendré par les $\sigma \cdot x$, pour $\sigma \in \mathrm{S}_4$, est égal à V_2. Il existe $i \neq j$ tels que $x_i \neq x_j$. Soit τ la transposition (ij). Alors $x - \tau \cdot x$ est un multiple non nul de $e_i - e_j$. On en déduit l'appartenance de $e_i - e_j$ à U_x, et donc aussi

celle de $\sigma \cdot (e_i - e_j) = e_{\sigma(i)} - e_{\sigma(j)}$, pour tout $\sigma \in \mathrm{S}_4$. Comme $(\sigma(i), \sigma(j))$ décrit les couples d'éléments distincts de $\{1,2,3,4\}$ quand σ décrit S_4, cela montre que U_x contient $e_1 - e_2$, $e_1 - e_3$ et $e_1 - e_4$, et comme ces vecteurs engendrent V_2, cela permet de conclure.

(c) La représentation V_1 est la représentation triviale, et donc $\chi_{\mathrm{V}_1}(\mathrm{C}) = 1$ pour tout $\mathrm{C} \in \mathrm{Conj}(\mathrm{S}_4)$. Comme $\chi_{\mathrm{V}_1} + \chi_{\mathrm{V}_2} = \chi_{\mathrm{V}}$, cela permet de déterminer le caractère de χ_{V_2} et de remplir les première et quatrième colonnes de la table.

(ii) (a) La seconde représentation de dimension 1 est la signature ε ; ses valeurs sont bien celles reportées dans la seconde colonne. La seconde représentation de dimension 3 est $\mathrm{V}_1 \otimes \varepsilon$. Si elle pouvait se décomposer sous la forme $\mathrm{V}_1 \otimes \varepsilon = \mathrm{W}_1 \oplus \mathrm{W}_2$, alors $\mathrm{V}_1 = (\mathrm{V}_1 \otimes \varepsilon) \otimes \varepsilon$ pourrait se décomposer sous la forme $(\mathrm{W}_1 \otimes \varepsilon) \oplus (\mathrm{W}_2 \otimes \varepsilon)$, ce qui est absurde. On a $\chi_{\mathrm{V}_1 \otimes \varepsilon}(g) = \chi_{\mathrm{V}_1}(g)\varepsilon(g)$ (alinéa 2.1 du § I.1), et donc $\chi_{\mathrm{V}_1 \otimes \varepsilon}(\mathrm{C}_2) = -1$ est différent de $\chi_{\mathrm{V}_1}(\mathrm{C}_2) = 1$, ce qui prouve que les représentations $\mathrm{V}_1 \otimes \varepsilon$ et V_1 ne sont pas isomorphes puisque leurs caractères sont distincts.

(b) Comme S_4 a 5 classes de conjugaison, il a 5 représentations irréductibles (cor. I.2.16). Si on note d la dimension de la représentation manquante et θ son caractère, la formule de Burnside montre que $24 = 1^2 + 1^2 + 3^2 + 3^2 + d^2$, et donc que $d = 2$. Pour remplir la dernière colonne, on utilise le fait que $1 + \varepsilon + 2\theta + 3\chi_1 + 3\chi_2$ est le caractère de la représentation régulière ((i) du cor. I.2.23) qui est connu (alinéa 2.3 du § I.1).

Exercice H.1.3. (i) On a $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} c & ad+(1-c)b \\ 0 & 1 \end{smallmatrix}\right)$. On en déduit qu'un conjugué de $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)$ est de la forme $\left(\begin{smallmatrix} c & d' \\ 0 & 1 \end{smallmatrix}\right)$, et que tout élément de cette forme est un conjugué de $\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right)$, si $c \neq 1$. Les D_a, pour $a \in \mathrm{K}^* - \{1\}$ forment donc des classes de conjugaison. Par ailleurs C_1 est la classe de conjugaison de l'élément neutre, et N est la classe de conjugaison de $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, car $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, si $a \neq 0$.

(iii) On a $g \cdot \left(\sum_{x \in \mathrm{K}} \lambda_x e_x\right) = \sum_{x \in \mathrm{K}} \lambda_x e_{g \cdot x} = \sum_{x \in \mathrm{K}} \lambda_{g^{-1} \cdot x} e_x$. Or $x \mapsto g^{-1} \cdot x$ est une bijection de K, et donc $\sum_{x \in \mathrm{K}} \lambda_{g^{-1} \cdot x} = \sum_{x \in \mathrm{K}} \lambda_x$, ce qui prouve que $g \cdot v = \sum_{x \in \mathrm{K}} \lambda_{g^{-1} \cdot x} e_x \in \mathrm{W}$, si $v = \sum_{x \in \mathrm{K}} \lambda_x e_x \in \mathrm{W}$.

(iv) V est une représentation de permutation, et donc $\chi_{\mathrm{V}}(g)$ est le nombre de points fixes de g agissant sur K. On est donc amené à calculer le nombre de solutions de l'équation $ax + b = x$ dans K, ce qui nous donne $\chi_{\mathrm{V}}(\mathrm{C}_1) = q$, $\chi_{\mathrm{V}}(\mathrm{N}) = 0$ et $\chi_{\mathrm{V}}(\mathrm{D}_a) = 1$, si $a \in \mathrm{K}^* - \{1\}$.

Maintenant V est la somme directe de W et de la droite engendrée par $\sum_{x \in \mathrm{K}} e_x$, sur laquelle G agit trivialement. On en déduit que $\chi_{\mathrm{V}}(g) = \chi_{\mathrm{W}}(g) + 1$, ce qui nous donne $\chi_{\mathrm{W}}(\mathrm{C}_1) = q - 1$, $\chi_{\mathrm{W}}(\mathrm{N}) = -1$ et $\chi_{\mathrm{W}}(\mathrm{D}_a) = 0$, si $a \in \mathrm{K}^* - \{1\}$.

Alors $\langle \chi_{\mathrm{W}}, \chi_{\mathrm{W}} \rangle = \frac{1}{q(q-1)}((q-1)^2 + |\mathrm{N}| \cdot 1^2 + \sum_{a \in \mathrm{K}^* - \{1\}} |\mathrm{D}_a| \cdot 0^2) = \frac{1}{q(q-1)}((q-1)^2 + (q-1)) = 1$, ce qui permet d'en déduire l'irréductibilité de W, en utilisant le cor. I.2.21.

(v) Comme $|\mathrm{Irr}(\mathrm{G})| = |\mathrm{Conj}(\mathrm{G})|$, d'après le cor. I.2.16, et comme $|\mathrm{Conj}(\mathrm{G})| = q$, il y a $q - 1$ autres représentations irréductibles. Notons $d_1, \ldots, d_{q-1}$ leurs dimensions. La formule de Burnside nous donne alors $q(q-1) = |\mathrm{G}| = (\dim \mathrm{W})^2 + \sum_{i=1}^{q-1} d_i^2$, et comme $\dim \mathrm{W} = q - 1$, on obtient $\sum_{i=1}^{q-1} d_i^2 = q(q-1) - (q-1)^2 = q - 1$. Une somme de $q - 1$ entiers $\geqslant 1$ ne pouvant être égale à $q - 1$ que si tous les entiers sont égaux à 1, on voit que les $q - 1$ autres représentations de G sont de dimension 1 (i.e. sont des caractères linéaires).

(vi) Si χ est un caractère linéaire de K^*, alors $\chi \circ \det$ est un caractère linéaire de G. Le groupe $\mathbf{F}_5^*$ est cyclique d'ordre 4, engendré par 2 (on a $2^2 = 4$, $2^3 = 8 = 3$ et $2^4 = 16 = 1$). Un caractère de $\mathbf{F}_5^*$ est donc déterminé par sa valeur en 2, qui doit être une racine 4-ième de l'unité (i.e. 1, i, -1 ou $-i$). Il y a donc 4 tels caractères et si on note η celui pour lequel $\eta(2) = i$, les autres sont η^2, η^3 et η^4 qui n'est autre que le caractère trivial. Les 4 caractères de G que l'on cherche sont donc exactement les $\eta^i \circ \det$, pour $0 \leqslant i \leqslant 3$, ce qui nous fournit bien la table annoncée.

(vii) Le groupe K^* est de cardinal 3, et donc est cyclique, engendré par n'importe quel $a \neq 1$. (K^* est toujours cyclique, si K est un corps fini ; dans le cas présent, si $a \in \mathrm{K}^* - \{1\}$, le sous-groupe engendré

par a a un cardinal qui divise $|\mathrm{K}^*| = 3$, et donc est égal à 3, ce qui fait que ce sous-groupe est K^*). Un caractère linéaire de K^* est donc déterminé par sa valeur en a, qui est une racine cubique de l'unité. Il y a 3 tels caractères, et si on note η celui pour lequel $\eta(a) = j = e^{2i\pi/3}$, les autres sont η^2 et $\eta^3 = \mathbf{1}$. Ceci nous fournit la table suivante.

	$\mathbf{1}$	η	η^2	χ_{W}
C_1	1	1	1	3
N	1	1	1	-1
D_a	1	j	j^2	0
D_{a^2}	1	j^2	j	0

FIGURE 3. Table des caractères de G, si $\mathrm{K} = \mathbf{F}_4$

On reconnaît la table des caractères de A_4, ce qui n'est pas très étonnant car G est isomorphe à A_4. En effet, le choix d'une bijection entre K et $\{1,2,3,4\}$ transforme l'action de G sur K en une action de G sur $\{1,2,3,4\}$, et donc fournit une injection de G dans S_4. L'image H de cette injection est donc un sous-groupe de S_4, isomorphe à G. Un tel groupe est distingué dans S_4 : si $g \notin \mathrm{H}$, on a $g\mathrm{H} = \mathrm{H}g = \mathrm{S}_4 - \mathrm{H}$ pour des raisons de cardinal (on remarquera que $|\mathrm{H}| = |\mathrm{G}| = 12 = |\mathrm{A}_4|$ et $|\mathrm{S}_4| = 24 = 2|\mathrm{H}|$), et donc $g\mathrm{H}g^{-1} = \mathrm{H}gg^{-1} = \mathrm{H}$. Le quotient G/H est de cardinal 2, et donc isomorphe à $\{\pm 1\}$, ce qui nous fournit un caractère linéaire $\eta : \mathrm{S}_4 \to \{\pm 1\}$. La restriction de η à A_4 est encore un caractère linéaire, mais les caractères de A_4 sont à valeurs dans μ_3, ce qui implique $\eta = 1$ sur A_4 ; autrement dit, A_4 est inclus dans le noyau H de η, et donc lui est égal pour des raisons de cardinal. On a donc bien $\mathrm{G} \cong \mathrm{A}_4$. (On aurait aussi pu remarquer que l'image d'un élément de D_a ou D_{a^2} est un 3-cycle, et donc appartient à A_4, et que G est engendré par $\mathrm{D}_a \cup \mathrm{D}_{a^2}$, car $\mathrm{D}_a \cup \mathrm{D}_{a^2}$ est de cardinal $8 > \frac{|\mathrm{G}|}{2}$ et ne peut donc pas être inclus dans un sous-groupe strict de G ; on peut aussi démontrer directement, en utilisant le fait que K est de caractéristique 2, que l'image d'un élément de N est un produit de deux transpositions et donc appartient à A_4.)

Exercice H.1.4. (i) La fonction f est sommable ainsi que $t \mapsto tf(t)$. Il en résulte ((ii) du th. IV.2.8) que $\hat{f}$ est bien définie et est de classe $\mathscr{C}^1$. De plus, f est de classe $\mathscr{C}^\infty$, et $f^{(\mathrm{N})}(t) = \frac{(-3)(-4)\cdots(-\mathrm{N}-2)}{(t+i)^{3+\mathrm{N}}}$ est sommable ; il en résulte ((i) du th. IV.2.8) que $|t^{\mathrm{N}}\hat{f}(t)| \to 0$ quand $|t| \to +\infty$, pour tout $\mathrm{N} \in \mathbf{N}$.

(ii) $\hat{g}(x) = \int_0^{+\infty} e^{-2\pi t(1+ix)}\,dt = [\frac{e^{-2\pi t(1+ix)}}{-2\pi(1+ix)}]_0^{+\infty} = \frac{1}{2\pi(1+ix)}$. Comme $t^2 g(t)$ est sommable, sa transformée de Fourier est $\frac{1}{(-2i\pi)^2}\hat{g}^{(2)}(x) = \frac{2}{(2i\pi)^3}\,\frac{1}{(x-i)^3}$ ((ii) du th. IV.2.8) ; en particulier elle est sommable, et on peut appliquer la formule d'inversion de Fourier dans L^1, ce qui nous donne $\overline{\mathscr{F}}\big(\frac{2}{(2i\pi)^3}\,\frac{1}{(x-i)^3}\big) = t^2 g(t)$. Comme $\overline{\mathscr{F}}\big(\frac{1}{(x-i)^3}\big)(t) = \int_{\mathbf{R}} e^{2i\pi\,tx}\frac{1}{(x-i)^3}\,dx = (-1)^3\hat{f}(t)$, grâce au changement de variable $x = -y$, on obtient finalement $\hat{f}(t) = \frac{(-2i\pi)^3}{2}t^2 g(t)$.

(iii) La fonction $\mathrm{F}_t(z)$ est méromorphe sur $\mathbf{C}$, holomorphe en dehors d'un pôle d'ordre 3 en $z = -i$, et comme

$$e^{-2i\pi\,tz} = e^{-2\pi t}e^{-2i\pi\,t(z+i)} = e^{-2\pi t}(1 - 2i\pi\,t(z+i) + \frac{1}{2}(2i\pi\,t(z+i))^2 + \cdots),$$

on a $\mathrm{F}_t(z) = e^{-2\pi t}(\frac{1}{(z+i)^3} - \frac{2i\pi\,t}{(z+i)^2} + \frac{(2i\pi\,t)^2}{2(z+i)} + \cdots)$, et donc $\mathrm{Res}(\mathrm{F}_t, -i) = \frac{(2i\pi)^2}{2}t^2 e^{-2\pi t}$.

Supposons $t \geqslant 0$. Si $\mathrm{R} > 1$, soit γ_{R} le lacet formé du segment $[-\mathrm{R}, \mathrm{R}]$ et du demi-cercle $\mathrm{C}_{\mathrm{R}}^-$ paramêtré par $t \mapsto \mathrm{R}e^{-i\pi t}$, pour $t \in [0,1]$. Soient

$$\mathrm{I}_1(\mathrm{R}) = \int_{[-\mathrm{R},\mathrm{R}]} \mathrm{F}_t(z)\,dz \quad \text{et} \quad \mathrm{I}_2(\mathrm{R}) = \int_{\mathrm{C}_{\mathrm{R}}^-} \mathrm{F}_t(z)\,dz.$$

On a $\mathrm{I}(\gamma_{\mathrm{R}}, -i) = -1$, et donc

$$\mathrm{I}_1(\mathrm{R}) + \mathrm{I}_2(\mathrm{R}) = \int_{\gamma_{\mathrm{R}}} \mathrm{F}_t(z)dz = 2i\pi \mathrm{I}(\gamma_{\mathrm{R}}, -i)\mathrm{Res}(\mathrm{F}_t, -i) = \frac{(-2i\pi)^3}{2} t^2 e^{-2\pi t}, \quad \text{quel que soit } \mathrm{R} > 1.$$

Or $\mathrm{I}_1(\mathrm{R}) \to \hat{f}(t)$ quand $\mathrm{R} \to +\infty$. Par ailleurs, $|e^{-2i\pi\, tz}| \leqslant 1$, si $\mathrm{Im}(z) \leqslant 0$, et $|z+i| \geqslant |z| - 1 = \mathrm{R} - 1$, si $z \in \mathrm{C}_{\mathrm{R}}^-$; d'où la majoration $|\mathrm{F}_t(z)| \leqslant \frac{1}{(\mathrm{R}-1)^3}$, si $z \in \mathrm{C}_{\mathrm{R}}^-$. Donc $|\mathrm{I}_2(\mathrm{R})| \leqslant \frac{1}{(\mathrm{R}-1)^3}\mathrm{lg}(\mathrm{C}_{\mathrm{R}}^-) = \frac{\pi \mathrm{R}}{(\mathrm{R}-1)^3} \to 0$ quand $\mathrm{R} \to +\infty$. En passant à la limite, cela nous donne $\hat{f}(t) = \frac{(-2i\pi)^3}{2} t^2 e^{-2\pi t}$.

Si $t \leqslant 0$, on remplace le demi-cercle $\mathrm{C}_{\mathrm{R}}^-$ par le demi-cercle $\mathrm{C}_{\mathrm{R}}^+$ dans le demi-plan supérieur. On a alors $\mathrm{I}(\gamma_{\mathrm{R}}, -i) = 0$, et la même méthode que ci-dessus montre que $\hat{f}(t) = 0$.

Exercice H.1.5. (i) Si ϕ est $\mathscr{C}^\infty$ à support compact, il en est de même de ses dérivées, et il résulte du (i) du th. IV.2.5 que la transformée de Fourier de $\phi^{(n)}$ est $t \mapsto (2i\pi t)^n \hat{\phi}(t)$; la transformée de Fourier de $\phi'' + a\phi$ est donc $t \mapsto (a - 4\pi^2 t^2)\hat{\phi}(t)$, et la formule que l'on cherche est un cas particulier de la formule $\int_{\mathbf{R}} \hat{f}(x)g(x)\,dx = \int_{\mathrm{R}} f(t)\hat{g}(t)\,dt$ de la prop. IV.3.24, valable pour toutes $f, g \in \mathrm{L}^1(\mathbf{R})$.

(ii) Dans le cas $f(t) = \frac{1}{t^2+2i}$ et $a = -8i\pi^2$, on obtient $\int_{\mathbf{R}} \hat{f}(x)(\phi''(x) + a\phi(x)) = -4\pi^2 \int_{\mathbf{R}} \hat{\phi}(t)\,dt$, d'après le (i). Or $\int_{\mathbf{R}} \hat{\phi}(t)\,dt$ est la valeur en 0 de la transformée de Fourier inverse de $\hat{\phi}$, c'est-à-dire $\phi(0)$, d'après la formule d'inversion dans $\mathscr{S}(\mathbf{R})$ (th. IV.3.14).

(iii) Pour calculer la tranformée de Fourier $u \mapsto \hat{f}(u)$ de f, on introduit la fonction g_u définie par $g_u(z) = e^{-2i\pi uz}\frac{1}{z^2+2i}$, qui est méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples en $1-i$ et $i-1$, et on a $\mathrm{Res}(g_u, 1-i) = e^{-2i\pi u(1-i)}\frac{1}{2(1-i)} = \frac{1}{2-2i}e^{-2\pi u(1+i)}$ et $\mathrm{Res}(g_u, i-1) = \frac{1}{2i-2}e^{2\pi u(1+i)}$.

Si $u \geqslant 0$, on intègre $g_u(z)dz$ sur le lacet constitué du segment $[-\mathrm{R}, \mathrm{R}]$ et du demi-cercle inférieur de centre 0 et de rayon R. Si $\mathrm{R} > \sqrt{2}$, on a $\mathrm{I}(\gamma_{\mathrm{R}}, 1-i) = -1$ et $\mathrm{I}(\gamma_{\mathrm{R}}, i-1) = 0$, et la formule des résidus nous donne

$$\int_{\gamma_{\mathrm{R}}} g_u(z)dz = -2i\pi\,\mathrm{Res}(g_u, 1-i) = \frac{\pi}{1+i}e^{-2\pi u(1+i)}.$$

Maintenant, quand $\mathrm{R} \to +\infty$, l'intégrale sur $[-\mathrm{R}, \mathrm{R}]$ tend vers $\hat{f}(u)$, tandis que sur le demi-cercle, on a les majorations $|e^{-2i\pi uz}| \leqslant 1$ et $|\frac{1}{z^2+2i}| \leqslant \frac{1}{\mathrm{R}^2-2}$. Comme la longueur du demi-cercle est $\pi\mathrm{R}$, l'intégrale sur le demi-cercle est majorée, en module, par $\frac{\pi\mathrm{R}}{\mathrm{R}^2-2}$, et donc tend vers 0 quand $\mathrm{R} \to +\infty$. Un passage à la limite nous donne donc $\hat{f}(u) = \frac{\pi}{1+i}e^{-2\pi u(1+i)}$.

Si $u < 0$, on intègre sur le chemin γ_{R}^+ constitué du segment $[-\mathrm{R}, \mathrm{R}]$ et du demi-cercle supérieur de centre 0 et de rayon R. Si $\mathrm{R} > \sqrt{2}$, on a $\mathrm{I}(\gamma_{\mathrm{R}}, 1-i) = 0$ et $\mathrm{I}(\gamma_{\mathrm{R}}, i-1) = 1$, et les mêmes arguments que ci-dessus nous donnent $\hat{f}(u) = \frac{\pi}{1+i}e^{2\pi u(1+i)}$. (On aurait aussi pu utiliser la parité de f pour en déduire celle de $\hat{f}$.)

(iv) Des intégrations par partie nous donnent [3]

$$\begin{aligned}\int_0^{+\infty} e^{-2\pi(1+i)u}\phi''(u)\,du &= [\phi'(u)e^{-2\pi(1+i)u}]_0^{+\infty} + 2\pi(1+i)\int_0^{+\infty} e^{-2\pi(1+i)u}\phi'(u)\,du \\ &= -\phi'(0) - 2\pi(1+i)\phi(0) + (2\pi(1+i))^2 \int_0^{+\infty} e^{-2\pi(1+i)u}\phi(u)du.\end{aligned}$$

3. Ce calcul peut se réinterpréter en disant que $\hat{f}$ est, au sens des distributions, solution de l'équation différentielle $u'' - 8i\pi^2 u = -4\pi^2\delta_0$, où δ_0 est la masse de Dirac en 0.

De même, $\int_{-\infty}^0 e^{2\pi(1+i)u}\phi''(u)\,du = \phi'(0) - 2\pi(1+i)\phi(0) + (2\pi(1+i))^2\int_{-\infty}^0 e^{2\pi(1+i)u}\phi(u)du$, et donc $\int_{\mathbf{R}}\hat{f}(u)(\phi''(u) - 8i\pi^2\phi(u))\,du = \frac{\pi}{1+i}(-4\pi(1+i)\phi(0)) = -4\pi^2\phi(0)$, ce que l'on voulait.

Exercice H.1.6. (i) La fonction e^{-z} est holomorphe sur $\mathbf{C}$ qui est contractile. Son intégrale sur tout lacet est donc nulle ((i) de la rem. VI.1.4 ou formule des résidus). On en déduit que

$$\int_0^{\mathrm{R}} t^n e^{-t}dt + \int_0^{\frac{b\mathrm{R}}{a}} (\mathrm{R}+it)^n e^{-\mathrm{R}-it}\,i\,dt + \int_{\mathrm{R}}^0 (\alpha t)^n e^{-\alpha t}\alpha\,dt = 0.$$

Quand $\mathrm{R}\to+\infty$, on a $\int_0^{\mathrm{R}} t^n e^{-t}dt \to \int_0^{+\infty} t^n e^{-t}dt = n!$ et

$$|\int_0^{\frac{b\mathrm{R}}{a}} (\mathrm{R}+it)^n e^{-\mathrm{R}-it}\,i\,dt| \leqslant e^{-\mathrm{R}}\int_0^{\frac{b\mathrm{R}}{a}} |(\mathrm{R}+it)|^n\,dt \leqslant e^{-\mathrm{R}}\frac{b\mathrm{R}}{a}(\mathrm{R}^2+(\frac{b\mathrm{R}}{a})^2)^{n/2} \to 0.$$

Comme $\int_{\mathrm{R}}^0(\alpha t)^n e^{-\alpha t}\alpha\,dt \to -\alpha^{n+1}\int_0^{+\infty} t^n e^{-\alpha t}\,dt$, on obtient $\alpha^{n+1}\int_0^{+\infty} t^n e^{-\alpha t}\,dt = n!$ en passant à la limite, ce qui permet de conclure.

(ii) $\hat{f}_\lambda(x) = \int_{\mathbf{R}} e^{-2i\pi xt}f_\lambda(t)\,dt = \int_0^{+\infty} te^{-(\lambda+2i\pi x)t}dt = \frac{1}{(\lambda+2i\pi x)^2}$ d'après le (i), car $\lambda+2i\pi x\in\Omega$.

(iii) Si $\hat{f}_\lambda$ n'est pas sommable, sa restriction à $\mathbf{R}-[-1,1]$ n'est pas sommable puisque $\hat{f}_\lambda$ est continue d'après le théorème de Riemann-Lebesgue, et donc sommable sur $[-1,1]$. Comme $|x\hat{f}_\lambda(x)| \geqslant |\hat{f}_\lambda(x)|$ sur $\mathbf{R}-[-1,1]$, cela implique que $x\hat{f}_\lambda(x)$ n'est pas sommable sur cet ouvert ni, a fortiori, sur $\mathbf{R}$.

Si $\hat{f}_\lambda$ est sommable et si $x\hat{f}_\lambda(x)$ est sommable, alors d'après le (ii) du th. IV.2.8, $\mathscr{F}\hat{f}_\lambda$ est de classe $\mathscr{C}^1$ et $\mathscr{F}(x\hat{f}_\lambda(x))(t) = \frac{-1}{2i\pi}(\mathscr{F}\hat{f}_\lambda)'(t)$. Maintenant, la formule d'inversion de Fourier dans L^1, appliquée à f_λ, montre que $(\mathscr{F}\hat{f}_\lambda)(t) = f_\lambda(-t)$. On aboutit à une contradiction puisque f_λ n'est pas dérivable en 0 ; c'est donc que $x\hat{f}_\lambda(x)$ n'est pas sommable.

(iv) La fonction $\hat{f}_\lambda$ et sa dérivée sont des $\mathrm{O}(|x|^{-2})$ en l'infini. On peut donc lui appliquer la formule de Poisson. Par ailleurs, $\hat{f}_\lambda$ étant sommable, la formule d'inversion de Fourier dans L^1 appliquée à f_λ montre que $(\mathscr{F}\hat{f}_\lambda)(t) = f_\lambda(-t)$. La formule de Poisson devient donc

$$\begin{aligned}\sum_{n\in\mathbf{Z}}\frac{1}{(\lambda+2i\pi n)^2} = \sum_{n\in\mathbf{Z}}\hat{f}_\lambda(n) &= \sum_{n\in\mathbf{Z}} f_\lambda(-n) = \sum_{n=0}^{+\infty} ne^{-n\lambda}\\ &= -\Big(\sum_{n=0}^{+\infty} e^{-n\lambda}\Big)' = -\big(\frac{1}{1-e^{-\lambda}}\big)' = \frac{e^{-\lambda}}{(1-e^{-\lambda})^2} = \frac{e^{\lambda}}{(e^{\lambda}-1)^2}.\end{aligned}$$

(L'interversion de la dérivée et de la série est justifiée par le fait que l'on a affaire à des séries entières (en $e^{-\lambda}$).)

(v) On remarque que $(-1)^n = e^{i\pi n}$. On peut donc évaluer la série en utilisant la formule de Poisson pour $e^{i\pi x}\hat{f}_\lambda(x)$ dont la transformée de Fourier est $t\mapsto f_\lambda(\frac{1}{2}-t)$.

(vi) Si K est un compact de $\mathbf{C}-2i\pi\mathbf{Z}$, il existe $\mathrm{R}>0$ tel que $|z|\leqslant\mathrm{R}$, pour tout $z\in\mathrm{K}$. Si $|n|>\frac{\mathrm{R}}{2\pi}$, on a alors $\big|\frac{1}{(z+2i\pi n)^2}\big| \leqslant \frac{1}{(2\pi|n|-\mathrm{R})^2}$, et comme $\sum_{|n|>\frac{\mathrm{R}}{2\pi}}\frac{1}{(2\pi|n|-\mathrm{R})^2} < +\infty$, la série est normalement convergente (et donc en particulier convergente en tout point) sur K. On note $f(z)$ la somme de la série. Comme chaque $\frac{1}{(z+2i\pi n)^2}$ est holomorphe sur $\mathbf{C}-2i\pi\mathbf{Z}$, il résulte du th. V.5.1 que f est holomorphe sur $\mathbf{C}-2i\pi\mathbf{Z}$. Or elle coïncide avec la fonction holomorphe $z\mapsto\frac{e^z}{(e^z-1)^2}$ sur $\mathbf{R}_+^*$. Comme $\mathbf{C}-2i\pi\mathbf{Z}$ est connexe, il résulte du théorème des zéros isolés que $f(z) - \frac{e^z}{(e^z-1)^2} = 0$ pour tout $z\in\mathbf{C}-2i\pi\mathbf{Z}$.

Exercice H.1.7. (i) $z\mapsto \operatorname{ch}\pi z$ est holomorphe car $z\mapsto e^{\lambda z}$ l'est et qu'une combinaison linéaire de fonctions holomorphes est holomorphe. Sa dérivée est $\pi\operatorname{sh}\pi z$.

On a $\operatorname{ch}\pi z = 0$ si et seulement si $e^{\pi z} = -e^{-\pi z}$, ce qui équivaut à $e^{2\pi z} = -1$, et donc à $z = \frac{i}{2} + ki$, avec $k\in\mathbf{Z}$.

(ii) La fonction f_u est méromorphe sur $\mathbf{C}$, avec des pôles simple en les $\frac{i}{2}+ki$, pour $k\in\mathbf{Z}$. Maintenant, on a $\mathrm{I}(\gamma_\mathrm{R},\frac{i}{2}+ki)=0$ sauf si $k=0$, où $\mathrm{I}(\gamma_\mathrm{R},\frac{i}{2})=1$. On en déduit, grâce à la formule des résidus, que

$$\mathrm{I}(\mathrm{R})=2i\pi\,\mathrm{Res}(f_u,\frac{i}{2})=2i\pi\big(e^{-2i\pi u\frac{i}{2}}\frac{1}{\pi\,\mathrm{sh}\,\pi\frac{i}{2}}\big)=2e^{\pi u}.$$

(iii) Quand $\mathrm{R}\to+\infty$, $\int_{[-\mathrm{R},\mathrm{R}]}f_u(z)\,dz\to\hat g_1(u)$. Comme $f_u(z+i)=-e^{2\pi u}f_u(z)$, on en déduit que $\int_{[\mathrm{R}+i,-\mathrm{R}+i]}f_u(z)\,dz=e^{2\pi u}\int_{[-\mathrm{R},\mathrm{R}]}f_u(z)\,dz$ tend vers $e^{2\pi u}\hat g_1(u)$, quand $\mathrm{R}\to+\infty$. Enfin, sur $[\mathrm{R},\mathrm{R}+i]$ et $[-\mathrm{R}+i,-\mathrm{R}]$, on a $|e^{-2i\pi uz}|\leqslant e^{2\pi u}$ et $\big|\frac{1}{\mathrm{ch}\,\pi z}\big|\leqslant\frac{2}{e^{\pi\mathrm{R}}-e^{-\pi\mathrm{R}}}$; on en déduit que $\int_{[\mathrm{R},\mathrm{R}+i]}f_u(z)\,dz$ et $\int_{[-\mathrm{R}+i,-\mathrm{R}]}f_u(z)\,dz$ sont majorés, en module, par $\frac{2e^{2\pi u}}{e^{\pi\mathrm{R}}-e^{-\pi\mathrm{R}}}$, et donc tendent vers 0, quand $\mathrm{R}\to+\infty$. On a donc $\mathrm{I}(\mathrm{R})\to(1+e^{2\pi u})\hat g_1(u)$, et comme $\mathrm{I}(\mathrm{R})=2e^{\pi u}$, pour tout $\mathrm{R}>0$, on obtient $\hat g_1(u)=\frac{2e^{\pi u}}{1+e^{2\pi u}}=\frac{1}{\mathrm{ch}\,\pi u}$.

Le cas $y>0$ s'en déduit via la formule pour les dilatations ($\mathscr{F}(f(ty))(x)=\frac{1}{y}\hat f(\frac{x}{y})$).

(iv) Si $a>0$ et si $z\in\Omega_a$, on a $\big|\frac{1}{\mathrm{ch}\,\pi nz}\big|\leqslant\frac{2}{e^{\pi|n|a}-e^{-\pi|n|a}}$; il en résulte que la série converge normalement sur Ω_a, et donc que sa somme $\mathrm{F}(z)$ est une fonction holomorphe sur Ω_a. Elle est donc aussi holomorphe sur $\Omega_0=\cup_{a>0}\Omega_a$.

Maintenant, si $y>0$, alors $t\mapsto\frac{1}{\mathrm{ch}\,\pi yt}$ est sommable sur $\mathbf{R}$, et sa dérivée $t\mapsto\frac{-\pi y\,\mathrm{sh}\,\pi yt}{\mathrm{ch}^2\pi yt}$ aussi. On peut donc lui appliquer la formule de Poisson, ce qui nous donne, en utilisant le (iii), l'identité $\sum_{n\in\mathbf{Z}}\frac{1}{\mathrm{ch}\,\pi yn}=\frac{1}{y}\sum_{n\in\mathbf{Z}}\frac{1}{\mathrm{ch}\,\pi\frac{n}{y}}$, que l'on peut retraduire sous la forme $\mathrm{F}(y)=\frac{1}{y}\mathrm{F}(\frac{1}{y})$.

Enfin, la fonction $z\mapsto z\mathrm{F}(z)-\mathrm{F}(\frac{1}{z})$, qui est holomorphe sur Ω_0, est nulle sur $\mathbf{R}_+^*$; elle est donc identiquement nulle sur l'ouvert connexe Ω_0, d'après le th. des zéros isolés.

Exercice H.1.8. (i) Comme le chemin γ_R formé du segment $[0,\mathrm{R}]$, de l'arc de cercle de centre 0 allant de R à $e^{i\theta}\mathrm{R}$, et du segment $[e^{i\theta}\mathrm{R},0]$ est un lacet, on a

$$\mathrm{I}_1(\mathrm{R})+\mathrm{I}_2(\mathrm{R})+\mathrm{I}_3(\mathrm{R})=2i\pi\big(\sum_{a^n+1=0}\mathrm{I}(\gamma_\mathrm{R},a)\mathrm{Res}(\frac{1}{z^n+1},a)\big),$$

d'après la formule des résidus. Les solutions de $a^n+1=0$ sont les $e^{i\pi(2k+1)/n}$, pour $k=\{0,1,\dots,n-1\}$ et le pôle de $\frac{1}{z^n+1}$ en chacun d'eux est simple ; son résidu est donc $\frac{1}{na^{n-1}}=\frac{-a}{n}$. Par ailleurs, l'indice $\mathrm{I}(\gamma_\mathrm{R},e^{i\pi(2k+1)/n})$ est égal à 1, si $0<\frac{(2k+1)\pi}{n}<\theta$, et vaut 0 sinon. On a donc

$$\mathrm{I}_1(\mathrm{R})+\mathrm{I}_2(\mathrm{R})+\mathrm{I}_3(\mathrm{R})=\frac{-2i\pi}{n}\sum_{0<\frac{(2k+1)\pi}{n}<\theta}e^{i\pi(2k+1)/n}.$$

(ii) Les fonctions $\frac{1}{1+t^n}$ et $\frac{1}{1+t^ne^{in\theta}}$ étant sommables sur $\mathbf{R}_+$, on a $\mathrm{I}_1(\mathrm{R})\to\int_0^{+\infty}\frac{dt}{1+t^n}$ et $\mathrm{I}_3(\mathrm{R})\to-e^{i\theta}\int_0^{+\infty}\frac{dt}{1+t^ne^{in\theta}}$. Maintenant, $\mathrm{I}_2(\mathrm{R})=\int_0^\theta\frac{i\mathrm{R}e^{it}dt}{1+\mathrm{R}^ne^{int}}$, et on peut majorer $\big|\frac{i\mathrm{R}e^{it}}{1+\mathrm{R}^ne^{int}}\big|$ par $\frac{\mathrm{R}}{\mathrm{R}^n-1}$. On a donc $|\mathrm{I}_2(\mathrm{R})|\leqslant\frac{\theta\,\mathrm{R}}{\mathrm{R}^n-1}$, et comme $n\geqslant2$, cela montre que $\mathrm{I}_2(\mathrm{R})\to0$.

(iii) Prenons $\theta=\frac{2\pi}{n}$. En passant à la limite dans la formule du (i), on obtient

$$(1-e^{2i\pi/n})\int_0^{+\infty}\frac{dt}{1+t^n}=\frac{-2i\pi}{n}e^{i\pi/n},$$

et donc

$$\int_0^{+\infty}\frac{dt}{1+t^n}=\frac{2i\pi\;e^{i\pi/n}}{n(e^{2i\pi/n}-1)}=\frac{\pi/n}{\sin(\pi/n)}.$$

Exercice H.1.9. (i) La fonction $z\mapsto\mathrm{tg}\,z$ est holomorphe en dehors des zéros de $\cos z$. Comme le disque $\mathrm{D}(0,(\frac{\pi}{2})^-)$ ne contient aucun de ces zéros, $\mathrm{tg}\,z$ est somme de sa série de Taylor en 0 sur tout le disque ((i) de la rem. V.4.9), et donc a fortiori sur $]\frac{-\pi}{2},\frac{\pi}{2}[$.

(ii) La fonction $z \mapsto \frac{\sin \pi z}{z-1}$ est holomorphe sur $\mathbf{C}$ sauf peut-être en $z = 1$ où elle peut avoir un pôle d'ordre 1. Or, en $z = 1$, la fonction $\sin \pi z$ s'annule ; il n'y a donc pas de pôle et $\frac{\sin \pi z}{z-1}$ est holomorphe sur $\mathbf{C}$ tout entier. Le rayon de convergence de sa série de Taylor en 0 est donc $+\infty$.

Exercice H.1.10. (i) Sur $\mathrm{D}(0, \mathrm{R}^-)$, on a $\left|\frac{z^2}{n^2}\right| \leqslant \left|\frac{\mathrm{R}^2}{n^2}\right|$, et comme $\sum_{n \geqslant 1} \frac{\mathrm{R}^2}{n^2} < +\infty$, le produit converge absolument sur $\mathrm{D}(0, \mathrm{R}^-)$. Chacun de ses termes étant holomorphe, il en est de même du produit, d'après le th. V.5.4. On en déduit que la fonction $z \mapsto \mathrm{F}(z)$, ainsi construite, est holomorphe sur $\mathbf{C} = \cup_{\mathrm{R}>0} \mathrm{D}(0, \mathrm{R}^-)$.

(ii) $\frac{1}{\sin \pi z}$ est méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples aux entiers, et ne s'annule pas. Par ailleurs, il résulte du (ii) du th. V.5.4 que les zéros de F sont des zéros simples aux entiers non nuls. Il en résulte que les zéros de $z \mapsto \pi z \mathrm{F}(z)$ sont les entiers et que ce sont des zéros simples, ce qui fait qu'ils compensent exactement les pôles de $\frac{1}{\sin \pi z}$, et que $\mathrm{G}(z)$ est holomorphe sur $\mathbf{C}$ et ne s'annule pas. Enfin, G est paire car F l'est et que $z \mapsto \sin \pi z$ et $z \mapsto \pi z$ sont impaires.

(iii) Comme $\mathbf{C}$ est contractile et comme G est holomorphe sur $\mathbf{C}$ et ne s'annule pas, il existe, d'après la prop. VI.2.3, une fonction h, holomorphe sur $\mathbf{C}$, telle que $e^h = \mathrm{G}$.

Maintenant, h est somme de sa série de Taylor $\sum_{n \in \mathbf{N}} a_n z^n$ en 0 sur $\mathbf{C}$ tout entier, d'après le (i) de la rem. V.4.9. Enfin, on a $\mathrm{G}(0) = 1$ car $\mathrm{F}(0) = 1$ et $\lim_{z \to 0} \frac{\sin \pi z}{\pi z} = 1$, et donc $h(0) = a_0 \in 2i\pi\mathbf{Z}$. Il en résulte que l'on a aussi $\mathrm{G} = e^g$, si $g(z) = h(z) - a_0 = \sum_{n \geqslant 1} a_n z^n$. Ceci permet de conclure.

(iv) D'après le principe du maximum, $\mathrm{C_N}$ est le maximum de $|\mathrm{G}(z)|$ sur le bord du carré. De plus, comme G est paire, on peut se contenter d'étudier $|\mathrm{G}(z)|$ sur les segments $[(\mathrm{N} + \frac{1}{2})(1 - i), (\mathrm{N} + \frac{1}{2}(1 + i)]$ et $[(\mathrm{N} + \frac{1}{2})(1 + i), (\mathrm{N} + \frac{1}{2})(i - 1)]$.

Sur ces segments, on a $\left|\frac{1}{\sin \pi z}\right| \leqslant 1$, d'après les minorations fournies dans l'énoncé. On obtient la majoration voulue pour $\mathrm{C_N}$ en majorant $|\pi z|$ par $\pi \mathrm{R_N}$, chaque $\left|1 - \frac{z^2}{n}\right|$, pour $n \leqslant \mathrm{N}$, par $1 + |z|^2 \leqslant \mathrm{R_N^2} + 1$, et par $1 + \frac{|z|^2}{n^2} \leqslant e^{|z|^2/n^2}$, si $n \geqslant \mathrm{N} + 1$.

Comme $\sum_{n \geqslant \mathrm{N}+1} \frac{1}{n^2} \leqslant \sum_{n \geqslant \mathrm{N}+1} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \frac{1}{\mathrm{N}}$, on obtient $\log \mathrm{C_N} \leqslant \mathrm{N} \log(\mathrm{R_N^2} + 1) + \frac{\mathrm{R_N^2}}{\mathrm{N}} + \log \pi \mathrm{R_N}$, et comme $\mathrm{R_N} = \mathrm{O}(\mathrm{N})$, on a $\log \mathrm{C_N} = \mathrm{O}(\mathrm{N} \log \mathrm{N})$, ce qui permet de conclure.

(v) On a $\mathrm{Re}(g(re^{i\theta})) = \mathrm{Re}\big(\sum_{n \geqslant 1} |a_n| r^n e^{i(n\theta + \alpha_n)}\big) = \sum_{n \geqslant 1} |a_n| r^n \cos(n\theta + \alpha_n)$. On en déduit que $\mathrm{I}_n(r) = \sum_{n \geqslant 1} |a_n| r^n \int_0^{2\pi} (1 + \cos(k\theta + \alpha_k)) \cos(n\theta + \alpha_n)\, d\theta = \pi |a_k| r^k$. (On peut intervertir série et intégrale en utilisant la convergence normale de la série sur $[0, 2\pi]$.)

Par ailleurs, $\mathrm{Re}(g(re^{i\theta})) = \log |\mathrm{G}(re^{i\theta})| \leqslant \log \mathrm{C_N}$, où $\mathrm{N} = [r] + 1$. On en déduit la majoration $\mathrm{I}_n(r) = \int_0^{2\pi} (1 + \cos(k\theta + \alpha_k)) \mathrm{Re}(g(re^{i\theta}))\, d\theta \leqslant 2 \log \mathrm{C_N}$, car $0 \leqslant 1 + \cos(k\theta + \alpha_k) \leqslant 2$.

On en déduit, pour tout $r > 0$, la majoration $|a_k| \leqslant \frac{2}{\pi} \frac{\log \mathrm{C}_{[r]+1}}{r^k} = \frac{2}{\pi} \frac{\log \mathrm{C}_{[r]+1}}{([r]+1)^k} \frac{([r]+1)^k}{r^k}$, qui tend vers 0, si $k \geqslant 2$, d'après le (iv). Ceci permet de conclure.

(vi) Il résulte des (iv) et (v) que $\mathrm{G}(z) = e^{a_1 z}$, et comme G est paire, on a $a_1 = 0$ et $\mathrm{G} = 1$, et donc $\mathrm{F}(z) = \frac{\sin \pi z}{\pi z}$, ce que l'on cherchait à démontrer.

Exercice H.1.11. (i) La fonction $s \mapsto \Gamma(s)\Gamma(1 - s)$ est holomorphe en dehors de pôles simples en les entiers, et comme $s \mapsto \sin \pi s$ a des zéros en les entiers, cela implique que F est holomorphe sur $\mathbf{C}$. Maintenant, on a $\mathrm{F}(s + 1) = \big(\sin \pi(s + 1)\big)\, \Gamma(s + 1)\Gamma(-s) = (-\sin \pi s)(s\Gamma(s))\big(\frac{\Gamma(1-s)}{-s}\big) = \mathrm{F}(s)$.

(ii) Comme $\frac{\log z}{2i\pi}$ est bien défini à addition près d'un entier, et comme F est périodique de période 1, la quantité $\mathrm{F}(\frac{\log z}{2i\pi})$ ne dépend pas du choix de $\log z$; notons la $f(z)$. Si $z_0 \in \mathbf{C}^*$, on peut choisir une détermination h du logarithme qui est holomorphe sur $\mathrm{D}(z_0, |z_0|^-)$ [par exemple celle obtenue en retirant la demi-droite $\mathbf{R}_+(-z_0)$], et on a alors $f = \mathrm{F} \circ h$ sur $\mathrm{D}(z_0, |z_0|^-)$, ce qui prouve que f est holomorphe sur $\mathrm{D}(z_0, |z_0|^-)$. Ceci étant vrai pour tout $z_0 \in \mathbf{C}^*$, il en résulte que f est holomorphe sur $\cup_{z_0 \in \mathbf{C}^*} \mathrm{D}(z_0, |z_0|^-) = \mathbf{C}^*$.

(iii) L'existence des a_n résulte du cor. VI.3.2 appliqué à $z_0 = 0$, $\mathrm{R}_1 = 0$ et $\mathrm{R}_2 = +\infty$. Par ailleurs, d'après ce corollaire, on a $a_n = \frac{1}{2i\pi} \int_{\mathrm{C}(0,r)} z^{-n-1} f(z) dz$, pour tout $r > 0$. Maintenant, soit $\varphi : \mathbf{C} \to \mathbf{C}^*$

défini par $\varphi(s) = e^{2i\pi s}$. D'après l'ex. V.4.5, on a $\int_{[i\mathrm{T},1+i\mathrm{T}]}(g\circ\varphi)\varphi'(s)\,ds = \int_{\varphi([i\mathrm{T},1+i\mathrm{T}])} g(z)dz$, pour toute $g : \mathbf{C}^* \to \mathbf{C}$ continue. Comme $\varphi([i\mathrm{T}, 1+i\mathrm{T}]) = \mathrm{C}(0,r)$, avec $r = e^{-2\pi\mathrm{T}}$, on obtient pour $g(z) = z^{-n-1}f(z)$, l'identité $a_n = \frac{1}{2i\pi}\int_{[i\mathrm{T},1+i\mathrm{T}]} e^{-(n+1)2i\pi s}\mathrm{F}(s)(2i\pi e^{2i\pi s})ds = \int_{[i\mathrm{T},1+i\mathrm{T}]} e^{-2i\pi ns}\mathrm{F}(s)\,ds$, ce que l'on voulait.

(iv) Comme F et $\mathrm{Im}(s)$ sont périodiques de période 1, il suffit de prouver que G est bornée dans une bande verticale de largeur 1, par exemple $\mathrm{B} = \{s,\ 1 \leqslant \mathrm{Re}(s) \leqslant 2\}$, et comme G est continue, elle est bornée sur le compact $\mathrm{K} = \{s \in \mathrm{B},\ |\mathrm{Im}(s)| \leqslant 1\}$, et il suffit de prouver que G est bornée sur $\mathrm{B} - \mathrm{K}$. Or $\Gamma(s)$ est bornée sur B, et comme $\Gamma(1-s) = \frac{\Gamma(3-s)}{(1-s)(2-s)}$, et que $3 - s \in \mathrm{B}$ si $s \in \mathrm{B}$, il s'ensuit que $\Gamma(1-s)$ est aussi borné sur $\mathrm{B} - \mathrm{K}$. Enfin, $|\sin\pi s| \leqslant \frac{1}{2}\big(e^{\pi|\mathrm{Im}(s)|} + e^{-\pi|\mathrm{Im}(s)|}\big) \leqslant e^{\pi|\mathrm{Im}(s)|}$. On en déduit le résultat.

(v) D'après le (iv), il existe $\mathrm{C} > 0$ tel que $|e^{-2i\pi ns}\mathrm{F}(s)| \leqslant \mathrm{C}e^{2\pi n\mathrm{T}+\pi|\mathrm{T}|}$, si $s \in [i\mathrm{T}, 1+i\mathrm{T}]$. On en déduit la majoration $|a_n| \leqslant \mathrm{C}e^{2\pi n\mathrm{T}+\pi|\mathrm{T}|}$, pour tout $\mathrm{T} \in \mathbf{R}$. En faisant tendre T vers $-\infty$ (resp. $+\infty$) si $n \geqslant 1$ (resp. $n \leqslant -1$), on en déduit que $a_n = 0$, si $n \neq 0$. Il en résulte que f est constante ; il en est donc de même de F, et comme on a $\mathrm{F}(0) = \lim_{s\to 0}\frac{\sin\pi s}{s}\Gamma(s+1)\Gamma(1-s) = \pi$, cela permet de conclure.

Exercice H.1.12. (i) D'après l'inégalité de Cauchy ((i) de la rem. V.4.9), on a $|g'(z_0)| \leqslant \frac{1}{r}\sup_{z\in\mathrm{C}(z_0,r)}|g(z)|$, si $z_0 = x_0 + iy_0$. Si $|y_0| \geqslant \mathrm{M}' = 2\mathrm{M}$, et si $r = \frac{|y_0|}{2}$, on a $\mathrm{M} \leqslant |\mathrm{Im}(z)| \leqslant \frac{3|y_0|}{2}$, pour tout $z \in \mathrm{C}(z_0,r)$, et donc $|g(z)| \leqslant \mathrm{C}\big(\frac{3|y_0|}{2}\big)^{\mathrm{N}}$. On en déduit que $|g'(z_0)| \leqslant \mathrm{C}'|y_0|^{\mathrm{N}-1}$, avec $\mathrm{C}' = 3^{\mathrm{N}}2^{1-\mathrm{N}}$, si $|y_0| \geqslant \mathrm{M}'$.

(ii) Soit $g = f^2 + f'$. Comme f est holomorphe sur $\mathrm{D}(0,1^-) - \{0\}$, impaire, et a un pôle simple de résidu 1 en 0, on a $f(z) = \frac{1}{z} + \sum_{n=0}^{+\infty} a_{2k+1}z^{2k+1}$ sur $\mathrm{D}(0,1^-)$ (fonction holomorphe sur un disque épointé, n° 2 du § VI.3). On en déduit que $f'(z) = \frac{-1}{z^2} + \sum_{n=0}^{+\infty}(2k+1)a_{2k+1}z^{2k}$, que $f(z)^2 = \frac{1}{z^2} + 2a_1 + \cdots$, et que $g(z)$ est holomorphe en 0. Comme elle est périodique de période 1, elle est holomorphe en tous les entiers, et comme f est holomorphe sur $\mathbf{C} - \mathbf{Z}$, elle est holomorphe sur $\mathbf{C}$ tout entier.

De plus, il résulte du (i) que g est un $\mathrm{O}(y^{2\mathrm{N}})$ et que $g^{(k)}$ est un $\mathrm{O}(y^{2\mathrm{N}-k})$ pour tout k. On en déduit que $g^{(2\mathrm{N})}$ est bornée sur $\{z,\ 0 \leqslant \mathrm{Re}(z) \leqslant 1,\ |\mathrm{Im}(z)| \geqslant \mathrm{M}_{\mathrm{N}}\}$, si M_{N} est assez grand. Comme $g^{(2\mathrm{N})}$ est continue (car holomorphe) sur $\{z,\ 0 \leqslant \mathrm{Re}(z) \leqslant 1\}$, et comme $\{z,\ 0 \leqslant \mathrm{Re}(z) \leqslant 1,\ |\mathrm{Im}(z)| \leqslant \mathrm{M}_{\mathrm{N}}\}$ est compact, on en déduit l'existence de C_{N} tel que $|g^{(2\mathrm{N})}(z)| \leqslant \mathrm{C}_{\mathrm{N}}$, si $0 \leqslant \mathrm{Re}(z) \leqslant 1$. La périodicité de $g^{(2\mathrm{N})}$ implique alors que $|g^{(2\mathrm{N})}(z)| \leqslant \mathrm{C}_{\mathrm{N}}$, pour tout $z \in \mathbf{C}$, et le théorème de Liouville permet d'en conclure que $g^{(2\mathrm{N})}$ est constante. On en déduit que g est un polynôme de degré $\leqslant 2\mathrm{N}$, et comme g est périodique, cela implique que g est une constante, ce que l'on cherchait à démontrer.

On aurait pu aussi constater que $h(z) = f(z) - \pi\operatorname{cotg}\pi z$ est holomorphe sur $\mathbf{C}$, impaire, périodique de période 1, et $\mathrm{O}(y^{\mathrm{N}})$. Les même arguments que ci-dessus permettent alors de montrer que $h = 0$, et donc que $f^2 + f' = -\pi^2$.

Exercice H.1.13. (i) Soit $\Omega' = \{z \in \Omega,\ |f(z) - g(z)| < |f(z)|\}$. Alors Ω' est un ouvert comme image réciproque de l'ouvert $\{(x,y),\ x < y\}$ de $\mathbf{R}^2$ par l'application continue $z \mapsto (|f(z) - g(z)|, |f(z)|)$, et Ω' contient C par hypothèse. Maintenant, si $z \in \Omega'$, on a $|\frac{g(z)}{f(z)} - 1| < 1$, ce qui permet de définir h comme la composée de $\frac{g}{f} : \Omega' \to \mathrm{D}(1,1^-)$ et $\log : \mathrm{D}(1,1^-) \to \mathbf{C}$, où log est la détermination principale du logarithme. On a alors $h' = \frac{(e^h)'}{e^h} = \frac{(g/f)'}{g/f} = \frac{g'}{g} - \frac{f'}{f}$.

(ii) La fonction $\frac{f'}{f} - \frac{g'}{g}$ admet $-h$ comme primitive sur Ω' et donc a une intégrale nulle sur tout lacet contenu dans Ω'. En particulier, $\int_{\mathrm{C}}\big(\frac{f'(z)}{f(z)} - \frac{g'(z)}{g(z)}\big)\,dz = 0$ (où C est parcouru dans le sens direct). On en déduit, en utilisant la prop. VI.3.14 (car f ne s'annule pas sur C par hypothèse, et g non plus puisque $|f(z) - g(z)| < |f(z)|$, si $z \in \mathrm{C}$) que f et g ont le même nombre de zéros dans D, comptés avec multiplicité.

(iii) D étant compact et G continue sur D, il existe $z_0 \in \mathrm{D}$ tel que $|\mathrm{G}|$ atteigne son maximum en z_0, et le principe du maximum montre que $z_0 \in \mathrm{C}$. Comme $|\mathrm{G}(z_0)| < 1$, par hypothèse, on a $|\mathrm{G}(z)| < 1$, si $z \in \mathrm{D}$, et donc $\mathrm{G}(\mathrm{D}) \subset \mathrm{D}$. En appliquant le (ii) à $f(z) = z$ et $g(z) = z - \mathrm{G}(z)$, on en déduit que f et g ont le même nombre de zéros dans D, et comme f a un unique zéro en 0, cela implique que g a un unique zéro et donc que G a un unique point fixe dans D.

Exercice H.1.14. (i) Si $a > 1$ et $\mathrm{Re}(s) > a$, alors $|\frac{1}{(n+x)^s}| \leqslant \frac{1}{(n+x)^a}$ sauf pour l'ensemble fini de n tels que $|n+x| < 1$. Comme $\sum_{n=0}^{+\infty} \frac{1}{(n+x)^a} < +\infty$, la série $\sum_{n\in\mathbf{N}} \frac{1}{(n+x)^s}$ converge normalement sur $\mathrm{Re}(s) > a$. Il résulte du (ii) du th. V.5.1 que la somme $\mathrm{F}(x,s)$ de cette série est holomorphe sur $\mathrm{Re}(s) > a$. Ceci étant vrai pour tout $a > 1$, la fonction $\mathrm{F}(x,s)$ est holomorphe sur $\mathrm{Re}(s) > 1$.

(ii) On a $\frac{1}{(n+x)^s} = \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-(n+x)t} t^{s-1} dt$, si $\mathrm{Re}(s) > 0$. Les sommes partielles de $\sum_{n=0}^{+\infty} e^{-(n+x)t} t^{s-1}$ sont majorées en valeur absolue par $\sum_{n=0}^{+\infty} e^{-(n+x)t} t^{\mathrm{Re}(s)-1} = \frac{te^{-tx}}{1-e^{-t}} t^{\mathrm{Re}(s)-2}$, sommable si $\mathrm{Re}(s) - 2 > -1$ car à décroissance rapide en $+\infty$ et équivalente à $t^{\mathrm{Re}(s)-2}$ en 0. On peut donc, si $\mathrm{Re}(s) > 1$, utiliser le théorème de convergence dominée pour échanger somme et intégrale, ce qui nous donne

$$\mathrm{F}(x,s) = \sum_{n=0}^{+\infty} \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-(n+x)t} t^{s-1} dt = \frac{1}{\Gamma(s)} \int_0^{+\infty} \sum_{n=0}^{+\infty} e^{-(n+x)t} t^{s-1} dt = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{e^{-tx}}{1-e^{-t}} t^{s-1} dt.$$

(iii) Posons $g_x(t) = \frac{te^{-tx}}{1-e^{-t}}$. Alors g_x est $\mathscr{C}^\infty$ sur $\mathbf{R}_+$ comme restriction d'une fonction holomorphe en dehors de $2i\pi\mathbf{Z} - \{0\}$, et à décroissance rapide à l'infini ainsi que toutes ses dérivées. On est donc dans les conditions d'application de la prop. VII.2.6, et $\mathrm{M}(g_x,s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{te^{-tx}}{1-e^{-t}} t^{s-1} dt$ admet un prolongement holomorphe à $\mathbf{C}$ vérifiant $\mathrm{M}(g_x,0) = g_x(0) = 1$. Or on a $\Gamma(s) = (s-1)\Gamma(s-1)$, et donc $\mathrm{F}(x,s) = \frac{1}{s-1}\mathrm{M}(g_x, s-1)$. Le résultat s'en déduit.

H.2. Table des caractères de A_5

Le but de ce problème est l'établissement de la table des caractères (fig. 4) du groupe A_5 d'ordre 60, appelé aussi *groupe de l'icosaèdre*.

		$\mathbf{1}$	χ_U	χ_V	χ_W	$\chi_{W'}$
1	C_1	1	4	5	3	3
20	C_3	1	1	-1	0	0
15	$C_{2,2}$	1	0	1	-1	-1
12	C_5	1	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
12	C'_5	1	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

FIGURE 4. Table des caractères de A_5

On utilisera sans démonstration les faits suivants :
• Si i, j, k (resp. i', j', k') sont des éléments distincts de $\{1, \dots, 5\}$, il existe $g \in A_5$ tel que $g(i) = i'$, $g(j) = j'$ et $g(k) = k'$ (en fait g est unique).
• Le groupe A_5 a 5 classes [4] de conjugaison :
— La classe C_1 de l'élément neutre 1, de cardinal 1.
— La classe C_3 des 3-cycles (d'orde 3), de cardinal 20.

4. Les classes de conjugaison de A_5 peuvent se déduire de celles de S_5. On rappelle que si G est un groupe, si $x \in G$, et si Z_x est le centralisateur de x (i.e. l'ensemble des éléments de G commutant à x), la classe de conjugaison de x est isomorphe à G/Z_x par $g \mapsto gxg^{-1}$; en particulier elle est de cardinal $|G|/|Z_x|$. Pour comprendre ce que devient une classe de conjugaison de S_5 dans A_5, il s'agit donc de comprendre le lien du centralisateur Z_x de x dans S_5 avec son centralisateur $Z_x \cap A_5$ dans A_5.

Or A_5 est le noyau de la signature $\varepsilon : S_5 \mapsto \{\pm 1\}$. On en déduit que si H est un sous-groupe de S_5, alors soit $H \subset A_5$, soit $\varepsilon : H \to \{\pm 1\}$ est surjective et donc $H \cap A_5$ qui en est le noyau est de cardinal $|H|/2$.

Soit $C \in \mathrm{Conj}(S_5)$. Si $C \cap A_5 \neq \varnothing$, alors le caractère ε de S_5 prend la valeur 1 sur un élément de C et donc sur C tout entier ; autrement dit $C \subset A_5$. Maintenant, si $x \in C$, la classe de conjugaison C_x dans A_5 est incluse dans C, et si Z_x est son centralisateur dans S_5, il y a deux cas :

• $Z_x \subset A_5$ et alors $|C_x| = \frac{|A_5|}{|Z_x|} = \frac{1}{2}\frac{|S_5|}{|Z_x|} = \frac{1}{2}|C|$, et C se scinde en deux classes de conjugaison dans A_5 ;

• Z_x contient un élément de signature -1, et alors $|Z_x \cap A_5| = \frac{1}{2}|Z_x|$, ce qui implique que C_x est de cardinal $\frac{|A_5|}{|Z_x \cap A_5|} = \frac{|S_5|/2}{|Z_x|/2} = \frac{|S_5|}{|Z_x|} = |C|$, que $C_x = C$ et que C reste une classe de conjugaison dans A_5.

Comme (45) commute à (123), la classe des 3-cycles reste une classe de conjugaison dans A_5. De même, (12) commute à (12)(34) et donc $C_{2,2}$ est une classe de conjugaison de A_5. Par contre, les 5-cycles sont au nombre de 24, et comme 24 ne divise pas $|A_5| = 60$, cela implique que la classe des 5-cycles se scinde en deux dans A_5. Comme $(13524) = \sigma(12345)\sigma^{-1}$, avec $\sigma = (2354)$ et $\varepsilon(\sigma) = -1$, on en déduit que t_0 et t_0^2 ne sont pas dans la même classe de conjugaison dans A_5, et comme les 5-cycles sont tous conjugués dans S_5, cela permet de montrer que t et t^2 ne sont pas dans la même classe, pour tout 5-cycle t.

— La classe $C_{2,2}$ des produits de deux transpositions de supports disjoints (d'ordre 2), de cardinal 15.

— Deux classes C_5 et C_5' de cardinal 12 dont la réunion est l'ensemble des 5-cycles (d'ordre 5). De plus, si t est un 5-cycle, alors t et t^2 ne sont pas dans la même classe. Pour fixer les idées, on note C_5 la classe de $t_0 = (12345)$ et C_5' celle de $t_0^2 = (13524)$.

Question 1. (a) Montrer que A_5 a 5 représentations irréductibles dont au moins une est de dimension 1.

(b) Montrer que ces représentations sont de dimensions respectives 1, 3, 3, 4 et 5.

(c) Quelle est la représentation de dimension 1 ? On note U la représentation de dimension 4, V celle de dimension 5, et W, W′ les deux représentations de dimension 3. Quel morceau de la table peut-on déduire de ce qui précède ?

Question 2. On note T la matrice 5×5 définie par la table des caractères de A_5.

(a) Montrer que TT^* est la matrice diagonale de coefficients 60, 3, 4, 5 et 5. (On utilisera la rem. I.2.35.)

(b) En déduire une majoration de $|\chi(g)|$, puis que $|\chi(g)| \neq |\chi(1)|$ pour tous $\chi \in \mathrm{Irr}(A_5) - \{\mathbf{1}\}$ et $g \neq 1$.

(c) En déduire que A_5 est simple (on rappelle que si G n'est pas simple, alors il existe un morphisme de groupes surjectif $f : G \to H$, avec $H \neq \{1\}$, dont le noyau n'est pas réduit à $\{1\}$).

Question 3. Soit U′ la représentation de permutation de A_5 associée à l'action naturelle de A_5 sur $\{1, \dots, 5\}$ (i.e. $g(e_i) = e_{g(i)}$, si $g \in A_5$ et $i \in \{1, \dots, 5\}$), et soit U l'hyperplan de U′ d'équation $x_1 + \cdots + x_5 = 0$.

(a) Calculer $g \cdot x$, si $x = (x_1, \dots, x_5)$ et $g \in A_5$, et montrer que U est stable par A_5.

(b) Soit $x \in U$. Montrer que le sous-espace U_x de U engendré par les $g \cdot x$, pour $g \in A_5$, est stable par A_5, et qu'il contient un vecteur non nul dont 3 des coordonnées sont nulles (on commencera par montrer qu'il contient un vecteur non nul dont 2 des coordonnées sont nulles en considérant les éléments de la forme $g \cdot x - x$).

(c) En déduire que U est irréductible.

(d) Calculer les caractères de U′ et U ; retrouver le fait que U est irréductible.

Question 4. (a) Soit Y une représentation de A_5. Montrer que $g \mapsto \det \rho_Y(g)$ est un caractère de A_5. En déduire que $\det \rho_Y(g) = 1$ pour tout $g \in A_5$.

(b) Remplir les deux premières lignes des deux dernières colonnes de T. (On considérera une représentation irréductible Y de dimension 3 de A_5, on s'intéressera aux valeurs propres $\lambda_1, \lambda_2, \lambda_3$ de $\rho_Y(g)$, et on utilisera le (b) de la question 2.)

(c) Montrer que C_5 et C_5' sont stables par $g \mapsto g^{-1}$. En déduire que, si g est un 5-cyle, les valeurs propres de $\rho_Y(g)$ sont globalement stables par $\lambda \mapsto \lambda^{-1}$.

(d) Terminer le remplissage des deux dernières colonnes de T. (On utilisera les formules $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$, $\cos \frac{4\pi}{5} = \frac{-\sqrt{5}-1}{4}$.)

(e) Comment peut-on compléter la table des caractères de A_5 ?

Question 5. Soit Y la représentation de permutation associée à l'action de A_5 sur l'ensemble à 10 éléments des paires d'éléments distincts de $\{1, \dots, 5\}$. Calculer le caractère χ_Y de Y et les produits scalaires $\langle \chi_Y, \mathbf{1} \rangle$ et $\langle \chi_Y, \chi_U \rangle$. En déduire une autre manière de calculer χ_V.

Corrigé

Question 1. (a) D'après le cor. I.2.16, le nombre de représentations irréductibles de A_5 est égal au nombre de ses classes de conjugaison, c'est-à-dire 5. Par ailleurs, tout groupe admet la représentation triviale (de dimension 1) comme représentation irréductible.
(b) D'après la formule de Burnside, si d_2, d_3, d_4 et d_5 désignent les dimensions des représentations irréductibles de A_5 distinctes de la triviale, on a $1 + d_2^2 + d_3^2 + d_4^2 + d_5^2 = |A_5| = 60$. Or 59 s'écrit d'une seule manière (à permutation près) comme une somme de 4 carrés, à savoir $59 = 5^2 + 4^2 + 3^2 + 3^2$. (Cela peut se voir en faisant une recherche systématique ; on peut aller un peu plus vite en regardant modulo 8, ce qui permet de montrer que l'un des d_i est 4 (car les autres multiples de 4 sont trop grands) et les autres d_i sont impairs.)
(c) La représentation de dimension 1 est la représentation triviale, et comme $\chi(1)$ est la dimension de la représentation correspondant à χ, on peut remplir la première ligne et la première colonne de la table des caractères.

Question 2. (a) D'après la rem. I.2.35, TT^* est la matrice diagonale dont le coefficient sur la ligne correspondant à la classe C est $|G|/|C|$. C'est donc la matrice diagonale de coefficients $60/1 = 60$, $60/20 = 3$, $60/15 = 4$, $60/12 = 5$ et $60/12 = 5$.
(b) Le coefficient diagonal de TT^* sur la ligne correspondant à la classe C est aussi égal à $\sum_{\chi\in\mathrm{Irr}(A_5)} |\chi(C)|^2$. Comme ce coefficient est $\leqslant 5$ si $C \neq C_1$, d'après le (a), cela montre que $|\chi(C)| < 3$ pour tout $\chi \in \mathrm{Irr}(A_5)$, si $C \neq C_1$, et comme $|\chi(1)| \geqslant 3$, si $\chi \in \mathrm{Irr}(A_5) - \{\mathbf{1}\}$, cela permet de conclure.
(c) Si A_5 n'était pas simple, il existerait un morphisme de groupes surjectif $f : A_5 \to H$, avec $H \neq \{1\}$, de noyau $\mathrm{Ker}\, f \neq \{1\}$. Comme $H \neq \{1\}$, il existe une représentation irréductible V de H, distincte de la représentation triviale (cela découle de la formule de Burnside). Mais alors $\rho_V \circ f$ est un morphisme de groupes de A_5 dans GL(V), ce qui permet de considérer V comme une représentation de A_5. Les images de $v \in V$ sous l'action de A_5 étant les mêmes que celles sous l'action de H, la représentation V de A_5 est irréductible, et on a $\chi_V(g) = \chi_V(1)$, pour tout $g \in \mathrm{Ker}\, f$. Ceci contredit le (b) et permet de conclure.

Question 3. (a) On a $g \cdot (x_1e_1 + \cdots + x_5e_5) = x_1e_{g(1)} + \cdots + x_5e_{g(5)}$ et donc $g \cdot (x_1, \ldots, x_5) = (x_{g^{-1}(1)}, \ldots, x_{g^{-1}(5)})$. On en déduit le fait que les coordonnées de $g \cdot x$ sont les mêmes que celles de x à permutation près, et donc que les sommes des coordonnées de x et $g \cdot x$ sont les mêmes. D'où la stabilité de U sous l'action de A_5.
(b) La stabilité de U_x par A_5 résulte de ce que $h \cdot (g \cdot x) = hg \cdot x$, et donc que le translaté d'une combinaison linéaire de translatés de x est encore une combinaison linéaire de translatés de x.

Soit $x = (x_1, \ldots, x_5)$. Comme $x \in U$, il existe $i \neq j$ tels que $x_i \neq x_j$. Quitte à remplacer x par $h \cdot x$, avec $h \in A_5$ vérifiant $h(1) = i$ et $h(2) = j$, on peut supposer que $i = 1$ et $j = 2$. Soit $g = (132)$. Alors $g \cdot x = (x_2, x_3, x_1, x_4, x_5)$ et $y = g \cdot x - x = (y_1, y_2, y_3, 0, 0)$, avec $y_1 = x_2 - x_1 \neq 0$. Comme $y \in U_x$, on a établi l'existence d'un élément non nul y de U_x ayant deux coordonnées nulles.

Comme $y \in U_x$, les trois coordonnées non nulles de y ne sont pas toutes égales, et il existe $i \neq j$ tels que $y_i \neq y_j$. Comme ci-dessus, on peut supposer $i = 1$ et $j = 2$, et $y_4 = y_5 = 0$. Soit $g' = (12)(45)$, et soit $w = g' \cdot y - y$. Alors $w \in U_x$, et $w = (y_2 - y_1, y_1 - y_2, 0, 0, 0)$ est non nul et a 3 coordonnées nulles.
(c) Il s'agit de prouver que le sous-espace U_x de U engendré par les $g \cdot x$ est égal à U, si $x \in U$ est non nul. Or U_x contient un vecteur de la forme $e_i - e_j$, avec $i \neq j$, d'après le (b). Comme $g \cdot (e_i - e_j) = e_{g(i)} - e_{g(j)}$, et comme pour tout couple $i' \neq j'$, il existe $g \in A_5$ tel que $g(i) = i'$ et $g(j) = j'$, on voit que U_x contient $e_i - e_j$ pour tout couple $i \neq j$. Il contient donc en particulier la base $e_i - e_1$, pour $2 \leqslant i \leqslant 5$, de U, ce qui permet de conclure.
(d) Comme U′ est une représentation de permutation, $\chi_{U'}(g)$ est le nombre de points fixes de $g \in A_5$ agissant sur $\{1, \ldots, 5\}$. On a donc $\chi_{U'}(C_1) = 5$; $\chi_{U'}(C_3) = 2$, $\chi_{U'}(C_{2,2}) = 1$, et $\chi_{U'}(C_5) = \chi_{U'}(C_5') = 0$.

La représentation U′ est la somme directe de U et de la droite engendrée par $e_1 + \cdots + e_5$ sur laquelle A_5 agit trivialement. On a donc $\chi_{U'}(g) = \chi_U(g) + \chi_{\mathbf{1}}(g)$, d'où $\chi_U(g) = \chi_{U'}(g) - 1$, pour tout $g \in A_5$. En reportant les valeurs de $\chi_{U'}$, cela nous fournit la seconde colonne de la table des caractères.

Enfin, $\langle \chi_U, \chi_U \rangle = \frac{1}{60}(4^2 + 20 \cdot 1^2 + 15 \cdot 0^2 + 12 \cdot (-1)^2 + 12 \cdot (-1)^2) = \frac{1}{60}(16 + 20 + 12 + 12) = 1$, ce qui prouve que U est irréductible (cor. I.2.21).

Question 4. (a) L'application $g \mapsto \det \rho_Y(g)$ est un morphisme de groupes de G dans $\mathbf{C}^*$ comme composée des morphismes $g \mapsto \rho_Y$ et $u \mapsto \det u$; c'est donc un caractère linéaire de A_5. Or un caractère linéaire définit une représentation de dimension 1 qui est irréductible par la force des choses. Comme A_5 a une seule représentation irréductible de dimension 1 (la représentation triviale), cela permet de conclure.
(b) • Si g est un 3-cycle, alors $\rho_Y(g)^3 = \rho_Y(g^3) = 1$, et $\lambda_1, \lambda_2, \lambda_3$ sont des racines 3-ièmes de l'unité dont le produit est égal à 1 d'après le (a), et qui ne sont pas toutes les trois égales, d'après le (b) de la question 2. On a donc $\{\lambda_1, \lambda_2, \lambda_3\} = \{1, e^{2i\pi/3}, e^{-2i\pi/3}\}$, et donc $\chi_Y(g) = \lambda_1 + \lambda_2 + \lambda_3 = 0$, ce qui remplit la deuxième ligne des deux dernières colonnes de T.

• Si g est d'ordre 2, alors $\lambda_1, \lambda_2, \lambda_3$ valent ± 1, et ne sont pas toutes égales à 1, et leur produit vaut 1. Il y en a donc deux qui valent -1 et une qui vaut 1. On en déduit que $\chi_Y(g) = \lambda_1 + \lambda_2 + \lambda_3 = -1$, ce qui remplit la troisième ligne des deux dernières colonnes de T.
(c) $g \mapsto g^2$ échange C_5 et C_5', et donc $g \mapsto g^4$ laisse stable C_5 et C_5'. Or $g^4 = g^{-1}$, si g est un 5-cycle puisque $g^5 = 1$.

On en déduit que, si g est un 5-cycle, alors g et g^{-1} sont dans la même classe de conjugaison, et donc qu'il existe $h \in A_5$ tel que $g^{-1} = hgh^{-1}$. Ceci implique que $\rho_Y(g)^{-1} = \rho_Y(g^{-1}) = \rho_Y(h)\rho_Y(g)\rho_Y(h)^{-1}$, et donc que $\rho_Y(g)^{-1}$ et $\rho_Y(g)$ ont les mêmes valeurs propres comptées avec multiplicité. Comme les valeurs propres de $\rho_Y(g)^{-1}$ sont les inverses de celles de $\rho_Y(g)$, cela permet de conclure.
(d) Si $g \in C_5$, les valeurs propres $\lambda_1, \lambda_2, \lambda_3$ de $\rho_Y(g)$ sont des racines 5-ièmes de l'unité, qui ne sont pas toutes égales à 1, et l'ensemble est stable par $\lambda \mapsto \lambda^{-1}$ d'après le (d). Il n'y a donc que deux possibilités : $\{\lambda_1, \lambda_2, \lambda_3\} = \{1, e^{2i\pi/5}, e^{-2i\pi/5}\}$ ou $\{\lambda_1, \lambda_2, \lambda_3\} = \{1, e^{4i\pi/5}, e^{-4i\pi/5}\}$. Dans le premier cas, on aurait $\chi_Y(g) = \frac{1+\sqrt{5}}{2}$ et dans le second $\chi_Y(g) = \frac{1-\sqrt{5}}{2}$. De plus, $g^2 \in C_5'$ et les valeurs propres de $\rho_Y(g^2)$ sont les carrés des valeurs propres de $\rho_Y(g)$. Il s'en suit que, si $\chi_Y(C_5) = \frac{1+\sqrt{5}}{2}$, alors $\chi_Y(C_5') = \frac{1-\sqrt{5}}{2}$, et que si $\chi_Y(C_5) = \frac{1-\sqrt{5}}{2}$, alors $\chi_Y(C_5') = \frac{1+\sqrt{5}}{2}$. Comme A_5 a deux représentations irréductibles de dimension 3, et comme le caractère détermine la représentation (cor. I.2.19), cela implique que les deux possibilités apparaissent. Ceci permet de conclure.
(e) Il suffit d'utiliser la décomposition de la régulière (cor. I.2.23), qui nous fournit, pour $g \neq 1$, la formule $1 + 4\chi_U(g) + 5\chi_V(g) + 3\chi_W(g) + 3\chi_{W'}(g) = 0$, et comme on connait tous les termes sauf $\chi_V(g)$, cela permet de conclure.

Question 5. Comme Y est une représentation de permutation, $\chi_Y(g)$ est le nombre de points fixes de $g \in A_5$ agissant sur l'ensemble des paires d'éléments distincts de $\{1, \ldots, 5\}$. Comme il y a 10 telles paires, on a $\chi_Y(C_1) = 10$. La seule paire fixe par (123) est $\{4, 5\}$, et donc $\chi_Y(C_3) = 1$. Il y a deux paires fixes par (12)(34), à savoir $\{1, 2\}$ et $\{3, 4\}$, et donc $\chi_Y(C_{2,2}) = 2$. Enfin, aucune paire n'est fixe par un 5-cycle et donc $\chi_Y(C_5) = \chi_Y(C_5') = 0$. Maintenant,

$$\begin{aligned}\langle \chi_Y, \mathbf{1} \rangle &= \frac{1}{60}(10 + 20 \cdot 1 + 15 \cdot 2 + 12 \cdot 0 + 12 \cdot 0) = \frac{1}{60}(10 + 20 + 30) = 1\\ \langle \chi_Y, \chi_U \rangle &= \frac{1}{60}(40 + 20 \cdot 1 + 15 \cdot 0 + 12 \cdot 0 + 12 \cdot 0) = \frac{1}{60}(40 + 20) = 1\end{aligned}$$

On en déduit le fait que Y se décompose sous la forme $\mathbf{1} \oplus U \oplus Y'$, où Y′ est de dimension 5 et ne contient pas de composante irréductible isomorphe à $\mathbf{1}$ ou U. Comme les représentations irréductibles restantes sont de dimensions 5, 3 et 3, on voit que Y est irréductible, isomorphe à V, et donc $\chi_V = \chi_Y - \chi_U - \chi_{\mathbf{1}}$.

Remarque : On peut construire géométriquement la représentation W en partant d'un *icosaèdre* (polyèdre régulier à 12 sommets, de chacun desquels partent 5 arètes, et dont les faces, au nombre de 20, sont des triangles équilatéraux). Réciproquement, un travail non négligeable permet de construire à l'intérieur de W un sous-**R**-espace vectoriel W_0 de dimension 3, stable par A_5 (et tel que $W = W_0 \oplus iW_0$). En prenant un produit scalaire sur W invariant sous A_5 (cf. th. I.2.6), cela munit W_0 d'un produit scalaire pour lequel A_5 agit par des isométries (et même par des rotations d'après le (a) de la question 4). En particulier, $t_0 = (12345)$ agit par une rotation d'angle $\pm\frac{2\pi}{5}$, et si f est un vecteur unitaire de l'axe de cette rotation, le stabilisateur de f est le groupe d'ordre 5 engendré par t_0, ce qui fait que f a $60/5 = 12$ translatés sous l'action de A_5. On peut montrer que ces translatés sont les sommets d'un icosaèdre.

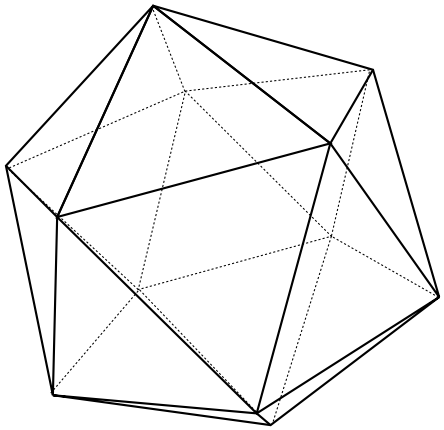


FIGURE 5. L'icosaèdre

De même, si f est un vecteur unitaire de l'axe de la rotation d'angle $\pm\frac{2\pi}{3}$ définie par l'action de (123), alors f a $60/3 = 20$ translatés sous l'action de A_5. On peut montrer que ces translatés sont les sommets d'un *dodécaèdre* (polyèdre régulier à 20 sommets, de chacun desquels partent 3 arètes, et dont les faces, au nombre de 12, sont des pentagones réguliers).

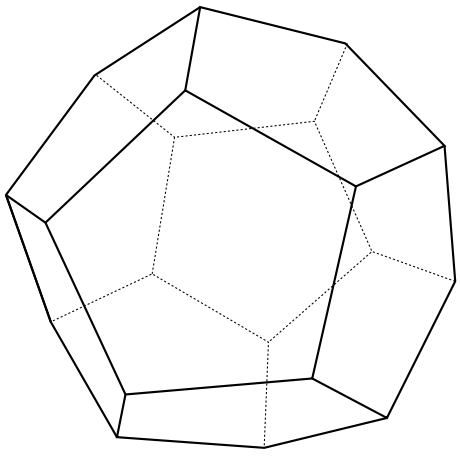


FIGURE 6. Le dodécaèdre

H.3. Représentations de $\mathbf{GL}_2(\mathbf{F}_3)$

Le but de ce devoir est la construction de la table des caractères du groupe $\mathrm{G} = \mathbf{GL}_2(\mathbf{F}_3)$, où $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$ est le corps à 3 éléments (notés généralement 0, 1 et -1) par dévissages [5] successifs du groupe G. Une autre approche est proposée dans l'annexe C.

Le groupe G est un groupe de cardinal [6] 48 qui agit sur le $\mathbf{F}_3$ espace vectoriel $\mathbf{F}_3 \times \mathbf{F}_3$, et comme il agit linéairement, il transforme une droite vectorielle en droite vectorielle ; il agit donc sur l'ensemble $\mathbf{P}^1(\mathbf{F}_3)$ de ces droites qui a 4 éléments : les droites $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ engendrées respectivement par $e_1, e_2, e_1 + e_2, e_1 - e_2$, où e_1, e_2 désigne la base canonique de $\mathbf{F}_3 \times \mathbf{F}_3$ sur $\mathbf{F}_3$. On en déduit un morphisme $\sigma : \mathrm{G} \to \mathrm{S}_4$, défini par $g \cdot \Delta_i = \Delta_{\sigma(g)(i)}$, pour tout $i \in \{1, 2, 3, 4\}$.

	$\mathbf{1}$	ε	θ
1	1	1	2
$(1,2)$	1	-1	0
$(1,2,3)$	1	1	-1

	$\mathbf{1}$	ε	θ	χ_1	χ_2
1	1	1	2	3	3
$(1,2)$	1	-1	0	1	-1
$(1,2)(3,4)$	1	1	2	-1	-1
$(1,2,3)$	1	1	-1	0	0
$(1,2,3,4)$	1	-1	0	-1	1

FIGURE 7. Table des caractères de S_3 et S_4

Nous allons utiliser ce morphisme pour construire la table de G à partir de celle de S_4, que nous admettrons [7].

Si $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{G}$, on note $-g$ l'élément $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$ de G. On définit les éléments suivants de G :

$$\mathrm{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ \mathrm{S} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right),\ \mathrm{D} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right),\ \mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),\ \mathrm{C} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right).$$

Question 1. (i) Soit K un corps et soit $g \in \mathbf{GL}_2(\mathrm{K})$ qui n'est pas une homothétie

(a) Montrer qu'il existe $v \in \mathrm{K}^2$ tel que v et $g(v)$ forment une base de K^2 sur K.

5. Le démarrage de la démonstration de Wiles du théorème de Fermat repose sur les deux petits miracles que constituent l'existence de ces dévissages et celle de la représentation V de G, construite dans le problème, qui est un relèvement en caractéristique 0 de la représentation naturelle de G modulo 3 : elle est de dimension 2, et la réduction modulo 3 de la trace de $\rho_{\mathrm{V}}(g)$ est la trace de g.

6. L'application qui associe à $g \in \mathrm{G}$ ses deux vecteurs colonnes est une bijection de G sur l'ensemble des bases de $\mathbf{F}_3 \times \mathbf{F}_3$ sur $\mathbf{F}_3$. Comme une base est constituée d'un premier vecteur non nul et d'un second n'appartenant pas à la droite engendrée par le premier, on a $|\mathrm{G}| = (9-1)(9-3) = 48$.

7. La méthode utilisée permettrait de construire la table de S_4 à partir de celle de S_3 : on peut faire agir S_4 sur la classe de conjugaison de $(1,2)(3,4)$ qui a 3 éléments, ce qui nous fournit un morphisme surjectif de groupes $\mathrm{S}_4 \to \mathrm{S}_3$, et permet d'obtenir les trois premières colonnes de la table de S_4. On peut, comme au (i) de la question 3, montrer qu'il manque 2 représentations qui sont toutes les deux de dimension 3. Celle V_1 correspondant à χ_1 est obtenue en retirant la représentation triviale à la représentation de permutation associée à l'action de S_4 sur $\{1, 2, 3, 4\}$ (cf. ex. 1.9) ; l'autre est obtenue en tordant V_1 par le caractère linéaire ε qui n'est autre que la signature.

(b) En déduire que la classe de conjugaison de g dans $\mathbf{GL}_2(\mathrm{K})$ est celle de $\left(\begin{smallmatrix} 0 & -\det(g) \\ 1 & \mathrm{Tr}(g) \end{smallmatrix}\right)$.

(ii) Justifier la liste des classes de conjugaison de la table de G ci-dessous (les éléments de Irr(G) sont indexés par des représentations au lieu de leurs caractères).

	$\mathbf{1}$	ε	U	V_1	V_2	W	V	V′
I	1	1	2	3	3	4	2	2
−I	1	1	2	3	3	−4	−2	−2
S	1	−1	0	1	−1	0	0	0
D	1	1	2	−1	−1	0	0	0
T	1	1	−1	0	0	1	−1	−1
−T	1	1	−1	0	0	−1	1	1
C	1	−1	0	−1	1	0	$i\sqrt{2}$	$-i\sqrt{2}$
−C	1	−1	0	−1	1	0	$-i\sqrt{2}$	$i\sqrt{2}$

FIGURE 8. Table des caractères de $\mathbf{GL}_2(\mathbf{F}_3)$

Question 2. (i) Montrer que le noyau de $\sigma : \mathrm{G} \to \mathrm{S}_4$ est $\{\pm\mathrm{I}\}$, et que σ est surjectif.

(ii) Déterminer $\sigma(g)$, pour $g \in \{\mathrm{I}, -\mathrm{I}, \mathrm{S}, \mathrm{D}, \mathrm{T}, -\mathrm{T}, \mathrm{C}, -\mathrm{C}\}$.

(iii) Construire, à partir des représentations de S_4, cinq des représentations irréductibles de G. Quelles colonnes de la table cela permet-il de remplir ?

Question 3. (i) Calculer le nombre et les dimensions des représentations irréductibles manquantes.

(ii) Montrer que, si V est une représentation de G, alors $\mathrm{V}^+ = \{v \in \mathrm{V},\ (-\mathrm{I}) \cdot v = v\}$ et $\mathrm{V}^- = \{v \in \mathrm{V},\ (-\mathrm{I}) \cdot v = -v\}$ sont des sous-représentations de V, et que $\mathrm{V} = \mathrm{V}^+ \oplus \mathrm{V}^-$. En déduire que $-\mathrm{I}$ agit par -1 sur les représentations manquantes.

(iii) Expliquer comment en déduire les 4 premières lignes des 3 colonnes manquantes (on s'intéressera au lien entre $\rho_{\mathrm{V}}(g)$ et $\rho_{\mathrm{V}}(-g)$).

Question 4. Soit X une des représentations de dimension 2 manquantes.

(i) Montrer que $\chi_{\mathrm{X}}(\mathrm{C}) = \pm i\sqrt{2}$ (considérer les valeurs propres de u, u^3 et u^4, où $u = \rho_{\mathrm{X}}(\mathrm{C})$).

(ii) En déduire le lien entre les deux représentations de dimension 2 manquantes, et montrer que l'une des deux (que l'on note V ; l'autre est notée V′) vérifie $\chi_{\mathrm{V}}(\mathrm{C}) = i\sqrt{2}$.

(iii) Montrer que $\mathrm{H} = \{g \in \mathrm{G},\ \chi_{\mathrm{V}}(g) = 2\}$ est un sous-groupe distingué de G ; en déduire que $\chi_{\mathrm{V}}(\mathrm{T}) \neq 2$ (on pourra considérer $\mathrm{STS}^{-1}\mathrm{T}$), puis que $\chi_{\mathrm{V}}(\mathrm{T}) = -1$.

(iv) Expliquer comment compléter la table de G.

Question 5. Calculer le caractère de la représentation de permutation Y associée à l'action de G sur $\mathbf{F}_3 \times \mathbf{F}_3$ et la multiplicité des représentations irréductibles dans la décomposition de Y.

Question 6. Soit $\mathrm{B} \subset \mathrm{G}$ le sous-groupe des matrices triangulaires supérieures et soit $\eta : \mathrm{B} \to \{\pm 1\}$ le caractère linéaire défini par $\eta\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\right) = 1$ si $d = 1$ et $\eta\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\right) = -1$, si $d = -1$.

(i) Calculer $|\mathrm{B}|$.
(ii) Soit $\mathrm{W}' = \mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}}\eta$. Montrer que $\mathrm{W}' \cong \mathrm{W}$ (calculer $\chi_{\mathrm{W}'}(\pm\mathrm{I})$ et le signe de $\chi_{\mathrm{W}'}(\mathrm{T})$).

Question 7. Calculer la multiplicité des représentations irréductibles dans la décomposition de $\mathrm{Z} = \mathrm{W} \otimes \mathrm{W} \otimes \mathrm{W}$.

Corrigé

Question 1. (i) (a) Si $v \neq 0$ et si $(v, g(v))$ n'est pas une base de K^2, c'est que $g(v)$ est un multiple de v. Soit e_1, e_2 la base canonique de K^2. Si $g(e_1) = \lambda_1 e_1$ et $g(e_2) = \lambda_2 e_2$, et si g n'est pas une homothétie, on a $\lambda_2 \neq \lambda_1$, et alors $g(e_1 + e_2)$ n'est pas un multiple de $e_1 + e_2$; on en déduit qu'au moins un des trois vecteurs $e_1, e_2, e_1 + e_2$ est tel que v et $g(v)$ forment une base de K^2 sur K.

(i) (b) Comme g n'est pas une homothétie, il existe $v \in \mathrm{K}^2$ tel que $(v, g(v))$ soit une base de K^2. La matrice de g dans cette base est alors $\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$, dont la trace est b et donc $b = \mathrm{Tr}(g)$, et le déterminant est $-a$ et donc $a = -\det(g)$. On a alors $g = \mathrm{P}\left(\begin{smallmatrix} 0 & -\det(g) \\ 1 & \mathrm{Tr}(g) \end{smallmatrix}\right)\mathrm{P}^{-1}$, où P est la matrice dont les colonnes sont v et $g(v)$, ce qui permet de conclure.

(ii) Les homothéties commutent à tout et donc leur classe de conjugaison n'a qu'un élément. Comme il y a exactement deux homothéties dans G, à savoir I et $-\mathrm{I}$, cela nous fournit déjà deux classes de conjugaison.

Les autres classes sont, d'après le (ii), en bijection avec les valeurs possibles du couple $(\det(g), \mathrm{Tr}(g))$. Or $\det(g)$ peut prendre 2 valeurs (à savoir 1 et -1) puisque $\mathbf{F}_3^*$ a deux éléments et qu'un élément de G a un déterminant non nul, et $\mathrm{Tr}(g)$ peut prendre 3 valeurs. Ce qui nous fournit 6 classes, et on vérifie que les images de S, D, T, $-\mathrm{T}$, C et $-\mathrm{C}$ par $g \mapsto (\det(g), \mathrm{Tr}(g))$ sont respectivement $(-1, 0)$, $(1, 0)$, $(1, -1)$, $(1, -1)$, $(-1, 1)$ et $(-1, -1)$, et donc que l'on a bien un représentant de chaque classe de conjugaison.

Question 2. (i) g est dans le noyau de σ si et seulement si toute droite vectorielle est invariante par g, et donc si et seulement si $g(v)$ est colinéaire à v, pour tout v non nul. D'après le (i) de la question 1, cela implique que g est une homothétie. On en déduit que le noyau de σ est $\{\pm\mathrm{I}\}$. Comme le noyau de σ est de cardinal 2, son image est de cardinal $\frac{1}{2}|\mathrm{G}| = 24 = |\mathrm{S}_4|$, ce qui prouve que σ est surjectif.

(ii) On remarque que $\sigma(-g) = \sigma(g)$ puisque $-\mathrm{I}$ est dans le noyau de σ, et on trouve :
- $\sigma(\mathrm{I}) = \sigma(-\mathrm{I}) = \mathrm{id}$,
- $\sigma(\mathrm{S}) = (1, 2)$,
- $\sigma(\mathrm{D}) = (1, 2)(3, 4)$,
- $\sigma(\mathrm{T}) = \sigma(-\mathrm{T}) = (2, 3, 4)$,
- $\sigma(\mathrm{C}) = \sigma(-\mathrm{C}) = (1, 2, 3, 4)$.

(iii) Comme $\sigma : \mathrm{G} \to \mathrm{S}_4$ est un morphisme de groupes surjectif, l'application $\chi \mapsto \chi \circ \sigma$ induit une injection de l'ensemble des caractères irréductibles de S_4 dans celui des caractères irréductibles de G, ce qui permet, en utilisant la table des caractères de S_4 et le (ii), de remplir les 5 premières colonnes de la table de G.

Question 3. (i) Comme il y a autant de représentations irréductibles que de classes de conjugaison (cor. I.2.13), il manque $8 - 5 = 3$ représentations. Si on note d_1, d_2, d_3 leurs dimensions, la formule de Burnside (cor. I.2.20) implique que $d_1^2 + d_2^2 + d_3^2 + 1^2 + 1^2 + 2^2 + 3^2 + 3^2 = 48$, et donc $d_1^2 + d_2^2 + d_3^2 = 24$. Cette équation n'a qu'une seule solution (à permutation près), à savoir $d_1 = 4$, $d_2 = 2$ et $d_3 = 2$.

(ii) Comme $(-\mathrm{I})^2 = \mathrm{I}$, on a $\rho_{\mathrm{V}}(-\mathrm{I})^2 = 1$, ce qui montre que $\rho_{\mathrm{V}}(-\mathrm{I})$ est une symétrie, et donc que V est la somme directe des espaces propres V^+ et V^- de $\rho_{\mathrm{V}}(-\mathrm{I})$ pour les valeurs propres 1 et -1. Par ailleurs, comme $-\mathrm{I}$ commute à tout élément de G, on a $(-\mathrm{I}) \cdot (g \cdot v) = g \cdot ((-\mathrm{I}) \cdot v) = \lambda\,(g \cdot v)$, si v est

vecteur propre de $\rho_V(-I)$ pour la valeur propre λ ; il en résulte que V^+ et V^- sont stables pour l'action de G et donc sont des sous-représentations de V.

Maintenant, si V est irréductible, on a $V = V^+$ ou $V = V^-$, mais si $V = V^+$, le noyau de σ agit trivialement sur V, ce qui fait que V est une représentation irréductible de S_4 ; elle ne fait donc pas partie des représentations manquantes, ce qui prouve que $-I$ agit par -1 sur les représentations manquantes.

(iii) La première ligne est constituée des dimensions des représentations, d'où les 4, 2, 2. Maintenant, on a $\rho_V(-g) = \rho_V(-I)\rho_V(g) = -\rho_V(g)$, et donc $\chi_V(-g) = -\chi_V(g)$. On en déduit la seconde ligne et la nullité de $\chi_V(S)$ et $\chi_V(D)$ car les classes de conjugaison de S et D sont invariantes par $g \mapsto -g$ car $\mathrm{Tr}(-g) = -\mathrm{Tr}(g)$ et $\det(-g) = \det(g)$.

Question 4. (i) On a $C^3 = \left(\begin{smallmatrix} 1 & -1 \\ -1 & 0 \end{smallmatrix}\right)$ et $C^4 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Notons λ, μ les valeurs propres de u. Comme $C^4 = -I$, on a $u^4 = -1$ et donc $\lambda^4 = \mu^4 = -1$. Maintenant, C^3 est dans la classe de conjugaison de C puisque $\mathrm{Tr}(C^3) = 1 = \mathrm{Tr}(C)$ et $\det(C^3) = -1 = \det(C)$. Si $g \in G$ est tel que $C^3 = gCg^{-1}$, et si $h = \rho_X(g)$, on a $u^3 = huh^{-1}$, et donc u^3 et u ont les mêmes valeurs propres. Comme ces valeurs propres sont des racines 4-ième de -1, on a $\{\lambda, \mu\} = \{e^{i\pi/4}, e^{3i\pi/4}\}$ ou $\{\lambda, \mu\} = \{-e^{i\pi/4}, -e^{3i\pi/4}\}$, et donc $\chi_C(X) = \mathrm{Tr}(u) = \pm(e^{i\pi/4} + e^{3i\pi/4}) = \pm i\sqrt{2}$.

(ii) La représentation $X \otimes \varepsilon$ est une représentation de dimension 2 de G, qui est irréductible puisque X l'est, et distincte de X puisque $\chi_{X\otimes\varepsilon}(C) = \varepsilon(C)\chi_X(C) = -\chi_X(C)$ et $\chi_X(C) \neq 0$. Comme par ailleurs $\varepsilon(-I) = 1$, cela implique que $-I$ agit par -1 sur $X \otimes \varepsilon$, et donc que la seconde représentation manquante de dimension 2 est $X \otimes \varepsilon$. Comme $\{\chi_X(C), \chi_{X\otimes\varepsilon}(C)\} = \{i\sqrt{2}, -i\sqrt{2}\}$, cela permet de conclure.

(iii) Si $g \in G$, alors $\chi_V(g)$ est la somme de deux racines de l'unité, puisque c'est la somme des valeurs propres de $\rho_V(g)$. On a donc $\chi_V(g) = 2$ si et seulement si ces deux valeurs propres sont égales à 1, et donc si et seulement si $\rho_V(g) = 1$ puisque $\rho_V(g)$ est diagonalisable (rem. I.1.7). Autrement dit H est le noyau de ρ_V ; c'est donc un sous-groupe distingué de G.

Si $T \in H$, il en est de même de $STS^{-1}T = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, qui est dans la classe de conjugaison de D, ce qui conduit à une contradiction puisque $\chi_V(D) = 0$; on a donc $\chi_V(T) \neq 2$.

Par ailleurs, $T^3 = 1$, et donc les valeurs propres de $v = \rho_V(T)$ sont des racines 3-ièmes de l'unité. De plus, $T^2 = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ est dans la classe de conjugaison de T et donc v^2 a les mêmes valeurs propres que v, et comme au moins une de ces valeurs propres est différente de 1, ces valeurs propres sont $e^{2i\pi/3}$ et $e^{-2i\pi/3}$, et donc $\chi_V(T) = \mathrm{Tr}(v) = e^{2i\pi/3} + e^{-2i\pi/3} = -1$.

(iv) On complète la septième colonne en utilisant la relation $\chi_V(-g) = -\chi_V(g)$, et la huitième en utilisant la relation $\chi_{V'}(g) = \varepsilon(g)\chi_V(g)$. Enfin, pour compléter la sixième, on peut soit utiliser la décomposition de la régulière (cor. I.2.20), soit l'orthogonalité des lignes de la table des caractères (rem. I.2.32), ce qui, dans le cas présent, revient au même, car on est forcé d'utiliser la première ligne au signe près.

Question 5. Comme Y est une représentation de permutation, $\chi_Y(g)$ est le nombre de points fixes de g, c'est-à-dire $3^{d(g)}$, où $d(g)$ est la dimension de l'espace propre associé à la valeur propre 1. Or 1 est valeur propre si et seulement si $X^2 - \mathrm{Tr}(g)X + \det(g)$ est égal à $(X-1)^2$ ou $(X-1)(X+1)$, et $d(g)$ est alors égal à 1, sauf si $g = I$; on obtient donc :

$$\chi_Y(I) = 9,\ \chi_Y(-I) = 1,\ \chi_Y(S) = 3,\ \chi_Y(D) = 1,\ \chi_Y(T) = 3,\ \chi_Y(-T) = 1,\ \chi_Y(C) = 1,\ \chi_Y(-C) = 1.$$

En comparant les caractères, on en déduit que $Y \cong 2\,\mathbf{1} \oplus V_1 \oplus W$. Il y a des tas de manières d'arriver à ce résultat, s'il ne saute pas aux yeux.

• On peut remarquer que l'action de G sur $\mathbf{F}_3 \times \mathbf{F}_3$ a deux orbites, à savoir $(0,0)$ et le reste, et donc que Y contient deux copies de la représentation triviale, à savoir la droite engendré par $e_{(0,0)}$ et celle engendrée par $\sum_{(x,y)\neq(0,0)} e_{(x,y)}$, ce qui permet de décomposer Y sous la forme $Y \cong 2\,\mathbf{1} \oplus Y'$. Comme $\chi_{Y'}(I) = 7$ et $\chi_{Y'}(-I) = -1$, et comme $\chi_{Y'}(C) = \chi_{Y'}(-C)$, on en déduit que Y' peut se décomposer soit sous la forme $W \oplus Y''$ soit sous la forme $V \oplus V' \oplus Y''$, où Y'' est une représentation de dimension 3 sur

laquelle $-\mathrm{I}$ agit trivialement. On a alors $\chi_{\mathrm{Y}''}(\mathrm{C}) = -1$ et $\chi_{\mathrm{Y}''}(\mathrm{S}) = 1$, et la seule possibilité qui reste est $\mathrm{Y}'' = \mathrm{V}_1$. On élimine alors la possibilité $\mathrm{Y} \cong \mathrm{V} \oplus \mathrm{V}' \oplus \mathrm{Y}''$ en regardant $\chi_{\mathrm{Y}}(\mathrm{T})$.

• Une méthode un peu plus conceptuelle consiste à décomposer Y sous la forme $\mathrm{Y}^+ \oplus \mathrm{Y}^-$, où Y^+ et Y^- sont les sous-espaces propres de $\rho_{\mathrm{Y}}(-\mathrm{I})$ pour les valeurs propres 1 et -1. L'espace Y^+ est engendré par les $e_x + (-\mathrm{I}) \cdot e_x$, pour $x \in \mathbf{F}_3 \times \mathbf{F}_3$, et il se décompose comme la somme directe des deux représentations constituées de la droite Y_0 engendré par $e_{(0,0)}$ et l'espace Y_1 engendré par les f_i, où $f_i = \sum_{x \in \Delta_i} e_x$. La représentation Y_0 est la représentation triviale, la représentation Y_1 est la représentation de permutation induite par l'action de G sur les droites vectorielles (elle correspond à la représentation de permutation de S_4 associée à l'action de S_4 sur $\{1,2,3,4\}$) ; son caractère est $\mathbf{1} + \chi_1$, et on termine en calculant χ_{Y^-} grâce à la formule $\chi_{\mathrm{Y}^-} = \chi_{\mathrm{Y}} - \chi_{\mathrm{Y}^+}$. On peut utiliser cette méthode pour déterminer les composantes isotypiques de Y, ce qui est plus précis que de calculer les multiplicités des représentations irréductibles.

• Une solution moins artisanale consiste à utiliser la formule générale pour la multiplicité (cor. I.2.15), ce qui demande de calculer le cardinal des classes de conjugaison (cela peut se faire en reliant les classes de conjugaison de G à celles de S_4) pour calculer des produits scalaires de caractères.

Question 6. (i) On a $|\mathrm{B}| = 12$ car $g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto (a, d, b)$ induit une bijection de B sur $(\mathbf{F}_3^*)^2 \times \mathbf{F}_3$.

(ii) D'après le th. I.3.11, on a $\chi_{\mathrm{W}'}(g) = \frac{1}{|\mathrm{B}|} \sum_{s \in \mathrm{G},\ sgs^{-1} \in \mathrm{B}} \eta(sgs^{-1})$. Maintenant, $|\mathrm{B}| = 12$, et la formule ci-dessus pour I et $-\mathrm{I}$ nous donne $\chi_{\mathrm{W}'}(\mathrm{I}) = \frac{48}{12} = 4$ et $\chi_{\mathrm{W}'}(-\mathrm{I}) = -4$ puisque I et $-\mathrm{I}$ commutent à tout et appartiennent à B. Il en résulte que W' est de dimension 4 et que $-\mathrm{I}$ agit par -1 sur W' ; on a donc $\mathrm{W}' \cong \mathrm{W}$ ou $\mathrm{W}' \cong \mathrm{Z} \oplus \mathrm{Z}'$, avec $\{\mathrm{Z}, \mathrm{Z}'\} \subset \{\mathrm{V}, \mathrm{V}'\}$.

Par ailleurs, la seule valeur propre de $s\mathrm{T}s^{-1}$ est 1, et donc, si $s\mathrm{T}s^{-1} \in \mathrm{B}$, alors $s\mathrm{T}s^{-1} = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, ce qui fait que $\eta(s\mathrm{T}s^{-1}) \geqslant 0$. On en déduit que $\chi_{\mathrm{W}'}(\mathrm{T}) \geqslant 0$, ce qui ne laisse que la possibilité $\mathrm{W}' \cong \mathrm{W}$.

Question 7. On a $\chi_{\mathrm{Z}}(g) = \chi_{\mathrm{W}}(g)^3$. En particulier, $\chi_{\mathrm{Z}}(-\mathrm{I}) = -\chi_{\mathrm{Z}}(\mathrm{I})$, ce qui fait que $-\mathrm{I}$ agit par -1 sur Z, et donc que $\mathrm{Z} \cong m_{\mathrm{W}}\mathrm{W} \oplus m_{\mathrm{V}}\mathrm{V} \oplus m_{\mathrm{V}'}\mathrm{V}'$, et $\chi_{\mathrm{Z}} = m_{\mathrm{W}}\chi_{\mathrm{W}} + m_{\mathrm{V}}\chi_{\mathrm{V}} + m_{\mathrm{V}'}\chi'_{\mathrm{V}}$. En spécialisant cette identité en C, on obtient $m_{\mathrm{V}} = m_{\mathrm{V}'}$, et en la spécialisant en I et T, on obtient $4m_{\mathrm{W}} + 4m_{\mathrm{V}} = 64$ et $m_{\mathrm{W}} - 2m_{\mathrm{V}} = 1$, et donc $m_{\mathrm{W}} = 11$, $m_{\mathrm{V}} = 5$ et $\mathrm{Z} \cong 11\,\mathrm{W} \oplus 5\,\mathrm{V} \oplus 5\,\mathrm{V}'$.

H.4. Table des caractères de $\mathbf{GL}_3(\mathbf{F}_2)$

Le but de ce devoir est la construction de la table des caractères du groupe $\mathrm{G} = \mathbf{GL}_3(\mathbf{F}_2)$, où $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ est le corps à 2 éléments (on a $1 = -1$ et $2 = 0$ dans ce corps).

	card	Car	Min	ord
C_1	1	$(\mathrm{X}-1)^3$	$\mathrm{X}-1$	1
C_2	21	$(\mathrm{X}-1)^3$	$(\mathrm{X}-1)^2$	2
C_4	42	$(\mathrm{X}-1)^3$	Car	4
C_3	56	X^3-1	Car	3
C_7	24	$\mathrm{X}^3+\mathrm{X}+1$	Car	7
C'_7	24	$\mathrm{X}^3+\mathrm{X}^2+1$	Car	7

	χ_1	χ_3	χ'_3	χ_6	χ_7	χ_8
C_1	1	3	3	6	7	8
C_2	1	-1	-1	2	-1	0
C_4	1	1	1	0	-1	0
C_3	1	0	0	0	1	-1
C_7	1	α	$\overline{\alpha}$	-1	0	1
C'_7	1	$\overline{\alpha}$	α	-1	0	1

FIGURE 9. Classes de conjugaison et table des caractères de $\mathbf{GL}_3(\mathbf{F}_2)$

I. Classes de conjugaison

Si K est un corps (sous-entendu commutatif), et si $\mathrm{A} \in \mathbf{M}_n(\mathrm{K})$, on note $\mathrm{Car}(\mathrm{A})$ le polynôme caractéristique de A et $\mathrm{Min}(\mathrm{A})$ son polynôme minimal [8].

Question 0. Montrer que, si p est premier, le nombre de bases de $\mathbf{F}_p^n$ sur $\mathbf{F}_p$ est $\prod_{i=0}^{n-1}(p^n - p^i)$. En déduire que $|\mathrm{G}| = 168$.

Question 1. Soient K un corps, $\mathrm{P} = \mathrm{X}^3 + a_2\mathrm{X}^2 + a_1\mathrm{X} + a_0 \in \mathrm{K}[\mathrm{X}]$ et X_P l'ensemble des $\mathrm{A} \in \mathbf{M}_3(\mathrm{K})$, avec $\mathrm{Car}(\mathrm{A}) = \mathrm{Min}(\mathrm{A}) = \mathrm{P}$.

(i) Montrer que $\mathrm{A} \in \mathrm{X}_\mathrm{P}$ si et seulement si A est conjuguée à $\left(\begin{smallmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{smallmatrix}\right)$.

(ii) Soit $\mathrm{A} \in \mathrm{X}_\mathrm{P}$. Montrer que $\dim \mathrm{Ker}(\mathrm{A}-1) = 0$ ou 1 suivant que $\mathrm{P}(1) = 0$ ou $\mathrm{P}(1) \neq 0$.

(iii) Que vaut A si $\mathrm{Car}(\mathrm{A}) = (\mathrm{X}-1)^3$ et $\mathrm{Min}(\mathrm{A}) = \mathrm{X}-1$? Que vaut $\dim \mathrm{Ker}(\mathrm{A}-1)$?

(iv) Montrer que $\dim \mathrm{Ker}(\mathrm{A}-1) = 2$, si $\mathrm{Car}(\mathrm{A}) = (\mathrm{X}-1)^3$ et $\mathrm{Min}(\mathrm{A}) = (\mathrm{X}-1)^2$. En déduire qu'alors A est conjuguée à $\left(\begin{smallmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. (On choisira $v \notin \mathrm{Ker}(\mathrm{A}-1)$, et on cherchera une relation entre v, $\mathrm{A}v$ et A^2v.)

Question 2. Quelles sont les valeurs possibles de $\mathrm{Car}(\mathrm{A})$, pour un élément de $\mathrm{G} = \mathbf{GL}_3(\mathbf{F}_2)$. En déduire la liste des classes de conjugaison de G et exhiber un élément de chaque classe.

---

8. On aura à utiliser les résultats suivants.

• Les polynômes $\mathrm{Car}(\mathrm{A})$ et $\mathrm{Min}(\mathrm{A})$ sont invariants par conjugaison par un élément de $\mathbf{GL}_n(\mathrm{A})$ (i.e. $\mathrm{Car}(\mathrm{PAP}^{-1}) = \mathrm{Car}(\mathrm{A})$ et $\mathrm{Min}(\mathrm{PAP}^{-1}) = \mathrm{Min}(\mathrm{A})$, si $\mathrm{P} \in \mathbf{GL}_n(\mathrm{K})$).

• $\mathrm{Car}(\mathrm{A})$ est de degré n, $\mathrm{Min}(\mathrm{A})$ divise $\mathrm{Car}(\mathrm{A})$ (th. de Cayley-Hamilton), et on a $\mathrm{Min}(\mathrm{A}) = \mathrm{Car}(\mathrm{A})$ si $\mathrm{Car}(\mathrm{A})$ n'a pas de facteur avec un exposant $\geqslant 2$ dans sa factorisation en polynômes irréductibles.

• Si $v \in \mathrm{K}^n$, l'ensemble des $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{P}(\mathrm{A}) \cdot v = 0$ est un idéal qui contient $\mathrm{Min}(\mathrm{A})$, et il existe $v \in \mathrm{K}^n$ tel que $\mathrm{Min}(\mathrm{A})$ engendre cet idéal, auquel cas $v, \mathrm{A}v, \ldots, \mathrm{A}^{d-1}v$ forment une famille libre de K^n, si $d = \deg(\mathrm{Min}(\mathrm{A}))$.

Question 3. (i) Calculer l'ordre des différentes classes [9] (on utilisera les factorisations (dans $\mathbf{F}_2[\mathrm{X}]$) $\mathrm{X}^2-1=(\mathrm{X}-1)^2$, $\mathrm{X}^4-1=(\mathrm{X}-1)^4$ et $\mathrm{X}^8-\mathrm{X}=\mathrm{X}(\mathrm{X}-1)(\mathrm{X}^3+\mathrm{X}+1)(\mathrm{X}^3+\mathrm{X}^2+1)$).

(ii) Montrer que $\{g^k,\ g\in \mathrm{C}\}\in \mathrm{Conj}(\mathrm{G})$, si $\mathrm{C}\in\mathrm{Conj}(\mathrm{G})$ et si $k\in\mathbf{Z}$.

(iii) Montrer que C_4 est stable par $g\mapsto g^3$, et que C_3 est stable par $g\mapsto g^2$.

(iv) Montrer que $g\mapsto g^2$ envoie C_4 sur C_2 et $\mathrm{C}_1,\mathrm{C}_2$ sur C_1.

(v) Montrer que C_7 et C_7' sont échangées par $g\mapsto g^{-1}$ et sont stables par $g\mapsto g^2$ (on pourra utiliser la formule $\mathrm{P}(\mathrm{X})^2=\mathrm{P}(\mathrm{X}^2)$ dans $\mathbf{F}_2[\mathrm{X}]$).

Question 4. (i) Montrer que $\mathrm{N}=\left\{\left(\begin{smallmatrix}1&a&b\\0&1&c\\0&0&1\end{smallmatrix}\right),\ a,b,c\in\mathbf{F}_2\right\}$ est un sous-groupe de G inclus dans le centralisateur de $u=\left(\begin{smallmatrix}1&0&1\\0&1&0\\0&0&1\end{smallmatrix}\right)$. En déduire que $|\mathrm{C}_2|$ divise 21 ; que signifierait une égalité ?

(ii) Montrer que $|\mathrm{C}|$ divise $|\mathrm{G}|/n$, si $\mathrm{C}\in\mathrm{Conj}(\mathrm{G})$ est d'ordre n. A quelle condition y a-t-il égalité ?

(iii) Calculer le cardinal de chacune des classes, montrer que le centralisateur d'un élément g de C_3, C_4, C_7 ou C_7' est le sous-groupe de G engendré par g, et que le centralisateur d'un élément de C_2 est de cardinal 8.

II. Table des caractères

Question 0. Soient $\omega=e^{2i\pi/7}$ et $\alpha=\omega+\omega^2+\omega^4$. Calculer $\sum_{i=0}^{6}\omega^i$. En déduire que $\alpha=\frac{-1+i\sqrt{7}}{2}$ (on pourra calculer α^2).

Question 1. Soit V une représentation de G. (On utilisera les résultats de la question 3 du I.)

(i) Montrer que $\chi_{\mathrm{V}}(\mathrm{C}_2)\in\mathbf{Z}$.

(ii) Montrer que les valeurs propres de $\rho_{\mathrm{V}}(\mathrm{C}_4)$, comptées avec multiplicité, sont stables par $\lambda\mapsto\lambda^3$. En déduire que $\chi_{\mathrm{V}}(\mathrm{C}_4)\in\mathbf{Z}$.

(iii) Montrer de même que $\chi_{\mathrm{V}}(\mathrm{C}_3)\in\mathbf{Z}$.

(iv) Montrer qu'il existe des entiers a,b,c tels que $a+3b+3c=\dim\mathrm{V}$ et $\chi_{\mathrm{V}}(\mathrm{C}_7)=a+b\alpha+c\overline{\alpha}$, $\chi_{\mathrm{V}}(\mathrm{C}_7')=a+c\alpha+b\overline{\alpha}$.

Question 2. D'où sort le caractère χ_1 de la table ? On note V_1 la représentation associée.

Question 3. Le groupe G agit sur l'espace vectoriel $\mathbf{F}_2^3$, et cette action préserve l'ensemble X des éléments non nuls de $\mathbf{F}_2^3$. On note V_{X} la représentation de permutation associée.

(i) Calculer le caractère de V_{X}. (Utiliser la question 1 du I.)

(ii) Montrer que l'hyperplan $\mathrm{V}=\{\sum_{x\in\mathrm{X}}\alpha_x e_x,\ \sum_{x\in\mathrm{X}}\alpha_x=0\}$ est stable par G, et calculer le caractère χ de V.

(iii) En déduire que G a une représentation irréductible V_6 de dimension 6 (on note χ_6 son caractère) ; quelle partie de la table cela permet-il de remplir ?

Question 4. Soit W le carré alterné de V_6.

(i) Calculer χ_{W}, $\langle\chi_{\mathrm{W}},\chi_{\mathrm{W}}\rangle$ et $\langle\chi_{\mathrm{W}},\chi_6\rangle$. (Utiliser la question 3 du I.)

(ii) Quelles sont les solutions de $131=a^2+b^2+c^2+d^2$, avec $a\geqslant 8$? En déduire qu'en dehors de V_1 et V_6, le groupe G admet comme représentations irréductibles, une représentation V_8 de dimension 8, une V_7 de dimension 7, et deux $\mathrm{V}_3,\mathrm{V}_3'$ de dimension 3, et que $\mathrm{W}\cong\mathrm{V}_7\oplus\mathrm{V}_8$ (on

9. L'ordre d'une classe de conjugaison est celui de n'importe quel de ses éléments.

note χ_8, χ_7, χ_3 et χ_3' les caractères de ces représentations). Quelle partie de la table cela permet-il de remplir ?

Question 5. (i) Montrer que si χ est le caractère d'une représentation de G, alors $\overline{\chi}$ est aussi le caractère d'une représentation de G. En déduire que Irr(G) est invariant par $\chi \mapsto \overline{\chi}$.

(ii) Montrer que χ_7 est réel.

(iii) Montrer que $|\chi_7(\mathrm{C}_7)| < \sqrt{168/24}$. En déduire que $\chi_7(\mathrm{C}_7) = \chi_7(\mathrm{C}_7') = 0$.

(iv) Que valent $\langle \chi_7, \chi_1 \rangle$, $\langle \chi_7, \chi_6 \rangle$ et $\langle \chi_7, \chi_7 \rangle$? En déduire χ_7, puis χ_8.

Question 6. (i) Soit V une représentation de dimension 3 de G. Montrer que si $\chi_{\mathrm{V}}(\mathrm{C}_7)$ est réel, alors $\chi_{\mathrm{V}}(\mathrm{C}_7) = \chi_{\mathrm{V}}(\mathrm{C}_7') = 3$. En déduire qu'alors V n'est pas irréductible.

(ii) Montrer que $\chi_3' = \overline{\chi}_3$ et expliquer comment compléter la table des caractères.

Question 7. G agit par conjugaison sur C_7 ; soit Y la représentation de permutation associée.

(i) Montrer, en utilisant la question 4 (iii) du I, que $g \neq 1$ est dans le centralisateur de $h \in \mathrm{C}_7$ si et seulement si h est une puissance de g.

(ii) Calculer χ_{Y} et en déduire que $\mathrm{Y} \cong \mathrm{V}_1 \oplus \mathrm{V}_7 \oplus 2\mathrm{V}_8$.

(iii) Construire des sous-représentations $\mathrm{W}_1, \mathrm{W}_7, \mathrm{W}_8, \mathrm{W}_8'$ de Y telles que $\mathrm{Y} = \mathrm{W}_1 \oplus \mathrm{W}_7 \oplus \mathrm{W}_8 \oplus \mathrm{W}_8'$. (On pourra considérer les $f_{g,\beta} = e_g + \beta e_{g^2} + \beta^2 e_{g^4}$, pour $g \in \mathrm{C}_7$ et $\beta \in \{1, j, j^2\}$, où $j = e^{2i\pi/3}$.)

Question 8. Montrer, grâce à la table des caractères, que G est simple [10]. (Considérer une représentation de G obtenue à partir d'une représentation irréductible d'un quotient de G, si G n'était pas simple.)

Corrigé

I. Classes de conjugaison

Question 0. Si K est un corps, une base de K^n sur K est constituée d'un premier vecteur e_1 non nul, d'un second vecteur e_2 pas dans la droite engendrée par e_1, d'un troisième e_3 pas dans le plan engendré par e_1, e_2, etc. Si $|\mathrm{K}| = q$, il y a donc $q^n - 1$ choix pour e_1, $q^n - q$ pour e_2, $q^n - q^2$ pour e_3, etc., soit au total $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$ bases.

Maintenant, l'application qui envoie une matrice $\mathrm{A} \in \mathbf{GL}_n(\mathrm{K})$ sur ses n vecteurs colonnes est une bijection de $\mathbf{GL}_n(\mathrm{K})$ sur l'ensemble des bases de K^n ; le cardinal de $\mathbf{GL}_n(\mathrm{K})$ est donc $\prod_{i=0}^{n-1}(q^n - q^i)$. Dans le cas qui nous intéresse, on a $n = 3$ et $q = 2$, ce qui nous donne $|\mathrm{G}| = (8-1)(8-2)(8-4) = 168$.

Question 1. (i) Comme Min(A) est de degré 3, il existe v tel que v, $\mathrm{A}v$ et A^2v forment une base de K^3. De plus, $\mathrm{Min}(\mathrm{A}) \cdot v = 0$ et donc $\mathrm{A} \cdot (\mathrm{A}^2 v) = -a_2\mathrm{A}^2v - a_1\mathrm{A}v - a_0 v$. On en déduit que $\mathrm{U}^{-1}\mathrm{AU} = \mathrm{B}$, avec $\mathrm{B} = \left(\begin{smallmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{smallmatrix}\right)$, si $\mathrm{U} \in \mathbf{GL}_3(\mathrm{K})$ est la matrice dont les colonnes sont v, $\mathrm{A}v$ et A^2v.

Réciproquement, si A est conjugué à B, alors $\mathrm{Car}(\mathrm{A}) = \mathrm{Car}(\mathrm{B})$ et $\mathrm{Min}(\mathrm{A}) = \mathrm{Min}(\mathrm{B})$. Maintenant, on obtient $\mathrm{Car}(\mathrm{B}) = (\mathrm{X}+a_2)\mathrm{X}^2 - a_1(-\mathrm{X}) + a_0 = \mathrm{P}$, en développant $\left|\begin{smallmatrix} \mathrm{X} & 0 & a_0 \\ -1 & \mathrm{X} & a_1 \\ 0 & -1 & \mathrm{X}+a_2 \end{smallmatrix}\right|$ par rapport à la dernière colonne. Enfin, si on note e_1, e_2, e_3 la base canonique de K^3, on a $\mathrm{B}e_1 = e_2$ et $\mathrm{B}^2 e_1 = e_3$, ce qui fait que

10. C'est le plus petit groupe simple non commutatif après A_5 (qui est de cardinal 60) ; il est aussi isomorphe à $\mathbf{PSL}_2(\mathbf{F}_7) = \mathbf{SL}_2(\mathbf{F}_7)/\{\pm 1\}$, mais il faut se fatiguer un peu pour construire un tel isomorphisme.

e_1, Be_1, B^2e_1 forment une famille libre et qu'un polynôme non nul vérifiant $Q(B)\cdot e_1 = 0$ est de degré $\geqslant 3$. Il en résulte que Min(B) est de degré $\geqslant 3$, et comme il divise Car(B), on a Min(B) = Car(B) = P, ce qui permet de conclure.

(ii) Soit v tel que v, Av et A^2v forment une base de K^3. Comme $A^3v = -a_0v - a_1Av - a_2A^2v$, on obtient $(A-1)(x_0v + x_1Av + x_2A^2v) = (-a_0x_2 - x_0)v + (x_0 - a_1x_2 - x_1)Av + A^2(x_1 - a_2x_2 - x_2)$. Il en résulte que Ker(A − 1) est l'ensemble des $x_0v + x_1Av + x_2A^2v$ vérifiant $x_0 = -a_0x_2$, $x_1 = -(a_0 + a_1)x_2$ et $x_2(a_2 + a_0 + a_1 + 1) = 0$, et comme $a_2 + a_0 + a_1 + 1 = P(1)$, on voit que cet espace est de dimension 0, si $P(1) \neq 0$ et de dimension 1, si $P(1) = 0$.

(iii) Si Min(A) = X − 1, on a A = 1 et donc Ker (A − 1) est de dimension 3.

(iv) Si $(A-1)^2 = 0$, on a Im(A − 1) ⊂ Ker(A − 1) et comme dim(Im(A − 1)) + dim(Ker(A − 1)) = 3, cela implique dim(Ker(A − 1)) $\geqslant 2$. On en déduit que Ker (A − 1) est de dimension 2, car A ≠ 1, et donc dim(Ker(A − 1)) < 3.

Si $v \notin \mathrm{Ker}(A-1)$, alors v et Av forment une famille libre car 1 est la seule valeur propre. En particulier, v n'appartient pas à Ker(A − 1), et donc le plan engendré par v et Av n'est pas égal à Ker(A − 1), ce qui permet de compléter v et Av par un élément w de Ker(A − 1), pour obtenir une base de K^3. Par ailleurs, on a $(A-1)^2v = 0$, et donc $A\cdot(Av) = -v + 2Av$. Il en résulte que, si on note $U \in \mathbf{GL}_3(K)$ la matrice dont les colonnes sont v, Av et w, alors $U^{-1}AU = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, ce qui permet de conclure.

Question 2. Comme le terme constant du polynôme caractéristique est le déterminant, il est non nul si et seulement si la matrice est inversible. Il y a donc 4 polynômes caractéristiques possibles pour un élément de G, à savoir $X^3+1 = X^3-1 = (X-1)(X^2+X+1)$, X^3+X+1, X^3+X^2+1 et $X^3+X^2+X+1 = (X-1)^3$.

• Si Car(A) = $X^3 + 1 = X^3 - 1$, on a Min(A) = $X^3 + 1$ car $X^3 + 1$ n'a pas de facteur multiple, et donc A est conjuguée à $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, d'après le (i) de la Question 1.

• De même, si Car(A) = $X^3 + X + 1$, alors A est conjuguée à $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

• De même, si Car(A) = $X^3 + X^2 + 1$, alors A est conjuguée à $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

• Si Car(A) = $(X - 1)^3$, il y a trois possibilités pour Min(A).

— Si Min(A) = (X − 1), on a A = $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

— Si Min(A) = $(X - 1)^2$, alors A est conjuguée à $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, d'après le (iii) de la Question 1.

— Si Min(A) = $(X - 1)^3$, alors A est conjuguée à $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, d'après le (i) de la Question 1.

Comme Car(A) et Min(A) sont invariants par conjugaison, la discussion précédente montre que les classes de conjugaison sont en bijection avec les couples (Car(A), Min(A)) possibles. On obtient donc les classes C_1, C_2, C_4, C_3, C_7 et C_7' de la table, avec pour représentants respectifs :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Question 3. (i) • C_1 est réduit à l'élément neutre qui est d'ordre 1.

• Comme $(X-1)^2 = X^2 - 1$ dans $\mathbf{F}_2[X]$, l'ordre d'un élément de C_2 divise 2, et comme ce n'est pas 1, c'est 2.

• Comme $(X-1)^3$ divise X^4-1 dans $\mathbf{F}_2[X]$, l'ordre d'un élément A de C_4 divise 4, et comme $A^2-1 \neq 0$, puisque le polynôme minimal de A est $(X - 1)^3$, l'ordre de A est 4.

• Comme les éléments de C_3 sont annulés par $X^3 - 1$, ils sont d'ordre divisant 3 et donc d'ordre 3.

• Comme $X^3 + X + 1$ et $X^3 + X^2 + 1$ divisent $X^7 - 1$ dans $\mathbf{F}_2[X]$, l'ordre d'un élément de C_7 ou C_7' divise 7, et donc est 7.

(ii) Soit $g_0 \in C$. Alors $C = \{hg_0h^{-1},\ h \in G\}$, et comme $(hg_0h^{-1})^k = hg_0^kh^{-1}$, on en déduit que $\{g^k,\ g \in C\}$ est la classe de conjugaison de g_0^k.

(iii) Si g est d'ordre 4, alors g^3 est d'ordre 4. On en déduit que $g \mapsto g^3$ envoie C_4 sur une classe de conjugaison constituée d'éléments d'ordre 4, et comme il n'y en a qu'une, à savoir C_4, cela prouve que $g \mapsto g^3$ laisse stable C_4. Le raisonnement est le même pour C_3 qui est la seule classe constituée d'éléments d'ordre 3 et donc est stable par $g \mapsto g^2$.

(iv) Le résultat suit de ce que g^2 est d'ordre de 2, si g est d'ordre 4, et d'ordre 1, si g est d'ordre 1 ou 2, et de ce qu'il n'existe qu'une seule classe d'ordre 1 ou 2.

(v) Si $A \in \mathbf{GL}_n(K)$, et si $\mathrm{Car}(A) = P$, le polynôme caractéristique de A^{-1} est donné par $\mathrm{Car}(A^{-1}) = \det(A^{-1} - X) = (\det A^{-1})X^n \det(X^{-1} - A) = (\det A)^{-1}X^n P(X^{-1})$. Cette formule montre que le polynôme caractéristique de g^{-1} est $X^3 + X + 1$ si celui de g est $X^3 + X^2 + 1$, et réciproquement. Les classes C_7 et C_7' sont donc échangées par $g \mapsto g^{-1}$.

Si $P(A) = 0$, on a $P(A)^2 = 0$, et comme on travaille dans $\mathbf{F}_2$, on a $P(A)^2 = P(A^2)$, ce qui prouve que le polynôme minimal de A^2 divise celui de A. Dans le cas de C_7 et C_7', ces polynômes sont irréductibles, et la divisibilité implique l'égalité, ce qui prouve que C_7 et C_7' sont stables par $g \mapsto g^2$.

Question 4. (i) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$. Il est apparent sur cette formule que N est stable par multiplication et donc est un sous-groupe du groupe fini G, et que tout élément de N commute à u.

Maintenant, C_2 est la classe de u, puisque C_2 contient tous les éléments d'ordre 2. Donc $|C_2| = |G|/|Z_u|$, si Z_u est le centralisateur de u. Or Z_u contient N et donc $|Z_u|$ est un multiple de $|N| = 8$. Il en résulte que $|C_2|$ divise $|G|/8 = 21$, avec égalité si et seulement si $|Z_u| = 8$.

(ii) Soit $g \in C$. Si C est d'ordre n, alors le sous-groupe engendré par g est de cardinal n. Comme il est inclus dans le centralisateur Z_g de g, on a $n \mid |Z_g|$, et comme $|C| = |G|/|Z_g|$, on voit que $|C|$ divise $|G|/n$, avec égalité si et seulement si Z_g est engendré par g.

(iii) On a $|C_1| = 1$, et il ressort des (i) et (ii) que $|C_2|$ divise 21, que $|C_4|$ divise $168/4 = 42$, que $|C_3|$ divise $168/3 = 56$, et que $|C_7|$ et $|C_7'|$ divisent $168/7 = 24$. Comme $168 = |G| = |C_1| + |C_2| + |C_4| + |C_3| + |C_7| + |C_7'|$, et comme $1 + 21 + 42 + 56 + 24 + 24 = 168$, toutes les divisibilités précédentes sont des égalités. On en déduit le résultat.

II. Table des caractères

Question 0. On a $\sum_{i=0}^{6} \omega^i = \frac{\omega^7 - 1}{\omega - 1} = 0$. On en déduit que

$$\alpha^2 = \omega^2 + \omega^4 + \omega + 2\omega^3 + 2\omega^5 + 2\omega^7 = -2 - \alpha.$$

On a donc $\alpha = \frac{-1 \pm i\sqrt{7}}{2}$, et comme $\mathrm{Im}(\alpha) = \sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7} > 0$, cela permet de conclure.

Question 1. (i) $\chi_V(g)$ est la somme des valeurs propres de $\rho_V(g)$, comptées avec multiplicité, et comme $\rho_V(g)^2 = \rho_V(g^2) = 1$, si $g \in C_2$, ces valeurs propres sont ± 1, et sont donc des entiers, ce qui permet de conclure.

(ii) Soit $g \in C_4$. Il résulte de la question 3 (iii) du I, que $g^3 \in C_4$ et donc qu'il existe $h \in G$ tel que $g^3 = hgh^{-1}$. On a alors $\rho_V(g)^3 = \rho_V(g^3) = \rho_V(hgh^{-1}) = u\rho_V(g)u^{-1}$, où $u = \rho_V(h)$. Il s'ensuit que $\rho_V(g)^3$ et $\rho_V(g)$ sont conjugués et donc qu'ils ont les mêmes valeurs propres avec les mêmes multiplicités. Comme les valeurs propres de $\rho_V(g)^3$ sont obtenues en élevant au cube celles de $\rho_V(g)$, cela prouve que les valeurs propres de $\rho_V(g)$, comptées avec multiplicité, sont stables par $\lambda \mapsto \lambda^3$.

Maintenant, comme g est d'ordre 4, les valeurs propres de $\rho_V(g)$ appartiennent à $\{1, -1, i, -i\}$. Notons a, b, c et d leurs multiplicités respectives. Comme $i^3 = -i$, on a $c = d$ d'après ce qui précède, et donc $\chi_V(g) = a + b(-1) + ci + d(-i) = a - b \in \mathbf{Z}$, ce qu'il fallait démontrer.

(iii) Les valeurs propres de $\rho_V(g)$ appartiennent à $\{1, j, j^2\}$, où $j = e^{2i\pi/3}$ et comme g est conjugué à g^2 d'après la question 3 (iii) du I, on en déduit, comme ci-dessus, que les multiplicités de j et j^2 sont les mêmes, et comme $j + j^2 = -1 \in \mathbf{Z}$, cela permet de conclure.

(iv) Soit $g \in \mathrm{C}_7$. Comme g est d'ordre 7, les valeurs propres de $\rho_\mathrm{V}(g)$ appartiennent à $\{\omega^i,\ 0 \leqslant i \leqslant 6\}$. De plus, comme C_7 est stable par $g \mapsto g^2$, la multiplicité de ω est la même que celles de ω^2 et ω^4 et celle de $\omega^{-1} = \omega^6$ est la même que celles de $\omega^{-2} = \omega^5$ et $\omega^{-4} = \omega^3$. Si on note a la multiplicité de 1, b celle de ω et c celle de ω^{-1}, on a alors $a+3b+3c = \dim \mathrm{V}$ et $\chi_\mathrm{V}(\mathrm{C}_7) = \chi_\mathrm{V}(g) = a+b(\omega+\omega^2+\omega^4)+c(\omega^{-1}+\omega^{-2}+\omega^{-4}) = a + b\alpha + c\overline{\alpha}$. Enfin, comme $g^{-1} \in \mathrm{C}_7'$, et comme les valeurs propres de $\rho_\mathrm{V}(g^{-1})$ sont les inverses de celles de $\rho_\mathrm{V}(g)$, on a $\chi_\mathrm{V}(\mathrm{C}_7') = \chi_\mathrm{V}(g^{-1}) = a + b\overline{\alpha} + c\alpha$.

Question 2. Le caractère χ_1 est le caractère de la représentation triviale.

Question 3. (i) Comme $\mathrm{V_X}$ est une représentation de permutation, $\chi_{\mathrm{V_X}}(g)$ est le nombre de points fixes de g, et comme les points fixes de g sont l'espace propre pour la valeur 1 privé de l'origine, on a $\chi_{\mathrm{V_X}}(g) = 0$ si cet espace propre est nul, $\chi_{\mathrm{V_X}}(g) = 1$ s'il est de dimension 1, $\chi_{\mathrm{V_X}}(g) = 3$ s'il est de dimension 2, et $\chi_{\mathrm{V_X}}(g) = 7$ s'il est de dimension 3. On obtient donc :

- $\chi_{\mathrm{V_X}}(\mathrm{C}_7) = \chi_{\mathrm{V_X}}(\mathrm{C}_7') = 0$ puisque 1 n'est pas racine du polynôme caractéristique.
- $\chi_{\mathrm{V_X}}(\mathrm{C}_3) = 1$, d'après la question 2 (ii) du I.
- $\chi_{\mathrm{V_X}}(\mathrm{C}_1) = 7$, $\chi_{\mathrm{V_X}}(\mathrm{C}_2) = 3$ et $\chi_{\mathrm{V_X}}(\mathrm{C}_4) = 1$, d'après les (iii), (iv) et (ii) de la question 2 du I.

(ii) $g \cdot \sum_{x\in\mathrm{X}} \alpha_x e_x = \sum_{x\in\mathrm{X}} \alpha_x e_{g\cdot x} = \sum_{x\in\mathrm{X}} \alpha_{g^{-1}\cdot x} e_x$, et comme $x \mapsto g^{-1}\cdot x$ est une bijection de X, on a $\sum_{x\in\mathrm{X}} \alpha_{g^{-1}\cdot x} = \sum_{x\in\mathrm{X}} \alpha_x$. On en déduit la stabilité de l'hyperplan $\mathrm{V} = \{\sum_{x\in\mathrm{X}} \alpha_x e_x,\ \sum_{x\in\mathrm{X}} \alpha_x\}$.

La droite Δ engendrée par $\sum_{x\in\mathrm{X}} e_x$ est fixe par G, et donc fournit une sous-représentation de $\mathrm{V_X}$ dont le caractère est χ_1. Comme $\mathrm{V_X} = \Delta \oplus \mathrm{V}$, on a $\chi_\mathrm{V} = \chi_{\mathrm{V_X}} - \chi_1$, ce qui nous donne $\chi_\mathrm{V}(\mathrm{C}_1) = 6$, $\chi_\mathrm{V}(\mathrm{C}_2) = 3$, $\chi_\mathrm{V}(\mathrm{C}_4) = 0$, $\chi_\mathrm{V}(\mathrm{C}_3) = 0$, $\chi_\mathrm{V}(\mathrm{C}_7) = \chi_\mathrm{V}(\mathrm{C}_7') = -1$.

(iii) $\langle \chi_\mathrm{V}, \chi_\mathrm{V}\rangle = \frac{1}{168}(6^2 + 21\cdot 2^2 + 42\cdot 0^2 + 56\cdot 0^2 + 24\cdot(-1)^2 + 24\cdot(-1)^2) = 1$, ce qui prouve que V est une représentation irréductible, et comme $\chi_\mathrm{V}(\mathrm{C}_1) = 6$, elle est de dimension 6. Cela permet de remplir la colonne de la table correspondant à χ_6.

Question 4. (i) On a $\chi_\mathrm{W}(g) = \frac{1}{2}(\chi_6(g)^2 - \chi_6(g^2))$. On en déduit, en utilisant les (iii), (iv) et (v) de la question 3 du I, que

$$\chi_\mathrm{W}(\mathrm{C}_1) = \frac{1}{2}(\chi_6(\mathrm{C}_1)^2 - \chi_6(\mathrm{C}_1)) = 15, \quad \chi_\mathrm{W}(\mathrm{C}_2) = \frac{1}{2}(\chi_6(\mathrm{C}_2)^2 - \chi_6(\mathrm{C}_1)) = -1,$$
$$\chi_\mathrm{W}(\mathrm{C}_4) = \frac{1}{2}(\chi_6(\mathrm{C}_4)^2 - \chi_6(\mathrm{C}_2)) = -1 \quad \chi_\mathrm{W}(\mathrm{C}_3) = \frac{1}{2}(\chi_6(\mathrm{C}_3)^2 - \chi_6(\mathrm{C}_3)) = 0,$$
$$\chi_\mathrm{W}(\mathrm{C}_7) = \frac{1}{2}(\chi_6(\mathrm{C}_7)^2 - \chi_6(\mathrm{C}_7)) = 1, \quad \chi_\mathrm{W}(\mathrm{C}_7') = \frac{1}{2}(\chi_6(\mathrm{C}_7')^2 - \chi_6(\mathrm{C}_7')) = 1.$$

On obtient donc $\langle \chi_\mathrm{W}, \chi_\mathrm{W}\rangle = \frac{1}{168}(15^2 + 21\cdot(-1)^2 + 42\cdot(-1)^2 + 56\cdot 0^2 + 24\cdot 1^2 + 24\cdot 1^2) = 2$, ainsi que $\langle \chi_\mathrm{W}, \chi_6\rangle = \frac{1}{168}(15\cdot 6 + 21\cdot(-1)\cdot 2 + 42\cdot(-1)\cdot 0 + 56\cdot 0^2 + 24\cdot 1\cdot(-1) + 24\cdot 1\cdot(-1)) = 0$.

(ii) Il résulte de la question précédente que W est somme de deux représentations irréductibles dont la somme des dimensions est 15, et qui ne sont pas isomorphes à V_6 ; en particulier, G a une représentation irréductible de dimension $\geqslant 8$.

Par ailleurs, comme G a 6 classes de conjugaison, il a quatre autres représentations irréductibles que V_1 et V_6. Si on note a, b, c, d leurs dimensions, il résulte de la formule de Burnside que l'on a $a^2 + b^2 + c^2 + d^2 = 168 - 1^2 - 6^2 = 131$. Les seules solutions de cette équation avec $a \geqslant 8$ sont $131 = 9^2 + 5^2 + 4^2 + 3^2$ et $131 = 8^2 + 7^2 + 3^2 + 3^2$.

La première de ces solutions est exclue car elle imposerait à W d'être la somme de V_6 et d'une représentation de dimension 9, et V_6 ne fait pas partie des composantes irréductibles de W. On est donc dans le second cas, ce qui permet de conclure.

Question 5. (i) Soient χ le caractère d'une représentation de G, et $\rho : \mathrm{G} \to \mathbf{GL}_n(\mathbf{C})$ un morphisme de groupes dont la représentation associée a χ pour caractère. Alors $\overline{\rho}$, défini en prenant les conjugués des coefficients de $\rho(g)$, est aussi un morphisme de groupes, et le caractère de la représentation associée

est $\overline{\chi}$ puisque $\mathrm{Tr}(\overline{\rho}(g)) = \overline{\mathrm{Tr}(\rho(g))}$ (on aurait aussi pu prendre la représentation duale). Maintenant, on a $\langle\overline{\chi},\overline{\chi}\rangle = \langle\chi,\chi\rangle$, et donc $\langle\overline{\chi},\overline{\chi}\rangle = 1$ si et seulement si $\langle\chi,\chi\rangle = 1$, ce qui prouve que $\overline{\chi} \in \mathrm{Irr(G)}$ si et seulement si $\chi \in \mathrm{Irr(G)}$. Ceci permet de conclure.

(ii) Comme il y a une seule représentation de dimension 7, on a $\overline{\chi}_7 = \chi_7$, et donc χ_7 est réel.

(iii) On a $1 = \langle\overline{\chi}_7,\overline{\chi}_7\rangle > \frac{24}{168}|\chi_7(\mathrm{C}_7)|^2$, et donc $|\chi_7(\mathrm{C}_7)| < \sqrt{168/24} < 7$. Par ailleurs (question 1 (iv)), il existe des entiers a, b, c vérifiant $a + 3b + 3c = 7$ et $a + b\alpha + c\overline{\alpha} = \chi_7(\mathrm{C}_7)$. Comme $\chi_7(\mathrm{C}_7) \in \mathbf{R}$, cela implique que $b = c$. On a donc deux possibilité : soit $a = 7$, $b = c = 0$, et $\chi_7(\mathrm{C}_7) = 7$, ce qui est contraire à l'inégalité $|\chi_7(\mathrm{C}_7)| < 7$, soit $a = b = c = 1$ et alors $\chi_7(\mathrm{C}'_7) = \chi_7(\mathrm{C}_7) = 1 + \alpha + \overline{\alpha} = \sum_{i=0}^{6} \omega^i = 0$.

(iv) Les relations d'orthonormalité des caractères impliquent $\langle\chi_7,\chi_1\rangle = 0$, $\langle\chi_7,\chi_6\rangle = 0$ et $\langle\chi_7,\chi_7\rangle = 1$. En posant $a = \chi_7(\mathrm{C}_2)$, $b = \chi_7(\mathrm{C}_4)$ et $c = \chi_7(\mathrm{C}_3)$, et en utilisant le fait que $\chi_7(\mathrm{C}_1) = \dim \mathrm{V}_7 = 7$, on en déduit les relations $7 + 21a + 42b + 56c = 0$, $42 + 21 \cdot 2a = 0$ et $7^2 + 21a^2 + 42b^2 + 56c^2 = 168$. D'où $a = -1$, $3b + 4c = 1$ et $3b^2 + 4b^2 = 7$. Comme b et c sont des entiers, cela nous donne $b = -1$ et $c = 1$, ce qui permet de remplir la colonne de χ_7.

On détermine χ_8 à partir de la formule $\chi_8 = \chi_{\mathrm{W}} - \chi_7$.

Question 6. (i) D'après la question 1 (iv), il existe des entiers a, b, c vérifiant $a + 3b + 3c = 3$ et $a + b\alpha + c\overline{\alpha} = \chi_{\mathrm{V}}(\mathrm{C}_7)$. Si $\chi_{\mathrm{V}}(\mathrm{C}_7)$ est réel, on a $b = c$, ce qui implique que $b = c = 0$ et donc $a = 3$. On a alors $\chi_{\mathrm{V}}(\mathrm{C}'_7) = a + b\overline{\alpha} + c\alpha = 3$. On en déduit que $\langle\chi_{\mathrm{V}},\chi_{\mathrm{V}}\rangle \geqslant \frac{1}{168}(24 \cdot 3^2 + 24 \cdot 3^2) > 1$, ce qui prouve que V n'est pas irréductible.

(ii) Il résulte de la proposition précédente que χ_3 n'est pas réel, et donc $\overline{\chi}_3 \neq \chi_3$. Comme le seul autre caractère de degré 3 de G est χ'_3, on a $\chi'_3 = \overline{\chi}_3$. De plus, comme $\chi_3(\mathrm{C}_7)$ n'est pas réel, on a $\chi_3(\mathrm{C}_7) \in \{\alpha, \overline{\alpha}\}$ et, quitte à remplacer χ_3 par son conjugué, on peut imposer que $\chi_3(\mathrm{C}_7) = \alpha$. On a alors $\chi_3(\mathrm{C}'_7) = \overline{\alpha}$, $\chi'_3(\mathrm{C}_7) = \overline{\alpha}$ et $\chi'_3(\mathrm{C}'_7) = \alpha$.

Par ailleurs, $\chi_3(\mathrm{C}_1)$, $\chi_3(\mathrm{C}_2)$, $\chi_3(\mathrm{C}_4)$ et $\chi_3(\mathrm{C}_3)$ sont réels, puisque entiers. On a donc $\chi_3(\mathrm{C}_1) = \chi'_3(\mathrm{C}_1)$, $\chi_3(\mathrm{C}_2) = \chi'_3(\mathrm{C}_2)$, $\chi_3(\mathrm{C}_4) = \chi'_3(\mathrm{C}_4)$ et $\chi_3(\mathrm{C}_3) = \chi'_3(\mathrm{C}_3)$. On termine de remplir la table en utilisant le fait que $\chi_1 + 3\chi_3 + 3\chi'_3 + 6\chi_6 + 7\chi_7 + 8\chi_8$ est le caractère de la régulière.

Question 7. (i) D'après la question 4 (v) du I, le centralisateur de h est le sous-groupe engendré par h, qui est isomorphe à $\mathbf{Z}/7\mathbf{Z}$. Il en résulte que tout élément $g \neq 1$ de ce centralisateur, en est un générateur, et donc que h est une puissance de g, si $g \neq 1$ est dans le centralisateur de h. La réciproque étant évidente, cela permet de conclure.

(ii) Comme Y est une représentation de permutation, $\chi_{\mathrm{Y}}(g)$ est le nombre de points fixes de g. Or $ghg^{-1} = h$ si et seulement si g est dans le centralisateur de h.

Si $g = 1$, c'est toujours le cas, et on a $\chi_{\mathrm{Y}}(\mathrm{C}_1) = |\mathrm{C}_7| = 24$.

Si $g \neq 1$, il résulte du (i) que c'est le cas si et seulement si h est une puissance de g. Autrement dit, on est amené à compter le nombre de puissances de g appartenant à C_7, ce qui nous donne :

• $\chi_{\mathrm{Y}}(\mathrm{C}_2) = \chi_{\mathrm{Y}}(\mathrm{C}_4) = \chi_{\mathrm{Y}}(\mathrm{C}_3) = 0$ car un élément d'ordre 2, 3 ou 4 ne peut pas être la puissance d'un élément d'ordre 7,

• $\chi_{\mathrm{Y}}(\mathrm{C}_7) = 3$ (g, g^2, $g^4 \in \mathrm{C}_7$, si $g \in \mathrm{C}_7$) et $\chi_{\mathrm{Y}}(\mathrm{C}'_7) = 3$ (g^{-1}, g^{-2}, $g^{-4} \in \mathrm{C}_7$, si $g \in \mathrm{C}'_7$).

On a $\chi_{\mathrm{Y}} = \chi_1 + \chi_7 + 2\chi_8$, ce qui prouve que Y est isomorphe à $\mathrm{V}_1 \oplus \mathrm{V}_7 \oplus 2\mathrm{V}_8$.

(iii) Les vecteurs $f_{x,\beta}$, $f_{x^2,\beta}$ et $f_{x^4,\beta}$ sont colinéaires, et on a $g \cdot f_{x,\beta} = f_{gxg^{-1},\beta}$. Il en résulte que l'espace Y_β engendré par les $f_{x,\beta}$, pour $x \in \mathrm{C}_7$, est un espace de dimension $\leqslant 8$, stable par G. De plus, l'espace engendré par $f_{x,\beta}$, $f_{x^2,\beta}$ et $f_{x^4,\beta}$ est le même que celui engendré par e_x, e_{x^2} et e_{x^4}. On en déduit que $\mathrm{Y} = \mathrm{Y}_1 + \mathrm{Y}_j + \mathrm{Y}_{j^2}$, et donc, pour des raisons de dimension, que $\mathrm{Y} = \mathrm{Y}_1 \oplus \mathrm{Y}_j \oplus \mathrm{Y}_{j^2}$.

Maintenant, Y_1 peut se décomposer comme la somme directe de la droite W_1 engendrée par $\sum_{x\in\mathrm{C}_7} e_x$ et de l'intersection W_7 de Y_1 avec l'hyperplan des $\sum_{x\in\mathrm{C}_7} \alpha_x e_x$ avec $\sum_{x\in\mathrm{C}_7} \alpha_x = 0$, qui sont stables par

G pour les raisons habituelles. En posant $\mathrm{Y}_j = \mathrm{W}_8$ et $\mathrm{Y}_{j^2} = \mathrm{W}'_8$, cela nous fournit la décomposition de Y cherchée.

Question 8. Soit H un sous-groupe distingué de G, distinct de G. Si on note G' le quotient G/H, et si V est une représentation irréductible non triviale de G', alors V peut aussi être vue comme une représentation de G en faisant agir $g \in \mathrm{G}$ par son image dans G'. Cette représentation est irréductible puisque l'ensemble des $g \cdot v$, pour $g \in \mathrm{G}$, est celui des $g' \cdot v$, pour $g' \in \mathrm{G}'$, et que cet ensemble engendre V, pour tout $v \neq 0$. Le caractère χ_{V} prend la valeur $\dim(\mathrm{V}) = \chi_{\mathrm{V}}(\mathrm{C}_1)$ sur H. Or le seul élément de $\mathrm{Irr}(\mathrm{G})$ pour lequel il existe $\mathrm{C} \neq \mathrm{C}_1$ avec $\chi(\mathrm{C}) = \chi(\mathrm{C}_1)$ est χ_1. On en déduit que $\mathrm{H} = 1$, et donc que G est simple.

H.5. Coefficients de Fourier des fonctions continues

L'objet de ce problème est de montrer que les coefficients de Fourier d'une fonction de $\mathrm{L}^1(\mathbf{R}/\mathbf{Z})$ tendent vers 0 (version discrète du th. de Riemann-Lebesgue), mais qu'une suite tendant vers 0 n'est pas forcément la suite des coefficients de Fourier d'un élément de $\mathrm{L}^1(\mathbf{R}/\mathbf{Z})$.

Partie 1. Notons E l'espace $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ muni de la norme $\| \ \|_\infty$, et notons $\mathrm{F} = \mathrm{L}^1(\mathbf{R}/\mathbf{Z})$ le complété de E pour la norme $\| \ \|_1$ définie par $\|f\|_1 = \int_0^1 |f(x)|\,dx$. Enfin, soit E^* le dual de E, muni de la norme du dual notée $\| \ \|_{\mathrm{E}^*}$.

(i) Si $f, g \in \mathrm{E}$, on pose $\Lambda_f(g) = \int_0^1 f(x)g(x)\,dx$. Montrer que $g \mapsto \Lambda_f(g)$ définit un élément de E^*, et que $f \mapsto \Lambda_f$ est linéaire continue de E, muni de la norme $\| \ \|_1$, dans E^*.

(ii) En déduire que $f \mapsto \Lambda_f$ se prolonge de manière unique en une application linéaire continue de F dans E^*.

(iii) Si $n \in \mathbf{N} - \{0\}$, soit $\phi_n : \mathbf{R} \to [-1, 1]$ la fonction impaire continue, définie pour $x \geqslant 0$, par $\phi_n(x) = 0$, si $x \leqslant 1/2n$, $\phi_n(x) = 2nx - 1$, si $1/2n \leqslant x \leqslant 1/n$, et $\phi_n(x) = 1$, si $x \geqslant 1/n$. Soit $f \in \mathrm{E} - \{0\}$. Soit g_n définie par $g_n(x) = \frac{\overline{f(x)}}{|f(x)|}\phi_n(|f(x)|)$, si $f(x) \neq 0$, et $g_n(x) = 0$, si $f(x) = 0$. Montrer que $g_n \in \mathrm{E}$, et que $\|g_n\|_\infty = 1$, si n est assez grand.

(iv) Soit $h_n = |f| - g_n f$. Montrer que $\|h_n(x)\|_\infty \leqslant \frac{1}{n}$. En déduire que $\|\Lambda_f\|_{\mathrm{E}^*} = \|f\|_1$.

(v) Montrer que $f \mapsto \Lambda_f$ est une isométrie de F dans E^*.

Partie 2. Si $n \in \mathbf{Z}$, et si $f \in \mathrm{F}$, soit $c_n(f) = \Lambda_f(e^{-2i\pi\, nx})$, et soit $c(f)$ la suite $(c_n(f))_{n\in\mathbf{N}}$.

(i) Montrer que $f \mapsto c(f)$ est linéaire continue de F dans $\ell^\infty(\mathbf{Z})$ (muni de $\| \ \|_\infty$).

(ii) Montrer que l'espace $\ell_0^\infty(\mathbf{Z})$ des suites tendant vers 0 quand $|n| \to +\infty$ est fermé dans $\ell^\infty(\mathbf{Z})$.

(iii) Montrer que l'espace Trigo des polynômes trigonométriques est dense dans F.

(iv) En déduire que l'image de F par $f \mapsto c(f)$ est incluse $\ell_0^\infty(\mathbf{Z})$.

(v) Montrer que, si $c(f) = 0$, alors $\Lambda_f = 0$. En déduire que $f \mapsto c(f)$ est injective.

(vi) Soit $\mathrm{S}_k(x) = \frac{\sin(2k+1)\pi x}{\sin \pi x} = \sum_{n=-k}^{k} e^{2i\pi\, nx}$. Montrer que $\|c(\mathrm{S}_k)\|_\infty = 1$ et $\|\mathrm{S}_k\|_1 \to +\infty$ quand $k \to +\infty$. (On montrera que $\|\mathrm{S}_k\|_1 \geqslant \sum_{m=1}^{2k+1} \int_{(m-1)/(2k+1)}^{m/(2k+1)} \frac{|\sin(2k+1)\pi x|}{m\pi/(2k+1)}\,dx$.)

(vii) En déduire que $f \mapsto c(f)$ n'est pas une surjection de F sur $\ell_0^\infty(\mathbf{Z})$.

Corrigé

Partie 1.

(i) La linéarité de $g \mapsto \Lambda_f(g)$ résulte de la linéarité de l'intégration. De plus,

$$|\Lambda_f(g)| \leqslant \int_0^1 |f(t)|\,|g(t)|\,dt \leqslant \|g\|_\infty \int_0^1 |f(t)|\,dt = \|f\|_1\|g\|_\infty.$$

On en déduit la continuité de Λ_f (et donc son appartenance à E^*), ainsi que la majoration $\|\Lambda_f\|_{\mathrm{E}^*} \leqslant \|f\|_1$. Enfin, comme $f \mapsto \Lambda_f$ est linéaire, par linéarité de l'intégration, cette majoration montre que $f \mapsto \Lambda_f$ est continue, de E (muni de la norme $\| \ \|_1$) dans E^*.

(ii) La question précédente montre que l'application linéaire $f \mapsto \Lambda_f$ est continue de E muni de la norme de F dans E^* qui est complet (th. II.1.28). Comme F est le complété de E, le résultat suit du (ii) de la prop. II.1.18.

(iii) Si $f(x_0)=0$, on a $|f(x)|<\frac{1}{2n}$ et donc $g_n(x)=0$ dans un voisinage de x_0, la fonction g_n est donc continue en x_0. Si $f(x_0)\neq 0$, alors g_n est continue comme produit de composées de fonctions continues. Comme g_n est périodique de période 1 si f l'est, on a $g_n\in \mathrm{E}$. Par ailleurs, $\|\phi_n\|_\infty\leqslant 1$ par construction, et donc $\|g_n\|_\infty\leqslant 1$, et comme $|g_n(x)|=1$, si $|f(x)|\geqslant\frac{1}{n}$, on en déduit que $\|g_n\|_\infty\geqslant 1$ (et donc $\|g_n\|_\infty=1$), si $n\geqslant\frac{1}{\|f\|_\infty}$.
(iv) On a $h_n(x)=0$ si $|f(x)|\geqslant\frac{1}{n}$, et $|h_n(x)|\leqslant|f(x)|$, si $|f(x)|\leqslant\frac{1}{n}$. On en déduit la majoration $|h_n(x)|\leqslant\frac{1}{n}$ et $|\int_0^1 h_n(x)\,dx|\leqslant\frac{1}{n}$. Or $|\int_0^1 h_n(x)\,dx|=|\|f\|_1-\Lambda_f(g_n)|$, et donc $|\Lambda_f(g_n)|\geqslant\|f\|_1-\frac{1}{n}$. Comme $\|g_n\|_\infty=1$ si n est assez grand, on en déduit, en passant à la limite, la minoration $\|\Lambda_f\|_{\mathrm{E}^*}\geqslant 1$. Comme la majoration $\|\Lambda_f\|_{\mathrm{E}^*}\leqslant 1$ est immédiate (et a déjà été démontrée), on a $\|\Lambda_f\|_{\mathrm{E}^*}=1$.
(v) $f\mapsto\|f\|_1$ est continue sur F par définition de F. Par ailleurs, $f\mapsto\|\Lambda_f\|_{\mathrm{E}^*}$ est la composée de $f\mapsto\Lambda_f$ qui est continue de F dans E^*, et de $\Lambda\mapsto\|\Lambda\|_{\mathrm{E}^*}$ qui est continue sur E^* ; elle est donc continue. Comme les deux applications continues $f\mapsto\|f\|_1$ et $f\mapsto\|\Lambda_f\|_{\mathrm{E}^*}$ coïncident sur E qui est dense dans F, elles sont égales, ce qui montre que $f\mapsto\Lambda_f$ est une isométrie de F dans E^*.

Partie 2.

(i) La linéarité de $f\mapsto c(f)$ résulte de celle de $f\mapsto\Lambda_f$. De plus, $|c_n(f)|\leqslant\|\Lambda_f\|_{\mathrm{E}^*}\,\|e^{-2i\pi\,nx}\|_\infty=\|f\|_1$, si $n\in\mathbf{Z}$, et donc $\|c(f)\|_\infty\leqslant\|f\|_1$. On en déduit l'appartenance de $c(f)$ à $\ell^\infty(\mathbf{Z})$ et la continuité de $f\mapsto c(f)$.
(ii) Soit $c^{(k)}=(c_n^{(k)})_{n\in\mathbf{Z}}$, pour $k\in\mathbf{N}$, une suite d'éléments de $\ell_0^\infty(\mathbf{Z})$ ayant une limite $c=(c_n)_{n\in\mathbf{Z}}$ dans $\ell^\infty(\mathbf{Z})$. Soit $\varepsilon>0$. Comme $c^{(k)}\to c$, il existe k tel que $\|c^{(k)}-c\|_\infty\leqslant\frac{\varepsilon}{2}$, et comme $c^{(k)}\in\ell_0^\infty(\mathbf{Z})$, il existe $\mathrm{N}\in\mathbf{N}$ tel que $|c_n^{(k)}|\leqslant\frac{\varepsilon}{2}$, si $|n|\geqslant\mathrm{N}$. On a alors $|c_n|\leqslant|c_n^{(k)}|+|c_n^{(k)}-c_n|\leqslant|c_n^{(k)}|+\|c^{(k)}-c\|_\infty\leqslant\varepsilon$, ce qui prouve que c_n tend vers 0 quand $|n|\to+\infty$, et donc que $c\in\ell_0^\infty(\mathbf{Z})$. Ceci permet de conclure.
(iii) Soient $g\in\mathrm{F}$ et $\varepsilon>0$. Comme E est dense dans F, il existe $f\in\mathrm{E}$ avec $\|g-f\|_1\leqslant\frac{\varepsilon}{2}$. Par ailleurs comme Trigo est dense dans E, d'après le théorème de Stone-Weierstrass ((iii) de l'ex. II.1.10), il existe $\mathrm{P}\in\mathrm{Trigo}$ vérifiant $\|f-\mathrm{P}\|_\infty\leqslant\frac{\varepsilon}{2}$. On a alors $\|f-\mathrm{P}\|_1=\int_0^1|f(t)-\mathrm{P}(t)|\,dt\leqslant\|f-\mathrm{P}\|_\infty\leqslant\frac{\varepsilon}{2}$, et donc $\|g-\mathrm{P}\|_1\leqslant\varepsilon$. Ceci permet de montrer que Trigo est dense dans F.
(iv) Si $\mathrm{P}\in\mathrm{Trigo}$, $c_n(\mathrm{P})=0$ sauf pour un nombre fini de n ; en particulier, $c(\mathrm{P})\in\ell_0^\infty(\mathbf{Z})$. Maintenant, si $f\in\mathrm{F}$, il existe une suite $(\mathrm{P}_k)_{k\in\mathbf{N}}$ d'éléments de Trigo tendant vers f dans F. Comme $g\mapsto c(g)$ est continue, $c(\mathrm{P}_k)\to c(f)$ dans $\ell^\infty(\mathbf{Z})$, et comme $\ell_0^\infty(\mathbf{Z})$ est fermé dans $\ell^\infty(\mathbf{Z})$, et que chacun des $c(\mathrm{P}_k)$ est dans $\ell_0^\infty(\mathbf{Z})$, il en est de même de la limite $c(f)$.
(v) Si $c(f)=0$, alors $\Lambda_f(\mathrm{P})=0$, quel que soit $\mathrm{P}\in\mathrm{Trigo}$. Comme Trigo est dense dans E et Λ_f est continue sur E, cela implique $\Lambda_f=0$. On a donc $0=\|\Lambda_f\|_{\mathrm{E}^*}=\|f\|_1$, ce qui prouve que $f=0$ et donc que le noyau de $f\mapsto c(f)$ est réduit à 0, ce qui permet de conclure.
(vi) On a $c_n(\mathrm{S}_k)=1$ si $|n|\leqslant k$, et $c_n(\mathrm{S}_k)=0$, si $|n|>k$. On en déduit que $\|c(\mathrm{S}_k)\|_\infty=1$. Par ailleurs, comme $0\leqslant\sin\pi t\leqslant\pi t$, si $t\in[0,1]$, on a

$$\|\mathrm{S}_k\|_1=\int_0^1\frac{|\sin(2k+1)\pi t|}{\sin\pi t}\,dt\geqslant\sum_{m=1}^{2k+1}\int_{(m-1)/(2k+1)}^{m/(2k+1)}\frac{|\sin(2k+1)\pi t|}{m\pi/(2k+1)}\,dt=\frac{2}{\pi^2}\sum_{m=1}^{2k+1}\frac{1}{m},$$

et comme la somme des $\frac{1}{m}$ diverge, cela permet de conclure.
(vii) Si $f\mapsto c(f)$ est une surjection de F sur $\ell_0^\infty(\mathbf{Z})$, alors c'est une bijection (d'après le (iv)), continue (d'après le (i)), et comme F et $\ell_0^\infty(\mathbf{Z})$ sont des espaces de Banach, son inverse u est continue (cor. II.1.26). Il existe donc $\mathrm{C}>0$ tel que $\|u(c)\|_1\leqslant\mathrm{C}\|c\|_\infty$, si $c\in\ell_0^\infty(\mathbf{Z})$. En appliquant ceci à $c=c(\mathrm{S}_k)$, on en déduit que $\|u(c(\mathrm{S}_k))\|_1=\|\mathrm{S}_k\|_1\leqslant\mathrm{C}\|\mathrm{S}_k\|_\infty=\mathrm{C}$, quel que soit $k\in\mathbf{N}$, ce qui est en contradiction avec la question (v).

H.6. Fonctions d'Hermite et transformée de Fourier dans L^2

Ce problème fournit une définition de la transformée de Fourier dans $\mathrm{L}^2(\mathbf{R})$ en passant par la construction d'une base hilbertienne de $\mathrm{L}^2(\mathbf{R})$.

Partie 1. Soit E l'espace $\mathscr{C}_c^\infty(\mathbf{R})$ muni de la norme $\|\ \|_\infty$. On munit le dual E^* de E de la norme $\|\ \|_{\mathrm{E}^*}$ du dual.

(i) Soit $f \in \mathscr{L}^1(\mathbf{R})$. Montrer que $\phi \mapsto \Lambda_f(\phi) = \int_{\mathbf{R}} f(t)\phi(t)\,dt$ définit un élément de E^* qui ne dépend que de l'image de f dans $\mathrm{L}^1(\mathbf{R})$, et que l'application $f \mapsto \Lambda_f$ ainsi définie est linéaire continue de $\mathrm{L}^1(\mathbf{R})$ dans E^*.

(ii) Soit $f \in \mathrm{Esc}(\mathbf{R})$. On écrit f sous la forme $f = \sum_{i\in \mathrm{I}} \alpha_i \mathbf{1}_{[\frac{k_i}{2^r}, \frac{k_i+1}{2^r}[}$, où $\mathrm{I} \subset \mathbf{Z}$ est fini, les k_i sont distincts et $\alpha_i \neq 0$, si $i \in \mathrm{I}$. Soit $\phi_n : \mathbf{R} \to [0,1]$ de classe $\mathscr{C}^\infty$, nulle en dehors de $[0,1]$ et valant 1 sur $[\frac{1}{n}, 1-\frac{1}{n}]$. Soit $g_n = \sum_{i\in \mathrm{I}} \frac{\overline{\alpha_i}}{|\alpha_i|}\phi_n\big(2^r x - k_i\big)$. Montrer que $\int_0^1 |1-\phi_n(t)|\,dt \leqslant \frac{2}{n}$. En déduire que $\Lambda_f(g_n) \to \|f\|_1$ quand $n \to +\infty$, et que $\|\Lambda_f\|_{\mathrm{E}^*} = \|f\|_1$.

(iii) Soit $f \in \mathrm{L}^1(\mathbf{R})$. Montrer que $\|\Lambda_f\|_{\mathrm{E}^*} = \|f\|_1$. En déduire que si $\int_{\mathbf{R}} f\phi = 0$, pour tout $\phi \in \mathrm{E}$, alors $f = 0$.

Partie 2. Injectivité de la transformée de Fourier dans L^1.

(i) Soit $\phi \in \mathrm{E}$.

(a) Soit $t_0 \in \mathbf{R}$. Montrer que, si $\lambda > 0$, alors $f_\lambda(x,t) = e^{-\lambda|x|}e^{-2i\pi\, x(t-t_0)}\phi(t)$ est sommable sur $\mathbf{R}^2$. En déduire la formule.

$$\int_{-\infty}^{+\infty} e^{-\lambda|x|}e^{2i\pi\, t_0 x}\hat{\phi}(x)\,dx = \frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0 + (2\pi)^{-1}\lambda u)}{1+u^2}\,du.$$

(b) Montrer que $\frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}\,du$ tend vers $\phi(t_0)$ quand $\lambda \to 0$.

(c) Montrer que $\hat{\phi}$ est sommable et que $\int_{-\infty}^{+\infty} e^{-\lambda|x|}e^{2i\pi\, t_0 x}\hat{\phi}(x)\,dx \to \overline{\mathscr{F}}\hat{\phi}(t_0)$ quand $\lambda \to 0$.

(d) Montrer qu'il existe $g \in \mathrm{L}^1(\mathbf{R})$ tel que $\phi = \hat{g}$.

(ii) Soit $f \in \mathrm{L}^1(\mathbf{R})$ vérifiant $\hat{f} = 0$. Montrer que $\int_{\mathbf{R}} f\phi = 0$ quel que soit $\phi \in \mathrm{E}$. En déduire que $f = 0$.

Partie 3. Fonctions d'Hermite. On rappelle que $\int_{\mathbf{R}} e^{-\pi t^2}\,dt = 1$.

(i) Montrer que $(\frac{d}{dt})^n e^{-2\pi t^2} = e^{-2\pi t^2}\mathrm{H}_n(t)$, où H_n est un polynôme de degré exactement n dont on calculera le coefficient dominant.

(ii) On définit Ψ_n par la formule $\Psi_n(t) = e^{-\pi t^2}\mathrm{H}_n(t)$. Montrer que $\langle \Psi_n, \Psi_m\rangle = 0$, si $n \neq m$, et calculer $\langle \Psi_n, \Psi_n\rangle$ (on fera une intégration par partie).

(iii) Montrer que, si $\phi_1, \phi_2 \in \mathrm{L}^2(\mathbf{R})$, alors $\phi_1\phi_2 \in \mathrm{L}^1(\mathbf{R})$.

(iv) Soit $f \in \mathrm{L}^2(\mathbf{R})$ et soit g définie par $g(t) = e^{-\pi t^2}f(t)$. Montrer rapidement que $t^n g(t)$ et $e^{2\pi|tx|}g(t)$ sont sommables, quels que soient $n \in \mathbf{N}$ et $x \in \mathbf{R}$. En déduire que, si $x \in \mathbf{R}$,

$$\lim_{n\to+\infty} \sum_{k=0}^{n} \int_{\mathbf{R}} \frac{(-2i\pi\, tx)^k}{k!} g(t)\,dt = \hat{g}(x).$$

(v) On suppose f orthogonale à tous les Ψ_n. Montrer que $\hat{g} = 0$, puis que $f = 0$.

(vi) Montrer que le sous-espace engendré par les Ψ_n, pour $n \in \mathbf{N}$, est dense dans $\mathrm{L}^2(\mathbf{R})$.

(vii) Soit $e_n = (\|\Psi_n\|_2)^{-1}\Psi_n$. Si $f \in \mathrm{L}^2(\mathbf{R})$, soit $\mathrm{A}(f)$ la suite $(a_n(f))_{n\in\mathbf{N}}$, où $a_n(f) = \langle e_n, f\rangle$. Montrer que $\mathrm{A}(f) \in \ell^2$ et que A est une isométrie de $\mathrm{L}^2(\mathbf{R})$ sur ℓ^2.

Partie 4. Transformée de Fourier dans $\mathrm{L}^2(\mathbf{R})$.

(i) Montrer que $\hat\Psi_0$ est $\mathscr{C}^\infty$ sur $\mathbf{R}$, et vérifie l'équation différentielle $\hat\Psi_0'(x) = -2\pi x\hat\Psi_0(x)$. En déduire que $\hat\Psi_0 = \Psi_0$.

(ii) Montrer que $\Psi_{n+1}(t) = \Psi_n'(t) - 2\pi t\Psi_n(t)$. En déduire que $\hat\Psi_n = (-i)^n\Psi_n$, si $n \in \mathbf{N}$.

(iii) Soit σ l'application $(a_n)_{n\in\mathbf{N}} \mapsto ((-i)^n a_n)_{n\in\mathbf{N}}$. Montrer que σ est une isométrie de ℓ^2 sur ℓ^2.

(iv) Montrer qu'il existe une unique application linéaire continue $\mathscr{F}_2 : \mathrm{L}^2(\mathbf{R}) \to \mathrm{L}^2(\mathbf{R})$, telle que $\mathscr{F}_2(\Psi_n) = \hat\Psi_n$, quel que soit $n \in \mathbf{N}$, et que $\mathscr{F}_2$ est une isométrie.

(v) Montrer que $\mathscr{F}_2 \circ \mathscr{F}_2 = s$, où $(s(\phi))(x) = \phi(-x)$ p.p.

Corrigé

Partie 1.

(i) La linéarité de $\phi \mapsto \Lambda_f(\phi)$ résulte de la linéarité de l'intégration. Maintenant,

$$|\Lambda_f(\phi)| \leqslant \int_0^1 |f(t)|\,|\phi(t)|\,dt \leqslant \|\phi\|_\infty \int_0^1 |f(t)|\,dt = \|f\|_1\|\phi\|_\infty.$$

On en déduit la continuité de Λ_f (et donc son appartenance à E^*), ainsi que la majoration $\|\Lambda_f\|_{\mathrm{E}^*} \leqslant \|f\|_1$. De plus $f \mapsto \Lambda_f$ est linéaire, par linéarité de l'intégration, et $\Lambda_f = 0$, si f est nulle p.p., ce qui montre que Λ_f ne dépend que de l'image de f dans $\mathrm{L}^1(\mathbf{R})$. Enfin, la majoration ci-dessus montre que $f \mapsto \Lambda_f$ est continue, de $\mathrm{L}^1(\mathbf{R})$ (muni de la norme $\|\ \|_1$) dans E^*.

(ii) La majoration $\int_0^1 |1-\phi_n| \leqslant \frac{2}{n}$ est immédiate. On a $(|f| - g_nf)(t) = \sum_{i\in\mathrm{I}} |\alpha_i|(\mathbf{1}_{[0,1[} - \phi_n)(2^rt - k_i)$, et comme $\int_0^1 |\mathbf{1}_{[0,1[} - \phi_n| \leqslant \frac{2}{n}$, on en déduit que $|\int_{\mathbf{R}} |f| - g_nf| \leqslant \frac{2}{n}\sum_{i\in\mathrm{I}} 2^{-r}|\alpha_i| = \frac{2}{n}\|f\|_1$. Comme $\int_{\mathbf{R}} |f| - g_nf = \|f\|_1 - \Lambda_f(g_n)$, cela montre que $\Lambda_f(g_n) \to \|f\|_1$ quand $n \to +\infty$.

Comme $\|\phi_n\|_\infty = 1$ par construction, on en déduit la minoration $\|\Lambda_f\|_{\mathrm{E}^*} \geqslant \|f\|_1$, et comme la majoration $\|\Lambda_f\|_{\mathrm{E}^*} \leqslant \|f\|_1$ est immédiate, cela permet de conclure.

(iii) $f \mapsto \|\Lambda_f\|_{\mathrm{E}^*}$ est continue sur $\mathrm{L}^1(\mathbf{R})$ d'après la question (i), et $f \mapsto \|f\|_1$ aussi, par définition. Or ces deux fonctions coïncident sur $\mathrm{Esc}(\mathbf{R})$ d'après la question (ii), et comme $\mathrm{Esc}(\mathbf{R})$ est dense dans $\mathrm{L}^1(\mathbf{R})$ (th. III.2.11), elles sont égales sur $\mathrm{L}^1(\mathbf{R})$ tout entier ; autrement dit, $\|\Lambda_f\|_{\mathrm{E}^*} = \|f\|_1$, quel que soit $f \in \mathrm{L}^1(\mathbf{R})$. Maintenant, si $\int_{\mathbf{R}} f\phi = 0$ quel que soit $\phi \in \mathrm{E}$, alors $\Lambda_f = 0$ et donc $\|\Lambda_f\|_{\mathrm{E}^*} = 0$; on en déduit que $\|f\|_1 = 0$, et donc que $f = 0$.

Partie 2.

(i) (a) On a $|f_\lambda(x,t)| = e^{-\lambda|x|}|\phi(t)|$, et donc, d'après le th. de Fubini pour les fonctions positives,

$$\int_{\mathbf{R}^2} |f_\lambda(x,t)| = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-\lambda|x|}|\phi(t)|\,dx\Big)\,dt = \int_{\mathbf{R}} \frac{2}{\lambda}|\phi(t)|\,dt = \frac{2}{\lambda}\|\phi\|_1 < +\infty,$$

ce qui prouve que f_λ est sommable. On peut donc appliquer le th. de Fubini pour calculer $\int_{\mathbf{R}^2} f_\lambda$ de deux manières différentes, ce qui nous donne :

$$\int_{\mathbf{R}^2} f_\lambda = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-\lambda|x|}e^{-2i\pi\,x(t-t_0)}\phi(t)\,dt\Big)\,dx = \int_{\mathbf{R}} e^{-\lambda|x|}e^{2i\pi\,t_0x}\hat\phi(x)\,dx$$

$$\int_{\mathbf{R}^2} f_\lambda = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-\lambda|x|}e^{-2i\pi\,x(t-t_0)}\phi(t)\,dx\Big)\,dt = \int_{\mathbf{R}} \Big(\frac{1}{\lambda + 2i\pi(t-t_0)} + \frac{1}{\lambda - 2i\pi(t-t_0)}\Big)\phi(t)\,dt$$

et le résultat suit en faisant le changement de variable $t = t_0 + \frac{\lambda}{2\pi}u$.

(b) $\frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}$ est majoré en module par $\frac{\|\phi\|_\infty}{1+u^2}$, qui est sommable. Comme $\lambda \mapsto \phi(t_0+(2\pi)^{-1}\lambda u)$ est continue pour tout $u \in \mathbf{R}$ et vaut $\phi(t_0)$ pour $\lambda = 0$, le th. de continuité d'une intégrale dépendant d'un paramètre (th. IV.1.1) montre que $\frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}\,du \to \frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0)}{1+u^2}\,du = \phi(t_0)$, quand $\lambda \to 0$.

(c) Comme ϕ est en particulier de classe $\mathscr{C}^2$ et à support compact, il résulte du (i) du th. IV.2.8 que $(1+x^2)\hat{\phi}(x)$ tend vers 0 à l'infini, et comme $\hat{\phi}$ est continue d'après le th. IV.2.7, elle est sommable. Maintenant, $e^{-\lambda|x|}e^{2i\pi\, t_0 x}\hat{\phi}(t)$ est majoré en module par $|\hat{\phi}|$, quel que soit $\lambda > 0$, ce qui permet de déduire du th. de continuité d'une intégrale dépendant d'un paramètre que $\int_{\mathbf{R}} e^{-\lambda|x|}e^{2i\pi\, t_0 x}\hat{\phi}(x)\,dx$ tend vers $\int_{\mathbf{R}} \lim_{\lambda\to 0^+}\big(e^{-\lambda|x|}e^{2i\pi\, t_0 x}\hat{\phi}(x)\big)\,dx = \int_{\mathbf{R}} e^{2i\pi\, t_0 x}\hat{\phi}(x)\,dx = \overline{\mathscr{F}}\hat{\phi}(t_0)$, quand $\lambda \to 0$.

(d) D'après ce qui précède, on a $\phi = \hat{g}$, où g est la transformée de Fourier de $t \mapsto \phi(-t)$, qui est sommable d'après le (c).

(ii) Si $\phi \in \mathrm{E}$, il existe $g \in \mathrm{L}^1(\mathbf{R})$ tel que $\phi = \hat{g}$ d'après le (d) de la question (i). Or, d'après la prop. IV.3.24, on a $\int_{\mathbf{R}} f\phi = \int_{\mathbf{R}} f\,\hat{g} = \int_{\mathbf{R}} \hat{f}\,g$. En particulier, si $\hat{f} = 0$, alors $\int_{\mathbf{R}} f\phi = 0$, quel que soit $\phi \in \mathrm{E}$. D'après la question (iii) de la partie 1, ceci implique $f = 0$.

Partie 3.

(i) Si $(\frac{d}{dt})^n e^{-2\pi t^2} = e^{-2\pi t^2}\mathrm{H}_n(t)$, alors $(\frac{d}{dt})^{n+1}e^{-2\pi t^2} = e^{-2\pi t^2}\mathrm{H}_{n+1}(t)$, avec $\mathrm{H}_{n+1}(t) = \mathrm{H}_n'(t) - 4\pi t\,\mathrm{H}_n(t)$. Comme $\mathrm{H}_0 = 1$, une récurrence immédiate montre que H_n est un polynôme de degré exactement n de coefficient dominant $(-4\pi)^n$.

(ii) Supposons $m \leqslant n$. On a

$$\langle \Psi_n, \Psi_m\rangle = \int_{-\infty}^{+\infty} e^{-2\pi t^2}\mathrm{H}_n(t)\mathrm{H}_m(t)\,dt = \int_{-\infty}^{+\infty} \big((\frac{d}{dt})^n e^{-2\pi t^2}\big)\mathrm{H}_m(t)\,dt.$$

En utilisant le fait que $[\mathrm{P}(t)e^{-2\pi t^2}]_{-\infty}^{+\infty} = 0$, si P est un polynôme, on obtient, après une intégration par partie,

$$\langle \Psi_n, \Psi_m\rangle = -\int_{-\infty}^{+\infty} \big((\frac{d}{dt})^{n-1} e^{-2\pi t^2}\big)\mathrm{H}_m'(t)\,dt = (-1)^n \int_{-\infty}^{+\infty} e^{-2\pi t^2}\mathrm{H}_m^{(n)}(t)\,dt.$$

En particulier, si $m < n$, alors $\mathrm{H}_m^{(n)} = 0$ et $\langle \Psi_n, \Psi_m\rangle = 0$, et si $m = n$, alors $\mathrm{H}_m^{(n)} = n!(-4\pi)^n$, et donc $\langle \Psi_n, \Psi_n\rangle = n!(4\pi)^n \int_{\mathbf{R}} e^{-2\pi t^2}\,dt = \frac{n!(4\pi)^n}{\sqrt{2}}$.

(iii) On a $\int_{\mathbf{R}} |\phi_1\phi_2| \leqslant (\int_{\mathbf{R}} |\phi_1|^2)^{1/2}(\int_{\mathbf{R}} |\phi_2|^2)^{1/2}$ d'après l'inégalité de Cauchy-Schwarz, ce qui montre que si ϕ_1 et ϕ_2 sont de carré sommable, alors $\phi_1\phi_2$ est sommable.

(iv) Les fonctions $t^n e^{-\pi t^2}$, pour $n \in \mathbf{N}$, et $e^{2\pi|xt|}e^{-\pi t^2}$, pour $x \in \mathbf{R}$, sont de carré sommable ; on déduit, en utilisant la question (iii), que les $t^n g(t)$ et les $e^{2\pi|xt|}g(t)$ sont sommables. Maintenant,

$$\Big|\sum_{k=0}^{n} \frac{(-2i\pi\, tx)^k}{k!}g(t)\Big| \leqslant |g(t)| \sum_{k=0}^{+\infty} \frac{(2\pi\,|tx|)^k}{k!} = e^{2\pi|xt|}|g(t)|,$$

et comme $t \mapsto e^{2\pi|xt|}|g(t)|$ est sommable, on peut appliquer le théorème de convergence dominée, et intervertir limite et intégrale, ce qui nous donne

$$\lim_{n\to+\infty}\sum_{k=0}^{n}\int_{\mathbf{R}} \frac{(-2i\pi\, tx)^k}{k!}g(t)\,dt = \int_{\mathbf{R}} \Big(\lim_{n\to+\infty}\sum_{k=0}^{n}\frac{(-2i\pi\, tx)^k}{k!}\Big)g(t)\,dt = \int_{\mathbf{R}} e^{-2i\pi\, tx}g(t)\,dt = \hat{g}(x).$$

(v) Comme $\Psi_n(t) = e^{-\pi t^2}\mathrm{H}_n(t)$, où H_n est un polynôme de degré exactement n, l'espace vectoriel engendré par les Ψ_n est l'espace des $e^{-\pi t^2}\mathrm{P}(t)$, où P est un polynôme. Donc, si f est orthogonale à tous les Ψ_n, on a $\int_{\mathbf{R}} f(t)e^{-\pi t^2}\mathrm{P}(t)\,dt = \int_{\mathbf{R}} \mathrm{P}(t)g(t)\,dt = 0$, quel que soit le polynôme P. Tous les termes du membre de gauche de l'identité de la question (iv) sont donc nuls, et donc $\hat{g} = 0$. Il résulte alors de la question (ii) de la partie 2 que $g = 0$, et donc que $f = e^{\pi t^2}g = 0$.

(vi) L'adhérence $\overline{\mathrm{F}}$ de F est un sous-espace fermé de $\mathrm{L}^2(\mathbf{R})$. Si $\overline{\mathrm{F}}$ est strictement inclus dans $\mathrm{L}^2(\mathbf{R})$, son orthogonal est non nul (cf. prop. II.2.11 (ii)), ce qui contredit la question (v). Ceci permet de conclure.
(vii) Il résulte des questions (ii) et (vi) que les e_n, pour $n \in \mathbf{N}$, forment une base hilbertienne de $\mathrm{L}^2(\mathbf{R})$. Le résultat est donc une conséquence directe du (ii) du th. II.2.6.

Partie 4.
(i) Quel que soit $k \in \mathbf{N}$, la fonction $(1+t^2)^{k/2}\psi_0(t)$ est sommable, et donc $\hat{\Psi}_0$ est de classe $\mathscr{C}^k$ ((ii) du th. IV.2.8). De plus,

$$\begin{aligned}\hat{\Psi}_0'(x) &= \int_{-\infty}^{+\infty} (-2i\pi\, t)e^{-2i\pi\, xt}e^{-\pi t^2}\, dt \\ &= [ie^{-\pi t^2}e^{-2i\pi\, xt}]_{-\infty}^{+\infty} - \int_{-\infty}^{+\infty} ie^{-\pi t^2}(-2i\pi x\, e^{-2i\pi\, xt})\, dt = -2\pi x\, \hat{\Psi}_0(x).\end{aligned}$$

On en déduit l'existence de $a \in \mathbf{C}$ tel que $\hat{\Psi}_0(x) = ae^{-\pi x^2}$, et comme $\hat{\Psi}_0(0) = \int_{\mathbf{R}} e^{-\pi t^2}\, dt = 1$, on a $a = 1$, ce qui permet de conclure.
(ii) $\Psi_{n+1}(t) = e^{\pi t^2}(\frac{d}{dt})^{n+1}e^{-2\pi t^2} = \frac{d}{dt}\big(e^{\pi t^2}(\frac{d}{dt})^n e^{-2\pi t^2}\big) - 2\pi t\, e^{\pi t^2}(\frac{d}{dt})^n e^{-2\pi t^2} = \Psi_n'(t) - 2\pi t\Psi_n(t)$. Comme d'après le th. IV.2.8, on a $\mathscr{F}(\Psi_n')(x) = 2i\pi x\hat{\Psi}_n(x)$ et $\mathscr{F}(2\pi t\Psi_n(t))(x) = i\hat{\Psi}_n'(x)$, on obtient :

$$\hat{\Psi}_{n+1}(x) = 2i\pi x\hat{\Psi}_n(x) - i\hat{\Psi}_n'(x) = (-i)\big(\hat{\Psi}_n'(x) - 2\pi x\hat{\Psi}_n(x)\big).$$

On en déduit que $i^n\hat{\Psi}_n$ et Ψ_n vérifient la même relation de récurrence, et comme $\hat{\Psi}_0 = \Psi_0$, on a $i^n\hat{\Psi}_n = \Psi_n$, pour tout n, ce qui permet de conclure.
(iii) C'est immédiat.
(iv) L'unicité résulte du fait que l'espace engendré par les Ψ_n est dense (partie 3, question (vi)). Pour l'existence, il suffit de poser $\mathscr{F}_2 = \mathrm{A}^{-1} \circ \sigma \circ \mathrm{A}$, où A est l'application définie à la question (vii) de la partie 3, ce qui réalise $\mathscr{F}_2$ comme la composée de trois isométries surjectives, et montre que $\mathscr{F}_2$ est une isométrie de $\mathrm{L}^2(\mathbf{R})$ sur $\mathrm{L}^2(\mathbf{R})$.
(v) Comme $\mathscr{F}_2 \circ \mathscr{F}_2$ et s sont linéaires et continues, il suffit de prouver qu'elles coïncident sur une base hilbertienne, par exemple celle des e_n, pour $n \in \mathbf{N}$. Or $\mathscr{F}_2 \circ \mathscr{F}_2(e_n) = (-i)^n\mathscr{F}_2(e_n) = (-1)^n e_n$ d'après la question (ii), et par ailleurs $s(e_n) = (-1)^n e_n$ car $e^{-2\pi t^2}$ est une fonction paire, ce qui montre que $\Psi_n = e^{\pi t^2}\frac{d^n}{dt^n}e^{-2\pi t^2}$ est une fonction paire si n est pair et impaire si n est impair.

H.7. Transformée de Fourier et convolution

Ce problème est une variation sur le thème Fourier-Poisson. On rappelle que $\int_{\mathbf{R}} e^{-\pi x^2}\,dx = 1$. On ne demande pas de vérifier la mesurabilité des fonctions rencontrées, celle-ci étant automatique d'après Solovay.

Question 1. Soient $f, g \in \mathscr{L}^1(\mathbf{R})$.

(i) Montrer que $\int_{\mathbf{R}^2} |f(x-y)g(y)|\,dx\,dy = \|f\|_1\|g\|_1$.

(ii) Montrer que, pour presque tout $x \in \mathbf{R}$ la fonction $y \mapsto f(x-y)g(y)$ est sommable, que la fonction $f*g$ définie par $f*g(x) = \int_{\mathbf{R}} f(x-y)g(y)\,dy$, si l'intégrale converge, et $f*g(x) = 0$ sinon, est dans $\mathscr{L}^1(\mathbf{R})$, et que $\|f*g\|_1 \leqslant \|f\|_1\|g\|_1$.

(iii) Montrer que si $f_1 = f_2$ p.p. et si $g_1 = g_2$ p.p., alors $f_1 * g_1 = f_2 * g_2$ p.p.

(iv) Montrer que les fonctions continues $\widehat{f*g}$ et $\hat{f}\hat{g}$ sont égales. (On introduira la fonction $\mathrm{H}(t,y) = e^{-2i\pi\,tx} f(t-y)g(y)$, et on justifiera soigneusement les étapes du calcul.)

(v) Existe-t-il une fonction $\phi : \mathbf{R} \to \mathbf{R}_+$, de classe $\mathscr{C}^\infty$ à support compact, non identiquement nulle, telle que $\hat{\phi}$ soit à valeurs dans $\mathbf{R}_+$?

Question 2. Soit $\phi_1 = \mathbf{1}_{[\frac{-1}{2},\frac{1}{2}]}$.

(i) Montrer qu'il n'existe aucune fonction continue sur $\mathbf{R}$ qui soit égale à ϕ_1 p.p.

(ii) Montrer que, si $f \in \mathscr{L}^1(\mathbf{R})$, alors $\phi_1 * f$ est une fonction continue sur $\mathbf{R}$.

(iii) On définit par récurrence ϕ_k, par $\phi_{k+1} = \phi_1 * \phi_k$, si $k \geqslant 1$. Montrer que ϕ_k est continue et paire, pour tout $k \geqslant 2$.

(iv) Calculer $\hat{\phi}_k$, pour tout k. Pour quelles valeurs de k la fonction $\hat{\phi}_k$ est-elle sommable ? Quelle est alors sa transformée de Fourier ?

(v) Montrer que ϕ_k est de classe $\mathscr{C}^{k-2}$, pour tout $k \geqslant 2$.

(vi) Calculer ϕ_2. En déduire la valeur de $\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2}$, puis celle de $\zeta(2) = \sum_{n\geqslant 1} \frac{1}{n^2}$. (On pourra considérer $f(t) = \hat{\phi}_2(\frac{t}{2})$.)

(vii) Que faudrait-il faire pour démontrer avec ce genre de méthodes que $\pi^{-2m}\zeta(2m) \in \mathbf{Q}$, pour tout $m \geqslant 1$? (On demande juste d'établir une stratégie, pas de mener à bien les calculs.)

Question 3. Si $a > 0$, soit $\psi_a : \mathbf{R} \to \mathbf{R}$ définie par $\psi_a(x) = e^{-\pi a x^2}$. On remarquera que $\psi_a \in \mathscr{S}$.

(i) Montrer que $\psi_a * \psi_b = \frac{1}{\sqrt{a+b}}\psi_{ab/(a+b)}$.

(ii) Montrer que $\hat{\psi}_1(x)^k = \hat{\psi}_1(\sqrt{k}\,x)$, pour tous $x \in \mathbf{R}$ et $k \in \mathbf{N}$.

(iii) Montrer que $\hat{\psi}_1$ est à valeurs réelles.

(iv) Montrer qu'il existe $a \in \mathbf{R}$ tel que $\hat{\psi}_1(x) = e^{-\pi a x^2}$ pour tout $x \in \mathbf{R}$.

(v) Montrer que $a > 0$, puis que $a = 1$.

Question 4. (i) Montrer qu'il existe $\varepsilon > 0$ tel que $\left|\frac{\sin \pi u}{\pi u}\right| \leqslant 1 - \varepsilon u^2$, si $|u| \leqslant 3$.

(ii) Montrer que $\left|\hat{\phi}_k\left(\frac{x}{\sqrt{k}}\right)\right| \leqslant \sup\left(e^{-\varepsilon x^2}, \frac{1}{1+x^2}\right)$, pour tous $k \geqslant 4$ et $x \in \mathbf{R}$.

(iii) Soit f_k la fonction définie par $f_k(x) = \hat{\phi}_k\left(\frac{x}{\sqrt{k}}\right)$, et soit f donnée par $f(x) = e^{-\frac{\pi^2 x^2}{6}}$. Montrer que f_k tend vers f dans $\mathrm{L}^1(\mathbf{R})$.

(iv) Soit g_k la fonction définie par $g_k(x) = \sqrt{k}\,\phi_k(\sqrt{k}\,x)$. Montrer que g_k tend uniformément sur $\mathbf{R}$ vers une fonction g que l'on déterminera. Ce résultat vous évoque-t-il quelque chose ?

Corrigé

Question 1.
(i) D'après le th. de Fubini pour les fonctions positives ((ii) du th. III.3.3), on a

$$\int_{\mathbf{R}^2} |f(x-y)g(y)|\,dx\,dy = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} |f(x-y)g(y)|\,dx\Big)\,dy.$$

Le changement de variable $t = x - y$ dans l'intégrale entre parenthèses nous donne alors

$$\int_{\mathbf{R}^2} |f(x-y)g(y)|\,dx\,dy = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} |f(t)g(y)|\,dt\Big)\,dy = \int_{\mathbf{R}} \|f\|_1\,|g(y)|\,dy = \|f\|_1\|g\|_1.$$

(ii) D'après le (i), la fonction $h(x,y) = f(x-y)g(y)$ est sommable sur $\mathbf{R}^2$ et donc, d'après le théorème de Fubini ((i) du th. III.3.3), pour presque tout x la fonction $y \mapsto h(x,y)$ est sommable sur $\mathbf{R}$, et $x \mapsto \int_{\mathbf{R}} h(x,y)\,dy = f * g(x)$ p.p. est sommable.

De plus, $|f*g(x)| \leqslant \int_{\mathbf{R}} |h(x,y)|\,dy$ pour tout x et donc $\|f*g\|_1 \leqslant \int_{\mathbf{R}} \big(\int_{\mathbf{R}} |h(x,y)|\,dy\big)\,dx$. Or cette dernière quantité vaut $\|f\|_1\|g\|_1$, d'après le th. de Fubini pour les fonctions positives et le (i).
(iii) En dehors de l'ensemble de mesure nulle où l'une des intégrales diverge, on a $f_1 * g_1 - f_2 * g_2 = (f_1 - f_2) * g_1 + f_2 * (g_1 - g_2)$. On en déduit, en utilisant le (ii), la majoration $\|f_1 * g_1 - f_2 * g_2\|_1 \leqslant \|f_1 - f_2\|_1\|g_1\|_1 + \|f_2\|_1\|g_1 - g_2\|_1$. Or le second membre est nul puisque $\|f_1 - f_2\|_1 = \|g_1 - g_2\|_1 = 0$. On conclut en utilisant le fait que $\|f\|_1 = 0$ équivaut à $f = 0$ p.p.
(iv)

$$\widehat{f*g}(x) = \int_{\mathbf{R}} e^{-2i\pi\,tx} f*g(t)\,dt = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-2i\pi\,tx} f(t-y)g(y)\,dy\Big)\,dt.$$

Soit $\mathrm{H}(t,y) = e^{-2i\pi\,tx} f(t-y)g(y)$. On a $|\mathrm{H}(t,y)| = |f(t-y)g(t)|$, ce qui fait que H est sommable sur $\mathbf{R}^2$ d'après le (i). On peut donc utiliser le th. de Fubini pour obtenir $\widehat{f*g}(x) = \int_{\mathbf{R}^2} e^{-2i\pi\,tx} f(t-y)g(y)\,dy\,dt$. On fait alors le changement de variable $y = u$, $t = u + v$ dont le jacobien est 1, ce qui nous donne $\widehat{f*g}(x) = \int_{\mathbf{R}^2} e^{-2i\pi\,(u+v)x} f(u)g(v)\,du\,dv$, la fonction à intégrer étant sommable d'après le th. III.3.9. On conclut en utilisant la formule $e^{-2i\pi\,(u+v)x} = e^{-2i\pi\,ux} e^{-2i\pi\,vx}$ et le th. de Fubini, ce qui nous donne

$$\widehat{f*g}(x) = \int_{\mathbf{R}} \Big(\int_{\mathbf{R}} e^{-2i\pi\,ux} e^{-2i\pi\,vx} f(u)g(v)\,du\Big)\,dv = \int_{\mathbf{R}} \hat{f}(x) e^{-2i\pi\,vx} g(v)\,dv = \hat{f}(x)\hat{g}(x).$$

(v) Partons de $\phi_0 : \mathbf{R} \to \mathbf{R}_+$, de classe $\mathscr{C}^\infty$ à support compact, non identiquement nulle. Notons ϕ_1 la fonction définie par $\phi_1(x) = \phi_0(-x)$, et considérons $\phi = \phi_0 * \phi_1$. Le changement de variable $t \mapsto -t$ dans l'intégrale définissant $\hat{\phi}_1$ montre que l'on a $\hat{\phi}_1(x) = \overline{\hat{\phi}_0(x)}$ pour tout $x \in \mathbf{R}$. On en déduit que $\hat{\phi}(x) = |\hat{\phi}_0(x)|^2$ est à valeurs dans $\mathbf{R}_+$.

Il reste à vérifier que ϕ est à valeurs dans $\mathbf{R}_+$ (ce qui est immédiat sur sa définition puisque ϕ_0 et ϕ_1 le sont), que ϕ est à support compact (si ϕ_0 est nulle en dehors de $[-\mathrm{M},\mathrm{M}]$, il en est de même de ϕ_1, et $\phi_0(x-y)\phi_1(y)$ est identiquement nulle sur $\mathbf{R}$ si $x \notin [-2\mathrm{M}, 2\mathrm{M}]$, ce qui prouve que ϕ est à support dans $[-2\mathrm{M}, 2\mathrm{M}]$), et que ϕ est $\mathscr{C}^\infty$ (ce qui résulte de ce que $\phi = \overline{\mathscr{F}}\hat{\phi}$ appartient à $\mathscr{S}$ puisque $\hat{\phi} = \hat{\phi}_0\hat{\phi}_1$ appartient à $\mathscr{S}$ comme produit de deux fonctions de $\mathscr{S}$; on peut aussi utiliser le th. de dérivation sous le signe somme (th. IV.1.2) pour vérifier que $f * g$ est $\mathscr{C}^\infty$, si $f \in \mathscr{C}^\infty_c(\mathbf{R})$ et $g \in \mathrm{L}^1(\mathbf{R})$).

Question 2.
(i) Si $g = \phi_1$ p.p., alors tout voisinage de $\frac{1}{2}$ contient un ensemble de mesure non nul (et donc non vide) sur lequel $g = 1$ et un autre sur lequel $g = 0$. On en déduit que g ne peut pas être continue en $\frac{1}{2}$.
(ii) On a $\phi_1 * f(x) = \int_{\mathbf{R}} h(x,y)\,dy$, avec $h(x,y) = \mathbf{1}_{[\frac{-1}{2},\frac{1}{2}]}(x-y)f(y)$. Maintenant,

- $x \mapsto h(x,y)$ est continue en x_0 sauf si $y = x_0 + \frac{1}{2}$ ou $y = x_0 - \frac{1}{2}$,
- $|h(x,y)| \leqslant |f(y)|$ qui est sommable et indépendante de x.

On est donc sous les hypothèses du th. IV.1.1, ce qui prouve que $\phi_1 * f$ est continue en x_0 et donc sur $\mathbf{R}$ puisque x_0 est arbitraire.
(iii) Que ϕ_k soit continue suit, par récurrence, du (ii). La parité de ϕ_k se démontre aussi par récurrence en faisant le changement de variable $t = -y$ dans l'intégrale définissant $\phi_1 * \phi_k(-x)$: en effet, on a $\phi_{k+1}(-x) = \int_{\mathbf{R}} \phi_1(-x-y)\phi_k(y)\,dy = \int_{\mathbf{R}} \phi_1(-x+t)\phi_k(-t)\,dt = \int_{\mathbf{R}} \phi_1(x-t)\phi_k(t)\,dt$ puisque ϕ_1 et ϕ_k sont paires. Comme la dernière intégrale vaut $\phi_{k+1}(x)$, cela prouve que ϕ_{k+1} est bien paire.
(iv) On a $\hat\phi_1(x) = \int_{-1/2}^{1/2} e^{-2i\pi xt}\,dt = \frac{-1}{2i\pi x}\big[e^{-2i\pi xt}\big]_{-1/2}^{1/2} = \frac{\sin \pi x}{\pi x}$. Une récurrence immédiate utilisant le (iv) de la question (i) montre que $\hat\phi_k(x) = \big(\frac{\sin \pi x}{\pi x}\big)^k$.

La fonction $\hat\phi_k$ est sommable si $k \geqslant 2$ car continue et $\mathrm{O}(\frac{1}{x^2})$ à l'infini. La formule d'inversion de Fourier dans L^1 (prop. IV.3.25) appliquée à ϕ_k nous donne $\mathscr{F}\hat\phi_k(x) = \phi_k(-x)$, et comme ϕ_k est paire, on en déduit que la transformée de Fourier de $\hat\phi_k$ est ϕ_k.

La fonction $\hat\phi_1$ n'est pas sommable. En effet, si elle l'était, sa transformée de Fourier serait ϕ_1 (dans L^1) par le même argument que ci-dessus, et comme il n'existe pas de fonction continue égale à ϕ_1 p.p., cela contredit le th. de Riemann-Lebesgue.
(v) $(1+|x|^2)^{k-2/2}\hat\phi_k(x)$ est un $\mathrm{O}(\frac{1}{x^2})$ au voisinage de l'infini, et donc est sommable. Il en résulte, grâce au (ii) du th. IV.2.8, que la transformée de Fourier de $\hat\phi_k$ est de classe $\mathscr{C}^{k-2}$, et comme cette transformée de Fourier est ϕ_k d'après le (iv), cela permet de conclure.
(vi) $\phi_2(x)$ est la longueur de l'intervalle $[\frac{-1}{2}, \frac{1}{2}] \cap [x-\frac{1}{2}, x+\frac{1}{2}]$. On a donc $\phi_2(x) = 0$, si $|x| \geqslant 1$ et $\phi_2(x) = 1-|x|$, si $|x| \leqslant 1$.

Soit $f(t) = \hat\phi_2(\frac{t}{2})$. Alors f est de classe $\mathscr{C}^1$ (et même $\mathscr{C}^\infty$) et f et f' sont des $\mathrm{O}(\frac{1}{t^2})$ au voisinage de l'infini. On peut donc lui appliquer la formule de Poisson du th. IV.3.18. Comme $\hat f(x) = 2\mathscr{F}\hat\phi_2(2x) = 2\phi_2(2x)$, cette formule devient $2\sum_{n\in\mathbf{Z}} \phi_2(2n) = \sum_{n\in\mathbf{Z}} \hat\phi_2(\frac{n}{2})$. Dans le membre de gauche, le seul terme non nul est $\phi_2(0) = 1$, et dans le membre de droite, seuls 0 et les entiers impairs contribuent, et la formule devient :

$$2 = 1 + \sum_{n \text{ impair}} \frac{1}{(\pi n/2)^2} = 1 + \frac{8}{\pi^2}\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2}, \quad \text{et donc} \quad \sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2} = \frac{\pi^2}{8}.$$

Pour en déduire $\sum_{n\geqslant 1} \frac{1}{n^2}$, on écrit n sous la forme $2^k(2m+1)$, ce qui nous donne :

$$\sum_{n\geqslant 1} \frac{1}{n^2} = \sum_{k,m\in\mathbf{N}} \frac{1}{2^{2k}}\,\frac{1}{(2m+1)^2} = \Big(\sum_{k\in\mathbf{N}} \frac{1}{2^{2k}}\Big)\Big(\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2}\Big) = \frac{1}{1-\frac{1}{4}}\,\frac{\pi^2}{8} = \frac{\pi^2}{6}.$$

(vii) Il suffirait de prouver que $\phi_k(2n) \in \mathbf{Q}$ et est nul sauf pour un nombre fini de $n \in \mathbf{Z}$. Or il n'est pas très difficile de prouver que ϕ_k est nulle en dehors de $[\frac{-k}{2}, \frac{k}{2}]$, et est un polynôme, de degré $k-1$, à coefficients dans $\mathbf{Q}$, sur chaque intervalle de la forme $[\frac{-k}{2}+i, \frac{-k}{2}+i+1]$, pour $i \in \{0, \dots, k-1\}$.

Question 3.
(i) $\psi_a * \psi_b(x) = \int_{\mathbf{R}} e^{-\pi(a(x-t)^2+bt^2)}\,dt$. Or $a(x-t)^2 + bt^2 = (a+b)\big(t - \frac{ax}{a+b}\big)^2 + \frac{ab}{a+b}x^2$, et on déduit le résultat en faisant le changement de variable $u = \frac{1}{\sqrt{a+b}}\big(t - \frac{ax}{a+b}\big)$ et en utilisant la formule $\int_{\mathbf{R}} e^{-\pi u^2}\,du = 1$.
(ii) On note ψ_1^{*k} la fonction $\psi_1 * \cdots * \psi_1$ (k facteurs). Alors, d'après le (iv) de la question 1, $\hat\psi_1^k$ est la transformée de Fourier de ψ_1^{*k}. Or on vérifie, par récurrence sur k, en utilisant le (i), que $\psi_1^{*k} = \frac{1}{\sqrt{k}}\psi_{1/k}$, et comme $\psi_{1/k}(x) = \psi_1(\frac{x}{\sqrt{k}})$, la formule pour les dilatations permet de conclure.
(iii) La fonction ψ_1 étant paire, on a $\hat\psi_1(x) = \int_0^{+\infty}(e^{-2i\pi xt} + e^{2i\pi xt})\psi_1(t)\,dt$ comme le montre un changement de variable $t \mapsto -t$ sur $]-\infty, 0]$ dans l'intégrale définissant $\hat\psi_1(x)$. La fonction intégrée étant réelle, cela permet de conclure.

(iv) D'après le (ii), on a $\hat{\psi}_1(x) = \hat{\psi}_1\big(\frac{x}{\sqrt{k}}\big)^k$, pour tout $k \geqslant 1$. L'appartenance de ψ_1 à $\mathscr{S}$ implique que $\hat{\psi}_1$ est de classe $\mathscr{C}^\infty$ sur $\mathbf{R}$ (cor. IV.3.17). En particulier, elle a un développement limité de la forme $\hat{\psi}_1(x) = 1 + \alpha x + \beta x^2 + o(x^2)$ en 0 (on a $\hat{\psi}_1(0) = \int_{\mathbf{R}} e^{-\pi t^2}\, dt = 1$). En passant au logarithme dans l'identité $\hat{\psi}_1(x) = \hat{\psi}_1\big(\frac{x}{\sqrt{k}}\big)^k$, et en faisant tendre k vers $+\infty$, on en déduit que $\alpha = 0$ (ce qui peut aussi se déduire de la parité de ψ_1), et $\log \hat{\psi}_1(x) = \lim_{k\to+\infty} k \log\big(1 + \beta\frac{x^2}{k} + o(\frac{1}{k})\big) = \beta x^2$. On a donc $\hat{\psi}_1(x) = e^{-\pi a x^2}$, avec $a = \frac{-\beta}{\pi}$.

(v) D'après Riemann-Lebesgue, $\hat{\psi}_1$ tend vers 0 à l'infini, et donc $a > 0$. Maintenant, d'après la formule d'inversion de Fourier dans $\mathscr{S}$ (th. IV.3.21), la transformée de Fourier de $\hat{\psi}_1$ est $\psi_1(-x) = \psi_1(x)$ et en particulier, $1 = \psi_1(0) = \int_{\mathbf{R}} e^{-\pi a x^2} = \frac{1}{\sqrt{a}}$, et donc $a = 1$. (On peut aussi remarquer que

$$\beta = \frac{1}{2}\hat{\psi}_1'(0) = \frac{1}{2}\int_{\mathbf{R}} (-2i\pi t)^2 e^{-\pi t^2}\, dt = -4\pi^2 \int_0^{+\infty} t^2 e^{-\pi t^2} dt.$$

Le changement de variable $t = \frac{\sqrt{u}}{\sqrt{\pi}}$ permet d'écrire l'intégrale sous la forme $\frac{1}{2(\sqrt{\pi})^3}\int_0^{+\infty} u^{1/2} e^{-u}\, du = \frac{1}{2(\sqrt{\pi})^3}\Gamma(\frac{3}{2})$, et comme $\Gamma(\frac{3}{2}) = \frac{1}{2}\Gamma(\frac{1}{2}) = \frac{\sqrt{\pi}}{2}$, on obtient $\beta = -4\pi^2 \frac{1}{2(\sqrt{\pi})^3}\,\frac{\sqrt{\pi}}{2} = -\pi$, et donc $a = 1$.)

Question 4.

(i) Comme $\frac{\sin \pi u}{\pi u}$ est paire, il suffit de considérer $u \in [0, 3]$. Soit $g(u) = u^{-2}(1 - \frac{\sin \pi u}{\pi u})$. On peut prolonger g par continuité en 0 en posant $g(0) = \frac{\pi^2}{6}$. La fonction g atteint donc son minimum ε sur le compact $[0, 3]$, et comme g est strictement positive sur $\mathbf{R}_+$ car $\sin x < x$, si $x > 0$, on a $\varepsilon > 0$. L'inégalité $g(u) \geqslant \varepsilon$ si $u \in [0, 3]$ se traduit alors par l'inégalité cherchée

(ii) Si $|x| \leqslant 3\sqrt{k}$, on a $\hat{\phi}_k\big(\frac{x}{\sqrt{k}}\big) \leqslant (1 - \varepsilon\frac{x^2}{k})^k$ d'après le (i), et donc $\hat{\phi}_k\big(\frac{x}{\sqrt{k}}\big) \leqslant e^{-\varepsilon x^2}$, car $\log(1-u) \leqslant -u$, si $0 < u < 1$.

Si $|x| \geqslant 3\sqrt{k}$, alors $|\hat{\phi}_k\big(\frac{x}{\sqrt{k}}\big)| \leqslant (\frac{\sqrt{k}}{|x|})^k$. Pour montrer que ceci est $\leqslant \frac{1}{1+x^2}$, on passe au logarithme et on fait le changement de variable $u = \frac{|x|}{\sqrt{k}}$. On est ramené à montrer que $k \log u - \log(1 + ku^2) \geqslant 0$, si $k \geqslant 4$ et $u \geqslant 3$. Or la fonction $u \mapsto k \log u - \log(1 + ku^2)$ admet comme dérivée $\frac{k}{u} - \frac{2ku}{1+ku^2} = \frac{k}{u(1+ku^2)}(1 + (k-2)u^2)$ qui est toujours positive ; elle atteint donc son minimum en $u = 3$, et comme $k \mapsto k \log 3 - \log(1 + 9k)$ est croissante sur $[4, +\infty[$ et $\geqslant 0$ en $k = 4$, cela permet de conclure.

(iii) On a $\frac{\sin \pi u}{\pi u} = 1 - \frac{\pi^2 u^2}{6} + o(u^2)$ au voisinage de 0. On en déduit que $f_k(x) = (\frac{\sin \pi x/\sqrt{k}}{\pi x/\sqrt{k}})^k$ tend vers $e^{-\frac{\pi^2 x^2}{6}}$ quand k tend vers $+\infty$. Comme par ailleurs f_k est majorée par $\sup\big(e^{-\varepsilon x^2}, \frac{1}{1+x^2}\big)$ qui est sommable et indépendante de k, il résulte du théorème de convergence dominée (th. III.1.32) que f_k tend vers $e^{-\frac{\pi^2 x^2}{6}}$ dans $\mathrm{L}^1(\mathbf{R})$.

(iv) g_k est la transformée de Fourier de f_k. Or, d'après le th. IV.2.7 (Riemann-Lebesgue), la transformée de Fourier est continue de $\mathrm{L}^1(\mathbf{R})$ dans $\mathscr{C}_0(\mathbf{R})$ (muni de la norme $\| \ \|_\infty$). Comme f_k tend, d'après le (iii), vers f dans $\mathrm{L}^1(\mathbf{R})$, cela implique que g_k tend uniformément sur $\mathbf{R}$ vers $\hat{f}$. Or $f(t) = \psi_1(\frac{\sqrt{\pi}}{\sqrt{6}}t)$, et donc $\hat{f}(x) = \frac{\sqrt{6}}{\sqrt{\pi}}\hat{\psi}_1(\frac{\sqrt{6}}{\sqrt{\pi}}x) = \frac{\sqrt{6}}{\sqrt{\pi}}e^{-6x^2}$. Il s'agit, à normalisation près, d'un cas particulier d'une variante du théorème de la limite centrale.

H.8. Loi d'addition sur une courbe elliptique

Soit (ω_1, ω_2) une base directe ($\mathrm{Im}(\frac{\omega_2}{\omega_1}) > 0$) de $\mathbf{C}$ sur $\mathbf{R}$, et soit $\Lambda = \{m\omega_1 + n\omega_2,\ m, n \in \mathbf{Z}\}$. On dit que $f : \mathbf{C} \to \mathbf{C}$ est Λ-périodique si $f(z+\omega) = f(z)$, quels que soient $z \in \mathbf{C}$ et $\omega \in \Lambda$.

Partie I

(o) Montrer qu'il existe $\mathrm{C} > 0$ tel que $|a\omega_1 + b\omega_2| \geqslant \mathrm{C}\sup(|a|, |b|)$, quels que soient $a, b \in \mathbf{R}$, et montrer que $r(\Lambda) = \inf_{\omega\in\Lambda-\{0\}} |\omega|$ est non nul.

(i) Soit $\mathrm{A} = \{\alpha\omega_1 + \beta\omega_2,\ \alpha, \beta \in [0,1]\}$. Montrer que A est compact et que , si $z \in \mathbf{C}$, il existe $\omega \in \Lambda$ et $u \in \mathrm{A}$ tels que $z = \omega + u$. En déduire que si $f : \mathbf{C} \to \mathbf{R}_+$ est continue et Λ-périodique, alors f est bornée et atteint son maximum.

(ii) Montrer qu'une fonction Λ-périodique, holomorphe sur $\mathbf{C}$, est constante.

(iii) Montrer que $\sum_{\omega\in\Lambda-\{0\}} \frac{1}{|\omega|^k}$ converge si k est un entier $\geqslant 3$.

(iv) Montrer que, si $\mathrm{R} > 0$ et si $|\omega| \geqslant 2\mathrm{R}$, alors $z + \omega$ ne s'annule pas sur $\mathrm{D}(0,\mathrm{R})$ et les séries

$$\sum_{\omega\in\Lambda,\,|\omega|\geqslant 2\mathrm{R}} \Big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\Big) \quad \text{et} \quad \sum_{\omega\in\Lambda,\,|\omega|\geqslant 2\mathrm{R}} \frac{1}{(z+\omega)^3}$$

convergent normalement sur $\mathrm{D}(0,\mathrm{R})$.

(v) En déduire que, si $z \in \mathbf{C} - \Lambda$, alors la série $\mathrm{F}(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda-\{0\}} \big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\big)$ converge, et que $z \mapsto \mathrm{F}(z)$ est holomorphe [11] sur $\mathbf{C} - \Lambda$.

(vi) Montrer que F' est Λ-périodique et que F est paire. En déduire que F est Λ-périodique.

(vii) Si $k \geqslant 3$, soit $\mathrm{G}_k = \sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^k}$. Montrer que la série $\sum_{n=1}^{+\infty}(-1)^n(n+1)\mathrm{G}_{n+2}\, z^n$ est de rayon de convergence exactement $r(\Lambda)$, et que sa somme est $\mathrm{G}(z) = \mathrm{F}(z) - \frac{1}{z^2}$, si $|z| < r(\Lambda)$.

(viii) Montrer que $\mathrm{G}_k = 0$, si k est impair. En déduire que, si l'on pose $g_2 = 60\mathrm{G}_4$ et $g_3 = 140\mathrm{G}_6$, alors $\mathrm{H}(z) = \mathrm{F}'(z)^2 - 4\mathrm{F}(z)^3 + g_2\mathrm{F}(z) + g_3$ est holomorphe et nulle en 0.

(ix) Montrer que $\mathrm{F}'(z)^2 = 4\mathrm{F}(z)^3 - g_2\mathrm{F}(z) - g_3$, quel que soit $z \in \mathbf{C} - \Lambda$.

Partie II

Soit $\mathbf{C}/\Lambda$ le quotient de $\mathbf{C}$ par son sous-groupe Λ. Rappelons que cela signifie que l'on dispose d'un morphisme de groupes $\pi : \mathbf{C} \to \mathbf{C}/\Lambda$ surjectif et tel que $\pi(z) = 0$ si et seulement si $z \in \Lambda$ (où l'on a noté 0 l'élément neutre du groupe commutatif $\mathbf{C}/\Lambda$). L'équation [12] $u = -u$ a 4 solutions dans $\mathbf{C}/\Lambda$, à savoir : 0, $e_1 = \pi(\frac{\omega_1}{2})$, $e_2 = \pi(\frac{\omega_2}{2})$ et $e_3 = \pi(\frac{\omega_1+\omega_2}{2})$.

Si $a \in \mathbf{C}$, soit $\mathrm{S}_a = \{a + \alpha\omega_1 + \beta\omega_2,\ \alpha, \beta \in [0,1[\}$. On peut écrire tout élément z de $\mathbf{C}$ de manière unique sous la forme $z = \omega + u$, avec [13] $u \in \mathrm{S}_a$ et $\omega \in \Lambda$. On en déduit que π induit une bijection de S_a sur $\mathbf{C}/\Lambda$, et donc que S_a est un système de représentants de $\mathbf{C}/\Lambda$ dans $\mathbf{C}$. On note $s_a : (\mathbf{C}/\Lambda) \to \mathrm{S}_a$ la bijection réciproque, et donc $s_a(u)$ est le représentant de u dans S_a, si $u \in \mathbf{C}/\Lambda$.

---

11. La notation standard est $\wp(z)$ ou $\wp(z,\mathrm{L})$; c'est la fonction $\wp$ de Weierstrass.

12. Elle est équivalente à $2u = 0$ dans $\mathbf{C}/\Lambda$, ce qui se traduit, en choisissant $\tilde{u} \in \mathbf{C}$ avec $\pi(\tilde{u}) = u$, par $2\tilde{u} \in \Lambda$, ou encore $\tilde{u} \in \frac{1}{2}\Lambda$, et tout élément de $\frac{1}{2}\Lambda$ peut s'écrire de manière unique sous la forme ω ou $\frac{\omega_1}{2} + \omega$ ou $\frac{\omega_2}{2} + \omega$ ou $\frac{\omega_1+\omega_2}{2} + \omega$, avec $\omega \in \Lambda$.

13. On écrit $z - a$ sous la forme $x\omega_1 + y\omega_2$, avec $x, y \in \mathbf{R}$, et alors $\omega = [x]\omega_1 + [y]\omega_2$, et $u = a + \{x\}\omega_1 + \{y\}\omega_2$.

On note $\Omega_a = \{a+\alpha\omega_1+\beta\omega_2,\ \alpha,\beta \in]0,1[\}$ l'intérieur de S_a, et γ_a le bord de Ω_a parcouru dans le sens direct. C'est le composé des segments $[a, a+\omega_1]$, $[a+\omega_1, a+\omega_1+\omega_2]$, $[a+\omega_1+\omega_2, a+\omega_2]$ et $[a+\omega_2, a]$. On remarquera que $S_a \subset \Omega_a \cup \gamma_a$. On note simplement [14] $\int_\alpha^\beta f(z)\,dz$ l'intégrale $\int_{[\alpha,\beta]} f(z)\,dz$.

Une fonction $f : \mathbf{C} \to \mathbf{C}$ qui est Λ-périodique peut être considérée comme une fonction de $\mathbf{C}/\Lambda$ dans $\mathbf{C}$. Si f est une fonction méromorphe sur $\mathbf{C}$, Λ-périodique, on dit que les zéros (resp. les pôles) de f dans $\mathbf{C}/\Lambda$ sont les u_i, pour $i \in I$, avec multiplicités $m_i \geqslant 1$, si les zéros (resp. les pôles) de f dans S_a sont les $s_a(u_i)$, pour $i \in I$, et si la valuation de f en $s_a(u_i)$ est m_i (resp. $-m_i$), ce qui ne dépend pas du choix de $a \in \mathbf{C}$. Si tel est le cas, on note $N_0(f) = \sum_{i\in I} m_i$ (resp. $N_\infty(f) = \sum_{i\in I} m_i$) le nombre de zéros (resp. de pôles) de f dans $\mathbf{C}/\Lambda$, comptés avec multiplicité.

(i) Soit f une fonction méromorphe sur $\mathbf{C}$ non identiquement nul. Montrer que, si $a \in \mathbf{C}$, il existe $r_a > 0$ tel que f n'ait aucun zéro ni pôle dans $D(a, r_a^-) - \{a\}$. En déduire que si K est un compact de C, alors f n'a qu'un nombre fini de zéros et de pôles dans K.

(ii) Soit f une fonction Λ-périodique, non identiquement nulle, méromorphe sur $\mathbf{C}$. Montrer qu'il existe $a \in \mathbf{C}$ tel que f n'ait ni zéro ni pôle sur le chemin γ_a.

(iii) Montrer que $\int_{\gamma_a} \frac{f'(z)}{f(z)}\,dz = 2i\pi(N_0(f) - N_\infty(f))$. En déduire que $N_0(f) = N_\infty(f)$.

(iv) Dans tout ce qui suit, F est la fonction de Weierstrass définie à la question (v) de la partie I. Calculer $N_0(F')$, et montrer que F' est impaire. En déduire que les zéros de F' dans $\mathbf{C}/\Lambda$ sont e_1, e_2 et e_3, et que ce sont des zéros simples.

(v) Calculer $N_\infty(F - b)$, si $b \in \mathbf{C}$. En déduire que $F : (\mathbf{C}/\Lambda) - \{0\} \to \mathbf{C}$ est surjective, et que $F(a) = F(a')$ si et seulement si $a' = \pm a$. (On fera attention au cas $F(a) \in \{F(e_1), F(e_2), F(e_3)\}$.)

(vi) En déduire que $z \mapsto P(z) = (F(z), F'(z))$ est une bijection de $(\mathbf{C}/\Lambda) - \{0\}$ sur l'ensemble $E(\mathbf{C})$ des solutions (X, Y) dans $\mathbf{C}^2$ de l'équation $Y^2 = 4X^3 - g_2X - g_3$.

(vii) Soient $\Omega \subset \mathbf{C}$ un ouvert contractile et $f : \Omega \to \mathbf{C}$, holomorphe et ne s'annulant pas sur Ω. Montrer qu'il existe g holomorphe sur Ω telle que $f = e^g$, et que $g' = \frac{f'}{f}$.

(viii) Si $a, b \in \mathbf{C}$, et si $r > 0$, soit $\Omega_r(a,b) = \{z \in \mathbf{C},\ \exists c \in [a,b],\ |z-c| < r\}$. Montrer que $\Omega_r(a,b)$ est un ouvert convexe.

(ix) Soit f une fonction Λ-périodique, non identiquement nulle, méromorphe sur $\mathbf{C}$, et soient $a \in \mathbf{C}$ et $\omega \in \Lambda$ tels que f n'ait ni zéro ni pôle sur $[a, a+\omega]$. Montrer que, si $r > 0$ est assez petit, f n'a ni zéro ni pôle dans $\Omega_r(a, a+\omega)$. En déduire que $\frac{1}{2i\pi}\int_a^{a+\omega} \frac{f'(z)}{f(z)}\,dz \in \mathbf{Z}$.

(x) Soit f une fonction Λ-périodique, non identiquement nulle, méromorphe sur $\mathbf{C}$.

(a) Montrer que l'ensemble X_a des éléments de S_a tels que $v_z(f) \neq 0$ est fini et que l'image de $\sum_{z\in X_a} v_z(f)\,z$ dans $\mathbf{C}/\Lambda$ ne dépend pas de $a \in \mathbf{C}$. On la note $\pi(f)$.

(b) Soit $a \in \mathbf{C}$ tel que f n'ait ni zéro ni pôle sur le chemin γ_a. Montrer que

$$I_1 = \frac{1}{2i\pi}\Big(\int_a^{a+\omega_1} z\frac{f'(z)}{f(z)}\,dz + \int_{a+\omega_1+\omega_2}^{a+\omega_2} z\frac{f'(z)}{f(z)}\,dz\Big) \quad \text{et} \quad I_2 = \frac{1}{2i\pi}\Big(\int_{a+\omega_1}^{a+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}\,dz + \int_{a+\omega_2}^{a} z\frac{f'(z)}{f(z)}\,dz\Big)$$

appartiennent à Λ. (On ne traitera que I_1 ou I_2.)

(c) En déduire que $\pi(f) = 0$.

14. Ça prend moins de place si α et β sont compliqués.

(xi) Soit $\overline{\mathrm{E}}(\mathbf{C}) = \mathrm{E}(\mathbf{C}) \cup \{\infty\}$. On étend l'application $z \mapsto \mathrm{P}(z)$ de la question (vi) en une bijection de $\mathbf{C}/\Lambda$ sur $\overline{\mathrm{E}}(\mathbf{C})$, en posant $\mathrm{P}(0) = \infty$, et on note $\iota : \overline{\mathrm{E}}(\mathbf{C}) \to \mathbf{C}/\Lambda$ la bijection réciproque. On définit $\mathrm{Q}_1 \oplus \mathrm{Q}_2$, si $\mathrm{Q}_1, \mathrm{Q}_2 \in \overline{\mathrm{E}}(\mathbf{C})$ par $\mathrm{Q}_1 \oplus \mathrm{Q}_2 = \mathrm{P}(\iota(\mathrm{Q}_1) + \iota(\mathrm{Q}_2))$. Montrer que $\oplus$ est une loi de groupe commutatif d'élément neutre ∞ sur $\overline{\mathrm{E}}(\mathbf{C})$, et que, si $\mathrm{Q}_1, \mathrm{Q}_2, \mathrm{Q}_3 \in \mathrm{E}(\mathbf{C})$ sont distincts, alors $\mathrm{Q}_1 \oplus \mathrm{Q}_2 \oplus \mathrm{Q}_3 = \infty$ si et seulement si $\mathrm{Q}_1, \mathrm{Q}_2, \mathrm{Q}_3$ sont sur une même droite complexe de $\mathbf{C}^2$. (On pourra s'intéresser aux zéros de la fonction $\mathrm{G}(z)$, déterminant des vecteurs $(\mathrm{F}(z), \mathrm{F}'(z), 1)$, $(\mathrm{F}(z_1), \mathrm{F}'(z_1), 1)$ et $(\mathrm{F}(z_2), \mathrm{F}'(z_2), 1)$.)

Corrigé

Partie I

(o) L'application $(a, b) \mapsto a\omega_1 + b\omega_2$ est un isomorphisme de $\mathbf{R}^2$ sur $\mathbf{C}$ et $(a, b) \mapsto |a\omega_1 + b\omega_2|$ est une norme sur $\mathbf{R}^2$; elle est donc équivalente à la norme $\|(a, b)\| = \sup(|a|, |b|)$ (on est en dimension finie) ; on en déduit l'existence de $\mathrm{C} > 0$ tel que $|a\omega_1 + b\omega_2| \geqslant \mathrm{C} \sup(|a|, |b|)$, quels que soient $a, b \in \mathbf{R}$. Finalement, on a $r(\Lambda) \geqslant \mathrm{C} > 0$.

(i) A est compact car c'est l'image du compact $[0, 1] \times [0, 1]$ par l'application $(\alpha, \beta) \mapsto \alpha\omega_1 + \beta\omega_2$, qui est continue. On peut écrire z sous la forme $a\omega_1 + b\omega_2$, avec $a, b \in \mathbf{R}$, et il suffit de poser $\omega = [a]\omega_1 + [b]\omega_2$ et $u = \{a\}\omega_1 + \{b\}\omega_2$ pour obtenir une décomposition de z sous la forme $z = \omega + u$ voulue. On en déduit que, si f est Λ-périodique, on a $f(\mathbf{C}) = f(\mathrm{A})$, et comme A est compact, si f est de plus continue, cela implique que f est bornée et atteint son maximum sur A.

(ii) Si F est Λ-périodique, holomorphe sur $\mathbf{C}$, alors $f = |\mathrm{F}|$ est continue et Λ-périodique. D'après la question (i), cela implique que $|\mathrm{F}|$ atteint son maximum, et d'après le th. de Liouville (th. V.3.11), cela implique que F est constante.

(iii) D'après la question (o), on a $\sum_{\omega \in \Lambda - \{0\}} \frac{1}{|\omega|^k} \leqslant \mathrm{C}^{-k} \sum_{(n,m) \in \mathbf{Z}^2 - \{(0,0)\}} \frac{1}{\sup(|m|, |n|)^k}$. Or il y a $8\mathrm{N}$ couples (m, n) vérifiant $\sup(|m|, |n|) = \mathrm{N}$, ce qui nous fournit la majoration

$$\sum_{\omega \in \Lambda - \{0\}} \frac{1}{|\omega|^k} \leqslant \mathrm{C}^{-k} \sum_{\mathrm{N}=1}^{+\infty} \frac{8\mathrm{N}}{\mathrm{N}^k} \leqslant 8\mathrm{C}^{-k} \zeta(k-1) < +\infty, \quad \text{si } k > 2.$$

(iv) On a $\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \frac{2\omega z + z^2}{\omega^2(\omega+z)^2}$ et $|\omega + z| \geqslant |\omega| - |z| \geqslant \frac{|\omega|}{2}$, si $|\omega| \geqslant 2\mathrm{R}$ et $z \in \mathrm{D}(0, \mathrm{R})$. En particulier, $z + \omega$ ne s'annule pas sur $\mathrm{D}(0, \mathrm{R})$, et on a

$$\Big|\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\Big| \leqslant \frac{2|\omega|\mathrm{R} + \mathrm{R}^2}{|\omega|^4/4} = \frac{8\mathrm{R}}{|\omega|^3} + \frac{4\mathrm{R}^2}{|\omega|^4},$$

si $z \in \mathrm{D}(0, \mathrm{R})$ et $|\omega| \geqslant 2\mathrm{R}$. On déduit la convergence normale de la première série sur $\mathrm{D}(0, \mathrm{R})$ de la question (iii). Pour démontrer celle de la seconde, on remarque que $|\frac{1}{(\omega+z)^3}| \leqslant \frac{8}{|\omega|^3}$, si $z \in \mathrm{D}(0, \mathrm{R})$ et $|\omega| \geqslant 2\mathrm{R}$, et on conclut de la même manière.

(v) $\mathrm{F}(z)$ est la somme, sur $\mathrm{D}(0, \mathrm{R}^-)$ de la somme finie $\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\},\, |\omega| < 2\mathrm{R}} \big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\big)$, dont chacun des termes est une fonction holomorphe en dehors de Λ, et de la série normalement convergente $\sum_{\omega \in \Lambda,\, |\omega| \geqslant 2\mathrm{R}} \big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\big)$ qui est holomorphe sur $\mathrm{D}(0, \mathrm{R}^-)$ d'après le th. V.5.1. On en déduit l'holomorphie de F sur $\mathrm{D}(0, \mathrm{R}^-) - \Lambda$ et, ceci étant vrai pour tout R, l'holomorphie de F sur $\mathbf{C} - \Lambda$.

(vi) La convergence de la série $\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\big)$ étant uniforme sur tout compact de $\mathbf{C} - \Lambda$, on peut calculer la dérivée de F en dérivant la série terme à terme (th. V.5.1) ; on a donc $\mathrm{F}'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z+\omega)^3}$. Maintenant, si $\alpha \in \Lambda$, on a $\mathrm{F}'(z + \alpha) = \sum_{\omega \in \Lambda} \frac{-2}{(z+\alpha+\omega)^3}$, et la série étant absolument convergente, elle peut se sommer dans l'ordre que l'on veut et on peut utiliser le fait que $\omega \mapsto \alpha + \omega$ est une bijection de Λ pour en déduire que $\mathrm{F}'(z + \alpha) = \mathrm{F}'(z)$.

La parité de F résulte de ce que $\big(\frac{1}{(-z+\omega)^2} - \frac{1}{\omega^2}\big) = \big(\frac{1}{(z-\omega)^2} - \frac{1}{(-\omega)^2}\big)$, et $\omega \mapsto -\omega$ est une bijection de Λ.

Maintenant, si $\omega \in \Lambda$, la fonction $\mathrm{F}(z+\omega)-\mathrm{F}(z)$ a une dérivée nulle et donc est constante sur $\mathbf{C}-\Lambda$. Notons $c(\omega)$ cette constante. On a $c(-\omega)=c(\omega)$ car F est paire, et

$$c(\omega_1+\omega_2)=\mathrm{F}(z+\omega_1+\omega_2)-\mathrm{F}(z+\omega_1)+\mathrm{F}(z+\omega_1)-\mathrm{F}(z)=c(\omega_2)+c(\omega_1).$$

En prenant $\omega_1=\omega$ et $\omega_2=-\omega$, on en déduit que $2c(\omega)=0$, et donc que F est Λ-périodique.
(vii) La fonction $\mathrm{G}(z)$ est holomorphe sur $\mathbf{C}-(\Lambda-\{0\})$, mais a un pôle en tous les éléments de $\Lambda-\{0\}$. Le plus grand disque ouvert de centre 0 contenu dans $\mathbf{C}-(\Lambda-\{0\})$ étant $\mathrm{D}(0,r(\Lambda)^-)$ par définition de $r(\Lambda)$, la série de Taylor de G en 0 a pour rayon de convergence $r(\Lambda)$ d'après le (i) de la rem. V.4.9 Maintenant, $\mathrm{G}(0)=0$ d'après la formule définissant F, et, d'après le th. V.5.1, on peut calculer $\mathrm{G}^{(n)}(0)$ comme la somme de la série des dérivées ; on obtient, si $n \geqslant 1$,

$$\mathrm{G}^{(n)}(0)=\sum_{\omega\in\Lambda-\{0\}}\frac{(-1)^n(n+1)!}{\omega^{n+2}}=(-1)^n(n+1)!\mathrm{G}_{n+2}.$$

Comme, d'après le (i) de la rem. V.4.9, on a $\mathrm{G}(z)=\sum_{n=0}^{+\infty}\frac{\mathrm{G}^{(n)}(0)}{n!}z^n$, si $|z|<r(\Lambda)$, cela permet de conclure.
(viii) La fonction G étant paire, on a $\mathrm{G}_k=0$, si k est impair, et donc

$$\mathrm{F}(z)=\frac{1}{z^2}+3\mathrm{G}_4z^2+5\mathrm{G}_6z^4+\mathrm{O}(z^5)\quad\text{et}\quad\mathrm{F}'(z)=\frac{-2}{z^3}+6\mathrm{G}_4z+20\mathrm{G}_6z^3+\mathrm{O}(z^4)$$
$$\mathrm{F}(z)^3=\frac{1}{z^6}+\frac{9\mathrm{G}_4}{z^2}+15\mathrm{G}_6+\mathrm{O}(z)\quad\text{et}\quad(\mathrm{F}'(z))^2=\frac{4}{z^6}-\frac{24\mathrm{G}_4}{z^2}-80\mathrm{G}_6+\mathrm{O}(z)$$

On en déduit que $\mathrm{H}(z)$ se prolonge en une fonction holomorphe nulle en 0.
(ix) La fonction $\mathrm{H}(z)$ est Λ-périodique, holomorphe sur $\mathbf{C}-\Lambda$ et holomorphe en 0. Par Λ-périodicité, elle est aussi holomorphe en tous les points de Λ, et donc est holomorphe sur $\mathbf{C}$. Elle est donc constante, d'après la question (ii), et comme elle vaut 0 en 0, elle est identiquement nulle.

Partie II.

(i) Soit $k=v_a(f)$. Alors $g(z)=(z-a)^{-k}f(z)$ est holomorphe dans un voisinage de a et non nulle en a ; il existe donc $r_a>0$ tel que g ne s'annule pas sur $\mathrm{D}(a,r_a^-)$, et alors f n'a ni zéro ni pôle sur $\mathrm{D}(a,r_a^-)-\{a\}$. Maintenant, si K est compact, on peut extraire un recouvrement fini [15] du recouvrement de K par les $\mathrm{D}(a,r_a^-)$, pour $a\in\mathrm{K}$; autrement dit, il existe un sous-ensemble fini A de K tel que $\mathrm{K}\subset\cup_{a\in\mathrm{A}}\mathrm{D}(a,r_a^-)$. Par construction de r_a, l'ensemble des zéros et pôles de f sur K est alors inclus dans A, et donc est fini.
(ii) Soit $\mathrm{B}=\{\alpha\omega_1+\beta\omega_2,\ \alpha,\beta\in[-1,1]\}$. Comme B est compact, f n'a qu'un nombre fini de zéros et de pôles dans B d'après la question (i). Si les zéros et pôles de f dans B sont les $\alpha_i\omega_1+\beta_i\omega_2$, pour $i\in\mathrm{I}$ fini, il suffit de prendre a de la forme $\alpha\omega_1+\beta\omega_2$, où $\alpha\in[-1,0]$ n'est pas de la forme α_i ou α_i-1, et $\beta\in[-1,0]$ n'est pas de la forme β_i ou β_i-1, pour $i\in\mathrm{I}$.
(iii) Si $w\in\Omega_a$, le résidu de $\frac{f'(z)}{f(z)}$ en w est $v_w(f)$; on déduit donc de la formule des résidus que $\frac{1}{2i\pi}\int_{\gamma_a}\frac{f'(z)}{f(z)}\,dz=\sum_{w\in\Omega_a}v_w(f)$. Par ailleurs, comme f n'a ni zéro ni pôle sur $\mathrm{S}_a-\Omega_a$, cette dernière somme est aussi égale à $\sum_{w\in\mathrm{S}_a}v_w(f)=\mathrm{N}_0(f)-\mathrm{N}_\infty(f)$.

Comme $\frac{f'(z)}{f(z)}$ est Λ-périodique, on a $\int_{a+\omega_1+\omega_2}^{a+\omega_2}\frac{f'(z)}{f(z)}\,dz=\int_{a+\omega_1}^{a}\frac{f'(z+\omega_2)}{f(z+\omega_2)}\,dz=-\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}\,dz$. On a donc $\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}\,dz+\int_{a+\omega_1+\omega_2}^{a+\omega_2}\frac{f'(z)}{f(z)}\,dz=0$ et $\int_{a+\omega_1}^{a+\omega_1+\omega_2}\frac{f'(z)}{f(z)}\,dz+\int_{a+\omega_2}^{a}\frac{f'(z)}{f(z)}\,dz=0$. On en déduit que $\int_{\gamma_a}\frac{f'(z)}{f(z)}\,dz=0$, et donc que $\mathrm{N}_0(f)=\mathrm{N}_\infty(f)$.

15. On peut aussi raisonner en termes de suites, en disant que, si l'ensemble Z des zéros et pôles de f dans K est infini, et si $(a_n)_{n\in\mathbf{N}}$ est une suite d'éléments distincts de Z, alors on peut extraire de $(a_n)_{n\in\mathbf{N}}$ une sous-suite ayant une limite a dans K, mais alors $\mathrm{D}(a,r_a^-)$ contient une infinité de a_n, ce qui est contraire à la définition de r_a.

(iv) F' a un pôle d'ordre 3 en 0 et est holomorphe en dehors de Λ ; on a donc $\mathrm{N}_\infty(\mathrm{F}') = 3$. Par ailleurs, F étant paire, F' est impaire et $\mathrm{F}'(z) = 0$, si $z = -z$ dans $\mathbf{C}/\Lambda$. On en déduit que e_1, e_2 et e_3 sont des zéros de F' dans $\mathbf{C}/\Lambda$. Comme $\mathrm{N}_0(\mathrm{F}') = \mathrm{N}_\infty(\mathrm{F}') = 3$, ce sont les seuls zéros de F' et ils sont simples.
(v) Si $b \in \mathbf{C}$, la fonction $\mathrm{F}(z) - b$ a un pôle double en 0 et est holomorphe en dehors de Λ. On a donc $\mathrm{N}_\infty(\mathrm{F} - b) = 2$, et aussi $\mathrm{N}_0(\mathrm{F} - b) = 2$, ce qui implique en particulier que l'ensemble des solutions de l'équation $\mathrm{F}(z) = b$ dans $(\mathbf{C}/\Lambda) - \{0\}$ n'est pas vide. On en déduit la surjectivité de $\mathrm{F} : (\mathbf{C}/\Lambda) - \{0\} \to \mathbf{C}$.

Maintenant, la fonction F étant paire, si a est une solution de $\mathrm{F}(z) = b$, alors $-a$ aussi. Comme $\mathrm{N}_0(\mathrm{F} - b) = 2$, ce sont les seules solutions si $a \neq -a$, c'est-à-dire si $a \notin \{e_1, e_2, e_3\}$. On en déduit que, si $\mathrm{F}(a) \notin \{\mathrm{F}(e_1), \mathrm{F}(e_2), \mathrm{F}(e_3)\}$, et si $\mathrm{F}(a') = \mathrm{F}(a)$, alors $a' = \pm a$.

Si $a \in \{e_1, e_2, e_3\}$, comme $\mathrm{F}'(a) = 0$ d'après le (i), la fonction $\mathrm{F}(z) - \mathrm{F}(a)$ a un zéro double en $z = a$, et comme $\mathrm{N}_0(\mathrm{F}(z) - \mathrm{F}(a)) = 2$, ce zéro est l'unique zéro de $\mathrm{F}(z) - \mathrm{F}(a)$ dans $\mathbf{C}/\Lambda$; on en déduit encore dans ce cas que $\mathrm{F}(a') = \mathrm{F}(a)$ si et seulement si $a' = \pm a$ (et $a = -a$).
(vi) L'appartenance de $\mathrm{P}(z)$ à $\mathrm{E}(\mathbf{C})$ résulte de la question (ix) de la partie I. Si $\mathrm{P}(z_1) = \mathrm{P}(z_2)$, on a en particulier $\mathrm{F}(z_1) = \mathrm{F}(z_2)$, et donc $z_1 = \pm z_2$ d'après la question (v). Si $z_1 = -z_2$, alors $\mathrm{F}'(z_2) = -\mathrm{F}'(z_1)$, et donc $\mathrm{P}(z_1) = \mathrm{P}(z_2)$ et $z_1 \neq z_2$ impliquent $\mathrm{F}'(z_1) = 0$. Or ceci implique $z_1 \in \{e_1, e_2, e_3\}$, et donc $z_1 = -z_1$ et $z_1 = z_2$. On en déduit l'injectivité de $z \mapsto \mathrm{P}(z)$. Pour prouver la surjectivité, il suffit de constater que si $(a, b) \in \mathrm{E}(\mathbf{C})$, il existe z tel que $\mathrm{F}(z) = a$, et alors $\mathrm{F}'(z) = \pm b$, ce qui fait que $(a, b) = \mathrm{P}(z)$ ou $(a, b) = \mathrm{P}(-z)$.
(vii) cf. prop. VI.2.3.
(viii) $\Omega_r(a, b)$ est la réunion des $\mathrm{D}(c, r^-)$, pour $c \in [a, a + \omega]$, et donc est un ouvert en tant que réunion d'ouverts. Si $z_1, z_2 \in \Omega_r$, il existe $c_1, c_2 \in [a, a+\omega]$ tels que $|z_i - c_i| < r$, si $i = 1, 2$. Maintenant, si $t \in [0, 1]$, alors $tc_1 + (1-t)c_2 \in [a, a + \omega]$ et $|(tz_1 + (1-t)z_2) - (tc_1 + (1-t)c_2)| = |t(z_1 - c_1) + (1-t)(z_2 - c_2)| < r(t + (1-t)) = r$, ce qui prouve que $tz_1 + (1-t)z_2 \in \Omega_r(a, b)$, et que $\Omega_r(a, b)$ est convexe.
(ix) $\Omega_1(a, a + \omega)$ est un ouvert borné contenant $[a, a + \omega]$. Son adhérence K est un compact et donc ne contient qu'un nombre fini de zéros et de pôles de f, d'après la question (i). Il suffit de prendre pour r le minimum des distances de ces zéros et pôles au segment $[a, a + \omega]$ pour être sûr que $\Omega_r(a, a + \omega)$ ne contient ni zéro ni pôle de f.

Un ouvert convexe étant contractile, il existe g holomorphe sur $\Omega_r(a, a + \omega)$ telle que $e^g = f$, et donc $g' = \frac{f'}{f}$. On a alors $\int_a^{a+\omega} \frac{f'(z)}{f(z)}\, dz = g(a + \omega) - g(a)$, et donc $\exp(\int_a^{a+\omega} \frac{f'(z)}{f(z)}\, dz) = f(a + \omega)/f(a) = 1$, puisque f est Λ-périodique. On en déduit que $\int_a^{a+\omega} \frac{f'(z)}{f(z)}\, dz \in 2i\pi\mathbf{Z}$.
(x) (a) Comme S_a est borné, l'ensemble des zéros et des pôles de f dans l'adhérence de S_a est fini ; il en est donc a fortiori de même dans S_a. Par ailleurs, si on change a en b, alors $z \mapsto s_b(\pi(z))$ est une bijection de S_a sur S_b qui induit une bijection de X_a sur X_b, et on a $z - s_b(\pi(z)) \in \Lambda$ et $v_z(f) = v_{s_b(\pi(z))}(f)$. On en déduit que

$$\sum_{z \in \mathrm{X}_a} v_z(f)\, z - \sum_{z \in \mathrm{X}_b} v_z(f)\, z = \sum_{z \in \mathrm{X}_a} v_z(f)(z - s_b(\pi(z))) \in \Lambda,$$

et donc que $\pi(f)$ est bien indépendant de a.

(b) $\int_{a+\omega_1+\omega_2}^{a+\omega_2} z \frac{f'(z)}{f(z)}\, dz = \int_{a+\omega_1}^{a} (z + \omega_2) \frac{f'(z+\omega_2)}{f(z+\omega_2)}\, dz = \int_{a+\omega_1}^{a} (z + \omega_2) \frac{f'(z)}{f(z)}\, dz$ puisque f est Λ-périodique. On en déduit que $\mathrm{I}_1 = \frac{-1}{2i\pi} \int_a^{a+\omega_1} \omega_2 \frac{f'(z)}{f(z)}\, dz$, et comme $\frac{1}{2i\pi} \int_a^{a-\omega_1} \frac{f'(z)}{f(z)}\, dz \in \mathbf{Z}$ d'après la question (ix), on a $\mathrm{I}_1 \in \mathbf{Z}\omega_2 \subset \Lambda$. L'argument est le même pour I_2.

(c) Il résulte du (b) que $\frac{1}{2i\pi} \int_{\gamma_a} z \frac{f'(z)}{f(z)}\, dz = \mathrm{I}_1 + \mathrm{I}_2 \in \Lambda$. Par ailleurs, il résulte de la formule des résidus que $\frac{1}{2i\pi} \int_{\gamma_a} z \frac{f'(z)}{f(z)}\, dz = \sum_{u \in \Omega_a} v_u(f)\, u$, et comme f n'a ni zéro ni pôle sur $\mathrm{S}_a - \Omega_a$, on a $\sum_{u \in \mathrm{S}_a} v_u(f)\, u = \sum_{u \in \Omega_a} v_u(f)\, u \in \Lambda$. L'image $\pi(f)$ de $\sum_{u \in \mathrm{S}_a} v_u(f)\, u$ dans $\mathbf{C}/\Lambda$ est donc nulle.

(xi) Par construction, $Q_1 \oplus Q_2 = Q_3$ si et seulement si $\iota(Q_1) + \iota(Q_2) = \iota(Q_3)$. Comme $(\mathbf{C}/\Lambda, +)$ est un groupe commutatif d'élément neutre 0, et comme ι est une bijection de $\overline{E}(\mathbf{C})$ sur $\mathbf{C}/\Lambda$, cela implique que $(\overline{E}(\mathbf{C}), \oplus)$ est un groupe commutatif d'élément neutre $\iota^{-1}(0) = \infty$.

Maintenant, $Q_1, Q_2, Q_3 \in E(\mathbf{C})$ sont distincts et vérifient $Q_1 \oplus Q_2 \oplus Q_3 = \infty$ si et seulement si $z_1 = \iota(Q_1)$, $z_2 = \iota(Q_2)$ et $z_3 = \iota(Q_3)$ sont distincts, non nuls, et vérifient $z_1 + z_2 + z_3 = 0$. En particulier, $z_1 \neq \pm z_2$, et donc $F(z_1) \neq F(z_2)$. Ceci implique que si on écrit $G(z)$ sous la forme $\alpha F(z) + \beta F'(z) + \gamma$, alors $\beta \neq 0$ puisque $\beta = F(z_2) - F(z_1)$.

Comme F' a un pôle d'ordre 3 en $z = 0$, et F a un pôle d'ordre 2, le pôle en $z = 0$ de $\beta F' + \alpha F + \gamma$ est d'ordre 3 exactement. On a donc $N_\infty(G) = 3$, et on déduit de la question (iii) que G a 3 zéros dans $\mathbf{C}/\Lambda$ comptés avec multiplicité.

Il est clair que z_1 et z_2 sont deux zéros de G, et si z' est le troisième, alors $\pi(G) = z_1 + z_2 + z' - 3 \cdot 0$. Il résulte alors du (c) de la question (x) que $z_1 + z_2 + z' = 0$, et donc $z' = z_3$. On a donc prouvé que $G(z) = 0$ si et seulement si $z \in \{z_1, z_2, z_3\}$.

Par ailleurs $\alpha X + \beta Y + \gamma = 0$ est l'équation de la droite passant par $P(z_1) = Q_1$ et $P(z_2) = Q_2$; on en déduit que $G(z) = 0$ si et seulement si $P(z)$ appartient à la droite (Q_1, Q_2). Ceci permet de conclure.

H.9. Coefficients de Fourier des fonctions analytiques

On dit que $f : \mathbf{R} \to \mathbf{C}$ est *analytique* si, pour tout $a \in \mathbf{R}$, il existe $\delta > 0$ tel que f soit somme de sa série de Taylor en a pour tout $x \in]a-\delta, a+\delta[$. On se propose de démontrer qu'*une fonction périodique est analytique si et seulement si la suite de ses coefficients de Fourier* $(c_n(f))_{n\in\mathbf{Z}}$ *est à décroissance exponentielle* (i.e. il existe $r > 1$ tel que $|r^{|n|}c_n(f)| \to 0$ quand $|n| \to +\infty$).

Question 1. (i) Montrer que, si F est holomorphe sur un ouvert Ω contenant $\mathbf{R}$, alors la restriction de F à $\mathbf{R}$ est analytique.

(ii) Soit $(a_n)_{n\in\mathbf{Z}}$ telle qu'il existe $r < 1$ et $C > 0$, avec $|a_n| \leqslant Cr^{|n|}$, pour tout $n \in \mathbf{Z}$. Montrer que la série $\sum_{n\in\mathbf{N}} a_n e^{2i\pi\, nt}$ converge pour tout $t \in \mathbf{R}$ et définit une fonction analytique sur $\mathbf{R}$, périodique de période 1.

Question 2. (i) Montrer que si f est analytique sur $\mathbf{R}$, alors pour tout $a \in \mathbf{R}$, il existe un disque ouvert D_a de centre a et une fonction holomorphe F_a sur D_a dont la restriction à $\mathbf{R} \cap D_a$ est f.

(ii) Montrer que, si $D_a \cap D_b \neq \varnothing$, alors F_a et F_b coïncident sur $D_a \cap D_b$. En déduire qu'il existe un ouvert Ω de $\mathbf{C}$ contenant $\mathbf{R}$, et une fonction holomorphe F sur Ω dont la restriction à $\mathbf{R}$ est f.

(iii) Montrer qu'un ouvert Ω de $\mathbf{C}$ contenant $\mathbf{R}$ contient un ouvert rectangulaire de la forme $\Omega(\delta) = \{z,\ -\delta < \mathrm{Re}(s) < 1+\delta,\ |\mathrm{Im}(z)| < \delta\}$.

(iv) On suppose $f : \mathbf{R} \to \mathbf{C}$ analytique et périodique de période 1. Soit Ω un ouvert de $\mathbf{C}$ contenant $\mathbf{R}$ sur lequel il existe une fonction holomorphe F dont la restriction à $\mathbf{R}$ est f, et soit $\delta > 0$ tel que $\Omega(\delta)$ soit contenu dans Ω. Montrer que pour tout $r \in]e^{-2\pi\delta}, 1[$, il existe $C(r) > 0$ tel que $|c_n(f)| \leqslant C(r)r^{|n|}$, pour tout $n \in \mathbf{Z}$.

(v) Conclure.

Corrigé

Question 1. (i) Il suffit de revenir à la définition d'une fonction holomorphe : si $a \in \mathbf{R}$, alors F est somme de sa série de Taylor en a sur un petit disque de centre a, elle est donc a fortiori somme de sa série de Taylor sur un segment de la forme $]a-\delta, a+\delta[$.

(ii) La série $\sum_{n\in\mathbf{N}} a_n e^{2i\pi\, nz}$ est normalement convergente dans la bande $|\mathrm{Im}(z)| < \delta$, si $re^{2\pi\delta} < 1$ (i.e. si $\delta < \frac{1}{2\pi}\log\frac{1}{r}$). Elle définit donc une fonction holomorphe, périodique de période 1, sur cette bande puisque chacun des termes de la série est holomorphe et périodique de période 1. Sa restriction à $\mathbf{R}$ est donc analytique d'après le (i), ce qui permet de conclure.

Question 2. (i) Par hypothèse, il existe $\delta > 0$ tel que $f(t) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(t-a)^n$, quel que soit $t \in]a-\delta, a+\delta[$. En particulier, la série $\sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}T^n$ est de rayon de convergence $> \delta$ et il suffit de prendre $D_a = D(a, \delta^-)$ et $F_a(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n$, si $z \in D_a$.

(ii) Si $D_a \cap D_b \neq \varnothing$, alors $D_a \cap D_b$ est connexe (car convexe et donc connexe par arcs), et son intersection avec $\mathbf{R}$ est un intervalle ouvert I non vide. Par ailleurs, F_a et F_b coïncident sur I, et le théorème des zéros isolés implique que F_a et F_b coïncident sur $D_a \cap D_b$ tout entier.

Ceci permet de définir une fonction F sur l'ouvert $\Omega = \cup_{a\in\mathbf{R}} D_a$ (qui contient $\mathbf{R}$ par construction), en posant $F(z) = F_a(z)$ si $z \in D_a$. Comme F_a et F_b coïncident sur $D_a \cap D_b$, on voit que la définition de $F(z)$ ne dépend pas du choix de $a \in \mathbf{R}$ tel que $z \in D_a$. De plus, F est holomorphe sur D_a pour tout a, et donc est holomorphe sur Ω tout entier.

(iii) Comme $[a,b]$ est compact, que $\mathbf{C}-\Omega$ est fermé et d'intersection vide avec $[a,b]$, la distance d de $[a,b]$ à $\mathbf{C}-\Omega$ est >0. On peut alors prendre $\delta = d/2$.

(iv) Comme $f(z)e^{-2i\pi nz}$ est holomorphe sur $\Omega_0 = \{z,\ -\delta < \mathrm{Re}(s) < 1+\delta,\ |\mathrm{Im}(z)| < \delta\}$ qui est contractile car convexe, l'intégrale de $f(z)e^{-2i\pi nz}dz$ sur le rectangle de sommets $0, 1, 1+ic, ic$ est nulle, pour tout choix de $c \in]-\delta,\delta[$. De plus, $f(z)e^{-2i\pi nz}$ étant périodique de période 1, les deux intégrales sur les côtés verticaux se compensent, et comme l'intégrale sur $[0,1]$ n'est autre que $c_n(f)$, on en déduit que $c_n(f) = e^{2\pi nc}\int_0^1 f(t+ic)e^{-2i\pi\, nt}\,dt$, pour tout $c \in]-\delta,\delta[$. En prenant $c = \frac{-\log r}{2\pi}$ si $n \leqslant 0$ et $c = \frac{\log r}{2\pi}$ si $n \geqslant 0$, et en posant $\mathrm{C}(r) = \sup_{t\in[0,1]} \max(|f(t+i\frac{\log r}{2\pi})|, |f(t-i\frac{\log r}{2\pi})|$, on obtient la majoration voulue.

(v) L'énoncé cherché est la conjonction des (ii) de la question 1 et (iv) de la question 2.

H.10. Prolongement analytique d'intégrales et de séries

Le but de ce devoir est d'illustrer la souplesse que procure la possibilité de déplacer le chemin sur lequel on intègre, et de montrer comment combiner cette souplesse avec la formule de Poisson pour prolonger analytiquement certaines séries.

Si $s \in \mathbf{C}$, on note $\phi_s : \mathbf{R} \to \mathbf{C}$ la fonction définie par la formule $\phi_s(t) = \frac{1}{(t^2+1)^s}$, la détermination du logarithme choisie étant la détermination principale (on rappelle qu'avec cette détermination, $|z^s| \leqslant e^{\pi\,|\mathrm{Im}(s)|}|z|^{\mathrm{Re}(s)}$, pour tous $z \in \mathbf{C}^*$ et $s \in \mathbf{C}$).

Question 1. Dans cette question, s est réel (et $> \frac{1}{2}$ pour le (i), $> \frac{3}{2}$ pour (ii)-(vi)).

(i) Calculer $\int_0^{+\infty} e^{-u(1+t^2)} u^s \frac{du}{u}$. En déduire que $\hat{\phi}_s(0) = \frac{\sqrt{\pi}\,\Gamma(s-\frac{1}{2})}{\Gamma(s)}$.

(ii) Montrer que $\hat{\phi}_s$ est de classe $\mathscr{C}^2$ et que $\hat{\phi}'_s$ est la transformée de Fourier de $\frac{-2i\pi t}{(t^2+1)^s}$.

(iii) Montrer que $\hat{\phi}_s$ et $\hat{\phi}'_s$ sont à décroissance rapide (on rappelle que f est à décroissance rapide si $|x^{\mathrm{N}} f(x)| \to 0$, pour tout $\mathrm{N} \in \mathbf{N}$, quand $|x| \to +\infty$).

(iv) Trouver une relation linéaire à coefficients dans $\mathbf{C}[t]$ entre ϕ_s, ϕ'_s et ϕ''_s. En déduire que $\psi_s(x) = \hat{\phi}_s(\frac{x}{2\pi})$ est solution de l'équation différentielle $x^2 v'' + 2(1-s)xv' - x^2 v = 0$.

(v) Montrer que $\hat{\phi}_s$ est de classe $\mathscr{C}^\infty$ sur $\mathbf{R}^*$ et que toutes ses dérivées sont à décroissance rapide. Existe-t-il $s > \frac{3}{2}$ tel que $\hat{\phi}_s$ soit de classe $\mathscr{C}^\infty$ sur $\mathbf{R}$?

(vi) Que peut-on attendre du comportement à l'infini de $\hat{\phi}_s$, compte-tenu des (iii) et (iv) ? (On demande juste un argument heuristique, pas une justification détaillée.)

Question 2. On note Ω l'ouvert obtenu en retirant au demi-plan $\mathrm{Im}(s) > -1$ la demi-droite $[i, i\infty[$; c'est un ouvert contractile car il est étoilé par rapport à tout point du segment $]-i, i[$. On note encore $\phi_s : \Omega \to \mathbf{C}$ la fonction $z \mapsto \frac{1}{(z^2+1)^s}$.

(i) Montrer que ϕ_s est holomorphe sur Ω.

(ii) Montrer que ϕ_s peut se prolonger en une fonction méromorphe sur le demi-plan $\mathrm{Im}(s) > -1$ si et seulement si $s \in \mathbf{Z}$.

(iii) Soit $\mathrm{U_N} = \{z,\ |\mathrm{Im}(z)| < \mathrm{N},\ |\mathrm{Re}(z)| < \mathrm{N}\}$. Montrer que, si $s \in \mathrm{U_N}$, si $\alpha \in \mathbf{R}_+ - \{1\}$ et si $t \in [-1,1]$, alors $\left|\frac{1}{(1+(i\alpha+t)^2)^s}\right| \leqslant \mathrm{C_N}(\alpha)$, où $\mathrm{C_N}(\alpha) = e^{\pi \mathrm{N}} \sup\left(\frac{1}{|1-\alpha^2|^{\mathrm{N}}}, (\alpha^4+4)^{\mathrm{N}/2}\right)$.

(iv) Montrer que, si $s \in \mathrm{U_N}$ et si $t \in \mathbf{R}$, alors $\left|\frac{1}{(1+(\pm 1+it)^2)^s}\right| \leqslant e^{\pi \mathrm{N}}(t^4+4)^{\mathrm{N}/2}$, si $t \in \mathbf{R}$.

Question 3. Si $0 < \alpha < 1$, on note γ_α le chemin constitué de la demi-droite verticale $\gamma_{1,\alpha} =]-1+i\infty, -1+i\alpha]$, du segment $\gamma_{2,\alpha} = [-1+i\alpha, 1+i\alpha]$ et de la demi-droite verticale $\gamma_{3,\alpha} = [1+i\alpha, 1+i\infty[$. Si $\xi < 0$, soit

$$\mathrm{F}_\alpha(s,\xi) = \int_{\gamma_\alpha} \frac{e^{-2i\pi\,\xi z}}{(1+z^2)^s} dz.$$

On note $\mathrm{I}_{1,\alpha}(s,\xi)$ (resp. $\mathrm{I}_{2,\alpha}(s,\xi)$, resp. $\mathrm{I}_{3,\alpha}(s,\xi)$) l'intégrale sur $\gamma_{1,\alpha}$ (resp. $\gamma_{2,\alpha}$, resp. $\gamma_{3,\alpha}$).

(i) Montrer que $s \mapsto \mathrm{I}_{2,\alpha}(s,\xi)$ est holomorphe sur $\mathbf{C}$ tout entier et $|\mathrm{I}_{2,\alpha}(s,\xi)| \leqslant 2\mathrm{C_N}(\alpha) e^{2\pi\alpha\xi}$, pour tous $\xi < 0$ et $s \in \mathrm{U_N}$.

(ii) Montrer que $s \mapsto \mathrm{I}_{1,\alpha}(s,\xi)$ et $s \mapsto \mathrm{I}_{3,\alpha}(s,\xi)$ sont holomorphes sur $\mathbf{C}$ tout entier et qu'il existe $\mathrm{C'_N}(\alpha)$ tel que $|\mathrm{I}_{1,\alpha}(s,\xi)| \leqslant \mathrm{C'_N}(\alpha) e^{2\pi\xi\alpha}$, si $i = 1, 3$, pour tous $\xi \leqslant -1$ et $s \in \mathrm{U_N}$. (On se contentera de traiter $\mathrm{I}_{1,\alpha}(s,\xi)$ car les arguments sont les mêmes pour $\mathrm{I}_{3,\alpha}(s,\xi)$.)

(iii) Montrer que $s \mapsto \mathrm{F}_\alpha(s,\xi)$ est holomorphe sur $\mathbf{C}$ tout entier et qu'il existe $\mathrm{C}''_{\mathrm{N}}(\alpha)$ tel que $|\mathrm{F}_\alpha(s,\xi)| \leqslant \mathrm{C}''_{\mathrm{N}}(\alpha)e^{2\pi\xi\alpha}$, pour tous $\xi \leqslant -1$ et $s \in \mathrm{U}_{\mathrm{N}}$.

Question 4. (i) Soit $f \in \mathrm{L}^1(\mathbf{R}_+)$. Montrer que $\int_\alpha^{+\infty} |f(t)|dt \to 0$ quand $\alpha \to +\infty$.

(ii) Montrer que $\mathrm{I}_{1,\alpha}(s,\xi) \to 0$ quand $\alpha \to +\infty$, puis que $\mathrm{F}_\alpha(s,\xi) \to 0$ quand $\alpha \to +\infty$.

(iii) En déduire, en termes du résidu de $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ en i, la valeur de $\mathrm{F}_\alpha(k,\xi)$, si $k \in \mathbf{Z}$. (On s'intéressera à $\mathrm{F}_\alpha(k,\xi) - \mathrm{F}_\beta(k,\xi)$, si $\alpha < \beta$, et on discutera suivant les positions de α, β et 1.)

(iv) En déduire que $\mathrm{F}_\alpha(k,\xi) = 0$, si $k \leqslant 0$, et calculer $\mathrm{F}_\alpha(k,\xi)$, si $\alpha \in]0,1[$, pour $k = 1, 2$.

Question 5. On suppose $\mathrm{Re}(s) > \frac{1}{2}$, ce qui fait que $\phi_s \in \mathrm{L}^1(\mathbf{R})$.

(i) Montrer que $\hat{\phi}_s(-x) = \hat{\phi}_s(x)$, pour tout $x \in \mathbf{R}$.

(ii) Si $\mathrm{R} > 1$, soit $\gamma_{\alpha,\mathrm{R}}$ le chemin composé des segments $[-\mathrm{R},\mathrm{R}]$, $[\mathrm{R},\mathrm{R}+i\mathrm{R}]$, $[\mathrm{R}+i\mathrm{R},1+i\mathrm{R}]$, $[1+i\mathrm{R},1+i\alpha]$, $[1+i\alpha,-1+i\alpha]$, $[-1+i\alpha,-1+i\mathrm{R}]$, $[-1+i\mathrm{R},-\mathrm{R}+i\mathrm{R}]$ et $[-\mathrm{R}+i\mathrm{R},-\mathrm{R}]$. Que vaut l'intégrale de $e^{-2i\pi\xi z}\phi_s(z)dz$ le long de ce chemin ? En déduire que $\mathrm{F}_\alpha(s,\xi) = \hat{\phi}_s(\xi)$, pour tout $\alpha \in]0,1[$.

(iii) Montrer qu'au voisinage de l'infini, $\hat{\phi}_s(\xi) = \mathrm{O}(e^{-2\pi\alpha|\xi|})$, pour tout $\alpha \in]0,1[$. Ceci s'accorde-t-il avec votre heuristique du (vi) de la question 1 ?

Question 6. (i) Montrer que $\sum_{n\in\mathbf{Z}} \frac{1}{1+n^2} = \pi\,\frac{1+e^{-2\pi}}{1-e^{-2\pi}}$ et $\sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^2} = \frac{\pi}{2}\,\frac{1+e^{-2\pi}}{1-e^{-2\pi}} + 2\pi^2\frac{e^{-2\pi}}{(1-e^{-2\pi})^2}$.

(ii) Montrer que la série $\sum_{n=1}^{+\infty} \mathrm{F}_{1/2}(s,-n)$ converge pour tout $s \in \mathbf{C}$, et que la somme $\mathrm{F}(s)$ est une fonction holomorphe sur $\mathbf{C}$ tout entier.

(iii) Montrer que $\mathrm{G}(s) = \sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^s}$ converge sur $\mathrm{Re}(s) > \frac{1}{2}$ et est holomorphe sur ce demi-plan.

(iv) Montrer que G admet un prolongement méromorphe à $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples aux $-k+\frac{1}{2}$, pour $k \in \mathbf{N}$.

(v) Que vaut $\mathrm{G}(-k)$, si $k \in \mathbf{N}$.

Question 7.

(i) Soit $f : [0,1] \to \mathbf{R}_+^*$ de classe $\mathscr{C}^\infty$, et soient $a, b \in \mathbf{R}$, $a > 0$. Montrer que la fonction $s \mapsto \int_0^1 t^{as+b} f(t)^s\,dt$ se prolonge en une fonction méromorphe sur $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples éventuels en les $\frac{-b-k}{a}$, avec k entier $\geqslant 1$. (On pourra utiliser la formule de Taylor avec reste intégral à l'ordre n pour $t \mapsto f(t)^s$.)

(ii) Soit P un polynôme unitaire, de degré $d \geqslant 2$, à coefficients réels, ne s'annulant pas sur $\mathbf{R}$. Montrer, que $\int_{-\infty}^{+\infty} \frac{1}{\mathrm{P}(t)^s}\,dt$ se prolonge en une fonction méromorphe sur $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples potentiels aux $\frac{1-k}{d}$, pour $k \in \mathbf{N}$.

(iii) Soient α (resp. A) le minimum des $|\mathrm{Im}(a)|$ (resp. le maximum des $|\mathrm{Re}(a)|$), pour a racine de P. Soient Ω^+ l'ouvert obtenu en retirant au demi-plan $\mathrm{Re}(s) > -\alpha$ la bande fermée $\{z,\ |\mathrm{Re}(z)| \leqslant \mathrm{A},\ \mathrm{Im}(z) \geqslant \alpha\}$ et Ω^- le symétrique de Ω^+ par rapport à l'axe réel. Montrer que $z \mapsto \frac{1}{\mathrm{P}(z)^s}$ se prolonge en une fonction holomorphe $\phi_{\mathrm{P},s}$ sur Ω^+ et sur Ω^-. (On pourra factoriser P et se ramener à ϕ_s.)

(iv) Montrer que $\mathrm{G}_{\mathrm{P}}(s) = \sum_{n\in\mathbf{Z}} \frac{1}{\mathrm{P}(n)^s}$ se prolonge en une fonction méromorphe sur $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples potentiels aux $\frac{1-k}{d}$, pour $k \in \mathbf{N}$.

Corrigé

Question 1. (i) Le changement de variable $v = (1+t^2)u$ fournit la formule $\int_0^{+\infty} e^{-u(1+t^2)} u^s \frac{du}{u} = \frac{\Gamma(s)}{(1+t^2)^s}$. Il en résulte que $\hat{\phi}_s(0) = \frac{1}{\Gamma(s)} \int_{-\infty}^{+\infty} \Big(\int_0^{+\infty} e^{-u(1+t^2)} u^s \frac{du}{u} \Big)\, dt$.

On peut alors utiliser Fubini pour les fonctions positives pour intervertir les deux intégrations, et comme $\int_{-\infty}^{+\infty} e^{-u(1+t^2)} dt = e^{-u} \int_{-\infty}^{+\infty} e^{-ut^2} dt = \sqrt{\frac{\pi}{u}}\, e^{-u}$ (le changement de variable $t = \sqrt{\frac{\pi}{u}} v$ nous ramène à l'intégrale de la gaussienne), on obtient finalement $\hat{\phi}_s(0) = \frac{\sqrt{\pi}}{\Gamma(s)} \int_0^{+\infty} e^{-u} u^{s-\frac{1}{2}} \frac{du}{u} = \frac{\sqrt{\pi}\,\Gamma(s-\frac{1}{2})}{\Gamma(s)}$.

(ii) La fonction $t \mapsto (1+t^2)\phi_s(t)$ étant sommable, le résultat suit du (ii) du th. IV.2.8.

(iii) La dérivée k-ième de ϕ_s est, comme le montre une récurrence immédiate, de la forme $t \mapsto \frac{\mathrm{P}_k(t)}{(t^2+1)^{s+k}}$, où P_k est un polynôme de degré k ; elle est donc sommable pour tout k, ce qui permet d'utiliser le (i) du th. IV.2.8, pour en déduire que $x^k \hat{\phi}_s \to 0$ en l'infini, pour tout $k \in \mathbf{N}$. Ceci permet de conclure pour $\hat{\phi}_s$. le raisonnement pour $\hat{\phi}'_s$ est identique : la dérivée k-ième de $t\phi_s(t)$ est de la forme $\frac{\mathrm{Q}_k(t)}{(t^2+1)^{s+k}}$, où Q_k est un polynôme de degré $k+1$; elle est donc sommable pour tout k.

(iv) On a $(t^2+1)\phi''_s + 2(s+1)t\phi'_s + 2s\phi_s = 0$. On en déduit que

$$\big(-\frac{d^2}{dx^2} + 1\big)(-x^2\psi_s) + 2(s+1)\frac{-i\,d}{dx}(-ix\psi_s) + 2s\psi_s = 0.$$

Le résultat s'en déduit par des calculs sans mystère.

(v) L'équation différentielle satisfaite par $\hat{\phi}_s$ montre, par récurrence, que $\hat{\phi}_s$ est de classe $\mathscr{C}^k$ sur $\mathbf{R}^*$ et que $\hat{\phi}_s^{(k)}$ est une combinaison linéaire de $\hat{\phi}_s$ et $\hat{\phi}'_s$, à coefficients dans $\mathbf{C}[\frac{1}{x}]$. Comme $\hat{\phi}_s$ et $\hat{\phi}'_s$ sont à décroissance rapide à l'infini, il en est de même de $\hat{\phi}_s^{(k)}$, pour tout k.

Si $\hat{\phi}_s$ est $\mathscr{C}^\infty$ sur $\mathbf{R}$, elle appartient à l'espace de Schwartz, et donc sa transformée de Fourier inverse aussi (cor. IV.3.17). Par ailleurs, comme ϕ_s et $\hat{\phi}_s$ sont dans L^1, la transformée de Fourier inverse de $\hat{\phi}_s$ est ϕ_s (prop. IV.3.25). Comme ϕ_s n'est pas à décroissance rapide, on aboutit à une contradiction qui prouve que $\hat{\phi}_s$ n'est jamais $\mathscr{C}^\infty$ sur $\mathbf{R}$.

(vi) Au voisinage de l'infini, l'équation différentielle satisfaite par $\hat{\phi}_s$ se rapproche de l'équation différentielle $v'' = 4\pi^2 v$ dont une base de solutions est constituée de $e^{2\pi x}$ et $e^{-2\pi x}$. Parmi les solutions de l'équation $v'' = 4\pi^2 v$, seuls les multiples de $e^{-2\pi x}$ (resp. $e^{2\pi x}$) n'explosent pas en $+\infty$ (resp. $-\infty$) ; on peut donc s'attendre à ce que $\hat{\phi}_s$ ressemble à un multiple de $e^{-2\pi x}$ au voisinage de $+\infty$ et de $e^{2\pi x}$ au voisinage de $-\infty$.

En fait, on a $\frac{\Gamma(s)}{\pi^s}\hat{\phi}_s(x) = |x|^{s-\frac{1}{2}} \mathrm{K}_{s-\frac{1}{2}}(2\pi|x|)$, où K_ν est la fonction de Bessel de l'ex. IV.1.9 donnée par la formule $\mathrm{K}_\nu(y) = \frac{1}{2}\int_0^{+\infty} e^{-y(t+t^{-1})/2} t^\nu \frac{dt}{t}$, si $\nu \in \mathbf{C}$ et $y \in \mathbf{R}_+^*$, ce qui permet d'utiliser le (ii) de cet exercice pour en déduire un équivalent de $\hat{\phi}_s$ au voisinage de l'infini. La formule précédente résulte du calcul ci-dessous, où l'on a utilisé successivement le (i), le th. de Fubini, le fait que la transformée de Fourier de e^{-ut^2} est $\sqrt{\frac{\pi}{u}} e^{u^{-1}\pi^2 x^2}$, et le changement de variable $u = \pi|x|w$:

$$\begin{aligned}
\hat{\phi}_s(x) &= \int_{\mathbf{R}} \frac{1}{(t^2+1)^s} e^{-2i\pi tx}\, dt = \frac{1}{\Gamma(s)} \int_{\mathbf{R}} \int_0^{+\infty} e^{-u(t^2+1)} u^s e^{-2i\pi tx}\, \frac{du}{u}\, dt \\
&= \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-u} u^s \frac{du}{u} \int_{\mathbf{R}} e^{-ut^2} e^{-2i\pi tx}\, dt \\
&= \frac{\sqrt{\pi}}{\Gamma(s)} \int_0^{+\infty} e^{-u-u^{-1}\pi^2x^2} u^{s-\frac{1}{2}} \frac{du}{u} \\
&= \frac{\pi^s}{\Gamma(s)} |x|^{s-\frac{1}{2}} \int_0^{+\infty} e^{-2\pi|x|(w+w^{-1})} w^{s-\frac{1}{2}} \frac{dw}{w}
\end{aligned}$$

Question 2. (i) L'image de Ω par $z \mapsto z^2+1$ est incluse dans $\mathbf{C}-\mathbf{R}_-$ et ϕ_s est la composée de $z \mapsto z^2+1$ de Ω dans $\mathbf{C}-\mathbf{R}_-$ avec $z \mapsto \exp(s \log z)$ de $\mathbf{C}-\mathbf{R}_-$ dans $\mathbf{C}$ qui sont toutes les deux holomorphes. On en déduit l'holomorphie de ϕ_s.

(ii) Si $s \in \mathbf{Z}$, la fonction $z \mapsto \frac{1}{(z^2+1)^s}$ est méromorphe sur $\mathbf{C}$ tout entier (et même holomorphe si $s<0$), comme quotient de deux fonctions holomorphes sur $\mathbf{C}$.

Par ailleurs, si $a>1$ et si ε tend vers 0, alors $(ia+\varepsilon)^2+1 = 1+\varepsilon^2-a^2+2ia\varepsilon$ tend vers un nombre négatif avec une partie imaginaire positive si $\varepsilon>0$ et négative si $\varepsilon<0$. Il en résulte que les limites en $ia+0^+$ et $ia+0^-$ de $\log(z^2+1)$ différent de $2i\pi$ et donc que celles de $\frac{1}{(z^2+1)^s}$ diffèrent d'une multiplication par $e^{-2i\pi s}$, qui n'est pas égal à 1 si $s \notin \mathbf{Z}$. On ne peut donc prolonger par continuité ϕ_s en aucun point de la demi-droite $[i, i\infty[$, et donc ϕ_s ne se prolonge à aucun ouvert de $\mathrm{Im}(s) > -1$ contenant strictement Ω.

(iii) On a $|1+(i\alpha+t)|^2 = (1-\alpha^2)^2+t^4+2t^2+2t^2\alpha^2$, et donc $(1-\alpha^2)^2 \leqslant |1+(i\alpha+t)|^2 \leqslant \alpha^4+4$, si $|t| \leqslant 1$. Il en résulte que $\left|\frac{1}{(1+(i\alpha+t)^2)^s}\right| \leqslant e^{\pi|\mathrm{Im}(s)|} \sup\left(\frac{1}{|1-\alpha^2|^{\mathrm{Re}(s)}}, (\alpha^4+4)^{\mathrm{Re}(s)/2}\right)$, et le résultat suit de l'appartenance de s à $\mathrm{U_N}$.

(iv) On a $|1+(\pm 1+it)^2|^2 = t^4+4$, et donc $\left|\frac{1}{(1+(\pm 1+it)^2)^s}\right| \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}}{(t^4+4)^{\mathrm{Re}(s)/2}}$, et le résultat suit de l'appartenance de s à $\mathrm{U_N}$.

Question 3. (i) Soit $g(t,s) = \frac{e^{-2i\pi\xi(i\alpha+t)}}{(1+(i\alpha+t)^2)^s}$ de telle sorte que $\mathrm{I}_{2,\alpha}(s,\xi) = -\int_{-1}^{1} g(t,s)\,dt$.

• Si $t \in [-1,1]$ est fixé, alors $s \mapsto g(t,s)$ est holomorphe sur $\mathrm{U_N}$.

• $|g(t,s)| = \frac{e^{2\pi\xi\alpha}}{|(1+(i\alpha+t)^2)^s|} \leqslant \mathrm{C_N}(\alpha)e^{2\pi\xi\alpha}$, pour tous $t \in [-1,1]$ et $s \in \mathrm{U_N}$, d'après le (iii) de la question 2.

Comme $t \mapsto \mathrm{C_N}(\alpha)e^{2\pi\xi\alpha}$ est sommable sur $[-1,1]$, on est dans les conditions d'application du th. V.5.7, ce qui montre que $s \mapsto \mathrm{I}_{2,\alpha}(s,\xi)$ est holomorphe sur $\mathrm{U_N}$. Comme ceci est vrai pour tout N, elle est aussi holomorphe sur $\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{U_N} = \mathbf{C}$.

Enfin, $|\mathrm{I}_{2,\alpha}(s,\xi)| \leqslant \int_{-1}^{1}|g(s,t)|\,dt \leqslant 2\mathrm{C_N}(\alpha)e^{2\pi\xi\alpha}$, ce qui permet de conclure.

(ii) Soit $g(t,s) = \frac{e^{-2i\pi\xi(-1+it)}}{(1+(-1+it)^2)^s}$ de telle sorte que $\mathrm{I}_{1,\alpha}(s,\xi) = -\int_{\alpha}^{+\infty} g(t,s)\,dt$.

• Si $t \in [\alpha,+\infty[$ est fixé, alors $s \mapsto g(t,s)$ est holomorphe sur $\mathrm{U_N}$.

• $|g(t,s)| = \frac{e^{2\pi\xi t}}{|(2-t^2-2it)^s|} \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}e^{2\pi\xi t}}{(t^2+4)^{\mathrm{Re}(s)/2}} \leqslant e^{\pi\,\mathrm{N}}(t^4+4)^{\mathrm{N}/2}e^{2\pi\xi t}$, pour tout $t \in [\alpha,+\infty[$ et $s \in \mathrm{U_N}$.

Comme $\xi<0$, la fonction $t \mapsto e^{\pi\,\mathrm{N}}(t^4+4)^{\mathrm{N}/2}e^{2\pi\xi t}$ est sommable sur $[\alpha,+\infty[$, et on est donc dans les conditions d'application du th. V.5.7, ce qui montre que $s \mapsto \mathrm{I}_{1,\alpha}(s,\xi)$ est holomorphe sur $\mathrm{U_N}$. Comme ceci est vrai pour tout N, elle est aussi holomorphe sur $\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{U_N} = \mathbf{C}$.

Enfin, $|\mathrm{I}_{1,\alpha}(s,\xi)| \leqslant \int_{\alpha}^{+\infty}|g(t,s)| \leqslant e^{2\pi\xi\alpha}\int_0^{+\infty} e^{\pi\mathrm{N}}((t+\alpha)^4+4)^{\mathrm{N}/2}e^{2\pi\xi t}\,dt$, et comme on suppose $\xi \leqslant -1$, on peut majorer l'intégrale par $\mathrm{C'_N}(\alpha) = \int_0^{+\infty} e^{\pi\mathrm{N}}((t+\alpha)^4+4)^{\mathrm{N}/2}e^{-2\pi t}\,dt$, ce qui permet de conclure.

(iii) Comme $\mathrm{F}_\alpha(s,\xi) = \sum_{i=1}^{3}\mathrm{I}_{i,\alpha}(s,\xi)$, c'est une conséquence immédiate des (i) et (ii), et on peut prendre $\mathrm{C''_N}(\alpha) = 2\mathrm{C_N}(\alpha)+2\mathrm{C'_N}(\alpha)$.

Question 4. (i) Si α_n est une suite tendant vers $+\infty$, et si $f_n(t) = f(t)\mathbf{1}_{[\alpha_n,+\infty[}(t)$, alors f_n est majorée, en valeur absolue par $|f|$ et $f_n \to 0$ en tout point de $[0,+\infty[$. Il en résulte, d'après le th. de convergence dominée, que $\int_{\alpha_n}^{+\infty} f = \int_0^{+\infty} f_n \to 0$, pour toute suite tendant vers $+\infty$. Ceci permet de conclure.

(ii) $\mathrm{I}_{1,\alpha}(s,\xi)$ est l'intégrale sur $[\alpha,+\infty[$ de la fonction sommable $g(t) = \frac{e^{-2i\pi\xi(-1+it)}}{(1+(-1+it)^2)^s}$; il en résulte que $\mathrm{I}_{1,\alpha}(s,\xi) \to 0$ quand $\alpha \to +\infty$.

Maintenant, $\mathrm{F}_\alpha(s,\xi) = \mathrm{I}_{1,\alpha}(s,\xi)+\mathrm{I}_{2,\alpha}(s,\xi)+\mathrm{I}_{3,\alpha}(s,\xi)$. Les arguments utilisés pour prouver que $\mathrm{I}_{1,\alpha}(s,\xi) \to 0$ montrent que $\mathrm{I}_{3,\alpha}(s,\xi) \to 0$. Enfin, $|\mathrm{I}_{2,\alpha}(s,\xi)| \leqslant \mathrm{C_N}(\alpha)e^{2\pi\xi\alpha}$, si $s \in \mathrm{U_N}$, et quand $\alpha \to +\infty$, on a $\mathrm{C_N}(\alpha) = e^{\pi\mathrm{N}}(\alpha^4+4)^{\mathrm{N}/2}$. Comme $(\alpha^4+4)^{\mathrm{N}/2}e^{2\pi\xi\alpha} \to 0$ puisque $\xi<0$, cela permet de conclure.

(iii) Si $\alpha<\beta$, alors $\mathrm{F}_\alpha(k,\xi)-\mathrm{F}_\beta(k,\xi)$ est l'intégrale de $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}dz$ sur le rectangle de sommets $-1+i\alpha, 1+i\alpha, 1+i\beta, -1+i\beta$. Comme $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}dz$ est holomorphe sur le demi-plan $\mathrm{Im}(s) > -1$ privé de i, la formule des résidus montre que $\mathrm{F}_\alpha(k,\xi)-\mathrm{F}_\beta(k,\xi) = 0$, si $\alpha<\beta<1$ ou si $1<\alpha<\beta$,

et que $\mathrm{F}_\alpha(k,\xi) - \mathrm{F}_\beta(k,\xi) = 2i\pi\,\mathrm{Res}\big(\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}, i\big)$, si $\alpha < 1 < \beta$. En particulier, $\alpha \mapsto \mathrm{F}_\alpha(k,\xi)$ est constant sur $]1,+\infty[$, et comme $\mathrm{F}_\alpha(k,\xi) \to 0$ quand $\alpha \to +\infty$, on a $\mathrm{F}_\alpha(k,\xi) = 0$ si $\alpha > 1$ et $\mathrm{F}_\alpha(k,\xi) = 2i\pi\,\mathrm{Res}\big(\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}, i\big)$, si $\alpha < 1$.

(iv) Si $k \leqslant 0$, la fonction $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ est holomorphe en i et son résidu est nul, et donc $\mathrm{F}_\alpha(k,\xi) = 0$.

Si $k = 1$, la fonction $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ a un pôle simple en $z = i$ de résidu $\lim_{z\to i}(z-i)\frac{e^{-2i\pi\xi z}}{1+z^2} = \lim_{z\to i}\frac{e^{-2i\pi\xi z}}{z+i} = \frac{1}{2i}e^{2\pi\xi}$. On a donc $\mathrm{F}_\alpha(1,\xi) = \pi e^{2\pi\xi}$.

Si $k = 2$, la fonction $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ a un pôle d'ordre 2 en $z = i$, et le résidu est le terme de degré 1 du développement de Taylor de $\frac{e^{-2i\pi\xi z}}{(z+i)^2}$ en $z = i$. Comme

$$\frac{e^{-2i\pi\xi z}}{(z+i)^2} = \frac{e^{2\pi\xi}(1 - 2i\pi\xi(z-i) + \cdots)}{-4 + 4i(z-i) + \cdots} = \frac{-1}{4}e^{2\pi\xi}(1 + (i - 2i\pi\xi)(z-i) + \cdots),$$

on a $\mathrm{F}_\alpha(2,\xi) = 2i\pi \cdot \frac{-1}{4}(i - 2i\pi\xi)e^{2\pi\xi} = (\frac{\pi}{2} - \pi^2\xi)e^{2\pi\xi}$.

Question 5. (i) Cela résulte du changement de variable $u = -t$ et de la parité de ϕ_s.

(ii) Comme $\gamma_{\alpha,\mathrm{R}}$ est un lacet inclus dans Ω qui est contractile, l'intégrale de $e^{2\pi\xi z}\phi_s(z)dz$ le long de ce chemin est nulle, et ce, pour tout R. Sur chacun des segments $[\mathrm{R}, \mathrm{R}+i\mathrm{R}]$, $[\mathrm{R}+i\mathrm{R}, 1+i\mathrm{R}]$, $[-1+i\mathrm{R}, -\mathrm{R}+i\mathrm{R}]$ et $[-\mathrm{R}+i\mathrm{R}, -\mathrm{R}]$, on a $|z^2+1| \geqslant \mathrm{R}^2 - 1$ et $|e^{2\pi\xi z}| \leqslant 1$, et donc $|e^{2\pi\xi z}\phi_s(z)| \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}}{(\mathrm{R}^2-1)^{\mathrm{Re}(s)}}$. Par ailleurs, ces quatre segments sont de longueur $\leqslant \mathrm{R}$, et donc la somme des intégrales sur ces segments est, en valeur absolue, majorée par $\frac{4\mathrm{R}e^{\pi|\mathrm{Im}(s)|}}{(\mathrm{R}^2-1)^{\mathrm{Re}(s)}}$, et donc tend vers 0 quand R tend vers $+\infty$ puisque $\mathrm{Re}(s) > \frac{1}{2}$. Comme l'intégrale sur $[-\mathrm{R}, \mathrm{R}]$ tend vers $\hat{\phi}_s(\xi)$, et comme la somme des intégrales sur les trois morceaux restants tend vers $-\mathrm{F}_\alpha(s,\xi)$, cela permet de conclure.

(iii) C'est une conséquence immédiate du (iii) de la question 3.

Question 6. (i) La fonction $\frac{1}{1+t^2}$ est sommable, ainsi que sa dérivée $\frac{-2t}{(1+t^2)^2}$; on peut donc lui appliquer la formule de Poisson ce qui nous donne, en utilisant la formule $\hat{\phi}_1(n) = \pi e^{-2\pi|n|}$, conséquence du (ii) de la question 5 et du (iv) de la question 4 (pour $n < 0$), et de la parité de $\hat{\phi}_1$ (pour en déduire le cas $n > 0$) :

$$\sum_{n\in\mathbf{Z}} \frac{1}{1+n^2} = \pi + 2\pi\sum_{n=1}^{+\infty} e^{-2\pi n} = \pi\big(1 + 2\frac{e^{-2\pi}}{1-e^{-2\pi}}\big) = \pi\,\frac{1+e^{-2\pi}}{1-e^{-2\pi}}.$$

De même,

$$\sum_{n\in\mathbf{Z}} \frac{1}{(1+n^2)^2} = \hat{\phi}_2(0) + 2\sum_{n=1}^{+\infty} \mathrm{F}_{1/2}(2,-n) = \frac{1}{2}\pi + 2\sum_{n=1}^{+\infty}\big(\frac{\pi}{2} + \pi^2 n\big)e^{-2\pi n}.$$

On conclut via la formule $\sum_{n=0}^{+\infty} nz^n = \frac{z}{(1-z)^2}$ obtenue en dérivant l'identité $\frac{1}{1-z} = \sum_{n=0}^{+\infty} z^n$.

(ii) D'après le (iii) de la question 3 (utilisé pour $\alpha = \frac{1}{2}$), on a $|\mathrm{F}_{1/2}(s,-n)| \leqslant \mathrm{C}''_{\mathrm{N}}(\frac{1}{2})e^{-\pi n}$, pour tous $n \geqslant 1$ et $s \in \mathrm{U}_{\mathrm{N}}$. Il en résulte que la série $\sum_{n=1}^{+\infty} \mathrm{F}_{1/2}(s,-n)$ est normalement convergente sur U_{N}, et comme chacun des termes est holomorphe sur $\mathbf{C}$ tout entier ((iii) de la question 3), sa somme $\mathrm{F}(s)$ est, d'après le th. V.5.1, holomorphe sur U_{N}. On en déduit l'holomorphie de F sur $\cup_{\mathrm{N}\in\mathbf{N}}\mathrm{U}_{\mathrm{N}} = \mathbf{C}$, ce que l'on voulait démontrer.

(iii) Si $\mathrm{Re}(s) > \sigma$, alors $\big|\frac{1}{(n^2+1)^s}\big| \leqslant \frac{1}{(n^2+1)^\sigma}$, et comme la série $\sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^\sigma}$ est convergente si $\sigma > \frac{1}{2}$, il en résulte que la série $\sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^s}$ est normalement convergente sur le demi-plan $\mathrm{Re}(s) > \sigma$, pour tout $\sigma > \frac{1}{2}$. Comme chaque fonction $s \mapsto \frac{1}{(n^2+1)^s}$ est holomorphe sur $\mathbf{C}$, et qu'une série normalement convergente de fonctions holomorphes est holomorphe (th. V.5.1), G est holomorphe sur le demi-plan $\mathrm{Re}(s) > \sigma$, pour tout $\sigma > \frac{1}{2}$, et donc aussi sur la réunion de ces demi-plans, ce qui permet de conclure.

(iv) Si $\mathrm{Re}(s) > \frac{1}{2}$, la fonction ϕ_s et sa dérivée $t \mapsto \frac{2st}{(1+t^2)^{s+1}}$ sont sommables sur $\mathbf{R}$; on peut donc lui appliquer la formule de Poisson, ce qui nous donne, en tenant compte de ce que $\hat{\phi}_s(n) = \hat{\phi}_s(-n)$,

$$\mathrm{G}(s) = \hat{\phi}_s(0) + 2\sum_{n=1}^{+\infty} \mathrm{F}_{1/2}(s,-n), \quad \text{si } \mathrm{Re}(s) > \frac{1}{2}.$$

Maintenant, la série dans le second membre aussi égale à $\hat{\phi}_s(0) + 2\mathrm{F}(s)$. Comme F est holomorphe sur $\mathbf{C}$ tout entier et G l'est sur le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$, on en déduit que $\hat{\phi}_s(0)$ est holomorphe sur ce demi-plan, et donc coïncide avec $\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$ sur ce demi-plan puisque $\hat{\phi}_s(0) - \frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$ est identiquement nulle sur $]\frac{1}{2}, +\infty[$. La fonction $\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)} + 2\mathrm{F}(s)$ est alors méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples aux $-k+\frac{1}{2}$, pour $k \in \mathbf{N}$, et est égale à $\mathrm{G}(s)$ sur le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$; c'est donc le prolongement voulu.

(v) Si $s = -k$, avec $k \in \mathbf{N}$, tous les termes de la série définissant $\mathrm{G}(s)$ sont nuls (pour $\hat{\phi}_s(0)$ c'est dû à la présence de pôles de Γ aux entiers négatifs, pour $\mathrm{F}_{1/2}(s,-n)$, cela fait l'objet du (iv) de la question 3) et donc $\mathrm{G}(-k) = 0$, si $k \in \mathbf{N}$.

Question 7. (i) La dérivée k-ième $f_{s,k}(t)$ de $t \mapsto f(t)^s$ est de la forme $t \mapsto f(t)^{s-k}\mathrm{P}_k(s, f(t), \dots, f^{(k)}(t))$, où P_k est un polynôme. En particulier, $f_{s,k}(0)$ est de la forme $\mathrm{Q}_k(s)f(0)^{s-k}$, où Q_k est un polynôme en s. La formule de Taylor avec reste intégral nous donne

$$f(t)^s = \sum_{k=0}^{n} \frac{f(0)^{s-k}\mathrm{Q}_k(s)}{k!}t^k + \frac{t^{n+1}}{n!}\int_0^1 f_{s,n+1}(tu)(1-u)^n\,du.$$

On en déduit que

$$\int_0^1 t^{as+b}f(t)^s\,dt = \sum_{k=0}^{n} \frac{f(0)^{s-k}\mathrm{Q}_k(s)}{k!(as+b+k+1)} + \int_0^1\int_0^1 t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n\,du\,dt.$$

Maintenant, $s \mapsto g(s,t,u) = t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n$ est holomorphe sur $\mathrm{Re}(s) > -\frac{b+n+1}{a}$, pour tout $(t,u) \in [0,1]\times[0,1]$, et est une fonction continue de (s,t,u), ce qui implique l'existence, pour tout compact K de $\mathrm{Re}(s) > -\frac{b+n+1}{a}$, d'une constante $\mathrm{C_K}$ telle que $|g(s,t,u)| \leqslant \mathrm{C_K}$, si $(s,t,u) \in \mathrm{K}\times[0,1]^2$. On peut donc utiliser le th. V.5.7 pour en déduire que $s \mapsto \int_0^1\int_0^1 t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n\,du\,dt$ est holomorphe sur le demi-plan $\mathrm{Re}(s) > -\frac{b+n+1}{a}$. Comme les autres termes sont méromorphes sur $\mathbf{C}$ tout entier, avec des pôles simples aux $\frac{-b-k}{a}$, pour $k \in \{1,\dots,n+1\}$, on voit que $s \mapsto \int_0^1 t^{as+b}f(t)^s\,dt$ admet un prolongement méromorphe au demi-plan $\mathrm{Re}(s) > -\frac{b+n+1}{a}$, avec des pôles simples aux $\frac{-b-k}{a}$, pour $k \in \{1,\dots,n\}$. Comme ceci est vrai pour tout $n \in \mathbf{N}$, cela permet de conclure.

(ii) On découpe l'intégrale $\int_{-\infty}^{+\infty}$ en trois morceaux : $]-\infty,-1]$, $[-1,1]$ et $[1,+\infty[$. Sur $]-\infty,-1]$ (resp. $[1,+\infty[$), on fait le changement de variable $t = \frac{-1}{u}$ (resp. $t = \frac{1}{u}$), et on tombe sur l'intégrale $\int_0^1 u^{ds-2}\frac{1}{(u^d\mathrm{P}(-1/u))^s}\,du$ (resp. $\int_0^1 u^{ds-2}\frac{1}{(u^d\mathrm{P}(1/u))^s}\,du$) qui peut se traiter en utilisant le (i). Comme les méthodes habituelles montrent que $s \mapsto \int_{-1}^1 \frac{1}{\mathrm{P}(t)^s}\,dt$ est holomorphe sur $\mathbf{C}$ tout entier, cela permet de conclure.

(iii) On écrit P sous la forme $\prod_{j=0}^{d/2}(z-a_j-ib_j)(z-a_j+ib_j)$, avec $b_j > 0$, pour tout j. On a alors $\frac{1}{\mathrm{P}(z)^s} = \prod_{j=0}^{d/2}\big(b_j^{-2s}\phi_s\big(\frac{z-a_j}{b_j}\big)\big)$, si $z \in \mathbf{R}$, et comme la formule définit une fonction holomorphe sur Ω^+ et sur Ω^-, cela permet de conclure (en fait, il suffit d'enlever des demi-droites verticales partant des zéros de P dans le demi-plan $\mathrm{Im}(z) > 0$ (resp. $\mathrm{Im}(z) < 0$)).

(iv) La série converge normalement sur tout demi-plan de $\mathrm{Re}(s) > \sigma$, si $\sigma > \frac{1}{d}$, et donc $\mathrm{G_P}$ est holomorphe sur $\mathrm{Re}(s) > \frac{1}{d}$. Par ailleurs, sur ce demi-plan, $t \mapsto \frac{1}{\mathrm{P}(t)^s}$ est sommable, ainsi que sa dérivée $t \mapsto \frac{-s\mathrm{P}'(t)}{\mathrm{P}(t)^{s+1}}$, ce qui permet d'utiliser la formule de Poisson et d'obtenir $\mathrm{G_P}(s) = \sum_{n\in\mathbf{Z}}\hat{\phi}_{\mathrm{P},s}(n)$. La fonction

$s \mapsto \hat{\phi}_{\mathrm{P},s}(0)$ fait l'objet du (ii) ; elle admet un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples aux $\frac{1-k}{d}$, pour $k \in \mathbf{N}$.

La méthode du (ii) de la question 5 permet d'écrire $\hat{\phi}_{\mathrm{P},s}(\xi)$ comme l'intégrale de $e^{-2i\pi\xi z}\phi_{\mathrm{P},s}(z)$ sur le chemin constitué de $]-\mathrm{B}+i\infty, -\mathrm{B}+i\beta]$, $[-\mathrm{B}+i\beta, \mathrm{B}+i\beta]$ et $[\mathrm{B}+i\beta, \mathrm{B}+i\infty[$ (resp. de $]-\mathrm{B}-i\infty, -\mathrm{B}-i\beta]$, $[-\mathrm{B}-i\beta, \mathrm{B}-i\beta]$ et $[\mathrm{B}-i\beta, \mathrm{B}-i\infty[$), où $\mathrm{B} = \mathrm{A}+1$ et $\beta \in]0, \alpha[$, si $\xi < 0$ (resp. si $\xi > 0$). Ceci permet de montrer, comme au (iii) de la question 3, que $s \mapsto \hat{\phi}_{\mathrm{P},s}(\xi)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$, et qu'il existe une constante $\mathrm{C_N}$ telle que l'on ait $|\hat{\phi}_{\mathrm{P},s}(\xi)| \leqslant \mathrm{C_N} e^{-2\pi\beta|\xi|}$, pour tous $s \in \mathrm{U_N}$ et ξ vérifiant $|\xi| \geqslant 1$. On en déduit, comme au (ii) de la question 6, que $s \mapsto \sum_{n \in \mathbf{Z}-\{0\}} \hat{\phi}_{\mathrm{P},s}(n)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$, et donc que $\mathrm{G_P}$ se prolonge en une fonction méromorphe sur $\mathbf{C}$, holomorphe en dehors de pôles simples aux $\frac{1-k}{d}$, pour $k \in \mathbf{N}$.

H.11. La fonction η de Dedekind

L'objet de ce problème est d'établir les identités suivantes [16], dues à Euler et à Jacobi,

$$q^{1/24}\prod_{n\geqslant 1}(1-q^n)=\sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$$
$$\sum_{m\in\mathbf{Z}}q^{m^2}w^m=\prod_{n\geqslant 1}(1-q^{2n})(1+q^{2n-1}w)(1+q^{2n-1}w^{-1})$$

Il s'agit d'identités formelles, mais si on pose $q=e^{2i\pi\tau}$, les deux membres convergent pour τ appartenant au demi-plan de Poincaré $\mathscr{H}=\{z\in\mathbf{C},\ \mathrm{Im}(z)>0\}$, et nous allons montrer que les deux fonctions ainsi définies sur $\mathscr{H}$ sont égales. Le chemin que nous allons suivre [17] pour arriver au résultat va demander d'utiliser une bonne partie des techniques introduites dans le cours.

Si $t\in\mathbf{R}$, on note Ω_t le demi-plan ouvert $\{z\in\mathbf{C},\ \mathrm{Re}(z)>t\}$.

On note $\log:\mathbf{C}^*\to\mathbf{C}$ la détermination du logarithme définie par $-\pi\leqslant\mathrm{Im}(\log z)<-\pi$ (on rappelle que $\mathrm{Im}(\log z)$ est aussi l'argument $\arg(z)$ de z). La fonction log est holomorphe sur $\mathbf{C}-\mathbf{R}_-$, de dérivée $\frac{1}{z}$, et la dérivée de la fonction $t\mapsto\log(t+i)$ sur $\mathbf{R}$ est donc $t\mapsto\frac{1}{t+i}$.

Si $x\in\mathbf{C}^*$ et si $s\in\mathbf{C}$, on pose $z^s=\exp(s\log z)$. On a $|z^s|\leqslant e^{\pi|\mathrm{Im}(s)|}|z|^{\mathrm{Re}(s)}$.

On note Γ la fonction Γ d'Euler ; c'est une fonction méromorphe sur $\mathbf{C}$ ne s'annulant nulle part, holomorphe en dehors de pôles simples en les $-n$ avec $\lim_{s\to -n}(s+n)\Gamma(s)=\frac{(-1)^n}{n!}$, pour $n\in\mathbf{N}$, qui vérifie l'équation fonctionnelle $\Gamma(s+1)=s\Gamma(s)$, et qui est donnée par $\Gamma(s)=\int_0^{+\infty}e^{-t}t^{s-1}\,dt$, si $s\in\Omega_0$ (cf. th. VII.2.1).

On note ζ la fonction zêta de Riemann ; c'est une fonction méromorphe sur $\mathbf{C}$, holomorphe en dehors d'un pôle simple en $s=1$, et qui est donnée par $\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$, si $s\in\Omega_1$ (cf. th. VII.3.4). On a $\zeta(0)=\frac{-1}{2}$ (ex. VII.3.6).

Question 1. Si $s\in\Omega_1$, on définit $\phi_s:\mathbf{R}\to\mathbf{C}$ par $\phi_s(t)=\frac{1}{(t+i)^s}$.

(i) Vérifier que $\phi_s\in\mathscr{L}^1(\mathbf{R})$, est dérivable sur $\mathbf{R}$ et que $\phi_s'=\frac{-s}{t+i}\phi_s$.

(ii) Montrer que $\hat{\phi}_s$ est à décroissance rapide à l'infini.

(iii) Montrer que $\hat{\phi}_s$ est solution de l'équation différentielle $xy'+(2\pi x+1-s)y=0$.

(iv) En déduire que $\hat{\phi}_s(x)=0$, si $x\leqslant 0$, et qu'il existe une constante $c(s)$ telle que $\hat{\phi}_s(x)=c(s)e^{-2\pi x}x^{s-1}$, si $x>0$.

Question 2. Soit $s\in\Omega_0$.

(i) Montrer que $\int_0^{+\infty}e^{-\tau x}x^{s-1}dx$ converge si $\tau\in\Omega_0$, et que la fonction G_s ainsi définie est holomorphe (en τ) sur Ω_0.

(ii) Que vaut $\mathrm{G}_s(\tau)$, si $\tau\in\mathbf{R}_+^*$? En déduire que $\mathrm{G}_s(\tau)=\frac{\Gamma(s)}{\tau^s}$, pour tout $\tau\in\Omega_0$.

(iii) Montrer que $(1-it)^s=e^{-i\frac{\pi}{2}s}(t+i)^s$, si $t\in\mathbf{R}$.

(iv) Calculer la transformée de Fourier inverse de $\hat{\phi}_s$. En déduire que $c(s)=e^{-\frac{i\pi}{2}s}\frac{(2\pi)^s}{\Gamma(s)}$.

Question 3. (i) Calculer $\hat{\phi}_s$, si s est un entier $\geqslant 2$, par la méthode des résidus.

16. Elles montrent qu'il se passe de drôles de choses quand on développe les produits.

17. Il existe des démonstrations combinatoires de cette identité : cf. Hardy & Wright, *An introduction to the theory of numbers*, § 19.11.

(ii) Que donne la méthode des résidus si s n'est pas entier ?

Question 4. Soient $\mathrm{Y}_0 = \{(m,n) \in \mathbf{Z}^2,\ m > 0,\ n \geqslant 0\}$, $\mathrm{Y}_1 = \{(m,n) \in \mathbf{Z}^2,\ m \leqslant 0,\ n > 0\}$, et soit $\mathrm{Y} = \mathrm{Y}_0 \cup \mathrm{Y}_1$. (On remarquera que cette réunion est disjointe, et que $\mathbf{Z}^2 - \{(0,0)\}$ est la réunion disjointe de Y et de $-\mathrm{Y} = \{-\omega,\ \omega \in \mathrm{Y}\}$.) Soit $\tau \in \mathscr{H}$, et soit $s \in \Omega_2$.

(i) Soit K un compact de Ω_2. Montrer qu'il existe $\mathrm{C(K)} > 0$ et $a(\mathrm{K}) < -2$ tels que, pour tous $s \in \mathrm{K}$ et $(m,n) \in \mathrm{Y}$, on ait $\left|\frac{1}{(m+n\tau)^s}\right| \leqslant \mathrm{C(K)} \sup(|m|,|n|)^{a(\mathrm{K})}$.

(ii) Montrer que la série $\sum_{(m,n)\in \mathrm{Y}} \frac{1}{(m+n\tau)^s}$ converge, et définit une fonction $s \mapsto \mathrm{E}(\tau,s)$, holomorphe sur Ω_2.

(iii) Montrer que $\sum_{m\in\mathbf{Z}} \frac{1}{(m+n\tau)^s} = \sum_{\ell=1}^{+\infty} c(s) k^{s-1} e^{2i\pi n\ell\tau}$, si $n \geqslant 1$. (On s'intéressera à la transformée de Fourier de $t \mapsto h(t) = \frac{1}{(t+n\tau)^s}$, en écrivant $n\tau$ sous la forme $\alpha + i\beta$.)

(iv) En déduire que $\mathrm{E}(\tau,s) = \zeta(s) + e^{-\frac{i\pi}{2}s} \frac{(2\pi)^s}{\Gamma(s)} \sum_{k=1}^{+\infty} \sigma_{s-1}(k) e^{2i\pi k\tau}$, où $\sigma_t(k)$ désigne la somme des puissances t-ièmes des diviseurs de k (i.e. $\sigma_t(6) = 1 + 2^t + 3^t + 6^t$). (On commencera par montrer que $\sum_{d|k} |d^{s-1}| \leqslant k^{\mathrm{Re}(s)}$.)

(v) Montrer que $s \mapsto \mathrm{E}(\tau,s)$ possède un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors d'un pôle simple en $s = 1$, et que $\mathrm{E}(\tau,0) = \frac{-1}{2}$.

Question 5. Soit φ une fonction méromorphe sur un ouvert contenant la demi-droite réelle $[0,+\infty[$, holomorphe en dehors d'un pôle d'ordre k en $z = 0$.

(i) Montrer qu'il existe $r > 0$ et des $a_n \in \mathbf{C}$, tels que $\sum_{n\geqslant -k} |a_n| r^n < +\infty$ et $\varphi(z) = \sum_{n=-k}^{+\infty} a_n z^n$, si $|z| \leqslant r$.

(ii) Montrer que $\mathrm{I}_1(s) = \int_0^r \varphi(t) t^{s-1}\, dt$ converge si $\mathrm{Re}(s) > k$, possède un prolongement méromorphe à $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples aux entiers $\leqslant k$, et que $\lim_{s\to n}(s-n)\mathrm{I}_1(s) = a_{-n}$, si $n \leqslant k$. (On commencera par montrer que $\mathrm{I}_1(s) = \sum_{n\geqslant -k} \frac{a_n r^{s+n}}{s+n}$.)

(iii) On suppose de plus que φ est à décroissance rapide en $+\infty$. Montrer que $\Lambda(\varphi,s) = \int_0^{+\infty} \varphi(t) t^{s-1} dt$ converge si $\mathrm{Re}(s) > k$, possède un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples aux entiers $\leqslant k$, et que $\lim_{s\to n}(s-n)\Lambda(\varphi,s) = a_{-n}$, si $n \leqslant k$.

Question 6. Si $i = 0, 1$, soit $f_i(\tau,s) = \sum_{(m,n)\in \mathrm{Y}_i} \frac{1}{(m+n\tau)^s}$; on a $\mathrm{E}(\tau,s) = f_0(\tau,s) + f_1(\tau,s)$, si $s \in \Omega_2$.

(i) Soit $\alpha \in \Omega_0$ tel que $\alpha\tau \in \Omega_0$. Montrer que $\frac{1}{(\alpha(m+n\tau))^s} = \frac{1}{\alpha^s (m+n\tau)^s}$, si $(m,n) \in \mathrm{Y}_0$.

(ii) Soit $\mathrm{G}_\alpha(t) = \frac{1}{(e^{\alpha t}-1)(1-e^{-\alpha\tau t})}$. Montrer que $f_0(\tau,s) = \frac{\alpha^s}{\Gamma(s)} \int_0^{+\infty} \mathrm{G}_\alpha(t) t^{s-1} dt$, si $s \in \Omega_2$. (Utiliser la question 2 pour exprimer $\frac{1}{(\alpha(m+n\tau))^s}$.)

(iii) En déduire que $s \mapsto f_0(\tau,s)$ possède un prolongement méromorphe à $\mathbf{C}$ tout entier, holomorphe en dehors de pôles simples en $s = 1$ et $s = 2$.

(iv) Calculer les premiers termes du développement de G_α en 0. En déduire les formules [18] $\lim_{s\to 2}(s-2) f_0(\tau,s) = \frac{1}{\tau}$, $\lim_{s\to 1}(s-1) f_0(\tau,s) = \frac{\tau-1}{2\tau}$ et $f_0(\tau,0) = \frac{\tau}{12} + \frac{1}{12\tau} - \frac{1}{4}$.

Question 7. (i) Que deviennent Y_0 par $(m,n) \mapsto (-n,m)$ et Y_1 par $(m,n) \mapsto (n,-m)$? En déduire que $\mathrm{E}(\frac{-1}{\tau}, 2k) = \tau^{2k} \mathrm{E}(\tau, 2k)$, si k est un entier $\geqslant 2$.

---

18. La même méthode fournit la formule $f_1(\tau,s) = \frac{\alpha^s}{\Gamma(s)} \int_0^{+\infty} \frac{1}{(e^{\alpha t}-1)(1-e^{\alpha\tau t})} t^{s-1} dt$, avec α vérifiant $\mathrm{Re}(\alpha\tau) > 0$ et $\mathrm{Re}(-\alpha) > 0$, ce qui permet de prouver que $f_1(\tau,s)$ possède aussi un prolongement méromorphe à $\mathbf{C}$, holomorphe en dehors de pôles simples en $s = 2$ (résidu $\frac{-1}{\tau}$) et $s = 1$ (résidu $\frac{1+\tau}{2\tau}$), et de retrouver le (v) de la question 4, ainsi que les propriétés de ζ rappelées dans le préambule.

(ii) Montrer que $\log \frac{\tau}{-n+m\tau} = \begin{cases} \log\tau - \log(-n+m\tau) & \text{si } (m,n) \in \mathrm{Y}_0, \\ \log\tau - \log(n-m\tau) - i\pi & \text{si } (m,n) \in \mathrm{Y}_1. \end{cases}$

(iii) En déduire que, pour tout $s \in \mathbf{C}$, on a $\mathrm{E}(\frac{-1}{\tau}, s) = \tau^s\big(\mathrm{E}(\tau,s) + (e^{-i\pi s}-1)f_0(\tau,s)\big)$. (On commencera par supposer $s \in \Omega_2$.)

(iv) Montrer que $\mathrm{E}(\frac{-1}{\tau}, 2) = \tau^2 \mathrm{E}(\tau,2) - i\pi\tau$.

Question 8. On note $\mathrm{F}(\tau)$ la dérivée en $s=0$ de $s \mapsto \mathrm{E}(\tau,s)$.

(i) Montrer que le produit $e^{i\pi\tau/12}\prod_{n=1}^{+\infty}(1-e^{2i\pi n\tau})$ converge si $\tau \in \mathscr{H}$, et que la fonction $\eta : \mathscr{H} \to \mathbf{C}$ ainsi définie est holomorphe sur $\mathscr{H}$ et ne s'y annule pas.

(ii) Montrer qu'il existe une fonction g, holomorphe sur $\mathscr{H}$, vérifiant $e^g = \eta$, et qu'il existe $a \in \mathbf{Z}$ tel que l'on ait $g = h + a2i\pi$, où $h(\tau) = \frac{i\pi\tau}{12} + \sum_{n=1}^{+\infty}\log(1-e^{2i\pi n\tau})$, pour tout $\tau \in \mathscr{H}$ (on notera $\log\eta$ la fonction h.)

(iii) Montrer qu'il existe $\mathrm{C} \in \mathbf{C}$ telle que $\log\eta(\tau) = -\mathrm{F}(\tau) + \frac{i\pi\tau}{12} + \mathrm{C}$, pour tout $\tau \in \mathscr{H}$.

(iv) En déduire que $\log\eta(\frac{-1}{\tau}) = \frac{1}{2}\log\tau + \log\eta(\tau) - \frac{i\pi}{4}$ et que $\eta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\eta(\tau)$, pour tout $\tau \in \mathscr{H}$, où $\sqrt{\frac{\tau}{i}}$ est la branche valant 1 en $\tau = i$.

(v) Montrer, en utilisant l'identité du (iii), que $\frac{\eta'(\tau)}{\eta(\tau)} + \frac{1}{2i\pi}\mathrm{E}(\tau,2) = 0$. En déduire que $\zeta(2) = \frac{\pi^2}{6}$.

Question 9. Si $\tau \in \mathscr{H}$, la série $\sum_{m\in\mathbf{Z}}(-1)^m e^{2i\pi\frac{(6m+1)^2\tau}{24}}$ converge, et la fonction $\tau \mapsto \mathrm{H}(\tau)$, ainsi définie, est holomorphe sur $\mathscr{H}$ pour les raisons habituelles. Nous laissons au lecteur le soin de se convaincre que l'on a aussi $\mathrm{H}(\tau) = \frac{1}{2}\sum_{n\in\mathbf{Z}}\chi(n)e^{2i\pi\frac{n^2\tau}{24}}$, où $\chi : (\mathbf{Z}/12\mathbf{Z})^* \to \{\pm 1\}$ est le caractère de Dirichlet défini par $\chi(1) = \chi(-1) = 1$ et $\chi(5) = \chi(-5) = -1$, que l'on voit comme une fonction de $\mathbf{Z}$ dans $\{\pm1\}$, périodique de période 12, nulle sur les entiers non premiers à 12 (i.e. divisibles par 2 ou 3).

(i) On rappelle que la transformée de Fourier de $t \mapsto e^{-\pi t^2}$ est $x \mapsto e^{-\pi x^2}$. Calculer la transformée de Fourier de $t \mapsto e^{-2i\pi\frac{at}{12}}e^{-\pi\frac{yt^2}{12}}$, si $y > 0$ et $a \in \mathbf{Z}$. En déduire l'identité

$$\sum_{n\in\mathbf{Z}} e^{-2i\pi\frac{an}{12}}e^{-\pi\frac{yn^2}{12}} = \sqrt{\frac{12}{y}}\sum_{n\in\mathbf{Z}} e^{-\frac{\pi}{12y}(12n+a)^2}.$$

(ii) Vérifier [19] que $\frac{1}{\sqrt{12}}\sum_{a=-5}^{6}\chi(a)e^{-2i\pi\frac{an}{12}} = \chi(n)$, pour tout $n \in \mathbf{Z}$.

(iii) En déduire que $\mathrm{H}(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\mathrm{H}(\tau)$, pour tout $\tau \in \mathscr{H}$. (Commencer par $\tau \in i\mathbf{R}_+^*$.)

(iv) Montrer que $\mathrm{J}(\tau) = \mathrm{H}(\tau)/\eta(\tau)$ est une fonction holomorphe sur $\mathscr{H}$, vérifiant les équations fonctionnelles [20] $\mathrm{J}(\tau+1) = \mathrm{J}(\tau)$ et $\mathrm{J}(\frac{-1}{\tau}) = \mathrm{J}(\tau)$, pour tout $\tau \in \mathscr{H}$.

(v) Montrer qu'il existe une unique fonction $q \mapsto \tilde{\mathrm{J}}(q)$, holomorphe sur $\mathrm{D}(0,1^-)$, telle que $\mathrm{J}(\tau) = \tilde{\mathrm{J}}(e^{2i\pi\tau})$, pour tout $\tau \in \mathscr{H}$. Que vaut $\tilde{\mathrm{J}}(0)$?

(vi) Soit $\mathrm{X} = \{\tau = x+iy,\ |x| < \frac{2}{3},\ y > \frac{1}{3}\}$. On note $\partial\mathrm{X}$ la frontière de l'ouvert X (constituée des demi-droites verticales $[\frac{-2+i}{3}, \frac{-2}{3}+i\infty[$ et $[\frac{2+i}{3}, \frac{2}{3}+i\infty[$, et du segment horizontal $[\frac{-2+i}{3}, \frac{2+i}{3}]$), et $\overline{\mathrm{X}} = \mathrm{X} \cup \partial\mathrm{X}$ l'adhérence de X. Montrer qu'il existe $c > 0$ telle que $|\mathrm{J}(\tau) - 1| \leqslant c\,e^{-2\pi y}$, pour tout $\tau = x+iy \in \overline{\mathrm{X}}$. En déduire que $|\mathrm{J}-1|$ atteint son maximum sur $\overline{\mathrm{X}}$ en un point de $\partial\mathrm{X}$.

19. C'est un cas particulier du lemme VII.4.3.

20. Autrement dit, J est une forme modulaire de poids 0 (cf. § VII.6).

(vii) Soit $\tau \in \partial X$. Montrer qu'au moins un des 5 nombres $\tau+1$, $\tau-1$, $\frac{-1}{\tau}$, $\frac{-1}{\tau}+1$, $\frac{-1}{\tau}-1$ appartient à X. En déduire que J est constante [21] puis que $H = \eta$.

Question 10. (i) Montrer que le produit $\prod_{n\geqslant 1}(1-q^{2n})(1+q^{2n-1}w)(1+q^{2n-1}w^{-1})$ converge pour tout $w \in \mathbf{C}^*$, si $|q|<1$, et que la fonction $w \mapsto A(q,w)$, ainsi définie, est holomorphe sur $\mathbf{C}^*$.

(ii) En déduire l'existence et l'unicité de fonctions $q \mapsto a_m(q)$, pour $m \in \mathbf{Z}$, définies sur $D(0,1^-)$, telles que $A(q,w) = \sum_{m\in\mathbf{Z}} a_m(q)w^m$, pour tous $w \in \mathbf{C}^*$ et $q \in D(0,1^-)$.

(iii) Montrer que $A(q,q^2w) = q^{-1}w^{-1}A(q,w)$, pour tous $w \in \mathbf{C}^*$ et $q \in D(0,1^-)$.

(iv) En déduire que $a_m(q) = q^{m^2}a_0(q)$, pour tout $m \in \mathbf{Z}$.

(v) Calculer de deux manières $A(e^{3i\pi\tau}, -e^{i\pi\tau})$, si $\tau \in \mathscr{H}$; en déduire la *formule du produit triple de Jacobi* :

$$\sum_{m\in\mathbf{Z}} q^{m^2}w^m = \prod_{n\geqslant 1}(1-q^{2n})(1+q^{2n-1}w)(1+q^{2n-1}w^{-1}).$$

(vi) La fonction thêta de Jacobi est définie, sur $\mathscr{H}$, par $\theta(\tau) = \sum_{m\in\mathbf{Z}} e^{i\pi m^2\tau}$. Montrer que $\theta(\tau) = \frac{\eta(\tau)^5}{\eta(2\tau)^2\eta(\tau/2)^2}$, pour tout $\tau \in \mathscr{H}$.

Corrigé

Question 1. (i) On a $|\phi_s(t)| \leqslant e^{\pi \mathrm{Im}(s)}(1+t^2)^{-\mathrm{Re}(s)/2}$, et donc $\phi_s(t) = O(|t|^{-\mathrm{Re}(s)})$ au voisinage de $\pm\infty$, ce qui prouve que ϕ_s est sommable, la fonction ϕ_s étant continue sur $\mathbf{R}$ puisque $t \mapsto \log(t+i)$ l'est. Par ailleurs, $t \mapsto \log(t+i)$ étant dérivable de dérivée $\frac{1}{t+i}$, cela implique que $\phi_s = \exp(-s\log(t+i))$ est dérivable de dérivée $t \mapsto -s\frac{1}{t+i}\exp(s\log(t+i)) = \frac{-s}{t+i}\phi_s$, ce que l'on voulait.

(ii) On déduit du (i) que ϕ_s est de classe $\mathscr{C}^k$, pour tout k, et $\phi_s^{(k)} = (-s)(-s-1)\cdots(-s-k+1)\phi_{s+k}$ est sommable pour tout k. Il résulte donc du (i) du th. IV.2.8 que $(1+x^2)^{k/2}|\hat{\phi}_s(x)|$ tend vers 0 à l'infini pour tout $k \in \mathbf{N}$, et donc que $\hat{\phi}_s$ est à décroissance rapide à l'infini.

(iii) Notons y la transformée de Fourier de ϕ_s. Il résulte du (i) du th. IV.2.8 et du (ii) de la question que la transformée de Fourier de ϕ_s' est $2i\pi xy$, et du (ii) du th. IV.2.8 que celle de $t \mapsto t\phi_s'$ est

21. Les fonctions $E_{2k} = E(\tau,2k) = \zeta(2k) + (-1)^k\frac{(2\pi)^{2k}}{(2k-1)!}\sum_{n\geqslant 1}\sigma_{2k-1}(n)q^n$ de la question 7 sont des formes modulaires appelées *séries d'Eisenstein* ; la fonction η est la *fonction η de Dedekind* ; sa puissance 24-ième $\Delta = q\prod_{n\geqslant 1}(1-q^n)^{24}$ est l'objet romantique de la théorie des formes modulaires ; Ramanujan lui a consacré de nombreux travaux. On peut démontrer, avec les mêmes méthodes, que $\zeta(6)^2E_4^3 - \zeta(4)^3E_6^2 = \alpha\Delta$, avec $\alpha = 3\frac{(2\pi)^4}{3!}\zeta(6)^2\zeta(4)^2 + 2\frac{(2\pi)^6}{5!}\zeta(4)^3\zeta(6)$, ou que $\zeta(8)E_4^2 = \zeta(4)^2E_8$ [en considérant $\Delta^{-2}(\zeta(8)E_4^2 - \zeta(4)^2E_8)^3$], ou encore que E_{2k} est un polynôme en E_4 et E_6.

La fonction η apparaît dans des contextes assez variés. Par exemple, écrivons le nombre de solutions de l'équation $y^2+y = x^3-x^2$ dans $\mathbf{F}_p$ sous la forme $p+a_p$, et formons le produit $\frac{1}{1-11^{-s}}\prod_{p\neq 11}\frac{1}{1-a_pp^{-s}+p^{1-2s}}$, que l'on développe sous la forme $\sum_{n\geqslant 1}a_nn^{-s}$. Alors $\sum_{n\geqslant 1}a_nq^n = \eta(\tau)^2\eta(11\tau)^2$ (Eichler, 1954). Ce résultat a donné naissance à une conjecture célèbre (la conjecture de Taniyama-Weil) reliant courbes elliptiques et formes modulaires, dont une solution partielle a permis à Wiles (1994) de démontrer le th. de Fermat ; le cas général a été établi par Breuil, Conrad, Diamond et Taylor (1999).

$x \mapsto \frac{-1}{2i\pi}(2i\pi xy)' = -xy' - y$. Appliquer $\mathscr{F}$ à l'identité $t\phi_s' + i\phi_s' + s\phi_s = 0$ nous fournit donc la relation $-xy' - y - 2\pi xy + sy = 0$, soit $xy' + (2\pi x + 1 - s)y = 0$, ce que l'on cherchait.

(iv) L'équation différentielle ci-dessus peut se réécrire sous la forme $\frac{y'}{y} = -2\pi + \frac{s-1}{x}$, dont les solutions sur $\mathbf{R}_+^*$ et $\mathbf{R}_-^*$ sont de la forme $c^{\pm}e^{-2\pi x}|x|^{s-1}$. Or on sait que $\hat{\phi}_s$ est à décroissance rapide à l'infini, ce qui implique que $c^- = 0$. On en déduit le résultat.

Question 2. (i) Si $a > 0$, on a $|e^{-\tau x}x^{s-1}| \leqslant e^{-ax}x^{s-1}$, pour tous $x \in \mathbf{R}_+$ et $\tau \in \Omega_a$, et comme $x \mapsto e^{-ax}x^{s-1}$ est sommable sur $\mathbf{R}_+$ et $\tau \mapsto e^{-\tau x}x^{s-1}$ est holomorphe sur Ω_a, pour tout $x \in \mathbf{R}_+$, on peut appliquer le th. V.5.7 pour en déduire que $\tau \mapsto \mathrm{G}_s(\tau) = \int_0^{+\infty} e^{-\tau x}x^{s-1}\,dx$ est holomorphe sur Ω_a. Comme ceci est vrai pour tout $a > 0$, G_s est holomorphe sur $\cup_{a>0}\Omega_a = \Omega_0$.

(ii) Si $\tau \in \mathbf{R}_+^*$, on obtient $\mathrm{G}_s(\tau) = \int_0^{+\infty} e^{-u}u^{s-1}\tau^{1-s}\frac{du}{\tau} = \frac{\Gamma(s)}{\tau^s}$, via le changement de variable $x = \frac{u}{\tau}$. Maintenant, $\tau \mapsto \frac{\Gamma(s)}{\tau^s}$ est holomorphe sur Ω_0, et donc $\mathrm{G}_s(\tau) - \frac{\Gamma(s)}{\tau^s}$ est une fonction holomorphe sur l'ouvert connexe Ω_0, nulle sur $\mathbf{R}_+^*$. Elle est donc identiquement nulle d'après le th. des zéros isolés, ce qui permet de conclure.

(iii) On a $\mathrm{Im}(\log(t+i)) \in]0, \pi[$, si $t \in \mathbf{R}$, il s'ensuit que $\mathrm{Im}(\log(t+i) - \frac{i\pi}{2}) \in]-\frac{\pi}{2}, \frac{\pi}{2}[\subset [-\pi, \pi[$, et donc que $\log(1-it) = \log\frac{t+i}{i} = \log(t+i) - \frac{i\pi}{2}$. Ceci permet de conclure.

(iv) Comme $\hat{\phi}_s$ est à décroissance rapide et continue, elle est sommable, et il résulte de la formule d'inversion de Fourier dans L^1 (prop. IV.3.25), que $\overline{\mathscr{F}}\hat{\phi}_s = \phi_s$. Par ailleurs, on a

$$\overline{\mathscr{F}}\hat{\phi}_s(t) = \int_{-\infty}^{+\infty} e^{2i\pi tx}\hat{\phi}_s(x) = c(s)\int_0^{+\infty} e^{2i\pi tx}e^{-2\pi x}x^{s-1}\,dx,$$

et les (ii) et (iii) nous donnent $\overline{\mathscr{F}}\hat{\phi}_s(t) = \frac{c(s)\Gamma(s)}{(2\pi(1-it))^s} = \frac{c(s)e^{i\frac{\pi}{2}s}\Gamma(s)}{(2\pi)^s}\phi_s(t)$. On en déduit le résultat.

Question 3. (i) Si $x > 0$, on intègre la fonction $g_s(z) = \frac{e^{-2i\pi zx}}{(z+i)^s}$ le long du chemin γ_{R} composé du segment $[-\mathrm{R}, \mathrm{R}]$ et du demi-cercle inférieur de centre 0 et de rayon R. La fonction g est méromorphe sur $\mathbf{C}$, holomorphe en dehors d'un pôle en $z = -i$, et le résidu $\mathrm{res}(g_s, -i)$ en ce point est le terme de degré $s-1$ dans le développement de Taylor de $e^{-2i\pi zx}$, à savoir $\frac{1}{(s-1)!}(-2i\pi x)^{s-1}e^{-2i\pi(-i)x} = (-i)^{s-1}\frac{(2\pi)^{s-1}}{(s-1)!}e^{-2\pi x}$. Quand $\mathrm{R} > 1$, on a $\mathrm{I}(\gamma_{\mathrm{R}}, -i) = -1$, et donc $\int_{\gamma_{\mathrm{R}}} g_s(z)dz = -2i\pi(-i)^{s-1}\frac{(2\pi)^{s-1}}{(s-1)!}e^{-2\pi x} = (-i)^s\frac{(2\pi)^s}{\Gamma(s)}e^{-2\pi x}$.

Quand $\mathrm{R} \to +\infty$, l'intégrale sur le segment tend vers $\hat{\phi}_s(x)$, et sur le demi-cercle on a les majorations $|e^{-2i\pi zx}| \leqslant 1$ et $\left|\frac{1}{(z+i)^s}\right| \leqslant \frac{1}{(\mathrm{R}-1)^s}$, et comme le demi-cercle est de longueur $\pi\mathrm{R}$, l'intégrale sur le demi-cercle est majorée, en module, par $\frac{\pi\mathrm{R}}{(\mathrm{R}-1)^s}$; elle tend donc vers 0. Un passage à la limite nous donne donc $\hat{\phi}_s(x) = (-i)^s\frac{(2\pi)^s}{\Gamma(s)}e^{-2\pi x}$, ce qui est compatible avec les résultats de la question 2.

Si $x \leqslant 0$, on intègre $g_s(z)$ le long du chemin γ_{R}^+ composé du segment $[-\mathrm{R}, \mathrm{R}]$ et du demi-cercle supérieur de centre 0 et de rayon R. La seule chose qui change avec le calcul précédent est que $\mathrm{I}(\gamma_{\mathrm{R}}^+, -i) = 0$, et donc que l'intégrale le long de ce chemin est nulle, ce qui nous donne $\hat{\phi}_s(x) = 0$.

(ii) Si s n'est pas un entier, la méthode des résidus permet, comme ci-dessus, de montrer que $\hat{\phi}_s(x) = 0$, si $x \leqslant 0$, car g_s est holomorphe dans un ouvert contenant γ_{R}^+. Par contre, on ne peut pas calculer $\hat{\phi}_s$ par un calcul de résidu car g_s n'est pas méromorphe dans un ouvert contenant γ_{R} (il y a une discontinuité le long d'une demi-droite partant de $-i$ et dépendant du choix [22] de la détermination de log).

22. On peut choisir de couper la demi-droite verticale $[-i, -i\infty[$, et d'intégrer sur un chemin composé du segment $[-\mathrm{R}, \mathrm{R}]$, d'un quart (presque) de cercle de centre 0 et de rayon R, du segment $[-i\mathrm{R}+\varepsilon, -i-\varepsilon]$, d'un demi-cercle de centre $-i$ et de rayon ε parcouru dans le sens trigonométrique, du segment $[-i-\varepsilon, -i\mathrm{R}-\varepsilon]$, et d'un second quart (presque) de cercle de centre 0 et de rayon R (faire un dessin). L'intégrale de g_s sur ce chemin fermé est nulle car on peut le déformer sur un point en restant dans le complémentaire de la demi-droite. Par ailleurs, quand R et ε tendent vers $+\infty$ et 0, les intégrales sur les morceaux de cercles

Question 4. (i) Les normes $|x+\tau y|$ et $\sup(|x|,|y|)$ sont équivalentes sur $\mathbf{R}^2$; il existe donc $c>0$ tel que $|x+\tau y| \geqslant c\sup(|x|,|y|)$, pour tout $(x,y)\in\mathbf{R}^2$. On a donc $\left|\frac{1}{(m+n\tau)^s}\right| \leqslant c^{-\mathrm{Re}(s)}e^{\pi|\mathrm{Im}(-s)|}\frac{1}{\sup(|m|,|n|)^{\mathrm{Re}(s)}}$. On en déduit le résultat avec $a(\mathrm{K}) = -\inf_{s\in\mathrm{K}}\mathrm{Re}(s)$ (on a $a(\mathrm{K})<-2$ car l'inf est atteint en un point du compact) et $\mathrm{C}(\mathrm{K}) = \sup_{s\in\mathrm{K}} c^{-\mathrm{Re}(s)}e^{\pi|\mathrm{Im}(-s)|}$ (on a $\mathrm{C}(\mathrm{K})<+\infty$ car le sup. est atteint en un point du compact).

(ii) Si $k\in\mathbf{N}-\{0\}$, il y a $(2k+1)^2-(2k-1)^2 = 8k$ couples $(m,n)\in\mathbf{Z}^2$ vérifiant $\sup(|m|,|n|)=k$, et donc $4k$ dans Y. Si K est un compact de Ω_2, on a donc $\sum_{(m,n)\in\mathrm{Y}}\left|\frac{1}{(m+n\tau)^s}\right| \leqslant \sum_{k=1}^{+\infty} 4k\mathrm{C}(\mathrm{K})k^{a(\mathrm{K})} < +\infty$ car $1+a(\mathrm{K})<-1$. La série est donc normalement convergente sur tout compact de Ω_2, ce qui permet d'utiliser le th. V.5.1 pour montrer que la somme est holomorphe sur Ω_2, chacune des fonctions $s\mapsto\frac{1}{(m+n\tau)^s}$, étant holomorphe de manière évidente.

(iii) La fonction h est sommable et sa dérivée aussi. On peut donc utiliser la formule de Poisson (th. IV.3.11) pour obtenir $\sum_{m\in\mathbf{Z}} h(m) = \sum_{\ell\in\mathbf{Z}}\hat{h}(\ell)$. On a $\hat{h}(x) = \int_{\mathbf{R}} e^{-2i\pi tx}\frac{1}{(t+\alpha+i\beta)^s}dt$. Le changement de variable $t=\alpha u-\beta$ nous donne

$$\hat{h}(x) = \beta^{1-s}e^{2i\pi\alpha x}\hat{\phi}_s(\beta x) = \beta^{1-s}e^{2i\pi\alpha x}c(s)e^{-2\pi\beta x}(\beta x)^{s-1} = c(s)x^{s-1}e^{2i\pi n\tau x}.$$

On en déduit le résultat.

(iv) La formule s'obtient en transformant la somme $\sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}$ en $\sum_{k=1}^{+\infty}\sum_{d|k}$, via le changement de variables $d=n$, $k=\ell n$. Il faut quand même vérifier qu'on a le droit de réordonner les termes comme on veut, et pour cela il s'agit de vérifier que la série double est absolument convergente, i.e. que $\sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}\ell^{\sigma-1}e^{-2\pi\alpha n\ell}<+\infty$, si $\sigma=\mathrm{Re}(s)>2$ et $\alpha=\mathrm{Im}(\tau)>0$. Or on peut utiliser le changement de variables ci-dessus dans cette série à termes positifs, et obtenir $\sum_{k=1}^{+\infty}\sum_{d|k} d^{\sigma-1}e^{-2\pi\alpha k}$, et comme k a au plus k diviseurs, qui sont $\leqslant k$, on peut majorer ceci par $\sum_{k=1}^{+\infty}k^{\sigma}e^{-2\pi\alpha k}$, dont la somme est finie. Ceci permet de conclure.

(v) $s\mapsto\sum_{k=1}^{+\infty}\sigma_{s-1}(k)e^{2i\pi k\tau}$ est une série de fonctions holomorphes, qui converge normalement dans tout demi-plan de la forme $\mathrm{Re}(s)\leqslant a$, avec $a\geqslant 1$ (on a $|\sigma_{s-1}(k)|\leqslant k^a$ sur un tel demi-plan). On peut donc utiliser le (ii) du th. V.5.1 pour en déduire l'holomorphie de $\sum_{k=1}\sigma_{s-1}(k)e^{2i\pi k\tau}$ sur $\mathbf{C}$. On conclut en utilisant les propriétés des fonctions ζ et Γ rappelées dans le préambule (dont on déduit, en particulier, que $s\mapsto e^{-i\frac{\pi}{2}s}\frac{(2\pi)^s}{\Gamma(s)}$ est holomorphe sur $\mathbf{C}$, avec des zéros en $s=-n$, pour $n\in\mathbf{N}$).

Comme $\frac{1}{\Gamma}$ s'annule en $s=0$, on a $\mathrm{E}(\tau,0)=\zeta(0)=\frac{-1}{2}$.

Question 5. (i) Soit Ω un ouvert contenant $[0,+\infty[$ sur lequel φ est holomorphe en dehors d'un pôle en 0. On a donc $\varphi(z)=\sum_{i=1}^{k}\frac{a_{-i}}{z^i}+u(z)$, où u est holomorphe sur Ω. Soit $r_1=d(0,\mathbf{C}-\Omega)$. Alors u est somme de sa série de Taylor sur $\mathrm{D}(0,r_1^-)$ (cf. (i) de la rem. V.4.9), qui converge donc absolument sur tout disque fermé $\mathrm{D}(0,r)$, avec $r<r_1$. Pour un tel r, on peut donc écrire $\varphi(z)$ sous la forme $\sum_{n\geqslant -k}a_nz^n$, pour tout $|z|\leqslant r$, et on a $\sum_{n\geqslant -k}|a_n|r^n<+\infty$.

(ii) On a $t^{s-1}\varphi(t)=\sum_{n=-k}^{+\infty}a_nt^{s+n-1}$. Or $\sum_{n=-k}^{+\infty}\int_0^r|a_nt^{s+n-1}|dt\leqslant\sum_{n=-k}^{+\infty}\frac{|a_n|r^{\mathrm{Re}(s)+n}}{\mathrm{Re}(s+n)}<+\infty$, si $\mathrm{Re}(s)>k$, car $\mathrm{Re}(s+n)\geqslant 1$, si $n\neq -k$ et $\sum_{n=-k}^{+\infty}|a_n|r^{\mathrm{Re}(s)+n}<+\infty$. On déduit du th. de Fubini

---

tendent vers 0, l'intégrale sur $[-\mathrm{R},\mathrm{R}]$ tend vers $\hat{\phi}_s(x)$, et les intégrales sur les segments verticaux tendent vers l'intégale sur la demi-droite $[-i\infty,-i[$ (il faut faire attention au fait que la valeur du logarithme n'est pas la même sur les deux demi-droites qui apparaissent). On en déduit, en faisant le changement de variable $t=-i(1+u)$ sur les 2 demi-droites allant de $-i\infty$ à $-i$ et de $-i$ à $-i\infty$,

$$\int_{-\infty}^{+\infty}\frac{1}{(t+i)^s}e^{-2i\pi tx}dt = i(e^{-\frac{3i\pi}{2}s}-e^{\frac{i\pi}{2}s})e^{-2\pi x}\int_0^{+\infty}e^{-2\pi xu}u^{-s}du = 2e^{-\frac{i\pi}{2}s}\sin\pi s\Gamma(1-s)\frac{e^{-2\pi x}}{(2\pi x)^{1-s}}.$$

Une comparaison avec la question 2 fait apparaître la formule des compléments $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}$.

sur $\mathbf{N}\times \mathrm{X}$ que la série converge dans $\mathrm{L}^1([0,r])$ (et donc que la somme est sommable), et que l'on peut intervertir la somme et l'intégrale, ce qui nous donne $\mathrm{I}_1(s)=\sum_{n\geqslant -k}\frac{a_n r^{s+n}}{s+n}$.

Soit $\mathrm{N}\geqslant k$. On découpe la série en $\sum_{n=-k}^{\mathrm{N}}\frac{a_n r^{s+n}}{s+n}$, qui est une fonction méromorphe sur $\mathbf{C}$, avec des pôles simples de résidu a_{-n} en les $n\in\mathbf{Z}$ vérifiant $-\mathrm{N}\leqslant n\leqslant k$, et $\sum_{n\geqslant \mathrm{N}+1}\frac{a_n r^{s+n}}{s+n}$ qui converge normalement sur $\mathrm{D}(0,\mathrm{N}^-)$ car $\left|\frac{a_n r^{s+n}}{s+n}\right|\leqslant r^{\mathrm{Re}(s)}|a_n r^n|$, si $n\geqslant \mathrm{N}+1$ et $|s|<\mathrm{N}$. Il s'ensuit, d'après le th. V.5.1, que $\sum_{n\geqslant \mathrm{N}+1}\frac{a_n r^{s+n}}{s+n}$ définit une fonction holomorphe sur $\mathrm{D}(0,\mathrm{N}^-)$, et donc que I_1 est méromorphe sur $\mathrm{D}(0,\mathrm{N}^-)$, holomorphe en dehors de pôles simples de résidu a_{-n} en les $n\in\mathbf{Z}$ vérifiant $-\mathrm{N}\leqslant n\leqslant k$. Le résultat cherché s'en déduit en écrivant $\mathbf{C}$ comme la réunion des $\mathrm{D}(0,\mathrm{N}^-)$, pour $\mathrm{N}\in\mathbf{N}$.

(iii) On décompose $\Lambda(\varphi,s)$ comme $\mathrm{I}_1(s)+\mathrm{I}_2(s)$, avec $\mathrm{I}_1(s)=\int_0^r\varphi(t)t^{s-1}dt$ et $\mathrm{I}_2(s)=\int_r^{+\infty}\varphi(t)t^{s-1}dt$. La fonction $s\mapsto \mathrm{I}_1(s)$ a été étudiée au (ii) ; il suffit donc d'étudier la fonction $s\mapsto \mathrm{I}_2(s)$. Si φ est à décroissance rapide, $\int_r^{+\infty}\varphi(t)t^{s-1}$ converge pour tout $s\in\mathbf{C}$. Sur une bande verticale $a<\mathrm{Re}(s)<b$, on peut majorer $|t^{s-1}\varphi(t)|$ par $\sup(t^a,t^b)|\varphi(t)|$, qui est sommable sur $[r,+\infty[$. On en déduit, en utilisant le th. V.5.7, que $s\mapsto \mathrm{I}_2(s)$ est holomorphe sur cette bande, et comme $\mathbf{C}$ est la réunion de ces bandes, cela prouve que $s\mapsto \mathrm{I}_2(s)$ est holomorphe sur $\mathbf{C}$. Le résultat s'en déduit.

Question 6. (i) Les conditions $\mathrm{Re}(\alpha)>0$ et $\mathrm{Re}(\alpha\tau)>0$ se traduisent par $0<\arg(\alpha)<\pi-\arg(\tau)$. Par ailleurs, on a $0\leqslant\arg(m+n\tau)\leqslant\arg(\tau)$, si $(m,n)\in \mathrm{Y}_0$, et donc $0\leqslant\arg(\alpha)+\arg(m+n\tau)<\pi$; on en déduit que $\arg(\alpha(m+n\tau))=\arg(\alpha)+\arg(m+n\tau)$, ce qui permet de conclure.

(ii) D'après la question 2, on a $\frac{1}{(\alpha\omega)^s}=\frac{1}{\Gamma(s)}\int_0^{+\infty}e^{-t\alpha\omega}t^{s-1}dt$, si $\omega\in\mathrm{Y}_0$. Il s'ensuit que $f_0(\tau,s)=\frac{\alpha^s}{\Gamma(s)}\sum_{\omega\in\mathrm{Y}_0}\int_0^{+\infty}e^{-t\alpha\omega}t^{s-1}dt$. On a

$$\sum_{\omega\in\mathrm{Y}_0}|e^{-t\alpha\omega}t^{s-1}|=t^{\sigma-1}\sum_{m=1}^{+\infty}\sum_{n=0}^{+\infty}e^{-t(n\mathrm{Re}(\alpha)+m\mathrm{Re}(\alpha\tau))}=\frac{t^{\sigma-1}}{(e^{t\mathrm{Re}(\alpha)}-1)(1-e^{-t\mathrm{Re}(\alpha\tau)})},$$

qui est sommable, car à décroissance rapide à l'infini et $\mathrm{O}(t^{\sigma-3})$ au voisinage de 0 (et $\sigma-3>-1$). On peut donc intervertir somme et intégrale, et le même calcul que ci-dessus montre que $\sum_{\omega\in\mathrm{Y}_0}e^{-t\alpha\omega}=\mathrm{G}_\alpha(t)$, ce qui permet de conclure.

(iii) La fonction G_α vérifie les conditions du (iii) de la question 5. On en déduit que $\Gamma(s)\alpha^{-s}f_0(\tau,s)$ admet un prolongement méromorphe à $\mathbf{C}$, avec des pôles simples en les entiers $\leqslant 2$. Comme $\frac{1}{\Gamma(s)}$ est holomorphe sur $\mathbf{C}$, avec des zéros simples aux entiers négatifs, cela implique que $f_0(\tau,s)$ est holomorphe en dehors de pôles simples en $s=1$ et $s=2$.

(iv) On a

$$\begin{aligned}\mathrm{G}_\alpha(z)=\frac{1}{(e^{\alpha z}-1)(1-e^{-\alpha\tau z})}&=\frac{1}{\alpha^2\tau z^2}\frac{1}{(1+\frac{\alpha z}{2}+\frac{\alpha^2z^2}{6}+\cdots)(1-\frac{\alpha\tau z}{2}+\frac{\alpha^2\tau^2z^2}{6}+\cdots)}\\&=\frac{1}{\alpha^2\tau z^2}+\frac{1}{\alpha z}\frac{\tau-1}{2\tau}+\frac{1}{12\tau}+\frac{\tau}{12}-\frac{1}{4}+\cdots.\end{aligned}$$

Maintenant, d'après le (ii), $\lim_{s\to n}(s-n)\Gamma(s)\alpha^{-s}f_0(\tau,s)$ est le coefficient de degré $-n$ dans le développement de G_α en série de laurent au voisinage de 0. On en déduit que $\alpha^{-2}\lim_{s\to2}(s-2)f_0(\tau,s)=\frac{1}{\alpha^2\tau}$, et donc $\lim_{s\to2}(s-2)f_0(\tau,s)=\frac{1}{\tau}$. De même, $\alpha^{-1}\lim_{s\to1}(s-1)f_0(\tau,s)=\frac{\tau-1}{2\alpha\tau}$, et donc $\lim_{s\to1}(s-1)f_0(\tau,s)=\frac{\tau-1}{2\tau}$. Enfin, comme $\lim_{s\to0}\alpha^{-s}s\Gamma(s)=1$, on a $f_0(\tau,0)=\frac{1}{12\tau}+\frac{\tau}{12}-\frac{1}{4}$.

Question 7. (i) $(m,n)\mapsto(-n,m)$ induit une bijection de Y_0 sur Y_1 et $(m,n)\mapsto(n,-m)$ induit une bijection de Y_1 sur Y_0.

Maintenant, $\mathrm{E}\big(\frac{-1}{\tau},2k\big)=\sum_{(m,n)\in\mathrm{Y}}\big(m+\frac{-n}{\tau}\big)^{-2k}=\tau^k\sum_{(m,n)\in\mathrm{Y}}\frac{1}{(-n+m\tau)^{2k}}$. La série étant absolument convergente, on peut sommer les termes dans l'ordre que l'on veut, et comme $(-n+m\tau)^{2k}=(n-m\tau)^{2k}$, on a $\mathrm{E}\big(\frac{-1}{\tau},2k\big)=\sum_{(m,n)\in\mathrm{Y}_0}\frac{1}{(-n+m\tau)^{2k}}+\sum_{(m,n)\in\mathrm{Y}_1}\frac{1}{(n-m\tau)^{2k}}$. Or $(m,n)\mapsto(-n,m)$ induit une bijection

de Y_0 sur Y_1, ce qui fait que la première somme vaut $\sum_{(m,n)\in \mathrm{Y}_1} \frac{1}{(m+n\tau)^{2k}}$, tandis que la seconde vaut $\sum_{(m,n)\in \mathrm{Y}_0} \frac{1}{(m+n\tau)^{2k}}$, puisque $(m,n) \mapsto (n,-m)$ induit une bijection de Y_1 sur Y_0. On en déduit le résultat.

(ii) On a $0 < \arg(\tau) < \pi$.

Si $(m,n) \in \mathrm{Y}_0$, alors $0 \leqslant \arg(-n+m\tau) < \pi$, et donc $-\pi < \arg(\tau) - \arg(-n+m\tau) < \pi$, ce qui fait que $\arg(\frac{\tau}{-n+m\tau}) = \arg(\tau) - \arg(-n+m\tau)$. On en déduit le résultat dans ce cas.

Si $(m,n) \in \mathrm{Y}_1$, on a $0 \leqslant \arg(n-m\tau) < \arg(\tau)$, et donc $0 < \arg(\frac{\tau}{n-m\tau}) = \arg(\tau) - \arg(n-m\tau) < \pi$. On en déduit que $\arg(\frac{\tau}{-n+m\tau}) = \arg(\frac{\tau}{n-m\tau}) - \pi$, ce qui permet de conclure.

(iii) Commençons par supposer que $\mathrm{Re}(s) > 2$, de telle sorte que toutes les séries considérées sont absolument convergentes. Comme ci-dessus $f_i\big(\frac{-1}{\tau}, s\big) = \sum_{(m,n)\in \mathrm{Y}_i} \big(\frac{\tau}{-n+m\tau}\big)^s$. Or $\big(\frac{\tau}{-n+m\tau}\big)^s = \frac{\tau^s}{(-n+m\tau)^s}$, si $(m,n) \in \mathrm{Y}_0$, et comme $(m,n) \mapsto (-n,m)$ induit une bijection de Y_0 sur Y_1, on en déduit que $f_0\big(\frac{-1}{\tau}, s\big) = \tau^s f_1(\tau, s)$. De même, $\big(\frac{\tau}{-n+m\tau}\big)^s = e^{-i\pi s}\frac{\tau^s}{(n-m\tau)^s}$, si $(m,n) \in \mathrm{Y}_1$, et comme $(m,n) \mapsto (n,-m)$ induit une bijection de Y_1 sur Y_0, on en déduit que $f_1\big(\frac{-1}{\tau}, s\big) = e^{-i\pi s}\tau^s f_0(\tau, s)$. Le résultat s'en déduit (si $\mathrm{Re}(s) > 2$) via la formule $\mathrm{E}\big(\frac{-1}{\tau}, s\big) = f_0\big(\frac{-1}{\tau}, s\big) + f_1\big(\frac{-1}{\tau}, s\big)$.

Le cas général s'en déduit par unicité du prolongement analytique (les deux membres sont des fonctions méromorphes sur $\mathbf{C}$, qui coïncident dans le demi-plan Ω_2 ; leur différence est donc identiquement nulle).

(iv) En utilisant la formule $\lim_{s\to 2}(s-2)f_0(\tau,s) = \frac{1}{\tau}$, on obtient $\lim_{s\to 2}(e^{-i\pi s}-1)f_0(\tau,s) = -i\pi\frac{1}{\tau}$, ce qui permet d'obtenir la formule voulue par passage à la limite à partir du (iii).

Question 8. (i) On a $|-e^{2i\pi n\tau}| \leqslant e^{-2\pi n a}$, si $\mathrm{Im}(\tau) > a$. Il en résulte que la série des $-e^{2i\pi n\tau}$ converge normalement sur le demi-plan $\mathrm{Im}(\tau) > a$, si $a > 0$, et donc que le produit $\prod_{n=1}^{+\infty}(1-e^{2i\pi n\tau})$ converge et définit une fonction holomorphe sur ce demi-plan, d'après le th. V.5.4. De plus, comme aucun des termes du produit ne s'annule, la fonction ainsi définie ne s'annule pas non plus. On conclut en écrivant $\mathscr{H}$ comme la réunion des demi-plans $\mathrm{Im}(\tau) > a$, pour $a > 0$.

(ii) Comme η est une fonction holomorphe qui ne s'annule pas sur l'ouvert contractile $\mathscr{H}$, il existe g, holomorphe sur $\mathscr{H}$, telle que $e^g = \eta$. Par ailleurs, la série $\frac{i\pi\tau}{12} + \sum_{n=1}^{+\infty}\log(1-e^{2i\pi n\tau})$ est normalement convergente sur tout demi-plan $\mathrm{Im}(\tau) > a$, et donc définit une fonction holomorphe h sur $\mathscr{H}$. Or les exponentielles des sommes partielles de cette série ne sont autres que les produits partiels de η ; un passage à la limite montre donc que $e^h = \eta$. On en déduit que $g-h$ est une fonction holomorphe sur $\mathscr{H}$, à valeurs dans $2i\pi\mathbf{Z}$; elle est donc constante (par connexité de l'image, ou par le th. de l'image ouverte). Ceci permet de conclure.

(iii) Comme $\lim_{s\to 0}\frac{1}{s}\frac{1}{\Gamma(s)} = 1$, on a $\mathrm{F}(\tau) = \mathrm{C} + \sum_{k=1}^{+\infty}\sigma_{-1}(k)e^{2i\pi k\tau}$, où $\mathrm{C} = \zeta'(0)$.

Par ailleurs, $\log\eta = \frac{i\pi\tau}{12} + \sum_{n=1}^{+\infty}\log(1-e^{2i\pi n\tau}) = \frac{i\pi\tau}{12} - \sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}\frac{1}{\ell}e^{2i\pi n\ell\tau}$. On obtient le résultat en transformant la somme $\sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}$ en $\sum_{k=1}^{+\infty}\sum_{d|k}$, via le changement de variables $d = \ell$, $k = \ell n$.

(iv) En dérivant par rapport à s l'identité $\mathrm{E}(\frac{-1}{\tau}, s) = \tau^s(\mathrm{E}(\tau,s) + (e^{-i\pi s}-1)f_0(\tau,s))$, et en évaluant en 0, on obtient $\mathrm{F}(\frac{-1}{\tau}) = (\log\tau)\mathrm{E}(\tau,0) + \mathrm{F}(\tau) - i\pi f_0(\tau,0)$, ce qui peut se réécrire, en utilisant les formules $\mathrm{E}(\tau,0) = \frac{-1}{2}$ et $f_0(\tau) = \frac{1}{12\tau} + \frac{\tau}{12} - \frac{1}{4}$ des questions 4.(v) et 6.(iv), $\mathrm{F}(\frac{-1}{\tau}) + \frac{i\pi}{12\tau} = -\frac{1}{2}\log + \tau\mathrm{F}(\tau) - \frac{i\pi\tau}{12} + \frac{i\pi}{4}$. La première formule s'en déduit en utilisant le (iii) ; on obtient la seconde en prenant l'exponentielle des deux membres.

(v) En dérivant l'identité du (iii), on obtient $\frac{\eta'(\tau)}{\eta(\tau)} = -\mathrm{F}'(\tau) + \frac{i\pi}{12}$. Par ailleurs, comme une série convergente de fonctions holomorphes se dérive terme à terme, on a $\mathrm{F}'(\tau) = 2i\pi\sum_{k=1}^{+\infty}k\sigma_{-1}(k)e^{2i\pi k\tau}$. Or $k\sigma_{-1}(k) = \sum_{d|k}\frac{k}{d} = \sigma_1(k)$, car $d \mapsto \frac{k}{d}$ induit une bijection des diviseurs de k. Il s'ensuit que $\mathrm{F}'(\tau) = \frac{-1}{2i\pi}(\mathrm{E}(\tau,2) - \zeta(2))$, et donc que $\frac{\eta'(\tau)}{\eta(\tau)} + \frac{1}{2i\pi}\mathrm{E}(\tau,2) = \frac{i\pi}{12} + \frac{1}{2i\pi}\zeta(2)$.

Maintenant, si on dérive l'identité du (iv), on obtient la relation $\frac{1}{\tau^2}\frac{\eta'(-1/\tau)}{\eta(-1/\tau)} = \frac{1}{2\tau} + \frac{\eta'(\tau)}{\eta(\tau)}$. On en déduit, en utilisant le (iv) de la question 7, que la fonction $h(\tau) = \frac{\eta'(\tau)}{\eta(\tau)} + \frac{1}{2i\pi}\mathrm{E}(\tau,2)$ vérifie l'équation fonctionnelle

$h(-1/\tau) = \tau^2 h(\tau)$. Comme h est constante d'après ce qui précède, cela implique que $h = 0$, et donc que $\frac{i\pi}{12} + \frac{1}{2i\pi}\zeta(2) = 0$. On en déduit le résultat.

Question 9. (i) Le changement de variable $t = \sqrt{\frac{12}{y}}u$ (ou les formules pour les dilatations translations) nous donne

$$\int_{\mathbf{R}} e^{-2i\pi tx} e^{-2i\pi \frac{at}{12}} e^{-\pi \frac{yt^2}{12}} dt = \sqrt{\frac{12}{y}} \int_{\mathbf{R}} e^{-2i\pi\sqrt{\frac{12}{y}}(x+\frac{a}{12})u} e^{-\pi u^2} du = \sqrt{\frac{12}{y}} e^{-\pi\frac{12}{y}(x+\frac{a}{12})^2} = \sqrt{\frac{12}{y}} e^{-\frac{\pi}{12y}(12x+a)^2}.$$

La formule $\sum_{n\in\mathbf{Z}} e^{-2i\pi\frac{an}{12}} e^{-\pi\frac{yn^2}{12}} = \sqrt{\frac{12}{y}} \sum_{n\in\mathbf{Z}} e^{-\frac{\pi}{12y}(12n+a)^2}$ est donc juste la formule de Poisson pour la fonction $t \mapsto e^{-2i\pi\frac{at}{12}} e^{-\pi\frac{yt^2}{12}}$, qui appartient à $\mathscr{S}(\mathbf{R})$.

(ii) On a $\sum_{a=-5}^{6} \chi(a) e^{-2i\pi\frac{an}{12}} = 2(\cos\frac{n\pi}{6} - \cos\frac{5n\pi}{6})$, et le résultat suit de ce que

$$\cos\frac{n\pi}{6} = \cos\frac{5n\pi}{6} = \begin{cases} 1 & \text{si } n \equiv 0 \bmod 12, \\ -1 & \text{si } n \equiv 6 \bmod 12, \\ 0 & \text{si } n \equiv \pm 3 \bmod 12, \\ \frac{1}{2} & \text{si } n \equiv \pm 2 \bmod 12, \\ \frac{-1}{2} & \text{si } n \equiv \pm 4 \bmod 12, \end{cases} \quad \text{et} \quad \cos\frac{n\pi}{6} = -\cos\frac{5n\pi}{6} = \begin{cases} \frac{\sqrt{3}}{2} & \text{si } n \equiv \pm 1 \bmod 12, \\ \frac{-\sqrt{3}}{2} & \text{si } n \equiv \pm 5 \bmod 12. \end{cases}$$

(iii) On a $\mathrm{H}(iy) = \frac{1}{2}\sum_{n\in\mathbf{Z}} \chi(n) e^{-\pi\frac{n^2 y}{12}} = \frac{1}{2\sqrt{12}} \sum_{n\in\mathbf{Z}} \big(\sum_{a=-5}^{6} \chi(a) e^{-2i\pi\frac{an}{12}}\big) e^{-\pi\frac{n^2 y}{12}}$, ce qui se réécrit, en utilisant le (i) et la convergence absolue de la série, sous la forme $\frac{1}{2\sqrt{y}} \sum_{a=-5}^{6} \chi(a) \sum_{n\in\mathbf{Z}} e^{-\pi\frac{(12n+a)^2}{12y}}$. Par ailleurs, $\chi(12n+a) = \chi(a)$, et l'application $(a,n) \mapsto 12n+a$ est une bijection de $\{-5,\dots,6\}\times\mathbf{Z}$ sur $\mathbf{Z}$, ce qui permet de réécrire la dernière somme sous la forme $\frac{1}{2\sqrt{y}} \sum_{m\in\mathbf{Z}} \chi(m) e^{-\pi\frac{m^2}{12y}} = \frac{1}{\sqrt{y}}\mathrm{H}(\frac{i}{y})$. On a donc bien $\mathrm{H}(\frac{i}{y}) = \sqrt{y}\,\mathrm{H}(iy)$, si $y \in \mathbf{R}_+^*$.

Maintenant, la fonction $\tau \mapsto \mathrm{H}(\frac{-1}{\tau}) - \sqrt{\frac{\tau}{i}}\mathrm{H}(\tau)$ est holomorphe sur $\mathscr{H}$, et nulle sur $i\mathbf{R}_+^*$ d'après ce qui précède. Elle est donc, d'après le th. des zéros isolés, identiquement nulle, ce qui permet de conclure.

(iv) Que $\mathrm{J}(\frac{-1}{\tau}) = \mathrm{J}(\tau)$ résulte du (iii) et de la question 8.(iv). Par ailleurs, $e^{-i\pi\tau/12}\eta(\tau)$ est périodique de période 1 puisque tous les termes du produit le sont. Il en est de même de $e^{-i\pi\tau/12}\mathrm{H}(\tau) = \frac{1}{2}\sum_{n\in\mathbf{Z}} (-1)^n e^{-i\pi\frac{(6n+1)^2-1}{12}}$ car $\frac{(6n+1)^2-1}{12} = 3n^2+n$ est un entier pair, pour tout $n \in \mathbf{Z}$. Le quotient de $e^{-i\pi\tau/12}\mathrm{H}(\tau)$ par $e^{-i\pi\tau/12}\eta(\tau)$, qui n'est autre que $\mathrm{J}(\tau)$, est donc aussi périodique de période 1, ce qui permet de conclure.

(v) On a $\mathrm{J}(\tau) = \tilde{\mathrm{J}}(e^{2i\pi\tau})$, où $\tilde{\mathrm{J}}(q)$ est le quotient de $\sum_{n\in\mathbf{Z}} (-1)^n q^{(3n^2+n)/2}$, qui est une fonction holomorphe sur $\mathrm{D}(0,1^-)$ (utiliser le th. V.5.1), par $\prod_{n\geqslant 1}(1-q^n)$, qui est une fonction holomorphe ne s'annulant pas sur $\mathrm{D}(0,1^-)$ (cf. th. V.5.4) ; c'est donc une fonction holomorphe sur $\mathrm{D}(0,1^-)$. On a $\tilde{\mathrm{J}}(0) = 1$, comme on le voit en posant $q = 0$ dans les série et produit ci-dessus.

(vi) Comme $\tilde{\mathrm{J}}(0) = 1$, la fonction $q \mapsto q^{-1}(\tilde{\mathrm{J}}(q) - 1)$ a une limite ℓ en $q = 0$. Ceci se traduit par le fait que $\tau \mapsto e^{-2i\pi\tau}(\mathrm{J}(\tau) - 1)$ tend vers ℓ quand $\mathrm{Im}(\tau) \to +\infty$. Il existe donc $\mathrm{M} > 0$ tel que l'on ait $|\mathrm{J}(\tau) - 1| \leqslant (|\ell| + 1)e^{-2\pi\mathrm{Im}(\tau)}$, si $\mathrm{Im}(\tau) > \mathrm{M}$. Comme la fonction continue $\tau \mapsto e^{2\pi\mathrm{Im}(\tau)}|\mathrm{J}(\tau) - 1|$ est bornée sur le compact $\overline{\mathrm{X}} \cap \{\tau,\ \mathrm{Im}(\tau) \leqslant \mathrm{M}\}$, cela prouve que $e^{2\pi\mathrm{Im}(\tau)}|\mathrm{J}(\tau) - 1|$ est bornée sur $\overline{\mathrm{X}}$, et donc qu'il existe $c > 0$ tel que $|\mathrm{J}(\tau) - 1| \leqslant c\, e^{-2\pi\mathrm{Im}(\tau)}$, pour tout $\tau \in \overline{\mathrm{X}}$.

Supposons $\mathrm{J} - 1$ non identiquement nulle sur $\overline{\mathrm{X}}$, et soit τ_0, avec $|\mathrm{J}(\tau_0) - 1| > 0$. On choisit alors M tel que $c\, e^{-2\pi\mathrm{M}} < |\mathrm{J}(\tau_0) - 1|$ de telle sorte que $|\mathrm{J}(\tau) - 1| < |\mathrm{J}(\tau_0) - 1|$, si $\mathrm{Im}(\tau) \geqslant \mathrm{M}$. Le maximum de $|\mathrm{J} - 1|$ sur $\overline{\mathrm{X}}$ est donc le même que sur le compact $\overline{\mathrm{X}} \cap \{\tau,\ \mathrm{Im}(\tau) \leqslant \mathrm{M}\}$, et le principe du maximum implique qu'il est atteint sur le bord de ce compact. Comme il n'est pas atteint sur le segment $[\frac{-2}{3} + i\mathrm{M}, \frac{2}{3} + i\mathrm{M}]$, car on a $|\mathrm{J}(\tau) - 1| < |\mathrm{J}(\tau_0) - 1|$ sur ce segment, cela prouve qu'il l'est en un point de $\partial\mathrm{X}$.

(vii) Si τ est dans la demi-droite $]\frac{-2+i}{3}, \frac{-2}{3}+i\infty[$, alors $\tau+1 \in \mathrm{X}$. De même, si τ est dans la demi-droite $]\frac{2+i}{3}, \frac{2}{3}+i\infty[$, alors $\tau-1 \in \mathrm{X}$. Si $\tau = x+iy \in [\frac{-2+i}{3}, \frac{2+i}{3}]$, alors $\frac{-1}{\tau} = \frac{-x+\frac{i}{3}}{x^2+\frac{1}{9}} = x'+iy'$ vérifie $y' > \frac{1}{3}$ car $x^2+\frac{1}{9} \leqslant \frac{5}{9} < 1$, et $|x'| < \frac{|x|}{x^2} \leqslant \frac{3}{2}$; il s'ensuit qu'au moins un des trois nombres $\frac{-1}{\tau}$, $\frac{-1}{\tau}+1$ ou $\frac{-1}{\tau}-1$ appartient à X.

Soit $\tau_0 \in \partial\mathrm{X}$ tel que $|\mathrm{J}(\tau_0)-1|$ réalise le maximum de $|\mathrm{J}-1|$. Comme J prend la même valeur en les nombres τ_0+1, τ_0-1, $\frac{-1}{\tau_0}$, $\frac{-1}{\tau_0}+1$ et $\frac{-1}{\tau_0}-1$ qu'en τ_0, et qu'un de ces nombres appartient à X, on voit que $|\mathrm{J}-1|$ atteint son maximum dans l'ouvert X. D'après le principe du maximum, cela implique que $\mathrm{J}-1$ est constante, et comme $\lim_{\tau\to i\infty}\mathrm{J}(\tau)-1=0$, cela prouve que $\mathrm{J}-1$ est identiquement nulle sur X, et donc aussi sur $\mathscr{H}$, d'après le th. des zéros isolés. On en déduit les identités $\mathrm{J}=1$ et $\eta=\mathrm{H}$ que l'on cherchait à établir.

Question 10. (i) Si $q \in \mathrm{D}(0,1^-)$ est fixé, la série $\sum_{n\geqslant 1}|q^{2n}|+|q^{2n-1}w|+|q^{2n-1}w^{-1}|$ est normalement convergente sur tout compact de $\mathbf{C}^*$, et donc le produit définit une fonction holomorphe de w sur $\mathbf{C}^*$, d'après le th. V.5.4.

(ii) L'existence et l'unicité des $a_m(q)$ est un cas particulier du cor. VI.3.2, appliqué à $z_0=0$, $\mathrm{R}_1=0$ et $\mathrm{R}_2=+\infty$.

(iii) Quand on remplace w par q^2w, on perd le terme $1+qw$ de $\prod_{n\geqslant 1}(1+q^{2n-1}w)$, et on gagne un terme $1+q^{-1}w^{-1}$ dans $\prod_{n\geqslant 1}(1+q^{2n-1}w^{-1})$. On a donc $\mathrm{A}(q,q^2w)=\frac{1+q^{-1}w^{-1}}{1+qw}\mathrm{A}(q,w)=q^{-1}w^{-1}\mathrm{A}(q,w)$.

(iv) On a $\sum_{m\in\mathbf{Z}}a_m(q)w^m = qw\mathrm{A}(q,q^2w) = \sum_{m\in\mathbf{Z}}a_m(q)q^{2m+1}w^{m+1}$. On en déduit la relation $a_m(q)=q^{2m-1}a_{m-1}(q)$, pour tout $m\in\mathbf{Z}$. En écrivant $a_m(q)$ sous la forme $q^{m^2}b_m(q)$, cette relation devient $b_m(q)=b_{m-1}(q)$, pour tout $m\in\mathbf{Z}$; on en déduit que $b_m(q)=b_0(q)=a_0(q)$ pour tout $m\in\mathbf{Z}$, ce qui permet de conclure.

(v) On a $\mathrm{A}(e^{3i\pi\tau},-e^{i\pi\tau})=\prod_{n\geqslant 1}(1-e^{i\pi 3n\tau})(1-e^{i\pi(3n-1)\tau})(1-e^{i\pi(3n-2)\tau})=\prod_{k\geqslant 1}(1-e^{i\pi k\tau})$, et donc $\mathrm{A}(e^{3i\pi\tau},-e^{i\pi\tau})=e^{-i\pi\tau/12}\eta(\tau)$, si $\tau\in\mathscr{H}$. Par ailleurs, il résulte des (ii) et (iv) que l'on a aussi $\mathrm{A}(e^{3i\pi\tau},-e^{i\pi\tau})=a_0(e^{3i\pi\tau})\sum_{m\in\mathbf{Z}}(-1)^m e^{i\pi(3m^2+m)/2}$, et donc $\mathrm{A}(e^{3i\pi\tau},-e^{i\pi\tau})=a_0(e^{3i\pi\tau})e^{-i\pi\tau/12}\mathrm{H}(\tau)$, si $\tau\in\mathscr{H}$. Comme $\mathrm{H}=\eta$ sur $\mathscr{H}$, d'après la question 9.(vii), cela montre que $a_0=1$; la formule du produit triple s'en déduit.

(vi) On utilise la formule du produit triple avec $q=e^{i\pi\tau}$ et $w=1$, et on écrit $1+q^{2n-1}$ sous la forme $\frac{\big((1-q^{4n-2})(1-q^{4n})\big)(1-q^{2n})}{\big((1-q^{2n-1})(1-q^{2n})\big)(1-q^{4n})}$, ce qui nous donne

$$\begin{aligned}\prod_{n\geqslant 1}(1+q^{2n-1}) &= \Big(\prod_{n\geqslant 1}(1-q^{4n-2})(1-q^{4n})\Big)\Big(\prod_{n\geqslant 1}(1-q^{2n})\Big)\Big(\prod_{n\geqslant 1}(1-q^{2n-1})(1-q^{2n})\Big)^{-1}\Big(\prod_{n\geqslant 1}(1-q^{4n})\Big)^{-1}\\ &= \big(e^{-i\pi\tau/12}\eta(\tau)\big)^2\big(e^{-i\pi\tau/24}\eta(\tau/2)\big)^{-1}\big(e^{-i\pi\tau/6}\eta(2\tau)\big)^{-1}\end{aligned}$$

On en déduit que

$$\theta(\tau)=\Big(\prod_{n\geqslant 1}(1-q^{2n})\Big)\Big(\prod_{n\geqslant 1}(1+q^{2n-1})\Big)^2=\frac{\big(e^{-i\pi\tau/12}\eta(\tau)\big)^5}{\big(e^{-i\pi\tau/24}\eta(\tau/2)\big)^2\big(e^{-i\pi\tau/6}\eta(2\tau)\big)^2}=\frac{\eta(\tau)^5}{\eta(2\tau)^2\eta(\tau/2)^2}.$$

H.12. Irrationalité de $\zeta(3)$

Le but de ce devoir est de démontrer (Apéry, 1979) que $\zeta(3) = \sum_{k=1}^{+\infty} \frac{1}{k^3}$ est un nombre irrationnel [23]. La démonstration proposée est adaptée d'une relecture de la démonstration d'Apéry par Nesterenko. Elle fait appel aux fonctions holomorphes et, de manière cruciale, aux propriétés de la fonction Γ. Nous aurons en particulier grand usage de la formule de Stirling (prop. VII.2.9). Soit Ω le demi-plan $\{s \in \mathbf{C},\ \mathrm{Re}(s) > \frac{1}{4}\}$, soit $g : \Omega \to \mathbf{C}$ la fonction $z \mapsto z \log z - z$, où log est la détermination principale du logarithme, et soit $\varepsilon(z) = \log \Gamma(z) - g(z) + \frac{1}{2} \log z - \frac{1}{2} \log 2\pi$. Alors la formule de Stirling implique l'existence de $\mathrm{C}_1 > 0$ tel que $|\varepsilon(z)| \leqslant \frac{\mathrm{C}_1}{|z|}$, pour tout $z \in \Omega$.

Question 1. Soit $\mathrm{Q}_n(\mathrm{X}) = \frac{(\mathrm{X}-1)\cdots(\mathrm{X}-n)}{\mathrm{X}(\mathrm{X}+1)\cdots(\mathrm{X}+n)}$ et $\mathrm{R}_n = \mathrm{Q}_n^2$. Soit $d_n = \mathrm{ppcm}(1, 2, \ldots, n)$.

(i) Montrer que les a_i, définis par $\mathrm{Q}_n = \sum_{i=0}^{n} \frac{a_i}{\mathrm{X}+i}$, appartiennent à $\mathbf{Z}$.

(ii) Soit $\sum_{i=0}^{n} \frac{\alpha_i}{(\mathrm{X}+i)^2} + \frac{\beta_i}{\mathrm{X}+i}$ la décomposition de R_n en éléments simples. Montrer que $\alpha_i \in \mathbf{Z}$, que $d_n\beta_i \in \mathbf{Z}$ et que $\sum_{i=0}^{n} \beta_i = 0$.

(iii) Soit $\mathrm{S}_n = \sum_{k=1}^{+\infty}(-\mathrm{R}_n'(k))$. Montrer que $\mathrm{S}_n = u_n\zeta(3) - \frac{v_n}{d_n^3}$, avec $u_n, v_n \in \mathbf{Z}$.

Question 2. Soit $\mathrm{F}_n(s) = \left(\frac{\pi}{\sin \pi s}\right)^2 \mathrm{R}_n(s)$.

(i) Montrer que F_n est méromorphe sur Ω, holomorphe en dehors de pôles doubles aux entiers $\geqslant n+1$, et est à décroissance rapide sur toute droite verticale incluse dans Ω.

(ii) Montrer que $\left(\frac{\pi}{\sin \pi s}\right)^2 = \frac{1}{(s-k)^2} + \mathrm{O}(1)$ au voisinage de $s = k$; en déduire une expression du résidu de F_n en $s = k$ en termes de R_n.

(iii) Vérifier que $\left|\frac{\pi}{\sin \pi s}\right| \leqslant \pi$, si $\mathrm{Re}(s) = \frac{1}{2} + a$, avec $a \in \mathbf{Z}$, ou si $s \in \Omega$ et $|\mathrm{Im}(s)| \geqslant 1$.

(iv) En déduire que $|\mathrm{F}_n(s)| \leqslant \frac{\pi^2}{|s|^2}$ si $\frac{1}{2} \leqslant \mathrm{Re}(s) \leqslant n + \frac{1}{2}$, ou si $s \in \Omega$ et $\mathrm{Re}(s) = \frac{1}{2} + a$, avec $a \in \mathbf{Z}$, ou $|\mathrm{Im}(s)| \geqslant 1$.

(v) Soit $\mathrm{C} \in [\frac{1}{2}, n+\frac{1}{2}]$. Si N est un entier $\geqslant n$, on note $\mathrm{I}_1(\mathrm{N})$, $\mathrm{I}_2(\mathrm{N})$, $\mathrm{I}_3(\mathrm{N})$ et $\mathrm{I}_4(\mathrm{N})$ les intégrales de $\frac{1}{2i\pi}\mathrm{F}_n(s)ds$ le long des segments $[\mathrm{C}+i\mathrm{N}, \mathrm{C}-i\mathrm{N}]$, $[\mathrm{C}-i\mathrm{N}, \mathrm{N}+\frac{1}{2}-i\mathrm{N}]$, $[\mathrm{N}+\frac{1}{2}-i\mathrm{N}, \mathrm{N}+\frac{1}{2}+i\mathrm{N}]$ et $[\mathrm{N}+\frac{1}{2}+i\mathrm{N}, \mathrm{C}+i\mathrm{N}]$ respectivement. Calculer $\sum_{j=1}^{4} \mathrm{I}_j(\mathrm{N})$; en déduire que $\mathrm{S}_n = \frac{1}{2i\pi} \int_{\mathrm{C}-i\infty}^{\mathrm{C}+i\infty} \mathrm{F}_n(s)\, ds$.

Question 3. Soit $c = \frac{1}{\sqrt{2}}$. Si $u \geqslant 1$ et $t \in \mathbf{R}$, soit $\mathrm{G}(t,u) = \frac{\Gamma(1+(1-c)u^2-iut)}{\Gamma(1+(1+c)u^2+iut)}\Gamma(cu^2+iut)^2$. Soient de plus $\alpha_1 = 1-c$, $\beta_1 = -it$, $m_1 = 1$, $\alpha_2 = 1+c$, $\beta_2 = it$, $m_2 = -1$, $\alpha_3 = c$, $\beta_3 = it$, $m_3 = 2$, de telle sorte que $\mathrm{G}(t,u) = \frac{\alpha_1u^2+\beta_1u}{\alpha_2u^2+\beta_2u} \prod_{i=1}^{3} \Gamma(\alpha_iu^2+\beta_iu)^{m_i}$. On définit $\log \mathrm{G}(t,u)$ par $\log \mathrm{G}(t,u) = \log \frac{\alpha_1u^2+\beta_1u}{\alpha_2u^2+\beta_2u} + \sum_{i=1}^{3} m_i \log(\Gamma(\alpha_iu^2+\beta_iu))$, et la formule de Stirling nous donne

$$\log \mathrm{G}(t,u) = g(t,u) - 2\log u + \log 2\pi + r(t,u) + \varepsilon(t,u),$$

où g, ε et r sont données par $g(t,u) = \sum_{i=1}^{3} m_i g(\alpha_iu^2+\beta_iu)$, $\varepsilon(t,u) = \sum_{i=1}^{3} m_i\varepsilon(\alpha_iu^2+\beta_iu)$ et $r(t,u) = \frac{1}{2}\sum_{i=1}^{3} m_i' \log(\alpha_i + \frac{\beta_i}{u})$, avec $m_1' = 1$, $m_2' = -1$ et $m_3' = -2$.

(i) Calculer $\frac{\Gamma(n+1-s)}{\Gamma(1-s)}$ et $\frac{\Gamma(n+1+s)}{\Gamma(s)}$; en déduire, en utilisant la formule des compléments, que $\mathrm{F}_n(cn + i\sqrt{n}t) = \mathrm{G}(t, \sqrt{n})^2$, si $n \geqslant 1$.

(ii) En déduire que $\mathrm{S}_n = \frac{\sqrt{n}}{2\pi} \int_{-\infty}^{+\infty} \mathrm{G}(t, \sqrt{n})^2 dt$.

23. La démonstration d'Apéry a suscité de nombreux travaux mais toutes les tentatives pour démontrer que $\zeta(5)$ est irrationnel ont échoué.

(iii) Vérifier que $g(\alpha u^2+\beta u) = 2\alpha u^2\log u+(\alpha\log\alpha-\alpha)u^2+2\beta u\log u+(\beta\log\alpha)u+\frac{\beta^2}{2\alpha}+\mathrm{O}(\frac{1}{u})$ au voisinage de $+\infty$, si $\alpha>0$ et $\beta\in i\mathbf{R}$.

(iv) Vérifier que $\sum_{i=1}^3 m_i\alpha_i = \sum_{i=1}^3 m_i\beta_i = \sum_{i=1}^3 m_i\beta_i\log\alpha_i = 0$; en déduire l'existence de $\mathrm{A}\in\mathbf{R}$ tel que $\lim_{u\to+\infty}\log\mathrm{G}(t,u)-\delta u^2+2\log u = \mathrm{A}-\gamma t^2$, où l'on a posé $\delta=\sum_{i=1}^3 m_i\alpha_i\log\alpha_i$ et $\gamma=\frac{1}{2}\sum_{i=1}^3\frac{m_i}{\alpha_i}$.

(v) Vérifier que $\delta = 2\log(\sqrt{2}-1)$ et $\gamma=2\sqrt{2}$. En déduire, grâce à l'existence d'une majoration de la forme $u^2e^{-\delta u^2}|\mathrm{G}(t,u)|\leqslant \mathrm{C}\,(1+|t|)|\mathrm{G}(t,1)|$, pour tous $u\geqslant 1$ et $t\in\mathbf{R}$ (cf. question 5), que $(\sqrt{2}-1)^{-4n}n^{3/2}\mathrm{S}_n$ tend vers une limite non nulle B, quand $n\to+\infty$.

Question 4. (i) Soit $a>e$. Montrer, en utilisant le théorème des nombres premiers, que $d_n\leqslant a^n$, pour tout n assez grand. (On calculera $v_p(d_n)$, si p est un nombre premier.)

(ii) Vérifier que $(\sqrt{2}-1)^4e^3<1$. En déduire que $\zeta(3)$ est irrationnel. (Considérer $d_n^3\mathrm{S}_n$.)

Question 5. Les quantités α_i,β_i et m_i sont celles introduites à la question 3. Si $\alpha>0$ et $\beta\in i\mathbf{R}$, on définit $\mathrm{H}_{\alpha,\beta}:\mathbf{R}\to\mathbf{R}$, par $\mathrm{H}_{\alpha,\beta}(v)=\mathrm{Re}((2\alpha+\beta v)\log(\alpha+\beta v))$. On note h_t la fonction $u\mapsto\mathrm{Re}(g(t,u))$.

(i) Vérifier que $\mathrm{H}'_{\alpha,\beta}(0)=0$, et que $\mathrm{H}''_{\alpha,\beta}(v)=\frac{-2\alpha\beta^4v^2}{(\alpha^2-\beta^2v^2)^2}$.

(ii) Montrer que $\mathrm{I}(w)=\sum_{i=1}^3 m_i\frac{\alpha_i}{(2\alpha_i^2+w)^2}$ est $\geqslant 0$, pour tout $w\geqslant 0$.

(iii) Si $v\in]0,1]$, soit $\mathrm{H}(v)=vh'_t(\frac{1}{v})$. Vérifier que $\mathrm{H}(v)=\sum_{i=1}^3 m_i\mathrm{H}_{\alpha_i,\beta_i}(v)$; en déduire que $\mathrm{H}''(v)\leqslant 0$.

(iv) Montrer que $h_t(u)-\delta u^2\leqslant h_t(1)-\delta$, pour tout $u\geqslant 1$.

(v) Montrer qu'il existe $\mathrm{C}_2,\mathrm{C}_3$ tels que $\mathrm{Re}(r(t,u))\leqslant\mathrm{C}_2$, pour tous $u\geqslant 1$ et $t\in\mathbf{R}$, et $\mathrm{Re}(r(t,1))\geqslant-\log(1+|t|)-\mathrm{C}_3$, pour tout $t\in\mathbf{R}$.

(vi) En déduire l'existence de C, tel que $|u^2e^{-\delta u^2}\mathrm{G}(t,u)|\leqslant\mathrm{C}\,(1+|t|)|\mathrm{G}(t,1)|$, pour tous $u\geqslant 1$ et $t\in\mathbf{R}$.

Corrigé

Question 1. (i) On a $a_i=\lim_{\mathrm{X}\to-i}\frac{(\mathrm{X}-1)\cdots(\mathrm{X}-n)}{\mathrm{X}\cdots(\mathrm{X}+i-1)(\mathrm{X}+i+1)\cdots(\mathrm{X}+n)}=\frac{(-1)^n(n+i)!}{i!(-1)^ii!(n-i)!}=(-1)^{n-i}\frac{(n+i)!}{n!i!}\frac{n!}{(n-i)!i!}=(-1)^{n-i}\binom{n+i}{i}\binom{n}{i}$, ce qui prouve que $a_i\in\mathbf{Z}$.

(ii) $\sum_{i=0}^n\frac{\alpha_i}{(\mathrm{X}+i)^2}+\frac{\beta_i}{\mathrm{X}+i}=\big(\sum_{i=0}^n\frac{a_i}{\mathrm{X}+i}\big)^2=\sum_{i=0}^n\frac{a_i^2}{(\mathrm{X}+i)^2}+\sum_{i\neq j}\frac{a_ia_j}{(\mathrm{X}+i)(\mathrm{X}+j)}$. Comme $\frac{1}{(\mathrm{X}+i)(\mathrm{X}+j)}=\frac{1}{j-i}\big(\frac{1}{\mathrm{X}+i}-\frac{1}{\mathrm{X}+j}\big)$, on en déduit que $\alpha_i=a_i^2\in\mathbf{Z}$, et que $\beta_i=2\sum_{j\neq i}\frac{a_ia_j}{j-i}$. Comme $|j-i|\leqslant n$, on a $\frac{d_n}{j-i}\in\mathbf{Z}$, et donc $d_n\beta_i\in\mathbf{Z}$.

Enfin $\sum_{i=0}^n\beta_i=0$ car R_n est de degré -2.

(iii) On a $-\mathrm{R}'_n(k)=\sum_{i=0}^n\frac{2\alpha_i}{(k+i)^3}+\frac{\beta_i}{(k+i)^2}$. On en déduit que

$$\mathrm{S}_n=\sum_{i=0}^n\Big(2\alpha_i\big(\sum_{k=1}^{+\infty}\frac{1}{(k+i)^3}\big)+\beta_i\big(\sum_{k=1}^{+\infty}\frac{1}{(k+i)^2}\big)\Big)=\sum_{i=0}^n\Big(2\alpha_i\big(\zeta(3)-\sum_{k=1}^{i}\frac{1}{k^3}\big)+\beta_i\big(\zeta(2)-\sum_{k=1}^{i}\frac{1}{k^2}\big)\Big).$$

$\zeta(2)$ disparaît puisque $\sum_{i=0}^n\beta_i=0$, et on obtient $\mathrm{S}_n=u_n\zeta(3)-\frac{v_n}{d_n^3}$, avec $u_n=2\sum_{i=0}^n\alpha_i\in\mathbf{Z}$ et $v_n=\sum_{i=0}^n\big(2\alpha_i\big(\sum_{k=1}^i\frac{d_n^3}{k^3}\big)+d_n\beta_i\big(\sum_{k=1}^i\frac{d_n^2}{k^2}\big)\big)$, où tous les termes sont entiers puisque $k\leqslant i\leqslant n$ implique $k\mid d_n$.

Question 2. (i) La première partie résulte de ce que les zéros doubles de $\mathrm{R}_n(s)$ en $1,2,\ldots,n$ compensent les pôles doubles de $\big(\frac{\pi}{\sin\pi s}\big)^2$ en ces points. La décroissance rapide sur une droite verticale vient de ce que

R_n est bornée sur une telle droite car de degré $\leqslant 0$, et que $|\frac{1}{\sin(c+i\mathrm{T})}| \leqslant \frac{2}{e^{|\mathrm{T}|}-e^{-|\mathrm{T}|}}$, ce qui fait que $\frac{\pi}{\sin \pi s}$ est à décroissance rapide sur une droite verticale.

(ii) La fonction $s \mapsto \big(\frac{\pi}{\sin \pi s}\big)^2$ est périodique de période 1 ; il suffit donc de vérifier le résultat en 0. Or on a $\frac{\pi}{\sin \pi s} = \frac{1}{s}\,\frac{1}{1-\frac{\pi^2 s^2}{6}+\cdots} = \frac{1}{s} + \frac{\pi^2 s}{6} + \cdots$, et donc $\big(\frac{\pi}{\sin \pi s}\big)^2 = \frac{1}{s^2} + \frac{\pi^2}{3} + \cdots$.

Maintenant, $\mathrm{R}_n(s) = \mathrm{R}_n(k) + (s-k)\mathrm{R}_n'(k) + \cdots$ et donc $\mathrm{F}_n(s) = \frac{\mathrm{R}_n(k)}{(s-k)^2} + \frac{\mathrm{R}_n'(k)}{s-k} + \mathrm{O}(1)$ au voisinage de $s=k$; il s'ensuit que $\mathrm{res}(\mathrm{F}_n, k) = \mathrm{R}_n'(k)$.

(iii) $|\sin \pi s| = \frac{1}{2}|e^{\frac{i\pi}{2}+ia\pi-\pi\mathrm{Im}(s)} - e^{\frac{-i\pi}{2}-ia\pi+\pi\mathrm{Im}(s)}| = \frac{1}{2}|(-1)^a i(e^{-\pi\mathrm{Im}(s)} + e^{\pi\mathrm{Im}(s)})|$, si $\mathrm{Re}(s) = \frac{1}{2}+a$ avec $a \in \mathbf{Z}$, et le dernier terme est $\geqslant 1$ par l'inégalité entre moyenne géométrique et moyenne arithmétique.

Si $|\mathrm{Im}(s)| \geqslant 1$, on a $|\sin \pi s| \geqslant \frac{1}{2}(e^{\pi|\mathrm{Im}(s)|} - e^{-\pi|\mathrm{Im}(s)|}) \geqslant \frac{1}{2}\big(e^{\pi} - e^{-\pi}\big) \geqslant 1$.

(iv) Remarquons que dans tous les cas, on a $s \in \Omega$, ce qui implique $\big|\frac{s-i}{s+i}\big| \leqslant 1$, si $i \in \{1, 2, \ldots, n\}$. Comme $|s^2\mathrm{F}_n(s)| = \big|\frac{\pi}{\sin \pi s}\big|^2 \big|\frac{s-1}{s+1}\cdots\frac{s-n}{s+n}\big|^2$, on déduit la majoration voulue, si $\mathrm{Re}(s) = \frac{1}{2}+a$, avec $a \in \mathbf{Z}$, ou si $|\mathrm{Im}(s)| \geqslant 1$, du (iii). La majoration dans la bande $\frac{1}{2} \leqslant \mathrm{Re}(s) \leqslant \frac{1}{2}+n$ s'obtient alors en appliquant le principe du maximum à $s^2\mathrm{F}_n(s)$ dans le rectangle de sommets $\frac{1}{2}-i\mathrm{T}$, $n+\frac{1}{2}-i\mathrm{T}$, $n+\frac{1}{2}+i\mathrm{T}$ et $\frac{1}{2}+i\mathrm{T}$, et en faisant tendre T vers $+\infty$.

(v) La formule des résidus montre que $\sum_{j=1}^4 \mathrm{I}_j(\mathrm{N}) = \sum_{k=n+1}^{\mathrm{N}} \mathrm{R}_n'(k)$ $(= \sum_{k=1}^{\mathrm{N}} \mathrm{R}_n'(k)$ car $\mathrm{R}_n'(k) = 0$ si $k \in \{1, 2, \ldots, n\})$. Il s'ensuit que $\sum_{j=1}^4 \mathrm{I}_j(\mathrm{N}) \to -\mathrm{S}_n$ quand $\mathrm{N} \to +\infty$. Par ailleurs, quand $\mathrm{N} \to +\infty$,

- $\mathrm{I}_1(\mathrm{N})$ tend vers $-\frac{1}{2i\pi}\int_{\mathrm{C}-i\infty}^{\mathrm{C}+i\infty} \mathrm{F}_n(s)\,ds$,
- $|\mathrm{I}_2(\mathrm{N})| \leqslant \frac{1}{2\pi}|\mathrm{N}+\frac{1}{2}-\mathrm{C}|\sup_{s\in[\mathrm{C}-i\mathrm{N},\mathrm{N}+\frac{1}{2}-i\mathrm{N}]}|\mathrm{F}_n(s)| \leqslant \frac{1}{2\pi}|\mathrm{N}+\frac{1}{2}-\mathrm{C}|\frac{\pi^2}{\mathrm{N}^2}$, et donc $\mathrm{I}_2(\mathrm{N}) \to 0$,
- Pour la même raison, $\mathrm{I}_4(\mathrm{N}) \to 0$,
- $|\mathrm{I}_3(\mathrm{N})| \leqslant \frac{1}{2\pi}2\mathrm{N}\sup_{s\in[\mathrm{N}+\frac{1}{2}-i\mathrm{N},\mathrm{N}+\frac{1}{2}+i\mathrm{N}]}|\mathrm{F}_n(s)| \leqslant \frac{\mathrm{N}}{\pi}\frac{\pi^2}{(\mathrm{N}+\frac{1}{2})^2}$, et donc $\mathrm{I}_3(\mathrm{N}) \to 0$.

Un passage à la limite nous donne donc $-\mathrm{S}_n = -\frac{1}{2i\pi}\int_{\mathrm{C}-i\infty}^{\mathrm{C}+i\infty} \mathrm{F}_n(s)\,ds$, ce qui permet de conclure.

Question 3. (i) On a $\frac{\Gamma(n+1-s)}{\Gamma(1-s)} = (-1)^n(s-1)\cdots(s-n)$ et $\frac{\Gamma(n+1+s)}{\Gamma(s)} = s(s+1)\cdots(s+n)$, et comme $\frac{\pi}{\sin \pi s} = \Gamma(s)\Gamma(1-s)$, on obtient $\mathrm{F}_n(s) = \big(\frac{\Gamma(n+1-s)}{\Gamma(1-s)}\big)^2\big(\frac{\Gamma(s)}{\Gamma(n+1+s)}\big)^2(\Gamma(s)\Gamma(1-s))^2 = \big(\frac{\Gamma(n+1-s)}{\Gamma(n+1+s)}\Gamma(s)^2\big)^2$. Le résultat s'en déduit en remplaçant s par $cn + i\sqrt{n}t$.

(ii) On peut appliquer le **2**.(v) à $\mathrm{C} = cn \in [\frac{1}{2}, n+\frac{1}{2}]$, et paramétrer la droite $]\mathrm{C}-i\infty, \mathrm{C}+i\infty[$ par $s = cn + i\sqrt{n}t$, pour $t \in \mathbf{R}$; on en déduit le résultat (en utilisant le (i) pour exprimer $\mathrm{F}_n(cn+i\sqrt{n}t)$).

(iii) Comme $g(\alpha u^2+\beta u) = (\alpha u^2+\beta u)(-1+\log(\alpha u^2)+\log(1+\frac{\beta}{\alpha u}))$, le résultat s'obtient en développant $(\alpha u^2+\beta u)\big(-1+2\log u+\log\alpha+\frac{\beta}{\alpha u}-\frac{\beta^2}{2\alpha^2u^2}+\mathrm{O}(\frac{1}{u^3})\big)$.

(iv) Les identités $\sum_{i=1}^3 m_i\alpha_i = \sum_{i=1}^3 m_i\beta_i = 0$ sont immédiates. Maintenant, on a $\sum_{i=1}^3 m_i\beta_i\log\alpha_i = it\big(-\log(1-\frac{1}{\sqrt{2}})-\log(1+\frac{1}{\sqrt{2}})+2\log\frac{1}{\sqrt{2}}\big)$, et comme $\big(1-\frac{1}{\sqrt{2}}\big)\big(1+\frac{1}{\sqrt{2}}\big) = \frac{1}{2} = \big(\frac{1}{\sqrt{2}}\big)^2$, la parenthèse est nulle et donc $\sum_{i=1}^3 m_i\beta_i\log\alpha_i = 0$. Il s'ensuit que $g(t,u)-\delta u^2 \to \sum_{i=1}^3 m_i\frac{\beta_i^2}{2\alpha_i} = -\gamma t^2$. On en déduit le résultat avec $\mathrm{A} = \log 2\pi + \frac{1}{2}\sum_{i=1}^3 m_i'\log\alpha_i$ puisque $\varepsilon(\alpha_i u^2+\beta_i u) \to 0$, si $i \in \{1,2,3\}$.

(v) On a $\delta = (1-c)\log(1-c)-(1+c)\log(1+c)+2c\log c = \log(1-c)-\log(1+c)$ d'après le calcul fait au (iv), et comme $\frac{1-c}{1+c} = \frac{\sqrt{2}-1}{\sqrt{2}+1} = (\sqrt{2}-1)^2$, on obtient la première formule. Pour la seconde, on constate que $\frac{1}{1-c}-\frac{1}{1+c}+\frac{2}{c} = \frac{2c}{1-c^2}+2\sqrt{2} = 4\sqrt{2}$, ce qui nous donne $\gamma = 2\sqrt{2}$.

Maintenant, $u^4e^{-2\delta u^2}\mathrm{G}(t,u)^2 \to e^{2\mathrm{A}}e^{-2\gamma t^2}$, quand $t \to +\infty$. Comme

$$|u^4e^{-2\delta u^2}\mathrm{G}(t,u)^2| \leqslant \mathrm{C}^2(1+|t|)^2|\mathrm{G}(t,1)|^2 = \mathrm{C}^2(1+|t|)^2|\mathrm{F}_1(c+it)|,$$

qui est sommable puisque F_1 est à décroissance rapide sur la droite verticale $c+i\mathbf{R}$ (cf. **2**.(i)), on obtient que $u^4(\sqrt{2}-1)^{-4u^2}\int_{-\infty}^{+\infty}\mathrm{G}(t,u)^2\,dt \to e^{2\mathrm{A}}\int_{-\infty}^{+\infty}e^{-4\sqrt{2}t^2}dt$ (cette dernière intégrale vaut $\mathrm{B}' = e^{2\mathrm{A}}\sqrt{\frac{\pi}{4\sqrt{2}}}$) en échangeant limite et intégrale (ce qui est licite d'après le th. de convergence dominée). Le résultat s'en déduit, avec $\mathrm{B} = \mathrm{B}'/2\pi e^{2\mathrm{A}}$, en posant $u = \sqrt{n}$, et en utilisant le (ii).

Question 4. (i) Si $p^v \mid d_n$, c'est qu'il existe $i \in \{1, \dots n\}$ tel que $p^v \mid i$; en particulier, $p^v \leqslant n$. On en déduit que $v_p(d_n) = \big[\frac{\log n}{\log p}\big]$. On a donc $\log d_n = \sum_{p \leqslant n} \big[\frac{\log n}{\log p}\big] \log p \leqslant (\log n)|\{p,\ p \leqslant n\}|$, et il résulte du th. des nombres premiers que $\log d_n \leqslant n \log a$ pour tout n assez grand.

(ii) On a $(\sqrt{2}-1)^4 e^3 = \frac{e^3}{(\sqrt{2}+1)^4} = \frac{e^3}{(3+2\sqrt{2})^2} = \frac{e^3}{17+12\sqrt{2}} \leqslant \frac{3^3}{17+12} < 1$. Si $\zeta(3)$ est rationnel, on peut l'écrire sous la forme $\frac{a}{\mathrm{N}}$, et alors $d_n^3 \mathrm{S}_n = d_n^3 u_n \zeta(3) - v_n$ est un entier, si $n \geqslant \mathrm{N}$, puisque d_n^3 est divisible par N. De plus, $d_n^3 \mathrm{S}_n$ est non nul pour n assez grand puisque $\mathrm{S}_n \sim \mathrm{B} n^{-3/2} (\sqrt{2}-1)^{4n}$, et $\mathrm{B} \neq 0$. Or on peut choisir $a > e$ tel que $b = a^3(\sqrt{2}-1)^4 < 1$, et on a $|d_n^3 \mathrm{S}_n| \leqslant \mathrm{B} n^{-3/2} b^n$, pour tout n assez grand d'après le (i), et donc $d_n^3 \mathrm{S}_n \to 0$. Comme une suite d'entiers non nuls ne peut pas tendre vers 0, on aboutit à une contradiction qui permet de conclure.

Question 5. (i) $\mathrm{H}'_{\alpha,\beta}(v) = \mathrm{Re}\big(\beta \log(\alpha+\beta v) + \frac{\alpha\beta}{\alpha+\beta v} + \beta\big)$, et donc $\mathrm{H}'_{\alpha,\beta}(0) = 0$ car $\beta \in i\mathbf{R}$ et $\alpha > 0$. Enfin,

$$\mathrm{H}''_{\alpha,\beta}(v) = \mathrm{Re}\Big(\frac{\beta^2}{\alpha+\beta v} - \frac{\alpha\beta^2}{(\alpha+\beta v)^2}\Big) = \beta^2\Big(\frac{\alpha}{\alpha^2-\beta^2 v^2} - \frac{\alpha(\alpha^2+\beta^2 v^2)}{(\alpha^2-\beta^2 v^2)^2}\Big) = \frac{-2\alpha\beta^4 v^2}{(\alpha^2-\beta^2 v^2)^2}$$

(ii) On a $\mathrm{I}(w) = \frac{1}{\sqrt{2}}\big(\frac{\sqrt{2}-1}{(3-2\sqrt{2}+w)^2} - \frac{\sqrt{2}+1}{(3+2\sqrt{2}+w)^2} + \frac{2}{(1+w)^2}\big)$. Après réduction au même dénominateur, on voit que $\mathrm{I}(w)$ a même signe que

$$(1+w)^2\big((\sqrt{2}-1)(3+2\sqrt{2}+w)^2 + (-\sqrt{2}-1)(3-2\sqrt{2}+w)^2\big) + 2(3+2\sqrt{2}+w)^2(3-2\sqrt{2}+w)^2$$
$$= 2\big((1+w)^2(-w^2+2w+7) + (1+6w+w^2)^2\big) = 2(12w^3+32w^2+44w+8),$$

qui est $\geqslant 0$, pour tout $w \geqslant 0$.

(iii) On a $g(t,u) = \sum_{i=1}^3 m_i g(\alpha_i u^2 + \beta_i u)$; comme la dérivée de g est log, la dérivée de $g(t,u)$ par rapport à u est $\sum_{i=1}^3 m_i(2\alpha_i u + \beta_i)\log(\alpha_i u^2 + \beta_i u)$, et donc

$$\mathrm{H}(v) = \mathrm{Re}\Big(\sum_{i=1}^3 m_i(2\alpha_i + \beta_i v)\big(\log(\alpha_i + \beta_i v) - 2\log v\big)\Big).$$

Le terme en $\log v$ disparaît car $\sum_{i=1}^3 m_i\alpha_i = \sum_{i=1}^3 m_i\beta_i = 0$, et il reste $\mathrm{H}(v) = \sum_{i=1}^3 m_i \mathrm{H}_{\alpha_i,\beta_i}(v)$.

Comme $\beta_i^2 = -t^2$, si $i = 1,2,3$, on obtient $\mathrm{H}''(v) = -8t^4 v^2 \mathrm{I}(2t^2v^2)$, et donc $\mathrm{H}''(v) \leqslant 0$ d'après le (ii).

(iv) On a $\mathrm{H}'(0) = 0$ d'après le (i), et $\mathrm{H}''(v) \leqslant 0$ d'après le (iii) ; il s'ensuit que $\mathrm{H}'(v) \leqslant 0$, si $v \in]0,1]$. Comme $\mathrm{H}(0) = 2\sum_{i=1}^3 m_i\alpha_i \log\alpha_i = 2\delta$, on a $\mathrm{H}(v) \leqslant 2\delta$, si $v \in]0,1]$, et donc $h_t'(u) - 2\delta u \leqslant 0$, pour tout $u \geqslant 1$. La fonction $u \mapsto h_t(u) - \delta u^2$ est donc décroissante, ce qui permet de conclure.

(v) On a $\mathrm{Re}(r(t,u)) = \frac{1}{2}\log\big|\frac{1-c-i\frac{t}{u}}{1+c+i\frac{t}{u}}\big| - \log\big|c + i\frac{t}{u}\big|$; en particulier, cela ne dépend que de $x = \frac{t^2}{u^2}$ car c'est déjà le cas pour $|\alpha + i\frac{t}{u}|$ si $\alpha \in \{1-c, 1+c, c\}$, et comme cela tend vers $-\infty$ quand $x \to +\infty$ et est continu sur $\mathbf{R}_+$, on en déduit l'existence de C_2.

L'existence de C_3 résulte de ce que $t \mapsto \log\big|\frac{1-c-it}{1+c+it}\big|$ est bornée car $t \mapsto \frac{1-c-it}{1+c+it}$ l'est et ne s'approche pas de zéro, et de ce que $t \mapsto -\log|c+it| + \log(1+|t|)$ aussi puisque $t \mapsto \frac{c+it}{1+|t|}$ l'est.

(vi) On a $\log\big|\frac{u^2 e^{-\delta u^2}\mathrm{G}(t,u)}{\mathrm{G}(t,1)}\big| = -\delta u^2 + h_t(u) - h_t(1) + \mathrm{Re}(r(t,u) - r(t,1)) + \mathrm{Re}(\varepsilon(t,u) - \varepsilon(t,1))$. Or,

- $h_t(u) - \delta u^2 - h_t(1) \leqslant -\delta$ d'après le (iv),
- $\mathrm{Re}(r(t,u) - r(t,1)) \leqslant \mathrm{C}_2 + \mathrm{C}_3 + \log(1+|t|)$, d'après le (v),
- $\varepsilon(t,u) = \sum_{i=1}^3 m_i \varepsilon(\alpha_i + \beta_i u)$, et comme $|\alpha_i + \beta_i u| \geqslant 1 - c$, si $u \geqslant 1$, $t \in \mathbf{R}$ et $i = 1,2,3$, on a $\mathrm{Re}(\varepsilon(t,u) - \varepsilon(t,1)) \leqslant 2\big(\sum_{i=1}^3 |m_i|\big)\frac{\mathrm{C}_1}{1-c}$, d'après la formule de Stirling rappelée en préambule.

On en déduit le résultat avec $\mathrm{C} = \exp\big(-\delta + \mathrm{C}_2 + \mathrm{C}_3 + \frac{8\mathrm{C}_1}{1-c}\big)$.

H.13. Le critère de Borel

Soit f une fonction méromorphe sur $\mathrm{D}(0,r^-)$, avec $r>1$, holomorphe en 0. Soit $\sum_{n=0}^{+\infty} a_n z^n$ le développement de Taylor de f en 0. On se propose de prouver que si les a_n sont des entiers, alors f est une fraction rationnelle (résultat dû à Borel, 1894). La démonstration comporte deux parties : la partie I donne un critère purement algébrique pour qu'une série formelle soit une fraction rationnelle ; l'autre, qui utilise les propriétés des fonctions holomorphes, montre que l'on est sous les conditions d'utilisation du critère de la partie I dans le cas qui nous intéresse.

Partie I

Soient K un corps et $(a_n)_{n\in\mathbf{N}}$ une suite d'éléments de K. On note $\mathrm{F}\in\mathrm{K}[[\mathrm{T}]]$ la série formelle $\sum_{n\in\mathbf{N}} a_n\mathrm{T}^n$, et on se propose d'établir un critère permettant de décider si F est une fraction rationnelle (ou plus exactement son développement de Taylor à l'origine).

Si $\mathrm{N}\geqslant 1$ et $n\in\mathbf{N}$, soit $\mathrm{A_N}(n)=(a_n,a_{n+1},\dots,a_{n+\mathrm{N}-1})\in\mathrm{K}^{\mathrm{N}}$, et soit $\Delta_{\mathrm{N}}(n)$ le déterminant *de Hankel* $\det\big(\mathrm{A_N}(n),\dots,\mathrm{A_N}(n+\mathrm{N}-1)\big)$ (donc $\Delta_{\mathrm{N}}(n)=\det(a_{n+i+j})_{0\leqslant i,j\leqslant \mathrm{N}-1}$).

(i) Soient $c_1,\dots,c_{\mathrm{N}}\in\mathrm{K}$ et $\mathrm{P}=1+c_1\mathrm{T}+\cdots+c_{\mathrm{N}}\mathrm{T}^{\mathrm{N}}$. Montrer qu'il y a équivalence entre :

- il existe $\mathrm{Q}\in\mathrm{K}[\mathrm{T}]$ tel que $\mathrm{F}=\frac{\mathrm{Q}}{\mathrm{P}}$;
- il existe $n_0\in\mathbf{N}$ tel que $a_{n+\mathrm{N}}+c_1a_{n+\mathrm{N}-1}+\cdots+c_{\mathrm{N}}a_n=0$, pour tout $n\geqslant n_0$.

En déduire que si F est une fraction rationnelle, alors il existe $\mathrm{M}\geqslant 1$ et $m_0\in\mathbf{N}$ tels que $\Delta_{\mathrm{M}}(n)=0$, pour tout $n\geqslant m_0$.

(ii) On suppose que $\Delta_{\mathrm{N}+1}(n)=0$ et $\Delta_{\mathrm{N}}(n+1)\neq 0$. Montrer que $\Delta_{\mathrm{N}}(n)\neq 0$. (On pourra prouver que $\mathrm{A_N}(n+\mathrm{N})$ appartient au sous-espace de K^{N} engendré par $\mathrm{A_N}(n),\dots,\mathrm{A_N}(n+\mathrm{N}-1)$, en considérant la matrice $\mathrm{B}=(a_{n+i+j})_{0\leqslant i,j\leqslant \mathrm{N}}$ dont les $\mathrm{A_N}(n+i)$ sont des lignes et des colonnes de sous-matrices.)

(iii) On suppose qu'il existe $\mathrm{M}\geqslant 1$ et $m_0\in\mathbf{N}$ tels que $\Delta_{\mathrm{M}}(n)=0$, pour tout $n\geqslant m_0$. Montrer qu'il existe $\mathrm{N},n_0\in\mathbf{N}$, tels que $\Delta_{\mathrm{N}+1}(n)=0$ et $\Delta_{\mathrm{N}}(n)\neq 0$, pour tout $n\geqslant n_0$.

(iv) Montrer que $\mathrm{A_N}(n_0+\mathrm{N})+c_1\mathrm{A_N}(n_0+\mathrm{N}-1)+\cdots+c_{\mathrm{N}}\mathrm{A_N}(n_0)=0$ pour $c_1,\dots,c_{\mathrm{N}}\in\mathrm{K}$ uniquement déterminés, et que l'on a $\mathrm{A_N}(n+\mathrm{N})+c_1\mathrm{A_N}(n+\mathrm{N}-1)+\cdots+c_{\mathrm{N}}\mathrm{A_N}(n)=0$, pour tout $n\geqslant n_0$. Comment ceci se traduit-il pour la suite $(a_n)_{n\in\mathbf{N}}$?

(v) Montrer que F est une fraction rationnelle s'il existe $\mathrm{M}\geqslant 1$ et $m_0\in\mathbf{N}$ tels que $\Delta_{\mathrm{M}}(n)=0$, pour tout $n\geqslant m_0$.

Partie II

Soit f une fonction méromorphe sur $\mathrm{D}(0,r^-)$, avec $r>1$, holomorphe en 0. Soit $\sum_{n=0}^{+\infty} a_n z^n$ le développement de Taylor de f en 0.

(i) Soit $\mathrm{R}\in]1,r[$. Montrer que f n'a qu'un nombre fini de pôles $\alpha_1,\dots,\alpha_d$ (répétés avec multiplicité) dans $\mathrm{D}(0,\mathrm{R})$.

(ii) Montrer qu'il existe $\mathrm{R}_0>0$ et $\mathrm{C}_0>0$ tels que $|a_n|\leqslant \mathrm{C}_0\mathrm{R}_0^{-n}$, pour tout $n\in\mathbf{N}$.

(iii) Soient $c_1,\dots,c_d\in\mathbf{C}$ définis par $1+c_1\mathrm{X}+\cdots+c_d\mathrm{X}^d=\prod_{j=1}^d(1-\alpha_j^{-1}\mathrm{X})$. Montrer qu'il existe $\mathrm{C}>0$ et $\mathrm{R}>1$ tels que $|a_{n+d}+c_1a_{n+d-1}+\cdots+c_da_n|\leqslant \mathrm{CR}^{-n}$, pour tout $n\in\mathbf{N}$. [On pourra s'intéresser à la fonction $f(z)\prod_{j=1}^d(1-\alpha_j^{-1}z)$.]

(iv) En déduire qu'il existe $\mathrm{N}\geqslant 1$ et $n_0\in\mathbf{N}$ tels que $|\Delta_{\mathrm{N}}(\mathbf{a},n)|<1$, pour tout $n\geqslant n_0$. (On pourra majorer les coordonnées de $\mathrm{B_N}(n+i)=\mathrm{A_N}(n+i+d)+c_1\mathrm{A_N}(n+i+d-1)+\cdots+c_d\mathrm{A_N}(n+i)$.)

(v) Montrer que f est une fonction rationnelle si les a_n sont des entiers.

Corrigé

Partie I

(i) On a $(1+c_1\mathrm{T}+\cdots+c_\mathrm{N}\mathrm{T}^\mathrm{N})\mathrm{F}(\mathrm{T}) = \sum_{n\in\mathbf{N}} b_n\mathrm{T}^n$, avec $b_{n+\mathrm{N}} = a_{n+\mathrm{N}}+c_1a_{n+\mathrm{N}-1}+\cdots+c_\mathrm{N}a_n$; on voit donc que $(1+c_1\mathrm{T}+\cdots+c_\mathrm{N}\mathrm{T}^\mathrm{N})\mathrm{F}(\mathrm{T})$ est un polynôme si et seulement si $a_{n+\mathrm{N}}+c_1a_{n+\mathrm{N}-1}+\cdots+c_\mathrm{N}a_n = 0$ pour tout n assez grand, d'où l'équivalence des deux conditions de la question.

Maintenant, si F est une fraction rationnelle, on peut l'écrire sous la forme $\mathrm{F} = \frac{\mathrm{Q}}{\mathrm{P}}$, avec P et Q premiers entre eux. Comme F n'a pas de pôle en 0, on a $\mathrm{P}(0) \neq 0$ et, quitte à diviser P et Q par $\mathrm{P}(0)$, on peut supposer que $\mathrm{P}(0) = 1$, et donc que $\mathrm{P} = 1 + c_1\mathrm{T} + \cdots + c_\mathrm{N}\mathrm{T}^\mathrm{N}$. D'après ce qui précède, il existe donc $n_0 \in \mathbf{N}$ tel que $a_{n+\mathrm{N}} + c_1a_{n+\mathrm{N}-1} + \cdots + c_\mathrm{N}a_n = 0$ pour tout $n \geqslant n_0$. Mais alors $\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N}) + c_1\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N}-1) + \cdots + c_\mathrm{N}\mathrm{A}_{\mathrm{N}+1}(n) = 0$, pour tout $n \geqslant n_0$, et donc $\Delta_{\mathrm{N}+1}(n) = 0$ pour tout $n \geqslant n_0$ puisque $\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N})$ est une combinaison linéaire de $\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N}-1), \ldots, \mathrm{A}_{\mathrm{N}+1}(n)$. Ceci permet de conclure avec $\mathrm{M} = \mathrm{N}+1$ et $m_0 = n_0$.

(ii) L'hypothèse $\Delta_\mathrm{N}(n+1) \neq 0$ équivaut à ce que $\mathrm{A}_\mathrm{N}(n+1), \ldots, \mathrm{A}_\mathrm{N}(n+\mathrm{N})$ est une base de K^N ; elle implique que $\mathrm{A}_{\mathrm{N}+1}(n), \ldots, \mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N}-1)$, qui sont les N premières lignes de la matrice B, sont linéairement indépendants. Comme $\mathrm{A}_{\mathrm{N}+1}(n), \ldots, \mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N})$ forment une famille liée puisque $\Delta_{\mathrm{N}+1}(n) = 0$, on peut écrire la dernière ligne $\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N})$ de B sous la forme $\lambda_\mathrm{N}\mathrm{A}_{\mathrm{N}+1}(n)+\cdots+\lambda_1\mathrm{A}_{\mathrm{N}+1}(n+\mathrm{N}-1)$. En ignorant la dernière colonne, cela nous fournit la relation $\mathrm{A}_\mathrm{N}(n+\mathrm{N}) = \lambda_\mathrm{N}\mathrm{A}_\mathrm{N}(n)+\cdots+\lambda_1\mathrm{A}_\mathrm{N}(n+\mathrm{N}-1)$, qui prouve que $\mathrm{A}_\mathrm{N}(n+\mathrm{N})$ est dans le sous-espace de K^N engendré par $\mathrm{A}_\mathrm{N}(n), \ldots, \mathrm{A}_\mathrm{N}(n+\mathrm{N}-1)$; cet espace est donc K^N puisqu'il contient la base $\mathrm{A}_\mathrm{N}(n+1), \ldots, \mathrm{A}_\mathrm{N}(n+\mathrm{N})$. Autrement dit, $\mathrm{A}_\mathrm{N}(n), \ldots, \mathrm{A}_\mathrm{N}(n+\mathrm{N}-1)$ est une famille génératrice de K^N, et donc une base puisqu'elle a N éléments ; son déterminant $\Delta_\mathrm{N}(n)$ est donc non nul, ce que l'on cherchait à prouver.

(iii) Soit N le plus grand entier tel qu'il existe $n_0 \in \mathbf{N}$ pour lequel $\Delta_{\mathrm{N}+1}(n) = 0$ pour tout $n \geqslant n_0$. Alors il existe une infinité de n tels que $\Delta_\mathrm{N}(n) \neq 0$, et une récurrence immédiate utilisant le (ii) montre que l'on a $\Delta_\mathrm{N}(n') \neq 0$ si $n_0 \leqslant n' \leqslant n$ et $\Delta_\mathrm{N}(n) \neq 0$. Comme n peut être pris arbitrairement grand, on a $\Delta_\mathrm{N}(n) \neq 0$, pour tout $n \geqslant n_0$, ce qui permet de conclure.

(iv) $\mathrm{A}_\mathrm{N}(n_0), \ldots, \mathrm{A}_\mathrm{N}(n_0+\mathrm{N}-1)$ forment une base de K^N puisque $\Delta_\mathrm{N}(n_0) \neq 0$. On en déduit l'existence et l'unicité de $c_1, \ldots, c_\mathrm{N}$. Maintenant, $\mathrm{A}_{\mathrm{N}+1}(n_0), \ldots, \mathrm{A}_{\mathrm{N}+1}(n_0+\mathrm{N})$ forment une famille liée puisque $\Delta_{\mathrm{N}+1}(n_0) = 0$, et comme $\mathrm{A}_{\mathrm{N}+1}(n_0), \ldots, \mathrm{A}_{\mathrm{N}+1}(n_0+\mathrm{N}-1)$ forment une famille libre, il existe $\lambda_1, \ldots, \lambda_\mathrm{N}$ tels que $\mathrm{A}_{\mathrm{N}+1}(n_0+\mathrm{N})+\lambda_1\mathrm{A}_{\mathrm{N}+1}(n_0+\mathrm{N}-1)+\cdots+\lambda_\mathrm{N}\mathrm{A}_{\mathrm{N}+1}(n_0) = 0$. En ignorant la dernière coordonnée de chaque $\mathrm{A}_{\mathrm{N}+1}(n_0+i)$, on obtient $\mathrm{A}_\mathrm{N}(n_0+\mathrm{N}) + \lambda_1\mathrm{A}_\mathrm{N}(n_0+\mathrm{N}-1) + \cdots + \lambda_\mathrm{N}\mathrm{A}_\mathrm{N}(n_0) = 0$, et donc $\lambda_1 = c_1, \ldots, \lambda_\mathrm{N} = c_\mathrm{N}$. Maintenant, on obtient $\mathrm{A}_\mathrm{N}(n_0+1+\mathrm{N})+c_1\mathrm{A}_\mathrm{N}(n_0+1+\mathrm{N}-1)+\cdots+c_\mathrm{N}\mathrm{A}_\mathrm{N}(n_0+1) = 0$, en ignorant la première coordonnée. On peut recommencer le même raisonnement avec n_0+1 au lieu de n_0 et une récurrence immédiate montre que $\mathrm{A}_\mathrm{N}(n+\mathrm{N}) + c_1\mathrm{A}_\mathrm{N}(n+\mathrm{N}-1) + \cdots + c_\mathrm{N}\mathrm{A}_\mathrm{N}(n) = 0$ pour tout $n \geqslant n_0$.

Ceci se traduit par la relation de récurrence $a_{n+\mathrm{N}} + c_1a_{n+\mathrm{N}-1} + \cdots + c_\mathrm{N}a_n = 0$, pour tout $n \geqslant n_0$.

(v) D'après la question précédente, il existe $\mathrm{N}, n_0 \in \mathbf{N}$ tels que $a_{n+\mathrm{N}} + c_1a_{n+\mathrm{N}-1} + \cdots + c_\mathrm{N}a_n = 0$, pour tout $n \geqslant n_0$. Soit $\mathrm{Q}(\mathrm{T}) = (1 + c_1\mathrm{T} + \cdots + c_\mathrm{N}\mathrm{T}^\mathrm{N})\mathrm{F}(\mathrm{T}) = \sum_{n\in\mathbf{N}} b_n\mathrm{T}^n$. Alors $b_n = 0$, si $n \geqslant n_0+\mathrm{N}$, puisque $b_{n+\mathrm{N}} = a_{n+\mathrm{N}} + c_1a_{n+\mathrm{N}-1} + \cdots + c_\mathrm{N}a_n$; ceci prouve que Q est un polynôme (de degré $< n_0+\mathrm{N}$), et donc que $\mathrm{F} = \frac{\mathrm{Q}(\mathrm{T})}{1+c_1\mathrm{T}+\cdots+c_\mathrm{N}\mathrm{T}^\mathrm{N}}$ est une fraction rationnelle.

Partie II

(i) Si $\alpha \in \mathrm{D}(0,\mathrm{R})$, il existe $r_\alpha > 0$ tel que f ait au plus un pôle sur $\mathrm{D}(\alpha, r_\alpha^-)$: en effet, si α n'est pas un pôle, la continuité de f implique qu'il existe $r_\alpha > 0$ tel que f n'ait pas de pôle sur $\mathrm{D}(\alpha, r_\alpha^-)$; si α est un pôle d'ordre k alors $(z-\alpha)^k f$ est holomorphe en α et il existe $r_\alpha > 0$ tel que $(z-\alpha)^k f$ n'ait pas de pôle sur $\mathrm{D}(\alpha, r_\alpha^-)$, et alors α est le seul pôle de f sur $\mathrm{D}(\alpha, r_\alpha^-)$. Les $\mathrm{D}(\alpha, r_\alpha^-)$ forment un recouvrement ouvert

de $\mathrm{D}(0,\mathrm{R})$ et, $\mathrm{D}(0,\mathrm{R})$ étant compact, on peut en extraire un sous-recouvrement par des $\mathrm{D}(\alpha, r_\alpha^-)$, avec $\alpha \in \mathrm{A}$ fini. Le nombre de pôles de f sur $\mathrm{D}(0,\mathrm{R})$ est alors $\leqslant |\mathrm{A}|$ et comme chacun est d'ordre fini, cela permet de conclure.

(ii) Comme f est holomorphe en 0, elle est holomorphe sur un disque $\mathrm{D}(0,\mathrm{R}_1^-)$, avec $\mathrm{R}_1 > 0$. Si $0 < \mathrm{R}_0 < \mathrm{R}_1$, on déduit des inégalités de Cauchy (rem. V.4.9 (iii)) que $|a_n| \leqslant \mathrm{C}_0 \mathrm{R}_0^{-n}$, avec $\mathrm{C}_0 = \sup_{|z|=\mathrm{R}_0} |f(z)|$.

(iii) Soit $g(z) = f(z)\prod_{j=1}^{d}(1-\alpha_j^{-1}z)$ et soit $\sum_{n\in\mathbf{N}} b_n z^n$ sa série de Taylor en 0 ; on a donc $b_{n+d} = a_{n+d} + c_1 a_{n+d-1} + \cdots + c_d a_n$. Par construction g est méromorphe sur $\mathrm{D}(0,r^-)$ et holomorphe sur $\mathrm{D}(0,\mathrm{R})$ puisqu'on s'est débrouillé pour supprimer les pôles éventuels dans $\mathrm{D}(0,\mathrm{R})$; elle est donc holomorphe dans un ouvert Ω contenant strictement $\mathrm{D}(0,\mathrm{R})$. On déduit donc des inégalités de Cauchy qu'il existe $\mathrm{C}' > 0$ tel que $|b_n| \leqslant \mathrm{C}'\mathrm{R}^{-n}$, pour tout $n \in \mathbf{N}$. Ceci permet de conclure avec $\mathrm{C} = \mathrm{C}'\mathrm{R}^{-d}$.

(iv) $\Delta_\mathrm{N}(n)$ est le déterminant de $\mathrm{A}_\mathrm{N}(n), \ldots, \mathrm{A}_\mathrm{N}(n+\mathrm{N}-1)$; il ne change pas si on ajoute à $\mathrm{A}_\mathrm{N}(n+i)$ une combinaison linéaire des $\mathrm{A}_\mathrm{N}(n+j)$, avec $j < i$. Il s'ensuit que $\Delta_\mathrm{N}(n)$ est aussi le déterminant de $\mathrm{A}_\mathrm{N}(n), \ldots, \mathrm{A}_\mathrm{N}(n+d-1), \mathrm{B}_\mathrm{N}(n), \ldots, \mathrm{B}_\mathrm{N}(n+\mathrm{N}-1-d)$. C'est donc la somme de N! termes dont chacun est le produit de d termes qui sont des coordonnées des $\mathrm{A}_\mathrm{N}(n+j)$ et de $\mathrm{N}-d$ termes qui sont des coordonnées des $\mathrm{B}_\mathrm{N}(n+i)$.

Or les coordonnées de $\mathrm{B}_\mathrm{N}(n+i)$ sont $b_{n+i}, \ldots, b_{n+i+\mathrm{N}-1}$, où $b_n = a_{n+d} + c_1 a_{n+d-1} + \cdots + c_d a_n$; elles sont donc plus petites, en module, que $\mathrm{C}\mathrm{R}^{-n}$ d'après le (iii). Par ailleurs, les coordonnées de $\mathrm{A}_\mathrm{N}(n+j)$ sont, d'après le (ii), plus petites que $\mathrm{C}_0\mathrm{R}_0^{-n-d-\mathrm{N}+2}$, si $0 \leqslant j \leqslant d-1$. On en déduit la majoration $|\Delta_\mathrm{N}(n)| \leqslant \mathrm{N}!(\mathrm{C}_0\mathrm{R}_0^{-n-d-\mathrm{N}+2})^d(\mathrm{C}\mathrm{R}^{-n})^{\mathrm{N}-d}$, ce qui tend vers 0 quand $n \to +\infty$, si $\mathrm{R}^{\mathrm{N}-d}\mathrm{R}_0^d > 1$. Comme cette condition est satisfaite si N est assez grand, cela permet de conclure.

(v) Si les a_n sont des entiers, il en est de même des $\Delta_\mathrm{N}(n)$, et la majoration $|\Delta_\mathrm{N}(n)| < 1$ pour $n \geqslant n_0$ entraîne que $\Delta_\mathrm{N}(n) = 0$ si $n \geqslant n_0$. On en déduit que f est rationnelle en utilisant le I.

H.14. Le théorème de Mordell-Weil

Dans tout ce problème [24], D est un entier impair sans facteur carré. Si $S = \{p_1, \ldots, p_s\}$, où s est le cardinal de S, est l'ensemble des nombres premiers divisant D, alors $2 \notin S$ et D est le produit des p_i, pour $1 \leqslant i \leqslant s$.

L'objet du problème est l'étude de l'ensemble $C(\mathbf{Q})$ des solutions $(x, y) \in \mathbf{Q}^2$ de l'équation $y^2 = x^3 - D^2x$, avec $x > 0$. Plus précisément, il s'agit de démontrer que l'on peut munir $\overline{C}(\mathbf{Q}) = C(\mathbf{Q}) \cup \{\infty\}$ d'une structure de groupe commutatif *de type fini* (cas particulier du *théorème de Mordell-Weil*). On note C l'ensemble des solutions dans $\mathbf{R}^2$ de l'équation $y^2 = x^3 - D^2x$, avec $x > 0$; on a donc $C(\mathbf{Q}) = C \cap \mathbf{Q}^2$.

I

Dans cette partie, Γ est un groupe commutatif pour une loi notée $+$. L'élément neutre de Γ est noté 0 et l'opposé d'un élément x de Γ est noté $-x$. Si $n \in \mathbf{Z}$ et $x \in \Gamma$, on note nx l'élément de Γ évident ($0x = 0$ et $(n+1)x = nx + x$ si $n \in \mathbf{Z}$).

On dit que Γ est *de type fini* s'il existe $r \in \mathbf{N}$ et $x_1, \ldots, x_r \in \Gamma$ tels que tout élément x de Γ puisse s'écrire sous la forme $\sum_{i=1}^{r} n_i x_i$, avec $n_i \in \mathbf{Z}$, si $1 \leqslant i \leqslant r$. On dit que Γ est *de type fini modulo* 2 s'il existe un sous-ensemble fini Z de Γ tel que tout élément x de Γ puisse s'écrire sous la forme $z + 2y$, avec $z \in Z$ et $y \in \Gamma$.

On appelle *hauteur* sur Γ une application $h : \Gamma \to \mathbf{R}_+$ telle qu'il existe $M \geqslant 0$ tel que, quels que soient $(x, y) \in \Gamma^2$, on ait

$$|h(x+y) + h(x-y) - 2h(x) - 2h(y)| \leqslant M.$$

On dit que h est *admissible* si, quel que soit $B \geqslant 0$, l'ensemble des éléments x de Γ vérifiant $h(x) \leqslant B$ est un ensemble fini.

1. On note Γ_{tors} l'ensemble des $x \in \Gamma$ tels qu'il existe $n \in \mathbf{Z} - \{0\}$ tel que $nx = 0$.

1.a. Montrer que Γ_{tors} est un sous-groupe de Γ.

1.b. Le groupe Γ_{tors} est-il nécessairement fini ?

2. Soit h une hauteur sur Γ.

2.a. Montrer que, si $x \in \Gamma$, la suite de terme général $4^{-n}h(2^n x)$ tend vers une limite $\widehat{h}(x)$ quand n tend vers $+\infty$, et qu'il existe $M' \geqslant 0$ tel que $|h(x) - \widehat{h}(x)| \leqslant M'$, quel que soit $x \in \Gamma$.

2.b. Montrer que $\widehat{h}$ vérifie l'identité :

$$\widehat{h}(x+y) + \widehat{h}(x-y) = 2\widehat{h}(x) + 2\widehat{h}(y) \quad \text{quels que soient } x, y \in \Gamma.$$

24. Il s'agit de l'épreuve de 6 heures du concours d'entrée 2003 à l'École Normale. La partie I donne un critère permettant de montrer qu'un groupe commutatif est de type fini. La partie II munit $\overline{C} = C \cup \{\infty\}$ d'une structure de groupe commutatif (on peut préférer utiliser les fonctions holomorphes, comme dans le problème H.8, pour atteindre ce but). La partie III donne un certain nombre de formules relatives à cette loi de groupe, et la partie IV est consacrée à la démonstration du théorème de Mordell-Weil. Ces 4 parties reposent sur des techniques différentes et peuvent se traiter de manière indépendante (pour la partie III, on n'a besoin que de la définition de la loi d'addition donnée dans la question **6.b** de la partie II, et la partie IV utilise de manière intensive les formules de la partie III mais pas leur démonstration).

2.c. Calculer $\widehat{h}(nx)$ en fonction de $\widehat{h}(x)$, si $n \in \mathbf{Z}$.

3. On suppose que l'on peut munir Γ d'une hauteur admissible h.

3.a. Montrer que $\widehat{h}$ est une hauteur admissible sur Γ.

3.b. Montrer que $\widehat{h}(x) = 0$ si et seulement si $x \in \Gamma_{\mathrm{tors}}$.

3.c. Montrer que Γ_{tors} est fini.

3.d. Montrer que, si $x = z + 2y$, alors $\widehat{h}(y) \leqslant \frac{1}{2}(\widehat{h}(x) + \widehat{h}(z))$.

3.e. Montrer que si Γ est de type fini modulo 2, alors il est de type fini.

II

On rappelle que C est l'ensemble des solutions $(x, y) \in \mathbf{R}^2$ de l'équation $y^2 = x^3 - \mathrm{D}^2 x$ avec $x > 0$. (Il n'est probablement pas inutile de faire un dessin grossier de C.) Si $(x_0, y_0) \in \mathrm{C}$, la tangente à C en (x_0, y_0) est la droite d'équation $2y_0(y - y_0) = (3x_0^2 - \mathrm{D}^2)(x - x_0)$.

Si $(u, v) \in \mathbf{R}^* \times \mathbf{R}$, notons (u', v') le couple défini par $u' = \frac{1}{u}$, $v' = -\frac{v}{u}$, et $\mathrm{P}_{u,v}$ et $\mathrm{Q}_{u',v'}$ les polynômes définis par

$$\mathrm{P}_{u,v}(x) = x^3 - \mathrm{D}^2 x - (ux + v)^2 \quad \text{et} \quad \mathrm{Q}_{u',v'}(y) = (u'y + v')^3 - \mathrm{D}^2(u'y + v') - y^2.$$

On note $\mathrm{D}_{u,v}$ la droite d'équation $y = ux + v$. On pourra utiliser sans démonstration les équivalences (I1) $\Leftrightarrow$ (I2) $\Leftrightarrow$ (I3), avec

(I1) $(x, y) \in \mathrm{D}_{u,v} \cap \mathrm{C}$

(I2) $x > 0$, $\mathrm{P}_{u,v}(x) = 0$ et $y = ux + v$

(I3) $\mathrm{Q}_{u',v'}(y) = 0$ et $x = u'y + v' > 0$

et, si $(x_0, y_0) \in \mathrm{C} \cap \mathrm{D}_{u,v}$, les équivalences (T1) $\Leftrightarrow$ (T2) $\Leftrightarrow$ (T3), avec

(T1) $\mathrm{D}_{u,v}$ est tangente à C en (x_0, y_0)

(T2) $\mathrm{P}_{u,v}$ a un zéro double en x_0

(T3) $\mathrm{Q}_{u',v'}$ a un zéro double en y_0.

1. Soit $n(u, v)$ le cardinal de l'intersection de C avec la droite $\mathrm{D}_{u,v}$ d'équation $y = ux + v$.

1.a. Montrer que $n(u, v) \leqslant 3$.

1.b. Montrer que $\mathrm{U} = \{(u, v) \in \mathbf{R}^* \times \mathbf{R},\ n(u, v) = 3\}$ est un ouvert de $\mathbf{R}^2$.

1.c. Montrer que, si $n(u, v) \geqslant 2$ et si $\mathrm{D}_{u,v}$ n'est pas tangente à C, alors $n(u, v) = 3$.

1.d. Montrer que, si $(a, b) \in \mathbf{R}^2$, il n'existe qu'un nombre fini de points P de C tels que la tangente à C en P passe par (a, b).

2. Si $\mathrm{P} = (x, y) \in \mathrm{C}$, on pose $x(\mathrm{P}) = x$ et $y(\mathrm{P}) = y$.

2.a. Montrer que, si $t \in \mathbf{R}$, il existe un unique point $\mathrm{P}(t)$ de C vérifiant $y(\mathrm{P}(t)) = t$, et que, si on pose $\mathrm{F}(t) = x(\mathrm{P}(t))$, alors C est l'ensemble des couples $(\mathrm{F}(y), y)$, avec $y \in \mathbf{R}$.

2.b. Montrer que $\mathrm{F}(y) \geqslant \mathrm{D}$ quel que soit $y \in \mathbf{R}$, que F est paire, que l'on a $\mathrm{F}(y_1) = \mathrm{F}(y_2)$ si et seulement si $y_1 = \pm y_2$, et que F est de classe $\mathscr{C}^1$ sur $\mathbf{R}$.

2.c. Montrer que $|y|^{-2/3}\mathrm{F}(y)$ tend vers 1 quand y tend vers $+\infty$ ou vers $-\infty$.

2.d. Soient $a \in \mathbf{R}^*$ et $t \in \mathbf{R} - \{0, a, -a\}$. Notons $\mathrm{D}(a, t)$ la droite joignant $\mathrm{P}(t)$ à $\mathrm{P}(a)$ et $\mathrm{H}_a(t)$ l'élément de $\mathbf{R}$ défini par

$$a\,t\,\mathrm{H}_a(t) = -\Big(\frac{t-a}{\mathrm{F}(t)-\mathrm{F}(a)}\Big)^3\Big[\Big(\frac{t\mathrm{F}(a)-a\mathrm{F}(t)}{t-a}\Big)^3 - \mathrm{D}^2\frac{t\mathrm{F}(a)-a\mathrm{F}(t)}{t-a}\Big].$$

Montrer que l'on a les équivalences suivantes :

(i) $\mathrm{H}_a(t) \notin \{a,t\} \Leftrightarrow \mathrm{P}(\mathrm{H}_a(t))$ est le troisième point d'intersection de C et $\mathrm{D}(a,t)$;
(ii) $\mathrm{H}_a(t) = a \Leftrightarrow \mathrm{D}(a,t)$ est la tangente à C en $\mathrm{P}(a)$;
(iii) $\mathrm{H}_a(t) = t \Leftrightarrow \mathrm{D}(a,t)$ est la tangente à C en $\mathrm{P}(t)$.

2.e. Calculer la limite de $\mathrm{H}_a(t)$ quand t tend vers $+\infty$. Que devient la droite $\mathrm{D}(a,t)$?

3. On déduit des questions **2.b** et **2.c** la convergence absolue de l'intégrale $\int_{-\infty}^{+\infty} \frac{2\,dt}{3\mathrm{F}(t)^2-\mathrm{D}^2}$. On note Ω la valeur de l'intégrale $\int_{-\infty}^{+\infty} \frac{2\,dt}{3\mathrm{F}(t)^2-\mathrm{D}^2}$, et on définit une fonction $y \mapsto \mathrm{L}(y)$ par la formule

$$\mathrm{L}(y) = \int_{-\infty}^{y} \frac{2\,dt}{3\mathrm{F}(t)^2 - \mathrm{D}^2}.$$

3.a. Montrer que L induit une bijection de $\mathbf{R}$ sur $]0,\Omega[$.

3.b. Calculer $\mathrm{L}(y) + \mathrm{L}(-y)$ si $y \in \mathbf{R}$.

4. Soient $x_1, \dots, x_n$, des nombres complexes distincts deux à deux.

4.a. Montrer que, si $\mathrm{Q} \in \mathbf{C}[\mathrm{X}]$ est de degré $\leqslant n-1$, alors

$$\mathrm{Q}(\mathrm{X}) = \sum_{i=1}^{n} \mathrm{Q}(x_i)\Big(\prod_{j\neq i} \frac{\mathrm{X}-x_j}{x_i-x_j}\Big).$$

4.b. Montrer que, si $\mathrm{P}(\mathrm{X}) = \prod_{i=1}^{n}(\mathrm{X}-x_i)$, alors $\sum_{i=1}^{n} \frac{x_i^k}{\mathrm{P}'(x_i)} = 0$ si $k \in \{0,\dots,n-2\}$ (avec la convention $0^0 = 1$) et calculer $\sum_{i=1}^{n} \frac{x_i^{n-1}}{\mathrm{P}'(x_i)}$.

5.

5.a. Soit I un intervalle ouvert de $\mathbf{R}$, et soient $t \mapsto y_1(t)$, $t \mapsto y_2(t)$ et $t \mapsto y_3(t)$ des fonctions de classe $\mathscr{C}^1$ de I dans $\mathbf{R}$ telles que, quel que soit $t \in \mathrm{I}$, les points $\mathrm{P}_i(t) = (x_i(t), y_i(t)) = \mathrm{P}(y_i(t))$, $i \in \{1,2,3\}$, soient distincts deux à deux et alignés. Montrer que la fonction

$$t \mapsto \mathrm{G}(t) = \mathrm{L}(y_1(t)) + \mathrm{L}(y_2(t)) + \mathrm{L}(y_3(t))$$

est constante sur I. (On introduira l'équation $y = u(t)x + v(t)$ de la droite contenant les $\mathrm{P}_i(t)$ et on commencera par vérifier que u et v sont de classe $\mathscr{C}^1$ sur I.)

5.b. Montrer que, si $\mathrm{H}_a(t)$ est la quantité introduite à la question **2.d**, alors pour tous $a > 0$ et $t > a$, on a $\mathrm{L}(a) + \mathrm{L}(t) + \mathrm{L}(\mathrm{H}_a(t)) = 2\Omega$.

5.c. Montrer que, si y_1, y_2, y_3 sont trois éléments de $\mathbf{R}$, distincts deux à deux, tels que $\mathrm{P}(y_1)$, $\mathrm{P}(y_2)$ et $\mathrm{P}(y_3)$ sont alignés, alors $\mathrm{L}(y_1) + \mathrm{L}(y_2) + \mathrm{L}(y_3) \in \{\Omega, 2\Omega\}$.

5.d. Montrer que, si $y_1 \neq y_2$, et si $\mathrm{P}(y_2)$ est sur la tangente à C en $\mathrm{P}(y_1)$, alors $2\mathrm{L}(y_1) + \mathrm{L}(y_2)$ appartient à $\{\Omega, 2\Omega\}$.

5.e. Montrer que, si y_1, y_2, y_3 sont trois éléments de $\mathbf{R}$, distincts deux à deux, tels que $\mathrm{L}(y_1) + \mathrm{L}(y_2) + \mathrm{L}(y_3) \in \Omega\mathbf{Z}$, alors $\mathrm{P}(y_1)$, $\mathrm{P}(y_2)$ et $\mathrm{P}(y_3)$ sont alignés.

6. Soit $\mathbf{G}$ le groupe des nombres complexes de module 1 et soit $\mathrm{E} : \overline{\mathrm{C}} \to \mathbf{G}$ l'application définie par $\mathrm{E}(\infty) = 1$ et $\mathrm{E}(\mathrm{P}(y)) = \exp(\frac{2i\pi}{\Omega}\mathrm{L}(y))$ si $y \in \mathbf{R}$.

6.a. Montrer qu'il existe, sur $\overline{\mathrm{C}}$, une unique loi de groupe commutatif $+$ telle que l'on ait $\mathrm{E}(\mathrm{P}+\mathrm{Q}) = \mathrm{E}(\mathrm{P})\mathrm{E}(\mathrm{Q})$. Montrer de plus, que, si $\mathrm{P}+\mathrm{Q} \neq \infty$, alors $\mathrm{L}(y(\mathrm{P}+\mathrm{Q})) = \mathrm{L}(y(\mathrm{P}))+\mathrm{L}(y(\mathrm{Q}))$ si $\mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) < \Omega$ et $\mathrm{L}(y(\mathrm{P}+\mathrm{Q})) = \mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) - \Omega$ si $\mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) > \Omega$.

6.b. Montrer que ∞ est l'élément neutre pour $+$ et que, si $\mathrm{P}_1 = (x_1, y_1)$, $\mathrm{P}_2 = (x_2, y_2)$ et $\mathrm{P}_3 = (x_3, y_3)$ sont trois éléments distincts de C, alors $\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 = \infty$ si et seulement si P_1, P_2 et P_3 sont alignés.

6.c. Montrer que, si $\mathrm{P} \in \mathrm{C}$, alors l'opposé $-\mathrm{P}$ de P pour la loi $+$ est le symétrique de P par rapport à l'axe des x.

6.d. Montrer que si $\mathrm{P} \in \overline{\mathrm{C}}$, l'équation $2\mathrm{Q} = \mathrm{P}$ a toujours des solutions ; combien en a-t-elle ?

6.e. Montrer que, si $y_1 + y_2 \neq 0$, et si z_1 tend vers y_1 et z_2 tend vers y_2, alors $y(\mathrm{P}(z_1) + \mathrm{P}(z_2))$ tend vers $y(\mathrm{P}(y_1) + \mathrm{P}(y_2))$. Que se passe-t-il si $y_1 + y_2 = 0$?

III

Dans les questions **1.b**, **2.b** et **4**, les formules que l'on cherche à établir vont par groupe ; dans chaque groupe, on démontrera la formule qui n'est pas entre crochets, et on admettra les autres.

1. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de C, avec $x_1 \neq x_2$, et $\mathrm{P}_3 = (x_3, y_3) \in \mathrm{C}$ défini par $\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 = \infty$.

1.a. Montrer que x_1, x_2, x_3 sont les racines du polynôme

$$\mathrm{P}(x) = x^3 - \mathrm{D}^2 x - \Big(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\Big)^2.$$

En déduire que l'on a

$$x_3 = \big(\frac{x_1^2 + x_1 x_2 + x_2^2 - \mathrm{D}^2}{y_1 + y_2}\big)^2 - x_1 - x_2 \quad \text{et} \quad y_3 = \frac{x_1^2 + x_1 x_2 + x_2^2 - \mathrm{D}^2}{y_1 + y_2}(x_3 - x_1) + y_1.$$

(On commencera par supposer que P_1, P_2 et P_3 sont distincts.)

1.b. Établir les formules (la formule entre crochets sera admise sans démonstration) :

$$(x_1 + \mathrm{D})(x_2 + \mathrm{D})(x_3 + \mathrm{D}) = \Big(\frac{(x_1 + \mathrm{D})y_2 - (x_2 + \mathrm{D})y_1}{x_2 - x_1}\Big)^2$$
$$\Big[x_1 x_2 x_3 = \Big(\frac{x_1 y_2 - x_2 y_1}{x_2 - x_1}\Big)^2\Big].$$

2. Soit $\mathrm{P} = (x, y) \in \mathrm{C}$, avec $y \neq 0$ et $2\mathrm{P} = (x', y')$.

2.a. Établir les formules :

$$x' = \big(\frac{3x^2 - \mathrm{D}^2}{2y}\big)^2 - 2x \quad \text{et} \quad -y' = \frac{3x^2 - \mathrm{D}^2}{2y}(x' - x) + y.$$

2.b. Montrer que l'on a $x' = \big(\frac{x^2 + \mathrm{D}^2}{2y}\big)^2$. On admettra que, de même,

$$\Big[x' + \mathrm{D} = \Big(\frac{x^2 + 2\mathrm{D}x - \mathrm{D}^2}{2y}\Big)^2 \quad \text{et} \quad x' - \mathrm{D} = \Big(\frac{x^2 - 2\mathrm{D}x - \mathrm{D}^2}{2y}\Big)^2\Big].$$

3. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})$ est un sous-groupe de $\overline{\mathrm{C}}$.

4. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de $\mathrm{C}(\mathbf{Q})$, avec $x_1 \neq x_2$, et soient $\mathrm{P}_3 = \mathrm{P}_1 + \mathrm{P}_2 = (x_3, y_3)$ et $\mathrm{P}_4 = \mathrm{P}_1 - \mathrm{P}_2 = (x_4, y_4)$. Établir les formules (la formule entre crochets sera admise sans démonstration) :

$$(x_3 + \mathrm{D})(x_4 + \mathrm{D}) = \Big(\frac{x_1 x_2 + \mathrm{D}(x_1 + x_2) - \mathrm{D}^2}{x_2 - x_1}\Big)^2 \quad \text{et} \quad \Big[x_3 x_4 = \Big(\frac{x_1 x_2 + \mathrm{D}^2}{x_2 - x_1}\Big)^2\Big].$$

IV

IV. A

1. Si p est un nombre premier et $a \in \mathbf{Z} - \{0\}$, on définit l'entier $v_p(a)$ comme le plus grand entier n tel que p^n divise a (par exemple $48 = 3 \cdot 2^4$ et donc $v_2(48) = 4$, $v_3(48) = 1$ et $v_p(48) = 0$ si $p \notin \{2, 3\}$). On a $v_p(ab) = v_p(a) + v_p(b)$, ce qui permet d'étendre v_p à $\mathbf{Q}^*$ grâce à la formule $v_p(ab^{-1}) = v_p(a) - v_p(b)$. Si $a \in \mathbf{Q}^*$, alors $v_p(a) = 0$ sauf pour un nombre fini de nombres premiers p et, si a est positif, alors $a = \prod_p p^{v_p(a)}$. Si $v \in \mathbf{Z}$, on note $\overline{v}$ son image dans $\mathbf{Z}/2\mathbf{Z}$.

1.a. Montrer que $a \in \mathbf{Q}^*$ est un carré si et seulement si $a > 0$ et $\overline{v_p(a)} = 0$ quel que soit le nombre premier p.

1.b. Montrer que, si $a, b \in \mathbf{Q}^*$ vérifient $v_p(a) < v_p(b)$, alors $v_p(a + b) = v_p(a)$.

2. Soit $\mathrm{P} = (x, y) \in \mathrm{C}(\mathbf{Q})$, et soit $c \in \{1, 4, 9, 16, \ldots\}$ le plus petit carré (d'entier) tel que $a = cx \in \mathbf{Z}$.

2.a. Montrer que, si $v_p(c) \geqslant 1$, alors $v_p(c) \geqslant 2$ et $v_p(a) \in \{0, 1\}$.

2.b. Montrer que $a(a - \mathrm{D}c)(a + \mathrm{D}c)$ est un carré.

2.c. Montrer que, si $p \notin \mathrm{S} \cup \{2\}$, alors $v_p(a)$ et $v_p(a + \mathrm{D}c)$ sont des nombres pairs.

3. Soit $\varphi : \overline{\mathrm{C}}(\mathbf{Q}) \to (\mathbf{Z}/2\mathbf{Z})^{2s+2}$ l'application qui envoie ∞ sur $(0, \ldots, 0)$ et $\mathrm{P} = (x, y)$ sur

$$(\overline{v_2(x)}, \overline{v_{p_1}(x)}, \ldots, \overline{v_{p_s}(x)}, \overline{v_2(x + \mathrm{D})}, \overline{v_{p_1}(x + \mathrm{D})}, \ldots, \overline{v_{p_s}(x + \mathrm{D})}).$$

3.a. Montrer que φ est un morphisme de groupes de $\overline{\mathrm{C}}(\mathbf{Q})$ dans $(\mathbf{Z}/2\mathbf{Z})^{2s+2}$.

3.b. Montrer que, si $\mathrm{P} = (x', y') \in \mathrm{C}(\mathbf{Q})$ est tel que x', $x' - \mathrm{D}$ et $x' + \mathrm{D}$ sont des carrés dans $\mathbf{Q}$, et si $\mathrm{Q} \in \mathrm{C}$ est une solution de l'équation $2\mathrm{Q} = \mathrm{P}$, alors $\mathrm{Q} \in \mathrm{C}(\mathbf{Q})$.

3.c. Caractériser le noyau de φ.

3.d. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})$ est de type fini modulo 2.

IV. B

On définit une fonction $h : \overline{\mathrm{C}}(\mathbf{Q}) \to \mathbf{R}_+$ en envoyant ∞ sur 0 et $\mathrm{P} = (x, y)$ sur $\log(a + \mathrm{D}c) = \log(c(x + \mathrm{D}))$, si c est le plus petit carré rendant $a = cx$ entier.

1. Montrer que, quel que soit $\mathrm{P} \in \overline{\mathrm{C}}(\mathbf{Q})$, on a

$$h(2\mathrm{P}) \leqslant 4h(\mathrm{P}).$$

2. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de $\mathrm{C}(\mathbf{Q})$, avec $x_1 \neq x_2$, et soient $\mathrm{P}_3 = \mathrm{P}_1 + \mathrm{P}_2 = (x_3, y_3)$ et $\mathrm{P}_4 = \mathrm{P}_1 - \mathrm{P}_2 = (x_4, y_4)$. Soit c_1 (resp. c_2) le plus petit carré rendant $a_1 = c_1 x_1$ (resp. $a_2 = c_2 x_2$) entier.

2.a. Montrer que, si d divise $\mathrm{T} = a_1 a_2 + \mathrm{D}^2 c_1 c_2$, $\mathrm{U} = a_1 a_2 - \mathrm{D}^2 c_1 c_2 + \mathrm{D}(a_1 c_2 + a_2 c_1)$ et $\mathrm{V} = a_1 c_2 - a_2 c_1$, alors d divise aussi $2a_1(a_2 + \mathrm{D}c_2)$ et $2a_2(a_1 + \mathrm{D}c_1)$ ainsi que $4\mathrm{D}^2 a_1 c_2^2$ et $4\mathrm{D}^2 a_2 c_1^2$.

2.b. Montrer que, si $p \notin \mathrm{S} \cup \{2\}$, alors p ne divise pas $4\mathrm{D}^2 a_1 c_2^2$, $4\mathrm{D}^2 a_2 c_1^2$ ou $a_1 a_2 + \mathrm{D}^2 c_1 c_2$ (on commencera par montrer que p ne divise ni le p.g.c.d. de a_1 et c_1, ni celui de a_2 et c_2).

2.c. Montrer que, si $p \in \mathrm{S} \cup \{2\}$, alors p^4 ne divise pas $4\mathrm{D}^2 a_1 c_2^2$, $4\mathrm{D}^2 a_2 c_1^2$ ou $a_1 a_2 + \mathrm{D}^2 c_1 c_2$.

2.d. Montrer que le p.g.c.d. de $a_1 a_2 + \mathrm{D}^2 c_1 c_2$, $a_1 a_2 - \mathrm{D}^2 c_1 c_2 + \mathrm{D}(a_1 c_2 + a_2 c_1)$ et $a_1 c_2 - a_2 c_1$ divise $(2\mathrm{D})^3$.

2.e. Montrer que, si $x_3x_4 = \frac{d}{e}$ et $(x_3 + \mathrm{D})(x_4 + \mathrm{D}) = \frac{d'}{e}$, où d, d' et e sont des entiers, si c_3 (resp. c_4) est le plus petit carré rendant $a_3 = c_3x_3$ (resp. $a_4 = c_4x_4$) entier, et si $\delta = \text{p.g.c.d.}(d, d', e)$, alors $\frac{c_3c_4\delta}{e}$ est entier et $h(\mathrm{P}_3) + h(\mathrm{P}_4) \geqslant \log d' - \log \delta$.

2.f. Montrer que, quels que soient $(\mathrm{P}_1, \mathrm{P}_2) \in \mathrm{C}(\mathbf{Q})^2$ avec $\mathrm{P}_1 \pm \mathrm{P}_2 \neq \infty$, on a

$$h(\mathrm{P}_1 + \mathrm{P}_2) + h(\mathrm{P}_1 - \mathrm{P}_2) \geqslant 2(h(\mathrm{P}_1) + h(\mathrm{P}_2)) - \log(32\,\mathrm{D}^3).$$

3. On suppose dorénavant que le groupe $\overline{\mathrm{C}}(\mathbf{Q})$ est infini.

3.a. Montrer que les seules solutions de l'équation $2\mathrm{P} = \infty$ sont $\mathrm{P} = \infty$ et $\mathrm{P} = (\mathrm{D}, 0)$.

3.b. Montrer que $h(2\mathrm{P}) \geqslant 4h(\mathrm{P}) - 6\log(2(2\mathrm{D})^3)$ quel que soit $\mathrm{P} \in \overline{\mathrm{C}}(\mathbf{Q})$.

3.c. Montrer qu'il existe $\mathrm{A} > 0$ tel que, quels que soient $(\mathrm{P}, \mathrm{Q}) \in \overline{\mathrm{C}}(\mathbf{Q})^2$, on ait

$$h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q}) \geqslant 2(h(\mathrm{P}) + h(\mathrm{Q})) - \mathrm{A}.$$

3.d. Montrer que h est une hauteur sur $\overline{\mathrm{C}}(\mathbf{Q})$.

3.e. Montrer que h est une hauteur admissible sur $\overline{\mathrm{C}}(\mathbf{Q})$.

3.f. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})_{\mathrm{tors}}$ est un groupe fini et que $\overline{\mathrm{C}}(\mathbf{Q})$ est de type fini.

Corrigé

I

1.a. Si $nx = 0$ et $my = 0$, alors $nm(x - y) = mnx - nmy = 0$.

1.b. Non : par exemple, si $\Gamma = \mathbf{C}^*$, alors Γ_{tors} est l'ensemble des racines de l'unité d'ordre quelconque et donc est infini.

2.a. Posons $x_n = 4^{-n}h(2^nx)$ et $\mathrm{M}_0 = \mathrm{M} + h(0)$. On a $|h(2^{n+1}x) + h(0) - 4h(2^nx)| \leqslant \mathrm{M}$, et donc $|x_{n+1} - x_n| \leqslant \frac{\mathrm{M}_0}{4^{n+1}}$. On a donc $|x_{n+k} - x_n| \leqslant \sum_{i=1}^{k} \frac{\mathrm{M}_0}{4^{n+1}} \leqslant \sum_{i=1}^{+\infty} \frac{\mathrm{M}_0}{4^{n+1}} = \frac{\mathrm{M}_0}{3\cdot 4^n}$ quels que soient $(n, k) \in \mathbf{N}^2$, ce qui prouve que la suite x_n est de Cauchy, et que sa limite $\widehat{h}(x)$ vérifie $|\widehat{h}(x) - x_0| \leqslant \frac{\mathrm{M}_0}{3}$. Comme $x_0 = h(x)$, on peut prendre $\mathrm{M}' = \frac{\mathrm{M}_0}{3}$.

2.b. $|\frac{h(2^n(x+y))}{4^n} + \frac{h(2^n(x-y))}{4^n} - 2\frac{h(2^nx)}{4^n} - 2\frac{h(2^ny)}{4^n}| \leqslant \frac{\mathrm{M}}{4^n}$ et le résultat s'en déduit en passant à la limite.

2.c. Montrons par récurrence sur $n \geqslant 0$ que $\widehat{h}(kx) = k^2\widehat{h}(x)$, si $0 \leqslant k \leqslant n$. En prenant $x = y = 0$, on obtient $2\widehat{h}(0) = 4\widehat{h}(0)$ et donc $\widehat{h}(0) = 0$, et la propriété est vraie pour $n = 0$ et $n = 1$. Pour passer de n à $n + 1$, constatons que

$$\widehat{h}((n+1)x) = 2\widehat{h}(nx) + 2\widehat{h}(x) - \widehat{h}((n-1)x) = (2n^2 + 2 - (n-1)^2)\widehat{h}(x) = (n+1)^2\widehat{h}(x).$$

La propriété est donc vraie pour tout $n \geqslant 0$. Par ailleurs, en prenant $x = 0$, $y = a$, on obtient $\widehat{h}(a) + \widehat{h}(-a) = 2\widehat{h}(a)$ et donc $\widehat{h}(-a) = \widehat{h}(a)$ et la fonction $\widehat{h}$ est paire. La fonction $n \mapsto \widehat{h}(nx) - n^2\widehat{h}(x)$ est donc une fonction paire de $n \in \mathbf{Z}$ s'annulant pour $n \in \mathbf{N}$; elle est donc identiquement nulle.

3.a. On a $\widehat{h}(x) \geqslant 0$ par passage à la limite et c'est une hauteur en vertu de la question **2.b** ; elle est admissible car $\widehat{h}(x) \leqslant \mathrm{B}$ implique $h(x) \leqslant \mathrm{B} + \mathrm{M}'$ d'après la question **2.a**.

3.b. Si $mx = 0$, alors $\widehat{h}(mx) = m^2\widehat{h}(x) = 0$ et $\widehat{h}(x) = 0$.

Réciproquement, si $\widehat{h}(x) = 0$, alors $\widehat{h}(nx) = 0$ quel que soit $n \in \mathbf{Z}$ d'après la question **2.c**, et comme $\widehat{h}$ est admissible, l'ensemble $\{nx,\ n \in \mathbf{Z}\}$ est fini. Il existe donc $n_1 \neq n_2$ tels que $n_1x = n_2x$, et donc $(n_1 - n_2)x = 0$ et $x \in \Gamma_{\mathrm{tors}}$.

3.c. C'est une conséquence immédiate de la question précédente et de l'admissibilité de $\widehat{h}$.

3.d. Comme $\widehat{h}(x + z) \geqslant 0$, on a $4\widehat{h}(y) = \widehat{h}(2y) = \widehat{h}(x - z) \leqslant 2\widehat{h}(x) + 2\widehat{h}(z)$.

3.e. Par hypothèse, il existe un ensemble fini Z tel que tout élément x de Γ puisse s'écrire sous la forme $x = z + 2y$ avec $z \in \mathrm{Z}$ et $y \in \Gamma$. Soit $\mathrm{B} = \sup_{z \in \mathrm{Z}} \widehat{h}(z)$ et soit $\mathrm{A} = \{a \in \Gamma,\ \widehat{h}(a) \leqslant 2\mathrm{B}\}$. Alors A

est un ensemble fini ; on note $a_1, \dots, a_r$ ses éléments. Montrons par récurrence sur k que tout élément x de Γ vérifiant $\widehat{h}(x) \leqslant (2^k+1)\mathrm{B}$ peut s'écrire sous la forme $n_1a_1 + \cdots + n_ra_r$. C'est vrai pour $k=0$ par construction. Si $k \in \mathbf{N}$ et $\widehat{h}(x) \leqslant (2^{k+1}+1)\mathrm{B}$, on peut écrire x sous la forme $x = z+2y$, avec $z \in \mathrm{Z}$ et $y \in \Gamma$ vérifie $\widehat{h}(y) \leqslant \frac{1}{2}(\widehat{h}(z)+\widehat{h}(x)) \leqslant \frac{1}{2}(\mathrm{B}+(2^{k+1}+1)\mathrm{B}) = (2^k+1)\mathrm{B}$, ce qui permet d'utiliser l'hypothèse de récurrence pour y, et on conclut en remarquant que $z \in \mathrm{Z} \subset \mathrm{A}$.

II

1.a. $\mathrm{D}_{u,v} \cap \mathrm{C}$ est en bijection avec un sous-ensemble des racines de $\mathrm{P}_{u,v}$ qui est de degré 3.

1.b. Soit $(a,b) \in \mathbf{R}^* \times \mathbf{R}$ vérifiant $n(a,b) = 3$. Alors le polynôme $\mathrm{P}_{a,b}$ a trois zéros simples réels $0 < x_1 < x_2 < x_3$ et, comme $\mathrm{P}_{a,b}$ est < 0 au voisinage de $-\infty$, on a $\mathrm{P}_{a,b}(0) < 0$, $\mathrm{P}_{a,b}(\frac{x_1+x_2}{2}) > 0$ et $\mathrm{P}_{a,b}(\frac{x_2+x_3}{2}) < 0$. Par continuité, il existe un ouvert $\mathrm{U}_{a,b}$ contenant (a,b) tel que, si $(u,v) \in \mathrm{U}_{a,b}$, alors $\mathrm{P}_{u,v}(0) < 0$, $\mathrm{P}_{u,v}(\frac{x_1+x_2}{2}) > 0$ et $\mathrm{P}_{u,v}(\frac{x_2+x_3}{2}) < 0$, ce qui implique que $\mathrm{P}_{u,v}$ a un zéro entre 0 et $\frac{x_1+x_2}{2}$, un entre $\frac{x_1+x_2}{2}$ et $\frac{x_2+x_3}{2}$ et un entre $\frac{x_2+x_3}{2}$ et $+\infty$, et donc $n(u,v) = 3$. On a donc montré $\mathrm{U} \supset \mathrm{U}_{a,b}$, ce qui permet de conclure.

1.c. Si $n(u,v) \geqslant 2$ et si $\mathrm{D}_{u,v}$ n'est pas tangente à C, le polynôme $\mathrm{P}_{u,v}$ a 3 racines réelles distinctes dont deux sont > 0. Le coefficient constant de $\mathrm{P}_{u,v}$ est $-v^2$ et il y a priori deux cas :

— $v = 0$ et alors le produit des deux racines non nulles de $\mathrm{P}_{u,v}$ est $-\mathrm{D}^2$ qui est < 0, ce qui contredit le fait que ces deux racines sont > 0 ; ce cas est donc exclus ;

— $v \neq 0$ et le produit v^2 des racines de $\mathrm{P}_{u,v}$ est > 0, ce qui implique que la troisième racine de $\mathrm{P}_{u,v}$ est > 0 et $n(u,v) = 3$.

1.d. L'ensemble des points $\mathrm{P} = (x,y)$ appartenant à C tels que (a,b) appartienne à la tangente à C en P est l'ensemble des couples $(x,y) \in \mathbf{R}^2$ vérifiant $y^2 = x^3 - \mathrm{D}^2x$, $x > 0$ et $2y(b-y) = (3x^2 - \mathrm{D}^2)(a-x)$. En particulier, $2by = (3x^2-\mathrm{D}^2)(a-x) + 2y^2 = 2x^3 + 3ax^2 + 3\mathrm{D}^2x - \mathrm{D}^2a$. Si $b = 0$, alors x est racine d'un polynôme de degré 3 et comme $y^2 = x^3 - \mathrm{D}x$, pour chaque valeur de x, il y a au plus 2 valeurs de y, ce qui nous fait au plus 6 couples (x,y) solutions. Si $b \neq 0$, en reportant la valeur de y dans l'équation $y^2 = x^3 - \mathrm{D}x$, on voit que x est racine d'un polynôme de degré 6 et donc qu'il y a au plus 12 couples (x,y) solutions.

2.a. Si $t \in \mathbf{R}$, la fonction $x \mapsto x^3 - \mathrm{D}^2x - t^2$ est décroissante de 0 à $\frac{\mathrm{D}}{\sqrt{3}}$ et croissante de $\frac{\mathrm{D}}{\sqrt{3}}$ à $+\infty$. Comme elle est $\leqslant 0$ en $x = 0$ et $x = \mathrm{D}$, elle ne s'annulle pas sur $]0,\mathrm{D}[$ et comme elle tend vers $+\infty$ en $+\infty$, elle s'annulle une et une seule fois sur $[\mathrm{D},+\infty[$. Si on note $\mathrm{F}(t)$ le point où elle s'annule, alors $\mathrm{P}(t) = (\mathrm{F}(t),t)$ est l'unique point de C vérifiant $y(\mathrm{P}(t)) = t$, ce qui permet de conlure.

2.b. La fonction $x \mapsto x^3 - \mathrm{D}^2x$ est croissante et de classe $\mathscr{C}^1$ sur $]\frac{\mathrm{D}}{\sqrt{3}},+\infty[$; c'est donc une bijection de $]\frac{\mathrm{D}}{\sqrt{3}},+\infty[$ sur $]-\frac{2\mathrm{D}^3}{3\sqrt{3}},+\infty[$ et son inverse G est de classe $\mathscr{C}^1$ et vérifie $\mathrm{G}(0) = \mathrm{D}$; comme on a $\mathrm{F}(t) = \mathrm{G}(t^2)$, cela permet de conclure.

2.c. Si $y \in \mathbf{R}$, soit $f_y(x) = x^3 - \mathrm{D}^2x - y^2$. Soit $\varepsilon > 0$. Alors $f_y((1+\varepsilon)|y|^{2/3})$ et $f_y((1-\varepsilon)|y|^{2/3})$ sont équivalents respectivement à $((1+\varepsilon)^3-1)y^2$ et $((1-\varepsilon)^3-1)y^2$ au voisinage de $|y| = +\infty$. En particulier, si $|y|$ est suffisamment grand, alors $f_y((1+\varepsilon)|y|^{2/3})$ et $f_y((1-\varepsilon)|y|^{2/3})$ sont de signes opposés et on a $(1-\varepsilon)|y|^{2/3} \leqslant \mathrm{F}(y) \leqslant (1+\varepsilon)|y|^{2/3}$. On en déduit le fait que $|y|^{-2/3}\mathrm{F}(y)$ tend vers 1 quand $|y|$ tend vers $+\infty$.

2.d. L'équation de la droite $\mathrm{D}(a,t)$ est $x - \mathrm{F}(a) = \frac{\mathrm{F}(t)-\mathrm{F}(a)}{t-a}(y-a)$ que l'on peut réécrire sous la forme $x = \frac{\mathrm{F}(t)-\mathrm{F}(a)}{t-a}y + \frac{\mathrm{F}(a)t-a\mathrm{F}(t)}{t-a}$. Pour comprendre l'intersection de $\mathrm{D}(a,t)$ avec C, on peut utiliser l'équivalence (I1) $\Leftrightarrow$ (I3) et considérer le polynôme $\mathrm{Q}_{u,v}$, avec $u = \frac{\mathrm{F}(t)-\mathrm{F}(a)}{t-a}$ et $v = \frac{\mathrm{F}(a)t-a\mathrm{F}(t)}{t-a}$ dont le coefficient dominant est u^3 et le terme constant est $v^3 - \mathrm{D}^2v$. Le produit des racines de $\mathrm{Q}_{u,v}$ est donc $-\frac{v^3-\mathrm{D}^2v}{u^3}$, et comme $\mathrm{Q}_{u,v}$ a comme racines a et t par construction, sa troisième racine est $-\frac{v^3-\mathrm{D}^2v}{atu^3} = \mathrm{H}_a(t)$.

Les résultats à démontrer sont alors des conséquences immédiates de la question **1.c.** et de l'équivalence (T1) $\Leftrightarrow$ (T3).

2.e. Comme $\mathrm{F}(t) \sim t^{2/3}$ au voisinage de $+\infty$, on a $\frac{1}{t}(\frac{t-a}{\mathrm{F}(t)-\mathrm{F}(a)})^3$ qui tend vers 1 quand t tend vers $+\infty$ et $\mathrm{H}_a(t)$ tend vers $-\frac{1}{a}(\mathrm{F}(a)^3 - \mathrm{D}^2\mathrm{F}(a)) = -\frac{1}{a}\cdot a^2 = -a$ et la droite $\mathrm{D}(t,a)$ devient verticale.

3.a. On a $\mathrm{L}'(y) = \frac{2}{3\mathrm{F}(y)^2-\mathrm{D}^2} > 0$, ce qui montre que L est une bijection croissante de $\mathbf{R}$ sur son image. Comme $\lim_{y\to-\infty}\mathrm{L}(y) = 0$ et $\lim_{y\to+\infty}\mathrm{L}(y) = \Omega$, cela permet de conlure.

3.b. Comme F est paire, on a $\mathrm{L}(-y) = \int_{-\infty}^{-y}\frac{2}{3\mathrm{F}(t)^2-\mathrm{D}^2}dt = \int_{y}^{+\infty}\frac{2}{3\mathrm{F}(t)^2-\mathrm{D}^2}dt$, ce qui fait que $\mathrm{L}(y)+\mathrm{L}(-y) = \int_{-\infty}^{+\infty}\frac{2}{3\mathrm{F}(t)^2-\mathrm{D}^2}dt = \Omega$.

4.a. Les deux membres sont des polynômes de degré $\leqslant n-1$, prenant les mêmes valeurs en $x_1,\dots,x_n$; la différence est donc un polynôme de degré $\leqslant n-1$ ayant n racines et donc est nulle.

4.b. Si on applique ce qui précède au polynôme X^k, que l'on identifie les termes de degré $n-1$ et que l'on remarque que $\prod_{j\neq i}(x_i - x_j) = \mathrm{P}'(x_i)$, on obtient $\sum_{i=1}^n \frac{x_i^k}{\mathrm{P}'(x_i)} = 0$ si $k \leqslant n-2$ et $\sum_{i=1}^n \frac{x_i^k}{\mathrm{P}'(x_i)} = 1$ si $k = n-1$.

5.a. $u(t) = \frac{y_2(t)-y_1(t)}{\mathrm{F}(y_2(t))-\mathrm{F}(y_1(t))}$ et $v(t) = y_1(t) - \frac{y_2(t)-y_1(t)}{\mathrm{F}(y_2(t))-\mathrm{F}(y_1(t))}\mathrm{F}(y_1(t))$ sont de classe $\mathscr{C}^1$ car y_1, y_2 et F le sont et $\mathrm{F}(y_1(t)) - \mathrm{F}(y_2(t))$ ne s'annulle pas puisque $y_1(t) \neq y_2(t)$ sont > 0 (et donc $y_1(t) \neq \pm y_2(t)$). On a $\frac{1}{2}\mathrm{G}' = \sum_{i=1}^3 \frac{y_i'}{3x_i^2-\mathrm{D}^2}$. Par ailleurs, on a aussi

$$2y_iy_i' = (3x_i^2 - \mathrm{D}^2)x_i' \quad \text{et} \quad y_i' = ux_i' + u'x_i + v'.$$

On peut éliminer x_i' entre ces deux équations pour obtenir

$$(3x_i^2 - \mathrm{D}^2 - 2uy_i)y_i' = (3x_i^2 - \mathrm{D}^2)(u'x_i + v')$$

et

$$\frac{1}{2}\mathrm{G}' = u'\sum_{i=1}^3 \frac{x_i}{3x_i^2 - \mathrm{D}^2 - 2uy_i} + v'\sum_{i=1}^3 \frac{1}{3x_i^2 - \mathrm{D}^2 - 2uy_i}.$$

De plus, x_1, x_2, x_3 sont les racines du polynôme $\mathrm{P}(x) = x^3 - \mathrm{D}^2x - (ux+v)^2$ dont la dérivée est $3x^2 - \mathrm{D}^2 - 2u(ux+v)$ et comme $y_i = ux_i + v$, on obtient $\frac{1}{2}\mathrm{G}' = u'\sum_{i=1}^3 \frac{x_i}{\mathrm{P}'(x_i)} + v'\sum_{i=1}^3 \frac{1}{\mathrm{P}'(x_i)} = 0$ d'après la question précédente. La fonction G a donc une dérivée nulle sur I et est donc constante.

5.b. La formule donnant $\mathrm{H}_a(t)$ montre que la fonction $\mathrm{H}_a(t)$ est de classe $\mathscr{C}^1$. La question précédente montre alors que $\mathrm{G}(t) = \mathrm{L}(a)+\mathrm{L}(t)+\mathrm{L}(\mathrm{H}_a(t))$ est constante sur tout intervalle I pour lequel $\mathrm{H}_a(t) \notin \{a,t\}$ quel que soit $t \in \mathrm{I}$. Par ailleurs, l'ensemble des points où $\mathrm{H}_a(t) = a$ est fini (c'est l'intersection de la tangente à C en $\mathrm{P}(a)$ avec C) et l'ensemble des points t tels que $\mathrm{H}_a(t) = t$ est aussi fini d'après la question **1.d**. La réunion des intervalles I pour lequels on a $\mathrm{H}_a(t) \notin \{a,t\}$ quel que soit $t \in \mathrm{I}$ recouvre donc $]a,+\infty[$ à un nombre fini de points près, et comme G est constante sur chacun de ces intervalles et continue sur $]a,+\infty[$, elle est constante sur $]a,+\infty[$. On a donc, d'après les questions **2.e** et **3.b.**, $\mathrm{G}(t) = \lim_{t\to+\infty}\mathrm{G}(t) = \mathrm{L}(a) + \mathrm{L}(-a) + \lim_{t\to+\infty}\mathrm{L}(t) = 2\Omega$.

5.c. Si parmi y_1, y_2 et y_3, deux sont > 0, la question précédente montre que $\mathrm{L}(y_1)+\mathrm{L}(y_2)+\mathrm{L}(y_3) = 2\Omega$. Si deux sont < 0, alors $\mathrm{L}(y_1)+\mathrm{L}(y_2)+\mathrm{L}(y_3) = 3\Omega - (\mathrm{L}(-y_1)+\mathrm{L}(-y_2)+\mathrm{L}(-y_3)) = \Omega$. Le cas $y_1 = 0$, $y_2 > 0$, $y_3 < 0$ est impossible car $y_1 = 0$ implique $x_1 = \mathrm{D}$ et comme x_2 et x_3 sont $> \mathrm{D}$, les points (x_1,y_1), (x_2,y_2) et (x_3,y_3) ne peuvent pas être alignés.

5.d. Posons $a = y_2$. Comme il n'y a qu'un nombre fini de tangentes à C qui passent par $\mathrm{P}(a)$, il existe un intervalle ouvert I contenant y_1 tel que la droite $\mathrm{D}(a,t)$ ne soit pas tangente à C si $t \in \mathrm{I} - \{y_1\}$. Mais alors $\mathrm{H}_a(t)$ est continue en $t = y_1$ et $\mathrm{L}(a)+\mathrm{L}(t)+\mathrm{L}(\mathrm{H}_a(t))$ est à valeurs dans $\{\Omega, 2\Omega\}$ sur $\mathrm{I} - \{y_1\}$; elle est donc constante sur I et à la limite, on obtient $2\mathrm{L}(y_1)+\mathrm{L}(y_2) \in \{\Omega, 2\Omega\}$.

5.e. D'après la question **1.c**, la droite joignant $\mathrm{P}(y_1)$ à $\mathrm{P}(y_2)$ coupe C en un troisième point $\mathrm{P}(z)$ ou est tangente à C en $\mathrm{P}(y_1)$ (resp. en $\mathrm{P}(y_2)$) auquel cas on pose $z = y_1$ (resp. $z = y_2$). D'après les

questions **5.c.** et **5.d.**, on a dans tous les cas $\mathrm{L}(y_1)+\mathrm{L}(y_2)+\mathrm{L}(z) \in \Omega\mathbf{Z}$ et donc $\mathrm{L}(z)-\mathrm{L}(y_3) \in \Omega\mathbf{Z}$. Mais comme $\mathrm{L}(z)-\mathrm{L}(y_3) \in]-\Omega,\Omega[$, cela implique $\mathrm{L}(z)-\mathrm{L}(y_3)=0$ et donc $z=y_3$ puisque L est injective.

6.a. D'après la question **3.a**, E est une bijection de $\overline{\mathrm{C}}$ sur $\mathbf{G}$ et on peut (et doit) définir + par la formule $\mathrm{P}+\mathrm{Q}=\mathrm{E}^{-1}(\mathrm{E}(\mathrm{P})\mathrm{E}(\mathrm{Q}))$. On doit alors avoir $\exp\left(\frac{2i\pi}{\Omega}(\mathrm{L}(y(\mathrm{P}+\mathrm{Q}))-\mathrm{L}(y(\mathrm{P}))-\mathrm{L}(y(\mathrm{Q})))\right)=1$ et donc $\mathrm{L}(y(\mathrm{P}+\mathrm{Q}))-\mathrm{L}(y(\mathrm{P}))-\mathrm{L}(y(\mathrm{Q})) \in \Omega\mathbf{Z}$. Le reste de la question résulte de ce que $\mathrm{L}(y(\mathrm{P}))+\mathrm{L}(y(\mathrm{Q})) \in]0,2\Omega[$ et $\mathrm{L}(y(\mathrm{P}+\mathrm{Q})) \in]0,\Omega[$.

6.b. $\infty=\mathrm{E}^{-1}(1)$ est l'élément neutre de + par construction et $\mathrm{P}_1+\mathrm{P}_2+\mathrm{P}_3=\infty$ si et seulement si $\mathrm{L}(y_1)+\mathrm{L}(y_2)+\mathrm{L}(y_3) \in \Omega\mathbf{Z}$, c'est-à-dire si et seulement si P_1, P_2 et P_3 sont alignés d'après les questions **5.c** et **5.e**.

6.c. Si $\mathrm{P}=(x,y)$ et $-\mathrm{P}=(x',y')$, on a $\mathrm{L}(y)+\mathrm{L}(y') \in \Omega\mathbf{Z}$ et comme $\mathrm{L}(y)$ et $\mathrm{L}(y')$ appartiennent à $]0,\Omega[$, cela implique $\mathrm{L}(y')=\Omega-\mathrm{L}(y)=\mathrm{L}(-y)$ et donc $y'=-y$ puisque L est injective.

6.d. Comme E induit un isomorphisme du groupe $\overline{\mathrm{C}}$ sur $\mathbf{G}$, l'ensemble des solutions de l'équation $2\mathrm{Q}=\mathrm{P}$ est en bijection avec celui de l'équation $z^2=\mathrm{E}(\mathrm{P})$; l'équation $2\mathrm{Q}=\mathrm{P}$ a donc toujours 2 solutions.

6.e. Si $y_1+y_2 \neq 0$, on a $\mathrm{L}(y_1)+\mathrm{L}(y_2) \neq \Omega$ et, quitte à remplacer y_1 par $-y_1$ et y_2 par $-y_2$, on peut supposer $0<\mathrm{L}(y_1)+\mathrm{L}(y_2)<\Omega$. Comme L est continue, il existe des intervalles ouverts $\mathrm{I}_1 \ni y_1$ et $\mathrm{I}_2 \ni y_2$ tels que l'on ait $0<\mathrm{L}(z_1)+\mathrm{L}(z_2)<\Omega$ si $(z_1,z_2) \in \mathrm{I}_1 \times \mathrm{I}_2$. La bijection réciproque $\mathrm{L}^{-1}:]0,\Omega[\to \mathbf{R}$ étant continue, la fonction $(z_1,z_2) \mapsto \mathrm{L}^{-1}(\mathrm{L}(z_1)+\mathrm{L}(z_2))=y(\mathrm{P}(z_1)+\mathrm{P}(z_2))$ est continue sur $\mathrm{I}_1 \times \mathrm{I}_2$, ce qui permet de conclure.

III

1.a. Commençons par supposer P_1, P_2 et P_3 distincts. La droite passant par P_1 et P_2 est la droite d'équation $y=y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)$. On en déduit le fait que x_1,x_2,x_3 sont les racines du polynôme

$$\mathrm{P}(x)=x^3-\mathrm{D}^2x-\left(y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2.$$

La somme des racines de ce polynôme est alors $\left(\frac{y_2-y_1}{x_2-x_1}\right)^2$ et comme

$$\frac{y_2-y_1}{x_2-x_1}=\frac{y_2^2-y_1^2}{(y_1+y_2)(x_2-x_1)}=\frac{x_2^3-\mathrm{D}^2x_2-x_1^3+\mathrm{D}^2x_1}{(y_1+y_2)(x_2-x_1)}=\frac{x_1^2+x_1x_2+x_2^2-\mathrm{D}^2}{y_1+y_2},$$

on obtient $x_3=\left(\frac{x_1^2+x_1x_2+x_2^2-\mathrm{D}^2}{y_1+y_2}\right)^2-x_1-x_2$. La formule pour y_3 s'en déduit en utilisant la formule précédente et le fait que P_3 est sur la droite d'équation $y=y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)$. Le cas où $\mathrm{P}_3 \in \{\mathrm{P}_1,\mathrm{P}_2\}$ se déduit du cas général par continuité (cf. question **6.e** de la partie II).

1.b. $x_1+\mathrm{D}$, $x_2+\mathrm{D}$ et $x_3+\mathrm{D}$ sont les racines du polynôme $\mathrm{P}(x-\mathrm{D})$ dont le terme constant est $-\left(\frac{y_2-y_1}{x_2-x_1}(-\mathrm{D}-x_1)+y_1\right)^2=-\left(\frac{y_1(x_2+\mathrm{D})-y_2(x_1+\mathrm{D})}{x_2-x_1}\right)^2$.

2.a. Ces formules se déduisent de celles de la question **1.a** par continuité.

2.b. On a $x'=\left(\frac{3x^2-\mathrm{D}^2}{2y}\right)^2-2x=\frac{9x^4-6\mathrm{D}^2x^2+\mathrm{D}^4-8xy^2}{4y^2}$, et comme $y^2=x^3-\mathrm{D}^2x$, on a aussi $9x^4-6\mathrm{D}^2x^2+\mathrm{D}^4-8xy^2=x^4+2\mathrm{D}^2x^2+\mathrm{D}^4=(x^2+\mathrm{D}^2)^2$.

3. Comme $-\mathrm{P}$ est le symétrique de P par rapport à l'axe des x, $\overline{\mathrm{C}}(\mathbf{Q})$ est stable par passage à l'opposé. Soient P et Q appartenant à $\overline{\mathrm{C}}(\mathbf{Q})$. Il s'agit de prouver que $\mathrm{P}+\mathrm{Q} \in \overline{\mathrm{C}}(\mathbf{Q})$. C'est trivial si $\mathrm{P}=\infty$ ou si $\mathrm{Q}=\infty$ ou si $\mathrm{P}=-\mathrm{Q}$. Dans tous les autres cas, on $y(\mathrm{P})+y(\mathrm{Q}) \neq 0$ et on peut utiliser les formules des questions **2.a** et **3.a** pour conclure.

4. D'après la question **2.b**, on a

$$(x_1+\mathrm{D})(x_2+\mathrm{D})(x_3+\mathrm{D}) = \Big(\frac{(x_1+\mathrm{D})y_2-(x_2+\mathrm{D})y_1}{x_2-x_1}\Big)^2$$
$$(x_1+\mathrm{D})(x_2+\mathrm{D})(x_4+\mathrm{D}) = \Big(\frac{(x_1+\mathrm{D})y_2+(x_2+\mathrm{D})y_1}{x_2-x_1}\Big)^2$$

et $(x_3+\mathrm{D})(x_4+\mathrm{D})$ est le carré de $\frac{(x_1+\mathrm{D})^2y_2^2-(x_2+\mathrm{D})^2y_1^2}{(x_1+\mathrm{D})(x_2+\mathrm{D})(x_1-x_2)^2}$. Comme $y_i^2 = x_i^3-\mathrm{D}^2x_i = x_i(x_i+\mathrm{D})(x_i-\mathrm{D})$, cela implique que $(x_3+\mathrm{D})(x_4+\mathrm{D})$ est aussi le carré de

$$\frac{(x_1+\mathrm{D})x_2(x_2-\mathrm{D})-(x_2+\mathrm{D})x_1(x_1-\mathrm{D})}{(x_1-x_2)^2} = \frac{x_1x_2+\mathrm{D}(x_1+x_2)-\mathrm{D}^2}{x_2-x_1}.$$

IV.A

1.a. Si $b\in\mathbf{Q}^*$ et si $a=b^2$, alors $a>0$ et $v_p(a)=2v_p(b)$ est divisible par 2. Réciproquement, si $a>0$ et si $v_p(a)=2n_p$, alors a est le carré de $\prod_p p^{n_p}$ (le produit est un produit fini).

1.b. On a $v_p(da)=v_p(a)+v_p(d)$, $v_p(da)=v_p(a)+v_p(d)$ et $v_p(d(a+b))=v_p(a+b)+v_p(d)$, ce qui permet, en prenant pour d le produit des dénominateurs de a et b, de se ramèner au cas où a et b sont entiers. On a alors $a=p^{v_p(a)}a'$ et $b=p^{v_p(a)}p^{v_p(b)-v_p(a)}b'$ avec a' et b' premiers à p. Comme $v_p(b)-v_p(a)>0$, on a p qui divise $p^{v_p(b)-v_p(a)}b'$ et comme a' est premier à p, cela fait que p ne divise pas $c=a'+p^{v_p(b)-v_p(a)}b'$ et donc que $a+b=p^{v_p(a)}c$ vérifie $v_p(a+b)=v_p(a)$.

2.a. Comme c est un carré, $v_p(c)$ est pair et $v_p(c)\geqslant 1$ implique $v_p(c)\geqslant 2$. D'autre part, a n'est pas divisible par p^2 car sinon, $(p^{-2}c)a$ serait entier, ce qui contredit la minimalité de c; donc $v_p(a)\leqslant 1$ et $v_p(a)\in\{0,1\}$.

2.b. On a $a(a-\mathrm{D}c)(a+\mathrm{D}c)=c^3y^2$ et comme c est un carré, il en est de même de $a(a-\mathrm{D}c)(a+\mathrm{D}c)$.

2.c. Soit p un nombre premier divisant $a(a-\mathrm{D}c)(a+\mathrm{D}c)$ et pas 2D. Si p divise a et c, alors $v_p(a)=1$ et $v_p(c)\geqslant 2$ d'après la question **2.a**, et on a $v_p(a-\mathrm{D}c)=1$ et $v_p(a+\mathrm{D}c)=1$ (question **1.b**) et donc $v_p(a(a-\mathrm{D}c)(a+\mathrm{D}c))=3$ ce qui est impossible puisque $a(a-\mathrm{D}c)(a+\mathrm{D}c)$ est un carré. Donc p ne divise pas (a,c) et p divise un seul des trois nombres a, $a-\mathrm{D}c$ et $a+\mathrm{D}c$ et, comme le produit de ces trois nombres est un carré, deux des nombres $v_p(a)$, $v_p(a-\mathrm{D}c)$ et $v_p(a+\mathrm{D}c)$ sont nuls et le troisième est pair.

3.a. Il s'agit de vérifier que l'on a $\varphi(\mathrm{P}+\mathrm{Q})=\varphi(\mathrm{P})+\varphi(\mathrm{Q})$ ou encore, comme $\varphi(\mathrm{P})=-\varphi(\mathrm{P})$, que $\varphi(\mathrm{P}+\mathrm{Q})+\varphi(\mathrm{P})+\varphi(\mathrm{Q})=0$. C'est trivial si $\mathrm{P}=\infty$ ou $\mathrm{Q}=\infty$; ça l'est aussi si $\mathrm{P}+\mathrm{Q}=0$ car alors $x(\mathrm{P})=x(\mathrm{Q})$. Si $\mathrm{Q}\notin\{\mathrm{P},-\mathrm{P}\}$, la formule $\varphi(\mathrm{P}+\mathrm{Q})+\varphi(\mathrm{P})+\varphi(\mathrm{Q})=0$ résulte de la question **2.b** de la partie III et, si $\mathrm{Q}=\mathrm{P}$, on a $2\varphi(\mathrm{P})=0=\varphi(2\mathrm{P})$ d'après la question **3.b** de la partie III.

3.b. Si $\mathrm{Q}=(x,y)\in\mathrm{C}$ vérifie $2\mathrm{Q}=\mathrm{P}$, l'hypothèse selon laquelle x', $x'-\mathrm{D}$ et $x'+\mathrm{D}$ sont des carrés dans $\mathbf{Q}$ nous dit, d'après la question **3.b** de la partie III, qu'il existe des rationnels a,b,c tels que l'on ait

$$\frac{x^2+\mathrm{D}^2}{2y}=a,\quad \frac{x^2+2\mathrm{D}x-\mathrm{D}^2}{2y}=b\quad\text{et}\quad \frac{x^2-2\mathrm{D}x-\mathrm{D}^2}{2y}=c.$$

On a alors $2a-b-c=\frac{2\mathrm{D}^2}{y}$, ce qui prouve que y est rationnel, et $b-c=\frac{2\mathrm{D}x}{y}$, ce qui prouve que x est rationnel et donc $\mathrm{Q}\in\mathrm{C}(\mathbf{Q})$.

3.c. Si $\mathrm{P}=(x,y)\in\mathrm{C}(\mathbf{Q})$ est dans le noyau de φ, c'est que $v_p(x)$ et $v_p(x+\mathrm{D})$ sont pairs quels que soit le nombre premier p. D'autre part, comme $x\geqslant\mathrm{D}$, on a $x>0$ et $x+\mathrm{D}>0$ et x et $x+\mathrm{D}$ sont des carrés dans $\mathbf{Q}$ d'après la question **1.a**. Comme $x(x-\mathrm{D})(x+\mathrm{D})=y^2$ est un carré, il en est de même de $x-\mathrm{D}$. D'après la question **6.d** de la partie III, l'équation $2\mathrm{Q}=\mathrm{P}$ a au moins une solution $\mathrm{Q}=(x,y)$ dans C et la question précédente montre que $\mathrm{Q}\in\mathrm{C}(\mathbf{Q})$ et $\mathrm{P}\in 2\overline{\mathrm{C}}(\mathbf{Q})$. Réciproquement, si $\mathrm{P}=2\mathrm{Q}$, $\mathrm{P}\neq\infty$ et $\mathrm{Q}\in\mathrm{C}(\mathbf{Q})$, alors la question **3.b** de la partie III montre que x et $x+\mathrm{D}$ sont des carrés dans $\mathbf{Q}$ et P est dans le noyau de φ. On a donc $\operatorname{Ker}\varphi=2\overline{\mathrm{C}}(\mathbf{Q})$.

3.d. Soit $Z \subset \overline{C}(\mathbf{Q})$ tel que φ induise une bijection de Z sur l'image de $C(\mathbf{Q})$ dans $(\mathbf{Z}/2\mathbf{Z})^{2s+2}$. Alors Z est fini (puisqu'il est en bijection avec un sous-ensemble d'un ensemble fini) et, si $P \in \overline{C}(\mathbf{Q})$, il existe $R \in Z$ tel que $\varphi(P - R) = 0$; il existe alors $Q \in \overline{C}(\mathbf{Q})$ tel que $P - R = 2Q$ et $P = Z + 2Q$, ce qui prouve que $\overline{C}(\mathbf{Q})$ est de type fini modulo 2.

IV.B

1. Si $2P = \infty$, il n'y a rien à démontrer. Sinon, si $2P = (x', y')$, on a $x' + D = \left(\frac{x^2+2Dx-D^2}{2y}\right)^2$ d'après la question **3.b** de la partie III. Ceci peut se réécrire sous la forme

$$x' + D = \frac{\left(\frac{a^2}{c^2} + 2D\frac{a}{c} - D^2\right)^2}{4\left(\frac{a^3}{c^3} - D^2\frac{a}{c}\right)} = \frac{(a^2 + 2Dac - D^2c^2)^2}{4ca(a - Dc)(a + Dc)}.$$

Alors $c' = 4ca(a - Dc)(a + Dc)$ est un carré puisque c en est un et $a(a - Dc)(a + Dc)$ aussi d'après la question **2.b** de la partie IV.A. On a donc

$$h(2P) \leqslant \log(c'(x' + D)) = 2\log((a + cD)^2 - 2D^2c^2) \leqslant 4\log(a + Dc) = 4h(P).$$

2.a. Si d divise T, U et V, alors d divise aussi les quantités $T + U + DV = 2Da_1(a_2 + Dc_2)$ et $T + U - DV = 2Da_2(a_1 + Dc_1)$. Il divise donc aussi $(a_1 + Dc_1)(T + U + DV) - 2Da_1U = 4D^3a_1c_1c_2$ et $(a_1 + Dc_1)(T + U + DV) - 2Da_1U - 4D^3c_1V = 4D^3a_2c_1^2$. Par symétrie, il divise aussi $4D^3a_1c_2^2$.

2.b. D'après la question **2.c** de la partie IV.A, $v_p(a_i)$ est pair et d'après la question **2.a** de la partie IV.A, on a $v_p(a_i) \leqslant 1$ si $v_p(c_i) \neq 0$; ceci implique que, si $v_p(c_i) \neq 0$, alors $v_p(a_i) = 0$ et donc que p ne divise pas le p.g.c.d. de a_i et c_i.

Maintenant, comme p est premier à $4D^3$, il divise a_1 ou c_2. S'il divise a_1, alors il ne divise pas c_1 et donc il divise a_2 et donc il ne divise pas pas c_2 ni $a_1a_2 + D^2c_1c_2$. De même, s'il divise c_2, alors il ne divise pas a_2 et donc il divise c_1 et pas a_1 et pas non plus $a_1a_2 + D^2c_1c_2$.

2.c. Supposons le contraire ; il y a plusieurs cas :

— p divise c_1 et c_2 ; auquel cas, p^2 ne divise ni a_1 ni a_2 d'après la question **2.a.** de la partie IV.A et p^3 ne divise ni a_1a_2 ni $a_1a_2 - D^2c_1c_2$ puisque c_1c_2 est divisible par p^4 ; ce cas est donc exclus ;

— p divise c_1 mais pas c_2, auquel cas p^2 ne divise pas a_1 et p^5 ne divise pas $4D^3a_1c_2$; ce cas est donc aussi exclus ainsi que le cas symétrique p divise c_2 mais pas c_1 ;

— p ne divise ni c_1 ni c_2 ; auquel cas p^2 divise a_1 et a_2 et $a_1a_2 + D^2c_1c_2$ n'est pas divisible par p^5 puisque D^2 n'est divisible que par p^2 et a_1a_2 est divisible par p^4 ; ce cas est donc aussi exclus.

2.d. Il suffit de regrouper les résultats des 3 questions précédentes.

2.e. Soit c_3 (resp. c_4) le plus petit carré tel que c_3x_3 (resp. c_4x_4) soit entier. Soient $n = c_3c_4$, $a = \frac{d}{\delta}$, $b = \frac{d'}{\delta}$ et $c = \frac{e}{\delta}$. Alors a, b et c sont premiers dans leur ensemble et $\frac{na}{c} = \frac{nd}{e} = c_3x_3c_4x_4$ est entier ainsi que $\frac{nb}{c} = \frac{nd'}{e} = c_3(x_3 + D)c_4(x_4 + D)$. Il existe q, r, s entiers tels que l'on ait $qa + rb + sc = 1$, et $\frac{\delta c_3c_4}{e} = \frac{n}{c} = q\frac{na}{c} + r\frac{nb}{c} + sn$ est entier. Maintenant, un entier > 0 étant $\geqslant 1$, on a

$$\begin{aligned} h(P_3) + h(P_4) &= \log(c_3(x_3 + D)) + \log(c_4(x_4 + D)) \\ &= \log(c_3c_4) + \log\frac{d'}{e} = \log d' - \log\delta + \log\frac{\delta c_3c_4}{e} \geqslant \log d' - \log\delta. \end{aligned}$$

2.f. D'après la question **5** de la partie III, on a

$$\begin{aligned} x_3x_4 &= \left(\frac{x_1x_2 - D^2}{x_1 - x_2}\right)^2 = \left(\frac{a_1a_2 - D^2c_1c_2}{a_1c_2 - a_2c_1}\right)^2 \\ (x_3 + D)(x_4 + D) &= \left(\frac{a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2}{a_1c_2 - a_2c_1}\right)^2 \end{aligned}$$

On peut utiliser la question précédente avec $d = (a_1a_2 - \mathrm{D}^2c_1c_2)^2$, $d' = (a_1a_2 + \mathrm{D}(a_1c_2 + a_2c_1) - \mathrm{D}^2c_1c_2)^2$ et $e = (a_1c_2 - a_2c_1)^2$. La question **2.c.** montre que le p.g.c.d. δ de d, d' et e divise $(2\mathrm{D})^3$; on a donc

$$h(\mathrm{P}_3) + h(\mathrm{P}_4) \geqslant 2\log(a_1a_2 + \mathrm{D}(a_1c_2 + a_2c_1) - \mathrm{D}^2c_1c_2) - \log(2\mathrm{D})^3.$$

Par ailleurs, on a

$$\begin{aligned} a_1a_2 + \mathrm{D}(a_1c_2 + a_2c_1) - \mathrm{D}^2c_1c_2 =& (a_1 + \mathrm{D}c_1)(a_2 + \mathrm{D}c_2) - 2\mathrm{D}^2c_1c_2 \\ =& (a_1 + \mathrm{D}c_1)(a_2 + \mathrm{D}c_2)\Big(1 - \frac{2\mathrm{D}^2}{(x_1 + \mathrm{D})(x_2 + \mathrm{D})}\Big), \end{aligned}$$

et comme $x_1 \geqslant \mathrm{D}$ et $x_2 \geqslant \mathrm{D}$, on obtient

$$a_1a_2 + \mathrm{D}(a_1c_2 + a_2c_1) - \mathrm{D}^2c_1c_2 \geqslant \frac{1}{2}(a_1 + \mathrm{D}c_1)(a_2 + \mathrm{D}c_2),$$

et donc

$$h(\mathrm{P}_3) + h(\mathrm{P}_4) \geqslant 2\log(\frac{1}{2}(a_1 + \mathrm{D}c_1)(a_2 + \mathrm{D}c_2)) - \log(2\mathrm{D})^3 \geqslant 2(h(\mathrm{P}_1) + h(\mathrm{P}_2)) - \log(32\,\mathrm{D}^3).$$

3.a. Il suffit de regarder les formules de la question **2.a** de la partie III.

3.b. Si $\mathrm{P} = \infty$ ou si $\mathrm{P} = (0, \mathrm{D})$, le résultat est évident. Sinon, choisisons $\mathrm{Q} \notin \{\mathrm{P}, -\mathrm{P}, \infty, (0, \mathrm{D})\}$. On a, en utilisant deux fois la question **2.f.**, la première fois avec $\mathrm{P}_1 = \mathrm{P} + \mathrm{Q}$ et $\mathrm{P}_2 = \mathrm{P} - \mathrm{Q}$,

$$h(2\mathrm{P}) + h(2\mathrm{Q}) \geqslant 2(h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q})) - 2\log(2(2\mathrm{D})^3) \geqslant 4(h(\mathrm{P}) + h(\mathrm{Q})) - 6\log(2(2\mathrm{D})^3),$$

et on conclut en utilisant l'inégalité $4h(\mathrm{Q}) \geqslant h(2\mathrm{Q})$ de la question **1**.

3.c. Si $\mathrm{P} = \infty$ ou $\mathrm{Q} = \infty$, on peut prendre $\mathrm{A} = 0$. Si $\mathrm{P} = \mathrm{Q}$ ou $\mathrm{P} = -\mathrm{Q}$, on peut prendre $\mathrm{A} = 6\log(2(2\mathrm{D})^3)$ d'après la question précédente et si $\mathrm{P} \neq \pm\mathrm{Q}$ et $(\mathrm{P}, \mathrm{Q}) \in \mathrm{C}(\mathbf{Q})$, on peut prendre $\mathrm{A} = \log(2(2\mathrm{D})^3)$ d'après la question **2.f.** Finalement, $\mathrm{A} = 6\log(2(2\mathrm{D})^3)$ marche dans tous les cas.

3.d. En utilisant la question précédente pour $\mathrm{P} + \mathrm{Q}$ et $\mathrm{P} - \mathrm{Q}$, on en déduit la minoration $h(2\mathrm{P}) + h(2\mathrm{Q}) \geqslant 2(h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q})) - \mathrm{A}$, et comme $h(2\mathrm{P}) \leqslant 4h(\mathrm{P})$ et $h(2\mathrm{Q}) \leqslant 4h(\mathrm{Q})$ d'après la question **1**, on obtient $h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q}) \leqslant 2h(\mathrm{P}) + 2h(\mathrm{Q}) + \frac{\mathrm{A}}{2}$. Donc finalement, on a, quel que soit $(\mathrm{P}, \mathrm{Q}) \in \overline{\mathrm{C}}(\mathbf{Q})^2$,

$$|h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q}) - 2h(\mathrm{P}) - 2h(\mathrm{Q})| \leqslant \mathrm{A}.$$

3.e. Soit $\mathrm{B} > 0$. Si $h(\mathrm{P}) \leqslant \mathrm{B}$, on a soit $\mathrm{P} = \infty$, soit il existe des entiers positifs a et c vérifiant $a + \mathrm{D}c \leqslant e^{\mathrm{B}}$ tel que $\mathrm{P} = (\frac{a}{c}, y)$. Comme l'ensemble de ces couples d'entiers est fini et que pour chaque valeur de x, il y a au plus deux valeurs de y possibles, l'ensemble des P vérifiant $h(\mathrm{P}) \leqslant \mathrm{B}$ est fini quel que soit $\mathrm{B} > 0$.

3.f. Le groupe $\overline{\mathrm{C}}(\mathbf{Q})$ est de type fini modulo 2 d'après la question **3.d** de la partie IV.A et possède une hauteur admissible ; on peut donc utiliser les résultats de la question **3.e** de la partie I.

INDEX

Index terminologique

Énoncés mathématiques

Index des noms propres

Repères chronologiques