

Master-1 de mathématiques (MAlg 1), 2004/2005 module MAlg 1 "Algèbre" (Master-1, MAT 401i)

A. A. Pantchichkine*

Institut Fourier, B.P.74, 38402 St.-Martin d'Hères, FRANCE
e-mail : panchish@mozart.ujf-grenoble.fr, FAX : 33 (0) 4 76 51 44 78

Résumé

Mon cours porte sur les fondements algébriques nécessaires pour la poursuite d'études en **M2P "CRYPTOLOGIE, SÉCURITÉ ET CODAGE D'INFORMATION"** (mais aussi souhaitables pour **M2R**, dans la géométrie algébrique et la théorie des nombres).

Il s'agit premièrement des outils d'algèbre commutative : *anneaux, corps, polynômes* utilisés en
– théorie des codes-correcteurs d'erreurs
– cryptologie à clef publique.

Il existe une analogie profonde entre l'ensemble \mathbb{Z} des nombres entiers et l'ensemble des polynômes $\mathbb{Q}[x]$ à coefficients dans l'ensemble \mathbb{Q} des nombres rationnels (ou l'ensemble des polynômes $\mathbb{K}[x]$ à coefficients dans un corps \mathbb{K}). En effet, tous les deux ensembles sont des *anneaux* avec une division euclidienne (division avec reste).

Il est utile d'étudier la divisibilité des polynômes de point de vue de divisibilité des nombres, et réciproquement, on expliquera dans le cours comment on peut voir les nombres comme un analogue des fonctions. Dans le cours on développe systématiquement cette analogie : *le théorème chinois des restes* est analogue au *théorème de l'interpolation de Lagrange*, ce que permet d'effectuer *la multiplication rapide des polynômes*. Les *polynômes irréductibles* sont analogues des *nombres premiers*. *La théorie des corps finis* est entièrement basée sur cette analogie.

Vers la fin du cours on considère les systèmes algébriques sur \mathbb{Z} ou sur un corps fini vus comme des *variétés algébriques*.

Table des matières

I	Arithmétique élémentaire	6
1	Les entiers	6
1.1	Divisibilité des entiers. Lien de l'arithmétique avec l'algèbre et l'analyse.	6
1.2	Lien de l'arithmétique avec l'informatique et l'algorithmique.	9
1.3	Application à la multiplication rapide.	12
1.4	pgcd, ppcm	13
1.5	Congruences	19
2	Entiers modulo n	21
2.1	Relations d'équivalence et ensembles quotients	21
2.2	Arithmétique modulo n	21
2.3	Une procédure pour calcul de $a^m \bmod n$ en Maple	23
3	Rappels sur la notion de groupe, exemples	26
3.1	Structure de groupe	26
3.2	Exemple : éléments inversibles mod n	27
3.3	Sous-groupes	31
3.4	Classes à gauche, à droite	32
3.5	Sous-groupes distingués, groupes quotient	33
3.6	Ordre d'un élément, théorème de Lagrange	34
4	Rappels sur la notion d'anneau, exemples	36
4.1	Structure d'anneau et idéaux	36
4.2	Anneau quotient	37
4.3	Idéaux premiers	38
4.4	Divisibilité dans les anneaux	39
4.5	Anneaux euclidiens et anneaux principaux	40
4.6	Décomposition en facteurs premiers	42
5	Théorème des restes chinois	44
5.1	Théorème des restes dans les anneaux principaux	44
5.2	Application : éléments inversibles mod n	46
5.3	Application à la cryptographie : RSA	47
5.4	Principaux protocoles.	48
6	Primalité	52
6.1	$\mathbb{Z}/p\mathbb{Z}$ est un corps	53
6.2	Petit théorème de Fermat	53
6.3	Nombres pseudopremiers de Fermat	53
II	Polynômes et corps finis	56

7	Polynômes	56
7.1	Anneau de polynômes, division euclidienne	56
7.2	Division euclidienne sur les anneaux	57
7.3	Valeurs et racines d'un polynôme	58
7.4	Formule d'interpolation de Lagrange	61
7.5	Anneau de polynômes à plusieurs variables	62
8	Carrés dans $\mathbb{Z}/p\mathbb{Z}$	66
8.1	Racines primitives	66
8.2	Symbole de Legendre.	71
8.3	Congruence d'Euler	72
8.4	Lois de réciprocité de Gauss	73
8.5	Une démonstration élémentaire de la loi de réciprocité	74
8.6	Une démonstration de la loi de réciprocité utilisant sommes de Gauss	79
8.7	Nombres pseudopremiers d'Euler	81
8.8	Loi de réciprocité quadratique et tests de primalité.	83
9	Notions de corps et d'espace vectoriel, rappels et exemples	88
9.1	Corps des fractions	88
9.2	Caractéristique d'un corps, sous-corps premier	89
9.3	Modules et espaces vectoriels	89
9.4	Rappels sur les espaces vectoriels	90
9.5	Matrices de changement de bases	92
9.6	Caractères d'un groupe	93
10	Extensions.	95
10.1	Polynômes irréductibles.	95
10.2	Extensions, degré.	95
10.3	Eléments algébriques	96
10.4	Corps de rupture, corps de décomposition	97
10.5	Sous-groupes finis dans K^*	100
11	Morphisme de Frobenius, structure des corps finis	103
11.1	Structure	103
11.2	Polynômes sur les corps finis. Nombre de polynômes irréductibles	104
11.3	Construction d'isomorphismes à partir des polynômes irréductibles	110
11.4	Théorème de la base normale	111
12	Algorithme de factorisation de Berlekamp dans $\mathbb{F}_q[X]$	114
III	Equations algébriques et variétés affines	116
13	Equations algébriques et variétés affines	116
13.1	Systèmes algébriques	116
13.2	Variétés affines (préparation).	117
13.3	Résolution d'un système linéaire dans un anneau euclidien	118
13.4	Systèmes diophantiens linéaires.	120
13.5	Variétés algébriques (exemples)	123

13.6	Le principe de Minkowski–Hasse pour les formes quadratiques	128
13.7	Espace projectif \mathbb{P}^n , variétés algébriques	130
14	Courbes planes.	132
14.1	Courbes planes affines.	132
14.2	Courbes planes projectives.	132
14.3	Points singuliers.	133
14.4	Equations cubiques	134
14.5	Points des courbes algébriques sur les corps finis (exemples)	140
IV	Compléments et annexes	151
A	Annexe : Postulat de Bertrand (C.Moser)	151
A.1	Construction d’une table de nombres premiers.	154
B	Annexe : Factorisation des Polynômes (F. SERGERAERT)	157
B.1	Rappels sur les corps finis.	157
B.2	Bases de la méthode de Berlekamp	159
B.3	Trouver les facteurs irréductibles.	162
B.4	Factorisation des polynômes à coefficients entiers.	167
B.5	Lemme de Hensel.	170
C	Annexe : Systèmes linéaires dans $\mathbf{GF}(p^d)$ (F. SERGERAERT)	178
D	Exercices de préparation à l’examen	180
D.1	EXAMEN du lundi 6 septembre 2004, 9h à 12h, à l’Institut Fourier	180
D.2	EXAMEN du 27 janvier 2004, de 14h à 17h, à l’Institut Fourier	181

Certificat "Algèbre I" (MAT401i)

I. Arithmétique élémentaire

- Divisibilité des entiers, pgcd, ppcm, congruences
- Entiers modulo n , théorème des restes chinois
- $\mathbb{Z}/p\mathbb{Z}$ est un corps, petit théorème de Fermat
- Carrés dans $\mathbb{Z}/p\mathbb{Z}$, Symboles de Legendre et Jacobi, loi de réciprocité de Gauss
- Applications à la primalité

II. Corps finis et polynômes

- Rappels sur anneaux et corps, anneaux de polynômes
- Division euclidienne dans $\mathbb{K}[x]$, racines d'un polynôme, formule d'interpolation de Lagrange
- Polynômes irréductibles, extensions, degré, corps de rupture
- Sous-groupes finis dans \mathbb{K}^*
- Morphisme de Frobenius, structure des corps finis
- Algorithme de factorisation de Berlekamp dans $\mathbb{F}_p[x]$

III. Equations algébriques et variétés affines

- Solution d'un système linéaire sur les anneaux
- Solution d'un système algébrique et homomorphismes d'anneaux
- Variétés affines (exemples). Courbes planes, points singuliers
- Cubiques planes, lois de groupe, points rationnels sur des exemples

PRÉREQUIS : Le cours est accessible aux étudiants de Master 1 en Mathématiques et en Informatique. Tous les résultats des cours d'algèbre de L3 utilisés seront révisés. Le cours fournit en particulier le bagage algébrique nécessaire pour la spécialité *Cryptologie, Sécurité et Codage d'information* du Master 2e année.

REMARQUE : Nouveaux éléments par rapport aux cours d'algèbre de L3 :

- *aspects algorithmiques des opérations algébriques*
- *bases algébriques pour :*
 - cryptographie à clef publique
 - théorie des codes-correcteurs d'erreurs
- *Analogies entre les nombres et les polynômes. Equations algébriques et variétés affines.*

Cours N°1. Mercredi le 29 septembre 2004

(disponible sur : <http://www-fourier.ujf-grenoble.fr/~panchish>).

Première partie

Arithmétique élémentaire

1 Les entiers

1.1 Divisibilité des entiers. Lien de l'arithmétique avec l'algèbre et l'analyse.

NOTATIONS. On notera \mathbb{Z} l'ensemble des entiers relatifs, \mathbb{N} l'ensemble des nombres naturels, \mathbb{Q} l'ensemble des nombres rationnels, \mathbb{R} l'ensemble des nombres réels et \mathbb{C} l'ensemble des nombres complexes.

Si X est un ensemble, on note $\#X$ son cardinal :

$$\#X = \text{Card}(X) = |X|.$$

On écrit $|X| < \infty$, si X est un ensemble fini. Si a est un nombre réel, on note $|a| = \sup(a, -a)$ sa valeur absolue.

Donc,

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}, \quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

La notation \mathbb{Z} vient de l'allemand (“**Z**ahlen”) (depuis la 19^e siècle).

DÉFINITION 1.1.1 *Si a et b sont deux entiers relatifs, on dit que a divise b et on note $a|b$ s'il existe un entier relatif c tel que $b = ac$. On dit également que b est un multiple de a ou a un diviseur de b . On note $a\mathbb{Z}$ l'ensemble des multiples de a , donc $b \in a\mathbb{Z}$.*

Un nombre entier positif p est dit premier s'il est strictement supérieur à 1 et si ses seuls diviseurs positifs sont 1 et p .

On notera \mathcal{P} l'ensemble de tous les nombres premiers.

Un nombre entier positif n est dit composé s'il n'est pas premier.

Par exemple, $2 | 6$ et $389 | 97734562907$:

$$97734562907 = 389 \cdot 251245663 = 41 \cdot 193 \cdot 389 \cdot 31751.$$

Les nombres premiers sont

$$2, 3, 5, 7, 11, \dots, 41, \dots, 193, \dots, 389, \dots, 2003, \dots, 31751, \dots$$

et les nombres composés sont

$$4, 6, 8, 9, 10, 12, \dots, 666 = 2 \cdot 3^2 \cdot 37, \dots, 2001 = 3 \cdot 23 \cdot 29, \dots$$

(voir [Stein], Chap. 1).

L'existence d'une décomposition en produit de nombres premiers.

Maintenant supposons que n est tout entier positif. Alors, de même façon, n peut être écrit comme un produit des nombres premiers :

- Si n est premier, c'est fait.
- Si n est composé alors $n = ab$ avec $a, b < n$.

En utilisant raisonnement par récurrence, a, b sont tous les deux produits des nombres premiers, donc n est aussi un produit des nombres premiers. Ce résultat explique le terme *nombre premier* : tous les autres entiers positifs sont construites comme leurs produits.

Deux résultats de base de la théorie des nombres

(connues des cours de licence) disent :

- (1) L'ensemble \mathcal{P} de tous les nombres premiers est *infini*;
- (2) THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE :

Tout entier positif n se décompose de façon unique sous la forme

$$m = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} \text{ avec } p_i \in \mathcal{P}, p_1 < p_2 < \dots < p_t, k_i \in \mathbb{N}$$

Le premier résultat se démontre par l'absurde : si l'on avait $\mathcal{P} = \{p_1, p_2, \dots, p_n\}$, on considèrerait $q = 1 + p_1 p_2 \dots p_n$. Alors, $q \notin \mathcal{P}$ par l'hypothèse, mais aucun p_i ne divise q , contradiction avec ce qui précède.

On rappellera une démonstration du deuxième résultat plus tard, sous une forme plus générale (pour tous les anneaux euclidiens).

Rappelons quelques propriétés de base de la divisibilité :

PROPOSITION 1.1.2 Si a, b, c sont des entiers relatifs, on a

- (i) $a|a$
- (ii) si $a|b$ et $b|c$, alors $a|c$
- (iii) si $a|b$ et $a|c$, alors $a|b + c$

DÉFINITION 1.1.3 Si b est un entier relatif non nul, et si a est un entier relatif il existe une unique paire (q, r) d'entiers relatifs tels que $a = bq + r$ avec $0 \leq r < |b|$. L'entier q est appelé le quotient de a par b , et r le reste de la division, on le notera ici $a \% b$ (ou $a \bmod b$).

EXERCICE 1.1.4 Démontrer en détails Proposition 1.1.2

Lien de l'arithmétique avec l'algèbre et l'analyse. Analogies entre nombres et fonctions.

L'ensemble \mathbb{Z} est un *anneau commutatif* : il existe deux opérations suivantes : pour tous paires $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ on a

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z}, (a, b) &\mapsto c = a + b \in \mathbb{Z} \quad (\text{"addition"}); \\ \times : \mathbb{Z} \times \mathbb{Z}, (a, b) &\mapsto d = a \times b = a \cdot b \in \mathbb{Z} \quad (\text{"multiplication"}); \end{aligned}$$

avec les propriétés des axiomes d'anneaux (commutativité et associativité de $+$ et de \times , distributivité $a(b_1 + b_2) = ab_1 + ab_2$, l'existence de 0 et de 1, l'existence d'un (unique) élément opposé $-a \in \mathbb{Z}$ à tout $a \in \mathbb{Z}$.

L'anneau des nombres entiers \mathbb{Z} est un objet algébrique fondamental, aussi bien que l'anneau $\mathbb{R}[X]$ ($\mathbb{C}[X]$) des polynômes à coefficients réels (complexes). Ces deux anneaux sont commutatifs, associatifs unitaires sans diviseurs de zéro. Il est commode d'exprimer la notion de divisibilité dans un anneau R ci-dessus à l'aide de la notion d'*idéal* :

rappelons qu'un idéal I de R est une partie de R qui est fermée par rapport aux opérations : pour tous $a, b \in I$

l'*addition* $a + b \in I$, *passage à l'opposé*, $a \mapsto -a$, et la *multiplication externe* par tout élément x de R : $a \mapsto ax$.

Tout élément $a \in R$ définit l'idéal $I = (a) = \{ax \mid x \in R\}$, et l'affirmation " a divise b " est équivalent à " $b \in (a)$ ".

Un idéal de type (a) est appelé idéal *principal*, et on rappellera que les anneaux $R = \mathbb{Z}, \mathbb{R}[X], \mathbb{C}[X]$ sont principaux, c'est à dire, tous ces idéaux sont *principaux*.

La démonstration de ce fait est la même pour les nombres et pour les polynômes : pour un idéal I quelconque on effectue la division avec reste par un élément non nul de I avec la plus petite valeur absolue (le plus petit degré respectivement), et la définition d'idéal implique que le reste doit être zéro.

On verra que le théorème de l'existence et de l'unicité de décomposition en facteurs irréductibles est valable dans tout anneau principal.

EXEMPLE 1.1.5 *L'unicité dans la deuxième propriété n'est pas toujours valable même si l'existence d'une décomposition en éléments premiers a lieu. Un exemple connu est donné par l'anneau $\mathbb{Z}[\sqrt{-5}]$ dans lequel il existe essentiellement différentes factorisations en éléments premiers :*

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

EXEMPLE. PROBLÈME DE FERMAT. Pierre de Fermat (1601–1665) a soulevé son problème célèbre (c.1637) dans la marge d'une traduction des "Arithmétiques" de Diophante :

"Décomposer un cube en deux autres cubes, une quatrième puissance, et généralement, une puissance quelconque, en deux puissances de même nom au-dessus de la seconde puissance, est une chose impossible et j'en ai assurément trouvé l'admirable démonstration. La marge trop exigüe ne la contiendrait pas".

En langage moderne :

$$\text{pour } n > 2 \quad \begin{cases} x^n + y^n = z^n \\ x, y, z \in \mathbb{Z} \end{cases} \implies xyz = 0 \quad (FLT(n))$$

("Fermat's Last Theorem").

Le 11 mars 1847 G.Lamé informait l'Académie des Sciences de Paris d'une démonstration complète à la base de l'identité

$$x^p + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1}y), \quad \zeta = \zeta_p = \exp(2\pi i/p), p \neq 2$$

admettant la factorialité de l'anneau $\mathbb{Z}[\zeta_p]$ (c'est à dire, que la décomposition en facteurs premiers dans cet anneau soit unique).

Immédiatement J.Liouville dit : "N'y a-t-il pas là une lacune à remplir ?" (et dans quelques mois A.Cauchy publia une note sur la non-factorialité de $\mathbb{Z}[\zeta_{23}]$).

L'idée de divisibilité dans les anneaux a beaucoup influencé la théorie des nombres.

Nombres comme analogues des fonctions

L'opération de division avec reste permet de voir tout nombre entier a comme une fonction

$$f_a : \mathcal{P} \rightarrow \mathbb{N}, \quad p \mapsto a \% p = a \bmod p. \quad (1.1)$$

EXEMPLE 1.1.6

$$\begin{aligned} f_{20}(3) = 2, f_{20}(7) = 6, f_{20}(2) = 0, f_{20}(5) = 0, f_{20}(257) = 20 \\ f_{-1}(3) = 2, f_{-1}(7) = 6, f_{-1}(2) = 1, f_{-1}(5) = 4, f_{-1}(257) = 256 \end{aligned}$$

Ceci dit, les fonctions f_{20} et f_{-1} prennent les mêmes valeurs en $p = 3$ et $p = 7$. La fonction f_{20} possède "un zéro double" en $p = 2$, car $20 = 2^2 \cdot 5$, tandis que la fonction f_{-1} n'a pas de zéros.

EXERCICE 1.1.7 Montrer que si n est premier alors la fonction f_n ne s'annule qu'en un seul point. L'affirmation réciproque est-elle vraie ?

EXERCICE 1.1.8 Dessiner la fonction f_6 .

EXERCICE 1.1.9 Montrer que tout nombre entier a est déterminé par la fonction correspondante f_a

Cette idée a été généralisé par A.Grothendieck pour tout anneau commutatif.

1.2 Lien de l'arithmétique avec l'informatique et l'algorithmique.

Ecriture en base $m \in \mathbb{N}$.

Pour effectuer les opérations algébriques dans \mathbb{Z} on utilise un système de numération de la base $m \in \mathbb{N}$: la notation

$$d = (d_{k-1}, d_{k-2}, \dots, d_1, d_0)_m$$

signifie que $d = d_{k-1}m^{k-1} + \dots + d_0$ avec des chiffres $d_i \in \{0, 1, \dots, m-1\}$. Le nombre de chiffres d_i utilisés pour cela est égale à $\lceil \log_m n \rceil + 1$. Une méthode commode utilisée par les ordinateurs correspond à $m = 2$, et on appelle le système de numération binaire (de la base 2). Le chiffre (digit) binaire (c'est à dire 0 ou 1) s'appelle "bit" (en anglais "bit" est une abréviation de "binary digit").

L'analyse simple des algorithmes "scolaires" pour l'addition et pour la multiplication montre que pour l'addition de deux nombres écrits avec k et l bit, $k \geq l$, on a besoin de k opérations booléennes (bit-opérations) qui se réduisent à l'addition des chiffres correspondants, (avec mémorisation et transfert du chiffre 1 à la position précédente dans le cas "1 + 1").

EXEMPLE 1.2.1

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & 1 & & 1 & & 1 & & 1 \\
 & 1 & 1 & 1 & 1 & 0 & 0 & 0_{(2)} \\
 + & 0 & 0 & 1 & 1 & 1 & 1 & 0_{(2)} \\
 & - & - & - & - & - & - & - \\
 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0_{(2)}
 \end{array}
 & (120 + 30 = 150)
 \end{array}$$

Dans cet exemple $(1111000)_2 = 8 \cdot 15 = 120$, $(0011110)_2 = 2 \cdot 15 = 30$.

On voit que pour la multiplication des nombres à k et l chiffres on a besoin de $2kl$ bit-opérations.

EXEMPLE 1.2.2

$$\begin{array}{r}
 \begin{array}{cccccccc}
 & & & & 1 & 1 & 0 & 1_{(2)} \\
 \times & & & & & 1 & 1 & 1_{(2)} \\
 & - & - & - & - & - & - & - \\
 & & & & 1 & 1 & 0 & 1 & - \\
 & & & & 1 & 1 & 0 & 1 & \\
 + & 1 & 1 & 0 & 1 & & & & \\
 & - & - & - & - & - & - & - & - \\
 1 & 0 & 1 & 1 & 0 & 1 & 1_{(2)} & - &
 \end{array}
 & (13 \times 7 = 91).
 \end{array}$$

Le nombre de bit-opérations nécessaires pour l'exécution d'un algorithme caractérise essentiellement *le temps d'exécution*.

Passage d'un système de numération à un autre.

Le temps nécessaire pour passer de la forme binaire d'un nombre n vers la forme de la base m est facile à estimer par $\mathcal{O}(k^2l)$ car on a besoin pour cela de $\mathcal{O}(k)$ divisions avec reste, avec pour chaque division $\mathcal{O}(kl)$ bit-opérations ("division en colonne") où l est le nombre de bit dans l'écriture de m , k est le nombre de bit dans l'écriture de n .

Ces méthodes d'addition, de multiplication, de division avec reste, de passage d'une forme d'écriture à une autre donnent des exemples d'algorithmes. On va appeler *algorithme* une procédure de calcul décrite pas par pas. On appelle *algorithme polynômial* de calcul sur des nombres naturels n_1, n_2, \dots, n_r , décrits à l'aide de k_1, k_2, \dots, k_r bit respectivement, un algorithme avec le temps d'exécution inférieur ou égal à $\mathcal{O}(k_1^{d_1} k_2^{d_2} \dots k_r^{d_r})$ (pour des constantes $d_1, d_2, \dots, d_r \in \mathbb{N}$).

Dans ce qui suit on va donner d'autres exemples des algorithmes polynômiaux : exponentiation modulo un nombre naturel fixé, algorithme d'Euclide.



Factorisation des nombres.

Soit $n = 1275$, et remarquons que $17 \mid 1275$, alors n est certainement composé, $n = 17 \cdot 75$. Puis, 75 est $5 \cdot 15 = 5 \cdot 5 \cdot 3$. Donc finalement, $1275 = 3 \cdot 5 \cdot 5 \cdot 17$.

Remarquer qu'on peut agir différemment pour factoriser le nombre 1275, par exemple $1275 = 5 \cdot 255$. On obtient $255 = 5 \cdot 51$ et $51 = 17 \cdot 3$, donc le résultat final est le même. Le résultat sur l'unicité ci-dessus dis que c'est toujours le cas.

Un défi (“challenge”) à \$10,000

Dès mois de février 2002, si vous arrivez à factoriser le nombre suivant de 174-chiffres décimales, connu sous le nom “RSA-576”, alors la compagnie RSA vous payera DIX MILLE DOLLARS!

1881988129206079638386972394616504398071635633794173827007
6335642298885971523466548531906060650474304531738801130339
6716199692321205734031879550656996221305168759307650257059

Ce nombre est appelé RSA-576, car il possède 576 chiffres binaires. Voir [Stein], Chap. 1, et

<http://www.rsasecurity.com/rsalabs/challenges/factoring/index.html>

pour les détails (il y a même un défi à \$200,000).

1.3 Application à la multiplication rapide.

Il est clair, que les opérations algébriques (l’addition, la multiplication, l’exponentiation) dans les anneaux sont très importantes; c’est pourquoi on va considérer des méthodes commodes pour effectuer ces opérations.

Soit m un entier strictement positif. Alors on peut voir l’écriture en base m d’un entier positif

$$n = (c_{k-1} \cdots c_1 c_0)_m$$

(i.e.

$$n = \sum_{i=0}^{k-1} c_i m^i \text{ avec } 0 \leq c_i \leq m-1$$

comme un analogue d’un polynôme $g_n(x) = \sum_{i=0}^r c_i x^i$ parce que $n = g(m)$. Pour multiplier deux nombres n et $n' = \sum_{i=0}^r c'_i x^i$ on peut utiliser une *multiplication rapide* des polynômes : $g_{n'}(x) = \sum_{i=0}^r c'_i x^i$, $n' = g_{n'}(m)$, alors

$$nn' = g_n(m)g_{n'}(m) = (g_n g_{n'})(m).$$

Un exemple modèle pour la multiplication rapide des nombres et des polynômes est donné par la règle :

$$\boxed{(ax + b)(cx + d) = ac(x^2 + x) + (b - a)(c - d)x + bd(x + 1)} \quad (1.2)$$

donc la multiplication des polynômes de degré ≤ 1 nécessite seulement 3 multiplications essentiels au lieu de 4 multiplications par la méthode traditionnelle. On utilise cette règle avec $x = 2^l$.

Rapellons que l’algorithme traditionnel pour la multiplication de deux nombres de $\leq k$ chiffres binaires ($m = 2$) nécessite $\leq k^2$ opérations élémentaires (de type $1_2 + 1_2 = 10_2$).

La règle (1.2) amène à un algorithme rapide de multiplication dont le temps d’exécution est majoré par $\mathcal{O}(k^{\log_2 3})$.

REMARQUE. Rappelons que la *méthode de Hörner* permet de trouver facilement la valeur $n = \sum_{i=0}^r c_i m^i$.

On considère le polynôme

$$f(x) = g_n(x) = \sum_{i=0}^r c_i x^i, \text{ et } x = m \text{ on calcule } g_n(m) \text{ de façon suivante : soient}$$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0, \quad a_n \neq 0$$

un polynôme, et on cherche un autre polynôme

$$q(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \dots + b_0, \quad b_{n-1} \neq 0$$

tel que

$$f(x) = (x - c)q(x) + r,$$

En comparant les coefficients des puissances de x on obtient

$$\begin{aligned} a_n &= b_{n-1}, \quad a_{n-2} = b_{n-2} - c b_{n-1}, \quad \dots, \quad a_1 = b_0 - c b_1, \quad a_0 = r - c b_0, \quad r = f(c) \\ \implies b_{n-1} &= a_n, \quad b_{n-k} = c b_{n-k+1} + a_{n-k} \quad (k = 2, \dots, n) \end{aligned}$$



Il est commode de faire le tableau suivant (le schéma de Hörner)

	a_n	a_{n-1}	\dots	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = c b_{n-1} + a_{n-1}$	\dots	$b_0 = c b_1 + a_1$	$f(c) = c b_0 + a_0$

En particulier, pour un nombre $n = \sum_{i=0}^r c_i m^i$ on considère le polynôme

$$f(x) = g_n(x) = \sum_{i=0}^r c_i x^i, \text{ et } x = m \text{ on obtient}$$

	c_r	c_{r-1}	\dots	c_1	c_0
m	$b_{r-1} = c_r$	$b_{r-2} = m b_{r-1} + c_{r-1}$	\dots	$b_0 = m b_1 + c_1$	$g_n(m) = m b_0 + c_0$

1.4 pgcd, ppcm

DÉFINITION 1.4.1 Soit I un ensemble et $(a_i)_{i \in I}$ une famille d'entiers.

(i) On dit que $d \in \mathbb{N}$ est un pgcd de la famille $(a_i)_{i \in I}$ si

$$\forall (i \in I, d | a_i) \text{ et } \forall r \in \mathbb{Z}, \forall (i \in I, r | a_i) \implies r | d$$

(ii) On dit que $m \in \mathbb{N}$ est un ppcm de la famille $(a_i)_{i \in I}$ si

$$\forall (i \in I, a_i | m) \text{ et } \forall r \in \mathbb{Z}, \forall (i \in I, a_i | r) \Rightarrow m | r$$

NOTATIONS. $r = \text{pgcd}((a_i)_{i \in I})$, $m = \text{ppcm}((a_i)_{i \in I})$.

REMARQUE.

Si $I = \emptyset$, alors le pgcd vaut 0 et ppcm vaut 1. Si $I = \{0\}$ et $a_0 > 0$, alors le pgcd et ppcm coïncident avec a_0 .

Cours N°2. Mercredi le 6 octobre 2004

Algorithme d'Euclide pour le calcul de pgcd

Pour des entiers a, b on écrit $a|b$ si a divise b , c'est à dire, que $b = ad$ pour un entier d . Si p est premier et p^α le plus grande puissance de p divisant n on écrit $p^\alpha || n$ et $\alpha = \text{ord}_p n$. Le théorème de factorisation peut être facilement déduit de son cas particulier : si un nombre premier p divise ab alors soit $p|a$ soit $p|b$. Cette propriété découle de l'algorithme d'Euclide.

Si l'on connaît les factorisations de a et b en produit de nombres premiers on voit directement l'existence et la forme explicite du plus grand commun diviseur (notation : $\text{pgcd}(a, b)$) et du plus petit commun multiple (notation $\text{ppcm}(a, b)$). Notamment, posons $m_p = \min(\text{ord}_p(a), \text{ord}_p(b))$, $g_p = \max(\text{ord}_p(a), \text{ord}_p(b))$. Alors

$$\text{pgcd}(a, b) = \prod_p p^{m_p}, \quad \text{ppcm}(a, b) = \prod_p p^{g_p}.$$

Un fait surprenant est qu'on peut calculer facilement le pgcd, par exemple $\text{pgcd}(2261, 1275)$, sans utiliser la factorisation. Plus précisément :

$$2261 = 1 \cdot 1275 + 986.$$

On remarque que si un nombre d divise 2261 et 1275, alors d divise automatiquement leur différence 986.

De même façon, si un nombre divise les deux 1275 et 986, alors il divise aussi leur somme 2261. Donc on progresse :

$$\text{pgcd}(2261, 1275) = \text{pgcd}(1275, 986).$$

Essayons encore :

$$1275 = 1 \cdot 986 + 289,$$

donc $\text{pgcd}(1275, 986) = \text{pgcd}(986, 289)$:

$$986 = 3 \cdot 289 + 119$$

$$289 = 2 \cdot 119 + 51$$

$$119 = 2 \cdot 51 + 17.$$

Ceci dit, $\text{pgcd}(2261, 1275) = \dots = \text{pgcd}(51, 17)$, i.e. 17 car $17 | 51$, et

$$\text{pgcd}(2261, 1275) = 17.$$

Cette méthode est très efficace et elle donne l'algorithme classique suivant :

Algorithme d'Euclide :

On fix $a, b \in \mathbb{N}$ avec $a > b$. En utilisant "division avec reste" (division euclidienne), on écrit

$$a = bq + r, \text{ avec } 0 \leq r < b. \tag{1.3}$$

Alors, comme ci-dessus,

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

On pose $a_1 = b$, $b_1 = r$, et on répète jusqu'à $r = 0$. On calcule assez rapidement $\text{pgcd}(a, b)$. L'algorithme d'Euclide se compose donc du calcul d'une suite

$$d_0, \quad d_1, \quad d_2, \dots$$

où $d_0 = a$, $d_1 = b$ et d_{i+1} est le résidu de d_{i-1} modulo d_i :

$$d_{i+1} = d_{i-1} - td_i.$$

On s'arrête lorsque $d_k = 0$; alors $d_{k-1} = \text{pgcd}(a, b)$. On peut montrer (en exercice) que le nombre des divisions est borné par $5 \log_{10} \max(a, b)$ (le théorème de Lamé).

THÉORÈME 1.4.2 *Soit $a, b \in \mathbb{N}$ des entiers positifs. Alors il existe $\text{pgcd}(a, b)$.*

PREUVE. On observe simplement que $d = d_{k-1} = \text{pgcd}(a, b)$ satisfait les conditions de définition 1.4.1.

EXEMPLE. On pose $a = 15$ et $b = 6$.

$$\begin{array}{ll} 15 &= 6 \cdot 2 + 3 & \text{pgcd}(15, 6) = \text{pgcd}(6, 3) \\ 6 &= 3 \cdot 2 + 0 & \text{pgcd}(6, 3) = \text{pgcd}(3, 0) = 3 \end{array}$$

EXEMPLE. Soit $a = 150$ et $b = 60$.

$$\begin{array}{ll} 150 &= 60 \cdot 2 + 30 & \text{pgcd}(150, 60) = \text{pgcd}(60, 30) \\ 60 &= 30 \cdot 2 + 0 & \text{pgcd}(60, 30) = \text{pgcd}(30, 0) = 30 \end{array}$$

Avec l'algorithme d'Euclide on va prouver maintenant que si un nombre premier divise le produit de deux nombres entiers, alors il divise l'un d'eux. Ce résultat est la clé pour prouver l'unicité de factorisation.

THÉORÈME 1.4.3 (LEMME D'EUCLIDE) *Soit p un nombre premier et $a, b \in \mathbb{N}$ des entiers positifs. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.*

PREUVE. Si $p \mid a$, c'est fait. Si $p \nmid a$ alors $\text{pgcd}(p, a) = 1$, car seulement 1 et p divisent p . A partir de l'algorithme d'Euclide, on voit $\text{pgcd}(pb, ab) = b$. A chaque étape on multiplie l'équation par b . Comme $p \mid pb$ et, par l'hypothèse, $p \mid ab$, on obtient que $p \mid \text{pgcd}(pb, ab) = b$.

COROLLAIRE 1.4.4 *Soit p un nombre premier, $s \in \mathbb{N}$, et $a_1, \dots, a_s \in \mathbb{N}$ des entiers positifs. Si $p \mid a_1 \dots a_s$ alors p divise l'un des a_i : $\exists p \mid a_i$.*

Unicité de décomposition

d'un entier positif n en produit de nombres premiers est directement impliquée par le Lemme d'Euclide 1.4.3 (et son corollaire 1.4.4) : soient $r, s \in \mathbb{N}$, p_1, \dots, p_r et q_1, \dots, q_s des nombres premiers tels que

$$n = p_1 \dots p_r = q_1 \dots q_s$$

alors $r = s$ et p_1, \dots, p_r coïncident q_1, \dots, q_s à une permutation près.

En effet, on peut supposer $r \geq s$. On procède par récurrence sur r . Si $r=0$, alors $n=1$, $s = 0$, et le résultat annoncé est vrai. Supposons le résultat montré pour $r - 1$ avec $r \geq 1$. On a

$$p_1 | q_1 \dots q_s.$$

Donc p_1 divise l'un des q_i .

Quitte à échanger les q_i , on peut supposer que $p_1 | q_1$. Comme le nombre q_1 est premier, on obtient $p_1 = q_1 = 1$, d'où

$$p_2 \dots p_r = q_2 \dots q_s$$

(après la simplification), et il reste à appliquer l'hypothèse de récurrence au produit $p_2 \dots p_r$ de $r - 1$ nombres premiers.

EXERCICE 1.4.5 *Montrer que si $a_1, a_2 > 0$,*

$$\text{pgcd}(a_1, a_2) \cdot \text{ppcm}(a_1, a_2) = a_1 \cdot a_2$$

EXERCICE 1.4.6 *Algorithmes pour calculer le pgcd d'une famille finie $\{a_1, \dots, a_r\}$. Montrer par récurrence que*

$$\text{pgcd}(a_1, \dots, a_r) = \text{pgcd}(\text{pgcd}(a_1, \dots, a_{r-1}), a_r),$$

et que

$$\text{ppcm}(a_1, \dots, a_r) = \text{ppcm}(\text{ppcm}(a_1, \dots, a_{r-1}), a_r),$$

Programme pour trouver le pgcd (en Maple), disponible à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-2pgcd (Tue Oct 05 20 :08 :13 2004))

Pour travailler avec ce fichier, on peut : 1) l'ouvrir avec Netscape, 2) enregistrer sous... comme un fichier .mws, 3) taper "xmaple" pour l'ouvrir avec Maple-7.

```
> restart;
> a:=691;
> b:=1000;
> i:=0;
> print('i'=i, 'a'=a, 'b'=b);
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> while(b<>0) do
> r:=irem( a,b );
> print('i'=i, 'a'=a, 'b'=b, 'r'=r):
> i:=i+1;
> a:=b;
> b:=r;
> od;
```

$i = 0, a = 691, b = -1000$
 $i = 0, a = 691, b = 1000, r = 691$
 $i = 1, a = 1000, b = 691, r = 309$
 $i = 2, a = 691, b = 309, r = 73$
 $i = 3, a = 309, b = 73, r = 17$
 $i = 4, a = 73, b = 17, r = 5$
 $i = 5, a = 17, b = 5, r = 2$
 $i = 6, a = 5, b = 2, r = 1$
 $i = 7, a = 2, b = 1, r = 0$

Une procedure pour trouver le pgcd (en Maple)

```
> pgcd:=proc(a::integer,b::integer)
> local r,d0,d1,i;
> i:=0;
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> r:=b;
> d0:=a; d1:=b;
> r:=b;
> while(d1<>0) do
> i:=i+1;
> r:=irem( d0,d1 );
> d0:=d1;
> d1:= r;
> od;
> return d0;
> end proc;
```

Exemples

```
> pgcd(12,14);
2
> pgcd(91,65);
13
> pgcd(2261,1275);
17
```

1.5 Congruences

DÉFINITION 1.5.1 Si a, b sont deux entiers relatifs, on dit que a est congru à b modulo m et on note

$$a \equiv b \pmod{m}$$

si et seulement si m divise $a - b$.

PROPOSITION 1.5.2 Si a, b, c, d, m et n sont des entiers relatifs,

- (i) $a \equiv a \pmod{m}$,
- (ii) si $a \equiv b \pmod{m}$, alors $b \equiv a \pmod{m}$,
- (iii) si $a \equiv b \pmod{m}$ et $b \equiv c \pmod{m}$, alors $a \equiv c \pmod{m}$,
- (iv) si m est non nul et si b est le reste de la division euclidienne de a par m , alors on a $a \equiv b \pmod{m}$,
- (v) si $a \equiv b \pmod{m}$ et si $n|m$, alors on a $a \equiv b \pmod{n}$,
- (vi) si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, alors $a + c \equiv b + d \pmod{m}$,
- (vii) si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, alors $ac \equiv bd \pmod{m}$,
- (viii) si $a \equiv b \pmod{m}$ et si n est un entier positif, alors $a^n \equiv b^n \pmod{m}$.

PREUVE. C'est un exercice facile. Montrons (vii) à titre d'exemple : si $a \equiv b \pmod{m}$, et $c \equiv d \pmod{m}$, alors il existe des entiers relatifs q_1 et q_2 tels que

$$a - b = mq_1 \text{ et } c - d = mq_2;$$

par conséquent,

$$ac - bd = (a - b)c + b(c - d) = m(q_1 + q_2);$$

d'où l'assertion.

EXEMPLE 1.5.3

Si a est entier positif ou nul et $a_r a_{r-1} \dots a_0$ son écriture en base 10 (i.e. $a = \sum_{i=0}^r a_i 10^i$), alors

- (i) $a \equiv a_0 \pmod{10}$,
- (ii) $a \equiv \sum_{i=0}^r a_i \pmod{9}$
- (iii) $a \equiv \sum_{i=0}^r (-1)^i a_i \pmod{11}$

Règles de divisibilité

PROPOSITION 1.5.4 Un nombre $n \in \mathbb{Z}$ est divisible par 3 si et seulement si la somme des chiffres décimaux de n est divisible par 3.

PREUVE. On écrit

$$n = a + 10b + 100c + \dots$$

Comme $10 \equiv 1 \pmod{3}$,

$$n = a + 10b + 100c + \dots \equiv a + b + c + \dots \pmod{3},$$

d'où la proposition.

De même façon, on trouve les règles de divisibilité par 5, 2, 4, 9 et 11 (voir exemple 1.5.3).

EXERCICE 1.5.5 Proposer une règle de divisibilité par 7, utilisant les faits $10 \equiv 3(\text{mod}7)$, $100 \equiv 2(\text{mod}7)$, $1000 \equiv -1(\text{mod}7)$.



EXERCICES

- 1.1 Proposer une règle de divisibilité par 13, en utilisant $1001 = 7 \cdot 11 \cdot 13$.
- 1.2 Calculer de tête le dernier chiffre de l'écriture en base 10 des nombres suivants : 2309786^{34657} , $8786652^{35444619}$ et $654565198^{3548217}$.
- 1.3 alculer de tête le reste de la division par 9 des nombres suivants : $8^{68498353}$, 54648381^{54648} et 354872846^{21353} .pey12
- 1.4 Existe-t-il des nombres entiers x, y tels que $x^2 + y^2 = 2003$?
- 1.5 Existe-t-il des nombres entiers x, y tels que $x^2 + 5y^2 = 2003$?
- 1.6 Soit b un entier strictement positif, énoncer et démontrer l'analogue de l'exemple 1.5.3 pour l'écriture en base b d'un entier positif a (i.e. $a = \sum_{i=0}^r a_i b^i$ avec $0 \leq a_i \leq b - 1$).
- 1.7 Trouver tous entiers n tels que la fonction f_n (definite par l'égalité(1.1)) ne s'annule pas.
- 1.8 Dessiner la fonction f_{15} .
- 1.9 La fonction f_n est-elle croissante (decroissante) ?
- 1.10 Trouver tous entiers x, y, z tels que

$$x^3 + 2y^3 + 4z^3 = 0.$$

- 1.11 Combien de zéros se trouvent à la fin de $20!$?
- 1.12 Montrer que si $2^p - 1$ est premier alors $2^{p-1}(2^p - 1)$ est *parfait*, c'est à dire, qu'il est égal à la somme de ses diviseurs propres (e.g. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$) (Euler a démontré que tous les nombres pairs parfaits sont de ce type).
- 1.13 Trouver une formule explicite pour les nombres de Fibonacci $a = u_k$, $b = u_{k-1}$ où $u_0 = u_1 = 1$ et $u_{i+1} = u_i + u_{i-1}$:

$$u_i = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{i+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{i+1} \right).$$

- 1.14 On définit le nombre d'or comme la solution positive de la proportion d'or

$$\frac{1}{x} = \frac{x}{1-x}$$

("le quotient de l'unité par une partie est égale au quotient de cette partie par la partie complémentaire"), c'est à dire, que $x = \frac{\sqrt{5}-1}{2}$. Montrer que

$$\frac{u_i}{u_{i+1}} \rightarrow \frac{2}{1 + \sqrt{5}} = \frac{\sqrt{5} - 1}{2}.$$

- 1.15 Soient a, k, l des nombres entiers positifs. Trouver

$$\text{pgcd}(a^k - 1, a^l - 1).$$

2 Entiers modulo n

2.1 Relations d'équivalence et ensembles quotients

La congruence est une relation d'équivalence. Rappelons ce dont il s'agit.

DÉFINITION 2.1.1 Une relation binaire \mathcal{R} sur un ensemble E est une partie

$$E_{\mathcal{R}} \subset E \times E = \{(a, b) \mid a, b \in E\}$$

on écrit $a \overset{\mathcal{R}}{\sim} b$ si et seulement si $(a, b) \in E_{\mathcal{R}}$

DÉFINITION 2.1.2 Une relation binaire \mathcal{R} sur un ensemble E est une relation d'équivalence si et seulement si elle vérifie les trois conditions suivantes :

- Réflexive. $\forall a \in E, a \overset{\mathcal{R}}{\sim} a$.
- Symétrique. Si a et b appartiennent à E et si $a \overset{\mathcal{R}}{\sim} b$, alors $b \overset{\mathcal{R}}{\sim} a$
- Transitivité. Si a, b et c appartiennent à E et si $a \overset{\mathcal{R}}{\sim} b$ et $b \overset{\mathcal{R}}{\sim} c$, alors $a \overset{\mathcal{R}}{\sim} c$

Pour tout x de E on appelle classe d'équivalence de x modulo \mathcal{R} , notée \bar{x} , la partie

$$\{y \in E \mid y \overset{\mathcal{R}}{\sim} x\}$$

de E . On dit également que x est un représentant de la classe d'équivalence \bar{x} .

L'ensemble des classes d'équivalence modulo \mathcal{R} est appelé ensemble-quotient de E par \mathcal{R} . On le note E/\mathcal{R} .

PROPOSITION 2.1.3 L'ensemble quotient E/\mathcal{R} forme une partition de E autrement dit aucune classe d'équivalence n'est vide et deux classes d'équivalence sont soit disjointes soit identiques.

DÉFINITION 2.1.4 L'application

$$E \rightarrow E/\mathcal{R}, x \mapsto \bar{x}$$

est surjective, on l'appelle la projection canonique.

2.2 Arithmétique modulo n

PROPOSITION 2.2.1 Pour tout entier n la relation de congruence $x \equiv y \pmod{n}$ est une relation d'équivalence sur \mathbb{Z} . On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient associé.

PREUVE. Il suffit d'utiliser les propriétés (i), (ii) et (iii) de Proposition 1.5.2. La propriété (iv) montre que

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{n-1} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup \dots \cup (n-1 + n\mathbb{Z})$$

On suppose $a, a', b, b' \in \mathbb{Z}$ et

$$a \equiv a' \pmod{n}, \quad b \equiv b' \pmod{n}.$$

Alors

$$a + b \equiv a' + b' \pmod{n} \quad (2.1)$$

$$a \cdot b \equiv a' \cdot b' \pmod{n} \quad (2.2)$$

Ceci permet de définir une addition $+$ et une multiplication \times (ou \cdot) sur $\mathbb{Z}/n\mathbb{Z}$ par les formules

$$\bar{a} + \bar{b} = \overline{a + b} \text{ et } \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Ceci implique que si $m > 0$ la puissance m -ème d'un élément a de $\mathbb{Z}/n\mathbb{Z}$ est donné par

$$\bar{a}^m = \overline{a^m}.$$

De point de vue pratique, ces calculs peuvent être implémentés de la façon suivante : pour l'addition

ALGORITHME 2.2.2

Entrée :

- Entier n de congruence.
- Entiers a et b (entre 0 et $n - 1$).

Sortie :

- Représentant de $a + b$ (entre 0 et $n - 1$).

Algorithme :

- Calculer $c = a + b$.
- Calculer le reste r de la division de c par n .

Un algorithme analogue peut être écrit pour la *multiplication*.

Pour l'*exponentiation*, il convient de minimiser le nombre de multiplications effectuées. L'idée pour cela est de considérer l'écriture en base 2 de la puissance cherchée :

$$m = \sum_{i=0}^r m_i 2^i \text{ avec } m_i = 0 \text{ ou } 1.$$

On a la relation

$$\bar{a}^m = \prod_{\substack{0 \leq i \leq r \\ m_i = 1}} \bar{a}^{2^i}.$$

La formule

$$m = m_r 2^r + \dots + m_0 = 2(2(\dots 2(2m_r + m_{r-1}) + \dots) + m_1) + m_0$$

montre que dans cet exemple

$$\begin{aligned} \bar{a}^m &= \bar{a}^{2(2(\dots 2(2m_r + m_{r-1}) + \dots) + m_1) + m_0} \\ &= (\dots ((\bar{a}^{m_r})^2 \bar{a}^{m_{r-1}})^2 \dots)^2 \bar{a}^{m_0} \end{aligned}$$

ALGORITHME 2.2.3

Entrée :

- Entier n de congruence.
- Puissance m .
- Element a de $\mathbb{Z}/n\mathbb{Z}$

Sortie :

- Valeur de a^m dans $\mathbb{Z}/n\mathbb{Z}$.

Algorithme :

1. $x := a, y = m$;
2. $z := 1$;
3. Tant que y n'est pas nul
 - 3.1 si y est impaire, $z := z * x \bmod n$
 - 3.2 $x := x * x \bmod n$
 - 3.3 $m := m/2$
4. renvoyer z

2.3 Une procédure pour calcul de $a^m \bmod n$ en Maple

On peut simplement utiliser

```
> a &^ m mod n;
```

Sinon, on écrit une procédure :

```
> Puismod:=  
> proc(a::nonnegint, m::nonnegint, n::nonnegint)  
> local x, y, z, mi;  
> x:=a;  
> y:=m;  
> z:=1;  
> while (y<>0) do  
> mi:=y mod 2;  
> if (mi=1) then z := z*x mod n;  
> else fi;  
> x:=x*x mod n;  
> y:=floor(y/2);  
> printf("mi=%d, x=%d, y=%d, z=%d\n",mi,x,y,z)  
> od;  
> return z;  
> end proc;
```

```

Puismod := proc(a : :nonnegint, m : :nonnegint, n : :nonnegint)
local x, y, z, mi;
  x := a;
  y := m;
  z := 1;
  while y ≠ 0 do
    mi := y mod 2;
    if mi = 1 then z := z * x mod n else end if;
    x := x2 mod n;
    y := floor(1/2 * y);
    printf("mi=%d, x=%d, y=%d, z=%d\n", mi, x, y, z)
  end do;
  return z
end proc
> Puismod(2,11,100);
mi=1, x=4, y=5, z=2
mi=1, x=16, y=2, z=8
mi=0, x=56, y=1, z=8
mi=1, x=36, y=0, z=48

```

48

vérification :

```
> 2^11;
```

2048

Simplification dans $\mathbb{Z}/n\mathbb{Z}$

PROPOSITION 2.3.1 Si $\text{pgcd}(c, n) = 1$ et

$$ac \equiv bc \pmod{n}$$

alors $a \equiv b \pmod{n}$.

PREUVE. Par définition

$$n \mid ac - bc = (a - b)c.$$

Comme $\text{pgcd}(n, c) = 1$, on a $n \mid a - b$, donc

$$a \equiv b \pmod{n},$$

d'où la proposition.

COROLLAIRE 2.3.2 Si $\text{pgcd}(c, n) = 1$ alors l'application $x \mapsto cx$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est bijective, en particulier, pour tout b dans $\mathbb{Z}/n\mathbb{Z}$ il existe un seul x dans $\mathbb{Z}/n\mathbb{Z}$ tel que

$$ax \equiv b \pmod{n}.$$

EXERCICES

2.1. Justifier une version de l'algorithme d'Euclide donnée par la division avec reste de plus petite valeur absolue :

$$\begin{aligned} x_0 &= a_0x_1 + \varepsilon_1x_2, \\ x_1 &= a_1x_2 + \varepsilon_2x_3, \dots, \quad 0 \leq x_k < x_{k-1}/2, \quad \varepsilon_i = \pm, \\ &\dots\dots\dots \\ x_{n-1} &= a_{n-1}x_n. \end{aligned}$$

2.2. Posons $D_0 = 0, D_1 = 1, \dots, D_n = 2D_{n-1} + D_{n-2}$. (la suite des nombres de Dupré). Démontrer : Théorème (Athanasie Dupré, 1846) Soient $u, v > 0$ des nombres naturels tels que l'algorithme d'Euclide marche pour n divisions (avec reste de plus petite valeur absolue), et u est minimal avec cette propriété. Alors

$$u = D_n + D_{n-1}, \quad v = D_n,$$

2.3. En déduire : Pour $(u, v), u > v > 0$, l'algorithme d'Euclide marche pour au plus

$$1, 14 \log u - 0, 79 + 0, 41u^{-1}$$

divisions avec reste de plus petite valeur absolue.

Solution : voir [Knu81], p. 605. On utilise ci-dessus la formule

$$D_n = \frac{1}{2\sqrt{2}} \left((1 + \sqrt{2})^n - (1 - \sqrt{2})^n \right).$$

3 Rappels sur la notion de groupe, exemples

3.1 Structure de groupe

DÉFINITION 3.1.1 Un groupe est un ensemble G muni d'une loi interne

$$G \times G \rightarrow G, \quad (x, y) \mapsto xy = x \cdot y$$

qui est associative

$$\text{Gr1 } \forall x, y, z \in G, x(yz) = (xy)z,$$

admet un élément neutre e :

$$\text{Gr2 } \forall x \in G, xe = ex = x,$$

et tout élément x du groupe G admet un inverse (ou symétrique) y :

$$\text{Gr3 } \forall x \in G, \exists y \in G, xy = yx = e,$$

cet élément est alors unique, on le note x^{-1} .



En outre le groupe G est dit commutatif ou abélien s'il vérifie également la condition suivante :

$$\text{Comm. } \forall x, y \in G, xy = yx.$$

REMARQUE 3.1.2 On prend souvent une notation additive pour la loi d'un groupe abélien, la loi s'écrira alors $(x, y) \mapsto x + y$, l'élément neutre sera noté 0 et le symétrique (ou opposé) d'un élément x sera noté $-x$.

EXEMPLE 3.1.3 L'ensemble \mathbb{Z} muni de l'addition est un groupe commutatif. Il est de même pour \mathbb{Q} , \mathbb{R} , \mathbb{C} muni de l'addition. L'addition muni également $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe abélien.



DÉFINITION 3.1.4 Un groupe G est dit monogène, s'il existe un élément g de G tel que $\{g\}$ engendrent G , i.e. pour tout $h \in G$ il existe un entier positif n tel que soit $h = g^n$ soit $h = g^{-n} = (g^{-1})^n$. On dit alors que g est un générateur de G . Un groupe monogène fini est dit cyclique.

En particulier, le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et de générateur $\bar{1}$:

$$\bar{1} + \bar{1} = \bar{2}, \bar{1} + \bar{1} + \bar{1} = \bar{3}, \dots$$

Le groupe additif \mathbb{Z} est monogène de générateur 1 (ou de générateur -1).

EXERCICE 3.1.5 Trouver tous les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$. Montrer qu'une classe $\bar{a} = a \pmod{n}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(a, n) = 1$.

(Utiliser le corollaire 2.3.2 pour montrer : $\text{pgcd}(a, n) = 1 \iff$ l'application $x \mapsto ax$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est bijective, en particulier, pour tout b dans $\mathbb{Z}/n\mathbb{Z}$ il existe un seul m dans $\mathbb{Z}/n\mathbb{Z}$ tel que

$$am \equiv b \pmod{n},$$

c'est à dire, que a est un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$.

EXEMPLE 3.1.6 Si X est un ensemble, l'ensemble des bijections de X dans X , aussi appelées permutations de X , forment un groupe pour la loi de composition que l'on note \mathfrak{S}_X . On note \mathfrak{S}_n pour le groupe des permutations de $\{1, \dots, n\}$. Si $n \geq 3$, alors ce groupe n'est pas abélien.

DÉFINITION 3.1.7

(a) Soient G et H deux groupes. Une application $\phi : G \rightarrow H$ est un morphisme de groupes si elle vérifie la condition

$$\text{Mor } \forall x, y \in G, \phi(xy) = \phi(x)\phi(y).$$

(b) Un isomorphisme de groupes est un morphisme de groupes qui est bijectif. Son inverse est alors un isomorphisme de groupes.

(c) Un automorphisme d'un groupe G est un isomorphisme de G dans G . Son inverse est alors un automorphisme de G .

EXERCICE 3.1.8 Trouver tous les morphismes du groupe $\mathbb{Z}/10\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.

EXERCICE 3.1.9 Trouver tous les automorphismes des groupes $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.

3.2 Exemple : éléments inversibles mod n .

Rapellons que pour un élément $a \text{ mod } n \in \mathbb{Z}/n\mathbb{Z}$ l'application $x \mapsto ax$ de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est bijective si et seulement si $\text{pgcd}(a, n) = 1$, en particulier, dans ce cas pour tout b dans $\mathbb{Z}/n\mathbb{Z}$ il existe un seul x dans $\mathbb{Z}/n\mathbb{Z}$ tel que

$$ax \equiv b \pmod{n}.$$

(voir Corollaire 2.3.2).

DÉFINITION 3.2.1 On appelle groupe d'éléments inversibles mod n l'ensemble d'éléments $a \text{ mod } n \in \mathbb{Z}/n\mathbb{Z}$ tels que $\text{pgcd}(a, n) = 1$, et on le note $(\mathbb{Z}/n\mathbb{Z})^\times$. L'élément neutre e de $(\mathbb{Z}/n\mathbb{Z})^\times$ est la classe $1 \text{ mod } n = 1 + n\mathbb{Z}$, et l'élément symétrique de $a \text{ mod } n$ est la classe $x \text{ mod } n$, où $ax \equiv 1 \pmod{n}$.

Pour trouver un élément x tel que $ax \equiv b \pmod{n}$, il suffit de résoudre l'équation $ax + ny = b$ en entiers x, y , on utilisera une information supplémentaire sur le pgcd donnée par

PROPOSITION 3.2.2 On suppose $a, b \in \mathbb{Z}$ et $\text{pgcd}(a, b) = d$. Alors il existe $x, y \in \mathbb{Z}$ tels que

$$ax + by = d.$$

On donne d'abord un exemple concret de calcul de solution d'une équation comme $ax \equiv 1 \pmod{n}$.

EXEMPLE 3.2.3 Soit $a = 5$ et $b = 7$. Les étapes de l'algorithme d'Euclide sont :

$$\begin{array}{ll} 7 = 1 \cdot 5 + 2 & \text{donc } 2 = 7 - 5 \\ 5 = 2 \cdot 2 + 1 & \text{donc } 1 = 5 - 2 \cdot 2 = 3 \cdot 5 - 2 \cdot 7. \end{array}$$

A droite, nous avons écrit tout reste comme une combinaison linéaire de a et de b . Finalement, on a écrit $\text{pgcd}(a, b)$ comme une combinaison linéaire a et b .

Cet exemple n'été pas compliqué, et on pourrait aborder un exemple plus long.

EXEMPLE 3.2.4 Soit $a = 130$ et $b = 61$. Nous avons

$$\begin{array}{ll} 130 = 2 \cdot 61 + 8 & \text{donc } 8 = 130 - 2 \cdot 61 \\ 61 = 7 \cdot 8 + 5 & \text{donc } 5 = -7 \cdot 130 + 15 \cdot 61 \\ 8 = 1 \cdot 5 + 3 & \text{donc } 3 = 8 \cdot 130 - 17 \cdot 61 \\ 5 = 1 \cdot 3 + 2 & \text{donc } 2 = -15 \cdot 130 + 32 \cdot 61 \\ 3 = 1 \cdot 2 + 1 & \text{donc } 1 = 23 \cdot 130 - 49 \cdot 61. \end{array}$$

Alors $x = 130$ et $y = -49$.

REMARQUE 3.2.5 Il est suffit pour nous de trouver une solution de $ax + by = d$. En effet, il existe toujours une infinité de solutions. Si x, y est une solution de

$$ax + by = d,$$

alors pour tous $\alpha \in \mathbb{Z}$,

$$a \left(x + \alpha \cdot \frac{b}{d} \right) + b \left(y - \alpha \cdot \frac{a}{d} \right) = d,$$

est aussi une solution, et toutes les solutions sont de cette forme pour un α .

Identité de Bezout.

L'algorithme d'Euclide se compose du calcul d'une suite

$$d_0, \quad d_1, \quad d_2, \dots$$

où $d_0 = a$, $d_1 = b$ et d_{i+1} est le residu de d_{i-1} modulo d_i :

$$d_{i+1} = d_{i-1} - td_i.$$

On s'arrête lorsque $d_k = 0$; alors $d_{k-1} = \text{pgcd}(a, b)$. On peut montrer que le nombre des divisions est borné par $5 \log_{10} \max(a, b)$ (le théorème de Lamé).

De l'algorithme d'Euclide provient aussi une représentation

$$\text{pgcd}(a, b) = ua + vb \tag{3.1}$$

où u, v sont des entiers. Pour les construire on calcule successivement les paires (u_i, v_i) tels que $d_i = u_i a + v_i b$. Posons $u_0 = v_1 = 1, u_1 = v_0 = 0$ et pour $i \geq 1$

$$u_{i+1} = u_{i-1} - tu_i, \quad v_{i+1} = v_{i-1} - tv_i$$

où t est pris de la relation $d_{i+1} = d_{i-1} - td_i$.

Comme $\text{pgcd}(a, b) = d_{k-1}$ on peut prendre $u = u_{k-1}$, $v = v_{k-1}$.

Un programme pour calculer u et v (voir 4ma1-4bezout.mws)

```

> bezout:=proc(a::integer,b::integer)
> local u0,u1,u2,v0,v1,v2,d0,d1,r,t,i;
> if a<0 then a:=-a;
> else fi;
> if b<0 then b:=-b;
> else fi;
> u0:=1:v0:=0;
> u1:=0:v1:=1;
> d0:=a; d1:=b;
> r:=b;
> i:=0;
> while(d1<>0) do
> i:=i+1;
> t:=iquo( d0,d1 );
> r:=irem( d0,d1 );
> d0:=d1;
> d1:= r;
> u2:=u0-t*u1;
> v2:=v0-t*v1;
> u0:=u1;
> u1:= u2;
> v0:=v1;
> v1:= v2;
> printf("i=%d,%d*%d+%d*%d=%d\n"
> ,i,a,(u0) , b,v0, d0)
> od;
> printf("les valeurs de [d, u, v] sont :");
> return [d0,
> u0, v0]
> ;
> end proc:

```

```

> bezout(12,14);
i=1,12*0+14*1=14
i=2,12*1+14*0=12 i=3,12*-1+14*1=2 les valeurs de [d, u, v] sont :

```

[2, -1, 1]

```

> bezout(691,1000);
i=1,691*0+1000*1=1000 i=2,691*1+1000*0=691 i=3,691*-1+1000*1=309 i=4,691*3+1000*-2=73
i=5,691*-13+1000*9=17 i=6,691*55+1000*-38=5 i=7,691*-178+1000*123=2 i=8,691*411+1000*-284=1
les valeurs de [d, u, v] sont :

```

[1, 411, -284]

```

> bezout(17,61);
i=1,17*0+61*1=61 i=2,17*1+61*0=17 i=3,17*-3+61*1=10 i=4,17*4+61*-1=7 i=5,17*-7+61*2=3
i=6,17*18+61*-5=1 les valeurs de [d, u, v] sont :

```

[1, 18, -5]

Une autre possibilité : igcdex - un algorithme euclidien élargi pour les entiers (une fonction de Maple) :

```

Calling Sequence
igcdex(a, b, 'u', 'v')
Parameters
a,b - integers
u,v - (optional) names

```

Déscription

igcdex returns $g = \text{igcd}(a, b)$, and optionally s and/or t such that $g = u a + v b$

Exemples

```
> igcdex(2,3,'u','v');
                                1
> [u,v];
                                [-1, 1]
> a:=2:b:=3:igcdex(2,3,'u','v'):w:=[u,v];
                                w := [-1, 1]
```

Résolution de l'équation $a*u+b*v=c$

```
> restart;
> Bezout := proc(a::posint, b::posint,
> c::nonnegint
> )
> local u, v, gcd, w;
> gcd := igcdex(a, b, 'u', 'v') ;
> if c mod gcd <> 0 then ERROR(
> sprintf("l'équation n'est pas résoluble sur Z"))
> fi ;
> w:=|
> c*u/gcd , c*v/gcd, gcd];
> printf("%a*u+%a*v=%a,
> a=%a, b=%a, u=%a, v=%a, gcd=%a,
> la solution générale sur Z est
> u=%a+%a*t, v=%a-%a*t,
> %a*(%a*(%a)/%a + t*%a/%a) + %a*(%a*(%a)/%a - t*%a/%a)=
> %a",
> a, b, c,
> a, b, c*u/gcd, c*v/gcd, gcd,
> c*u/gcd, b/gcd, c*v/gcd, a/gcd,
> a, c, u, gcd, b, gcd,b,c,v,gcd, a, gcd, c);
> evalb(a*(c*u/gcd+t*b/gcd)+b*(c*v/gcd-t*a/gcd)=c);
> RETURN(w)
> end :
```

```
> a:=6:b:=9:c:=15:W:=Bezout(a, b, c):
> U:=W[1]:V:=W[2]:d:=W[3]:
> print('[U,V,d]=W, 'a*(U+t*b/d)+b*(V-t*a/d)=c');
> #for t from 1 to 10 do
> #print(a*(U+t*b/d)+b*(V-t*a/d)=c);od;
> evalb(a*(U+t*b/d)+b*(V-t*a/d)=c);
```

$6*u+9*v=15$, $a=6$, $b=9$, $u=-5$, $v=5$, $\text{gcd}=3$,

la solution générale sur Z est $u=-5+3*t$, $v=5-2*t$, $6*(15*(-1)/3 + t*9/3) + 9*(15*(1)/3 - t*6/3)=$

15

$$[U, V, d] = [-5, 5, 3], a(U + \frac{tb}{d}) + b(V - \frac{ta}{d}) = c$$

true

EXERCICES

EXERCICE 3.2.6 Montrer que $2 \bmod 61$ et $17 \bmod 61$ sont des générateurs du groupe cyclique $(\mathbb{Z}/61\mathbb{Z})^*$.

EXERCICE 3.2.7 Trouver le nombre total des générateurs de ce groupe.

3.3 Sous-groupes

DÉFINITION 3.3.1 Si G est un groupe, un sous-groupe de G est une partie H de G vérifiant les trois conditions suivantes :

- SG1 $e \in H$,
- SG2 $\forall x, y \in H, xy \in H$,
- SG3 $\forall x \in H, x^{-1} \in H$.

H est alors un groupe pour la loi induite

$$H \times H \rightarrow H, (h_1, h_2) \mapsto h_1 h_2$$

EXEMPLE 3.3.2 Si G est un groupe, G et $\{e\}$ sont des sous-groupes de G .

EXEMPLE 3.3.3 Si $(H_i)_{i \in I}$ est une famille des sous-groupes d'un groupe G , alors l'intersection $\bigcap_{i \in I} H_i$ est un sous-groupe de G . En particulier, si X est une partie de G , l'intersection des sous-groupes de G contenant X , est un sous-groupe de G . C'est le plus petit sous-groupe de G contenant X , on l'appelle le sous-groupe de G engendré par X . On notera $\langle X \rangle$ le sous-groupe engendré par X .

EXEMPLE 3.3.4 Si $\phi : G \rightarrow H$ un morphisme de groupes, alors pour tout sous-groupe H' de H , son image inverse dans G , $\phi^{-1}(H') \subset G$ est un sous groupe de G , et pour tout sous-groupe G' de G , son image $\phi(G') \subset H$ est un sous groupe de H . En particulier, l'ensemble

$$\text{Ker}(\phi) = \phi^{-1}(e) \subset G = \{x \in G \mid \phi(x) = e\}$$

est un sous-groupe de G appelé le noyau de ϕ . L'image de ϕ , notée $\text{Im}(\phi)$, est un sous-groupe de H .

THÉORÈME 3.3.5 Si G est un groupe, et g est un élément de G alors il existe un seul morphisme $\phi : \mathbb{Z} \rightarrow G$ déterminé par la formule

$$k \mapsto g^k \text{ pour } k \in \mathbb{Z}.$$

L'image de ϕ , notée $\text{Im}(\phi)$, est le sous-groupe $H = \langle g \rangle$ de G , engendré par g .

PREUVE. Il suffit de remarquer que g^k est définie de la façon suivante

$$g^0 = e, \forall k \in \mathbb{N}, g^{k+1} = g^k g, \text{ et } g^{-k} = (g^k)^{-1},$$

donc on a un morphisme déterminé par la formule

$$\phi : k \mapsto g^k \text{ pour } k \in \mathbb{Z} \text{ car } \phi(k+l) = g^{k+l} = g^k g^l = \phi(k)\phi(l).$$

THÉORÈME 3.3.6 Soit I un sous-groupe du groupe additif \mathbb{Z} . Alors tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$, pour un élément n de \mathbb{Z} .

PREUVE. Si I est distinct du sous-groupe $\{0\}$, alors I contient un élément non-nul et, contenant aussi son opposé, un élément strictement positif. Soit n le plus petit élément strictement positif de I . Soit i un élément quelconque de I . La division euclidienne de i par n s'écrit $i = nq + r$ avec $0 \leq r < n$. Mais $r = i - nq$ appartient également à I . Par conséquence, par minimalité de n , on a $r = 0$. Donc $i \in n\mathbb{Z}$. Réciproquement, tout élément de $n\mathbb{Z}$ est dans I . En notant que $\{0\} = 0\mathbb{Z}$, on obtient que tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$, pour un élément n de \mathbb{Z} .

COROLLAIRE 3.3.7 Soit $G = \langle g \rangle$ un groupe cyclique d'ordre N . Alors tout sous-groupe H de G est cyclique.

PREUVE. On utilise le morphisme $\phi : \mathbb{Z} \rightarrow G$ déterminé par la formule

$$k \mapsto g^k \text{ pour } k \in \mathbb{Z}.$$

Alors ϕ est *surjectif* parce que G est engendré par g . On considère l'image inverse du sous-groupe $H \subset G$: $\phi^{-1}(H) \subset \phi^{-1}(G) = \mathbb{Z}$.

Selon théorème 3.3.6, tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$, pour un élément n de \mathbb{Z} . Ceci implique que $H = \phi(I) = \langle g^n \rangle$.

3.4 Classes à gauche, à droite

DÉFINITION 3.4.1 Soit G groupe et H un sous-groupe de G . Si $g \in G$, l'ensemble

$$gH = \{gh \mid h \in H\} \text{ (resp. } Hg = \{hg \mid h \in H\})$$

est appelé *classe à gauche* (resp. *à droite*) de g pour H . On note G/H (resp. $H \backslash G$) l'ensemble des classes à gauche (resp. à droite) de G pour H .

Notons que si a et b sont des éléments de G , alors on a une bijection

$$\begin{aligned} aH &\rightarrow bH \\ g &\mapsto ba^{-1}g \end{aligned}$$

De même façon on a une bijection

$$\begin{aligned} aH &\rightarrow Ha^{-1} \\ g &\mapsto g^{-1} \end{aligned}$$

En particulier, toutes les classes ont le même cardinal, à savoir, le cardinal du sous-groupe H . En outre cela définit une bijection

$$\begin{aligned} G/H &\rightarrow H \backslash G \\ aH &\mapsto Ha^{-1} \end{aligned}$$

DÉFINITION 3.4.2 Soit G groupe et H un sous-groupe de G . Si l'ensemble G/H ou $H \backslash G$ des classes à gauche (resp. à droite) est fini, alors tous ces deux ensembles sont finis et de même cardinal, qu'on appelle *indice* de H dans G . On le note $(G : H)$.

Nous avons montré la propriété suivante :

PROPOSITION 3.4.3 Si G est un groupe fini et H est un sous-groupe de G , alors

$$\#G = \#H \cdot (G : H).$$

En particulier, le cardinal du sous-groupe divise le cardinal de G .

3.5 Sous-groupes distingués, groupes quotient

Soit $\phi : G \rightarrow H$ un morphisme de groupes, alors pour tout x de $\text{Ker}(\phi)$ et tout g de G on a

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e.$$

Par conséquent, gxg^{-1} appartient également au noyau de ϕ . Ceci amène à la définition suivante :

DÉFINITION 3.5.1 *Soit G groupe et H un sous-groupe de G . On dit que H est distingué dans G , et on note $H \triangleleft G$ si et seulement si*

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H.$$

Nous venons de voir que si ϕ est un morphisme, son noyau est distingué. Montrons qu'inversement tout sous-groupe distingué est le noyau d'un morphisme.

DÉFINITION 3.5.2 *Si H est un sous-groupe distingué de G , alors il existe sur G/H une unique loi de groupe de sorte que la projection canonique*

$$\phi : G \rightarrow G/H, g \mapsto gH$$

soit un morphisme de groupes. On dit alors que G/H est le groupe-quotient de G par H .

EXEMPLE 3.5.3 *Si G est un groupe abélien, alors tout sous-groupe H de G est distingué. En particulier, le sous-groupe $n\mathbb{Z}$ est distingué dans \mathbb{Z} . On retrouve ainsi une addition dans $\mathbb{Z}/n\mathbb{Z}$.*

EXEMPLE 3.5.4 *Si $\phi : G \rightarrow H$ est un morphisme de groupes et H' un sous-groupe distingué de H , alors $\phi^{-1}(H')$ est un sous-groupe distingué de G .*

PREUVE : en exercice obligatoire.

Cours N°4. Mercredi le 20 octobre 2004

THÉORÈME 3.5.5 (SUR L'ISOMORPHISME) *Si $\phi : G \rightarrow H$ est un morphisme de groupes, et $K = \text{Ker}(\phi)$ son noyau, $K \triangleleft G$, alors il existe un unique isomorphisme de groupes $\bar{\phi} : G/K \xrightarrow{\sim} \text{Im}(\phi)$ tel que ϕ coïncide avec la composée*

$$G \xrightarrow{\pi} G/K \xrightarrow{\bar{\phi}} \text{Im}(\phi) \xrightarrow{j} H$$

où π désigne la projection canonique, et j l'injection canonique.

THÉORÈME 3.5.6 (SUR L'ISOMORPHISME DES GROUPES MONOGÈNES) *Si $G = \langle g \rangle$ est un groupe monogène, alors seulement deux cas sont possibles*

- (i) G est infini et isomorphe à \mathbb{Z} ;
- (ii) G est fini d'ordre N et isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

PREUVE. On considère le morphisme de groupe $\phi : \mathbb{Z} \rightarrow G$, qui est surjectif par l'hypothèse. Soit $I = \text{Ker}(\phi) \subset \mathbb{Z}$ son noyau, alors selon théorème 3.5.5, il existe un isomorphisme de groupes $\bar{\phi} : \mathbb{Z}/I \xrightarrow{\sim} \text{Im}(\phi) = G$. Alors tout sous-groupe de \mathbb{Z} est de la forme $N\mathbb{Z}$, pour un élément N de \mathbb{Z} .

Si $N = 0$, G est infini et isomorphe à \mathbb{Z} ;

Si $N \neq 0$, G est fini d'ordre N et isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

3.6 Ordre d'un élément, théorème de Lagrange

DÉFINITION 3.6.1 *Soit g un élément d'un groupe G . S'il existe un entier strictement positif n tel que $g^n = e$, alors on peut choisir n minimal avec cette propriété. On dit alors que g est un élément d'ordre n , et on le note $n = \text{ord}(g)$.*

S'il n'existe pas d'entier strictement positif n tel que $g^n = e$, on dit que g est un élément d'ordre infini.

PROPOSITION 3.6.2 *Soit g est un élément d'ordre N d'un groupe G , $N = \text{ord}(g)$.*

Alors $N = \text{ord}(g)$ coïncide avec l'ordre du sous-groupe $\langle g \rangle$ engendré par g .

PREUVE. Selon le théorème 3.5.6 sur les groupes monogènes, il existe un isomorphisme $\bar{\phi} : \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \langle g \rangle = \text{Im}(\phi)$, où $\text{Ker}\phi = N\mathbb{Z}$ et N est le plus petit nombre positif tel que $N \in \text{Ker}\phi$, i.e. $g^N = e$. On voit donc que N coïncide avec l'ordre d'élément g , CQFD.

THÉORÈME 3.6.3 (LAGRANGE) (voir Proposition 3.4.3)

Si H un sous-groupe d'un groupe fini G , alors $|H|$ divise $|G|$.

De plus, $|G| = |H| \cdot |G/H|$.

COROLLAIRE 3.6.4 *Soit g est un élément d'ordre n d'un groupe fini G , alors $\text{ord}(g)$ divise $|G|$.*

De plus, $|G| = |G/\langle g \rangle| \cdot \text{ord}(g)$

EXERCICE 3.6.5 *Montrer que pour tout diviseur d d'un nombre entier positif N , il existe un élément d'ordre d dans le groupe cyclique $\mathbb{Z}/N\mathbb{Z}$.*

EXERCICE 3.6.6 *Trouver tous les ordres d'éléments dans le groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$*

EXERCICE 3.6.7 Trouver l'ordre des éléments $\overline{17}$, $\overline{2}$ et $\overline{3}$ du groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$

> $17^{20} \pmod{61}$;	13
> $17^{30} \pmod{61}$;	60
> $17^{12} \pmod{61}$;	20
> $2^{20} \pmod{61}$;	47
> $2^{30} \pmod{61}$;	60
> $2^{12} \pmod{61}$;	9
> $3^{20} \pmod{61}$;	1
> $3^{10} \pmod{61}$;	1
> $3^5 \pmod{61}$;	60
> $3^2 \pmod{61}$;	9

Réponse : $\text{ord}(\overline{17}) = 60$, $\text{ord}(\overline{2}) = 60$ et $\text{ord}(\overline{3}) = 10$.

EXERCICES

- 3.1 Trouver pour tout diviseur d d'un nombre entier positif N , tous les éléments d'ordre d dans le groupe cyclique $\mathbb{Z}/N\mathbb{Z}$.
- 3.2 Trouver tous les éléments d'ordre maximal dans le groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$
- 3.3 Les groupes multiplicatifs $(\mathbb{Z}/8\mathbb{Z})^\times$ et $(\mathbb{Z}/18\mathbb{Z})^\times$ sont-ils cycliques ?
- 3.4 Trouver l'ordre des éléments $\overline{5}$ et $\overline{7}$ du groupe multiplicatif $(\mathbb{Z}/61\mathbb{Z})^\times$
- 3.5 Trouver tous les éléments d'ordre maximal dans les groupes de permutations \mathfrak{S}_3 et \mathfrak{S}_4 .

4 Rappels sur la notion d'anneau, exemples

4.1 Structure d'anneau et idéaux

DÉFINITION 4.1.1 Un anneau est un groupe abélien A muni d'une loi interne

$$A \times A \rightarrow A, (x, y) \mapsto xy = x \cdot y$$

appelé produit ou multiplication, qui est associative

$$\text{An1 } \forall x, y, z \in A, x(yz) = (xy)z,$$

et distributive à droite et à gauche par rapport à l'addition :

$$\text{An2 } \forall x, y, z \in A, x(y + z) = xy + xz,$$

$$\text{An3 } \forall x, y, z \in A, (y + z)x = yx + zx,$$

On prendra également la convention que tout anneau est unifié, c'est à dire que la multiplication est munie d'un élément neutre 1 :

$$\text{An3 } \forall x \in A, 1x = x1 = x.$$

L'anneau est dit commutatif si la loi de multiplication est commutative :

$$\text{Comm. } \forall x, y \in A, xy = yx.$$

DÉFINITION 4.1.2 Un morphisme d'anneau $\varphi : A \rightarrow B$ est une application telle que

$$\text{MorAn } \forall x, y, z \in A, \varphi(xy + z) = \varphi(x)\varphi(y) + \varphi(z) \in A, \varphi(1_A) = 1_B$$

SAn Une partie $A \subset B$ est dit un sous-anneau, si l'inclusion $A \hookrightarrow B$ est un morphisme d'anneau.

EXEMPLE. On pose $B = \mathbb{Z} \times \mathbb{Z} = \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{Z}\}$, alors $A = \{0\} \times \mathbb{Z}$ est un anneau, mais non un sous-anneau de B .

DÉFINITION 4.1.3 Soit A un anneau commutatif. Une partie $I \subset A$ est dit un idéal si c'est un sous-groupe additif pour l'addition, stable par la multiplication externe (par un élément quelconque $y \in A$

$$\text{Idéal } \forall x \in I, \forall a \in A, ax \in I.$$

Opérations sur les idéaux

DÉFINITION 4.1.4 (a) Soient I, J deux idéaux de A . Leur somme

$$I + J = \{x + y \mid x \in I, y \in J\}$$

est le plus petit idéal de A contenant I et J .

La somme d'une famille d'idéaux $(I_\alpha)_{\alpha \in \Gamma}$ est formée par toutes les sommes finies

$$\sum_{\alpha \in \Gamma} I_\alpha = \left\{ \sum_{\alpha \in \Gamma} x_\alpha, x_\alpha \in I_\alpha \right\}$$

où $x_\alpha = 0$ sauf un nombre fini de $\alpha \in \Gamma$.

(b) L'intersection ensembliste

$$\bigcap_{\alpha \in \Gamma} I_\alpha$$

d'une famille d'idéaux $(I_\alpha)_{\alpha \in \Gamma}$ est toujours un idéal de A .

(c) Soit X une partie d'un anneau A . L'intersection de tous les idéaux de A , contenant X , est dit l'idéal engendré par X

(d) Le produit

$$I_1 \cdot I_2 \cdots I_n$$

d'un nombre fini d'idéaux est l'idéal engendré par

$$\{x_1 \cdot x_2 \cdots x_n \mid x_1 \in I_1, x_2 \in I_1, \dots, x_n \in I_n\}$$

En particulier, l'idéal I^n est engendré par

$$\{x_1 \cdot x_2 \cdots x_n \mid x_1, x_2 \in I_1, \dots, x_n \in I\}$$

EXEMPLE.

a) Si $A = \mathbb{Z}$, $I = (m)$, $J = (n)$, alors

$$I + J = (\text{pgcd}(m, n)), I \cap J = (\text{ppcm}(m, n)), I \cdot J = (mn).$$

REMARQUE.

L'idéal, engendré par une famille x_α , coïncide avec la somme

$$\sum_{\alpha \in \Gamma} (x_\alpha)$$

de tous les idéaux principaux $(x_\alpha) = x_\alpha A$.

REMARQUE. Montrer en exercice que l'union d'une famille d'idéaux $(I_\alpha)_{\alpha \in \Gamma}$ n'est pas un idéal en général, mais c'est le cas si les idéaux I_α sont totalement ordonnés par l'inclusion :

$$\forall \alpha, \beta, \text{ soit } I_\alpha \subset I_\beta, \text{ soit } I_\beta \subset I_\alpha.$$

4.2 Anneau quotient

DÉFINITION 4.2.1 Soit A un anneau commutatif, $I \subset A$ un idéal de A . Alors il existe sur le groupe quotient additif A/I une unique structure d'anneau telle que la projection canonique $\pi : A \rightarrow A/I$ est un morphisme d'anneaux.

PROPOSITION 4.2.2 (a) Soit A un anneau commutatif, $I \subset A$ un idéal de A . Alors il existe une bijection entre l'ensemble

$$\{J \subset A \mid J \supset I\}$$

d'idéaux contenant I , et l'ensemble

$$\{\bar{J} \subset A/I\}$$

d'idéaux de A/I , donnée par $J = \pi^{-1}(\bar{J})$, où $\pi : A \rightarrow A/I$ est la projection canonique.

(b) Soit $\psi : A \rightarrow B$ un morphisme d'anneaux, alors $I = \text{Ker}\psi := \psi^{-1}(0)$ est un idéal de A , $\psi(A) = C$ est un sous-anneau de B , et il y a un isomorphisme d'anneaux

$$\bar{\psi} : A/I \xrightarrow{\sim} C.$$

NOTATIONS.

On écrit

$$x \equiv y \pmod{I} \iff x - y \in I.$$

Diviseurs de zéro, éléments nilpotents et unités

DÉFINITION 4.2.3

(a) Un $x \in A \setminus \{0\}$ est dit **diviseur de zéro**, s'il existe un $y \in A \setminus \{0\}$ tel que $xy = 0$. Un anneau $A \neq \{0\}$ sans diviseurs de zéro est dit **intègre**.

(b) Un élément $x \in A \setminus \{0\}$ est dit **nilpotent**, si $x^n = 0$ pour un $n \geq 1$.

(c) Un élément $x \in A$ est dit **inversible** (ou une **unité**) de A s'il existe $y \in A$, $xy = 1$. On notera $x \in A^\times$.

DÉFINITION 4.2.4 Un **corps** est un anneau commutatif A , non réduit à $\{0\}$ dans lequel tout élément non-nul est inversible :

$$\text{Corps } \forall x \in A, x \neq 0, \exists y \in A, xy = 1$$

PROPOSITION 4.2.5 (a) Soit A un corps, alors A est un anneau intègre.

(b) Soit A un corps, I un idéal de A . Alors soit $I = \{0\}$ soit $I = A$.

4.3 Idéaux premiers

DÉFINITION 4.3.1

(a) Un idéal $I \neq A$ est dit **premier**, si

$$\forall x, y \in A, x \cdot y \in I \iff x \in I \text{ ou } y \in I,$$

i.e. l'anneau quotient A/I est intègre.

(b) Un idéal $I \neq A$ est dit **maximal**, si

$$\forall \text{ idéal } J \subset A, I \subset J \Rightarrow I = J, \text{ ou } J = A$$

PROPOSITION 4.3.2

(a) Un idéal $I \neq A$ est dit **maximal**, si et seulement si A/I est un corps

(b) Tout idéal maximal est premier.

PREUVE (a) On suppose I maximal. Si $x \notin I$, on considère l'idéal (x, I) engendré par x et I . Alors $(x, I) \neq I$ donc $(x, I) = A$; ceci dit, il existe $a \in A$ et $b \in I$ tels que $ax + b = 1$; ceci dit, $\overline{ax} = \bar{1}$ dans A/I .

Réciproquement, si A/I est un corps, les seuls idéaux de A/I sont $\{0\}$ et A/I . Par la proposition 4.2.2, a), il existe une bijection entre l'ensemble

$$\{J \subset A \mid J \supset I\}$$

d'idéaux contenant I , et l'ensemble

$$\{\bar{J} \subset A/I\}$$

d'idéaux de A/I . Donc il n'y a pas d'idéaux stricts intermédiaires entre I et A , i.e. I est maximal.

(b) Un corps est toujours un anneau intègre, donc I est premier.

EXEMPLE.

Dans l'anneau $A = \mathbb{C}[X, Y]$ l'idéal $I = (X, Y)$ est maximal, $A/I \simeq \mathbb{C}$.

L'idéal $J = (X)$ n'est pas maximal, mais premier : $A/J \simeq \mathbb{C}[Y]$.

EXERCICE. (à faire en TD) Montrer que tous les idéaux maximaux M de l'anneau $A = \mathbb{Z}[X]$ sont de la forme : $M = (p, f)$, où $f \in \mathbb{Z}[X]$ est un polynôme tel que $f \bmod p \in \mathbb{F}_p[X]$ est irréductible. Ici $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est le corps de p éléments.

L'idéal $J = (p)$ n'est pas maximal, mais premier : $A/J \simeq \mathbb{F}_p[X]$.

4.4 Divisibilité dans les anneaux

DÉFINITION 4.4.1 Soit A un anneau commutatif.

(a) Si a et $b \in A$, on dit que a divise b et on note $a|b$ s'il existe un $c \in A$ tel que $b = ac$. On dit également que b est un multiple de a ou a un diviseur de b . On note $(a) = aA$ l'ensemble des multiples de a . C'est un idéal de A engendré par a .

(b) Soit A un anneau intègre. Deux éléments a et $b \in A$ sont dits associés si et seulement s'ils vérifient une des conditions équivalentes suivantes :

- (i) $\exists u \in A^\times, b = ua$
- (ii) $a|b$ et $b|a$
- (iii) $(a) = (b)$

On notera dans ce paragraphe $a \sim b$ (c'est une relation d'équivalence).

DÉFINITION 4.4.2 Un élément $a \in A$ est dit irréductible, si et seulement si il vérifie les deux conditions suivantes :

lrr1. $a \notin A^\times$

lrr2. Si $a = bc$ avec $a, b \in A$ alors $a \in A^\times$ ou $b \in A^\times$.

EXEMPLE. Les éléments irréductibles de \mathbb{Z} sont les éléments de la forme p ou $-p$ avec p un nombre premier parce que $\mathbb{Z}^\times = \{\pm 1\}$.

PROPOSITION 4.4.3 Soit $p \in A \setminus \{0\}$. Si (p) est premier alors p est irréductible. La réciproque est fautive en générale.

DÉFINITION 4.4.4 Soit A un anneau commutatif intègre, I un ensemble et $(a_i)_{i \in I}$ une famille d'éléments de A .

(i) On dit que $d \in A$ est un pgcd de la famille $(a_i)_{i \in I}$, $d = \text{pgcd}(a_i)_{i \in I}$, si

$$\forall i \in I, d|a_i \text{ et } \forall r \in A, \forall i \in I, r|a_i \Rightarrow r|d$$

(ii) On dit que $m \in A$ est un ppcm de la famille $(a_i)_{i \in I}$, $m = \text{ppcm}(a_i)_{i \in I}$, si

$$\forall i \in I, a_i|m \text{ et } \forall r \in A, \forall i \in I, a_i|r \Rightarrow m|r$$

EXEMPLE 4.4.5 Le pgcd et ppcm n'existe pas toujours dans un anneau commutatif. Un exemple connu est donné par l'anneau $\mathbb{Z}[\sqrt{-5}]$ dans lequel il existe essentiellement différentes factorisations en éléments premiers :

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

On pose $a = 6$ et $b = 2(1 + \sqrt{-5})$. Montrer que $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ n'existe pas dans A .

REMARQUE. Si $d = \text{pgcd}(a_i)_{i \in I}$ et $m = \text{ppcm}(a_i)_{i \in I}$ existent, il ne sont en fait pas uniques. Seules leurs classes d'équivalence dans A/\sim le sont.

4.5 Anneaux euclidiens et anneaux principaux

La notion de division sur les polynômes et les entiers conduit à la notion d'anneau euclidien.

DÉFINITION 4.5.1 Un anneau intègre A est dit euclidien s'il existe une application $\phi : A \rightarrow \mathbb{N}$ appelée stathme telle que

$$\forall a \in A \setminus \{0\} \forall b \in A, \exists (q, r) \in A^2, b = aq + r \text{ avec } r = 0 \text{ ou } \phi(r) < \phi(a)$$

EXEMPLE. L'anneau des entiers \mathbb{Z} est euclidien pour la valeur absolue.

EXERCICE. Montrer que les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont euclidiens pour le carré de la valeur absolue complexe.

DÉFINITION 4.5.2 Un anneau intègre A est dit principal si tout idéal I de A est principal, c'est à dire, il existe un $a \in A$, tel que $I = (a)$.

THÉORÈME 4.5.3 Tout anneau A euclidien est principal.

PREUVE. Soit A un anneau euclidien et I un idéal de A . Si $I \neq \{0\}$, il existe un élément non nul dans I . On choisit un élément x de I tel que $\phi(x)$ soit minimal. Alors $I = (x)$. En effet, pour tout $y \in I$, on écrit $y = xq + r$ avec $r = 0$ ou $\phi(r) < \phi(x)$. Comme $r = y - xq$, $r \in I$ et par minimalité de $\phi(x)$, $r = 0$. Donc $y \in (x)$, CQFD

PROPOSITION 4.5.4 Soit A un anneau principal. Les assertions suivantes sont équivalentes :

- (i) \mathfrak{a} est un idéal maximal non nul de A ;
- (ii) \mathfrak{a} est un idéal premier non nul de A ;
- (iii) il existe un élément p irréductible de A tel que $\mathfrak{a} = (p)$.

PREUVE. (i) \Rightarrow (ii) Puisqu'un idéal maximal est premier.

(ii) \Rightarrow (iii) Comme A est principal, il existe p tel que $\mathfrak{a} = (p)$ mais comme (p) est premier, p est irréductible.

(iii) \Rightarrow (i) Soit p irréductible et $\mathfrak{a} = (p)$. Par l'hypothèse, $p \notin A^\times$, donc $\mathfrak{a} \neq A$. Soit \mathfrak{b} tel que $\mathfrak{a} \subset \mathfrak{b}$. Comme A est principal, $\mathfrak{b} = (q)$. Donc $q|p$, si $\mathfrak{a} \neq \mathfrak{b}$, alors q et p ne sont pas associés. Donc $q \in A^\times$, et $\mathfrak{b} = A$.

COROLLAIRE 4.5.5 (LEMME D'EUCLIDE) Soit A un anneau principal, p un élément irréductible dans A . Alors

$$p|ab \Rightarrow (p|a \text{ ou } p|b).$$

PROPOSITION 4.5.6 Soit A un anneau principal, alors toute famille $(a_i)_{i \in I}$ d'éléments de A admet un pgcd et ppcm.

PREUVE. Le pgcd est donné comme un générateur de l'idéal $\sum_{i \in I} (a_i)$ et le ppcm comme générateur de l'idéal $\bigcap_{i \in I} (a_i)$.

PROPOSITION 4.5.7 (BEZOUT) Si A est un anneau principal et $a_1, \dots, a_n \in A$, alors il existe $b_1, \dots, b_n \in A$ tels que

$$a_1 b_1 + \dots + a_n b_n = \text{pgcd}(a_1, \dots, a_n)$$

PREUVE. Le pgcd est un générateur de l'idéal (a_1, \dots, a_n) , donc il existe $b_1, \dots, b_n \in A$ tels que

$$a_1 b_1 + \dots + a_n b_n = \text{pgcd}(a_1, \dots, a_n).$$

DÉFINITION 4.5.8 Si A est un anneau principal et $a_1, \dots, a_n \in A$, Si $\text{pgcd}(a_1, \dots, a_n) = 1$ alors on dit que a_1, \dots, a_n sont premiers entre eux. Dans ce cas il existe $b_1, \dots, b_n \in A$ tels que

$$a_1 b_1 + \dots + a_n b_n = 1$$

PROPOSITION 4.5.9 (LEMME DE GAUSS) Soit A est un anneau principal et $b, c \in A$ deux éléments premiers entre eux. Si $c|ab$, alors $c|a$.

PREUVE. Par le théorème de Bezout, il existe u, v tels que $bu + cv = 1$. Comme $c|ab$ par l'hypothèse,

$$c|a(bu + cv) = abu + acv = a, \quad \square$$

ceci implique que $c|a$.



4.6 Décomposition en facteurs premiers

DÉFINITION 4.6.1 Un anneau intègre A est dit *factoriel* si et seulement si il vérifie les conditions suivantes :

Existence. Pour tout élément non nul a de A il existe un élément inversible $u \in A^\times$ et des éléments irréductibles p_1, \dots, p_m de A tels que

$$a = up_1 \dots p_m$$

(il se peut que $m = 0$, dans ce cas $a \in A^\times$).

Unicité. Soient m, n, p_1, \dots, p_m et q_1, \dots, q_n des éléments irréductibles de A et $u, v \in A^\times$ des éléments inversibles de A tels que

$$up_1 \dots p_m = vq_1 \dots q_n,$$

alors $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $q_i \sim p_{\sigma(i)}$ pour $i = 1, \dots, n$.

THÉORÈME 4.6.2 Tout anneau A principal est factoriel.

PREUVE. Existence. On raisonne par l'absurde : soit a_0 un élément de $A \setminus \{0\}$, non-inversible, qui ne s'écrit pas comme produit d'éléments irréductibles. En particulier, a_0 n'est pas irréductible et on peut écrire : $a_0 = a_1 a'_1$ avec a_1 et a'_1 non inversibles. Si ces deux éléments sont produit d'irréductibles, alors il en est de même de a_0 . Quitte à échanger a_1 et a'_1 , on peut supposer que a_1 n'est pas produit d'irréductibles. En itérant, on obtient une suite infinie $a_0, a_1, \dots, a_n \dots$ d'éléments tels que

$$(a_0) \subsetneq (a_1) \subsetneq (a_n) \subsetneq \dots \subsetneq \dots$$

La réunion $I = \bigcup_{n=0}^{\infty} (a_n)$ est un idéal de A . En effet $0 \in I$ et si b_1 et b_2 appartiennent à I , il existe n_1 et n_2 tels que $b_1 \in (a_{n_1})$ et $b_2 \in (a_{n_2})$. Soit $n = \sup(n_1, n_2)$, alors $b_1 - b_2 \in (a_n)$ donc I est un sous groupe de A et si b appartient à I et a à A il existe n tel que $b \in (a_n)$ et $ab \in (a_n) \subset I$. Comme A est principal, $I = (a)$ pour un $a \in A$. Mais comme $a \in I$, il existe n tel que $a \in (a_n)$ donc

$$(a_n) \subsetneq (a_{n+1}) \subsetneq (a_n) \subset I = (a) \subset (a_n),$$

ce que est absurde.

Unicité. Si on a une égalité de la forme

$$up_1 \dots p_m = vq_1 \dots q_n,$$

avec p_1, \dots, p_m et q_1, \dots, q_n des éléments irréductibles, et $u, v \in A^\times$ des éléments inversibles de A , on peut supposer que $m \geq n$. On procède alors par récurrence sur m . Si $m = 0$, alors $n = 0$ et le résultat annoncé est vrai. Mais, par le lemme d'Euclide (Corollaire 4.5.5, p_1 divise v ou l'un des q_i . Comme v est inversible, si $p_1|v$ alors p_1 est inversible ce que contredit le fait que p_1 soit irréductible. On a

$$p_1 | q_1 \dots q_n.$$

Donc p_1 divise l'un des q_i .

Quitte à échanger les q_i , on peut supposer que $p_1 | q_1$. Comme le nombre q_1 est premier, on obtient $p_1 = wq_1$ avec $w \in A^\times$, d'où

$$p_2 \dots p_m = (vw)q_2 \dots q_n$$

(après la simplification), et il reste à appliquer l'hypothèse de récurrence au produit $p_2 \dots p_m$ de $m - 1$ facteurs irréductibles.

EXERCICES

- 4.1 Le pgcd et ppcm n'existe pas toujours dans un anneau commutatif. Un exemple connu est donné par l'anneau $\mathbb{Z}[\sqrt{-5}]$ dans lequel il existe essentiellement différentes factorisations en éléments premiers :

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

On pose $a = 6$ et $b = 2(1 + \sqrt{-5})$. Montrer que $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$ n'existe pas dans A .

- 4.2 Trouver tous les diviseurs de zéro dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

- 4.3 Trouver tous les éléments nilpotents dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

- 4.4 Trouver tous les éléments inversibles dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

- 4.5 Montrer qu'un anneau fini A est intègre si et seulement s'il est un corps.

- 4.6 Montrer que les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont euclidiens pour le carré de la valeur absolue complexe.

- 4.7 Trouver tous les éléments inversibles dans les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.

- 4.8 Décrire tous les éléments irréductibles dans les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$.

- 4.9 Montrer que l'anneau des nombres décimaux

$$\mathcal{O} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b = 10^k, k \in \mathbb{N} \right\}$$

est un anneau euclidien.

- 4.10 Montrer que tout corps est un anneau euclidien.

5 Théorème des restes chinois

5.1 Théorème des restes dans les anneaux principaux

Commençons par énoncer un résultat préliminaire :

PROPOSITION 5.1.1 *Si A est un anneau principal et a_1, \dots, a_n des éléments premiers entre eux deux-à-deux, alors*

$$\text{ppcm}(a_1, \dots, a_n) = \prod_{i=1}^n a_i.$$

LEMME 5.1.2 *Soit A un anneau principal. Si b est premier avec chacun des a_1, \dots, a_n , alors b est premier avec $a_1 \dots a_n$.*

PREUVE du lemme. On procède par récurrence. L'énoncé est vrai si $n = 1$. Montrons le pour $n = 2$. Par le théorème de Bezout, comme b est premier avec a_1 et a_2 , il existe des éléments x_1, x_2, y_1, y_2 de A tels que

$$1 = x_1 b + y_1 a_1, \text{ et } 1 = x_2 b + y_2 a_2.$$

Par conséquent,

$$1 = (x_1 b + y_1 a_1)(x_2 b + y_2 a_2) = (x_1 x_2 b + y_1 a_1 x_2 + x_1 y_2 a_2) b + y_1 y_2 a_1 a_2,$$

ce que implique le résultat dans ce cas. Si le résultat est vrai pour $n - 1$ par hypothèse de récurrence, b est premier avec $a_1 \dots a_{n-1}$ et a_n . Donc, en utilisant $n = 2$, on obtient que b est premier avec le produit $a_1 \dots a_n$.

PREUVE de la proposition. On montre la proposition par récurrence. Elle est vraie pour $n = 1$. Si $n = 2$, comme

$$a_1 \mid \frac{\text{ppcm}(a_1, a_2)}{a_2} \times a_2,$$

en appliquant le lemme de Gauss (Proposition 4.5.9), a_1 divise $\frac{\text{ppcm}(a_1, a_2)}{a_2}$ et donc $a_1 a_2 \mid \text{ppcm}(a_1, a_2)$. Enfin pour la récurrence on utilise l'assertion qui précède et l'égalité

$$\text{ppcm}(a_1, \dots, a_n) = \text{ppcm}(\text{ppcm}(a_1, \dots, a_{n-1}), a_n).$$

THÉORÈME 5.1.3 (THÉORÈME DES RESTES) *Si A est un anneau principal et a_1, \dots, a_n des éléments premiers entre eux deux-à-deux, alors*

$$A/(a_1 \dots a_n) \simeq \prod_{i=1}^n A/(a_i).$$

PREUVE du théorème. On considère l'application

$$A \rightarrow \prod_{i=1}^n A/(a_i),$$

produit des projections canoniques. Son noyau est $\bigcap_{i=1}^n (a_i)$ qui par la proposition précédente coïncide avec $\prod_{i=1}^n (a_i)$. On obtient donc un morphisme injectif

$$A/(a_1 \cdots a_n) \rightarrow \prod_{i=1}^n A/(a_i).$$

Il reste donc à montrer que cette application est surjective. Cela revient donc à montrer que, sous les hypothèses du théorème, pour toute famille (x_1, \dots, x_n) de A^n , il existe x dans A tel que $a_i | x - x_i$ pour tout i entre 1 et n . Là encore, nous allons procéder par récurrence. Pour $n = 1$, le résultat est vrai. Pour $n = 2$, en utilisant Bezout, on peut écrire $1 = a_1 b_1 + a_2 b_2$, avec b_1 et b_2 des éléments de A . On pose $x = a_1 b_1 x_2 + a_2 b_2 x_1$. On obtient

$$x - x_1 = a_1 b_1 (x_2 - x_1) \text{ et } x - x_2 = a_2 b_2 (x_1 - x_2).$$

Donc x convient.

Si le résultat est vrai pour $n - 1$, il existe y tel que $a_i | (y - x_i)$ pour $1 \leq i \leq n - 1$, et en utilisant le cas $n = 2$, il existe un élément x de A tel que

$$\prod_{i=1}^{n-1} a_i | (x - y) \text{ et } a_n | (x_n - y).$$

Par conséquent $a_i | (y - x_i)$ pour $1 \leq i \leq n$, CQFD.

(Voir aussi des exemples, disponibles à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-7chrem.mws)

REMARQUE 5.1.4 (THÉORÈME DE BEZOUT : UNE FORME EXPLICITE) *Si A est un anneau principal et a_1, \dots, a_n des éléments premiers entre eux deux-à-deux, alors on peut explicitement donner un $x \in A$ tel que pour toute collection de classes $x_i \bmod a_i = x_i + (a_i)$, $x \equiv x_i \bmod a_i$. On pose $A_i = \prod_{\substack{j=1 \\ j \neq i}}^n a_j$. Alors*

on a $\text{pgcd}(A_1, \dots, A_n) = 1$ puisque a_1, \dots, a_n sont des éléments premiers entre eux deux-à-deux. Cici dit, par l'identité de Bezout, qu'il existe $u_i \in A$ tels que

$$A_1 u_1 + \cdots + A_n u_n = 1$$

Il vient que

$$A_i u_i \equiv \begin{cases} 0 \bmod a_j, & \text{si } j \neq i \\ 1 \bmod a_i \end{cases}$$

Ceci implique qu'on peut définir x comme

$$x = x_1 A_1 u_1 + \cdots + x_n A_n u_n.$$

En effet, la congruence précédente montre que

$$\forall i = 1, \dots, n, \quad x = x_1 A_1 u_1 + \cdots + x_n A_n u_n \equiv x_i \bmod a_i.$$

5.2 Application : éléments inversibles mod n

PROPOSITION 5.2.1 Soit m un entier strictement positif et a un entier relatif. Les conditions suivantes sont équivalentes

- (i) \bar{a} est un générateur du groupe $\mathbb{Z}/m\mathbb{Z}$,
- (ii) \bar{a} est inversible dans l'anneau $\mathbb{Z}/m\mathbb{Z}$,
- (iii) a est premier à m .

On note $\varphi(m)$ le cardinal de $(\mathbb{Z}/m\mathbb{Z})^\times$. La fonction $\varphi(m)$ est appelée la *fonction indicatrice d'Euler*. On a la relation suivante :

$$\varphi(m) = m \prod_{p \in \mathcal{P} \mid p|m} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^r p_i^{m_i-1} (p_i - 1).$$

PREUVE de i) et ii) est déjà fait dans la Proposition 2.3.1 (sur la simplification dans $\mathbb{Z}/n\mathbb{Z}$) : si $\text{pgcd}(a, n) = 1$ et

$$ax \equiv ay \pmod{n}$$

alors $x \equiv y \pmod{n}$.

On va déduire iii) de l'isomorphisme d'anneaux

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(p_1^{m_1} \dots p_r^{m_r}) \simeq \prod_{i=1}^r \mathbb{Z}/(p_i^{m_i}).$$

En considérant les éléments inversibles, on obtient un isomorphisme de groupes

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/(p_i^{m_i}))^\times.$$

Par conséquent

$$\varphi(m) = \prod_{i=1}^r \varphi(p_i^{m_i}).$$

Mais si p est premier, a est premier à p si et seulement s'il n'est pas divisible par p .
Donc

$$\begin{aligned} \varphi(p^n) &= p^n - p^{n-1} = p^{n-1}(p-1), \\ \varphi(p_1^{n_1} \dots p_r^{n_r}) &= p_1^{n_1-1}(p_1-1) \dots p_r^{n_r-1}(p_r-1). \end{aligned}$$

EXEMPLE.

$$\varphi(4) = 2, \varphi(25) = 20, \varphi(100) = 40, \varphi(1000) = 4 \cdot 100 = 400.$$

EXERCICE. Trouver la factorisation en produit des nombres premiers de $\varphi(8!)$.

REMARQUE. Le problème de calcul de $\varphi(n)$ est difficile pour les grands nombres entiers n , puisque il dépend de la factorisation de n .

COROLLAIRE 5.2.2 (THÉORÈME DE FERMAT-EULER) *Pour tout entier strictement positif n et tout élément a de $(\mathbb{Z}/n\mathbb{Z})^\times$, on a*

$$a^{\varphi(n)} = 1.$$

PREUVE. Cela résulte du théorème de Lagrange (théorème 3.6.3), appliqué au groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

EXEMPLE.

> 3⁴⁰⁰ mod 100000;

88001

5.3 Application à la cryptographie : RSA

La *cryptographie théorique* est une science qui étudie les systèmes d'échange d'information protégé.

On considère un système d'utilisateurs $U_1, U_2, U_3 \dots$. De temps en temps chaque couple d'utilisateurs aurait pu besoin d'échanger de messages que doivent rester secret pour les autres utilisateurs ou pour toute autre person non autorisée.

Dans les *systèmes classiques* de cryptographie, ils doivent échanger d'abord les clés et après les garder secret. La cryptographie à *clef publique* évite la dernière restriction : les communications secretes deux-à-deux devient possible en utilisant seulement une information ouverte pour tout le monde. Un tel système peut être réalisé de façon suivante : Pour l'ensemble $\{U_i\}$ d'utilisateurs et un ensemble fini \mathcal{M} des "messages", et on associe à tout U_j deux applications

$$\mathcal{E}_j : \mathcal{M} \rightarrow \mathcal{M}, \text{ et } \mathcal{D}_j : \mathcal{M} \rightarrow \mathcal{M},$$

de telle façon que \mathcal{D}_j est secret, \mathcal{E}_j est publique (ouverte), et

$$\mathcal{E}_j \circ \mathcal{D}_j = id = \mathcal{D}_j \circ \mathcal{E}_j : \mathcal{M} \rightarrow \mathcal{M}.$$

(donc le savoir de \mathcal{E}_j ne donne pas $\mathcal{D}_j = \mathcal{E}_j^{-1}$).

Cryptographie asymétrique.

Les méthodes anciennes utilisées pour cryptage et pour décryptage ont été *symétriques* : les applications

$$\mathcal{E}_{ij} : \mathcal{M} \rightarrow \mathcal{M}, \text{ et } \mathcal{D}_{ij} : \mathcal{M} \rightarrow \mathcal{M},$$

ont été connu pour U_i et U_j , mais secrets pour tout autre utilisateur U_k , avec $k \neq i, j$.

Par exemple, on a utilisé souvent le cryptage *par permutation* \mathcal{E}_{ij} , ou cryptage par *addition avec un grand nombre aléatoire* dans $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$.

En 1976, des nouveaux systèmes de cryptographie *asymétriques* ont été découverts par Diffie, Hellman, Rivest, Shamir, Adleman à la base de la difficulté du *problème d'inversion*.

Fonctions sens unique à trappe.

Soient \mathcal{E} et \mathcal{F} deux ensembles finis, par exemple $\mathcal{E} = \mathcal{F} = \mathcal{M}$. Une fonction ψ bijective de \mathcal{E} dans \mathcal{F} est dite une *fonction sens unique* (FSU) si étant donné $y \in \mathcal{F}$ tel qu'il existe $x \in \mathcal{E}$ avec $\psi(x) = y$, la seule donnée de ψ et de y ne permet pas de calculer x ; c'est le *problème d'inversion*, c'est-à-dire calculer la fonction inverse ψ^{-1} de ψ . La fonction ψ est dite *fonction sens unique à trappe* (FSUT) si c'est une FSU telle que il existe une information supplémentaire, la *clé secrète* \mathcal{K} , qui permet de résoudre le problème d'inversion.

Utilisations des fonctions sens unique à trappe.

Soit ψ une FSUT de \mathcal{E} dans \mathcal{F} avec la clé secrète \mathcal{K} . Les messages possibles sont les éléments de \mathcal{E} et les messages cryptés sont les éléments de \mathcal{F} . Afin de recevoir des messages cryptés, *Alice* (un utilisateur) rend publique la fonction ψ (fonction de cryptage), elle garde secret néanmoins la clé \mathcal{K} . Pour transmettre un message $x \in \mathcal{E}$ à *Alice*, *Bob* calcule $y = \psi(x)$ et envoie y . Afin de décoder le message y , il faut pouvoir calculer $x = \psi^{-1}(y)$, or seule *Alice*, qui possède \mathcal{K} , arrive à calculer ψ^{-1} (fonction de décryptage). Ainsi, tout le monde peut coder un message, mais seule *Alice* peut le décoder.

5.4 Principaux protocoles.

Les principaux protocoles existants utilisant des FSU ou des FSUT sont le protocole RSA, et les protocoles de type ElGamal basés sur le problème du logarithme discret : dans le groupe des éléments inversibles d'un corps fini ou dans le groupe des points d'une courbe elliptique sur un corps fini.

Le protocole RSA (comme Rivest, Shamir, Adleman), voir [RSA]

Soient p et q deux nombres premiers de grande taille, on pose $n = p \cdot q$. L'ensemble \mathcal{E} et l'ensemble \mathcal{F} sont le même ensemble : l'ensemble $\mathcal{M} = \{0, \dots, n - 1\}$ des nombres entiers entre 0 et $n - 1$. Soit e un nombre entier premier avec $(p - 1)(q - 1)$. La fonction ψ est la fonction

$$\psi(x) = x^e \pmod{n},$$

la clef secrète \mathcal{K} est un entier d tel que

$$e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)},$$

alors on a

$$\psi^{-1}(x) = x^d \pmod{n}.$$

Cette assertion est vraie pour tous les $x \pmod{pq}$.

Si $\text{pgcd}(x, pq) = 1$, on utilise le théorème 5.2.2 d'Euler-Fermat :

$$x^{ed} \equiv x \pmod{pq}.$$

Si, par exemple $p|x$, mais $q \nmid x$, on a donc

$$ed = 1 + (p-1)(q-1)t \Rightarrow x^{ed} = (x)^{1+(p-1)(q-1)t} = x(x^{(p-1)t})^{q-1} \equiv x \pmod{pq}$$

$$\Rightarrow x^{ed} = \begin{cases} x((x)^{(p-1)})^{q-1} \equiv x \cdot 1 \pmod{q}, \\ \equiv 0 \pmod{p} \end{cases} \Rightarrow x^{ed} \equiv x \pmod{pq}.$$

La sécurité du protocole RSA

réside sur le fait que pour calculer l'entier d , il faut connaître les nombres p et q , et donc être à même de factoriser l'entier n .

Pour réaliser ce schéma on utilise la difficulté technique de factorisation de grands nombres entiers en produit de nombres premiers.

Système RSA pour plusieurs utilisateurs

a) Chaque utilisateur U_i choisit deux grand nombres premiers p_i, q_i , et deux classes $e_i, d_i \pmod{n_i}$ où $n_i = p_i q_i$ telles que $e_i d_i \equiv 1 \pmod{\varphi(n_i)}$ où $\varphi(n_i) = (p_i - 1)(q_i - 1)$ désigne la fonction de Euler.

b) Les nombres (e_i, n_i) sont publiques pour tous les utilisateurs (ils sont publiés dans une sorte de "pages blanches").

On suppose qu'il n'est pas possible de calculer d_i à partir de (e_i, n_i) , donc d_i peut être considéré comme une clef secrète de décryptage connue seulement à U_i . En effet, on montrera qu'un algorithme efficace pour calculer d_i trouve aussi la *factorisation* de n_i (ceci dit, un tel algorithme est *équivalente* à la résolution d'un problème supposé difficile). Supposons qu'on connaît d_i . Alors on connaît que $\varphi(n_i)$ *divise* $e_i d_i - 1$. Si l'on avait connu $\varphi(n_i)$ on aurait pu trouver facilement p_i, q_i car

$$\varphi(n_i) = (p_i - 1)(q_i - 1) = p_i q_i - (p_i + q_i) + 1 \Rightarrow$$

$$p_i + q_i = n_i + 1 - \varphi(n_i) \text{ et } p_i - q_i = \sqrt{(p_i + q_i)^2 - 4n_i}.$$

On peut montrer même que si l'on connaît seulement un multiple de $\varphi(n_i)$ on puisse trouver p_i, q_i .

c) Supposons qu'un utilisateur U_i souhaite à transmettre à U_j un message secret représenté comme un suite de bits. Tout d'abord, il décompose cette suite en blocs de longueur $\lceil \log_2 n_j \rceil$, alors il considère tout bloc comme une classe des résidue $m \pmod{n_j}$ et finalement il crypte le message par la classe $m^{e_j} \pmod{n_j}$. Ceci dit, (n_j, e_j) sers comme une *clef de cryptage* de j -e utilisateur.

d) Ayant reçu le message crypté, U_j le décrypte bloc-par-bloc $b \pmod{n_j}$ par calcule de $b^{d_j} \pmod{n_j}$ (rapellons qu'il connaît seulement sa *clef de décryptage* d_j). Ceci est impliqué immédiatement par le théorème d'Euler-Fermat (corollaire 5.2.2).

Exemple de cryptage avec RSA (disponible à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier **4ma1-6rsa.mws**)

On suppose qu'on travaille avec un alphabet de N symboles, alors on utilise une base d'écriture $= N$. Soient $k < l$ deux entiers strictement positifs tel que $N^k < n_j < N^l$, par exemple $k = \lceil \log_N n_j \rceil$. Alors

les blocs de k lettres correspondent aux nombres

$0 \leq m < n_j$. Tout message est présenté comme une suite de tel blocs, et on crypte par blocs $M = m \bmod n_j$. Soit $f(M) = \mathcal{E}_j(M)$, $f : \mathbb{Z}/n_j\mathbb{Z} \rightarrow \mathbb{Z}/n_j\mathbb{Z}$. L'image $f(M)$ peut être présentée comme un bloc de l lettres car $n_j < N^l$ mais pas tous les blocs de l lettres paraissent de telle façon.

EXEMPLE. Soit $N = 26$ (l'alphabet de 26 lettres), $p_j = 281$, $q_j = 167$, $n_j = 46927$, $e_j = 39423$, $d_j = 26767$, $k = 3$, $l = 4$, $N^3 = 17576 < 46927 < N^4 = 456976$.

Le mot "YES" correspond à $24 \cdot N^2 + 4 \cdot N + 18 = 16346 = m \bmod n_j$.

$$16346^{39423} \bmod 46927 = 21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 = \text{"BFIC"} \bmod n_j$$

Pour décrypter le message, l'utilisateur U_j applique

$$b \mapsto b^{d_j} \bmod n_j, \quad 21166^{26767} \bmod 46927 = 16346.$$

Signatures électroniques

Bien évidemment, on peut varier les détails de ce schéma *ad infinitum*. Par exemple, on peut construire une procédure d'authentification ("electronic signature") qui utilise une forme *signé* d'un message secret de U_i à U_j permettant U_j de convaincre une troisième personne (un "juge") que l'auteur du message est bien U_i donc ce message n'été pas falsifié par U_j lui-même. Ceci peut être crucial pour certaines transactions interbancaires.

On considère l'application \mathcal{E}_i de cryptage pour les messages adressés à U_i et soit \mathcal{D}_i l'application de décryptage de U_i . Alors on a vu que \mathcal{E}_i est publique tandis que \mathcal{D}_i est privé (la propriété de U_i). Pour tout message M on a $\mathcal{D}_i(\mathcal{E}_i(M)) = M$ et $\mathcal{E}_i(\mathcal{D}_i(M)) = M$. L'utilisateur U_i en envoyant à U_j son message M utilise comme sa signature $S = \mathcal{D}_i(M)$ et il transmet à U_j sa version cryptée $\mathcal{E}_j(S)$. A son tour, U_j d'abord calcule $S = \mathcal{D}_j(\mathcal{E}_j(S))$ et ensuite $M = \mathcal{E}_i(S)$ en utilisant la clef publique \mathcal{E}_i . Le récepteur peut convaincre un juge que M vient de U_i parce que seulement avec l'application \mathcal{E}_i on peut transformer S en un message sensé M .

De plus, le récepteur de $S = \mathcal{D}_i(M)$ ne peut pas le falsifier car il ne connaît pas \mathcal{D}_i .

Maintenant on discutera plutôt des aspects arithmétiques que les aspects informatiques de la théorie des cryptosystèmes à clef publique. On montrera que les résultats classiques de l'arithmétique peuvent être appliqués dans ce domaine.

Problème 1. Comment produire des grands nombres premiers ?

On a besoin d'une méthode vraiment efficace pour organiser une production en masse des grands nombres premiers "suffisamment aléatoires" pour permettre à un utilisateur à calculer (à l'aide d'un ordinateur) son couple customisé (p_i, q_i) et d'être sûr qu'aucun autre utilisateur ne prendra cette paire.

Problème 2. Comment factoriser grands nombres entiers ?

Ce problème est clé pour la troisième partie qui souhaite casser le cryptosystème mais aussi, bien-sûr, pour les développeurs essayant assurer la fiabilité d'un tel système.

Cours N°6. Mercredi le 10 novembre 2004

(disponible sur : <http://www-fourier.ujf-grenoble.fr/~panchish>).

Le protocole ElGamal

Ce protocole s'applique dès que l'on a un groupe cyclique fini G . On fixe g un générateur de G et on note M l'ordre du groupe G . L'ensemble \mathcal{E} est égal à G et l'ensemble \mathcal{F} est une partie du produit $G \times G$, c'est-à-dire à l'ensemble formé des couples de deux éléments de G . Alice choisit, au hasard, un élément a dans $\{0, \dots, M-1\}$ et calcule g^a . Puis elle rend publique G , g et g^a . La clé secrète \mathcal{K} est l'entier a . Pour crypter un message $x \in G$, Bob choisit un entier k au hasard dans $\{0, \dots, M-1\}$ et calcule $y_1 = g^k$, puis $y_2 = x \cdot (g^a)^k$ (ce qui est possible puisque g^a est publique). Le message crypté est le couple $(y_1, y_2) \in G \times G$.

La fonction de cryptage FSUT ("Fonction sens unique à trappe")

En d'autres termes, la fonction de cryptage FSUT ψ est donnée par

$$\psi(x) = (g^k, x \cdot (g^a)^k)$$

avec k un entier choisi au hasard dans $\{0, \dots, M-1\}$ et différent à chaque fois. Pour décrypter un tel message (y_1, y_2) , Alice calcule y_1^{-a} et obtient

$$y_1^{-a} \cdot y_2 = g^{-ak} \cdot x \cdot g^{ak} = g^{ak-ak} \cdot x = x.$$

La sécurité du protocole ElGamal

Ainsi la fonction de décryptage

$$\psi^{-1}(y_1, y_2) = y_1^{-a} \cdot y_2$$

n'est calculable que si on connaît la clé secrète \mathcal{K} .

La sécurité de ce protocole repose sur la difficulté de résoudre le *problème du logarithme discret*. Plus précisément, le problème de retrouver l'entier a étant donnés g et g^a . C'est un problème difficile dans la plupart des cas si l'ordre du G groupe est divisible par un grand nombre premier.

EXERCICES

5.1. On considère l'équation

$$X^2 - X = 0$$

Trouver toutes ses solutions dans les anneaux

$$\mathbb{Z}/100\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

5.2. Soit p, q deux nombres premiers. Combien l'équation

$$X^3 - X = 0$$

a-t-elle de solutions dans les anneaux

$$\mathbb{Z}/pq\mathbb{Z}, \mathbb{Z}/72\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}.$$

6 Primalité

On considère maintenant la question suivante : le nombre naturel donné est-il premier ou composé ?

Une méthode très ancienne du “crible” d’Eratosthène (3e siècle avant notre ère) donne la liste de tous les nombres premiers $\leq n$. Il fournit aussi le plus petit nombre premier qui divise n et donc est un test de primalité, voir ci-dessus *Construction d’une table de nombres premiers*.

Cependant elle n’est pas très efficace car elle utilise plus de n divisions, et dépend exponentiellement de la longueur de l’écriture de n .

La démonstration d’Euclide du fait que l’ensemble des nombres premiers est infini utilise la réduction *ad absurdum*. Une démonstration plus moderne est due à Euler : le produit étendu sur tous les nombres premiers

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \quad (6.1)$$

devrait être fini si l’on suppose que l’ensemble des nombres premiers est fini. Cependant, la partie droite de (6.2.1) se réduit à une série divergente $\sum_{n=1}^{\infty} n^{-1}$ par le théorème de factorisation unique.

Voici un programme en TEX pour construire une table des nombres premiers (disponible sur : <http://www-fourier.ujf-grenoble.fr/~panchish>) :

```
\newif\ifprime\newif\ifunknown
\newcount\n \newcount\p \newcount\d \newcount\a
\def\primes#1{2,~3% assume that #1 is at least 3
\n=#1 \advance\n by -2
\p=5
\loop\ifnum\n>0 \printifprime\advance\p by2 \repeat}
\def\printp{,
\ifnum\n=1 et~\fi
\number\p \advance\n by -1 }
\def\printifprime{\testprimality \ifprime\printp\fi}
\def\testprimality{{\d=3 \global\primetrue
\loop\trialdivision \ifunknown\advance\d by 2 \repeat}}
\def\trialdivision{\a=\p \divide\a by\d
\ifnum\a>\d \unknowntrue\else\unknownfalse\fi
\multiply\a by\d
\ifnum\a=\p \global\primefalse\unknownfalse\fi}
```

Par exemple, les quatre cent premiers nombres premiers sont
`\primes{400}`

Par exemple, les quatre cent premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983,

991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, et 2741

Fibonacci a suggéré (en 1202) un test plus rapide de primalité en remarquant que le plus petit diviseur non-trivial de n est $\leq \lfloor \sqrt{n} \rfloor$ donc il suffit d'essayer seulement de tels nombres.

Rapellons une propriété importante des nombres premiers.

6.1 $\mathbb{Z}/p\mathbb{Z}$ est un corps

THÉORÈME 6.1.1 *Soit $n \geq 2$ un entier. Alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

PREUVE. \Rightarrow On raisonne par l'absurde : si n n'était pas premier, on aurait une décomposition $n = ab$ avec $a, b < n$ et strictement positifs. Dans ce cas les classes $\bar{a} = a \bmod n$ et $\bar{b} = b \bmod n$ sont non nuls donc inversibles dans le corps $\mathbb{Z}/n\mathbb{Z}$, ce que contredit l'égalité $\bar{a}\bar{b} = 0$.

\Leftarrow Si n est premier, et $\bar{a} = a \bmod n$ un élément non-nul, alors n ne divise pas a , donc n et a sont premiers entre eux. Par l'identité de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$, donc $\overline{au} = 1$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, ceci dit, $\mathbb{Z}/n\mathbb{Z}$ est un corps.

6.2 Petit théorème de Fermat

La contribution essentielle suivante dans le problème de vérification de primalité est liée au petit théorème de Fermat (dix-septième siècle). Ce résultat donne une condition nécessaire de primalité

THÉORÈME 6.2.1 (PETIT THÉORÈME DE FERMAT) *Soit n un nombre premier et a premier à n . Alors*

$$a^{n-1} \equiv 1 \pmod{n}. \quad (6.2)$$

6.3 Nombres pseudopremiers de Fermat

La condition (6.2) (avec a fixe) est nécessaire mais n'est pas suffisante en général pour que n soit premier. Mais si elle n'est pas satisfaite pour n , alors sûrement n est composé (mais en général on ne connaît aucun de ses diviseurs). On appelle n *pseudopremier par rapport à a* si $\text{PGCD}(a, n) = 1$ et la condition (6.2) est satisfaite.

EXEMPLE 6.3.1 Soit $p = 323$. Est-ce que p est premier ? On calcule 2^{322} modulo 323. On organise les calculs dans une table :

i	m	m_i	$2^{2^i} \bmod 323$
0	322	0	2
1	161	1	4
2	80	0	16
3	40	0	256
4	20	0	290
5	10	0	120
6	5	1	188
7	2	0	137
8	1	1	35

Alors

$$2^{322} \equiv 4 \cdot 188 \cdot 35 \equiv 157 \pmod{323},$$

donc 323 n'est pas premier. En effet, $323 = 17 \cdot 19$.

Les nombres composés $n = 561 = 3 \cdot 11 \cdot 17, 1105 = 5 \cdot 13 \cdot 17, 1729 = 7 \cdot 13 \cdot 19$ sont pseudopremiers par rapport à tout a (premier à n). On appelle un tel nombre *nombre de Carmichael*.

En 1994 il a été démontré par Alford, Granville et Pomerance que l'ensemble des nombres de Carmichael est infini (voir [AGP94]). Par exemple, un nombre n sans diviseurs carrés est un nombre de Carmichael si et seulement si pour tout diviseur premier p de n , $p - 1$ divise $n - 1$.

De la condition (6.2) provient un test rapide *probabiliste* de vérification de primalité. Il est basé sur l'observation que les grandes puissances $a^m \bmod n$ peuvent être calculées assez rapidement.

Fermat lui-même a découvert ce théorème en étudiant les nombres $F_n = 2^{2^n} + 1$. Il a cru qu'ils étaient tous premiers, mais il n'a pu vérifier cela que pour $n \leq 4$. Plus tard Euler a trouvé une factorisation non triviale de $F_5 = 4294967297 = 641 \cdot 6700417$. Aucun nouveau nombre premier de Fermat n'a été trouvé, et beaucoup de mathématiciens croient qu'il n'y a pas plus de tels nombres premiers.



Voici quelques calculs de la factorisation de F_5, F_6, F_7, F_8 , avec le logiciel PARI

PARI/GP is free software, covered by the GNU General Public License, and comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.

Type ?12 for how to get moral (and possibly technical) support.

```
realprecision = 28 significant digits
seriesprecision = 16 significant terms
format = g0.28
```

```
parisize = 4000000, primelimit = 500000
? factor(2^32+1)
%1 =
[641 1]
```

```
[6700417 1]
```

```
? factor(264+1)
```

```
%2 =
```

```
[274177 1]
```

```
[67280421310721 1]
```

```
? factor(2128+1)
```

```
%3 =
```

```
[59649589127497217 1]
```

```
[5704689200685129054721 1]
```

```
? factor(2256+1)
```

```
%4 =
```

```
[1238926361552897 1]
```

```
[93461639715357977769163558199606896584051237541638188580280321 1]
```

(Le dernier calcul a pris quelques seconds sur mon ordinateur)

Deuxième partie

Polynômes et corps finis

7 Polynômes

7.1 Anneau de polynômes, division euclidienne

Sur un corps fini, il convient de distinguer les polynômes et les fonctions polynômes. Nous revenons donc sur la définition des polynômes.

DÉFINITION 7.1.1 *Si A un anneau commutatif, l'anneau des polynômes à une variable X sur A est l'anneau $A[X]$ formé des suites $(a_i)_{i \in \mathbb{N}}$ d'éléments de A telles que $a_i = 0$ sauf un nombre fini d'entiers i . Cet ensemble est muni de la somme*

$$(a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}} = (a_i + b_i)_{i \in \mathbb{N}}$$

et du produit

$$(a_i)_{i \in \mathbb{N}} \times (b_i)_{i \in \mathbb{N}} = \left(\sum_{i=j+k} a_j b_k \right)_{i \in \mathbb{N}}$$

On a une application injective $A \rightarrow A[X]$ qui envoie a sur $(a, 0, \dots)$, et on identifie A avec son image. Tout élément de $A[X]$ s'écrit de façon unique $\sum_{i \in \mathbb{N}} a_i X^i$, où on note par X la suite :

$$(0, 1, 0, 0, \dots).$$

Soit A un anneau. Il est commode de voir un polynôme $f(X)$ à coefficients dans A une expression formelle du type

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$$

qui est donnée par la suite de ces coefficients $a_0, a_1, \dots, a_n \in A$, $n \in \mathbb{N}$ telle que presque tous a_n (sauf un nombre fini) sont nuls.

Si tous les coefficients a_i sont nuls on appelle $f(X)$ polynôme nul : $f = 0$. Si $f(X)$ est non-nul soit $a_n \neq 0$.

DÉFINITION 7.1.2 *Le plus grand indice n avec cette propriété est appelé le degré de $f(X)$ et il est noté $\deg f$. Le degré du polynôme nul n'est pas défini, mais parfois on pose $\deg 0 = -\infty$.*

L'anneau $A[X]$ est défini comme l'ensemble des expressions $f(X)$ ci-dessus avec des opérations données par les règles suivants : si

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0, \quad a_n \neq 0$$

$$g(X) = b_s X^s + b_{s-1} X^{s-1} + \dots + b_0, \quad b_s \neq 0$$

deux polynômes et si par exemple $n \geq s$, on appelle leur somme le polynôme

$$(f + g)(X) = f(X) + g(X) = c_n X^n + c_{n-1} X^{n-1} + \dots + c_0,$$

dont les coefficients sont obtenus par l'addition des coefficients correspondants de X dans f et dans g , c'est à dire $c_i = a_i + b_i$, $i = 0, 1, \dots, n$, où pour $i > s$ les coefficients b_i sont considérés comme zéros.

Le produit des polynômes $f(X)$ et $g(X)$ est le polynôme

$$(fg)(X) = f(X) \cdot g(X) = d_{n+s}X^{n+s} + d_{n+s-1}X^{n+s-1} + \dots + d_0,$$

où

$$d_i = \sum_{k+l=i} a_k b_l,$$

et les coefficients a_i, b_j sont considérés comme zéros pour $i > n$, et $j > s$, $d_0 = a_0 b_0$, $d_1 = a_0 b_1 + a_1 b_0$, \dots , $d_{n+s} = a_n b_s$.

THÉOREME 7.1.3 *Si l'anneau A n'a pas de diviseurs de zéro, l'anneau des polynômes $A[X]$ aussi n'a pas de diviseurs de zéro. Le degré du produit des polynômes non nuls est égal à la somme de ces degrés.*

Démonstration est directement entraîné des formules ci-dessus, en particulière de $d_{n+s} = a_n b_s$, où $n = \deg f$, $s = \deg g$.

L'anneau A peut être s'identifié avec un sous-anneau de $A[X]$ formé par des constantes (polynômes de degré nul et le polynôme nul). Ceci implique que la multiplication des éléments $a \in A$ par $f(X) \in A[X]$ est aussi défini. En particulier, si $A = K$ est un corps, l'anneau $K[X]$ est aussi un espace vectoriel. Du point de vu de la structure algébrique l'anneau $K[X]$ devient un algèbre de dimension infini sur K , c'est à dire, un anneau et un espace vectoriel en même temps dans lequel la multiplication d'éléments commute avec multiplication par des constantes.

7.2 Division euclidienne sur les anneaux

Division des polynômes avec reste

PROPOSITION 7.2.1 *Soit A un anneau commutatif intègre. On se donne un polynôme*

$$P(X) = \sum_{i=0}^d a_i X^i$$

à coefficients dans A tel que a_d soit un élément inversible de A . Alors pour tout polynôme $f(X)$ de $A[X]$ il existe une unique paire $(Q, R) \in A[X]^2$ telle que

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P$$

PREUVE. Existence. Nous allons procédé par récurrence sur le degré de f . Si $\deg f < d$, alors $(0, f)$ convient. Sinon on écrit

$$f = \sum_{i=0}^n b_i X^i \text{ avec } b_n \neq 0 \text{ et } n \geq d.$$

Alors

$$f - b_n a_d^{-1} X^{n-d} P = PQ_1 + R_1 \text{ avec } R_1 = 0 \text{ ou } \deg R_1 < d.$$

La paire $(Q_1 + b_n a_d^{-1} X^{n-d}, R_1)$ convient.

Unicité. Si

$$PQ_0 + R_0 = PQ_1 + R_1$$

avec $\deg R_0 < \deg P$ et $\deg R_1 < \deg P$ alors $P(Q_0 - Q_1) = (R_1 - R_0)$. Comme le coefficient dominant de P est inversible, on a $\deg(P(Q_0 - Q_1)) = \deg P + \deg(Q_0 - Q_1)$ mais ce degré est strictement inférieur à celui de P si et seulement si $Q_0 - Q_1 = 0$, c'est à dire, $Q_0 = Q_1$, ce qui entraîne que $R_0 = R_1$.

EXEMPLE. Illustrons sur un exemple la façon d'effectuer une telle division dans $\mathbb{Z}[X]$:

$$\begin{array}{r|l}
 \begin{array}{r}
 3X^4 + 7X^3 - 7X^2 + 16X - 5 \\
 -3X^4 - 9X^3 + 6X^2 \\
 \hline
 -2X^3 - X^2 + 16X - 5 \\
 2X^3 + 6X^2 - 4X \\
 \hline
 5X^2 + 12X - 5 \\
 -5X^2 - 15X + 10 \\
 \hline
 -3X + 5
 \end{array} & \begin{array}{l}
 X^2 + 3X - 2 \\
 \hline
 3X^2 - 2X + 5
 \end{array}
 \end{array}$$

Division euclidienne dans $K[x]$ sur un corps K

THÉOREME 7.2.2 *Pour tous polynômes $f(X)$ et $P(X)$ tels que $P(X)$ soit non nul à coefficients dans un corps K il existe une unique paire $(Q, R) \in A[X]^2$ telle que*

$$f = PQ + R \text{ avec } R = 0 \text{ ou } \deg R < \deg P$$

Les polynômes $Q(X)$ et $R(X)$ sont uniquement déterminés par cette condition.

DÉFINITION 7.2.3 *Le polynôme $Q(X)$ est appelé le quotient de la division $f(X)$ par $Q(X)$, et $R(X)$ le reste.*

Divisibilité des polynômes

Soit K un corps. Soient $f(X), \phi(X) \in K[X]$. Si le reste de la division de $f(X)$ par $\phi(X)$ est nul, on dit que $f(X)$ est divisible par $\phi(X)$ où de même que $\phi(X)$ divise $f(X)$, la notation : $\phi \mid f$. La condition $\phi \mid f$ est équivalente au fait qu'il existe un polynôme $\psi(X)$ tel que $f(X) = \phi(X) \cdot \psi(X)$.

La définition implique directement les propriétés suivantes de la divisibilité :

- 1) Si f est divisible par g , et g est divisible par h , f est divisible par h .
- 2) Si f et g sont divisibles par ϕ , leur somme et leur différence sont divisibles par ϕ .
- 3) Tout polynôme est divisible par n'importe quel polynôme de degré zéro.
- 4) $f(X)$ divise $g(X)$ et $g(X)$ divise $f(X)$ en même temps si et seulement si $g(X) = cf(X)$, où $c \in K^*$ est un élément inversible.
- 5) Les ensembles de diviseurs de $f(X)$ et $cf(X)$ coïncident.

On appelle le pgcd (le plus grand diviseur commun) de $f(X)$ et $g(X)$ le polynôme $d(X)$ tel que d divise f et g , et d est divisible par tout autre diviseur commun de ces polynômes.

THÉOREME 7.2.4 *Pour tous polynômes f et g dans $K[X]$ sur un corps K il existe leur pgcd que est uniquement déterminé à constante multiplicative près.*

C'est une propriété générale dans les anneaux euclidiens.

7.3 Valeurs et racines d'un polynôme

PROPOSITION 7.3.1 *Soit A un anneau commutatif. On se donne un polynôme*

$$f(X) = \sum_{i=0}^n a_i X^i$$

à coefficients dans A , et soit c un élément de A . Alors la valeur de f en c est définie comme $f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_0 \in A$.

(a) L'application

$$\psi_c : A[X] \rightarrow A, f \mapsto f(c) = \sum_{i=0}^n a_i c^i \in A$$

est un seul morphisme d'anneaux tel que la restriction de ψ_c sur le sous-anneau $A \subset A[X]$ soit triviale, et que $\psi_c(X) = c$.

(b) Réciproquement, pour tout morphisme d'anneaux $\psi : A[X] \rightarrow A$ tel que la restriction de ψ sur le sous-anneau $A \subset A[X]$ soit triviale, il existe un seul $c \in A$ tel que $\psi = \psi_c$.

PREUVE de la proposition 7.3.1 découle de la définition 4.1.2 de morphisme d'anneaux.

Fonctions polynômes.

DÉFINITION 7.3.2 (a) L'application

$$f : A \rightarrow A, c \mapsto f(c)$$

notée par la même lettre f , est dit la fonction polynôme.

(b) Si $f(c) = 0$ (c'est à dire f s'annule en c), on appelle c racine de f .

REMARQUE. La fonction polynôme en général ne définit pas le polynôme de manière unique. Par exemple, sur un corps fini K , il convient de distinguer les polynômes et les fonctions polynômes.

Soit par exemple $A = K = \mathbb{F}_2 = \{0, 1\}$ (le corps de deux éléments). Considérons le polynôme $f(X) = X^2 + X + 1$, alors $f(0) = 1$ et $f(1) = 1$ c'est à dire f définit une fonction constante sur K mais $f(X)$ n'est pas une constante (polynôme de degré zéro) comme polynôme.

THÉORÈME 7.3.3 Soit $A = K$ un corps. Si $f(X) \in K[X]$, le reste de la division de $f(X)$ par $(X - c)$ est égal à $f(c)$. En particulier, c est une racine de $f(X)$ si et seulement si $f(X)$ est divisible par $X - c$.

Démonstration est impliquée par l'unicité de la division avec reste :

$$f(X) = q(X)(X - c) + r,$$

où $r = f(c)$.

COROLLAIRE 7.3.4 Si $f(X) \in K[X]$, le nombre des racines $c \in K$ est majoré par le degré $\deg(f)$.

Démonstration est impliquée par l'unicité de décomposition en facteurs irréductibles dans un anneau euclidien.

Méthode d'Hörner

permet de trouver facilement le quotient $q(X)$ de la division par $X - c$

$$f(X) = q(X)(X - c) + r,$$

et la valeur $r = f(c)$.

On considère le polynôme

$f(X) = \sum_{i=0}^n a_i X^i$, et sa valeur en $X = c$; on calcule $f(c)$ de façon suivante : soient

$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$, $a_n \neq 0$ un polynôme, et on cherche un autre polynôme $q(X) = b_{n-1} X^{n-1} + b_{n-2} X^{n-2} + \dots + b_0$, $b_{n-1} \neq 0$ tel que

$$f(X) = (X - c)q(X) + r,$$

En comparant les coefficients des puissances de X on obtient

$$a_n = b_{n-1}, \quad a_{n-1} = b_{n-2} - cb_{n-1}, \quad \dots,$$

$$a_1 = b_0 - cb_1, \quad a_0 = r - cb_0, \quad r = f(c).$$

Ceci implique

$$b_{n-1} = a_n, \quad b_{n-k} = cb_{n-k+1} + a_{n-k} \quad (k = 2, \dots, n)$$

Il est commode de faire le tableau suivant (le schéma de Hörner)

	a_n	a_{n-1}	\dots	a_1	a_0
c	$b_{n-1} = a_n$	$b_{n-2} = cb_{n-1} + a_{n-1}$	\dots	$b_0 = cb_1 + a_1$	$f(c) = cb_0 + a_0$

La formule de Taylor

Soit K un corps. On se donne un polynôme

$$f(X) = \sum_{i=0}^n a_i X^i$$

à coefficients dans K , et soit c un élément de K . Alors il existe $b_1, \dots, b_n \in K$ tels que

$$f(X) = f(c) + b_1(X - c) + b_2(X - c)^2 + \dots + b_n(X - c)^n,$$

avec la propriété

$$k!b_k = f^{(k)}(c), \quad k = 1, \dots, n, \tag{7.1}$$

où

$$f'(X) = na_n X^{n-1} + (n-1)a_{n-1} X^{n-2} + \dots + a_1$$

est la dérivée formelle de $f(X)$.

PREUVE. L'existence des $b_1, \dots, b_n \in K$ découle de la division euclidienne dans $K[X]$, par récurrence à partir de

$$f(X) = (X - c)q(X) + f(c).$$

Ensuite, on déduit la formule (7.1) par récurrence à partir de l'identité :

$$f(X) = f(c) + b_1(X - c) + b_2(X - c)^2 + \dots + b_n(X - c)^n,$$

en utilisant l'égalité formelle $((X - c)^k)' = k(X - c)^{k-1}$.

7.4 Formule d'interpolation de Lagrange

La formule d'interpolation de Lagrange donne un polynôme sur un corps K de degré inférieure ou égale à n qui prend pour les valeurs distinctes de la variable X en $\alpha_0, \alpha_1, \dots, \alpha_n \in K$, les valeurs $\beta_0, \beta_1, \dots, \beta_n \in K$. La solution est donnée par le polynôme de Lagrange

$$f(X) = \sum_{i=0}^n \beta_i \frac{(X - \alpha_0) \dots (X - \alpha_{i-1})(X - \alpha_{i+1}) \dots (X - \alpha_n)}{(\alpha_i - \alpha_0) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots (\alpha_i - \alpha_n)} \quad (7.2)$$

En effet son degré est inférieure ou égale à n , et $f(\alpha_i) = \beta_i$ ($i = 0, 1, \dots, n$).

PROPOSITION 7.4.1 *Le polynôme de Lagrange (7.2) est l'unique polynôme*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in K[X]$$

de degré $\leq n$ tel que $f(\alpha_i) = \beta_i$ ($i = 0, 1, \dots, n$) pour arbitraires distincts éléments α_i ($i = 0, 1, \dots, n$) du corps K et pour arbitraires $\beta_i \in K$ ($i = 0, 1, \dots, n$).

En effet si l'on considère les coefficients a_j ($j = 0, 1, \dots, n$) comme des inconnues on obtiendrait le système des équations linéaires suivant :

$$\begin{cases} f(\alpha_0) = a_n \alpha_0^n + a_{n-1} \alpha_0^{n-1} + \dots + a_0 = \beta_0 \\ f(\alpha_1) = a_n \alpha_1^n + a_{n-1} \alpha_1^{n-1} + \dots + a_0 = \beta_1 \\ \dots \dots \dots \\ f(\alpha_n) = a_n \alpha_n^n + a_{n-1} \alpha_n^{n-1} + \dots + a_0 = \beta_n \end{cases}$$

Le déterminant de ce système carré coïncide (à signe près) avec le déterminant de Vandermonde

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \dots & \alpha_n \\ \alpha_0^2 & \alpha_1^2 & \dots & \alpha_n^2 \\ \dots & \dots & \dots & \dots \\ \alpha_0^n & \alpha_1^n & \dots & \alpha_n^n \end{vmatrix} = \prod_{0 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

qui est non-nul, d'où l'existence et l'unicité des coefficients cherchés a_j ($j = 0, 1, \dots, n$) du polynôme $f(X)$ (dans le corps K).

PROPOSITION 7.4.2 Soit K un corps infini. Alors un polynôme $f(X)$ est uniquement déterminé par la fonction polynôme correspondente $c \mapsto f(c) : K \rightarrow K$.

REMARQUE. Au contraire, sur un corps fini K toute fonction $f : K \rightarrow K$ est polynomiale, mais le polynôme correspondant f n'est pas uniquement déterminé par cette fonction, car il existe des polynômes non-nuls représentant la fonction identiquement nulle. Par exemple, le polynôme non-nulle de degré p

$$f(X) = X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$$

s'annule en tous les points du corps $K = \mathbb{Z}/p\mathbb{Z}$.

7.5 Anneau de polynômes à plusieurs variables

DÉFINITION 7.5.1 Soit A un anneau commutatif. L'anneau des polynômes à n variables peut être défini par récurrence comme

$$A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n].$$

Si $\alpha = (\alpha_1, \dots, \alpha_n)$ appartient à \mathbb{N}^n , on note X^α pour le produit $\prod_{i=1}^n X_i^{\alpha_i}$. Tout polynôme s'écrit alors de manière unique

$$P = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$

avec $(a_\alpha)_{\alpha \in \mathbb{N}^n}$ une famille de $A^{\mathbb{N}^n}$ telle que $a_\alpha = 0$ sauf pour un nombre fini d'éléments $\alpha \in \mathbb{N}^n$.

Pour un élément $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, on note $|\alpha| = \sum_{i=1}^n \alpha_i$. On définit alors le degré total d'un polynôme non nul $P = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$ comme

$$\deg(P) = \sup\{|\alpha| \mid a_\alpha \neq 0\}$$

PROPOSITION 7.5.2 Soit A un anneau commutatif. Pour tous polynômes non nuls

$$P, Q \in A[X_1, \dots, X_n],$$

on a

$$(i) \text{ si } P + Q \neq 0, \text{ alors } \deg(P + Q) \leq \sup(\deg P, \deg Q)$$

avec l'égalité si $\deg P \neq \deg Q$;

$$(ii) \deg(PQ) \leq \deg P + \deg Q$$

avec l'égalité si A est intègre.

DÉFINITION 7.5.3 Soit A un anneau commutatif. Un polynôme non nul

$$P \in A[X_1, \dots, X_n],$$

est dit homogène de degré d si et seulement si

$$\alpha \in \mathbb{N}^n, |\alpha| \neq d \Rightarrow a_\alpha = 0.$$

PROPOSITION 7.5.4 Soient A et B deux anneaux commutatifs, $\phi : A \rightarrow B$ un morphisme d'anneaux, et b_1, \dots, b_n des éléments de B , il existe un unique morphisme d'anneaux

$$\psi : A[X_1, \dots, X_n] \rightarrow B,$$

$$P = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha \mapsto P(b_1, \dots, b_n) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha b_1^{\alpha_1} \dots b_n^{\alpha_n},$$

tel que la restriction de ψ sur le sous-anneau $A \subset A[X_1, \dots, X_n]$ coïncide avec ϕ .

Exemples de calculs avec polynômes de plusieurs variables (disponible à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-8poly.mws)

> restart;

EXEMPLE. On considère l'anneau $\mathbb{Z}[X_1, X_2, X_3, X_4]$. On pose

> Q:=mul(X[1]-i*X[2]-i*(X[3]+X[4]+1)+1,
> i=0..2) ;

$$Q := (X_1 + 1)(X_1 - X_2 - X_3 - X_4)(X_1 - 2X_2 - 2X_3 - 2X_4 - 1)$$

• Pour développer Q en monômes, on utilise :

> expand(Q) ;

$$\begin{aligned} & -2X_1X_2 - 2X_1X_3 - 2X_1X_4 - 3X_1^2X_2 - 3X_1^2X_3 - 3X_1^2X_4 + 2X_1X_2^2 + 2X_1X_3^2 \\ & + 2X_1X_4^2 + 2X_2^2 + 4X_2X_3 + 4X_2X_4 + 2X_3^2 + 4X_3X_4 + 2X_4^2 - X_1 + X_2 + X_3 \\ & + X_4 + 4X_1X_2X_3 + 4X_1X_2X_4 + 4X_1X_3X_4 + X_1^3 \end{aligned}$$

• Pour développer Q en monômes dans l'ordre lexicographique, on utilise :

> sort(expand(Q), [X[1], X[2], X[3], X[4]], plex) ;

$$\begin{aligned} & X_1^3 - 3X_1^2X_2 - 3X_1^2X_3 - 3X_1^2X_4 + 2X_1X_2^2 + 4X_1X_2X_3 + 4X_1X_2X_4 - 2X_1X_2 \\ & + 2X_1X_3^2 + 4X_1X_3X_4 - 2X_1X_3 + 2X_1X_4^2 - 2X_1X_4 - X_1 + 2X_2^2 + 4X_2X_3 \\ & + 4X_2X_4 + X_2 + 2X_3^2 + 4X_3X_4 + X_3 + 2X_4^2 + X_4 \end{aligned}$$

>

• Pour développer Q suivant les puissances X_1 , on utilise :

> collect(%, X[1]) ;

$$\begin{aligned} & X_1^3 + (-3X_3 - 3X_4 - 3X_2)X_1^2 + \\ & (-1 - 2X_3 + 2X_4^2 - 2X_4 + 2X_2^2 + 4X_2X_3 + 4X_2X_4 - 2X_2 + 2X_3^2 + 4X_3X_4)X_1 \\ & + X_2 + 2X_2^2 + 4X_2X_3 + 4X_2X_4 + 2X_4^2 + 2X_3^2 + 4X_3X_4 + X_3 + X_4 \end{aligned}$$

• Pour réduire Q modulo 3, on utilise :

> Expand(Q) mod 3 ;

```

X1^3 + 2 X1 X2^2 + X1 X2 X3 + X1 X2 X4 + X1 X2 + 2 X1 X3^2 + X1 X3 X4 + X1 X3 + 2 X1 X4^2
+ X1 X4 + 2 X1 + 2 X2^2 + X2 X3 + X2 X4 + X2 + 2 X3^2 + X3 X4 + X3 + 2 X4^2 + X4
• Pour développer Q suivant les puissances de X2 :
> collect(expand(Q),X[2]);

(2 X1 + 2) X2^2 + (1 + 4 X3 + 4 X4 - 3 X1^2 + 4 X1 X3 + 4 X1 X4 - 2 X1) X2 + X1^3 + 2 X3^2
- 3 X1^2 X3 - 3 X1^2 X4 + 2 X1 X3^2 + 4 X1 X3 X4 + 4 X3 X4 + X3 - 2 X1 X4 - X1
- 2 X1 X3 + 2 X1 X4^2 + 2 X4^2 + X4
>

• Pour calculer le degré total de Q, on utilise :
> degree(Q, [X[1],X[2],X[3],X[4]]);

3
> degree(Q,X[4]);

2
> degree(Q,X[1]);

3
> degree(Q, [X[1],X[4]]);

3

• Pour trouver le quotient de la division euclidienne de Q par un polynôme de terme dominant
inversible (par exemple X1^2 + X1X2 + X3) par rapport à la variable X1, on utilise :
> quo(Q,X[1]^2+X[1]*X[2]+X[3], X[1]);

X1 - 3 X3 - 3 X4 - 4 X2

• Pour trouver le reste de la division euclidienne de Q par le polynôme de terme dominant inversible
X1^2 + X1X2 + X3 par rapport à la variable X1, on utilise :
> rem(Q,X[1]^2+X[1]*X[2]+X[3], X[1]);

(-1 - 3 X3 + 2 X4^2 - 2 X4 + 6 X2^2 + 7 X2 X3 + 7 X2 X4 - 2 X2 + 2 X3^2 + 4 X3 X4) X1 + X2
+ 2 X2^2 + 8 X2 X3 + 4 X2 X4 + 2 X4^2 + 5 X3^2 + 7 X3 X4 + X3 + X4

```

Vérification :

```

> (X[1]^2+X[1]*X[2]+X[3])*(X[1]-3*X[3]-3*X[4]-4*X[2])+
> ^2-2*X[4]+6*X[2]^2+7*X[2]*X[3]+7*X[2]*X[4]-2*X[2]+2*X[3]^2+4*X[3]*X[4]
> )*X[1]+X[2]+2*X[2]^2+8*X[2]*X[3]+4*X[2]*X[4]+2*X[4]^2+5*X[3]^2+7*X[3]*X[4]
> X[4]+X[3]+X[4];

(X1^2 + X1 X2 + X3) (X1 - 3 X3 - 3 X4 - 4 X2) +
(-1 - 3 X3 + 2 X4^2 - 2 X4 + 6 X2^2 + 7 X2 X3 + 7 X2 X4 - 2 X2 + 2 X3^2 + 4 X3 X4) X1
+ X2 + 2 X2^2 + 8 X2 X3 + 4 X2 X4 + 2 X4^2 + 5 X3^2 + 7 X3 X4 + X3 + X4
> %-Q;

```



```

(X1^2 + X1 X2 + X3) (X1 - 3 X3 - 3 X4 - 4 X2) +
(-1 - 3 X3 + 2 X4^2 - 2 X4 + 6 X2^2 + 7 X2 X3 + 7 X2 X4 - 2 X2 + 2 X3^2 + 4 X3 X4) X1
+ X2 + 2 X2^2 + 8 X2 X3 + 4 X2 X4 + 2 X4^2 + 5 X3^2 + 7 X3 X4 + X3 + X4
- (X1 + 1) (X1 - X2 - X3 - X4) (X1 - 2 X2 - 2 X3 - 2 X4 - 1)
> expand(%);
0

```

EXERCICES

- 7.1 Soit P un polynôme dans $A[X]$, A anneau commutatif. Montrer que $P(P(X)) - X$ est divisible par $P(X) - X$
- 7.2 Soit P un polynôme dans $\mathbb{R}[X]$ tel que $P(1) = 1$ et $P(2) = 4$. On pose $B(X) = X^2 - 3X + 2$. Déterminer le reste de la division de P par B .
- 7.3 Soit P un polynôme dans $\mathbb{Q}[X]$ tel que $P(X) = (X - a)^2(X - b)$ où $a, b \in \mathbb{C}$. En considérant $P'(X)$, montrer que $a, b \in \mathbb{Q}$.
- 7.4 Soit

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Z}[X],$$

et p/q fraction irréductible telle que $P(p/q) = 0$. Montrer que q divise a_n , p divise a_0 , et pour tout m , $p - mq$ divise $P(m)$.

- 7.5 Dans $\mathbb{R}[X]$ montrer qu'il existe un unique polynôme P de degré ≤ 7 tel que $P+1$ soit divisible par $(X-1)^4$, et $P-1$ soit divisible par $(X+1)^4$. Déterminer P
- 7.6 Soit $a \in \mathbb{Z}$, n un entier ≥ 2 tel que $\text{pgcd}(a, n) = 1$ Montrer que n est premier si et seulement si les polynômes $(X+a)^n$, et $X^n + a$ sont congrus modulo n .

8 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

8.1 Racines primitives

L'idée clé : *Il existe un élément de $(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p - 1$.*

Polynômes sur $\mathbb{Z}/p\mathbb{Z}$

PROPOSITION 8.1.1 *Soit $f \in (\mathbb{Z}/p\mathbb{Z})[x]$ un polynôme non nul sur le corps $\mathbb{Z}/p\mathbb{Z}$. Alors il existe au plus $\deg(f)$ éléments $\alpha \in \mathbb{Z}/p\mathbb{Z}$ tels que $f(\alpha) = 0$.*

PREUVE (comparer avec Corollaire 7.3.4). On procède par récurrence sur $\deg(f)$. Les cas $\deg(f) = 0, 1$ sont clairs. On écrit $f = a_n x^n + \dots + a_1 x + a_0$. Si $f(\alpha) = 0$ alors

$$\begin{aligned} f(x) &= f(x) - f(\alpha) = a_n(x^n - \alpha^n) + \dots + a_1(x - \alpha) + a_0(1 - 1) \\ &= (x - \alpha)(a_n(x^{n-1} + \dots + \alpha^{n-1}) + \dots + a_1) = (x - \alpha)g(x), \end{aligned}$$

pour un polynôme $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Ensuite, on suppose que $f(\beta) = 0$ avec $\beta \neq \alpha$. Alors $(\beta - \alpha)g(\beta) = 0$, donc, puisque $\beta - \alpha \neq 0$ (et $\text{pgcd}(\beta - \alpha, p) = 1$, on a $g(\beta) = 0$.

Par l'hypothèse de récurrence, g possède au plus $n - 1$ racines, donc il y a au plus $n - 1$ possibilités pour β . Il vient que f a au plus n racines.

EXEMPLE 8.1.2 *Trouver les racines de*

$$f = x^4 - x^3 + x^2 + x + 1 \in (\mathbb{Z}/3\mathbb{Z})[x].$$

Solution : $f(0) = 1, f(1) = 0, f(2) = 0$, donc les racines sont $\{1, 2\}$. De plus,

$$f = (x + 1)(x + 2)(x^2 + 2x + 2).$$

Bien-sûr, on peut factoriser rapidement ce polynôme mod 3 en Maple :

```
> Factor(x^4 - x^3 + x^2 + x + 1) mod 3;
```

$$(x^2 + 2x + 2)(x + 2)(x + 1)$$

PROPOSITION 8.1.3 *Soit p un nombre premier, et soit d un diviseur de $p - 1$. Alors $f(x) = x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ possède exactement d racines.*

PREUVE. Soit e tel que $de = p - 1$. On a

$$\begin{aligned} x^{p-1} - 1 &= (x^d)^e - 1 \\ &= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \dots + 1) \\ &= (x^d - 1)g(x), \end{aligned}$$

où $\deg(g(x)) = p - 1 - d$. Rappelons que le petit théorème de Fermat implique : $x^{p-1} - 1$ possède exactement $p - 1$ racines dans $\mathbb{Z}/p\mathbb{Z}$. Par proposition 8.1.1, $g(x)$ possède *au plus* $p - 1 - d$ racines et $x^d - 1$ a au plus d racines, donc $g(x)$ possède exactement $p - 1$ racines et $x^d - 1$ possède exactement d racines, CQFD.

ATTENTION : L'analogie de ce théorème est faux pour un $f \in (\mathbb{Z}/n\mathbb{Z})[x]$ avec n composé. Par exemple, si $n = n_1 \cdot n_2$ avec $n_1, n_2 \neq 1$, alors $f = n_1 x$ possède au moins *deux* zéros distincts, notamment 0 et $n_2 \neq 0$.

Un autre exemple : $x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[X]$ possède 4 racines : $x = \bar{1}, x = \bar{3}, x = \bar{5}, x = \bar{7}$.

La structure de $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p - 1\}$

Dans cette section on montrera que le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

DÉFINITION 8.1.4 Une racine primitive modulo p est un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $p - 1$.

LEMME 8.1.5 On suppose que $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ sont d'ordre r et s , respectivement, et que $\text{pgcd}(r, s) = 1$. Alors ab est d'ordre rs .

C'est un fait général sur les éléments d'un groupe, qui *commutent entre eux*.

PREUVE. Lorsque $(ab)^{rs} = a^{rs}b^{rs} = 1$, l'ordre de ab est un diviseur $r_1 s_1$ de rs , où $r_1 \mid r$ et $s_1 \mid s$. Donc

$$a^{r_1 s_1} b^{r_1 s_1} = (ab)^{r_1 s_1} = 1.$$

On élève les deux parties en la puissance r_2 , où $r_1 r_2 = r$. Alors

$$a^{r_1 r_2 s_1} b^{r_1 r_2 s_1} = 1,$$

donc, puisque $a^{r_1 r_2 s_1} = (a^{r_1 r_2})^{s_1} = 1$,

$$b^{r_1 r_2 s_1} = 1.$$

Ceci implique que $s \mid r_1 r_2 s_1$, et, car $\text{pgcd}(s, r_1 r_2) = 1$, il vient que $s = s_1$. Un argument similaire montre que $r = r_1$, donc l'ordre de ab est rs .

THÉORÈME 8.1.6 Pour tout nombre premier p il existe une racine primitive mod p . Autrement dit, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p - 1$.

PREUVE. On écrit

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$$

comme un produit de nombres premiers distincts q_i .

Par la proposition 8.1.3, le polynôme $x^{q_i^{n_i}} - 1$ a exactement $q_i^{n_i}$ racines, et le polynôme $x^{q_i^{n_i-1}} - 1$ a exactement $q_i^{n_i-1}$ racines. Alors il existe un $a_i \in \mathbb{Z}/p\mathbb{Z}$ tel que $a_i^{q_i^{n_i}} = 1$ mais $a_i^{q_i^{n_i-1}} \neq 1$. Un tel a_i est d'ordre $q_i^{n_i}$. Pour tout $i = 1, \dots, r$, on choisit un tel a_i . Lorsque'on applique le lemme 8.1.5 plusieurs fois, on voit que

$$a = a_1 a_2 \cdots a_r$$

est d'ordre $q_1^{n_1} \cdots q_r^{n_r} = p - 1$, donc a est une racine primitive.

REMARQUE. Il existe $\varphi(p - 1)$ racines primitives modulo p , puisque il y a $q_i^{n_i} - q_i^{n_i-1}$ façons de choisir a_i . Pour le voir, on peut simplement utiliser le fait que le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p - 1)\mathbb{Z}$ contient

$\varphi(p-1)$ générateurs (voir la proposition 5.2.1). Sinon, on vérifie que deux choix différents de suites a_1, \dots, a_r définissent deux racines primitives différentes. On suppose que

$$a_1 a_2 \cdots a_r = a'_1 a'_2 \cdots a'_r,$$

avec a_i, a'_i d'ordre $q_i^{n_i}$, pour $i = 1, \dots, r$. Lorsqu'on élève les deux parties de l'égalité en la puissance $s = q_2^{n_2} \cdots q_r^{n_r}$, on voit que $a_1^s = a'_1{}^s$. Puisque $\text{pgcd}(s, q_1^{n_1}) = 1$, il existe un t tel que $st \equiv 1 \pmod{q_1^{n_1}}$. Il vient que

$$a_1 = (a_1^s)^t = (a_1'^s)^t = a_1'.$$

Par la simplification de a_1 dans les deux parties, on voit que $a_2 \cdots a_r = a'_2 \cdots a'_r$; on répète cet argument si nécessaire, et on montre que $a_i = a'_i$ pour tout i . Donc les choix différents de a_i amènent aux choix différents de racines primitives; autrement dit, si les racines primitives sont les mêmes, alors les a_i coïncident.

Le nombre total des racines primitives est donc égale à

$$(q_1^{n_1} - q_1^{n_1-1}) \cdots (q_r^{n_r} - q_r^{n_r-1}) = \varphi(p-1)$$

puisque

$$p-1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}.$$

Exemples de racines primitives mod 17 (disponible à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple>
dans le fichier 4ma1-09primr.mws)

Il existe $\varphi(16) = 2^4 - 2^3 = 8$ racines primitives mod 17 :

```
> with(numtheory):d:=17;i:=1;for n from 1 to d-1 do
> if (order(n,d)=d-1) then
> printf("i=%d,n=%d mod %d\n"
> ,i,n,d);
> i:=i+1;
> fi;
> od;
```

i=1,n=3 mod 17

i=2,n=5 mod 17

i=3,n=6 mod 17

i=4,n=7 mod 17

i=5,n=10 mod 17

i=6,n=11 mod 17

i=7,n=12 mod 17

i=8,n=14 mod 17

EXEMPLE 8.1.7 Dans cet exemple, on donne une illustration pour la preuve du théorème 8.1.6 dans le cas $p = 13$. On a

$$p-1 = 12 = 2^2 \cdot 3.$$

Le polynôme $x^4 - 1$ a les racines $\{1, 5, 8, 12\}$ et $x^2 - 1$ a les racines $\{1, 12\}$, donc on prend $a_1 = 5$. Le polynôme $x^3 - 1$ a les racines $\{1, 3, 9\}$, donc on pose $a_2 = 3$. Finalement, $a = 5 \cdot 3 = 15 \equiv 2 \pmod{13}$. On remarque que les puissances successives de 2 sont

2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1,

donc 2 est en réalité d'ordre 12.

EXEMPLE 8.1.8 Le résultat est faux si, par exemple p est remplacé par une grande puissance de 2. Les éléments de $(\mathbb{Z}/8\mathbb{Z})^*$ tous sont d'ordre divisant 2, mais $\varphi(8) = 4$.

THÉORÈME 8.1.9 Soit p^n une puissance d'un nombre premier impaire. Alors il existe un élément de $(\mathbb{Z}/p^n\mathbb{Z})^*$ d'ordre $\varphi(p^n)$, c'est à dire, $(\mathbb{Z}/p^n\mathbb{Z})^*$ est cyclique.

(en exercice).

Exemples de calcul du logarithme discret dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ (disponible à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-10dislog.mws)

%%%%%%%%%

LOGARITHME DISCRET

```
> restart;with(numtheory);
```

Warning, the protected name order has been redefined and unprotected

[GIgcd, bigomega, cfrac, cfracpol, cyclotomic, divisors, factorEQ, factorset, fermat, imagunit, index, integral_basis, invcfrac, invphi, issqrfree, jacobi, kronecker, lambda, legendre, mcombine, mersenne, minkowski, mipolys, mlog, mobius, mroot, msqrt, nearestp, nthconver, nthdenom, nthnumer, nthpow, order, pdexpand, phi, pi, pprimroot, primroot, quadres, rootsunity, safeprime, sigma, sq2factor, sum2sqr, tau, thue]

Examples

```
> with(numtheory):
> order(13,100);
20
> order(5,8);
2
> order(8,12);
FAIL
> primroot(20,239);
21
> order(%,239);
238
> phi(239);
238
```

```

> dislog:=proc(x::integer,g::integer,p::integer)
> local s, t, n,d;
> s:=g;t:=order(g,p);
> for n from 1 to t do
> if x=s then d:=n;
> fi;
> s:= s*g mod p; od;
> return (d);
> end proc;

      dislog := proc(x : integer, g : integer, p : integer)
      local s, t, n, d;
      s := g;
      t := order(g, p);
      for n to t do if x = s then d := n end if; s := s * g mod p end do;
      return d
      end proc
> dislog(18,5,23);
                                     12
> primroot(9048610007);
                                     5
> dislog(7320,2,9587);
                                     389
> 5^678 mod 9048610007;
                                     3757843958
> nextprime(1000);
                                     1009
> dislog(15625,5,9048610007);
Warning, computation interrupted
> primroot(1009);
                                     11
> 11^345 mod 1009;
                                     23
> dislog(23,11,1009);
                                     345

```

GP/PARI CALCULATOR Version 2.1.1 (released) i686 running cygwin (ix86 kernel) 32-bit version
(readline v4.0 enabled, extended help not available)

Copyright (C) 2000 The PARI Group

PARI/GP is free software, covered by the GNU General Public License, and
comes WITHOUT ANY WARRANTY WHATSOEVER.

```
? znprimroot(9048610007)
%1 = Mod(5, 9048610007)
? znlog(15625,%1)
%2 = 6
? znlog(3757843958,%1)
%3 = 678
```

8.2 Symbole de Legendre.

Soit p, q des nombres premiers impairs distincts. La partie principale de la *loi de réciprocité quadratique* démontrée par Gauss dit que pour $p \equiv q \equiv 3 \pmod{4}$ la résolubilité d'une des congruences $x^2 \equiv p \pmod{q}$ et $x^2 \equiv q \pmod{p}$ implique la non-résolubilité de l'autre; sinon elles sont simultanément résolubles ou non-résolubles. Gauss a utilisé ce fait pour des calculs des grandes tables de nombres premiers.

Pour cela il a suggéré une modification plus fine de la condition nécessaire de primalité basée sur la congruence de Fermat (6.2). Notamment on définit le symbole de Legendre $\left(\frac{a}{n}\right)$ pour un nombre premier $n = p$ par

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{n}, \\ 1 & \text{si } a \equiv b^2 \pmod{n}, \text{ pour un certain } b, n \nmid b, \\ -1 & \text{sinon.} \end{cases} \quad (8.1)$$

PROPOSITION 8.2.1 *Soit $n = p$ un nombre premier impair. L'application*

$$\phi : a \mapsto \left(\frac{a}{n}\right), \quad (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \{\pm 1\}$$

définie un morphisme $\phi : (\mathbb{Z}/n\mathbb{Z})^ \rightarrow \{\pm 1\}$ de groupes cycliques. Son noyau $\text{Ker}(\phi)$ coïncide avec le sousgroupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^{*2}$ des carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$, avec $\text{Card}((\mathbb{Z}/n\mathbb{Z})^{*2}) = (n-1)/2$.*

Exemples de calcul du symbole de Legendre (disponible à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-12legen.mws)

```
> with(numtheory):
```

```
Warning, the protected name order has been redefined and
unprotected
```

```
> legendre(74,101);
```

```
-1
```

```
> legendre(3,73);
```

```
1
```

```
> legendre(22,11);
```

```
0
```

- > legendre(5,2); -1
- > legendre(-2342, 1901); 1

8.3 Congruence d'Euler

PROPOSITION 8.3.1 *Soit n un nombre premier impair. Alors*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{8.2}$$

PREUVE est impliqué par la cyclicité du groupe $(\mathbb{Z}/n\mathbb{Z})^*$. En effet, les deux parties de l'égalité (8.2) sont les morphismes non-triviales du groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$ dans le groupe $\{\pm 1\}$. Si n n'est pas nécessairement premier, la congruence (8.2) peut être utilisée comme un test de primalité (une condition nécessaire et suffisante) si l'on définit le symbole de Jacobi à droite par multiplicativité : pour un nombre impair positif $n = p_1 p_2 \dots p_k$, où p_i sont premiers (non nécessairement différents) posons

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \tag{8.3}$$

Cependant, on montrera que le symbole de Jacobi peut être calculé sans connaissance de la factorisation de n en produit des nombres premiers.

REMARQUE. Si n est composé, il se peut que $\left(\frac{a}{n}\right) = 1$ mais a n'est pas un carré mod n . Par exemple, si $n = pq$, il suffit d'utiliser le théorème chinois des restes pour construire un $a \pmod{pq}$ tel que $\left(\frac{a}{p}\right) = -1$ et $\left(\frac{a}{q}\right) = -1$. Alors $\left(\frac{a}{n}\right) = 1$ mais a n'est pas un carré mod n . Au contraire, si a est pas un carré mod n , alors $\left(\frac{a}{n}\right) = -1$ par multiplicativité.

En effet, le symbole de Jacobi peut être étendu sur toutes les valeurs du "numérateur" et du "dénominateur" et il peut être calculé sans connaissance de la factorisation de n en produit de nombres premiers.

Pour cela on utilise la loi de réciprocité quadratique étendue

$$\left(\frac{Q}{P}\right) \left(\frac{P}{Q}\right) = (-1)^{\frac{(P-1)}{2} \frac{(Q-1)}{2}} \tag{8.4}$$

pour P, Q positifs impairs, et on a les deux compléments suivants de cette loi

$$\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}, \quad \left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}, \tag{8.5}$$

aussi bien que la multiplicativité du symbole par rapport au "numérateur" et au "dénominateur". Le calcul suit la même procédure que celle suivie pour l'algorithme d'Euclide et il utilise moins de $5 \log \max(P, Q)$ divisions avec reste.



8.4 Lois de réciprocité de Gauss

(voir [Stein]). Le symbol $\left(\frac{a}{p}\right)$ ne dépends que de la classe résiduelle de a modulo p . Ensuite, on fixe a et on commence par faire une tableau suivante :

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2
11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3

Cette table fait deviner que $\left(\frac{5}{p}\right)$ ne dépends que de la classe de p modulo 5 ; plus précisément, $\left(\frac{5}{p}\right) = 1$ si et seulement si $p \equiv 1, 4 \pmod{5}$, i.e., p est un carré modulo 5. Cependant, on ne peut pas voir directement de la valeur

$$5^{(p-1)/2} \pmod{p},$$

que $p \equiv 1, 4 \pmod{5}$ permet d'évaluer cette expression.

A la base de tels calculs, plusieurs mathématiciens ont trouvé une explication conjecturale de ce mystère de 18 siècle. Finalement, Gauss a prouvé cette conjecture en 1801.

THÉORÈME 8.4.1 (LA LOI DE RÉCIPROCITÉ QUADRATIQUE) *Soit p, q des nombres premiers impairs distincts. Alors*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right), \quad (8.6)$$

c'est à dire que pour $p \equiv q \equiv 3 \pmod{4}$ la résolubilité d'une des congruences $x^2 \equiv p \pmod{q}$ et $x^2 \equiv q \pmod{p}$ implique la non-résolubilité de l'autre ; sinon elles sont simultanément résolubles ou non-résolubles.

On donnera une démonstration très élémentaire de ce résultat, basé sur le critère de Euler (8.2).

REMARQUE 8.4.2 *Dans l'exemple considéré plus haut, on obtient*

$$\left(\frac{5}{p}\right) = (-1)^{2 \cdot \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 4 \pmod{5} \\ -1 & \text{if } p \equiv 2, 3 \pmod{5}. \end{cases}$$

Ceci dit, la loi de réciprocité quadratique "explique" pourquoi la connaissance de p modulo 5 permet de calculer $5^{\frac{p-1}{2}} \pmod{p}$.

Il existe environ 200 démonstration du théorème 8.4.1, voir

<http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html>

THÉORÈME 8.4.3 (LA LOI DE RÉCIPROCITÉ QUADRATIQUE ÉTENDUE)

$$\left(\frac{Q}{P}\right) \left(\frac{P}{Q}\right) = (-1)^{\frac{(P-1)(Q-1)}{2}} \quad (8.7)$$

pour P, Q positifs impairs, et on a les deux compléments suivants de cette loi

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2} = \varepsilon(P), \quad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8} = \omega(P), \quad (8.8)$$

où on utilise les fonctions multiplicatives $\varepsilon : (\mathbb{Z}/4\mathbb{Z})^* \rightarrow \{\pm 1\}$ et $\omega : (\mathbb{Z}/8\mathbb{Z})^* \rightarrow \{\pm 1\}$, données par :

$$\varepsilon(a) = (-1)^{\frac{a-1}{2}}, = \begin{cases} 1, & \text{si } a \equiv 1 \pmod{4} \\ -1, & \text{si } a \equiv 3 \pmod{4} \end{cases}, \quad \text{et } \omega(a) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1, & \text{si } a \equiv \pm 1 \pmod{8} \\ -1, & \text{si } a \equiv \pm 3 \pmod{8} \end{cases}.$$

PREUVE découle du théorème 8.4.1 et des définitions (8.20) : si, par exemple, $P = p_1 \dots p_k$, $Q = q_1 \dots q_l$, alors

$$\left(\frac{Q}{P}\right) = \left(\frac{q_1 \dots q_l}{p_1 \dots p_k}\right) = \left(\frac{Q}{p_1}\right) \dots \left(\frac{Q}{p_k}\right) = \prod_{i=1}^k \prod_{j=1}^l \left(\frac{q_j}{p_i}\right),$$

$$\left(\frac{P}{Q}\right) = \left(\frac{p_1 \dots p_k}{q_1 \dots q_l}\right) = \prod_{i=1}^k \prod_{j=1}^l \left(\frac{p_i}{q_j}\right),$$

donc on obtient par multiplicativité :

$$\left(\frac{Q}{P}\right) \left(\frac{P}{Q}\right) = \prod_{i=1}^k \prod_{j=1}^l \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) = \prod_{i=1}^k \prod_{j=1}^l (-1)^{\frac{p_i-1}{2} \cdot \frac{q_j-1}{2}} = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}},$$

puisque la fonction

$$a \mapsto \varepsilon(a) = (-1)^{\frac{a-1}{2}}, \quad (\mathbb{Z}/4\mathbb{Z})^* \rightarrow \{\pm 1\}$$

est multiplicative $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$. Ensuite, le calcul du symbole de Jacobi suit alors la même procédure que celle suivie pour l'algorithme d'Euclide puisque $\left(\frac{P}{Q}\right)$ ne dépend que de P modulo Q , et il utilise moins de $5 \log \max(P, Q)$ divisions avec reste.

8.5 Une démonstration élémentaire de la loi de réciprocité

Un lemme de Gauss

La preuve donnée dans cette section est basée sur le lemme de Gauss suivant :

LEMME 8.5.1 Soit p un nombre premier impair, et soit a un entier $\not\equiv 0 \pmod{p}$. On considère les nombres,

$$a, 2a, 3a, \dots, \frac{p-1}{2}a$$

et on les réduit modulo p de telle façon que le résultat se trouve dans le segment $(-\frac{p}{2}, \frac{p}{2})$. Soit ν le nombre total de nombres négatifs obtenus de cette manière. Alors

$$\left(\frac{a}{p}\right) = (-1)^\nu.$$

PREUVE. Pour définir ν , on exprime tout nombre

$$S = \left\{ a, 2a, \dots, \frac{p-1}{2}a \right\}$$

comme un nombre congru au nombre de l'ensemble

$$\left\{ 1, -1, 2, -2, \dots, \frac{p-1}{2}, -\frac{p-1}{2} \right\}.$$

Chaque nombre $1, 2, \dots, \frac{p-1}{2}$ apparaît une seule fois, avec un des deux choix de signe, sinon on obtiendrait deux éléments de S qui sont congrus modulo p , ou deux éléments de S dont la somme soit congrue à 0 modulo p , ce que est impossible. Alors l'ensemble obtenu doit être de la forme

$$T = \left\{ \varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \dots, \varepsilon_{(p-1)/2} \cdot \frac{p-1}{2} \right\},$$

ou tout ε_i est $+1$ ou -1 . En multipliant les éléments de S et de T , on voit que

$$(1a) \cdot (2a) \cdot (3a) \cdots \left(\frac{p-1}{2}a\right) \equiv (\varepsilon_1 \cdot 1) \cdot (\varepsilon_2 \cdot 2) \cdots \left(\varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right) \pmod{p},$$

donc

$$a^{(p-1)/2} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_{(p-1)/2} \pmod{p}.$$

Le lemme donc découle de proposition 8.3.1.

Conjecture d'Euler

Tout d'abord, on fait une observation élémentaire :

LEMME 8.5.2 Soit $a, b \in \mathbb{Q}$. Alors pour tout $n \in \mathbb{Z}$,

$$\#((a, b) \cap \mathbb{Z}) \equiv \#((a, b + 2n) \cap \mathbb{Z}) \equiv \#((a + 2n, b) \cap \mathbb{Z}) \pmod{2}.$$

PREUVE. Si $n > 0$, alors

$$(a, b + 2n) = (a, b) \cup [b, b + 2n),$$

où l'union est disjointe. Soit $[x]$ note la partie entière de x , $[x] \leq x$. Il y a exactement $2n$ entiers dans l'intervalle $[b, b + 2n)$:

$$\begin{cases} b, b + 1, \dots, b + 2n - 1, & \text{si } b \in \mathbb{Z} \\ [b] + 1, [b] + 2, \dots, [b] + 2n, & \text{si } b \notin \mathbb{Z} \end{cases}$$

donc l'assertion du lemme est vraie dans ce cas. On a aussi

$$(a, b - 2n) = (a, b) \setminus [b - 2n, b)$$

et $[b - 2n, b)$ aussi contient exactement $2n$ entiers, donc le lemme est vrai aussi pour n négatif. L'affirmation sur $\#((a + 2n, b) \cap \mathbb{Z})$ est déduit de manière similaire.

La proposition suivante a été conjecturé par Euler, à la base des nombreux calculs. La loi de réciprocité quadratique sera facilement déduit de cette proposition.

PROPOSITION 8.5.3 (CONJECTURE D'EULER) *Soit p un nombre premier impair et $a \in \mathbb{N}$ un nombre entier positif tel que $p \nmid a$.*

1. *Le symbol $\left(\frac{a}{p}\right)$ ne dépend que de p modulo $4a$.*
2. *Si q est un nombre premier tel que $q \equiv -p \pmod{4a}$, alors $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

PREUVE. Pour pouvoir appliquer le lemme de Gauss ci-dessus, on a besoin de calculer la parité du cardinal $\#(S \cap I)$ de l'intersection des ensembles

$$S = \left\{ a, 2a, 3a, \dots, \frac{p-1}{2}a \right\}$$

et

$$I = \left(\frac{1}{2}p, p\right) \cup \left(\frac{3}{2}p, 2p\right) \cup \dots \cup \left(\left(b - \frac{1}{2}\right)p, bp\right),$$

où soit $b = \frac{1}{2}a$ soit $\frac{1}{2}(a - 1)$, on choisit un entier parmi les deux nombres rationnels. En effet, on vérifie que tout élément de S qui se réduit à un nombre dans l'intervalle $(-\frac{p}{2}, 0)$, appartient à I :

$$\begin{aligned} ka = pl + r, \text{ avec } k = 1, 2, \dots, \frac{p-1}{2}, r \in \left(-\frac{p}{2}, 0\right) \cap \mathbb{Z} \\ \iff ka \in \left(\frac{1}{2}p, p\right) \cup \left(\frac{3}{2}p, 2p\right) \cup \dots \cup \left(\left(b - \frac{1}{2}\right)p, bp\right). \end{aligned}$$

Ceci est clair si $b = \frac{1}{2}a < \frac{p-1}{2}a$ (l'extrémité droite bp de I se trouve à gauche de l'extrémité droite de S). Si $b = \frac{1}{2}(a - 1)$, alors l'extrémité suivant (à droite de I) $bp + \frac{p}{2} = \frac{1}{2}(a - 1)p + \frac{p}{2} > \frac{p-1}{2}a$, donc $\left(\left(b - \frac{1}{2}\right)p, bp\right)$ est le dernier intervalle qui peut contenir un tel élément de S qui se réduit à $(-\frac{p}{2}, 0)$.) Remarquer aussi que les extrémités entières de I n'appartiennent pas à S , puisque ces extrémités entières sont divisibles par p , mais aucun élément de S est divisible par p .

En divisant I par a , on voit que

$$\#(S \cap I) = \# \left(\mathbb{Z} \cap \frac{1}{a}I \right), \text{ où } \frac{1}{a}I = \left(\left(\frac{p}{2a}, \frac{p}{a}\right) \cup \left(\frac{3p}{2a}, \frac{2p}{a}\right) \cup \dots \cup \left(\frac{(2b-1)p}{2a}, \frac{bp}{a}\right) \right).$$

On pose $p = 4ac + r$, et soit

$$J = \left(\left(\frac{r}{2a}, \frac{r}{a}\right) \cup \left(\frac{3r}{2a}, \frac{2r}{a}\right) \cup \dots \cup \left(\frac{(2b-1)r}{2a}, \frac{br}{a}\right) \right).$$

On observe que la seule différence entre I et J est que les extrémités des intervalles sont changés par l'addition d'un entier pair. En appliquant le lemme 8.5.2, on a

$$\nu = \# \left(\mathbb{Z} \cap \frac{1}{a}I \right) \equiv \#(\mathbb{Z} \cap J) \pmod{2}.$$

Alors $\left(\frac{a}{p}\right) = (-1)^\nu$ ne dépend que de r , i.e., ne dépend que de p modulo $4a$.

Si $q \equiv -p \pmod{4a}$, alors le seul changement dans le calcul ci-dessus est que r est remplacé par $4a - r$. Ceci remplace l'ensemble $\frac{1}{a}I$ pour l'ensemble

$$K = \left(\left(2 - \frac{r}{2a}, 4 - \frac{r}{a} \right) \cup \left(6 - \frac{3r}{2a}, 8 - \frac{2r}{a} \right) \cup \dots \cup \left(4b - 2 - \frac{(2b-1)r}{2a}, 4b - \frac{br}{a} \right) \right).$$

Alors K est le même que $-\frac{1}{a}I$, à l'exception de l'addition des entiers pairs aux extrémités. De nouveau, le lemma 8.5.2 implique

$$\#(K \cap \mathbb{Z}) \equiv \# \left(\left(\frac{1}{a}I \right) \cap \mathbb{Z} \right) \pmod{2},$$

donc $\left(\frac{a}{p} \right) = \left(\frac{a}{q} \right)$, CQFD.

L'analyse suivante plus fine dans le cas spécial où $a = 2$ donne aussi une illustration de la démonstration précédente du lemme, et ce résultat est souvent utilisé dans les calculs.

PROPOSITION 8.5.4 *Soit p un nombre premier impair. Alors*

$$\left(\frac{2}{p} \right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8} \\ -1 & \text{si } p \equiv \pm 3 \pmod{8} \end{cases}. \quad (8.9)$$

REMARQUE. La fonction

$$a \mapsto \omega(a) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1 & \text{si } a \equiv \pm 1 \pmod{8} \\ -1 & \text{si } a \equiv \pm 3 \pmod{8} \end{cases}, \quad \omega : (\mathbb{Z}/8\mathbb{Z})^* \rightarrow \{\pm 1\} \quad (8.10)$$

est multiplicative $\omega(ab) = \omega(a)\omega(b)$.

PREUVE. Si $a = 2$, l'ensemble $S = \{a, 2a, \dots, 2 \cdot \frac{p-1}{2}\}$ est

$$\{2, 4, 6, \dots, p-1\}.$$

Nous pouvons compter la parité des nombres d'éléments de S qui appartiennent à l'intervalle $I = (\frac{p}{2}, p)$. On pose $p = 8c + r$, alors

$$\begin{aligned} \#(I \cap S) &= \# \left(\frac{1}{2}I \cap \mathbb{Z} \right) = \# \left(\left(\frac{p}{4}, \frac{p}{2} \right) \cap \mathbb{Z} \right) \\ &= \# \left(\left(2c + \frac{r}{4}, 4c + \frac{r}{2} \right) \cap \mathbb{Z} \right) \equiv \# \left(\left(\frac{r}{4}, \frac{r}{2} \right) \cap \mathbb{Z} \right) \pmod{2}, \end{aligned}$$

où l'égalité dernière vient du Lemme 8.5.2. Les possibilités pour r sont 1, 3, 5, 7. Si $r = 1$, le cardinal est 0, si $r = 3, 5$ il est 1, et si $r = 7$ il est 2 : $\mathbb{Z} \cap \left(\frac{7}{4}, \frac{7}{2} \right) = \{2, 3\}$.

Cours N°8, Mardi le 23 novembre 2004
(Salle 017, 10h15-12h15 (exceptionnellement))

Rappel de la loi de réciprocité quadratique de Gauss, Théorème 8.4.3 :

Pour les nombres premiers positifs impairs p, q on a

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

et on a les deux compléments suivants de cette loi :

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

Rappel de la Conjecture d'Euler, Proposition 8.5.3 :

Soit p un nombre premier impair et $a \in \mathbb{N}$ un nombre entier positif tel que $p \nmid a$.

1. Le symbol $\left(\frac{a}{p}\right)$ ne dépend que de p modulo $4a$.
2. Si q est un nombre premier tel que $q \equiv -p \pmod{4a}$, alors $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Fin de la démonstration de la loi de réciprocité quadratique

Avec le lemme on déduit directement la loi de réciprocité quadratique (théorème 8.4.1 de Gauss) :
Soit p, q des nombres premiers impairs distincts. Alors

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

PREUVE. On suppose d'abord que $p \equiv q \pmod{4}$. Quite à échanger p et q on peut supposer $p > q$, et on pose $p - q = 4a$. Puisque $p = 4a + q$,

$$\left(\frac{p}{q}\right) = \left(\frac{4a + q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right),$$

on a

$$\left(\frac{q}{p}\right) = \left(\frac{p - 4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right).$$

Proposition 8.5.3 (Conjecture d'Euler) implique que $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, puisque $p \equiv q \pmod{4a}$. Alors

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

où la dernière égalité vient du fait que dans ce cas $\frac{p-1}{2}$ est pair si et seulement si $\frac{q-1}{2}$ est pair.

Ensuite, on suppose que $p \not\equiv q \pmod{4}$, alors $p \equiv -q \pmod{4}$. On écrit $p + q = 4a$. On a

$$\left(\frac{p}{q}\right) = \left(\frac{4a - q}{q}\right) = \left(\frac{a}{q}\right), \quad \text{and} \quad \left(\frac{q}{p}\right) = \left(\frac{4a - p}{p}\right) = \left(\frac{a}{p}\right).$$

Puisque $p \equiv -q \pmod{4a}$, Proposition 8.5.3 implique que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Mais dans ce cas $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1$, d'où la preuve.



Exemples de racines carrées (disponible à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-11sq.mws)

EXEMPLE 8.5.5 *Est-ce que 6 est un carré modulo 389 ? On a*

$$\left(\frac{6}{389}\right) = \left(\frac{2 \cdot 3}{389}\right) = \left(\frac{2}{389}\right) \cdot \left(\frac{3}{389}\right) = (-1) \cdot (-1) = 1.$$

Ici on a trouvé que $\left(\frac{2}{389}\right) = -1$ en utilisant Proposition 8.5.4 et le fait que $389 \equiv 5 \pmod{8}$. On a trouvé $\left(\frac{3}{389}\right)$ de manière suivante :

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Alors 6 est un carré modulo 389.

Cependant, on connaît pas de x tel que $x^2 \equiv 6 \pmod{389}$, mais on peut le trouver

```
> restart;for a from 1 to 388 do
> if a^2 mod 389 = 6 then
> print(a); fi; od;
```

28

361

8.6 Une démonstration de la loi de réciprocité utilisant sommes de Gauss

On utilise le morphisme de groupes multiplicatifs $\chi : (\mathbb{Z}/q\mathbb{Z})^* \rightarrow \{\pm 1\}$, donné par le symbole de Legendre $a \mapsto \left(\frac{a}{q}\right) = \chi(a)$, où q est un nombre premier, et on utilise le morphisme $x \mapsto \zeta^x = \exp(2i\pi x/q)$ du groupe additif $\mathbb{Z}/q\mathbb{Z}$ dans \mathbb{C}^* , ($\zeta = \exp(2i\pi/q)$).

Nous allons considérer les sommes de Gauss comme un analogue discret de la fonction gamma $\Gamma(s)$ qui pour $\text{Re}(s) > 0$ est définie par l'intégrale

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}. \quad (8.11)$$

Ici la fonction intégrée est le produit d'un caractère additif de \mathbb{R} (l'homomorphisme $y \mapsto e^{-y}$, c'est à dire, un morphisme de groupes $\mathbb{R} \rightarrow \mathbb{C}$), et d'un caractère multiplicatif $y \mapsto y^s$ de \mathbb{R}_+^\times , c'est à dire, un morphisme $\mathbb{R}_+^\times \rightarrow \mathbb{C}$). L'intégration est effectuée par rapport à la mesure invariante multiplicative $\frac{dy}{y}$.

Pour définir la somme de Gauss, on remplace ici \mathbb{R} par $\mathbb{Z}/N\mathbb{Z}$ avec un $N > 1$, e^{-y} par un caractère additif

$$\mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}^\times : y \mapsto \zeta_N^y, \quad \zeta_N = \exp\left(\frac{2\pi i}{N}\right),$$

(c'est à dire, un morphisme de groupes $\mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$), et on remplace y^s par un caractère multiplicatif $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ (c'est à dire, un morphisme de groupes $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}$). Le caractère de Dirichlet $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ correspondant à χ (désigné aussi par χ) est défini par $\chi(a) = \chi(a \bmod N)$ pour $(a, N) = 1$ et par $\chi(a) = 0$ pour $(a, N) > 1$. La somme de Gauss $G(\chi)$ est définie par

$$G(\chi) = \sum_{x=1}^{N-1} \chi(x) \zeta_N^x. \quad (8.12)$$

Pour $a \in \mathbb{Z}$, on utilise souvent la notation suivante :

$$G_a(\chi) = \sum_{x=1}^{N-1} \chi(x) \zeta_N^{ax}.$$

Remarquons aussi que la fonction $a \mapsto G_a(\chi)$ coïncide avec la "transformation de Fourier discrète" du caractère χ .

La similitude entre (8.11) et (8.12) implique que leurs propriétés sont similaires. Pour les décrire on introduit tout d'abord la notion importante de caractère de Dirichlet primitif. Un caractère χ est dit primitif modulo N s'il ne s'est pas réduit à un autre caractère $\chi' : \mathbb{Z}/M\mathbb{Z} \rightarrow \mathbb{C}^*$ définie modulo un nombre M plus petit qui est un diviseur propre de N (par la composée avec la projection $\mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/M\mathbb{Z}$). De même, la restriction de χ sur un tout sous-groupe $H_M = ((1 + M\mathbb{Z})/(1 + N\mathbb{Z}))^\times$ ne soit pas triviale. Par exemple, tout caractère non-triviale modulo un nombre premier q , est primitif, y compris le symbole de Legendre $a \mapsto \left(\frac{a}{q}\right)$.

PROPOSITION 8.6.1 *Si χ est primitif, on a*

$$G_a(\chi) = \overline{\chi}(a)G(\chi) \quad (a \in \mathbb{Z}), \quad (8.13)$$

$$\overline{G(\chi)} = \chi(-1)G(\overline{\chi}), \quad (8.14)$$

$$|G(\chi)|^2 = N. \quad (8.15)$$

REMARQUE 8.6.2 *La propriété (8.13) correspond à la formule*

$$\int_0^\infty e^{-ay} y^s \frac{dy}{y} = a^{-s} \Gamma(s) \quad (\operatorname{Re}(s) > 0),$$

et (8.15), réécrite sous la forme $G(\chi)G(\chi^{-1}) = \chi(-1)N$, correspond à l'équation fonctionnelle de la fonction gamma

$$\Gamma(s)\Gamma(-s) = -\frac{\pi}{s \sin \pi s} \quad \left(\text{ou } \Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s} \right)$$

PREUVE des égalités (8.13)–(8.15) (en exercice) est impliquée par des changement d'indice de sommation.

Par exemple, si $(a, N) = 1$, $G_a(\chi) = \sum_{x=1}^{N-1} \chi(x) \zeta_N^{ax} = \sum_{x=1}^{N-1} \overline{\chi}(a) \chi(ax) \zeta_N^{ax} = \overline{\chi}(a) \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(ay) \zeta_N^{ay}$. Si $(a, N) = t > 1$, on utilise le fait que ζ_N^{ax} ne dépend que de $x \bmod N/t$, et que la somme $\sum_{\substack{b \bmod N \\ b \equiv c \bmod M}} \chi(b)$

s'annule pour tout caractère primitif χ , et pour tout propre diviseur M de N , donc $G_a(\chi) = 0 = \overline{\chi}(a)G(\chi)$ dans ce cas, d'où (8.13). En particulier, pour $a = -1$ on a (8.14), car

$$\overline{G_{-1}(\chi)} = \sum_{x=1}^{N-1} \overline{\chi(x) \zeta_N^{-x}} = \chi(-1)G(\overline{\chi}), \text{ et}$$

$$\begin{aligned} |G(\chi)|^2 &= G(\chi)\overline{G(\chi)} = \chi(-1)G(\chi)G(\overline{\chi}) = \sum_{x \bmod N} \overline{\chi(x)}G(\chi)\zeta_N^{-x} = \\ &= \sum_{x \bmod N} G_x(\overline{\chi})\zeta_N^{-x} = \sum_{x, z \bmod N} \overline{\chi}(z)\zeta_N^{-x+zx} = \sum_{z \bmod N} \overline{\chi}(z) \sum_{x \bmod N} \zeta_N^{x(-1+z)} = N \end{aligned}$$

puisque la seule somme non-nulle sur x correspond à $z = 1$, et $\chi(1) = 1$, d'où (8.15).

Les propriétés (8.13)–(8.15) impliquent la loi de réciprocité quadratique.

Démontrons la formule principale (8.6) :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \quad (8.16)$$

où p, q sont des nombres premiers distincts. Remarquons premièrement que le symbole quadratique $\chi(a) = \left(\frac{a}{q}\right)$ est un caractère de Dirichlet primitif modulo q . La somme de Gauss correspondante $G(\chi)$ est un élément de l'anneau $R = \mathbb{Z}[\zeta_q]$. Dans un anneau commutatif on a toujours la congruence $(a+b)^p \equiv a^p + b^p \pmod{pR}$ grâce à la divisibilité des coefficients binomiaux C_p^i par p pour $1 \leq i \leq p-1$. Comme $\chi^p(a) = \chi(a) = \pm 1$, on a

$$G(\chi)^p \equiv G_p(\chi^p) \pmod{pR}, \quad G_p(\chi^p) = \overline{\chi(p)}G(\chi), \text{ donc}$$

$$G(\chi)^{p-1} \equiv \left(\frac{p}{q}\right) \pmod{pR}. \quad (8.17)$$

De l'autre côté, $\chi = \overline{\chi}$, et l'égalité (8.15) implique

$$G(\chi)^2 = \chi(-1)q = (-1)^{\frac{q-1}{2}}q. \quad (8.18)$$

Si l'on représente la partie gauche de (8.17) comme $G(\chi)^{2\frac{p-1}{2}}$ on obtient

$$(-1)^{\frac{q-1}{2} \cdot \frac{p-1}{2}} q^{\frac{p-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{pR}. \quad (8.19)$$

Finalement, (8.19) et la congruence d'Euler assurent

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$$

d'où (8.6).

De façon plus facile on montre l'égalité (8.9) à l'aide de l'anneau $S = \mathbb{Z}[\varepsilon]$, où $\varepsilon = \exp(2\pi i/8)$. On pose $b = \varepsilon + \varepsilon^{-1}$, et on observe que $b^2 = (\varepsilon + \varepsilon^{-1})^2 = 2$. Ensuite $(\varepsilon + \varepsilon^{-1})^p \equiv \varepsilon + \varepsilon^{-1} \pmod{pS}$ si $p \equiv \pm 1 \pmod{8}$, et $(\varepsilon + \varepsilon^{-1})^p \equiv -(\varepsilon + \varepsilon^{-1}) \pmod{pS}$ si $p \equiv \pm 3 \pmod{8}$. De plus, $b^2 \equiv 2 \pmod{pS}$ implique que b est inversible dans l'anneau quotient S/pS (car $p \neq 2$), et $\varepsilon^4 = -1, \varepsilon^5 = -\varepsilon, \varepsilon^6 = -\varepsilon^2, \varepsilon^7 = -\varepsilon^3$. Donc $(\varepsilon + \varepsilon^{-1})^p \equiv \varepsilon + \varepsilon^{-1} \pmod{pS}$ implique $b^p \equiv b \pmod{pS}$, d'où $b^{p-1} \equiv 1 \pmod{pS}$, et

$$b^2 \equiv 2 \pmod{p} \Rightarrow 2^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{pS} \Rightarrow 2^{(p-1)/2} \equiv 1 \pmod{p}.$$

Si $b^p \equiv -b \pmod{pS}$, alors $b^{p-1} \equiv -1 \pmod{pS}$, et

$$b^2 \equiv 2 \pmod{p} \Rightarrow 2^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv -1 \pmod{pS} \Rightarrow 2^{(p-1)/2} \equiv -1 \pmod{p}.$$

8.7 Nombres pseudopremiers d'Euler

Rappels : Congruence d'Euler

PROPOSITION 8.3.1 *Soit n un nombre premier impair. Alors on a la congruence (8.2) :*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \quad (8.2)$$

DÉFINITION 8.7.1 Un nombre naturel n est appelé un nombre pseudopremier de Euler par rapport à a si $\text{pgcd}(a, n) = 1$ et (8.2) soit satisfaite.

Si n n'est pas nécessairement premier, la congruence (8.2) peut être utilisée comme une condition de primalité si l'on définit le symbole de Jacobi à droite par la multiplicativité : pour un nombre impair positif $n = p_1 p_2 \dots p_k$, où p_i sont premiers (non nécessairement différents) posons

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right) \quad (8.20)$$

En effet, le symbole de Jacobi peut être étendu sur toutes les valeurs du "numérateur" et du "dénominateur" et il peut être calculé sans connaissance de la factorisation en produit des nombres premières de n .

Maintenant on va démontrer, en utilisant le théorème chinois (voir théorème 8.7.2), que si n est un nombre pseudopremier d'Euler par rapport à tout $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ alors n est premier. C'est à dire, il n'y a pas d'analogues eulériens des nombres de Carmichael.

THÉORÈME 8.7.2 (SOLOWAY-STRASSEN) Un nombre impair n est premier si et seulement si pour tout a avec $\text{pgcd}(a, n) = 1$,

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \quad (8.21)$$

PREUVE (voir [Dem], p. 125).

CAS I) On suppose qu'il existe un nombre premier p impair tel que $p^2 | n$, et on utilise le morphisme **surjectif** de groupes multiplicatifs

$$(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^\times, \quad (8.22)$$

où le groupe $(\mathbb{Z}/p^2\mathbb{Z})^\times$ est cyclique d'ordre $p(p-1)$. Ceci implique (par la surjectivité) qu'il existe $\bar{a} \pmod{n}$ tel que

$$\begin{aligned} p(p-1) \text{ divise } \text{ord}(\bar{a}) &\Rightarrow p \text{ divise } \text{ord}(\bar{a})^{(n-1)/2} = \frac{\text{ord}(\bar{a})}{\text{pgcd}((n-1)/2, \text{ord}(\bar{a}))} \\ &\Rightarrow (\bar{a})^{(n-1)/2} \not\equiv \pm 1 \pmod{n}. \end{aligned}$$

(ou bien : $n = p^2 m$; $a = 1 + mp \Rightarrow \bar{a}^{n-1} \neq 1$, car $\bar{a}^p = 1$. En effet, $(1 + mp)^p = 1 + p \cdot mp + \dots \equiv 1 \pmod{n}$ implique $\bar{a}^{n-1} = \bar{a}^n \bar{a}^{-1} = \bar{a}^{-1} \neq 1$).

CAS II) Soit $n = p_1 \dots p_r$ distincts, et $r \geq 2$,

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/(p_i))^\times.$$

Supposons qu'il existe un a tel que

$$a^{(n-1)/2} \equiv -1 \pmod{n}.$$

L'existence d'un tel a est nécessaire pour la congruence (8.21) puisque le théorème chinois permet de trouver, pour un choix arbitraire de $\eta_i = \pm 1$, un a avec

$$\left(\frac{a}{p_i}\right) = \eta_i, \quad (8.23)$$

donc on choisit $\prod_{i=1}^r \eta_i = -1$, puisque

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$$

Notons a_i la classe de a modulo p_i . On a d'une part,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right) = \left(\frac{a_1}{p_1}\right) \cdots \left(\frac{a_r}{p_r}\right)$$

D'autre part, réduisant modulo p_1 l'égalité initiale, on obtient

$$\left(\frac{a_1}{p_1}\right) \cdots \left(\frac{a_r}{p_r}\right) \equiv a_1^{(n-1)/2} \pmod{p_1}.$$

D'après le théorème chinois, on peut choisir les différentes a_i indépendamment. Mais le second membre ne dépend que de a_1 , tandis qu'on peut changer le signe du premier sans modifier a_1 , par exemple en modifiant a_r . Cela est absurde et contredit l'hypothèse $r \geq 2$.

8.8 Loi de réciprocité quadratique et tests de primalité.

Dans des tests modernes de primalité (Soloway-Strassen, Miller-Rabin...) on utilise la congruence (8.2) et le théorème 8.7.2. Ces tests de primalité, marchent beaucoup plus rapidement que toutes les méthodes connues de factorisation des grands nombres premiers "aléatoires".

Test de primalité de Soloway-Strassen

C'est un test probabiliste. Selon Emile Borel, "Un phénomène dont la probabilité est 10^{-50} , ne se produira donc jamais ou du moins ne sera jamais observé ("La probabilité et la vie").

Rappelons qu'un nombre naturel n est appelé un *nombre pseudopremier de Euler par rapport à a* si $\text{pgcd}(a, n) = 1$ et (8.2) soit satisfaite. Si (8.2) n'est pas satisfaite pour un a avec $\text{pgcd}(a, n) = 1$, alors n n'est pas premier, et on appelle a un *témoin d'Euler de non-primalité de n* . Selon le théorème 8.7.2, il existe toujours un témoin d'Euler de non-primalité d'un nombre composé impair n , mais la question qui reste est qu'il est le plus petit valeur de a , ou qui est la proportion de tels témoins.

Le test de primalité de Soloway-Strassen est basé sur l'observation suivante :

REMARQUE 8.8.1 *Soit n un nombre impair. Si (8.2) n'est pas satisfaite pour un a avec $\text{pgcd}(a, n) = 1$, alors elle n'est pas satisfaite pour au moins de 50 % de a .*

En effet, soit $H = \{a_1, a_2, \dots, a_j, \dots\}$ l'ensemble de tous les $a = a_j$ pour lesquels (8.2) est satisfaite :

$$a_j^{(n-1)/2} \equiv \left(\frac{a_j}{n}\right) \pmod{n}. \quad (8.2)$$

Alors H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ donc $a \notin H \Rightarrow aH \cap H = \emptyset$, ceci dit, la condition (8.2) n'est pas satisfaite pour au moins de 50 % de a .

Description d'algorithme. Soit n impair. On choisit **au hasard** k nombres b , $0 < b < n$. Pour tout b on calcul les deux parties de la congruence d'Euler (8.2), $b^{(n-1)/2} \pmod{n}$ et $\left(\frac{b}{n}\right)$.

Le calcul de $b^{(n-1)/2} \pmod n$ coûte $\mathcal{O}(\log^3 n)$ opération bouléennes par la méthode de carrés successifs.

Le calcul de $\left(\frac{b}{n}\right)$ coûte $\mathcal{O}(\log^3 n)$ opération bouléennes à l'aide de la loi de réciprocité quadratique en utilisant divisions euclidiennes.

Si (8.2) est valable pour k choix au hasard de b , alors la probabilité du fait que n est composé en dépit d'avoir passé k tests avec succès, est inférieure ou égale à $1/2^k$, donc pour $k \sim 167$ on obtient une probabilité suffisante (selon E.Borel) :

$$2^{167} \approx 10^{50} \cdot 1.870722095783555735300716588.$$

Test conditionnel de primalité de Miller

Ce test utilise le fait d'existence d'un témoin d'Euler relativement petit.

Cependant, pour le montrer, on a besoin de l'Hypothèse de Riemann généralisée.

Soit $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ un caractère de Dirichlet (c'est à dire, un morphisme de groupes $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathbb{C}$), et on pose pour $a \in \mathbb{Z}$, $\chi(a) = \chi(a \pmod N)$ pour $(a, N) = 1$ et $\chi(a) = 0$ pour $(a, N) > 1$. On considère la fonction L de Dirichlet

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$$

qui converge absolument et ne s'annule pas pour $\operatorname{Re}(s) > 1$. Elle admette un prolongement analytique sur tout le plan complexe.

HYPOTHÈSE DE RIEMANN GÉNÉRALISÉE. Pour toute fonction L de Dirichlet $L(s, \chi)$ on a

$$L(s, \chi) = 0, \operatorname{Re}(s) > 0 \Rightarrow \operatorname{Re}(s) = \frac{1}{2}.$$

THÉORÈME 8.8.2 (G.MILLER) *Supposons que pour tout $b < 2 \log^2 n$ la condition (8.2) soit satisfaite, et que l'Hypothèse de Riemann généralisée soit valable.*

Alors n est premier.

Description de l'algorithme de Miller

On vérifie la condition de la congruence d'Euler (8.2),

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n$$

pour tout $b < 2 \log^2 n$. Si n passe tous ces tests, il est premier (conditionnel). L'analyse simple de coût T de cet algorithme montre que $T = \mathcal{O}(\log^5 n)$.

REMARQUE. On a observé récemment des "preuves" numériques que pour n composé il existe un témoin $a \leq 2 \log n \log \log n$ tel que n pour que n soit un nombre pseudopremier d'Euler par rapport à a .

Pseudopremiers forts et le test de primalité de Miller-Rabin

On peut encore améliorer la condition de la congruence d'Euler (8.2),

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n$$

qui est valable pour un nombre premier n . On remarque que dans le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})^*$ les seules racines carrés de 1 sont ± 1 . Cette condition, qui n'est pas suffisante pour la primalité d'un nombre impair n , peut être utilisée comme une condition efficace probabiliste de primalité.

DÉFINITION 8.8.3 Un nombre naturel n est appelé un nombre pseudopremier fort par rapport à b si $\text{pgcd}(b, n) = 1$ et (8.2), et pour la présentation $n - 1 = 2^s t$ avec t impair, il existe un r , $0 \leq r < s$ tel que

$$b^{2^r t} \equiv -1 \pmod{n}.$$



THÉORÈME 8.8.4 (MILLER-RABIN)

(a) Soit n un nombre impair composé, alors n n'est pas un nombre pseudopremier fort par rapport à b au moins de 75 % de b .

(b) Tout pseudopremier fort par rapport à b est un pseudopremier d'Euler par rapport à b .

PREUVE (voir [Kob87], p.117, V.1.6, V.1.7).

Description de l'algorithme de Miller-Rabin On choisit au hasard k nombres b , $0 < b < n$. Pour tout b on vérifie les condition que n est un nombre pseudopremier fort par rapport à b : on calcule

$$b^{2^r t} \pmod{n}, \quad 0 \leq r < s$$

jusqu'on obtient $-1 \pmod{n}$.

Le calcul coûte $\mathcal{O}(\log^3 n)$ opération booléennes seulement par la méthode de carrés successifs.

Si n est passé ces k tests pour k choix au hasard de b , alors la probabilité du fait que n est composé en dépit d'avoir passé k tests avec succès, est inférieure ou égale à $1/4^k$.

REMARQUE. On peut vérifier que $n = 3215031751$ est le seul nombre composé $n \leq 2.5 \cdot 10^{10}$ qui est pseudopremier fort pour $b = 2, 3, 5, 7$

```
? factor(3215031751)
```

```
%1 =
```

```
[151 1]
```

```
[751 1]
```

```
[28351 1]
```



Test polynômial déterministe de primalité de Agrawal, Kayal et Saxena ("PRIMES is in P", 2002)

Ce test utilise une version polynômiale de la condition nécessaire du petit théorème de Fermat, et il arrive qu'une telle version et suffisante et qu'elle amène à un algorithme très efficace polynômial de primalité, voir une jolie exposition dans [Bor03], F.BORNEMANN, PRIMES is in P, une avancée accessible à "l'homme ordinaire" ", Gazette des mathématiciens, SMF, No 98, octobre 2003, pp. 14–30.



EXERCICES

8.1 Si p est un nombre premier, et $p \equiv 1 \pmod{4}$, montrer que

$$-1 \equiv \left[\left(\frac{p-1}{2} \right)! \right]^2 \pmod{p}.$$

[Indication : En considérant $X^{p-1} - 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ montrer d'abord que $(p-1)! + 1 \equiv 0 \pmod{p}$].

8.2 713 est-il un carré modulo $p = 1009$?

8.3 (a) Soit $p = 2^{2^n} + 1$ un nombre de Fermat premier, avec $n \geq 2$. Montrer que a est une racine primitive modulo p si et seulement si $\left(\frac{a}{p} \right) = -1$. Motrer que 3, 5 et 7 sont racines primitives modulo p .

(b) Montrer le critère de Pépin :

$$p = 2^{2^n} + 1 \text{ est un nombre premier} \iff 3^{(p-1)/2} \equiv -1 \pmod{p}.$$

8.4 Montrer que 2 est racine primitive modulo les premiers de la forme $4q + 1$ ou $2q + 1$ avec q premier, $q \equiv 1 \pmod{4}$. Et si $p = 2q + 1$ avec q premier, $q \equiv 3 \pmod{4}$?

8.5 Calculer de tête les symboles : $\left(\frac{3}{97} \right)$, $\left(\frac{5}{389} \right)$, $\left(\frac{2003}{11} \right)$, et $\left(\frac{5!}{7} \right)$.

8.6 Montrer que pour un nombre premier $p \geq 5$ on a $\left(\frac{3}{p} \right) = \begin{cases} 1 & \text{si } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{si } p \equiv 5, 7 \pmod{12}. \end{cases}$

8.7 Montrer qu'il n'y a pas de racines primitives modulo 2^n pour tout $n \geq 3$.

8.8 Montrer que si p est un nombre premier, alors il existe une racine primitive modulo p^2 . [Indication : Ecrire un élément de $(\mathbb{Z}/p^2\mathbb{Z})^*$ sous la forme du produit de deux éléments. Rappeler que si a, b sont d'ordres n, m , avec $\text{pgcd}(n, m) = 1$, alors ab est d'ordre nm .]

8.9 En utilisant le fait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique montrer directement que $\left(\frac{-3}{p} \right) = 1$ pour $p \equiv 1 \pmod{3}$. [Indication : Il existe un élément $c \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre 3. Montrer que $(2c + 1)^2 = -3$.]

8.10 Si $p \equiv 1 \pmod{5}$, montrer directement que $\left(\frac{5}{p} \right) = 1$ par la méthode d'exercice 9. [Indication : Soit $c \in (\mathbb{Z}/p\mathbb{Z})^*$ un élément d'ordre 5. Montrer que $(c + c^4)^2 + (c + c^4) - 1 = 0$, etc.]

8.11 Pour quels nombres premiers p on a $\sum_{a=1}^{p-1} \left(\frac{a}{p} \right) = 0$?

8.12 Combien de nombres naturels $x < 2^{13}$ satisfont l'équation

$$x^2 \equiv 5 \pmod{2^{13} - 1}?$$

(On peut utiliser le fait que $2^{13} - 1$ est premier.)

8.13 Trouver un nombre naturel $x < 97$ tel que $x \equiv 4^{48} \pmod{97}$.

8.14 Soit $n = p_1 \cdot \dots \cdot p_r$ distincts, et $r \geq 2$, et soit a tel que

$$a^{(n-1)/2} \equiv -1 \pmod{n}.$$

Posons $n - 1 = 2^s t$ avec t impaire, et soit $p|n$, $p - 1 = 2^{s'} t'$ avec t' impaire.

Montrer que

$$s' \geq s, \text{ et } \left(\frac{a}{p_i} \right) = \varepsilon_i = \begin{cases} -1, & \text{si } s = s' \\ 1, & \text{si } s < s' \end{cases}, \quad (8.24)$$

Solution : On suppose, par l'absurde, $s' < s$, alors

$$a^{(n-1)/2} = a^{2^{s-1} t} \equiv -1 \pmod{n} \Rightarrow$$

$$a^{2^{s-1}t} \equiv (a^{2^{s-1}t'})^{t'} \equiv a^{2^{s-1}t'} \equiv -1 \pmod{n} \Rightarrow a^{2^{s-1}t'} \equiv -1 \pmod{p},$$

puisque t et t' sont impaires. Ensuite, l'hypothèse $s' < s$ implique

$$a^{2^{s'}t'} \equiv 1 \pmod{p} \Rightarrow a^{2^{s-1}t'} \equiv 1 \pmod{p},$$

et on a une contradiction avec la congruence précédente $a^{2^{s-1}t'} \equiv -1 \pmod{p}$.

- CAS $s' = s$: $\left(\frac{a}{p}\right) = a^{(p-1)/2} = a^{2^{s'-1}t'} \equiv -1$
puisque $(a^{2^{s'-1}t'})^{t'} \equiv -1 \pmod{p}$.

- CAS $s' > s$:

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} = a^{2^{s'-1}t'} \equiv (a^{2^{s'-1}t'})^{2^{s'-1}} \equiv 1 \pmod{p}. \quad \square$$

8.15 Sur l'anneau $\mathbb{Z}/N\mathbb{Z}$, il existe aussi un analogue de la fonction bêta :

$$B(s, t) = \int_0^1 x^{s-1}(1-x)^{t-1} dx = \int_{\mathbb{R}_+^*} \frac{y^s}{(1+y)^{s+t}} \frac{dy}{y} \quad (\operatorname{Re}(s), \operatorname{Re}(t) > 0).$$

Il est appelé somme de Jacobi de deux caractères de Dirichlet $\chi, \psi \pmod{N}$. Par la définition

$$J(\chi, \psi) = \sum_{x \pmod{N}} \chi(x)\psi(1-x) = \sum_{y \pmod{N}} \chi(y)\overline{(\chi\psi)}(1+y). \quad (8.25)$$

En utilisant le changement de variables $y(1-x) \mapsto x$, $x(1+y) \mapsto y$, démontrer l'égalité entre les deux expressions

8.16 En supposant χ, ψ , et $\chi\psi$ tous primitifs modulo N , montrer que

$$J(\chi, \psi) = G(\chi)G(\psi)/G(\chi\psi) = J(\psi, \chi) \quad (8.26)$$

correspondant à l'identité classique $B(s, t) = \Gamma(s)\Gamma(t)/\Gamma(s+t)$.

Solution : si l'on calcule le produit

$$G(\chi)G(\psi) = \sum_{x \pmod{N}} \chi(x)\zeta_N^x G(\psi) = \sum_{x \pmod{N}} \chi\psi(x)\zeta_N^x \overline{\psi(x)} G(\psi). \quad (8.27)$$

En appliquant (8.13), on obtient

$$\overline{\psi(x)} G(\psi) = G_x(\psi) = \sum_{y \pmod{N}} \zeta_N^{xy} \psi(y)$$

et (8.27) se transforme en

$$\begin{aligned} \sum_{x, y \pmod{N}} (\chi\psi)(x)\psi(y)\zeta_N^{x(1+y)} &= \sum_{y \pmod{N}} \psi(y)G_{1+y}(\chi\psi) = \\ \sum_{y \pmod{N}} \psi(y)\overline{(\chi\psi)}(1+y)G(\chi\psi) &= J(\psi, \chi)G(\chi\psi). \end{aligned} \quad (8.28)$$

9 Notions de corps et d'espace vectoriel, rappels et exemples

Nous avons déjà vu dans la section 4, partie I, la définition suivante :

DÉFINITION 4.2.4

Un corps est un anneau commutatif A , non réduit à $\{0\}$ dans lequel tout élément non-nul est inversible :

$$\text{Corps } \forall x \in A, x \neq 0, \exists y \in A, xy = 1$$

PROPOSITION 4.2.5

- (a) Soit A un corps, alors A est un anneau intègre.
 (b) Soit A un corps, I un idéal de A . Alors soit $I = \{0\}$ soit $I = A$.

EXEMPLE.

- On note par \mathbb{Z} l'anneau des entiers relatifs,
 \mathbb{Q} le corps des nombres rationnels,
 \mathbb{R} le corps des nombres réels et
 \mathbb{C} le corps des nombres complexes.

9.1 Corps des fractions

PROPOSITION 9.1.1 Si A est un anneau intègre, alors il existe un corps K appelé corps des fractions de A et noté $\text{Frac}(A)$ tel que

- (i) $A \subset K$;
 (ii) Pour tout corps L et tout morphisme d'anneaux injectif $\phi : A \rightarrow L$, il existe un unique morphisme de corps $\psi : K \rightarrow L$ tel que $\psi|_A = \phi$.

PREUVE. Construction. On définit sur $A \times (A \setminus \{0\})$ la relation \mathcal{R} par

$$(a, b)\mathcal{R}(c, d) \iff ad = bc.$$

On vérifie en utilisant l'intégrité de A que \mathcal{R} est une relation d'équivalence. On note K l'ensemble quotient $A \times A \setminus \{0\} / \mathcal{R}$, et $\frac{a}{b}$ l'image de (a, b) dans ce quotient. L'application de A dans K qui envoie a sur $(a, 1) = \frac{a}{1}$ est injective, et on identifie A avec son image. On muni alors K des lois

$$\begin{aligned} + : K \times K &\rightarrow K, \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ad + bc}{bd} \in K \quad (\text{"addition"}); \\ \times : K \times K &\rightarrow K, \left(\frac{a}{b}, \frac{c}{d}\right) \mapsto \frac{ac}{bd} \in K \quad (\text{"multiplication"}); \end{aligned}$$

On vérifie que ces lois sont bien définies et munissent K d'une structure de corps, l'élément neutre pour l'addition étant $0/1$, l'élément neutre pour la multiplication étant $1/1$, et l'inverse d'un élément non nul $\frac{a}{b}$ étant $\frac{b}{a}$.

Propriété universelle. Soient L un corps et $\phi : A \rightarrow L$ un morphisme d'anneaux injectif il existe un unique morphisme de corps $\psi : K \rightarrow L$ tel que $\psi|_A = \phi$. L'application

$$A \times A \setminus (\{0\}) \rightarrow L, \quad (a, b) \mapsto \frac{\phi(a)}{\phi(b)} \in L$$

passé au quotient $(a, b) \mapsto \frac{a}{b}$ et définit un morphisme de corps $K \rightarrow L$ qui convient.

D'autre part, si ψ est un tel morphisme de corps, alors on a $\psi(a/b) = \frac{\psi(a)}{\psi(b)}$, ce qui montre l'unicité de ψ .

9.2 Caractéristique d'un corps, sous-corps premier

DÉFINITION 9.2.1 Si A est un anneau commutatif, il existe un unique morphisme d'anneaux $\phi : \mathbb{Z} \rightarrow A$, donné par $\phi(n) = n \cdot 1$. Son noyau, $\text{Ker}\phi$, est un sous-groupe de \mathbb{Z} . Le générateur positif de ce sous-groupe est appelé la caractéristique de A et est noté $\text{car}(A)$.

PROPOSITION 9.2.2 La caractéristique d'un corps K est nul ou un nombre premier $p = \text{car}(K)$. Si la caractéristique du corps est nulle, celui-ci contient un sous-corps, isomorphe à \mathbb{Q} . Sinon, il contient un sous-corps, isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où p est sa caractéristique. Le corps ainsi obtenu est le plus petit corps contenu dans K , on l'appelle sous-corps premier de K .

PREUVE. D'après le théorème d'isomorphisme, on a $\mathbb{Z}/\text{Ker}\phi \simeq \text{Im}\phi$, ce quotient est donc un anneau intègre, c'est à dire $\text{Ker}\phi$ est un idéal premier de \mathbb{Z} , $\{0\}$ ou $p\mathbb{Z}$, p premier. Si c'est $\{0\}$, la propriété 9.1.1(ii) montre que \mathbb{Q} est isomorphe à un sous-corps K' de K ; K' est alors le sous-corps engendré par 1 donc le plus petit sous-corps de K . Si $\text{Ker}\phi = p\mathbb{Z}$, alors le sous-anneau $\text{Im}\phi$ de K engendré par 1 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, donc c'est un corps et le plus petit sous-corps de K .

9.3 Modules et espaces vectoriels

DÉFINITION 9.3.1 Si A est un anneau commutatif. Un A -module est la donnée d'un groupe abélien M , muni d'une loi externe

$$\times : A \times M \rightarrow M, (a, m) \mapsto am \in M \quad (\text{"multiplication externe"})$$

satisfaisant les propriétés suivantes :

$$\text{Mo1 } \forall a \in A, \forall x, y \in M, a(x + y) = ax + ay,$$

$$\text{Mo2 } \forall a, b \in A, \forall x \in M, (a + b)x = ax + bx,$$

$$\text{Mo3 } \forall a, b \in A, \forall x \in M, a(bx) = (ab)x.$$

Si K est un corps, un espace vectoriel sur K est un K -module.

EXEMPLE. La notion de \mathbb{Z} -module coïncide avec celle de groupe abélien :

$$\times : \mathbb{Z} \times M \rightarrow M, (a, m) \mapsto am \in M$$

EXEMPLE 9.3.2 Si A est un anneau commutatif, et $n \in \mathbb{N}$, A^n est un A -module pour la lois externe

$$\times : A \times A^n \rightarrow A^n, (a, (a_1, \dots, a_n)) \mapsto (aa_1, \dots, aa_n) \in A^n$$

EXEMPLE 9.3.3 Soit A un anneau commutatif, et soit M un A -module. Si X est un ensemble, alors pour tout $a \in A$ et pour toute application $f : X \rightarrow M$ on pose

$$\forall x \in X, (af)(x) = a(f(x)) \in M.$$

L'ensemble M^X de toutes les applications $f : X \rightarrow M$ est un A -module avec la loi externe

$$\times : A \times M^X \rightarrow M^X, (a, f) \mapsto af \in M^X$$

DÉFINITION 9.3.4 Soit A un anneau commutatif, et soient M, N deux A -modules. Une application $\phi : M \rightarrow N$ est dit un **morphisme** de A -modules (ou une application A -linéaire) si c'est un morphisme de groupe abéliens, et si elle vérifie la condition suivante :

$$\text{Mor. } \forall \lambda \in A, \forall m \in M, \phi(\lambda m) = \lambda \phi(m)$$

Un isomorphisme de A -modules est un morphisme A -modules qui est bijectif. Son inverse est alors un morphisme A -modules.

Sous- A -modules, sous-espaces vectoriels

DÉFINITION 9.3.5 Soit A un anneau commutatif, et soit M un A -module. Un sous-groupe abélien $N \subset M$ est dit un sous- A -module si il vérifie la condition suivante :

$$\text{Sous - module } \forall \lambda \in A, \forall x \in N, \lambda x \in N.$$

Si K est un corps, un sous- K -module d'un espace vectoriel sur K est dit un sous-espace vectoriel sur K .

EXEMPLE 9.3.6 Soit A un anneau commutatif, et soient M, N deux A -modules. L'ensemble $\mathcal{L}(M, N)$ des applications A -linéaires $\phi : M \rightarrow N$ est un sous- A -module du module N^M de toutes les applications de M vers N . En particulier, si K est un corps, et E un K -espace vectoriel, le dual de E , noté E^\vee est l'espace vectoriel $\mathcal{L}(E, K)$.

9.4 Rappels sur les espaces vectoriels

DÉFINITION 9.4.1 Soit K un corps. Une famille $(a_i)_{i \in I}$ d'éléments de K est dite **presque nulle** si et seulement si l'ensemble

$$\{i \in I \mid a_i \neq 0\}$$

est fini.

Soient E un espace vectoriel sur K et $\mathbf{e} = (e_i)_{i \in I}$ une famille d'éléments de E . La famille \mathbf{e} est

- une famille **génératrice** si et seulement si pour tout x de E , il existe une famille presque nulle $(a_i)_{i \in I}$ d'éléments de K tels que

$$x = \sum_{i \in I} a_i e_i$$

- une famille **libre** si et seulement si pour toute famille presque nulle $(a_i)_{i \in I}$ d'éléments de K , on a

$$\sum_{i \in I} a_i e_i = 0 \Rightarrow \forall i \in I, a_i = 0$$

On dit alors que les éléments de $(e_i)_{i \in I}$ sont **linéairement indépendants**

- une **base** de E si elle est à la fois libre et génératrice. Pour tout x de E , il existe alors une seule famille presque nulle $(a_i)_{i \in I}$ d'éléments de K tels que

$$x = \sum_{i \in I} a_i e_i.$$

On dit que $(a_i)_{i \in I}$ sont les **coordonnées** de x dans la base \mathbf{e} .

THÉORÈME 9.4.2 (SUR L'EXISTENCE D'UNE BASE) Si E est un espace vectoriel sur K , alors il existe une base de E . Toutes les bases ont le même cardinal appelé **dimension** de E et noté $\dim E$.

On ne donne pas de démonstration ici, mais on remarque :



PROPOSITION 9.4.3 Soit K un corps. Soient E un espace vectoriel sur K et $\mathbf{e} = (e_i)_{i \in I}$ une famille d'éléments de E . Les conditions suivantes sont équivalentes :

- (i) la famille \mathbf{e} est une **base** de E ,
- (ii) la famille \mathbf{e} est une famille **génératrice** et toute sous-famille propre de \mathbf{e} n'est pas génératrice
- (iii) la famille \mathbf{e} est une famille **libre** et toute famille contenant \mathbf{e} distincte de \mathbf{e} n'est pas libre



DÉFINITION 9.4.4 Un espace vectoriel E sur K est dit de **dimension finie**, si et seulement s'il admet une famille **génératrice finie**

THÉORÈME 9.4.5 Si E est un espace vectoriel sur K de dimension finie, toutes les bases de E ont le même cardinal appelé **dimension** de E et noté $\dim E$. En outre :

- (i) une famille **génératrice** a au moins $\dim E$ éléments, et c'est une base si elle en a exactement $\dim E$,
- (ii) une famille **libre** a au plus $\dim E$ éléments, et est une base si elle en a exactement $\dim E$.

EXEMPLE 9.4.6 Si E est un espace vectoriel sur K de dimension finie, et si (e_1, \dots, e_n) une base de E , alors E^\vee est un espace vectoriel de dimension finie, une base étant donnée par $(e_1^\vee, \dots, e_n^\vee)$ où e_i^\vee est définie par

$$\forall (a_1, \dots, a_n) \in K^n, e_i^\vee(a_1 e_1 + \dots + a_n e_n) = a_i \in K.$$

Cette base $(e_1^\vee, \dots, e_n^\vee)$ est appelée la **base duale** de (e_1, \dots, e_n) .



9.5 Matrices de changement de bases

DÉFINITION 9.5.1 Soit E est un K -espace vectoriel de dimension finie et soient $\mathbf{e} = (e_1, \dots, e_n)$, $\mathbf{e}' = (e'_1, \dots, e'_n)$ deux bases de E .

La matrice

$$P = P_{\mathbf{e}}^{\mathbf{e}'} = (p_{ij}), p_{ij} = e_i^\vee(e'_j) \in K$$

qui a pour j -ème colonne les coordonnées de e'_j dans la base (e_1, \dots, e_n) , est appelée matrice de changement de base de \mathbf{e} à \mathbf{e}' .

PROPOSITION 9.5.2

(i) Soit x un élément d'un K -espace vectoriel E de dimension finie et soient $\mathbf{e} = (e_1, \dots, e_n)$, $\mathbf{e}' = (e'_1, \dots, e'_n)$ deux bases de E .

On pose

$$x = x_1 e_1 + \dots + x_n e_n, \quad x = x'_1 e'_1 + \dots + x'_n e'_n,$$

Alors

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P_{\mathbf{e}}^{\mathbf{e}'} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$$

où $P_{\mathbf{e}}^{\mathbf{e}'}$ est matrice de changement de bases.

(ii) On a les relations

$$P_{\mathbf{e}'}^{\mathbf{e}''} P_{\mathbf{e}''}^{\mathbf{e}'} = P_{\mathbf{e}''}^{\mathbf{e}''} \text{ et } P_{\mathbf{e}}^{\mathbf{e}'^{-1}} = P_{\mathbf{e}'}^{\mathbf{e}}.$$

DÉFINITION 9.5.3 Soit $\phi : E \rightarrow E$ une application linéaire d'un K -espace vectoriel E de dimension finie vers E , et soit $\mathbf{e} = (e_1, \dots, e_n)$ une bases de E .

La matrice

$$A = A_{\phi, \mathbf{e}} = (a_{ij}), p_{ij} = e_i^\vee(\phi(e_j)) \in K$$

qui a pour j -ème colonne les coordonnées de $\phi(e_j)$ dans la base (e_1, \dots, e_n) , est appelée matrice de l'application linéaire dans la base donnée.

PROPOSITION 9.5.4

(i) Soit $\phi : E \rightarrow E$ une application linéaire d'un K -espace vectoriel E de dimension finie vers E , et soient $\mathbf{e} = (e_1, \dots, e_n)$, $\mathbf{e}' = (e'_1, \dots, e'_n)$ deux bases de E .

On pose

$$x = x_1 e_1 + \dots + x_n e_n, \quad x = x'_1 e'_1 + \dots + x'_n e'_n, \\ \phi(x) = y_1 e_1 + \dots + y_n e_n, \quad \phi(x) = y'_1 e'_1 + \dots + y'_n e'_n,$$

Alors

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A_{\phi, \mathbf{e}} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

où $A_{\phi, \mathbf{e}}$ est matrice de l'application linéaire dans la base \mathbf{e} .

(ii) On a les relations

$$A_{\phi, e'} = P_e^{e'-1} A_{\phi, e} P_e^{e'}.$$

9.6 Caractères d'un groupe

DÉFINITION 9.6.1 *Etant donné un groupe G et un corps K , on appelle caractère de G dans K tout morphisme de groupes de G dans K^* .*

Si G est abélien, on note $X^*(G) = \text{Hom}(G, \mathbb{C}^*)$ le groupe des caractères de G dans \mathbb{C} avec la lois

$$(\chi_1 \chi_2)(g) = \chi_1(g) \chi_2(g).$$

EXEMPLE 9.6.2 *Si $G = \mathbb{Z}/n\mathbb{Z}$ un morphisme de G dans \mathbb{C}^* est déterminé par l'image de $\bar{1}$ qui vérifie*

$$\chi(\bar{1})^n = \chi(n\bar{1}) = \chi(\bar{0}) = 1.$$

C'est donc une racine n -ième de l'unité dans \mathbb{C}^ .*

Inversement si ζ est une racine n -ième de l'unité, l'application

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^\times, \quad \bar{x} \mapsto \zeta^x$$

est un caractère de $\mathbb{Z}/n\mathbb{Z}$; on a ainsi obtenu une bijection du groupe $\mu_n(\mathbb{C})$ sur $X^(\mathbb{Z}/n\mathbb{Z})$. Notons en outre que l'exponentielle complexe fournit un isomorphisme de groupes*

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n(\mathbb{C}), \quad \bar{x} \mapsto \exp\left(\frac{2i\pi x}{n}\right)$$

THÉORÈME 9.6.3 (D'INDÉPENDANCE LINÉAIRE DE CARACTÈRES) *Soient $\sigma_1, \dots, \sigma_n \in \text{Hom}(G, K^*)$ n caractères distincts d'un groupe G dans un corps K . Alors ce sont n éléments linéairement indépendants du K -espace vectoriel des applications de G dans K .*

PREUVE : On raisonne par récurrence sur l'entier n . Un caractère n'était jamais nul, l'assertion est vraie pour $n = 1$.

Pour $n \geq 2$, supposons l'assertion vraie pour tout $i < n$, et choisissons dans K des éléments a_i ($1 \leq i \leq n$) tels que pour tout $x \in G$ on ait l'égalité

$$e(x) = a_1 \sigma_1(x) + \dots + a_n \sigma_n(x) = 0$$

Si α appartient à G , on a aussi pour tout x de G

$$e(\alpha x) - \sigma_n(\alpha) e(x) = 0,$$

soit

$$a_1(\sigma_1(\alpha) - \sigma_n(\alpha))\sigma_1(x) + \cdots + a_{n-1}(\sigma_{n-1}(\alpha) - \sigma_n(\alpha))\sigma_{n-1}(x) = 0.$$

Comme les σ_i sont distincts, il existe un α dans G tel que $\sigma_1(\alpha) - \sigma_n(\alpha)$ soit non nul; et d'après l'hypothèse de récurrence, les caractères $\sigma_1, \dots, \sigma_{n-1}$ sont linéairement indépendants, donc on a

$$a_1(\sigma_1(\alpha) - \sigma_n(\alpha)) = 0 = a_{n-1}(\sigma_{n-1}(\alpha) - \sigma_n(\alpha))$$

d'où $a_1 = 0$. On utilise de nouveau l'hypothèse de récurrence avec les caractères $\sigma_2, \dots, \sigma_n$, d'où $a_2 = \dots = a_n$, ce qui prouve que $\sigma_1, \dots, \sigma_n$ sont linéairement indépendants.

COROLLAIRE 9.6.4 *Soient E et E' deux corps, et $\sigma_1, \dots, \sigma_n \in \text{Hom}(E, E')$ n morphismes distincts de E dans E' . Alors ce sont n éléments linéairement indépendants du E' -espace vectoriel des applications de E dans E' .*

PREUVE : il suffit de poser $G = E^*$, $K = E'$, et d'utiliser le théorème 9.6.3.

NOTATIONS. Si X est un ensemble fini, on considère la forme

$$\mathbb{C}^X \times \mathbb{C}^X \rightarrow \mathbb{C}, \quad (f, g) \rightarrow \langle f, g \rangle = \frac{1}{\#X} \sum_{x \in X} \overline{f(x)}g(x).$$

PROPOSITION 9.6.5 *Si G est un groupe fini et χ, χ' deux caractères de G , dans \mathbb{C} , alors*

$$\langle \chi, \chi' \rangle = \begin{cases} 1, & \text{si } \chi = \chi' \\ 0, & \text{sinon.} \end{cases}$$

COROLLAIRE 9.6.6 *Si G est un groupe fini, la famille $(\chi)_{\chi \in X^*(G)}$ est une famille libre du \mathbb{C} -espace vectoriel \mathbb{C}^G*

10 Extensions.

10.1 Polynômes irréductibles.

Rappelons que si K est un corps l'anneau de polynômes $K[X]$ est euclidien, donc principal et factoriel, en particulier tout polynôme non nul s'écrit de manière unique comme produit de son coefficient dominant et de polynômes irréductibles unitaires.

Et on obtient la définition suivante pour les éléments irréductibles de $K[X]$:

DÉFINITION 10.1.1 Soit K un corps. Un polynôme $P \in K[X]$ est dit irréductible, s'il vérifie les deux conditions suivantes :

Irr1. $P \notin K$

Irr2. Si $P = QR$ avec $Q, R \in K[X]$ alors $Q \in K^\times$ ou $R \in K^\times$.

EXEMPLES 10.1.2 Soit K un corps.

(i) Un polynôme $P \in K[X]$ de degré un est irréductible.

(ii) Un polynôme $P \in K[X]$ de degré 2 ou 3 est irréductible si et seulement s'il n'admet pas de racine dans K .

(iii) Tout polynôme irréductible sur \mathbb{C} est de degré un.

(iv) Tout polynôme irréductible sur \mathbb{R} est de degré ≤ 2 .

PROPOSITION 10.1.3 Soit K un corps. Un polynôme $f \in K[X]$ est irréductible si et seulement si l'anneau quotient $K[X]/(f)$ est un corps.

10.2 Extensions, degré.

DÉFINITION 10.2.1

(i) Soit K un corps et L un autre corps, contenant K . On dit que L est une extension de K . C'est un espace vectoriel sur K .

(ii) Soit L une extension d'un corps K . On appelle degré de L sur K la dimension $\dim_K L$ de L considéré comme espace vectoriel sur K . On le note $[L : K]$, le degré est éventuellement infini. Si le degré $[L : K]$ est fini on dit que L est une extension finie de K .

(iii) Si L est une extension de K et $A = (\alpha_i)_{i \in I}$ une partie de L , on appelle extension de K engendrée par A le sous-corps minimal $K(A)$ de L contenant K et A . Les α_i s'appellent les générateurs de $K(A)$ sur K . Tout élément de $K(A)$ s'écrit comme une fraction rationnelle à coefficients dans K d'éléments α_i .

Par exemple, \mathbb{C} est une extension finie de \mathbb{R} de degré 2.

De plus $\mathbb{C} = \mathbb{R}(i)$

THÉORÈME 10.2.2 Si K, L et E sont trois corps emboîtés tels que $K \subset L \subset E$, alors

$$[E : K] = [E : L] \cdot [L : K]$$

PREUVE : On note $(a_i)_{i \in I}$ une base de E sur L , et $(b_j)_{j \in J}$ une base de L sur K .

Pour tout $x \in E$, il existe une famille finie $(\alpha_i)_{i \in I_1}$, $I_1 \subset I$, d'éléments de L tels que $x = \sum_{i \in I_1} \alpha_i a_i$.

Mais chaque α_i est combinaison linéaire à coefficients dans K d'éléments b_j : $\alpha_i = \sum_{j \in J_1} \beta_{i,j} b_j$, pour une

famille finie $\beta_{i,j} \in K$. Ceci implique que $x = \sum_{(i,j) \in I_1 \times J_1} \beta_{i,j} a_i b_j$, et donc la famille $(a_i b_j)_{i \in I, j \in J}$ est génératrice pour le K -espace vectoriel E .

C'est une famille libre : si $(\beta_{i,j})_{(i,j) \in X}$, $X \subset I_1 \times J_1 \subset I \times J$ est une famille finie d'éléments de K telle que $\sum_{(i,j) \in X} \beta_{i,j} a_i b_j = 0$, alors les images I_1 et J_1 de X par projection sur I et J sont finies et on a :

$$\sum_{(i,j) \in X} \beta_{i,j} a_i b_j = \sum_{i \in I_1} \left(\sum_{j \in J_1} \beta_{i,j} b_j \right) a_i = 0$$

et comme pour tout $i \sum_{j \in J_1} \beta_{i,j} b_j$ appartient à L , on trouve $\sum_{j \in J_1} \beta_{i,j} b_j = 0$ pour tout $i \in I_1$, puis $\beta_{i,j} = 0$ pour tout $(i,j) \in X$. \square

COROLLAIRE 10.2.3 *Pour n corps emboîtés*

$$K \subset K_1 \subset \dots \subset K_n,$$

on a l'égalité

$$[K_n : K] = [K_1 : K] \cdot [K_2 : K_1] \cdot \dots \cdot [K_n : K_{n-1}].$$

EXEMPLE 10.2.4 *On considère le sous-corps $K = \mathbb{Q}(\sqrt[3]{2}, i)$ de \mathbb{C} , il contient $\mathbb{Q}(\sqrt[3]{2})$, et $K = \mathbb{Q}(\sqrt[3]{2})(i)$, donc*

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2})(i) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Le polynôme $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ et le polynôme $X^2 + 1$ l'est dans $\mathbb{Q}(\sqrt[3]{2})[X]$. Donc,

$$[\mathbb{Q}(\sqrt[3]{2})(i) : \mathbb{Q}(\sqrt[3]{2})] = 2, [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3, \text{ et } [K : \mathbb{Q}] = 6.$$

10.3 Éléments algébriques

Soit E une extension d'un corps K .

DÉFINITION 10.3.1

(i) Un élément α de E est dit **algébrique sur K** s'il existe un polynôme non nul P de $K[X]$ tel que $P(\alpha) = 0$.

(ii) Une extension E de K est dite **algébrique** si tout élément α de E est algébrique sur K .

(iii) Si $\alpha \in E$ est un élément algébrique sur K l'ensemble des polynômes $P \in K[X]$ tels que $P(\alpha) = 0$, forme un idéal de $K[X]$, non réduit à (0) . Cet idéal est principal, et son générateur unitaire s'appelle le **polynôme minimal de α sur K** .

PROPOSITION 10.3.2 *Soit E une extension d'un corps K , et soit α un élément de E algébrique sur K de polynôme minimal P .*

i) *Si $Q \in K[X]$ admet α comme racine, alors P divise Q dans $K[X]$.*

(ii) *Le polynôme P est irréductible dans $K[X]$.*

(iii) *Le sous-anneau $K[\alpha]$ de E est un corps $K(\alpha)$ et on a $[K(\alpha) : K] = \deg P$. La famille $(1, \alpha, \dots, \alpha^{n-1})$, où $n = \deg P$, est une base de $K(\alpha)$ sur K .*

PREUVE : L'assertion (i) traduit que P engendre l'idéal des éléments de $K[X]$, ayant α comme racine.

(ii) Si P se factorise en QR dans $K[X]$, alors on a $P(\alpha) = Q(\alpha)R(\alpha) = 0$ dans le corps E , donc $Q(\alpha) = 0$ ou $R(\alpha) = 0$, et P divise Q ou R . \square

(iii) Le sous-anneau $K[\alpha]$ est l'image de l'homomorphisme d'évaluation $Q \mapsto Q(\alpha)$ de $K[X]$ dans E , dont le noyau est l'idéal (P) , maximal d'après (ii) (voir 4.5.4). Par le théorème d'isomorphisme, l'anneau $K[\alpha]$ est donc isomorphe au quotient $K[X]/(P)$, qui est un corps. Si $n = \deg P$, la famille $(1, \alpha, \dots, \alpha^{n-1})$ est libre sur K car P est le polynôme non nul de plus petit degré qui annule α . Elle est génératrice car pour tout $Q \in K[X]$ on a $Q(\alpha) = R(\alpha)$, où R est le reste de la division euclidienne de Q par P , et donc $R(\alpha) = \sum_{i=0}^{n-1} r_i \alpha^i$, $r_i \in K$. La famille est donc une base de $K(\alpha)$ sur K . En particulier on a $[K(\alpha) : K] = n = \deg P$. \square

PROPOSITION 10.3.3 Soit E une extension finie d'un corps K ($[E : K] = n \in \mathbb{N}$), alors E est algébrique sur K .

PREUVE. Soit α un élément de E . Si $n = [E : K]$, la famille de $n + 1$ éléments $(1, \alpha, \dots, \alpha^n)$ n'est pas libre, donc il existe $P(X) = \sum_{i=0}^n a_i X^i$ non nul dans $K[X]$ tel que $\sum_{i=0}^n a_i \alpha^i = P(\alpha) = 0$. \square

REMARQUE. L'assertion réciproque est fautive : l'extension $E = \overline{\mathbb{Q}} \subset \mathbb{C}$ de \mathbb{Q} , formée par tous les nombres complexes algébriques sur \mathbb{Q} (E est bien un corps, exercice), est algébrique par définition, mais $[E : \mathbb{Q}]$ n'est pas finie. En effet, on vérifie qu'il existe des polynômes irréductibles sur \mathbb{Q} de tout degré $n \geq 1$, par exemple $X^n - 2$ (exercice).

10.4 Corps de rupture, corps de décomposition

Remarquons que pour un corps arbitraire K et pour tout polynôme P non constant de $K[X]$ on peut construire une extension L de K dans laquelle P possède une racine : quitte à factoriser P on peut le supposer irréductible, auquel cas on a vu que l'anneau quotient $K[X]/(P)$ est un corps. La classe $X + (P)$ est alors une **racine** de P dans $K[X]/(P)$.

THÉORÈME 10.4.1 (SUR L'ISOMORPHISME) Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.

C'est clair d'après le paragraphe précédent, proposition 10.3.2 et sa preuve, puisque P est à un facteur constant près le polynôme minimal de α sur K .

DÉFINITION 10.4.2 Soit K un corps, et P un polynôme irréductible. On dit qu'un corps L contenant K est un corps de rupture de P sur K s'il existe un $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.

REMARQUE 10.4.3 Avec les notations de la proposition, on peut donner une construction matricielle de l'anneau $K[X]/(P)$, corps de rupture de P sur K .

En effet, on écrit $P = \sum_{j=0}^n a_j X^j$, et on suppose que $a_n = 1$, alors dans la base

$$(\overline{1}, \overline{X}, \dots, \overline{X^{n-1}}) \bmod (P)$$

de $K[X]/(P)$ la multiplication $\mu : Q \mapsto \overline{X}Q \bmod (P)$ a pour matrice

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix},$$

dont le polynôme minimal est P . Il vient que $K[A] \simeq K[X]/\text{Ker}(\mu)$ est isomorphe à $K[X]/(P)$.

En itérant la construction de corps de rupture ci-dessus (on choisit à chaque étape un facteur irréductible de P de degré > 1 sur le corps obtenu), on peut construire pour tout polynôme $P \in K[X]$ une extension finie L' de K dans laquelle P s'écrit comme produit de facteurs du premier degré. La construction implique que L' peut être choisi de telle façon que $[L' : K] \leq n!$.

Cours N°10. Mercredi le 8 decembre 2004

RAPPEL :

THÉORÈME SUR L'ISOMORPHISME 10.4.1 Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.

DÉFINITION 10.4.4 On considère un polynôme P de $K[X]$ de degré supérieur ou égal à 1, et une extension E de K , dans laquelle P s'écrit $P(X) = (X - \alpha_1) \cdots (X - \alpha_n)$. Alors le corps $L = K(\alpha_1, \dots, \alpha_n)$ s'appelle corps de décomposition de P dans E . C'est l'extension minimale de K dans E , dans laquelle P se décompose en produit de facteurs linéaires.

On va vérifier que ce corps est uniquement déterminé à isomorphisme près :

THÉORÈME 10.4.5 (SUR UN PROLONGEMENT D'ISOMORPHISME) On considère un isomorphisme de corps $\sigma : K \rightarrow K'$, et un polynôme irréductible $P(X) = \sum_{j=0}^n a_j X^j \in K[X]$. On note $P^\sigma = \sum_{j=0}^n \sigma(a_j) X^j \in K'[X]$. On choisit une extension de K contenant une racine β de P , et une extension de K' , contenant une racine β' de $P^\sigma(X)$. Alors il existe un isomorphisme de corps

$$\tilde{\sigma} : K(\beta) \rightarrow K'(\beta'),$$

qui prolonge σ et tel que $\tilde{\sigma}(\beta) = \beta'$.

PREUVE. Comme σ est un isomorphisme de corps de K dans K' , l'application

$$\varphi : K[X] \rightarrow K'[X], \quad Q(X) = \sum_{j=0}^n b_j X^j \mapsto Q^\sigma(X) = \sum_{j=0}^n \sigma(b_j) X^j$$

est un isomorphisme d'anneaux. On en déduit

$$\begin{array}{ccc} \tilde{\sigma} : & K(\beta) & \rightarrow & K'(\beta') \\ & \uparrow & & \uparrow \\ \bar{\varphi} : & K[X]/(P) & \rightarrow & K'[X]/(P^\sigma), \\ & Q + (P) & \mapsto & Q^\sigma + (P^\sigma) \end{array}$$

Cela montre à la fois que P^σ est un élément irréductible de $K'[X]$ (par le théorème sur l'isomorphisme 10.4.1, $K'[X]/(P^\sigma)$ est un corps), et que si $\theta = Q(\beta) \in K(\beta)$, son image par $\tilde{\sigma}$ est bien définie par l'égalité $\tilde{\sigma}(\theta) = Q^\sigma(\beta')$. \square

THÉORÈME 10.4.6 (DE L'UNICITÉ) Soient $\sigma : K \xrightarrow{\sim} K'$ un isomorphisme de corps, $P(X) = \sum_{j=0}^n a_j X^j$ un polynôme de $K[X]$, et notons $P^\sigma = \sum_{j=0}^n \sigma(a_j) X^j \in K'[X]$.

A P , on associe une extension E de K , dans laquelle il se factorise en produit de termes du premier degré, $P(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$, et on note $B = K(\alpha_1, \dots, \alpha_n)$ le corps de décomposition de P dans E .

On définit de même E' et B' pour le polynôme P^σ . Il existe alors un isomorphisme de corps

$$\tau : B \xrightarrow{\sim} B',$$

dont la restriction à K est égale à σ .

PREUVE. Le polynôme P s'écrit $P(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$, les α_i étant des éléments de E . Raisonnons par récurrence sur le nombre N d'éléments α_i , qui n'appartiennent pas à K .

Si $N = 0$, tous les α_i appartiennent à K , donc $B = K$ est isomorphe à $B' = K'$, et $\tau = \sigma$.

Pour $N \geq 1$, supposons que α_1 n'appartienne pas à K .

C'est un élément algébrique sur K , de polynôme minimal S , et il existe $Q \in K[X]$ tel que $P = SQ$.

Dans $E'[X]$, on a les égalités

$$P^\sigma = S^\sigma Q^\sigma = a'(X - \alpha'_1) \cdots (X - \alpha'_n).$$

Si β est une racine de S^σ dans une extension de E' , il vient

$$P^\sigma(\beta) = 0 = a'(\beta - \alpha'_1) \cdots (\beta - \alpha'_n),$$

donc il existe un indice i , qu'on peut supposer égal à 1, tel que $\beta = \alpha'_1 \in E'$. On utilise le théorème 10.4.5 pour le polynôme irréductible S : il existe un isomorphisme de corps

$$\tau : K(\alpha_1) \xrightarrow{\sim} K'(\alpha'_1),$$

qui prolonge σ .

On considère maintenant P comme un polynôme à coefficients dans $L = K(\alpha_1)$.

Le nombre de racines de P qui n'appartiennent pas à L est strictement inférieur à N , et l'hypothèse de récurrence nous donne l'existence d'un prolongement de τ ,

$$\pi : L(\alpha_2, \dots, \alpha_n) \xrightarrow{\sim} L'(\alpha'_2, \dots, \alpha'_n),$$

avec $L' = K'(\alpha'_1)$. On termine en remarquant que $L(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, et que $L'(\alpha'_2, \dots, \alpha'_n) = K'(\alpha'_1, \alpha'_2, \dots, \alpha'_n)$. \square

COROLLAIRE 10.4.7 (DE L'UNICITÉ) *Soient K un corps, P un polynôme de $K[X]$, et L, L' deux corps de décomposition de P sur K . Alors il existe un isomorphisme de corps de L sur L' dont la restriction à K est l'identité.*

En effet, il suffit d'utiliser le résultat précédent pour $\sigma = id : K \rightarrow K$.

10.5 Sous-groupes finis dans K^*

Exposant d'un groupe abélien fini

Soit G un groupe abélien fini. On note $\omega(G)$, et on appelle exposant de G le ppcm des ordres des éléments de G . C'est le plus petit entier strictement positif tel que $x^{\omega(G)} = e$ pour tout élément $x \in G$. Alors par définition du ppcm, et par le théorème de Lagrange, $\omega(G)$ divise $|G|$.

Soient K un corps, et G un sous-groupe fini de K^\times . Alors tout $x \in G$ est racine du polynôme $X^{\omega(G)} - 1$, et ce polynôme a au plus $\omega(G)$ racines dans le corps K . Par suite $\omega(G) \geq |G|$, donc $\omega(G) = |G|$.

LEMME 8.1.5. *Soit G un groupe. On suppose que $a, b \in G$ sont deux éléments tels que $ab = ba$, et qui sont d'ordre r et s , respectivement, où r et s sont premiers entre eux. Alors ab est d'ordre rs .*

C'est un fait général sur les éléments d'un groupe qui commutent entre eux.

PREUVE (rappel). Puisque $(ab)^{rs} = a^{rs}b^{rs} = 1$, l'ordre de ab est un diviseur r_1s_1 de rs , où $r_1 \mid r$ et $s_1 \mid s$. Donc

$$a^{r_1s_1}b^{r_1s_1} = (ab)^{r_1s_1} = 1.$$

On élève les deux parties en la puissance r_2 , où $r_1r_2 = r$. Alors

$$a^{r_1r_2s_1}b^{r_1r_2s_1} = 1,$$

donc, puisque $a^{r_1r_2s_1} = (a^{r_1r_2})^{s_1} = 1$,

$$b^{r_1r_2s_1} = 1.$$

Ceci implique que $s \mid r_1r_2s_1$, et, car $\text{pgcd}(s, r_1r_2) = 1$, il vient que $s = s_1$. Un argument similaire montre que $r = r_1$, donc l'ordre de ab est rs .

PROPOSITION 10.5.1 *Dans un groupe commutatif, l'ensemble des ordres des éléments est stable par ppcm.*

PREUVE. Soient en effet x un élément d'ordre r et y un élément d'ordre s . Il s'agit de construire un élément d'ordre $\text{ppcm}(r, s)$, soit m . Or on peut écrire $m = r's'$, où r' divise r , s' divise s , et les deux entiers sont premiers entre eux, puisque $\text{ppcm}(r, s)\text{pgcd}(r, s) = rs$. Par exemple, si

$$r = \prod_{i=1}^k p_i^{\alpha_i}, s = \prod_{i=1}^k p_i^{\beta_i}, \text{ on pose } r' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^k p_i^{\alpha_i}, s' = \prod_{\substack{i=1 \\ \alpha_i \leq \beta_i}}^k p_i^{\beta_i}.$$

(voir la remarque ci-dessous pour une autre construction). De là on a $x^{r/r'}$ d'ordre r' , et $y^{s/s'}$ d'ordre s' , on peut donc appliquer le lemme 8.1.5 et conclure.

EXEMPLE.

$$r = 120 = 2^3 \cdot 3 \cdot 5, s = 180 = 2^2 \cdot 3^2 \cdot 5, r' = 8 = 2^3, s = 45 = 3^2 \cdot 5.$$

REMARQUE. Voici une autre construction pour la proposition 10.5.1 : (disponible à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-13ppcm.mws) Notons $d = \text{pgcd}(r, s)$.

Il s'agit de construire un diviseur s' de s qui soit premier à r/d , et tel que $r' := \text{ppcm}(r, s)/s'$ divise r . Pour ce faire, on part de $s' = s$ et on réécrit s' en $s'/\text{pgcd}(s', r/d)$ tant que ce $\text{pgcd} \neq 1$:

```
> restart;r:=120; s:=180;sprime:=s;
> i:=0;d:=gcd (r,s);
> while (gcd(sprime, r/d)<>1) do
> gcd(sprime, d);
> sprime:=(sprime/gcd(sprime, r/d));
> printf("i=%d,lcm=%d,sprime=%d, rprime=%d\n"
> ,i,
> lcm(r,s),sprime, lcm(r,s)/sprime);
> i:=i+1;od;
```

$i := 0$

$sprime := 90$

$i=0, lcm=360, sprime=90, rprime=4$

$$i := 1$$

$$sprime := 45$$

$$i=1, lcm=360, sprime=45, rprime=8$$

$$i := 2$$

Autrement dit, pour $r = 120, s = 180, d = \text{pgcd}(120, 180) = 60, r/d = 2,$

$$\text{ppcm}(120, 180) = 360 = 2 \cdot 180 = 4 \cdot 90 = 8 \cdot 45.$$

Application : $x^{r/r'}$ est d'ordre r' , et $y^{s/s'}$ est d'ordre s' , donc on peut utiliser le lemme 8.1.5.

Cyclicité des sousgroupes finies de K^\times

THÉORÈME 10.5.2 *Soit K un corps. Tout sous-groupe fini G de K^\times est cyclique.*

PREUVE. Par définition du ppcm, et par le théorème de Lagrange, l'exposant $\omega(G)$ divise $|G|$, et tous les $x \in G$ sont solution de $x^{\omega(G)} = 1$, mais le polynôme $X^{\omega(G)} - 1$ possède au plus $\omega(G)$ racines dans le corps K . Donc, $\omega(G) = |G|$, et on conclut avec la proposition 10.5.1.

EXERCICES

- 10.1 Soit $K \subset E$ une extension de corps. Montrer que $\overline{K_E} = \{x \in E, x \text{ est algébrique sur } K\}$ est un sous-corps de E .
- 10.2 Montrer qu'il existe des polynômes irréductibles sur \mathbb{Q} de tout degré $n \geq 1$, par exemple $X^n - p$, où p est un nombre premier.
- 10.3 Soit K un corps. En considérant l'ordre des élément d'un groupe cyclique, montrer que $n = \sum_{d|n} \varphi(d)$. En déduire une autre preuve que tout sous-groupe d'ordre n de K^* est cyclique.
- 10.4 Soit K un corps à q éléments, $q \geq 4$. Montrer que $\sum_{x \in K} x^2 = 0$. Plus généralement, calculer, pour $s \geq 1$, la somme $\sum_{x \in K} x^s$.
- 10.5 Si H est un sous-groupe de \mathbb{C}^* tel que \mathbb{C}^*/H est fini, montrer que $H = \mathbb{C}^*$.
- 10.6 Montrer qu'il existe des polynômes irréductibles sur \mathbb{Q} de degré arbitraire n , par exemple $X^n - p$, p un nombre premier.

11 Morphisme de Frobenius, structure des corps finis

Pour un plus large développement sur les corps finis le lecteur est renvoyé aux textes d'E. Peyre [Pey], ainsi que Lidl-Niederreiter, [Li-Ni].

Jusqu'ici nous avons rencontré l'exemple fondamental des corps finis $\mathbb{Z}/p\mathbb{Z}$ (p premier), quotients de \mathbb{Z} par un idéal maximal. Il s'agit maintenant de décrire tous les corps finis.

11.1 Structure

PROPOSITION-DÉFINITION 11.1.1 *Soit A un anneau commutatif de caractéristique p un nombre premier. L'application*

$$\text{Fr}_p : x \mapsto x^p, x \in A$$

est un morphisme d'anneau appelé morphisme de Frobenius. Plus généralement, si A est un anneau commutatif de caractéristique p premier et si q est une puissance de p , on note $\text{Fr}_q : x \mapsto x^q$.

PREUVE. Le point à montrer est l'additivité. Or si $x, y \in A$ on développe $(x + y)^p$ par la formule du binôme, et on conclut par le fait que si $1 \leq i \leq p - 1$, p divise l'entier C_p^i .

THÉORÈME 11.1.2 : *Soit \mathcal{K} un corps fini. Alors \mathcal{K} est de caractéristique p un nombre premier, \mathcal{K} est de cardinal $q = p^d$, avec $d = [\mathcal{K} : \mathbb{Z}/p\mathbb{Z}]$, et Fr_p est un automorphisme du corps \mathcal{K} .*

Inversement, si p est premier et d est un entier strictement positif, il existe à isomorphisme près un unique corps à $q = p^d$ éléments, qui est le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. On note ce corps \mathbb{F}_q . De plus, le groupe $(\mathbb{F}_q, +)$ est isomorphe au groupe $(\mathbb{Z}/p\mathbb{Z})^d, +)$ et le groupe multiplicatif \mathbb{F}_q^ est isomorphe à $\mathbb{Z}/(q - 1)\mathbb{Z}$ (groupe cyclique d'ordre $q - 1$).*

PREUVE. Vérifions ensuite qu'un corps \mathcal{K} à q éléments est un corps de décomposition pour le polynôme $X^q - X$. Comme \mathcal{K} a q éléments, \mathcal{K}^* est un groupe d'ordre $q - 1$. Par conséquent,

$$\forall x \in \mathcal{K}^*, x^{q-1} = 1.$$

Autrement dit les q éléments de \mathcal{K} sont racines de $X^q - X$. Du fait du degré, on obtient

$$X^q - X = \prod_{\alpha \in \mathcal{K}} (X - \alpha).$$

En particulier, \mathcal{K} est un corps de décomposition pour le polynôme $X^q - X$.

Soit inversement \mathcal{K} un corps de décomposition pour le polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$, où p est premier et q est une puissance de p . Comme Fr_q est un morphisme de corps de \mathcal{K} , l'ensemble de ses points fixes les racines de $X^q - X$ est un sous-corps de \mathcal{K} . Comme \mathcal{K} est engendré par ces racines sur \mathbb{F}_p , \mathcal{K} est l'ensemble des racines de $P(X) = X^q - X$. Comme $P' = -1$, toutes les racines de P sont simples (par les propriétés de la dérivé formelle P' d'un polynôme), P a donc ses q racines distinctes dans \mathcal{K} et \mathcal{K} a exactement q éléments. D'après 10.4.7 ceci établit l'assertion d'existence et unicité à isomorphisme près du corps \mathbb{F}_q .

Enfin la cyclicité du groupe \mathbb{F}_q^* est un cas particulier du théorème 10.5.2. \square

THÉORÈME 11.1.3 : Soit $q = p^n$ où p est premier. Tout sous-corps du corps \mathbb{F}_q est de cardinal p^m , où m est un diviseur de n . Et pour tout diviseur m de n , \mathbb{F}_q possède un unique sous-corps de cardinal p^m , qui est l'ensemble des racines du polynôme $X^{p^m} - X$ dans \mathbb{F}_q .

PREUVE. Si \mathcal{K} est un sous-corps de \mathbb{F}_q , alors il contient le sous-corps premier F_p , donc c'en est une extension finie et \mathbb{F}_q est une extension finie de \mathcal{K} . De là \mathcal{K} a pour cardinal p^m , et le cardinal de \mathbb{F}_q est une puissance de $(p^m)^d$ de celui de \mathcal{K} . Ainsi $n = md$. Inversement, si m divise n , alors $p^m - 1$ divise $p^n - 1$, donc le polynôme $X^{p^m-1} - 1$ divise le polynôme $X^{p^n-1} - 1$, donc le polynôme $X^{p^m} - X$ divise $X^{p^n} - X$, ce qui entraîne que $X^{p^m} - X$ a p^m racines distinctes dans \mathbb{F}_q . Ces racines forment l'unique sous-corps de cardinal p^m de \mathbb{F}_q . \square

Dans la pratique, pour pouvoir faire les calculs, le corps \mathbb{F}_{p^n} ($n > 1$) sera construit comme anneau quotient de type $\mathbb{F}_p[X]/(Q)$, en choisissant un polynôme irréductible Q de degré n . (voir le théorème 11.2.1).

11.2 Polynômes sur les corps finis. Nombre de polynômes irréductibles

THÉORÈME 11.2.1 Soient p un nombre premier et q une puissance de p . Pour tout entier $m \geq 1$, il existe $\theta \in \mathbb{F}_{q^m}$ tel que $\mathbb{F}_{q^m} = \mathbb{F}_q[\theta]$ et il existe P polynôme irréductible de degré m sur \mathbb{F}_q .

PREUVE. Soient θ un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$, et P son polynôme minimal sur \mathbb{F}_q . Alors on a $\mathbb{F}_{q^m} = \mathbb{F}_q[\theta]$ et P est un polynôme irréductible sur \mathbb{F}_q dont \mathbb{F}_{q^m} est un corps de rupture. Autrement dit, on a un isomorphisme

$$\mathbb{F}_q[X]/(P) \xrightarrow{\sim} \mathbb{F}_{q^m}$$

qui envoie la classe de X sur θ . En particulier, on a $\deg P = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = m$.

REMARQUE 11.2.2 Si on a un tel polynôme et α une racine de P dans \mathbb{F}_{q^n} , la famille $\{1, \alpha, \dots, \alpha^{n-1}\}$ est une base du \mathbb{F}_q -espace vectoriel \mathbb{F}_{q^n} .

PROPOSITION 11.2.3 Soient P un polynôme irréductible sur \mathbb{F}_q et α une racine de P dans une extension de \mathbb{F}_q . Alors, pour tout polynôme Q sur \mathbb{F}_q , $Q(\alpha) = 0$ si et seulement si P divise Q .

En effet, P est alors le polynôme minimal de α sur \mathbb{F}_q , voir la proposition 10.3.2.

LEMME 11.2.4 Soit P un polynôme irréductible de degré m sur \mathbb{F}_q . Alors P divise $X^{q^n} - X$ si et seulement si m divise n .

PREUVE. Le corps de rupture de P sur \mathbb{F}_q est de cardinal q^m , donc tout élément y vérifie $x^{q^m} = x$, donc aussi en itérant si m divise n , $x^{q^n} = x$. On conclut que P divise $X^{q^n} - X$ en appliquant la proposition précédente avec $Q = X^{q^n} - X$. Inversement si P divise $X^{q^n} - X$ alors le corps \mathbb{F}_{q^n} contient un corps de rupture de P , de cardinal q^m , donc par le théorème 11.1.3 m divise n .

THÉORÈME 11.2.5 Soit P un polynôme irréductible sur \mathbb{F}_q de degré m . Alors P est scindé sur le corps \mathbb{F}_{q^m} et a toutes ses racines simples. Si α est l'une d'elles, ces m racines sont $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$. En particulier si $P \neq X$ toutes les racines de P ont le même ordre multiplicatif dans $\mathbb{F}_{q^m}^*$.

PREUVE. On a vu que le corps de rupture de P , $\mathbb{F}_q[X]/(P)$, de cardinal q^m , est formé de l'ensemble des racines du polynôme $X^{q^m} - X$. Par suite $X^{q^m} - X$ s'annule en une racine de P , donc par la proposition il est divisible par P sur \mathbb{F}_q et à fortiori sur \mathbb{F}_{q^m} . Ainsi puisque $X^{q^m} - X$ est scindé à racines simples sur \mathbb{F}_{q^m} , il en est de même pour P .

Ensuite, on écrit $P = \sum_{i=0}^m a_i X^i$ avec $a_i \in \mathbb{F}_q$. Si α est une racine de P , alors

$$\text{Fr}_q(P(\alpha)) = \sum_{i=0}^m \text{Fr}_q(a_i) \text{Fr}_q(\alpha)^i = P(\text{Fr}_q(\alpha)) = 0$$

où l'avant-dernière égalité vient du fait que $\text{Fr}_q(x) = x$ pour tout $x \in \mathbb{F}_q$. Par conséquent $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ sont des racines de P . Montrons par l'absurde que ces m racines sont distinctes. En effet, dans le cas contraire, il existe i, j avec $0 \leq i < j \leq m-1$ tels que $\alpha^{q^i} = \alpha^{q^j}$ et donc $\alpha^{q^j - q^i} = 1$. Par conséquent

$$\text{ord}(\alpha) | q^j - q^i = q^i (q^{j-i} - 1).$$

Mais comme $\alpha \in \mathbb{F}_{q^m}^*$, l'ordre de α est premier à q donc, par le lemme de Gauss, $\text{ord}(\alpha) | q^{j-i} - 1$, et $\alpha^{q^{j-i}} = \alpha$, donc α appartient au corps $\mathbb{F}_{q^{j-i}}$, ce qui est en contradiction avec le fait que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg P = m$. Ainsi on a

$$P(X) = (X - \alpha)(X - \alpha^q) \dots (X - \alpha^{q^{m-1}}).$$

La dernière assertion résulte de ce que Fr_q est un automorphisme du corps \mathbb{F}_{q^m} , donc il conserve l'ordre multiplicatif des éléments.

COROLLAIRE 11.2.6 *Le corps de décomposition de tout polynôme de degré m irréductible sur \mathbb{F}_q est \mathbb{F}_{q^m} .*

Tout élément $t \in \mathbb{F}_{q^n}$ est racine d'un unique polynôme irréductible unitaire $P = P_t$ de $\mathbb{F}_q[X]$ de degré d divisant n , ainsi

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{P \text{ unitaire} \\ \text{irréductible sur } \mathbb{F}_q \\ \deg P = d}} P(X)$$

(dans cette formule comme dans la suite du paragraphe, on convient que la notation $d|n$ signifie que d est un diviseur POSITIF de n).

PREUVE. Puisque $\mathbb{F}_q[X]$ est factoriel, on applique le lemme 11.2.4 en utilisant que $X^{q^n} - X$ est premier avec sa dérivée, donc sa factorisation est sans multiplicité.

Soit $\nu_n(q)$ le nombre de polynômes unitaires irréductibles de degré n sur \mathbb{F}_q . Alors l'identité ci-dessus montre que

$$q^n = \sum_{d|n} d \nu_d(q),$$

et pour récupérer $\nu_d(q)$ de cette formule on utilise la formule d'inversion de Möbius.

Formule d'inversion de Möbius

DÉFINITION 11.2.7 On appelle fonction de Möbius la fonction définie sur \mathbb{N} par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers distincts,} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

On voit que $\mu(nm) = \mu(n)\mu(m)$, si m et n sont premiers entre eux.

REMARQUE. On peut aussi définir la fonction de Möbius $\mu(n)$ par l'égalité formelle

$$\sum_{n=1}^{\infty} \mu(n)n^{-s} = \prod_{p \text{ premier}} (1 - p^{-s}) = \zeta(s)^{-1}.$$

PROPOSITION 11.2.8 (FORMULE D'INVERSION) Soient $(a_n), (b_n)$ ($n \geq 1$) deux suites d'entiers liées par

$$b_n = \sum_{d|n} a_d \quad (n \geq 1).$$

Alors on a

$$a_n = \sum_{d|n} \mu(n/d)b_d \quad (n \geq 1).$$

En effet on a

$$\sum_{d|n} \mu(n/d)b_d = \sum_{d|n} \mu(n/d) \sum_{d'|d} a_{d'} = \sum_{d'|n} a_{d'} \sum_{\delta|(n/d')} \mu(\delta),$$

où $\delta = n/d$ divise n/d' . Pour $m > 1$, si s désigne le nombre de diviseurs premiers distincts positifs de m , on a

$$\sum_{\delta|m} \mu(\delta) = \sum_{t=0}^s C_t^s (-1)^t = (1-1)^s = 0.$$

REMARQUE. La formule d'inversion $a_n = \sum_{d|n} \mu(n/d)b_d$ résulte aussi facilement de l'identité formelle

$$\sum_{n=1}^{\infty} b_n n^{-s} = \sum_{n=1}^{\infty} a_n n^{-s} \zeta(s), \quad \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

c'est à dire

$$\sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} b_n n^{-s} \zeta(s)^{-1}.$$

Une application directe de la formule d'inversion nous permet d'énoncer :

THÉORÈME 11.2.9 Pour tout corps fini \mathbb{F}_q et tout entier $n \geq 1$ on a :

$$(i) X^{q^n} - X = \prod_{d|n} \prod_{\substack{P \text{ unitaire} \\ \text{irréductible sur } \mathbb{F}_q \\ \deg P=d}} P(X),$$

$$(ii) q^n = \sum_{d|n} d\nu_d(q).$$

(iii) Le nombre de polynômes irréductibles unitaires de degré n sur \mathbb{F}_q est

$$\nu_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

REMARQUE. On voit facilement par l'absurde que l'expression à droite est non nulle, car il y a unicité de l'écriture (éventuelle) d'un entier comme somme de puissances différentes de q . Comme $\nu_n \geq 0$, on obtient $\nu_n > 0$; on a ainsi une nouvelle preuve du fait qu'il existe un polynôme irréductible de degré n sur \mathbb{F}_q (théorème 11.2.1).

EXEMPLE. Soit $q = 3$, $n = 2$, alors $\nu_2(3) = \frac{1}{2}(3^2 - 3) = 3$.

> Factor(T^9-T) mod 3;

$$T(T+2)(T^2+T+2)(T^2+2T+2)(T+1)(T^2+1)$$

Ordre d'un polynôme, polynômes primitifs

La notion d'ordre est présentée ici comme complément, les démonstrations sont laissées en exercice (voir [Li-Ni]).

DÉFINITION 11.2.10 Soit P un polynôme non nul sur \mathbb{F}_q . Si $P(0) \neq 0$, l'ordre de P est le plus petit entier strictement positif e tel que P divise $X^e - 1$. Si $P(0) = 0$, alors il existe Q dans $\mathbb{F}_q[X]$ non nul en 0 et h entier positif tels que $P = X^h Q$, et dans ce cas on pose $\text{ord}(P) = \text{ord}(Q)$.

EXERCICE. Montrer l'existence d'un tel nombre e , avec $e \leq q^m - 1$ si $m = \deg P \geq 1$ [Indication : raisonner dans l'anneau fini $\mathbb{F}_q[X]/(P)$].

REMARQUE 11.2.11 Si P est irréductible de degré m sur \mathbb{F}_q , alors l'ordre e de P divise $q^m - 1$. De plus d'après le lemme 11.2.4 si $e > 1$ (donc $P(X) \neq X$), m est minimal > 0 pour cette propriété, donc le degré m de P est l'ordre multiplicatif de q modulo e .

THÉORÈME 11.2.12 Soient $m \geq 1$ et $e > 1$. Le nombre de polynômes irréductibles unitaires sur \mathbb{F}_q de degré m et d'ordre e est

$$N_{q,m,e} = \begin{cases} \varphi(e)/m & , \text{ si } m \text{ est l'ordre multiplicatif de } q \text{ mod } e \\ 0 & , \text{ sinon,} \end{cases}$$

où $\varphi(e)$ est l'indicateur d'Euler de e .

PREUVE (en exercice).

On considère le groupe cyclique $\mathbb{F}_{2^{11}}^*$ d'ordre $2^{11} - 1 = 23 \cdot 89$. Soit $\alpha \in \mathbb{F}_{2^{11}}^*$ un élément d'ordre 23. La factorisation de $X^{23} - 1$ en irréductibles sur \mathbb{F}_2 est :

$$\begin{aligned} X^{23} - 1 &= X^{23} + 1 = (X + 1)P_0(X)P_1(X) = \\ &(X + 1)(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1) \end{aligned}$$

où

$$P_0(X) = X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1 = \prod_{i \in I} (X - \alpha^i), I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

$$P_1(X) = X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1 = \prod_{j \in J} (X - \alpha^j), J = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}.$$

(Notons que toute racine $\neq 1$ de $X^{23} - 1$ est d'ordre 23. Pour écrire les racines de P_0 et P_1 ci-dessus, on a noté α une racine de P_0 et appliqué le théorème 11.2.5.)

Pour $e = 23$ et $q = 2$, on a bien $\text{ord}(2 \bmod 23) = 11$: les polynômes irréductibles d'ordre 23 sur \mathbb{F}_2 sont de degré 11, il y en a $\varphi(23)/11 = 2$.

REMARQUE. L'ensemble

$$I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

coïncide avec l'ensemble des **résidus quadratiques** modulo 23, et l'ensemble complémentaire

$$J = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

coïncide avec l'ensemble des **non-résidus quadratiques** modulo 23.

Le **morphisme de Frobenius** $\alpha^k \mapsto \alpha^{2k}$ laisse bien sûr les ensembles d'exposants I et J stables, et en effet on a $\left(\frac{2}{23}\right) = 1$ (voir la loi complémentaire de la loi de réciprocité quadratique 8.5.4). L'application $\alpha^k \mapsto \alpha^{-k}$ échange les ensembles I et J puisque $\left(\frac{-1}{23}\right) = -1$ par le critère d'Euler 8.3.1 ; en particulier P_1 est le polynôme minimal de α^{-1} sur \mathbb{F}_2 .

REMARQUE 11.2.13 : *Le degré de P irréductible sur \mathbb{F}_q d'ordre e est l'ordre multiplicatif de q modulo e .*

En effet, on a $e|q^m - 1$, avec un m minimal. Par exemple, si $e = 23$, $q = 2$, alors $\text{ord}(2) \bmod 23 = 11$.

DÉFINITION 11.2.14 *Un polynôme P de degré m sur \mathbb{F}_q est dit **primitif** sur \mathbb{F}_q s'il est le polynôme minimal sur \mathbb{F}_q d'une racine primitive de \mathbb{F}_{q^m} (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$).*

Une étude de l'ordre des produits de polynômes fournit la caractérisation suivante, où on voit qu'à degré m fixé ce sont les polynômes primitifs qui atteignent l'ordre maximum $q^m - 1$ (voir l'exercice 11.2.10) :

THÉORÈME 11.2.15 *Un polynôme P de degré m est primitif sur \mathbb{F}_q si et seulement si P est unitaire, non nul en 0 et d'ordre $q^m - 1$.*

Résumé des propriétés des polynômes irréductibles sur \mathbb{F}_q

THÉORÈME 11.2.16 *Soit α un élément de \mathbb{F}_{q^m} , une extension de \mathbb{F}_q . Soient d le degré, et P le polynôme minimal de α sur \mathbb{F}_q . Alors,*

- (i) P est irréductible sur \mathbb{F}_q et son degré d divise m .
- (ii) un polynôme Q sur \mathbb{F}_q s'annule α si et seulement si P divise Q .
- (iii) tout polynôme irréductible unitaire sur \mathbb{F}_q nul en α est égal à P .
- (iv) P divise $X^{q^d} - X$ et $X^{q^m} - X$.
- (v) Les racines de P sont $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$ et P est le polynôme minimal sur \mathbb{F}_q de toutes ces racines. Si de plus $\alpha \neq 0$, on a :
- (vi) l'ordre de P est égal à celui de α dans le groupe multiplicatif $\mathbb{F}_{q^m}^*$.
- (vii) P est un polynôme primitif sur \mathbb{F}_q si et seulement si α est d'ordre $q^d - 1$ dans $\mathbb{F}_{q^m}^*$.

EXERCICES

11.1 Ecrire les tables d'addition et de multiplication des corps \mathbb{F}_4 , \mathbb{F}_8 et \mathbb{F}_9 .

11.2 Ecrire la factorisation de $T^9 - T$ (resp. $T^8 - T$) en irréductibles sur \mathbb{F}_3 (resp. sur \mathbb{F}_2). Quels sont les facteurs primitifs ?

11.3 Soit p premier. Calculer "directement" le nombre de polynômes irréductibles de degré 5 sur \mathbb{F}_p .

- 11.4 Soit $P \in \mathbb{F}_{q^m}[X]$. Montrer $P \in \mathbb{F}_q[X]$ si et seulement si $P(X)^q = P(X^q)$.
- 11.5 Ecrire tous les polynômes irréductibles unitaires de degré 4 sur \mathbb{F}_2 et trouver leur ordre.
- 11.6 Montrer que $X^4 + 2$ est irréductible sur \mathbb{F}_5 et trouver son ordre.
- 11.7 Un polynôme P de degré m sur \mathbb{F}_q est dit primitif sur \mathbb{F}_q s'il est le polynôme minimal sur \mathbb{F}_q d'une racine primitive de \mathbb{F}_{q^m} (un générateur du groupe cyclique $\mathbb{F}_{q^m}^*$). Trouver le nombre des polynômes primitifs de degré m sur \mathbb{F}_q .
- 11.8 Soit p premier impair. Montrer que \mathbb{F}_{p^2} est un corps de rupture de $X^4 + 1$ sur \mathbb{F}_p . Si $\alpha^4 + 1 = 0$ dans \mathbb{F}_{p^2} , montrer que $y = \alpha + \alpha^{-1}$ vérifie $y^2 = 2$. En déduire que 2 est un carré dans \mathbb{F}_p si et seulement si $p \equiv \pm 1 \pmod{8}$.

11.3 Construction d'isomorphismes à partir des polynômes irréductibles

Les calculs dans un corps fini d'ordre non premier $q = p^d$ passent par le choix d'un polynôme irréductible P sur \mathbb{F}_p de sorte que $\mathbb{F}_q = \mathbb{F}_p[T]/(P)$. Il est important de savoir transposer ces calculs dans le corps construit en choisissant un autre polynôme irréductible Q . Il s'agit donc d'explicitier un isomorphisme de corps entre $\mathbb{F}_p[T]/(P)$ et $\mathbb{F}_p[T]/(Q)$.

RAPPEL :

THÉORÈME SUR L'ISOMORPHISME 10.4.1 Soient L une extension de K et $\alpha \in L$ une racine d'un polynôme irréductible P de $K[X]$. Alors l'anneau $K[\alpha]$ est un corps isomorphe à $K[X]/(P)$.

Pour construire un isomorphisme $\sigma : \mathbb{F}_p[T]/(Q) \xrightarrow{\sim} \mathbb{F}_p[T]/(P)$, on cherche une racine β de Q dans $\mathbb{F}_p[T]/(P) = \mathbb{F}_p[\alpha]$, et on pose $\sigma(T \bmod Q) = \beta \in \mathbb{F}_p[\alpha]$. Ici $\alpha = T \bmod P$.

Un exemple de calcul en Maple (disponible à l'adresse cachée :

<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple>
dans le fichier 4ma1-14irr.mws)

```
> Factor(T^27-T) mod 3;

      T (T + 2) (T + 1) (T^3 + 2T + 2) (T^3 + T^2 + 2T + 1) (T^3 + T^2 + T + 2) (T^3 + 2T + 1)
      (T^3 + T^2 + 2) (T^3 + 2T^2 + 1) (T^3 + 2T^2 + T + 1) (T^3 + 2T^2 + 2T + 2)
> P:=T^3+2*T^2+T+1;
      P := T^3 + 2T^2 + T + 1
> alias(alpha = RootOf(P)) ;
      alpha
> Q:=T^3+T^2+2*T+1;
      Q := T^3 + T^2 + 2T + 1
> Factor(Q, alpha) mod 3;
      (T + 2alpha^2 + 1) (T + alpha + 2) (T + alpha^2 + 2alpha + 1)
> Factor(T^27-T, alpha) mod 3;

      T (T + 2alpha^2 + 1) (T + 2alpha^2) (T + alpha^2 + 2) (T + 2alpha^2 + alpha) (T + 2) (T + alpha^2) (T + 1)
      (T + alpha^2 + 2alpha + 2) (T + 2alpha^2 + 2) (T + 2alpha) (T + alpha^2 + 2alpha) (T + 2alpha + 1) (T + alpha)
      (T + 2alpha^2 + 2alpha + 2) (T + alpha + 2) (T + alpha^2 + alpha + 1) (T + 2alpha^2 + alpha + 2)
      (T + alpha^2 + 2alpha + 1) (T + 2alpha + 2) (T + alpha^2 + alpha) (T + alpha + 1) (T + alpha^2 + 1)
      (T + 2alpha^2 + 2alpha) (T + 2alpha^2 + 2alpha + 1) (T + 2alpha^2 + alpha + 1) (T + alpha^2 + alpha + 2)
```

Les polynômes $P(T) = T^3 + 2T^2 + T + 1$ et $Q(T) = T^3 + T^2 + 2T + 1$ sont irréductibles sur \mathbb{F}_3 , car sans racines.

EXEMPLE 11.3.1 Construire un isomorphisme entre les corps $\mathbb{F}_3[T]/(P)$ et $\mathbb{F}_3[T]/(Q)$.

Soit $\alpha = T \bmod P$, c'est une racine de P dans $\mathbb{F}_3[T]/(P)$.

On utilise le fait que Q a aussi une racine dans $\mathbb{F}_3[T]/(P)$, par exemple $\beta = \alpha^2 - 1$ (voir le calcul en Maple ci-dessus). On obtient un isomorphisme $\sigma : \mathbb{F}_3[T]/(Q) \xrightarrow{\sim} \mathbb{F}_3[T]/(P)$ en posant $\sigma(T \bmod Q) = \beta = \alpha^2 - 1$.

Pour trouver β "à la main", on peut le chercher sous la forme $c_0 + c_1\alpha + c_2\alpha^2$ avec $c_0, c_1, c_2 \in \mathbb{F}_3$ (faire l'exercice).

11.4 Théorème de la base normale

EXEMPLE 11.4.1 *Considérons le polynôme $P(X) = X^4 + X + 1$. Il est primitif sur \mathbb{F}_2 et toute racine α de P dans son corps de décomposition \mathbb{F}_{16} est un élément primitif de \mathbb{F}_{16} :*

$$\begin{aligned}\alpha^4 &= 1 + \alpha, \alpha^5 = \alpha + \alpha^2, \alpha^6 = \alpha^2 + \alpha^3, \alpha^7 = 1 + \alpha + \alpha^3, \alpha^8 = 1 + \alpha^2, \\ \alpha^9 &= \alpha + \alpha^3, \alpha^{10} = 1 + \alpha + \alpha^2, \alpha^{11} = \alpha + \alpha^2 + \alpha^3, \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3, \\ \alpha^{13} &= 1 + \alpha^2 + \alpha^3, \alpha^{14} = 1 + \alpha^3, \alpha^{15} = 1.\end{aligned}$$

On a une base $\{1, \alpha, \alpha^2, \alpha^3\}$ de \mathbb{F}_{16} sur \mathbb{F}_2 . Les éléments

$$\alpha, \text{Fr}_2(\alpha) = \alpha^2, \text{Fr}_2^2(\alpha) = \alpha^4 = 1 + \alpha, \text{Fr}_2^3(\alpha) = \alpha^8 = 1 + \alpha^2$$

sont toutes les racines de $P(X) = X^4 + X + 1$. On observe que ces éléments sont linéairement dépendants : $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ n'est pas une base de \mathbb{F}_{16} sur \mathbb{F}_2 .

On a cependant le résultat suivant :

THÉORÈME 11.4.2 (DE LA BASE NORMALE) *Soient p un nombre premier et $q = p^d$. Alors il existe un élément θ de \mathbb{F}_q pour lequel $(\theta, \text{Fr}_p(\theta), \dots, \text{Fr}_{p^{d-1}}(\theta))$ est une base de \mathbb{F}_q sur \mathbb{F}_p .*

PREUVE. On considère le morphisme d'anneaux

$$\varphi : \mathbb{F}_p[T] \rightarrow \text{End}_{\mathbb{F}_p}(\mathbb{F}_q), \quad \sum_{i=0}^n a_i T^i \mapsto \sum_{i=0}^n a_i \text{Fr}_p^i$$

et on pose pour tout P de $\mathbb{F}_p[T]$ et tout x de \mathbb{F}_q , $P \cdot x = \varphi(P)(x)$. En particulier, $T \cdot x = \text{Fr}_p(x) = x^p$. On note \mathfrak{a} le noyau de φ . Comme tout x de \mathbb{F}_q est solution de $X^q - X = 0$, on a que $\text{Fr}_q = \text{Id}_{\mathbb{F}_q}$, et donc $T^d - 1$ appartient au noyau \mathfrak{a} . Inversement, si $P(T) = \sum_{i=0}^m a_i T^i$ appartient à ce noyau avec $m < d$, on a la relation

$$\sum_{i=0}^m a_i \text{Fr}_p^i = 0,$$

donc le polynôme $\sum_{i=0}^m a_i X^{p^i}$ s'annule sur tout \mathbb{F}_q . Or son degré est strictement inférieur à p^d , donc c'est le polynôme nul, et on a $P = 0$. Ceci prouve que $\mathfrak{a} = (T^d - 1)$ (autrement dit $T^d - 1$ est le polynôme minimal de Fr_p sur \mathbb{F}_q).

La factorisation de $\mu(T) = T^d - 1$ en polynômes irréductibles de $\mathbb{F}_p[T]$ donne une décomposition de l'espace \mathbb{F}_q en somme directe de \mathbb{F}_p -sous-espaces stables par Fr_p :

$$\mu = \prod_{i=1}^s P_i^{r_i} \text{ et } \mathbb{F}_q = \bigoplus_{i=1}^s \text{Ker}(P_i(\text{Fr}_p)^{r_i}).$$

Chaque $E_i = \text{Ker}(P_i(\text{Fr}_p)^{r_i})$ est un \mathbb{F}_p -sous-espace stable par Fr_p , et par l'indépendance linéaire des Fr_p^i établie ci-dessus, il contient un élément α_i tel que $\left(\frac{\mu}{P_i}\right)(\text{Fr}_p)(\alpha_i)$ soit non nul. Pour un tel α_i , on pose $\beta_i = \left(\frac{\mu}{P_i^{r_i}}\right)(\text{Fr}_p)(\alpha_i)$; alors la famille

$$\beta_i, P_i(\text{Fr}_p)(\beta_i), \dots, P_i^{r_i-1}(\text{Fr}_p)(\beta_i),$$

est libre, en effet, pour tous $a_0, a_1, \dots, a_{r_i-1}$ dans \mathbb{F}_p on a

$$\begin{aligned} a_0\beta_i + a_1P_i(\text{Fr}_p)(\beta_i) + \dots + a_{r_i-1}P_i^{r_i-1}(\text{Fr}_p)(\beta_i) &= 0 \\ \text{donc } a_0P_i^{r_i-1}(\text{Fr}_p)(\beta_i) + a_1P_i^{r_i}(\text{Fr}_p)(\beta_i) + \dots + a_{r_i-1}P_i^{2r_i-1}(\text{Fr}_p)(\beta_i) &= 0. \\ \text{De là } a_0 = 0 \text{ puis } a_1 = 0 \dots \text{ puis } a_{r_i-1} = 0, \end{aligned}$$

puisque $P_i^{r_i}(\text{Fr}_p)(\beta_i) = \mu(\text{Fr}_p)(\beta_i) = 0$. Ceci dit que l'ensemble des polynômes Q de $\mathbb{F}_p[T]$ tels que $Q(\text{Fr}_p)(\beta_i) = 0$, est l'idéal de $\mathbb{F}_p[T]$ engendré par $P_i^{r_i}$.

Considérons l'élément $\theta = \beta_1 + \dots + \beta_s$ de \mathbb{F}_q . Si des éléments (a_k) de \mathbb{F}_p vérifient $\sum_{k=0}^{d-1} a_k \text{Fr}_p^k(\theta) = 0$, alors le polynôme $\sum_{k=0}^{d-1} a_k T^k \in \mathbb{F}_p[T]$ est divisible par $P_i^{r_i}$ pour tout i tel que $1 \leq i \leq s$, donc par μ , et donc les a_k sont tous nuls. Cela signifie que l'élément θ engendre bien une base normale de \mathbb{F}_q sur \mathbb{F}_p .

REMARQUE 11.4.3 Pour les corps finis de caractéristique 2, les bases normales permettent de calculer les carrés et donc les puissances. En effet, si $(\theta, \theta^2, \dots, \theta^{2^{d-1}})$ est une base de \mathbb{F}_{2^d} sur \mathbb{F}_2 , alors pour tout $(a_0, a_1, \dots, a_{d-1}) \in \mathbb{F}_2^d$ on a

$$\begin{aligned} (a_0\theta + a_1\theta^2 + \dots + a_{d-1}\theta^{2^{d-1}})^2 &= a_0^2\theta^2 + a_1^2\theta^4 + \dots + a_{d-1}^2\theta^{2^d} = \\ &= a_{d-1}\theta + a_0\theta^2 + \dots + a_{d-2}\theta^{2^{d-1}}, \end{aligned}$$

où la dernière égalité est obtenue en notant que $\theta^{2^d} = \theta$.

Autrement dit le carré s'obtient par **permutation circulaire** des coordonnées. Pour un corps fini arbitraire, on a une expression similaire pour le calcul du Frobenius.

Un exemple de calcul en Maple d'une base normale est disponible à l'adresse cachée :
<http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple>
dans le fichier 4ma1-16base-n.mws

EXERCICES

- 11.1 Déterminer l'exposant des groupes abéliens $(\mathbb{Z}/60\mathbb{Z})^*$, $(\mathbb{Z}/100\mathbb{Z})^*$, $(\mathbb{Z}/187\mathbb{Z})^*$. Trouver pour chacun un élément d'ordre l'exposant.
- 11.2 En considérant l'ordre des éléments dans le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, montrer que $n = \sum_{d|n} \varphi(d)$. En déduire une autre preuve du fait que tout sous-groupe d'ordre n de K^* , où K est un corps, est cyclique.
- 11.3 Soit K un corps à q éléments, $q \geq 4$. Montrer que $\sum_{x \in K} x^2 = 0$. Plus généralement, calculer, pour $s \geq 1$, la somme $\sum_{x \in K} x^s$.

- 11.4 Soit G l'ensemble de toutes les racines de l'unité dans \mathbb{C} . Montrer que G est un sous-groupe infini de \mathbb{C}^\times , non monogène. Pour tout $n \geq 1$, montrer que G possède un unique sous-groupe cyclique d'ordre n .
- 11.5 Soit $P \in \mathbb{F}_q[X]$. Montrer que $P \in \mathbb{F}_q[X]$ si et seulement si $P(X)^q = P(X^q)$.
- 11.6 Donner une construction puis écrire les tables d'addition et de multiplication des corps \mathbb{F}_4 , \mathbb{F}_8 et \mathbb{F}_9 .
- 11.7 Écrire la factorisation de $X^9 - X$ (resp. $X^8 - X$) en irréductibles sur \mathbb{F}_3 (resp. sur \mathbb{F}_2). Quels en sont les facteurs primitifs ?
- 11.8 Soit p premier. Calculer "directement" le nombre de polynômes irréductibles de degré 5 sur \mathbb{F}_p .
- 11.9 Soit P polynôme de degré m sur le corps \mathbb{F}_q . Démontrer que P est irréductible si et seulement si les deux conditions suivantes sont vérifiées :
- (i) P divise $X^{q^m} - X$,
 - (ii) pour tout diviseur premier l de m , P est premier avec $X^{q^{m/l}} - X$.
- 11.10 Montrer l'existence de l'ordre e d'un polynôme $P \neq 0$ sur \mathbb{F}_q , et que $e \leq q^m - 1$ si $m = \deg P \geq 1$ et $P(0) \neq 0$ [Indication : raisonner dans l'anneau fini $\mathbb{F}_q[X]/(P)$].
- 11.11 Écrire tous les polynômes irréductibles unitaires de degré 4 sur \mathbb{F}_2 et trouver leur ordre.
- 11.12 Montrer que $X^4 + 2$ est irréductible sur \mathbb{F}_5 et trouver son ordre.
- 11.13 Soit p premier impair. Montrer que le polynôme $X^4 + 1$ admet une racine α dans \mathbb{F}_{p^2} . Montrer que $y = \alpha + \alpha^{-1}$ vérifie $y^2 = 2$. En déduire que 2 est un carré dans \mathbb{F}_p si et seulement si $p \equiv \pm 1 \pmod{8}$.
- 11.14 Soit $m \geq 1$. (a) Trouver le nombre de polynômes primitifs de degré m sur \mathbb{F}_q .
 (b) Montrer qu'un polynôme P de degré m est primitif sur \mathbb{F}_q si et seulement si P est unitaire, non nul en 0 et d'ordre $q^m - 1$ [Indication : pour la condition suffisante, on montrera que P est sans facteur multiple, et n'est pas produit de polynômes non constants premiers entre eux].

12 Algorithme de factorisation de Berlekamp dans $\mathbb{F}_q[X]$

On va présenter une méthode classique de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$ non constant (la méthode de Berlekamp). On suppose que P n'a pas de facteurs multiples (c'est à dire $\text{pgcd}(P, P') = 1$; dans le cas contraire, on vérifie en exercice que soit $\text{pgcd}(P, P')$ est un diviseur propre D de P et le polynôme P/D est sans facteurs multiples, soit P est la puissance p -ième d'un polynôme qu'on factorise à son tour). Soit donc $P = P_1 \dots P_s$ une factorisation inconnue de P en produit d'irréductibles non associés. Soit $A = \mathbb{F}_q[X]$, et considérons l'anneau quotient

$$A/(P) \simeq A/(P_1) \times \dots \times A/(P_s),$$

où chaque $A/(P_i)$ est un corps fini à q^{d_i} éléments, $d_i = \deg P_i$, l'isomorphisme résultant du théorème chinois. L'anneau $A/(P)$ est en particulier un espace vectoriel sur \mathbb{F}_q , de dimension $d = \deg P$, et l'endomorphisme de Frobenius $\text{Fr}_q : x \mapsto x^q$ y opère \mathbb{F}_q -linéairement. Par l'isomorphisme cette opération se traduit en une action linéaire diagonale de Fr_q sur la somme directe des espaces $A/(P_i)$. Soit \mathcal{K} le corps de décomposition de P sur \mathbb{F}_q , alors chaque corps $A/(P_i)$ est isomorphe à un sous-corps \mathcal{K}_i de \mathcal{K} tel que $\mathcal{K}_i \supset \mathbb{F}_q$, $[\mathcal{K}_i : \mathbb{F}_q] = d_i$.

De plus $A/(P_i) \simeq \mathcal{K}_i \simeq \mathbb{F}_{q^{d_i}}$ est donné par la condition :

$$\mathcal{K}_i = \{x \in \mathcal{K} \mid x^{q^{d_i}} = x\} \simeq \mathbb{F}_{q^{d_i}},$$

et son sous-corps des constantes (les points fixes sous Fr_q) est $\mathbb{F}_q = \{x \in A/(P_i) \mid x^q = x\}$. Alors

$$\text{Ker}(\text{Fr}_q - \text{Id})|_{A/(P)} \simeq \text{Ker}(\text{Fr}_q - \text{Id})|_{A/(P_1)} \oplus \dots \oplus \text{Ker}(\text{Fr}_q - \text{Id})|_{A/(P_s)} \simeq \mathbb{F}_q^s,$$

où s est le nombre des facteurs irréductibles P_i .

On obtient ainsi un critère d'irréductibilité de P :

THÉORÈME 12.0.1 (CRITÈRE D'IRRÉDUCTIBILITÉ) *Soit P un polynôme de degré d sur \mathbb{F}_q , premier avec sa dérivée. Alors P est irréductible si et seulement si le rang r de l'endomorphisme $\text{Fr}_q - \text{Id}$ du \mathbb{F}_q -espace vectoriel $A/(P)$ est égal à $d - 1$.*

En pratique on écrit la matrice de $\text{Fr}_q - \text{Id}$ dans une base de $A/(P)$, par exemple dans la base

$$1 + (P), X + (P), X^2 + (P), \dots, X^{d-1} + (P).$$

Supposons maintenant $r < d - 1$; pour trouver les facteurs P_i inconnus on cherche tout d'abord un polynôme Q tel que

$$Q + (P) \in \text{Ker}(\text{Fr}_q - \text{Id}) \subset A/(P)$$

et $Q + (P)$ n'est pas une constante mod (P) . Cela est possible grâce au fait que

$$\dim(\text{Im}(\text{Fr}_q - \text{Id})) = \text{rg}(\text{Fr}_q - \text{Id}) = d - s < d - 1 \Rightarrow \dim(\text{Ker}(\text{Fr}_q - \text{Id})) = d - \text{rg}(\text{Fr}_q - \text{Id}) \geq 2.$$

Alors $P|Q^q - Q$ puisque $Q + (P) \in \text{Ker}(\text{Fr}_q - \text{Id}) \subset A/(P)$, on a

$$Q^q - Q = \prod_{\alpha \in \mathbb{F}_q} (Q - \alpha),$$

mais $Q - \alpha \not\equiv 0 \pmod{(P)}$. Ceci implique que

$$P = \text{pgcd}(P, Q^q - Q) = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, Q - \alpha),$$

où la deuxième égalité vient de ce que les facteurs $Q - \alpha$ sont deux à deux premiers entre eux ; de plus la factorisation à droite n'est pas triviale car tous les $\text{pgcd}(P, Q - \alpha)$ sont distincts de P .

En pratique on cherche Q (un "polynôme décomposant") sous la forme $Q(X) = a_1X + a_2X^2 + \dots + a_{d-1}X^{d-1}$, et on trouve les coefficients a_i comme une solution non triviale du système des d équations linéaires qui traduisent que $(\text{Fr}_q - \text{Id})(Q) = 0$ dans $A/(P)$.

Exemples de calcul en Maple avec l'algorithme de Berlekamp sont disponibles à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans le fichier 4ma1-15berl.mws

EXERCICES

- 12.1 Dans l'algorithme ci-dessus, expliquer précisément où on a utilisé que P n'a pas de facteurs multiples. Donner un contre-exemple au théorème 12.0.1 lorsque cette hypothèse est en défaut [on pourra montrer plus précisément que le rang de l'endomorphisme $\text{Fr}_q - \text{Id}$ de l'anneau quotient est $d - s$, où s désigne le nombre des facteurs irréductibles unitaires distincts de P].
- 12.2 Soit $P \in \mathbb{F}_q[X]$ un polynôme ayant des facteurs multiples. Montrer que, soit $\text{pgcd}(P, P')$ est un diviseur propre D de P et le polynôme P/D est sans facteurs multiples, soit P est la puissance p -ième d'un polynôme $Q \in \mathbb{F}_q[X]$.

Troisième partie

Equations algébriques et variétés affines

13 Equations algébriques et variétés affines

13.1 Systèmes algébriques

Soit K un anneau commutatif. On considère un système algébrique sur K :

$$X : F_i(T_1, \dots, T_n) = 0 \quad (i \in I) \text{ où } F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n].$$

L'ensemble des solutions de X dans K est

$$X(K) = \{(x_1, \dots, x_n) \in K^n \mid \forall i, F_i(x_1, \dots, x_n) = 0\},$$

Il se peut que $X(K) = \emptyset$, c'est à dire, que le système n'a pas de solutions dans K , mais il existe des solutions dans un autre anneau.

Soit L une K -algèbre commutative, c'est à dire, un anneau muni de morphisme de structure $\gamma : K \rightarrow L$. Alors on obtient une multiplication externe d'éléments $x \in L$ par $a \in K$, donnée par la formule : $a \cdot x = \gamma(a)x \in L$. Par exemple, \mathbb{C} est une \mathbb{R} -algèbre, et tout anneau B est une \mathbb{Z} -algèbre.

Alors pour tout $(x_1, \dots, x_n) \in L^n$ on définit la valeur du polynôme $F_i(x_1, \dots, x_n) \in L$, et on pose

$$X(L) = \{(x_1, \dots, x_n) \in L^n \mid \forall i, F_i(x_1, \dots, x_n) = 0\},$$

l'ensemble des solutions de X dans L .

En particulier, tout anneau B est une \mathbb{Z} -algèbre, donc $X(B)$ est défini pour tout système algébrique sur \mathbb{Z} .

PROPOSITION 13.1.1 Soit (P_X) l'idéal de $K[T_1, \dots, T_n]$, engendré par les polynômes

$$F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n] (i \in I),$$

et on considère l'anneau quotient $A_X = K[T_1, \dots, T_n]/(P_X)$.

(a) Il existe une bijection

$$X(L) \leftrightarrow \text{Hom}_{K\text{-alg}}(A_X, L) \text{ tel que } \mathbf{x} = (x_1, \dots, x_n) \in L^n \leftrightarrow (s_{\mathbf{x}} : T_j \mapsto x_j).$$

(b) Pour tout morphisme $f : L_1 \rightarrow L_2$ de K -algèbres, il existe une application canonique d'ensembles des solutions

$$f_X : X(L_1) \rightarrow X(L_2) \text{ tel que } f_X((x_1, \dots, x_n)) = (f(x_1), \dots, f(x_n))$$

PREUVE. (a) On vérifie que

$$s_{\mathbf{x}} : K[T_1, \dots, T_n] \rightarrow L, \quad s_{\mathbf{x}} : T_j \mapsto x_j,$$

est bien défini sur l'anneau quotient $A_X = K[T_1, \dots, T_n]/(P_X)$.

(b) On vérifie que la formule $f_X((x_1, \dots, x_n)) = (f(x_1), \dots, f(x_n))$ détermine f_X de façon unique.

EXEMPLE 13.1.2 Pour voir que $N = 4m + 3$ n'est pas une somme de deux carrés : prenons

$$L_1 = \mathbb{Z}, L_2 = \mathbb{Z}/4\mathbb{Z}, \quad X : T_1^2 + T_2^2 - N = 0,$$

alors

$$X(L_2) = \emptyset \Rightarrow X(L_1) = \emptyset.$$

13.2 Variétés affines (préparation).

Soit K un corps algébriquement clos. Dans ce cas un système algébrique X sur K est essentiellement déterminé par l'ensemble des solutions $X(K) \subset K^n$, selon un résultat important de l'algèbre commutative :

THÉORÈME 13.2.1 ("NULLSTELLENSATZ") (LE THÉORÈME DES ZÉROS DE HILBERT, SANS DÉMONSTRATION) Soit K un corps algébriquement clos. Soit $(P_X) = (F_i)_{i \in I}$ l'idéal de $K[T_1, \dots, T_n]$, engendré par les polynômes

$$F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n] \quad (i \in I),$$

et on considère l'anneau quotient $A_X = K[T_1, \dots, T_n]/(P_X)$. Alors

$$F \in K[T_1, \dots, T_n] \text{ s'annule sur } X(K) \iff \exists N, F^N \in P_X = (F_i)_{i \in I}$$

REMARQUE 13.2.2 Soit $(P_X) = (F_i)_{i \in I}$ l'idéal de $K[T_1, \dots, T_n]$, engendré par les polynômes

$$F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n] \quad (i \in I).$$

Alors la condition

$$\exists N, F^N \in P_X = (F_i)_{i \in I}$$

signifie qu'on a $\overline{F}^N = 0$ dans l'anneau quotient $A_X = K[T_1, \dots, T_n]/(P_X)$, où $\overline{F} = F \bmod P_X$

DÉFINITION 13.2.3 (VARIÉTÉ AFFINE SUR UN CORPS) Soit K un corps (supposé souvent algébriquement clos). Alors l'ensemble des solutions $X(K) \subset K^n$ d'un système algébrique sur K ,

$$X : F_i(T_1, \dots, T_n) = 0 \quad (i \in I) \text{ où } F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n],$$

est dit une **variété affine** sur K

On peut supposer que l'anneau quotient $A_X = K[T_1, \dots, T_n]/(P_X)$ n'a pas d'éléments nilpotents, où $(P_X) = (F_i)_{i \in I}$ l'idéal de $K[T_1, \dots, T_n]$, engendré par les polynômes

$$F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n] \quad (i \in I).$$

13.3 Résolution d'un système linéaire dans un anneau euclidien

On considère un système linéaire sur un anneau euclidien \mathcal{A} :

$$Ax = b, \text{ où } A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{pmatrix} \in M_{mn}(\mathcal{A}),$$

$$x = \begin{pmatrix} x_1 \\ \cdots \\ \cdots \\ x_n \end{pmatrix} \in M_{n1}(\mathcal{A}), b = \begin{pmatrix} b_1 \\ \cdots \\ \cdots \\ b_m \end{pmatrix} \in M_{m1}(\mathcal{A}).$$

Pour résoudre un tel système on a besoin de la **théorie des diviseurs élémentaires**. Rappelons qu'une **transformation élémentaire** de lignes d'une matrice sur un anneau commutatif \mathcal{A} c'est l'addition à une ligne d'une autre, multipliée par un élément de \mathcal{A} . De façon similaire on définit les transformations élémentaires entières de colonnes. Une transformation élémentaire de lignes (resp. de colonnes) est équivalente à la multiplication à gauche (respectivement, à droite) de la matrice initiale par une matrice de type $E_{ij} = E + \lambda e_{ij}$ (avec $i \neq j$) dans le groupe $SL_m(\mathcal{A})$ (resp. $SL_n(\mathcal{A})$). Si l'on fait plusieurs telles transformations à la suite, on remplace la matrice A par UAV où $U \in GL_m(\mathcal{A})$, $V \in GL_n(\mathcal{A})$ sont des matrices à coefficients entiers inversibles sur \mathcal{A} , c'est à dire, telles que $\det U, \det V \in \mathcal{A}^*$.

DÉFINITION 13.3.1 On définit des **matrices élémentaires** $U \in GL_m(\mathcal{A})$ et $V \in GL_n(\mathcal{A})$ comme les matrices obtenues à partir des matrices unités I_m et I_n par une transformation élémentaire des lignes (colonnes) sur \mathcal{A} .

REMARQUE 13.3.2 On vérifie que la matrice UAV est obtenue en appliquant aux lignes (colonnes) de A les mêmes transformations élémentaires qui ont été utilisé dans la définition de U et V ci-dessus.

PROPOSITION 13.3.3 Pour toute matrice

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{pmatrix} \in M_{mn}(\mathcal{A}),$$

on peut choisir des produits $U = U_1 \cdot U_2 \cdot \cdots \cdot U_k$ et $V = V_1 \cdot V_2 \cdot \cdots \cdot V_l$ des matrices élémentaires de telle façon que $UAV = D$, avec

$$D = \begin{pmatrix} d_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & d_r & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{pmatrix} \in M_{mn}(\mathcal{A}),$$

où r est le rang de A ,
et $d_1, \dots, d_r \neq 0$
avec $d_1 | d_2 \cdots | d_r$.

COROLLAIRE 13.3.4 On en déduit que

$$Ax = b \iff UAVV^{-1}x = Ub \iff Dy = c, \text{ où } c = Ub, y = V^{-1}x, x = Vy,$$

et s'il existe une solutions, alors la solution générale sur \mathcal{A} est donnée par les formules

$$d_i y_i = c_i, \text{ pour } i \leq r, y_i \in \mathcal{A} \text{ pour } i > r, \begin{pmatrix} x_1 \\ \dots \\ \dots \\ \dots \\ x_n \end{pmatrix} = V \begin{pmatrix} c_1/d_1 \\ \dots \\ c_r/d_r \\ y_{r+1} \\ y_n \end{pmatrix}.$$

Calculs avec les matrices élargies

Pour trouver U et V on utilise les matrices élargies

$$\left(\begin{array}{c|c} A & b \\ \hline I_n & 0 \end{array} \right)$$

Montrer que par les transformations élémentaires de lignes et de colonnes la matrice élargie se transforme en

$$\left(\begin{array}{c|c} A & b \\ \hline I_n & 0 \end{array} \right) \sim \left(\begin{array}{c|c} UAV & Ub \\ \hline V & 0 \end{array} \right)$$

EXEMPLE 13.3.5 Résoudre les système linéaires sur \mathbb{Z} :

(a)

$$5x_1 + 6x_2 + 7x_3 = 4.$$

(b)

$$\begin{cases} x_1 + x_2 + x_3 = 2 \\ 4x_1 + x_2 + 4x_3 = 5 \\ x_1 - 2x_2 + x_3 = -1. \end{cases}$$

SOLUTION. (a) Ecrivons les matrices correspondantes :

$$\begin{pmatrix} 5 & 6 & 7 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 5 & 1 & 2 & 4 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 4 \\ -1 & 6 & 1 & 0 \\ 1 & -5 & -2 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

d'où

$$V = \begin{pmatrix} -1 & 6 & 1 \\ 1 & -5 & -2 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -1 & 6 & 1 \\ 1 & -5 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ y_2 \\ y_3 \end{pmatrix},$$

avec $y_2, y_3 \in \mathbb{Z}$.

SOLUTION. (b) Ecrivons les matrices correspondantes :

$$\begin{pmatrix} 1 & 1 & 1 & 2 \\ 4 & 1 & 4 & 5 \\ 1 & -2 & 1 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & -3 & 0 & -3 \\ 0 & -3 & 0 & -3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 3 & 0 & 3 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

d'où

$$V = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ y_3 \end{pmatrix},$$

avec $y_3 \in \mathbb{Z}$.

13.4 Systèmes diophantiens linéaires.

L'algorithme d'Euclide nous permet d'étudier un système diophantien linéaire (comme un cas particulier de section 13.3) :

$$Ax = b, \tag{13.1}$$

où

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(\mathbb{Z}), \quad x = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix}.$$

De l'autre côté, le système

$$UAVy = Ub \tag{13.2}$$

est équivalent à (13.1) car ses solutions correspondent bijectivement aux solutions de (13.1) par $x = Vy$. On utilise cette observation pour remplacer A par une matrice plus simple $A' = UAV$. En effet, si l'on utilise l'algorithme d'Euclide et une version de la procédure d'élimination de Gauss sans divisions, on trouve A' de la forme

$$D = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ \dots & \dots & \ddots & \dots & 0 \\ 0 & 0 & \dots & d_r & \dots \\ 0 & 0 & \dots & \dots & 0 \end{pmatrix} = UAV \quad (r = \text{rk}A). \tag{13.3}$$

Alors on voit que soit notre système est non-résoluble même sur \mathbb{Q} , soit on obtient toutes les solutions des équations $d_i y_i = c_i$, $c = Ub$ pour $i \leq r$, $0y_i = 0$ pour $i > r$. Il est donc clair que l'ensemble des solutions entières est non-vidé si et seulement si d_i divise c_i pour $i \leq r$ et il est paramétré de façon évidente. Le nombre $d_1 \dots d_r$ coïncide avec le pgcd de tous les mineurs d'ordre i de A donc on peut supposer que $d_i | d_{i+1}$. Ils sont appelés *les diviseurs élémentaires* de A .

Pour trouver la matrice $V \in GL_n(\mathbb{Z})$ il est commode d'utiliser la matrice élargie $\begin{pmatrix} A & b \\ E_n & 0 \end{pmatrix}$, et si l'on applique les transformations élémentaires de n premières colonnes et m premières lignes ci-dessus, on obtient

$$\begin{pmatrix} A' & b' \\ V & 0 \end{pmatrix} = \begin{pmatrix} UAV & Ub \\ V & 0 \end{pmatrix}.$$

PROPOSITION 13.4.1 (a) Un système linéaire

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \dots\dots\dots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases} \quad (13.4)$$

sur \mathbb{Z} est résoluble si et seulement si il est résoluble mod N pour tout nombre naturel positif N .

(b) Un système linéaire

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \dots\dots\dots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases}$$

sur \mathbb{Z} est résoluble si et seulement si pour tout nombre naturel positif $k \leq m, n$ le PGCD de tous les mineurs d'ordre k de la matrice A est égal au PGCD de tous les mineurs d'ordre k de la matrice élargie $(A|b)$.

En effet, cette méthode montre que (13.4) est résoluble si et seulement si ses diviseurs élémentaires coïncident avec ceux de la matrice étendue (avec la colonne b ajoutée). C'est équivalent à la résolubilité de toutes les congruences

$$Ax \equiv b \pmod{N}$$

où N un entier (on le voit sous la forme diagonale). Cette condition peut être étendue pour un système général diophantien. Il est clair, qu'une telle condition est nécessaire pour l'existence d'une solution. Notre étude montre que cette condition est aussi suffisante pour un système linéaire. Quand c'est vrai pour une classe d'équations diophantiennes, on dit que pour cette classe le **principe de Minkowski–Hasse** est vérifié. Le problème de validité du principe de Minkowski–Hasse pour les classes d'équations diophantiennes est un des problèmes centraux en théorie des nombres.



Groupes abéliens

(a) Soit F un groupe abélien libre (additif) de base $\{e_1, \dots, e_n\}$, $F \cong \mathbb{Z}^n$, et soit H son sous-groupe engendré par des éléments

$$f_j = \sum_{i=1}^n a_{ij}e_i \quad (i = 1, \dots, n).$$

Montrer que le groupe quotient F/H est fini si et seulement si $\det(a_{ij}) \neq 0$ et dans ce cas $\text{Card}(F/H) = |\det(a_{ij})|$.

(b) Décomposer en somme directe de groupes cycliques le groupe quotient F/H d'un groupe abélien fini F de base (e_1, e_2, e_3) , $F \cong \mathbb{Z}^3$, par son sous-groupe H engendré par des éléments f_1, f_2, f_3 , avec

$$\begin{cases} f_1 = 7e_1 + 2e_2 + 3e_3 \\ f_2 = 21e_1 + 8e_2 + 9e_3 \\ f_3 = 5e_1 - 4e_2 + 3e_3. \end{cases}$$

(c) Décomposer en somme directe de groupes cycliques le groupe quotient F/H d'un groupe abélien fini F d'une base (e_1, e_2, e_3) , $F \cong \mathbb{Z}^3$, par son sous-groupe H engendré par des éléments f_1, f_2, f_3 , avec

$$\begin{cases} f_1 = 2e_1 + 3e_2 + 4e_3 \\ f_2 = 5e_1 + 5e_2 + 6e_3 \\ f_3 = 2e_1 + 6e_2 + 9e_3. \end{cases}$$

(d) Même question pour les éléments f_1, f_2, f_3 , avec

$$\begin{cases} f_1 = 4e_1 + 7e_2 + 3e_3 \\ f_2 = 2e_1 + 3e_2 + 2e_3 \\ f_3 = 6e_1 + 10e_2 + 5e_3. \end{cases}$$

Cours N°13. Mercredi le 5 janvier 2005

13.5 Variétés algébriques (exemples)

DÉFINITION 13.2.3 (RAPPEL : VARIÉTÉ AFFINE SUR UN CORPS) Soit K un corps. Alors l'ensemble des solutions $X(K) \subset K^n$ d'un système algébrique sur K ,

$$X : F_i(T_1, \dots, T_n) = 0 \quad (i \in I) \text{ où } F_i(T_1, \dots, T_n) \in K[T_1, \dots, T_n],$$

est dit une variété affine sur K

Equations sur les corps finis : solution d'une équation affine sur \mathbb{F}_q

Soit $K = \mathbb{F}_{p^l}$. On considère une équation affine $F(X, Y) = 0$ sur \mathbb{F}_{p^l} , par exemple $X^3 + Y^3 = 1$ sur \mathbb{F}_8 ($p = 2, l = 3$). On représente les éléments de $K = \mathbb{F}_{p^l}$ sous la forme des nombres n vérifiant $0 \leq n < p^l$. En effet, étant donné un tel nombre n , on le transforme en un élément de K en utilisant l'écriture de n en base p : il existe des entiers uniques ("Chiffres" de n en base p) m_0, \dots, m_{l-1} vérifiant $0 \leq m_i < p$ et tels que $n = m_0 + m_1 p + m_2 p^2 + \dots + m_{l-1} p^{l-1}$, ce qui permet d'associer de manière unique à l'entier n , l'élément $\mu = m_0 + m_1 T + \dots + m_{l-1} T^{l-1}$ de K , $\alpha = \overline{T} = T \bmod f$.

Exemples de calcul en Maple avec les systèmes affines (disponibles à l'adresse cachée : <http://www-fourier.ujf-grenoble.fr/~panchish/04ma1-maple> dans les fichiers 4ma1-18aff.mws, 4ma1-17sys-aff.mws)

```
> restart;
> F:=(X,Y)->X^3+Y^3-1;
> p:=2;l:=3;
> %%%%%%%%%%
> (la procedure gf engendre un générateur alpha d'un corps fini F_{p^l})
> gf:= proc(p::nonnegint,l::nonnegint)
> local u,i,m, v;
> if ((p-2)^2+(l-2)^2=0) then
> alias(alpha = RootOf(x^2+x+1) mod 2);
> fi;
> if l=1 then
> alpha=1;
> else fi;
> u:=op(1, select(has, Factor(z^(p^l)-z) mod p, z^l)) ;
> alias(alpha = RootOf(u) mod p);
> return alpha,u;
> end proc;
```

$$F := (X, Y) \rightarrow X^3 + Y^3 - 1$$

$$p := 2$$

$$l := 3$$

```

> Chiffres:= proc( d::nonnegint,l::nonnegint,n::nonnegint )
> local i,m, v;
> v:=vector(l);
> m:=n;
> for i from 0 to l-1 do
> v[l-i]:=modp(m,d);m:=floor(m/d); od;
> return v;
> #gf(p,l):
> end proc:
> gf(p,l):
> g:= proc( p::nonnegint,l::nonnegint,n::nonnegint )
> local h, v, i;
> v:=vector(l);
> for i from 1 to l do
> v:=evalm(Chiffres(p,l,n));h:=add(alpha^(l-j)*v[j],j=1..l);return h;
> od;end proc:
> gf(p,l):
> points:= proc( p::nonnegint,l::nonnegint,F::polynom )
> local n1,n2,n3, L,c,v,f1, f2;
> c:=0;
> L:=NULL;
> for n1 from 0 to p^l-1 do
> for n2 from 0 to p^l-1 do
> if Eval(F(X,Y,Z),{X=g(p,l,n1),Y=g(p,l,n2)}) mod p =0 then c:=c+1;
> L:= L,(' c'=c,[g(p,l,n1),g(p,l,n2)]);fi; od; od;
> return(' L'=L):end:
> points(p,l,F);

```

$L = (c = 1, [0, 1], c = 2, [1, 0], c = 3, [\alpha, 1 + \alpha^2 + \alpha], c = 4, [1 + \alpha, \alpha^2], c = 5, [\alpha^2, 1 + \alpha], c = 6, [\alpha^2 + 1, \alpha^2 + \alpha], c = 7, [\alpha^2 + \alpha, \alpha^2 + 1], c = 8, [1 + \alpha^2 + \alpha, \alpha])$



Equations sur les corps finis : solution d'un système affine sur \mathbb{F}_q

Soit $K = \mathbb{F}_{p^l}$. On considère un système d'équations affines

$$\begin{cases} F_1(X, Y, Z) = 0 \\ F_2(X, Y, Z) = 0 \end{cases}$$

sur \mathbb{F}_{p^l} , par exemple

$$\begin{cases} X^3 + Y^3 + Z^5 = 0 \\ X + Y + 1 = 0 \end{cases}$$

sur \mathbb{F}_8 ($p = 2, l = 3$). On représente les éléments de $K = \mathbb{F}_{p^l}$ sous la forme des nombres n vérifiant $0 \leq n < p^l$. En effet, étant donné un tel nombre n , on le transforme en un élément de K en utilisant l'écriture de n en base p : il existe des entiers uniques ("Chiffres" de n en base p) m_0, \dots, m_{l-1} vérifiant $0 \leq m_i < p$ et tels que

$$n = m_0 + m_1 p + m_2 p^2 + \dots + m_{l-1} p^{l-1},$$

ce qui permet d'associer de manière unique à l'entier n , l'élément

$$\mu = \overline{m_0 + m_1 T + \dots + m_{l-1} T^{l-1}}$$

de K , $\alpha = \overline{T} = T \bmod f$.

```
> restart;
> F1:=(X,Y,Z)->X^3+Y^3+Z^5;
> F2:=(X,Y,Z)->X+Y+1;
> p:=2;l:=3;
> %%%%%%%%%%
```

(la procedure gf engendre un g n rateur alpha d'un corps fini $F_{\{p^l\}}$)

```
> gf:= proc(p::nonnegint,l::nonnegint)
> local u,i,m, v;
> if ((p-2)^2+(l-2)^2=0) then
> alias(alpha = RootOf(x^2+x+1) mod 2);
> fi;
> if l=1 then
> alpha=1;
> else fi;
> u:=op(1, select(has, Factor(z^(p^l)-z) mod p, z^1)) ;
> alias(alpha = RootOf(u) mod p);
> return alpha,u;
> end proc:
```

$$F1 := (X, Y, Z) \rightarrow X^3 + Y^3 + Z^5$$

$$F2 := (X, Y, Z) \rightarrow X + Y + 1$$

$$p := 2$$

$$l := 3$$

```
> Chiffres:= proc( d::nonnegint,l::nonnegint,n::nonnegint )
> local i,m, v;
> v:=vector(l);
> m:=n;
> for i from 0 to l-1 do
> v[l-i]:=modp(m,d);m:=floor(m/d); od;
> return v;
> #gf(p,l):
> end proc:
> gf(p,l):
> g:= proc( p::nonnegint,l::nonnegint,n::nonnegint )
> local h, v, i, n3;
> v:=vector(l);
> for i from 1 to l do
> v:=evalm(Chiffres(p,l,n));h:=add(alpha^(l-j)*v[j],j=1..l);return h;
> #gf(p,l):
> od;end proc:
> gf(p,l):
```

```

> points:= proc( p::nonnegint,l::nonnegint,F::polynom )
> local n1,n2,n3, L,c,v,f1, f2;
> c:=0;
> L:=NULL:
> for n1 from 0 to p^l-1 do
> for n2 from 0 to p^l-1 do
> for n3 from 0 to p^l-1 do
> if (Eval(F1(X,Y,Z),{X=g(p,l,n1),Y=g(p,l,n2),Z=g(p,l,n3)}) mod p=0
> and Eval(F2(X,Y,Z),{X=g(p,l,n1),Y=g(p,l,n2),Z=g(p,l,n3)}) mod p=0)
> then c:=c+1;
> L:= L,(' c'=c,[g(p,l,n1),g(p,l,n2),g(p,l,n3)]);fi; od; od;
> od;return(gf(p,l),' L'=L):end:
> points(p,l,F);

```

$\alpha, z^3 + z + 1, L = (c = 1, [0, 1, 0], c = 2, [0, 1, 1], c = 3, [0, 1, \alpha], c = 4, [0, 1, 1 + \alpha],$
 $c = 5, [0, 1, \alpha^2], c = 6, [0, 1, 1 + \alpha^2], c = 7, [0, 1, \alpha^2 + \alpha], c = 8, [0, 1, 1],$
 $c = 9, [1 + \alpha, \alpha, 0], c = 10, [1 + \alpha, \alpha, 1], c = 11, [1 + \alpha, \alpha, \alpha], c = 12,$
 $[1 + \alpha, \alpha, 1 + \alpha], c = 13, [1 + \alpha, \alpha, \alpha^2], c = 14, [1 + \alpha, \alpha, 1 + \alpha^2], c = 15,$
 $[1 + \alpha, \alpha, \alpha^2 + \alpha], c = 16, [1 + \alpha, \alpha, 1], c = 17, [1 + \alpha^2, \alpha^2, 0], c = 18,$
 $[1 + \alpha^2, \alpha^2, 1], c = 19, [1 + \alpha^2, \alpha^2, \alpha], c = 20, [1 + \alpha^2, \alpha^2, 1 + \alpha], c = 21,$
 $[1 + \alpha^2, \alpha^2, \alpha^2], c = 22, [1 + \alpha^2, \alpha^2, 1 + \alpha^2], c = 23, [1 + \alpha^2, \alpha^2, \alpha^2 + \alpha], c = 24,$
 $[1 + \alpha^2, \alpha^2, 1], c = 25, [1, \alpha^2 + \alpha, 0], c = 26, [1, \alpha^2 + \alpha, 1], c = 27,$
 $[1, \alpha^2 + \alpha, \alpha], c = 28, [1, \alpha^2 + \alpha, 1 + \alpha], c = 29, [1, \alpha^2 + \alpha, \alpha^2], c = 30,$
 $[1, \alpha^2 + \alpha, 1 + \alpha^2], c = 31, [1, \alpha^2 + \alpha, \alpha^2 + \alpha], c = 32, [1, \alpha^2 + \alpha, 1])$
 $1 := 1 + \alpha^2 + \alpha$



Equations de degré deux

On considère l'équation diophantienne suivante aux coefficients entiers :

$$f(x_1, x_2, \dots, x_n) = \sum_{i,j} a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c = 0. \quad (13.5)$$

Ici on commence par trouver l'ensemble de toutes les solutions en nombres rationnels. Ce problème est plus facile que ce de trouver les solutions en nombres entiers, mais il n'est pas trivial.

Un exemple classique est donné par la **paramétrisation rationnelle du cercle** $x^2 + y^2 = 1$:

$$x = \frac{2t}{1+t^2}, y = \frac{1-t^2}{1+t^2}, \quad (x = \cos \varphi, y = \sin \varphi, t = \tan\left(\frac{\varphi}{2}\right)), \quad (13.6)$$

$$(\text{à l'exception du point } (0, -1)). \quad (13.7)$$

Cette paramétrisation nous permet de décrire toutes les triples primitifs de Pythagore (X, Y, Z) , c'est à dire, les solutions en entiers naturels de l'équation $X^2 + Y^2 = Z^2$ avec $\text{pgcd}(X, Y, Z) = 1$. La réponse

est : $X = 2uv$, $Y = u^2 - v^2$, $Z = u^2 + v^2$, où $u > v > 0$ sont des entiers premiers entre eux. Pour le prouver, il suffit de poser $t = u/v$ dans (13.6).

De façon similaire, trouver les solutions rationnelles de (13.5) est équivalent à trouver les solutions rationnelles de l'équation homogène

$$\begin{aligned} F(X_0, X_1, \dots, X_n) &= \sum_{i,j=0}^n f_{ij} X_i X_j \\ &= \sum_{i,j=1}^n f_{ij} X_i X_j + 2 \sum_{i,j=1}^n f_{i0} X_i X_0 + f_{00} X_0^2 \end{aligned} \quad (13.8)$$

où $f_{ij} = f_{ji} = a_{ij}/2$ pour $1 \leq i < j \leq n$ et $f_{0i} = f_{i0} = b_i/2$ pour $i = 1, 2, \dots, n$, $f_{00} = c$. Les *coordonnées non-homogènes* x_1, \dots, x_n sont reliées aux *coordonnées homogènes* X_0, \dots, X_n par $X_i = x_i X_0$ ($i = 1, 2, \dots, n$). La forme quadratique $F(X)$ peut être écrit de façon commode sous la forme

$$F(X) = X^t A_F X, \quad X^t = (X_0, X_1, \dots, X_n),$$

où $A_F = (f_{ij})$ est la matrice des coefficients. S'il existe une solution rationnelle non-triviale de $F(X) = 0$, on dit que la forme F représente zéro sur \mathbb{Z} .

Cette équation définit une **conique** Q_F (c'est à dire, une hypersurface de $\mathbb{C}\mathbb{P}^n$ de degré deux). Ses points sont toutes les solutions (à l'exception de la solution triviale) considérées comme points de l'**espace projectif complexe** $\mathbb{C}\mathbb{P}^n$:

$$Q_F = \{(z_0 : z_1 : \dots : z_n) \in \mathbb{C}\mathbb{P}^n \mid F(z_0, z_1, \dots, z_n) = 0\}.$$

Toute solution non-triviale de $F(X) = 0$ donne un point sur cette conique. S'il on connaît une solution X^0 alors on peut trouver toutes les autres en considérant les intersections de Q_F avec les droites (projectifs) définies sur \mathbb{Q} et contenant X^0 . Algébriquement, une droite passant par X^0 et Y^0 est formée par tous les points de la forme $uX^0 + vY^0$. L'équation $F(uX^0 + vY^0) = 0$ se réduit alors à

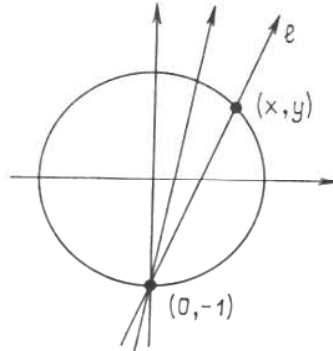
$$uv \sum_{i=1}^n \frac{\partial F}{\partial X_i} (X^0) Y_i^0 + v^2 F(Y^0) = 0.$$

En général, toutes les dérivées partielles $\frac{\partial F}{\partial X_i}$ ne s'annulent pas nécessairement. Dans ce cas, pour tout Y^0 on peut trouver un point d'intersection de Q_F avec notre droite :

$$v = -u \sum_{i=1}^n \frac{\partial F}{\partial X_i} (X^0) Y_i^0 / F(Y^0). \quad (13.9)$$

(Si, par hasard, $F(Y^0) = 0$ alors Y^0 se trouve déjà sur Q_F). De nouveau, ce point n'est pas unique en général. Les cas limites peut être bien compris en termes géométriques : si toutes les dérivées partielles s'annulent en X^0 alors notre conique est un cône de sommet X^0 , et le problème se réduit à ce de trouver tous les points rationnels sur la base d'un cône, cette base étant une conique de dimension inférieure ; s'il arrive qu'ils tous se trouvent entièrement sur Q_F alors tous ces points rationnels doivent être considérés etc.

Cette **méthode de la projection stéréographique**, appliquée à $x^2 + y^2 = 1$ et au point $(0,-1)$ donne exactement (13.6) s'il on note t la pente de la droite passant par $(0,-1)$ et (x,y) : $y + 1 = tx$.



Concernant l'équation

$$F(X_0, X_1, \dots, X_n) = 0 \quad (13.10)$$

(avec F comme dans (13.8)) sur les nombres rationnels, on peut commencer par la diagonalisation de A_F avec une substitution linéaire non-dégénérée $X = CY$ où $C \in M_{n+1}(\mathbb{Q})$. La matrice C peut être trouvée effectivement par le méthode classique de l'extraction successive des carrés.

Pour les équations homogènes comme (13.10) les problèmes de trouver toutes les solutions dans \mathbb{Q} et dans \mathbb{Z} sont essentiellement équivalents. Lorsque on peut trouver toutes les solutions à partir d'une seule, la question-clé est donc de décider, s'il existe une solution. La réponse est donnée par le résultat suivante.

13.6 Le principe de Minkowski–Hasse pour les formes quadratiques

DÉFINITION 13.6.1 Une solution $(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n$ d'une equation $F(x_1, x_2, \dots, x_n) = 0$ en nombres entiers est dit primitive modulo N , si $\text{pgcd}(N, x_1, x_2, \dots, x_n) = 1$.

THÉORÈME 13.6.2 Une forme quadratique $F(x_1, x_2, \dots, x_n)$ de rang n de coefficients entiers représente un zéro sur les nombres rationnels si et seulement si pour tout N , la congruence $F(x_1, \dots, x_n) \equiv 0 \pmod{N}$ admet une solution primitive, et de plus F représente un zéro sur les nombres réels, c'est à dire, elle est indéfinie.

Pour une preuve générale, voire [BS85]. Bien-sûr, la nécessité de cette condition est clair.

On donne ici une jolie démonstration de la suffisance de cette condition dans le cas $n = 3$ dûe à Legendre ([BS85]). Soit

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \quad (a_1a_2a_3 \neq 0).$$

Puisque F est indéfinie, on peut supposer que les deux premiers coefficients soient positifs, tandis que le troisième soit négatif. De plus, on peut les supposer sans facteurs carrés et premiers entre eux : on obtient ceci par des changements de variables et en divisant la forme par le pgcd de ses coefficients. On va noter une forme avec telles propriétés par

$$ax^2 + by^2 - cz^2. \quad (13.11)$$

Considérons un nombre premier p divisant c . Puisque $F \equiv 0 \pmod{p}$ admet une solution primitive, on peut trouver une solution non-primitive (x_0, y_0) de la congruence $ax^2 + by^2 \equiv 0 \pmod{p}$. Alors

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Dans le cas $p = 2$ on a bien sûr

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod{2}.$$

Donc pour tout $p|2abc$ on peut trouver des formes linéaires $L^{(p)}$, $M^{(p)}$ en x, y, z de coefficients entiers telles que $F \equiv L^{(p)}M^{(p)} \pmod{p}$. En utilisant le théorème chinois, on trouve L (resp. M) de coefficients entiers congrue à $L^{(p)}$ (resp. $M^{(p)}$) \pmod{p} pour tout $p|abc$. On obtient donc

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}. \quad (13.12)$$

Considérons maintenant les points entiers dans la boîte suivante :

$$0 \leq x < \sqrt{bc}, \quad 0 \leq y < \sqrt{ac}, \quad 0 \leq z < \sqrt{ab}. \quad (13.13)$$

Si l'on exclut le cas trivial $a = b = c = 1$, on constate que les racines carrées dans les inégalités (13.13) ne sont pas toutes de nombres entiers, donc le nombre total des points entiers sera strictement plus grand que le volume de cette boîte, i.e. abc . Ceci implique qu'il existe deux points différents pour lesquels L prends la même valeur mod abc . En considérant leurs différence, on trouve

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc} \quad (13.14)$$

pour un point $|x_0| \leq \sqrt{bc}$, $|y_0| \leq \sqrt{ac}$, $|z_0| \leq \sqrt{ab}$. Donc

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc} \quad (13.15)$$

et

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Il vient que soit

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \quad (13.16)$$

soit

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \quad (13.17)$$

Dans le premier cas le théorème est démontré. Dans le second cas on obtient explicitement la solution suivante :

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

L'énoncé originale de Legendre a été que $ax^2 + by^2 - cz^2 = 0$ est résoluble si et seulement si toutes les classes résiduelles $bc \pmod{a}$, $ac \pmod{b}$, $-ab \pmod{c}$ sont des carrés. EXEMPLE. $x^2 + y^2 - 3z^2$ ne représente pas de zéro sur \mathbb{Z} , mais $2x^2 + 3y^2 - 5z^2$ le représente, et $\left(\frac{-6}{5}\right) = \left(\frac{15}{2}\right) = \left(\frac{10}{3}\right) = 1$.

On peut démontrer qu'une forme quadratique indefinite de rang ≥ 5 représente toujours un zéro sur les rationnels, voire [BS85].

Cours N°14. Mercredi le 12 janvier 2005

13.7 Espace projectif \mathbb{P}^n , variétés algébriques

Soit K un corps et $n \geq 1$ un entier. On considère l'espace projectif de dimension n sur K et on note \mathbb{P}_K^n ou simplement \mathbb{P}^n l'ensemble des classes d'équivalence de $(n+1)$ -uplets

$$(x_0, \dots, x_n) \in K^{n+1} \setminus (0, \dots, 0),$$

sous la relation $(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n)$ pour tout $\lambda \in K^*$. Une classe d'équivalence x , notée $(x_0 : \dots : x_n)$ est dit un point de \mathbb{P}^n .

Soit $K[T] = K[T_0, \dots, T_n]$. On interprète les éléments de $K[T]$ comme des fonctions régulières de l'espace affine \mathbb{A}^{n+1} , et on interprète les éléments de

$$K \left(\frac{T_1}{T_0}, \frac{T_2}{T_0}, \dots, \frac{T_n}{T_0} \right),$$

comme des fonctions rationnelles de \mathbb{P}^n .

REMARQUE. Soit $x = (x_0 : \dots : x_n) \in \mathbb{P}^n$, et soit $F = F_0 + F_1 + \dots + F_m \in K[T_0, \dots, T_n]$ un polynôme avec des composantes homogènes F_i de degré i , alors

$$F(\lambda x_0, \dots, \lambda x_n) = F_0(x_0, \dots, x_n) + \lambda F_1(x_0, \dots, x_n) + \dots + \lambda^m F_m(x_0, \dots, x_n).$$

Il vient que pour un polynôme homogène F , la condition $F(x) = 0$ ne dépend que de la classe $x = (x_0 : \dots : x_n) \in \mathbb{P}^n$.

DÉFINITION 13.7.3 Une partie $X \subset \mathbb{P}^n$ est dit une variété algébrique projective irréductible si

$$X = V(P) = \{x \in \mathbb{P}^n \mid \forall F \in P, F(x) = 0\}$$

où P est un idéal premier homogène de $K[T_0, \dots, T_n]$, c'est à dire, un idéal premier engendré par des polynômes homogènes.

Il y a une grande différence entre les fonctions rationnelles des coordonnées affines et des coordonnées projectives : une fraction

$$f(T_0, \dots, T_n) = \frac{R(T_0, \dots, T_n)}{S(T_0, \dots, T_n)}$$

ne définit pas une fonction d'un point $x = (x_0 : \dots : x_n) \in \mathbb{P}^n$, même si $S(x_0, \dots, x_n) \neq 0$, car sa valeur dépend de choix des coordonnées homogènes de x .

Cependant, pour les polynômes homogènes R et S de même degré, tels que $S(x_0, \dots, x_n) \neq 0$, la valeur

$$f(x_0, \dots, x_n) = \frac{R(x_0, \dots, x_n)}{S(x_0, \dots, x_n)}$$

est bien définie.

DÉFINITION 13.7.4 Soit X une variété projective. L'idéal de X est l'ensemble

$$I(X) = \{F \in F[T_0, \dots, T_n] \mid F(x) = 0, \forall x \in X\}.$$

Pour définir le corps des fonctions d'une variété projective irréductible $K(X)$ on considère d'abord le sous-anneau suivant de $K(T_0, T_1, \dots, T_n)$.

$$\mathcal{O}_X = \left\{ f(T_0, \dots, T_n) = \frac{F(T_0, \dots, T_n)}{G(T_0, \dots, T_n)} \right. \\ \left. \mid F, G \in F[T_0, \dots, T_n] \text{ sont des polynômes homogènes de même degré, tels que } G \notin I(X) \right\}.$$

Alors l'idéal

$$M_X = \left\{ f(T_0, \dots, T_n) = \frac{F(T_0, \dots, T_n)}{G(T_0, \dots, T_n)} \mid F, G \in F[T_0, \dots, T_n], F \in I(X), G \notin I(X) \right\}$$

est un seul idéal maximal de l'anneau \mathcal{O}_X , et l'anneau quotient \mathcal{O}_X/M_X est un corps, dit le corps des fractions sur X .

DÉFINITION 13.7.5

(a) Soit U une partie d'une variété projective X . On dit que U est un voisinage ouvert contenant un point $x \in X$, s'il existe un polynôme homogène $G(T_0, \dots, T_n) \in K[T_0, \dots, T_n]$ tel que

$$U = X \cap \{x = (X_0, \dots, X_n) \in \mathbb{P}^n \mid G(X_0, \dots, X_n) \neq 0\}.$$

(b) Une application $f : U \rightarrow K$ est dite une fonction régulière au point x s'ils existe $F, G \in K[T_0, \dots, T_n]$ des polynômes homogènes de même degré tels que $G(x) \neq 0$ et $f = F/G$ dans un voisinage de x ; f est régulière sur U si elle est régulière en tout x de U .

EXEMPLE. On considère la variété projective $X \subset \mathbb{P}^2$ sur $K = \mathbb{C}$, donné par l'équation homogène irréductible $u^3 = v^3 - w^3$. Alors la fonction rationnelle

$$\frac{u}{v-w} = \frac{u(v^2 + vw + w^2)}{(v-w)(v^2 + vw + w^2)} = \frac{v^2 + vw + w^2}{u^2}$$

est régulière si $v \neq w$, même si $u = 0$, par exemple en $(0 : 1 : j)$ et en $(0 : 1 : j^2)$.

REMARQUE 13.7.6 Si K est algébriquement clos, et X une variété projective irréductible, alors on peut démontrer que toute fonction rationnelle est régulière partout sur X , doit être constante.

14 Courbes planes.

14.1 Courbes planes affines.

Une courbe algébrique plane sur un corps K est formée par les points

$$\mathcal{C} : \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

pour un polynôme non-constant $f(x, y)$ dans l'anneau factoriel $K[x, y]$, donc $f = f_1^{k_1} \cdots f_r^{k_r}$, où f_i sont **irréductibles** non-proportionnels. Ceci implique que

$$\mathcal{C} = \bigcup_{i=1}^r \mathcal{C}_i,$$

où $\mathcal{C}_i : f_i = 0$ est une courbe dite **irréductible**.

REMARQUE 14.1.1

(a) Si K est algébriquement clos, alors $\mathcal{C} = \mathcal{C}(K)$ est infinie

(en effet, il suffit d'écrire $f(x, y)$ sous la forme $a_m(y)x^m + \cdots + a_0$).

(b) Si K est algébriquement clos, alors un polynôme g de $K[x, y]$ s'annule sur toute la courbe irréductible $\mathcal{C}_i(K)$ si et seulement si $f_i \mid g$

(en effet, le théorème 13.2.1 (des zéros de Hilbert) implique que $f_i \mid g^r$ pour un $r \geq 1$, donc $f_i \mid g$ par la factoriabilité de l'anneau $K[x, y]$).

EXERCICE. Trouver le cardinal de l'ensemble fini $\mathbb{P}_{\mathbb{F}_q}^n$.

14.2 Courbes planes projectives.

Rappelons qu'un point P du plan projectif $\mathbb{P}^2 = \mathbb{P}_K^2$ est donnée comme la classe d'équivalence, notée $(X : Y : Z)$, d'un triplet non-nul $(X, Y, Z) \in K^3 \setminus \{(0, 0, 0)\}$, de telle façon que $(X, Y, Z) \sim (X', Y', Z') = (\lambda X, \lambda Y, \lambda Z)$ ($\lambda \in K^*$).

On a l'inclusion

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2, \quad (x, y) \mapsto (x, y, 1),$$

qui donne tous les points de \mathbb{P}^2 avec $Z \neq 0$.

On a les relations suivantes entre les coordonnées affines (x, y) et les coordonnées projectives $(X : Y : Z)$:

$$X = xZ, Y = yZ, \quad x = \frac{X}{Z}, y = \frac{Y}{Z}$$

Cartes affines

On a les trois parties suivantes de \mathbb{P}^2 :

$$\mathbb{A}_1^2, \mathbb{A}_2^2, \mathbb{A}_3^2 \subset \mathbb{P}^2, \text{ telles que } \mathbb{A}_1^2 : X \neq 0, \mathbb{A}_2^2 : Y \neq 0, \mathbb{A}_3^2 : Z \neq 0.$$

isomorphes à K^2 , et on a les coordonnées

$$\begin{aligned} \text{sur } \mathbb{A}_1^2 : X = xZ, Y = yZ, \quad x = \frac{X}{Z}, y = \frac{Y}{Z} \\ \text{sur } \mathbb{A}_2^2 : X = x'Y, Z = y'Y, \quad x' = \frac{X}{Y}, y' = \frac{Z}{Y} \\ \text{sur } \mathbb{A}_3^2 : Y = x''X, Z = y''X, \quad x'' = \frac{Y}{X}, y'' = \frac{Z}{X} \end{aligned}$$

EXERCICE. Réécrire l'équation de la courbe de Fermat $X^n + Y^n = Z^n$ en coordonnées (x', y') et en (x'', y'') .



14.3 Points singuliers.

Soit K un corps. Rappelons qu'une courbe projective plane \mathcal{C} sur K est définie par une équation de type $F(X : Y : Z) = 0$, où $F(X : Y : Z) \in K[X, Y, Z]$ est une forme homogène des variables projectives X, Y, Z .

L'équation de la tangente dans les coordonnées affines a la forme

$$f'_x(P)(x - \alpha) + f'_y(P)(y - \beta) = 0.$$

Par la construction,

$$f(x, y) = F(x, y, 1), \text{ où } F(X, Y, Z) = 0 \text{ l'équation homogène de la courbe.}$$

Ceci implique : $f'_x = F'_x, f'_y = F'_y$, et selon le théorème connu de Euler (sur les fonctions homogènes) on a

$$XF'_X + YF'_Y + ZF'_Z = nF \text{ où } n \text{ est le degré de } F$$

Lorsque $P = (\alpha : \beta : 1)$ se trouve sur la courbe alors

$$\alpha F'_X(P) + \beta F'_Y(P) + F'_Z(P) = nF,$$

donc l'équation de la tangente se transforme vers

$$x F'_X(P) + y F'_Y(P) + F'_Z(P) = 0 \iff XF'_X + YF'_Y + ZF'_Z = 0.$$

(c'est la forme projective de la droite tangente).

DÉFINITION 14.3.1

(a) Un **point singulier** sur une courbe projective plane \mathcal{C} sur K est toute solution du système

$$F = F'_X = F'_Y = F'_Z = 0$$

dans une extension de K .

(b) On dit qu'une courbe projective plane \mathcal{C} sur K est **lisse** si le système

$$F = F'_X = F'_Y = F'_Z = 0$$

n'a pas de solutions non-triviales dans toute extension de K .

EXEMPLE.

(a) Soit $Q(X, Y, Z)$ une forme quadratique de matrice A_Q , sur un corps K de caractéristique $\text{Car}(K) \neq 0$. Montrer que la conique $Q(X, Y, Z) = 0$ est non-singulière si et seulement si A_Q est inversible.

(b) Soit $\text{Car}(K) \neq 2, 3$, et soit \mathcal{C} donnée par l'équation homogène correspondante

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad O = (0 : 1 : 0).$$

On vérifie que cette courbe est **lisse** si et seulement si le polynôme cubique $x^3 + ax + b$ n'a pas de racines multiples (directement par la définition des points singuliers comme des solutions de l'équation $F = F'_X = F'_Y = F'_Z = 0$ dans le cas général $F(X, Y, Z) = Y^2 + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$).

(c) Soit $K = \mathbb{F}_2$, et soit \mathcal{C} une courbe sur K donnée par l'équation affine

$$y^2 + y = x^3 + ax + b, \quad a, b \in \mathbb{F}_2$$

Montrer que cette courbe est toujours lisse (on n'a plus besoin d'exclure ici le cas des racines multiples).

(d) Soit $K = \mathbb{F}_3$, et soit \mathcal{C} une courbe sur K donnée par l'équation affine :

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_3$$

Montrer que cette courbe est lisse si et seulement si le polynôme cubique à droite n'a pas de racines multiples.

14.4 Equations cubiques

Le problème de l'existence d'une solution.

Pour les *formes cubiques* $F(X, Y, Z)$ en trois variables de coefficients entiers, on ne connaît pas d'algorithme qui décide en générale si l'équation $F = 0$ possède une solution non-triviale en nombres entiers. Grandes classes de telles equations ont été étudiées de point de vue théorique et numérique ; par exemple Selmer E.S. en 1951–1954 a étudié en détail les équations de type

$$aX^3 + bY^3 + cZ^3 = 0.$$

Il arrive que même pour des équations simple comme $3X^3 + 4Y^3 + 5Z^3 = 0$ le principe de Minkowski–Hasse n'est pas valable : on peut montrer que cette équation n'a pas de solutions en nombres entiers, quoiqu'il existe des solutions réelles et des solution primitives modulo tout $N > 1$.

Addition de points sur une cubique plane

Toute forme cubique non-nulle $F(X, Y, Z)$ à coefficients entiers définit une courbe cubique \mathcal{C} dans l'espace projectif \mathbb{P}^2 (sur \mathbb{Q} et sur \mathbb{C}) :

$$\mathcal{C} = \{(X : Y : Z) \mid F(X, Y, Z) = 0\}. \quad (14.1)$$

Si \mathcal{C} est non-singulière et si $F = 0$ possède au moins une solution rationnelle, alors on peut trouver un changement de variables inversible à coefficients rationnelles qui réduit F à la **forme normale de Weierstrass**

$$Y^2Z - X^3 - aXZ^2 - bZ^3 \quad (a, b \in \mathbb{Q}). \quad (14.2)$$

On peut aussi supposer que la solution rationnelle de départ devient la solution évidente $(0 : 1 : 0)$ de l'équation ainsi obtenue (14.2). La condition de non-singularité de (14.2) est équivalente à la non-annulation du discriminant $4a^3 + 27b^2$. Une courbe cubique plane non-singulière est dite *elliptique*, s'elle possède un point rationnel. En utilisant les coordonnées affines $x = X/Z, y = Y/Z$ on réduit $F = 0$ à la forme suivante :

$$y^2 = x^3 + ax + b, \quad (14.3)$$

où le polynôme cubique dans la partie droite n'a pas de racines multiples. Sous cette forme affine, la solution rationnelle ci-dessus devient le point à l'infinie O . Il existe une jolie description géométrique de la loi de composition sur l'ensemble des points rationnels de \mathcal{C} qui devient un groupe abélien avec le point à l'infinie O comme l'élément neutre. Cette loi est donnée par la "**méthode de sécantes et tangentes**" de Poincaré. Notamment, pour une pair de points $P, Q \in \mathcal{C}(\mathbb{Q})$, on construit d'abord une droite passant par P, Q . Une telle droite intersecte aussi \mathcal{C} en un troisième point bien définie P' . Ensuite, on construit de nouveau une droite passant par P' et O . Enfin, son troisième point d' intersection avec \mathcal{C} est dit la **somme** $P + Q$. Si $P = Q$, la première droite à construire doit bien-sûr être tangente à \mathcal{C} en P .

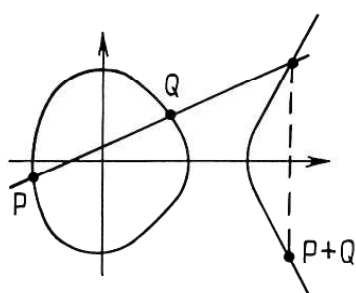


Fig. 6

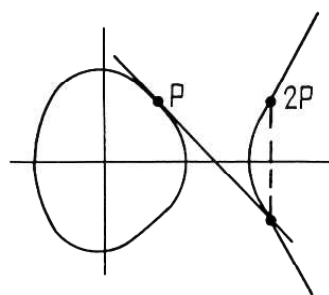


Fig. 7

Un calcul simple en coordonnées affines $P = (x_1, y_1), Q = (x_2, y_2)$ montre que $P + Q = (x_3, y_3)$ où

$$\begin{aligned} x_3 &= -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2} \right)^2, \\ y_3 &= \frac{y_1 - y_2}{x_1 - x_2} (x_1 - x_3) - y_1. \end{aligned} \quad (14.4)$$

Dans le cas limite $P = Q$ on remarque que $2y'_x y = 3x^2 + a$, et on obtient

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + a}{2y_1} \right)^2, \quad y_3 = \frac{3x_1^2 + a}{2y_1} (x_1 - x_3) - y_1. \quad (14.5)$$

Si $x_1 = x_2$ et $y_1 = -y_2$ alors $P + Q = O$, est le point à l'infinie, qui est l'élément neutre pour la loi de groupe.

Cette méthode nous permet de construire de nouveaux points rationnels à partir des points connus. Tels points forment un sous-groupe engendré par des points de départ, par exemple, $mP, m \in \mathbb{Z}$, à partir juste un seul point P .

Pour les **courbes cubiques singulières** cette construction ne marche pas. Par exemple, on considère la courbe

$$\mathcal{C} : y^2 = x^2 + x^3, \quad (14.6)$$

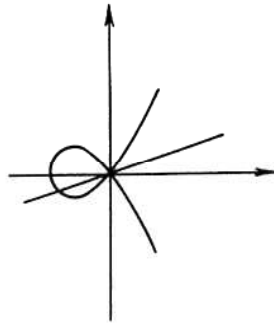


Fig. 8

qui est représentée par Fig. 8. Toute droite passant par $(0,0)$ n'a qu'un seul autre point d'intersection avec \mathcal{C} : sur $y = tx$ il est donné par l'équation $x^2(t^2 - x - 1) = 0$. A part de la solution triviale $x = 0$, on obtient $x = t^2 - 1$ et $y = t(t^2 - 1)$ donc nous avons trouvé tous les points sur \mathcal{C} à l'aide d'une paramétrisation rationnelle. Dans le cas non-singulier il n'existe pas de telle paramétrisation.

Une courbe admettant une paramétrisation rationnelle est dite une **courbe rationnelle**. Rappelons qu'un autre exemple d'une courbe rationnelle est donné par une **conique plane** et sa projection stéréographique.

La structure de groupe des points rationnels sur une cubique plane

Une propriété très remarquable de la "méthode de sécantes et tangentes" de Poincaré est que cette méthode nous permet de construire tous les points rationnels à partir d'un nombre fini des points rationnels. De point de vue de la théorie des groupes, cela signifie, que le résultat suivant a lieu :

THÉORÈME 14.4.1 (MORDELL, 1922) *Le groupe abélien $\mathcal{C}(\mathbb{Q})$ est de génération finie.*

On obtient alors du théorème de structure des groupes abéliens que

$$\mathcal{C}(\mathbb{Q}) \cong \Delta \times \mathbb{Z}^r$$

où Δ est le sous-groupe fini formé par les points de torsion, et \mathbb{Z}^r est le produit de r copies du groupe cyclique infini. Le nombre r est dit le **rang** de \mathcal{C} sur \mathbb{Q} . Il est connu que le groupe de torsion Δ peut être déterminée explicitement. Par exemple, Nagell et Lutz (Lutz E. (1937)) ont démontré que les points de torsion d'une courbe $y^2 = x^3 + ax + b$ avec a et b des nombres entiers, ont les coordonnées entiers x, y . De plus, l'ordonnée y d'un point de torsion soit nulle soit divise le nombre entier $D = -4a^3 - 27b^2$.

B.Mazur a démontré en 1976 que le sous-groupe de torsion Δ sur \mathbb{Q} est isomorphe à l'un des quinze groupes suivants :

$$\mathbb{Z}/m\mathbb{Z} \ (m \leq 10, m = 12), \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \ (n \leq 4), \quad (14.7)$$

et toutes ces possibilités se réalisent.

Une question ouverte importante est si r peut être infiniment grand. En 1982 J.-L. Mestre a construit des exemples de courbes de rang au moins 14. Il a donné aussi un exemple relativement simple d'une courbe de rang ≥ 9 : $y^2 + 9767y = x^3 + 3576x^2 + 425x - 2412$.

En 2000 Martin – Mcmillen ont trouvé une courbe elliptique de rang ≥ 24 :

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116$$

(voir <http://www.math.hr/~duje/tors/rankhist.html> pour d'autres exemples).

Exemples.

1. Soit \mathcal{C} donnée par l'équation

$$y^2 + y = x^3 - x.$$

dont les solutions en nombre entiers donnent la liste des cas où le produit de deux entiers consécutifs est égale au produit de trois entiers consécutifs. Alors le groupe Δ est trivial et $\mathcal{C}(\mathbb{Q})$ est cyclique de générateur $P = (0, 0)$.

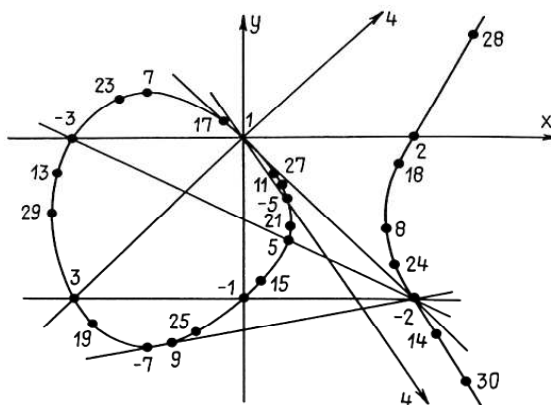


Fig. 9

2. Les points mP (numérotés par m) sont montrés dans le Fig. 9.
3. Soit \mathcal{C} donnée par l'équation

$$y^2 + y = x^3 - 7x + 6.$$

Alors $\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}^3$, et les points $(1,0)$, $(6,0)$, $(0,2)$ forment une base de ce groupe.

4. Considérons la courbe $y^2 = x^3 + px$, $p = 877$. Un générateur modulo torsion du groupe des points rationnels de cette courbe a l'abscisse x

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}.$$

Cet exemple montre que les méthodes naïves de recherche des ponts rationnels deviennent rapidement inefficace.

Congruences cubiques modulo un nombre premier p

Soit p un nombre premier et soit $F(X_0, X_1, X_2)$ une forme cubique à coefficients entiers. La réduction de F modulo p , donne une forme cubique sur le corps fini \mathbb{F}_p . Cette réduction est dit non-singulère s'elle n'a pas de zéros communs avec ces dérivées partielles dans toute extension de \mathbb{F}_p . On peut montrer que la plupart des résultats de la géométrie algébrique complexe restent valable sur les corps de caractéristique positive. Cependant, les formes normales d'une courbe elliptique sont légèrement plus compliquées. En utilisant un changement de variables inversible des coordonnées projectives, on peut toujours réduire l'équation $F = 0$ en coordonnées affines pour $p \neq 2, 3$ à la forme à l'un des types suivantes(Koblitz N. (1987)) :

$$y^2 = x^3 + ax + b \quad (4a^3 + 27b^2 \neq 0), \quad a, b \in \mathbb{F}_p. \quad (14.8)$$

(on interdit le cas des racines multiples).

La courbe projective ainsi défini possède toujours le point $O = (0 : 1 : 0)$, rationnel sur \mathbb{F}_p (rappelons que l'ensemble $\mathcal{C}(\mathbb{F}_p)$ des points rationnels sur \mathbb{F}_p d'une courbe projective $\mathcal{C} : F(X, Y, Z) = 0$ est le sous-ensemble de $\mathbb{P}_{\mathbb{F}_p}^2$ des points

$$\left\{ (X : Y : Z) \in \mathbb{P}_{\mathbb{F}_p}^2 \mid F(X, Y, Z) = 0 \right\}$$

Combien de points sur \mathbb{F}_p , c'est à dire, combien de solutions projectives de la congruence $F \equiv 0 \pmod{p}$, peut-on avoir ? Bien évidemment, le nombre total est au plus $2p + 1$ (on compt O), puisque sous la forme affine tout point fini x donne au plus deux valeurs de y . D'un autre coté, seulement une moitié des classes résiduelles sont les carrés (pour p impaire). Donc on peut espérer que $x^3 + ax + b$ est un carré pour environ une moitié des x .

Plus précisément, soit $\chi(x) = \left(\frac{x}{p}\right)$ le symbole de Legendre (8.1). Alors on a par la définition, que le nombre de solutions de $y^2 = u$ dans \mathbb{F}_p est $1 + \chi(u)$. Ceci implique,

$$\begin{aligned} \text{Card } \mathcal{C}(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + ax + b)) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right). \end{aligned}$$

N. Koblitz (1987) compare la dernière somme avec un résultat sur les marches aléatoires sur une droite. Après p marches on peut espérer d'être à distance environ \sqrt{p} de zéro. En fait, on peut démontrer le théorème suivant remarquable :



THÉORÈME 14.4.2 (H.HASSE (1937)) Soit $N_p = \text{Card } \mathcal{C}(\mathbb{F}_p)$. Alors

$$|N_p - (p + 1)| \leq 2\sqrt{p}.$$

Un preuve élémentaire a été donné par Yu.I.Manin (1956).

REMARQUE. Les courbes elliptiques sur les corps finis trouvent beaucoup d'applications. En particulier, les cas où un tel groupe est cyclique de grand taille amènent au cryptosystèmes ECDLP ("Elliptic curve discrete logarithm problem"), voir [Kob87].

EXERCICES

14.1 On considère la courbe affine sur \mathbb{Q} donnée par l'équation

$$\mathcal{C} : 2x^2 + 3y^2 = 5.$$

- (a) Montrer qu'il existe un point rationnel $(x_0, y_0) \in \mathcal{C}(\mathbb{Q})$.
(b) Soit $t \in \mathbb{Q}$. Trouver tous les points d'intersection de la droite

$$y - y_0 = t(x - x_0)$$

avec la courbe $\mathcal{C}(\mathbb{Q})$.

- (c) En déduire une paramétrisation rationnelle de la courbe \mathcal{C} .
(d) Trouver tous les points rationnels de la courbe projective, donnée par l'équation homogène $2X^2 + 3Y^2 - 5Z^2 = 0$.

14.2 On considère la courbe affine sur \mathbb{F}_{49} , donnée par l'équation

$$\mathcal{C} : 2x^2 + 3y^2 = 5.$$

- (a) Montrer qu'il existe un point rationnel $(x_0, y_0) \in \mathcal{C}(\mathbb{F}_{49})$.
(b) Soit $t \in \mathbb{F}_{49}$. Trouver tous les points d'intersection de la droite

$$y - y_0 = t(x - x_0)$$

avec la courbe $\mathcal{C}(\mathbb{F}_{49})$.

- (c) En déduire une paramétrisation rationnelle sur \mathbb{F}_{49} de la courbe \mathcal{C} .
(d) Trouver tous les points rationnels sur \mathbb{F}_{49} de la courbe projective donnée par l'équation homogène $2X^2 + 3Y^2 - 5Z^2 = 0$.

14.3 On considère la courbe cubique plane $\mathcal{E} \subset \mathbb{P}^2$ sur \mathbb{Q} , donnée sous la forme affine suivante $y^2 = x(x+9)(x-16)$.

- (a) Trouver l'équation de \mathcal{E} en coordonnées projectives.
(b) Montrer que la courbe \mathcal{E} est lisse.
(c) Montrer que l'ensemble

$$G = \{(\infty, \infty), (0, 0), (0, -9), (0, 16), (-4, 20), (-4, -20), (36, 180), (36, -180)\} \subset \mathbb{P}^2$$

est un sous-groupe de $\mathcal{E}(\mathbb{Q})$.

- (d) Le groupe G est-il cyclique ?

14.4 On considère une courbe cubique plane $\mathcal{F} \subset \mathbb{P}^2$ sur \mathbb{F}_4 , donnée sous la forme affine suivante $y^2 + y = x^3 + x + 1$.

- (a) Montrer que la courbe \mathcal{F} est lisse.
(b) Trouver l'ordre du groupe $H = \mathcal{F}(\mathbb{F}_4)$.
(c) Le groupe H est-il cyclique ?
-
-

14.5 Points des courbes algébriques sur les corps finis (exemples)

COURBE de FERMAT sur GF(4)

$$x^3 + y^3 + z^3 = 0$$

> restart ;

> with(linalg) :

Warning, the protected names norm and trace have been redefined and unprotected

> g:=x^2+x+1 mod 2;

$$g := x^2 + x + 1$$

> alias(alpha = RootOf(g)) ;

$$\alpha$$

> f:=(x,y,z)->x^3+y^3+z^3;

$$f := (x, y, z) \rightarrow x^3 + y^3 + z^3$$

> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,2,h);

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} \\ x_{1,0} & x_{1,1} \\ x_{2,0} & x_{2,1} \end{bmatrix}$$

> u:=(i,j)-> alpha^(i-1):U:=Matrix(2,1,u);

$$U := \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$$

> with(LinearAlgebra):

> Y:= Multiply(X, U);

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1} \alpha \\ x_{1,0} + x_{1,1} \alpha \\ x_{2,0} + x_{2,1} \alpha \end{bmatrix}$$

> v[1]:=f(0, 1, x[2]);

$$v_1 := 1 + x_2^3$$

> v[2]:=f(1, x[1], x[2]);

$$v_2 := 1 + x_1^3 + x_2^3$$

> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;

$$vv_1 := 1 + (x_{2,0} + x_{2,1} \alpha)^3$$

> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;

$$vv_2 := 1 + (x_{1,0} + x_{1,1} \alpha)^3 + (x_{2,0} + x_{2,1} \alpha)^3$$

```

> c:=0;
> if f(0,0,1) mod 2 =0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j}) mod 2 =0 then c:=c+1;
> print (c,[0, 1, i+j*alpha]) fi ;od ;od;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2, x[1,0]=i1,x[1,1]=j1}) mod 2
> =0 then c:=c+1;
> print (c,[1, (i1+j1*alpha)mod 2,
> (i2+j2*alpha)mod 2]) fi od; od ;od ;od;

```

```

c := 0
1, [0, 1, alpha]
2, [0, 1, 1]
3, [0, 1, 1 + alpha]
4, [1, alpha, 0]
5, [1, 1, 0]
6, [1, 1 + alpha, 0]
7, [1, 0, alpha]
8, [1, 0, 1]
9, [1, 0, 1 + alpha]

```

COURBE de FERMAT sur GF(16)

$$x^3 + y^3 + z^3 = 0$$

```

> restart ;
> with(linalg) :

```

Warning, the protected names norm and trace have been redefined and unprotected

```

> g:=x^4+x+1 mod 2;

```

$$g := x^4 + x + 1$$

```

> alias(alpha = RootOf(g)) ;

```

α

```

> f:=(x,y,z)->x^3+y^3+z^3;

```

$$f := (x, y, z) \rightarrow x^3 + y^3 + z^3$$

```

> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,4,h);

```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \end{bmatrix}$$

```

> u:=(i,j)-> alpha^(i-1):U:=Matrix(4,1,u);

```

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{bmatrix}$$

```
> with(LinearAlgebra):
> Y:= Multiply(X, U);
```

Warning, the assigned name GramSchmidt now has a global binding

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1} \alpha + x_{0,2} \alpha^2 + x_{0,3} \alpha^3 \\ x_{1,0} + x_{1,1} \alpha + x_{1,2} \alpha^2 + x_{1,3} \alpha^3 \\ x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2 + x_{2,3} \alpha^3 \end{bmatrix}$$

```
> v[1]:=f(0, 1, x[2]);
```

$$v_1 := 1 + x_2^3$$

```
> v[2]:=f(1, x[1], x[2]);
```

$$v_2 := 1 + x_1^3 + x_2^3$$

```
> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;
```

$$vv_1 := 1 + (x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2 + x_{2,3} \alpha^3)^3$$

```
> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;
```

$$vv_2 := 1 + (x_{1,0} + x_{1,1} \alpha + x_{1,2} \alpha^2 + x_{1,3} \alpha^3)^3 + (x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2 + x_{2,3} \alpha^3)^3$$

```
> c:=0;
```

```
> if f(0,0,1) mod 2 =0 then c:=c+1;
```

```
> print (c, [0, 0, 1]) fi;
```

```
> for i from 0 to 1 do
```

```
> for j from 0 to 1 do
```

```
> for k from 0 to 1 do
```

```
> for l from 0 to 1 do
```

```
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k,x[2,3]=1}) mod 2 =0
```

```
> then c:=c+1;
```

```
> print (c,[0, 1,
```

```
> i+j*alpha+k*alpha^2+l*alpha^3]) fi; od; od ;od ;od;
```

```
> for i2 from 0 to 1 do
```

```
> for j2 from 0 to 1 do
```

```
> for k2 from 0 to 1 do
```

```
> for l2 from 0 to 1 do
```

```
> for i1 from 0 to 1 do
```

```
> for j1 from 0 to 1 do
```

```
> for k1 from 0 to 1 do
```

```
> for l1 from 0 to 1 do
```

```
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,x[2,3]=l2,
```

```
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1,x[1,3]=l1}) mod 2 =0 then c:=c+1;
```

```
> print (c,[1,
```

```
> i1+j1*alpha+k1*alpha^2+l1*alpha^3, i2+j2*alpha+k2*alpha^2+l2*alpha^3])
```

```
> fi; od; od ;od ;od;od;od; od;
```

$$c := 0$$

$$1, [0, 1, \alpha + \alpha^2]$$

$$2, [0, 1, 1]$$

- 3, $[0, 1, 1 + \alpha + \alpha^2]$
- 4, $[1, \alpha + \alpha^2, 0]$
- 5, $[1, 1, 0]$
- 6, $[1, \alpha + \alpha^2 + 1, 0]$
- 7, $[1, 0, \alpha^2 + \alpha]$
- 8, $[1, 0, 1]$
- 9, $[1, 0, \alpha + 1 + \alpha^2]$

COURBE de KLEIN sur GF(16)

$$x^3y + y^3z + z^3x = 0$$

> `fk:=(x,y,z)->x^3*y+y^3*z+z^3*x;`

$$fk := (x, y, z) \rightarrow x^3y + y^3z + z^3x$$

> `vk[1]:=fk(0, 1, x[2]);`

$$vk_1 := x_2$$

> `vk[2]:=fk(1, x[1], x[2]);`

$$vk_2 := x_1 + x_1^3 x_2 + x_2^3$$

> `vvk[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1],x[2]=Y[3,1],vk[1]);`

$$vvk_1 := x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2 + x_{2,3}\alpha^3$$

> `vvk[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1],x[2]=Y[3,1],vk[2]);`

$$\begin{aligned} vvk_2 := & x_{1,0} + x_{1,1}\alpha + x_{1,2}\alpha^2 + x_{1,3}\alpha^3 \\ & + (x_{1,0} + x_{1,1}\alpha + x_{1,2}\alpha^2 + x_{1,3}\alpha^3)^3 (x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2 + x_{2,3}\alpha^3) \\ & + (x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2 + x_{2,3}\alpha^3)^3 \end{aligned}$$

```

> c:=0;
> if fk(0,0,1) mod 2 =0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> for l from 0 to 1 do
> if Eval(vvk[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k,x[2,3]=l}) mod 2 =0
> then c:=c+1;
> print (c,[0, 1,
> i+j*alpha+k*alpha^2+l*alpha^3]) fi; od; od ;od ;od ;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for k2 from 0 to 1 do
> for l2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> for l1 from 0 to 1 do
> if Eval(vvk[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,x[2,3]=l2,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1,x[1,3]=l1}) mod 2 =0 then c:=c+1;
> print (c,[1,
> i1+j1*alpha+k1*alpha^2+l1*alpha^3, i2+j2*alpha+k2*alpha^2+l2*alpha^3])
> fi; od; od ;od ;od ;od;od;od; od;

```

```

c := 0
c := 1
1, [0, 0, 1]
2, [0, 1, 0]
3, [1, 0, 0]
4, [1, 1 +  $\alpha^2$ ,  $\alpha^3$ ]
5, [1,  $\alpha$ ,  $\alpha^3 + \alpha^2$ ]
6, [1,  $\alpha + 1$ ,  $\alpha + \alpha^3$ ]
7, [1,  $\alpha^3$ ,  $\alpha + \alpha^2$ ]
8, [1,  $1 + \alpha^2 + \alpha$ ,  $\alpha + \alpha^2$ ]
9, [1,  $1 + \alpha + \alpha^2 + \alpha^3$ ,  $\alpha + \alpha^2$ ]
10, [1,  $\alpha + \alpha^2$ ,  $\alpha^3 + \alpha + \alpha^2$ ]
11, [1,  $\alpha^2 + \alpha$ ,  $\alpha^3 + 1$ ]
12, [1,  $1 + \alpha + \alpha^2$ ,  $\alpha^3 + 1 + \alpha^2$ ]
13, [1,  $\alpha + \alpha^2 + 1$ ,  $1 + \alpha^3 + \alpha$ ]
14, [1,  $\alpha^3 + \alpha^2$ ,  $\alpha + \alpha^2 + 1$ ]
15, [1,  $\alpha + \alpha^3$ ,  $\alpha + \alpha^2 + 1$ ]
16, [1,  $\alpha + \alpha^2$ ,  $\alpha + \alpha^2 + 1$ ]
17, [1,  $\alpha^2$ ,  $1 + \alpha + \alpha^2 + \alpha^3$ ]

```


COURBE de KLEIN sur GF(8)

$$x^3y + y^3z + z^3x = 0$$

> restart ;

> with(linalg) :

Warning, the protected names norm and trace have been redefined and unprotected

> g:=x^3+x+1 mod 2;

$$g := x^3 + x + 1$$

> alias(alpha = RootOf(g)) ;

α

> fk:=(x,y,z)->x^3*y+y^3*z+z^3*x;

$$fk := (x, y, z) \rightarrow x^3y + y^3z + z^3x$$

> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,3,h);

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} \\ x_{1,0} & x_{1,1} & x_{1,2} \\ x_{2,0} & x_{2,1} & x_{2,2} \end{bmatrix}$$

> u:=(i,j)-> alpha^(i-1):U:=Matrix(3,1,u);

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}$$

> with(LinearAlgebra):

> Y:= Multiply(X, U);

Warning, the assigned name GramSchmidt now has a global binding

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1}\alpha + x_{0,2}\alpha^2 \\ x_{1,0} + x_{1,1}\alpha + x_{1,2}\alpha^2 \\ x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2 \end{bmatrix}$$

> vk[1]:=fk(0, 1, x[2]);

$$vk_1 := x_2$$

> vk[2]:=fk(1, x[1], x[2]);

$$vk_2 := x_1 + x_1^3x_2 + x_2^3$$

> vvk[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[1]) ;

$$vvk_1 := x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2$$

> vvk[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],vk[2]) ;

$$vvk_2 := x_{1,0} + x_{1,1}\alpha + x_{1,2}\alpha^2 + (x_{1,0} + x_{1,1}\alpha + x_{1,2}\alpha^2)^3(x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2) + (x_{2,0} + x_{2,1}\alpha + x_{2,2}\alpha^2)^3$$

```

> c:=0;
> if fk(0,0,1) mod 2 = 0 then c:=c+1;
> print (c, [0, 0, 1]) fi;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> if Eval(vvk[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k}) mod 2 =0 then
> c:=c+1;
> print (c, [0, 1, i+j*alpha+k*alpha^2])
> fi; od; od ;od ;
> for i2 from 0 to 1 do
> for j2 from 0 to 1 do
> for k2 from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> if Eval(vvk[2],{x[2,0]=i2,x[2,1]=j2,x[2,2]=k2,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1}) mod 2 =0 then c:=c+1;
> print (c, [1, i1+j1*alpha+k1*alpha^2,
> i2+j2*alpha+k2*alpha^2]) fi; od; od ;od ;od;od;od;

```

```

c := 0
c := 1
1, [0, 0, 1]
2, [0, 1, 0]
3, [1, 0, 0]
4, [1,  $\alpha$ ,  $\alpha^2$ ]
5, [1, 1,  $\alpha^2$ ]
6, [1,  $1 + \alpha$ ,  $\alpha^2$ ]
7, [1,  $\alpha^2 + \alpha$ ,  $\alpha$ ]
8, [1, 1,  $\alpha$ ]
9, [1,  $1 + \alpha + \alpha^2$ ,  $\alpha$ ]
10, [1,  $\alpha^2$ ,  $\alpha^2 + \alpha$ ]
11, [1, 1,  $\alpha^2 + \alpha$ ]
12, [1,  $1 + \alpha^2$ ,  $\alpha^2 + \alpha$ ]
13, [1,  $\alpha^2$ , 1]
14, [1,  $\alpha$ , 1]
15, [1,  $\alpha^2 + \alpha$ , 1]
16, [1,  $\alpha$ ,  $1 + \alpha^2$ ]
17, [1,  $1 + \alpha^2$ ,  $1 + \alpha^2$ ]
18, [1,  $1 + \alpha + \alpha^2$ ,  $1 + \alpha^2$ ]
19, [1,  $\alpha^2 + \alpha$ ,  $1 + \alpha$ ]
20, [1,  $1 + \alpha^2$ ,  $1 + \alpha$ ]
21, [1,  $1 + \alpha$ ,  $1 + \alpha$ ]

```

$$22, [1, \alpha^2, 1 + \alpha + \alpha^2]$$

$$23, [1, 1 + \alpha, 1 + \alpha + \alpha^2]$$

$$24, [1, 1 + \alpha + \alpha^2, 1 + \alpha + \alpha^2]$$

COURBE de FERMAT sur GF(8)

> restart ;

> with(linalg) :

Warning, the protected names norm and trace have been redefined and unprotected

> g:=x^3+x+1 mod 2;

$$g := x^3 + x + 1$$

> alias(alpha = RootOf(g)) ;

α

> f:=(x,y,z)->x^3+y^3+z^3;

$$f := (x, y, z) \rightarrow x^3 + y^3 + z^3$$

> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,3,h);

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} & x_{0,2} \\ x_{1,0} & x_{1,1} & x_{1,2} \\ x_{2,0} & x_{2,1} & x_{2,2} \end{bmatrix}$$

> u:=(i,j)-> alpha^(i-1):U:=Matrix(3,1,u);

$$U := \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}$$

> with(LinearAlgebra):

> Y:= Multiply(X, U);

Warning, the assigned name GramSchmidt now has a global binding

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1} \alpha + x_{0,2} \alpha^2 \\ x_{1,0} + x_{1,1} \alpha + x_{1,2} \alpha^2 \\ x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2 \end{bmatrix}$$

> v[1]:=f(0, 1, x[2]);

$$v_1 := 1 + x_2^3$$

> v[2]:=f(1, x[1], x[2]);

$$v_2 := 1 + x_1^3 + x_2^3$$

> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;

$$vv_1 := 1 + (x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2)^3$$

> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;

$$vv_2 := 1 + (x_{1,0} + x_{1,1} \alpha + x_{1,2} \alpha^2)^3 + (x_{2,0} + x_{2,1} \alpha + x_{2,2} \alpha^2)^3$$

```

> c:=0;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j,x[2,2]=k}) mod 2 =0 then
> c:=c+1;
> print (c,[0, 1, i+j*alpha+k*alpha^2])
> fi; od; od ;od ;
> for i from 0 to 1 do
> for j from 0 to 1 do
> for k from 0 to 1 do
> for i1 from 0 to 1 do
> for j1 from 0 to 1 do
> for k1 from 0 to 1 do
> if Eval(vv[2],{x[2,0]=i,x[2,1]=j,x[2,2]=k,
> x[1,0]=i1,x[1,1]=j1,x[1,2]=k1}) mod 2 =0 then c:=c+1;
> print (c,[1, (i+j1*alpha+k1*alpha^2)
> mod 2 ,(i+j*alpha+k*alpha^2) mod 2]) fi; od; od ;od ;od;od;od;

```

```

c := 0
1, [0, 1, 1]
2, [1, 1, 0]
3, [1, 1 + alpha, alpha^2]
4, [1, alpha^2 + alpha + 1, alpha]
5, [1, alpha^2 + 1, alpha + alpha^2]
6, [1, 0, 1]
7, [1, alpha + alpha^2, 1 + alpha^2]
8, [1, alpha^2, alpha + 1]
9, [1, alpha, 1 + alpha + alpha^2]

```

COURBE de FERMAT sur GF(9)

$$x^4 + y^4 + z^4 = 0$$

```

> restart ;
> with(linalg) :
> g:=x^2+1 mod 3;

```

Warning, the protected names norm and trace have been redefined and unprotected

```

g := x^2 + 1
> alias(alpha = RootOf(g)) ;
alpha
> f:=(x,y,z)->x^4+y^4+z^4;
f := (x, y, z) -> x^4 + y^4 + z^4

```

```

> h:=(i,j)->x[i-1,j-1]: X:=Matrix(3,2,h);

```

$$X := \begin{bmatrix} x_{0,0} & x_{0,1} \\ x_{1,0} & x_{1,1} \\ x_{2,0} & x_{2,1} \end{bmatrix}$$

```

> u:=(i,j)-> alpha^(i-1):U:=Matrix(2,1,u);

```

$$U := \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$$

```

> with(LinearAlgebra):
> Y:= Multiply(X, U);

```

Warning, the assigned name GramSchmidt now has a global binding

$$Y := \begin{bmatrix} x_{0,0} + x_{0,1} \alpha \\ x_{1,0} + x_{1,1} \alpha \\ x_{2,0} + x_{2,1} \alpha \end{bmatrix}$$

```

> v[1]:=f(0, 1, x[2]);

```

$$v_1 := 1 + x_2^4$$

```

> v[2]:=f(1, x[1], x[2]);

```

$$v_2 := 1 + x_1^4 + x_2^4$$

```

> vv[1]:=subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[1]) ;

```

$$vv_1 := 1 + (x_{2,0} + x_{2,1} \alpha)^4$$

```

> vv[2]:= subs(x[0]=Y[1,1],x[1]=Y[2,1], x[2]=Y[3,1],v[2]) ;

```

$$vv_2 := 1 + (x_{1,0} + x_{1,1} \alpha)^4 + (x_{2,0} + x_{2,1} \alpha)^4$$

```

> c:=0;
> for i from 0 to 2 do
> for j from 0 to 2 do
> if Eval(vv[1],{x[2,0]=i,x[2,1]=j}) mod 3 =0 then c:=c+1;
> print (c,[0, 1, i+j*alpha]) fi; od; od
> ;for i2 from 0 to 2 do
> for j2 from 0 to 2 do
> for i1 from 0 to 2 do
> for j1 from 0 to 2 do
> if Eval(vv[2],{x[2,0]=i2,x[2,1]=j2,x[1,0]=i1,x[1,1]=j1})
> mod 3 =0 then c:=c+1;
> print (c,[1, (i1+j1*alpha)mod 3
> ,(i2+j2*alpha) mod 3]) fi; od; od ;od ;od;

```

$$c := 0$$

- 1, [0, 1, 1 + α]
- 2, [0, 1, 1 + 2 α]
- 3, [0, 1, 2 + α]
- 4, [0, 1, 2 + 2 α]
- 5, [1, 1 + α , 0]
- 6, [1, 1 + 2 α , 0]
- 7, [1, 2 + α , 0]
- 8, [1, 2 + 2 α , 0]

- 9, $[1, \alpha, \alpha]$
- 10, $[1, 2\alpha, \alpha]$
- 11, $[1, 1, \alpha]$
- 12, $[1, 2, \alpha]$
- 13, $[1, \alpha, 2\alpha]$
- 14, $[1, 2\alpha, 2\alpha]$
- 15, $[1, 1, 2\alpha]$
- 16, $[1, 2, 2\alpha]$
- 17, $[1, \alpha, 1]$
- 18, $[1, 2\alpha, 1]$
- 19, $[1, 1, 1]$
- 20, $[1, 2, 1]$
- 21, $[1, 0, 1 + \alpha]$
- 22, $[1, 0, 1 + 2\alpha]$
- 23, $[1, \alpha, 2]$
- 24, $[1, 2\alpha, 2]$
- 25, $[1, 1, 2]$
- 26, $[1, 2, 2]$
- 27, $[1, 0, 2 + \alpha]$
- 28, $[1, 0, 2 + 2\alpha]$

Quatrième partie

Compléments et annexes

A Annexe : Postulat de Bertrand (C.Moser)

Un des problèmes de l'arithmétique est celui de la "répartition" des nombres premiers, en quelque sorte de leur essaimage parmi les nombres entiers. On étudie ci-dessous quelques propriétés de cette répartition.

PROPOSITION A.0.1 *Pour tout entier $n \geq 2$ il existe une séquence de longueur n d'entiers consécutifs dont aucun terme n'est premier.*

On considère la séquence $f : 1, \dots, n \mapsto \mathbb{N}$ définie par $f(k) = (n+2)! + k + 1$. Pour tout $k \in 1, \dots, n$ le nombre $f(k)$ est divisible par $k+1$ avec un quotient supérieur à $(n+1)!$.

THÉORÈME A.0.2 *Pour tout entier $n \geq 753$ on a*

$$\frac{3}{5} \cdot \frac{n}{\log(n)} < \frac{13 \log(4)}{30} \cdot \frac{n}{\log(n)} < \pi(2n) - \pi(n) < \log(4) \cdot \frac{n}{\log(n)} \frac{7}{5} \cdot \frac{n}{\log(n)}.$$

En particulier pour tout $n \geq 2$ il existe un nombre premier entre n et $2n$. La dernière assertion est connue comme étant le postulat de Bertrand.

La démonstration s'appuie sur une suite de lemmes donnant les propriétés de divisibilité des coefficients du binôme $\binom{2n}{n}$.

LEMME A.0.3 *Pour tout entier $n \geq 2$ on a l'encadrement $\frac{4^n}{2\sqrt{n}} < \binom{2n}{n} < 4^n$.*

La propriété est évidemment vraie pour $n = 2$. La seconde inégalité résulte directement de la formule du binôme car on a raisonnant par récurrence sur n , on obtient les inégalités :

$$\binom{2n+2}{n+1} > \frac{(2n+2)(2n+1)}{(n+1)^2} \frac{4^n}{2\sqrt{n}} = \frac{4^{n+1}}{2\sqrt{n+1}} \cdot \frac{(n+1/2)}{\sqrt{n(n+1)}} > \frac{4^{n+1}}{2\sqrt{n+1}}.$$

qui permettent de conclure.

LEMME A.0.4 *Pour tout entier $n \geq 2$ et pour tout nombre premier p , l'exposant de p dans la décomposition primaire de $n!$ est la somme finie $\sum_{a=1}^{\infty} \left\lfloor \frac{n}{p^a} \right\rfloor$.*

Parmi les facteurs naturels de $n!$, le nombre de ceux qui sont divisibles par p est le quotient de n par p , ce qui fournit un exposant 1 pour chacun d'eux. Le nombre de ceux qui sont divisibles par p^2 est le quotient de n par p^2 , ce qui fournit un exposant 1 supplémentaire pour chacun d'eux, et ainsi de suite jusqu'au plus grand exposant a tel que $p^a = n$.

LEMME A.0.5 *Pour tout $n \geq 2$, soit p un nombre premier divisant $\binom{2n}{n}$ et strictement supérieur à $\sqrt{2n}$. Alors p divise exactement $\binom{2n}{n}$.*

On applique le lemme précédent en remarquant que l'exposant de p dans $\binom{2n}{n}$ est la somme

$$\sum_{a=1}^{\infty} \left(\left\lfloor \frac{2n}{p^a} \right\rfloor - 2 \left\lfloor \frac{n}{p^a} \right\rfloor \right).$$

Si p est strictement supérieur à $\sqrt{2n}$, cette somme se réduit à son premier terme qui est compris entre 0 et 1 et qui est égal à 1 si p divise $\binom{2n}{n}$.

LEMME A.0.6 *Pour tout $n \geq 2$ tout nombre premier p et tout entier r , si p^r divise $\binom{2n}{n}$ alors p^r est strictement inférieur à $2n$.*

Pour tout entier $n > 2$, tout nombre premier p et tout entier r , on a

$$0 \leq \left\lfloor \frac{2n}{p^a} \right\rfloor - 2 \left\lfloor \frac{n}{p^a} \right\rfloor \leq 1.$$

Dans la somme donnant l'exposant b de p dans $\binom{2n}{n}$, le nombre de sommants est inférieur ou égal au plus grand entier a tel que $p^a < 2n$. On a donc $p^b = p^a < 2n$.

LEMME A.0.7 *Pour tout $n > 2$, tout nombre premier p inférieur à n et strictement supérieur à $2n/3$ ne divise pas $\binom{2n}{n}$.*

On a simplement $[2n/p] = 2[n/p] = 2$. Le même raisonnement montre que pour tout $\varepsilon \in]0, 1/2[$ on peut remplacer $2/3$ par $\varepsilon + 1/2$.

LEMME A.0.8 *Pour tout entier $n \geq 2$ le produit des nombres premiers strictement inférieurs à n est strictement inférieur à $4n$.*

Comme dans le Lemme A.0.3, on montre que pour tout entier k on a . De plus, si p est un nombre premier compris entre $k + 1$ et $2k + 1$, l'application directe du Lemme A.0.4 montre que p divise $\binom{2k+1}{k+1}$ avec l'exposant 1. On a donc la majoration

$$\prod_{k+1 \leq p \leq 2k+1} p \mid \binom{2k+1}{k+1}$$

et $\prod_{k+1 \leq p \leq 2k+1} p < 4^k$. On conclut à l'aide d'un raisonnement par récurrence sur n à partir de $n \geq 3$.

PROPOSITION A.0.9 - *Pour tout entier $n > 2$ soit $R(n)$ le produit des nombres premiers strictement compris entre n et $2n$. On a une décomposition $\binom{2n}{n} = R(n)Q(n)$ qui a les propriétés :*

- Les nombres $R(n)$ et $Q(n)$ sont premiers entre eux ;
- Pour tout $\varepsilon > 0$ le nombre $Q(n)$ est strictement inférieur à $4^{(n+\varepsilon)/2}(2n)\sqrt{n/2}$.
- Pour tout $\varepsilon > 0$ on a

$$\frac{4^{(n-\varepsilon)/2}}{2\sqrt{n}(2n)\sqrt{n/2}} < R(n) < (2n)^{\pi(2n)-\pi(n)}.$$

Il est clair que $R(n)$ divise $\binom{2n}{n}$ car tout nombre premier strictement supérieur à n et strictement inférieur à $2n$ divise $(2n)!$ et est premier avec $n!$. Ceci prouve l'existence d'une telle décomposition. Si p est un nombre premier divisant $\binom{2n}{n}$ et compris entre n et $2n$, il divise $\binom{2n}{n}$ avec un exposant 1 d'après le Lemme A.0.5, ce qui prouve que $R(n)$ et $Q(n)$ sont premiers entre eux et en particulier que tout les diviseurs premiers de $Q(n)$ sont inférieurs à n . Ceux qui sont supérieurs à $\sqrt{2n}$ sont inférieurs à $(n + \varepsilon)/2$ et y figurent avec l'exposant 1 ; les facteurs premiers p qui sont inférieurs à $\sqrt{2n}$ y figurent avec un exposant r tel que p^r soit strictement inférieur à $2n$. Tout nombre premier étant 2 ou 3 ou de la forme $6s \pm 1$, leur nombre est majoré par $2 + \sqrt{2n}/3$.

La seconde assertion résulte directement de cette considération et du Lemme A.0.8. La majoration de $R(n)$ est évidente. Par ailleurs on a d'après ce qui précède et le Lemme A.0.3, en passant à la limite sur ε :

$$R(n) = \frac{\binom{2n}{n}}{Q(n)} \geq \frac{4^n}{2\sqrt{n}} \cdot \frac{1}{4^{n/2}(2n)^{2+\sqrt{n}/2/3}} = \frac{4^{n/2}}{2\sqrt{n}(2n)^{2+\sqrt{n}/2/3}}.$$

Démonstration du Théorème A.0.2. La majoration de $\pi(2n) - \pi(n)$ résulte directement de la minoration de $R(n)$ donnée dans la Proposition A.0.9. En ce qui concerne la minoration on a brutalement

$$\pi(2n) - \pi(n) \geq \frac{n \log(4)}{2 \log(2n)} - \frac{\log(2)}{\log(2n)} - \frac{\log(n)}{2 \log(2n)} - 2 - \frac{\sqrt{2n}}{3}$$

Dans l'expression ci-dessus, on voit sans peine que pour n assez grand, la fonction

$$n \mapsto \frac{13 \log(4)}{30} \cdot \frac{n}{\log(n)}$$

est inférieure à la fonction de droite de l'expression ci-dessus. Pour déterminer le n seuil qui est 753, on considère une petite session MAPLE résumée ci-dessous. On termine "à la main" pour démontrer le postulat de Bertrand.

```
> f := x -> 2*x/15;
g := x -> (x*(ln(4)/2)-ln(2)-ln(x)-2-sqrt(2*x)/3)/ln(2*x) - (x-f(x))*ln(4)/(2*ln(x));
evalf(g(752));evalf(g(753));
```

THÉORÈME A.0.10 *Soit $n \mapsto p(n)$ la suite des nombres premiers. La série de terme général $1/p(n)$ est divergente.*

Bien entendu ce théorème est plus riche que celui qui dit que l'ensemble des nombres premiers est infini. La première démonstration de ce résultat est semble-t-il due à Leonard Euler. Ce théorème repose sur le lemme élémentaire

LEMME A.0.11 *Pour tout réel strictement positif x , et pour tout entier n , soit $N(j, x)$ le cardinal de l'ensemble*

$$\mathcal{N}(j, x) = \{n \mid n \in \mathbb{N} \vee (0 < n \leq x) \vee (p \text{ premier et } p \text{ divise } n \Rightarrow p \leq p(j))\},$$

ensemble des entiers naturels non nuls inférieurs à x dont tous les diviseurs premiers sont inférieurs ou égaux à $p(j)$. Alors on a $N(j, x) \leq 2^{j+1} \sqrt{x}$.

Tout entier naturel non nul n peut se décomposer de façon unique sous la forme $q(n)^2 m(n)$ où $m(n)$ est produit de nombres premiers tous différents (on dit que $m(n)$ est la partie sans facteur carrée ou "quadratfrei" de n). Le nombre des entiers quadratfrei appartenant à $\mathcal{N}(j, x)$ est au plus égal à $2j + 1$. Le nombre des entiers carrés inférieurs à x est inférieur à \sqrt{x} . D'où le résultat, "à la louche".

Raisonnons par l'absurde et supposons que la dite série soit convergente. Il existerait un entier j tel que le reste de cette série $\sum_{k=j+1}^{\infty} \frac{1}{p(k)}$ soit inférieur à $1/2$. Soit alors x un réel strictement supérieur à 2^{2j+4} . Le nombre des entiers inférieurs à x dont tous les diviseurs premiers sont inférieurs ou égaux à $p(j)$ est $N(j, x)$. Le nombre des entiers inférieurs à x dont au moins un diviseur premier est $p(k)$ avec $k = j + 1$ est au plus $x/p(k)$. Dans ces conditions on a

$$x \leq N(j, x) + x \sum_{k=j+1}^{\infty} \frac{1}{p(k)} \leq N(j, x) + \frac{x}{2}$$

Ceci implique $N(j, x) = x/2 > 2^{2j+3} > 2j + \frac{1}{x}$ et une contradiction avec le lemme. On en conclut que la série est divergente.

Un autre sujet d'excitation sur la répartition des nombres premiers est le Théorème des nombres premiers :

THÉORÈME A.0.12 *Pour tout réel positif x , soit $\pi(x)$ le nombre des nombres premiers strictement inférieurs à x . Lorsque x tend vers l'infini, $\pi(x)$ est équivalent à $x/\ln(x)$. Plus précisément, il existe une constante c telle que*

$$\pi(x) = \sum_{p < x} 1 = \int_2^x \frac{du}{\log u} + (x \exp(-c\sqrt{\log(x)}))$$

La première démonstration de ce théorème est due à De La Vallée Poussin en 1896. La difficulté dans ce genre de théorème est la détermination du "terme d'erreur", voir [Tenenbaum G., Mendes-France, Les nombres premiers, Collection Que Sais-Je, PUF, 1997]

A.1 Construction d'une table de nombres premiers.

Pour construire une (petite) table de nombre premiers, on peut utiliser de proche en proche les nombres premiers déjà déterminés. Dans la procédure suivante, on construit un tableau des M premiers nombres premiers et on détermine la liste complète de nombres premiers inférieurs au carré du M_i ème nombre premier. On gardera pour le texte le cas $M = 400$. On part du fait que tout nombre premier différent de 2 et de 3 est de la forme $6s \pm 1$.

```

program tabprim ;
const M0 =401 ; M1=400 ;
type indice =0..M1 ;
      table = tableau[indice] de entier ;
      liste = liste de entier ;

```

```

var j : indice ;
    m,n,n2,x : entier ;
    prim : table ;
    prim_1 : liste ;
debut adjoindre à prim_1 les nombres 2 et 3 ; prim[0] :=5 ;
    j :=0 ; x :=2 ; n := 5 ; n2 := 2 ; tant que j < M0 faire
    debut k :=0 ; tant que n mod prim[k] ≠ 0 et prim[k] ≤ n2 faire k := k+1 ;
        si n mod prim[k] > 0 alors
            debut j := j+1 ; prim[j] :=n ; adjoindre n à prim_1 fin ;
            n :=n+x ; x := 6-x ; m := n2*n2 ;
            tant que m < n faire debut m :=m + 2*n2 + 1 ; n2 := n2 + 1 fin
        fin ; à ce stade on a M0 nombres premiers en tableau
    tant que n2 = prim[M1] faire
        debut k :=0 ; tant que n mod prim[k] ≠ 0 et prim[k] = n2 faire k := k+1 ;
            si n mod prim[k] > 0 alors adjoindre n à prim_1 ;
            n :=n+x ; x := 6-x ; m := n2*n2 ;
            tant que m < n faire debut m :=m + 2*n2 + 1 ; n2 := n2 + 1 fin
        fin
    sortir (prim_1)
fin.

```

Voici un programme en TEX pour construire une table des nombres premiers :

```

\newif\ifprime\newif\ifunknown
\newcount\n \newcount\p \newcount\d \newcount\a
\def\primes#1{2,~3% assume that #1 is at least 3
\n=#1 \advance\n by -2
\p=5
\loop\ifnum\n>0 \printifprime\advance\p by2 \repeat}
\def\printp{,
\ifnum\n=1 et~\fi
\number\p \advance\n by -1 }
\def\printifprime{\testprimality \ifprime\printp\fi}
\def\testprimality{{\d=3 \global\primetrue
\loop\trialdivision \ifunknown\advance\d by 2 \repeat}}
\def\trialdivision{\a=\p \divide\a by\d
\ifnum\a>\d \unknowntrue\else\unknownfalse\fi
\multiply\a by\d
\ifnum\a=\p \global\primefalse\unknownfalse\fi}

```

Par exemple, les quatre cent premiers nombres premiers sont
\primes{400}

Par exemple, les quatre cent premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683,

691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999, 2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099, 2111, 2113, 2129, 2131, 2137, 2141, 2143, 2153, 2161, 2179, 2203, 2207, 2213, 2221, 2237, 2239, 2243, 2251, 2267, 2269, 2273, 2281, 2287, 2293, 2297, 2309, 2311, 2333, 2339, 2341, 2347, 2351, 2357, 2371, 2377, 2381, 2383, 2389, 2393, 2399, 2411, 2417, 2423, 2437, 2441, 2447, 2459, 2467, 2473, 2477, 2503, 2521, 2531, 2539, 2543, 2549, 2551, 2557, 2579, 2591, 2593, 2609, 2617, 2621, 2633, 2647, 2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713, 2719, 2729, 2731, et 2741

B Annexe : Factorisation des Polynômes

(F. SERGERAERT)

- **Référence : Don Knuth, The Art of Computer Programming, vol. 2, pp. 381-398.**

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

- La factorisation des polynômes n'est pas un sujet vraiment facile, pas plus que la factorisation des entiers ! On présente ici le principal outil, la *méthode de Berlekamp*, qui concerne en fait la factorisation dans le cas du *corps de base fini*, puis on explique dans les cas les plus simples comment elle peut être utilisée pour obtenir la factorisation des polynômes à coefficients rationnels.

B.1 Rappels sur les corps finis.

- On rappelle que p est premier si et seulement si tous les coefficients du binôme $C(p, k)$ sont divisibles par p pour $0 < k < p$:

```
> seq(evalb(binomial(13,k) mod 13 = 0), k = 0..13) ;
> seq(evalb(binomial(9,k) mod 9 = 0), k = 0..9) ;
```

```
false, true, true, true, true, true, true, true, true, true, true, true, true, false
false, true, true, false, true, true, false, true, true, false
```

- Il en résulte que si on travaille dans Z/p , la formule $(a+b)^p = a^p + b^p$ est valide, en particulier $(a+1)^p = a^p + 1$ et il en résulte par récurrence, partant de $1^p = 1$, que $a^p = a$ dans Z/p .
- Un corps K fini est de caractéristique bien définie p : c'est le plus petit entier positif vérifiant $p \times 1 = (\text{déf.}) 1 + 1 + \dots + 1$ (p fois) $= 0$. Nécessairement, p est *premier*, sinon on aurait dans K des diviseurs de 0. Le corps K contient donc en particulier le sous-corps $\{0, 1, 2, \dots, p-1\} = Z/p$ qu'on notera simplement Z_p et K est donc un espace vectoriel sur Z_p de dimension d ; il a alors p^d éléments. La formule démontrant que le *morphisme de Frobenius* $a \rightarrow a^p$ est Z -linéaire (et donc aussi Z_p -linéaire) : $(a+b)^p = a^p + b^p$ reste valable, mais il est maintenant *faux*, sauf si $d=1$, que $a^p = a$ pour tout a de K . En effet, puisque $X^p - X$ est de degré p , il ne peut avoir que p racines dans K , à savoir les éléments de Z_p dans K . On verra que cette remarque est la clé de la *méthode de Berlekamp* pour factoriser un polynôme à coefficients dans Z_p .
- Le groupe *multiplicatif* des éléments non nuls de K a pour cardinal $p^d - 1$, et il en résulte que pour tous ces éléments, la relation $a^{(p^d-1)} = 1$ est satisfaite ; le polynôme $X^{(p^d)} - X$ a donc pour racines tous ces éléments, et de plus l'élément nul. Les éléments de K sont donc tous racines de ce polynôme, et il en résulte que $X^{(p^d)} - X = \prod_a (X - a)$ où a parcourt exactement tous les éléments de K . Donc K est un (donc *le*) corps de décomposition de ce polynôme et il en résulte qu'il n'existe qu'un seul corps de cardinal p^d .

- Soit P dans $Z_p[X]$ un polynôme *irréductible* de degré d . Alors le quotient $Z_p[X]/P$ est un corps à p^d éléments. Il résulte de ce qui précède que la *classe d'isomorphisme* de ce corps est indépendante de P . Le polynôme P divise nécessairement le polynôme $X^{(p^d)} - X$; en effet, si x est la classe de X dans $Z_p[X]/P$, le polynôme minimal de x ne peut être que P , mais d'après ce qui est dit ci-dessus, x est aussi racine de $X^{(p^d)} - X$ et donc ce dernier polynôme est divisible par P . Il en résulte aussi que P est *entièrement* scindé dans K , donc une seule extension suffit toujours pour obtenir le corps de décomposition d'un polynôme irréductible : toute extension de Z_p est *galoisienne*.

Illustration.

> `rnd := rand(0..2) :`

- Contrairement au cas des coefficients entiers banals, il faut «tâtonner» un peu pour trouver un polynôme irréductible à coefficients dans Z_3 .

> `_seed := 1639 :`

> `P := sort(X^3 + add(rnd()*X^i, i=0..2)) ;`

$$P := X^3 + 2X^2 + 1$$

> `Irreduc(P) mod 3 ;`

true

- Il en résulte que le même polynôme est Q -irréductible :

> `irreduc(P) ;`

true

- Mais la réciproque est *fausse* : il arrive souvent qu'un polynôme soit Q -irréductible, mais pas Z_p -irréductible ; il arrive même que ceci se produise *quel que soit* p pour le même polynôme Q -irréductible, c'est le cas de $X^4 + 1$.

> `irreduc(X^4+1) ;`

true

> `Irreduc(X^4+1) mod 67 ;`

false

> `Factor(X^4+1) mod 67 ;`

$$(X^2 + 47X + 66)(X^2 + 20X + 66)$$

> `Factor(X^4+1) mod nextprime(10^6) ;`

$$(X^2 + 410588X + 1000002)(X^2 + 589415X + 1000002)$$

- Pour travailler *sous Maple* dans des extensions de Z_p , on procède comme pour les extensions de Q , mais il n'y a *aucune différence* dans l'usage initial de **RootOf**, c'est seulement *en fin de calcul* qu'on précise qu'on veut travailler dans Z_p et ses extensions, en *suffixant* par «**mod p**».

> `alias(alpha = RootOf(P)) ;`

α

- Le quotient $Z_3[X]/P$ est un espace vectoriel de degré 3 sur Z_3 , dont les éléments sont tous de la forme $i + j\alpha + k\alpha^2$ pour i, j et k parcourant Z_3 .

- Calcul du polynôme ayant *exactement* tous les éléments de $Z_3[X]/P$ comme racine

```
> mul(mul(mul(X-i-j*alpha-k*alpha^2,
> k=0..2),
> j=0..2),
> i=0..2) ;
```

$$\begin{aligned}
& X(X-\alpha^2)(X-2\alpha^2)(X-\alpha)(X-\alpha-\alpha^2)(X-\alpha-2\alpha^2)(X-2\alpha)(X-2\alpha-\alpha^2) \\
& (X-2\alpha-2\alpha^2)(X-1)(X-1-\alpha^2)(X-1-2\alpha^2)(X-1-\alpha)(X-1-\alpha-\alpha^2) \\
& (X-1-\alpha-2\alpha^2)(X-1-2\alpha)(X-1-2\alpha-\alpha^2)(X-1-2\alpha-2\alpha^2)(X-2) \\
& (X-2-\alpha^2)(X-2-2\alpha^2)(X-2-\alpha)(X-2-\alpha-\alpha^2)(X-2-\alpha-2\alpha^2) \\
& (X-2-2\alpha)(X-2-2\alpha-\alpha^2)(X-2-2\alpha-2\alpha^2)
\end{aligned}$$

- Développement du produit.

```
> Expand(%) mod 3 ;
```

$$2X + X^{27}$$

- ... autrement dit $X^{27} - X$. A comparer avec :

```
> collect(evala(expand(%)), [X, alpha]) :
```

- Vérification de la propriété de divisibilité.

```
> Divide(X^27-X, P) mod 3 ;
```

true

- Et pour cause :

```
> Factor(P, alpha) mod 3 ;
```

$$(X + \alpha^2 + \alpha + 1)(X + 2\alpha^2 + 1)(X + 2\alpha)$$

- Car, comme expliqué plus haut, *une seule extension* suffit toujours à décomposer *complètement* le polynôme initial. Propriété en général fautive dans le cas rationnel :

```
> factor(P, alpha) ;
```

$$(X - \alpha)(X^2 + 2X + X\alpha + 2\alpha + \alpha^2)$$

B.2 Bases de la méthode de Berlekamp

- On travaille dans l'anneau de polynômes $Z_p[X]$, pour un premier p , et sauf indication contraire, $Z_7[X]$ dans les exemples

- Soit P dans $Z_p[X]$ et $P = P_1 \dots P_r$ sa décomposition en facteurs irréductibles. On suppose d'abord que P est sans facteur multiple, sinon ceci est détecté facilement par le PGCD du polynôme et du polynôme dérivé. Construisons un exemple de cette sorte.

```
> rnd := rand(0..6) :
> rndP := proc(n)
> RETURN(sort(X^n + add(rnd()*X^i, i=0..(n-1))))
> end :
> _seed := 1730 :
> P1, P2 := rndP(3), rndP(3) ;
```

$$P1, P2 := X^3 + X^2 + 2X + 4, X^3 + 4X^2 + 4X + 2$$

- Le polynôme qui suit va certainement avoir un facteur multiple, mais on *fait semblant* de ne rien savoir à ce propos.

> P := sort(Expand(P1^2 * P2) mod 7) ;

$$P := X^9 + 6X^8 + 3X^7 + 3X^4 + 5X^3 + 5X^2 + 5X + 4$$

- On détecte un facteur multiple éventuel par l'examen du PGCD entre le polynôme et son dérivé.

> Gcd(P, diff(P, X) mod 7) mod 7 ;

$$X^3 + X^2 + 2X + 4$$

- Et on commencerait par factoriser $X^3 + X^2 + 2X + 4$. Presque toujours (pas toujours, pourquoi?) le polynôme initial est divisible par le carré de ce terme.

> Rem(P, %^2, X) mod 7 ;

$$0$$

> Quo(P, %%^2, X) mod 7 ;

$$X^3 + 4X^2 + 4X + 2$$

- ce qui redonne comme par hasard nos polynômes initiaux.

- On suppose donc désormais qu'il n'y a aucun facteur multiple dans P .

- Si $P = P_1 \dots P_r$ est la décomposition de P en facteurs irréductibles, le *théorème du reste chinois* donne un isomorphisme canonique :

Z_p

$[X]/P = Z_p[X]/P_1 + \dots Z_p[X]/P_r$. Les facteurs du second membre sont tous des corps, le premier membre n'est un corps que si P est irréductible, autrement dit si $r = 1$.

- Il en résulte, c'est l'astuce de Berlekamp, un test permettant, *sans connaître* r , de «deviner» sa valeur. Considérons en effet l'équation où l'inconnue V est un élément de $Z_p[X]/P$:

$$V^p - V = 0$$

- Si on traduit cette équation vers le second membre (qu'on ne connaît pas!), l'inconnue V devient un r -uplet (V_1, \dots, V_r) , et comme l'isomorphisme utilisé *est un isomorphisme d'anneaux*, l'équation se transforme en r équations $V_i^p = V_i$. Comme l'inconnue V_i est cette fois dans le *corps* $Z_p[X]/P_i$, on sait qu'il y a *exactement* les p racines $0, \dots, p-1$ dans $Z_p[X]/P_i$. On en déduit que le cardinal des solutions est *exactement* p^r . Ainsi le cardinal de l'ensemble des solutions va nous donner le nombre fatidique r . D'une façon très approximative, on peut dire que Berlekamp observe que *plus* P est réductible, *moins* $Z_p[X]/P$ est un corps, et plus l'ensemble des solutions de notre équation va être vaste.

- Le deuxième élément clé de la méthode de Berlekamp consiste à remarquer que puisque l'application $V \rightarrow V^p$ est *linéaire*, l'équation $V^p - V = 0$ est, malgré les apparences, une *équation linéaire*, et on dispose donc de tous les outils linéaires classiques pour la traiter.

- **Exemple.** Soit à étudier si notre polynôme **P1** est irréductible dans Z_7 . Il faut construire la matrice de l'application linéaire $V \rightarrow V^p - V$ dans $Z_p[X]/P_1$. On prend la base canonique $1, X, X^2$ (ou plus précisément leurs classes modulo P_1). L'image de X^j est donc la classe de $X^{(pj)} - X^j$, et les éléments de colonne correspondants sont les coefficients appropriés. On construit à part la procédure **BerlTerm** permettant le calcul du terme d'indices (i, j) de la *matrice de Berlekamp* du polynôme P par rapport à Z_p .

```
> BerlTerm := proc(p::posint, P::polynom(integer, X),
> i::posint, j::posint)
> RETURN(coeff(Rem(X^(p*(j-1))-X^(j-1), P, X) mod p,
> X, i-1))
> end ;
> BerlMatrix1 := matrix(3, 3, (i,j) -> BerlTerm(7, P1, i,j)) ;
```

$$BerlMatrix1 := \begin{bmatrix} 0 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 6 & 1 \end{bmatrix}$$

- La *dimension du noyau* nous donne la dimension de l'espace des solutions, c'est-à-dire le nombre des facteurs irréductibles. On voit que le rang est 2, l'espace des solutions est donc de dimension 1, ce ne peut être que Z_7 , solutions «inévitables», et notre polynôme est donc irréductible. Pour obtenir le rang de cette matrice dans le cas général, il faut utiliser la procédure **Nullspace** combinée avec **mod**.

```
> Nullspace(BerlMatrix1) mod 7 ;
{[1, 0, 0]}
```

- Vérification.

```
> Irreduc(P1) mod 7 ;
true
```

- Même travail avec P_2 .

```
> BerlMatrix2 := matrix(3, 3, (i,j) -> BerlTerm(7, P2, i,j)) ;
```

$$BerlMatrix2 := \begin{bmatrix} 0 & 4 & 0 \\ 0 & 5 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

```
> Nullspace(BerlMatrix2) mod 7 ;
{[1, 0, 0], [0, 0, 1]}
```

```
> Irreduc(P2) mod 7 ;
false
```

- On voit qu'ici notre équation $V^p - V$ a 49 solutions, $49 = 7^2$, et notre polynôme a donc *deux* facteurs irréductibles. Il reste à les déterminer. Dans un cas si simple, c'est très facile, il suffit de chercher l'élément a de Z_7 nécessairement racine de P_2 et le quotient par $X - a$ donnera l'autre facteur irréductible. Mais on veut expliquer comment il faut procéder dans le cas général. C'est le sujet de la section suivante.

```
> for i from 0 to 6 do
> if Eval(P2, X=i) mod 7 = 0 then print(i) fi
> od ;
```

3

> Quo(P2, X-3, X) mod 7 ;

$X^2 + 4$

> Irreduc(%) mod 7 ;

true

> Factor(P2) mod 7 ;

$(X^2 + 4)(X + 4)$

B.3 Trouver les facteurs irréductibles.

- Les solutions de l'équation $V^p - V = 0$ ne donnent pas seulement le *nombre* de facteurs irréductibles, chaque solution donne aussi une décomposition, en général *partielle*, mais toujours *non triviale*, du polynôme proposé en facteurs de degrés plus petits. Ceci est dû au fait que dans Z_p , nous avons la décomposition :

$$V^p - V = V(V - 1) \dots (V - p - 1).$$

- Dire que V est une solution de $V^p - V$ dans $Z_p[X]/P$ revient à dire que P divise $V^p - V$, mais la factorisation ci-dessus de $V^p - V$ va justement nous permettre de «découper en tranches» le polynôme P .
- D'abord si P est irréductible, les seules solutions de $V^p - V = 0$ sont les éléments de Z_p , auquel cas le «polynôme» $V^p - V$ est non seulement divisible par P , il est même nul ! et aucune «information» ne peut être obtenue, heureusement.
- Par contre si P est factorisable, on va avoir des solutions différentes. Ces solutions vont être de «vrais» polynômes (non constants), et un tel polynôme V va être de degré forcément $< d = \text{degree}(P)$. On a alors le résultat suivant :

$$P = \prod_{i=0}^{p-1} \text{PGCD}(P, V - i)$$

- En effet $V^p - V$ est divisible par P , et donc tout facteur irréductible de P va diviser $V^p - V$ et se retrouver dans l'un des PGCD. Donc P divise le produit. Inversement, comme les $V - i$ sont *premiers deux à deux* (pourquoi?), le même facteur de P ne peut pas se retrouver deux fois à droite. Compte tenu par ailleurs du fait que $\text{degree}(V - i) < d$, on voit donc qu'on a ainsi, quel que soit V solution «non constante» de $V^p - V = 0$, une factorisation non triviale de P .
- Essayons ce mécanisme avec notre polynôme P_2 . Un V non trivial est à trouver dans le noyau de la matrice de Berlekamp :

> eval(BerlMatrix2) ;

$$\begin{bmatrix} 0 & 4 & 0 \\ 0 & 5 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

> Nullspace(BerlMatrix2) mod 7 ;

$\{[1, 0, 0], [0, 0, 1]\}$

- Le générateur $[1,0,0]$ du noyau correspond aux solutions triviales de $V^p - V = 0$, mais l'autre, $[0,0,1]$, expression dans notre base du polynôme X^2 , est une solution non triviale.

```
> Divide(X^14-X^2, P2) mod 7 ;
                                     true
> seq(Gcd(P2, X^2-i) mod 7, i=0..6) ;
                                     1, 1, X + 4, X^2 + 4, 1, 1, 1
```

- Et on a bien notre décomposition.

```
> evalb(P2 = Expand(mul(gcdi, gcdi=[%]))) mod 7) ;
                                     true
```

- Dans le cas général, il n'y a pas de raison que la décomposition *complète* de P soit ainsi obtenue à l'aide d'une seule solution non triviale V . C'est forcément ce qui arrive si le nombre de facteurs de P est plus grand que p . Construisons P de sorte qu'il ait au moins 8 facteurs.

```
> _seed := 1054 ;
> for i from 1 to 8 do
> P||i := rndP(2)
> end do ;

P1 := X^2 + 4X + 2
P2 := X^2 + 2X + 3
P3 := X^2 + 3X + 2
P4 := X^2 + 2X
P5 := X^2 + 5X + 5
P6 := X^2 + 2X + 5
P7 := X^2 + 6X
P8 := X^2 + 5X + 1

> P := sort(Expand(mul(P||i, i=1..8)) mod 7) ;
```

$$P := X^{16} + X^{15} + 6X^{14} + 4X^{13} + 3X^{12} + 6X^{11} + 6X^{10} + 5X^9 + 3X^8 + 3X^7 + 5X^6 + X^5 + 2X^4 + X^3 + 2X^2$$

- Mais on peut avoir des facteurs multiples, qu'il faut éliminer pour que notre exemple soit correct.

```
> Gcd(P, diff(P,X) mod 7) mod 7 ;
                                     X^5 + 6X^4 + 4X^3 + 5X^2 + 5X
> P := Quo(P, %, X) mod 7 ;
                                     P := X^{11} + 2X^{10} + 4X^9 + 2X^8 + 2X^7 + 5X^6 + X^5 + X^4 + 4X^2 + 6X
> Gcd(P, diff(P,X) mod 7) mod 7 ;
```

1

- Donc plus de facteurs multiples.

```
> BerlMatrix := matrix(11,11, (i,j) -> BerlTerm(7,P,i,j)) :
> Kernel := Nullspace(%) mod 7 ;
```

```
Kernel := {[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1],
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0], [0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0],
[0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0], [0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0],
[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0], [0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0]}
```

- Les éléments du noyau sont des *vecteurs*, ce qui est techniquement désagréable pour la suite, on les transforme tous en *listes*.

```
> Kernel := map(convert, Kernel, list) ;
```

```
Kernel := {[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
[0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1], [0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0],
[0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0], [0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0],
[0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0], [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]}
```

```
> r := nops(Kernel) ;
```

```
r := 8
```

- Donc 8 facteurs irréductibles. On retire l'élément de noyau correspondant aux solutions triviales.

```
> Kernel := Kernel minus {[1, 0$10]} ;
```

```
Kernel := {[0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0], [0, 5, 2, 5, 0, 0, 0, 0, 0, 0, 1],
[0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0], [0, 3, 0, 1, 0, 0, 0, 0, 0, 1, 0],
[0, 1, 0, 3, 0, 1, 0, 0, 0, 0, 0], [0, 4, 6, 4, 1, 0, 0, 0, 0, 0, 0],
[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]}
```

```
> Vvector1 := Kernel[1] ;
```

```
Vvector1 := [0, 5, 3, 5, 0, 0, 1, 0, 0, 0, 0]
```

```
> V1 := sort(add(Vvector1[i]*X^(i-1), i=1..11)) ;
```

```
V1 := X6 + 5X3 + 3X2 + 5X
```

```
> factors1 := {seq(Gcd(V1-i, P) mod 7, i=0..6)} minus{1} ;
```

```
factors1 := {X2 + 2X + 5, X2 + 5X + 5, X + 1, X3 + 4X2 + 6, X3 + 4X2 + 2X}
```

```
> nops(factors1) ;
```

```
5
```

```
> evalb(P = Expand(mul(gcdi, gcdi=factors1)) mod 7) ;
```

```
true
```

- On voit qu'une décomposition non triviale de P est bien obtenue, mais ce n'est évidemment pas là la décomposition *complète* en facteurs irréductibles, puisqu'on a construit P comme un produit de facteurs de degré 2. Comme seulement 7 cases sont disponibles dans le résultat, certainement certains facteurs ainsi obtenus sont encore réductibles.

- Le point suivant consiste à dire qu'en essayant au besoin les autres éléments «non triviaux» du noyau de la matrice de Berlekamp, on va réussir, en *recoupant* les résultats, à obtenir la factorisation complète. Expliquons ce qu'il faut entendre par *recouper*.

- Prenons un autre vecteur de notre noyau.

```

> Vvector2 := Kernel[2] ;
      Vvector2 := [0, 5, 2, 5, 0, 0, 0, 0, 0, 1]
> V2 := sort(add(Vvector2[i]*X^(i-1), i=1..11)) ;
      V2 := X10 + 5X3 + 2X2 + 5X
> factors2 := {seq(Gcd(V2-i, P) mod 7, i=0..6)} minus {1} ;
      factors2 := {X2 + X, X + 2, X + 5, X4 + 4X3 + 5X2 + 2X + 1, X3 + 4X2 + 2}
> nops(factors2) ;

```

5

- On voit que la factorisation n'est pas la même que celle précédemment obtenue. On va démontrer juste après que c'est toujours le cas. On obtient donc une «meilleure» factorisation en prenant l'*intersection*, à coups de PGCD, des deux factorisations.

```

> factors12 := {seq(seq(Gcd(f1,f2) mod 7,
> f2 = factors2),
> f1 = factors1)}
> minus {1} ;
      factors12 := {X2 + 2X + 3, X2 + 2X + 5, X2 + 5X + 5, X, X + 1, X + 2, X + 5, X + 6}
> nops(factors12) ;

```

8

- La factorisation est donc complète. D'autres fois, il faut encore continuer.
- Expliquons pourquoi la méthode des *recouvrements* aboutit. Pour mieux faire comprendre, on se contente du cas $r = 3$. Donc $P = P_1 P_2 P_3$ et :

$$K[X] / P = K[X] / P_1 + K[X] / P_2 + K[X] / P_3.$$

- Toute solution de notre équation $V^p - V = 0$ a deux interprétations. Du côté «gauche», c'est un polynôme «modulo P » ; mais du côté droit, comme pour chaque facteur les seules solutions sont les polynômes «constants», ces solutions sont essentiellement des triplets $(\alpha_1, \alpha_2, \alpha_3)$ d'entiers modulo p . La correspondance de la droite vers la gauche n'est rien d'autre que le *théorème des restes chinois*. Le relèvement de $(1,0,0)$ est le produit $B_1 P_2 P_3$ de la relation de Bezout $A_1 P_1 + B_1 P_2 P_3 = 1$, car il s'agit d'avoir un polynôme divisible par P_2 et P_3 , mais égal à 1 modulo P_1 . De la même façon, le relèvement de $(0,1,0)$ (resp. $(0,0,1)$) est le produit $B_2 P_1 P_3$ (resp. $B_3 P_1 P_2$) avec des interprétations analogues. Une solution «triviale» est de la forme (α, α, α) . Donc une solution non triviale vérifie par exemple $\alpha_1 \not\equiv \alpha_2$. Soit V l'interprétation polynôme de cette solution. Alors $V - \alpha_1 = (\alpha_2 - \alpha_1) B_2 P_1 P_3 + (\alpha_3 - \alpha_1) B_3 P_1 P_2$, alors que $V - \alpha_2 = (\alpha_1 - \alpha_2) B_1 P_2 P_3 + (\alpha_3 - \alpha_2) B_3 P_1 P_2$. Il en résulte que $V - \alpha_1$ est divisible par P_1 et $V - \alpha_2$ est divisible par P_2 . Donc le «traitement» de V va forcément «séparer» les facteurs P_1 et P_2 . Maintenant l'ensemble des solutions à gauche correspond à l'ensemble des solutions à droite, et il y a donc forcément une solution à gauche correspondant (sans qu'on le «voie») à un cas où $\alpha_1 \not\equiv \alpha_2$. Il en est forcément de même pour l'un des vecteurs de la base du noyau, sinon on aurait $\alpha_1 = \alpha_2$ pour tous les éléments du noyau, ce qui est exclu. Le même travail peut être fait en général pour toutes les paires d'indices, d'où le fait que les éléments de la base du noyau suffisent à complètement factoriser. CQFD.

- On est prêt maintenant pour une procédure générale de factorisation. Elle va utiliser notre procédure **BerlTerm** déjà construite.

```

> Berl := proc(p::posint, P::polynom(integer, X))
> local d, r, i,
> BerlMatrix, Kernel,
> Vvector, V,
> result, new_factors ;
> d := degree(P, X) ;
> # Erreur si facteur multiple.
> if Gcd(P, diff(P, X)) mod p <> 1 then
> ERROR('The polynom is not squarefree.')
> fi ;
> BerlMatrix := matrix(d,d, (i,j) -> BerlTerm(p,P,i,j)) ;
> Kernel := Nullspace(BerlMatrix) mod p ;
> # r = nombre de facteurs irréductibles.
> r := nops(Kernel) ;
> # Si r = 1, le polynôme est irréductible.
> if r = 1 then RETURN([P]) fi ;
> Kernel := map(convert, Kernel, list) ;
> # Suppression de la solution triviale.
> Kernel := Kernel minus {[1, 0$(d-1)]} ;
> # Pour signaler le début de l'algorithme.
> result := {} ;
> # Il faut parcourir les solutions non triviales et # arrêter quand le nombre de facteurs requis est
atteint.
> for Vvector in Kernel while nops(result) < r do
> # Expression polynômiale du nouveau vecteur solution considéré.
> V := add(Vvector[i]*X^(i-1), i=1..d) ;
> # Découpage en tranches.
> new_factors := {seq(Gcd(P, V-i) mod p, i=0..(p-1))}
> minus {1} ;
> # Recoupement (éventuel) avec ce qui a été précédemment fait.
> if nops(result) > 1 then
> result := {seq(seq(Gcd(f1,f2) mod p,
> f2 = new_factors),
> f1 = result)}
> minus {1}
> else result := new_factors
> fi
> od ;
> result := convert(result, list) ;
> result := map(sort, result) ;
> result := sort(result,
> (P1,P2)->evalb(degree(P1)<degree(P2))) ;
> RETURN(map(sort,result))
> end ;
> fs := Berl(7, P) ;
    fs := [X + 6, X + 5, X + 2, X + 1, X, X2 + 5X + 5, X2 + 2X + 5, X2 + 2X + 3]
> nops(fs) ;
    8
> P - Expand(mul(f, f=fs)) mod 7 ;
    0
> Berl(73, X4+1) ;

```

$$[X + 51, X + 10, X + 63, X + 22]$$

- Des polynômes complexes peuvent ainsi être factorisés.

```
> _seed := 1535 ;
> P := rndP(50) ;
```

$$P := X^{50} + 2X^{49} + 5X^{48} + 6X^{47} + 3X^{46} + 2X^{45} + X^{43} + X^{42} + 4X^{41} + 2X^{40} + 5X^{39} + 5X^{38} \\ + 6X^{37} + 3X^{36} + 3X^{35} + 3X^{31} + 4X^{29} + 2X^{28} + 3X^{27} + 4X^{26} + 3X^{25} + X^{23} \\ + 3X^{22} + 6X^{20} + X^{19} + X^{18} + 4X^{17} + 3X^{16} + 5X^{15} + 6X^{13} + X^{12} + 6X^{11} + 3X^{10} \\ + 3X^9 + 6X^8 + X^7 + 3X^6 + 5X^5 + 3X^4 + 2X^3 + 5X + 6$$

```
> fs := Berl(7, P) ;
```

```
> map(print, fs) :
```

$$X^2 + 5X + 2 \\ X^{11} + X^{10} + X^9 + 6X^7 + 6X^6 + 5X^5 + 5X^4 + 4X^3 + 2X^2 + 4X + 4$$

$$X^{37} + 3X^{36} + 3X^{34} + 5X^{33} + X^{31} + 5X^{30} + 5X^{28} + 3X^{27} + 3X^{26} + 5X^{25} + 3X^{24} + 2X^{23} \\ + 3X^{22} + 3X^{21} + 3X^{20} + X^{19} + 6X^{17} + 3X^{16} + 6X^{15} + 6X^{14} + 6X^{13} + 4X^{12} \\ + 3X^{10} + 6X^9 + X^8 + 6X^7 + X^6 + 3X^5 + 2X^4 + 3X^3 + 5X + 6$$

```
> nops(fs) ;
```

3

```
> map(item -> Irreduc(item) mod 7, fs) ;
```

[true, true, true]

```
> P - Expand(mul(item, item=fs)) mod 7 ;
```

0

- Un cas irréductible.

```
> Berl(7, fs[1]) ;
```

$$[X^2 + 5X + 2]$$

B.4 Factorisation des polynômes à coefficients entiers.

- Les méthodes efficaces de factorisation des polynômes à coefficients entiers commencent toutes par \mathbb{Z}_p -factoriser pour un p premier, ou puissance d'un nombre premier, avec p assez grand. Par examen de la taille des coefficients pour une \mathbb{Z} -factorisation éventuelle, on finit par en déduire la \mathbb{Z} -factorisation cherchée. Le point clé dans cette direction consiste à majorer les racines (en général complexes) du polynôme à factoriser.

- Soit donc $P = X^n + a_{n-1}X^{(n-1)} + \dots + a_0$ un polynôme *unitaire* à coefficients complexes. Alors toute racine de P est *strictement* majorée par : $A = 2 \max(|a_i|^{\frac{1}{n-i}}, i = 0..n-1)$. En effet on peut écrire $P = X^n (1 + (\sum_{i=1}^n \frac{a_{n-i}}{X^i}))$ où $|a_{n-i}| \leq (\frac{A}{2})^i$. La somme de la dernière expression devient une progression géométrique *strictement* majorée par $\frac{A}{2X} \frac{1}{1 - \frac{A}{2X}} = \frac{A}{2X-A} \leq 1$ si $A \leq |X|$. Donc la dernière inégalité implique $P(X)$ non nul. Le raisonnement est en défaut si $A = 0$, mais ce cas est sans intérêt, car alors toutes les racines sont nulles. Procédure conséquente.

```

> RootsSup := proc(P::polynom(rational, X))
> local dgr ;
> dgr := degree(P, X) ;
> if coeff(P, X, dgr) <> 1 then
> ERROR(sprintf("Polynôme %a non unitaire.", P))
> fi ;
> RETURN(2 * max(seq(evalf(abs(coeff(P, X, i))^(1/(dgr-i))),
> i=0..(dgr-1))))
> end :

```

- Soit donc P un Z -polynôme *unitaire* (il est facile de se ramener à ce cas par «changement de variable») où les coefficients sont majorés par A . Il est élémentaire d'en déduire que les racines (complexes) sont aussi *strictement* majorées en module par $A + 1$; il existe des inégalités sensiblement plus fines à ce sujet, mais pour simplifier, on se contentera ici de celle-ci. Puisqu'un facteur potentiel de P est un produit de $(X - \alpha)$ où α parcourt certaines racines de P , on en déduit des majorations pour les coefficients d'une Z -factorisation éventuelle. On peut alors conclure en examinant la Z_p -factorisation de P pour p assez grand.

- Examinons par exemple le cas de $X^4 + 1$. Ici $A = 2$ mais on sait bien que les quatre racines sont de module 1. Tentons la Z_3 -factorisation.

```

> RootsSup(X^4+1) ;
> Berl(3, X^4+1) ;

```

$$2. \\ [X^2 + 2X + 2, X^2 + X + 2]$$

- Il en résulte qu'une Z -factorisation a au plus deux facteurs de degré 2, où les termes constants sont de la forme $3n + 2$, mais ce pourrait être -1 , et on ne peut conclure. On augmente p .

```

> Berl(5, X^4+1) ;

```

$$[X^2 + 3, X^2 + 2]$$

- Cette fois on a gagné, parce que l'un des facteurs a un terme constant de la forme $5n + 2$, incompatible avec les modules connus des racines de $X^4 + 1$. Donc $X^4 + 1$ est Z -irréductible et donc (voir la démonstration du théorème de Gauss sur la factorialité de $Z[X]$) Q -irréductible.

```

> irreduc(X^4+1) ;

```

true

- Avec un polynôme moins trivial.

```

> _seed := 921 ;
> P := rndP(10) ;
> RootsSup(P) ;

```

$$P := X^{10} + 2X^9 + 3X^8 + 5X^7 + 2X^6 + 4X^5 + 4X^4 + 2X^3 + 5X^2 + X + 6$$

4.

- Toute racine est majorée par 4, et si une factorisation non triviale est possible, elle aura un facteur de degré au plus 5 où le coefficient du terme après le terme de plus haut degré sera donc majoré par 20 d'où l'idée d'utiliser 41.

```

> Berl(41,P) ;

```


$$[X^{10} + 2X^9 + 3X^8 + 5X^7 + 2X^6 + 4X^5 + 4X^4 + 2X^3 + 5X^2 + X + 6]$$

- On est chanceux, le polynôme est donc irréductible.

```
> _seed := 1529 ;
> P := rndP(10) ;
> RootsSup(P) ;
```

$$P := X^{10} + 6X^9 + 3X^8 + 6X^7 + X^6 + 6X^5 + 2X^4 + 2X^3 + 5X^2 + 2X + 3$$

12.

- On essaie un nombre premier $> 10 \cdot 12 = 120$, par exemple 127

```
> Berl(127, P) ;
```

$$[X + 45, X + 6, X^3 + 86X^2 + 108X + 28, X^5 + 123X^4 + 105X^3 + 51X^2 + 13X + 19]$$

- Le facteur $X + 45$ seul ne peut pas provenir d'une Z -factorisation, ni le facteur de degré 3. Dans une telle situation il faut essayer si -6 est racine :

```
> subs(X=-6, P) ;
```

3361563

- Le produit $(X + 6)(X + 45)$ va commencer par $X^2 + 51X$ et est aussi exclu. Essayons un autre nombre premier, pour voir.

```
> Berl(131, P) ;
```

$$[X^2 + 104X + 55, X^8 + 33X^7 + 53X^6 + 15X^5 + 111X^4 + 82X^3 + 41X^2 + 5X + 112]$$

- Mais le facteur de degré 2 est impossible et le polynôme P est donc Q -irréductible. Vérification.

```
> irreduc(P) ;
```

true

- Il se trouve qu'on aurait pu essayer dans ce cas un entier un peu plus... petit. Ce polynôme est en effet déjà irréductible modulo 5!

```
> Berl(5, P) ;
```

$$[X^{10} + 6X^9 + 3X^8 + 6X^7 + X^6 + 6X^5 + 2X^4 + 2X^3 + 5X^2 + 2X + 3]$$

- Un polynôme aléatoire est presque toujours irréductible. Forçons le choix d'un polynôme exercice certainement *réductible*.

```
> _seed := 940 ;
> P1, P2 := rndP(4), rndP(6) ;
> P := sort(expand(P1 * P2)) ;
```

$$P := X^{10} + 4X^9 + 7X^8 + 16X^7 + 30X^6 + 34X^5 + 49X^4 + 51X^3 + 28X^2 + 30X + 20$$

```
> RootsSup(P) ;
```

8.

```
> nextprime(2*5*8) ;
```

83

```
> Berl(83, P) ;
```

$$[X + 9, X + 74, X + 68, X + 2, X + 1, X^2 + 37X + 64, X^3 + 62X^2 + 40X + 67]$$

- On doit donc examiner si -1 et -2 sont racines.

```
> eval(P, X=-1) ;
0
```

```
> eval(P, X=-2) ;
0
```

- Le reste est un peu confus. Divisons et réexaminons la question.

```
> P2 := quo(P, (X+1)*(X+2), X) ;
      P2 := X^8 + X^7 + 2 X^6 + 8 X^5 + 2 X^4 + 12 X^3 + 9 X^2 + 10
> RootsSup(P2) ;
      4.000000000
> Berl(37, P2) ;
      [X^2 + 2, X^6 + X^5 + 6 X^3 + 2 X^2 + 5]
```

- Essai.

```
> rem(P2, X^2+2, X) ;
0
```

- D'où la Q -factorisation définitive. Vérification.

```
> factor(P) ;
      (X + 1) (X + 2) (X^6 + X^5 + 6 X^3 + 2 X^2 + 5) (X^2 + 2)
```

- En «bricolant» de la sorte, on arrive en général à factoriser les polynômes pas trop compliqués, mais *programmer* une méthode *générale* est autrement complexe. Il serait confortable de savoir faire la factorisation modulo un *grand* nombre premier, mais la méthode de Berlekamp, telle qu'elle a été programmée précédemment, échoue alors, parce que l'équation de Berlekamp $V^p - V = 0$ devient trop difficile à résoudre, à cause de la taille de p .

```
> # Ne pas effectuer sous Maple 6.
> # Berl(nextprime(10^6), P) ;
```

- Beaucoup d'améliorations peuvent être intégrées à la procédure **Berl**, mais elle n'ira jamais très loin pour une factorisation par rapport à de *grands nombres premiers*. Le corps «fini» Z_p est bien trop grand pour mener les calculs bien loin. Penser en particulier à la factorisation qu'il faut utiliser $V^p - V = V(V-1) \dots V-p-1$, où le nombre de facteurs est justement p !! Une autre solution devient alors beaucoup plus intéressante, basée sur le *lemme de Hensel*.

B.5 Lemme de Hensel.

- Le *lemme de Hensel* est une méthode largement utilisée en algèbre commutative consistant à résoudre un problème d'abord «approximativement» modulo un idéal m puis à *affiner* en travaillant modulo les puissances de cet idéal, puissances *de plus en plus petites*. Le problème de la factorisation des polynômes est justement un cadre parfait pour comprendre le mécanisme.

- L'outil essentiel pour démontrer le lemme de Hensel consiste à utiliser judicieusement une relation à la Bezout pour exprimer un élément quelconque, et pas seulement 1, en fonction de deux éléments u et v premiers entre eux dans un anneau principal.

- Commençons pour comprendre le principe par le cas entier.

PROPOSITION B.5.1 *Si u et v sont deux entiers positifs premiers entre eux, alors tout entier $x \in]0, uv[$ s'exprime d'une façon et d'une seule sous la forme :*

$$x = \alpha u + \beta v \pmod{uv}$$

avec $\alpha \in [0, v[$ et $\beta \in [0, u[$.

DÉMONSTRATION. Soit $1 = au + bv$ une relation de Bezout entre u et v . Par multiplication par x , on obtient $x = xau + xbv$, mais $x a$ et $x b$ sont en général trop grands; on les divise donc respectivement par v et u , pour obtenir $x = \alpha u + \beta v + \gamma uv$ où on peut choisir α et β dans les intervalles requis. Si un autre choix était possible, on trouverait par différences une relation $\alpha u + \beta v = 0 \pmod{uv}$ avec α non nul et de module $< v$; mais ceci contredit la divisibilité de α par v .

- Programme conséquent.

```
> Bezout2 := proc(x::nonnegint, u::posint, v::posint)
> local a, b, gcd ;
> gcd := igcdex(u, v, 'a', 'b') ;
> if gcd <> 1 then ERROR(
> sprintf("les nombres %a et %a
> ne sont pas premiers entre eux.",
> u, v))
> fi ;
> RETURN(x*a mod v, x*b mod u)
> end ;
> Bezout2(4, 6, 15) ;
```

```
Error, (in Bezout2) les nombres 6 et 15
ne sont pas premiers entre eux.
```

```
> Bezout2(4, 3, 5) ;
3, 2
> evalb(4 = 3 * 3 + 2 * 5 mod (3*5)) ;
true
```

- Le même résultat est valide pour les polynômes à coefficients dans un corps, sous une forme encore plus confortable.

PROPOSITION B.5.2 *Si U et V sont deux polynômes de degrés respectifs m et n , premiers entre eux, alors pour tout polynôme P de degré $< m + n$, il existe un unique polynôme A (resp. B) de degré $< n$ (resp. $< m$) tel que $P = AU + BV$.*

- La démonstration est la même mais un examen de degrés montre qu'on peut même se dispenser de l'imprécision «modulo UV ». Le programme conséquent suit.

```

> Bezout3 := proc(P::polynom(rational, X),
> U::polynom(rational, X),
> V::polynom(rational, X))
> local gcd, A, B ;
> gcd := gcdex(U, V, X, 'A', 'B') ;
> if gcd <> 1 then ERROR(
> sprintf("les polynômes %a et %a
> ne sont pas premiers entre eux.",
> U, V))
> fi ;
> RETURN(rem(P*A, V, X), rem(P*B, U, X))
> end :
> _seed := 1925 :
> P, U, V := rndP(5), rndP(3), rndP(3) ;
> P, U, V := X5 + 5X4 + 6X3 + 2X2 + 6X + 2, X3 + X2 + X + 6, X3 + 2X2 + 3
> A, B := Bezout3(P, U, V) ;
> A, B :=  $\frac{1}{6} - \frac{7}{18}X^2 - \frac{2}{3}X, \frac{25}{18}X^2 + \frac{59}{18}X + \frac{1}{3}$ 
> expand(P - A*U - B*V) ;
0

```

- Ceci est valable quel que soit le corps, par exemple Z_7 , mais il faut adapter la procédure.

```

> 'type/Z7' := proc(obj::anything)
> RETURN(type(obj, And(integer, Range(-1, 7))))
> end :
> type(3, Z7), type(-3, Z7) ;
true, false
> Bezout4 := proc(P::polynom(Z7, X),
> U::polynom(Z7, X),
> V::polynom(Z7, X))
> local gcd, A, B ;
> gcd := Gcdex(U, V, X, 'A', 'B') mod 7 ;
> if gcd <> 1 then ERROR(
> ### WARNING: %x or %X format should be %y or %Y if used with
> floating point arguments
> ### WARNING: incomplete string; use " to end the string
> sprintf("les polynômes %a et %a
> ne sont pas premiers entre eux.",
> U, V))
> fi ;
> RETURN(Rem(P*A, V, X) mod 7, Rem(P*B, U, X) mod 7)
> end :

```

- On prend les mêmes polynômes, mais l'interprétation est différente.

```

> A, B := Bezout4(P, U, V) ;
> A, B := 4X + 6, X2 + 6X + 5
> Expand(P - A*U - B*V) mod 7 ;
0

```

- Un énoncé équivalent est obtenu pour des polynômes à coefficients entiers, à condition de faire intervenir une égalité « modulo p » pour un premier p . Cet énoncé va pouvoir être généralisé au cas p^k où le quotient Z/p^k n'est plus un corps.

PROPOSITION B.5.3 : soient U et V des polynômes unitaires à coefficients entiers dans $[0, p]$, p -premiers entre eux, de degrés respectifs m et $n > 0$. Alors pour tout polynôme P de degré $< m + n$, il existe des polynômes uniques A et B , à coefficients entiers dans $[0, p]$, de degrés respectifs $< n$ et $< m$, et un polynôme R de degré $< m + n$, tels que $P = AU + BV + pR$.

Il suffit en effet d'appliquer le résultat précédent, mais quand on finit le calcul, il n'est exact que modulo p . Il n'y a rien à changer à la procédure **Bezout4**, seule la fin de la vérification est différente.

```
> R := expand(P - A*U - B*V) / 7 ;
```

$$R := -X^4 - 3X^3 - 3X^2 - 6X - 7$$

- On énonce maintenant un résultat analogue modulo p^k . Cette fois l'anneau des polynômes à coefficients modulo p^k n'est plus principal, car il n'est même pas intègre. On se place donc dans une situation où on suppose donnée une relation de Bezout entre U et V .

PROPOSITION B.5.4 Soient U et V deux polynômes unitaires à coefficients entiers dans $[0, p^k]$, de degrés respectifs m et n . On suppose donnée une relation de Bezout : $1 = AU + BV + p^k C$ où le degré de A (resp. B, C) est $< n$ (resp. $< m, < m + n$). Alors, pour tout polynôme P à coefficients entiers de degré $< m + n$, il existe des polynômes uniques E (resp. F, G), de degré $< n$ (resp. $< m, < m + n$), à coefficients entiers dans $[0, p^k]$, (resp. dans $[0, p^k]$, entiers), tels que $P = EU + FV + p^k G$.

DÉMONSTRATION. Analogue avec les adaptations évidentes. Prendre $E = PA$ et $F = PB$ est tentant, mais les degrés sont trop grands. Comme V est unitaire, on peut diviser PA par V pour obtenir un reste à coefficients entiers E qu'on réduit modulo p^k : $PA = QV + E + p^k R$, et de même on divise PB par U pour obtenir $PB = SU + F + p^k T$. En reportant dans $P = PAU + PBV + p^k PC$, il vient $P = EU + FV + (Q + S)UV + p^k(PC + RU + TV)$. La réduction modulo p^k de tous les termes laisse un polynôme UV unitaire de degré $m + n$. Comme $P - EU - FV$ est de degré $< m + n$, il en résulte que le polynôme $Q + S$ est nul modulo p^k ; on peut donc « glisser » le terme $(Q + S)UV$ dans le facteur de p^k et finalement le degré résultant est nécessairement $< m + n$. Si on avait deux solutions différentes, on déduirait une relation $EU + FV = p^k R$; en multipliant par A , il vient $E AU + F AV = p^k AR$ ou, compte tenu de la relation presque-Bezout, $E - EB V + F AV = p^k (AR + EC)$. Mais si on réduit modulo p^k , E devient divisible par V , ce qui est incompatible avec V unitaire et degré de $E <$ degré de V , à moins que E soit nul. CQFD.

```
> Bezout5 := proc
> (p::posint, k::posint, P::polynom(integer, X),
> U::polynom(integer, X), V::polynom(integer, X),
> A::polynom(integer, X), B::polynom(integer, X))
> RETURN(Rem(P*A, V, X) mod p^k, Rem(P*B, U, X) mod p^k)
> end ;
```

- On redéfinit **rndP** pour que l'entier modulaire soit libre.

```
> rndP := proc(p::posint, d::posint)
> local rnd ;
> rnd := rand(0..(p-1)) ;
> RETURN(sort(X^d + add(rnd()*X^i, i=0..(d-1))))
> end ;
> _seed := 2210 ;
> p, k := 7, 2 ; U, V := seq(rndP(49, 3), i=1..2) ;
```

$$p, k := 7, 2$$

```

      U, V := X^3 + 43 X^2 + 28 X + 48, X^3 + 18 X^2 + 12 X + 24
> Gcdex(U, V, X, 'A', 'B') mod 49 ;
      1
> sort(expand(1-A*U-B*V)/49) ;
      -X^5 - 38 X^4 - 63 X^3 - 85 X^2 - 56 X - 23
> P := rndP(49, 5) ;
      P := X^5 + 22 X^4 + 26 X^3 + 11 X^2 + 39 X + 4
> E, F := Bezout5(7, 2, P, U, V, A, B) ;
      E, F := 43 X^2 + 22 X + 19, 7 X^2 + 34 X + 3
> expand(P-E*U-F*V)/49 ;
      -X^5 - 41 X^4 - 58 X^3 - 84 X^2 - 49 X - 20

```

- Nous pouvons maintenant énoncer le *lemme de Hensel* pour les polynômes modulo une puissance de nombre premier.

PROPOSITION B.5.5 (lemme de Hensel) : *On suppose qu'on dispose de deux relations :*

$$P = UV + p^k R; \quad 1 = AU + BV + p^k S;$$

où les degrés de U (resp. V, P, R, A, B, S) sont m (resp. $n, m+n, < m+n, < n, < m, < m+n$). Par ailleurs P, U et V sont supposés unitaires, et les coefficients de A, U, B et V sont des entiers dans $[0, p^k[$. Alors il existe $U_0, V_0, R_0, A_0, U_0, B_0, V_0$ et S_0 vérifiant les mêmes conditions à ceci près que p^k doit être remplacé par $p^{(2k)}$. De plus U_0, V_0, A_0 et B_0 sont uniques. Il en résulte la même propriété pour R_0 et S_0 .

DÉMONSTRATION. On pose $U_0 = U + p^k U_1$ et de même pour V, A et B . En reportant dans les équations à satisfaire et en réduisant modulo $p^{(2k)}$, il vient les équations suivantes.

$$R = (V_1 U + U_1 V) \bmod p^k$$

;

$$S - AU_1 - BV_1 = (A_1 U + B_1 V) \bmod p^k$$

. On va donc trouver les correctifs d'indice 1 par application de **Bezout5**. CQFD.

```

> Hensel := proc
> (p::posint, k::posint, P::polynom(integer, X),
> U::polynom(integer, X), V::polynom(integer, X),
> A::polynom(integer, X), B::polynom(integer, X))
> local R, S, U1, V1, A1, B1 ;
> R := expand(P - U*V)/p^k ;
> S := expand(1 - A*U - B*V)/p^k ;
> if not type(R, polynom(integer, X)) then
> ERROR("P, U, V not coherent for Hensel.")
> fi ;
> if not type(S, polynom(integer, X)) then
> ERROR("A, U, B, V not coherent for Hensel.")
> fi ;
> V1, U1 := Bezout5(p, k, R, U, V, A, B) ;
> A1, B1 := Bezout5(p, k, S-A*U1-B*V1, U, V, A, B) ;
> RETURN(p, 2*k, P, sort(U+p^k*U1), sort(V+p^k*V1),
> sort(A+p^k*A1), sort(B+p^k*B1))
> end ;

```

- On a maintenant l'outil ad hoc pour augmenter très vite l'entier modulaire par rapport auquel on effectue une factorisation de polynômes à coefficients entiers. On trouve ainsi assez vite une factorisation éventuelle pour un polynôme à coefficients entiers, ou au contraire son irréductibilité.

```
> _seed := 1713 ;
> P := rndP(10, 10) ;
> RootsSup(P) ;
```

_seed := 1713

$$P := X^{10} + 4X^9 + 8X^8 + 2X^7 + 9X^6 + 3X^5 + 4X^4 + X^3 + 9X^2 + 5X + 8.$$

```
> fs := Berl(11, P) ;
```

$$fs := [X^2 + 4X + 2, X^8 + 6X^6 + 8X^4 + 4X^3 + 5X^2 + 6X + 8]$$

- Deux facteurs, c'est la situation idéale pour Hensel. Il faut préparer les données.

```
> U, V := op(fs) ;
```

$$U, V := X^2 + 4X + 2, X^8 + 6X^6 + 8X^4 + 4X^3 + 5X^2 + 6X + 8$$

```
> Gcdex(U, V, X, 'A', 'B') mod 11 ;
```

1

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
```

$$X^2 + 92X + 68$$

$$X^8 + 33X^7 + 50X^6 + 55X^5 + 19X^4 + 81X^3 + 93X^2 + 94X + 41$$

- Le facteur de degré 2 n'est pas possible, car il devrait être $X^2 - 29X + \dots$ mais ceci est incompatible avec la majoration par 8 des racines. Vérification.

```
> irreduc(P) ;
```

true

- Considérons comme plus haut un cas certainement factorisable.

```
> _seed := 16 ;
> P := sort(expand(rndP(5,4)*rndP(5,6))) ;
> RootsSup(P) ;
```

$$P := X^{10} + 2X^8 + 4X^7 + 2X^6 + 12X^5 + 4X^4 + 16X^3 + 8X^2 + 8X + 8$$

3.287503660

```
> fs := Berl(11, P) ;
```

$$fs := [X + 4, X^4 + 2X^2 + 2, X^5 + 7X^4 + 5X^3 + 6X^2 + 9X + 1]$$

- Une racine est majorée par 3.3 et $X + 4$ ne peut pas venir d'un Z -facteur. Regroupons les deux premiers facteurs.

```
> U := Expand(fs[1]*fs[2]) mod 11 ; V := fs[3] ;
```

$$U := X^5 + 2X^3 + 2X + 4X^4 + 8X^2 + 8$$

$$V := X^5 + 7X^4 + 5X^3 + 6X^2 + 9X + 1$$

```
> Gcdex(U, V, X, 'A', 'B') mod 11;
```

1

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
      X5 + 70 X4 + 2 X3 + 19 X2 + 2 X + 19
      X5 + 51 X4 + 60 X3 + 39 X2 + 53 X + 45
```

• Mais les coefficients de X^4 sont impossibles. On essaie l'autre combinaison.

```
> U := Expand(fs[1]*fs[3]) mod 11 ; V := fs[2] ;
      U := X6 + 4 X3 + 4 X + 4
      V := X4 + 2 X2 + 2
```

```
> Gcdex(U, V, X, 'A', 'B') mod 11;
```

1

```
> p,k,P,U,V,A,B := Hensel(11,1,P,U,V,A,B) : U ; V ;
      X6 + 4 X3 + 4 X + 4
      X4 + 2 X2 + 2
```

• Cette fois les facteurs potentiels restent curieusement constants. Continuons.

```
> p,k,P,U,V,A,B := Hensel(11,2,P,U,V,A,B) : U ; V ;
      X6 + 4 X3 + 4 X + 4
      X4 + 2 X2 + 2
```

```
> p,k,P,U,V,A,B := Hensel(11,4,P,U,V,A,B) : U ; V ;
      X6 + 4 X3 + 4 X + 4
      X4 + 2 X2 + 2
```

• Cette fois il s'agit d'une factorisation certaine modulo :

```
> 11^8 ;
      214358881
```

• On est donc certain d'avoir une vraie factorisation entière, qu'on aurait pu essayer plus vite. Vérification.

```
> factor(P) ;
      (X4 + 2 X2 + 2) (X6 + 4 X3 + 4 X + 4)
```

• Jouons à trouver ainsi des factorisations élevées de $X^4 + 1$;

```
> P := X^4+1 ;
      P := X4 + 1
> Berl(3, P) ;
      [X2 + 2 X + 2, X2 + X + 2]
```

```
> U,V := op(%);
> Gcdex(U,V,X,'A','B') mod 3 ;
> p,k := 3, 1 ;
```

```
      U, V := X2 + 2 X + 2, X2 + X + 2
      1
```



```

> for i from 1 to 6 do
>   p, k := 3, 1
>   p, k, P, U, V, A, B := Hensel(p, k, P, U, V, A, B)
>   od :
>   k, p^k ; U ; V ;
64, 3433683820292512484657849089281
X2 + 1352955588233944339554610415792 X + 3433683820292512484657849089280
X2 + 2080728232058568145103238673489 X + 3433683820292512484657849089280

```

C Annexe : Systèmes linéaires dans $\text{GF}(p^d)$ (F. SERGERAERT)

> restart ;

- Exemple dans $\text{GF}(3^4)$.

- On prend un polynôme irréductible de degré 4 dans F_3 , affecté à **irr34**.

> irr34 := op(1, select(has, Factor(x^4-x) mod 3, 4)) ;

$$\text{irr34} := x^4 + 2x^3 + 2x^2 + x + 2$$

- Le polynôme irréductible obtenu par ce procédé n'est pas forcément le même d'une session à l'autre.

- On aliasse α à une racine de ce polynôme dans une extension de F_3 , de sorte que $\text{GF}(3^4) = F_3[\alpha]$.

> alias(alpha = RootOf(irr34) mod 3) ;

α

- La procédure **rnd3** génère un entier modulo 3 pseudo-aléatoire.

> rnd3 := rand(0..2) ;

> seq(rnd3(), i = 1..5) ;

0, 2, 0, 2, 1

- La procédure **rnd34** génère un élément pseudo-aléatoire de $\text{GF}(3^4)$.

> rnd34 := () -> add(rnd3()*alpha^i, i=0..3) ;

> seq(rnd34(), i = 1..5) ;

$$2 + 2\alpha + 2\alpha^2 + \alpha^3, 1 + \alpha, 2 + 2\alpha + \alpha^2, 2\alpha^2, \alpha^2$$

- La matrice A est une matrice 3x3 pseudo-aléatoire à coefficients dans $\text{GF}(3^4)$.

> A := matrix(3, 3, rnd34) ;

$$A := \begin{bmatrix} 1 + 2\alpha^2 + 2\alpha^3 & 2 + 2\alpha + 2\alpha^3 & 2 + 2\alpha^2 + 2\alpha^3 \\ 2\alpha^2 & 2 + \alpha + \alpha^2 & 1 + \alpha^3 \\ 2 + 2\alpha + \alpha^3 & 1 + \alpha^2 & \alpha + 2\alpha^2 \end{bmatrix}$$

- Idem pour un vecteur second membre.

> b := vector(3, rnd34) ;

$$b := [\alpha^3, \alpha^3, 2 + 2\alpha^2]$$

- Linsolve(...) mod 3 permet de résoudre dans $\text{GF}(3^4)$.

> x := Linsolve(A,b) mod 3 ;

$$x := [\alpha^3 + 2\alpha^2 + 2, \alpha + \alpha^2, 2]$$

- Vérification. Calcul de $Ax - b$.

> zerov := evalm(A &* x - b) ;

$$\begin{aligned}
zerov := & \left[(1 + 2\alpha^2 + 2\alpha^3)(\alpha^3 + 2\alpha^2 + 2) + (2 + 2\alpha + 2\alpha^3)(\alpha + \alpha^2) + 4 + 4\alpha^2 + 3\alpha^3, \right. \\
& 2\alpha^2(\alpha^3 + 2\alpha^2 + 2) + (2 + \alpha + \alpha^2)(\alpha + \alpha^2) + \alpha^3 + 2, \\
& \left. (2 + 2\alpha + \alpha^3)(\alpha^3 + 2\alpha^2 + 2) + (1 + \alpha^2)(\alpha + \alpha^2) + 2\alpha + 2\alpha^2 - 2 \right]
\end{aligned}$$

- Les termes du vecteur obtenu ne sont pas « réduits » à leur forme canonique dans $\text{GF}(3^4) = F_3[\alpha]$. Pour obtenir la réduction.

```

> map(item -> Expand(item) mod 3, zerov) ;
      [0, 0, 0]

```

D Exercices de préparation à l'examen

D.1 EXAMEN du lundi 6 septembre 2004, 9h à 12h, à l'Institut Fourier

- I) On considère l'anneau quotient $A = \mathbb{Z}[X]/(X^2 - 5, 19)$.
- (a) Montrer que A est isomorphe à l'anneau quotient $B = \mathbb{F}_{19}[X]/(X^2 - 5)$.
 - (b) Trouver tous les idéaux premiers de A .
 - (c) Trouver tous les diviseurs de zéro de A .
 - (d) Trouver le nombre d'éléments inversibles de l'anneau A .
- II) Soit le polynôme $P(X) = X^6 + X^3 + 1$ de $\mathbb{F}_2[X]$.
- (a) Montrer que $P(X)$ est irréductible. Quel est son corps de rupture F ?
 - (b) On note α une racine de P dans F , et $\beta = \alpha^4 + \alpha^5$. Déterminer l'ordre de α dans le groupe F^* et calculer β^7 .
 - (c) Montrer que le plus petit sous-corps de F contenant α^3 est \mathbb{F}_4 .
 - (d) Déterminer les autres sous-corps de F , et donner la liste de leurs éléments en fonction de α ou β .
- III) On considère le corps fini \mathbb{F}_{71} .
- (a) Montrer que $\bar{7}$ est un générateur de \mathbb{F}_{71}^* .
 - (b) Calculer $\bar{7}^{-1}$ et $\bar{7}^{100}$ dans le corps \mathbb{F}_{71} .
 - (c) Combien l'équation $x^2 + x + \bar{20} = 0$ a-t-elle de solutions dans \mathbb{F}_{71} ?
- IV) On considère l'entier $n = pq$ où p et q sont premiers distincts, on note $d = \text{pgcd}(p - 1, q - 1)$. Pour tout entier $b \geq 1$, l'entier n est dit **pseudopremier de base b** si n est premier avec b et $b^{n-1} \equiv 1 \pmod{n}$.
Montrer que n est pseudopremier de base b si et seulement si on a $b^d \equiv 1 \pmod{n}$.
- b) Parmi les entiers b premiers à n compris entre 1 et n , quelle est la proportion des bases pour lesquelles n
 - c) Calculer cette proportion pour le nombre $n = 341$.

D.2 EXAMEN du 27 janvier 2004, de 14h à 17h, à l'Institut Fourier

I) Soit p un nombre premier impair.

(a) Dans $\mathbb{Z}/p\mathbb{Z}$, on pose $\overline{-1} = -1 \pmod{p}$. Montrer que $\overline{-1}$ est de la forme x^4 ($x \in \mathbb{Z}/p\mathbb{Z}$), si et seulement si $p \equiv 1 \pmod{8}$.

(b) On suppose $p \equiv 3 \pmod{8}$. Déterminer le symbole de Legendre $\left(\frac{-2}{p}\right)$.

(c) Factoriser le polynôme $X^4 + 1$ de $(\mathbb{Z}/11\mathbb{Z})[X]$ en irréductibles.

II) (a) Soit $\mathbb{Z}[i]$ le sous-anneau $\{a + bi \mid a, b \in \mathbb{Z}\}$ de \mathbb{C} . Montrer que $\mathbb{Z}[i]$ est euclidien.

(b) Résoudre le système linéaire suivant sur $\mathbb{Z}[i]$:

$$\begin{cases} (4+i)x_1 + (1+i)x_2 + (4+i)x_3 = 5 + 2i \\ 4x_1 + x_2 + 4x_3 = 5 \\ x_1 - 2x_2 + x_3 = -1. \end{cases}$$

III) (a) Construire un corps \mathbb{F}_9 de 9 éléments.

(b) Déterminer tous les éléments d'ordre donné dans le groupe multiplicatif \mathbb{F}_9^* .

(c) Trouver tous les points rationnels sur \mathbb{F}_9 de la conique projective

$$\mathcal{C} : X^2 + 2XY + 2Y^2 + Z^2 = 0$$

(d) Montrer que la courbe \mathcal{C} est rationnelle, et donner une paramétrisation de la courbe en coordonnées affines x, y telles que $X = xZ, Y = yZ$.

(e) La courbe \mathcal{C} est-elle lisse ?

IV) Soit le polynôme $P(X) = X^4 + X^2 - 1$ de $\mathbb{F}_3[X]$.

(a) Montrer que $P(X)$ est irréductible et qu'il existe une racine α de P dans \mathbb{F}_{81} .

(b) Soit $\beta = \alpha^2$. Montrer que $\beta \in \mathbb{F}_9$ est un générateur du groupe \mathbb{F}_9^* .

(c) Trouver l'ordre du polynôme P .

(d) Est-ce que $\alpha + \alpha^2$ engendre une base normale de \mathbb{F}_{81} ?

V) On considère avec les notations usuelles, une clef publique RSA :

$$(n, e) = (55, 3),$$

et soit $\mathcal{E} : x \mapsto x^e \pmod{n}$ l'application de cryptage de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

(a) Calculer la clef secrète d correspondante, telle que l'application $\mathcal{D} : y \mapsto y^d \pmod{n}$ soit réciproque de \mathcal{E} .

(b) On considère le message $m = 7$. Déterminer le message C obtenu en cryptant m avec la clef publique $\text{RSA}(n, e)$.

(c) Décrypter le message C avec la clef secrète d .

Références

Livres de base :

- [AF] JEAN-MARIE ARNAUDIÈS et HENRI FRAYSSE *Algèbre*, Dunod, Paris, 1987. xi+691 pp.
- [Dem] MICHEL DEMAZURE, *Cours d'algèbre. Primalité. Divisibilité. Codes.*, Nouvelle Bibliothèque Mathématique, 1. Cassini, Paris, 1997. xviii+302 pp.
- [God] ROGER GODEMENT, *Cours d'algèbre.*, Hermann, Paris, 1969
- [La] SERGE LANG, *Algebra*. Reading, Mass. : Addison–Wesley (1965).
- [Se70] J.– P. SERRE, *Cours d'arithmétique*. Paris, Press Univ. France, 1970.
- [VdW71] B.L. VAN DER WAERDEN, *Algebra I,II*, New York : Springer Verlag, 1971, 1967.

Livres supplémentaires :

- [BS85] BOREVICH, Z.I., SHAFAREVICH, I.R. *Number Theory*. Traduction anglaise. : New York/London : Academic Press, 1966.
- [Coh96] COHEN, H. *A course in computational algebraic number theory*. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1996. xii+534 pp. Third printing
- [Kob87] NEAL KOBLITZ, *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York : Springer Verlag, 1987.
- [Knu81] D.E. KNUTH *The art of computer programming*. Vol 2. Seminumerical algorithms. 2nd edition. Addison–Wesley, Reading (1981).
- [Li-Ni] RUDOLF LIDL et HARALD NIEDERREITER, *Introduction to finite fields and their applications*. Addison–Wesley : Reading, 1983
- [Ma-Pa] YU.I. MANIN et A.A.PANCHISHKIN, *Number Theory I : Introduction to Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49, Springer-Verlag, 1995, 303 p.
- [Mon88] D. MONASSE, *Mathématique et Informatique*. Classes préparatoires. Vuibert, 1988
- [Se70] J.– P. SERRE, *Cours d'arithmétique*. Paris : Presses Univ. France, 1970.
- [Ste] S. A. STEPANOV, *Codes on algebraic curves*. Kluwer Academic Publishers. vii, 350 p., 1999
- [T-MF] TENENBAUM G., MENDES-FRANCE, *Les nombres premiers*, Collection Que Sais-Je, Paris, Press Univ. France, 1997

Articles et autres sources :

- [AGP94] ALFORD W.-R. GRANVILLE A. POMERANCE C. *There are infinitely many Carmichael numbers*. Ann. Math. **139**, 703–722 (1994).
- [Bor03] BORNEMANN, F. *Primes is in P, une avancée accessible à "l'homme ordinaire"*. Gazette des Mathématiciens No 98, pp.14-30, Octobre 2003.
- [Le1] H.W.LENSTRA, JR., *Factoring integers with elliptic curves*, Ann. Math., 126, no. 3 (1987), 649-673
- [Pey] EMMANUEL PEYRE, *Corps finis et courbes elliptiques*. DESS Cryptologie, sécurité et codage d'information, Modules A1A et A1B, Grenoble, 2002, pp. 1-128
- [RSA] R. L. RIVEST, A. SHAMIR et L. M. ADLEMAN, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, CACM, 21,1978, 120–126

[Stein] WILLIAM STEIN, *An Explicit Approach to Number Theory* (à paraître, voir page internet : <http://modular.fas.harvard.edu/edu/Fall2001/124/lectures>).