TD
Structures algébriques

Exercices d'application du cours

Exercice 1 ◩□□ Un exemple à avoir en tête

Trouver un exemple, à garder en tête,

- d'un groupe non commutatif,
- d'un anneau commutatif non intègre,
- d'un anneau intègre non commutatif,
- d'un corps non commutatif,
- d'un anneau avec aucun élément inversible pour la loi '$\times$' autres que son élément neutre et l'opposé de son neutre,
- d'un endomorphisme de groupes ni injectif, ni surjectif,
- d'un morphisme d'anneau surjectif mais pas injectif,
- d'un morphisme d'anneau injectif, mais pas surjectif

▶ Indication ▶ Correction

Exercice 2 ◩□□

Soient G un groupe et E est un ensemble. Dire si H est un sous-groupe du groupe G,

(1) $G = (\mathbb{Z}, +)$ et $H = \{$ nombres pairs $\}$.

(2) $G = (\mathbb{Z}, +)$ et $H = \{$ nombres impairs $\}$.

(3) $G = (\mathbb{R}^{\mathbb{R}}, +)$ et $H = \{$fonctions constantes sur $\mathbb{R}\}$.

(4) $G = (\mathbb{R}^*, \times)$ et $H = \mathbb{Q}^*$.

(5) $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$ et $H = \{f \in G \mid f(1) = 0\}$

▶ Indication ▶ Correction

Exercice 3 ◩□□ Conseil du coach

Soit $*$ la loi interne définie dans $\mathbb{R}$ par

$$\forall (x, y) \in \mathbb{R}^2, x * y = x + y + x^2 y^2$$

(1) Vérifier que $*$ est commutative.

(2) La loi $*$ est-elle associative ?

(3) Montrer que $\mathbb{R}$ admet un neutre pour $*$ et calculer ce neutre.

(4) Résoudre les deux équations suivantes, d'inconnue $x \in \mathbb{R}$

(4.a) $1 * x = 0$.

(4.b) $1 * x = 1$.

▶ Indication ▶ Correction

Exercice 4 ■□□ Conseil du coach On refait le cours

Soit A et B deux anneaux. Soit f un morphisme d'anneaux de A dans B. Soit A' un sous-anneau de A et B' un sous-anneau de B. Montrer que

(1) $f(A')$ est un sous-anneau de B.

(2) $f^{-1}(B')$ est un sous-anneau de A.

▶ Indication ▶ Correction

Exercice 5 ■ (A) ■ Une caractérisation des groupes

Soit G un ensemble muni d'une loi de composition interne associative notée $*$. On suppose qu'il existe $e \in G$ tel que

$$\forall x \in G \quad x * e = x \qquad \text{et} \qquad \forall x \in G \quad \exists x' \in G \quad x * x' = e$$

Montrer que $(G, *)$ est un groupe. ▶ Indication ▶ Correction

Exercice 6 ■ (A) ■ Une autre caractérisation des groupes

Soit G un ensemble non vide muni d'une loi associative $*$ telle que, pour tous $a, b \in G$, il existe $x \in G$ et $y \in G$ tels que $a * x = b$ et $y * a = b$.
Montrer que G est un groupe pour $*$. ▶ Indication ▶ Correction

Exercice 7 ◩□□

Parmi les ensembles suivants, lesquels sont, ou ne sont pas, des sous-espaces vectoriels?

(1) $E_1 = \left\{(x, y, z) \in \mathrm{R}^3 \mid x + y + 3z = 0\right\}$,

(2) $E_2 = \{(x,y,z) \in \mathrm{R}^3 \mid x+y+3z = 2\}$,

(3) $E_3 = \{(x,y,z,t) \in \mathrm{R}^4 \mid x = y = 2z = 4t\}$,

(4) $E_4 = \{(x,y) \in \mathrm{R}^2 \mid xy = 0\}$,

(5) $E_5 = \{(x,y) \in \mathrm{R}^2 \mid y = x^2\}$,

(6) $E_6 = \{(x,y,z) \in \mathrm{R}^3 \mid 2x+3y-5z = 0\} \cap \{(x,y,z) \in \mathrm{R}^3 \mid x-y+z = 0\}$,

(7) $E_7 = \{(x,y,z) \in \mathrm{R}^3 \mid 2x+3y-5z = 0\} \cup \{(x,y,z) \in \mathrm{R}^3 \mid x-y+z = 0\}$,

(8) $E_8 = \{P \in \mathbb{R}[X] \mid P(0) = P(2)\}$,

(9) $E_9 = \{P \in \mathbb{R}[X] \mid P'(0) = 2\}$,

(10) $E_{10} = \{P \in \mathbb{R}[X] \mid A \mid P\}$, pour $A \in \mathbb{R}[X]$ non-nul fixé,

(11) $\mathcal{D}$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ qui sont dérivables,

(12) L'ensemble des solutions de l'équation différentielle $y' + a(x)y = 0$, où $a \in \mathcal{D}$,

(13) L'ensemble des solutions de l'équation différentielle $y' + a(x)y = x$, où $a \in \mathcal{D}$.

▶ Indication ▶ Correction

Exercice 8 ■◩□ Conseil du coach

Soit E un espace vectoriel et soient F et G deux sous-espaces vectoriels de E. Montrer que $F \cup G$ est encore un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

▶ Indication ▶ Correction

Exercices techniques

Exercice 9 ■□□

On note $*$ la loi interne dans $G = \mathbb{C} \times \mathbb{R}$ définie, pour tous $(z,t),(z',t') \in G$ par

$$(z,t) * (z',t') = (z+z', t+t' + \mathrm{Im}\,(\bar{z}z'))\,.$$

Montrer que $(G,*)$ est un groupe. Est-il commutatif ? ▶ Indication ▶ Correction

Exercice 10 ◩□□

Soit $(A,+,\cdot)$ un anneau. On définit le centre C de A par

$$C = \{x \in A \mid \forall a \in A, ax = xa\}.$$

Montrer que C est un sous-anneau de A. ▶ Indication ▶ Correction

Exercice 11 ■□□

On note G l'ensemble des applications $f : [0+\infty[\longrightarrow [0+\infty[$, de classe C^1, telles que $f > 0, f(0) = 0, \lim_{x\to+\infty} f(x) = +\infty$.

(1) Montrer que $(G,\circ)$ est un groupe. Est-il commutatif?

(2) On note H l'ensemble des $f \in G$ telles que $\dfrac{f(x)}{x} \underset{x\to+\infty}{\to} 1$. Montrer que H est un sous-groupe de G et que $H \neq G$.

▶ Indication ▶ Correction

Exercice 12 ■◩□

Soit $(G,\cdot)$ un groupe. Démontrer que les parties suivantes sont des sous-groupes de G.

(1) $Z(G) = \{x \in G; \forall y \in G, xy = yx\}$;

(2) $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

(3) On suppose de plus que G est commutatif. On dit que x est un élément de torsion de G s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G.

▶ Indication ▶ Correction

Exercices "Comme en colle"

Exercice 13 ■□□

Soient $(G,\cdot)$ un groupe, H,K deux sous-groupes de G.
Montrer que $H\cup K$ est un sous-groupe de G si et seulement si $H\subset K$ ou $K\subset H$.
► Indication ► Correction

Exercice 14 ■■◩

Montrer que tout anneau intègre fini est un corps. ► Indication ► Correction

Exercice 15 ■■□

Deux groupes sont *isomorphes* s'il existe un isomorphisme entre les deux.
Montrer que les groupes $(\mathbb{Z},+)$ et $(\mathbb{Z}^2,+)$ ne sont pas isomorphes. ► Indication ► Correction

Exercice 16 ■□□

Soit $(G,+)$ un groupe commutatif. On note $\mathrm{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi '+' par,

$$f+g:\ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & f(x)+g(x)\ . \end{array}$$

Démontrer que $(\mathrm{End}(G),+,\circ)$ est un anneau. ► Indication ► Correction

Exercice 17 ■□□

Soit

$$A=\left\{\frac{m}{n}\ \middle|\ m\in\mathbb{Z}, n\in 2\mathbb{N}+1\right\}\ .$$

A est donc l'ensemble des rationnels à dénominateur impair.
Démontrer que $(A,+,\times)$ est un anneau. Quels sont ses éléments inversibles? ► Indication ► Correction

Exercice 18 ■□□

Soit $\mathbb{D}$ l'ensemble des nombres décimaux,

$$\mathbb{D}=\left\{\frac{n}{10^k}\ \middle|\ n\in\mathbb{Z}, k\in\mathbb{N}\right\}$$

Démontrer que $(\mathbb{D},+,\times)$ est un anneau. Quels sont ses éléments inversibles? ► Indication ► Correction

Exercice 19 ■■□

Soit A un anneau tel que $x^3=x$ pour tout $x\in A$.

1. Montrer que, pour tout $x\in A$, $6x=0_A$.
2. Soit $B=\{x\in A\mid 2x=0_A\}$ et $C=\{x\in A\mid 3x=0_A\}$. Montrer que $A=B+C$.

► Indication ► Correction

Exercice 20 ◩□□ Conseil du coach — Éléments nilpotents

Soit A un anneau. Un élément a de A est dit nilpotent si et seulement s'il existe $n\in\mathbb{N}^*$ tel que $a^n=0$.

1. Soit $(a,b)\in A^2$. Montrer que, si a est nilpotent et si $ab=ba$, alors ab est nilpotent.
2. Soit $a\in A$ nilpotent. Montrer que $1-a$ est inversible dans A et exprimer $(1-a)^{-1}$.
3. Soit $(a,b)\in A^2$. Montrer que, si a et b sont nilpotents et $ab=ba$, alors $a+b$ est nilpotent.

► Indication ► Correction

Exercice 21 ■◩□ Théorème de Lagrange

Soient $(G,\cdot)$ un groupe fini, H un sous-groupe de G, $\mathcal{R}$ la relation définie dans G par

$$x\mathcal{R}y \iff xy^{-1}\in H$$

On veut montrer

> Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence dans G.
2. Montrer que les classes d'équivalence modulo $\mathcal{R}$ ont toutes le même cardinal.
3. En déduire $\mathrm{Card}(G)=\mathrm{Card}(H)\times\mathrm{Card}(G/\mathcal{R})$.

► Indication ► Correction

Indications

Exercices d'application du cours

Indication pour l'exercice 1 **Un exemple à avoir en tête**

Essayez avec les exemples du cours

↶ retour à l'exercice 1

Indication pour l'exercice 2

On vérifie la caractérisation des sous-groupes.

↶ retour à l'exercice 2

Indication pour l'exercice 3 **Conseil du coach**

On vérifie les définitions tranquillement.

↶ retour à l'exercice 3

Indication pour l'exercice 4 **Conseil du coach** **On refait le cours**

On vérifie la caractérisation.

↶ retour à l'exercice 4

Indication pour l'exercice 5 **Une caractérisation des groupes**

Il suffit de montrer que l'inverse à gauche est aussi l'inverse à droite et la même chose pour le neutre.

↶ retour à l'exercice 5

Indication pour l'exercice 6 **Une autre caractérisation des groupes**

↶ retour à l'exercice 6

Indication pour l'exercice 7

↶ retour à l'exercice 7

Indication pour l'exercice 8 **Conseil du coach**

Le sens indirect est immédiat. Le sens direct est une preuve ensembliste *"On prend un élément de F et on montre qu'il appartient à G."*.

↶ retour à l'exercice 8

Exercices techniques

Indication pour l'exercice 9

On montre tranquillement tous les axiomes d'un groupe.

↶ retour à l'exercice 9

Indication pour l'exercice 10

Caractérisation d'un sous-anneau ! Go !

↶ retour à l'exercice 10

Indication pour l'exercice 11

On vérifie les axiomes d'un groupe tranquilement.
Caractérisation d'un sous-groupe ! Go !

↶ retour à l'exercice 11

Indication pour l'exercice 12

Caractérisation d'un sous-groupe !

retour à l'exercice 12

Exercices "Comme en colle"

Indication pour l'exercice 13

La preuve indirect est immédiate. La preuve directe demande un peu de travail et une preuve ensembliste *"On prend un élément de F et on montre qu'il appartient à G."*.

retour à l'exercice 13

Indication pour l'exercice 14

Essayer d'arriver à avoir un inverse à gauche et un à droite de a, puis à montrer que ces deux inverses sont les mêmes.

retour à l'exercice 14

Indication pour l'exercice 15

Par l'absurde évidemment. Utilisez les antécédents de $(1,0)$ et de $(0,1)$.

retour à l'exercice 15

Indication pour l'exercice 16

Même si cela fait peur, on vérifie tranquillement les axiomes d'un anneau.

retour à l'exercice 16

Indication pour l'exercice 17

Même si cela fait peur, on vérifie tranquillement les axiomes d'un anneau.

retour à l'exercice 17

Indication pour l'exercice 18

Même si cela fait peur, on vérifie tranquillement les axiomes d'un anneau.

retour à l'exercice 18

Indication pour l'exercice 19

binôme binôme...
On se souviendra du théorème de bézout (ou de l'algorithme d'euclide étendu).

retour à l'exercice 19

Indication pour l'exercice 20 — Conseil du coach — Éléments nilpotents

On aura besoin de la somme d'une suite géométrique.

retour à l'exercice 20

Indication pour l'exercice 21 — Théorème de Lagrange

retour à l'exercice 21

Corrections

Exercices d'application du cours

Correction de l'Exercice 1 Un exemple à avoir en tête

retour à l'exercice 1

Correction de l'Exercice 2

retour à l'exercice 2

Correction de l'Exercice 3 Conseil du coach

(1) On a, pour tout $(x,y) \in \mathbb{R}^2$

$$y * x = y + x + y^2x^2 = x + y + x^2y^2 = x * y$$

donc $*$ est commutative.

(2) On a, par exemple :

$$\begin{aligned}(1*1)*(-1) &= \left(1+1+1^2 1^2\right)*(-1) = 3*(-1)\\ &= 3+(-1)+3^2(-1)^2 = 11\\ 1*(1*(-1)) &= 1*\left(1+(-1)+1^2(-1)^2\right) = 1*1\\ &= 1+1+1^2 1^2 = 3 \neq 11\end{aligned}$$

donc $*$ n'est pas associative.

(3) On a, pour tout $x \in \mathbb{R}$: $0 * x = x * 0 = 0$, donc $\mathbb{R}$ admet un neutre pour $*$ et ce neutre est 0 .

(4) On a, pour tout $x \in \mathbb{R}$

$$1 * x = 0 \iff 1 + x + x^2 = 0$$

et cette équation du second degré n'a pas de solution dans $\mathbb{R}$ puisque son discriminant $\Delta = 1 - 4 = -3$ est < 0. On conclut que l'équation $1 * x = 0$ n'a pas de solution dans $\mathbb{R}$.

(5) On a, pour tout $x \in \mathbb{R}$

$$\begin{aligned}1 * x = 1 &\iff 1 + x + x^2 = 1 \iff x^2 + x = 0\\ &\iff (x = -1 \text{ ou } x = 0).\end{aligned}$$

On conclut que l'équation $1 * x = 1$ admet exactement deux solutions dans $\mathbb{R}$, les réels -1 et 0 .

retour à l'exercice 3

Correction de l'Exercice 4 Conseil du coach On refait le cours

(1) L'ensemble A' est un sous-groupe de $(A,+)$ et f est un morphisme de groupes donc $f(A')$ est un sous-groupe de $(B,+)$. Par ailleurs, $1_A \in A'$ et $f(1_A) = 1_B$ donc $1_B \in f(A')$. Enfin, soit $(x,y) \in f(A')^2$. On choisit $(a,b) \in A'^2$ tel que $x = f(a)$ et $y = f(b)$. Alors $ab \in A'$ et $f(ab) = f(a)f(b) = xy$ donc $xy \in f(A')$.

(2) Comme précédemment, $f^{-1}(B')$ est un sous-groupe de $(A,+)$.
Ensuite, $f(1_A) = 1_B \in B'$ donc $1_A \in f^{-1}(B')$. Enfin, soit $(a,b) \in f^{-1}(B')$. Alors $(f(a), f(b)) \in B'^2$ donc $f(ab) = f(a)f(b) \in B'$ puis $ab \in f^{-1}(B')$.

retour à l'exercice 4

Correction de l'Exercice 5 Une caractérisation des groupes

Vérifions que e est élément neutre de $(G,*)$ et que tout élément de G est symétrisable. Soit $x \in G$. On a déjà $xe = x$ par hypothèse. Choisissons $x' \in G$ tel que $xx' = e$. Enfin, choisissons $x'' \in G$ tel que $x'x'' = e$. On montre d'abord que $x'x = e$, relation qui servira pour montrer que $ex = x$ et conclure que e est le neutre de $(G,*)$ et x' le symétrique de x :

$$x'x = x'xe = x'x(x'x'') = x'(xx')x'' = x'ex'' = x'x'' = e.$$

On poursuit nos calculs : $ex = xx'x = xe = x$. Donc G est un groupe.

retour à l'exercice 5

Correction de l'Exercice 6 Une autre caractérisation des groupes

Comme $\star$ est associative, il suffit d'établir l'existence d'un élément neutre e puis de montrer que tout élément de G admet un symétrique.
Soit $a \in G$ (qui existe car G est non vide). D'après le premier point, il existe $e \in G$ tel

que $a \star e = a$. Pour tout $b \in G$, il existe d'après le second point, un élément $y \in G$ tel que $b = y \star a$. Alors,

$$b \star e = (y \star a) \star e = y \star (a \star e) = y \star a = b$$

On montre de même (en inversant l'ordre d'utilisation des deux propriétés) qu'il existe un élément $e' \in G$ tel que, pour tout $b \in G, e' \star b = b$. Mais alors, en utilisant ces deux propriétés tour à tour,

$$e' = e' \star e = e$$

Ainsi, e est l'élément neutre de $\star$.
Soit $a \in G$. D'après les propriétés, il existe des éléments $x, y \in G$ tels que $a \star x = y \star a = e$. Alors,

$$x = e \star x = (y \star a) \star x = y \star (a \star x) = y \star e = y.$$

Cet élément $x = y$ est donc le symétrique de a pour $\star$.

↶ retour à l'exercice 6

Correction de l'Exercice 7

(1) Soient $X = (x, y, z)$ et $X' = (x', y', z')$ éléments de E_1. Alors, $X + X' = (x + x', y + y', z + z')$ est aussi élément de E_1. En effet,

$$(x + x') + (y + y') + 3(z + z') = (x + y + 3z) + (x' + y' + 3z') = 0$$

De même, pour tout $\lambda \in \mathbb{R}$, on a $\lambda X = (\lambda x, \lambda y, \lambda z)$ est élément de E_1 puisque

$$\lambda x + \lambda y + 3\lambda z = \lambda(x + y + 3z) = 0$$

E_1 est donc un sous-espace vectoriel de $\mathbb{R}^3$.

(2) E_2 n'est pas un sous-espace vectoriel de $\mathbb{R}^3$ car $\overrightarrow{0} = (0, 0, 0)$ n'est pas élément de E_2.

(3) Soient $X = (x, y, z, t)$ et $X' = (x', y', z', t')$ deux éléments de E_3. Alors $X + X' = (x + x', y + y', z + z', t + t')$ est aussi élément de E_3. En effet,

$$x + x' = y + y' = 2z + 2z' = 2(z + z') = 4t + 4t' = 4(t + t')$$

De même, on prouve que pour tout $\lambda \in \mathbb{R}, \lambda X$ est élément de E_3.E_3 est donc un sous-espace vectoriel de $\mathbb{R}^4$.

(4) E_4 n'est pas un sous-espace vectoriel de $\mathbb{R}^2$ car il n'est pas stable par addition. En effet, $X = (1, 0)$ et $Y = (0, 1)$ sont tout les deux éléments de E_4, mais $X + Y = (1, 1)$ n'est pas élément de E_4.

(5) Les éléments $(1, 1)$ et $(-1, 1)$ sont éléments de E_5. Si on effectue leur somme, on trouve $(0, 2)$ qui n'est pas élément de E_5 : E_5 n'est pas un sous-espace vectoriel de $\mathbb{R}^2$. Plus généralement, un sous-espace vectoriel de $\mathbb{R}^2$ est une droite passant par $(0, 0)$, ou $\mathbb{R}^2$ lui-même, ou encore le singleton $\{(0, 0)\}$. E_5 est une parabole et n'est donc pas un sous-espace vectoriel.

(6) Posons $F = \{(x, y, z) \in \mathbb{R}^3; 2x + 3y - 5z = 0\}$ et $G = \{(x, y, z) \in \mathbb{R}^3; x - y + z = 0\}$. Comme à la première question, on montre que F et G sont deux sous-espaces vectoriels de $\mathbb{R}^3$. Leur intersection $F \cap G$ est donc un sous-espace vectoriel de $\mathbb{R}^3$.

(7) Cette fois, aucun théorème du cours ne dit qu'une réunion de deux sous-espaces vectoriels reste un sous-espace vectoriel. Ici, prenons $(5, 0, 2) \in F \subset F \cup G$ et $(1, 1, 0) \in G \subset F \cup G$. Alors $(5, 0, 2) + (1, 1, 0) = (6, 1, 2)$ n'est pas élément de F car $12 + 3 - 10 = 5 \neq 0$, et il n'est pas non plus élément de G car $6 - 1 + 2 = 7 \neq 0$. Ainsi, $F \cup G$ n'est pas stable par addition et n'est donc pas un sous-espace vectoriel de $\mathbb{R}^3$. Plus généralement, on prouve qu'une réunion de deux sous-espaces vectoriels est un sous-espace vectoriel si et seulement si l'un des deux est inclus dans l'autre.

(8) On va prouver que E_8 est un sous-espace vectoriel de $\mathbb{R}[X]$. Remarquons d'abord que le polynôme nul est un élément de E_8. Ensuite, prenons P et Q deux éléments de E_8, et $\lambda \in \mathbb{R}$. Alors $(P + Q)(0) = P(0) + Q(0) = P(2) + Q(2) = (P + Q)(2)$ et donc $P + Q \in E_8$. De même, $(\lambda P)(0) = \lambda \times P(0) = \lambda \times P(2) = (\lambda P)(2)$ et donc $\lambda P \in E_8$. Ceci prouve le résultat annoncé.

(9) E_9 n'est pas un espace vectoriel car le polynôme nul n'est pas élément de E_9. Donc E_9 n'est pas un sous-espace vectoriel.

(10) Remarquons que $E_{10} = \{AQ; Q \in \mathbb{R}[X]\}$. Soient $P_1 = AQ_1$ et $P_2 = AQ_2$ deux éléments de E_{10}, et soit également $\lambda \in \mathbb{R}$. Alors $P_1 + P_2 = A(Q_1 + Q_2) \in E_{10}$ et $\lambda P_1 = A(\lambda Q_1) \in E_{10}$, ce qui prouve que E_{10} est un sous-espace vectoriel de $\mathbb{R}[X]$.

(11) On sait que la somme de deux fonctions dérivables est une fonction dérivable, et que le produit d'une fonction dérivable par un scalaire est une fonction dérivable. Par conséquent, $\mathcal{D}$ est un sous-espace vectoriel de l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.

(12) Remarquons d'abord que cet espace est une partie de $\mathcal{D}$. Soient y_1, y_2 deux solutions et $\lambda \in \mathbb{R}$. Posons $y = y_1 + \lambda y_2$. Alors

$$y' + a(x)y = (y_1' + a(x)y_1) + \lambda(y_2' + a(x)y_2) = 0$$

ce qui prouve que y est bien dans cet espace. Ainsi, c'est un sous-espace vectoriel de $\mathcal{D}$.

(13) Ce n'est pas un espace vectoriel car 0 n'est pas solution de l'équation différentielle.

↶ retour à l'exercice 7

Correction de l'Exercice 8 — Conseil du coach

Bien sûr, si $F \subset G, F \cup G = G$ est un sous-espace vectoriel ce qui prouve une implication. Réciproquement, supposons que $F \cup G$ est un sous-espace vectoriel de E et que pourtant F n'est pas inclus dans G et G n'est pas inclus dans F. Prenons x dans $F \backslash G$ et y dans $G \backslash F$. Alors, puisque $F \cup G$ est un sous-espace vectoriel, il est stable par addition et donc $x+y \in F \cup G$. Mais, si $x+y$ est dans F , alors $y = (x+y) - x \in F$ (car F est un sev) ce qui n'est pas le cas. De même, si $x+y$ est dans G, alors $x = (x+y) - y \in G$ ce qui est impossible. On obtient donc une contradiction et l'autre implication.

↶ retour à l'exercice 8

Exercices techniques

Correction de l'Exercice 9

Remarquer d'abord que $*$ est bien une loi interne dans

$$G = \mathbb{C} \times \mathbb{R}$$

(1) Associativité On a, pour tous $(z,t),(z',t'),(z'',t'') \in G$

$$\begin{aligned}
&((z,t)*(z,t))*(z'',t'')\\
&= (z+z', t+t'+\operatorname{Im}(\bar{z}z'))*(z'',t'')\\
&= ((z+z')+z'', (t+t'+\operatorname{Im}\bar{z}z')) + t'' + \operatorname{Im}\left(\left(\overline{z+z'}\right)z''\right)\\
&= \left(z+z'+z'', t+t'+t''+\operatorname{Im}(\bar{z}z')+\operatorname{Im}(\bar{z}z'')+\operatorname{Im}\left(\overline{z'}z''\right)\right)
\end{aligned}$$

et

$$\begin{aligned}
&(z,t)*((z',t')*(z'',t''))\\
&= (z,t)*\left(z'+z'', t'+t''+\operatorname{Im}\left(\overline{z'}z''\right)\right)\\
&= \left(z+(z'+z''), t+\left(t'+t''+\operatorname{Im}\left(\overline{z'}z''\right)\right)+\operatorname{Im}(\bar{z}(z'+z''))\right)\\
&= \left(z+z'+z'', t+t'+t''+\operatorname{Im}\left(\overline{z'}z''\right)+\operatorname{Im}(\bar{z}z')+\operatorname{Im}(\bar{z}z'')\right)
\end{aligned}$$

On a donc

$$((z,t)*(z',t'))*(z'',t'') = (z,t)*((z',t')*(z'',t''))$$

et on conclut que $*$ est associative.

(2) Neutre: On a, pour tout $(z,t) \in G$,

$$(z,t)*(0,0) = (z,t) \quad \text{et} \quad (0,0)*(z,t) = (z,t),$$

donc $(0,0)$ est neutre pour $*$.

③ Symétriques Soit $(z,t)\in G$. On a, pour tout $(z',t')\in G$

$$\begin{cases}(z,t)*(z',t')=(0,0)\\(z',t')*(z,t)=(0,0)\end{cases}$$
$$\iff\begin{cases}(z+z',t+t'+\operatorname{Im}(\bar{z}z'))=(0,0)\\(z'+z,t'+t+\operatorname{Im}(\overline{z'}z))=(0,0)\end{cases}$$
$$\iff\begin{cases}z+z'=0\\t+t'+\operatorname{Im}(\bar{z}z')=0\\t'+t+\operatorname{Im}(-|z|^2)=0\end{cases}\iff\begin{cases}z'=-z\\t+t'+\operatorname{Im}(-|z|^2)=0\\t'+t+\operatorname{Im}(\overline{z'}z)=0\end{cases}$$
$$\iff\begin{cases}z'=-z\\t+t'=0\end{cases}\iff\begin{cases}z'=-z\\t'=-t.\end{cases}$$

Ceci montre que (z,t) admet un symétrique (et un seul) et que ce symétrique est $(-z,-t)$. On conclut que $(G,*)$ est un groupe.

④ Commutativité : On a

$$\begin{cases}(1,0)*(\mathrm{i},0)=(1+\mathrm{i},0+0+\mathrm{i}(\bar{1}\mathrm{i}))\\\qquad\qquad=(1+\mathrm{i},1)\\(\mathrm{i},0)*(1,0)=(\mathrm{i}+1,0+0+\mathrm{i}(\bar{1}1))\\\qquad\qquad=(1+\mathrm{i},-1),\end{cases}$$

donc $(1,0)*(\mathrm{Im},0)\neq(\mathrm{Im},0)*(1,0)$, et on conclut que $(G,*)$ n'est pas commutatif.

retour à l'exercice 9

Correction de l'Exercice 10

- Rappelons que, par définition, C est un sous-anneau de A si et seulement si

$$\begin{cases}1)\ (C,+)\text{ est un sous-groupe de }(A,+)\\2)\ \forall x,y\in C, xy\in C\\3)\ 1\in C.\end{cases}$$

- $C\subset A$, évident.
  - $C\neq\varnothing$ car $0\in C$, puisque : $\forall a\in A, a0=0a(=0)$.
  - Soit $(x,y)\in C^2$. On a

$$\forall a\in A, a(x-y)=ax-ay=xa-ya=(x-y)a,$$

donc $x-y\in C$. Ceci montre que $(C,+)$ est un sous-groupe de $(A,+)$.

- Soit $(x,y)\in C^2$. On a

$$\begin{aligned}\forall a\in A,(xy)a=x(ya)=x(ay)=(xa)y\\=(ax)y=a(xy),\end{aligned}$$

donc $xy\in C$.

- On a $\forall a\in A,\quad 1a=a1(=a)$, donc $1\in C$. On conclut que C est un sous-anneau de A.

retour à l'exercice 10

Correction de l'Exercice 11

①
- Loi interne : Soit $(f,g)\in G^2$. Alors, $g\circ f:[0;+\infty[\longrightarrow[0;+\infty[$ existe, $g\circ f$ est de classe C^1 par composition, $(g\circ f)'=(g'\circ f)\,f'>0$ car $f'>0$ et $g'>0$, $(g\circ f)(0)=g(f(0))=g(0)=0$, et $g\circ f(x)\underset{x\to+\infty}{\longrightarrow}+\infty$, par composition de limites, puisque $f(x)\underset{x\to+\infty}{\longrightarrow}+\infty$ et $g(y)\underset{y\to+\infty}{\longrightarrow}+\infty$. Il en résulte $g\circ f\in G$ et donc $\circ$ est interne dans G.
- Associativité :
  La loi $\circ$ est associative dans l'ensemble des applications de $[0+\infty[$ dans $[0+\infty[$, donc $\circ$ est associative dans G.
- Neutre En notant $\varepsilon=\mathrm{Id}_{[0+\infty[}$, ε est une application de $[0;+\infty[$ dans $[0;+\infty[$, de classe C^1, $\varepsilon'=1>0$, $\varepsilon(0)=0$, $\varepsilon(x)=x\underset{x\to+\infty}{\longrightarrow}+\infty$, donc $\varepsilon\in G$. On a
$$\forall f\in G, f\circ\varepsilon=\varepsilon\circ f=f,$$
donc ε est neutre pour $\circ$ dans G.
- Symétriques :
  Soit $f\in G$. Comme $f'>0, f$ est strictement croissante sur l'intervalle $[0+\infty[$. Puisque f est continue, strictement croissante, que $f(0)=0$ et que $f(x)\underset{x\longrightarrow+\infty}{\longrightarrow}+\infty$, d'après le théorème de la bijection monotone, f est bijective, f^{-1} est continue, $f^{-1}(0)=0$ et $f^{-1}(x)\underset{x\to+\infty}{\longrightarrow}+\infty$. De plus, puisque f est de classe C^1 et que f' ne s'annule pas (car $f'>0$) , f^{-1} est de classe C^1 sur $[0;+\infty[$ et $\left(f^{-1}\right)'=\frac{1}{f'\circ f^{-1}}>0$. On déduit : $f^{-1}\in G$. Ainsi : $f^{-1}\in G$ et $f\circ f^{-1}=f^{-1}\circ f=\varepsilon$. On conclut que tout élément de G admet un symétrique pour la loi * dans G. D'après 1), 2), 3), 4), G est un groupe pour la loi o.

- Commutativité : Il est clair que les applications

$$f : [0;+\infty[\longrightarrow [0;+\infty[, x \longmapsto 2x$$
$$\text{et} \quad \varphi : [0;+\infty[\longrightarrow [0;+\infty[, x \longmapsto \mathrm{e}^x - 1$$

sont éléments de G. On a, pour tout $x \in [0;+\infty[$,

$$\begin{cases} (\varphi \circ f)(x) = \varphi(2x) = \mathrm{e}^{2x} - 1 \\ (f \circ \varphi)(x) = f\left(\mathrm{e}^x - 1\right) = 2\left(\mathrm{e}^x - 1\right) = 2\mathrm{e}^x - 2 \end{cases}$$

En particulier : $(\varphi \circ f)(1) = \mathrm{e}^2 - 1$ et $(f \circ \varphi)(1) = 2\mathrm{e} - 2$, donc $(\varphi \circ f)(1) \neq (f \circ \varphi)(1)$, d'où $\varphi \circ f \neq f \circ \varphi$. Ceci montre que G n'est pas commutatif.

(2)
- Il est clair que $H \subset G$, par définition de H.
- Le neutre ε de G est dans H car $\varepsilon(x) = x \underset{x\to+\infty}{\sim} x$.
- Soient $f, g \in H$. Remarquons que, puisque g est strictement croissante (car $g' > 0$ sur l'intervalle $[0;+\infty[$) et que $g(0) = 0$, on a $g(x) > 0$ pour tout $x > 0$. On a alors, pour $x > 0$

$$\frac{(g \circ f)(x)}{x} = \frac{g(f(x))}{f(x)} \cdot \frac{f(x)}{x} \underset{x\to+\infty}{\longrightarrow} 1 \cdot 1 = 1$$

donc $(g \circ f)(x) \underset{x\to+\infty}{\sim} x$, d'où $g \circ f \in H$.
- Soit $f \in H$. Comme $f^{-1}(x) \underset{x\longrightarrow+\infty}{\longrightarrow} +\infty$ et $y \underset{y\longrightarrow+\infty}{\sim} f(y)$, on a, par composition de limites : $f^{-1}(x) \underset{x\to+\infty}{\sim} f\left(f^{-1}(x)\right) = x$, d'où $f^{-1} \in H$. On conclut : H est un sous-groupe de G.
- L'application $f : [0;+\infty[\longrightarrow [0;+\infty[, x \longmapsto 2x$ est élément de G (cf. a) 5)), mais n'est pas élément de H, car $f(x) \underset{x\to+\infty}{\not\sim} x$. Ceci montre : $H \neq G$.

retour à l'exercice 11

Correction de l'Exercice 12

(1) e est élément de $Z(G)$ car $ey = ye = y$ pour tout $y \in G$. Soient $x_1, x_2 \in C(G)$. Alors, pour tout $y \in G$, on a

$$x_1x_2y = x_1\left(x_2y\right) = \left(x_1y\right)x_2 = yx_1x_2$$

et donc $x_1x_2 \in Z(G)$. Enfin, si $x \in Z(G)$, alors pour tout $y \in G$,

$$xy = yx \Longrightarrow xyx^{-1} = yxx^{-1} = y \Longrightarrow x^{-1}xyx^{-1} = x^{-1}y \Longrightarrow yx^{-1} = x^{-1}y$$

où on a multiplié à droite puis à gauche par x^{-1}. On en déduit que $x^{-1} \in Z(G)$ qui est donc un sous-groupe de G.

(2) Puisque H est un sous-groupe de $G, e \in H$ et donc $aea^{-1} \in aHa^{-1}$. Mais $aea^{-1} = e$ et donc $e \in aHa^{-1}$. Soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a

$$xy = aha^{-1}ah'a^{-1} = ahh'a^{-1} \in aHa^{-1}$$

puisque $hh' \in H$(H est un sous-groupe de G). Enfin, si on choisit $h' = h^{-1}$, le calcul précédent montre que

$$xy = yx = e$$

et donc $x^{-1} = y \in aHa^{-1}$ puisque $h^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G.

(3) Notons T l'ensemble des éléments de torsion de G. On a $e^1 = e$, donc $e \in T$. De plus, si $x, y \in T$, avec respectivement $x^n = e$ et $y^m = e$, il suffit de remarquer que

$$\left(y^{-1}\right)^m = \left(y^m\right)^{-1} = e^{-1} = e$$

puis d'utiliser le fait que x et y^{-1} commutent pour prouver que

$$\left(xy^{-1}\right)^{nm} = \left(x^n\right)^m \left(\left(y^{-1}\right)^m\right)^n = e$$

Ainsi, xy^{-1} est élément de T, et T est bien un sous-groupe de G.

retour à l'exercice 12

Exercices "Comme en colle"

Correction de l'Exercice 13

Si $H \subset K$ ou $K \subset H$, alors $H \cup K = K$ ou $H \cup K = H$, donc $H \cup K$ est un sous-groupe de G.
Réciproquement, supposons que $H \cup K$ soit un sous-groupe de G. Raisonnons par l'absurde : supposons $H \not\subset K$ et $K \not\subset H$. Il existe alors $a \in H$ tel que $a \notin K$, et il existe $b \in K$ tel que $b \notin H$. Puisque $H \cup K$ est un sous-groupe de G et que a et b sont dans $H \cup K$, on a $ab \in H \cup K$, c'est-à-dire : $ab \in H$ ou $ab \in K$.
- Supposons $ab \in H$. Comme $b = a^{-1}(ab)$, que $a \in H$ et $ab \in H$ et que H est un sous-groupe de G, on déduit $b \in H$, contradiction.
- Supposons $ab \in K$. Comme $a = (ab)b^{-1}$, que $b \in K$ et $ab \in K$ et que K est un sous-groupe de G, on déduit $a \in K$, contradiction. Ce raisonnement par l'absurde, montre : $H \subset K$ ou $K \subset H$.

retour à l'exercice 13

Correction de l'Exercice 14

Soient A un anneau intègre fini, $a \in A - \{0\}$. Puisque A est intègre, les applications $\gamma_a : A \underset{x \mapsto ax}{\longrightarrow} A$ et $\delta_a : A \underset{x \longmapsto ya}{\longrightarrow} A$ sont injectives, car :

$$\begin{aligned}\forall (x,y) \in A^2, (\gamma_a(x) = \gamma_a(y) &\iff ax = ay \\ &\iff a(x-y) = 0 \\ &\iff x - y = 0 \iff x = y)\end{aligned}$$

et de même pour δ_a.
Comme A est fini, il en résulte que γ_a et δ_a sont bijectives. En particulier, il existe $(b,c) \in A^2$ tel que $\gamma_a(b) = 1$ et $\delta_a(c) = 1$, c'est-à-dire tel que $ab = 1$ et $ca = 1$.
On a $c = c(ab) = (ca)b = b$, donc $\forall a \in A - \{0\}, \exists b \in A, ab = ba = 1$.
Tout élément de $A - \{0\}$ admet un inverse, et finalement A est un corps.

retour à l'exercice 14

Correction de l'Exercice 15

Raisonnons par l'absurde. Supposons qu'il existe un isomorphisme de groupes $f : (\mathbb{Z}, +) \longrightarrow \left(\mathbb{Z}^2, +\right)$. Notons $(a,b) = f(1)$.
- Puisque $(1,0) \in \mathbb{Z}^2$ et que f est bijectif, il existe $\lambda \in \mathbb{Z}$ tel que : $f(\lambda) = (1,0)$. On a alors, puisque f est un morphisme de groupes

$$(1,0) = f(\lambda) = \lambda f(1) = \lambda(a,b) = (\lambda a, \lambda b).$$

D'où : $\lambda a = 1$ et $\lambda b = 0$, et donc $\lambda \neq 0$ et $b = 0$.
- Puisque $(0,1) \in \mathbb{Z}^2$ et que f est bijective, il existe $\mu \in \mathbb{Z}$ tel que, $f(\mu) = (0,1)$. On a alors, puisque f est un morphisme de groupes

$$(0,1) = f(\mu) = \mu f(1) = \mu(a,b) = (\mu a, \mu b)$$

D'où, $\mu a = 0$ et $\mu b = 1$, et donc $\mu \neq 0$ et $a = 0$. On a alors, $f(1) = (a,b) = (0,0) = f(0)$, ce qui contredit l'injectivité de f. Ce raisonnement par l'absurde montre qu'il n'existe pas d'isomorphisme du groupe $(\mathbb{Z}, +)$ dans le groupe $\left(\mathbb{Z}^2, +\right)$, c'est-à dire que les groupes $(\mathbb{Z}, +)$ et $\left(\mathbb{Z}^2, +\right)$ ne sont pas isomorphes.

retour à l'exercice 15

Correction de l'Exercice 16

On remarque d'abord que $+$ et $\circ$ sont bien des lois de composition interne sur $\mathrm{End}(G)$. Ensuite, on vérifie tous les points de la définition d'un anneau.

- $(\mathrm{End}(G), +)$ est un groupe commutatif. En effet, la loi $+$ est associative et commutative, l'application $0_G : G \to G, g \mapsto 0$ est un élément neutre pour la loi $+$, et tout élément $f \in \mathrm{End}(G)$ admet un inverse $-f : G \to G, x \mapsto -f(x)$.
- La loi $\circ$ est associative.
- La loi $\circ$ possède un élément neutre, qui est l'application identité.
- La loi $\circ$ est distributive par rapport à la loi $+$: pour tous $f, g, h \in \mathrm{End}(G)$ et tout $x \in G$,

  $$((f+g) \circ h)(x) = (f+g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x)$$

  et

  $$(f \circ (g+h))(x) = f((g+h)(x)) = f(g(x)+h(x)) = f(g(x)) + f(h(x)) = (f \circ g + f \circ h)(x)$$

  Ainsi, $(\mathrm{End}(G), +, \circ)$ est un anneau.

retour à l'exercice 16

Correction de l'Exercice 17

On va démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour cela, soient $x = \frac{m}{n}$ et $y = \frac{m'}{n'} \in A$. Alors

$$x - y = \frac{mn' - m'n}{nn'} \text{ et } xy = \frac{mm'}{nn'}$$

Comme nn', produit de deux nombres impairs, est impair, et que A est non vide puisqu'il contient 1 , on en déduit que A est bien un sous-anneau de $(\mathbb{Q},+,\times)$. Déterminons ensuite les inversibles de A. Soit $x=\frac{m}{n}\in A$ inversible, et soit $y=\frac{m'}{n'}\in A$ tel que $xy=1$. On en déduit que $mm'=nn'$. En particulier, m est nécessairement impair. Réciproquement, si $x=\frac{m}{n}$ avec m impair, alors $y=\frac{n}{m}$ est dans A (si jamais $m<0$, il suffit d'écrire $y=\frac{-n}{-m}$ pour vérifier qu'il est bien dans A), et $xy=1$. Ainsi, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m\in\mathbb{Z},n\in\mathbb{N}^*$, et m,n impairs.

retour à l'exercice 17

Correction de l'Exercice 18

On va prouver que $(\mathbb{D},+,\times)$ est un sous-anneau de $(\mathbb{Q},+,\times)$. On remarque d'abord que $\mathbb{D}\subset\mathbb{Q}$, puis que $1\in\mathbb{D}$. De plus, soient $x=\frac{n}{10^k}$ et $y=\frac{M}{10^l}$ deux éléments de $\mathbb{D}$. Alors

$$x-y=\frac{n10^l-m10^k}{10^{k+l}}\text{ et }xy=\frac{nm}{10^{k+l}}$$

sont clairement des éléments de $\mathbb{D}$, et $(\mathbb{D},+,\times)$ est bien un sous-anneau de $(\mathbb{Q},+,\times)$. Déterminons ensuite les inversibles de $(\mathbb{D},+,\times)$. Soit $x=\frac{n}{10^k}$ inversible, d'inverse $y=\frac{m}{10^2}$. Alors

$$xy=1\iff nm=10^{k+l}$$

On en déduit que les seuls diviseurs premiers de n sont 2 et 5 , autrement dit que n s'écrit $\pm2^p5^q$ pour $p,q\in\mathbb{N}$. Réciproquement, soit $x=\frac{\pm2^p5^q}{10^k}$ et montrons que x est inversible dans $\mathbb{D}$. Posons $y=\frac{\pm10^k}{2^p5^q}$. Il suffit de vérifier que y est élément de $\mathbb{D}$. Mais on peut aussi écrire

$$y=\frac{\pm10^k2^q5^p}{2^{p+q}5^{p+q}}=\frac{\pm10^k2^q5^p}{10^{p+q}}\in\mathbb{D}$$

Ainsi, les inversibles de $(\mathbb{D},+,\times)$ sont les éléments $\frac{\pm2^p5^q}{10^k}$, avec $p,q,k\in\mathbb{N}$.

retour à l'exercice 18

Correction de l'Exercice 19

(1) Pour tout $x\in A$, la formule du binôme donne (pour x et x qui commutent)

$$x+x=(x+x)^3=x^3+3x^2x+3xx^2+x^3=x+x+6x.$$

Ainsi, $6x=0_A$.

(2) Les entiers 2 et 3 sont premiers entre eux donc il existe, d'après la propriété de Bézout, des entiers u et v tels que $1=2u+3v$. Alors, pour tout $x\in A$,

$$x=2ux+3vx$$

et $2ux\in C\,(\text{car }3(2ux)=6(ux)=0_A)$ et $3vx\in B\,(\text{car }2(3vx)=6(vx)=0_A)$. En conclusion, $A\subset B+C$ donc $A=B+C$.

retour à l'exercice 19

Correction de l'Exercice 20 Conseil du coach Éléments nilpotents

(1) Soit $a\in A$ nilpotent et $b\in A$ tel que $ab=ba$. Montrons, par récurrence sur $k\in\mathbb{N}$, que $\forall k\in\mathbb{N}^*,ab^k=b^ka$.
- Pour $k=1$, on a $ab=ba$ par hypothèse.
- Si $ab^k=b^ka$ pour un $k\in\mathbb{N}^*$, alors

$$\begin{aligned}ab^{k+1}&=a\left(b^kb\right)=\left(ab^k\right)b=\left(b^ka\right)b=b^k(ab)=b^k(ba)\\&=\left(b^kb\right)a=b^{k+1}a.\end{aligned}$$

Ceci montre, par récurrence sur k, que $\forall k\in\mathbb{N}^*,ab^k=b^ka$.

Montrons, par récurrence sur $k:\forall k\in\mathbb{N}^*,(ab)^k=a^kb^k$.
Pour $k=1$, on a trivialement $ab=ab$. * Si$(ab)^k=a^kb^k$ pour un $k\in\mathbb{N}^*$, alors :

$$\begin{aligned}(ab)^{k+1}&=(ab)^k(ab)=\left(a^kb^k\right)(ab)=a^k\left(b^ka\right)b=a^k\left(ab^k\right)b\\&=\left(a^ka\right)\left(b^kb\right)=a^{k+1}b^{k+1}.\end{aligned}$$

Ceci montre, par récurrence sur $k:\forall k\in\mathbb{N}^*,(ab)^k=a^kb^k$. - Puisque a est nilpotent, il existe $n\in\mathbb{N}^*$ tel que $a^n=0$. Puisque $ab=ba$, on a : $(ab)^n=a^nb^n=0b^n=0$, donc ab est nilpotent.

(2) Puisque a est nilpotent, il existe $n\in\mathbb{N}^*$ tel que $a^n=0$. On a alors

$$\begin{cases}(1-a)\left(1+a+a^2+\cdots+a^{n-1}\right)=1-a^n=1-0=1\\\left(1+a+a^2+\cdots+a^{n-1}\right)(1-a)=1-a^n=1-0=1\end{cases}$$

donc $1-a$ est inversible et

$$(1-a)^{-1}=1+a+a^2+\cdots+a^{n-1}=\sum_{k=0}^{n-1}a^k$$

(3) Soient $a, b \in A$ nilpotents et tels que $ab = ba$.

Puisque a est nilpotent, il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$. Puisque b est nilpotent, il existe $p \in \mathbb{N}^*$ tel que $b^p = 0$. Calculons $(a+b)^{n+p-1}$ en utilisant la formule du binôme de Newton, ce qui est licite puisque $ab = ba$

$$\begin{aligned}(a+b)^{n+p-1} &= \sum_{k=0}^{n+p-1} \binom{n+p-1}{k} a^k b^{n+p-1-k} \\ &= \sum_{k=0}^{n-1} \binom{n+p-1}{k} a^k \underbrace{b^{n+p-1-k}}_{=0} \\ &\quad \text{car } n+p-1-k \geqslant p \\ &+ \sum_{k=n}^{n+p-1-k} \binom{n+p-1}{k} \underbrace{a^k}_{=0} b^{n+p-1-k} = 0, \\ &\quad \text{car } k \geqslant n\end{aligned}$$

donc $a+b$ est nilpotent.

↶ retour à l'exercice 20

Correction de l'Exercice 21 Théorème de Lagrange

(1) **Réflexivité.** $\forall x \in G, xx^{-1} = e \in H$.

Symétrie. Soit $(x, y) \in G^2$. On a

$$\begin{aligned}x\mathcal{R}y &\iff xy^{-1} \in H \implies yx^{-1} = \left(xy^{-1}\right)^{-1} \in H \\ &\iff y\mathcal{R}x.\end{aligned}$$

Transitivité. Soit $(x, y, z) \in G^3$. On a

$$\left\{ \begin{array}{ccc|c} x & \mathcal{R} & y & \\ y & \mathcal{R} & z & \end{array} \right. \iff \left| \begin{array}{l} xy^{-1} \in H \\ yz^{-1} \in H \end{array} \right.$$
$$\iff xz^{-1} = \left(xy^{-1}\right)\left(yz^{-1}\right) \in H \iff x\mathcal{R}z.$$

On conclut, $\mathcal{R}$ est une relation d'équivalence dans G.
Notons $\hat{x}$ la classe de x modulo $\mathcal{R}$, pour $x \in G$.

(2) Soit $(x, y) \in G^2$. Pour tout t de $\hat{x}$, on a $tx^{-1}y \in \hat{y}$, car $\left(tx^{-1}y\right)y^{-1} = tx^{-1} \in H$.
On peut donc considérer l'application $\alpha : \hat{x} \longmapsto \vec{t} \longmapsto$, et de même, $\beta : \underset{s}{\hat{y}} \longmapsto \vec{b} \longmapsto \hat{x}$.
On a : $\forall t \in \hat{x}, (\beta \circ \alpha)(t) = \left(tx^{-1}y\right)y^{-1}x = t$, donc $\beta \circ \alpha = \mathrm{Id}_{\hat{x}}$, et de même, $\alpha \circ \beta = \mathrm{Id}_{\mathrm{y}}$.
Ceci montre que α et β sont des bijections réciproques l'une de l'autre. Comme G est fini, $\hat{x}$ et $\hat{y}$ sont alors finis et de même cardinal.

(3) Puisque les classes modulo $\mathcal{R}$ sont deux à deux disjointes et ont le même cardinal, on a

$$\mathrm{Card}(G) = \mathrm{Card}(\hat{e}) \times \mathrm{Card}(G/\mathcal{R})$$

De plus, comme $\hat{e} = H$, on conclut

$$\mathrm{Card}(G) = \mathrm{Card}(H) \times \mathrm{Card}(G/\mathcal{R})$$

En particulier, $\mathrm{Card}(H) \mid \mathrm{Card}(G)$.

↶ retour à l'exercice 21