MP/MP*
MPI/MPI*

Colles de **mathématiques**

Rémi Coutens

NOUVEAUX PROGRAMMES !

500 EXERCICES CORRIGÉS

- Exercices de calcul
- Exercices de raisonnement
- Exercices avec questions ouvertes

ellipses

MP/MP*
MPI/MPI*

Colles de **mathématiques**

Rémi Coutens

NOUVEAUX PROGRAMMES

Sous la direction de François Pantigny

ellipses

Collection Colles de Prépas
dirigée par François Pantigny

Retrouvez tous les titres de la collection et des extraits sur
www.editions-ellipses.fr

Je remercie M. Pantigny pour ses relectures et ses pertinents conseils, mes collègues et amis MM. Devulder, Hoffbeck et Lucas pour leurs encouragements et leurs partages d'exercices. Ce livre doit également beaucoup à mon amie Emmanuelle Guillant qui n'aurait jamais imaginé qu'en déménageant à New York, elle y relirait les épreuves d'un livre de mathématiques.
Je dédie ce livre à tous ceux qui poursuivent des études de mathématiques au-delà du BAC+2, en particulier à ma fille Juliette.

ISBN 9782340-066526
©Ellipses Édition Marketing S.A., 2022
8/10 rue la Quintinie 75015 Paris

DANGER LE PHOTOCOPILLAGE TUE LE LIVRE

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

Avant-propos

En seconde année les interrogations orales n'engendrent plus d'appréhension. On sait que cette spécificité du système des classes préparatoires aux grandes écoles participe grandement aux progrès des étudiants. Cependant, cette seconde année est courte et à l'assimilation régulière du cours s'ajoute l'aspect de l'entraînement à l'oral. Néanmoins, de même qu'on ne se prépare pas à un marathon en faisant des marathons, un bon exercice pour l'oral d'un concours n'est pas forcément un bon exercice pour une « colle » au cours de l'année. C'est pourquoi même si certains sujets proviennent d'oraux de concours, ils ont parfois été modifiés afin de recentrer leurs questions sur un chapitre précis d'interrogation.

Dans l'objectif d'une préparation efficace, les exercices de ce livre sont classés en trois catégories :

- Les « exercices axés sur le calcul ». Souvent application quasiment directe du cours, ils ont pour objectif, via la pratique calculatoire, de vérifier la connaissance et la compréhension des notions du cours.
- Les « exercices axés sur le raisonnement ». Ces exercices demandant plus de recul, leur objectif est de renforcer l'assimilation des concepts.
- Les « exercices avec questions ouvertes ». Ces exercices amènent l'étudiant à avoir sa propre réflexion, à construire sa démonstration ou son contre-exemple selon les cas.

Plutôt que l'originalité ou la difficulté, nous avons privilégié des exercices qui nous ont paru formateurs. Néanmoins certains exercices, signalés par une ou deux étoiles, sont d'un niveau plus élevé.

Les corrections des exercices figurent après la liste des énoncés. Chaque exercice est entièrement corrigé parfois de plusieurs manières lorsque cela nous a semblé utile.

En début de chaque chapitre se trouve une figure, généralement réalisée par M. Pantigny, qui illustre soit une notion, soit un exercice. Nous encourageons le lecteur à faire le plus souvent possible ses propres représentations.

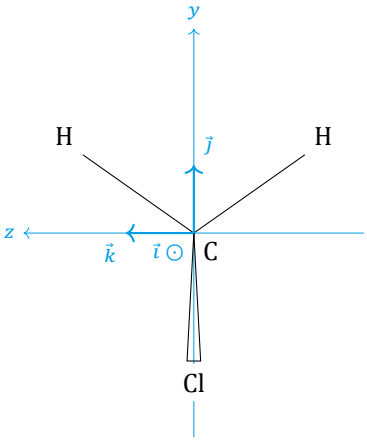
En espérant que ce livre contribue efficacement à leur préparation aux concours, nous adressons nos vœux de réussite aux lecteurs de ce livre.

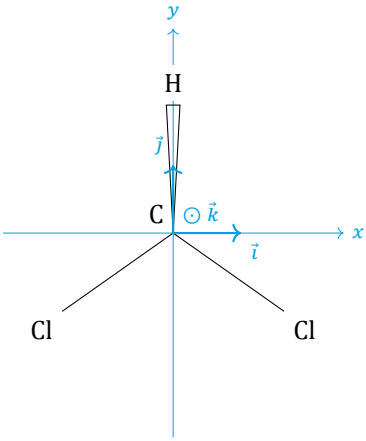
Sommaire

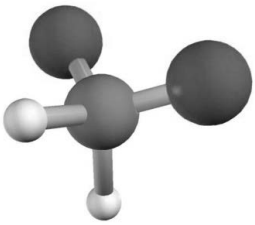
1	Groupes	3
2	Anneaux	27
3	Algèbre (révisions)	43
4	Matrices, déterminants (révisions)	57
5	Réduction des endomorphismes	77
6	Polynômes matriciels et d'endomorphismes	117
7	Espaces euclidiens et préhilbertiens	141
8	Endomorphismes d'un espace euclidien	159
9	Suites numériques	189
10	Séries numériques	205
11	Vocabulaire topologique	229
12	Espaces vectoriels normés	243
13	Compacité, convexité, connexité par arcs	267
14	Primitives, intégration sur un segment	279
15	Suites de fonctions	311
16	Intégrales généralisées	333
17	Limite d'intégrales	363
18	Fonction définie par une intégrale	387
19	Séries de fonctions	421
20	Séries entières	453
21	Sommes d'intégrales	481
22	Équations différentielles	503

23	**Calcul différentiel**	**535**
24	**Probabilités**	**553**
25	**Variables aléatoires discrètes**	**561**
26	**Couples de variables aléatoires**	**579**

Groupes 1







	Id	s_y	s_H	s_{Cl}
Id	Id	s_y	s_H	s_{Cl}
s_y	s_y	Id	s_{Cl}	s_H
s_H	s_H	s_{Cl}	Id	s_y
s_{Cl}	s_{Cl}	s_H	s_y	Id

Une molécule de dichlorométhane CH_2Cl_2 a quatre isométries qui la laissent invariante : l'identité Id, la symétrie s_y par rapport à la droite Oy, la réflexion s_H par rapport à xOy, qui échange les atomes d'hydrogène, et la réflexion s_{Cl} par rapport à yOz, qui échange les atomes de chlore.
Le groupe formé par ces quatre isométries (pour la loi $\circ$) est appelé le *groupe de symétrie* de la molécule. Il s'agit du groupe de Klein, isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Exercices axés sur le calcul

Exercice 1 *Image par un morphisme de l'itéré d'un élément*

Soient G et G' deux groupes notés additivement.
Pour $n \in \mathbb{Z}$ et $x \in G$, on désigne par nx l'itéré de x d'ordre n dans le groupe G.
Soit f un morphisme de G dans G'.

1) Montrer que pour $x \in G$ et tout $n \in \mathbb{N}$, on a $f(nx) = nf(x)$.
2) Montrer que l'égalité précédente est encore vraie quand $n \in \mathbb{Z}$.
3) Que deviennent ces égalités en notations multiplicatives ?

Exercice 2 *Classique*

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ vers $(\mathbb{R}, +)$.
Montrer que pour tout $r \in \mathbb{Q}, f(r) = rf(1)$.

Exercice 3

Soit $\sigma \in \mathfrak{S}_9$ définie par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$.

1) Décomposer σ en produit de cycles à supports disjoints.
2) Déterminer la signature et l'ordre de σ.

Exercice 4

Déterminer le sous-groupe (additif) de $\mathbb{Z}$ engendré par $\{12, 18, -27\}$.

Exercice 5

Montrer que le sous-groupe (multiplicatif) de $\mathbb{C}^*$, engendré par i et $\mathrm{j} = \exp(2\mathrm{i}\,\pi/3)$, est $\mathbb{U}_{12}$ (le groupe des racines 12-ièmes de l'unité).

Exercice 6

On rappelle que pour tout a réel, $b = \sqrt[3]{a}$ désigne l'unique réel b tel que $a = b^3$.
On munit $\mathbb{R}$ de la loi $\star$ définie par :

$$x \star y = \sqrt[3]{x^3 + y^3}.$$

1) Montrer que $(\mathbb{R}, \star)$ est un groupe abélien.
2) Montrer qu'il est isomorphe à $(\mathbb{R}, +)$.

Exercice 7 *Automorphismes intérieurs*

Soit $(G, *)$ un groupe. Pour $a \in G$, on note a^{-1} son symétrique pour la loi $*$ et τ_a l'application de G vers G définie par $x \mapsto a * x * a^{-1}$.

1) Montrer que τ_a est un automorphisme du groupe $(G, *)$ (c'est-à-dire un isomorphisme du groupe dans lui-même).
2) Vérifier que :
$$\forall a, b \in G, \quad \tau_a \circ \tau_b = \tau_{a*b}.$$
3) En déduire que $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

D'après Mines-Télécom

Exercice 8 *Centre d'un groupe*

1) Soit $(G, *)$ un groupe. On note :
$$Z(G) = \{x \in G \mid \forall y \in G,\ x * y = y * x\}.$$
Montrer que $Z(G)$ est un sous-groupe de G.
2) Montrer que l'ensemble des matrices de la forme $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ avec x, y et $z \in \mathbb{R}$ est un groupe pour le produit matriciel. Trouver le centre de ce groupe.

Exercice 9

On considère l'intervalle $I = [0, 1[$. Pour x et y dans I, on pose :
$$x \star y = x + y - \lfloor x + y \rfloor.$$
1) Montrer que $(I, \star)$ est un groupe abélien.
2) Résoudre l'équation $x \star x = 0$ d'inconnue $x \in I$.
En déduire qu'il existe un unique $d \in I$ qui soit d'ordre 2 dans $(I, \star)$.
3) Pour $n \in \mathbb{N}^*$, préciser, s'il en existe, les éléments d'ordre n de I.

Exercices axés sur le raisonnement

Exercice 10 *Classique*

Montrer que la réunion de deux sous-groupes est un sous-groupe si, et seulement si, l'un des deux sous-groupes est inclus dans l'autre.

Exercice 11

Soient $(G, *)$ un groupe d'élément neutre e et $f : x \mapsto x^{-1}$ l'application de G dans lui-même qui à tout élément de G associe son inverse pour la loi $*$.
Montrer que f est un automorphisme du groupe $(G, *)$ si, et seulement si, le groupe $(G, *)$ est commutatif.

Exercice 12

On note $\mathrm{GL}_2(\mathbb{Z})$ l'ensemble des matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$ dont le déterminant vaut 1 ou -1.

1) Soit M une matrice carrée d'ordre 2 à coefficients entiers et inversible.
   Montrer que si M^{-1} est à coefficients entiers, alors $\det(M) = \pm 1$.
2) Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est un groupe pour la multiplication.
3) On pose $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.
   Calculer l'ordre de A, de B et de AB. Que peut-on en conclure ?

Exercice 13

Soient H et K deux groupes notés multiplicativement.

1) Soient h un élément de H et k un élément de K. On suppose ces éléments d'ordres finis. On note p l'ordre de h, q celui de k et $r = \mathrm{ppcm}(p, q)$.
   Montrer que (h, k) est un élément d'ordre r dans le groupe $H \times K$.
2) On suppose que H et K sont des groupes cycliques.
   Montrer que le groupe produit $H \times K$ est cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 14

Soit G un sous-groupe fini de $(\mathbb{C}^*, \times)$.

1) Montrer que $G \subset \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
2) Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $G = \mathbb{U}_p$ (ensemble des racines p-ièmes de 1).

Exercice 15 ⋆⋆ *Groupes des éléments d'ordre fini de $\mathbb{C}^*$*

On note $\mathbb{U}_\infty = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^*,\ z^n = 1\}$.

1) Montrer que $\mathbb{U}_\infty$ est infini.
2) Montrer $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
3) Montrer que $\mathbb{U}_\infty$ n'est pas engendré par une partie finie.

Exercice 16 ⋆⋆

Soient G un groupe fini noté multiplicativement, H et K deux sous-groupes de G.
On note $f : H \times K \to G, (h,k) \mapsto hk$ et :

$$HK = \{hk; h \in H,\ k \in K\}.$$

1) Quelle est l'image de f ? Déterminer le nombre d'antécédents par f que possède un élément de cette image.
2) En déduire que :
$$\mathrm{Card}(HK)\mathrm{Card}(H \cap K) = \mathrm{Card}(H)\mathrm{Card}(K).$$

Exercice 17 *Sous-groupe d'un groupe cyclique*

On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique : on introduit un groupe cyclique $(G,*)$, a un générateur de G et H un sous-groupe de $(G,*)$.

1) Justifier l'existence d'un plus petit entier naturel non nul n tel que $a^n \in H$.
2) Établir qu'alors H est le groupe engendré par a^n.

Exercice 18

Soit $n \in \mathbb{N} \setminus \{0,1\}$ et $(G,*)$ un groupe de cardinal $2n$.
Soient A et B deux sous-groupes de G de cardinal n tels que $A \cap B = \{e\}$.

1) Montrer qu'il existe $c \in G$ tel que $A \cup B \cup \{c\} = G$.
2) Montrer que :
$$\forall a \in A \setminus \{e\}, \forall b \in B \setminus \{e\}, \quad a * b = c.$$
En déduire $n = 2$.

Exercice 19 ⋆

1) Soient f un homomorphisme de groupes de G dans G' et x un élément de G d'ordre fini p. Que peut-on dire de l'ordre de $f(x)$ dans G' ?
2) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.
3) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 20 ⋆

Montrer qu'il existe un multiple de 23 dont l'écriture décimale ne comporte que des 1.

D'après TPE Mines-Ponts

Exercices avec questions ouvertes

Exercice 21

Que dire d'un groupe dont le nombre d'éléments est un nombre premier ?

Exercice 22 *Ordre de xy et de yx*

Soient x et y éléments d'un groupe G (quelconque) noté multiplicativement.
Existe-t-il un lien entre l'ordre de xy et celui de yx ?

Exercice 23 ⋆⋆

Soit G un groupe noté multiplicativement. On suppose que tous les éléments du groupe (autres que l'élément neutre e) sont d'ordre 2.

1) Montrer que G est un groupe abélien.
   Indication : Pour x et $y \in G$, on pourra considérer $(xy)(xy)$.
2) Soit H un sous-groupe de G et $x \in G \setminus H$. On note K le sous-groupe engendré par $H \cup \{x\}$.
   a) Montrer que $K = H \cup xH$.
   b) Montrer que si H est fini, alors $\text{card}(K) = 2\,\text{card}(H)$.
3) En supposant de plus que G est un groupe fini, que peut-on dire de $|G|$?

Exercice 24 *Plus petit sous-groupe non commutatif*

Quel est le plus petit entier n pour lequel il existe un groupe de cardinal n non commutatif ?

Exercice 25 *Caractérisation des groupes finis par le nombre de sous-groupes*

Soit $(G, *)$ un groupe.

1) Justifier que si G est fini, alors G possède un nombre fini de sous-groupes.
2) Réciproquement, on suppose que G possède un nombre fini de sous-groupes.
   Tous les éléments de G sont-ils d'ordre fini ?
   L'ensemble G est-il fini ?

Exercice 26

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 27

Soit n un entier naturel supérieur à 4 et $\sigma \in \mathfrak{S}_n$.
Existe-t-il un lien entre la parité de l'ordre de σ et sa signature ?

Exercice 28 *Classique*

Quels sont les morphismes de groupes continus de $(\mathbb{R}, +)$ dans lui-même ?
Indication : Utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.

Corrections

Exercices axés sur le calcul

Exercice 1

On raisonne par récurrence.

1) Soit $x \in G$. Pour $n \in \mathbb{N}$, on appelle $\mathcal{P}_n$ la proposition « $f(nx) = nf(x)$ ».

• Initialisation

Par définition, $0x = 0_G$ et $0f(x) = 0_{G'}$.

Par ailleurs, puisque f est un morphisme, $f(0_G) = 0_{G'}$.

Donc $\mathcal{P}_0$ est vraie.

• Hérédité

Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie. On a alors :

$$\begin{aligned} f\big((n+1)x\big) &= f(nx + x) \\ &= f(nx) + f(x) && \text{car } f \text{ est un morphisme} \\ &= nf(x) + f(x) && \text{d'après } \mathcal{P}_n \\ &= (n+1)f(x) && \text{par définition} \end{aligned}$$

ce qui montre que $\mathcal{P}_{n+1}$ est vraie.

On a montré par récurrence que :

$$\forall n \in \mathbb{N}, \quad f(nx) = nf(x).$$

2) Soient $x \in G$ et $n \in \mathbb{Z} \setminus \mathbb{N}$. Puisque f est un morphisme, on a $f(nx) = -f(-nx)$.

Or, $-nx = (-n)x$ et $-n \in \mathbb{N}$, donc $f(-nx) = (-n)f(n)$.

Finalement $f(nx) = -(-n)f(x) = nf(x)$.

On a montré :

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f(nx) = nf(x).$$

3) En notations multiplicatives, on obtient :

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f\big(x^n\big) = \big(f(x)\big)^n.$$

Exercice 2

Soit $r \in \mathbb{Q}$. On choisit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $r = p/q$.

En utilisant les images des itérés d'un élément par un morphisme (voir exercice 1) on a :

$$\begin{aligned} qf(r) &= qf\big(\tfrac{p}{q}\big) \\ &= f\big(q\tfrac{p}{q}\big) && f(qx) = qf(x), \text{ car } f \text{ est un morphisme} \\ &= pf(1) && q\tfrac{p}{q} = p = p \cdot 1 \end{aligned}$$

En divisant l'égalité par q, on obtient $f(r) = rf(1)$.

Exercice 3

1) En étudiant les images successives de chacun des éléments de $[\![1,9]\!]$, on obtient :
$\sigma(1)=3, \sigma(3)=8, \sigma(8)=1$. De même, $\sigma(2)=7, \sigma(7)=2$.
Et $\sigma(4)=9, \sigma(9)=6, \sigma(6)=5, \sigma(5)=4$.
Donc :

$$\sigma = \langle 1,3,8\rangle \circ \langle 2,7\rangle \circ \langle 4,9,5,7\rangle.$$

2) • Signature
La transposition $\tau = \langle 2,7\rangle$ est de signature -1. Le cycle $c_3 = \langle 1,3,8\rangle$ est de signature $+1$ et le cycle $c_4 = \langle 4,9,5,7\rangle$ est de signature -1.
La signature étant un homomorphisme de groupe, on a :

$$\varepsilon(\sigma) = \varepsilon(\tau)\varepsilon(c_3)\varepsilon(c_4) = (-1)\cdot 1\cdot(-1) = 1.$$

• Ordre
Deux cycles de supports disjoints commutant pour la composition, on a pour tout $p \in \mathbb{N}$:

$$\sigma^p = \tau^p \circ c_3^p \circ c_4^p.$$

La transposition $\tau = \langle 2,7\rangle$ est d'ordre 2. Le cycle $c_3 = \langle 1,3,8\rangle$ est d'ordre 3 et le cycle $c_4 = \langle 4,9,5,7\rangle$ est d'ordre 4.
On en déduit que l'ordre de σ est égal à $\text{ppcm}(2,3,4) = 12$.

Remarque
On peut déterminer $\varepsilon(\sigma)$ en calculant le nombre d'inversions de σ. On trouve qu'il y a 22 couples (i,j) tels que $i<j$ et $\sigma(i)>\sigma(j)$. Donc $\varepsilon(\sigma) = (-1)^{22} = 1$. Mais il est plus rapide d'utiliser la décomposition en cycles. Quant à déterminer l'ordre de σ en calculant successivement σ^2, σ^3, etc., ce serait déraisonnable.

Exercice 4

On a $12 = 2^2\cdot 3$, $18 = 2\times 3^2$ et $-27 = -3^3$. Le PGCD de ces trois nombres est donc 3.
Donc le sous-groupe de $\mathbb{Z}$ engendré par $\{12, 18, -27\}$ est $3\mathbb{Z}$.

Remarque
On peut détailler par double inclusion en notant G le groupe engendré par $\{12, 18, -27\}$.

$\subset$ Les trois nombres sont des multiples de 3.
Ainsi $G \subset 3\mathbb{Z}$ (car G est le plus petit sous-groupe contenant $\{12, 18, -27\}$).

$\supset$ On a $1 = 45 - 44 = 5\cdot 9 - 11\cdot 4$, donc $3 = 5\cdot 27 - 11\cdot 12$. En particulier, $3 \in G$.
Donc G contient aussi le sous-groupe engendré par 3. D'où, $3\mathbb{Z} \subset G$.

Exercice 5

On note G le groupe engendré par i et j. On va montrer $G = \mathbb{U}_{12}$ par double inclusion.

$\subset$ On a $\mathrm{i}^{12} = (-1)^6 = 1$ et $\mathrm{j}^{12} = (\mathrm{j}^3)^4 = 1$. Donc le groupe $\mathbb{U}_{12}$ contient i et j.
Ainsi $G \subset \mathbb{U}_{12}$ (car G est le plus petit sous-groupe contenant i et j).

$\supset$ Puisque G est un sous-groupe, on a $\mathrm{i} \cdot \mathrm{j} \in G$.
D'autre part, on a $\mathrm{i} \cdot \mathrm{j} = \exp(\mathrm{i}\,\pi/2)\exp(2\mathrm{i}\,\pi/3) = \exp(7\mathrm{i}\,\pi/6)$.
On sait que les générateurs du groupe $\mathbb{U}_{12}$ sont les nombres complexes de la forme $\exp(2k\mathrm{i}\,\pi/12)$ avec k un nombre entier premier avec 12.
Comme $7 \wedge 12 = 1$, on en déduit que G contient un générateur de $\mathbb{U}_{12}$ et donc $\mathbb{U}_{12} \subset G$.

Remarque
On peut aussi utiliser $\mathrm{i}^{-1} \cdot \mathrm{j} = \exp(-\mathrm{i}\,\pi/2)\exp(2\mathrm{i}\,\pi/3) = \exp(\mathrm{i}\pi/6)$ qui est un générateur plus usuel de $\mathbb{U}_{12}$.

Exercice 6

1) • Montrons que la loi $\star$ est associative :
Soient x, y et z trois réels.

$$\begin{aligned}(x \star y) \star z &= \sqrt[3]{(x \star y)^3 + z^3} \\ &= \sqrt[3]{(x^3 + y^3) + z^3} \quad \text{car } x \star y = \sqrt[3]{x^3 + y^3} \text{ et } \left(\sqrt[3]{t}\right)^3 = t \\ &= \sqrt[3]{x^3 + (y^3 + z^3)} \quad \text{par associativité de } + \\ &= \sqrt[3]{x^3 + (y \star z)^3} \quad \text{car } y \star z = \sqrt[3]{y^3 + z^3} \\ &= x \star (y \star z).\end{aligned}$$

• De la même façon, la commutativité de $+$ entraîne celle de $\star$.
• Pour tout $x \in \mathbb{R}$, $0 \star x = x \star 0 = \sqrt[3]{x^3 + 0^3} = \sqrt[3]{x^3} = x$. Donc 0 est neutre pour $\star$.
• Pour tout $x \in \mathbb{R}$, $(-x) \star x = x \star (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0$. Donc tout réel admet un symétrique pour $\star$.

On a montré que $(\mathbb{R}, \star)$ est un groupe abélien.

2) Notons $f : t \mapsto t^3$. On a :

$$\forall x, y \in \mathbb{R}, \quad f(x \star y) = (x \star y)^3 = x^3 + y^3 = f(x) + f(y).$$

Donc f est un morphisme de groupes de $(\mathbb{R}, \star)$ dans $(\mathbb{R}, +)$.
Or, f est bijective, donc on a prouvé que $(\mathbb{R}, \star)$ est isomorphe à $(\mathbb{R}, +)$.

Exercice 7

1) Soit $a \in G$. Montrons que τ_a est un morphisme de groupes :
Soient x et y dans G.

$$\begin{aligned}\tau_a(x) * \tau_a(y) &= (a * x * a^{-1}) * (a * y * a^{-1}) \\ &= a * x * (a^{-1} * a) * y * a^{-1} \\ &= a * (x * y) * a^{-1} \\ &= \tau_a(x * y).\end{aligned}$$

par associativité

$a^{-1} * a = e$ (élément neutre)

Montrons que τ_a est une permutation de G :
Soient x et y dans G.

$$\begin{aligned}y = \tau_a(x) &\iff y = a * x * a^{-1} \\ &\iff y * a = a * x \\ &\iff a^{-1} * y * a = x.\end{aligned}$$

Donc tout élément de G a un unique antécédent dans G par τ_a.
Par conséquent, τ_a est bijection de G dans lui-même.

Remarque
On peut même préciser que $\tau_a^{-1} = \tau_{a^{-1}}$.

On a montré que τ_a est un automorphisme du groupe $(G, *)$.

2) Soient a et b dans G. On a pour tout $x \in G$:

$$\begin{aligned}\tau_a \circ \tau_b(x) &= \tau_a(\tau_b(x)) \\ &= a * (b * x * b^{-1}) * a^{-1} \\ &= (a * b) * x * \left(b^{-1} * a^{-1}\right) \\ &= \tau_{a*b}(x).\end{aligned}$$

$(a * b)^{-1} = b^{-1} * a^{-1}$

Donc $\tau_a \circ \tau_b = \tau_{a*b}$.

3) En notant $\mathfrak{S}(G)$ l'ensemble des permutations de G, on vient de montrer que $a \mapsto \tau_a$ est un homomorphisme de groupes de $(G, *)$ dans $\left(\mathfrak{S}(G), \circ\right)$. Puisqu'on a un homomorphisme, l'image du groupe G est un sous-groupe de $\mathfrak{S}(G)$. Donc $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

Remarque
$a \mapsto \tau_a$ étant un homomorphisme de groupes, on retrouve $\tau_a^{-1} = \tau_{a^{-1}}$.

Exercice 8

1) Par définition, $Z(G)$ est une partie de G.
- En notant e l'élément neutre de G, on a, pour tout $y \in G$, $e * y = y * e$, donc $e \in Z(G)$.

- Soient x_1 et x_2 deux éléments de $Z(G)$. On a, pour tout $y \in G$:

$$\begin{aligned}(x_1 * x_2) * y &= x_1 * (x_2 * y) \\ &= x_1 * (y * x_2) \\ &= (x_1 * y) * x_2 \\ &= (y * x_1) * x_2 \\ &= y * (x_1 * x_2).\end{aligned}$$

$x_2 \in Z(G)$; associativité de $*$; $x_1 \in Z(G)$

Donc $x_1 * x_2 \in Z(G)$.

- Soit x un élément de $Z(G)$. On a, pour tout $y \in G$, $x*y = y*x$. En multipliant à gauche et à droite par l'inverse x^{-1} de x, on obtient $e*y*x^{-1} = x^{-1}*y*e$, donc $y*x^{-1} = x^{-1}*y$. Donc $x^{-1} \in Z(G)$.

On a montré que $Z(G)$ est un sous-groupe de G.

2) Notons $\mathcal{G}$ l'ensemble des matrices de la forme $\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}$ avec x, y et $z \in \mathbb{R}$.

- $\mathcal{G}$ contient l'élément neutre I_3.
- Soient $M_1 = \begin{pmatrix}1 & x_1 & z_1\\ 0 & 1 & y_1\\ 0 & 0 & 1\end{pmatrix}$ et $M_2 = \begin{pmatrix}2 & x_2 & z_2\\ 0 & 1 & y_2\\ 0 & 0 & 1\end{pmatrix}$ deux élements de $\mathcal{G}$.

  On a $M_1M_2 = \begin{pmatrix}1 & x_1+x_2 & z_2+x_1y_2+z_1\\ 0 & 1 & y_1+y_2\\ 0 & 0 & 1\end{pmatrix} \in \mathcal{G}$.
- Soit $M = \begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}$ un élément de $\mathcal{G}$.

  M est une matrice triangulaire dont les coefficients diagonaux sont non nuls, donc M est inversible. On peut calculer son inverse à l'aide de la méthode de Gauss-Jordan ou à l'aide de la comatrice.

  On trouve $M^{-1} = \begin{pmatrix}1 & -x & xy-z\\ 0 & 1 & -y\\ 0 & 0 & 1\end{pmatrix}$. Ce qui prouve que $M^{-1} \in \mathcal{G}$.

Donc $\mathcal{G}$ est un sous-groupe du groupe linéaire et, par conséquent, c'est un groupe pour le produit matriciel.

Avec les notations précédentes, on a pour M_1 et M_2 dans $\mathcal{G}$:

$$M_1M_2 = M_2M_1 \iff z_2 + x_1y_2 + z_1 = z_1 + x_2y_1 + z_2 \iff x_1y_2 = x_2y_1.$$

Si $M_1 \in Z(\mathcal{G})$, on a, pour tous $x_2, y_2 \in \mathbb{R}$, $x_1y_2 = x_2y_1$.

En utilisant $(x_2, y_2) = (0,1)$, on obtient $x_1 = 0$. De même, avec $(x_2, y_2) = (1,0)$, on obtient $y_1 = 0$.

Réciproquement, si $M_1 = \begin{pmatrix}1 & 0 & z_1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$, on aura pour tout $M_2 \in \mathcal{G}$, $M_1M_2 = M_2M_1$.

Le centre du groupe $\mathcal{G}$ est l'ensemble des matrices de la forme $\begin{pmatrix}1 & 0 & z\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$ avec $z \in \mathbb{R}$.

Exercice 9

1) • Pour tout réel t, on a $t - \lfloor t \rfloor \in I$, donc $\star$ est une loi interne dans I.
• L'addition étant commutative, la loi $\star$ est clairement commutative.
• Associativité de $\star$
Soient x, y et $z \in I$. On a :

$$\begin{aligned}
(x \star y) \star z &= (x \star y) + z - \lfloor (x \star y) + z \rfloor \\
&= (x + y) - \lfloor x + y \rfloor + z - \big\lfloor (x + y) - \lfloor x + y \rfloor + z \big\rfloor && \text{par définition de } \star \\
&= (x + y) - \lfloor x + y \rfloor + z - \big\lfloor (x + y) + z \big\rfloor + \lfloor x + y \rfloor && (*) \\
&= (x + y) + z - \big\lfloor (x + y) + z \big\rfloor && \text{calculs dans } (\mathbb{R}, +) \\
&= x + (y + z) - \big\lfloor x + (y + z) \big\rfloor && \text{associativité de } + \\
&= x \star (y \star z). && (**)
\end{aligned}$$

(*) d'une part $(x+y) - \lfloor x+y \rfloor + z = (x+y) + z - \lfloor x+y \rfloor$, d'autre part $n = \lfloor x+y \rfloor \in \mathbb{Z}$ et $\lfloor t - n \rfloor = \lfloor t \rfloor - n$ si $n \in \mathbb{Z}$.
(**) par des calculs semblables aux précédents.

• Élément neutre
Pour tout $x \in I$, $\lfloor x \rfloor = 0$, donc $0 \star x = x \star 0 = x + 0 - \lfloor x + 0 \rfloor = x$.
Donc 0 est neutre pour $\star$.
• Symétrique d'un élément
Pour tout $x \in I$, $(-x) \star x = x \star (-x) = x - x - \lfloor 0 \rfloor = 0$.
Donc tout élément de I admet un symétrique pour $\star$.

On a montré que $(I, \star)$ est un groupe abélien.

2) Pour $x \in I$, $x \star x = 2x - \lfloor 2x \rfloor$ et $2x \in [0, 2[$, donc $\lfloor 2x \rfloor = 0$ ou 1.
Or, $2x = \lfloor 2x \rfloor \iff 2x \in \mathbb{Z}$. Donc $x \star x = 0 \iff (2x = 0 \text{ ou } 2x = 1)$.
Donc $x \star x = 0$ a deux solutions $x = 0$ et $x = 1/2$.
Parmi ces solutions, seul $1/2$ est d'ordre 2.

3) Pour $n \in \mathbb{N}$ et $x \in I$, on note $x^{[n]}$ l'itéré de x d'ordre n pour la loi $\star$.
Soit $x \in I$. Pour $n \in \mathbb{N}$, on note $\mathcal{P}_n$: « $x^{[n]} = nx - \lfloor nx \rfloor$ ».
• Initialisation
Par définition, 0 étant le neutre pour $\star$, $x^{[0]} = 0$. Donc $\mathcal{P}_0$ est vraie.
• Hérédité
Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie.

$$\begin{aligned}
x^{[n+1]} &= x^{[n]} \star x \\
&= x^{[n]} + x - \big\lfloor x^{[n]} + x \big\rfloor && \text{par définition de } \star \\
&= nx - \lfloor nx \rfloor + x - \big\lfloor nx - \lfloor nx \rfloor + x \big\rfloor && \text{d'après } \mathcal{P}_n \\
&= nx + x - \lfloor nx \rfloor - \lfloor nx + x \rfloor + \lfloor nx \rfloor && \lfloor nx \rfloor \in \mathbb{Z} \\
&= (n+1)x - \lfloor nx \rfloor - \big\lfloor (n+1)x \big\rfloor.
\end{aligned}$$

Donc $\mathcal{P}_{n+1}$ est vraie.
On a montré par récurrence que pour tout $n \in \mathbb{N}$, $x^{[n]} = nx - \lfloor nx \rfloor$.

Comme $x \in I, nx \in [0, n[$ et on obtient :

$$x^{[n]} = 0 \iff \exists k \in [\![0, n-1]\!], nx = k.$$

Donc $x^{[n]} = 0$ admet n solutions qui sont $x_k = \frac{k}{n}$ pour $k \in [\![0, n-1]\!]$.
Parmi ces solutions cherchons les éléments d'ordre exactement n :
On peut exclure $k = 0$, car 0 est d'ordre 1.
Soit $k \in [\![1, n-1]\!]$.
Pour $p \in [\![1, n]\!]$, on a :

$$x_k^{[p]} = 0 \iff px_k = \lfloor px_k \rfloor \iff p\frac{k}{n} \in \mathbb{Z} \iff n|pk.$$

- Si $k \wedge n = 1$. La condition « n divise pk » entraîne que « n divise p », donc $p = n$. Donc x_k est d'ordre exactement n.
- Sinon, notons $a = k \wedge n$. Il existe des entiers k' et n' tels que $k = ak'$ et $n = an'$.
  On remarque que $n' \in [\![1, n-1]\!]$ et que $n'k = n'ak' = nk'$, donc $x_k^{[n']} = 0$.
  On en déduit que x_k n'est pas d'ordre n.
  Les éléments d'ordre n sont les $x_k = \frac{k}{n}$ avec $k \in [\![1, n-1]\!]$ premier avec n.

Exercices axés sur le raisonnement

Exercice 10

Soient H_1 et H_2 deux sous-groupes du groupe G (noté multiplicativement).

$\Rightarrow$ Si $H_1 \subset H_2$, alors $H_1 \cup H_2 = H_2$, qui est un sous-groupe. Il en va de même si $H_2 \subset H_1$.

$\Leftarrow$ On suppose que $H_1 \cup H_2$ est un sous-groupe.
On raisonne par l'absurde en supposant que H_1 n'est pas inclus dans H_2 et que H_2 n'est pas inclus dans H_1.
Il existe donc $x_1 \in H_1 \setminus H_2$ et $x_2 \in H_2 \setminus H_1$.
x_1 et x_2 étant deux éléments du groupe $H_1 \cup H_2$, $x_1x_2 \in H_1 \cup H_2$. Par symétrie des rôles, on peut supposer que $x_1x_2 \in H_1$. Écrivant alors $x_2 = x_1^{-1}(x_1x_2)$, on obtient $x_2 \in H_1$ (produit de deux éléments du groupe H_1) ce qui amène une contradiction puisque $x_2 \in H_2 \setminus H_1$.
On a donc prouvé que H_1 est inclus dans H_2 ou H_2 est inclus dans H_1.

Exercice 11

On note $f : G \to G, x \mapsto x^{-1}$.
On sait que pour tout $x \in G, \left(x^{-1}\right)^{-1} = x$ ce qui s'écrit $f \circ f(x) = x$, donc f est une involution de G. En particulier, f est bijective de G dans lui-même.

Soient x et y dans G. On a les équivalences suivantes :

$$\begin{aligned} f(x*y)=f(x)*f(y) &\iff (x*y)^{-1}=x^{-1}*y^{-1} \\ &\iff x*y=\left(x^{-1}*y^{-1}\right)^{-1} \\ &\iff x*y=y*x. \end{aligned}$$

$a=b \iff a^{-1}=b^{-1}$

$(a*b)^{-1}=b^{-1}*a^{-1}$

Donc :

$$\forall x,y\in G, f(x*y)=f(x)*f(y) \quad\iff\quad \forall x,y\in G, x*y=y*x.$$

Donc f est un morphisme si, et seulement si, $*$ est commutative.
On a montré que f est un isomorphisme du groupe $(G,*)$ dans lui-même si, et seulement si, le groupe $(G,*)$ est commutatif.

Exercice 12

1) Si $M\in\mathcal{M}_2(\mathbb{Z})$, alors $\det(M)$ est un entier.
Si M est inversible, on a $M^{-1}M=I_2$, donc $\det(M^{-1})\det(M)=1$.
Donc si M^{-1} est aussi à coefficients entiers, alors $\det(M)$ est un entier inversible dans $\mathbb{Z}$.
Puisque $U(\mathbb{Z})=\{-1,1\}$, on en déduit $\det(M)=\pm 1$.

2) On sait que $\left(\mathrm{GL}_2(\mathbb{R}),\times\right)$ est un groupe.
- $\mathrm{GL}_2(\mathbb{Z})$ est inclus dans $\mathrm{GL}_2(\mathbb{R})$.
- $\mathrm{GL}_2(\mathbb{Z})$ est non vide (il contient la matrice I_2).
- $\mathrm{GL}_2(\mathbb{Z})$ est stable par multiplication (car le produit de deux matrices de déterminants ± 1 est également de déterminant ± 1 et le produit de deux matrices à coefficients dans $\mathbb{Z}$ est aussi à coefficients dans $\mathbb{Z}$).
- Soit $M\in\mathrm{GL}_2(\mathbb{Z})$.
On sait que $\det(M)=\pm 1$, donc M est inversible et $\det(M^{-1})=\frac{1}{\det(M)}=\pm 1$.
De plus, il existe $a,b,c,d\in\mathbb{Z}$ tels que $M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$.
On a alors $M^{-1}=\frac{1}{\det(M)}\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}=\pm\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z})$.

Par caractérisation des sous-groupes, $\mathrm{GL}_2(\mathbb{Z})$ est un sous-groupe de $\left(\mathrm{GL}_2(\mathbb{R}),\times\right)$.
Donc $\mathrm{GL}_2(\mathbb{Z})$ muni de $\times$ est un groupe.

3) Le calcul matriciel donne $A^2=-I_2$, $A^3=-A$ et $A^4=I_2$. A est donc d'ordre 4.
De même, $B^2=\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$ et $B^3=I_2$. B est donc d'ordre 3.
On a $C=AB=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$. Afin de calculer les puissances successives de C, on écrit $C=-I_2+N$ en posant $N=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$.
Cette matrice N commute avec I_2 et vérifie $N^2=0$. Donc la formule du binôme donne :

$$C^n=(-1)^nI_2+(-1)^{n-1}nN+0=(-1)^n\begin{pmatrix}1 & -n\\ 0 & 1\end{pmatrix}.$$

Remarque
On pouvait calculer les puissances successives de C par récurrence.

Donc $C^n \neq I_2$ pour $n \geqslant 1$. C est donc d'ordre infini.
On peut en conclure qu'il est possible que le produit de deux éléments d'ordre fini soit d'ordre infini.

Remarque
On peut aussi en déduire que A et B ne commutent pas. En effet, si $AB = BA$, on aurait $(AB)^{12} = A^{12}B^{12} = I_2$. Néanmoins, il suffit plus simplement de calculer BA pour constater $AB \neq BA$.

Exercice 13

1) Par définition de la loi produit, on a $(h,k)^n = (h^n, k^n)$ pour tout $n \in \mathbb{N}$. On sait que l'élément neutre de $H \times K$ est le couple $(1_H, 1_K)$.

$$(h,k)^n = 1_{H\times K} \iff (h^n,k^n) = (1_H,1_K)$$
$$\iff \begin{cases} h^n = 1_H \\ k^n = 1_K \end{cases}$$ (h est d'ordre p, k est d'ordre q)
$$\iff \begin{cases} p \mid n \\ q \mid n \end{cases}$$
$$\iff \text{ppcm}(p,q) \mid n.$$

Donc le plus petit entier naturel $n \geqslant 1$ tel que $(h,k)^n = 1_{H\times K}$ est $\text{ppcm}(p,q)$.
L'ordre de (h,k) est $\text{ppcm}(p,q)$.

2) On note h un générateur de H et k un générateur de K.
Donc h est d'ordre $p = \text{card}(H)$ et k est d'ordre $q = \text{card}(K)$.
On sait que $H \times K$ est de cardinal pq. Il est donc cyclique si, et seulement si, il possède un élément d'ordre pq.
Si p et q sont premiers entre eux, alors $\text{ppcm}(p,q) = pq$. D'après la question précédente (h,k) est d'ordre pq. En particulier, $H \times K$ est cyclique.
Si p et q ne sont pas premiers entre eux. Notons $r = \text{ppcm}(p,q)$. On a $r < pq$.
Soit $x \in H \times K$. Il existe $a \in K$ et $b \in K$ tels que $x = (a,b)$. On a $x^r = (a,b)^r = (a^r, b^r)$.
On a $a^r = 1_H$, car p divise r et $b^r = 1_K$, car q divise r. Donc $x^r = 1_{H\times K}$. L'ordre de r est donc strictement inférieur à pq (car il divise r).
$H \times K$ n'est pas cyclique.
On a montré que $H \times K$ est cyclique si, et seulement si, p et q sont premiers entre eux.

Exercice 14

On note p le cardinal de G.

1) Soit $z \in G$. On sait que $z^p = 1$. En particulier $|z| = 1$.
Donc $G \subset \{z \in \mathbb{C} \mid |z| = 1\}$.

CORRECTIONS

2) On a vu que $G \subset \mathbb{U}_p$ où $p = \text{card}(G)$.
Puisque $\mathbb{U}_p$ est aussi de cardinal p, on a $G = \mathbb{U}_p$.

Exercice 15

1) Puisque $\mathbb{U}_\infty = \bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ et que, pour tout $n \in \mathbb{N}^*$, $\exp\left(\frac{2i\pi}{n}\right) \in \mathbb{U}_n$, on a :

$$\left\{\exp\left(\frac{2i\pi}{n}\right), n \in \mathbb{N}^*\right\} \subset \mathbb{U}_\infty.$$

Or $\left(\frac{2\pi}{n}\right)_{n\in\mathbb{N}^*}$ est une suite de nombres 2 à 2 distincts de $]0, 2\pi]$, donc $\left(\exp\left(\frac{2i\pi}{n}\right)\right)_{n\in\mathbb{N}^*}$ est une suite de nombres complexes 2 à 2 distincts. Donc $\mathbb{U}_\infty$ est infini.

2) On sait que $(\mathbb{C}^*, \times)$ est un groupe.
- $\mathbb{U}_\infty$ est inclus dans $\mathbb{C}^*$.
- $\mathbb{U}_\infty$ est non vide (il est même infini).
- Soient z_1 et $z_2 \in \mathbb{U}_\infty$.
Notons n_1 et n_2 deux entiers naturels non nuls tels que $z_1^{n_1} = 1$ et $z_2^{n_2} = 1$.
On a $(z_1 z_2)^{n_1 n_2} = \left(z_1^{n_1}\right)^{n_2} \left(z_2^{n_2}\right)^{n_1} = 1$. Donc $z_1 z_2 \in \mathbb{U}_\infty$ (car $n_1 n_2 \in \mathbb{N}^*$).
$\mathbb{U}_\infty$ est stable par multiplication.
- Soient $z \in \mathbb{U}_\infty$ et $n \in \mathbb{N}^*$ tel que $z^n = 1$. On a alors $\left(z^{-1}\right)^n = (z^n)^{-1} = 1$. Donc $z^{-1} \in \mathbb{U}_\infty$.

Par caractérisation des sous-groupes, $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

3) On raisonne par l'absurde, on suppose qu'il existe une partie A finie et engendrant le sous-groupe $\mathbb{U}_\infty$.
En notant N le PPCM des ordres des éléments de A, on a pour tout $a \in A$, $a^N = 1$.
Comme la multiplication de $\mathbb{C}^*$ est commutative et que tout élément de $\mathbb{U}_\infty$ est un produit fini d'éléments de A, on aurait pour tout $z \in \mathbb{U}_\infty$, $z^N = 1$.
Or $\omega = \exp\left(\frac{i\pi}{N}\right)$ vérifie $\omega^N = \exp(i\pi) = -1$ et $\omega \in \mathbb{U}_\infty$, car $\omega^{2N} = 1$.
On a ainsi au moins un élément de $\mathbb{U}_\infty$ qui ne vérifie pas $z^N = 1$ ce qui constitue une contradiction.
On a prouvé que $\mathbb{U}_\infty$ n'est pas engendré par une partie finie.

Exercice 16

1) L'image de f est l'ensemble noté HK par l'énoncé.
Soit $(h, k) \in H \times K$. On va montrer que pour tout $(h_1, k_1) \in H \times K$:

$$f(h_1, k_1) = hk \iff \exists x \in H \cap K, h_1 = hx \text{ et } k_1 = x^{-1}k.$$

$\Rightarrow$ Soit $x \in H \cap K$. On pose $h_1 = hx$ et $k_1 = x^{-1}k$.
Puisque h et x appartiennent au sous-groupe H, $h_1 \in H$.
De même $k_1 \in K$, car k et x^{-1} appartiennent à ce sous-groupe.
De plus, on a $f(h_1, k_1) = hxx^{-1}k = hk$.

($\Leftarrow$) Soit $(h_1, k_1) \in K \times K$ tel que $h_1 k_1 = hk$.
En multipliant par h^{-1} à gauche et par k_1^{-1} à droite, on a $h^{-1}h_1 = kk_1^{-1}$.
Notons $x = h^{-1}h_1$. x appartient au sous-groupe H. Or $x = kk_1^{-1}$, donc x appartient aussi au sous-groupe K.
Donc $x \in H \cap K$. On a aussi $hx = h_1$ et $k_1 = x^{-1}k$.

Enfin, l'équivalence $(hx = hx' \iff x = x')$ montre qu'il y a autant de couples (h_1, k_1) tels que $f(h_1, k_1) = hk$ que d'éléments x dans $H \cap K$. Donc chaque élément de HK possède $\text{Card}(H \cap K)$ antécédents par f.

2) Notons $\tilde{f} : H \times K \to HK, (h, k) \mapsto hk$.
Par construction, $\tilde{f}$ est surjective. Tout élément de HK a exactement $n = \text{Card}(H \cap K)$ antécédents par $\tilde{f}$. Ce qui permet de former une partition de $H \times K$ en $\text{Card}(HK)$ parties, toutes de cardinal n. Donc $n\,\text{Card}(HK) = \text{Card}(H \times K) = \text{Card}(H)\text{Card}(K)$.
On a donc :

$$\text{Card}(HK)\text{Card}(H \cap K) = \text{Card}(H)\text{Card}(K).$$

Exercice 17

1) On sait que $a^{\text{card}(G)} = e$ et que $e \in H$, car H est un sous-groupe.
Donc l'ensemble $\{p \in \mathbb{N}^* \mid a^p \in H\}$ est non vide, car il contient $\text{card}(G)$. Il est inclus dans $\mathbb{N}$ et possède donc un minimum n.

2) Comme $a^n \in H$, le sous-groupe $\langle a^n \rangle$ engendré par a^n est un sous-groupe de H.
Il s'agit de voir que tout élément de H est un itéré de a^n.
Soit $x \in H$. Donc $x \in G$ et puisque a engendre G, il existe $p \geqslant 1$ tel que $x = a^p$.
On effectue la division euclidienne de p par n : $p = qn + r$ avec $0 \leqslant r \leqslant n - 1$.
On a alors $x = a^p = a^{nq}a^r$. Donc $a^r = (a^{nq})^{-1}x$. Or, $x \in H$ et $a^{nq} = (a^n)^q \in H$, donc $a^r \in H$ (car H est un sous-groupe). Par minimalité de n, on en déduit $r = 0$.
Donc $x = a^p = (a^n)^q \in \langle a^n \rangle$.
Finalement, on a prouvé que $H = \langle a^n \rangle$, donc que H est cyclique.

Exercice 18

1) $A \cup B$ est une partie de G de cardinal $\text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B) = 2n - 1$.
Donc il existe $c \in G$ tel que $A \cup B \cup \{c\} = G$.

2) Soient $a \in A \setminus \{e\}$ et $b \in B \setminus \{e\}$.
On raisonne par l'absurde. On suppose $a * b \neq c$. On a alors $a * b \in A \cup B$.
Les rôles de A et B étant symétriques, on peut supposer que $a * b \in A$ pour la démonstration . On a alors $b = a^{-1} * (a * b)$ qui appartiendrait au sous-groupe A. Donc $b \in A \cap B$.
On aurait donc $b \in \{e\}$ ce qui est impossible car $b \neq e$.
On a montré par l'absurde que $a * b = c$.

Donc :

$$\forall a \in A \setminus \{e\}, \forall b \in B \setminus \{e\}, \quad a * b = c.$$

Soient a et a' deux éléments de $A \setminus \{e\}$.

En utilisant un élément $b \in B \setminus \{e\}$, on a $a * b = c$ et $a' * b = c$. Donc $a * b = a' * b$ et, en multipliant par b^{-1} à droite, on obtient $a = a'$.

Donc $A \setminus \{e\}$ ne contient qu'un seul élément. D'où $n = 2$.

Remarque

On peut obtenir un exemple de cette situation en prenant $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et les sous-groupes $A = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ et $B = \{0\} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 19

1) En notant multiplicativement les lois, on a $x^p = e$, donc $f(x^p) = f(e)$. Or f étant un morphisme $f(e) = e'$ et $f(x)^p = f(x^p)$ (voir exercice 1), donc $f(x)^p = e'$. On peut donc affirmer que l'ordre de $f(x)$ dans G' est un diviseur de p.

Remarque

En version additive, on écrit $px = 0_G$, donc $pf(x) = f(px) = f(0_G) = 0_{G'}$.

2) Soit f un morphisme de groupe de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

Pour tout $x \in \mathbb{Z}/7\mathbb{Z}$, l'ordre de $f(x)$ divise 7 d'après la question précédente. Or $f(x)$ appartenant à $\mathbb{Z}/15\mathbb{Z}$, son ordre divise 15. Un entier naturel qui divise 7 et 15 est égal à 1. Donc $f(x)$ est d'ordre 1. Seul l'élément neutre étant d'ordre 1, on a $f(x) = 0$.

Donc f est l'application nulle.

Réciproquement, l'application nulle est un morphisme de groupe de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

3) Soit f un morphisme de groupe de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

On sait que $\mathbb{Z}/4\mathbb{Z}$ est un groupe cyclique engendré par la classe de 1 modulo 4 que nous noterons $\mathrm{cl}_4(1)$.

L'ordre de $f(\mathrm{cl}_4(1))$ divise 4 d'après la première question et appartenant à $\mathbb{Z}/6\mathbb{Z}$, son ordre divise également 6. Donc son ordre divise 2.

Si son ordre est 1, on obtient $f(\mathrm{cl}_4(1)) = 0$ et f est l'application nulle.

Si son ordre est 2. Alors $f(\mathrm{cl}_4(1)) = \mathrm{cl}_6(3)$ (seul élément de $\mathbb{Z}/6\mathbb{Z}$ dont l'ordre est 2).

On obtient ensuite pour tout $n \in \mathbb{Z}$, $f(n\mathrm{cl}_4(1)) = n\mathrm{cl}_6(3)$.

Ainsi, f est l'application qui, pour tout $n \in \mathbb{Z}$, associe à $\mathrm{cl}_4(n)$ l'élément $\mathrm{cl}_6(3n)$.

Cette application est bien définie, car si $n' \in \mathrm{cl}_4(n)$, il existe $k \in \mathbb{Z}$ tel que $n' = n + 4k$.

Donc $3n' = 3n + 12k$ et $\mathrm{cl}_6(3n') = \mathrm{cl}_6(3n)$.

Réciproquement, l'application nulle et l'application $f : \mathrm{cl}_4(n) \mapsto \mathrm{cl}_6(3n)$ précédente sont bien des morphismes de groupes (additifs) de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 20

On veut montrer qu'il existe $d \in \mathbb{N}^*$ tel que $N = 1 + 10 + 10^2 + \cdots + 10^{d-1}$ soit un multiple de 23.

Or, $\sum_{k=0}^{d-1} 10^k = \frac{10^d-1}{10-1} = \frac{10^d-1}{9}$. Il s'agit de prouver l'existence d'un d tel que $10^d - 1$ soit un multiple de $23 \times 9 = 207$.

Or, 10 est premier avec 207, donc la classe de 10 modulo 207 est dans le groupe des inversibles de $\mathbb{Z}/207\mathbb{Z}$. Cette classe est donc d'ordre fini dans ce groupe. Il existe $d \in \mathbb{N}^*$ tel que $10^d \equiv 1[207]$.

Il existe donc $q \in \mathbb{N}$ tel que $10^d - 1 = 23 \cdot 9q$. Donc $\frac{10^d-1}{9}$ est un multiple de 23 et il s'écrit uniquement avec des 1 en base dix.

Remarque

On peut être plus précis. Comme 9 et 23 sont premiers entre eux et que 9 divise $10^d - 1$, il suffit de chercher d tel que $10^d - 1$ soit un multiple de 23. On peut utiliser la démarche précédente dans $(\mathbb{Z}/23\mathbb{Z})^*$. L'ordre de la classe de 10 modulo 23 est un diviseur du cardinal du groupe des inversibles de $\mathbb{Z}/23\mathbb{Z}$, donc de $\varphi(23) = 22$ (car 23 est premier). En conclusion le nombre

$$N = \frac{10^{22} - 1}{9} = 1\,111\,111\,111\,111\,111\,111\,111$$

est un multiple de 23.

Exercices avec questions ouvertes

Exercice 21

Soit G un groupe de cardinal p avec p premier. On va montrer que G est un groupe monogène.

Soit a un élément de G autre que l'élément neutre e.

L'ordre de a devant diviser $|G| = p$ et ne pouvant être 1 (car $a \neq e$), a est d'ordre p. Donc G est engendré par a.

Donc G est un groupe monogène.

Exercice 22

On va montrer que l'ordre de xy est le même que celui de yx.

Soit $n \in \mathbb{N}^*$. On suppose $(xy)^n = e$ (l'élément neutre du groupe).

En multipliant par y à gauche, on a $y(xy)^n = ye = y$.

Puis, en multipliant par y^{-1} à droite : $y(xy)^n y^{-1} = yy^{-1} = e$.

D'autre part, en utilisant l'associativité de la loi :

$$\begin{aligned} y(xy)^n y^{-1} &= y\underbrace{(xy)(xy)\cdots(xy)(xy)}_{n \text{ fois}}y^{-1} \\ &= y\underbrace{(xy)(xy)\cdots(xy)}_{n-1 \text{ fois}}xyy^{-1} && \searrow\ yy^{-1}=e \\ &= y\underbrace{(xy)(xy)\cdots(xy)}_{n-1 \text{ fois}}x && \searrow\ \text{par associativité} \\ &= \underbrace{(yx)(yx)\cdots(yx)(yx)}_{n \text{ fois}} \\ &= (yx)^n. \end{aligned}$$

D'où finalement $(yx)^n = e$.
En échangeant les rôles de x et y, on obtient l'implication réciproque. Donc :

$$(yx)^n = e \quad \Leftrightarrow \quad (xy)^n = e.$$

Par conséquent, les éléments xy et yx ont le même ordre (fini ou non).

Exercice 23

1) Soient x et $y \in G$.
On a $(xy)^2 = e$ (d'après l'hypothèse faite sur G). Donc :

$$\begin{aligned} xy &= (xy)^{-1} \\ &= y^{-1}x^{-1} && \searrow\ \text{inverse d'un produit} \\ &= yx. && \searrow\ x^2 = e \text{ et } y^2 = e \end{aligned}$$

On a montré que $xy = yx$ pour tous x, y et donc $(G, \cdot)$ est un groupe abélien.

2) a) Par définition K est un sous-groupe de G contenant $\{x\} \cup H$.
Ainsi, $H \subset K$ et $x \in K$ et comme K est stable par produit, $xH \subset K$.
On a donc $H \cup xH \subset K$.
Réciproquement, $H \cup xH$ contient $\{x\} \cup H$ (car $x = x \cdot e \in xH$).
Montrons que $H \cup xH$ est un sous-groupe de G.
- $H \cup xH \subset G$
- $H \cup xH$ contient e, car $e \in H$ (H est un sous-groupe)
- Soient k_1 et k_2 deux éléments de $H \cup xH$. Quatre cas se présentent :
  - ⋆ Cas $k_1 \in H$ et $k_2 \in H$. On a $k_1k_2 \in H$, car H est un sous-groupe.
  - ⋆ Cas $k_1 \in xH$ et $k_2 \in H$. Il existe $h \in H$ tel que $k_1 = xh$.
    On a alors $k_1k_2 = xhk_2 \in xH$, car $hk_2 \in H$.
  - ⋆ Cas $k_1 \in xH$ et $k_2 \in H$. La loi étant commutative, on a $k_1k_2 \in xH$ d'après le cas précédent.
  - ⋆ Cas $k_1 \in xH$ et $k_2 \in xH$. Il existe $h_1, h_2 \in H$ tels que $k_1 = xh_1$ et $k_2 = xh_2$.
    On a alors :

$$\begin{aligned} k_1k_2 &= xh_1xh_2 \\ &= x^2h_1h_2 && \searrow\ \text{par commutativité} \\ &= h_1h_2. && \searrow\ x^2 = e \end{aligned}$$

Donc $k_1k_2 = h_1h_2 \in H$, car $h_1h_2 \in H$.
Dans tous les cas, $k_1k_2 \in H \cup xH$.
On a montré que $H \cup xH$ est stable par produit.

- Chaque élément étant son propre inverse, l'ensemble est stable par passage à l'inverse.

On a prouvé que $H \cup xH$ est un sous-groupe de G.
Comme K est le plus petit sous-groupe contenant $H \cup xH$, on a $K \subset H \cup xH$.
On a ainsi $K = H \cup xH$ par double inclusion.

b) On a $|K| = |H| + |xH| - |H \cap xH|$.
On a $|xH| = |H|$, car $f : H \to xH, h \mapsto xh$ est bijective [*].
Montrons que $H \cup xH = \emptyset$:
Si $h \in H \cup xH$, il existe $h_0 \in H$ tel que $h = xh_0$. Donc $x = hh_0^{-1} \in H$. C'est impossible, car $x \in G \setminus H$.
Compte tenu de tout cela, $|K| = |H| + |H| - 0 = 2|H|$.

3) Si G n'est pas réduit à $\{e\}$, son cardinal est pair, car l'ordre d'un élément divise le cardinal du groupe.
On va montrer (par l'absurde) que le cardinal de G est une puissance de 2.
On note $\mathcal{A}$ l'ensemble des sous-groupes de G dont le cardinal est une puissance de 2.
L'ensemble $\{|H|, H \in \mathcal{A}\}$ est alors une partie non vide de $\mathbb{N}$ (car $\mathcal{A}$ contient le sous-groupe $\{e\}$).
Cet ensemble admet donc un maximum et il existe un sous-groupe H de G tel que $|H|$ atteint ce maximum.
Si $|G|$ n'est pas une puissance de 2, on a $G \neq H$. Il existe $x \in G \setminus H$.
D'après la question précédente, $K = H \cup xH$ est un sous-groupe de G de cardinal $2|H|$.
Donc $K \in \mathcal{A}$ et $|K| > |H|$. C'est impossible par choix de H.
On a ainsi montré que $|G|$ est une puissance de 2.

Exercice 24

- D'après l'exercice 21, tout groupe de cardinal 2, 3 ou 5 est monogène donc commutatif.
- Soit $G = \{e, a, b, c\}$ un groupe de cardinal 4 (e désigne l'élément neutre). On va montrer que G est commutatif.
  - ⋆ Si l'un des éléments est d'ordre 4, alors G est monogène donc commutatif.
  - ⋆ Sinon, tous les éléments autres que e sont d'ordre 2. Il est classique (voir exercice 23) que G est commutatif. On peut proposer une démonstration plus élémentaire ici où $G = \{e, a, b, c\}$:
    Comme G est un groupe, $ab \in G$.
    Le cas $ab = a$ est impossible, car il entraînerait $b = a^{-1}a = e$. De même, $ab \neq b$.
    Le cas $ab = e$ est impossible, car alors on aurait $a^2b = a$, donc $b = a$ (car on a supposé $a^2 = e$).

[*] Sa bijection réciproque est $f^{-1} : xH \to H, y \mapsto x^{-1}y$.

Donc $ab = c$.
La même étude des cas possibles pour ba conduit à $ba = c$.
Ainsi, on a $ab = ba$.
Les rôles de a, b et c étant identiques, on a montré que G est commutatif.

Remarque
L'étude précédente montre qu'un groupe de cardinal 4 est soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (cas monogène), soit isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (cas où tous les éléments autres que l'élément neutre sont d'ordre 2).

⋆ On sait que $\mathfrak{S}_3$ est de cardinal $3! = 6$ et qu'il n'est pas commutatif, car les transpositions $\langle 1, 2\rangle$ et $\langle 1, 3\rangle$ ne commutent pas ($\langle 1, 2\rangle \circ \langle 1, 3\rangle = \langle 1, 3, 2\rangle$ et $\langle 1, 3\rangle \circ \langle 1, 2\rangle = \langle 1, 2, 3\rangle$).

En conclusion, 6 est le plus petit entier n pour lequel il existe un groupe de cardinal n non commutatif.

Exercice 25

1) Si G est fini, il y a un nombre fini de parties de G. En particulier, G a un nombre fini de sous-groupes.

2) Réciproquement, supposons que G ait un nombre fini de sous-groupes.

• Montrons que tout élément de G est d'ordre fini.

On raisonne par l'absurde. On suppose qu'il existe $x \in G$ d'ordre infini. Notons $H_k = \langle x^k \rangle$ pour $k \in \mathbb{N}$.

Soient k et $k' \in \mathbb{N}$. Montrons que si $H_k = H_{k'}$, alors $k = k'$.

Si $H_k = H_{k'}$, alors $x^k \in H_{k'}$. Donc il existe $p \in \mathbb{Z}$ tel que $x^k = x^{pk'}$. Or, x étant d'ordre infini, cela entraînerait que $k = pk'$. Donc k' divise k. Les rôles étant symétriques, on obtient aussi k divise k'. Finalement $k = k'$.

Donc les sous-groupes H_k pour $k \in \mathbb{N}$ sont deux à deux distincts.

On aurait une infinité de sous-groupes distincts, ce qui est impossible.

On a montré par l'absurde que tout élément est d'ordre fini.

• Montrons que G est fini.

En remarquant que $G = \bigcup_{x \in G} \langle x \rangle$, on en déduit, puisqu'il existe un nombre fini de sous-groupes distincts, qu'il existe $x_1, x_2, \ldots, x_n$ tels que :

$$G = \bigcup_{k=1}^{n} \langle x_k \rangle.$$

Or, les sous-groupes $\langle x_k \rangle$ sont finis, donc $G = \bigcup_{k=1}^{n} \langle x_k \rangle$ l'est aussi.

Exercice 26

Soit $\varphi : \mathbb{Q} \to \mathbb{Z}$ un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
On a en particulier :

$$\forall q \in \mathbb{N}^*, \quad \varphi(1) = \varphi\left(q\frac{1}{q}\right) = q\varphi\left(\frac{1}{q}\right).$$

Comme φ est à valeurs dans $\mathbb{Z}$, $\varphi(1)$ est ainsi un entier divisible par tout $q \in \mathbb{N}^*$. On a donc $\varphi(1) = 0$. Puis, pour tout $q \in \mathbb{N}^*$, $\varphi(1/q) = 0$ puisque $q\varphi(1/q) = \varphi(1) = 0$.
Finalement :

$$\forall p \in \mathbb{Z}, \forall q \in \mathbb{N}^*, \quad \varphi\left(\frac{p}{q}\right) = p\varphi\left(\frac{1}{q}\right) = 0.$$

φ est donc l'application nulle.
Réciproquement, l'application nulle est un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 27

Notons d l'ordre de σ. Montrons que si d est impair, alors $\varepsilon(\sigma) = 1$.
On sait que $\sigma^d = \mathrm{Id}_{[\![1,n]\!]}$ et que la signature est un morphisme de groupes donc :

$$\varepsilon(\sigma)^d = \varepsilon\left(\sigma^d\right) = \varepsilon\left(\mathrm{Id}_{[\![1,n]\!]}\right) = 1.$$

Comme d est impair, $\varepsilon(\sigma) = -1$ est impossible. Donc $\varepsilon(\sigma) = 1$.

En revanche, il n'y a pas de résultat général lorsque d est pair.
Par exemple, une transposition est d'ordre 2 et est de signature -1, alors que le produit $\langle 1, 2\rangle \circ \langle 3, 4\rangle$ est aussi d'ordre 2 mais de signature 1.

Exercice 28

Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de groupes continu sur $\mathbb{R}$.
Par une démonstration semblable à celle de l'exercice 2, on a :

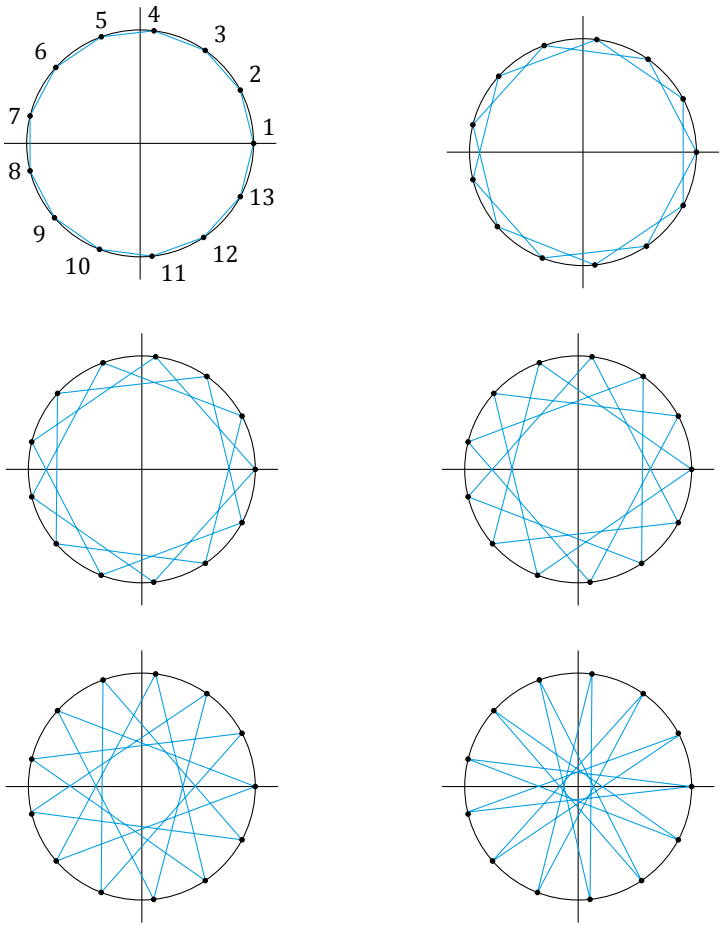
$$\forall r \in \mathbb{Q}, \quad f(r) = rf(1).$$

Pour $x \in \mathbb{R}$, on sait qu'il existe une suite $(r_n)_{n\in\mathbb{N}}$ de rationnels convergeant vers x. Par continuité de f, on a $f(r_n) \xrightarrow[n\to\infty]{} f(x)$. Or, $f(r_n) = r_n f(1) \xrightarrow[n\to\infty]{} xf(1)$.
Par unicité de la limite, on obtient $f(x) = xf(1)$.
Donc f est linéaire.
Réciproquement pour $a \in \mathbb{R}$, l'application $x \mapsto ax$ est continue sur $\mathbb{R}$ et est un morphisme de groupes.
Les morphismes de groupes continus de $(\mathbb{R}, +)$ dans lui-même sont les applications linéaires de $\mathbb{R}$ dans $\mathbb{R}$.

« *Si a est d'ordre n, alors $a^k = e \iff n|k$.* »

CORRECTIONS

Anneaux 2



13 est un nombre premier et donc $\mathbb{Z}/13\mathbb{Z}$ est un corps et donc chaque $\overline{k}$ pour $k \in [\![1, 12]\!]$ est un générateur du groupe $(\mathbb{Z}/13\mathbb{Z}, +)$ qui correspond à un polygone régulier (à 13 côtés). On a dessiné uniquement 6 polygones car chacun d'entre eux correspond à deux générateurs (un pour chaque sens de rotation).

Exercices axés sur le calcul

Exercice 1

Soit p un nombre premier. Dans $\mathbb{Z}/p\mathbb{Z}$, calculer les sommes $s_1 = \sum_{k=1}^{p} \overline{k}$ et $s_2 = \sum_{k=1}^{p} \overline{k}^{-2}$.

Exercice 2

Résoudre dans $\mathbb{Z}$ le système $(\mathcal{H})\begin{cases} x \equiv 0\ [10] \\ x \equiv 0\ [13] \end{cases}$, puis le système $(S)\begin{cases} x \equiv 2\ [10] \\ x \equiv 5\ [13] \end{cases}$.

Exercice 3

Déterminer le groupe des inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$. Ce groupe est-il cyclique ?

Exercice 4

Soit $A = \left\{ \frac{m}{2^n} \,\middle|\, m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$.

1) Montrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2) Quels en sont les éléments inversibles ?

Exercice 5

Soit E l'ensemble des matrices de la forme $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}$ avec a et b réels.

1) Montrer que E est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$ et donner sa dimension.
2) Montrer que E est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$, puis que E est un corps.
3) Résoudre dans E, l'équation $X^2 = I_2$.

D'après CCINP

Exercice 6 ⋆ *Symbole de Pochhammer*

Soit $(A, +, \times)$ un anneau commutatif. Pour $x \in A$ et $n \in \mathbb{N}$, on définit $x^{(n)}$ par :

$$x^{(0)} = 1_A, \qquad x^{(n)} = x(x-1)\cdots(x-n+1).$$

Montrer que pour tous x et $y \in A$ et tout $n \in \mathbb{N}$, on a :

$$(x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}.$$

Exercices axés sur le raisonnement

Exercice 7 *Classique*

Soit $(A, +, \times)$ un anneau. On note 1 l'élément unité.

1) Soient a un élément nilpotent et $n \in \mathbb{N}^*$ tels que $a^n = 0$.
   a) Montrer que $1 - a$ est inversible et préciser son inverse.
   b) En déduire que $b = 1 + 2a + \cdots + na^{n-1}$ est inversible.
2) Soient a et $b \in A$ tels que ab soit nilpotent.
   Montrer que ba est nilpotent.
3) Dans cette question, on suppose que l'anneau A est commutatif et on note N l'ensemble des éléments nilpotents.
   Montrer que N est un idéal de l'anneau A.

Exercice 8 *Radical d'un idéal*

Soient $(A, +, \times)$ un anneau commutatif et I un idéal de A.
On note $R(I)$ l'ensemble des éléments x de A tel qu'il existe n dans $\mathbb{N}^*$ tel que $x^n \in I$.

1) Montrer que $R(I)$ est un idéal de A contenant I.
2) On considère l'ensemble $E = \{n \in \mathbb{N}^* \mid R(n\mathbb{Z}) = n\mathbb{Z}\}$.
   Montrer que E est l'ensemble des entiers naturels qui ne sont pas divisibles par le carré d'un nombre premier.

D'après Mines-Télécom

Exercice 9 *Classique*

Soit p un nombre premier supérieur à 3. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On rappelle que $\mathbb{F}_p$ est un corps.

1) Montrer que $f : x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{F}_p^*, \times)$ dans lui-même.
2) Montrer que $\mathrm{Ker}(f) = \left\{\overline{1}, -\overline{1}\right\}$.
3) Montrer que pour tout $x \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}} = \overline{1}$ ou $-\overline{1}$.
4) Montrer qu'il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

D'après CCINP

Exercice 10 *Un anneau qui n'est pas un sous-anneau*

On considère le sous-espace vetoriel E engendré par les deux matrices réelles suivantes

$$A = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \text{ et } B = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}.$$

1) Montrer que $(E, +, \times)$ (où $\times$ est la multiplication matricielle usuelle) est un anneau, mais que ce n'est pas un sous-anneau de $\mathcal{M}_3(\mathbb{R})$.

2) La matrice A est-elle inversible dans $\mathcal{M}_3(\mathbb{R})$? Admet-elle un inverse dans l'anneau E c'est-à-dire une matrice $M \in E$ telle que $MA = AM = 1_E$ où 1_E désigne l'élément neutre pour $\times$ dans l'anneau E ?

Exercice 11 *Anneau de Boole*

Soit $(A, +, \times)$ un anneau. On suppose que :

$$\forall x \in A, \quad x^2 = x. \qquad (\star)$$

1) Montrer que pour tout $x \in A$, $2x = 0$.
2) Montrer que A est commutatif.
   Indication : On pourra envisager $(x + y)^2$.
3) Quels sont les éléments inversibles de A ?

Exercice 12

Soient a et n des entiers naturels strictement supérieurs à 1. On note $N = a^n - 1$.

1) Montrer que $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/N\mathbb{Z}$ et déterminer l'ordre de a dans le groupe des inversibles $U(\mathbb{Z}/N\mathbb{Z})$.
2) En déduire que n divise $\varphi(N)$ (φ désigne l'indicatrice d'Euler).

Exercice 13 ⋆

1) *Étude d'un exemple*
   Soit $k \in \mathbb{N}^*$. Préciser les diviseurs de 0 de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.
2) On considère A un anneau commutatif fini. On suppose que A possède n diviseurs de zéro, avec $n > 1$.
   a) Soit a un diviseur de 0.
      Montrer que $f : A \to A, x \mapsto ax$ est un morphisme de groupes de $(A, +)$ dans lui-même et que tout élément $y \in \mathrm{Im}(f)$ admet exactement $\mathrm{card}\big(\mathrm{Ker}(f)\big)$ antécédents.
   b) En déduire que A a au plus $(n + 1)^2$ éléments.

D'après ENS

Exercices avec questions ouvertes

Exercice 14

Que peut-on dire d'un anneau commutatif A dont les seuls idéaux sont $\{0\}$ et A ?

Exercice 15

Quels sont les morphismes d'anneaux de $(\mathbb{Z}, +, \times)$ dans lui-même ?

Exercice 16 *Classique*

Quels sont les morphismes d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même ?
Indication : On pourra montrer qu'un tel morphisme est croissant.

D'après Mines-Télécom

Exercice 17 ⋆⋆

Soit $(A, +, \times)$ un anneau.

1) Montrer que si la multiplication est commutative, alors $f : A \to A, x \mapsto x^2$ est un morphisme multiplicatif, c'est-à-dire qu'on a :

$$\forall x, y \in A, \quad (xy)^2 = x^2 y^2. \qquad (\star)$$

2) La réciproque est-elle vraie ?
Indication : On pourra commencer par utiliser $(\star)$ pour x et $1_A + y$.

Corrections

Exercices axés sur le calcul

Exercice 1

Notons $S_1 = \sum_{k=1}^{p} k$ et $S_2 = \sum_{k=1}^{p} k^2$. Ce sont des entiers naturels et on a $s_1 = \overline{S_1}$ et $s_2 = \overline{S_2}$.

On sait que $S_1 = \sum_{k=1}^{p} k = \frac{p(p+1)}{2}$. Donc 2 divise $p(p+1)$. Distinguons deux cas :

- Si $p = 2$, $S_1 = 3$, donc $S_1 \equiv 1\ [2]$. D'où $s_1 = \overline{1}$ dans $\mathbb{Z}/2\mathbb{Z}$.
- Sinon p est impair, donc $\frac{p+1}{2} \in \mathbb{N}$. D'où S_1 est un multiple de p et $s_1 = \overline{0}$.

De même $S_2 = \sum_{k=1}^{p} k^2 = \frac{p(p+1)(2p+1)}{6}$. Distinguons trois cas :

- Si $p = 2$, $S_2 = 5$ donc $S_2 \equiv 1\ [2]$. Donc $s_2 = \overline{1}$ dans $\mathbb{Z}/2\mathbb{Z}$.
- Si $p = 3$, $S_2 = 14$ donc $S_2 \equiv 2\ [3]$. Donc $s_2 = \overline{2}$ dans $\mathbb{Z}/3\mathbb{Z}$.
- Sinon p et 6 sont premiers entre eux donc 6 divise $(p+1)(2p+1)$. Donc S_2 est un multiple de p et $s_2 = \overline{0}$.

Exercice 2

On a $(x \equiv 0\ [13] \iff 13|x)$ et $(x \equiv 0\ [10] \iff 10|x)$. Puisque 10 et 13 sont premiers entre eux, on obtient :

$$\begin{cases} x \equiv 0\ [10] \\ x \equiv 0\ [13] \end{cases} \iff 130|x \iff \exists q \in \mathbb{Z}, x = 130q.$$

Soit x_0 une solution de (S). On a pour tout $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \begin{cases} x - x_0 \equiv 0 \ [10] \\ x - x_0 \equiv 0 \ [13] \end{cases} \iff \exists q \in \mathbb{Z}, x = x_0 + 130q.$$

Il reste à déterminer une solution [particulière] x_0.

Première méthode (méthode générale)

Soit $x \in \mathbb{Z}$.

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \exists k, k' \in \mathbb{Z}, \begin{cases} x = 2 + 10k \\ x = 5 + 13k' \end{cases}$$

$$\iff \exists k, k' \in \mathbb{Z}, \begin{cases} x = 2 + 10k \\ 10k - 13k' = 3 \end{cases}$$

Puisque 10 et 13 sont premiers entre eux, on sait qu'il existe des coefficients (dits de Bézout) u et v entiers tels que $10u + 13v = 1$.
En écrivant l'algorithme d'Euclide (ou en devinant), on constate que $10 \cdot 4 - 13 \cdot 3 = 1$. On a donc $10 \cdot 12 - 13 \cdot 9 = 3$. Donc $x_0 = 2 + 10 \cdot 12 = 122$ est une solution de (S).

Deuxième méthode (en utilisant les inverses de $\mathbb{Z}/13\mathbb{Z}$)

Soient $k \in \mathbb{Z}$ et $x = 2 + 10k$. On a ainsi $x \equiv 2 \ [10]$. Puis :

$x \equiv 5 \ [13] \iff 10k \equiv 3 \ [13]$.

Or, $4 \cdot 10 = 40 \equiv 1 \ [13]$ donc l'inverse de $\overline{10}$ dans $\mathbb{Z}/13\mathbb{Z}$ est $\overline{4}$. Donc

$x \equiv 5 \ [13] \iff k \equiv 4 \cdot 3 \ [13]$.

On peut choisir $k = 12$ et on a ainsi une solution particulière $x_0 = 2 + 120 = 122$.

Remarque

On a préféré travailler dans $\mathbb{Z}/13\mathbb{Z}$, car c'est un corps, mais on aurait pu travailler dans l'anneau $\mathbb{Z}/10\mathbb{Z}$ et déterminer l'inverse de la classe de 13 modulo 10 (c'est la classe de 7 car $7 \cdot 13 = 91 \equiv 1 \ [10]$).

Finalement :

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \exists q \in \mathbb{Z} \mid x = 122 + 130q.$$

Exercice 3

Parmi les entiers de 1 à 7, ceux qui sont premiers avec 8 sont 1, 3, 5 et 7. On a donc :

$$U(\mathbb{Z}/8\mathbb{Z}) = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}.$$

$\overline{1}$ est d'ordre 1. On a $\overline{3}^2 = \overline{9} = \overline{1}$. Donc $\overline{3}$ est d'ordre 2. Il n'engendre pas le groupe $\left(U(\mathbb{Z}/8\mathbb{Z}), \cdot\right)$.
De même $\overline{5}^2 = \overline{25} = \overline{1}$ et $\overline{7}^2 = \overline{49} = \overline{1}$, les éléments $\overline{5}$ et $\overline{7}$ sont aussi d'ordre 2.
Aucun des quatre éléments de $U(\mathbb{Z}/8\mathbb{Z})$ n'engendre le groupe $\left(U(\mathbb{Z}/8\mathbb{Z}), \cdot\right)$. Ce groupe n'est donc pas cyclique.

Exercice 4

1) Il est immédiat que $\mathbb{Z} \subset \mathbb{Q}$.
Pour tout $m \in \mathbb{Z}, m = \frac{m}{2^0}$, donc $\mathbb{Z} \subset A$ et en particulier A contient 1.
Soient a_1 et $a_2 \in A$. Pour $i \in \{1, 2\}$, on choisit $m_i \in \mathbb{Z}$ et $n_i \in \mathbb{N}$ tels que $a_i = \frac{m_i}{2^{n_i}}$.
On a alors :
- $-a_1 = \frac{-m_1}{2^{n_1}} \in A$;
- $a_1 + a_2 = \frac{m_1}{2^{n_1}} + \frac{m_2}{2^{n_2}} = \frac{2^{n_2}m_1 + 2^{n_1}m_2}{2^{n_1+n_2}}$, donc $a_1 + a_2 \in A$ (car $2^{n_2}m_1 + 2^{n_1}m_2 \in \mathbb{Z}$) ;
- $a_1a_2 = \frac{m_1}{2^{n_1}} \cdot \frac{m_2}{2^{n_2}} = \frac{m_1m_2}{2^{n_1+n_2}}$, donc $a_1a_2 \in A$.

Donc A est un sous-anneau de $(\mathbb{Q}, +, \times)$.

2) Soient $r = \frac{m}{2^n}$ avec $m \in \mathbb{Z}^*$ et $n \in \mathbb{N}$ un élément inversible de l'anneau A.
Il existe $r' = \frac{m'}{2^{n'}}$ avec $m' \in \mathbb{Z}^*$ et $n' \in \mathbb{N}$ tels que $rr' = 1$. D'où $2^{n+n'} = mm'$.
Donc m est une puissance de 2 (seul nombre premier pouvant diviser $2^{n+n'}$).
Il existe $k \in \mathbb{N}$ tel que $m = \pm 2^k$. Et donc $r = \pm 2^{k-n}$.

Les éléments inversibles sont de la forme $\pm 2^a$ avec $a \in \mathbb{Z}$.

Réciproquement, montrons que ces nombres sont inversibles dans A :
- Si $r = \pm 2^k$ avec $k \in \mathbb{N}$. On a $r \in \mathbb{Z}$, donc $r \in A$ et $r^{-1} = \pm\frac{1}{2^k} \in A$.
- Sinon $r = \pm\frac{1}{2^k}$ avec $k \in \mathbb{N}^*$. On a $r \in A$ et $r^{-1} = \pm 2^k \in A$.

On a montré :

$$U(A) = \{\pm 2^a, a \in \mathbb{Z}\}.$$

Exercice 5

1) Notons $J = \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$ ainsi $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} = aI_2 + bJ$.
Donc $E = \text{Vect}(I_2, J)$ et E est un espace vectoriel. La famille génératrice trouvée étant libre (J n'est pas colinéaire à I_2), E est de dimension 2.

2) • Puisque E est un sous-espace vectoriel, E est un sous-groupe de $(\mathcal{M}_2(\mathbb{R}), +)$.
• E contient le neutre I_2.
• Stabilité pour la multiplication
Soient $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} \in E$ et $M' = \begin{pmatrix} a' & 2b' \\ -b' & a' \end{pmatrix} \in E$.

$$MM' = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - 2bb' & 2(ab' + ba') \\ -(ba' + ab') & aa' - 2bb' \end{pmatrix} \in E.$$

Donc E est un sous-anneau de $(\mathcal{M}_2(\mathbb{R}), +, \times)$.

CORRECTIONS

Remarque

En utilisant la base trouvée et le développement :

$$(aI_2 + bJ)(a'I_2 + b'J) = aa'I_2 + (ab' + b'a)J + bb'J^2,$$

il suffisait, compte tenu de la stabilité par combinaison linéaire, de vérifier que la matrice $J^2 = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$ appartient effectivement à E.

Le calcul précédent montre également que deux matrices de E commutent pour $\times$.

Soit $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} \in E \setminus \{0\}$.

On a $(a, b) \neq (0, 0)$ et $\det(M) = a^2 + 2b^2 > 0$ (a et b sont des réels et au moins un des deux est non nul). Donc $\det(M) \neq 0$ ce qui prouve que M est inversible.

En outre, on a $M^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \in E$, car $a' = \frac{a}{\det(A)}$ et $b' = -\frac{b}{\det(A)}$ sont des réels.

Donc $(E, +, \times)$ est un anneau commutatif et tout élément non nul est inversible : c'est un corps.

3) Avec $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}$, on a $M^2 = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} = \begin{pmatrix} a^2 - 2b^2 & 4ab \\ -2ab & a^2 - 2b^2 \end{pmatrix}$. Donc :

$$M^2 = I_2 \iff \begin{cases} a^2 - 2b^2 = 1 \\ 2ab = 0 \end{cases} \iff \begin{cases} b = 0 \\ a^2 = 1 \end{cases} \text{ ou } \begin{cases} a = 0 \\ b^2 = -1/2 \end{cases}.$$

Le second système n'a pas de solution avec $b \in \mathbb{R}$.

L'équation $X^2 = I_2$ a deux solutions dans E qui sont I_2 et $-I_2$

Exercice 6

Soient x et $y \in A$.

Pour $n \in \mathbb{N}$, on note $\mathcal{P}_n$ la proposition « $(x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}$ ».

Pour $n = 0$, on a $(x+y)^{(0)} = 1_A$ et $\sum_{k=0}^{0} \binom{0}{k} x^{(k)} y^{(0-k)} = \binom{0}{0} x^{(0)} y^{(0)} = 1_A$, donc $\mathcal{P}_0$ est vraie.

Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie. On a alors :

$$\begin{aligned} (x+y)^{(n+1)} &= (x+y)^{(n)}(x+y-n) \\ &= \left(\sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}\right)(x+y-n) \quad \text{d'après } \mathcal{P}_n \\ &= \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}(x+y-n). \quad \text{par distributivité} \end{aligned}$$

Puis on utilise $x + y - n = x - k + y - (n-k)$ et on transforme $(x+y)^{(n+1)}$ en $S_1 + S_2$ avec $S_1 = \sum_{k=0}^{n} \binom{n}{k} x^{(k)}(x-k) y^{(n-k)}$ et $S_2 = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}\big(y - (n-k)\big)$.

Puisque $x^{(k)}(x-k) = x^{(k+1)}$, on a :

$$\begin{aligned} S_1 &= \sum_{k=0}^{n} \binom{n}{k} x^{(k+1)} y^{(n-k)} \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} x^{(k)} y^{(n-k)} && \text{par changement d'indice} \\ &= 1x^{(n+1)}y^{(0)} + \sum_{k=1}^{n} \binom{n}{k-1} x^{(k)} y^{(n-k)} && \binom{n}{n} = 1 \\ &= x^{(n+1)} + \sum_{k=1}^{n} \binom{n}{k-1} x^{(k)} y^{(n-k)}. && y^{(0)} = 1_A \end{aligned}$$

De même, $y^{(n-k)}\big(y-(n-k)\big) = y^{(n-k+1)}$ et :

$$\begin{aligned} S_2 &= \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k+1)} \\ &= 1x^{(0)}y^{(n+1)} + \sum_{k=1}^{n} \binom{n}{k} x^{(k)} y^{(n-k+1)} && \binom{0}{0} = 1 \\ &= y^{(n+1)} + \sum_{k=1}^{n} \binom{n}{k} x^{(k)} y^{(n-k+1)}. && x^{(0)} = 1_A \end{aligned}$$

Donc :

$$\begin{aligned} (x+y)^{(n+1)} &= S_1 + S_2 \\ &= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) x^{(k)} y^{(n-k+1)} \\ &= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^{n} \binom{n+1}{k} x^{(k)} y^{(n-k+1)} && \text{formule de Pascal} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{(k)} y^{(n-k+1)}. \end{aligned}$$

Cela montre que $\mathcal{P}_{n+1}$ est vraie.

On a montré par récurrence que :

$$\forall n \in \mathbb{N}, \quad (x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}.$$

Exercices axés sur le raisonnement

Exercice 7

1) a) Puisque $a^n = 0$, on a $1 = 1 - a^n$. D'où :

$$1 = (1-a)(1+a+a^2+\cdots+a^{n-1}) = (1+a+a^2+\cdots+a^{n-1})(1-a).$$

Donc $1-a$ est inversible et son inverse est $1+a+a^2+\cdots+a^{n-1}$.

CORRECTIONS

b) D'après les règles de calculs dans l'anneau, on a :

$$(1-a)b = 1+2a+\cdots+na^{n-1}-a-2a^2-\cdots-(n-1)a^{n-1}-0 = 1+a+a^2+\cdots+a^{n-1}.$$

D'après la question précédente, on a $(1-a)^2 b = 1$. De même, $b(1-a)^2 = 1$.
Donc $b = 1 + 2a + \cdots + na^{n-1}$ est inversible.

2) Soit $n \in \mathbb{N}^*$ tel que $(ab)^n = 0$. On a :

$$(ba)^{n+1} = b(ab)\cdots(ab)a = b(ab)^n a = b \cdot 0 \cdot a = 0.$$

Donc ba est nilpotent.

3) • N est un sous groupe de $(A, +)$

- N est une partie de A qui contient 0.
- Stabilité pour l'addition
  Soient a et b deux éléments nilpotents de A. Il existe n et $m \in \mathbb{N}^*$ tels que $a^n = 0$ et $b^m = 0$.
  Puisque l'anneau est commutatif, la formule du binôme donne :

$$(a+b)^{n+m} = \sum_{k=0}^{n-1} \binom{n+m}{k} a^k b^{n+m-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

  Or, pour $k \geqslant n$, $a^k = 0$, donc tous les termes de la seconde somme sont nuls.
  De même, dans la première somme, on a $b^{n+m-k} \geqslant m$, donc $b^{n+m-k} = 0$.
  Finalement, $(a+b)^{n+m} = 0$. Donc $a + b \in N$.
- Si $a^n = 0$, on a $(-a)^n = (-1)^n a^n = 0$.

On a montré que N est un sous-groupe de $(A, +)$.

• Stabilité par multiplication quelconque

Soient $a \in N$ et $x \in A$. Il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

Comme la multiplication est commutative, on a $(xa)^n = x^n a^n = x^n 0 = 0$. Donc $xa \in N$.

On a montré que N est un idéal de l'anneau A.

Exercice 8

1) Il est immédiat que $I \subset R(I)$ (si $x \in I$, on a $x^1 = x \in I$). En particulier, $R(I)$ est non vide.
Soient x et $y \in R(I)$. Il existe $n, m \in \mathbb{N}^*$ tels que $x^n \in I$ et $y^m \in I$.
L'anneau étant commutatif, la formule du binôme donne :

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Pour $k \geqslant n$, $x^k y^{n+m-k} = x^{k-n} y^{n+m-k} \times x^n \in I$, car I est un idéal.
Pour $k \leqslant n$, on a de même $x^k y^{n+m-k} = x^k y^{n-k} \times y^m \in I$.
$(I, +)$ étant un groupe, on a $(x+y)^{n+m} \in I$ (par addition) et donc $x + y \in R(I)$.

Et $(-x)^n = (-1_A)^n x^n \in I$, donc $-x \in R(I)$.
On a montré que $R(I)$ est un sous-groupe de $(A, +)$.

Soient $x \in R(I)$ et $n \in \mathbb{N}^*$ tels que $x^n \in I$.
Pour tout $z \in A$, la loi étant commutative, on a $(zx)^n = z^n x^n \in I$ et donc $zx \in R(I)$.
$R(I)$ est ainsi un idéal (et il contient I).

2) On travaille ici dans l'anneau $(\mathbb{Z}, +, \times)$ qui est bien commutatif. On sait aussi qu'il est principal, c'est-à-dire que les idéaux sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
Pour tout entier n, on a $n\mathbb{Z} \subset R(n\mathbb{Z})$ (question précédente). Il s'agit donc de trouver les n pour lesquels l'inclusion réciproque est vraie.

• Soit $n \in \mathbb{N}^*$ tel que $R(n\mathbb{Z}) = n\mathbb{Z}$.
Décomposons n en produit de facteurs premiers : $n = p_1^{a_1} \dots p_k^{a_k}$.
En notant $m = p_1 \cdot p_2 \dots p_k$. On a $m^{\max(a_1,\dots,a_k)}$ est multiple de n, donc $m \in R(n\mathbb{Z})$.
Donc $m \in n\mathbb{Z}$ puisque $R(n\mathbb{Z}) = n\mathbb{Z}$.
L'entier $p_1 \cdot p_2 \dots p_k$ étant un multiple de $n = p_1^{a_1} \dots p_k^{a_k}$, tous les a_i sont égaux à 1.
• Réciproquement, soit $n = p_1 \cdot p_2 \dots p_k$ (où les p_j sont des nombres premiers deux à deux distincts).
Montrons l'inclusion $R(n\mathbb{Z}) \subset n\mathbb{Z}$.
Soit $m \in R(n\mathbb{Z})$. Il existe $k \in \mathbb{N}^*$ tel que $m^k \in n\mathbb{Z}$. Chacun des nombres premiers p_j divisant n devant diviser m^k, on a p_j divise m^k donc divise m.
Donc $n = p_1 \cdot p_2 \dots p_k$ divise m, c'est-à-dire $m \in n\mathbb{Z}$.

On a donc montré :
$R(n\mathbb{Z}) = n\mathbb{Z}$ si, et seulement si, n n'est pas divisible par le carré d'un nombre premier.

Exercice 9

1) On sait que $(\mathbb{F}_p^*, \times)$ est un groupe commutatif. Donc pour tout $x \in \mathbb{F}_p^*, x^2 \in \mathbb{F}_p^*$ et :

$$\forall x, y \in \mathbb{F}_p^*, \quad f(xy) = (xy)^2 = x^2 y^2 = f(x) f(y).$$

Donc $f : x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{F}_p^*, \times)$ dans lui-même.

2) Soit $x \in \mathbb{F}_p^*$.

$$\begin{aligned} x \in \mathrm{Ker}(f) &\iff f(x) = \overline{1} && \text{par définition de } f \\ &\iff x^2 = \overline{1} && \text{calcul dans } (\mathbb{F}_p, +) \\ &\iff x^2 - \overline{1} = \overline{0} && \text{calcul dans l'anneau} \\ &\iff \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0} && \mathbb{F}_p \text{ est un corps} \\ &\iff x - \overline{1} = \overline{0} \quad \text{ou} \quad x + \overline{1} = \overline{0}. \end{aligned}$$

On a montré que $\mathrm{Ker}(f) = \left\{\overline{1}, -\overline{1}\right\}$.

CORRECTIONS

3) Soit $x \in \mathbb{F}_p^*$. L'entier p étant impair, on a $\frac{p-1}{2} \in \mathbb{N}$ et l'élément $y = x^{\frac{p-1}{2}}$ est bien défini.
On a alors $y^2 = x^{p-1}$. Or, $p-1$ est le cardinal du groupe $\mathbb{F}_p^*$, donc $x^{p-1} = \overline{1}$ (car l'ordre de x divise $p-1$).
Donc $y^2 = 1$. D'après la question précédente, $y = \pm\overline{1}$, donc $x^{\frac{p-1}{2}} = \overline{1}$ ou $-\overline{1}$.

4) Soient $C = \{a^2, a \in \mathbb{F}_p^*\}$ l'ensemble des carrés de $\mathbb{F}_p^*$ et $\hat{f} : \mathbb{F}_p^* \to C, x \mapsto x^2$.
Par construction $\hat{f}$ est surjective. Donc $\mathbb{F}_p^* = \bigcup_{c \in C} \hat{f}^{-1}(\{c\})$. Or, tout élément de C a exactement deux antécédents distincts par $\tilde{f}$ car :

$$x^2 = a^2 \iff x^2 - a^2 = \overline{0} \iff (x - a = \overline{0} \text{ ou } x + a = \overline{0}).$$

Ainsi, on peut former une partition de $\mathbb{F}_p^*$ en $\mathrm{Card}(C)$ parties du type $\{a, -a\}$, toutes de cardinal 2 (car $a \neq -a$). Donc $2\,\mathrm{Card}(C) = \mathrm{Card}(\mathbb{F}_p^*) = p-1$.
Donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

Exercice 10

1) On sait que E est un sous-espace vectoriel. En particulier, $(E, +)$ est un groupe.
Pour a et b réels, on a $aA+bB = \begin{pmatrix} -a-b & b & a \\ a & -a-b & b \\ b & a & -a \end{pmatrix}$. Il n'existe pas de couple (a, b) tel que $aA + bB = I_3$ donc $I_3 \notin E$. E n'est pas un sous-anneau de $\mathcal{M}_3(\mathbb{R})$.

• Stabilité pour la multiplication

Soient a, b, a' et b' quatre nombres réels.
Par distributivité, $(aA + bB)(a'A + b'B) = aa'A^2 + ab'AB + ba'BA + bb'B^2$.
Or, le calcul matriciel donne :

$$A^2 = \begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} = -2A + B \in E, \quad B^2 = \begin{pmatrix} 1 & -2 & 1 \\ 1 & 1 & -2 \\ -2 & 1 & 1 \end{pmatrix} = A - 2B \in E,$$

$$AB = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = -A - B \in E \quad \text{et} \quad BA = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = AB \in E.$$

On en déduit que $(aA + bB)(a'A + b'B) \in E$.
On remarque de plus que la multiplication induite sur E est commutative.

• Recherche d'un élément neutre

Soient x et $y \in \mathbb{R}$ et $X = xA + yB$.
Si X est neutre pour la multiplication induite sur E, on a en particulier $XA = A$.
Or, $XA = xA^2 + yAB = (-2x - y)A + (x - y)B$ et la famille (A, B) est libre :

$$XA = A \iff \begin{cases} -2x - y = 1 \\ x - y = 0 \end{cases} \iff \begin{cases} x = -1/3 \\ y = -1/3 \end{cases}$$

La seule matrice possible est $X = -\frac{1}{3}A - \frac{1}{3}B = \frac{1}{3}\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$.

Réciproquement, soit $X = -\frac{1}{3}A - \frac{1}{3}B$. On a vu que $AX = XA = A$.

Et on a $BX = XB = -\frac{1}{3}AB - \frac{1}{3}B^2 = \frac{1}{3}A + \frac{1}{3}B - \frac{1}{3}A + \frac{2}{3}B = B$.

On en déduit que pour toute $M \in E, MX = XM = M$. Donc X est neutre pour la multiplication induite sur E.

Donc $(E, +, \times)$ est un anneau.

2) Pour justifier que la matrice A n'est pas inversible, on peut faire remarquer qu'en ajoutant les trois colonnes de A, on forme la colonne nulle ou on peut calculer le déterminant de A :

$$\det(A) = \begin{vmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{vmatrix} = (-1)\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} - 1\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = -1 + 1 = 0.$$

Soient $a, b \in \mathbb{R}$ et $M = (aA + bB)$.

On a vu $MA = aA^2 + bBA = (-2a - b)A + (a - b)B$. D'où :

$$MA = X \iff (-2a - b)A + (a - b)B = -\frac{1}{3}A - \frac{1}{3}B$$

(la famille (A, B) est libre)

$$\iff \begin{cases} -2a - b = -1/3 \\ a - b = -1/3 \end{cases}$$

($L_2 - L_1$ donne $a = 0$)

$$\iff \begin{cases} a = 0 \\ b = 1/3 \end{cases}$$

La matrice A admet un inverse dans l'anneau E qui est la matrice $\frac{1}{3}B$.

Exercice 11 *Anneau de Boole*

1) Soit $x \in A$. D'une part, $(2x)^2 = (2x)(2x) = 4x^2$. D'autre part, d'après $(\star)$, on a $x^2 = x$ et $(2x)^2 = 2x$ (car $x + x \in A$). Donc $2x = 4x$. D'où $2x = 0$.

2) Soient x et y dans A. D'après $(\star)$, on a $x^2 = x, y^2 = y$ et $(x + y)^2 = x + y$. Donc :

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

On en déduit que $xy + yx = 0$. En ajoutant yx, on obtient $xy + 2yx = yx$. On en déduit, d'après la question précédente, $xy = yx$.

Par conséquent l'anneau A est commutatif.

3) Soit x un élément inversible de A. En multipliant $x^2 = x$ par x^{-1}, on obtient $x = 1_A$.

Réciproquement, l'élément neutre 1_A est bien inversible.

Le seul élément inversible de A est 1_A.

CORRECTIONS

Exercice 12

1) Comme $(\overline{a})^n = \overline{a^n} = \overline{N+1} = \overline{1}$, on a $\overline{a}$ est inversible d'inverse $(\overline{a})^{n-1}$.
Le calcul précédent indique également que l'ordre de $\overline{a}$ dans $U(\mathbb{Z}/N\mathbb{Z})$ est un diviseur n.
Puisque $a \geqslant 2$, on a $2 \leqslant a < a^2 < \cdots < a^{n-1} < a^n = N+1$.
Plus précisément, $a^{n-1} = \frac{N+1}{a} \leqslant \frac{N+1}{2} < N$. Donc $\overline{a}, (\overline{a})^2, \ldots, (\overline{a})^{n-2}$ et $(\overline{a})^{n-1}$ sont différents de $\overline{1}$. Donc l'ordre de $\overline{a}$ est exactement égal à n.

2) D'après le cours, $U(\mathbb{Z}/N\mathbb{Z})$ est un groupe de cardinal $\varphi(N)$. Comme l'ordre d'un élément dans un groupe divise le cardinal du groupe, on en déduit que n divise $\varphi(N)$.

Exercice 13

1) Soit $k \in \mathbb{N}^*$. Précisons l'ensemble $\mathcal{D}_0$ des diviseurs de 0 de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.
Soit $n \in [\![1, 2^k - 1]\!]$.
   - Si n est pair, alors $2^{k-1}n$ est divisible par 2^k. Donc $\overline{2^{k-1}} \cdot \overline{n} = 0$ dans $\mathbb{Z}/2^k\mathbb{Z}$ et $\overline{n} \in \mathcal{D}_0$.
   - Sinon $\overline{n}$ est inversible dans $\mathbb{Z}/2^k\mathbb{Z}$, car n et 2^k sont premiers entre eux. Donc $\overline{n}$ n'est pas un diviseur de 0.

   En conclusion, $\mathcal{D}_0 = \{\overline{n}, n \in [\![1, 2^k - 1]\!] \text{ et } n \text{ pair}\} = \{\overline{2p}, p \in [\![1, 2^{k-1} - 1]\!]\}$.

2) On considère A un anneau commutatif possèdant n diviseurs de zéro, avec $n \geqslant 1$.

   a) Soient a un diviseur de 0 et $f : A \to A, x \mapsto ax$.
   Pour tous x et y dans A, on a :
   $$\begin{aligned} f(x+y) &= a(x+y) \\ &= ax + ay \quad \text{(par distributivité de } \times \text{ sur } +) \\ &= f(x) + f(y). \quad \text{(par définition de } f) \end{aligned}$$
   Donc $f : A \to A, x \mapsto ax$ est un morphisme de groupes de $(A, +)$ dans lui-même.
   Soit $y \in \mathrm{Im}(f)$. On sait qu'il existe $x_0 \in A$ tel que $f(x_0) = y$ et qu'en notant A_y l'ensemble des antécédents de y par le morphisme f on a :
   $$A_y = \{x_0 + h, h \in \mathrm{Ker}(f)\}.$$
   L'application $h \mapsto x_0 + h$ étant bijective de $\mathrm{Ker}(f)$ dans A_y, ces ensembles ont le même cardinal.
   On a montré que tout élément de $\mathrm{Im}(f)$ admet exactement $\mathrm{card}(\mathrm{Ker}(f))$ antécédents.

   b) Avec les notations précédentes, on a $A = \bigcup_{y \in \mathrm{Im}(f)} A_y$, car f est définie sur A.
   De plus la réunion est disjointe. On a donc :
   $$\begin{aligned} \mathrm{card}(A) &= \sum_{y \in \mathrm{Im}(f)} \mathrm{card}(A_y) \\ &= \sum_{y \in \mathrm{Im}(f)} \mathrm{card}(\mathrm{Ker}(f)) \quad \text{(par la question précédente)} \\ &= \mathrm{card}(\mathrm{Im}(f))\mathrm{card}(\mathrm{Ker}(f)). \quad \text{(par définition de } f) \end{aligned}$$

Remarque

On remarquera la similitude avec le théorème du rang.

Si $x \in \mathrm{Ker}(f) \setminus \{0\}$, alors on a $ax = 0$ et $x \neq 0$, donc x est un diviseur de 0.
Donc $\mathrm{card}\big(\mathrm{Ker}(f)\big) \leqslant n + 1$.

Si $y \in \mathrm{Im}(f) \setminus \{0\}$, il existe $x \in A$ tel que $y = ax$. Or, a étant un diviseur de 0, il existe $b \in A \setminus \{0\}$ tel que $ba = 0$. Donc $by = b(ax) = (ba)x = 0$. Il en résulte que y est un diviseur de 0. Donc $\mathrm{card}\big(\mathrm{Im}(f)\big) \leqslant n + 1$.
Compte tenu des trois résultats précédents, A a au plus $(n + 1)^2$ éléments.

Remarque

Dans l'exemple de la première question, il y a $n = 2^{k-1} - 1$ diviseurs de 0 et $(n+1)^2 = 2^k$ est exactement le nombre d'éléments de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.

Exercices avec questions ouvertes

Exercice 14

On va montrer qu'un tel anneau est un corps.
Soit A un anneau commutatif dont les seuls idéaux sont $\{0\}$ et A.
Soit $x \in A \setminus \{0\}$. L'ensemble $I = \{ax, a \in A\}$ est un sous-groupe de $(A, +)$.
Soient $a' \in A$ et $y \in I$. Il existe $a \in A$ tel que $y = ax$.
On a alors $a'y = a'(ax) = (a'a)x \in I$, car $a'a \in A$ (anneau).
On a montré :

$$\forall a' \in A, \forall y \in I, \quad a'y \in I.$$

Donc I est un idéal de l'anneau A.
Comme I contient $x = 1x$, $I \neq \{0\}$ et donc $I = A$ d'après l'hypothèse faite sur les idéaux de A.
En particulier, $1 \in I$, donc il existe $x' \in A$ tel que $x'x = 1$. La loi étant commutative, cela prouve que x est inversible.
Tout élément non nul de l'anneau étant inversible, A est un corps.

Exercice 15

Si f est un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans lui-même, on a $f(1) = 1$.
On en déduit (voir exercice 1 du chapitre 1) que pour tout $n \in \mathbb{Z}$, $f(n) = f(n1) = nf(1) = n$.
Réciproquement, l'identité est un morphisme de $(\mathbb{Z}, +)$ dans lui-même

Exercice 16

Si f est un morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même, on a $f(1) = 1$.
On en déduit, par une démonstration semblable à celle de l'exercice 2 du chapitre 1, que pour tout $r \in \mathbb{Q}$, $f(q) = f(q1) = qf(1) = q$.

De plus f est croissante car si $x \leqslant y$, on a :

$$f(y) - f(x) = f(y-x) = f\left(\sqrt{y-x}^{\,2}\right) = f\left(\sqrt{y-x}\right)^2 \geqslant f(x).$$

Soit $x \in \mathbb{R}$. On sait qu'il existe (approximation décimale des réels) des suites $(m_n)_{n\in\mathbb{N}}$ et $(M_n)_{n\in\mathbb{N}}$ de rationnels [*] qui convergent vers x et telles que $m_n \leqslant x \leqslant M_n$.
On a alors $m_n = f(m_n) \leqslant f(x) \leqslant f(M_n) = M_n$ et par théorème d'encadrement, $f(x) = x$.
Réciproquement, $\mathrm{Id}_{\mathbb{R}}$ est un morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.
L'identité est le seul morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.

Exercice 17

1) Si la multiplication est commutative, on a pour tous x et y dans A :

$$(xy)^2 = xyxy = xxyy = x^2y^2.$$

2) Montrons que la réciproque est vraie.
On suppose :

$$\forall x, y \in A, \quad (xy)^2 = x^2y^2. \qquad (\star)$$

Soient x et y dans A. En utilisant $(\star)$ pour x et $1_A + y$, on a :

$$(x + xy)^2 = \big(x(1_A + y)\big)^2 = x^2(1_A + y)^2.$$

Or, $(x + xy)^2 = x^2 + x^2y + xyx + (xy)^2 = x^2 + x^2y + xyx + x^2y^2$
et $x^2(1_A + y)^2 = x^2(1_A + 2y + y^2) = x^2 + 2x^2y + x^2y^2$.
Donc $2x^2y = x^2y + xyx$, puis $x^2y = xyx$.
Cette dernière relation étant vraie pour tous x dans A, on peut utiliser $1_A + x$ et on obtient :

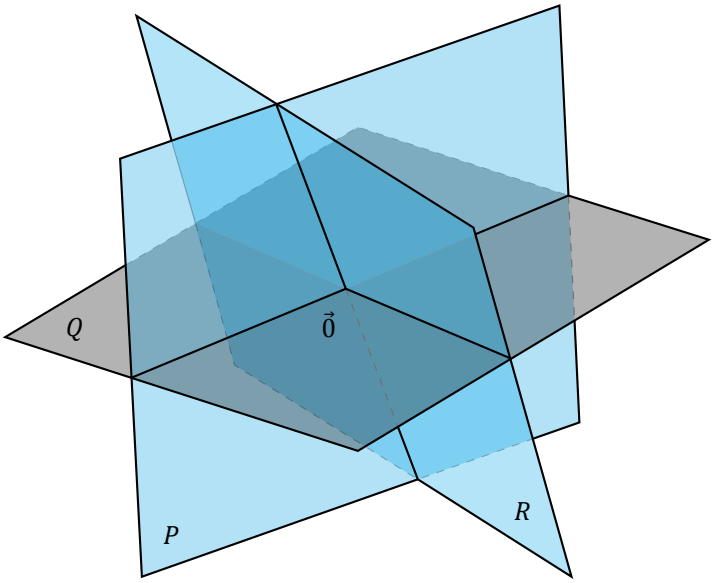
$$(1_A + x)^2y = (1_A + x)y(1_A + x).$$

Or, d'une part :
$(1_A + x)^2y = (1_A + 2x + x^2)y = y + 2xy + x^2y = y + 2xy + xyx$,
et d'autre part :
$(1_A + x)y(1_A + x) = (y + xy)(1_A + x) = y + yx + xy + xyx$.
On en déduit $yx + xy = 2xy$, donc $yx = xy$.
L'anneau est effectivement commutatif.

« *Quand l'anneau est intègre, tous les calculs se font bien.* »

[*] Par exemple $m_n = \lfloor 10^n x \rfloor / 10^n$ et $M_n = m_n + 10^{-n}$.

Algèbre (révisions) 3



Dans l'exercice n° 13, on considère une intersection d'hyperplans comme sur la figure ci-dessus : à chaque fois que l'on rajoute un hyperplan dans l'intersection, la dimension de l'intersection diminue d'une unité, à condition que l'hyperplan que l'on rajoute soit « indépendant » des autres (il faudra préciser mathématiquement ce que l'on entend par là).

Exercices axés sur le calcul

Exercice 1 *Polynômes de Legendre*

1) Soient $P \in \mathbb{R}[X]$, a et b deux racines de P de multiplicité $m \in \mathbb{N}^*$ telles que $a < b$.
Montrer que pour tout $k \in [\![1, m]\!]$, $P^{(k)}$ admet au moins k racines dans $]a, b[$.

2) Pour $n \in \mathbb{N}^*$, on note $Q_n = (X^2 - 1)^n$ et $L_n = Q_n^{(n)}$.

a) Quel est le degré de L_n ?

b) Montrer que L_n admet exactement n racines et qu'elles sont toutes dans $]-1, 1[$.

D'après Mines-Télécom

Exercice 2 *Somme et produit des racines d'un polynôme, transformation de* $e^{i\theta} \pm 1$

Soit $n \in \mathbb{N}^*$. On note $P_n = 1 + X + \cdots + X^n$.

1) Justifier que P_n admet n racines éventuellement confondues dans $\mathbb{C}$.

2) Préciser le produit et la somme de ces racines.

3) Résoudre $P_n(z) = 0$. Contrôler les résultats du 2).

4) Déduire de $P(1)$ la valeur de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right)$.

Exercices axés sur le raisonnement

Exercice 3 *Formule du binôme, unicité des coefficients d'un polynôme*

Pour $n \in \mathbb{N}$, on note $S_n = \sum_{k=0}^{n} \binom{n}{k}^2$.

Déterminer la valeur de S_n en utilisant le coefficient de X^n dans $(1 + X)^n(1 + X)^n$.

Exercice 4

Dans l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, on considère pour $n \in \mathbb{N}^*$, la fonction :

$$f_n : x \mapsto e^{x/n}.$$

Montrer que la famille $(f_n)_{n\in\mathbb{N}^*}$ est libre.

Exercice 5

Soient E un $\mathbb{K}$-espace vectoriel, f un endomorphisme de E et $a \in \mathbb{K} \setminus \{0\}$.
On suppose que $f^3 - 3af^2 + a^2 f = 0$.
Montrer que $E = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$.

D'après Mines-Télécom

Exercice 6 *Fréquent*

Soient E un $\mathbb{K}$-espace vectoriel et $f_1, f_2, \dots, f_n$ des endomorphismes de E.
On suppose que $f_1 + f_2 + \cdots + f_n = \mathrm{Id}_E$ et :

$$\forall i, j \in [\![1, n]\!], \quad i \neq j \Longrightarrow f_i \circ f_j = 0.$$

1) Montrer que pour tout $i \in [\![1, n]\!]$, f_i est une projection vectorielle.
2) Montrer que $\bigoplus_{i=1}^{n} \mathrm{Im}(f_i) = E$.

Exercice 7 *Classique*

Soient E un espace vectoriel et p, q des projecteurs de E.

1) Montrer que $p + q$ est un projecteur si, et seulement si, $p \circ q = q \circ p = 0$.
2) Dans ce cas, montrer que $\mathrm{Ker}(p+q) = \mathrm{Ker}(p) \cap \mathrm{Ker}(q)$ et $\mathrm{Im}(p+q) = \mathrm{Im}(p) \oplus \mathrm{Im}(q)$.

D'après CCINP

Exercice 8

Soient E et F deux $\mathbb{K}$-espaces vectoriels, $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, E)$. On suppose que :

$$u = u \circ v \circ u \quad \text{et} \quad v = v \circ u \circ v.$$

Montrer que :

$$E = \mathrm{Ker}(u) \oplus \mathrm{Im}(v).$$

D'après Mines-Télécom

Exercice 9

Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E. On suppose que l'endomorphisme u est nilpotent d'indice p, c'est-à-dire que $u^p = 0$ et $u^{p-1} \neq 0$. On note $\mathrm{e}^u = \sum_{k=0}^{p-1} \frac{1}{k!} u^k$.

1) Soient $x \in E$ et $k \in \mathbb{N}^*$ tels que $u^k(x) \neq 0_E$.
Montrer que la famille $\left(x, u(x), u^2(x), \dots, u^k(x)\right)$ est libre.
2) Déterminer $\mathrm{Ker}(\mathrm{e}^u - \mathrm{Id}_E)$.

D'après Mines-Télécom

Exercice 10 ⋆ *Supplémentaire commun*

Soient E_1 et E_2 deux sous-espaces supplémentaires d'un espace vectoriel E.
On suppose que E_1 et E_2 sont isomorphes et on note f un isomorphisme de E_1 sur E_2.
On pose $F = \{x - f(x), x \in E_1\}$.

1) Justifier que F est un sous-espace vectoriel de E.
2) Montrer que $F \oplus E_1 = E$.
3) Montrer qu'on a aussi $F \oplus E_2 = E$.