

Chapitre 11

Structures
algébriques

Du niveau de base au niveau concours

À connaître par cœur

Groupe : loi associative, neutre, symétriques

Morphisme : $f(x * y) = f(x) \otimes f(y)$ *Défi de concours*

Sur $I =]1, +\infty[: x * y = \sqrt{x^2 y^2 - x^2 - y^2 + 2}$.
 $(I, *)$ est-il un groupe ?

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

la table du groupe $(\mathbb{U}_4, \times)$: un carré latin

★★★★ Niveau 4 · Concours

★★★ Niveau 3 · Approfondissement

★★ Niveau 2 · Bac

★ Niveau 1 · Bases

Cours complet

Méthodes et pièges

66 exercices corrigés

Formulaire

Sommaire

1 Lois de composition interne	5
2 Propriétés d'une loi	6
3 Groupes	7
4 Sous-groupes	9
5 Morphismes de groupes	10
6 Isomorphismes et transport	11
7 Anneaux	13
8 Corps	14
9 Matrices carrées d'ordre 2 et 3	16
10 Matrices inversibles, puissances	17
11 Structures de matrices	19
12 Les pièges classiques	20
13 Les astuces des concours	21
14 L'essentiel du chapitre en une page	23
15 Niveau 1 · Bases	24
16 Niveau 2 · Bac	25
17 Niveau 3 · Approfondissement	27
18 Niveau 4 · Concours	28
19 Lois de composition interne	30
20 Groupes et sous-groupes	32
21 Morphismes et isomorphismes	34
22 Anneaux et corps	36
23 Matrices et structures	38

24 Défis de concours	39
25 Corrigés du niveau 1	43
26 Corrigés du niveau 2	45
27 Corrigés du niveau 3	48
28 Corrigés du niveau 4	50
29 Corrigés : lois internes	53
30 Corrigés : groupes	56
31 Corrigés : morphismes	60
32 Corrigés : anneaux et corps	63
33 Corrigés : matrices et structures	66
34 Corrigés : défis de concours	69

Comment utiliser ce livret

Les 4 niveaux d'exercices

Niveau 1 · Bases ★

les automatismes indispensables.

Niveau 2 · Bac ★★

le niveau de l'examen national.

Niveau 3 · Approfondissement ★★★

pour viser la mention Très bien.

Niveau 4 · Concours ★★★★★

problèmes de concours (classes préparatoires, écoles d'ingénieurs).

Les encadrés du cours

■ **Définition** : à savoir par cœur.

■ **Propriété / Théorème** : les outils.

■ **Méthode** : la démarche pas à pas.

■ **Exemple** : un calcul entièrement rédigé.

■ **Piège** : l'erreur classique à éviter.

■ **Astuce de concours** ★ : le petit plus qui fait gagner du temps.

Le livret contient 66 exercices corrigés : la partie B est un parcours en 4 niveaux (exercices 1 à 30) ; la partie C est une banque de 36 exercices classés par thème (Lois de composition interne, Groupes et sous-groupes, Morphismes et isomorphismes, Anneaux et corps, Matrices et structures, Défis de concours). Tous les corrigés sont regroupés dans la partie D.

Conseil : cherche chaque exercice au moins 10 minutes avant de lire le corrigé. Le numéro de page du corrigé est indiqué à droite de chaque énoncé.

La carte du chapitre



À la fin du chapitre, je sais...

- | | |
|--|---|
| ☐ montrer qu'une loi est interne, une partie stable ; | ☐ utiliser le transport de structure ; |
| ☐ lire une table, trouver neutre et symétriques ; | ☐ reconnaître un anneau, un anneau intègre ; |
| ☐ démontrer qu'un ensemble est un groupe ; | ☐ trouver les inversibles et les diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$; |
| ☐ calculer les puissances $x^{(n)}$ dans un groupe ; | ☐ montrer qu'une partie est un sous-corps ; |
| ☐ montrer qu'une partie est un sous-groupe ; | ☐ calculer un produit de matrices ; |
| ☐ connaître les sous-groupes de $(\mathbb{Z}, +)$; | ☐ inverser une matrice d'ordre 2 ou 3 ; |
| ☐ reconnaître un morphisme de groupes ; | ☐ calculer A^n (réurrence, binôme). |

Partie A • Le cours

Définitions, théorèmes, méthodes, pièges et astuces de concours

1 Lois de composition interne

Définition

Soit E un ensemble non vide. Une **loi de composition interne** sur E est une application $E \times E \rightarrow E$, $(x, y) \mapsto x * y$: à tout couple (x, y) d'éléments de E , elle associe un élément $x * y$ qui est **encore dans** E . On note les lois $*$, $\otimes$, $\oplus$, $\odot$, $\circ$, $\cdot$, $+$, $\times$...

Une partie A de E est **stable** par $*$ si $\forall (x, y) \in A^2, x * y \in A$; la restriction de $*$ à $A \times A$ est alors une loi interne sur A , la **loi induite** (notée encore $*$).

Exemples : $+$ et $\times$ sont internes sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; la soustraction est interne sur $\mathbb{Z}$, pas sur $\mathbb{N}$ ($2 - 5 \notin \mathbb{N}$) ; la division est interne sur $\mathbb{R}^*$, pas sur $\mathbb{R}$; $\circ$ est interne sur l'ensemble $F(E, E)$ des applications de E dans E .

- $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ est stable par $\times$ ($|zz'| = |z| |z'| = 1$) ; l'ensemble $i\mathbb{R}$ des imaginaires purs est stable par $+$, pas par $\times$ ($i \times i = -1$).
- Les entiers impairs sont stables par $\times$: $(2k+1)(2k'+1) = 2(2kk' + k + k') + 1$; pas par $+$: $1 + 1 = 2$.
- Les fonctions affines sont stables par $\circ$: si $f(x) = ax + b$ et $g(x) = cx + d$, alors $(f \circ g)(x) = (ac)x + (ad + b)$.

Méthode : montrer qu'une loi est interne sur un intervalle : factoriser

On écrit $x * y - \alpha$ (ou $1 + x * y$, $1 - x * y$...) comme un **produit** : son signe se lit directement.

Exemple : sur $\mathbb{R}$, on pose $x * y = x + y + xy$ (notre **fil rouge** jusqu'à la section 5). On remarque que $1 + x * y = (1 + x)(1 + y)$. Donc $]-1, +\infty[$ et $\mathbb{R} \setminus \{-1\}$ sont stables par $*$; mais $]-\infty, -1[$ ne l'est pas : $(-2) * (-2) = 0$.

Exemple : une table : $E = \{1, 3, 5, 7\}$ et $x * y =$ reste de la division euclidienne de xy par 8

$*$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Quand E est fini, on présente une loi par sa **table** : à l'intersection de la ligne de x et de la colonne de y , on lit $x * y$. Ici, $*$ est **interne** (xy est impair, son reste $xy - 8q$ aussi) ; la table est **symétrique** par rapport à la diagonale : $*$ est commutative ; la ligne et la colonne de 1 recopient les en-têtes : 1 est neutre ; la diagonale ne contient que des 1 : $x * x = 1$. Enfin $(x * y) * z \equiv xyz \equiv x * (y * z)$ [8], et deux éléments de E congrus modulo 8 sont égaux : $*$ est **associative**.

Remarque. L'associativité ne se lit pas sur une table (n^3 triplets à tester) : on la démontre, ou l'on reconnaît une structure connue. Ici, E est l'ensemble des classes inversibles de $\mathbb{Z}/8\mathbb{Z}$ (section 7), et $x^2 = \overline{1}$ y a **quatre** solutions.

2 Propriétés d'une loi

Définition

Soit $*$ une loi interne sur E . Elle est **commutative** si $x * y = y * x$ pour tous $x, y \in E$; **associative** si $(x * y) * z = x * (y * z)$ pour tous $x, y, z \in E$ (on écrit alors $x * y * z$). Un élément $e \in E$ est **neutre** si $x * e = e * x = x$ pour tout $x \in E$.

Exemples : la soustraction n'est ni commutative ni associative : $(1 - 2) - 3 = -4 \neq 1 - (2 - 3) = 2$; la loi $a * b = a^b$ sur $\mathbb{N}^*$ non plus : $(2^3)^2 = 64 \neq 2^{(3^2)} = 512$; $\cdot$ est associative, pas commutative : avec $f(x) = x + 1$ et $g(x) = 2x$, $(f \circ g)(x) = 2x + 1 \neq (g \circ f)(x) = 2x + 2$.

Théorème (unicité du neutre)

Si une loi admet un élément neutre, celui-ci est **unique**.

Démonstration. Si e et e' sont neutres : $e * e' = e'$ (e est neutre) et $e * e' = e$ (e' est neutre), donc $e = e'$. $\square$

Définition : symétrique, élément régulier

Soit $*$ une loi interne sur E , de neutre e . Un élément x est **symétrisable** s'il existe $x' \in E$ tel que $x * x' = x' * x = e$ (x' est un **symétrique** de x ; en additif : l'**opposé** $-x$; en multiplicatif : l'**inverse** x^{-1}).

Un élément a est **régulier** si, pour tous $x, y \in E$: $a * x = a * y \Rightarrow x = y$ et $x * a = y * a \Rightarrow x = y$.

Théorème

Soit $*$ une loi **associative** sur E , de neutre e .

1. Si x est symétrisable, son symétrique est **unique** ; on le note x' , et $(x')' = x$.
2. Si x et y sont symétrisables, $x * y$ l'est aussi, et $(x * y)' = y' * x'$ (l'ordre s'inverse !).
3. Tout élément symétrisable est régulier.

Démonstration. 1. Si x' et x'' sont deux symétriques de x : $x'' = x'' * e = x'' * (x * x') = (x'' * x) * x' = e * x' = x'$ (l'associativité est essentielle) ; et $x' * x = x * x' = e$ dit que x est le symétrique de x' . 2. $(x * y) * (y' * x') = x * (y * y') * x' = x * x' = e$, et de même $(y' * x') * (x * y) = e$. 3. Si $a * x = a * y$, alors $a' * (a * x) = a' * (a * y)$, soit $(a' * a) * x = (a' * a) * y$, donc $x = y$; de même à droite. $\square$

Exemple : le fil rouge : $x * y = x + y + xy$ sur $\mathbb{R}$

Commutative (symétrique en x, y) et **associative** : $1 + (x * y) * z = (1 + x * y)(1 + z) = (1 + x)(1 + y)(1 + z) = 1 + x * (y * z)$. **Neutre** : $x * e = x \iff e(1 + x) = 0$, vrai pour tout x si et seulement si $e = 0$. **Symétriques** : $x * x' = 0 \iff x'(1 + x) = -x$; si $x \neq -1$, $x' = -\frac{x}{1+x}$ (ainsi $1' = -\frac{1}{2}$: $1 - \frac{1}{2} - \frac{1}{2} = 0$). Mais $(-1) * y = -1$ pour tout y : -1 (élément **absorbant**) n'a pas de symétrique,

et il n'est pas régulier : $(-1) * 0 = (-1) * 1$.

Attention, piège ! régulier ne veut pas dire symétrisable

Sur $\mathbb{R}_+$, la loi $x * y = \sqrt{x^2 + y^2}$ est interne, commutative, associative ($(x * y) * z = \sqrt{x^2 + y^2 + z^2} = x * (y * z)$), de neutre 0, et tout a est régulier : $a * x = a * y \Rightarrow x^2 = y^2 \Rightarrow x = y$ (car $x, y \geq 0$). Pourtant $x * x' = 0 \iff x = x' = 0$: **seul 0 est symétrisable**. (De même dans $(\mathbb{N}, +)$.)

Définition : distributivité

Soit $*$ et $\otimes$ deux lois internes sur E . La loi $\otimes$ est **distributive** par rapport à $*$ si, pour tous $x, y, z \in E$:

$$x \otimes (y * z) = (x \otimes y) * (x \otimes z) \quad \text{et} \quad (y * z) \otimes x = (y \otimes x) * (z \otimes x).$$

Exemples : $*$ est distributive par rapport à $+$, mais pas l'inverse : $1 + (2 \times 3) = 7 \neq (1 + 2) \times (1 + 3) = 12$. Dans $P(E)$, $\cap$ et $\cup$ sont distributives l'une par rapport à l'autre. Dans $F(\mathbb{R}, \mathbb{R})$, $(f + g) \cdot h = f \cdot h + g \cdot h$, mais avec $h(x) = x^2$ et $f = g = \text{id}$: $h \cdot (f + g)(x) = 4x^2 \neq 2x^2$: $\cdot$ n'est distributive par rapport à $+$ qu'à droite.

3

Groupes

Définition

Un **groupe** est un ensemble G muni d'une loi interne $*$ **associative**, qui admet un **élément neutre** e , et pour laquelle **tout élément est symétrisable**. Si, de plus, $*$ est commutative, le groupe est dit **commutatif** (ou **abélien**).

Les groupes de référence

- **Additifs** : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$ (neutre $\bar{0}$, opposé de $\bar{a} : \overline{n - a}$).
- **Multipliatifs** : $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$, où $\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1 \right\}$.
- **Bijections** : l'ensemble $S(E)$ des bijections de E sur E , muni de $\circ$; **matrices** : sections 10 et 11.

Tous sont commutatifs, sauf $S(E)$ (si E a au moins trois éléments) et le groupe $GL_n(\mathbb{R})$ de toutes les matrices inversibles.

Démonstration (pour $S(E)$). La composée de deux bijections f, g est une bijection (de réciproque $g^{-1} \circ f^{-1}$) ; $\circ$ est associative, id_E est neutre, et f^{-1} est le symétrique de f . $\square$

Ne sont pas des groupes : $(\mathbb{N}, +)$ (1 n'a pas d'opposé) ; $(\mathbb{Z}, \times)$ (2 n'a pas d'inverse) ; $(\mathbb{R}, \times)$ (0 n'a pas d'inverse) ; $(\mathbb{Z}, -)$ (non associative, et 0 n'est neutre qu'à droite).

Théorème (règles de calcul dans un groupe)

Soit $(G, *)$ un groupe de neutre e et $a, b \in G$.

1. Tout élément est **régulier** ; $(a')' = a$ et $(a * b)' = b' * a'$.

2. L'équation $a * x = b$ a une **unique** solution, $x = a' * b$; l'équation $x * a = b$ a pour unique solution $x = b * a'$.
3. Si G est fini, chaque élément apparaît **exactement une fois** dans chaque ligne et dans chaque colonne de la table (**carré latin**).

Démonstration. 1 : section 2. 2. $a * (a' * b) = (a * a') * b = b$; et si $a * x = b$, alors $x = a' * (a * x) = a' * b$. 3. Dans la ligne de a , les cases $a * y$ sont distinctes (régularité) et tout b y figure (colonne $y = a' * b$) ; idem pour les colonnes. $\square$

Définition : puissances, multiples

Soit $x \in G$. On pose $x^{(0)} = e$, $x^{(n+1)} = x^{(n)} * x$ ($n \in \mathbb{N}$) et $x^{(-n)} = (x')^{(n)}$: $x^{(n)} = x * x * \dots * x$ (n facteurs). En notation multiplicative, on écrit x^n ; en notation additive, $nx = x + \dots + x$ (**multiples** de x). Pour tous $m, n \in \mathbb{Z}$:

$$x^{(m)} * x^{(n)} = x^{(m+n)}, \quad (x^{(m)})^{(n)} = x^{(mn)}, \quad (x^{(n)})' = x^{(-n)},$$

et, si $x * y = y * x$: $(x * y)^{(n)} = x^{(n)} * y^{(n)}$.

Démonstration (idée). Pour $m, n \in \mathbb{N}$, récurrence sur n : $x^{(m)} * x^{(n+1)} = (x^{(m)} * x^{(n)}) * x = x^{(m+n+1)}$; puis exposants négatifs avec $x * x' = e$. Le dernier point demande de faire passer les y à droite des x , donc $x * y = y * x$. $\square$

Exemple : le fil rouge : $(\mathbb{R} \setminus \{-1\}, *)$ est un groupe commutatif

La loi $x * y = x + y + xy$ est interne sur $G = \mathbb{R} \setminus \{-1\}$, associative, commutative, de neutre $0 \in G$, et $x' = -\frac{x}{1+x} \in G$ car $1 + x' = \frac{1}{1+x} \neq 0$. **Puissances** : par récurrence, $1 + x^{(n+1)} = 1 + x^{(n)} * x = (1 + x^{(n)})(1 + x)$, donc $1 + x^{(n)} = (1 + x)^n$; avec $1 + x' = (1 + x)^{-1}$, pour tout $n \in \mathbb{Z}$:

$$x^{(n)} = (1 + x)^n - 1 \quad \text{par exemple} \quad 1^{(5)} = 2^5 - 1 = 31 \quad \text{et} \quad 1^{(-1)} = 2^{-1} - 1 = -\frac{1}{2} = 1'.$$

Exemple : un groupe non commutatif de six bijections : sa table de Cayley

Sur $E = \mathbb{R} \setminus \{0, 1\}$, on considère les bijections

$$\begin{aligned} f_1(x) &= x, & f_2(x) &= \frac{1}{x}, & f_3(x) &= 1 - x, \\ f_4(x) &= \frac{1}{1-x}, & f_5(x) &= \frac{x-1}{x}, & f_6(x) &= \frac{x}{x-1}. \end{aligned}$$

Par exemple (cases encadrées) :

$$(f_2 \circ f_3)(x) = \frac{1}{1-x} = f_4(x), \quad (f_3 \circ f_2)(x) = 1 - \frac{1}{x} = f_5(x).$$

$G = \{f_1, \dots, f_6\}$ est stable par $\circ$, et $\circ$ n'y est **pas commutative**. La table montre que $f_1 = \text{id}$ est neutre, que f_1, f_2, f_3, f_6 sont leur propre réciproque et que $f_4^{-1} = f_5$: $(G, \circ)$ est un groupe (un sous-groupe de $S(E)$, section 4), et sa table est un carré latin.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_4	f_5	f_6	f_2	f_1
f_4	f_4	f_3	f_6	f_1	f_5	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_1	f_2	f_3	f_4

ligne f_i , colonne f_j : $f_i \circ f_j$

4

Sous-groupes

Définition

Soit $(G, *)$ un groupe et $H \subset G$. On dit que H est un **sous-groupe** de G si H est stable par $*$ et si H , muni de la loi induite, est un groupe.

Théorème (caractérisation des sous-groupes)

Soit $(G, *)$ un groupe de neutre e , et $H \subset G$. Les assertions suivantes sont équivalentes :

- (i) H est un sous-groupe de G ; (ii) $e \in H$, et pour tous $x, y \in H$: $x * y \in H$ et $x' \in H$;
 (iii) $H \neq \emptyset$ et $\forall (x, y) \in H^2, x * y' \in H$.

Le neutre de H est alors e , et le symétrique dans H de $x \in H$ est son symétrique x' dans G .

Démonstration. (i) $\Rightarrow$ (ii). Soit e_H le neutre de H : dans G , $e_H * e_H = e_H = e_H * e$, donc $e_H = e$ (régularité dans G). Si $x \in H$ a pour symétrique x'' dans H , alors $x * x'' = e = x * x'$, donc $x'' = x'$: ainsi $e \in H$, $x' \in H$, et H est stable. (ii) $\Rightarrow$ (iii). $e \in H$, donc $H \neq \emptyset$; si $x, y \in H$, alors $y' \in H$, puis $x * y' \in H$. (iii) $\Rightarrow$ (i). Soit $a \in H$: $e = a * a' \in H$; pour $y \in H$: $y' = e * y' \in H$; pour $x, y \in H$: $x * y = x * (y')' \in H$. La loi induite est associative (elle l'est sur G), $e \in H$ est neutre et tout $y \in H$ a son symétrique y' dans H . $\square$

Méthode : montrer qu'un ensemble est un groupe : le plonger dans un groupe connu

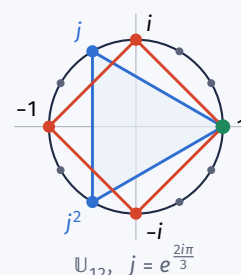
On vérifie 1. $H \subset G$; 2. $e \in H$; 3. $x * y' \in H$ pour tous $x, y \in H$ (en additif : $x - y \in H$; en multiplicatif : $xy^{-1} \in H$). On obtient gratuitement que $(H, *)$ est un **groupe**.

Exemple : sous-groupes classiques

- $\{e\}$ et G ; $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (sous-groupes additifs) ; $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, *)$ ($1 > 0$, et $\frac{x}{y} > 0$ si $x, y > 0$), mais pas $\mathbb{R}_-^*$ ($1 \notin \mathbb{R}_-^*$).
- $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*, *)$: $1 \in \mathbb{U}$, et $\left| \frac{z}{z'} \right| = 1$ si $|z| = |z'| = 1$. $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$: $1^n = 1$, et $\left(\frac{z}{z'} \right)^n = \frac{z^n}{z'^n} = 1$ si $z^n = z'^n = 1$. D'où la chaîne $\mathbb{U}_n \subset \mathbb{U} \subset \mathbb{C}^*$.
- Le fil rouge : $] -1, +\infty[$ est un sous-groupe de $(\mathbb{R} \setminus \{-1\}, *)$: il contient 0, et pour $x, y > -1$, $1 + x * y' = (1 + x)(1 + y') = \frac{1+x}{1+y} > 0$.
- $\mathbb{N}$ est stable dans $(\mathbb{Z}, +)$ et contient 0, mais ce n'est **pas** un sous-groupe : $-1 \notin \mathbb{N}$.

Exemple : racines de l'unité : $\mathbb{U}_d \subset \mathbb{U}_n$ si $d \mid n$, et $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m \wedge n}$

- Si $n = dk$ et $z^d = 1$, alors $z^n = (z^d)^k = 1$: $\mathbb{U}_d \subset \mathbb{U}_n$. Sur la figure, $\mathbb{U}_3$ (triangle bleu) et $\mathbb{U}_4$ (carré rouge) sont deux sous-groupes de $\mathbb{U}_{12}$.
- L'intersection de deux sous-groupes est un sous-groupe (on vérifie (iii)). Ici, si $z \in \mathbb{U}_m \cap \mathbb{U}_n$ et $d = m \wedge n = mu + nv$ (Bézout), alors $z^d = (z^m)^u (z^n)^v = 1$; comme $\mathbb{U}_d \subset \mathbb{U}_m \cap \mathbb{U}_n$: $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m \wedge n}$. Ainsi $\mathbb{U}_3 \cap \mathbb{U}_4 = \mathbb{U}_1 = \{1\}$.



Théorème (sous-groupes de $(\mathbb{Z}, +)$)

Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$. Réciproquement, pour tout sous-groupe H de $(\mathbb{Z}, +)$, il existe un **unique** $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration. $0 \in n\mathbb{Z}$ et $kn - k'n = (k - k')n \in n\mathbb{Z}$. Soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, H contient un $x \neq 0$, donc aussi $-x$: la partie $H \cap \mathbb{N}^*$ de $\mathbb{N}$ n'est pas vide ; soit n son plus petit élément. Les multiples de n sont dans H (stable, et contenant les opposés) : $n\mathbb{Z} \subset H$. Soit $h \in H$; la division euclidienne donne $h = nq + r$, $0 \leq r < n$, et $r = h - nq \in H$. Si $r \neq 0$, alors $r \in H \cap \mathbb{N}^*$ et $r < n$: absurde. Donc $r = 0$ et $h \in n\mathbb{Z}$. Unicité : si $n\mathbb{Z} = m\mathbb{Z}$ ($n, m \in \mathbb{N}$), alors $n \mid m$ et $m \mid n$, donc $n = m$. $\square$

Remarque. $a\mathbb{Z} \cap b\mathbb{Z}$ (multiples communs) est égal à $(a \vee b)\mathbb{Z}$: $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$; $a\mathbb{Z} + b\mathbb{Z} = \{au + bv, u, v \in \mathbb{Z}\}$ est un sous-groupe, égal à $(a \wedge b)\mathbb{Z}$ (Bézout) : $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. Mais $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe : $2 - (-3) = 5$ n'y est pas.

5

Morphismes de groupes**Définition**

Soit $(G, *)$ et $(G', \otimes)$ deux groupes. Une application $f : G \rightarrow G'$ est un **morphisme de groupes** si

$$\forall (x, y) \in G^2, \quad f(x * y) = f(x) \otimes f(y).$$

Si $(G', \otimes) = (G, *)$, on parle d'**endomorphisme** de G .

Théorème

Soit f un morphisme du groupe $(G, *)$, de neutre e , dans le groupe $(G', \otimes)$, de neutre e' .

1. $f(e) = e'$ et $f(x') = (f(x))'$ pour tout $x \in G$; plus généralement $f(x^{(n)}) = f(x)^{(n)}$ pour $n \in \mathbb{Z}$.
2. Si H est un sous-groupe de G , son **image** $f(H) = \{f(x), x \in H\}$ est un sous-groupe de G' (en particulier $f(G)$).
3. Si H' est un sous-groupe de G' , l'ensemble $f^{-1}(H') = \{x \in G, f(x) \in H'\}$ est un sous-groupe de G .

Démonstration. 1. $f(e) \otimes f(e) = f(e * e) = f(e) = f(e) \otimes e'$, donc $f(e) = e'$ (régularité dans G'). Puis $f(x) \otimes f(x') = f(x * x') = f(e) = e'$, et de même $f(x') \otimes f(x) = e'$: par unicité du symétrique, $f(x') = f(x)'$. Les puissances : récurrence pour $n \in \mathbb{N}$, puis $x^{(-n)} = (x')^{(n)}$. 2. $e' = f(e) \in f(H)$; si $y_1 = f(x_1), y_2 = f(x_2)$ avec $x_1, x_2 \in H$: $y_1 \otimes y_2 = f(x_1) \otimes f(x_2) = f(x_1 * x_2) \in f(H)$. 3. $f(e) = e' \in H'$; si $f(x), f(y) \in H'$, alors $f(x * y) = f(x) \otimes f(y) \in H'$. $\square$

Exemple : les morphismes de référence

- $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$, car $\ln(xy) = \ln x + \ln y$; $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$, car $e^{x+y} = e^x e^y$.
- $\theta \mapsto e^{i\theta} : (\mathbb{R}, +) \rightarrow (\mathbb{U}, \times)$, car $e^{i(\theta+\theta')} = e^{i\theta} e^{i\theta'}$; surjectif, non injectif ($e^{2i\pi} = e^0$). L'image du sous-groupe $\frac{2\pi}{n}\mathbb{Z}$ de $\mathbb{R}$ est $\mathbb{U}_n$: on retrouve que $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

- $z \mapsto |z| : (\mathbb{C}^*, \times) \rightarrow (\mathbb{R}_+^*, \times)$, car $|zz'| = |z| |z'|$; $z \mapsto z^n$ est un endomorphisme de $(\mathbb{C}^*, \times)$ ($\times$ est commutative) ; $k \mapsto \bar{k}$ est un morphisme de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Le fil rouge : $f(x) = 1 + x$ est un morphisme de $(\mathbb{R} \setminus \{-1\}, *)$ dans $(\mathbb{R}_+^*, \times)$, car $f(x * y) = 1 + x * y = (1 + x)(1 + y) = f(x)f(y)$; on retrouve que $] -1, +\infty[= f^{-1}(\mathbb{R}_+^*)$ est un sous-groupe (point 3).

Attention, piège !

Un morphisme envoie **le neutre sur le neutre** : c'est un test rapide. $f(x) = 2x$ n'est pas un morphisme de $(\mathbb{R}^*, \times)$ dans lui-même : $f(1) = 2 \neq 1$; c'est pourtant un endomorphisme de $(\mathbb{R}, +)$. On calcule $f(x * y)$ avec la loi de **départ** et $f(x) \otimes f(y)$ avec la loi d'**arrivée**.

6

Isomorphismes et transport**Définition**

Un **isomorphisme** de groupes est un morphisme **bijectif** ; deux groupes sont **isomorphes** s'il existe un isomorphisme de l'un sur l'autre (un isomorphisme de G sur G est un **automorphisme**).

Théorème

1. Si f est un isomorphisme de $(G, *)$ sur $(G', \otimes)$, alors f^{-1} est un isomorphisme de $(G', \otimes)$ sur $(G, *)$.
2. La composée de deux morphismes (resp. isomorphismes) est un morphisme (resp. un isomorphisme).

Démonstration. 1. Si $y_1 = f(x_1)$ et $y_2 = f(x_2)$: $f^{-1}(y_1 \otimes y_2) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2 = f^{-1}(y_1) * f^{-1}(y_2)$.
 2. Si $f : (G, *) \rightarrow (G', \otimes)$ et $g : (G', \otimes) \rightarrow (G'', \odot)$ sont des morphismes : $g(f(x * y)) = g(f(x) \otimes f(y)) = g(f(x)) \odot g(f(y))$. $\square$

Remarque. Deux groupes isomorphes ont « la même table » aux noms près, donc les mêmes propriétés. $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes (par exp), mais $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ne le sont pas : $x * x = 1$ a deux solutions dans $\mathbb{R}^*$, alors que $x + x = 0$ n'en a qu'une dans $\mathbb{R}$.

Théorème (transport de structure)

Soit $(F, \otimes)$ un groupe, E un ensemble muni d'une loi **interne** $*$, et $f : E \rightarrow F$ une **bijection** telle que

$$\forall (x, y) \in E^2, \quad f(x * y) = f(x) \otimes f(y).$$

Alors $(E, *)$ est un groupe, et f est un isomorphisme de $(E, *)$ sur $(F, \otimes)$. Le neutre de E est $f^{-1}(e_F)$, le symétrique de x est $f^{-1}(f(x)')$; si $(F, \otimes)$ est commutatif, $(E, *)$ l'est aussi.

Démonstration. *Associativité* : $f((x * y) * z) = (f(x) \otimes f(y)) \otimes f(z) = f(x) \otimes (f(y) \otimes f(z)) = f(x * (y * z))$, et f est injective. *Neutre* : si $e = f^{-1}(e_F)$, alors $f(x * e) = f(x) \otimes e_F = f(x)$, donc $x * e = x$; de même

$e * x = x$. Symétriques : si $x' = f^{-1}(f(x)')$, alors $f(x * x') = f(x) \otimes f(x)' = e_F = f(e)$, donc $x * x' = e$; de même $x' * x = e$. Commutativité : $f(x * y) = f(x) \otimes f(y) = f(y) \otimes f(x) = f(y * x)$. $\square$

Méthode : montrer que $(E, *)$ est un groupe par transport de structure

1. Vérifier que $*$ est **interne** sur E (factoriser, section 1). 2. Trouver une **bijection** f de E sur un groupe connu telle que $f(x * y) = f(x) \otimes f(y)$. 3. Conclure ; neutre, symétriques et puissances se calculent par $f^{-1} : x^{(n)} = f^{-1}(f(x)^{(n)})$.

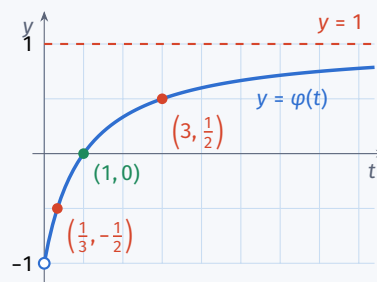
Exemple : type examen : $I =]-1, 1[$ et $x * y = \frac{x+y}{1+xy}$

1. **La loi est interne.** Pour $x, y \in I$, on a $|xy| < 1$, donc $1 + xy > 0$, et

$$1 - x * y = \frac{(1-x)(1-y)}{1+xy} > 0, \quad 1 + x * y = \frac{(1+x)(1+y)}{1+xy} > 0 :$$

ainsi $-1 < x * y < 1$.

2. **Une bijection.** Soit $f(x) = \frac{1+x}{1-x}$ sur I . Pour $t > 0$:
 $f(x) = t \iff 1+x = t - tx \iff x = \frac{t-1}{t+1}$, réel qui est dans I ($|t-1| < t+1$). Donc f est une bijection de I sur $\mathbb{R}_+^*$, de réciproque $\varphi(t) = \frac{t-1}{t+1}$ (courbe ci-contre).



3. **Un morphisme.** En divisant membre à membre les deux égalités du point 1 :

$$f(x * y) = \frac{1 + x * y}{1 - x * y} = \frac{(1+x)(1+y)}{(1-x)(1-y)} = f(x) f(y).$$

4. **Conclusion.** Par transport : $(I, *)$ est un groupe commutatif, isomorphe à $(\mathbb{R}_+^*, \times)$, et $\varphi = f^{-1}$ est un isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(I, *)$. Le neutre est $\varphi(1) = 0$; le symétrique de x est $\varphi\left(\frac{1}{f(x)}\right) = \varphi\left(\frac{1-x}{1+x}\right) = -x$. Sur la courbe : 3 et son inverse $\frac{1}{3}$ correspondent à $\frac{1}{2}$ et à son symétrique $-\frac{1}{2}$.

5. **Puissances, équations.** $f(x^{(n)}) = f(x)^n$, donc

$$x^{(n)} = \varphi\left(\left(\frac{1+x}{1-x}\right)^n\right) = \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n} ; \quad \text{par exemple} \quad \left(\frac{1}{2}\right)^{(3)} = \varphi(27) = \frac{26}{28} = \frac{13}{14}.$$

L'équation $\frac{1}{3} * x = \frac{1}{2}$ a pour unique solution $x = \left(\frac{1}{3}\right)' * \frac{1}{2} = \left(-\frac{1}{3}\right) * \frac{1}{2} = \frac{1/6}{5/6} = \frac{1}{5}$.

6. **Bonus.** $s \mapsto \varphi(e^s) = \frac{e^s - 1}{e^s + 1}$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(I, *)$ (composée) ; et $I \cap \mathbb{Q} = \varphi(\mathbb{Q}_+^*)$ (f et φ conservent les rationnels) est un sous-groupe de $(I, *)$, image du sous-groupe $\mathbb{Q}_+^*$ de $(\mathbb{R}_+^*, \times)$.

7 Anneaux

Définition

Soit A un ensemble muni de deux lois internes $+$ et $\times$. On dit que $(A, +, \times)$ est un **anneau** si 1. $(A, +)$ est un groupe **commutatif** (son neutre 0 , ou 0_A , est le **zéro**) ; 2. $\times$ est **associative** ; 3. $\times$ est **distributive** par rapport à $+$ (à gauche et à droite).
L'anneau est **commutatif** si $\times$ l'est, et **unitaire** si $\times$ admet un neutre, noté 1 ou 1_A (l'unité).

Théorème (règles de calcul)

Soit $(A, +, \times)$ un anneau et $a, b, c \in A$.

1. $a \times 0 = 0 \times a = 0$ (0 est **absorbant**) ; $(-a) \times b = a \times (-b) = -(a \times b)$; $(-a) \times (-b) = a \times b$;
 $a(b - c) = ab - ac$.
2. Si A est unitaire et si $\boxed{ab = ba}$, alors pour tout $n \in \mathbb{N}^*$:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \quad \text{et} \quad a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1}).$$

Démonstration. 1. $a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0$; on simplifie dans le groupe $(A, +)$: $a \times 0 = 0$; de même $0 \times a = 0$. Puis $ab + (-a)b = (a + (-a))b = 0 \times b = 0$, donc $(-a)b = -(ab)$, et de même à droite ; enfin $(-a)(-b) = -(a(-b)) = ab$. 2. Mêmes démonstrations que dans $\mathbb{R}$ (récurrence, triangle de Pascal) : elles n'utilisent que les axiomes d'anneau et $ab = ba$. $\square$

Définition : diviseurs de zéro, anneau intègre

Dans un anneau A , un élément $a \neq 0$ est un **diviseur de zéro** s'il existe $b \neq 0$ tel que $ab = 0$ ou $ba = 0$. Un anneau commutatif, unitaire ($1 \neq 0$) et sans diviseur de zéro est **intègre** :
 $\boxed{ab = 0 \Rightarrow a = 0 \text{ ou } b = 0}$.

Dans un anneau intègre, si $a \neq 0$ et $ab = ac$, alors $a(b - c) = 0$, donc $b = c$: tout élément non nul est **régulier** pour $\times$.

Exemple : anneaux de référence

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont commutatifs, unitaires et intègres ; $(2\mathbb{Z}, +, \times)$ est commutatif **non unitaire** (si $2u = 2$, alors $u = 1 \notin 2\mathbb{Z}$).
- $(F(\mathbb{R}, \mathbb{R}), +, \times)$ est commutatif, unitaire (la fonction constante 1), **non intègre** : avec $f(x) = x + |x|$ et $g(x) = x - |x|$, $f(x)g(x) = x^2 - |x|^2 = 0$ pour tout x , alors que $f(1) = 2$ et $g(-1) = -2$ (f est nulle sur $\mathbb{R}_-$, g sur $\mathbb{R}_+$).
- $(M_2(\mathbb{R}), +, \times)$ est unitaire, non commutatif et non intègre (section 9).

Théorème (éléments inversibles)

Dans un anneau unitaire A , l'ensemble A^* des éléments inversibles pour $\times$ est un **groupe** pour $\times$, et un élément inversible n'est jamais un diviseur de zéro.

Démonstration. $1 \in A^*$; si $a, b \in A^*$, alors ab est inversible d'inverse $b^{-1}a^{-1}$, et a^{-1} est inversible (section 2) : $\times$ est interne sur A^* , associative, de neutre 1, et chacun a son inverse dans A^* . Si a est inversible et $ab = 0$, alors $b = a^{-1}ab = a^{-1} \times 0 = 0$ (de même si $ba = 0$). $\square$

Théorème (l'anneau $\mathbb{Z}/n\mathbb{Z}$)

Soit $n \geq 2$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire, de zéro $\bar{0}$ et d'unité $\bar{1}$. Pour $a \in \mathbb{Z}$:

$\bar{a}$ est inversible $\iff a \wedge n = 1$; si $\bar{a} \neq \bar{0}$: $\bar{a}$ est un diviseur de zéro $\iff a \wedge n \neq 1$.

Démonstration. Les axiomes se transmettent de $\mathbb{Z}$: par exemple $\bar{a}(\bar{b} + \bar{c}) = \overline{a(b+c)} = \overline{ab+ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$. L'inversibilité découle de Bézout (chapitre 8) : $au \equiv 1 [n] \iff \exists v \in \mathbb{Z}, au + nv = 1$. Si $\bar{a} \neq \bar{0}$ et $d = a \wedge n > 1$, on écrit $a = da'$, $n = dn'$ avec $1 \leq n' < n$: $\bar{n'} \neq \bar{0}$ et $an' = a'n \equiv 0 [n]$: $\bar{a}$ est un diviseur de zéro. Si $a \wedge n = 1$, $\bar{a}$ est inversible, donc n'en est pas un. $\square$

Exemple : dans $\mathbb{Z}/10\mathbb{Z}$

- Inversibles : $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ ($\bar{3} \times \bar{7} = \overline{21} = \bar{1}$, $\bar{9} \times \bar{9} = \overline{81} = \bar{1}$) : c'est le groupe $(\mathbb{Z}/10\mathbb{Z})^*$. Diviseurs de zéro : $\bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$ ($\bar{2} \times \bar{5} = \bar{4} \times \bar{5} = \bar{6} \times \bar{5} = \bar{8} \times \bar{5} = \bar{0}$).
- $\bar{3}x + \bar{4} = \bar{1} \iff \bar{3}x = \bar{7} \iff x = \bar{7} \times \bar{7} = \bar{9}$ (on multiplie par $\bar{3}^{-1} = \bar{7}$) ; contrôle : $3 \times 9 + 4 = 31 \equiv 1 [10]$.
- $\bar{2}x = \bar{4}$ a **deux** solutions, $\bar{2}$ et $\bar{7}$ ($\bar{14} = \bar{4}$) : on ne peut pas « simplifier par $\bar{2}$ », qui n'est pas régulier.

8

Corps

Définition

Un **corps** est un anneau unitaire $(K, +, \times)$ tel que $1 \neq 0$ et dans lequel **tout élément non nul est inversible** : autrement dit, $(K^*, \times)$ est un groupe, où $K^* = K \setminus \{0\}$. Si $\times$ est commutative, le corps est dit **commutatif**.

Une partie L d'un corps K est un **sous-corps** si elle est stable par $+$ et $\times$ et si, munie des lois induites, c'est un corps ; il faut et il suffit que $1 \in L$, $x - y \in L$ et $xy^{-1} \in L$ pour tous $x \in L$, $y \in L^*$ (caractérisation des sous-groupes, appliquée à $(L, +)$ et à $(L^*, \times)$).

Théorème

Un corps n'a pas de diviseur de zéro : $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Un corps commutatif est donc un anneau intègre.

Démonstration. Si $ab = 0$ et $a \neq 0$, alors $b = a^{-1}(ab) = a^{-1} \times 0 = 0$. $\square$

Exemples : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps commutatifs ; $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et $\mathbb{R}$ un sous-corps de $\mathbb{C}$. $(\mathbb{Z}, +, \times)$ est intègre, mais ce n'est **pas** un corps : 2 n'a pas d'inverse dans $\mathbb{Z}$.

Théorème ($\mathbb{Z}/p\mathbb{Z}$)

Soit $n \geq 2$. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps $\iff n$ est premier.

Démonstration. Si $n = p$ est premier et $\bar{a} \neq \bar{0}$, alors $p \nmid a$, donc $a \wedge p = 1$: par Bézout, $au + pv = 1$, et $\bar{a}\bar{u} = \bar{1}$. Si n n'est pas premier, $n = ab$ avec $1 < a, b < n$: $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ et $\bar{a}\bar{b} = \bar{n} = \bar{0}$: $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro, ce n'est pas un corps. $\square$

Exemple : la table de $((\mathbb{Z}/7\mathbb{Z})^*, \times)$

$\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

- Chaque ligne contient $\bar{1}$ (en vert) : tout élément non nul est inversible ; $\bar{2}^{-1} = \bar{4}$, $\bar{3}^{-1} = \bar{5}$, $\bar{6}^{-1} = \bar{6}$.
- Les puissances de $\bar{3}$ sont $\bar{3}, \bar{2}, \bar{6}, \bar{4}, \bar{5}, \bar{1}$: elles décrivent tout $(\mathbb{Z}/7\mathbb{Z})^*$.
- Dans le corps $\mathbb{Z}/7\mathbb{Z}$, $(x - \bar{2})(x - \bar{4}) = x^2 - \bar{6}x + \bar{8} = x^2 + x + \bar{1}$; comme $\mathbb{Z}/7\mathbb{Z}$ est intègre : $x^2 + x + \bar{1} = \bar{0} \iff x \in \{\bar{2}, \bar{4}\}$.

Théorème $(\mathbb{Q}(\sqrt{2}))$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $(\mathbb{R}, +, \times)$, et l'écriture $a + b\sqrt{2}$ est unique. L'inverse de $x = a + b\sqrt{2} \neq 0$ s'obtient avec la **quantité conjuguée** :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Démonstration. *Unicité* : si $a + b\sqrt{2} = a' + b'\sqrt{2}$ avec $b \neq b'$, alors $\sqrt{2} = \frac{a-a'}{b'-b} \in \mathbb{Q}$: absurde ($\sqrt{2}$ est irrationnel). *Sous-corps* : $1 = 1 + 0\sqrt{2}$; $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$; $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Si $x = a + b\sqrt{2} \neq 0$, alors $a - b\sqrt{2} \neq 0$ (sinon $a = b\sqrt{2}$, donc $b = 0$ par irrationalité, puis $a = 0$), donc $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) \neq 0$, et x^{-1} est donné par la formule : il est dans $\mathbb{Q}(\sqrt{2})$. $\square$

Exemples : $\frac{1}{5 + 3\sqrt{2}} = \frac{5 - 3\sqrt{2}}{25 - 18} = \frac{5}{7} - \frac{3}{7}\sqrt{2}$; $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$. En revanche, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$ est un anneau (même calcul) mais pas un corps : $\frac{1}{\sqrt{2}} = \frac{1}{2}\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]$, alors que $1 + \sqrt{2}$ y est inversible, d'inverse $-1 + \sqrt{2}$.

Exemple : transport de structure pour les anneaux et les corps

Le théorème de transport s'étend : si f est une bijection de E sur un anneau (un corps) $(F, +, \times)$ telle que $f(x * y) = f(x) + f(y)$ et $f(x \otimes y) = f(x) \times f(y)$, alors $(E, *, \otimes)$ est un anneau (un corps), isomorphe à F . Sur $\mathbb{R}$, posons $x * y = x + y - 1$ et $x \otimes y = xy - x - y + 2$. Avec $f(x) = x - 1$ (bijection de $\mathbb{R}$ sur $\mathbb{R}$) :

$$f(x * y) = x + y - 2 = f(x) + f(y), \quad f(x \otimes y) = xy - x - y + 1 = (x - 1)(y - 1) = f(x)f(y).$$

Donc $(\mathbb{R}, *, \otimes)$ est un **corps commutatif**, de zéro $f^{-1}(0) = 1$ et d'unité $f^{-1}(1) = 2$; l'inverse de $x \neq 1$ pour $\otimes$ est $f^{-1}\left(\frac{1}{x-1}\right) = \frac{x}{x-1}$ (contrôle : $x \otimes \frac{x}{x-1} = (x - 1) \cdot \frac{1}{x-1} + 1 = 2$).

9

Matrices carrées d'ordre 2 et 3

Définition

Soit $n \in \{2, 3\}$. Une **matrice carrée d'ordre n** est un tableau $A = (a_{ij})$ de n lignes et n colonnes de réels ; a_{ij} est le coefficient de la ligne i et de la colonne j . On note $M_n(\mathbb{R})$ leur ensemble :

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R}), \quad A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in M_3(\mathbb{R}).$$

Deux matrices sont égales si leurs coefficients sont égaux un à un. On pose $A + B = (a_{ij} + b_{ij})$ et $\lambda A = (\lambda a_{ij})$ ($\lambda \in \mathbb{R}$) ; O est la matrice nulle, $-A = (-a_{ij})$, et la **matrice unité** I_n a des 1 sur la diagonale et des 0 ailleurs. Le **produit** $AB = (c_{ij})$ se calcule « ligne i de $A \times$ colonne j de B » :

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} ; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Exemple : un produit d'ordre 3, ligne par colonne

$$\begin{pmatrix} 1 & 2 & 0 \\ -1 & 1 & 3 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 2 \\ 1 & 1 & 7 \\ 5 & 3 & 2 \end{pmatrix}, \quad c_{23} = (-1) \times 0 + 1 \times 1 + 3 \times 2 = 7.$$

Dans l'autre ordre, la première ligne de BA est $(1 \ 5 \ 3)$: $BA \neq AB$.

Théorème

Pour $n \in \{2, 3\}$, $(M_n(\mathbb{R}), +, \times)$ est un **anneau unitaire** (unité I_n), **non commutatif** et **non intègre**. De plus, $(\lambda A)B = A(\lambda B) = \lambda(AB)$.

Démonstration. $(M_n(\mathbb{R}), +)$ est un groupe commutatif (on additionne coefficient par coefficient, dans $(\mathbb{R}, +)$). **Associativité** : le coefficient (i, j) de $(AB)C$ est

$$\sum_l \left(\sum_k a_{ik} b_{kl} \right) c_{lj} = \sum_k \sum_l a_{ik} b_{kl} c_{lj} = \sum_k a_{ik} \left(\sum_l b_{kl} c_{lj} \right),$$

celui de $A(BC)$. **Distributivité** : $\sum_k a_{ik} (b_{kj} + c_{kj}) = \sum_k a_{ik} b_{kj} + \sum_k a_{ik} c_{kj}$, et de même à droite. **Unité** : $\sum_k a_{ik} \delta_{kj} = a_{ij}$, où δ_{kj} (1 si $k = j$, 0 sinon) est le coefficient de I_n . Les contre-exemples suivants montrent le reste. $\square$

Exemple : non-commutativité, diviseurs de zéro

$$\bullet A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} : AB = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

$$\bullet C = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, D = \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix} : \boxed{CD = O} \text{ alors que } C \neq O \text{ et } D \neq O ; \text{ et pourtant } DC = \begin{pmatrix} -6 & -12 \\ 3 & 6 \end{pmatrix} \text{ n'est pas nulle.}$$

• $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ vérifie $N^2 = O$ (matrice **nilpotente**) ; $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ vérifie $S^2 = I_2$, et $S \neq \pm I_2$.

Attention, piège !

Comme $AB \neq BA$ en général : $(A+B)^2 = A^2 + AB + BA + B^2$ (et non $A^2 + 2AB + B^2$), $(AB)^2 = ABAB$ (et non A^2B^2) ; et comme l'anneau n'est pas intègre : $A^2 = O \nRightarrow A = O$, $AB = AC \nRightarrow B = C$. Seules les matrices λI_n commutent à coup sûr avec toutes les autres.

10 Matrices inversibles, puissances

Définition

Une matrice $A \in M_n(\mathbb{R})$ est **inversible** s'il existe $B \in M_n(\mathbb{R})$ telle que $AB = BA = I_n$; B est unique (section 2), c'est l'**inverse** A^{-1} . L'ensemble des matrices inversibles est noté $GL_n(\mathbb{R})$.

Théorème

$(GL_n(\mathbb{R}), \times)$ est un groupe (non commutatif) : c'est le groupe des inversibles de l'anneau $M_n(\mathbb{R})$ (section 7). En particulier $(AB)^{-1} = B^{-1}A^{-1}$, $(A^{-1})^{-1} = A$, et une matrice inversible est régulière : $AB = AC \Rightarrow B = C$.

Théorème (inverse d'ordre 2)

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\det(A) = ad - bc$ (le **déterminant** de A). Alors

A est inversible $\iff \det(A) \neq 0$,

et dans ce cas

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Démonstration. Soit $\tilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$: le calcul donne $A\tilde{A} = \tilde{A}A = (ad - bc)I_2$. Si $\det(A) \neq 0$, la matrice $\frac{1}{\det(A)}\tilde{A}$ est l'inverse de A . Si $\det(A) = 0$ et si A était inversible, alors $\tilde{A} = A^{-1}(A\tilde{A}) = A^{-1}O = O$, donc $a = b = c = d = 0$ et $A = O$, qui n'est pas inversible ($OB = O \neq I_2$) : contradiction. $\square$

Exemple : $A = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$, $\det(A) = 1$, $A^{-1} = \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$. Le système $\begin{cases} 4x + 3y = 5 \\ x + y = 2 \end{cases}$ s'écrit $A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$, donc $\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} -1 \\ 3 \end{pmatrix}$. On vérifie aussi par le calcul que $\det(AB) = \det(A)\det(B)$.

Méthode : inverser une matrice d'ordre 3 : résoudre $AX = Y$

On résout le système $AX = Y$, d'inconnue la colonne X (coefficients x, y, z), pour une colonne Y (coefficients a, b, c) quelconque. Si l'on obtient une unique solution $X = BY$ pour tout Y , alors A est inversible et $A^{-1} = B$ (en effet $A(BY) = Y$ pour tout Y donne $AB = I_3$, et $BAX = X$ pour tout X donne $BA = I_3$). Si le système n'a pas toujours une unique solution, A n'est pas inversible.

Exemple : l'inverse d'une matrice d'ordre 3 par un système

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 2 \end{pmatrix} : \quad AX = Y \iff \begin{cases} x + 2y + z = a \\ y + z = b \\ x + 2y + 2z = c \end{cases} \iff \begin{cases} z = c - a & (L_3 - L_1) \\ y = b - z = a + b - c \\ x = a - 2y - z = -2b + c \end{cases}$$

Pour tout Y , la solution est unique et l'on lit ses coefficients : $A^{-1} = \begin{pmatrix} 0 & -2 & 1 \\ 1 & 1 & -1 \\ -1 & 0 & 1 \end{pmatrix}$.

En revanche, pour la matrice ci-dessous, la ligne L_3 est la somme $L_1 + L_2$:

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} : \quad BX = Y \text{ avec } (a, b, c) = (0, 0, 1) \text{ donnerait } L_3 - L_1 - L_2 : 0 = 1;$$

ce système n'a pas de solution, donc B n'est pas inversible.

Méthode : inverse et puissances grâce à une relation polynomiale

Si $A^2 = \alpha A + \beta I$ avec $\beta \neq 0$, alors $A \cdot \frac{1}{\beta}(A - \alpha I) = \frac{1}{\beta}(A - \alpha I) \cdot A = I : A^{-1} = \frac{1}{\beta}(A - \alpha I)$.

Exemple :

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad A^2 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} = A + 2I_3, \quad \text{donc} \quad A^{-1} = \frac{1}{2}(A - I_3) = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

Théorème (binôme de Newton pour les matrices)

Si $AB = BA$, alors pour tout $n \in \mathbb{N}$: $(A + B)^n = \sum_{k=0}^n \binom{n}{k} A^k B^{n-k}$ (avec $A^0 = B^0 = I$).

C'est la règle de calcul de la section 7 dans l'anneau $M_n(\mathbb{R})$. Elle est très efficace avec I (qui commute avec tout) et une matrice **nilpotente** N ($N^p = O$) : la somme s'arrête au rang $p - 1$.

Exemple : trois calculs de A^n

• **Par récurrence**, pour $T = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$: si $T^n = \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}$, alors

$$T^{n+1} = T^n T = \begin{pmatrix} 2^{n+1} & 2^n + n2^n \\ 0 & 2^{n+1} \end{pmatrix} = \begin{pmatrix} 2^{n+1} & (n+1)2^n \\ 0 & 2^{n+1} \end{pmatrix}.$$

Par le binôme : $T = 2I_2 + N$, où $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ vérifie $N^2 = O$: $T^n = 2^n I_2 + n2^{n-1} N$, même résultat.

- Une matrice nilpotente : $M = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $M^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $M^3 = O$, donc

$$(I_3 + M)^n = I_3 + nM + \frac{n(n-1)}{2}M^2 = \begin{pmatrix} 1 & n & \frac{n(n-1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}, \quad (I_3 + M)^{-1} = I_3 - M + M^2 = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\text{car } (I_3 + M)(I_3 - M + M^2) = I_3 + M^3 = I_3.$$

- Avec la matrice J dont tous les coefficients valent 1 (ordre 3) : $J^2 = 3J$, donc $J^k = 3^{k-1}J$ pour $k \geq 1$. La matrice A de la méthode précédente s'écrit $A = J - I_3$, et J commute avec $-I_3$:

$$A^n = \sum_{k=0}^n \binom{n}{k} J^k (-I_3)^{n-k} = (-1)^n I_3 + \frac{1}{3} \sum_{k=1}^n \binom{n}{k} 3^k (-1)^{n-k} J = \boxed{(-1)^n I_3 + \frac{2^n - (-1)^n}{3} J}$$

(car $\sum_{k=0}^n \binom{n}{k} 3^k (-1)^{n-k} = 2^n$). Contrôle : $n = 2$ donne $I_3 + J = A + 2I_3$; et la formule reste vraie pour $n = -1$: $-I_3 + \frac{1}{2}J = \frac{1}{2}(A - I_3)$.

11

Structures de matrices

Méthode : étudier un ensemble de matrices $E = \{M(x)\}$ ou $F = \{M(a, b)\}$

1. Calculer $M(x)M(y)$ et le reconnaître : $M(x)M(y) = M(x+y)$, $M(xy)$, ... (E est alors **stable**).
2. Construire la bijection $x \mapsto M(x)$ (injective : on lit x sur un coefficient).
3. Conclure par **transport de structure** (ou montrer que E est un sous-groupe de $GL_n(\mathbb{R})$) ; inverses et puissances se lisent sur les paramètres.

Exemple : type examen : un groupe isomorphe à $(\mathbb{R}, +)$

Pour $x \in \mathbb{R}$, soit $M(x) = \begin{pmatrix} 1 & x & \frac{x^2}{2} \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}$ et $E = \{M(x), x \in \mathbb{R}\}$.

1. Le produit ligne par colonne donne

$$M(x)M(y) = \begin{pmatrix} 1 & y+x & \frac{y^2}{2} + xy + \frac{x^2}{2} \\ 0 & 1 & y+x \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y & \frac{(x+y)^2}{2} \\ 0 & 1 & x+y \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{soit } \boxed{M(x)M(y) = M(x+y)} :$$

E est stable par $\times$.

2. $\varphi : x \mapsto M(x)$ est une bijection de $\mathbb{R}$ sur E : surjective par définition de E , injective car x est le coefficient $(1, 2)$ de $M(x)$. Et $\varphi(x+y) = \varphi(x)\varphi(y)$.

3. Par transport (appliqué à $\varphi^{-1} : E \rightarrow \mathbb{R}$), $(E, \times)$ est un **groupe commutatif isomorphe à $(\mathbb{R}, +)$** : son neutre est $M(0) = I_3$, $M(x)^{-1} = M(-x)$, et $M(x)^n = M(nx)$ pour $n \in \mathbb{Z}$; par exemple $M(1)^{10} = M(10)$, dont la première ligne est $(1 \ 10 \ 50)$. L'équation $X^2 = M(4)$ a une seule solution dans E , $X = M(2)$ ($M(2x) = M(4) \iff x = 2$).

4. $t \mapsto M(\ln t)$ est un isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(E, \times)$ (composée de $\ln$ et de φ).

Exemple : type examen : un corps isomorphe à $\mathbb{C}$

Pour $(a, b) \in \mathbb{R}^2$, soit $M(a, b) = \begin{pmatrix} a-b & -2b \\ b & a+b \end{pmatrix}$ et $F = \{M(a, b), (a, b) \in \mathbb{R}^2\}$.

1. $M(a, b) = aI_2 + bJ$ avec $J = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}$, et $J^2 = \begin{pmatrix} 1-2 & 2-2 \\ -1+1 & -2+1 \end{pmatrix} = -I_2$.

2. $M(a, b) + M(c, d) = M(a+c, b+d)$ et $M(a, b)M(c, d) = acI_2 + (ad+bc)J + bdJ^2 = M(ac-bd, ad+bc)$: F est stable par $+$ et par $\times$, et $\times$ est commutative sur F .

3. $\varphi : a + ib \mapsto M(a, b)$ est une bijection de $\mathbb{C}$ sur F (si $M(a, b) = M(c, d)$, le coefficient $(2, 1)$ donne $b = d$, puis $a = c$), et, puisque $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$:

$$\varphi(z + z') = \varphi(z) + \varphi(z'), \quad \varphi(zz') = \varphi(z)\varphi(z').$$

Par transport, $(F, +, \times)$ est un corps commutatif isomorphe à $(\mathbb{C}, +, \times)$; $J = \varphi(i)$ « est » le nombre i .

4. Inverse : $M(a, b)^{-1} = \varphi\left(\frac{a-ib}{a^2+b^2}\right) = \frac{1}{a^2+b^2}M(a, -b)$ (cohérent avec $\det M(a, b) = a^2 - b^2 + 2b^2 = a^2 + b^2$). Puissances : $(1+i)^4 = -4$ et $(1+i)^8 = 16$, donc $M(1, 1)^4 = -4I_2$ et $M(1, 1)^8 = 16I_2$. Plus généralement, $\theta \mapsto M(\cos \theta, \sin \theta)$ est un morphisme de $(\mathbb{R}, +)$ dans $(F^*, \times)$, et $M(\cos \theta, \sin \theta)^n = M(\cos n\theta, \sin n\theta)$ (Moivre).

12

Les pièges classiques

× Faux	✓ Vrai
« pour le neutre, il suffit que $x * e = x$ »	il faut aussi $e * x = x$: pour la loi $x * y = y$, tout élément est neutre à gauche, et aucun n'est neutre
« $(x * y)' = x' * y'$ »	$(x * y)' = y' * x'$: $(f_2 \circ f_3)^{-1} = f_4^{-1} = f_5$, mais $f_2^{-1} \circ f_3^{-1} = f_4$ (section 3)
« un élément régulier est symétrisable »	dans $(\mathbb{N}, +)$, 2 est régulier sans opposé ; sur $\mathbb{R}_+$, pour $\sqrt{x^2 + y^2}$, seul 0 est symétrisable
« une partie stable qui contient e est un sous-groupe »	il faut aussi les symétriques : $\mathbb{N}$ est stable dans $(\mathbb{Z}, +)$, mais $-1 \notin \mathbb{N}$
« la réunion de deux sous-groupes est un sous-groupe »	$2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3, mais pas $2 + 3 = 5$; l'intersection, elle, est un sous-groupe
« $\mathbb{Z}/n\mathbb{Z}$ est toujours intègre »	seulement si n est premier : $\bar{2} \times \bar{5} = \bar{0}$ dans $\mathbb{Z}/10\mathbb{Z}$
« $1/(a + b\sqrt{2}) = 1/a + 1/(b\sqrt{2})$ »	on multiplie par la quantité conjuguée : $1/(a + b\sqrt{2}) = (a - b\sqrt{2})/(a^2 - 2b^2)$
« $AB = O \Rightarrow A = O$ ou $B = O$ » ; « une matrice non nulle est inversible »	$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix} = O$: $M_2(\mathbb{R})$ n'est pas intègre, et ces matrices non nulles ne sont pas inversibles ($\det = 0$)
« $(AB)^2 = A^2B^2$ » ; « $(A+B)^2 = A^2 + 2AB + B^2$ »	vrai seulement si $AB = BA$; sinon $(AB)^2 = ABAB$ et $(A+B)^2 = A^2 + AB + BA + B^2$

« $A^2 = I_2 \Rightarrow A = \pm I_2$ » ; « $A^2 = O \Rightarrow A = O$ »	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I_2$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = O$
« $\det(A + B) = \det A + \det B$ »	$\det(2I_2) = 4 \neq 2$; en revanche $\det(AB) = \det A \times \det B$
« $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & 1/b \\ 1/c & 1/d \end{pmatrix}$ »	$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, si $ad - bc \neq 0$

13

Les astuces des concours

★ Astuce de concours : une partie finie stable est un sous-groupe

Si H est une partie **finie**, non vide et stable du groupe $(G, *)$, alors H est un sous-groupe. En effet, pour $x \in H$, les puissances $x^{(1)}, x^{(2)}, \dots$ sont dans H , qui est fini : il existe $p < q$ tels que $x^{(p)} = x^{(q)}$, donc $x^{(q-p)} = e$ (régularité). Ainsi $e \in H$, et $x' = x^{(q-p-1)} \in H$. Exemples : $\mathbb{U}_n$ (stable par $*$) ; le groupe des six fonctions f_k (sa table montre qu'il est stable).

★ Astuce de concours : si $x * x = e$ pour tout x , le groupe est commutatif

On a alors $x' = x$ pour tout x , donc $x * y = (x * y)' = y' * x' = y * x$. Exemple : la table de $\{1, 3, 5, 7\}$ modulo 8 (section 1). Plus généralement, si $(x * y)^{(2)} = x^{(2)} * y^{(2)}$ pour tous x, y , alors $x * y * x * y = x * x * y * y$, et en simplifiant à gauche par x et à droite par y : $y * x = x * y$.

★ Astuce de concours : le noyau d'un morphisme

Si $f : (G, *) \rightarrow (G', \otimes)$ est un morphisme, son **noyau** $\text{Ker } f = f^{-1}(\{e'\})$ est un sous-groupe de G (section 5, point 3), et f injective $\iff \text{Ker } f = \{e\}$ car $f(x) = f(y) \iff f(x * y') = e' \iff x * y' \in \text{Ker } f$. Exemples : le noyau de $\theta \mapsto e^{i\theta}$ est $2\pi\mathbb{Z}$; celui de $z \mapsto |z|$ est $\mathbb{U}$; celui de $z \mapsto z^n$ sur $\mathbb{C}^*$ est $\mathbb{U}_n$: trois sous-groupes obtenus sans calcul.

★ Astuce de concours : deviner l'isomorphisme

Pour une loi « affine » $x * y = axy + bx + by + c$, on cherche α tel que $x * y - \alpha = a(x - \alpha)(y - \alpha)$: alors $f(x) = a(x - \alpha)$ vérifie $f(x * y) = f(x)f(y)$. Exemple : $x * y = 2xy - 2x - 2y + 3 = 2(x - 1)(y - 1) + 1$ sur $I =]1, +\infty[$; $f(x) = 2(x - 1)$ est une bijection de I sur $\mathbb{R}_+^*$ et $f(x * y) = 4(x - 1)(y - 1) = f(x)f(y)$: $(I, *)$ est un groupe, de neutre $f^{-1}(1) = \frac{3}{2}$, et $x' = f^{-1}\left(\frac{1}{f(x)}\right) = 1 + \frac{1}{4(x-1)}$.

Autres réflexes : pour $\frac{x+y}{1+xy}$, essayer $\frac{1+x}{1-x}$ (section 6) ; et si la loi est « déguisée », de la forme $x * y = g^{-1}(g(x) \otimes g(y))$ (avec une racine, un logarithme, une exponentielle...), l'isomorphisme cherché est g lui-même.

★ Astuce de concours : un anneau intègre fini est un corps

Si A est un anneau commutatif, unitaire, intègre et **fini**, et si $a \neq 0$, l'application $x \mapsto ax$ est injective ($ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x = y$), donc bijective (ensemble fini) : il existe u tel que $au = 1$. On retrouve que $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier (il est intègre par le lemme d'Euclide).

★ **Astuce de concours : la relation $A^2 - (a+d)A + (ad-bc)I_2 = 0$ (ordre 2)**

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, le calcul donne $A^2 = (a+d)A - (ad-bc)I_2$. On en tire l'inverse, et les puissances sous la forme $A^n = u_n A + v_n I_2$ avec des suites récurrentes. *Exemple :*

$$A = \begin{pmatrix} 3 & -2 \\ 1 & 0 \end{pmatrix} : \quad A^2 = 3A - 2I_2, \quad A^{-1} = \frac{1}{2}(3I_2 - A) = \begin{pmatrix} 0 & 1 \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix},$$

et, si $A^n = u_n A + v_n I_2$: $A^{n+1} = u_n(3A - 2I_2) + v_n A$, soit $u_{n+1} = 3u_n + v_n$ et $v_{n+1} = -2u_n$, avec $u_0 = 0$, $v_0 = 1$. Une récurrence immédiate donne alors

$$\boxed{A^n = (2^n - 1)A + (2 - 2^n)I_2} \quad \text{pour tout } n \in \mathbb{N} \quad (\text{et même pour } n = -1).$$

14

L'essentiel du chapitre en une page

Lois de composition interne

interne : $x, y \in E \Rightarrow x * y \in E$; A stable : idem dans A

neutre : $x * e = e * x = x$ (unique)

symétrique : $x * x' = x' * x = e$ (unique si $*$ associative)

$(x * y)' = y' * x'$; $(x')' = x$; symétrisable $\Rightarrow$ régulier

régulier : $a * x = a * y \Rightarrow x = y$ (et à droite)

distributivité : $x \otimes (y * z) = (x \otimes y) * (x \otimes z)$ (et à droite)

Groupes

associative, neutre e , tout élément symétrisable

$a * x = b \iff x = a' * b$; table finie = carré latin

$x^{(m)} * x^{(n)} = x^{(m+n)}$, $(x^{(m)})^{(n)} = x^{(mn)}$, $x^{(-n)} = (x')^{(n)}$

$(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(S(E), \circ)$

Sous-groupes

$H \neq \emptyset$ et $x, y \in H \Rightarrow x * y' \in H$

sous-groupes de $(\mathbb{Z}, +)$: les $n\mathbb{Z}$, $n \in \mathbb{N}$

$\mathbb{U}_n \subset \mathbb{U} \subset \mathbb{C}^*$; $\mathbb{U}_m \cap \mathbb{U}_n = \mathbb{U}_{m \wedge n}$

H fini, non vide et stable $\Rightarrow$ sous-groupe

Morphismes

$f(x * y) = f(x) \otimes f(y) \Rightarrow f(e) = e'$, $f(x') = f(x)'$

$f(H)$ et $f^{-1}(H')$ sont des sous-groupes

$\text{Ker } f = f^{-1}(\{e'\})$; f injective $\iff \text{Ker } f = \{e\}$

$\ln, \exp, \theta \mapsto e^{i\theta}, z \mapsto |z|, z \mapsto z^n$

Isomorphismes et transport

isomorphisme = morphisme bijectif ; f^{-1} aussi

$f : E \rightarrow (F, \otimes)$ bijective, $f(x * y) = f(x) \otimes f(y)$

$\Rightarrow (E, *)$ groupe, neutre $f^{-1}(e_F)$, $x' = f^{-1}(f(x)')$

$x^{(n)} = f^{-1}(f(x)^{(n)})$

$x * y = \frac{x+y}{1+xy}$: $f(x) = \frac{1+x}{1-x}$

$x * y - \alpha = a(x - \alpha)(y - \alpha)$: $f(x) = a(x - \alpha)$

Anneaux

$(A, +)$ groupe commutatif, $\times$ associative et distributive

$a \times 0 = 0$; $(-a)b = -ab$; binôme si $ab = ba$

intègre : $ab = 0 \Rightarrow a = 0$ ou $b = 0$

les inversibles forment un groupe $(A^*, \times)$

$\mathbb{Z}/n\mathbb{Z}$ et corps

$\bar{a}$ inversible $\iff a \wedge n = 1$; sinon $(\bar{a} \neq \bar{0})$

diviseur de zéro

corps : $(K^*, \times)$ groupe ; un corps est sans diviseur de zéro

$\mathbb{Z}/n\mathbb{Z}$ corps $\iff n$ premier ; $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2})$

$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$; intègre et fini $\Rightarrow$ corps

Matrices d'ordre 2 et 3

$c_{ij} = \sum_k a_{ik} b_{kj}$ (ligne $\times$ colonne)

$(M_n(\mathbb{R}), +, \times)$: anneau unitaire, ni commutatif, ni intègre

$(A + B)^2 = A^2 + AB + BA + B^2$; $AB = O$ avec $A, B \neq O$

Inverses

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ si $ad - bc \neq 0$

ordre 3 : résoudre $AX = Y$; $(AB)^{-1} = B^{-1}A^{-1}$

$A^2 = \alpha A + \beta I$, $\beta \neq 0 \Rightarrow A^{-1} = \frac{1}{\beta}(A - \alpha I)$

ordre 2 : $A^2 = (a + d)A - (ad - bc)I_2$

Puissances

par récurrence, ou binôme si $AB = BA$ (par exemple $\lambda I + N$)

$N^3 = O$: $(I + N)^n = I + nN + \binom{n}{2}N^2$, $(I + N)^{-1} = I - N + N^2$

J (que des 1, ordre 3) : $J^k = 3^{k-1}J$ ($k \geq 1$)

Structures de matrices

$M(x)M(y) = M(x + y)$: $(E, \times) \simeq (\mathbb{R}, +)$, $M(x)^{-1} = M(-x)$

$M(a, b) = aI + bJ$, $J^2 = -I$: $(F, +, \times)$ corps $\simeq (\mathbb{C}, +, \times)$

$M(a, b)^{-1} = \frac{1}{a^2 + b^2} M(a, -b)$

Bon courage ! La régularité bat le talent.

Maths Olympiad

Partie B • Le parcours

30 exercices sur 4 niveaux, du plus simple au niveau concours

Notations : I : matrice unité ; $\bar{k}$: classe de k dans $\mathbb{Z}/n\mathbb{Z}$; $a \wedge b, a \vee b$: PGCD, PPCM ; $x^{(n)} = x * \dots * x$ (n termes) ; $|G|$: nombre d'éléments de G .

15 Niveau I • Bases

Exercice 1 Lois et parties stables ★

corrigé p. 43

- Loi interne ? a) $\frac{x+y}{2}$ sur $\mathbb{Z}$, sur $\mathbb{Q}$; b) $x^2 + y^2$ sur $[0, 1]$, sur $\mathbb{N}$; c) $\ln(e^x + e^y)$ sur $\mathbb{R}_+$, sur $\mathbb{R}_-$.
- $\{n \in \mathbb{N} : n \equiv 1 [4]\}$: stable pour $*$? pour $+$? Fonctions impaires de $\mathbb{R}$ dans $\mathbb{R}$: pour $+$? $*$?
- Sur $\mathbb{R}$, $x * y = \ln(e^x + e^y)$: montrer que $*$ est commutative, associative, que tout réel est régulier, mais qu'il n'y a pas de neutre. Calculer $x^{(n)}$.

Exercice 2 Une loi qui cache l'addition ★

corrigé p. 43

On munit $\mathbb{R}$ de la loi $x * y = \sqrt[3]{x^3 + y^3}$.

- Montrer que $(\mathbb{R}, *)$ est un groupe commutatif (neutre ? symétrique de x ?). Calculer $x^{(n)}$, puis résoudre $x * 2 = 3$ et $x * x * x = 3$.
- Montrer que $*$ est distributive par rapport à $+$, mais pas $+$ par rapport à $*$.
- $\mathbb{R}_+$ est-il un sous-groupe de $(\mathbb{R}, *)$? Et $\{\sqrt[3]{n}, n \in \mathbb{Z}\}$?

Exercice 3 Deux tables de Cayley ★

corrigé p. 43

- Sur $\mathbb{R}^*$: $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$. Dresser la table de $\cdot$ sur $G = \{f_1, f_2, f_3, f_4\}$; en déduire que $(G, \cdot)$ est un groupe commutatif où chaque élément est son propre symétrique.
- Soit $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Dresser la table de $(H, \times)$, $H = \{I, R, R^2, R^3\}$: groupe commutatif (inverses ?).
- Montrer qu'aucune bijection $\varphi : G \rightarrow H$ ne vérifie $\varphi(f \cdot g) = \varphi(f)\varphi(g)$ pour tous $f, g \in G$.

Exercice 4 Sous-groupes : vrai ou faux ? ★

corrigé p. 44

H est-il un sous-groupe du groupe G ?

- a) $H = \{2^n 3^m, n, m \in \mathbb{Z}\}$, $G = (\mathbb{Q}_+^*, \times)$; b) H : rationnels $\frac{p}{q}$ avec p, q impairs, $G = (\mathbb{Q}_+^*, \times)$; $H = \{x : |x| \geq 1\}$, $G = (\mathbb{R}^*, \times)$.
- a) $\{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$, puis $\{a + b\sqrt{2}, a, b \in \mathbb{N}\}$, dans $(\mathbb{R}, +)$; b) $\{f : f(1) = 0\}$, puis $\{f : f(1) = 1\}$, dans $(F(\mathbb{R}, \mathbb{R}), +)$.
- a) $H = \{e^{i\pi r}, r \in \mathbb{Q}\}$, $G = (\mathbb{U}, \times)$; b) $H = \{z : \operatorname{Re}(z) > 0\}$, $G = (\mathbb{C}^*, \times)$.

Exercice 5 Un groupe non commutatif ★

corrigé p. 44

Sur $G = \mathbb{R}^2$, on pose $(a, b) * (c, d) = (a + c, b e^c + d)$.

1. Montrer que $(G, *)$ est un groupe non commutatif (neutre ? symétrique de (a, b) ?).
2. Résoudre $(1, 0) * X = (2, 3)$, puis $X * (1, 0) = (2, 3)$. Calculer $(1, 1)^{(n)}$ pour $n \in \mathbb{N}^*$.
3. Montrer que les éléments commutant avec $(1, 0)$ forment un sous-groupe isomorphe à $(\mathbb{R}, +)$.

Exercice 6 Morphisme ou pas ? ★

corrigé p. 44

L'application est-elle un morphisme de groupes ? Si oui, est-elle injective ? surjective ?

1. a) $x \mapsto 2^{-x}$, de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$; image de $\mathbb{Z}$? b) $z \mapsto \operatorname{Re}(z) + \operatorname{Im}(z)$, de $(\mathbb{C}, +)$ dans $(\mathbb{R}, +)$.
2. $z \mapsto z^2$, de $(\mathbb{C}^*, \times)$ dans $(\mathbb{C}^*, \times)$; images de $\mathbb{U}$ et de $\mathbb{R}^*$?
3. $A \mapsto \det A$, de $(\operatorname{GL}_2(\mathbb{R}), \times)$ dans $(\mathbb{R}^*, \times)$; en déduire que $\operatorname{SL}_2(\mathbb{R}) = \{A : \det A = 1\}$ est un sous-groupe.

Exercice 7 Anneaux, inversibles, diviseurs de zéro ★

corrigé p. 44

1. Montrer que $\mathbb{Z}^2$, muni de $(a, b) + (c, d) = (a + c, b + d)$ et $(a, b) \times (c, d) = (ac, bd)$, est un anneau commutatif unitaire non intègre. Inversibles ?
2. Dans $\mathbb{Z}/15\mathbb{Z}$: a) donner les inversibles et leurs inverses ; b) montrer que les autres éléments non nuls sont des diviseurs de zéro ; c) résoudre $\overline{7}x + \overline{2} = \overline{11}$, puis $\overline{6}x = \overline{9}$.

Exercice 8 Premiers calculs matriciels ★

corrigé p. 45

Soient $A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$, $N = \begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}$ et $C = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

1. Calculer AB et BA . Vérifier que $A^2 - 3A + 3I = 0$; en déduire que A est inversible et calculer A^{-1} .
2. Calculer N^2 ; en déduire l'inverse de $I + N$ et $(I + N)^n$ pour $n \in \mathbb{N}$.
3. Résoudre le système $CX = Y$, où $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $Y = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$; en déduire que C est inversible et C^{-1} .

16

Niveau 2 • Bac**Exercice 9** Type examen national (1) : un corps sur $\mathbb{R}_+^*$ ★★

corrigé p. 45

Pour $x, y \in \mathbb{R}_+^*$, on pose $x \otimes y = e^{\ln x \ln y}$ (autrement dit, $x \otimes y = x^{\ln y}$).

1. Montrer que $\otimes$ est commutative, distributive par rapport à $\times$, et que $\ln(x \otimes y) = \ln x \ln y$. En déduire que $(\mathbb{R}_+^*, \times, \otimes)$ est un corps commutatif (zéro ? unité ? symétrique pour $\otimes$ de $x \neq 1$?).
2. Montrer que $(]1, +\infty[, \otimes)$ est un groupe isomorphe à $(\mathbb{R}_+^*, \times)$. $]e, +\infty[$ en est-il un sous-groupe ?
3. Résoudre dans $\mathbb{R}_+^*$: a) $x \otimes x \otimes x = e^8$; b) $x \otimes x = 2 \otimes 8$.

Exercice 10 Type examen national (2) : un groupe de matrices ★★

corrigé p. 45

Soient $J = \begin{pmatrix} 2 & -1 \\ 2 & -1 \end{pmatrix}$ et, pour $x \in \mathbb{R}$, $M(x) = I + (x - 1)J = \begin{pmatrix} 2x-1 & 1-x \\ 2x-2 & 2-x \end{pmatrix}$; $E = \{M(x), x \in \mathbb{R}^*\}$.

1. Calculer J^2 , puis montrer que $M(x)M(y) = M(xy)$ pour tous réels x, y .
2. Montrer que $x \mapsto M(x)$ est un isomorphisme de $(\mathbb{R}^*, \times)$ sur $(E, \times)$; en déduire que $(E, \times)$ est un groupe commutatif (inverse de $M(x)$? contrôler avec $\det M(x)$).
3. Calculer $M(2)^{10}$. Résoudre dans E : $X^3 = M(-8)$, puis $X^2 = I$.

4. Montrer que $t \mapsto M(e^t)$ est un isomorphisme de $(\mathbb{R}, +)$ sur un sous-groupe de E .

Exercice 11 Type examen national (3) : un corps de matrices ★★

corrigé p. 46

Soient $K = \begin{pmatrix} 2 & -5 \\ 1 & -2 \end{pmatrix}$ et, pour $a, b \in \mathbb{R}$, $M(a, b) = aI + bK$; $F = \{M(a, b), (a, b) \in \mathbb{R}^2\}$.

1. Calculer K^2 , puis montrer que $M(a, b)M(c, d) = M(ac - bd, ad + bc)$.
2. Montrer que $\varphi : a + ib \mapsto M(a, b)$ est une bijection de $\mathbb{C}$ sur F qui vérifie $\varphi(z + z') = \varphi(z) + \varphi(z')$, $\varphi(zz') = \varphi(z)\varphi(z')$; en déduire que $(F, +, \times)$ est un corps commutatif. Inverse de $M(a, b) \neq 0$?
3. On pose $\Omega = M(1, \sqrt{3})$. Calculer Ω^3 et Ω^{2026} .
4. Résoudre dans $F : X^2 = -I$, puis $X^2 = \Omega$. $X^2 = -I$ a-t-elle d'autres solutions dans $M_2(\mathbb{R})$?

Exercice 12 Type examen national (4) : dans $\mathbb{Z}/17\mathbb{Z}$ ★★

corrigé p. 46

1. Justifier que $\mathbb{Z}/17\mathbb{Z}$ est un corps. Vérifier que $\overline{6}^2 = \overline{2}$, puis résoudre $x^2 = \overline{2}$ et $x^2 - \overline{2}x - \overline{1} = \overline{0}$.
2. Calculer $\overline{3}^k$ ($1 \leq k \leq 16$). Montrer que $k \mapsto \overline{3}^k$ est un morphisme surjectif de $(\mathbb{Z}, +)$ sur $((\mathbb{Z}/17\mathbb{Z})^*, \times)$ et que $\overline{3}^k = \overline{3}^m \iff k \equiv m [16]$.
3. Résoudre (poser $x = \overline{3}^k$) : $x^4 = -\overline{1}$, puis $x^5 = \overline{2}$. Montrer que les carrés de $(\mathbb{Z}/17\mathbb{Z})^*$ sont les $\overline{3}^{2j}$; $x^2 = \overline{3}$ a-t-elle des solutions ?

Exercice 13 Type examen national (5) : une loi sur $\mathbb{C}$ ★★

corrigé p. 47

On munit $\mathbb{C}$ de la loi $z * w = z + w + i zw$, et l'on pose $\varphi(z) = 1 + iz$.

1. Vérifier que $\varphi(z * w) = \varphi(z)\varphi(w)$; en déduire que $*$ est commutative et associative, de neutre 0, et que i est absorbant.
2. Soit $E = \mathbb{C} \setminus \{i\}$. Montrer que φ est un isomorphisme de $(E, *)$ sur $(\mathbb{C}^*, \times)$, donc que $(E, *)$ est un groupe commutatif. Symétrique de z ?
3. Montrer que le cercle $\Gamma : |z - i| = 1$ et la demi-droite $\Delta = \{iy, y < 1\}$ sont des sous-groupes.
4. Résoudre l'équation $z * z * z = 2i$ et placer ses solutions.

Exercice 14 Type examen national (6) : les nombres duaux ★★

corrigé p. 47

Sur $\mathbb{R}^2 : (a, b) + (c, d) = (a + c, b + d)$ et $(a, b) \otimes (c, d) = (ac, ad + bc)$. Soient $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $\psi(a, b) = aI + bN$.

1. Montrer que $A = \{aI + bN, a, b \in \mathbb{R}\}$ est un sous-anneau commutatif de $M_2(\mathbb{R})$ et que $\psi : \mathbb{R}^2 \rightarrow A$ est bijective, avec $\psi(u + v) = \psi(u) + \psi(v)$, $\psi(u \otimes v) = \psi(u)\psi(v)$; en déduire que $(\mathbb{R}^2, +, \otimes)$ est un anneau commutatif unitaire. Intègre ?
2. Montrer que (a, b) est inversible si et seulement si $a \neq 0$ (inverse ?), et que $(a, b)^n = (a^n, na^{n-1}b)$ pour $n \in \mathbb{N}^*$. Calculer $(2, 3)^5$.
3. Résoudre : $X \otimes X = (4, 12)$; $X \otimes X = (0, 0)$; $X \otimes X = (-1, 0)$.

Exercice 15 Matrices circulantes d'ordre 3 ★★

corrigé p. 47

Soient $P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, $M(a, b, c) = aI + bP + cP^2$ et $E = \{M(a, b, c), (a, b, c) \in \mathbb{R}^3\}$.

1. Calculer P^2, P^3 et écrire $M(a, b, c)$. Montrer que $(\{I, P, P^2\}, \times)$ est un groupe isomorphe à $(\mathbb{U}_3, \times)$.
2. Montrer que E est un sous-anneau commutatif de $M_3(\mathbb{R})$; calculer $(I + P + P^2)(I - P)$. Intègre ?
3. Calculer l'inverse de $I + P$ en résolvant un système, et vérifier qu'il appartient à E . Écrire $(I + P)^3$ et $(I + P)^6$ sous la forme $aI + bP + cP^2$.

Exercice 16 L'anneau $\mathbb{Z}[\sqrt{7}]$ ★★

corrigé p. 48

Soit $A = \{a + b\sqrt{7}, a, b \in \mathbb{Z}\}$; pour $x = a + b\sqrt{7}$, on pose $\sigma(x) = a - b\sqrt{7}$ et $N(x) = x\sigma(x) = a^2 - 7b^2$.

1. On admet que $\sqrt{7} \notin \mathbb{Q}$. Montrer que A est un sous-anneau de $\mathbb{R}$ et que $\sigma(xy) = \sigma(x)\sigma(y)$, $N(xy) = N(x)N(y)$.
2. Montrer que x est inversible dans A si et seulement si $N(x) = 1$ (raisonner modulo 7).
3. Soit $\varepsilon = 8 + 3\sqrt{7}$. Montrer que ε est inversible, calculer ε^2 ; en déduire que A a une infinité d'inversibles. $3 + \sqrt{7}$ est-il inversible dans A ?

17

Niveau 3 · Approfondissement**Exercice 17** Le groupe des symétries du carré ★★★

corrigé p. 48

Soient $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, et D l'ensemble des matrices d'ordre 2 à coefficients dans $\{-1, 0, 1\}$ ayant un seul coefficient non nul par ligne et par colonne.

1. Montrer que $D = \{I, R, R^2, R^3, S, RS, R^2S, R^3S\}$ (8 éléments); interpréter chaque $X \in D$ comme une isométrie conservant le carré de sommets $(\pm 1, \pm 1)$.
2. Vérifier que $SR^k = R^{-k}S$ pour $k \in \mathbb{Z}$; en déduire que $(D, \times)$ est un groupe non commutatif.
3. Déterminer les $X \in D$ tels que $X^2 = I$ et $X \neq I$. Montrer que $\{I, R, R^2, R^3\}$, $\{I, R^2, S, R^2S\}$ et $\{I, R^2, RS, R^3S\}$ sont des sous-groupes de D .

Exercice 18 Sous-groupes de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$ ★★★

corrigé p. 48

1. Soient $a, b \in \mathbb{N}^*$. Montrer que $a\mathbb{Z} + b\mathbb{Z} = \{au + bv, u, v \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$ égal à $(a \wedge b)\mathbb{Z}$ (on retrouve Bézout), et que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.
2. Soient $n \geq 2$, $\pi : k \mapsto \bar{k}$, de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$, et H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Montrer que $\pi^{-1}(H) = d\mathbb{Z}$ pour un diviseur $d \geq 1$ de n , que $H = \pi(d\mathbb{Z})$ et que $\pi(d\mathbb{Z})$ a $\frac{n}{d}$ éléments. Combien $\mathbb{Z}/n\mathbb{Z}$ a-t-il de sous-groupes? Donner ceux de $\mathbb{Z}/12\mathbb{Z}$.
3. Soit $k \in \mathbb{Z}$. Montrer que $\{m\bar{k}, m \in \mathbb{Z}\} = \pi((k \wedge n)\mathbb{Z})$; en déduire que tout élément de $\mathbb{Z}/n\mathbb{Z}$ est multiple de $\bar{k}$ si et seulement si $k \wedge n = 1$. Multiples de $\bar{8}$ dans $\mathbb{Z}/12\mathbb{Z}$?

Exercice 19 L'anneau $M_2(\mathbb{Z})$ et le groupe $SL_2(\mathbb{Z})$ ★★★

corrigé p. 49

$M_2(\mathbb{Z})$ désigne le sous-anneau de $M_2(\mathbb{R})$ formé des matrices à coefficients entiers.

1. Montrer que $\det(AB) = \det A \det B$, et que $A \in M_2(\mathbb{Z})$ a un inverse dans $M_2(\mathbb{Z})$ si et seulement si $\det A = \pm 1$. Inverser dans $M_2(\mathbb{Z})$, si possible : $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}$.
2. En déduire que $SL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) : \det A = 1\}$ est un groupe pour $\times$.
3. Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $U = ST$. Calculer S^2 , T^n ($n \in \mathbb{Z}$), U^3 . Plus petits $n \geq 1$ tels que $S^n = I$, $U^n = I$?
4. Déterminer les matrices de $SL_2(\mathbb{Z})$ qui commutent avec T . Le groupe $SL_2(\mathbb{Z})$ est-il commutatif?

Exercice 20 Équations du second degré dans $M_2(\mathbb{R})$ ★★★

corrigé p. 49

Pour $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on note $t = a + d$ et $\delta = ad - bc$; on rappelle (et l'on vérifiera) que $X^2 - tX + \delta I = 0$.

1. Montrer que X est diviseur de zéro ($X \neq 0$, $XY = 0$ avec $Y \neq 0$) si et seulement si $X \neq 0$ et $\delta = 0$.
2. Montrer que $X^2 = 0 \iff t = \delta = 0$, et décrire ces matrices.

- Montrer que les solutions de $X^2 = X$ sont 0, I et les matrices telles que $t = 1$ et $\delta = 0$.
- Résoudre $X^2 = I$. Comparer avec l'équation $x^2 = 1$ dans un corps.

Exercice 21 Anneaux de Boole ★★★

corrigé p. 49

Un anneau unitaire $(A, +, \times)$ est dit de Boole si $x^2 = x$ pour tout $x \in A$.

- Montrer que $x + x = 0$ (développer $(x + x)^2$), puis que A est commutatif (développer $(x + y)^2$).
- Montrer que $x(1 - x) = 0$; en déduire que si A est intègre, alors $A = \{0, 1\}$. Pour quels $n \geq 2$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il de Boole ?
- Soit E un ensemble ; on pose $X \oplus Y = (X \cup Y) \setminus (X \cap Y)$. À l'aide de $X \mapsto \chi_X$ ($\chi_X : E \rightarrow \mathbb{Z}/2\mathbb{Z}$ vaut $\bar{1}$ sur X , $\bar{0}$ ailleurs), montrer que $(P(E), \oplus, \cap)$ est un anneau de Boole (on admet que $F(E, \mathbb{Z}/2\mathbb{Z})$ est un anneau pour les lois point par point).

Exercice 22 Les éléments d'ordre 2 d'un groupe fini ★★★

corrigé p. 50

Soit $(G, *)$ un groupe fini de neutre e ; on note $x^2 = x * x$.

- On suppose $|G|$ pair. En groupant chaque élément avec son symétrique, montrer qu'il existe $x \neq e$ tel que $x^2 = e$.
- On suppose $x^2 = e$ pour tout x . Soient $H \neq G$ un sous-groupe, $a \notin H$, $aH = \{a * h, h \in H\}$. Montrer que $H \cup aH$ est un sous-groupe à $2|H|$ éléments ; en déduire que $|G|$ est une puissance de 2.
- Vérifier que $x^2 = \bar{1}$ pour les 8 inversibles x de $\mathbb{Z}/24\mathbb{Z}$. Existe-t-il un groupe à 6 éléments où $x^2 = e$ pour tout x ?

Exercice 23 Sous-corps de $\mathbb{R}$ ★★★

corrigé p. 50

Un sous-corps de $\mathbb{R}$ est un sous-anneau K de $\mathbb{R}$ tel que $\frac{1}{x} \in K$ si $x \in K^*$; exemple (cours) : $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$. On admet que $\sqrt{2}, \sqrt{3}, \sqrt{6} \notin \mathbb{Q}$.

- Montrer que tout sous-corps de $\mathbb{R}$ contient $\mathbb{Q}$, et que s'il contient $\sqrt{2}$, il contient $\mathbb{Q}(\sqrt{2})$.
- Montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, puis que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.
- Soit $L = \{u + v\sqrt{3}, u, v \in \mathbb{Q}(\sqrt{2})\} = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, a, b, c, d \in \mathbb{Q}\}$. Montrer que L est un sous-corps de $\mathbb{R}$ (vérifier que $u^2 - 3v^2 \neq 0$ si $(u, v) \neq (0, 0)$), et écrire $\frac{1}{1 + \sqrt{2} + \sqrt{3}}$ sous la forme $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$.

18

Niveau 4 • Concours**Exercice 24 Ordre d'un élément ★★★**

corrigé p. 50

Dans un groupe $(G, \cdot)$ de neutre e , l'ordre $\omega(a)$ de a est le plus petit $n \in \mathbb{N}^*$ tel que $a^n = e$.

- Soit a d'ordre n . Montrer que $a^m = e \iff n \mid m$ ($m \in \mathbb{Z}$), que $\{a^k, k \in \mathbb{Z}\} = \{e, a, \dots, a^{n-1}\}$ (éléments distincts) et que $\omega(a^k) = \frac{n}{n \wedge k}$ ($k \neq 0$).
- On suppose G commutatif, $\omega(a) = m$, $\omega(b) = n$ et $m \wedge n = 1$. Montrer que $\omega(ab) = mn$.
- Soient $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Montrer que $\omega(A) = \omega(B) = 2$, mais que AB n'est pas d'ordre fini.
- Dans $((\mathbb{Z}/31\mathbb{Z})^*, \times)$, calculer $\omega(\bar{2})$, $\omega(\bar{5})$, $\omega(\bar{-1})$, puis trouver un élément d'ordre 30. Conclure.

Exercice 25 Le théorème de Lagrange ★★★★★

corrigé p. 51

Soient $(G, \cdot)$ un groupe fini, H un sous-groupe et, pour $x \in G$, $xH = \{xh, h \in H\}$.

1. Montrer que $|xH| = |H|$, et que si $xH \cap yH \neq \emptyset$, alors $xH = yH$. En déduire que $|H|$ divise $|G|$.
2. Montrer que $\omega(a) \mid |G|$ et $a^{|G|} = e$ (exercice 24); en déduire le petit théorème de Fermat.
3. Si $|G| = p$ premier et $a \neq e$, montrer que $\bar{k} \mapsto a^k$ est un isomorphisme de $(\mathbb{Z}/p\mathbb{Z}, +)$ sur G .
4. Calculer 2^{-12} et 2^{-18} dans $\mathbb{Z}/37\mathbb{Z}$; en déduire, sans autre calcul, l'ordre de $\bar{2}$.

Exercice 26 Les ordres finis dans $SL_2(\mathbb{Z})$ ★★★★★

corrigé p. 51

Soit $A \in SL_2(\mathbb{Z})$, $A \neq \pm I$, de trace t : $A^2 = tA - I$ (exercice 20). Soit $u_0 = 0$, $u_1 = 1$, $u_{k+1} = tu_k - u_{k-1}$.

1. Montrer que $A^k = u_k A - u_{k-1} I$ pour $k \in \mathbb{N}^*$, puis que $A^n = I \iff (u_n = 0 \text{ et } u_{n-1} = -1)$.
2. Si $|t| \geq 3$, montrer que $|u_{k+1}| > |u_k|$ ($k \in \mathbb{N}$) : A n'est pas d'ordre fini; de même si $t = \pm 2$.
3. Étudier $t \in \{-1, 0, 1\}$; en déduire que les ordres finis dans $SL_2(\mathbb{Z})$ sont 1, 2, 3, 4, 6 (exemples ?).

Exercice 27 Les sous-groupes de $(\mathbb{R}, +)$ ★★★★★

corrigé p. 51

Soit $H \neq \{0\}$ un sous-groupe de $(\mathbb{R}, +)$. On pose $H^+ = H \cap]0, +\infty[$ (non vide : pourquoi ?) et $\alpha = \inf H^+$.

1. Si $\alpha > 0$, montrer que $\alpha \in H$ (sinon, trouver $h, h' \in H$ tels que $\alpha < h' < h < 2\alpha$), puis que $H = \alpha\mathbb{Z}$.
2. Si $\alpha = 0$, montrer que tout intervalle $]x, y[$ ($x < y$) rencontre H : H est dense dans $\mathbb{R}$.
3. Montrer que $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est dense, puis que tout $]x, y[\subset \mathbb{R}_+^*$ contient un $2^m 3^n$ ($m, n \in \mathbb{Z}$).

Exercice 28 Le centre de $M_2(\mathbb{R})$ ★★★★★

corrigé p. 52

Pour $A \in M_2(\mathbb{R})$, on note $C(A) = \{M \in M_2(\mathbb{R}) : AM = MA\}$ (commutant de A).

1. Montrer que $C(A)$ est un sous-anneau de $M_2(\mathbb{R})$ contenant les $xI + yA$ ($x, y \in \mathbb{R}$).
2. Montrer que les matrices commutant avec toutes les autres sont les λI (tester $E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$).
3. Si $A \neq \lambda I$, montrer que $C(A) = \{xI + yA, x, y \in \mathbb{R}\}$. $C(K)$ (exercice 11) ? $C(N)$ (exercice 14) ?

Exercice 29 Les éléments nilpotents d'un anneau ★★★★★

corrigé p. 52

Dans un anneau unitaire A , x est nilpotent s'il existe $k \in \mathbb{N}^*$ tel que $x^k = 0$.

1. Si $x^k = 0$, montrer que $1 - x$ et $1 + x$ sont inversibles, et, si y est nilpotent et $xy = yx$, que xy et $x + y$ sont nilpotents.
2. Dans $M_2(\mathbb{R})$, montrer que N nilpotente $\Rightarrow N^2 = 0$ (exercice 20), et que E_{12}, E_{21} (exercice 28) sont nilpotents, mais pas $E_{12} + E_{21}$.
3. Montrer que $\bar{x}$ est nilpotent dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si tout premier divisant n divise x . Nilpotents de $\mathbb{Z}/72\mathbb{Z}$? Inverse de $\bar{7}$ dans $\mathbb{Z}/72\mathbb{Z}$ (utiliser 1) ?

Exercice 30 Corps finis : quatre oui, six non ★★★★★

corrigé p. 52

Soit $(K, +, \times)$ un corps fini; on note $k \cdot x = x + \dots + x$ (k termes, $k \in \mathbb{N}^*$).

1. Montrer qu'il existe un plus petit $p \geq 2$ tel que $p \cdot 1 = 0$, qu'il est premier, et que $p \cdot x = 0$ ($x \in K$).
2. Si $p = 2$, montrer que $|K|$ est une puissance de 2 (exercice 22); sinon, que $x + x = 0 \Rightarrow x = 0$ et que $|K|$ est impair. Existe-t-il un corps à 6 éléments ? à 10 ?
3. Matrices à coefficients dans $\mathbb{Z}/2\mathbb{Z}$ (notés 0, 1) : soient $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ et $K_4 = \{O, I, A, I + A\}$. Calculer $A^2, A(I + A)$, dresser les tables de K_4 et montrer que c'est un corps commutatif. Montrer que $(K_4 \setminus \{O\}, \times) \simeq (\mathbb{Z}/3\mathbb{Z}, +)$, mais que $(K_4, +) \neq (\mathbb{Z}/4\mathbb{Z}, +)$.

Partie C • La banque

36 exercices supplémentaires classés par thème, du niveau Bases au niveau Concours

19 Lois de composition interne

Un contre-exemple numérique suffit pour réfuter la commutativité ou l'associativité ; pour les établir, il faut un calcul littéral. « Symétrique unique » et « symétrisable $\Rightarrow$ régulier » **supposent l'associativité**.

Exercice 31 Quatre lois, quatre profils ★

corrigé p. 53

On note $\mathbb{R}_+ = [0, +\infty[$ et l'on considère les quatre lois :

$$x * y = x + y + x^2 y^2 \text{ sur } \mathbb{R}, \quad x \oplus y = |x - y| \text{ sur } \mathbb{R}_+, \quad z \odot w = z \overline{w} \text{ sur } \mathbb{C}, \quad x \otimes y = \max(x, y) \text{ sur } \mathbb{R}_+.$$

1. Pour chacune, étudier la commutativité et l'associativité, et chercher un élément neutre (pour $\odot$: un neutre à droite, un neutre à gauche).
2. a) Montrer que $x \in \mathbb{R}$ est symétrisable pour $*$ si et seulement si $x \leq \frac{1}{\sqrt[3]{4}}$, et que -1 admet deux symétriques. b) En factorisant $(y + x^2 y^2) - (z + x^2 z^2)$, montrer que 0 est le seul élément régulier pour $*$.
3. Pour $\oplus$: montrer que tout élément est symétrisable, mais que 0 est le seul élément régulier. Pour $\otimes$: déterminer les éléments symétrisables et les éléments réguliers. Pour $\odot$: déterminer les éléments réguliers.
4. Quelles propriétés du cours les questions 2 et 3 semblent-elles contredire ? Résumer l'étude dans un tableau.

Exercice 32 Parties stables : oui ou non ? ★

corrigé p. 53

1. Soit $j = e^{2i\pi/3}$ et $E = \{m^2 + mn + n^2 ; (m, n) \in \mathbb{Z}^2\}$. a) Vérifier que $|m - nj|^2 = m^2 + mn + n^2$, puis montrer que E est stable pour la multiplication. b) Vérifier que 7 et 13 appartiennent à E , et en déduire deux écritures de 91 sous la forme $m^2 + mn + n^2$ avec $m, n \in \mathbb{N}$. c) E est-il stable pour l'addition ?
2. Dans l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, montrer que $F = \{f ; \forall x \in \mathbb{R}, f(x + 1) = f(x) + 1\}$ est stable pour $\circ$, mais pas pour $+$; vérifier que E et $x \mapsto x + \sin(2\pi x)$ sont dans F .

Exercice 33 Les lois $x * y = ax + by + c$ ★★

corrigé p. 54

Soit a, b, c trois réels. On munit $\mathbb{R}$ de la loi définie par $x * y = ax + by + c$.

1. Montrer que $*$ est commutative si et seulement si $a = b$.
2. a) Montrer que $(x * y) * z - x * (y * z) = (a^2 - a)x + (b - b^2)z + (a - b)c$ pour tous réels x, y, z . b) En déduire que $*$ est associative si et seulement si $a^2 = a$, $b^2 = b$ et $(a - b)c = 0$. c) Écrire toutes les lois associatives de cette forme (quatre familles).
3. Montrer que $*$ admet un élément neutre si et seulement si $a = b = 1$, et préciser ce neutre. En déduire les lois de cette forme qui font de $\mathbb{R}$ un groupe, et le symétrique de x .
4. Application. La loi $x * y = 3x + 3y - 2$ est-elle associative ? Calculer $(0 * 0) * 1$ et $0 * (0 * 1)$.

Exercice 34 PGCD et PPCM comme lois ★★

corrigé p. 54

Pour $a, b \in \mathbb{N}^*$, on note $a \wedge b$ leur PGCD et $a \vee b$ leur PPCM : ce sont deux lois internes sur $\mathbb{N}^*$. On rappelle que $d \mid a \wedge b \iff (d \mid a \text{ et } d \mid b)$ et que $a \vee b \mid m \iff (a \mid m \text{ et } b \mid m)$.

1. Montrer que $\wedge$ et $\vee$ sont commutatives et associatives, et que $a \wedge a = a \vee a = a$.
2. a) Montrer que $(\mathbb{N}^*, \vee)$ possède un élément neutre, mais pas $(\mathbb{N}^*, \wedge)$. b) Déterminer les éléments symétrisables de $(\mathbb{N}^*, \vee)$. c) Montrer que 1 est le seul élément régulier de $(\mathbb{N}^*, \vee)$, et que $(\mathbb{N}^*, \wedge)$ n'a aucun élément régulier.
3. a) Montrer que, pour tous réels x, y, z :

$$\min(x, \max(y, z)) = \max(\min(x, y), \min(x, z)), \quad \max(x, \min(y, z)) = \min(\max(x, y), \max(x, z)).$$

b) À l'aide des décompositions en facteurs premiers, en déduire que $\wedge$ est distributive par rapport à $\vee$, et $\vee$ par rapport à $\wedge$. Vérifier pour $a = 12$, $b = 18$, $c = 20$. c) $\wedge$ est-elle distributive par rapport à $+$?

Exercice 35 Les lois $x * y = axy + b(x + y) + c$ ★★★

corrigé p. 55

Soit $a \in \mathbb{R}^*$, $b, c \in \mathbb{R}$, et la loi commutative définie sur $\mathbb{R}$ par $x * y = axy + bx + by + c$.

1. Montrer que $(x * y) * z - x * (y * z) = (b^2 - b - ac)(x - z)$, et en déduire que $*$ est associative si et seulement si $b^2 - b = ac$.
2. On suppose $b^2 - b = ac$ et l'on pose $\varphi(x) = ax + b$. a) Montrer que φ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$ et que $\varphi(x * y) = \varphi(x)\varphi(y)$ pour tous réels x, y . b) En déduire que $*$ possède un neutre e et un élément absorbant ω ($x * \omega = \omega$ pour tout x), et que x est symétrisable si et seulement si $x \neq \omega$. Donner e, ω et le symétrique x' de x . c) On pose $x^{(1)} = x$ et $x^{(n+1)} = x^{(n)} * x$. Montrer que $x^{(n)} = \frac{(ax+b)^n - b}{a}$ pour tout $n \in \mathbb{N}^*$.
3. Application : $x * y = 2xy - 3x - 3y + 6$. a) Vérifier que $*$ est associative ; donner e, ω et x' . b) Résoudre $x * x * x = 15$. c) Montrer que $[1, 2]$ est stable pour $*$ et que $\left] \frac{3}{2}, +\infty \right[$, muni de $*$, est un groupe.

Exercice 36 Loi associative sur un ensemble fini ★★★

corrigé p. 56

Soit E un ensemble fini à $N \geq 1$ éléments, muni d'une loi associative $*$. Pour $x \in E$, on pose $x^1 = x$ et $x^{k+1} = x^k * x$; on admet que $x^m * x^n = x^{m+n}$ pour tous $m, n \in \mathbb{N}^*$.

1. Soit $x \in E$. Montrer qu'il existe deux entiers $p \geq 1$ et $q \geq 1$ tels que $x^{p+q} = x^p$.
2. Montrer que $x^{n+kq} = x^n$ pour tout entier $n \geq p$ et tout $k \in \mathbb{N}$. En déduire que $y = x^{pq}$ vérifie $y * y = y$: **tout ensemble fini muni d'une loi associative contient un élément idempotent.**
3. Exemple : $E = \mathbb{Z}/12\mathbb{Z}$ muni de $*$. Déterminer ses idempotents. Pour $x = \overline{2}$ et $x = \overline{3}$, calculer les puissances de x , les plus petits p, q convenables et x^{pq} .
4. On suppose de plus que E a un élément neutre e et que tous ses éléments sont réguliers. a) Montrer que e est le seul idempotent de E . b) En déduire que $(E, *)$ est un groupe.
5. Application : $E = \{\overline{1}, \overline{2}, \dots, \overline{10}\} \subset \mathbb{Z}/11\mathbb{Z}$, muni de la multiplication. Montrer, *sans calculer d'inverse*, que $(E, *)$ est un groupe. Calculer les puissances successives de $\overline{2}$ et en déduire l'inverse de $\overline{2}$.

20

Groupes et sous-groupes

Pour un groupe, on vérifie dans l'ordre : loi interne, associativité, neutre, symétriques. Pour une partie H d'un groupe connu, on préfère la caractérisation : $H \neq \emptyset$ et $x * y' \in H$ pour tous $x, y \in H$.

Exercice 37 Groupe ou pas ? ★

corrigé p. 56

L'ensemble muni de la loi indiquée est-il un groupe ? Si oui, préciser le neutre, les symétriques et la commutativité ; sinon, dire ce qui est en défaut.

1. L'ensemble I des entiers impairs, muni de $x \oplus y = x + y - 1$.
2. $]0, +\infty[$, muni de $x \otimes y = \frac{xy}{x+y}$ (on pourra calculer $\frac{1}{x \otimes y}$).
3. $\mathbb{Z}$, muni de $x * y = x + (-1)^x y$.
 - a) Justifier que $(-1)^{x+(-1)^x y} = (-1)^{x+y}$ pour tous $x, y \in \mathbb{Z}$, puis que $*$ est associative.
 - b) Montrer que $(\mathbb{Z}, *)$ est un groupe ; donner le symétrique de x selon la parité de x . Est-il commutatif ?
 - c) Résoudre dans $\mathbb{Z}$ les équations $3 * X = 10$ et $X * 3 = 10$.

Exercice 38 Tables de groupes à quatre éléments ★

corrigé p. 57

On rappelle (cours) que, dans la table d'un groupe fini, chaque élément apparaît exactement une fois dans chaque ligne et dans chaque colonne. Soit $G = \{e, a, b, c\}$ un groupe à quatre éléments distincts, de neutre e .

1. On suppose $a * a = b$. a) Montrer que $a * b = c$ et $a * c = e$. b) En écrivant $b = a^2$ et $c = a^3$, dresser la table complète de G . Ce groupe est-il commutatif ?
2. On suppose $a * a = b * b = c * c = e$. Montrer que $a * b = c$, puis dresser la table de G .
3. En déduire que tout groupe à quatre éléments a , après un éventuel changement de noms, l'une des deux tables précédentes (dites *cyclique* et *de Klein*).

4. a) Dans $\mathbb{Z}/10\mathbb{Z}$, on pose $P = \{\overline{2}, \overline{4}, \overline{6}, \overline{8}\}$. Dresser la table de multiplication de P et montrer que $(P, \times)$ est un groupe. Quel est son neutre ? Quel est le symétrique de $\overline{2}$? Quel est son type ?
 b) Dans $\mathbb{Z}/20\mathbb{Z}$, on pose $K = \{\overline{1}, \overline{9}, \overline{11}, \overline{19}\}$. Dresser la table de multiplication de K , montrer que $(K, \times)$ est un groupe et préciser son type.

Exercice 39 Sous-groupes de $(\mathbb{C}^*, \times)$ ★★

corrigé p. 57

1. Lesquelles des parties suivantes sont des sous-groupes de $(\mathbb{C}^*, \times)$? Décrire géométriquement A et B .

$$A = \{z \in \mathbb{C}^* ; z^4 \in \mathbb{R}_+^*\}, \quad B = \{z \in \mathbb{C}^* ; z^4 \in \mathbb{R}\}, \quad C = \{z \in \mathbb{C}^* ; |z| \in \mathbb{Q}\}, \\ D = \{a + ib ; (a, b) \in \mathbb{Q}^2 \setminus \{(0, 0)\}\}, \quad F = \{z \in \mathbb{U} ; \operatorname{Im} z \geq 0\}.$$

2. Soit H et K deux sous-groupes d'un groupe $(G, *)$. a) Montrer que $H \cap K$ est un sous-groupe de G . b) Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$. c) Vérifier directement que $\mathbb{U}_4 \cup \mathbb{U}_6$ n'est pas un sous-groupe de $\mathbb{C}^*$.
 3. Soit $\mathbb{U}_\infty = \{z \in \mathbb{C} ; \exists n \in \mathbb{N}^*, z^n = 1\}$, réunion de tous les $\mathbb{U}_n$. Montrer que $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{U}, \times)$, distinct de $\mathbb{U}$ (on admet que π est irrationnel). Pourquoi cela ne contredit-il pas 2.b) ?

Exercice 40 Les isométries de la droite ★★

corrigé p. 58

Pour $a \in \mathbb{R}$, on définit sur $\mathbb{R}$ les applications $t_a(x) = x + a$ (translation) et $\sigma_a(x) = a - x$ (symétrie de centre $\frac{a}{2}$), et l'on pose $G = \{t_a ; a \in \mathbb{R}\} \cup \{\sigma_a ; a \in \mathbb{R}\}$.

1. a) Montrer que, pour tous réels a, b : $t_a \circ t_b = t_{a+b}$, $t_a \circ \sigma_b = \sigma_{a+b}$, $\sigma_a \circ t_b = \sigma_{a-b}$, $\sigma_a \circ \sigma_b = t_{a-b}$.
 b) Montrer que $t_a = t_b$ ou $\sigma_a = \sigma_b$ entraîne $a = b$, et qu'une translation n'est jamais égale à une symétrie.
 2. a) En déduire que $(G, \circ)$ est un groupe (sous-groupe du groupe des bijections de $\mathbb{R}$) ; préciser les réciproques de t_a et de σ_a . Est-il commutatif ? b) Déterminer les $f \in G$ tels que $f \circ f = \operatorname{id}$.
 3. Montrer que l'ensemble T des translations t_a est un sous-groupe de G isomorphe à $(\mathbb{R}, +)$, et que $H = \{t_{2k}, \sigma_{2k+1} ; k \in \mathbb{Z}\}$ est un sous-groupe de G . L'ensemble $\{\sigma_a ; a \in \mathbb{R}\} \cup \{\operatorname{id}\}$ est-il un sous-groupe de G ?
 4. Retour à l'exercice 37. Pour $x \in \mathbb{Z}$, on pose $\Phi(x) = t_x$ si x est pair et $\Phi(x) = \sigma_x$ si x est impair, de sorte que $\Phi(x)(y) = x + (-1)^x y$ pour tout réel y . a) Montrer que Φ est une bijection de $\mathbb{Z}$ sur H et que $\Phi(x * y) = \Phi(x) \circ \Phi(y)$, où $*$ est la loi de l'exercice 37 (question 4). b) En déduire, sans nouveau calcul, que $(\mathbb{Z}, *)$ est un groupe non commutatif, isomorphe à $(H, \circ)$.

Exercice 41 Le groupe des similitudes ★★★

corrigé p. 59

Pour $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, on note $s_{a,b}$ l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par $s_{a,b}(z) = az + b$, et $S = \{s_{a,b} ; a \in \mathbb{C}^*, b \in \mathbb{C}\}$.

1. a) Montrer que $s_{a,b} \circ s_{c,d} = s_{ac, ad+b}$, puis que $s_{a,b}$ est une bijection de $\mathbb{C}$; préciser sa réciproque.
 b) En déduire que $(S, \circ)$ est un groupe. Est-il commutatif ? c) Montrer que $s_{a,b} = s_{c,d}$ entraîne $a = c$ et $b = d$.
 2. Montrer que $T = \{s_{1,b} ; b \in \mathbb{C}\}$ (translations), $H = \{s_{a,0} ; a \in \mathbb{C}^*\}$ et $I = \{s_{a,b} ; |a| = 1\}$ sont des sous-groupes de S . L'ensemble $\{s_{a,b} ; |a| = 1, a \neq 1\} \cup \{\operatorname{id}\}$, formé des rotations et de l'identité, en est-il un ?

3. Pour $f \in S$, on pose $C(f) = \{g \in S ; g \circ f = f \circ g\}$ (commutant de f). a) Montrer que $C(f)$ est un sous-groupe de S . b) Déterminer $C(t)$ pour $t = s_{1,1}$, puis $C(r)$ pour $r = s_{i,0}$. c) En déduire que l'identité est le seul élément de S qui commute avec tous les autres.

Exercice 42 Le groupe des périodes d'une fonction ★★★

corrigé p. 59

Pour une fonction $f : \mathbb{R} \rightarrow \mathbb{R}$, on note $P_f = \{T \in \mathbb{R} ; \forall x \in \mathbb{R}, f(x+T) = f(x)\}$ l'ensemble de ses périodes (0 compris).

1. Montrer que P_f est un sous-groupe de $(\mathbb{R}, +)$.
2. Déterminer P_f dans chacun des cas : a) $f = \cos$; b) $f = \cos^2$; c) $f(x) = x - E(x)$; d) $f = \mathbf{1}_{\mathbb{Q}}$ ($f(x) = 1$ si $x \in \mathbb{Q}$, $f(x) = 0$ sinon).
3. Soit $\varphi(x) = \cos \frac{\pi x}{2} + \cos \frac{\pi x}{5}$. a) Montrer que, si $T \in P_\varphi$, alors $\cos \frac{\pi T}{2} = \cos \frac{\pi T}{5} = 1$. b) En déduire que $P_\varphi = 4\mathbb{Z} \cap 10\mathbb{Z}$, puis déterminer P_φ .
4. Soit $\psi(x) = \cos x + \cos(\sqrt{2}x)$. Montrer que $P_\psi = \{0\}$: **une somme de deux fonctions périodiques n'est pas toujours périodique.**

21

Morphismes et isomorphismes

Un morphisme envoie le neutre sur le neutre, un symétrique sur le symétrique, un sous-groupe sur un sous-groupe. Pour montrer qu'une loi « exotique » fait de E un groupe, on cherche une bijection qui la transforme en une loi connue : c'est le **transport de structure**.

Exercice 43 Noyaux et images ★

corrigé p. 60

Pour un morphisme f de $(G, *)$ dans $(G', \otimes)$, de neutres e et e' , on note $N_f = \{x \in G ; f(x) = e'\}$ son *noyau* ; on rappelle (cours) que N_f est un sous-groupe de G , et que f est injectif si et seulement si $N_f = \{e\}$. Pour x, y réels, on pose $e^{x+iy} = e^x e^{iy}$.

1. Les applications suivantes sont-elles des morphismes de groupes ? Pour chaque morphisme, déterminer le noyau et l'image, et dire s'il est injectif, surjectif, bijectif.
 - a) $f_1 : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \times), t \mapsto e^{(1+i)t}$;
 - b) $f_2 : (\mathbb{C}, +) \rightarrow (\mathbb{C}^*, \times), z \mapsto e^z$;
 - c) $f_3 : (\mathbb{Z}, +) \rightarrow (\mathbb{R}^*, \times), k \mapsto (-1)^k$;
 - d) $f_4 : (\mathbb{C}^*, \times) \rightarrow (\mathbb{C}^*, \times), z \mapsto \bar{z}/z$.
2. En déduire que $\Sigma = \{e^{(1+i)t} ; t \in \mathbb{R}\}$, $2i\pi\mathbb{Z}$, $\mathbb{R}^*$ et $2\mathbb{Z}$ sont des sous-groupes de groupes que l'on précisera. Représenter Σ dans le plan complexe.

Exercice 44 Transport par la tangente ★

corrigé p. 60

Soit $I =]-\frac{\pi}{2}, \frac{\pi}{2}[$. Pour $x, y \in I$, on pose $x * y = \arctan(\tan x + \tan y)$.

1. Justifier que $*$ est une loi de composition interne sur I , et que $\tan$ est une bijection de I sur $\mathbb{R}$ telle que $\tan(x * y) = \tan x + \tan y$ pour tous $x, y \in I$.
2. En déduire que $(I, *)$ est un groupe commutatif ; préciser son neutre et le symétrique de x .
3. Calculer $\frac{\pi}{4} * \frac{\pi}{4}$. On note $x^{(n)} = x * x * \dots * x$ (n facteurs) : montrer que $x^{(n)} = \arctan(n \tan x)$.
4. Résoudre dans I l'équation $x * x * x = \frac{\pi}{4}$.
5. Montrer que $H = \{\arctan k ; k \in \mathbb{Z}\}$ est un sous-groupe de $(I, *)$, et que $J = \left[0, \frac{\pi}{2}\right[$ est stable pour

* sans être un sous-groupe.

Exercice 45 Une loi sur $]0, 1[$ ★★

corrigé p. 61

Soit $I =]0, 1[$. Pour $x, y \in I$, on pose $x * y = \frac{xy}{xy + (1-x)(1-y)}$, et l'on considère $f(x) = \frac{x}{1-x}$.

1. Montrer que $*$ est une loi de composition interne sur I , que f est une bijection de I sur $]0, +\infty[$ (préciser f^{-1}) et que $f(x * y) = f(x)f(y)$ pour tous $x, y \in I$.
2. En déduire que $(I, *)$ est un groupe commutatif. Déterminer son neutre et montrer que le symétrique de x est $1 - x$.
3. On note $x^{(n)} = x * \dots * x$ (n facteurs). Montrer que $x^{(n)} = \frac{x^n}{x^n + (1-x)^n}$, puis étudier $\lim_{n \rightarrow +\infty} x^{(n)}$ selon les valeurs de x . Résoudre l'équation $x * x * x = \frac{8}{9}$.
4. Montrer que $\mathbb{Q} \cap I$ est un sous-groupe de $(I, *)$.

Exercice 46 Morphismes définis sur $\mathbb{Z}$ et sur $\mathbb{Z}/n\mathbb{Z}$ ★★

corrigé p. 61

1. Soit $(G, *)$ un groupe de neutre e , et $a \in G$. Montrer que $\varphi_a : k \mapsto a^k$ est un morphisme de $(\mathbb{Z}, +)$ dans $(G, *)$, et que c'est le seul morphisme φ tel que $\varphi(1) = a$.
2. En déduire tous les morphismes de $(\mathbb{Z}, +)$ dans lui-même, puis tous les isomorphismes de $(\mathbb{Z}, +)$ sur lui-même.
3. Soit $n \geq 2$ et $\omega \in \mathbb{C}^*$. a) Montrer que la formule $\psi_\omega(\overline{k}) = \omega^k$ définit une application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$ (indépendante du représentant k choisi) si et seulement si $\omega^n = 1$. b) Montrer que ψ_ω est alors un morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$. c) Montrer que tout morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$ est de cette forme. Combien y en a-t-il ?
4. Soit $\omega = e^{2ik\pi/n}$ avec $0 \leq k \leq n-1$. a) Montrer que ψ_ω est injectif si et seulement si $k \wedge n = 1$. b) En déduire que ψ_ω est alors un isomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ sur $(\mathbb{U}_n, \times)$. c) Combien existe-t-il d'isomorphismes de $(\mathbb{Z}/12\mathbb{Z}, +)$ sur $(\mathbb{U}_{12}, \times)$? Les décrire.

Exercice 47 La loi du sinus hyperbolique ★★★

corrigé p. 62

On munit $\mathbb{R}$ de la loi $x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$, et l'on pose, pour $t \in \mathbb{R}$: $\text{sh } t = \frac{e^t - e^{-t}}{2}$ et $\text{ch } t = \frac{e^t + e^{-t}}{2}$.

1. Montrer que $\sqrt{1 + \text{sh}^2 t} = \text{ch } t$ et que $\text{sh}(s+t) = \text{sh } s \text{ch } t + \text{ch } s \text{sh } t$ pour tous réels s, t .
2. a) Montrer que sh est une bijection de $\mathbb{R}$ sur $\mathbb{R}$, de réciproque $\varphi : x \mapsto \ln(x + \sqrt{1+x^2})$. b) Montrer que $\text{sh}(s+t) = (\text{sh } s) * (\text{sh } t)$, puis que $\varphi(x * y) = \varphi(x) + \varphi(y)$.
3. En déduire que $(\mathbb{R}, *)$ est un groupe commutatif isomorphe à $(\mathbb{R}, +)$; préciser son neutre et le symétrique de x .
4. a) Calculer $1 * 1$ et vérifier que $\varphi\left(\frac{3}{4}\right) = \ln 2$. b) On note $x^{(n)} = x * \dots * x$ (n facteurs). Montrer que $x^{(n)} = \text{sh}(n \varphi(x))$ et calculer $\left(\frac{3}{4}\right)^{(n)}$. c) Résoudre l'équation $x * x = \frac{4}{3}$.
5. Montrer que $x \mapsto x + \sqrt{1+x^2}$ est un isomorphisme de $(\mathbb{R}, *)$ sur $(\mathbb{R}_+^*, \times)$.

Exercice 48 Isomorphes ou non ? ★★★

corrigé p. 62

Soit f un isomorphisme d'un groupe $(G, *)$ sur un groupe $(G', \otimes)$, de neutres e et e' . Pour $n \in \mathbb{N}^*$ et $x \in G$, on note $x^{(n)} = x * \dots * x$ (n facteurs), et de même dans G' (dans un groupe noté additivement, $x^{(n)} = nx$).

- Montrer que : a) G est commutatif si et seulement si G' l'est ; b) f réalise une bijection de $A_n = \{x \in G ; x^{(n)} = e\}$ sur $A'_n = \{y \in G' ; y^{(n)} = e'\}$; c) si tout élément de G est un « carré » (pour tout $y \in G$, il existe $x \in G$ tel que $y = x * x$), il en est de même dans G' .
- En déduire que les groupes suivants ne sont pas isomorphes :
 - $(\mathbb{U}, \times)$ et $(\mathbb{R}, +)$;
 - $(\mathbb{C}^*, \times)$ et $(\mathbb{R}^*, \times)$;
 - $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$;
 - $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$, alors que $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes ;
 - $(\mathbb{Z}, +)$ et le groupe $(\mathbb{Z}, *)$ de l'exercice 37, où $x * y = x + (-1)^x y$.
- On note G_{20} l'ensemble des éléments inversibles de $(\mathbb{Z}/20\mathbb{Z}, \times)$. a) Montrer que $(G_{20}, \times)$ est un groupe commutatif à 8 éléments, et résoudre dans G_{20} l'équation $x^2 = \overline{1}$ (exercice 38). b) Montrer que $(\mathbb{Z}/8\mathbb{Z}, +)$ et $(\mathbb{U}_8, \times)$ sont isomorphes, mais qu'aucun des deux n'est isomorphe à $(G_{20}, \times)$.

22 Anneaux et corps

Anneaux de nombres, de fonctions ou de classes : axiomes, inversibles, diviseurs de zéro, sous-corps.

Exercice 49 Les entiers de Gauss ★

corrigé p. 63

On note $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ et, pour $z \in \mathbb{C}$, $N(z) = |z|^2$.

- Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$, commutatif, unitaire et intègre.
- Vérifier que $N(a + ib) = a^2 + b^2 \in \mathbb{N}$ et que $N(z z') = N(z) N(z')$ pour tous $z, z' \in \mathbb{Z}[i]$.
- Montrer que $z \in \mathbb{Z}[i]$ est inversible dans $\mathbb{Z}[i]$ si et seulement si $N(z) = 1$. En déduire les éléments inversibles de $\mathbb{Z}[i]$. L'anneau $\mathbb{Z}[i]$ est-il un corps ?

Exercice 50 Changer la multiplication de $2\mathbb{Z}$ ★

corrigé p. 63

On sait (cours) que $(2\mathbb{Z}, +, \times)$ est un anneau commutatif *non unitaire*. Pour $a, b \in 2\mathbb{Z}$, on pose $a \odot b = \frac{ab}{2}$.

- Montrer que $\odot$ est une loi interne sur $2\mathbb{Z}$, commutative, associative, distributive par rapport à $+$, avec un élément neutre à préciser : $(2\mathbb{Z}, +, \odot)$ est un anneau commutatif unitaire.
- Montrer que $f : a \mapsto \frac{a}{2}$ est une bijection de $2\mathbb{Z}$ sur $\mathbb{Z}$ telle que $f(a + b) = f(a) + f(b)$ et $f(a \odot b) = f(a)f(b)$. En déduire que l'anneau $(2\mathbb{Z}, +, \odot)$ est intègre et déterminer ses éléments inversibles. Est-ce un corps ?
- Résoudre dans $2\mathbb{Z}$: a) $6 \odot x = 12$; b) $4 \odot x = 10$; c) $x \odot x = 18$; d) $x \odot x \odot x = -16$.
- Montrer qu'aucune bijection $h : 2\mathbb{Z} \rightarrow \mathbb{Z}$ ne vérifie $h(a + b) = h(a) + h(b)$ et $h(ab) = h(a)h(b)$ pour tous a, b : les anneaux $(2\mathbb{Z}, +, \times)$ et $(\mathbb{Z}, +, \times)$ ne sont pas isomorphes (les groupes $(2\mathbb{Z}, +)$ et $(\mathbb{Z}, +)$, eux, le sont).

Exercice 51 L'anneau des nombres décimaux ★★

corrigé p. 64

On note $\mathbb{D} = \left\{ \frac{a}{10^n}, a \in \mathbb{Z}, n \in \mathbb{N} \right\}$ l'ensemble des nombres décimaux.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$. Est-il intègre ?
2. Soit $x = \frac{p}{q}$ un rationnel écrit sous forme irréductible ($p \in \mathbb{Z}, q \in \mathbb{N}^*$). Montrer que $x \in \mathbb{D}$ si et seulement si q est de la forme $2^\alpha 5^\beta$ ($\alpha, \beta \in \mathbb{N}$). Les rationnels $\frac{7}{40}$, $\frac{3}{12}$ et $\frac{5}{12}$ sont-ils décimaux ?
3. Montrer que les éléments inversibles de l'anneau $\mathbb{D}$ sont les nombres $\pm 2^\alpha 5^\beta$, avec $\alpha, \beta \in \mathbb{Z}$. Donner l'inverse dans $\mathbb{D}$ de 0,8 et de 0,016. $\mathbb{D}$ est-il un corps ?

Exercice 52 L'anneau des fonctions continues ★★

corrigé p. 64

On note C l'anneau (commutatif, unitaire) des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$; son zéro est la fonction nulle θ , son unité la constante 1.

1. *Inversibles.* Montrer que $f \in C$ est inversible dans C si et seulement si f ne s'annule pas, et qu'une telle fonction garde un signe constant.
2. *Diviseurs de zéro.* a) On pose $f(x) = \max(0, 1 - |x|)$ et $g(x) = \max(0, 1 - |x - 2|)$. Tracer l'allure de f et g , puis vérifier que $fg = \theta$. b) Soit $f \in C, f \neq \theta$, nulle sur un intervalle $]a, b[$ ($a < b$). Construire $g \in C, g \neq \theta$, telle que $fg = \theta$. c) Réciproquement, soit $f, g \in C$ telles que $fg = \theta$ et $g \neq \theta$. Montrer que f est nulle sur un intervalle ouvert non vide. Les fonctions $x \mapsto x^2 - 1$ et $\sin$ sont-elles des diviseurs de zéro ?

Exercice 53 Les entiers de Gauss modulo p ★★★

corrigé p. 64

Soit p premier. On admet que l'ensemble K_p des $a + bi$ ($a, b \in \mathbb{Z}/p\mathbb{Z}$), muni des lois de $\mathbb{C}$ calculées modulo p (par exemple $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$), est un anneau commutatif unitaire à p^2 éléments. On pose $\bar{z} = a - bi$ et $N(z) = a^2 + b^2$.

1. Vérifier que $z\bar{z} = N(z)$ et que $N(zz') = N(z)N(z')$.
2. Montrer que K_p est un corps si et seulement si l'équation $x^2 = -1$ n'a pas de solution dans $\mathbb{Z}/p\mathbb{Z}$.
3. Cas $p = 3$. Montrer que K_3 est un corps à 9 éléments et calculer l'inverse de $1 + i$. Calculer $(1 + i)^2$, $(1 + i)^4$ et $(1 + i)^8$; montrer que les huit éléments non nuls de K_3 sont les $(1 + i)^k, 0 \leq k \leq 7$.
4. Cas $p = 5$. Calculer $(2 + i)(2 - i)$. Déterminer les $z \in K_5$ tels que $N(z) = 0$, puis le nombre d'inversibles de K_5 .

Exercice 54 Le corps $\mathbb{Q}(\sqrt[3]{2})$ ★★★

corrigé p. 65

On pose $\alpha = \sqrt[3]{2}$ et $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2, (a, b, c) \in \mathbb{Q}^3\}$.

1. Soit $(a, b, c) \in \mathbb{Z}^3$ tel que $a^3 + 2b^3 + 4c^3 = 6abc$. Montrer que a est pair et que $(b, c, \frac{a}{2})$ vérifie la même relation. En déduire que $a = b = c = 0$ (prendre une solution non nulle avec $|a| + |b| + |c|$ minimal).
2. Vérifier que, pour tous rationnels a, b, c :

$$(a + b\alpha + c\alpha^2)[(a^2 - 2bc) + (2c^2 - ab)\alpha + (b^2 - ac)\alpha^2] = a^3 + 2b^3 + 4c^3 - 6abc.$$

3. En déduire que, si $a + b\alpha + c\alpha^2 = 0$ avec $a, b, c \in \mathbb{Q}$, alors $a = b = c = 0$, puis que $\mathbb{Q}(\alpha)$ est un sous-corps de $(\mathbb{R}, +, \times)$.

4. Écrire sous la forme $a + b\alpha + c\alpha^2$ les inverses de α , de $1 + \alpha$ et de $\alpha - 1$.

23 Matrices et structures

Calculs, inverses, puissances, structures de matrices. I : matrice unité ; O : matrice nulle.

Exercice 55 Échauffement matriciel ★

corrigé p. 66

On pose $A = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

1. Calculer $2A - 3B$, AB et BA . Que constate-t-on ?
2. Calculer B^2 . En déduire B^n pour $n \in \mathbb{N}$, puis que B est inversible et donner B^{-1} .
3. Montrer que, pour tout réel x , la matrice $A - xI$ est inversible. En déduire A^{-1} .
4. Calculer D^2 , puis D^n pour $n \in \mathbb{N}$. Calculer $(I - D)(I + D)$: qu'en déduit-on pour l'anneau $(M_3(\mathbb{R}), +, \times)$?

Exercice 56 Inverser une matrice ★

corrigé p. 66

1. Montrer que $A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ est inversible et calculer A^{-1} . En déduire la solution du système $5x + 3y = 4$, $3x + 2y = 1$.
2. Soit $P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix}$. En résolvant le système $x + y + z = a$, $x + 2y + 3z = b$, $x + 3y + 6z = c$, d'inconnues x, y, z , montrer que P est inversible et calculer P^{-1} .
3. Soit $Q = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix}$. Calculer $Q^2 - 4Q$. En déduire que Q est inversible et donner Q^{-1} .

Exercice 57 L'anneau des matrices triangulaires ★★

corrigé p. 67

Pour $(a, b, c) \in \mathbb{R}^3$, on pose $M(a, b, c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ et $T = \{M(a, b, c), (a, b, c) \in \mathbb{R}^3\}$. On munit $\mathbb{R}^2$ des lois composante par composante, $(u, v) \cdot (u', v') = (uu', vv')$: c'est un anneau commutatif unitaire.

1. Montrer que $M(a, b, c)M(a', b', c') = M(aa', ab' + bc', cc')$, puis que T est un sous-anneau de $M_2(\mathbb{R})$. Est-il commutatif ? intègre ? (Calculer les produits de $M(1, 0, 0)$ et $M(0, 1, 0)$.)
2. Montrer que $M(a, b, c)$ est inversible si et seulement si $ac \neq 0$, et que son inverse appartient alors à T . En déduire que $T^* = \{M(a, b, c) : ac \neq 0\}$ est un sous-groupe de $(GL_2(\mathbb{R}), \times)$.
3. Soit $\varphi : T \rightarrow \mathbb{R}^2$, $M(a, b, c) \mapsto (a, c)$. a) Montrer que φ est surjective et compatible avec les additions et les multiplications. Est-elle injective ? b) Montrer que $U = \{M \in T : \varphi(M) = (1, 1)\}$ est un sous-groupe de T^* isomorphe à $(\mathbb{R}, +)$.
4. Soit $A = M(a, b, c)$ avec $a \neq c$. Montrer que $A^n = M\left(a^n, b \frac{a^n - c^n}{a - c}, c^n\right)$ pour tout $n \in \mathbb{N}$. Écrire $M(3, 2, 1)^n$, et vérifier que la formule obtenue reste vraie pour $n = -1$.

Exercice 58 Le groupe de Heisenberg (type examen) ★★

corrigé p. 67

Pour $(a, b, c) \in \mathbb{R}^3$, on pose $T(a, b, c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ et $H = \{T(a, b, c), (a, b, c) \in \mathbb{R}^3\}$.

1. Montrer que $T(a, b, c)T(a', b', c') = T(a + a', b + b', c + c' + ab')$, puis que $(H, \times)$ est un groupe, avec $T(a, b, c)^{-1} = T(-a, -b, ab - c)$. Est-il commutatif ?
2. Pour $X = T(a, b, c)$ et $Y = T(a', b', c')$, calculer $XYX^{-1}Y^{-1}$. À quelle condition X et Y commutent-elles ?

- Déterminer l'ensemble Z des éléments de H qui commutent avec tous les éléments de H . Montrer que $c \mapsto T(0, 0, c)$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(Z, \times)$.
- Sur $\mathbb{R}^3$, on pose $(a, b, c) * (a', b', c') = (a + a', b + b', c + c' + ab')$. Montrer, sans nouveau calcul, que $(\mathbb{R}^3, *)$ est un groupe non commutatif ; préciser son neutre et le symétrique de $(1, 2, 3)$.

Exercice 59 Un corps sans la matrice unité (type examen) ★★*corrigé p. 68*

On pose $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ et $Q = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$. Pour $(a, b) \in \mathbb{R}^2$, on pose $M(a, b) = aP + bQ$, et l'on note $E = \{M(a, b), (a, b) \in \mathbb{R}^2\}$.

- Calculer P^2 , PQ , QP et Q^2 . En déduire que $M(a, b)M(c, d) = M(ac - bd, ad + bc)$, puis que E est stable par $+$ et par $\times$.
- Soit $\varphi : \mathbb{C} \rightarrow E, a + ib \mapsto M(a, b)$. Montrer que φ est bijective, que $\varphi(z + z') = \varphi(z) + \varphi(z')$ et que $\varphi(zz') = \varphi(z)\varphi(z')$. En déduire que $(E, +, \times)$ est un corps commutatif isomorphe à $(\mathbb{C}, +, \times)$; préciser son zéro et son unité.
- a) Soit K la matrice d'ordre 3 dont le seul coefficient non nul est celui de la ligne 3 et de la colonne 3, égal à 1. Calculer $M(a, b)K$; en déduire qu'aucun élément de E n'est inversible dans $M_3(\mathbb{R})$. b) Montrer pourtant que $M(1, 1)$ est inversible dans le corps E et calculer son inverse. Expliquer ce paradoxe apparent.
- Résoudre dans E : a) $X^2 = M(0, 2)$; b) $X^3 = P$; montrer que l'ensemble des solutions de b) est un groupe pour $\times$, isomorphe à $(\mathbb{U}_3, \times)$. c) Calculer $M(\sqrt{3}, 1)^6$.

Exercice 60 Les nombres hyperboliques ★★★*corrigé p. 68*

Pour $(a, b) \in \mathbb{R}^2$, on pose $S(a, b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ et $S = \{S(a, b), (a, b) \in \mathbb{R}^2\}$. On munit $\mathbb{R}^2$ des lois de l'exercice 57.

- Montrer que $S(a, b)S(a', b') = S(aa' + bb', ab' + ba')$. En déduire que $(S, +, \times)$ est un anneau commutatif unitaire.
- Calculer $S(1, 1)S(1, -1)$. L'anneau S est-il intègre ? Montrer que $S(a, b)$ est inversible si et seulement si $a^2 \neq b^2$.
- Montrer que $\psi : S(a, b) \mapsto (a + b, a - b)$ est une bijection de S sur $\mathbb{R}^2$, compatible avec les additions et les multiplications (isomorphisme d'anneaux).
- Soit $G = \{S(a, b) : a^2 - b^2 = 1, a > 0\}$. Pour $t \in \mathbb{R}$, on pose $c(t) = \frac{e^t + e^{-t}}{2}$, $s(t) = \frac{e^t - e^{-t}}{2}$ et $H(t) = S(c(t), s(t))$. a) Vérifier que $H(t) \in G$, puis que $H(t)H(t') = H(t + t')$ (on pourra utiliser ψ). b) Montrer que $t \mapsto H(t)$ est une bijection de $\mathbb{R}$ sur G (poser $t = \ln(a + b)$). En déduire que $(G, \times)$ est un groupe isomorphe à $(\mathbb{R}, +)$.

24**Défis de concours**

Six problèmes de concours, à traiter dans l'ordre ; les exercices 63 et 64 s'enchaînent.

Exercice 61 Quand un groupe est-il commutatif ? ★★★★★

corrigé p. 69

$(G, \cdot)$ est un groupe de neutre e ; on note xy le composé de x et y , et x^{-1} le symétrique de x . On a vu dans le cours que, si $(xy)^2 = x^2y^2$ pour tous $x, y \in G$, alors G est commutatif.

1. Soit $k \in \mathbb{N}^*$. On suppose que $(xy)^n = x^n y^n$ pour tous $x, y \in G$ et pour $n \in \{k, k+1, k+2\}$. a) Montrer que $xy^k = y^k x$ et $xy^{k+1} = y^{k+1} x$ pour tous $x, y \in G$. b) En déduire que G est commutatif.
2. On suppose que $f : x \mapsto x^3$ est un automorphisme de G (morphisme bijectif de G sur G). a) Montrer que $(yx)^2 = x^2 y^2$ pour tous $x, y \in G$. b) En écrivant $(yx)^3$ de deux façons, montrer que $y^3 x^2 = x^2 y^3$, puis que tout élément de G commute avec tout carré. c) Conclure que G est commutatif.
3. Contre-exemple. On admet que $E = (\mathbb{Z}/3\mathbb{Z})^3$, muni de la loi $(a, b, c) * (a', b', c') = (a + a', b + b', c + c' + ab')$ (celle de l'exercice 58, modulo 3), est un groupe de neutre $e = (0, 0, 0)$. a) Montrer que E (qui a 27 éléments) n'est pas commutatif, que $x^n = \left(na, nb, nc + \frac{n(n-1)}{2} ab \right)$ pour $x = (a, b, c)$ et $n \in \mathbb{N}^*$, et que $x^3 = e$. b) En déduire que $(x * y)^n = x^n * y^n$ pour tous $x, y \in E$ dès que $n \equiv 0$ ou $1 \pmod{3}$. Que montre cet exemple à propos des questions 1 et 2 ?

Exercice 62 Les inversibles de $\mathbb{Z}/2^k\mathbb{Z}$ ★★★★★

corrigé p. 69

Soit $k \geq 3$. On note G_k le groupe des éléments inversibles de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$; on rappelle que $\bar{x} \in G_k \iff x$ est impair : G_k a 2^{k-1} éléments.

1. Montrer par récurrence que, pour tout $j \in \mathbb{N}$, $5^{2^j} = 1 + 2^{j+2} m_j$, avec m_j entier impair.
2. Soit $d \in \mathbb{N}^*$, écrit $d = 2^s r$ avec $s \in \mathbb{N}$ et r impair, et $u = 5^{2^s}$. a) Montrer que $5^d - 1 = (u - 1)(1 + u + \dots + u^{r-1})$, où le second facteur est impair. b) En déduire que $5^d \equiv 1 \pmod{2^k} \iff 2^{k-2} \mid d$.
3. Montrer que les classes $\bar{5}^j$, $0 \leq j \leq 2^{k-2} - 1$, sont deux à deux distinctes et que $5^j \equiv 1 \pmod{4}$. En déduire que $G_k = \{\pm \bar{5}^j, 0 \leq j \leq 2^{k-2} - 1\}$.
4. Montrer que l'équation $x^2 = \bar{1}$ a exactement quatre solutions dans $\mathbb{Z}/2^k\mathbb{Z}$: $\pm \bar{1}$ et $\pm \overline{1 + 2^{k-1}}$.

Exercice 63 Les quaternions, un corps non commutatif ★★★★★

corrigé p. 70

On admet que les matrices d'ordre 2 à coefficients complexes forment un anneau $M_2(\mathbb{C})$, où l'on calcule comme dans $M_2(\mathbb{R})$, et que $\det(MM') = \det M \det M'$. Pour $(z, w) \in \mathbb{C}^2$, on pose $q(z, w) = \begin{pmatrix} z & -\bar{w} \\ w & \bar{z} \end{pmatrix}$ et $\mathbb{H} = \{q(z, w), (z, w) \in \mathbb{C}^2\}$.

1. Montrer que $q(z, w)q(z', w') = q(zz' - \bar{w}w', wz' + \bar{z}w')$, puis que $(\mathbb{H}, +, \times)$ est un anneau unitaire.
2. On pose $\mathbf{i} = q(i, 0)$, $\mathbf{j} = q(0, 1)$ et $\mathbf{k} = q(0, -i)$. Calculer $\mathbf{i}^2$, $\mathbf{j}^2$, $\mathbf{k}^2$, $\mathbf{ij}$, $\mathbf{ji}$ et $\mathbf{ijk}$. L'anneau $\mathbb{H}$ est-il commutatif ?
3. On pose $N(q(z, w)) = |z|^2 + |w|^2$. Calculer $q(z, w)q(\bar{z}, -w)$ et en déduire que tout élément non nul de $\mathbb{H}$ est inversible dans $\mathbb{H}$: $\mathbb{H}$ est un corps non commutatif.
4. Vérifier que $N(q) = \det q$ et en déduire $N(qq') = N(q)N(q')$. En posant $z = a + ib$, $w = c + id$, $z' = a' + ib'$, $w' = c' + id'$, écrire $(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2)$ comme une somme de quatre carrés (identité d'Euler). Écrire ainsi $105 = 7 \times 15$ comme somme de quatre carrés.
5. Calculer $q(z, w)^2$. En déduire que l'équation $x^2 = -I$ a une infinité de solutions dans $\mathbb{H}$. Pourquoi est-ce impossible dans un corps commutatif ?

Exercice 64 Le théorème des quatre carrés ★★★★★

corrigé p. 71

On note Σ l'ensemble des entiers naturels de la forme $x_1^2 + x_2^2 + x_3^2 + x_4^2$, avec $x_1, \dots, x_4 \in \mathbb{Z}$. On admet l'identité $(\sum_{i=1}^4 x_i^2)(\sum_{i=1}^4 y_i^2) = T_1^2 + T_2^2 + T_3^2 + T_4^2$ (celle de l'exercice 63 appliquée à $(y_1, -y_2, -y_3, -y_4)$), où

$$\begin{aligned} T_1 &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4, & T_2 &= x_2 y_1 - x_1 y_2 + x_3 y_4 - x_4 y_3, \\ T_3 &= x_3 y_1 - x_1 y_3 + x_4 y_2 - x_2 y_4, & T_4 &= x_4 y_1 - x_1 y_4 + x_2 y_3 - x_3 y_2. \end{aligned}$$

1. Montrer que Σ est une partie stable de $(\mathbb{N}, \times)$. En déduire que, pour montrer que $\Sigma = \mathbb{N}$, il suffit de prouver que tout nombre premier impair appartient à Σ .
2. Soit p un nombre premier impair. a) Montrer que les entiers x^2 , pour $0 \leq x \leq \frac{p-1}{2}$, ont des restes deux à deux distincts modulo p ; de même pour les entiers $-1 - y^2$, $0 \leq y \leq \frac{p-1}{2}$. b) En déduire qu'il existe $x, y \in \{0, \dots, \frac{p-1}{2}\}$ tels que $p \mid x^2 + y^2 + 1$, puis un entier m tel que $1 \leq m < p$ et $mp \in \Sigma$.
3. Soit m_0 le plus petit entier $m \geq 1$ tel que $mp \in \Sigma$; on écrit $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ et on suppose $m_0 \geq 2$. a) Si m_0 est pair, montrer qu'on peut numérotter les x_i de sorte que $x_1 + x_2$ et $x_3 + x_4$ soient pairs, puis que $\frac{m_0}{2}p \in \Sigma$. Conclure. b) Si m_0 est impair, on choisit des entiers $y_i \equiv x_i [m_0]$ tels que $|y_i| \leq \frac{m_0-1}{2}$. Montrer que $y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1$ avec $1 \leq m_1 < m_0$. c) Montrer que T_1, T_2, T_3, T_4 sont divisibles par m_0 , puis que $m_1 p \in \Sigma$. Conclure.
4. En déduire le *théorème de Lagrange* : tout entier naturel est somme de quatre carrés. Écrire 23 comme somme de quatre carrés, et montrer (modulo 8) que 23 n'est pas somme de trois carrés.

Exercice 65 Les automorphismes de $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ ★★★★★

corrigé p. 71

Si K et L sont des sous-corps de $\mathbb{C}$, un *morphisme de corps* de K dans L est une application $f : K \rightarrow L$ telle que $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ pour tous $x, y \in K$, et $f(1) = 1$.

1. Soit f un morphisme de corps de K dans L . Montrer que $f(-x) = -f(x)$ et que, si $x \neq 0$, $f(x^{-1}) = f(x)^{-1}$; en déduire que f est injective.
2. Tout sous-corps de $\mathbb{C}$ contient $\mathbb{Q}$ (comme à l'exercice 23). Montrer que $f(r) = r$ pour tout $r \in \mathbb{Q}$. Morphismes de corps de $\mathbb{Q}$ dans $\mathbb{Q}$?
3. Le cas de $\mathbb{R}$. Soit f un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$. a) Montrer que $f(x) \geq 0$ pour tout $x \geq 0$, puis que f est croissante. b) En encadrant x par des rationnels, montrer que $f(x) = x$ pour tout $x \in \mathbb{R}$.
4. Le cas de $\mathbb{C}$. Soit f un morphisme de corps de $\mathbb{C}$ dans $\mathbb{C}$ tel que $f(\mathbb{R}) \subset \mathbb{R}$. Montrer que $f(i) = \pm i$, puis que $f = \text{id}$ ou $f : z \mapsto \bar{z}$. Ces deux applications conviennent-elles ?
5. Le cas de $\mathbb{Q}(\sqrt{2})$. On rappelle que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ et $\mathbb{Q}(\sqrt{3})$ sont des sous-corps de $\mathbb{R}$, où l'écriture $a + b\sqrt{2}$ (resp. $a + b\sqrt{3}$) est unique. a) Déterminer les morphismes de corps de $\mathbb{Q}(\sqrt{2})$ dans lui-même. b) Montrer qu'il n'existe aucun morphisme de corps de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{Q}(\sqrt{3})$: ces deux corps ne sont pas isomorphes.

Exercice 66 Le groupe $GL_2(\mathbb{Z}/p\mathbb{Z})$ ★★★★★

corrigé p. 72

Soit p premier et $K = \mathbb{Z}/p\mathbb{Z}$. On admet que les matrices d'ordre 2 à coefficients dans K forment un anneau $M_2(K)$ où l'on calcule comme dans $M_2(\mathbb{R})$ (exercice 30), avec $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ et $\det(AB) = \det A \det B$. On note $GL_2(K)$ l'ensemble des inversibles de $M_2(K)$ et $SL_2(K) = \{A : \det A = 1\}$.

1. Montrer que $A \in M_2(K)$ est inversible si et seulement si $\det A \neq 0$. En déduire que $\det$ est un morphisme surjectif du groupe $(GL_2(K), \times)$ sur $(K^*, \times)$, et que $SL_2(K)$ est un sous-groupe de $GL_2(K)$.
2. On suppose que la première colonne (a, c) de A est non nulle. Montrer que $\det A = 0$ si et seulement s'il existe $\lambda \in K$ tel que $(b, d) = (\lambda a, \lambda c)$. En déduire que $GL_2(K)$ a $(p^2 - 1)(p^2 - p)$ éléments.
3. Pour $\lambda \in K^*$, on pose $D_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ et $S_\lambda = \{A : \det A = \lambda\}$. Montrer que $A \mapsto D_\lambda A$ est une bijection de $SL_2(K)$ sur S_λ , puis que $SL_2(K)$ a $p(p^2 - 1)$ éléments. Application numérique pour $p = 2, 3$ et 5 .
4. Cas $p = 2$. Écrire les six éléments de $GL_2(\mathbb{Z}/2\mathbb{Z})$. Montrer que ce groupe n'est pas commutatif et donner, pour chacun de ses éléments X , le plus petit entier $n \geq 1$ tel que $X^n = I$.

Partie D • Corrigés

Des solutions détaillées, rédigées comme sur une copie

25 Corrigés du niveau I

■ Corrigé de l'exercice 1

1. a) $0 * 1 = \frac{1}{2} \notin \mathbb{Z}$: **non** sur $\mathbb{Z}$; **oui** sur $\mathbb{Q}$. b) $1 * 1 = 2 \notin [0, 1]$: **non** ; **oui** sur $\mathbb{N}$. c) Si $x, y \geq 0$, $e^x + e^y \geq 2$, donc $x * y \geq \ln 2 > 0$: **oui** sur $\mathbb{R}_+$; mais $0 * 0 = \ln 2 \notin \mathbb{R}_-$: **non**.
2. $(4a + 1)(4b + 1) = 4(4ab + a + b) + 1$: stable pour $\times$; $1 + 1 = 2 \neq 1$ [4] : pas pour $+$. Si f, g sont impaires, $(f + g)(-x) = -(f + g)(x)$ et $f(g(-x)) = f(-g(x)) = -f(g(x))$: stable pour $+$ et $\circ$. Mais $x \mapsto x \times x = x^2$ n'est pas impaire : pas pour $\times$.
3. Commutativité : évidente. $(x * y) * z = \ln(e^{x*y} + e^z) = \ln(e^x + e^y + e^z) = x * (y * z)$. Si $x * y = x * z$, alors $e^x + e^y = e^x + e^z$, donc $y = z$: tout réel est régulier. Un neutre ε vérifierait $e^x + e^\varepsilon = e^x$, soit $e^\varepsilon = 0$: impossible. Par récurrence, $x^{(n)} = \ln(ne^x) = \boxed{x + \ln n}$.

■ Corrigé de l'exercice 2

1. $\varphi : x \mapsto x^3$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}$ et $\varphi(x * y) = x^3 + y^3 = \varphi(x) + \varphi(y)$. Par transport de structure, $(\mathbb{R}, *)$ est un **groupe commutatif**, isomorphe à $(\mathbb{R}, +)$: neutre $\varphi^{-1}(0) = \boxed{0}$, symétrique de x : $\varphi^{-1}(-x^3) = \boxed{-x}$. Puis $\varphi(x^{(n)}) = nx^3$, d'où $\boxed{x^{(n)} = x \sqrt[3]{n}}$. $x * 2 = 3 \iff x^3 + 8 = 27 \iff \boxed{x = \sqrt[3]{19}}$; $x * x * x = 3 \iff 3x^3 = 27 \iff \boxed{x = \sqrt[3]{9}}$.
2. $\lambda(x * y) = \sqrt[3]{\lambda^3 x^3 + \lambda^3 y^3} = (\lambda x) * (\lambda y)$, et de même à droite : $\times$ est distributive par rapport à $*$. Mais $1 * (1 * 1) = \sqrt[3]{2} \neq (1 * 1) * (1 * 1) = \sqrt[3]{4}$.
3. $\mathbb{R}_+$ est stable et contient 0, mais le symétrique de 1 est $-1 \notin \mathbb{R}_+$: **non**. $\sqrt[3]{n} * (-\sqrt[3]{m}) = \sqrt[3]{n - m}$ et $0 = \sqrt[3]{0}$: **oui** (c'est $\varphi^{-1}(\mathbb{Z})$).

■ Corrigé de l'exercice 3

$\circ$	f_1	f_2	f_3	f_4	$\times$	I	R	R^2	R^3
f_1	f_1	f_2	f_3	f_4	I	I	R	R^2	R^3
f_2	f_2	f_1	f_4	f_3	R	R	R^2	R^3	I
f_3	f_3	f_4	f_1	f_2	R^2	R^2	R^3	I	R
f_4	f_4	f_3	f_2	f_1	R^3	R^3	I	R	R^2

1. Par exemple $f_2 \circ f_3(x) = -\frac{1}{x} = f_4(x)$ et $f_3 \circ f_4(x) = \frac{1}{-1/x} = -x = f_2(x)$ (table de gauche). G est stable, $\circ$ est associative (composition), f_1 est neutre et $f \circ f = f_1$ pour tout f : **groupe**, chaque élément étant son propre symétrique ; la table est symétrique : il est **commutatif**.

- $R^2 = -I, R^3 = -R, R^4 = I$, donc $R^i R^j = R^{i+j}$, exposants modulo 4 (table de droite). Stable, associatif, neutre I : groupe commutatif, avec $I^{-1} = I, R^{-1} = R^3, (R^2)^{-1} = R^2, (R^3)^{-1} = R$.
- Si φ existait : $\varphi(f_1) = \varphi(f_1 \cdot f_1) = \varphi(f_1)^2$, d'où $\varphi(f_1) = I$; puis $\varphi(f)^2 = \varphi(f \cdot f) = I$ pour tout f . Comme φ est surjective, tout $X \in H$ vérifierait $X^2 = I$; or $R^2 = -I$. **Contradiction** : dans G , 4 éléments ont un carré neutre, dans H seulement 2 (I, R^2).

■ Corrigé de l'exercice 4

- a) $1 = 2^0 3^0 \in H$ et $2^n 3^m (2^{n'} 3^{m'})^{-1} = 2^{n-n'} 3^{m-m'} \in H$: **oui**. b) $1 = \frac{1}{1} \in H$ et $\frac{p}{q} \left(\frac{p'}{q'}\right)^{-1} = \frac{pq'}{qp'}$ avec pq', qp' impairs : **oui**. c) $2 \in H$, mais $\frac{1}{2} \notin H$: **non**.
- a) $0 \in H$ et $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$: **oui**. Avec $a, b \in \mathbb{N}$: $1 \in H$, mais $-1 \notin H$ ($a + b\sqrt{2} \geq 0$) : **non**. b) La fonction nulle vérifie $f(1) = 0$, et $(f - g)(1) = 0$: **oui**. La fonction nulle (neutre) ne vérifie pas $f(1) = 1$: **non**.
- a) $1 = e^0 \in H$ et $e^{i\pi r} (e^{i\pi s})^{-1} = e^{i\pi(r-s)}, r - s \in \mathbb{Q}$: **oui**. b) $1 + i \in H$, mais $(1 + i)^2 = 2i \notin H$: **non**.

■ Corrigé de l'exercice 5

- $((a, b) * (c, d)) * (f, g) = (a + c + f, (be^c + d)e^f + g)$ et $(a, b) * ((c, d) * (f, g)) = (a, b) * (c + f, de^f + g)$ valent tous deux $(a + c + f, be^{c+f} + de^f + g)$: $*$ est associative. Neutre $(0, 0)$: $(a, b) * (0, 0) = (a, b) = (0, 0) * (a, b)$. $(a, b) * (c, d) = (0, 0) \iff c = -a, d = -be^{-a}$, et $(-a, -be^{-a}) * (a, b) = (0, -b + b)$: symétrique $(-a, -be^{-a})$. Enfin $(1, 0) * (0, 1) = (1, 1) \neq (0, 1) * (1, 0) = (1, e)$: **non commutatif**.
- $X = (c, d) : (1, 0) * X = (1 + c, d)$, d'où $X = (1, 3)$; $X * (1, 0) = (c + 1, de)$, d'où $X = \left(1, \frac{3}{e}\right)$. Puis $(1, 1)^{(n)} = (n, u_n)$ avec $u_1 = 1$ et $u_{n+1} = eu_n + 1$ (car $(n, u_n) * (1, 1) = (n+1, u_n e + 1)$) : $u_n = 1 + e + \dots + e^{n-1}$, soit $(1, 1)^{(n)} = \left(n, \frac{e^n - 1}{e - 1}\right)$.
- $(a, b) * (1, 0) = (a + 1, be)$ et $(1, 0) * (a, b) = (a + 1, b)$: égaux $\iff b = 0$. $C = \{(a, 0), a \in \mathbb{R}\}$ contient $(0, 0)$ et $(a, 0) * (c, 0)' = (a - c, 0) \in C$: sous-groupe ; $a \mapsto (a, 0)$ est bijective de $\mathbb{R}$ sur C et $(a, 0) * (c, 0) = (a + c, 0)$: isomorphisme de $(\mathbb{R}, +)$ sur $(C, *)$.

■ Corrigé de l'exercice 6

- a) $2^{-(x+y)} = 2^{-x} 2^{-y}$: morphisme ; $x \mapsto 2^{-x}$ est une bijection (strictement décroissante, continue) de $\mathbb{R}$ sur $\mathbb{R}_+^*$: **isomorphisme**. Image de $\mathbb{Z} : \{2^k, k \in \mathbb{Z}\}$. b) Morphisme (somme de deux applications additives), surjectif ($x \in \mathbb{R}$ est l'image de x), non injectif : $\operatorname{Re}(z) + \operatorname{Im}(z) = 0 \iff z \in (1 - i)\mathbb{R}$.
- $(zz')^2 = z^2 z'^2$: morphisme ; surjectif (tout complexe non nul a une racine carrée), non injectif ($(-1)^2 = 1^2$). $e^{i\theta} = (e^{i\theta/2})^2$: l'image de $\mathbb{U}$ est $\mathbb{U}$; l'image de $\mathbb{R}^*$ est $\mathbb{R}_+^*$ ($x^2 > 0$ et $y = (\sqrt{y})^2$).
- $\det(AB) = \det A \det B$ (calcul, voir l'exercice 19) : morphisme, surjectif ($\det \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = x$), non injectif ($\det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1$). $\operatorname{SL}_2(\mathbb{R})$ est l'image réciproque du sous-groupe $\{1\}$: c'est un **sous-groupe** (cours).

■ Corrigé de l'exercice 7

- Les axiomes se vérifient composante par composante, car $(\mathbb{Z}, +, \times)$ est un anneau commutatif : $(\mathbb{Z}^2, +)$ est un groupe commutatif, $\times$ est associative, commutative, distributive, d'unité $(1, 1)$. Mais $(1, 0) \times (0, 1) = (0, 0)$: **non intègre**. (a, b) est inversible $\iff ac = bd = 1$ possible $\iff (a, b) \in \{(\pm 1, \pm 1)\}$.

2. a) $\bar{k}$ inversible $\iff k \wedge 15 = 1 : \bar{1}^{-1} = \bar{1}, \bar{2}^{-1} = \bar{8}, \bar{4}^{-1} = \bar{4}, \bar{7}^{-1} = \bar{13}, \bar{11}^{-1} = \bar{11}, \bar{14}^{-1} = \bar{14}$ (16, 91, 121, 196 $\equiv 1$ [15]). b) $\bar{3} \times \bar{5} = \bar{6} \times \bar{5} = \bar{9} \times \bar{5} = \bar{12} \times \bar{5} = \bar{10} \times \bar{3} = \bar{0}$. c) $\bar{7}x = \bar{9} \iff x = \bar{13} \times \bar{9} = \boxed{\bar{12}}$.
 $\bar{6}x = \bar{9} \iff 15 \mid 6x - 9 \iff 5 \mid 2x - 3 \iff x \equiv 4$ [5] : $x \in \{\bar{4}, \bar{9}, \bar{14}\}$.

■ Corrigé de l'exercice 8

1. $AB = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \neq BA = \begin{pmatrix} 3 & 0 \\ 2 & 2 \end{pmatrix}$. $A^2 = \begin{pmatrix} 3 & -3 \\ 3 & 0 \end{pmatrix}$ et $A^2 - 3A + 3I = 0$. Donc $A(3I - A) = (3I - A)A = 3I$:
 $A^{-1} = \frac{1}{3}(3I - A) = \frac{1}{3} \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$ (c'est bien $\frac{1}{\det A} \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$, $\det A = 3$).
2. $N^2 = 0$, donc $(I + N)(I - N) = (I - N)(I + N) = I - N^2 = I$: $(I + N)^{-1} = I - N = \begin{pmatrix} 1 & 4 \\ -1 & 3 \end{pmatrix}$. I et N commutent
et $N^k = 0$ pour $k \geq 2$: binôme, $(I + N)^n = I + nN = \begin{pmatrix} 1+2n & -4n \\ n & 1-2n \end{pmatrix}$.
3. $x + y = \alpha$, $y + z = \beta$, $x + z = \gamma$; en sommant, $x + y + z = \frac{\alpha+\beta+\gamma}{2}$, d'où $x = \frac{\alpha-\beta+\gamma}{2}$, $y = \frac{\alpha+\beta-\gamma}{2}$, $z = \frac{-\alpha+\beta+\gamma}{2}$: solution unique $X = C'Y$. Alors $CC'Y = Y$ pour tout Y et $C'CX = X$ pour tout X : $CC' = C'C = I$,
 $C^{-1} = \frac{1}{2} \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}$.

26

Corrigés du niveau 2

■ Corrigé de l'exercice 9

1. $e^{\ln x \ln y} > 0$ et l'expression est symétrique : $\otimes$ est interne et commutative ; $\ln(x \otimes y) = \ln x \ln y$, et
 $x \otimes (yz) = e^{\ln x (\ln y \ln z)} = (x \otimes y)(x \otimes z)$. Ainsi $\ln$ est une bijection de $\mathbb{R}_+^*$ sur $\mathbb{R}$ qui transforme $\times$ en
 $+$ et $\otimes$ en $\times$: $(\mathbb{R}_+^*, \times)$ est un groupe commutatif ; $\otimes$ est associative ($\ln((x \otimes y) \otimes z) = \ln x \ln y \ln z =$
 $\ln(x \otimes (y \otimes z))$, $\ln$ injective) ; $x \otimes e = x$; si $x \neq 1$, $\ln x \neq 0$ et $x \otimes e^{1/\ln x} = e$. $(\mathbb{R}_+^*, \times, \otimes)$ est un **corps**
commutatif (isomorphe à $(\mathbb{R}, +, \times)$ par $\ln$), de zéro $\boxed{1}$, d'unité $\boxed{e}$, et le symétrique de $x \neq 1$ pour
 $\otimes$ est $\boxed{e^{1/\ln x}}$.
2. Si $x, y > 1$, $\ln x \ln y > 0$: $x \otimes y > 1$. $\ln$ est une bijection de $]1, +\infty[$ sur $\mathbb{R}_+^*$ avec $\ln(x \otimes y) = \ln x \times \ln y$
: par transport, $(]1, +\infty[, \otimes)$ est un groupe isomorphe à $(\mathbb{R}_+^*, \times)$ (neutre e). $]e, +\infty[$ est stable
($\ln x \ln y > 1$) mais ne contient pas le neutre e : **non**.
3. a) $(\ln x)^3 = 8 \iff \ln x = 2 \iff \boxed{x = e^2}$. b) $(\ln x)^2 = \ln 2 \ln 8 = 3(\ln 2)^2 \iff \ln x = \pm\sqrt{3} \ln 2 \iff$
 $\boxed{x \in \{2^{\sqrt{3}}, 2^{-\sqrt{3}}\}}$.

■ Corrigé de l'exercice 10

1. $J^2 = \begin{pmatrix} 4 & -2 \\ -2 & 1 \end{pmatrix} = I$, donc $M(x)M(y) = I + ((x-1) + (y-1) + (x-1)(y-1))J = I + (xy-1)J = M(xy)$.
2. $f : x \mapsto M(x)$ est surjective de $\mathbb{R}^*$ sur E , injective ($M(x) = M(y) \Rightarrow (x-y)J = 0 \Rightarrow x = y$) et
 $f(xy) = f(x)f(y)$; E est stable ($xy \neq 0$). Par transport, $(E, \times)$ est un **groupe commutatif** isomorphe
à $(\mathbb{R}^*, \times)$: neutre $M(1) = I$, $M(x)^{-1} = M\left(\frac{1}{x}\right)$. Contrôle : $\det M(x) = (2x-1)(2-x) - (1-x)(2x-2) = x$
et $\frac{1}{x} \begin{pmatrix} 2-x & x-1 \\ 2-2x & 2x-1 \end{pmatrix} = M\left(\frac{1}{x}\right)$ ✓.
3. $M(2)^{10} = M(2^{10}) = M(1024) = \begin{pmatrix} 2047 & -1023 \\ 2046 & -1022 \end{pmatrix}$. Pour $X = M(x) : X^3 = M(x^3) = M(-8) \iff x = -2$:
 $X = M(-2) = \begin{pmatrix} -5 & 3 \\ -6 & 4 \end{pmatrix}$; $X^2 = M(x^2) = M(1) \iff x = \pm 1$: $X \in \{I, M(-1) = \begin{pmatrix} -3 & 2 \\ -4 & 3 \end{pmatrix}\}$.

4. $g(t) = M(e^t)$ vérifie $g(s+t) = M(e^s e^t) = g(s)g(t)$ et est injective : c'est un isomorphisme de $(\mathbb{R}, +)$ sur son image $\{M(x), x > 0\}$, qui est un sous-groupe de E (image d'un groupe par un morphisme).

■ Corrigé de l'exercice 11

- $K^2 = \begin{pmatrix} 4 & -5 \\ 2 & -2 \end{pmatrix} \begin{pmatrix} -10 & 10 \\ -5 & 4 \end{pmatrix} = -I$, donc $M(a, b)M(c, d) = acI + (ad + bc)K + bdK^2 = M(ac - bd, ad + bc)$.
- $M(a, b) = \begin{pmatrix} a+2b & -5b \\ b & a-2b \end{pmatrix}$ détermine b , puis a : φ est injective, et surjective par définition de F . $\varphi(z+z') = \varphi(z) + \varphi(z')$ est clair et, comme $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$, la question 1 donne $\varphi(zz') = \varphi(z)\varphi(z')$. Par transport, $(F, +, \times)$ est un **corps commutatif** isomorphe à $\mathbb{C}$ (zéro 0, unité I), et $M(a, b)^{-1} = \varphi\left(\frac{a-ib}{a^2+b^2}\right) = \frac{1}{a^2+b^2}M(a, -b)$; en effet $\det M(a, b) = a^2 - 4b^2 + 5b^2 = a^2 + b^2$ et $\frac{1}{\det} \begin{pmatrix} a-2b & 5b \\ -b & a+2b \end{pmatrix} = \frac{M(a, -b)}{a^2+b^2}$ ✓.
- $\Omega = \varphi(1+i\sqrt{3})$ et $1+i\sqrt{3} = 2e^{i\pi/3}$. $(1+i\sqrt{3})^3 = 8e^{i\pi} = -8$: $\Omega^3 = -8I$. $2026 = 3 \times 675 + 1$: $\Omega^{2026} = (\Omega^3)^{675} \Omega = (-8)^{675} \Omega$, soit $\Omega^{2026} = -2^{2025} \Omega$.
- $X = \varphi(z) : X^2 = -I \iff z^2 = -1 \iff X = \pm K$. $X^2 = \Omega \iff z^2 = 2e^{i\pi/3} \iff z = \pm\sqrt{2}e^{i\pi/6} = \pm\left(\frac{\sqrt{6}}{2} + i\frac{\sqrt{2}}{2}\right) : X = \pm M\left(\frac{\sqrt{6}}{2}, \frac{\sqrt{2}}{2}\right)$. Dans $M_2(\mathbb{R})$, qui n'est pas un corps, $X^2 = -I$ a une **infinité** de solutions : $\begin{pmatrix} 0 & -t \\ 1/t & 0 \end{pmatrix}$, $t \neq 0$; pour $t = 1$, c'est une matrice qui n'est pas dans F (on aurait $b = 1$ et $-5b = -1$).

■ Corrigé de l'exercice 12

- 17 est premier : $\mathbb{Z}/17\mathbb{Z}$ est un corps (cours). $36 = 2 + 2 \times 17 : \bar{6}^2 = \bar{2}$. Donc $x^2 = \bar{2} \iff (x - \bar{6})(x + \bar{6}) = \bar{0} \iff x \in \{\bar{6}, \bar{11}\}$ (pas de diviseur de zéro). $x^2 - \bar{2}x - \bar{1} = \bar{0} \iff (x - \bar{1})^2 = \bar{2} \iff x - \bar{1} = \pm\bar{6} \iff x \in \{\bar{7}, \bar{12}\}$.
- Les classes $\bar{3}^{-k}$ sont :

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\bar{3}^{-k}$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

$\bar{3}^{-k+m} = \bar{3}^{-k} \bar{3}^{-m}$: morphisme ; les 16 éléments de $(\mathbb{Z}/17\mathbb{Z})^*$ apparaissent : surjectif. Si $k-m = 16q+r$ ($0 \leq r < 16$), $\bar{3}^{-k+m} = \bar{3}^{-r}$, et le tableau montre que $\bar{3}^{-r} = \bar{1}$ seulement pour $r = 0$: $\bar{3}^{-k} = \bar{3}^{-m} \iff 16 \mid k-m$.
- $x = \bar{3}^{-k}$ ($x = \bar{0}$ ne convient pas). $-\bar{1} = \bar{3}^{-8} : \bar{3}^{-4k} = \bar{3}^{-8} \iff 4k \equiv 8 [16] \iff k \equiv 2 [4]$, d'où $x \in \{\bar{9}, \bar{15}, \bar{8}, \bar{2}\}$ ($k = 2, 6, 10, 14$). $\bar{2} = \bar{3}^{-14} : 5k \equiv 14 [16] \iff k \equiv 14 \times 13 \equiv 6 [16]$ (car $5 \times 13 = 65 \equiv 1$), d'où $x = \bar{3}^{-6} = \bar{15}$ ($(-2)^5 = -32 \equiv 2$ ✓). Enfin $(\bar{3}^{-k})^2 = \bar{3}^{-2k}$: les carrés sont les puissances paires $\{\bar{1}, \bar{2}, \bar{4}, \bar{8}, \bar{9}, \bar{13}, \bar{15}, \bar{16}\}$, et $\bar{3} = \bar{3}^{-1} = \bar{3}^{-2j}$ exigerait $2j \equiv 1 [16]$: $x^2 = \bar{3}$ n'a **pas de solution**.

■ Corrigé de l'exercice 13

1. $\varphi(z)\varphi(w) = 1 + iz + iw - zw = 1 + i(z + w + izw) = \varphi(z * w)$. φ est une bijection de $\mathbb{C}$ sur $\mathbb{C}$ ($\varphi^{-1}(u) = i(1 - u)$); donc $\varphi(z * w) = \varphi(w * z)$ et $\varphi((z * w) * u) = \varphi(z)\varphi(w)\varphi(u) = \varphi(z * (w * u))$ donnent commutativité et associativité; $z * 0 = z$; $\varphi(i) = 0$, donc $\varphi(z * i) = 0 = \varphi(i)$: $z * i = i$.

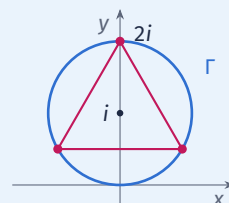
2. $\varphi(z) = 0 \iff z = i$: φ est une bijection de E sur $\mathbb{C}^*$; si $z, w \in E$, $\varphi(z * w) = \varphi(z)\varphi(w) \neq 0$: E est stable. Par transport, $(E, *)$ est un **groupe commutatif** isomorphe à $(\mathbb{C}^*, \times)$. $\varphi(z') = \frac{1}{1+iz}$ donne

$$z' = \frac{-z}{1+iz}.$$

3. $\varphi(z) = i(z - i)$, donc $|\varphi(z)| = |z - i|$: $\Gamma = \varphi^{-1}(\mathbb{U})$. Et $\varphi(iy) = 1 - y$: $\Delta = \varphi^{-1}(\mathbb{R}_+^*)$. Images réciproques de sous-groupes de $\mathbb{C}^*$ par un isomorphisme: ce sont des **sous-groupes** de $(E, *)$.

4. $\varphi(z)^3 = \varphi(2i) = -1 \iff \varphi(z) \in \{-1, e^{i\pi/3}, e^{-i\pi/3}\} \iff z = i(1 - \varphi(z))$:

$$z \in \left\{ 2i, \frac{\sqrt{3}}{2} + \frac{i}{2}, -\frac{\sqrt{3}}{2} + \frac{i}{2} \right\}.$$



Comme $|\varphi(z)| = 1$, ces points sont sur Γ : ce sont les sommets d'un **triangle équilatéral** inscrit dans Γ (centre i , rayon 1).

■ Corrigé de l'exercice 14

1. $N^2 = 0$; $I \in A$, A est stable par différence, et $(aI + bN)(cI + dN) = acI + (ad + bc)N \in A$, expression symétrique: A est un **sous-anneau commutatif**. $\psi(a, b) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ détermine (a, b) : ψ est bijective; $\psi(u + v) = \psi(u) + \psi(v)$ et, par le calcul précédent, $\psi(u \otimes v) = \psi(u)\psi(v)$. Par transport, $(\mathbb{R}^2, +, \otimes)$ est un **anneau commutatif unitaire** (unité $(1, 0)$), **non intègre**: $(0, 1) \otimes (0, 1) = (0, 0)$.

2. $(a, b) \otimes (c, d) = (1, 0)$ impose $ac = 1$, donc $a \neq 0$. Réciproquement, si $a \neq 0$: $(a, b) \otimes \left(\frac{1}{a}, -\frac{b}{a^2}\right) = (1, 0)$, inverse $\left(\frac{1}{a}, -\frac{b}{a^2}\right)$. Récurrence: $(a^n, na^{n-1}b) \otimes (a, b) = (a^{n+1}, a^n b + na^n b)$. $(2, 3)^5 = (32, 240)$.

3. $X = (a, b)$: $X \otimes X = (a^2, 2ab)$. $(4, 12)$: $X = \pm(2, 3)$. $(0, 0)$: $X = (0, b)$, $b \in \mathbb{R}$ (une infinité). $(-1, 0)$: $a^2 = -1$, **aucune solution**.

■ Corrigé de l'exercice 15

1. P envoie $e_1 \mapsto e_2 \mapsto e_3 \mapsto e_1$ (colonnes): $P^2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $P^3 = I$, et $M(a, b, c) = \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix}$. $P^i P^j = P^{(i+j) \bmod 3}$: $\{I, P, P^2\}$ est stable, de neutre I , avec $P^{-1} = P^2$; c'est un groupe, et $P^k \mapsto j^k$ ($j = e^{2i\pi/3}$, $k = 0, 1, 2$) est un isomorphisme sur $\mathbb{U}_3$ (exposants modulo 3 des deux côtés).

2. $I \in E$, E est stable par différence et, avec $P^3 = I$, $P^4 = P$: $M(a, b, c)M(a', b', c') = M(a'', b'', c'')$, où $a'' = aa' + bc' + cb'$, $b'' = ab' + ba' + cc'$, $c'' = ac' + bb' + ca'$ (expressions symétriques): **sous-anneau commutatif**. $(I + P + P^2)(I - P) = I - P^3 = 0$ avec deux facteurs non nuls: **non intègre**.

3. $I + P = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; $x + z = \alpha$, $x + y = \beta$, $y + z = \gamma$ donnent $x = \frac{\alpha + \beta - \gamma}{2}$, $y = \frac{-\alpha + \beta + \gamma}{2}$, $z = \frac{\alpha - \beta + \gamma}{2}$:

$$(I + P)^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} = \frac{1}{2} (I - P + P^2) \in E. \text{ Binôme } (I \text{ et } P \text{ commutent}): (I + P)^3 = 2I + 3P + 3P^2;$$

$$(I + P)^6 = \sum_k C_6^k P^k \text{ et, en groupant } k \text{ modulo } 3: (1 + 20 + 1)I + (6 + 15)P + (15 + 6)P^2 = 22I + 21P + 21P^2.$$

■ Corrigé de l'exercice 16

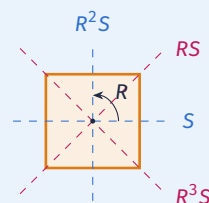
1. $1 \in A$, A est stable par différence et $(a+b\sqrt{7})(c+d\sqrt{7}) = (ac+7bd) + (ad+bc)\sqrt{7} \in A$: **sous-anneau**. Comme $\sqrt{7} \notin \mathbb{Q}$, l'écriture $a + b\sqrt{7}$ est unique ($b \neq b'$ donnerait $\sqrt{7} = \frac{a-a'}{b'-b}$) : σ est bien définie, et $\sigma(xy) = (ac+7bd) - (ad+bc)\sqrt{7} = \sigma(x)\sigma(y)$. Puis $N(xy) = xy\sigma(x)\sigma(y) = N(x)N(y)$.
2. Si $xy = 1$ dans A , $N(x)N(y) = N(1) = 1$ dans $\mathbb{Z}$: $N(x) = \pm 1$. Or $a^2 - 7b^2 = -1$ donnerait $a^2 \equiv 6 \pmod{7}$, alors que les carrés modulo 7 sont 0, 1, 4, 2 : donc $N(x) = 1$. Réciproquement, si $N(x) = 1$, $x\sigma(x) = 1$ avec $\sigma(x) \in A$: $x^{-1} = \sigma(x)$.
3. $N(\varepsilon) = 64 - 63 = 1$: $\varepsilon^{-1} = 8 - 3\sqrt{7}$. $\boxed{\varepsilon^2 = 127 + 48\sqrt{7}}$ ($127^2 - 7 \times 48^2 = 1$ ✓). Les ε^n ($n \in \mathbb{N}$) sont inversibles et deux à deux distincts ($\varepsilon > 1$) : **infinité d'inversibles**. $N(3 + \sqrt{7}) = 2 \neq 1$: $3 + \sqrt{7}$ n'est pas inversible dans A (son inverse dans $\mathbb{R}$, $\frac{3-\sqrt{7}}{2}$, n'est pas dans A).

27

Corrigés du niveau 3

■ Corrigé de l'exercice 17

1. Les coefficients non nuls (± 1) sont sur la diagonale ou sur l'autre diagonale : $2 \times 2 \times 2 = 8$ matrices. Or $R^2 = -I$, $R^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $RS = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $R^2S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $R^3S = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$: les huit matrices annoncées sont distinctes et dans D . Isométries : R, R^2, R^3 : rotations de centre O d'angles $\frac{\pi}{2}, \pi, -\frac{\pi}{2}$; S, R^2S : symétries d'axes $(Ox), (Oy)$; RS, R^3S : symétries d'axes $y = x, y = -x$. Chacune permute les sommets $(\pm 1, \pm 1)$.
2. $SR = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = R^3S = R^{-1}S$; par récurrence $SR^{k+1} = R^{-k}SR = R^{-k-1}S$ (et pour $k < 0$, on utilise $R^4 = I$). Donc $(R^aS^\varepsilon)(R^bS^\eta) = R^{a+b}S^{\varepsilon+\eta} \in D$ ($S^2 = I$) : D est stable ; $I \in D$, $(R^a)^{-1} = R^{4-a}$ et $(R^aS)^2 = R^aR^{-a}S^2 = I$. $D \subset GL_2(\mathbb{R})$ est donc un sous-groupe, **non commutatif** : $SR = R^3S \neq RS$.
3. $(R^aS)^2 = I, (R^2)^2 = I, R^2 = (R^3)^2 = -I$: $\boxed{X \in \{R^2, S, RS, R^2S, R^3S\}}$. $\{I, R, R^2, R^3\}$ est stable ($R^aR^b = R^{a+b}$) avec $(R^a)^{-1} = R^{4-a}$. Dans $\{I, R^2, S, R^2S\}$: $R^2 \cdot S = R^2S, S \cdot R^2S = R^{-2} = R^2, R^2S \cdot R^2 = S \dots$; dans $\{I, R^2, RS, R^3S\}$: $RS \cdot R^3S = R^{-2} = R^2, R^2 \cdot RS = R^3S, RS \cdot R^2 = R^{-1}S = R^3S \dots$ Ces parties sont stables et chaque élément y est son propre inverse : ce sont des **sous-groupes**.



■ Corrigé de l'exercice 18

1. $0 \in a\mathbb{Z} + b\mathbb{Z}$ et $(au + bv) - (au' + bv') = a(u - u') + b(v - v')$: sous-groupe de $\mathbb{Z}$, donc égal à $d\mathbb{Z}$, $d \in \mathbb{N}$ (cours), avec $d \geq 1$ ($a \neq 0$ en fait partie). $a, b \in d\mathbb{Z}$: $d \mid a \wedge b$; $a \wedge b$ divise tout $au + bv$, donc $d : \boxed{d = a \wedge b}$, et $d \in a\mathbb{Z} + b\mathbb{Z}$ s'écrit $a \wedge b = au + bv$ (**Bézout**). $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe $m\mathbb{Z}$ avec $m \geq 1$ (ab en fait partie) ; m est un multiple commun, et tout multiple commun est dans $m\mathbb{Z}$: m est le plus petit multiple commun positif, $\boxed{m = a \vee b}$.
2. $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ (image réciproque, cours) contenant $n\mathbb{Z} = \pi^{-1}(\{0\})$: $\pi^{-1}(H) = d\mathbb{Z}$ avec $d \geq 1$ et $n \in d\mathbb{Z}$, soit $d \mid n$. π étant surjective, $H = \pi(\pi^{-1}(H)) = \pi(d\mathbb{Z})$. Si $k = dq$ et $q = \frac{n}{d}s + r$ ($0 \leq r < \frac{n}{d}$), alors $k = ns + dr$ et $\bar{k} = \overline{dr}$: $\pi(d\mathbb{Z}) = \{\bar{0}, \bar{d}, \dots, \overline{n-d}\}$, de cardinal $\frac{n}{d}$ ($0 \leq dr < n$). Réciproquement, chaque diviseur d donne le sous-groupe $\pi(d\mathbb{Z})$ (image d'un sous-groupe), et des d distincts donnent des cardinaux distincts : **autant de sous-groupes que de diviseurs**.

positifs de n . Pour $\mathbb{Z}/12\mathbb{Z}$ ($d = 1, 2, 3, 4, 6, 12$) : $\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{2}, \dots, \overline{10}\}$, $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, $\{\overline{0}, \overline{4}, \overline{8}\}$, $\{\overline{0}, \overline{6}\}$, $\{\overline{0}\}$.

3. $\{m\overline{k}\} = \pi(k\mathbb{Z})$. Soit $d = k \wedge n$: $k\mathbb{Z} \subset d\mathbb{Z}$ donne $\pi(k\mathbb{Z}) \subset \pi(d\mathbb{Z})$; Bézout, $d = ku + nv$, donne $\overline{d} = u\overline{k}$, donc $\pi(d\mathbb{Z}) \subset \pi(k\mathbb{Z})$. Ce sous-groupe a $\frac{n}{k \wedge n}$ éléments : il vaut $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

$8 \wedge 12 = 4$: multiples de $\overline{8}$: $\{\overline{0}, \overline{4}, \overline{8}\}$.

■ Corrigé de l'exercice 19

1. Avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$: $\det(AB) = (aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') = ad(a'd' - b'c') - bc(a'd' - b'c') = \det A \det B$. Si $AB = I$ avec $B \in M_2(\mathbb{Z})$, alors $\det A \det B = 1$ dans $\mathbb{Z}$: $\det A = \pm 1$. Réciproquement, $A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbb{Z})$. D'où $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & -5 \\ -1 & 3 \end{pmatrix}$, $\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix}$ (déterminant 0) **non inversible**, $\begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -2 \\ -3 & 7 \end{pmatrix}$.
2. $I \in \text{SL}_2(\mathbb{Z}) \subset \text{GL}_2(\mathbb{R})$; si $A, B \in \text{SL}_2(\mathbb{Z})$, $B^{-1} \in M_2(\mathbb{Z})$ (1.) et $\det(AB^{-1}) = 1$: sous-groupe de $\text{GL}_2(\mathbb{R})$, donc groupe.
3. $S^2 = -I$; $T^{n+1} = T^n T$ donne $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ pour $n \in \mathbb{N}$, et $T^{-n} = (T^{-1})^n$ avec $T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$: $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{Z}$. $U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, $U^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $U^3 = -I$. Donc $S^n = I$ d'abord pour $n = 4$ ($S^3 = -S$), et $U^n = I$ d'abord pour $n = 6$ ($U^4 = -U$, $U^5 = -U^2$).
4. $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$: $MT = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$, $TM = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$; égalité $\iff c = 0$ et $a = d$, et $\det M = a^2 = 1$: $M = \pm T^n$, $n \in \mathbb{Z}$. S n'est pas de cette forme : $ST \neq TS$, $\text{SL}_2(\mathbb{Z})$ **n'est pas commutatif**.

■ Corrigé de l'exercice 20

$$X^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix} \text{ et } tX = \begin{pmatrix} a^2+ad & b(a+d) \\ c(a+d) & ad+d^2 \end{pmatrix} : X^2 - tX = (bc - ad)I = -\delta I \checkmark.$$

1. Soit $\tilde{X} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$: $X\tilde{X} = \delta I$. Si $\delta \neq 0$, X est inversible et $XY = 0 \Rightarrow Y = 0$. Si $\delta = 0$ et $X \neq 0$, alors $\tilde{X} \neq 0$ et $X\tilde{X} = 0$: X est un diviseur de zéro.
2. Si $t = \delta = 0$, $X^2 = tX - \delta I = 0$. Si $X^2 = 0$, X n'est pas inversible (sinon $X = X^{-1}X^2 = 0$), donc $\delta = 0$, puis $tX = X^2 = 0$: $t = 0$ (si $X = 0$, $t = 0$ aussi). Ce sont les $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, $a^2 + bc = 0$, par exemple $\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$.
3. 0 et I conviennent, ainsi que les X telles que $t = 1$, $\delta = 0$ ($X^2 = X$). Réciproquement, $X^2 = X$ donne $(1-t)X = -\delta I$: si $t \neq 1$, $X = \lambda I$ avec $\lambda^2 = \lambda$, d'où $X \in \{0, I\}$; si $t = 1$, $\delta = 0$.
4. $X^2 = I$ donne $tX = (1+\delta)I$. Si $t \neq 0$: $X = \lambda I$, $\lambda^2 = 1$, $X = \pm I$. Si $t = 0$: $\delta = -1$, et réciproquement $X^2 = 0 \cdot X + I$. Solutions : $\pm I$ et les $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, $a^2 + bc = 1$, une **infinité** (ex. $\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$). Dans un corps, $(x-1)(x+1) = 0$ force $x = \pm 1$; dans $M_2(\mathbb{R})$, $(X-I)(X+I) = 0$ n'impose pas qu'un facteur soit nul.

■ Corrigé de l'exercice 21

1. $x + x = (x+x)^2 = x^2 + x^2 + x^2 + x^2 = (x+x) + (x+x)$, d'où $x + x = 0$ (régularité dans $(A, +)$) : $-x = x$. Puis $x + y = (x+y)^2 = x + xy + yx + y$ donne $xy = -yx = yx$: **commutatif**.
2. $x(1-x) = x - x^2 = 0$. Si A est intègre : $x = 0$ ou $x = 1$, donc $A = \{0, 1\}$. Si $\mathbb{Z}/n\mathbb{Z}$ est de Boole, $\overline{1} + \overline{1} = \overline{0}$, donc $n \mid 2$; et $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ convient : $n = 2$.
3. $\chi_{X \cap Y}(e) = \overline{1} \iff e \in X \text{ et } e \in Y \iff \chi_X(e)\chi_Y(e) = \overline{1}$; $e \in X \oplus Y \iff e$ est dans un seul des deux ensembles $\iff \chi_X(e) + \chi_Y(e) = \overline{1}$ (car $\overline{1} + \overline{1} = \overline{0}$). Ainsi $\chi_{X \cap Y} = \chi_X \chi_Y$ et $\chi_{X \oplus Y} = \chi_X + \chi_Y$. $X \mapsto \chi_X$ est une bijection de $P(E)$ sur $F(E, \mathbb{Z}/2\mathbb{Z})$ (réciproque : $f \mapsto \{e : f(e) = \overline{1}\}$) qui transforme $\oplus, \cap$ en

$+, \times$: par transport, $(P(E), \oplus, \cap)$ est un anneau commutatif, de zéro $\emptyset$, d'unité E , et $X \cap X = X$: anneau de Boole.

■ Corrigé de l'exercice 22

- On répartit G en paires $\{x, x'\}$ avec $x \neq x'$ et en singletons $\{x\}$ avec $x = x'$, c'est-à-dire $x^2 = e$. Les paires contiennent un nombre pair d'éléments : le nombre de x tels que $x^2 = e$ a la parité de $|G|$, il est pair ; il vaut au moins 1 (e), donc au moins 2.
- Chaque élément est son propre symétrique, d'où $x * y = (x * y)^{-1} = y^{-1} * x^{-1} = y * x$: G est commutatif. $K = H \cup aH$ contient e ; $h * h' \in H$, $h * (a * h') = a * (h * h') \in aH$, $(a * h) * (a * h') = a^2 * h * h' \in H$: K est stable, et $x^{-1} = x$: **sous-groupe**. $H \cap aH = \emptyset$ ($a * h = h'$ donnerait $a = h' * h^{-1} \in H$) et $h \mapsto a * h$ est injective : $|K| = 2|H|$. En partant de $\{e\}$ et en doublant tant que le sous-groupe obtenu n'est pas G (fini), on obtient $|G| = 2^k$.
- Les inversibles sont $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}$, et 25, 49, 121, 169, 289, 361, 529 sont tous $\equiv 1$ [24]. Un groupe à 6 éléments vérifiant $x^2 = e$ pour tout x aurait (2.) un cardinal puissance de 2 : **non**.

■ Corrigé de l'exercice 23

- $1 \in K$, et K est stable par somme et opposé : $\mathbb{Z} \subset K$; puis $\frac{p}{q} = pq^{-1} \in K$: $\mathbb{Q} \subset K$. Si $\sqrt{2} \in K$, $a + b\sqrt{2} \in K$ pour $a, b \in \mathbb{Q}$: $\mathbb{Q}(\sqrt{2}) \subset K$.
- Si $\sqrt{3} = a + b\sqrt{2}$ ($a, b \in \mathbb{Q}$), alors $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Si $ab \neq 0$, $\sqrt{2} \in \mathbb{Q}$; si $b = 0$, $\sqrt{3} \in \mathbb{Q}$; si $a = 0$, $\sqrt{6} = \sqrt{2}\sqrt{3} = 2b \in \mathbb{Q}$: **absurde**. Si $x = a + b\sqrt{2} = c + d\sqrt{3}$ avec $d \neq 0$, alors $\sqrt{3} = \frac{x-c}{d} \in \mathbb{Q}(\sqrt{2})$ (corps) : absurde ; donc $d = 0$ et $x \in \mathbb{Q}$. D'où $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.
- $1 \in L$, L est stable par différence et $(u + v\sqrt{3})(u' + v'\sqrt{3}) = (uu' + 3vv') + (uv' + vu')\sqrt{3} \in L$: sous-anneau. Si $v \neq 0$ et $u^2 = 3v^2$, alors $\pm\sqrt{3} = \frac{u}{v} \in \mathbb{Q}(\sqrt{2})$: absurde ; si $v = 0$, $u \neq 0$. Donc pour $x = u + v\sqrt{3} \neq 0$, $v = u^2 - 3v^2 \in \mathbb{Q}(\sqrt{2})^*$ et $\frac{1}{x} = \frac{u}{v} - \frac{v}{v}\sqrt{3} \in L$: **sous-corps**. Avec $u = 1 + \sqrt{2}$, $v = 1$: $v = 2\sqrt{2}$ et $\frac{1}{1+\sqrt{2}+\sqrt{3}} = \frac{1+\sqrt{2}-\sqrt{3}}{2\sqrt{2}} = \frac{1}{2} + \frac{1}{4}\sqrt{2} + 0\sqrt{3} - \frac{1}{4}\sqrt{6}$.

28

Corrigés du niveau 4

■ Corrigé de l'exercice 24

- $m = nq + r$, $0 \leq r < n$: $a^m = (a^n)^q a^r = a^r$, et $a^r = e$ avec $0 \leq r < n$ impose $r = 0$ (minimalité) : $a^m = e \iff n \mid m$. Ainsi $a^k = a^r$ (r reste de k) : $\{a^k\} = \{e, \dots, a^{n-1}\}$, et $a^i = a^j$ avec $0 \leq i < j < n$ donnerait $a^{j-i} = e$, $0 < j - i < n$. Soient $d = n \wedge k$, $n = dn'$, $k = dk'$, $n' \wedge k' = 1$: $(a^k)^m = e \iff n \mid km \iff n' \mid k'm \iff n' \mid m$ (Gauss) : $\omega(a^k) = \frac{n}{n \wedge k}$.
- $(ab)^{mn} = (a^m)^n (b^n)^m = e$: ab est d'ordre fini r , et $r \mid mn$. $(ab)^r = e$ donne $a^r = b^{-r}$, puis $a^{rn} = (b^n)^{-r} = e$: $m \mid rn$, donc $m \mid r$ (Gauss) ; de même $n \mid r$, et $mn \mid r$ ($m \wedge n = 1$). Donc $\omega(ab) = mn$.
- $A^2 = B^2 = I$, $A, B \neq I$: ordres 2. $AB = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ et $(AB)^n = (-1)^n \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \neq I$ pour $n \geq 1$: **ordre infini**. Sans commutativité, le produit de deux éléments d'ordre fini peut être d'ordre infini : l'hypothèse de 2 est indispensable.

4. $\overline{2}^5 = \overline{32} = \overline{1}$ et $\overline{2} \neq \overline{1}$: $\omega(\overline{2}) = 5$ (5 premier). $5^3 = 125 = 4 \times 31 + 1$: $\omega(\overline{5}) = 3$; $\omega(\overline{-1}) = 2$. Par 2. : $\omega(\overline{10}) = 15$, puis $\omega(\overline{-10}) = \omega(\overline{21}) = 30$. Par 1., $\overline{1}, \overline{21}, \dots, \overline{21}^{29}$ sont 30 éléments distincts : ce sont **tous** les éléments de $(\mathbb{Z}/31\mathbb{Z})^*$, et $\overline{k} \mapsto \overline{21}^k$ est un isomorphisme de $(\mathbb{Z}/30\mathbb{Z}, +)$ sur $((\mathbb{Z}/31\mathbb{Z})^*, \times)$.

■ Corrigé de l'exercice 25

- $h \mapsto xh$ est une bijection de H sur xH (régularité) : $|xH| = |H|$. Si $xh_1 = yh_2$, alors $x = yh_2h_1^{-1}$ et $xh = y(h_2h_1^{-1}h) \in yH$: $xH \subset yH$, et de même $yH \subset xH$. Les xH recouvrent G ($x \in xH$) et sont deux à deux disjoints ou égaux : G est réunion disjointe de k parties à $|H|$ éléments, $|G| = k|H|$.
- G étant fini, $a^i = a^j$ pour certains $i < j$, d'où $a^{j-i} = e$: a est d'ordre fini n , et $\{e, a, \dots, a^{n-1}\}$ est un sous-groupe à n éléments (exercice 24). Lagrange : $n \mid |G|$, donc $a^{|G|} = e$. Si p est premier et $p \nmid a$, $\overline{a}$ appartient au groupe $(\mathbb{Z}/p\mathbb{Z})^*$ à $p-1$ éléments : $\overline{a}^{p-1} = \overline{1}$, soit $a^{p-1} \equiv 1 [p]$.
- $\omega(a) \mid p$ et $\omega(a) \neq 1$: $\omega(a) = p$. Si $k \equiv k' [p]$, $a^k = a^{k'}$: l'application est bien définie ; c'est un morphisme ($a^{k+m} = a^k a^m$), injectif ($a^k = a^m \iff p \mid k-m$), entre deux ensembles à p éléments : **isomorphisme**.
- $2^5 \equiv -5$, $2^6 \equiv -10$, $2^{12} \equiv 100 \equiv 26$, $2^{18} \equiv 26 \times (-10) = -260 = -7 \times 37 - 1 \equiv -1 [37]$. L'ordre de $\overline{2}$ divise $36 = 2^2 \times 3^2$; s'il était < 36 , il diviserait $\frac{36}{2} = 18$ ou $\frac{36}{3} = 12$, et $\overline{2}^{18}$ ou $\overline{2}^{12}$ vaudrait $\overline{1}$. Donc $\omega(\overline{2}) = 36$.

■ Corrigé de l'exercice 26

- $A^1 = u_1 A - u_0 I$; $A^{k+1} = u_k A^2 - u_{k-1} A = u_k (tA - I) - u_{k-1} A = u_{k+1} A - u_k I$. $A^n = I \iff u_n A = (1 + u_{n-1})I$. Si $u_n \neq 0$, $A = \lambda I$; à coefficients entiers et de déterminant $\lambda^2 = 1$, $A = \pm I$: exclu. Donc $u_n = 0$, puis $u_{n-1} = -1$; la réciproque est claire.
- $|u_1| > |u_0|$; si $|u_k| > |u_{k-1}|$, alors $|u_{k+1}| \geq |t||u_k| - |u_{k-1}| > 3|u_k| - |u_k| \geq |u_k|$. Donc $u_n \neq 0$ pour $n \geq 1$: $A^n \neq I$, **ordre infini**. Si $t = 2$, $u_k = k$; si $t = -2$, $u_k = (-1)^{k-1} k$ (récurrences immédiates) : encore $u_n \neq 0$.
- $t = 0$: $(u_k) = 0, 1, 0, -1, 0, \dots$: $u_4 = 0$, $u_3 = -1$, ordre $\boxed{4}$. $t = -1$: $0, 1, -1, 0, \dots$: $u_3 = 0$, $u_2 = -1$, ordre $\boxed{3}$. $t = 1$: $0, 1, 1, 0, -1, -1, 0, \dots$: $u_3 = 0$ mais $u_2 = 1$ ($A^3 = -I$), $u_6 = 0$, $u_5 = -1$: ordre $\boxed{6}$. Avec I (ordre 1) et $-I$ (ordre 2), les ordres finis sont exactement $\boxed{1, 2, 3, 4, 6}$; exemples (exercice 19) : S ($t = 0$), U^2 ($t = -1$), U ($t = 1$).

■ Corrigé de l'exercice 27

$H \neq \{0\}$ contient un $h \neq 0$, et h ou $-h$ est dans H^+ .

- Si $\alpha \notin H$: il existe $h \in H^+$ avec $\alpha < h < 2\alpha$, puis $h' \in H^+$ avec $\alpha < h' < h$; alors $h - h' \in H^+$ et $h - h' < 2\alpha - \alpha = \alpha$: absurde. Donc $\alpha \in H$ et $\alpha\mathbb{Z} \subset H$. Pour $x \in H$ et $k \in \mathbb{E}(\frac{x}{\alpha})$, $r = x - k\alpha \in H \cap [0, \alpha[$; $r > 0$ contredirait la définition de α : $r = 0$, $x = k\alpha$. $H = \alpha\mathbb{Z}$.
- Soient $x < y$ et $h \in H^+$ tel que $h < y - x$. Avec $k \in \mathbb{E}(\frac{x}{h}) + 1$: $(k-1)h \leq x < kh$, donc $x < kh \leq x+h < y$, et $kh \in H$.
- $H = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ est un sous-groupe (exercice 4). Si $H = \alpha\mathbb{Z}$, alors $1 = p\alpha$, $\sqrt{2} = q\alpha$, d'où $\sqrt{2} = \frac{q}{p} \in \mathbb{Q}$: absurde. Donc $\alpha = 0$ et H est **dense**. Si $\frac{\ln 3}{\ln 2} = \frac{p}{q}$ ($p, q \in \mathbb{N}^*$), alors $3^q = 2^p$ (impair = pair) : absurde. De même, $\mathbb{Z} \ln 2 + \mathbb{Z} \ln 3$ n'est pas de la forme $\alpha\mathbb{Z}$: il est dense, et $]\ln x, \ln y[$ contient un $m \ln 2 + n \ln 3$, soit $x < 2^m 3^n < y$. (Ex. : $2^{-19} 3^{12} \approx 1,0136 \in]1; 1,02[$.)

■ Corrigé de l'exercice 28

- $I \in C(A)$; si $M, N \in C(A)$: $A(M - N) = (M - N)A$ et $AMN = MAN = MNA$: **sous-anneau**. Et $A(xI + yA) = xA + yA^2 = (xI + yA)A$.
- $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$: $ME_{12} = \begin{pmatrix} 0 & p \\ 0 & r \end{pmatrix}$, $E_{12}M = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}$ donnent $r = 0$, $p = s$; $ME_{21} = \begin{pmatrix} q & 0 \\ s & 0 \end{pmatrix}$, $E_{21}M = \begin{pmatrix} 0 & 0 \\ p & q \end{pmatrix}$ donnent $q = 0$. Donc $M = pI$; réciproquement λI commute avec tout : le centre est $\boxed{\mathbb{R} \cdot I}$.
- Avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $AM = MA$ s'écrit : $br = cq$, $b(p - s) = q(a - d)$, $c(p - s) = r(a - d)$. Comme $A \neq \lambda I$: si $b \neq 0$, on pose $y = \frac{a}{b}$, $x = p - ya$; alors $r = yc$ et $s = p - y(a - d) = x + yd$, soit $M = xI + yA$; si $c \neq 0$, de même avec $y = \frac{r}{c}$; si $b = c = 0$ et $a \neq d$, alors $q = r = 0$, et $y = \frac{p-s}{a-d}$, $x = p - ya$ conviennent. Avec 1. : $C(A) = \{xI + yA\}$. Ainsi $C(K) = F$, le corps de l'exercice 11, et $C(N) = A$, l'anneau des nombres duaux de l'exercice 14.

■ Corrigé de l'exercice 29

- $(1 - x)(1 + x + \dots + x^{k-1}) = (1 + \dots + x^{k-1})(1 - x) = 1 - x^k = 1$: $\boxed{(1 - x)^{-1} = 1 + x + \dots + x^{k-1}}$; $-x$ est nilpotent, donc $1 + x$ est inversible, d'inverse $\sum (-1)^j x^j$. Si $y^m = 0$ et $xy = yx$: $(xy)^k = x^k y^k = 0$, et dans $(x + y)^{k+m-1} = \sum_j C_{k+m-1}^j x^j y^{k+m-1-j}$ (binôme, licite car $xy = yx$), chaque terme a $j \geq k$ ou $k + m - 1 - j \geq m$: il est nul.
- $N^k = 0$: N n'est pas inversible, $\delta = 0$ et $N^2 = tN$ (exercice 20), d'où $N^k = t^{k-1}N$; si $N \neq 0$, $t = 0$ et $N^2 = 0$. $E_{12}^2 = E_{21}^2 = 0$, mais $(E_{12} + E_{21})^2 = I$: ses puissances valent I ou $E_{12} + E_{21}$, **jamais** 0. Ici $E_{12}E_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq E_{21}E_{12} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$: l'hypothèse $xy = yx$ de 1. est indispensable.
- Si $n \mid x^k$ et si p premier divise n , alors $p \mid x^k$, donc $p \mid x$. Réciproquement, si $n = \prod p_i^{\alpha_i}$ et tous les p_i divisent x , avec $\alpha = \max \alpha_i$, les $p_i^{\alpha_i}$ (premiers entre eux) divisent x^α , donc $n \mid x^\alpha$. $72 = 2^3 \times 3^2$: nilpotents $\boxed{0, \overline{6}, \overline{12}, \dots, \overline{66}}$ (12 éléments). $\overline{7} = \overline{1+6}$, $\overline{6}^3 = \overline{216} = \overline{0}$: $\overline{7}^{-1} = \overline{1-6+36} = \boxed{31}$ ($217 = 3 \times 72 + 1$).

■ Corrigé de l'exercice 30

- K étant fini, $k \cdot 1 = m \cdot 1$ pour certains $k < m$, d'où $(m - k) \cdot 1 = 0$; soit p le plus petit tel entier ($p \geq 2$ car $1 \neq 0$). Si $p = ab$ avec $1 < a, b < p$, alors $(a \cdot 1)(b \cdot 1) = (ab) \cdot 1 = 0$, et, K n'ayant pas de diviseur de zéro, $a \cdot 1 = 0$ ou $b \cdot 1 = 0$: contredit la minimalité. p est **premier**, et $p \cdot x = (p \cdot 1)x = 0$.
- Si $p = 2$: $x + x = 0$ pour tout x , donc dans le groupe $(K, +)$ chaque élément est son propre symétrique : $|K| = 2^k$ (exercice 22, 2.). Si $p \neq 2$: $2 \cdot 1 \neq 0$ ($2 < p$), donc $x + x = (2 \cdot 1)x = 0 \Rightarrow x = 0$; dans $(K, +)$, seul 0 est son propre symétrique, et $|K|$ est **impair** (exercice 22, 1.). 6 et 10 sont pairs sans être des puissances de 2 : **aucun corps** à 6 ou 10 éléments.
- $A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \boxed{I + A}$, $A(I + A) = A + A^2 = I + A + A = \boxed{I}$, $(I + A)^2 = I + A^2 = A$.

+	O	I	A	I+A	×	O	I	A	I+A
O	O	I	A	I+A	O	O	O	O	O
I	I	O	I+A	A	I	O	I	A	I+A
A	A	I+A	O	I	A	O	A	I+A	I
I+A	I+A	A	I	O	I+A	O	I+A	I	A

K_4 est stable ; $(K_4, +)$ est un groupe commutatif ($X + X = O$) ; $\times$ est associative, distributive (calcul matriciel), commutative (table), d'unité I , et $A^{-1} = I + A$: **corps commutatif à 4 éléments**. $A^3 = I$: $\overline{k} \mapsto A^k$ est un isomorphisme de $(\mathbb{Z}/3\mathbb{Z}, +)$ sur $(K_4 \setminus \{O\}, \times)$. Un isomorphisme f de $(\mathbb{Z}/4\mathbb{Z}, +)$ sur $(K_4, +)$ donnerait $f(\overline{2}) = f(\overline{1}) + f(\overline{1}) = O = f(\overline{0})$: absurde.

29

Corrigés : lois internes

■ Corrigé de l'exercice 31

1. **Loi ***. L'expression est symétrique en x, y : $*$ est **commutative**. $1 * 1 = 3$, $(1 * 1) * (-1) = 3 - 1 + 9 = 11$, alors que $1 * (-1) = 1$ et $1 * (1 * (-1)) = 1 * 1 = 3$: $*$ **n'est pas associative**. $x * 0 = x$: **0 est neutre**.
- Loi $\oplus$** . $|x - y| = |y - x|$: commutative. $(3 \oplus 1) \oplus 1 = 2 \oplus 1 = 1$ et $3 \oplus (1 \oplus 1) = 3 \oplus 0 = 3$: non associative. Pour $x \geq 0$, $x \oplus 0 = |x| = x$: 0 est neutre.
- Loi $\odot$** . $i \odot 1 = i$ et $1 \odot i = -i$: non commutative. $(1 \odot 1) \odot i = 1 \odot i = -i$ et $1 \odot (1 \odot i) = 1 \odot (-i) = i$: non associative. $z \odot 1 = z \bar{1} = z$: 1 **est neutre à droite**. Si e était neutre à gauche, $e \bar{w} = w$ pour tout w : $w = 1$ donne $e = 1$, puis $w = i$ donne $-i = i$, absurde. **Pas de neutre**.
- Loi $\otimes$** . $\max(x, y) = \max(y, x)$, et $\max(\max(x, y), z) = \max(x, \max(y, z))$ est le plus grand des trois nombres : commutative et associative. Pour $x \geq 0$, $\max(x, 0) = x$: 0 est neutre.
2. a) La loi est commutative : x est symétrisable $\iff$ il existe y tel que $x^2 y^2 + y + x = 0$. Si $x = 0$: $y = 0$ convient. Si $x \neq 0$: équation du second degré en y , de discriminant $\Delta = 1 - 4x^3$, qui a une solution $\iff x^3 \leq \frac{1}{4} \iff x \leq \frac{1}{\sqrt[3]{4}}$. D'où **x symétrisable $\iff x \leq \frac{1}{\sqrt[3]{4}}$** .
- Pour $x = -1$: $y^2 + y - 1 = 0$, $y = \frac{-1 + \sqrt{5}}{2}$ ou $y = \frac{-1 - \sqrt{5}}{2}$: **deux symétriques**.
- b) $(y + x^2 y^2) - (z + x^2 z^2) = (y - z)[1 + x^2(y + z)]$. Si $x = 0$, $x * y = x * z \Rightarrow y = z$: 0 est régulier. Si $x \neq 0$, on prend $y = 0$ et $z = -\frac{1}{x^2}$: $x * 0 = x = x * (-\frac{1}{x^2})$ avec $0 \neq -\frac{1}{x^2}$: x n'est pas régulier.
3. $\oplus$: $x \oplus x = 0$: chaque x est son propre symétrique. $0 \oplus y = y$, donc 0 est régulier ; si $x > 0$: $x \oplus 0 = x = x \oplus (2x)$ avec $0 \neq 2x$: x n'est pas régulier.
- $\otimes$: $\max(x, x') = 0$ impose $x = x' = 0$: **seul 0 est symétrisable**. De même, si $x > 0$: $\max(x, 0) = x = \max(x, x)$: **seul 0 est régulier**.
- $\odot$: si $z \neq 0$: $z \odot w = z \odot w' \Rightarrow z \bar{w} = z \bar{w}' \Rightarrow w = w'$, et $w \odot z = w' \odot z \Rightarrow w \bar{z} = w' \bar{z} \Rightarrow w = w'$. 0 n'est pas régulier ($0 \odot 1 = 0 \odot i$). **Les éléments réguliers sont ceux de $\mathbb{C}^*$** .
4. Pour une loi **associative**, le symétrique est unique et tout élément symétrisable est régulier. Ici -1 a deux symétriques pour $*$, et 1 est symétrisable sans être régulier pour $\oplus$ (de même -1 pour $*$) : aucune contradiction, car **$ni * ni \oplus$ ne sont associatives**.

loi	commutative	associative	neutre	symétrisables	réguliers
*	oui	non	0	$x \leq 4^{-1/3}$	$\{0\}$
$\oplus$	oui	non	0	tous	$\{0\}$
$\odot$	non	non	aucun (1 à droite)	sans objet	$\mathbb{C}^*$
$\otimes$	oui	oui	0	$\{0\}$	$\{0\}$

■ Corrigé de l'exercice 32

1. a) $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, donc $m - nj = (m + \frac{n}{2}) - i\frac{\sqrt{3}}{2}n$ et $|m - nj|^2 = (m + \frac{n}{2})^2 + \frac{3}{4}n^2 = m^2 + mn + n^2$.
- Soit $N = |m - nj|^2$ et $N' = |m' - n'j|^2$ deux éléments de E . Alors $NN' = |(m - nj)(m' - n'j)|^2$ et, comme $j^2 = -1 - j$: $(m - nj)(m' - n'j) = mm' - (mn' + nm')j + nn'j^2 = M - Pj$ avec $M = mm' - nn' \in \mathbb{Z}$ et $P = mn' + nm' + nn' \in \mathbb{Z}$. Donc $NN' = M^2 + MP + P^2 \in E$: **E est stable pour $\times$** .

- b) $7 = 2^2 + 2 \times 1 + 1^2 = 1^2 + 1 \times 2 + 2^2$ et $13 = 3^2 + 3 \times 1 + 1^2$. La formule de a) donne, avec $(m, n) = (2, 1)$ et $(m', n') = (3, 1)$: $M = 6 - 1 = 5$, $P = 2 + 3 + 1 = 6$, $91 = 5^2 + 5 \times 6 + 6^2$; avec $(m, n) = (1, 2)$ et $(m', n') = (3, 1)$: $M = 3 - 2 = 1$, $P = 1 + 6 + 2 = 9$, $91 = 1^2 + 1 \times 9 + 9^2$ ($25 + 30 + 36 = 1 + 9 + 81 = 91$ ✓).
- c) $1 = 1^2 + 1 \times 0 + 0^2 \in E$, mais $1 + 1 = 2 \notin E$: $4(m^2 + mn + n^2) = (2m + n)^2 + 3n^2 = 8$ impose $n^2 \leq 2$, soit $n \in \{-1, 0, 1\}$; $n = 0$ donne $4m^2 = 8$ et $n = \pm 1$ donne $(2m \pm 1)^2 = 5$: impossible dans $\mathbb{Z}$. **E n'est pas stable pour $+$.**
2. Si $f, g \in F$: $(f \cdot g)(x+1) = f(g(x)+1) = f(g(x))+1$: $f \cdot g \in F$. En revanche $(f+g)(x+1) = (f+g)(x)+2$: avec $f = g = \text{id}$, $f+g = 2 \text{id} \notin F$. Enfin $E(x+1) = E(x)+1$ et $\sin(2\pi(x+1)) = \sin(2\pi x)$, d'où les deux exemples.

■ Corrigé de l'exercice 33

1. $x * y - y * x = (a - b)(x - y)$: il est nul pour tous x, y si et seulement si $a = b$.
2. a) $(x * y) * z = a(ax + by + c) + bz + c = a^2x + aby + bz + ac + c$ et $x * (y * z) = ax + b(ay + bz + c) + c = ax + aby + b^2z + bc + c$. La différence vaut $(a^2 - a)x + (b - b^2)z + (a - b)c$ (y a disparu).
- b) Si les trois conditions sont vraies, la différence est nulle. Réciproquement, si elle est nulle pour tous x, z : $x = z = 0$ donne $(a - b)c = 0$, puis $x = 1, z = 0$ donne $a^2 = a$, et $x = 0, z = 1$ donne $b^2 = b$.
- c) $a, b \in \{0, 1\}$: $x * y = x + y + c$ ($a = b = 1, c$ quelconque) ; $x * y = c$ ($a = b = 0$) ; $x * y = x$ ($a = 1, b = 0$, donc $c = 0$) ; $x * y = y$ ($a = 0, b = 1, c = 0$).
3. Si e est neutre : $e * y = y$ pour tout y s'écrit $(b - 1)y + ae + c = 0$, d'où $b = 1$; de même $x * e = x$ donne $a = 1$, puis $e = -c$. Réciproquement, si $a = b = 1$: $x * (-c) = x - c + c = x = (-c) * x$. **Neutre : $e = -c$.**
- Un groupe exige associativité et neutre, donc $a = b = 1$: $x * y = x + y + c$. Cette loi est associative (question 2) et de neutre $-c$; enfin $x + x' + c = -c \iff x' = -x - 2c$. **Les lois cherchées sont les $x * y = x + y + c$, avec $x' = -x - 2c$: groupes commutatifs.**
4. $a = 3$ et $a^2 \neq a$: **non associative**. Contrôle : $0 * 0 = -2$, $(0 * 0) * 1 = -6 + 3 - 2 = -5$, alors que $0 * 1 = 1$ et $0 * (0 * 1) = 0 * 1 = 1$.

■ Corrigé de l'exercice 34

1. La commutativité est claire. Pour $d \in \mathbb{N}^*$: $d \mid a \wedge (b \wedge c) \iff (d \mid a, d \mid b, d \mid c) \iff d \mid (a \wedge b) \wedge c$. Deux entiers naturels non nuls ayant les mêmes diviseurs se divisent mutuellement, donc sont égaux : $\wedge$ est associative. De même, $a \vee (b \vee c)$ et $(a \vee b) \vee c$ ont les mêmes multiples (les multiples communs de a, b, c), donc sont égaux. Enfin $a \wedge a = a \vee a = a$ (*idempotence*).
2. a) $a \vee 1 = a$: **1 est neutre pour $\vee$** . Si e était neutre pour $\wedge$, on aurait $e \wedge (e + 1) = e + 1$, donc $e + 1 \mid e$ avec $e + 1 > e \geq 1$: impossible.
- b) $a \vee a' = 1$ impose $a \mid 1$: **seul 1 est symétrisable** (et $1' = 1$).
- c) $1 \vee x = x$: **1 est régulier**. Si $a \geq 2$: $a \vee 1 = a = a \vee a$ avec $1 \neq a$. Pour $\wedge$: pour tout a , $a \wedge 1 = 1 = a \wedge (a + 1)$ (deux entiers consécutifs sont premiers entre eux), avec $1 \neq a + 1$: **aucun élément n'est régulier**.
3. a) Les égalités sont symétriques en y, z : supposons $y \leq z$. Alors $\max(y, z) = z$ et $\min(x, y) \leq \min(x, z)$, donc les deux membres de la première valent $\min(x, z)$. De même $\min(y, z) = y$ et $\max(x, y) \leq \max(x, z)$: les deux membres de la seconde valent $\max(x, y)$.

b) Écrivons $a = \prod p_i^{\alpha_i}$, $b = \prod p_i^{\beta_i}$, $c = \prod p_i^{\gamma_i}$ (mêmes nombres premiers, exposants ≥ 0). On sait que $a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}$ et $a \vee b = \prod p_i^{\max(\alpha_i, \beta_i)}$. D'après a) :

$$a \wedge (b \vee c) = \prod p_i^{\min(\alpha_i, \max(\beta_i, \gamma_i))} = \prod p_i^{\max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i))} = (a \wedge b) \vee (a \wedge c),$$

et de même $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ (les lois étant commutatives, la distributivité à droite en découle).

Vérification : $12 \wedge (18 \vee 20) = 12 \wedge 180 = 12$ et $(12 \wedge 18) \vee (12 \wedge 20) = 6 \vee 4 = 12$ ✓ ; $12 \vee (18 \wedge 20) = 12 \vee 2 = 12$ et $(12 \vee 18) \wedge (12 \vee 20) = 36 \wedge 60 = 12$ ✓.

c) $3 \wedge (1 + 2) = 3$, mais $(3 \wedge 1) + (3 \wedge 2) = 2$: **non**.

■ Corrigé de l'exercice 35

1. On développe :

$$(x * y) * z = a(x * y)z + b(x * y) + bz + c = a^2xyz + ab(xy + yz + zx) + b^2(x + y) + acz + bz + bc + c.$$

La loi étant commutative, $x * (y * z) = (z * y) * x$ s'obtient en échangeant x et z . Seuls les termes non symétriques en x, z subsistent dans la différence :

$$(x * y) * z - x * (y * z) = b^2(x - z) + ac(z - x) + b(z - x) = (b^2 - b - ac)(x - z).$$

Si $b^2 - b = ac$, la loi est associative ; réciproquement, $x = 1, z = 0$ donne $b^2 - b - ac = 0$.

2. a) φ est affine de coefficient $a \neq 0$: bijection de réciproque $t \mapsto \frac{t-b}{a}$. Et, avec $b^2 - ac = b$:

$$\varphi(x)\varphi(y) = a^2xy + abx + aby + b^2 = a(axy + bx + by + c) + b^2 - ac = a(x * y) + b = \varphi(x * y).$$

b) Comme φ est bijective, $x * y = \varphi^{-1}(\varphi(x)\varphi(y))$. Posons $e = \varphi^{-1}(1) = \frac{1-b}{a}$: $\varphi(x * e) = \varphi(x)$, donc $x * e = x$. Posons $\omega = \varphi^{-1}(0) = -\frac{b}{a}$: $\varphi(x * \omega) = 0$, donc $x * \omega = \omega$. Enfin $x * x' = e \iff \varphi(x)\varphi(x') = 1$: possible si et seulement si $\varphi(x) \neq 0$, c'est-à-dire $x \neq \omega$, et alors $\varphi(x') = \frac{1}{\varphi(x)}$:

$$e = \frac{1-b}{a}, \quad \omega = -\frac{b}{a}, \quad x' = \frac{1}{a} \left(\frac{1}{ax+b} - b \right) \quad (x \neq \omega).$$

c) Par récurrence, $\varphi(x^{(n+1)}) = \varphi(x^{(n)})\varphi(x) = \varphi(x)^{n+1}$, d'où $\varphi(x^{(n)}) = (ax+b)^n$ et $x^{(n)} = \frac{(ax+b)^n - b}{a}$.

3. a) $a = 2, b = -3, c = 6$: $b^2 - b = 12 = ac$ ✓. $\varphi(x) = 2x - 3$, $e = 2$, $\omega = \frac{3}{2}$, $x' = \frac{1}{2} \left(\frac{1}{2x-3} + 3 \right) = \frac{3x-4}{2x-3}$ ($x \neq \frac{3}{2}$).

b) $x * x * x = 15 \iff \varphi(x)^3 = \varphi(15) = 27 \iff 2x - 3 = 3 \iff x = 3$ ($3 * 3 = 6, 6 * 3 = 36 - 18 - 9 + 6 = 15$ ✓).

c) $x \in [1, 2] \iff \varphi(x) \in [-1, 1]$, et $[-1, 1]$ est stable pour $\times$: donc $[1, 2]$ est stable pour $*$. De même $x > \frac{3}{2} \iff \varphi(x) > 0$: $J =]\frac{3}{2}, +\infty[$ est stable, contient $e = 2$, et si $x \in J$, $\varphi(x') = \frac{1}{\varphi(x)} > 0$, donc $x' \in J$. La loi étant associative, $(J, *)$ **est un groupe commutatif**.

■ Corrigé de l'exercice 36

- Les $N + 1$ éléments $x^1, \dots, x^{N+1}$ de E , qui n'a que N éléments, ne sont pas deux à deux distincts (tiroirs) : il existe $1 \leq p < r \leq N + 1$ tels que $x^p = x^r$. On pose $q = r - p \geq 1$.
- Pour $n > p$: $x^{n+q} = x^{n-p} * x^{p+q} = x^{n-p} * x^p = x^n$; pour $n = p$, c'est l'hypothèse. Donc $x^{n+q} = x^n$ pour tout $n \geq p$, puis, par récurrence sur k , $x^{n+(k+1)q} = x^{(n+kq)+q} = x^{n+kq} = x^n$ (car $n + kq \geq p$).
Avec $n = pq \geq p$ et $k = p$: $y * y = x^{2pq} = x^{pq+pq} = x^{pq} = y$.
- $\bar{x}^2 = \bar{x} \iff 12 \mid x(x-1)$. On teste $x = 0, \dots, 11$: les idempotents sont $\bar{0}, \bar{1}, \bar{4}, \bar{9}$ ($16 \equiv 4, 81 \equiv 9 [12]$).
Pour $\bar{2}$: $\bar{2}, \bar{4}, \bar{8}, \bar{4}, \dots$: $x^4 = x^2$, $p = q = 2$ et $x^4 = \bar{16} = \bar{4}$; pour $\bar{3}$: $\bar{3}, \bar{9}, \bar{3}, \dots$: $x^3 = x^1$, $p = 1$, $q = 2$ et $x^2 = \bar{9}$.
- a) Si $y * y = y$, alors $y * y = y * e$ et, y étant régulier, $y = e$.
b) Soit $x \in E$. D'après 2, x^{pq} est idempotent, donc $x^{pq} = e$. Si $pq = 1$, $x = e$ est son propre symétrique ; sinon $x * x^{pq-1} = x^{pq-1} * x = x^{pq} = e$: x est symétrisable, de symétrique x^{pq-1} . La loi étant associative, avec un neutre, $(E, *)$ est un groupe. (La finitude est indispensable : dans $(\mathbb{N}^*, \times)$, tout élément est régulier, mais 2 n'a pas de symétrique.)
- Si $\bar{a}, \bar{b} \in E$: 11 est premier et ne divise ni a ni b , donc ne divise pas ab : $\bar{a}\bar{b} \in E$. La multiplication est associative, de neutre $\bar{1} \in E$. Si $\bar{a}\bar{b} = \bar{a}\bar{c}$, alors $11 \mid a(b-c)$ avec $11 \nmid a = 1$, donc $11 \mid b-c$ (Gauss) : $\bar{b} = \bar{c}$. Tout élément est régulier et E est fini : d'après 4, $(E, \times)$ est un groupe. Puissances de $\bar{2}$:

$$\bar{2}, \bar{4}, \bar{8}, \bar{5}, \bar{10}, \bar{9}, \bar{7}, \bar{3}, \bar{6}, \bar{1} \quad \text{donc} \quad \bar{2}^{10} = \bar{1} \quad \text{et} \quad \boxed{\bar{2}^{-1} = \bar{2}^9 = \bar{6}} \quad (2 \times 6 = 12 \equiv 1 \checkmark).$$

30

Corrigés : groupes

■ Corrigé de l'exercice 37

- La somme de deux impairs moins 1 est impaire : la loi est interne. $(x \oplus y) \oplus z = x + y + z - 2 = x \oplus (y \oplus z)$ et $x \oplus y = y \oplus x$. $x \oplus 1 = x$: neutre $1 \in I$; $x \oplus (2 - x) = 1$ avec $2 - x$ impair. **Groupe commutatif**, $e = 1$, $x' = 2 - x$.
- $x \oplus y > 0$ et $\frac{1}{x \oplus y} = \frac{1}{x} + \frac{1}{y}$. La loi est commutative, et associative car $\frac{1}{(x \oplus y) \oplus z} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{x \oplus (y \oplus z)}$. Un neutre e vérifierait $\frac{1}{x} + \frac{1}{e} = \frac{1}{x}$, soit $\frac{1}{e} = 0$: impossible. **Pas de neutre, pas un groupe.**
- a) $(-1)^x y = \pm y$ a la parité de y , donc $x + (-1)^x y$ a la parité de $x + y$. Alors

$$(x * y) * z = x + (-1)^x y + (-1)^{x+(-1)^x y} z = x + (-1)^x y + (-1)^{x+y} z = x + (-1)^x (y + (-1)^y z) = x * (y * z).$$

b) $0 * y = y$ et $x * 0 = x$: neutre 0. Si x est pair : $x * (-x) = 0 = (-x) * x$. Si x est impair : $x * x = x - x = 0$. **Groupe, avec $x' = -x$ si x est pair, $x' = x$ si x est impair. Non commutatif** : $1 * 2 = -1$ et $2 * 1 = 3$.
c) $3 * X = 10 \iff X = 3' * 10 = 3 * 10 = \boxed{-7}$ et $X * 3 = 10 \iff X = 10 * 3' = 10 * 3 = \boxed{13}$.
Contrôle : $3 * (-7) = 3 + 7 = 10$, $13 * 3 = 13 - 3 = 10 \checkmark$.

■ Corrigé de l'exercice 38

- a) La ligne de a contient $a * e = a$ et $a * a = b$; $a * b$ et $a * c$ valent donc c et e dans un certain ordre. Si $a * b = e$, alors $a * c = c = e * c$, et $a = e$ par régularité : absurde. Donc $a * b = c$ et $a * c = e$.

b) $c = a * b = a^3$ et $a^4 = a * c = e$: tous les produits se calculent par $a^i * a^j = a^{i+j}$, l'exposant étant pris modulo 4 (table cyclique ci-dessous). Le groupe est **commutatif**.
- $a * b \neq a$ (sinon $b = e$), $a * b \neq b$ (sinon $a = e$), $a * b \neq e$ (sinon $a * b = a * a$ et $b = a$) : $a * b = c$. Le même raisonnement donne $b * a = c$, $a * c = c * a = b$, $b * c = c * b = a$. Ce groupe est aussi commutatif.

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

table cyclique

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

table de Klein

- S'il existe $x \neq e$ tel que $x * x \neq e$, alors $x * x \neq x$ (sinon $x = e$) : en nommant $a = x$, $b = x * x$ et c le quatrième élément, on est dans le cas 1. Sinon, tous les carrés valent e : c'est le cas 2.
- a) On calcule les produits modulo 10 (par exemple $\overline{2} \overline{6} = \overline{12} = \overline{2}$, $\overline{4} \overline{4} = \overline{16} = \overline{6}$) :

$\times$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{4}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{8}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$

La table montre que P est stable ; la multiplication de $\mathbb{Z}/10\mathbb{Z}$ est associative ; la ligne de $\overline{6}$ reproduit l'en-tête : **le neutre est $\overline{6}$** (et non $\overline{1} \notin P$!). Chaque ligne contient $\overline{6}$: tout élément est symétrisable : le symétrique de $\overline{2}$ est $\overline{8}$, celui de $\overline{4}$ est $\overline{4}$. $(P, \times)$ est un groupe, de type **cyclique** : $\overline{2}^2 = \overline{4} \neq \overline{6}$ (avec $a = \overline{2}$, $b = \overline{4}$, $c = \overline{8}$).

- b) Modulo 20 : $9^2 = 81$, $11^2 = 121$ et $19^2 = 361$ sont congrus à 1 ; $9 \times 11 = 99 \equiv 19$, $9 \times 19 = 171 \equiv 11$, $11 \times 19 = 209 \equiv 9$.

$\times$	$\overline{1}$	$\overline{9}$	$\overline{11}$	$\overline{19}$
$\overline{1}$	$\overline{1}$	$\overline{9}$	$\overline{11}$	$\overline{19}$
$\overline{9}$	$\overline{9}$	$\overline{1}$	$\overline{19}$	$\overline{11}$
$\overline{11}$	$\overline{11}$	$\overline{19}$	$\overline{1}$	$\overline{9}$
$\overline{19}$	$\overline{19}$	$\overline{11}$	$\overline{9}$	$\overline{1}$

K est stable (table), la multiplication est associative, $\overline{1} \in K$ est neutre, et chaque élément est son propre symétrique ($x^2 = \overline{1}$) : $(K, \times)$ est un groupe de type **Klein**. On retrouvera K à l'exercice 48 : ce sont exactement les solutions de $x^2 = \overline{1}$ dans $\mathbb{Z}/20\mathbb{Z}$.

■ Corrigé de l'exercice 39

- On écrit $z = re^{i\theta}$, d'où $z^4 = r^4 e^{4i\theta}$.

 - $z^4 \in \mathbb{R}_+^* \iff 4\theta \equiv 0 [2\pi] \iff \theta \equiv 0 \left[\frac{\pi}{2} \right]$: $A = \mathbb{R}^* \cup i\mathbb{R}^*$, réunion des deux axes privés de O .
 $1 \in A$ et, si $z, w \in A$, $(zw^{-1})^4 = \frac{z^4}{w^4} \in \mathbb{R}_+^*$: **sous-groupe**.
 - $z^4 \in \mathbb{R} \iff 4\theta \equiv 0 [\pi] \iff \theta \equiv 0 \left[\frac{\pi}{4} \right]$: B est la réunion des **quatre droites** $y = 0$, $x = 0$, $y = x$, $y = -x$, privées de O . Même calcul : **sous-groupe**.
 - $1 \in C$ et $|zw^{-1}| = \frac{|z|}{|w|} \in \mathbb{Q}$: **sous-groupe**.
 - D est l'ensemble des complexes non nuls à parties réelle et imaginaire rationnelles : $1 \in D$ et, si $z = a + ib$, $w = c + id \in D$, alors $\frac{z}{w} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i \frac{bc-ad}{c^2+d^2} \in D$: **sous-groupe**.

- $i \in F$ et $-1 \in F$, mais $i \times (-1) = -i \notin F$; de plus l'inverse $-i$ de i n'est pas dans F : F n'est pas un sous-groupe.
- 2. a) $e \in H \cap K$, et si $x, y \in H \cap K$, alors $x * y'$ est dans H et dans K .
 b) Si $H \subset K$, $H \cup K = K$ est un sous-groupe (de même si $K \subset H$). Réciproquement, supposons $H \not\subset K$ et $K \not\subset H$: soit $h \in H \setminus K$ et $k \in K \setminus H$. Si $H \cup K$ était un sous-groupe, $h * k \in H \cup K$. Or $h * k \in H$ donnerait $k = h' * (h * k) \in H$, et $h * k \in K$ donnerait $h = (h * k) * k' \in K$: absurde.
 c) $i \in \mathbb{U}_4$, $e^{i\pi/3} \in \mathbb{U}_6$, et $u = i e^{i\pi/3} = e^{5i\pi/6}$: $u^4 = e^{4i\pi/3} \neq 1$ et $u^6 = e^{5i\pi} = -1 \neq 1$, donc $u \notin \mathbb{U}_4 \cup \mathbb{U}_6$.
- 3. $1 \in \mathbb{U}_\infty$, et $\mathbb{U}_\infty \subset \mathbb{U}$ (si $z^n = 1$, $|z|^n = 1$, donc $|z| = 1$). Si $z^n = 1$ et $w^m = 1$, alors $(zw^{-1})^{nm} = (z^n)^m (w^m)^{-n} = 1$: **sous-groupe**. Si $e^i \in \mathbb{U}_\infty$, il existe $n \geq 1$ avec $e^{in} = 1$, donc $n = 2k\pi$, $k \in \mathbb{Z}^*$, et $\pi = \frac{n}{2k} \in \mathbb{Q}$: absurde. Donc $\mathbb{U}_\infty \neq \mathbb{U}$. Pas de contradiction avec 2.b) : $\mathbb{U}_n$ et $\mathbb{U}_m$ sont tous deux contenus dans $\mathbb{U}_{nm}$.

■ Corrigé de l'exercice 40

1. a) Pour tout réel x : $t_a \cdot t_b(x) = x + b + a$, $t_a \cdot \sigma_b(x) = (b - x) + a = \sigma_{a+b}(x)$, $\sigma_a \cdot t_b(x) = a - (x + b) = \sigma_{a-b}(x)$, $\sigma_a \cdot \sigma_b(x) = a - (b - x) = x + (a - b) = t_{a-b}(x)$.
 b) L'image de 0 donne $a = b$ dans les deux premiers cas. Si $t_a = \sigma_b$, les images de 0 et de 1 donnent $a = b$ et $1 + a = b - 1$: absurde.
2. a) D'après 1.a), G est stable par composition ; il contient $\text{id} = t_0$; $t_a \cdot t_{-a} = t_{-a} \cdot t_a = t_0$ et $\sigma_a \cdot \sigma_a = t_0$: $\boxed{t_a^{-1} = t_{-a}}$ et $\boxed{\sigma_a^{-1} = \sigma_a}$. Ainsi G est un sous-groupe du groupe des bijections de $\mathbb{R}$, donc **un groupe. Non commutatif** : $t_1 \cdot \sigma_0 = \sigma_1$ alors que $\sigma_0 \cdot t_1 = \sigma_{-1} \neq \sigma_1$ (d'après 1.b).
 b) $t_a \cdot t_a = t_{2a} = t_0 \iff a = 0$, et $\sigma_a \cdot \sigma_a = \text{id}$ pour tout a : **ce sont id et toutes les symétries σ_a** .
3. T : $\text{id} \in T$ et $t_a \cdot t_b^{-1} = t_{a-b} \in T$: sous-groupe. L'application $a \mapsto t_a$ vérifie $t_{a+b} = t_a \cdot t_b$; elle est surjective sur T et injective (1.b) : **isomorphisme de $(\mathbb{R}, +)$ sur $(T, \cdot)$** .
 H : $t_0 \in H$ et $t_{2k} \cdot t_{2m} = t_{2(k+m)}$, $t_{2k} \cdot \sigma_{2m+1} = \sigma_{2(k+m)+1}$, $\sigma_{2k+1} \cdot t_{2m} = \sigma_{2(k-m)+1}$, $\sigma_{2k+1} \cdot \sigma_{2m+1} = t_{2(k-m)}$; les réciproques t_{-2k} et σ_{2k+1} sont dans H : **sous-groupe de G** .
 Enfin $\sigma_1 \cdot \sigma_0 = t_1$, qui n'est ni l'identité ni une symétrie : $\{\sigma_a\} \cup \{\text{id}\}$ n'est pas stable, ce n'est pas un sous-groupe.
4. a) Si x est pair, $\Phi(x)(y) = t_x(y) = x + y$; s'il est impair, $\Phi(x)(y) = \sigma_x(y) = x - y$: dans les deux cas $\Phi(x)(y) = x + (-1)^x y$. Les entiers pairs sont envoyés sur les t_{2k} et les impairs sur les σ_{2k+1} : Φ est surjective sur H , et injective d'après 1.b). Pour $u \in \mathbb{R}$, comme $x * y$ a la parité de $x + y$ (exercice 37) :

$$\Phi(x) \cdot \Phi(y)(u) = x + (-1)^x (y + (-1)^y u) = x + (-1)^x y + (-1)^{x+y} u = (x * y) + (-1)^{x+y} u = \Phi(x * y)(u).$$

- b) Φ est une bijection de $(\mathbb{Z}, *)$ sur le groupe $(H, \cdot)$ qui transforme $*$ en $\cdot$: par **transport de structure**, $(\mathbb{Z}, *)$ est un groupe et Φ un isomorphisme. Il n'est pas commutatif, car H ne l'est pas : $t_2 \cdot \sigma_1 = \sigma_3 \neq \sigma_1 \cdot t_2 = \sigma_{-1}$, ce qui correspond à $2 * 1 = 3$ et $1 * 2 = -1$.

■ Corrigé de l'exercice 41

- a) $s_{a,b}(s_{c,d}(z)) = a(cz + d) + b = acz + (ad + b)$, avec $ac \neq 0$. Alors $s_{a,b} \circ s_{\frac{1}{a}, -\frac{b}{a}} = s_{1, -b+b} = \text{id}$ et $s_{\frac{1}{a}, -\frac{b}{a}} \circ s_{a,b} = s_{1, \frac{b}{a} - \frac{b}{a}} = \text{id}$: $s_{a,b}$ est bijective et $s_{a,b}^{-1} = s_{\frac{1}{a}, -\frac{b}{a}}$.

b) S est une partie du groupe des bijections de $\mathbb{C}$, contient $\text{id} = s_{1,0}$, est stable par composition et par réciproque : c'est un sous-groupe, donc un groupe. **Non commutatif** : $s_{2,0} \circ s_{1,1} = s_{2,2} \neq s_{1,1} \circ s_{2,0} = s_{2,1}$.

c) Les images de 0 et de 1 donnent $b = d$ et $a + b = c + d$.
- On utilise la caractérisation $f \circ g^{-1}$. $s_{1,b} \circ s_{1,b'}^{-1} = s_{1,b} \circ s_{1,-b'} = s_{1,b-b'} \in T$; $s_{a,0} \circ s_{a',0}^{-1} = s_{\frac{a}{a'}, 0} \in H$; si $|a| = |a'| = 1$, $s_{a,b} \circ s_{a',b'}^{-1} = s_{\frac{a}{a'}, b - \frac{ab'}{a'}}$ avec $\left| \frac{a}{a'} \right| = 1$. Les trois parties contiennent id : **ce sont des sous-groupes**. En revanche, $s_{-1,0}$ et $s_{-1,2}$ sont des demi-tours, mais $s_{-1,0} \circ s_{-1,2} = s_{1,-2}$ est une translation distincte de l'identité : **l'ensemble n'est pas stable, ce n'est pas un sous-groupe**.
- a) $\text{id} \in C(f)$. Si $g, h \in C(f)$: $(g \circ h) \circ f = g \circ f \circ h = f \circ (g \circ h)$, et en composant $h \circ f = f \circ h$ à gauche et à droite par h^{-1} , on obtient $f \circ h^{-1} = h^{-1} \circ f$. $C(f)$ est un sous-groupe.

b) Pour $g = s_{c,d}$: $g \circ t = s_{c,c+d}$ et $t \circ g = s_{c,d+1}$; d'après 1.c), ils sont égaux $\iff c = 1$: $C(t) = T$.
 $g \circ r = s_{ci,d}$ et $r \circ g = s_{ic,id}$: égaux $\iff d = \text{id} \iff d = 0$: $C(r) = H$.

c) Un élément qui commute avec tous les autres est dans $C(t) \cap C(r) = T \cap H = \{s_{1,0}\} = \{\text{id}\}$, et id commute avec tout.

■ Corrigé de l'exercice 42

- $0 \in P_f$. Si $T, T' \in P_f$, pour tout x : $f(x + T - T') = f((x - T') + T) = f(x - T') = f((x - T') + T') = f(x)$: $T - T' \in P_f$. P_f est un sous-groupe de $(\mathbb{R}, +)$.
- a) Si $T \in P_{\cos}$: $\cos T = \cos(0 + T) = \cos 0 = 1$, donc $T \in 2\pi\mathbb{Z}$. Réciproquement, $2\pi \in P_{\cos}$, et le sous-groupe $P_{\cos}$ contient tous les multiples de 2π : $P_{\cos} = 2\pi\mathbb{Z}$.

b) $\cos^2 x = \frac{1 + \cos 2x}{2}$: $T \in P_{\cos^2} \iff \forall x, \cos(2x + 2T) = \cos 2x \iff 2T \in P_{\cos} = 2\pi\mathbb{Z}$ (car $u = 2x$ décrit $\mathbb{R}$) : $P_{\cos^2} = \pi\mathbb{Z}$.

c) $f(x) = x - E(x) \in [0, 1[$. Si $T \in P_f$: $f(T) = f(0) = 0$, donc $T = E(T) \in \mathbb{Z}$. Réciproquement, $E(x + k) = E(x) + k$ pour $k \in \mathbb{Z}$, donc $f(x + k) = f(x)$: $P_f = \mathbb{Z}$.

d) Si $T \in \mathbb{Q}$: $x + T \in \mathbb{Q} \iff x \in \mathbb{Q}$, donc $f(x + T) = f(x)$. Si $T \notin \mathbb{Q}$: $f(0 + T) = 0 \neq f(0) = 1$: $P_{1_0} = \mathbb{Q}$.
- a) $\varphi(T) = \varphi(0 + T) = \varphi(0) = 2$. Comme $\cos \frac{\pi T}{2} \leq 1$ et $\cos \frac{\pi T}{5} \leq 1$, la somme ne vaut 2 que si les deux cosinus valent 1.

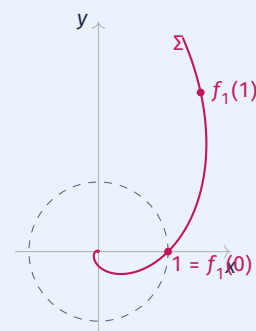
b) $\cos \frac{\pi T}{2} = 1 \iff \frac{\pi T}{2} \in 2\pi\mathbb{Z} \iff T \in 4\mathbb{Z}$, et de même $\cos \frac{\pi T}{5} = 1 \iff T \in 10\mathbb{Z}$: $P_\varphi \subset 4\mathbb{Z} \cap 10\mathbb{Z}$. Réciproquement, 4 est une période de $x \mapsto \cos \frac{\pi x}{2}$ et 10 une période de $x \mapsto \cos \frac{\pi x}{5}$; d'après 1, tout élément de $4\mathbb{Z} \cap 10\mathbb{Z}$ est période des deux termes, donc de φ . Ainsi $P_\varphi = 4\mathbb{Z} \cap 10\mathbb{Z}$.
 Si $T = 4k = 10m$ ($k, m \in \mathbb{Z}$), alors $2k = 5m$: 5 divise $2k$ et $5 \wedge 2 = 1$, donc $5 \mid k$ (Gauss) et $T \in 20\mathbb{Z}$. Réciproquement $20 = 4 \times 5 = 10 \times 2$: $P_\varphi = 20\mathbb{Z}$.
- Si $T \in P_\psi$: $\psi(T) = \psi(0) = 2$, donc (comme en 3.a) $\cos T = \cos(\sqrt{2}T) = 1$: $T = 2k\pi$ et $\sqrt{2}T = 2m\pi$ avec $k, m \in \mathbb{Z}$. Si $T \neq 0$, alors $k \neq 0$ et $\sqrt{2} = \frac{m}{k} \in \mathbb{Q}$: absurde. Donc $P_\psi = \{0\}$.

31

Corrigés : morphismes

■ Corrigé de l'exercice 43

1. a) $f_1(t+t') = e^{(1+i)t} e^{(1+i)t'} = f_1(t)f_1(t') : \text{morphisme. } |f_1(t)| = e^t, \text{ donc } f_1(t) = 1 \Rightarrow t = 0 : N_{f_1} = \{0\},$
injectif. Image : Σ . Non surjectif : $-1 \notin \Sigma$ (si $e^{(1+i)t} = -1$, alors $e^t = 1, t = 0$, et $f_1(0) = 1$). Donc f_1 est un isomorphisme de $(\mathbb{R}, +)$ sur $(\Sigma, \times)$.
 - b) Pour $z = x + iy$ et $w = x' + iy' : e^{z+w} = e^{x+x'} e^{i(y+y')} = e^x e^{iy} e^{x'} e^{iy'} = e^z e^w : \text{morphisme. } |e^z| = e^x$
et e^{iy} est un argument : $e^z = 1 \iff (x = 0 \text{ et } y \in 2\pi\mathbb{Z}), N_{f_2} = 2i\pi\mathbb{Z}, \text{ non injectif. Tout } w \in \mathbb{C}^*$
s'écrit $re^{i\theta} = e^{\ln r + i\theta} : \text{surjectif.}$
 - c) $(-1)^{k+l} = (-1)^k (-1)^l : \text{morphisme, } N_{f_3} = 2\mathbb{Z}, \text{ image } \{-1, 1\} : \text{ni injectif, ni surjectif.}$
 - d) Si $z = re^{i\theta}, \bar{z} = e^{-2i\theta}$, et $\frac{\bar{z}w}{zw} = \frac{\bar{z}}{z} \cdot \frac{w}{\bar{w}} : \text{morphisme. } e^{-2i\theta} = 1 \iff \theta \equiv 0 [\pi] : N_{f_4} = \mathbb{R}^*, \text{ non}$
injectif. L'image est contenue dans $\mathbb{U}$ et $e^{i\alpha} = f_4(e^{-i\alpha/2}) : \text{image } \mathbb{U}, \text{ non surjectif sur } \mathbb{C}^*.$
2. L'image d'un groupe par un morphisme est un sous-groupe : $\Sigma = f_1(\mathbb{R})$ **est un sous-groupe de $(\mathbb{C}^*, \times)$.** Les noyaux sont des sous-groupes : $2i\pi\mathbb{Z} = N_{f_2}$ est un sous-groupe de $(\mathbb{C}, +)$, $\mathbb{R}^* = N_{f_4}$ un sous-groupe de $(\mathbb{C}^*, \times)$, et $2\mathbb{Z} = N_{f_3}$ un sous-groupe de $(\mathbb{Z}, +)$.
- Le point $f_1(t)$ a pour module e^t et pour argument $t : \Sigma$ est une **spirale logarithmique**, qui tourne indéfiniment autour de O quand $t \rightarrow -\infty$ et ne coupe le cercle unité qu'au point $1 (N_{f_1} = \{0\})$.



■ Corrigé de l'exercice 44

1. Pour $x, y \in I, \tan x + \tan y \in \mathbb{R}$ et $\arctan$ prend ses valeurs dans I : la loi est interne. $\tan$ est continue et strictement croissante sur I , de limites $-\infty$ et $+\infty$ aux bornes : c'est une bijection de I sur $\mathbb{R}$, de réciproque $\arctan$. Enfin $\tan(x * y) = \tan(\arctan(\tan x + \tan y)) = \tan x + \tan y$.
2. $\tan$ est une bijection de $(I, *)$ sur le groupe commutatif $(\mathbb{R}, +)$ telle que $\tan(x * y) = \tan x + \tan y$: par transport de structure, $(I, *)$ **est un groupe commutatif et $\tan$ est un isomorphisme.** Neutre : $\tan e = 0, \boxed{e = 0}$; symétrique : $\tan x' = -\tan x = \tan(-x), \boxed{x' = -x}$.
3. $\frac{\pi}{4} * \frac{\pi}{4} = \boxed{\arctan 2}$. Par récurrence, $\tan(x^{(n)}) = n \tan x$, donc $x^{(n)} = \arctan(n \tan x)$.
4. $x * x * x = \frac{\pi}{4} \iff 3 \tan x = 1 \iff \boxed{x = \arctan \frac{1}{3}}$.
5. H est l'image du sous-groupe $\mathbb{Z}$ de $(\mathbb{R}, +)$ par l'isomorphisme $\arctan$: c'est un sous-groupe. Si $x, y \in J, \tan x + \tan y \geq 0$, donc $x * y \in J$: J est stable ; mais le symétrique $-\frac{\pi}{4}$ de $\frac{\pi}{4} \in J$ n'est pas dans J : **ce n'est pas un sous-groupe.**

■ Corrigé de l'exercice 45

1. Pour $x, y \in I$: $xy > 0$ et $(1-x)(1-y) > 0$, donc le dénominateur est strictement supérieur au numérateur, lui-même strictement positif : $0 < x * y < 1$.

f est continue, $f'(x) = \frac{1}{(1-x)^2} > 0$, $\lim_0 f = 0$ et $\lim_{1-} f = +\infty$: bijection de I sur $]0, +\infty[$. Et

$$f(x) = t \iff x = t(1-x) \iff x = \frac{t}{1+t} : \boxed{f^{-1}(t) = \frac{t}{1+t}}. \text{ Comme } 1 - x * y = \frac{(1-x)(1-y)}{xy + (1-x)(1-y)} :$$

$$f(x * y) = \frac{x * y}{1 - x * y} = \frac{xy}{(1-x)(1-y)} = f(x)f(y).$$

2. Par transport de structure (vers le groupe commutatif $(\mathbb{R}_+^*, \times)$), $(I, *)$ **est un groupe commutatif et f est un isomorphisme**. Neutre : $f(e) = 1$, $\boxed{e = \frac{1}{2}}$. Symétrique : $f(x') = \frac{1}{f(x)} = \frac{1-x}{x} = f(1-x)$, $\boxed{x' = 1-x}$ (contrôle : $x * (1-x) = \frac{x(1-x)}{2x(1-x)} = \frac{1}{2}$ ✓).

3. Par récurrence, $f(x^{(n)}) = f(x)^n = \frac{x^n}{(1-x)^n}$, d'où $x^{(n)} = f^{-1}\left(\frac{x^n}{(1-x)^n}\right) = \frac{x^n}{x^n + (1-x)^n} = \frac{1}{1+q^n}$ avec $q = \frac{1-x}{x} > 0$.

$$\lim_{n \rightarrow +\infty} x^{(n)} = 1 \text{ si } x > \frac{1}{2} \ (0 < q < 1); \quad \frac{1}{2} \text{ si } x = \frac{1}{2}; \quad 0 \text{ si } x < \frac{1}{2} \ (q > 1).$$

$$\text{Enfin } x * x * x = \frac{8}{9} \iff f(x)^3 = f\left(\frac{8}{9}\right) = 8 \iff f(x) = 2 \iff \boxed{x = \frac{2}{3}}.$$

4. $\mathbb{Q}_+^*$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$; son image par l'isomorphisme f^{-1} est un sous-groupe de $(I, *)$. Or cette image est $\mathbb{Q} \cap I$: si $t \in \mathbb{Q}_+^*$, $\frac{t}{1+t} \in \mathbb{Q} \cap I$; si $x \in \mathbb{Q} \cap I$, $x = f^{-1}(f(x))$ avec $f(x) = \frac{x}{1-x} \in \mathbb{Q}_+^*$.

■ Corrigé de l'exercice 46

1. D'après les règles de calcul sur les puissances (cours), $a^{k+l} = a^k * a^l$ pour $k, l \in \mathbb{Z}$: φ_a est un morphisme, et $\varphi_a(1) = a$. Si φ est un morphisme tel que $\varphi(1) = a$: $\varphi(0) = e$, puis par récurrence $\varphi(k+1) = \varphi(k) * \varphi(1) = a^{k+1}$ pour $k \geq 0$, et $\varphi(-k) = \varphi(k)' = a^{-k}$: $\varphi = \varphi_a$.
2. Dans $(\mathbb{Z}, +)$, la « puissance » a^k s'écrit ka : les morphismes sont les $\boxed{k \mapsto mk}$, $m \in \mathbb{Z}$. Si $k \mapsto mk$ est bijectif, 1 a un antécédent : $mk = 1$, donc $m = \pm 1$. **Les isomorphismes sont id et -id.**
3. a) Si $\omega^n = 1$ et $l = k + qn$, alors $\omega^l = \omega^k (\omega^n)^q = \omega^k$: la valeur ne dépend pas du représentant. Réciproquement, $\overline{0} = \overline{n}$ impose $\omega^0 = \omega^n$, soit $\omega^n = 1$.
- b) $\psi_\omega(\overline{k+l}) = \psi_\omega(\overline{k+l}) = \omega^{k+l} = \omega^k \omega^l$.
- c) Soit ψ un morphisme et $\omega = \psi(\overline{1})$. Pour $k \geq 1$, $\overline{k} = \overline{1} + \dots + \overline{1}$, donc $\psi(\overline{k}) = \omega^k$ (et $\psi(\overline{0}) = 1 = \omega^0$). Comme $\overline{n} = \overline{0}$, $\omega^n = 1$: $\psi = \psi_\omega$ avec $\omega \in \mathbb{U}_n$. Deux ω distincts donnent des morphismes distincts ($\psi_\omega(\overline{1}) = \omega$) : **il y a exactement n morphismes.**
4. a) $\psi_\omega(\overline{m}) = 1 \iff e^{2ikm\pi/n} = 1 \iff n \mid km$. Si $k \wedge n = 1$, $n \mid km \Rightarrow n \mid m$ (Gauss), donc $\overline{m} = \overline{0}$: noyau trivial, ψ_ω injectif. Si $d = k \wedge n \geq 2$, $m = \frac{n}{d}$ vérifie $km = \frac{k}{d}n$, donc $\psi_\omega(\overline{m}) = 1$ avec $\overline{m} \neq \overline{0}$ ($0 < m < n$) : non injectif.
- b) ψ_ω prend ses valeurs dans $\mathbb{U}_n$ (car $(\omega^m)^n = 1$) ; injectif entre deux ensembles à n éléments, il est bijectif : **isomorphisme sur $\mathbb{U}_n$.**
- c) $k \in \{0, \dots, 11\}$ et $k \wedge 12 = 1$: $k \in \{1, 5, 7, 11\}$: **4 isomorphismes**, $\overline{m} \mapsto e^{ikm\pi/6}$.

■ Corrigé de l'exercice 47

- $\text{ch}^2 t - \text{sh}^2 t = \frac{(e^t + e^{-t})^2 - (e^t - e^{-t})^2}{4} = \frac{4e^t e^{-t}}{4} = 1$, et $\text{ch} t > 0$, donc $\sqrt{1 + \text{sh}^2 t} = \sqrt{\text{ch}^2 t} = \text{ch} t$. Ensuite $\text{sh} s \text{ch} t + \text{ch} s \text{sh} t = \frac{1}{4} [(e^s - e^{-s})(e^t + e^{-t}) + (e^s + e^{-s})(e^t - e^{-t})] = \frac{1}{4} [2e^{s+t} - 2e^{-s-t}] = \text{sh}(s+t)$.
- a) sh est dérivable, $\text{sh}' = \text{ch} > 0$, et ses limites en $\pm\infty$ sont $\pm\infty$: bijection de $\mathbb{R}$ sur $\mathbb{R}$. Pour $x \in \mathbb{R}$, avec $u = e^t > 0$: $\text{sh} t = x \iff u^2 - 2xu - 1 = 0 \iff u = x + \sqrt{x^2 + 1}$ (l'autre racine, $x - \sqrt{x^2 + 1}$, est négative). Comme $\sqrt{1 + x^2} > |x|$, $x + \sqrt{1 + x^2} > 0$ et $t = \ln(x + \sqrt{1 + x^2}) = \varphi(x)$.
 b) D'après 1 : $(\text{sh} s) * (\text{sh} t) = \text{sh} s \text{ch} t + \text{sh} t \text{ch} s = \text{sh}(s+t)$. Avec $s = \varphi(x)$, $t = \varphi(y)$: $x * y = \text{sh}(\varphi(x) + \varphi(y))$, donc $\boxed{\varphi(x * y) = \varphi(x) + \varphi(y)}$.
- φ est une bijection de $(\mathbb{R}, *)$ sur le groupe commutatif $(\mathbb{R}, +)$ qui transforme $*$ en $+$: par transport de structure, $(\mathbb{R}, *)$ **est un groupe commutatif, isomorphe à $(\mathbb{R}, +)$ par φ** . Neutre $\text{sh} 0 = \boxed{0}$; symétrique $\text{sh}(-\varphi(x)) = \boxed{-x}$ (sh est impaire ; contrôle : $x * (-x) = 0$).
- a) $1 * 1 = 2\sqrt{2}$. $\frac{3}{4} + \sqrt{1 + \frac{9}{16}} = \frac{3}{4} + \frac{5}{4} = 2$, donc $\varphi\left(\frac{3}{4}\right) = \ln 2$.
 b) Par récurrence, $\varphi(x^{(n)}) = n\varphi(x)$, d'où $x^{(n)} = \text{sh}(n\varphi(x))$ et
$$\left(\frac{3}{4}\right)^{(n)} = \text{sh}(n \ln 2) = \boxed{\frac{2^n - 2^{-n}}{2}} \quad \left(\text{contrôle pour } n = 2 : \frac{15}{8} = 2 \cdot \frac{3}{4} \cdot \frac{5}{4} = \frac{3}{4} * \frac{3}{4} \checkmark\right).$$
 c) $x * x = \frac{4}{3} \iff 2\varphi(x) = \varphi\left(\frac{4}{3}\right) = \ln\left(\frac{4}{3} + \frac{5}{3}\right) = \ln 3 \iff \varphi(x) = \ln \sqrt{3} \iff x = \text{sh}(\ln \sqrt{3}) = \frac{\sqrt{3} - \frac{1}{\sqrt{3}}}{2} = \boxed{\frac{\sqrt{3}}{3}}$. Contrôle : $2 \cdot \frac{\sqrt{3}}{3} \cdot \frac{2}{\sqrt{3}} = \frac{4}{3} \checkmark$.
- $x + \sqrt{1 + x^2} = e^{\varphi(x)}$: composée de l'isomorphisme φ de $(\mathbb{R}, *)$ sur $(\mathbb{R}, +)$ et de l'isomorphisme $\exp$ de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$, c'est un **isomorphisme**.

■ Corrigé de l'exercice 48

- a) Si G est commutatif et $y_1 = f(x_1)$, $y_2 = f(x_2)$: $y_1 \otimes y_2 = f(x_1 * x_2) = f(x_2 * x_1) = y_2 \otimes y_1$. On applique ce résultat à l'isomorphisme f^{-1} pour la réciproque.
 b) Par récurrence, $f(x^{(n)}) = f(x)^{(n)}$; et f étant injective avec $f(e) = e'$, $x^{(n)} = e \iff f(x^{(n)}) = e' \iff f(x)^{(n)} = e'$. Donc $f(A_n) \subset A'_n$, et de même $f^{-1}(A'_n) \subset A_n$: **f réalise une bijection de A_n sur A'_n** . En particulier, si l'un est fini, ils ont le même nombre d'éléments.
 c) Si $y' \in G'$, on écrit $f^{-1}(y') = x * x$; alors $y' = f(x) \otimes f(x)$.
- On cherche à chaque fois un invariant qui diffère.
 - Dans $(\mathbb{U}, \times)$, $A_4 = \mathbb{U}_4$ a 4 éléments ; dans $(\mathbb{R}, +)$, $4x = 0 \iff x = 0$: $A_4 = \{0\}$.
 - Dans $\mathbb{C}^*$, $A_4 = \mathbb{U}_4$ a 4 éléments ; dans $\mathbb{R}^*$, $A_4 = \{-1, 1\}$ en a 2.
 - Dans $(\mathbb{Q}, +)$, tout élément est un « carré » : $y = \frac{y}{2} + \frac{y}{2}$. Dans $(\mathbb{Z}, +)$, $1 = x + x$ est impossible. Un isomorphisme de $\mathbb{Z}$ sur $\mathbb{Q}$ aurait une réciproque, isomorphisme de $\mathbb{Q}$ sur $\mathbb{Z}$, contredisant 1.c).
 - Même invariant : dans $(\mathbb{Q}_+^*, \times)$, 2 n'est pas le carré d'un rationnel ($\sqrt{2} \notin \mathbb{Q}$), alors que tout élément de $(\mathbb{Q}, +)$ est un « carré ». (Dans $\mathbb{R}$, $\ln$ est un isomorphisme : ce qui manque dans $\mathbb{Q}$, ce sont les racines carrées.)
 - $(\mathbb{Z}, +)$ est commutatif, $(\mathbb{Z}, *)$ ne l'est pas ($1 * 2 = -1$, $2 * 1 = 3$) : 1.a) conclut.

3. a) $\bar{a}$ est inversible dans $\mathbb{Z}/20\mathbb{Z}$ si et seulement si $a \wedge 20 = 1$ (cours) : $G_{20} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{17}, \bar{19}\}$, 8 éléments. Les inversibles d'un anneau forment un groupe pour $\times$ (cours), commutatif ici. Carrés modulo 20 :

$$3^2 \equiv 7^2 \equiv 13^2 \equiv 17^2 \equiv 9 \quad \text{et} \quad 1^2 \equiv 9^2 \equiv 11^2 \equiv 19^2 \equiv 1 \pmod{20},$$

donc $x^2 = \bar{1} \iff x \in K = \{\bar{1}, \bar{9}, \bar{11}, \bar{19}\}$ (4 solutions, le groupe de Klein de l'exercice 38).

b) D'après l'exercice 46 (avec $n = 8, k = 1$), $\bar{m} \mapsto e^{im\pi/4}$ est un isomorphisme de $(\mathbb{Z}/8\mathbb{Z}, +)$ sur $(\mathbb{U}_8, \times)$. Dans $\mathbb{U}_8, z^2 = 1 \iff z = \pm 1 : A_2$ a 2 éléments (dans $\mathbb{Z}/8\mathbb{Z} : 2x = \bar{0} \iff x \in \{\bar{0}, \bar{4}\}$), contre 4 dans G_{20} . D'après 1.b), **ni $\mathbb{Z}/8\mathbb{Z}$ ni $\mathbb{U}_8$ ne sont isomorphes à G_{20}** : avoir le même nombre d'éléments et être commutatifs ne suffit pas.

32

Corrigés : anneaux et corps

■ Corrigé de l'exercice 49

1. $1 \in \mathbb{Z}[i]$; si $z = a+ib$ et $z' = a'+ib'$ sont dans $\mathbb{Z}[i]$, alors $z+z', -z$ et $zz' = (aa'-bb')+i(ab'+a'b)$ aussi. Les lois de $\mathbb{C}$ induisent donc sur $\mathbb{Z}[i]$ une structure d'anneau (**sous-anneau** de $\mathbb{C}$), commutatif et unitaire comme $\mathbb{C}$; et si $zz' = 0$, alors $z = 0$ ou $z' = 0$ (c'est vrai dans $\mathbb{C}$) : **$\mathbb{Z}[i]$ est un anneau commutatif unitaire intègre.**
2. $N(a+ib) = a^2 + b^2 \in \mathbb{N}$, et $N(zz') = |zz'|^2 = |z|^2 |z'|^2 = N(z)N(z')$.
3. Si $zz' = 1$ avec $z' \in \mathbb{Z}[i]$, alors $N(z)N(z') = 1$ dans $\mathbb{N}$, donc $N(z) = 1$. Réciproquement, si $N(z) = 1$, alors $z\bar{z} = 1$ avec $\bar{z} = a-ib \in \mathbb{Z}[i]$: z est inversible. Or $a^2 + b^2 = 1$ avec a, b entiers impose $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$: **les inversibles de $\mathbb{Z}[i]$ sont $1, -1, i, -i$ ($\mathbb{U}_4$).** **$\mathbb{Z}[i]$ n'est pas un corps** : $N(2) = 4 \neq 1$, donc 2 n'est pas inversible.

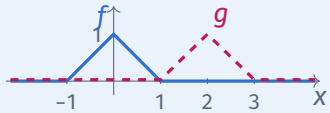
■ Corrigé de l'exercice 50

1. Si $a = 2k$ et $b = 2l$, alors $a \odot b = 2kl \in 2\mathbb{Z}$: la loi est interne. Elle est commutative, associative $((a \odot b) \odot c = \frac{abc}{4} = a \odot (b \odot c))$ et distributive $(a \odot (b+c) = \frac{ab+ac}{2} = a \odot b + a \odot c)$. Enfin $a \odot e = a$ pour tout $a \iff \frac{e}{2} = 1$: le neutre est $\boxed{2} \in 2\mathbb{Z}$. Comme $(2\mathbb{Z}, +)$ est un groupe commutatif, **$(2\mathbb{Z}, +, \odot)$ est un anneau commutatif unitaire**, d'unité 2.
2. f est bijective (réciproque $n \mapsto 2n$), $f(a+b) = f(a) + f(b)$ et $f(a \odot b) = \frac{ab}{4} = f(a)f(b)$: c'est un **isomorphisme d'anneaux** de $(2\mathbb{Z}, +, \odot)$ sur $(\mathbb{Z}, +, \times)$. Si $a \odot b = 0$, alors $f(a)f(b) = 0$, donc $f(a) = 0$ ou $f(b) = 0$, c'est-à-dire $a = 0$ ou $b = 0$: l'anneau est **intègre**. De même $a \odot b = 2 \iff f(a)f(b) = f(2) = 1$: les inversibles sont les a tels que $f(a) = \pm 1$, soit $\boxed{2 \text{ et } -2}$. Ce n'est **pas un corps** (4 n'est pas inversible).
3. a) $3x = 12 \iff \boxed{x = 4}$. b) $2x = 10 \iff x = 5 \notin 2\mathbb{Z}$: **pas de solution**. c) $x^2 = 36 \iff \boxed{x = \pm 6}$. d) $x \odot x \odot x = \frac{x^3}{4} = -16 \iff x^3 = -64 \iff \boxed{x = -4}$.
4. Supposons qu'une telle h existe, et soit $u = h^{-1}(1) \in 2\mathbb{Z}$. Pour tout $a \in 2\mathbb{Z}$: $h(ua) = h(u)h(a) = h(a)$, donc $ua = a$ (h est injective) ; avec $a = 2$: $u = 1 \notin 2\mathbb{Z}$, contradiction. Les anneaux $(2\mathbb{Z}, +, \times)$ et $(\mathbb{Z}, +, \times)$ **ne sont pas isomorphes** : le second a une unité, le premier non. Pourtant f , additive et bijective, est un **isomorphisme de groupes** de $(2\mathbb{Z}, +)$ sur $(\mathbb{Z}, +)$: seule la multiplication distingue ces anneaux, et la question 2 montre qu'il suffit de la « corriger ».

■ Corrigé de l'exercice 51

- $1 = \frac{1}{10^0} \in \mathbb{D}$. Si $x = \frac{a}{10^n}$ et $y = \frac{b}{10^m}$: $x + y = \frac{a10^m + b10^n}{10^{n+m}}$, $xy = \frac{ab}{10^{n+m}}$ et $-x = \frac{-a}{10^n}$ sont dans $\mathbb{D}$: $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$, intègre car $\mathbb{Q}$ l'est.
- ($\Leftarrow$) Si $q = 2^\alpha 5^\beta$ et $m = \max(\alpha, \beta)$, alors $x = \frac{p2^{m-\alpha}5^{m-\beta}}{10^m} \in \mathbb{D}$. ($\Rightarrow$) Si $\frac{p}{q} = \frac{a}{10^n}$, alors $q \mid p10^n$; comme $q \wedge p = 1$, le théorème de Gauss donne $q \mid 10^n = 2^n 5^n$, d'où $q = 2^\alpha 5^\beta$.
 $\frac{7}{40} = 0,175 \in \mathbb{D}$ ($40 = 2^3 \times 5$) ; $\frac{3}{12} = \frac{1}{4} = 0,25 \in \mathbb{D}$ (il faut d'abord simplifier !) ; $\frac{5}{12}$ est irréductible et $3 \nmid 12$: $\frac{5}{12} \notin \mathbb{D}$.
- Si $x = \pm 2^\alpha 5^\beta$ ($\alpha, \beta \in \mathbb{Z}$), x et $\frac{1}{x} = \pm 2^{-\alpha} 5^{-\beta}$ ont des formes irréductibles dont les dénominateurs sont de la forme $2^\gamma 5^\delta$: ils sont dans $\mathbb{D}$, et x est inversible. Réciproquement, si $x = \pm \frac{p}{q}$ (irréductible, $p, q \in \mathbb{N}^*$) est inversible, alors $q = 2^\alpha 5^\beta$ et $\frac{1}{x} = \pm \frac{q}{p}$ étant aussi dans $\mathbb{D}$ et irréductible, $p = 2^\gamma 5^\delta$: $x = \pm 2^{\gamma-\alpha} 5^{\delta-\beta}$. Donc $\text{inversibles de } \mathbb{D} = \{\pm 2^\alpha 5^\beta, (\alpha, \beta) \in \mathbb{Z}^2\}$.
 $0,8 = 2^2 \times 5^{-1}$ a pour inverse $\frac{5}{4} = 1,25$; $0,016 = \frac{2}{125}$ a pour inverse $\frac{125}{2} = 62,5$. $\mathbb{D}$ n'est pas un corps : $\frac{1}{3} \notin \mathbb{D}$.

■ Corrigé de l'exercice 52

- Si $fg = 1$, alors $f(x)g(x) = 1$, donc f ne s'annule pas. Réciproquement, si f ne s'annule pas, $\frac{1}{f} \in C$ et $f \times \frac{1}{f} = 1$. Une telle f garde un **signe constant** : sinon elle s'annulerait (théorème des valeurs intermédiaires).
- a) f est un « chapeau » de sommet $(0, 1)$, nul hors de $]-1, 1[$; g est le même chapeau translaté, de sommet $(2, 1)$, nul hors de $]1, 3[$. Si $x \notin]-1, 1[$, $f(x) = 0$; sinon $|x - 2| > 1$ et $g(x) = 0$. Donc $fg = \theta$ avec $f \neq \theta$, $g \neq \theta$: C n'est pas intègre.

- b) Avec $c = \frac{a+b}{2}$ et $r = \frac{b-a}{2}$, la fonction $g(x) = \max(0, r - |x - c|)$ est continue, > 0 sur $]a, b[$ et nulle ailleurs. Pour tout x : si $x \in]a, b[$, $f(x) = 0$; sinon $g(x) = 0$. Donc $fg = \theta$ avec $g \neq \theta$: f est un **diviseur de zéro**.
- c) Soit x_0 tel que $g(x_0) \neq 0$. Par continuité, g ne s'annule pas sur un intervalle $]x_0 - \eta, x_0 + \eta[$ ($\eta > 0$), où f est donc nulle. Bilan :

$f \neq \theta$ est un diviseur de zéro $\iff f$ est nulle sur un intervalle ouvert non vide.

Les fonctions $x \mapsto x^2 - 1$ et $\sin$ ne s'annulent qu'en des points isolés : **ce ne sont pas des diviseurs de zéro** (sans être inversibles !).

■ Corrigé de l'exercice 53

- $z\bar{z} = (a + bi)(a - bi) = (a^2 + b^2) + (-ab + ba)i = N(z)$. Avec $z' = c + di$: $N(zz') = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(z)N(z')$, les doubles produits $\mp 2abcd$ s'éliminant.
- Supposons que $x^2 = -1$ n'ait pas de solution, et soit $z = a + bi \neq 0$. Si l'on avait $N(z) = 0$, alors $b \neq 0$ (sinon $a^2 = 0$, $a = 0$ et $z = 0$), et $(ab^{-1})^2 = -b^2b^{-2} = -1$: contradiction. Donc $N(z) \neq 0$ et $z \times N(z)^{-1}\bar{z} = 1$: K_p est un corps. Réciproquement, si $x_0^2 = -1$, alors $(x_0 + i)(x_0 - i) = x_0^2 + 1 = 0$ avec $x_0 \pm i \neq 0$: K_p n'est pas un corps.

3. Dans $\mathbb{Z}/3\mathbb{Z}$, les carrés sont 0 et 1 ; $-1 = 2$ n'en est pas un : K_3 **est un corps à 9 éléments**.
 $N(1+i) = 2$ et $2^{-1} = 2$, donc $(1+i)^{-1} = 2(1-i) = \boxed{2+i}$ ($(1+i)(2+i) = 1+3i = 1$ ✓). Puis $(1+i)^2 = \boxed{2i}$,
 $(1+i)^4 = (2i)^2 = \boxed{2}$ ($= -1$) et $(1+i)^8 = \boxed{1}$. Les puissances successives sont

$$1, \quad 1+i, \quad 2i, \quad 1+2i, \quad 2, \quad 2+2i, \quad i, \quad 2+i \quad (k=0, \dots, 7):$$

huit éléments non nuls distincts, donc **tous les éléments non nuls de K_3** .

4. $(2+i)(2-i) = 4+1 = \boxed{0}$ dans $\mathbb{Z}/5\mathbb{Z}$: K_5 **n'est pas intègre**. Comme $-1 = 2^2$: $N(z) = 0 \iff (a-2b)(a+2b) = 0 \iff a = 2b$ ou $a = 3b$, d'où $z = 0$ et les 8 éléments $2b + bi$, $3b + bi$ ($b \neq 0$) : 9 éléments de norme nulle. Or z est inversible $\iff N(z) \neq 0$ (si $zz' = 1$, $N(z)N(z') = 1$; sinon, $z^{-1} = N(z)^{-1}\bar{z}$) : K_5 a $25 - 9 = \boxed{16}$ inversibles.

Remarque. D'après les exercices 20 et 61 du chapitre 8, pour p premier impair, K_p est un corps si et seulement si $p \equiv 3 \pmod{4}$.

■ Corrigé de l'exercice 54

1. $a^3 = 6abc - 2b^3 - 4c^3$ est pair, donc a est pair : $a = 2a'$. Alors $8a'^3 + 2b^3 + 4c^3 = 12a'bc$, soit $b^3 + 2c^3 + 4a'^3 = 6bca'$: $(b, c, \frac{a}{2})$ est solution. S'il existait une solution non nulle, on en choisirait une avec $S = |a| + |b| + |c|$ minimal ; en appliquant trois fois ce résultat, a, b, c sont pairs et $(\frac{a}{2}, \frac{b}{2}, \frac{c}{2})$ est une solution non nulle de somme $\frac{S}{2} < S$: contradiction. **Donc** $a = b = c = 0$.
2. On développe avec $\alpha^3 = 2$ et $\alpha^4 = 2\alpha$. Terme constant : $a(a^2 - 2bc) + 2b(b^2 - ac) + 2c(2c^2 - ab) = a^3 + 2b^3 + 4c^3 - 6abc$. Coefficient de α : $a(2c^2 - ab) + b(a^2 - 2bc) + 2c(b^2 - ac) = 0$. Coefficient de α^2 : $a(b^2 - ac) + b(2c^2 - ab) + c(a^2 - 2bc) = 0$.
3. Si a, b, c ne sont pas tous nuls, on les multiplie par un dénominateur commun : on obtient des entiers A, B, C non tous nuls avec $A^3 + 2B^3 + 4C^3 - 6ABC \neq 0$ (question 1), donc $A + B\alpha + C\alpha^2 \neq 0$ d'après 2. Ainsi $a + b\alpha + c\alpha^2 = 0 \Rightarrow a = b = c = 0$: l'écriture d'un élément de $\mathbb{Q}(\alpha)$ est unique. $\mathbb{Q}(\alpha)$ contient 1, est stable par différence et, avec $\alpha^3 = 2$, $\alpha^4 = 2\alpha$, par produit :

$$(a + b\alpha + c\alpha^2)(a' + b'\alpha + c'\alpha^2) = (aa' + 2bc' + 2cb') + (ab' + ba' + 2cc')\alpha + (ac' + bb' + ca')\alpha^2.$$

Si $x = a + b\alpha + c\alpha^2 \neq 0$, alors $D = a^3 + 2b^3 + 4c^3 - 6abc \neq 0$ (même argument) et, d'après 2, $x^{-1} = \frac{1}{D}[(a^2 - 2bc) + (2c^2 - ab)\alpha + (b^2 - ac)\alpha^2] \in \mathbb{Q}(\alpha)$: $\mathbb{Q}(\alpha)$ **est un sous-corps de $\mathbb{R}$** .

4. $\alpha \times \alpha^2 = 2$: $\alpha^{-1} = \boxed{\frac{1}{2}\alpha^2}$. Pour $(a, b, c) = (1, 1, 0)$, $D = 3$: $(1 + \alpha)^{-1} = \boxed{\frac{1}{3}(1 - \alpha + \alpha^2)}$ (en effet $(1 + \alpha)(1 - \alpha + \alpha^2) = 1 + \alpha^3 = 3$). Pour $(-1, 1, 0)$, $D = 1$: $(\alpha - 1)^{-1} = \boxed{1 + \alpha + \alpha^2}$ (car $(\alpha - 1)(1 + \alpha + \alpha^2) = \alpha^3 - 1 = 1$).

33

Corrigés : matrices et structures

■ Corrigé de l'exercice 55

- $2A - 3B = \begin{pmatrix} 1 & -8 \\ 2 & 9 \end{pmatrix}$, $AB = \begin{pmatrix} 2 & 5 \\ 1 & -1 \end{pmatrix}$, $BA = \begin{pmatrix} 4 & 5 \\ -1 & -3 \end{pmatrix}$: $AB \neq BA$, le produit matriciel n'est pas commutatif.
- $B^2 = \begin{pmatrix} 1 & 2-2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$. Donc $B^n = I$ si n est pair et $B^n = B$ si n est impair. Comme $B \times B = I$, B est inversible et $B^{-1} = B$.
- $\det(A - xI) = (2 - x)(3 - x) + 1 = x^2 - 5x + 7 = \left(x - \frac{5}{2}\right)^2 + \frac{3}{4} > 0$: $A - xI$ est inversible pour tout réel x . Pour $x = 0$: $\det A = 7$ et $A^{-1} = \frac{1}{7} \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}$ (contrôle : $A \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix} = 7I$ ✓).
- $D^2 = I$, donc $D^n = I$ si n est pair et $D^n = D$ si n est impair. Comme I et D commutent, $(I - D)(I + D) = I - D^2 = O$, alors que

$$I - D = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} \neq O \quad \text{et} \quad I + D = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq O :$$

l'anneau $(M_3(\mathbb{R}), +, \times)$ n'est pas intègre (et $X^2 = I$ y a d'autres solutions que $\pm I$).

■ Corrigé de l'exercice 56

- $5 \times 2 - 3 \times 3 = 1 \neq 0$: $A^{-1} = \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}$. Le système s'écrit $A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$, donc $\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} 4 \\ 1 \end{pmatrix}$: $(x, y) = (5, -7)$ ($25 - 21 = 4$, $15 - 14 = 1$ ✓).
- En soustrayant les équations deux à deux : $y + 2z = b - a$ et $y + 3z = c - b$, d'où

$$z = a - 2b + c, \quad y = -3a + 5b - 2c, \quad x = 3a - 3b + c.$$

Pour tout second membre, il y a une unique solution, donnée par une matrice P' : P est in-

versible et $P^{-1} = P' = \begin{pmatrix} 3 & -3 & 1 \\ -3 & 5 & -2 \\ 1 & -2 & 1 \end{pmatrix}$.

- $Q^2 = \begin{pmatrix} 5 & 0 & 4 \\ 4 & 1 & 4 \\ 4 & 0 & 5 \end{pmatrix}$, donc $Q^2 - 4Q = -3I$. Ainsi $Q \times \frac{1}{3}(4I - Q) = \frac{1}{3}(4I - Q) \times Q = I$: $Q^{-1} = \frac{1}{3}(4I - Q) = \frac{1}{3} \begin{pmatrix} 2 & 0 & -1 \\ -1 & 3 & -1 \\ -1 & 0 & 2 \end{pmatrix}$.

■ Corrigé de l'exercice 57

1. $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$. Donc T contient $I = M(1, 0, 1)$, est stable par différence et par produit : c'est un **sous-anneau** de $M_2(\mathbb{R})$. Avec $E = M(1, 0, 0)$ et $N = M(0, 1, 0)$: $EN = N$ mais $NE = O$. Ainsi T **n'est pas commutatif**, et il a des **diviseurs de zéro** : il n'est pas intègre.
2. $\det M(a, b, c) = ac$. Si $ac = 0$, $M(a, b, c)$ n'est pas inversible ; si $ac \neq 0$, elle l'est et

$$M(a, b, c)^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = M\left(\frac{1}{a}, -\frac{b}{ac}, \frac{1}{c}\right) \in T.$$

T^* contient I , est stable par produit ($aa'cc' \neq 0$) et par passage à l'inverse : **c'est un sous-groupe** de $GL_2(\mathbb{R})$.

3. a) $\varphi(M + M') = \varphi(M) + \varphi(M')$, $\varphi(MM') = (aa', cc') = \varphi(M) \cdot \varphi(M')$, et $(u, v) = \varphi(M(u, 0, v))$: φ est **surjective**. Elle n'est **pas injective** : $\varphi(N) = (0, 0) = \varphi(O)$.
 b) $U = \{M(1, b, 1), b \in \mathbb{R}\} \subset T^*$, et $\psi : b \mapsto M(1, b, 1)$ est une bijection de $\mathbb{R}$ sur U telle que $\psi(b)\psi(b') = M(1, b + b', 1) = \psi(b + b')$. C'est un morphisme de $(\mathbb{R}, +)$ dans $(T^*, \times)$, d'image U : **U est un sous-groupe, isomorphe à $(\mathbb{R}, +)$** .
4. Récurrence. Pour $n = 0$: $A^0 = I = M(1, 0, 1)$ ✓. Si la formule est vraie au rang n , $A^{n+1} = A^n A = M\left(a^{n+1}, a^n b + b \frac{a^n - c^n}{a - c}, c, c^{n+1}\right)$, et $a^n + \frac{c(a^n - c^n)}{a - c} = \frac{a^{n+1} - c^{n+1}}{a - c}$.
 Ainsi $M(3, 2, 1)^n = M(3^n, 3^n - 1, 1)$. Pour $n = -1$, on obtient $M\left(\frac{1}{3}, -\frac{2}{3}, 1\right)$, qui est bien l'inverse de $M(3, 2, 1)$ d'après 2 ✓.

■ Corrigé de l'exercice 58

1. $T(a, b, c)T(a', b', c') = \begin{pmatrix} 1 & a' + a & c' + ab' + c \\ 0 & 1 & b' + b \\ 0 & 0 & 1 \end{pmatrix} = T(a + a', b + b', c + c' + ab') \in H$. Le produit est associatif, $I = T(0, 0, 0) \in H$ et, d'après 1, $T(a, b, c)T(-a, -b, ab - c) = T(0, 0, 0) = T(-a, -b, ab - c)T(a, b, c)$: $(H, \times)$ est un groupe, avec $T(a, b, c)^{-1} = T(-a, -b, ab - c)$. Il **n'est pas commutatif** : $T(1, 0, 0)T(0, 1, 0) = T(1, 1, 1)$ et $T(0, 1, 0)T(1, 0, 0) = T(1, 1, 0)$.

2. $XY = T(s, t, u)$ et $YX = T(s, t, u')$, avec $s = a + a'$, $t = b + b'$, $u = c + c' + ab'$, $u' = c + c' + a'b$. Comme $X^{-1}Y^{-1} = (YX)^{-1} = T(-s, -t, st - u')$:

$$XYX^{-1}Y^{-1} = T(s, t, u)T(-s, -t, st - u') = T(0, 0, u - u') = T(0, 0, ab' - a'b).$$

$$\text{Donc } XY = YX \iff XYX^{-1}Y^{-1} = I \iff ab' = a'b.$$

3. $X = T(a, b, c)$ commute avec tout $T(a', b', c')$ si et seulement si $ab' - a'b = 0$ pour tous a', b' ; avec $(a', b') = (0, 1)$ puis $(1, 0)$: $a = b = 0$. Réciproquement $T(0, 0, c)$ convient : $Z = \{T(0, 0, c), c \in \mathbb{R}\}$. L'application $g : c \mapsto T(0, 0, c)$ vérifie $g(c)g(c') = g(c + c')$: c'est un morphisme injectif de $(\mathbb{R}, +)$ dans $(H, \times)$, d'image Z . Donc Z est un sous-groupe et g **est un isomorphisme de $(\mathbb{R}, +)$ sur $(Z, \times)$** .
4. $\Phi : (a, b, c) \mapsto T(a, b, c)$ est une bijection de $\mathbb{R}^3$ sur H telle que $\Phi(u * v) = \Phi(u)\Phi(v)$ (question 1). Par transport de structure, $(\mathbb{R}^3, *)$ est un groupe, isomorphe à $(H, \times)$, donc **non commutatif**. Son neutre est $\Phi^{-1}(I) = (0, 0, 0)$ et le symétrique de $(1, 2, 3)$ est $\Phi^{-1}(T(-1, -2, 2 - 3)) = (-1, -2, -1)$ $((1, 2, 3) * (-1, -2, -1) = (0, 0, 3 - 1 - 2) \checkmark)$.

■ Corrigé de l'exercice 59

1. Le calcul donne $P^2 = P$, $PQ = QP = Q$ et $Q^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} = -P$. Par distributivité :

$$M(a, b)M(c, d) = acP^2 + adPQ + bcQP + bdQ^2 = (ac - bd)P + (ad + bc)Q = M(ac - bd, ad + bc).$$

Avec $M(a, b) + M(c, d) = M(a + c, b + d)$: E est stable par $+$ et par $\times$.

2. $M(a, b) = \begin{pmatrix} a & -b & 0 \\ b & a & 0 \\ a & -b & 0 \end{pmatrix}$: ses coefficients $(1, 1)$ et $(2, 1)$ redonnent a et b , donc φ est injective ; elle est surjective par définition de E . Puis $\varphi(z + z') = \varphi(z) + \varphi(z')$ et, d'après 1, $\varphi(z z') = M(aa' - bb', ab' + ba')$. Par transport de structure (avec la bijection φ^{-1}), $(E, +, \times)$ est un corps commutatif isomorphe à $(\mathbb{C}, +, \times)$, de zéro $\varphi(0) = O$ et d'unité $\varphi(1) = P$.

3. a) La troisième colonne de $M(a, b)$ est nulle, donc $M(a, b)K = O$. Si $M(a, b)$ était inversible dans $M_3(\mathbb{R})$, on aurait $K = M(a, b)^{-1}M(a, b)K = O$: absurde. **Aucun élément de E n'est inversible dans $M_3(\mathbb{R})$** ; en particulier $I \notin E$.

b) $(1 + i)^{-1} = \frac{1-i}{2}$, donc $M(1, 1)^{-1} = M\left(\frac{1}{2}, -\frac{1}{2}\right)$ (contrôle : $M(1, 1)M\left(\frac{1}{2}, -\frac{1}{2}\right) = M(1, 0) = P$). Pas de contradiction : être inversible dépend de l'anneau. Dans E , l'unité est P et l'on demande $XY = P$; dans $M_3(\mathbb{R})$, on demande $XY = I$, ce qui est impossible.

4. On pose $X = \varphi(z)$ et l'on résout dans $\mathbb{C}$ (φ est un isomorphisme). a) $z^2 = 2i = (1 + i)^2 \iff z = \pm(1 + i)$: $X = \pm M(1, 1)$.

b) $z^3 = 1 \iff z \in \mathbb{U}_3 = \{1, j, j^2\}$, $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$: $X \in \left\{P, M\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right), M\left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)\right\} = \varphi(\mathbb{U}_3)$.

Comme φ induit un isomorphisme de $(\mathbb{C}^*, \times)$ sur le groupe $(E \setminus \{O\}, \times)$ (de neutre P), l'image du sous-groupe $\mathbb{U}_3$ est un sous-groupe isomorphe à $(\mathbb{U}_3, \times)$.

c) $\sqrt{3} + i = 2e^{i\pi/6}$, donc $(\sqrt{3} + i)^6 = 64e^{i\pi} = -64$ et $M(\sqrt{3}, 1)^6 = M(-64, 0) = -64P$ (et non $-64I$!).

■ Corrigé de l'exercice 60

1. $S(a, b)S(a', b') = \begin{pmatrix} aa' + bb' & ab' + ba' \\ ba' + ab' & bb' + aa' \end{pmatrix} = S(aa' + bb', ab' + ba')$. S contient $I = S(1, 0)$, est stable par différence et par produit : c'est un sous-anneau de $M_2(\mathbb{R})$, **commutatif** car la formule est symétrique.

2. $S(1, 1)S(1, -1) = O$: S n'est pas intègre. $\det S(a, b) = a^2 - b^2$. Si $a^2 \neq b^2$, l'inverse de $S(a, b)$ est $\frac{1}{a^2 - b^2} \begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = S\left(\frac{a}{a^2 - b^2}, \frac{-b}{a^2 - b^2}\right) \in S$; si $a^2 = b^2$, $S(a, b)$ n'est pas inversible.

3. φ a pour réciproque $(u, v) \mapsto S\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$; elle est additive et

$\varphi(S(a, b)S(a', b')) = (aa' + bb' + ab' + ba', aa' + bb' - ab' - ba') = ((a + b)(a' + b'), (a - b)(a' - b'))$,
c'est-à-dire $\varphi(S(a, b)S(a', b')) = \varphi(S(a, b)) \cdot \varphi(S(a', b'))$.

4. a) $c(t)^2 - s(t)^2 = 1$ et $c(t) > 0$: $H(t) \in G$. De plus $\varphi(H(t)) = (e^t, e^{-t})$, donc $\varphi(H(t)H(t')) = (e^{t+t'}, e^{-(t+t')}) = \varphi(H(t + t'))$ et, φ étant injective, $H(t)H(t') = H(t + t')$.

b) H est injective ($H(t) = H(t') \Rightarrow e^t = e^{t'}$). Elle est surjective : si $S(a, b) \in G$, alors $a = \sqrt{1 + b^2} > |b|$, donc $a + b > 0$; avec $t = \ln(a + b)$, $e^{-t} = \frac{1}{a+b} = a - b$, d'où $c(t) = a$ et $s(t) = b$. Ainsi H est

une bijection de $\mathbb{R}$ sur G qui vérifie $H(t+t') = H(t)H(t')$: par transport de structure, $(G, \times)$ est un **groupe** (c'est un sous-groupe de $GL_2(\mathbb{R})$, de neutre $H(0) = I$, avec $H(t)^{-1} = H(-t)$), **isomorphe** à $(\mathbb{R}, +)$ par H .

Remarque. G est l'analogue « hyperbolique » du groupe des rotations : c et s (cosinus et sinus hyperboliques) remplacent $\cos$ et $\sin$, et l'hyperbole $a^2 - b^2 = 1$ remplace le cercle.

34

Corrigés : défis de concours

■ Corrigé de l'exercice 61

- a) Avec $n = k$ et $n = k + 1$: $x^k y^k xy = (xy)^k(xy) = (xy)^{k+1} = x^{k+1}y^{k+1} = x^k xy^k y$. En simplifiant à gauche par x^k et à droite par y (tout élément d'un groupe est régulier) : $y^k x = xy^k$. Le même calcul avec $n = k + 1$ et $n = k + 2$ donne $y^{k+1}x = xy^{k+1}$.

b) D'une part $xy^{k+1} = (xy)y^k$; d'autre part, d'après a), $xy^{k+1} = y^{k+1}x = y(y^k x) = y(xy^k) = (yx)y^k$. Donc $(xy)y^k = (yx)y^k$ et, en simplifiant à droite par y^k : $xy = yx$.
- a) f est un morphisme : $(xy)^3 = x^3y^3$, c'est-à-dire $xyxyx y = x xxyy y$. En simplifiant à gauche par x et à droite par y : $xyyx = xxyy$, soit $(yx)^2 = x^2y^2$.

b) D'une part $(yx)^3 = f(yx) = y^3x^3$; d'autre part $(yx)^3 = (yx)^2(yx) = x^2y^2yx = x^2y^3x$. Donc $y^3x^3 = x^2y^3x$ et, en simplifiant à droite par x : $y^3x^2 = x^2y^3$. Comme f est surjective, tout $z \in G$ s'écrit $z = y^3$: $zx^2 = x^2z$ **pour tous** $x, z \in G$.

c) En échangeant les rôles dans a) : $xyxy = (xy)^2 = y^2x^2$. Comme y^2 commute avec x (question b) : $y^2x^2 = (y^2x)x = xy^2x = xy yx$. Ainsi $xyxy = xy yx$ et, en simplifiant à gauche par xy : $xy = yx$, G est commutatif.
- a) $(1, 0, 0) * (0, 1, 0) = (1, 1, 0 + 0 + 1 \times 1) = (1, 1, 1)$, mais $(0, 1, 0) * (1, 0, 0) = (1, 1, 0 + 0 + 0 \times 0) = (1, 1, 0)$: E **n'est pas commutatif**. Formule de x^n par récurrence : pour $n = 1$, la formule donne x . Si elle est vraie au rang n ,

$$x^{n+1} = x^n * x = \left((n+1)a, (n+1)b, nc + \frac{n(n-1)}{2}ab + c + na b \right) \quad \text{et} \quad \frac{n(n-1)}{2} + n = \frac{(n+1)n}{2}.$$

Pour $n = 3$: $x^3 = (3a, 3b, 3c + 3ab) = (0, 0, 0) = e$ dans $\mathbb{Z}/3\mathbb{Z}$.

b) Si $n = 3q$ ($q \geq 1$) : $x^n = (x^3)^q = e$ pour tout x , donc $(x * y)^n = e = x^n * y^n$. Si $n = 3q + 1$: $x^n = (x^3)^q * x = x$, donc $(x * y)^n = x * y = x^n * y^n$. L'égalité $(x * y)^n = x^n * y^n$ est donc vraie pour une **infinité** d'entiers n (en particulier pour les **deux** entiers consécutifs 3 et 4), et pourtant E n'est pas commutatif : dans la question 1, on ne peut pas se contenter de deux entiers consécutifs. De même, $x \mapsto x^3$ est ici un morphisme (constant, égal à e) qui n'est pas bijectif : dans la question 2, l'hypothèse de bijectivité est indispensable.

■ Corrigé de l'exercice 62

- Pour $j = 0$: $5 = 1 + 2^2 \times 1$, avec $m_0 = 1$ impair. Si $5^{2^j} = 1 + 2^{j+2}m_j$ avec m_j impair, alors

$$5^{2^{j+1}} = \left(1 + 2^{j+2}m_j \right)^2 = 1 + 2^{j+3}m_j + 2^{2j+4}m_j^2 = 1 + 2^{j+3} \left(m_j + 2^{j+1}m_j^2 \right),$$

et $m_{j+1} = m_j + 2^{j+1}m_j^2$ est impair (impair plus pair).

2. a) $5^d = (5^{2^s})^r = u^r$, et $u^r - 1 = (u - 1)(1 + u + \dots + u^{r-1})$. Le second facteur est une somme de r entiers impairs, avec r impair : il est impair.
 b) D'après 1, $u - 1 = 2^{s+2}m_s$ avec m_s impair ; donc $5^d - 1 = 2^{s+2} \times (\text{impair})$. Ainsi $2^k \mid 5^d - 1 \iff k \leq s + 2 \iff s \geq k - 2 \iff 2^{k-2} \mid d$.
3. Si $0 \leq i < j \leq 2^{k-2} - 1$ et $5^i \equiv 5^j [2^k]$, alors $2^k \mid 5^i(5^{j-i} - 1)$, donc $2^k \mid 5^{j-i} - 1$ (5^i est impair) et $2^{k-2} \mid j - i$ d'après 2, alors que $0 < j - i < 2^{k-2}$: impossible. De plus $5 \equiv 1 [4]$, donc $5^j \equiv 1 [4]$ et $-5^j \equiv 3 [4]$: une classe $\overline{5^j}$ ne peut pas être égale à une classe $\overline{-5^j}$ (on aurait $1 \equiv 3 [4]$). Les $2 \times 2^{k-2} = 2^{k-1}$ classes $\pm \overline{5^j}$ sont donc distinctes, et inversibles (représentants impairs) ; comme G_k a 2^{k-1} éléments : $G_k = \{\pm \overline{5^j}, 0 \leq j \leq 2^{k-2} - 1\}$.
4. Si $x^2 = \overline{1}$, x est inversible ($x \cdot x = \overline{1}$) : $x = \pm \overline{5^j}$ et $x^2 = \overline{5^{2j}} = \overline{1} \iff 2^{k-2} \mid 2j \iff 2^{k-3} \mid j \iff j \in \{0, 2^{k-3}\}$. D'après 1 (avec $j = k - 3$), $5^{2^{k-3}} = 1 + 2^{k-1}m$ avec m impair, donc $5^{2^{k-3}} \equiv 1 + 2^{k-1} [2^k]$ (car $2^{k-1}(m - 1)$ est divisible par 2^k). Les solutions sont les **quatre** classes distinctes $\overline{\pm 1}, \overline{\pm 1 + 2^{k-1}}$ (alors que $x^2 = \overline{1}$ n'a que deux solutions dans un corps $\mathbb{Z}/p\mathbb{Z}$).

■ Corrigé de l'exercice 63

1. Le produit vaut $\begin{pmatrix} zz' - \overline{ww'} & -z\overline{w'} - \overline{w}z' \\ wz' + \overline{zw'} & -w\overline{w'} + \overline{z}z' \end{pmatrix}$. Avec $Z = zz' - \overline{ww'}$ et $W = wz' + \overline{zw'}$: $\overline{Z} = \overline{z}z' - w\overline{w'}$ et $-\overline{W} = -\overline{w}z' - z\overline{w'}$: c'est bien $q(Z, W) \in \mathbb{H}$. Comme $I = q(1, 0) \in \mathbb{H}$ et $q(z, w) - q(z', w') = q(z - z', w - w')$, $\mathbb{H}$ est un sous-anneau de $M_2(\mathbb{C})$: **un anneau unitaire**.
2. Avec la formule de 1 : $\mathbf{i}^2 = q(\mathbf{i}^2, 0) = -I$, $\mathbf{j}^2 = q(-1, 0) = -I$, $\mathbf{k}^2 = q(-(-i)(-i), 0) = q(\mathbf{i}^2, 0) = -I$; $\mathbf{ij} = q(0, \overline{i} \times 1) = q(0, -i) = \mathbf{k}$, $\mathbf{ji} = q(0, 1 \times i) = \mathbf{-k}$, $\mathbf{ijk} = \mathbf{k}^2 = \mathbf{-I}$. Comme $\mathbf{k} \neq 0$, $\mathbf{ij} \neq \mathbf{ji}$: $\mathbb{H}$ **n'est pas commutatif**.
3. $q(z, w)q(\overline{z}, -w) = q(z\overline{z} + \overline{w}w, w\overline{z} - \overline{z}w) = q(|z|^2 + |w|^2, 0) = NI$, et de même $q(\overline{z}, -w)q(z, w) = q(\overline{z}z + \overline{w}w, -wz + zw) = NI$. Si $q(z, w) \neq 0$, alors $N > 0$ et $q(z, w)^{-1} = q(\frac{\overline{z}}{N}, -\frac{w}{N}) \in \mathbb{H}$. Tout élément non nul est inversible et $\times$ n'est pas commutative : $\mathbb{H}$ **est un corps non commutatif**.
4. $\det q(z, w) = z\overline{z} + \overline{w}w = N(q)$, donc $N(qq') = \det(qq') = \det q \det q' = N(q)N(q')$. Avec les notations de l'énoncé, $N(q) = a^2 + b^2 + c^2 + d^2$, et le calcul de Z et W (question 1) donne
 $Z = (aa' - bb' - cc' - dd') + i(ab' + ba' - cd' + dc')$, $W = (ac' + ca' + bd' - db') + i(ad' + da' + cb' - bc')$,
 d'où l'**identité d'Euler** : $(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = (aa' - bb' - cc' - dd')^2 + (ab' + ba' - cd' + dc')^2 + (ac' + ca' + bd' - db')^2 + (ad' + da' + cb' - bc')^2$.
 Avec $(a, b, c, d) = (2, 1, 1, 1)$ et $(a', b', c', d') = (3, 2, 1, 1)$: $105 = 7 \times 15 = 2^2 + 7^2 + 4^2 + 6^2$ ($4 + 49 + 16 + 36 = 105$ ✓).
5. $q(z, w)^2 = q(z^2 - |w|^2, (z + \overline{z})w)$. Donc $q(z, w)^2 = -I \iff z^2 - |w|^2 = -1$ et $2 \operatorname{Re}(z)w = 0$. Si $\operatorname{Re}(z) \neq 0$, alors $w = 0$ et $z^2 = -1$, donc $z = \pm i$: contradiction. Ainsi $z = i\beta$ ($\beta \in \mathbb{R}$) et la condition devient $\beta^2 + |w|^2 = 1$: les $q(i \cos \theta, \sin \theta)$, $\theta \in \mathbb{R}$, forment une **infinité** de solutions (parmi lesquelles $\pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}$).
- Dans un corps commutatif, si $x_0^2 = -1$, alors $x^2 = -1 \iff (x - x_0)(x + x_0) = 0 \iff x = \pm x_0$: au plus deux solutions. Dans $\mathbb{H}$, $(x - x_0)(x + x_0) = x^2 - x_0^2 + (xx_0 - x_0x)$: cette factorisation **utilise la commutativité** (elle tombe en défaut pour $x = \mathbf{i}$, $x_0 = \mathbf{j}$).

■ **Corrigé de l'exercice 64**

- Si $m = \sum x_i^2$ et $n = \sum y_i^2$, l'identité donne $mn = \sum T_i^2$ avec $T_i \in \mathbb{Z}$: Σ est stable par $\times$. Comme $0, 1 = 1^2$ et $2 = 1^2 + 1^2$ sont dans Σ , et que tout entier $n \geq 2$ est un produit de nombres premiers, il suffit que tout nombre premier impair soit dans Σ pour avoir $\Sigma = \mathbb{N}$.
- a) Si $0 \leq x < x' \leq \frac{p-1}{2}$ et $x^2 \equiv x'^2 [p]$, alors $p \mid (x' - x)(x' + x)$, avec $0 < x' - x < p$ et $0 < x' + x \leq p - 1$: par le lemme d'Eulclide, c'est impossible. Les restes des x^2 sont donc distincts ; de même pour les $-1 - y^2$, car $-1 - y^2 \equiv -1 - y'^2 \iff y^2 \equiv y'^2$.
b) Les deux familles ont chacune $\frac{p+1}{2}$ éléments, de restes deux à deux distincts ; il y a $p+1$ entiers en tout et seulement p restes possibles : un x^2 et un $-1 - y^2$ ont le même reste (principe des tiroirs), et $p \mid x^2 + y^2 + 1$. On écrit $x^2 + y^2 + 1^2 + 0^2 = mp \in \Sigma$ avec $m \geq 1$ et $mp \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2$, d'où $1 \leq m < p$.
- On a $m_0 \leq m < p$.
a) $\sum x_i^2 = m_0 p$ est pair, donc le nombre de x_i impairs est pair (0, 2 ou 4) : on peut numérotiser les x_i pour que x_1, x_2 soient de même parité, ainsi que x_3, x_4 . Comme $\left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2 = \frac{u^2+v^2}{2}$:

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 \in \Sigma,$$

avec $1 \leq \frac{m_0}{2} < m_0$: cela contredit la minimalité de m_0 . m_0 est donc impair.

b) Chaque classe modulo m_0 a un représentant dans $\left[-\frac{m_0-1}{2}, \frac{m_0-1}{2}\right]$. Alors $\sum y_i^2 \equiv \sum x_i^2 = m_0 p \equiv 0 [m_0]$, donc $\sum y_i^2 = m_0 m_1$ avec $m_1 \geq 0$, et $\sum y_i^2 \leq 4\left(\frac{m_0-1}{2}\right)^2 < m_0^2$, d'où $m_1 < m_0$. Si $m_1 = 0$, tous les y_i sont nuls, m_0 divise tous les x_i , donc $m_0^2 \mid m_0 p$ et $m_0 \mid p$, avec $1 < m_0 < p$: impossible. Ainsi $1 \leq m_1 < m_0$.

c) Modulo m_0 , on remplace y_i par x_i : $T_1 \equiv \sum x_i^2 \equiv 0$, $T_2 \equiv x_2 x_1 - x_1 x_2 + x_3 x_4 - x_4 x_3 = 0$, et de même $T_3 \equiv T_4 \equiv 0 [m_0]$. L'identité donne $(m_0 p)(m_0 m_1) = \sum T_i^2$, donc

$$m_1 p = \left(\frac{T_1}{m_0}\right)^2 + \left(\frac{T_2}{m_0}\right)^2 + \left(\frac{T_3}{m_0}\right)^2 + \left(\frac{T_4}{m_0}\right)^2 \in \Sigma,$$

avec $1 \leq m_1 < m_0$: nouvelle contradiction. Donc $m_0 = 1$: $p \in \Sigma$.

- D'après 1 et 3, $\Sigma = \mathbb{N}$: tout entier naturel est somme de quatre carrés. $23 = 3^2 + 3^2 + 2^2 + 1^2$. Un carré est congru à 0, 1 ou 4 modulo 8 ($(2m)^2 = 4m^2$ et $(2m+1)^2 \equiv 1$). Une somme de trois tels restes vaut, modulo 8 : 0, 1, 2, 3 (avec des 0 et des 1), 4, 5, 6 (avec un 4), 0, 1 (avec deux 4), 4 (avec trois 4) : jamais 7. Comme $23 \equiv 7 [8]$, 23 n'est pas somme de trois carrés.

■ **Corrigé de l'exercice 65**

- $f(0) = f(0+0) = 2f(0)$, donc $f(0) = 0$, puis $f(x) + f(-x) = f(0) = 0$. Si $x \neq 0$: $f(x)f(x^{-1}) = f(1) = 1$, donc $f(x) \neq 0$ et $f(x^{-1}) = f(x)^{-1}$. Si $f(x) = f(y)$, alors $f(x-y) = 0$, donc $x-y=0$: f est injective.
- Par récurrence, $f(n) = f(n-1) + f(1) = n$ pour $n \in \mathbb{N}$; puis $f(-n) = -f(n) = -n$; enfin, pour $r = \frac{p}{q}$ ($p \in \mathbb{Z}, q \in \mathbb{N}^*$) : $f(r) = f(p)f(q)^{-1} = \frac{p}{q} = r$. Le seul morphisme de corps de $\mathbb{Q}$ dans $\mathbb{Q}$ est donc l'identité.

3. a) Si $x \geq 0$: $f(x) = f(\sqrt{x}^2) = f(\sqrt{x})^2 \geq 0$. Si $x \leq y$: $f(y) - f(x) = f(y - x) \geq 0$: **f est croissante.**
- b) Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$; on pose $r_n = \frac{E(nx)}{n}$ et $s_n = r_n + \frac{1}{n}$: ce sont des rationnels et $r_n \leq x < s_n$. Par croissance, et puisque f fixe les rationnels : $r_n \leq f(x) \leq s_n$. Donc $|f(x) - x| \leq s_n - r_n = \frac{1}{n}$ pour tout n , et $f(x) = x$: **le seul morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$ est $\text{id}_{\mathbb{R}}$.**
4. La restriction de f à $\mathbb{R}$ est un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$, donc $f(x) = x$ pour x réel. Puis $f(i)^2 = f(i^2) = f(-1) = -1$, donc $f(i) = \pm i$, et $f(a+ib) = f(a) + f(b)f(i) = a \pm ib$: $f = \text{id}$ ou $f : z \mapsto \bar{z}$. Les deux conviennent : $\overline{z+z'} = \bar{z} + \bar{z'}$, $\overline{zz'} = \bar{z}\bar{z'}$ et $\bar{1} = 1$.
5. a) Soit f un morphisme de $\mathbb{Q}(\sqrt{2})$ dans lui-même. Il fixe $\mathbb{Q}$ (question 2), donc $f(a + b\sqrt{2}) = a + bf(\sqrt{2})$, avec $f(\sqrt{2})^2 = f(2) = 2$: $f(\sqrt{2}) = \pm\sqrt{2}$. Donc $f = \text{id}$ ou $f = \sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Réciproquement σ est bien définie (unicité de l'écriture), additive, $\sigma(1) = 1$, et
- $$\sigma((a + b\sqrt{2})(c + d\sqrt{2})) = \sigma(ac + 2bd + (ad + bc)\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}).$$
- Il y a donc exactement **deux** morphismes, id et σ , tous deux bijectifs ($\sigma \circ \sigma = \text{id}$) : ce sont les automorphismes de $\mathbb{Q}(\sqrt{2})$.
- b) Si $f : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3})$ était un morphisme, $u + v\sqrt{3} = f(\sqrt{2})$ ($u, v \in \mathbb{Q}$) vérifierait $u^2 + 3v^2 + 2uv\sqrt{3} = f(2) = 2$, donc (unicité de l'écriture) $uv = 0$ et $u^2 + 3v^2 = 2$. Si $v = 0$, $u^2 = 2$; si $u = 0$, $(3v)^2 = 6$: impossible dans $\mathbb{Q}$, car $\sqrt{2}$ et $\sqrt{6}$ sont irrationnels. **Il n'existe aucun morphisme**, donc aucun isomorphisme : ces corps ne sont pas isomorphes (alors que $a + b\sqrt{2} \mapsto a + b\sqrt{3}$ est un isomorphisme des groupes additifs).

■ Corrigé de l'exercice 66

1. Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a $A \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} A = (\det A)I$. Si $\det A \neq 0$, A est donc inversible, d'inverse $(\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Si A est inversible, $\det A \det A^{-1} = \det I = 1$, donc $\det A \neq 0$. Ainsi $\det$ envoie $\text{GL}_2(K)$ dans K^* et vérifie $\det(AB) = \det A \det B$: c'est un **morphisme, surjectif** car $\det \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} = \lambda$ pour tout $\lambda \in K^*$. $\text{SL}_2(K)$ est l'image réciproque du sous-groupe $\{1\}$ de K^* : c'est un **sous-groupe** de $\text{GL}_2(K)$.
2. Si $(b, d) = (\lambda a, \lambda c)$, alors $\det A = a\lambda c - \lambda a c = 0$. Réciproquement, supposons $ad = bc$. Si $a \neq 0$, on pose $\lambda = ba^{-1}$: $b = \lambda a$ et $d = a^{-1}bc = \lambda c$. Si $a = 0$, alors $c \neq 0$ et $bc = 0$, donc $b = 0$ (K est un corps) ; avec $\lambda = dc^{-1}$: $(b, d) = (0, \lambda c) = (\lambda a, \lambda c)$.
- Comptons : A est inversible si et seulement si sa première colonne est non nulle (sinon $\det A = 0$) et sa seconde colonne n'est pas l'un des $\lambda(a, c)$. Ces derniers sont exactement p couples distincts (si $\lambda(a, c) = \mu(a, c)$, une coordonnée non nulle donne $\lambda = \mu$). D'où $p^2 - 1$ choix pour la première colonne, puis $p^2 - p$ pour la seconde :

$$|\text{GL}_2(K)| = (p^2 - 1)(p^2 - p).$$

3. Si $\det A = 1$, alors $\det(D_\lambda A) = \lambda$: l'application envoie $\text{SL}_2(K)$ dans S_λ . Elle est injective (D_λ est inversible), et surjective : si $\det B = \lambda$, $A = D_\lambda^{-1}B$ vérifie $\det A = \lambda^{-1}\lambda = 1$ et $D_\lambda A = B$. Les $p - 1$ ensembles S_λ , deux à deux disjoints, ont donc tous $|\text{SL}_2(K)|$ éléments, et leur réunion est $\text{GL}_2(K)$:

$$(p - 1) |\text{SL}_2(K)| = (p^2 - 1)p(p - 1), \quad |\text{SL}_2(K)| = p(p^2 - 1).$$

Pour $p = 2$: 6 et 6 ; pour $p = 3$: 48 et 24 ; pour $p = 5$: 480 et 120.

4. Dans $\mathbb{Z}/2\mathbb{Z}$, $\det A \neq 0 \iff \det A = 1$. Les six éléments sont

$$I, \quad A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

$A_2 A_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = B_1$ mais $A_3 A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = B_2$: **le groupe n'est pas commutatif**. On calcule $A_1^2 = A_2^2 = A_3^2 = I$, puis $B_1^2 = B_2$ et $B_1^3 = B_1 B_2 = I$, $B_2^2 = B_1$, $B_2^3 = I$. Le plus petit n vaut donc 1 pour I , 2 pour A_1, A_2, A_3 , et 3 pour B_1, B_2 (comme pour le groupe des six fonctions du cours).

Mon bilan sur le chapitre

Partie B · Le parcours en 4 niveaux

Niveau	Exercices	Réussis seul(e)	À refaire
Niveau 1 · Bases ★	1 à 8	/ 8	
Niveau 2 · Bac ★★	9 à 16	/ 8	
Niveau 3 · Approfondissement ★★★	17 à 23	/ 7	
Niveau 4 · Concours ★★★★	24 à 30	/ 7	

Partie C · La banque d'exercices

Thème	Exercices	Réussis seul(e)	À refaire
Thème A · Lois de composition interne	31 à 36	/ 6	
Thème B · Groupes et sous-groupes	37 à 42	/ 6	
Thème C · Morphismes et isomorphismes	43 à 48	/ 6	
Thème D · Anneaux et corps	49 à 54	/ 6	
Thème E · Matrices et structures	55 à 60	/ 6	
Thème F · Défis de concours	61 à 66	/ 6	

Conseil : refais dans une semaine les exercices ratés, sans regarder le corrigé.

Prochain chapitre : *Espaces vectoriels*

Maths Olympiad