CORRIGÉ – CHAPITRE 11

STRUCTURES ALGÉBRIQUES USUELLES

⋆ *application directe* ⋆⋆ *mise en œuvre* ⋆⋆⋆ *problème* ⋆⋆⋆⋆ *problème long, en autonomie*

Lois de composition interne

EXERCICE 1 ⋆

(a) La moyenne. Elle est commutative, puisque $\dfrac{x+y}{2} = \dfrac{y+x}{2}$. Elle n'est pas associative : $(0 \star 0) \star 4 = 2$, alors que $0 \star (0 \star 4) = 1$. Si e était neutre, on aurait $\dfrac{x+e}{2} = x$, soit $e = x$, pour tout réel x, ce qui est impossible.

commutative, non associative, sans neutre

(b) Le maximum. Il est associatif et commutatif, car $\max(\max(x,y),z)$ et $\max(x,\max(y,z))$ valent tous deux le plus grand des trois nombres. Sur $\mathbb{R}_+$, le réel 0 est neutre, puisque $\max(x,0) = x$ pour $x \geqslant 0$; un élément x est inversible si $\max(x,y) = 0$ pour un $y \geqslant 0$, ce qui impose $x = 0$. Sur $\mathbb{R}$, un neutre e vérifierait $\max(e-1,e) = e-1$, ce qui est faux.

sur $\mathbb{R}_+$: neutre 0, seul 0 inversible; sur $\mathbb{R}$: pas de neutre

(c) La différence. Avec $E \neq \varnothing$, on a $E \setminus \varnothing = E$ et $\varnothing \setminus E = \varnothing$: la loi n'est pas commutative. On a $(E \setminus E) \setminus E = \varnothing$ et $E \setminus (E \setminus E) = E$: elle n'est pas associative. La partie $\varnothing$ vérifie $A \setminus \varnothing = A$, mais $\varnothing \setminus A = \varnothing \neq A$ dès que $A \neq \varnothing$: elle n'est neutre qu'à droite. Un neutre N vérifierait $N \setminus A = A$ pour tout A, donc $N \setminus N = N$, soit $N = \varnothing$, ce qui vient d'être exclu.

ni associative, ni commutative, sans neutre

(d) La puissance. On a $(2^3)^2 = 64$ et $2^{(3^2)} = 512$, puis $2^3 = 8 \neq 9 = 3^2$. L'entier 1 vérifie $a^1 = a$, mais $1^a = 1 \neq a$ pour $a \geqslant 2$: comme pour la différence, il n'est neutre que d'un côté.

ni associative, ni commutative, sans neutre

(e) La loi $a+b+ab$. On reconnaît $a \star b = (1+a)(1+b) - 1$. Ainsi

$$(a \star b) \star c = (1+a)(1+b)(1+c) - 1 = a \star (b \star c),$$

la loi est commutative, et 0 est neutre. L'entier a est inversible s'il existe $b \in \mathbb{Z}$ tel que $(1+a)(1+b) = 1$, c'est-à-dire si $1 + a \in \{-1, 1\}$.

associative, commutative, neutre 0, inversibles 0 et -2

À retenir. La bijection $a \mapsto 1 + a$ transporte cette loi sur la multiplication de $\mathbb{Z}$; c'est pourquoi elle en a toutes les propriétés, et les inversibles 0 et -2 correspondent aux inversibles 1 et -1 de $(\mathbb{Z}, \times)$. L'exercice 9 exploite la même idée.

EXERCICE 2 ⋆

1. On calcule chaque composée en évaluant en 1 et en 2. Par exemple, $(s \circ c_1)(x) = s(1) = 2$, donc $s \circ c_1 = c_2$, tandis que $(c_1 \circ s)(x) = 1$, donc $c_1 \circ s = c_1$.

$\circ$	id	s	c_1	c_2
id	id	s	c_1	c_2
s	s	id	c_2	c_1
c_1	c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2	c_2

2. La ligne et la colonne de id reproduisent les en-têtes : id est neutre. Un élément est inversible si sa ligne contient id dans une colonne dont la ligne contient aussi id au même endroit : seuls id et s le sont, et $s^{-1} = s$. Enfin $s \circ c_1 = c_2$ et $c_1 \circ s = c_1$.

$$\boxed{\text{neutre id;} \quad \text{inversibles id et } s; \quad s \circ c_1 \neq c_1 \circ s}$$

3. Seules les lignes de id et de s contiennent chaque élément une fois ; les lignes de c_1 et c_2 sont constantes. On retrouve ainsi que $(\mathcal{F}(E,E), \circ)$ n'est pas un groupe : c_1 et c_2, qui ne sont pas injectives, ne sont pas inversibles (chapitre 2, théorème 1). En revanche, la partie $\{\text{id}, s\}$, qui est $\mathfrak{S}_E$, est un groupe.

EXERCICE 3 ⋆⋆

1. Par associativité, on calcule de deux façons le produit $a \star x \star b$:

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

$$\boxed{a = b, \text{ et } x \text{ est inversible, d'inverse } a}$$

C'est la démonstration du point (i) de la proposition 2, qui ne demande en fait qu'un inverse de chaque côté.

2. Pour toute application g telle que $g(n) = n - 1$ pour $n \geqslant 1$, la valeur $g(0)$ étant quelconque, on a $g(d(n)) = g(n+1) = n$ pour tout n : chaque choix de $g(0) \in \mathbb{N}$ fournit une solution de $g \circ d = \text{id}_{\mathbb{N}}$, et il y en a une infinité. Si $d \circ h = \text{id}_{\mathbb{N}}$, alors $0 = d(h(0)) = h(0) + 1$, ce qui est impossible dans $\mathbb{N}$.

$$\boxed{\text{une infinité d'inverses à gauche, aucun inverse à droite}}$$

3. La question 1 suppose l'existence d'un inverse *de chaque côté*, ce qui n'est pas le cas ici. La proposition 2 affirme l'unicité de l'inverse, défini comme un élément qui convient des deux côtés ; un inverse d'un seul côté peut ne pas être unique. L'application d est injective sans être surjective : elle n'est pas inversible.

EXERCICE 4 ⋆⋆

1. Supposons f injective. Si $f \circ g = f \circ h$, alors $f(g(x)) = f(h(x))$ pour tout x, donc $g(x) = h(x)$: $g = h$. Réciproquement, supposons f simplifiable à gauche, et soit x, y tels que $f(x) = f(y)$. Les applications constantes g et h, de valeurs x et y, vérifient $f \circ g = f \circ h$, donc $g = h$ et $x = y$.

$$\boxed{f \text{ simplifiable à gauche} \iff f \text{ injective}}$$

2. Supposons f surjective et $g \circ f = h \circ f$. Tout $y \in E$ s'écrit $y = f(x)$, d'où $g(y) = h(y)$. Réciproquement, si f n'est pas surjective, soit y_0 hors de l'image de f, et $z_1 \neq z_2$ deux éléments de E. Les applications g et h égales à l'identité sauf en y_0, où $g(y_0) = z_1$ et $h(y_0) = z_2$, sont distinctes, mais $g \circ f = h \circ f$, puisque f ne prend jamais la valeur y_0.

$$\boxed{f \text{ simplifiable à droite} \iff f \text{ surjective}}$$

3. Si E est fini, une application de E dans E est injective si et seulement si elle est surjective (chapitre 2, théorème 2), d'où le résultat. Sur $\mathbb{N}$, le décalage d de l'exercice 3 est injectif sans être surjectif : il est simplifiable à gauche mais pas à droite.

$$\boxed{\text{vrai si } E \text{ est fini, faux pour } E = \mathbb{N}}$$

EXERCICE 5 ⋆⋆

1. La table est symétrique par rapport à sa diagonale, donc la loi est commutative ; la ligne et la colonne de e reproduisent les en-têtes, donc e est neutre. Chaque ligne et chaque colonne contient les six éléments. En particulier, e apparaît une fois dans chaque ligne : chaque élément x a un unique y tel que $x \star y = e$, et $y \star x = e$ par commutativité.

$$\boxed{a^{-1} = a, \qquad b^{-1} = d, \qquad c^{-1} = f}$$

2. On lit sur la table $b \star b = d$ et $b \star d = e$, d'où

$$(b \star b) \star d = d \star d = c \qquad \text{et} \qquad b \star (b \star d) = b \star e = b.$$

$$\boxed{(b \star b) \star d \neq b \star (b \star d) : \text{la loi n'est pas associative, } (E, \star) \text{ n'est pas un groupe}}$$

3. La remarque du cours dit que la table d'un groupe fini a la propriété de la question 1. Cet exemple montre que la réciproque est fausse : une table où chaque élément apparaît une fois par ligne et par colonne, avec un neutre, peut ne pas être associative. *À retenir :* l'associativité ne se lit pas sur l'aspect de la table, elle se vérifie, ou s'hérite d'un groupe connu (méthode de la section 11.3).

EXERCICE 6 ⋆⋆

Soit a et b dans A, et y, z dans E. On utilise trois fois la définition de A, pour a puis pour b :

$$(a \star b) \star (y \star z) = a \star (b \star (y \star z)) = a \star ((b \star y) \star z) = (a \star (b \star y)) \star z = ((a \star b) \star y) \star z.$$

La première et la troisième égalité utilisent $a \in A$, la deuxième $b \in A$, la dernière à nouveau $a \in A$. Ainsi $a \star b \in A$.

$$\boxed{A \text{ est stable par } \star}$$

La loi induite est associative, puisque l'égalité qui définit A vaut en particulier pour y et z dans A. Pour la soustraction sur $\mathbb{Z}$, $x - (y - z) = (x - y) - z$ équivaut à $z = -z$, ce qui est faux pour $z = 1$, quel que soit x.

$$\boxed{\text{pour la soustraction sur } \mathbb{Z},\ A = \varnothing}$$

EXERCICE 7 ⋆⋆⋆

On note $u = 1_*$ et $v = 1_\otimes$.

1. Avec $a = v$, $b = u$, $c = u$, $d = v$, l'hypothèse donne $(v \otimes u) * (u \otimes v) = (v * u) \otimes (u * v)$. Le membre de gauche vaut $u * u = u$, puisque v est neutre pour $\otimes$; celui de droite vaut $v \otimes v = v$, puisque u est neutre pour $*$.

$$\boxed{1_* = 1_\otimes}$$

2. On note 1 ce neutre commun. Avec $b = c = 1$, l'hypothèse donne $(a \otimes 1) * (1 \otimes d) = (a * 1) \otimes (1 * d)$, soit $a * d = a \otimes d$: les deux lois sont égales. Avec $a = d = 1$, elle donne $b * c = (1 * c) \otimes (b * 1) = c \otimes b = c * b$: la loi est commutative. Avec $b = 1$, elle donne $a * (c * d) = (a * c) * d$, en utilisant l'égalité des lois : la loi est associative.

$$\boxed{* = \otimes,\ \text{loi commutative et associative}}$$

3. Pour l'addition, l'hypothèse s'écrit $(a + b) + (c + d) = (a + c) + (b + d)$, qui est vraie. Avec l'addition pour $*$ et la multiplication pour $\otimes$, la question 1 imposerait $0 = 1$: l'hypothèse est fausse, et en effet $(1 \times 1) + (1 \times 1) = 2 \neq 4 = (1 + 1) \times (1 + 1)$.

À retenir. L'argument d'Eckmann et Hilton (1962) sert en topologie, pour montrer que certains groupes construits à partir de lacets sont abéliens : deux structures compatibles au sens de l'hypothèse sont forcément identiques et commutatives.

Groupes

EXERCICE 8 ⋆

(a) Oui. La bijection $a \mapsto a+1$ vérifie $(a \star b)+1 = (a+1)+(b+1)$: elle transporte $\star$ sur l'addition. Le neutre est -1, et le symétrique de a est $-a-2$. Le groupe est abélien.

(b) Non : $(8 \div 4) \div 2 = 1$, alors que $8 \div (4 \div 2) = 4$. La division n'est pas associative.

(c) Oui, groupe abélien de neutre la fonction nulle : chaque propriété se vérifie point par point.

(d) Non : $x \mapsto x^3$ et $x \mapsto -x$ sont monotones, mais leur somme $x \mapsto x^3 - x$ ne l'est pas, puisqu'elle s'annule en -1, 0 et 1. L'ensemble n'est pas stable.

(e) Non : 0 n'est pas inversible.

(f) Oui, groupe abélien : c'est $\mathbb{U}_2$.

(g) Non : $1 \notin 2\mathbb{Z}$, et il n'y a pas de neutre, puisque $2e = 2$ impose $e = 1$.

(h) Non, si $E \neq \varnothing$: le neutre est $\varnothing$, et $E \cup B = \varnothing$ est impossible.

$$\boxed{\text{groupes : (a), (c), (f), tous abéliens}}$$

EXERCICE 9 ⋆

1. On développe :

$$(1-x)(1-y) = 1 - x - y + xy = 1 - x \star y. \qquad \boxed{1 - x \star y = (1-x)(1-y)}$$

Si $x \neq 1$ et $y \neq 1$, le produit est non nul, donc $x \star y \neq 1$: la loi est interne sur G.

2. L'application φ est bijective de G sur $\mathbb{R}^*$, de réciproque $t \mapsto 1-t$, et la question 1 s'écrit $\varphi(x \star y) = \varphi(x)\varphi(y)$.

3. Par la question 1 de l'exercice 11, la loi transportée de $(\mathbb{R}^*, \times)$ par φ^{-1} est un groupe abélien, et c'est $\star$. Le neutre est $\varphi^{-1}(1) = 0$, et le symétrique de x est $\varphi^{-1}(\dfrac{1}{1-x}) = 1 - \dfrac{1}{1-x} = \dfrac{x}{x-1}$.

$$\boxed{\text{neutre } 0, \qquad x^{-1} = \frac{x}{x-1}}$$

Vérification : $x \star \dfrac{x}{x-1} = x + \dfrac{x}{x-1} - \dfrac{x^2}{x-1} = x + \dfrac{x(1-x)}{x-1} = 0$. ✓

EXERCICE 10 ⋆⋆

1. Pour tout réel t,

$$f_{x,y}(f_{x',y'}(t)) = x(x't + y') + y = xx't + (xy' + y). \qquad \boxed{f_{x,y} \circ f_{x',y'} = f_{(x,y)\star(x',y')}}$$

2. L'application $F : (x,y) \mapsto f_{x,y}$ est une bijection de G sur l'ensemble $\mathcal{A}$ des bijections affines, puisqu'une fonction affine détermine ses coefficients. D'après la question 1, $\mathcal{A}$ est stable par composition ; il contient $\mathrm{id}_{\mathbb{R}} = f_{1,0}$, et la réciproque de $f_{x,y}$ est $f_{1/x,-y/x}$. C'est donc un sous-groupe de $\mathfrak{S}_{\mathbb{R}}$ (proposition 7). La loi $\star$ est la loi transportée par F^{-1} (exercice 11), donc $(G, \star)$ est un groupe isomorphe à $\mathcal{A}$.

$$\boxed{\text{neutre } (1,0), \qquad (x,y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)}$$

Le groupe n'est pas abélien : $(2,0) \star (1,1) = (2,2)$ et $(1,1) \star (2,0) = (2,1)$.

3. Par récurrence, $(x,y)^n = (x^n, y(1 + x + \cdots + x^{n-1}))$, puisque $(x,y)^{n+1} = (x,y) \star (x,y)^n$ ajoute $x \cdot y(1 + \cdots + x^{n-1})$ à y. La somme géométrique donne

$$\boxed{(x,y)^n = \left(x^n,\ y\,\frac{x^n - 1}{x-1}\right) \text{ si } x \neq 1, \qquad (1,y)^n = (1, ny)}$$

C'est la n-ième itérée de $t \mapsto xt + y$, que le chapitre 7 a rencontrée avec les suites arithmético-géométriques.

EXERCICE 11 ⋆⋆

1. Par construction, $f(a*b) = f(a)\star f(b)$ pour tous a, b de G. On vérifie les axiomes en se ramenant à G : pour x, y, z dans E, avec $a = f^{-1}(x)$, $b = f^{-1}(y)$, $c = f^{-1}(z)$,

$$(x \star y) \star z = f((a * b) * c) = f(a * (b * c)) = x \star (y \star z).$$

De même, $f(e)$ est neutre, et l'inverse de x est $f(a^{-1})$. Ainsi $(E, \star)$ est un groupe, et f, bijectif et compatible avec les lois, est un isomorphisme.

2. On écrit $\operatorname{th} = \dfrac{\operatorname{sh}}{\operatorname{ch}}$ et l'on utilise les formules d'addition du chapitre 5 :

$$\operatorname{th}(a+b) = \frac{\operatorname{sh} a \operatorname{ch} b + \operatorname{ch} a \operatorname{sh} b}{\operatorname{ch} a \operatorname{ch} b + \operatorname{sh} a \operatorname{sh} b} = \frac{\operatorname{th} a + \operatorname{th} b}{1 + \operatorname{th} a \, \operatorname{th} b},$$

en divisant numérateur et dénominateur par $\operatorname{ch} a \operatorname{ch} b > 0$.

3. La fonction th est une bijection de $\mathbb{R}$ sur $]-1\,,1[$ (chapitre 5), et la question 2 dit que la loi transportée de $(\mathbb{R}, +)$ par th est $\star$. Par la question 1,

$$\boxed{(]-1\,,1[, \star) \text{ est un groupe abélien isomorphe à } (\mathbb{R}, +), \text{ par th}}$$

Le neutre est $\operatorname{th} 0 = 0$, et le symétrique de x est $-x$. Une vérification directe de l'associativité serait pénible ; le transport de structure la rend gratuite.

EXERCICE 12 ⋆

Pour tous x et y, l'hypothèse donne $x^{-1} = x$, $y^{-1} = y$ et $(xy)^{-1} = xy$. Par la proposition 2,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx. \qquad \boxed{G \text{ est abélien}}$$

Le groupe $(\mathcal{P}(E), \Delta)$, avec $E = \{1, 2\}$, convient : il a quatre éléments, et $A \,\Delta\, A = \varnothing$ pour toute partie A.

EXERCICE 13 ⋆⋆

1. Pour $k = 0$, les deux membres valent e. Si l'égalité est vraie au rang k, alors

$$(xyx^{-1})^{k+1} = (xy^kx^{-1})(xyx^{-1}) = xy^k(x^{-1}x)yx^{-1} = xy^{k+1}x^{-1}.$$

En d'autres termes, $\tau_x : g \mapsto xgx^{-1}$ est un morphisme (exercice 26), et la proposition 10 s'applique.

2. On applique τ_x à l'égalité $xyx^{-1} = y^2$, puis la question 1 :

$$x^2yx^{-2} = x\,(xyx^{-1})\,x^{-1} = xy^2x^{-1} = (xyx^{-1})^2 = y^4.$$

Une troisième fois, $x^3yx^{-3} = xy^4x^{-1} = (y^2)^4 = y^8$. Comme $x^3 = e$, le membre de gauche vaut y, d'où $y = y^8$.

$$\boxed{x^2yx^{-2} = y^4, \qquad y^7 = e}$$

3. Si de plus $y^5 = e$, alors $y = y^{15} \cdot y^{-14} = (y^5)^3\,((y^7)^2)^{-1} = e$.

$$\boxed{y = e}$$

À retenir. On a combiné $y^7 = e$ et $y^5 = e$ grâce à la relation $15 - 14 = 1$, c'est-à-dire $3 \times 5 - 2 \times 7 = 1$. Le chapitre 12 appellera cela une relation de Bézout.

EXERCICE 14 ⋆⋆

1. Le neutre commute avec tout, donc $e \in Z(G)$. Si x et y sont dans $Z(G)$ et $a \in G$, alors $ay = ya$ donne $y^{-1}a = ay^{-1}$, en multipliant à gauche et à droite par y^{-1} ; puis

$$a(xy^{-1}) = xay^{-1} = xy^{-1}a,$$

donc $xy^{-1} \in Z(G)$ (proposition 7). Deux éléments de $Z(G)$ commutent, puisque chacun commute avec tout élément de G. Enfin $Z(G) = G$ signifie exactement que tous les éléments commutent deux à deux.

$$\boxed{Z(G) \text{ est un sous-groupe abélien}, \quad Z(G) = G \iff G \text{ abélien}}$$

2. Soit $\sigma \in \mathfrak{S}_3$ distinct de l'identité, et a tel que $\sigma(a) = b \neq a$. Soit c le troisième élément de $\{1, 2, 3\}$, et τ l'échange de b et c, qui fixe a. Alors $(\sigma \circ \tau)(a) = \sigma(a) = b$, et $(\tau \circ \sigma)(a) = \tau(b) = c \neq b$. Ainsi $\sigma \notin Z(\mathfrak{S}_3)$.

$$\boxed{Z(\mathfrak{S}_3) = \{\mathrm{id}\}}$$

EXERCICE 15 ⋆

(a) Les entiers pairs forment le sous-groupe $2\mathbb{Z}$. Les impairs n'en forment pas un, puisque 0 n'est pas impair.

(b) Non : $0 - 2 = -2 \notin [-1\,, +\infty[$.

(c) Oui : $1 \in \mathbb{Q}^*$, et $\dfrac{x}{y} \in \mathbb{Q}^*$ si x et y sont des rationnels non nuls.

(d) Non : $\dfrac{1}{2}$ appartient à H, mais pas son inverse 2.

(e) Oui : $\mathrm{id}(a) = a$, et si $f(a) = g(a) = a$, alors $g^{-1}(a) = a$ et $(f \circ g^{-1})(a) = a$.

(f) Non : $\mathrm{id} \notin H$, puisque $\mathrm{id}(a) = a \neq b$.

(g) Oui : $(0, 0) \in H$ et $(k, k) - (\ell, \ell) = (k - \ell, k - \ell)$. Ce n'est pas un produit : si $H = H_1 \times H_2$, alors $(1, 1) \in H$ donne $1 \in H_1$ et $0 \in H_2$, puis $(1, 0) \in H$, ce qui est faux.

$$\boxed{\text{sous-groupes : } 2\mathbb{Z},\ \mathbb{Q}^*,\ \text{(e) et (g)}}$$

À retenir. La partie (g), la « diagonale », montre qu'un sous-groupe d'un groupe produit n'est pas toujours un produit de sous-groupes.

EXERCICE 16 ⋆

1. L'ensemble $\mathbb{U}_\infty$ contient 1. Si $z^n = 1$ et $w^m = 1$, alors $\left(\dfrac{z}{w}\right)^{nm} = \dfrac{(z^n)^m}{(w^m)^n} = 1$, donc $\dfrac{z}{w} \in \mathbb{U}_\infty$. C'est un sous-groupe de $\mathbb{C}^*$, contenu dans $\mathbb{U}$. Il n'est pas égal à $\mathbb{U}$: si $\left(\mathrm{e}^{\mathrm{i}\pi\sqrt{2}}\right)^n = 1$ avec $n \geqslant 1$, alors $n\pi\sqrt{2} \in 2\pi\mathbb{Z}$ (chapitre 4), donc $\sqrt{2} = \dfrac{2k}{n}$ serait rationnel.

$$\boxed{\mathbb{U}_\infty \text{ est un sous-groupe de } \mathbb{C}^*, \text{ strictement contenu dans } \mathbb{U}}$$

2. Le corps $\mathbb{Q}[\sqrt{2}]$ du cours a pour groupe des inversibles $\mathbb{Q}[\sqrt{2}] \setminus \{0\}$ (proposition 14), et ce groupe est contenu dans $\mathbb{R}^*$ avec la même loi : c'est un sous-groupe de $(\mathbb{R}^*, \times)$. Directement : 1 y appartient, et le cours a montré que l'inverse d'un élément non nul y appartient, ainsi que le produit de deux éléments.

EXERCICE 17 ⋆⋆

1. Si $x^2 - 3y^2 = 1$, alors $x^2 = 1 + 3y^2 > 3y^2$, donc $x > |y|\sqrt{3}$, puisque $x \geqslant 0$. Ainsi

$$x + y\sqrt{3} \geqslant x - |y|\sqrt{3} > 0.$$

2. Comme $\sqrt{3}$ est irrationnel, l'écriture $x + y\sqrt{3}$ est unique, et l'on peut parler de x et de y pour un élément de H. L'élément $1 = 1 + 0\sqrt{3}$ est dans H. Pour $u = x + y\sqrt{3}$ et $u' = x' + y'\sqrt{3}$ dans H, on a

$$uu' = (xx' + 3yy') + (xy' + x'y)\sqrt{3}, \qquad (xx' + 3yy')^2 - 3(xy' + x'y)^2 = (x^2 - 3y^2)(x'^2 - 3y'^2) = 1.$$

De plus $xx' > 3|yy'|$ par la question 1, donc $xx' + 3yy' \in \mathbb{N}$: $uu' \in H$. Enfin $(x + y\sqrt{3})(x - y\sqrt{3}) = 1$, donc $u^{-1} = x + (-y)\sqrt{3} \in H$.

$$\boxed{H \text{ est un sous-groupe de } (\mathbb{R}_+^*, \times)}$$

3. On a $2^2 - 3 \times 1^2 = 1$. Les puissances $(2 + \sqrt{3})^n$, pour $n \in \mathbb{N}$, sont dans H et deux à deux distinctes, puisque $2 + \sqrt{3} > 1$. On calcule les premières :

$$\boxed{(2, 1), \qquad (2 + \sqrt{3})^2 = 7 + 4\sqrt{3}, \qquad (2 + \sqrt{3})^3 = 26 + 15\sqrt{3}}$$

et $7^2 - 3 \times 4^2 = 1$, $26^2 - 3 \times 15^2 = 676 - 675 = 1$. ✓ C'est l'équation de Pell-Fermat ; on peut montrer que H est exactement l'ensemble des $(2 + \sqrt{3})^n$, $n \in \mathbb{Z}$.

EXERCICE 18 ⋆⋆

1. Si $H \subset K$, alors $H \cup K = K$ est un sous-groupe, de même si $K \subset H$. Réciproquement, supposons que $H \cup K$ soit un sous-groupe, et que $H \not\subset K$ et $K \not\subset H$. Soit $h \in H \setminus K$ et $k \in K \setminus H$. Le produit hk est dans $H \cup K$. S'il est dans H, alors $k = h^{-1}(hk) \in H$, ce qui est exclu ; s'il est dans K, alors $h = (hk)k^{-1} \in K$, exclu aussi. C'est absurde.

$$\boxed{H \cup K \text{ sous-groupe} \iff H \subset K \text{ ou } K \subset H}$$

2. Si $G = H \cup K$, alors $H \cup K$ est un sous-groupe, donc $G = K$ ou $G = H$ par la question 1.

3. Les trois parties $\{\varnothing, \{1\}\}$, $\{\varnothing, \{2\}\}$ et $\{\varnothing, \{1, 2\}\}$ sont des sous-groupes, puisque chaque partie est son propre inverse ; ils sont distincts de $\mathcal{P}(\{1, 2\})$, et leur réunion est $\mathcal{P}(\{1, 2\})$.

$$\boxed{\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}\} \cup \{\varnothing, \{2\}\} \cup \{\varnothing, \{1, 2\}\}}$$

Piège. La question 2 ne s'étend pas à trois sous-groupes, comme le montre cet exemple : l'argument de la question 1 utilise qu'il n'y a que deux sous-groupes en jeu.

EXERCICE 19 ⋆

1. Soit U la réunion. Elle contient $e \in H_0$. Si $x \in H_n$ et $y \in H_m$, avec par exemple $n \leqslant m$, alors x et y sont dans H_m, qui est un sous-groupe, donc $xy^{-1} \in H_m \subset U$.

$$\boxed{\bigcup_{n \in \mathbb{N}} H_n \text{ est un sous-groupe de } G}$$

C'est la croissance qui permet de ramener deux éléments dans un même H_m ; l'exercice 18 montre que la réunion de deux sous-groupes quelconques n'est pas un sous-groupe.

2. Comme 2^n divise 2^{n+1}, la proposition 9 donne $\mathbb{U}_{2^n} \subset \mathbb{U}_{2^{n+1}}$. Le nombre $e^{2i\pi/3}$ appartient à $\mathbb{U}_3$, et s'il appartenait à $\mathbb{U}_{2^n}$, on aurait $\mathbb{U}_3 \subset \mathbb{U}_{2^n}$, car $\mathbb{U}_3$ est formé de ses puissances, donc 3 diviserait 2^n par la proposition 9, ce qui est faux.

$$\boxed{e^{2i\pi/3} \notin \bigcup_n \mathbb{U}_{2^n}}$$

EXERCICE 20 ⋆⋆⋆

1. L'ensemble des sous-groupes contenant X est non vide, puisqu'il contient G. Leur intersection $\langle X\rangle$ est un sous-groupe (proposition 8), qui contient X. Si H est un sous-groupe contenant X, il fait partie de la famille, donc $\langle X\rangle \subset H$.

2. Soit P l'ensemble des produits décrits. Il contient e (produit vide) et X (produits d'un facteur, avec $\varepsilon = 1$). Il est stable par produit, en mettant bout à bout deux produits, et par inverse, puisque

$$\left(x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}\right)^{-1} = x_n^{-\varepsilon_n}\cdots x_1^{-\varepsilon_1}.$$

C'est donc un sous-groupe contenant X, et $\langle X\rangle \subset P$. Réciproquement, un sous-groupe qui contient X contient les $x_i^{\pm 1}$ et leurs produits, donc $P \subset \langle X\rangle$.

$$\boxed{\langle X\rangle = \{x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n} \mid n\in\mathbb{N},\ x_i\in X,\ \varepsilon_i = \pm 1\}}$$

3. Dans $(\mathbb{Z},+)$, les éléments de $\langle 4,6\rangle$ sont les $4m+6n$, qui sont pairs ; inversement, il contient $6-4=2$, donc $2\mathbb{Z}$. Dans $\mathbb{C}^*$, $\langle \mathrm{i}\rangle = \{\mathrm{i}^n \mid n\in\mathbb{Z}\} = \{1,\mathrm{i},-1,-\mathrm{i}\}$. Dans $\mathbb{Q}^*$, $\langle 2,3\rangle$ est formé des produits 2^a3^b, avec a et b dans $\mathbb{Z}$, puisque les facteurs commutent.

$$\boxed{\langle 4,6\rangle = 2\mathbb{Z}, \qquad \langle \mathrm{i}\rangle = \mathbb{U}_4, \qquad \langle 2,3\rangle = \{2^a3^b \mid (a,b)\in\mathbb{Z}^2\}}$$

Le chapitre 12 montrera que le sous-groupe de $\mathbb{Z}$ engendré par a et b est $d\mathbb{Z}$, où d est le PGCD de a et b : ici $d=2$.

EXERCICE 21 ⋆⋆

1. Le réel 0 est une période. Si T et T' sont des périodes, alors, pour tout réel x,

$$f(x+T-T') = f((x-T')+T) = f(x-T') = f((x-T')+T') = f(x).$$

Ainsi $P(f)$ est un sous-groupe de $\mathbb{R}$. Pour $f = \mathbf{1}_{\mathbb{Q}}$, un réel T est une période si et seulement si $x+T$ et x sont simultanément rationnels ou non, pour tout x ; c'est le cas si $T\in\mathbb{Q}$, et pas sinon, en prenant $x=0$.

$$\boxed{P(\mathbf{1}_{\mathbb{Q}}) = \mathbb{Q}}$$

2. La fonction f est de classe $\mathcal{C}^2$, et le calcul donne

$$f'' + \frac{\pi^2}{64}f = \left(\frac{\pi^2}{64} - \frac{\pi^2}{144}\right)\cos\frac{\pi x}{12} = \frac{5\pi^2}{576}\cos\frac{\pi x}{12}.$$

Si T est une période de f, c'en est une de f'', donc de $x\mapsto \cos\dfrac{\pi x}{12}$: $T\in 24\mathbb{Z}$. De même, $f''+\dfrac{\pi^2}{144}f$ est un multiple non nul de $\sin\dfrac{\pi x}{8}$, donc $T\in 16\mathbb{Z}$. Si $T = 24k = 16m$, alors $3k = 2m$, donc k est pair et $T\in 48\mathbb{Z}$; réciproquement, 48 est une période.

$$\boxed{P(f) = 48\mathbb{Z}}$$

3. De même, toute période de g appartient à $2\pi\mathbb{Z}$ et à $\sqrt{2}\pi\mathbb{Z}$, les périodes de $\sin(\sqrt{2}\,x)$. Si $T = 2\pi k = \sqrt{2}\pi m$ avec $T\neq 0$, alors $\sqrt{2} = \dfrac{2k}{m}$ serait rationnel.

$$\boxed{P(g) = \{0\} : g \text{ n'est pas périodique}}$$

La somme de deux fonctions périodiques n'est donc pas toujours périodique : il faut que les périodes aient un rapport rationnel. L'exercice 53 explique pourquoi : $2\pi\mathbb{Z} + \sqrt{2}\pi\mathbb{Z}$ est dense dans $\mathbb{R}$.

EXERCICE 22 ⋆

Dans chaque cas, on identifie les deux groupes, puis on cherche les antécédents du neutre.

(a) Le logarithme est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, de noyau $\{1\}$ et d'image $\mathbb{R}$: c'est un isomorphisme (chapitre 5).

(b) Le module est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$. Son noyau est $\mathbb{U}$ et son image $\mathbb{R}_+^*$, puisque $|r| = r$ pour $r > 0$: il est surjectif, non injectif.

(c) La racine carrée est un morphisme de $(\mathbb{R}_+^*, \times)$ dans lui-même, de noyau $\{1\}$, bijectif de réciproque $x \mapsto x^2$: c'est un automorphisme.

(d) La conjugaison est un morphisme de $(\mathbb{C}^*, \times)$ dans lui-même, de noyau $\{1\}$, et sa propre réciproque : c'est un automorphisme.

(e) L'application $t \mapsto \mathrm{e}^{\mathrm{i}t}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$, surjectif, de noyau $2\pi\mathbb{Z}$ (cours, exemple qui suit le théorème 2) : il n'est pas injectif.

(f) L'application $n \mapsto (-1)^n$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{U}_2, \times)$, surjectif, de noyau $2\mathbb{Z}$.

$$\boxed{\text{isomorphismes : (a), (c), (d)} ; \quad \text{noyaux non triviaux : } \mathbb{U},\ 2\pi\mathbb{Z},\ 2\mathbb{Z}}$$

EXERCICE 23 ⋆

L'application $x \mapsto x^2$ est un morphisme si et seulement si $(xy)^2 = x^2y^2$ pour tous x et y, c'est-à-dire, d'après la remarque qui suit la proposition 4, si et seulement si $xy = yx$ pour tous x, y. De même, $x \mapsto x^{-1}$ est un morphisme si et seulement si $(xy)^{-1} = x^{-1}y^{-1}$, soit $y^{-1}x^{-1} = x^{-1}y^{-1}$ pour tous x, y ; en passant à l'inverse, c'est $xy = yx$.

$$\boxed{x \mapsto x^2 \text{ et } x \mapsto x^{-1} \text{ sont des morphismes si et seulement si } G \text{ est abélien}}$$

À retenir. Dans un groupe abélien, $x \mapsto x^{-1}$ est même un automorphisme, puisqu'il est sa propre réciproque.

EXERCICE 24 ⋆⋆

1. D'après le chapitre 4, $\mathrm{e}^{z+w} = \mathrm{e}^z\mathrm{e}^w$ et $\mathrm{e}^z \neq 0$: exp est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$. Tout $a \in \mathbb{C}^*$ s'écrit $a = r\mathrm{e}^{\mathrm{i}\theta}$ avec $r > 0$, et $a = \mathrm{e}^{\ln r + \mathrm{i}\theta}$: le morphisme est surjectif. Enfin $\mathrm{e}^{x+\mathrm{i}y} = 1$ si et seulement si $\mathrm{e}^x = 1$ et $\mathrm{e}^{\mathrm{i}y} = 1$, soit $x = 0$ et $y \in 2\pi\mathbb{Z}$.

$$\boxed{\operatorname{Im}\exp = \mathbb{C}^*, \qquad \operatorname{Ker}\exp = 2\mathrm{i}\pi\mathbb{Z}}$$

2. D'après le point (i) du théorème 2, écrit en notation additive au départ, $\mathrm{e}^z = \mathrm{e}^{z_0}$ si et seulement si $z - z_0 \in \operatorname{Ker}\exp$. Pour $a = -2 = 2\mathrm{e}^{\mathrm{i}\pi}$, on peut prendre $z_0 = \ln 2 + \mathrm{i}\pi$.

$$\boxed{\{z \in \mathbb{C} \mid \mathrm{e}^z = a\} = z_0 + 2\mathrm{i}\pi\mathbb{Z}, \qquad \mathrm{e}^z = -2 \iff z \in \ln 2 + \mathrm{i}\pi + 2\mathrm{i}\pi\mathbb{Z}}$$

EXERCICE 25 ⋆⋆

1. D'après la proposition 10, $f(n\cdot 1) = f(1)^n$ pour tout $n \in \mathbb{Z}$, car $n = n\cdot 1$ dans $(\mathbb{Z}, +)$. Ainsi f est déterminé par $f(1)$, d'où l'unicité. Réciproquement, $n \mapsto x^n$ est un morphisme d'après la proposition 4, et il envoie 1 sur x.

$$\boxed{\text{les morphismes de } (\mathbb{Z}, +) \text{ dans } G \text{ sont les } n \mapsto x^n,\ x \in G}$$

2. En notation additive, les endomorphismes de $\mathbb{Z}$ sont les $n \mapsto kn$, avec $k \in \mathbb{Z}$. Un tel endomorphisme est injectif si et seulement si $k \neq 0$, puisque son noyau est $\{0\}$ si $k \neq 0$ et $\mathbb{Z}$ si $k = 0$. Il est surjectif si et seulement si 1 est atteint, c'est-à-dire $kn = 1$ pour un entier n, soit $k = \pm 1$.

$$\boxed{\text{endomorphismes } n \mapsto kn;\ \text{injectifs si } k \neq 0;\ \text{surjectifs si } k = \pm 1}$$

3. Pour $m \in \mathbb{N}$, on a $x = 2^m \cdot \dfrac{x}{2^m}$ dans $(\mathbb{Q}, +)$, donc $f(x) = 2^m f(\dfrac{x}{2^m})$ par la proposition 10 : l'entier $f(x)$ est divisible par 2^m. Si $f(x) \neq 0$, on aurait $2^m \leqslant |f(x)|$ pour tout m, ce qui est absurde.

$$\boxed{\text{le seul morphisme de } (\mathbb{Q}, +) \text{ dans } (\mathbb{Z}, +) \text{ est le morphisme nul}}$$

À retenir. Tout rationnel est « divisible » par tout entier dans $\mathbb{Q}$, alors qu'aucun entier non nul n'est divisible par toutes les puissances de 2 : un morphisme transporte la divisibilité, d'où l'obstruction.

EXERCICE 26 ⋆⋆

1. Pour x et y dans G,

$$\tau_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \tau_a(x)\tau_a(y), \qquad \tau_a(\tau_b(x)) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \tau_{ab}(x).$$

Comme $\tau_e = \mathrm{id}_G$, on a $\tau_a \circ \tau_{a^{-1}} = \tau_{a^{-1}} \circ \tau_a = \mathrm{id}_G$: τ_a est bijectif.

$$\boxed{\tau_a \text{ est un automorphisme,} \qquad \tau_a \circ \tau_b = \tau_{ab}}$$

2. La relation $\tau_{ab} = \tau_a \circ \tau_b$ dit exactement que Φ est un morphisme de G dans $(\mathfrak{S}_G, \circ)$. Son image est un sous-groupe par la proposition 12.

3. On a $\tau_a = \mathrm{id}_G$ si et seulement si $axa^{-1} = x$, soit $ax = xa$, pour tout x, c'est-à-dire si et seulement si $a \in Z(G)$.

$$\boxed{\operatorname{Ker} \Phi = Z(G)}$$

Pour $G = \mathfrak{S}_3$, le centre est réduit à l'identité (exercice 14), donc Φ est injectif. Pour G abélien, $Z(G) = G$ et Φ est constant, égal à id_G : il n'est injectif que si $G = \{e\}$.

EXERCICE 27 ⋆⋆

Si $f : G \to G'$ est un isomorphisme et si $x^k = e$, alors $f(x)^k = e'$, et réciproquement par f^{-1} : l'isomorphisme réalise une bijection entre les solutions de $x^k = e$ dans G et dans G'. Le même argument vaut pour toute propriété exprimée par la seule loi.

(a) Dans $(\mathbb{R}, +)$, l'équation $x + x = 0$ n'a que la solution 0 ; dans $(\mathbb{R}^*, \times)$, l'équation $x^2 = 1$ en a deux, 1 et -1.

(b) Dans $\mathbb{R}^*$, $x^4 = 1$ a deux solutions, ± 1 ; dans $\mathbb{C}^*$, elle en a quatre, les éléments de $\mathbb{U}_4$.

(c) Dans $(\mathbb{Q}, +)$, tout élément est le double d'un autre : $x = \dfrac{x}{2} + \dfrac{x}{2}$. Dans $(\mathbb{Q}_+^*, \times)$, cela s'écrirait : tout élément est un carré. Or 2 n'est pas le carré d'un rationnel, puisque $\sqrt{2}$ est irrationnel (chapitre 7).

(d) Supposons $f : \mathbb{R}^* \to \mathbb{Q}^*$ un isomorphisme. Le seul élément d'ordre 2 de chaque groupe est -1, donc $f(-1) = -1$. Tout réel non nul s'écrit $x = \pm y^2$, donc $f(x) = f(\pm 1) f(y)^2 = \pm f(y)^2$: tout élément de $\mathbb{Q}^*$ serait, au signe près, un carré de $\mathbb{Q}^*$. Or 2 ne l'est pas.

$$\boxed{\text{aucun des quatre couples n'est formé de groupes isomorphes}}$$

Piège. Pour montrer que deux groupes ne sont pas isomorphes, il ne suffit pas de constater qu'un isomorphisme particulier échoue : il faut trouver une propriété, exprimée avec la seule loi, que l'un possède et pas l'autre.

EXERCICE 28 ⋆⋆

Pour $z \in \mathbb{C}^*$, on pose $f(z) = (\frac{z}{|z|}, |z|)$, qui appartient à $\mathbb{U} \times \mathbb{R}_+^*$. Comme le module est multiplicatif,

$$f(zw) = \Big(\frac{z}{|z|} \cdot \frac{w}{|w|},\ |z|\,|w|\Big) = f(z)f(w)$$

pour la loi du groupe produit (proposition 6). L'application $(u, r) \mapsto ru$ est la réciproque de f, puisque $\dfrac{ru}{|ru|} = u$ et $|ru| = r$. Ainsi f est un isomorphisme. L'exponentielle est un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$; en le combinant avec l'identité de $\mathbb{U}$, on obtient un isomorphisme de $\mathbb{U} \times \mathbb{R}$ sur $\mathbb{U} \times \mathbb{R}_+^*$, et par composition (proposition 11),

$$\boxed{(\mathbb{C}^*, \times) \simeq \mathbb{U} \times \mathbb{R}_+^* \simeq \mathbb{U} \times (\mathbb{R}, +), \qquad z = |z|\,\frac{z}{|z|} = \mathrm{e}^{\ln|z|}\mathrm{e}^{\mathrm{i}\theta}}$$

C'est l'écriture trigonométrique $z = r\mathrm{e}^{\mathrm{i}\theta}$ du chapitre 4 : le produit de deux nombres complexes multiplie les modules et ajoute les arguments.

EXERCICE 29 ⋆⋆

1. Comme f n'est pas constant et que $f(e) = 1$, il existe a tel que $f(a) \neq 1$. L'application $x \mapsto ax$ est une bijection de G, de réciproque $x \mapsto a^{-1}x$ (proposition 3). Ainsi, quand x décrit G, ax décrit G, et

$$f(a)S = \sum_{x \in G} f(a)f(x) = \sum_{x \in G} f(ax) = \sum_{y \in G} f(y) = S.$$

Comme $f(a) \neq 1$, on en déduit $S = 0$. $\boxed{S = 0}$

2. On applique ce résultat à $G = \mathbb{U}_n$ et $f : z \mapsto z^k$, morphisme de $\mathbb{U}_n$ dans $\mathbb{C}^*$. Il n'est pas constant, puisque $f(\mathrm{e}^{2\mathrm{i}\pi/n}) = \mathrm{e}^{2\mathrm{i}k\pi/n} \neq 1$ lorsque n ne divise pas k.

$$\boxed{\sum_{z \in \mathbb{U}_n} z^k = 0 \quad \text{si } n \nmid k}$$

Si n divise k, la somme vaut n, puisque chaque terme vaut 1.

EXERCICE 30 ⋆⋆⋆

1. L'application σ_g est bijective, de réciproque $\sigma_{g^{-1}}$ (proposition 3). Pour tout $x \in G$, on a $\sigma_g(\sigma_h(x)) = ghx = \sigma_{gh}(x)$.

2. La relation $\sigma_{gh} = \sigma_g \circ \sigma_h$ dit que $g \mapsto \sigma_g$ est un morphisme de G dans $\mathfrak{S}_G$. Si $\sigma_g = \mathrm{id}_G$, alors $g = \sigma_g(e) = e$: le noyau est trivial, et le morphisme est injectif (théorème 2). Il induit donc un isomorphisme de G sur son image, qui est un sous-groupe de $\mathfrak{S}_G$ (proposition 12).

$$\boxed{G \text{ est isomorphe à un sous-groupe de } \mathfrak{S}_G}$$

3. Avec $\mathbb{U}_3 = \{1, j, j^2\}$, on a $\sigma_1 = \mathrm{id}$, puis

$$\boxed{\sigma_j : 1 \mapsto j,\ j \mapsto j^2,\ j^2 \mapsto 1; \qquad \sigma_{j^2} : 1 \mapsto j^2,\ j \mapsto 1,\ j^2 \mapsto j}$$

Ce sont les deux permutations circulaires des trois points : $\mathbb{U}_3$ s'identifie aux rotations du triangle équilatéral de sommets 1, j, j^2.

EXERCICE 31 ⋆⋆⋆

1. On a $x^{-1}x = e \in H$: la relation est réflexive. Si $x^{-1}y \in H$, son inverse $y^{-1}x$ y est aussi : elle est symétrique. Si $x^{-1}y$ et $y^{-1}z$ sont dans H, leur produit $x^{-1}z$ aussi : elle est transitive. Enfin $y \sim x$, c'est-à-dire $x^{-1}y = h \in H$, équivaut à $y = xh$.

$$\boxed{\text{la classe de } x \text{ est } xH = \{xh \mid h \in H\}}$$

2. L'application $h \mapsto xh$ est une bijection de H sur xH, injective par simplification (proposition 3) : chaque classe a $\text{card}(H)$ éléments. Soit $\mathcal{C}$ l'ensemble des classes, qui est fini, et $\pi : G \to \mathcal{C}$ l'application qui à x associe sa classe. La fibre de π au-dessus d'une classe est cette classe elle-même, qui a $\text{card}(H)$ éléments ; le lemme des bergers (chapitre 2, lemme 5) donne

$$\boxed{\text{card}(G) = \text{card}(\mathcal{C}) \times \text{card}(H)}$$

et $\text{card}(H)$ divise $\text{card}(G)$.

3. Les éléments $x^0, x^1, \dots, x^n$, où $n = \text{card}(G)$, sont $n+1$ éléments de G : par le principe des tiroirs (chapitre 2, lemme 1), deux d'entre eux sont égaux, $x^i = x^j$ avec $i < j$. Alors $x^{j-i} = e$ avec $j - i \geqslant 1$, et l'ensemble des entiers $k \geqslant 1$ tels que $x^k = e$ est une partie non vide de $\mathbb{N}$: elle a un plus petit élément p.

4. Soit $K = \{e, x, \dots, x^{p-1}\}$. Pour $k \in \mathbb{Z}$, la division euclidienne $k = qp + r$, avec $0 \leqslant r < p$, donne $x^k = (x^p)^q x^r = x^r \in K$. Ainsi K est l'ensemble des x^k, $k \in \mathbb{Z}$, qui est stable par produit et par inverse : c'est un sous-groupe. Ses éléments sont distincts : si $x^i = x^j$ avec $0 \leqslant i < j < p$, alors $x^{j-i} = e$ avec $0 < j - i < p$, ce qui contredit la minimalité de p. Par la question 2, p divise $n = \text{card}(G)$, et $x^n = (x^p)^{n/p} = e$.

$$\boxed{p \mid \text{card}(G), \qquad x^{\text{card}(G)} = e}$$

5. Soit $x \neq e$ dans G. Son ordre p divise q et n'est pas 1, donc $p = q$, et $G = \{e, x, \dots, x^{q-1}\}$. L'application $f : x^k \mapsto \mathrm{e}^{2\mathrm{i}k\pi/q}$ est bien définie, puisque $x^k = x^\ell$ si et seulement si q divise $k - \ell$; c'est un morphisme, car $x^k x^\ell = x^{k+\ell}$ et $\mathrm{e}^{2\mathrm{i}k\pi/q}\mathrm{e}^{2\mathrm{i}\ell\pi/q} = \mathrm{e}^{2\mathrm{i}(k+\ell)\pi/q}$, et elle est bijective de G sur $\mathbb{U}_q$ (chapitre 4).

$$\boxed{G \simeq (\mathbb{U}_q, \times)}$$

À retenir. Ce résultat, qui porte le nom de Lagrange bien qu'il ne l'ait pas énoncé sous cette forme, est le premier théorème de structure des groupes finis : le cardinal d'un groupe contraint fortement ses sous-groupes.

EXERCICE 32 ⋆⋆

1. D'après le point (i) du théorème 2, la fibre de f au-dessus d'un élément $f(x)$ de l'image est xK, où $K = \text{Ker}\, f$, et elle a $\text{card}(K)$ éléments (exercice 31, question 2). On applique le lemme des bergers à $f : G \to \text{Im}\, f$.

$$\boxed{\text{card}(G) = \text{card}(\text{Ker}\, f) \times \text{card}(\text{Im}\, f)}$$

2. Le noyau de $z \mapsto z^2$ sur $\mathbb{U}_n$ est $\mathbb{U}_n \cap \{-1, 1\}$. Si n est impair, il est réduit à $\{1\}$, et l'image a n éléments : c'est $\mathbb{U}_n$. Si n est pair, $-1 \in \mathbb{U}_n$, et l'image a $\dfrac{n}{2}$ éléments ; elle est contenue dans $\mathbb{U}_{n/2}$, puisque $(z^2)^{n/2} = 1$, et a le même nombre d'éléments, donc lui est égale.

$$\boxed{\text{image } \mathbb{U}_n \text{ si } n \text{ est impair}, \qquad \mathbb{U}_{n/2} \text{ si } n \text{ est pair}}$$

3. Comme G est abélien, $x \mapsto x^2$ est un endomorphisme (exercice 23). Si $x^2 = e$ et $x \neq e$, alors x est d'ordre 2, et 2 divise $\text{card}(G)$ (exercice 31), ce qui est exclu. Le noyau est donc $\{e\}$, le morphisme est injectif, donc bijectif puisque G est fini (chapitre 2, théorème 2).

$$\boxed{\text{dans un groupe abélien fini de cardinal impair, tout élément est un carré}}$$

EXERCICE 33 ⋆⋆

1. Les six permutations sont distinctes : id fixe tout, c et c^2 ne fixent rien, et t_k fixe exactement k. Comme $\mathfrak{S}_3$ a six éléments (on peut les énumérer en choisissant l'image de 1, puis celle de 2), ce sont toutes. On calcule chaque composée $f \circ g$, ligne f et colonne g, en suivant les images de 1, 2, 3 :

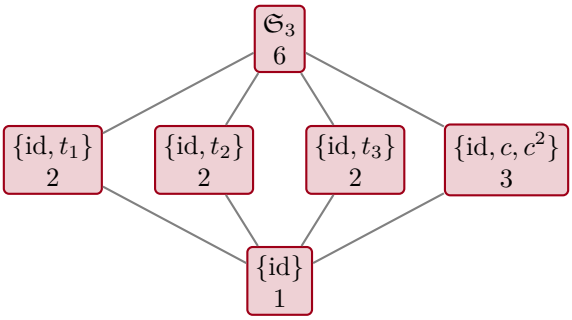
$\circ$	id	c	c^2	t_1	t_2	t_3
id	id	c	c^2	t_1	t_2	t_3
c	c	c^2	id	t_3	t_1	t_2
c^2	c^2	id	c	t_2	t_3	t_1
t_1	t_1	t_2	t_3	id	c	c^2
t_2	t_2	t_3	t_1	c^2	id	c
t_3	t_3	t_1	t_2	c	c^2	id

Par exemple, $(c \circ t_1)(1) = c(1) = 2$, $(c \circ t_1)(2) = c(3) = 1$ et $(c \circ t_1)(3) = c(2) = 3$: $c \circ t_1 = t_3$. La table n'est pas symétrique : $t_1 \circ c = t_2 \neq t_3$.

2. Un sous-groupe a 1, 2, 3 ou 6 éléments, par le théorème de Lagrange. Ceux à 1 et 6 éléments sont $\{\mathrm{id}\}$ et $\mathfrak{S}_3$. Un sous-groupe à 2 éléments est $\{\mathrm{id}, x\}$ avec $x^2 = \mathrm{id}$: ce sont les trois $\{\mathrm{id}, t_k\}$. Un sous-groupe à 3 éléments a 3 pour cardinal premier, donc il est formé des puissances d'un élément d'ordre 3 (exercice 31) : c'est $\{\mathrm{id}, c, c^2\}$.

$$\boxed{\{\mathrm{id}\},\ \{\mathrm{id}, t_1\},\ \{\mathrm{id}, t_2\},\ \{\mathrm{id}, t_3\},\ \{\mathrm{id}, c, c^2\},\ \mathfrak{S}_3 \text{ : six sous-groupes}}$$

3. Aucun sous-groupe à 2 éléments n'est contenu dans celui à 3 éléments, puisque 2 ne divise pas 3.



Le schéma se lit comme celui des $\mathbb{U}_d$ du cours : chaque trait monte d'un sous-groupe à un sous-groupe qui le contient. Contrairement au cas de $\mathbb{U}_{12}$, il y a plusieurs sous-groupes ayant le même nombre d'éléments.

EXERCICE 34 ⋆

On vérifie à chaque fois les trois conditions de la définition : $1 \in B$, stabilité par différence et par produit.

(a) $\mathbb{N}$ n'est pas un sous-anneau de $\mathbb{Z}$, puisque $0-1 \notin \mathbb{N}$, et $2\mathbb{Z}$ non plus, puisque $1 \notin 2\mathbb{Z}$.

(b) Les suites convergentes forment un sous-anneau : la suite constante égale à 1 converge, et la différence et le produit de deux suites convergentes convergent (chapitre 7). Les suites de limite nulle n'en forment pas un, puisque la suite constante 1 n'en fait pas partie. Les suites bornées en forment un : si $|u_n| \leqslant M$ et $|v_n| \leqslant M'$, alors $|u_n - v_n| \leqslant M + M'$ et $|u_n v_n| \leqslant MM'$.

(c) Les fonctions paires forment un sous-anneau ; les fonctions impaires non, puisque la fonction constante 1 n'est pas impaire, et que le produit de deux fonctions impaires est pair. Les fonctions continues en forment un (chapitre 8).

(d) $\mathbb{Z}[\sqrt{2}]$ contient 1, est stable par différence, et

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

En revanche, $B' = \{a+b\sqrt[3]{2}\}$ ne contient pas $\sqrt[3]{4} = (\sqrt[3]{2})^2$. Sinon, $\sqrt[3]{4} = a+b\sqrt[3]{2}$; en multipliant par $\sqrt[3]{2}$,

$$2 = a\sqrt[3]{2} + b\sqrt[3]{4} = ab + (a+b^2)\sqrt[3]{2}.$$

Comme $\sqrt[3]{2}$ est irrationnel, par le raisonnement du chapitre 7 pour $\sqrt{2}$, on obtient $a+b^2 = 0$ et $ab = 2$, d'où $-b^3 = 2$, ce qui est impossible dans $\mathbb{Z}$.

sous-anneaux : suites convergentes, bornées ; fonctions paires, continues ; $\mathbb{Z}[\sqrt{2}]$

EXERCICE 35 ⋆⋆

1. On a $1 = \dfrac{1}{1} \in A$. Si $x = \dfrac{m}{n}$ et $y = \dfrac{m'}{n'}$ avec n et n' impairs,

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

et nn' est impair. A est un sous-anneau de $\mathbb{Q}$

2. Si $\dfrac{m}{n} = \dfrac{m'}{n'}$ avec n et n' impairs, alors $mn' = m'n$. Le produit mn' a la parité de m, puisque n' est impair, et $m'n$ celle de m' : m et m' ont même parité.

3. Si m est impair, $x^{-1} = \dfrac{n}{m} = \dfrac{-n}{-m}$ a un dénominateur impair, positif dans l'une des deux écritures : x est inversible dans A. Si m est pair et $xy = 1$ avec $y = \dfrac{p}{q}$, q impair, alors $mp = nq$, où le membre de gauche est pair et celui de droite impair : c'est impossible.

$A^\times = \left\{ \dfrac{m}{n} \;\middle|\; m \text{ et } n \text{ impairs} \right\}$; A n'est pas un corps, 2 n'y est pas inversible

La question 2 est indispensable : sans elle, la condition « m impair » pourrait dépendre de l'écriture choisie.

EXERCICE 36 ⋆⋆

1. Par distributivité, $(a+b)^2 = a^2 + ab + ba + b^2$, qui est égal à $a^2 + 2ab + b^2$ si et seulement si $ba = ab$, par simplification dans le groupe $(A, +)$.

$$\boxed{(a+b)^2 = a^2 + 2ab + b^2 \iff ab = ba}$$

2. On pose $c = 1 + bua$, avec $u(1-ab) = (1-ab)u = 1$. On calcule, en factorisant b à gauche et a à droite :

$$(1-ba)c = 1 - ba + bua - babua = 1 - ba + b\big(u - abu\big)a = 1 - ba + b\big((1-ab)u\big)a = 1 - ba + ba = 1,$$

et de même $c(1-ba) = 1 - ba + b\big(u(1-ab)\big)a = 1$.

$$\boxed{(1-ba)^{-1} = 1 + b(1-ab)^{-1}a}$$

La formule se devine en écrivant formellement $\dfrac{1}{1-ba} = \sum (ba)^k = 1 + b\big(\sum (ab)^k\big)a$; ce calcul n'a pas de sens en général, mais sa conclusion se vérifie directement.

EXERCICE 37 ⋆⋆

1. L'addition fait de $\mathbb{R}^2$ un groupe abélien (groupe produit). La multiplication est commutative, par symétrie de la formule, et associative :

$$\big((a,b)(c,d)\big)(e,f) = (ace,\ acf + ade + bce) = (a,b)\big((c,d)(e,f)\big).$$

Elle est distributive, puisque ses composantes sont linéaires en chaque facteur, et $(1,0)(c,d) = (c,d)$.

$$\boxed{\text{anneau commutatif d'unité } (1,0)}$$

2. On a $a + b\varepsilon = (a,0) + (b,0)(0,1) = (a,0) + (0,b) = (a,b)$, et $\varepsilon^2 = (0\times 0,\ 0\times 1 + 1\times 0) = (0,0)$. Comme $\varepsilon \neq 0$ et $\varepsilon \times \varepsilon = 0$, l'anneau n'est pas intègre.

3. L'égalité $(a+b\varepsilon)(c+d\varepsilon) = 1$ s'écrit $ac = 1$ et $ad + bc = 0$. Elle a une solution si et seulement si $a \neq 0$, et alors $c = \dfrac{1}{a}$ et $d = -\dfrac{b}{a^2}$.

$$\boxed{a + b\varepsilon \text{ inversible} \iff a \neq 0, \qquad (a+b\varepsilon)^{-1} = \frac{1}{a} - \frac{b}{a^2}\varepsilon}$$

4. Les éléments a et $b\varepsilon$ commutent, et $(b\varepsilon)^k = 0$ pour $k \geqslant 2$. Le théorème 3 donne

$$\boxed{(a+b\varepsilon)^n = a^n + na^{n-1}b\,\varepsilon}$$

En particulier $(a+\varepsilon)^k = a^k + ka^{k-1}\varepsilon$, et en sommant avec les coefficients c_k,

$$P(a+\varepsilon) = \sum_{k=0}^{d} c_k a^k + \Big(\sum_{k=1}^{d} k c_k a^{k-1}\Big)\varepsilon = P(a) + P'(a)\varepsilon.$$

Par exemple, pour $P(x) = x^3 - 2x$, on trouve $(2+\varepsilon)^3 - 2(2+\varepsilon) = 8 + 12\varepsilon - 4 - 2\varepsilon = 4 + 10\varepsilon$, et en effet $P(2) = 4$ et $P'(2) = 10$. ✓ Le terme $\varepsilon^2 = 0$ joue le rôle du $o(h)$ d'un développement limité à l'ordre 1 (chapitre 10).

EXERCICE 38 ⋆⋆⋆

1. Si f et g sont des endomorphismes, alors, pour x et y dans G,

$$(f+g)(x+y) = f(x)+f(y)+g(x)+g(y) = (f+g)(x)+(f+g)(y),$$

où l'on a échangé $f(y)$ et $g(x)$: c'est là que sert la commutativité de G. Ainsi $f+g \in \mathrm{End}(G)$, et $(\mathrm{End}(G),+)$ est un groupe abélien, de zéro l'application nulle et d'opposé $-f : x \mapsto -f(x)$, chaque propriété se vérifiant point par point dans G. La composée de deux endomorphismes en est un (proposition 11), la composition est associative, d'unité id_G. Enfin, pour tout x,

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

la première égalité utilisant que f est un morphisme.

$$\boxed{(\mathrm{End}(G),+,\circ) \text{ est un anneau, de zéro } 0 \text{ et d'unité } \mathrm{id}_G}$$

2. On évalue en (a,b) :

$$(s\circ p)(a,b) = s(a,0) = (0,a), \qquad (p\circ s)(a,b) = p(b,a) = (b,0), \qquad (h\circ h)(a,b) = h(0,a) = (0,0).$$

$$\boxed{s\circ p \neq p\circ s, \qquad h\circ h = 0 \text{ avec } h \neq 0}$$

L'anneau $\mathrm{End}(\mathbb{Z}^2)$ n'est pas commutatif, et il n'est pas intègre : h est un diviseur de zéro.

3. D'après l'exercice 25, tout endomorphisme de $\mathbb{Z}$ s'écrit $n \mapsto kn$, avec $k = f(1)$. L'application $\Phi : f \mapsto f(1)$ est donc une bijection de $\mathrm{End}(\mathbb{Z})$ sur $\mathbb{Z}$. Elle vérifie $\Phi(f+g) = f(1)+g(1)$, $\Phi(\mathrm{id}) = 1$, et $\Phi(f\circ g) = f(g(1)) = f(1)g(1)$, puisque $f(n) = f(1)n$.

$$\boxed{\mathrm{End}(\mathbb{Z}) \simeq \mathbb{Z} \text{ comme anneaux}}$$

EXERCICE 39 ⋆⋆

1. Dans un anneau intègre, si $x^n = 0$ avec n minimal, et si $n \geqslant 2$, alors $x\cdot x^{n-1} = 0$ avec $x^{n-1} \neq 0$, donc $x = 0$; si $n = 1$, $x = 0$ directement. L'élément ε de l'exercice 37 et l'endomorphisme h de l'exercice 38 sont nilpotents et non nuls.

2. Si $(xy)^n = 0$, alors $(yx)^{n+1} = y(xy)^n x = 0$. $\boxed{yx \text{ est nilpotent}}$

3. Soit $x^n = 0$ et $y^m = 0$. Comme x et y commutent, $(xy)^n = x^n y^n = 0$. Par le théorème 3,

$$(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k},$$

et chaque terme est nul : si $k < n$, alors $n+m-1-k \geqslant m$ et $y^{n+m-1-k} = 0$.

$$\boxed{xy \text{ et } x+y \text{ sont nilpotents}}$$

4. On a $h^2 = 0$ (exercice 38) et $k^2(a,b) = k(b,0) = (0,0)$. Mais $(h+k)(a,b) = (b,a)$: c'est l'échange s, qui vérifie $s^2 = \mathrm{id}$, donc ses puissances valent id ou s et ne sont jamais nulles. De même, $(h\circ k)(a,b) = h(b,0) = (0,b)$: c'est un élément q tel que $q^2 = q \neq 0$, donc $q^n = q \neq 0$ pour tout n.

$$\boxed{h,k \text{ nilpotents}, \quad h+k \text{ et } h\circ k \text{ non nilpotents}}$$

L'hypothèse qui fait défaut est la commutation : $(k\circ h)(a,b) = (a,0) \neq (0,b)$.

5. Les éléments 1 et x commutent ; le théorème 3, avec $a = 1$ et $b = x$, donne

$$(1-x)(1+x+\cdots+x^{n-1}) = 1-x^n = 1,$$

et de même dans l'autre ordre. $\boxed{(1-x)^{-1} = 1+x+\cdots+x^{n-1}}$

EXERCICE 40 ⋆⋆

1. Pour toute partie A, on a $A \cap A = A$.

2. On a $x + x = (x+x)^2 = x^2 + x^2 + x^2 + x^2 = 4x$, d'où $x + x = 0$. Ensuite

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

donc $xy + yx = 0$, soit $xy = -yx = yx$, puisque tout élément est son propre opposé.

$$\boxed{x = -x, \qquad xy = yx}$$

3. Si A est intègre, $x^2 = x$ s'écrit $x(x-1) = 0$, donc $x = 0$ ou $x = 1$; comme A est non nul, $0 \neq 1$.

$$\boxed{\text{un anneau de Boole intègre a exactement deux éléments}}$$

L'anneau $\mathcal{P}(E)$ est donc intègre si et seulement si E a un seul élément : pour $E = \varnothing$, c'est l'anneau nul, et si E a deux éléments distincts a et b, $\{a\} \cap \{b\} = \varnothing$ (cours).

4. Un sous-anneau contenant X contient l'unité E, le zéro $\varnothing$, et $E \,\Delta\, X = E \setminus X$. Réciproquement, $S = \{\varnothing, X, E \setminus X, E\}$ contient E, et il est stable par Δ et par $\cap$, comme on le vérifie sur les couples d'éléments de S : par exemple $X \,\Delta\, (E \setminus X) = E$ et $X \cap (E \setminus X) = \varnothing$. Dans cet anneau, la différence est Δ, puisque tout élément est son propre opposé.

$$\boxed{\{\varnothing, X, E \setminus X, E\} \text{ est le plus petit sous-anneau contenant } X}$$

EXERCICE 41 ⋆⋆

1. Le nombre j est racine de z^2+z+1, puisque $1+j+j^2 = 0$ (chapitre 4). L'ensemble $\mathbb{Z}[j]$ contient 1, est stable par différence, et

$$(a+bj)(c+dj) = ac + (ad+bc)j + bd\,j^2 = (ac-bd) + (ad+bc-bd)j \in \mathbb{Z}[j].$$

2. Comme $\overline{j} = j^2$ et $j + \overline{j} = 2\cos\dfrac{2\pi}{3} = -1$,

$$|a+bj|^2 = (a+bj)(a+b\overline{j}) = a^2 + ab(j+\overline{j}) + b^2 j\overline{j} = a^2 - ab + b^2.$$

3. Comme pour $\mathbb{Z}[\mathrm{i}]$, si $x = a+bj$ est inversible, le produit $|x|^2|x^{-1}|^2$ vaut 1, et c'est un produit de deux entiers naturels, donc $a^2 - ab + b^2 = 1$. On écrit

$$a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4},$$

ce qui impose $|b| \leqslant 1$, puis on trouve les solutions $(\pm 1, 0)$, $(0, \pm 1)$, $(1,1)$ et $(-1,-1)$. Elles correspondent à ± 1, $\pm j$, $1+j = -j^2$ et $-1-j = j^2$. Réciproquement, ces six nombres sont de module 1, et l'inverse $\overline{x}$ de chacun est encore dans $\mathbb{Z}[j]$, puisque $\overline{j} = j^2 = -1 - j$.

$$\boxed{\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} = \mathbb{U}_6}$$

Les inversibles de $\mathbb{Z}[\mathrm{i}]$ formaient $\mathbb{U}_4$, ceux de $\mathbb{Z}[j]$ forment $\mathbb{U}_6$: ce sont les rotations qui laissent invariant un réseau carré, ou un réseau triangulaire.

EXERCICE 42 ⋆⋆⋆

1. Comme $\sqrt{2}$ est irrationnel, l'écriture $x = a + b\sqrt{2}$ est unique, donc σ est bien définie ; c'est la restriction à A de l'automorphisme de $\mathbb{Q}[\sqrt{2}]$ étudié dans le cours, et elle envoie A sur A, avec $\sigma \circ \sigma = \mathrm{id}_A$. Ensuite $N(xy) = xy\,\sigma(x)\sigma(y) = N(x)N(y)$, et

$$N(x) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}.$$

2. Si $xy = 1$ dans A, alors $N(x)N(y) = N(1) = 1$, avec deux entiers : $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors $x \cdot (\pm\sigma(x)) = 1$, avec $\pm\sigma(x) \in A$.

$$\boxed{x \in A^\times \iff N(x) = \pm 1}$$

3. On a $N(1 + \sqrt{2}) = 1 - 2 = -1$: $1 + \sqrt{2}$ est inversible, d'inverse $\sqrt{2} - 1$. Comme $1 + \sqrt{2} > 1$, la suite de ses puissances est strictement croissante.

$$\boxed{A^\times \text{ est infini, alors que } \mathbb{Z}[\mathrm{i}]^\times = \mathbb{U}_4 \text{ a quatre éléments}}$$

La différence vient de ce que $|x|^2$ est une somme de carrés, positive, alors que $N(x) = a^2 - 2b^2$ peut valoir ± 1 pour de grands a et b : c'est encore l'équation de Pell-Fermat, comme à l'exercice 17.

4. En développant, $(1 + \sqrt{2})^k = p + q\sqrt{2}$ avec p et q entiers naturels, et

$$p^2 - 2q^2 = N\big((1 + \sqrt{2})^k\big) = (-1)^k.$$

Ainsi p^2 et $2q^2$ sont deux entiers naturels consécutifs ; si a est le plus petit, on a

$$\boxed{(1 + \sqrt{2})^k = \sqrt{p^2} + \sqrt{2q^2} = \sqrt{a} + \sqrt{a+1}}$$

Pour $k = 2$, $3 + 2\sqrt{2} = \sqrt{9} + \sqrt{8}$, d'où $a = 8$; pour $k = 3$, $7 + 5\sqrt{2} = \sqrt{49} + \sqrt{50}$, d'où $a = 49$. ✓

EXERCICE 43 ⋆

(a) $\mathbb{Q}(\mathrm{i})$ est un sous-anneau de $\mathbb{C}$, comme $\mathbb{Z}[\mathrm{i}]$, et l'inverse de $a + \mathrm{i}b \neq 0$ est $\dfrac{a - \mathrm{i}b}{a^2 + b^2}$, qui est dans $\mathbb{Q}(\mathrm{i})$: c'est un corps.

(b) $\mathbb{D}$ n'est pas un corps, puisque $\dfrac{1}{3}$ n'est pas décimal (chapitre 7) ; $\mathbb{Z}[\mathrm{i}]$ non plus, puisque 2 n'est pas dans $\mathbb{U}_4$, groupe de ses inversibles.

(c) Non : $\varepsilon \neq 0$ n'est pas inversible (exercice 37).

(d) Non : l'indicatrice d'un singleton n'est pas nulle et n'est pas inversible.

(e) Oui : l'anneau $\{\varnothing, E\}$ est non nul, et son seul élément non nul, E, est l'unité.

$$\boxed{\text{corps : (a) et (e)}}$$

Le corps (e) a deux éléments ; c'est le plus petit corps possible, puisque $0 \neq 1$.

EXERCICE 44 ⋆⋆

1. Si $ax = ay$, alors $a(x-y) = 0$, et $x = y$ puisque $a \neq 0$ et que A est intègre : l'application $x \mapsto ax$ est injective. C'est une application de l'ensemble fini A dans lui-même, donc elle est bijective (chapitre 2, théorème 2). En particulier, il existe b tel que $ab = 1$, et $ba = 1$ par commutativité.

$$\boxed{\text{tout anneau intègre fini est un corps}}$$

2. On a $x = x^{-1}$ si et seulement si $x^2 = 1$, c'est-à-dire $(x-1)(x+1) = 0$, soit $x = \pm 1$ par intégrité. Les autres éléments non nuls se regroupent par paires $\{x, x^{-1}\}$ de deux éléments distincts, de produit 1. Le produit de tous les éléments non nuls vaut donc le produit des éléments de $\{1, -1\}$, qui est -1, que 1 et -1 soient distincts ou non.

$$\boxed{\prod_{x \in \mathbb{K}^*} x = -1}$$

3. Dans le corps $\{\varnothing, E\}$, le produit des éléments non nuls est $E = 1$, et $-1 = 1$, puisque $E \,\Delta\, E = \varnothing$.
✓ Ce résultat est l'analogue, dans un corps fini quelconque, du théorème de Wilson de l'arithmétique : $(p-1)! \equiv -1\ [p]$ lorsque p est premier.

EXERCICE 45 ⋆⋆⋆

1. Un morphisme d'anneaux $f : \mathbb{Z} \to A$ est un morphisme de groupes additifs tel que $f(1) = 1_A$; par l'exercice 25, $f(n) = n \cdot 1_A$. Réciproquement, cette application respecte l'addition, envoie 1 sur 1_A, et $(n \cdot 1_A)(m \cdot 1_A) = (nm) \cdot 1_A$ par la proposition 13.

$$\boxed{\text{l'unique morphisme d'anneaux de } \mathbb{Z} \text{ dans } A \text{ est } n \mapsto n \cdot 1_A}$$

2. Soit f un endomorphisme de $\mathbb{Q}$. Par la question 1, $f(n) = n$ pour $n \in \mathbb{Z}$. Pour $\dfrac{p}{q}$ avec $q \neq 0$, $qf(\dfrac{p}{q}) = f(p) = p$, donc $f(\dfrac{p}{q}) = \dfrac{p}{q}$. $\boxed{f = \mathrm{id}_{\mathbb{Q}}}$

3. *(a)* Le raisonnement de la question 2 s'applique : $f(x) = x$ pour $x \in \mathbb{Q}$.

(b) Si $x \geqslant 0$, alors $f(x) = f(\sqrt{x}^2) = f(\sqrt{x})^2 \geqslant 0$. Si $x \leqslant y$, alors $f(y) - f(x) = f(y-x) \geqslant 0$: f est croissante.

(c) Supposons $f(x) < x$ pour un réel x. Par densité, il existe un rationnel r tel que $f(x) < r < x$. Mais $r < x$ donne $r = f(r) \leqslant f(x)$, ce qui est absurde. De même, $f(x) > x$ est impossible.

$$\boxed{\text{le seul endomorphisme de l'anneau } \mathbb{R} \text{ est } \mathrm{id}_{\mathbb{R}}}$$

4. On a $f(\mathrm{i})^2 = f(-1) = -1$, donc $f(\mathrm{i}) = \pm \mathrm{i}$, et $f(a + \mathrm{i}b) = a + bf(\mathrm{i})$. Réciproquement, l'identité et la conjugaison conviennent.

$$\boxed{f = \mathrm{id}_{\mathbb{C}} \quad \text{ou} \quad f : z \mapsto \overline{z}}$$

5. Soit f un automorphisme de $\mathbb{Q}[\sqrt{2}]$. Comme à la question 2, f est l'identité sur $\mathbb{Q}$. De plus $f(\sqrt{2})^2 = f(2) = 2$, donc $f(\sqrt{2})$ vaut $\sqrt{2}$ ou $-\sqrt{2}$. Ainsi, pour tous rationnels a et b,

$$f(a + b\sqrt{2}) = a \pm b\sqrt{2},$$

et f est l'identité ou l'automorphisme σ du cours.

$$\boxed{\text{les automorphismes de } \mathbb{Q}[\sqrt{2}] \text{ sont id et } \sigma}$$

À retenir. L'ordre de $\mathbb{R}$ est « algébrique » : les réels positifs sont exactement les carrés. C'est ce qui rend $\mathbb{R}$ si rigide, alors que $\mathbb{C}$, qui n'est pas ordonnable (cours, section 11.4), possède la conjugaison.

EXERCICE 46 ⋆⋆

1. Faux. L'addition sur $\mathbb{N}^*$ est associative, sans élément neutre.

2. Vrai. C'est le point (iii) de la proposition 2.

3. Vrai. On a $x = x^3(x^2)^{-1} = y^3(y^2)^{-1} = y$.

4. Faux. La réunion $2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3, mais pas 5 (cours, remarque qui suit la proposition 8 ; exercice 18).

5. Vrai. Une application injective d'un ensemble fini dans lui-même est bijective (chapitre 2, théorème 2).

6. Faux. Dans $\mathcal{P}(\{1,2\})$, tout élément vérifie $x \,\Delta\, x = \varnothing$, alors que $\mathrm{i}^2 \neq 1$ dans $\mathbb{U}_4$ (cours, section 11.3.7).

7. Faux. Dans $\mathcal{F}(\mathbb{R},\mathbb{R})$, les indicatrices de $\mathbb{R}_+$ et de $\mathbb{R}_-^*$ sont non nulles, de produit nul.

8. Vrai. Un sous-anneau d'un corps est commutatif, non nul puisqu'il contient $1 \neq 0$, et sans diviseur de zéro, puisqu'un corps est intègre (proposition 15).

9. Vrai. On a $\mathbb{Z}[\mathrm{i}]^\times = \mathbb{U}_4$ (cours), et $r_k \mapsto \mathrm{i}^k$ est un isomorphisme du groupe des rotations du carré sur $\mathbb{U}_4$.

10. Vrai. C'est l'exercice 44.

$$\boxed{\text{vrais : } 2,3,5,8,9,10; \qquad \text{faux : } 1,4,6,7}$$

EXERCICE 47 ⋆⋆

1. Pour toute permutation σ et tous x, y, on a $\sigma(x \star y) = \sigma(x)$ et $\sigma(x) \star \sigma(y) = \sigma(x)$, qui sont égaux. En fait, toute application de E dans E respecte cette loi.

$$\boxed{\text{la loi } x \star y = x \text{ convient, quel que soit } E}$$

L'hypothèse seule ne limite donc pas le nombre d'éléments de E ; c'est la commutativité, ajoutée à partir de la question 3, qui le fera.

2. Supposons $x \star x = y$ avec $y \neq x$. Comme E a au moins trois éléments, il existe $z \notin \{x,y\}$. Soit τ la permutation qui échange y et z et fixe tous les autres éléments, en particulier x. Alors

$$\tau(x \star x) = \tau(y) = z, \qquad \text{alors que} \qquad \tau(x) \star \tau(x) = x \star x = y,$$

et $z \neq y$: c'est absurde. $\boxed{x \star x = x \text{ pour tout } x \in E}$

3. Soit τ la permutation qui échange x et y et fixe les autres éléments. Par hypothèse et par commutativité,

$$\tau(x \star y) = \tau(x) \star \tau(y) = y \star x = x \star y.$$

L'élément $x \star y$ est donc fixé par τ, alors que τ ne fixe ni x ni y. $\boxed{x \star y \notin \{x,y\}}$

Si $E = \{x,y\}$ avait exactement deux éléments, $x \star y$ appartiendrait à $E = \{x,y\}$, ce qui vient d'être exclu.

4. Supposons que E contienne quatre éléments distincts, et soit $x \neq y$ deux d'entre eux. Par la question 3, $z = x \star y$ est distinct de x et de y, et il existe un quatrième élément $w \notin \{x,y,z\}$. La permutation τ qui échange z et w fixe x et y, donc

$$\tau(x \star y) = \tau(z) = w, \qquad \text{alors que} \qquad \tau(x) \star \tau(y) = x \star y = z,$$

ce qui est absurde. Ainsi E est fini et a au plus trois éléments ; la question 3 exclut deux éléments, et un ensemble à un élément convient, avec son unique loi.

$$\boxed{\text{si la loi est commutative, } E \text{ a un ou trois éléments}}$$

5. Soit $\star$ une telle loi sur $E = \{a, b, c\}$. Par la question 2, $x \star x = x$; par la question 3, si $x \neq y$, alors $x \star y$ est le troisième élément de E. La loi est donc imposée. Réciproquement, cette loi convient : si σ est une permutation, $\sigma(x \star x) = \sigma(x) = \sigma(x) \star \sigma(x)$, et si x, y, z sont les trois éléments distincts de E, alors $\sigma(x)$, $\sigma(y)$, $\sigma(z)$ sont encore les trois éléments distincts de E, puisque σ est injective, donc $\sigma(x) \star \sigma(y) = \sigma(z) = \sigma(x \star y)$. On obtient la table suivante.

$\star$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

Elle n'est pas associative, puisque $(a \star a) \star b = a \star b = c$, alors que $a \star (a \star b) = a \star c = b$. Elle n'a pas d'élément neutre : si e était neutre, on aurait $e \star x = x$ pour un $x \neq e$, alors que $e \star x$ est le troisième élément.

une seule loi : $x \star x = x$, $x \star y =$ le troisième élément si $x \neq y$; ni associative, ni neutre

En numérotant a, b, c par 0, 1, 2, cette loi s'écrit $x \star y \equiv -(x+y)$ [3], avec les congruences du chapitre 2 : on vérifie que $-2x \equiv x$ [3], et que la somme des trois éléments est $3 \equiv 0$ [3].
Piège. On ne peut pas se passer de la commutativité dans les questions 3 et 4 : la question 1 fournit, sur tout ensemble, une loi que respectent toutes les permutations. Par ailleurs, une loi « parfaitement symétrique » n'est pas pour autant une bonne loi : celle que l'on obtient sur trois éléments n'est ni associative ni munie d'un élément neutre, et elle est très loin d'une loi de groupe.

EXERCICE 48 ⋆⋆

1. La fonction constante égale à 1 est continue, et la différence et le produit de deux fonctions continues sur D sont continus (chapitre 8) : $\mathcal{C}(D)$ est un sous-anneau de $\mathcal{F}(D, \mathbb{R})$. Une fonction p de D dans $\mathbb{R}$ vérifie $p^2 = p$ si et seulement si, pour tout $x \in D$, $p(x)(p(x)-1) = 0$, c'est-à-dire $p(x) \in \{0, 1\}$; elle est alors l'indicatrice de $X = \{x \in D \mid p(x) = 1\}$. Réciproquement, $\mathbf{1}_X^2 = \mathbf{1}_X$.

idempotents de $\mathcal{F}(D, \mathbb{R})$: les $\mathbf{1}_X$, $X \in \mathcal{P}(D)$

2. Soit p un idempotent de $\mathcal{C}(I)$; il ne prend que les valeurs 0 et 1. S'il prenait les deux, en a et en b, alors p serait continue sur le segment d'extrémités a et b, contenu dans l'intervalle I, et le théorème des valeurs intermédiaires (théorème 8 du chapitre 8) fournirait un point c où $p(c) = \dfrac{1}{2}$, ce qui est impossible. Ainsi p est constante.

les seuls idempotents de $\mathcal{C}(I)$ sont 0 et 1

3. L'ensemble D_n est la réunion disjointe des $n+1$ intervalles $J_0 =]-\infty, 1[$, $J_k =]k, k+1[$ pour $1 \leqslant k \leqslant n-1$, et $J_n =]n, +\infty[$; pour $n = 0$, il n'y a que $J_0 = \mathbb{R}$. Soit p un idempotent de $\mathcal{C}(D_n)$. Sa restriction à chaque J_k est un idempotent de $\mathcal{C}(J_k)$, donc elle est constante, égale à 0 ou à 1 par la question 2. Ainsi p est l'indicatrice de la réunion des J_k pour k dans une partie S de $[\![0\,;n]\!]$, et S est déterminée par p.
Réciproquement, pour toute partie S de $[\![0\,;n]\!]$, la fonction p_S qui vaut 1 sur les J_k avec $k \in S$ et 0 sur les autres est idempotente, et elle est continue : tout point x_0 de D_n appartient à un intervalle ouvert J_k, qui contient un intervalle $]x_0 - \eta, x_0 + \eta[$ sur lequel p_S est constante. L'application $S \mapsto p_S$ est donc une bijection de $\mathcal{P}([\![0\,;n]\!])$ sur l'ensemble des idempotents, et ce dernier a 2^{n+1} éléments (proposition 6 du chapitre 1).

$\mathcal{C}(D_n)$ possède 2^{n+1} idempotents

Pour $\mathbb{R}^*$, qui est la réunion des deux intervalles $]-\infty, 0[$ et $]0, +\infty[$, le même raisonnement donne quatre idempotents : 0, 1, $\mathbf{1}_{\mathbb{R}_+^*}$ et $\mathbf{1}_{\mathbb{R}_-^*}$.

4. Si $p^2 = p$, alors $f(p)^2 = f(p^2) = f(p)$: f envoie les idempotents de A dans ceux de B. La réciproque f^{-1} est encore un morphisme d'anneaux : pour u, v dans B, les éléments $f^{-1}(u+v)$ et $f^{-1}(u) + f^{-1}(v)$ ont la même image $u+v$ par f, donc sont égaux par injectivité ; de même pour le produit, et $f^{-1}(1_B) = 1_A$. Elle envoie donc les idempotents de B dans ceux de A, et f induit une bijection entre les deux ensembles d'idempotents.
Si $\mathcal{C}(D_n)$ et $\mathcal{C}(D_m)$ étaient isomorphes, on aurait $2^{n+1} = 2^{m+1}$, donc $n = m$.

$$\boxed{\mathcal{C}(D_n) \text{ et } \mathcal{C}(D_m) \text{ ne sont pas isomorphes si } n \neq m \text{ ; en particulier } \mathcal{C}(\mathbb{R}) \not\simeq \mathcal{C}(\mathbb{R}^*)}$$

5. Si $x \notin \mathbb{N}$, $g(x) = x$ est un réel non nul qui n'est pas dans $\mathbb{N}^*$; si $x \in \mathbb{N}$, $g(x) = x + 1 \in \mathbb{N}^*$. L'application g envoie donc $\mathbb{N}$ sur $\mathbb{N}^*$ par $x \mapsto x+1$, qui est bijective, et $\mathbb{R} \setminus \mathbb{N}$ sur $\mathbb{R}^* \setminus \mathbb{N}^* = \mathbb{R} \setminus \mathbb{N}$ par l'identité : g est une bijection de $\mathbb{R}$ sur $\mathbb{R}^*$. L'application $\Phi : \varphi \mapsto \varphi \circ g$ respecte les opérations, définies point par point, puisque

$$(\varphi + \psi) \circ g = \varphi \circ g + \psi \circ g \qquad \text{et} \qquad (\varphi\psi) \circ g = (\varphi \circ g)(\psi \circ g),$$

et elle envoie la constante 1 sur la constante 1. Elle est bijective, de réciproque $\chi \mapsto \chi \circ g^{-1}$.

$$\boxed{\mathcal{F}(\mathbb{R}^*, \mathbb{R}) \simeq \mathcal{F}(\mathbb{R}, \mathbb{R})}$$

L'hypothèse qui fait la différence est la continuité : g n'est pas continue, et $\varphi \circ g$ n'a aucune raison de l'être quand φ l'est. Sans continuité, l'anneau ne voit que le nombre d'éléments de l'ensemble de départ.
À retenir. Les idempotents d'un anneau de fonctions continues comptent les « morceaux » de l'ensemble de définition. Une propriété purement algébrique, invariante par isomorphisme, détecte ainsi une propriété géométrique ; c'est le théorème des valeurs intermédiaires qui fait le lien.

EXERCICE 49 ⋆⋆⋆

1. D'après l'exercice 31, l'ordre de tout élément divise 4.

$$\boxed{\text{ordres possibles : } 1, 2, 4}$$

2. Les éléments e, x, x^2, x^3 sont distincts (exercice 31, question 4), et G en a quatre, donc $G = \{e, x, x^2, x^3\}$. Comme à la question 5 de l'exercice 31, $x^k \mapsto \mathrm{i}^k$ est bien défini, puisque $x^k = x^\ell$ si et seulement si 4 divise $k - \ell$, et c'est un isomorphisme sur $\mathbb{U}_4$.

$$\boxed{G \simeq (\mathbb{U}_4, \times)}$$

3. Tout élément différent de e est alors d'ordre 2, donc $x^2 = e$ pour tout x, et G est abélien (exercice 12). Soit $a \neq e$ et $b \notin \{e, a\}$. Le produit ab n'est ni e, ce qui donnerait $b = a^{-1} = a$, ni a, ce qui donnerait $b = e$, ni b, ce qui donnerait $a = e$. Ainsi $G = \{e, a, b, ab\}$, et l'on obtient la table à l'aide de $a^2 = b^2 = e$ et $ab = ba$:

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

La bijection $e \mapsto \varnothing$, $a \mapsto \{1\}$, $b \mapsto \{2\}$, $ab \mapsto \{1, 2\}$ transporte cette table sur celle de la différence symétrique, puisque $\{1\} \,\Delta\, \{2\} = \{1, 2\}$.

$$\boxed{G \simeq (\mathcal{P}(\{1, 2\}), \Delta)}$$

4. Les deux cas s'excluent, puisque les groupes $\mathbb{U}_4$ et $\mathcal{P}(\{1,2\})$ ne sont pas isomorphes (cours, section 11.3.7).

$$\boxed{\text{deux groupes à quatre éléments, à isomorphisme près, tous deux abéliens}}$$

5. Les nombres 2, 3 et 5 sont premiers : un groupe ayant ce nombre d'éléments est isomorphe à $\mathbb{U}_2$, $\mathbb{U}_3$ ou $\mathbb{U}_5$ (exercice 31, question 5), donc abélien. Tout groupe d'au plus cinq éléments est ainsi abélien, et $\mathfrak{S}_3$, à six éléments, ne l'est pas.

$$\boxed{\text{le plus petit groupe non abélien a six éléments}}$$

EXERCICE 50 ⋆⋆⋆

1. La partie $X = G$ vérifie $\langle G\rangle = G$: l'ensemble des cardinaux des parties génératrices est une partie non vide de $\mathbb{N}$, qui admet un plus petit élément. Le sous-groupe $\langle\varnothing\rangle$ est l'intersection de tous les sous-groupes de G ; il contient e et il est contenu dans le sous-groupe $\{e\}$, donc $\langle\varnothing\rangle = \{e\}$. Ainsi $r(G) = 0$ si et seulement si $G = \{e\}$.
Soit $n \geqslant 2$ et $\omega = \mathrm{e}^{2\mathrm{i}\pi/n}$. D'après l'exercice 20, $\langle\{\omega\}\rangle$ est l'ensemble des puissances ω^k, $k \in \mathbb{Z}$, qui est $\mathbb{U}_n$ (chapitre 4). Comme $\mathbb{U}_n \neq \{1\}$, on obtient $r(\mathbb{U}_n) = 1$.
Le sous-groupe engendré par un seul élément x est formé des puissances de x, qui commutent entre elles d'après la proposition 4 ; or $\mathfrak{S}_3$ n'est pas abélien (proposition 5), donc $r(\mathfrak{S}_3) \geqslant 2$. Le sous-groupe $\langle\{c, t_1\}\rangle$ contient les quatre éléments distincts id, c, c^2 et t_1 ; par le théorème de Lagrange, son nombre d'éléments divise 6, donc il vaut 6.

$$\boxed{r(\mathbb{U}_n) = 1 \ (n \geqslant 2), \qquad r(\mathfrak{S}_3) = 2}$$

2. Le sous-groupe H de G, contenu dans K, est un sous-groupe du groupe K. Le théorème de Lagrange, appliqué dans K, montre que $\mathrm{card}(H)$ divise $\mathrm{card}(K)$. Comme $x \in K \setminus H$, on a $\mathrm{card}(K) > \mathrm{card}(H)$, et le quotient $\dfrac{\mathrm{card}(K)}{\mathrm{card}(H)}$ est un entier au moins égal à 2.

$$\boxed{\mathrm{card}(K) \geqslant 2\,\mathrm{card}(H)}$$

3. On pose $H_0 = \{e\} = \langle\varnothing\rangle$. Tant que $H_k \neq G$, on choisit $x_{k+1} \in G \setminus H_k$, et l'on pose $H_{k+1} = \langle H_k \cup \{x_{k+1}\}\rangle$. Par récurrence, $H_k = \langle\{x_1, \dots, x_k\}\rangle$: en effet, un sous-groupe contient $H_k \cup \{x_{k+1}\}$ si et seulement s'il contient $x_1, \dots, x_{k+1}$, puisque H_k est le plus petit sous-groupe contenant $x_1, \dots, x_k$. Par la question 2 et une récurrence immédiate,

$$2^k \leqslant \mathrm{card}(H_k) \leqslant \mathrm{card}(G).$$

La construction s'arrête donc, à un rang s tel que $H_s = G$ et $2^s \leqslant \mathrm{card}(G)$. La partie $\{x_1, \dots, x_s\}$ engendre G, donc $r(G) \leqslant s$.

$$\boxed{2^{r(G)} \leqslant \mathrm{card}(G), \quad \text{soit} \quad r(G) \leqslant \frac{\ln \mathrm{card}(G)}{\ln 2}}$$

4. Dans $(\mathcal{P}(E), \Delta)$, la loi est commutative et associative, de neutre $\varnothing$, et toute partie est son propre symétrique, puisque $A \,\Delta\, A = \varnothing$. D'après l'exercice 20, un élément de $\langle\{A_1, \dots, A_k\}\rangle$ est une différence symétrique de termes pris parmi les A_i. En regroupant les termes égaux, ce qui est permis par commutativité, et en supprimant les paires $A_i \,\Delta\, A_i = \varnothing$, on l'écrit sous la forme $\Delta_{i\in S} A_i$, différence symétrique des A_i pour i dans une partie S de $[\![1\,;k]\!]$. Il y a 2^k telles parties S (proposition 6 du chapitre 1).

$$\boxed{\mathrm{card}\,\langle\{A_1, \dots, A_k\}\rangle \leqslant 2^k}$$

Si k parties engendrent $\mathcal{P}(E)$, qui a 2^d éléments, alors $2^d \leqslant 2^k$, donc $k \geqslant d$. Réciproquement, les d singletons engendrent $\mathcal{P}(E)$, puisque toute partie A est la différence symétrique des singletons $\{a\}$, $a \in A$, deux à deux disjoints.

$$\boxed{r(\mathcal{P}(E)) = d, \qquad \operatorname{card}(\mathcal{P}(E)) = 2^{r(\mathcal{P}(E))}}$$

5. On calcule les puissances de $x = (-1, j)$ dans le groupe produit, à l'aide de $j^3 = 1$:

$$x^0 = (1,1), \quad x = (-1,j), \quad x^2 = (1,j^2), \quad x^3 = (-1,1), \quad x^4 = (1,j), \quad x^5 = (-1,j^2).$$

Ces six éléments sont distincts, et $\mathbb{U}_2 \times \mathbb{U}_3$ en a six : x engendre ce groupe. Dans $\mathbb{U}_2 \times \mathbb{U}_2$, en revanche, tout élément y vérifie $y^2 = (1,1)$, donc le sous-groupe engendré par y est $\{(1,1), y\}$, qui a au plus deux éléments sur quatre ; la question 3 donne $2^r \leqslant 4$.

$$\boxed{r(\mathbb{U}_2 \times \mathbb{U}_3) = 1, \qquad r(\mathbb{U}_2 \times \mathbb{U}_2) = 2}$$

À retenir. Le rang ne dépend pas seulement du nombre d'éléments : $\mathbb{U}_4$ et $\mathbb{U}_2 \times \mathbb{U}_2$ ont quatre éléments, mais des rangs 1 et 2. Comme un isomorphisme transporte les parties génératrices, cela redonne que ces deux groupes ne sont pas isomorphes (exercice 49). La borne $2^{r(G)} \leqslant \operatorname{card}(G)$ est atteinte par les groupes $\mathcal{P}(E)$, où chaque nouveau générateur double exactement le sous-groupe déjà obtenu.

EXERCICE 51 ⋆⋆⋆

1. Un point fixe de $f : t \mapsto at + b$ vérifie $(1-a)t = b$. Si $a = 1$ et $b \neq 0$, f est une translation, sans point fixe : elle n'appartient pas à Γ. Un élément de Γ avec $a = 1$ est donc l'identité. Si $a \neq 1$, le point fixe est unique, égal à $\dfrac{b}{1-a}$.

$$\boxed{\text{tout élément de } \Gamma \setminus \{\mathrm{id}\} \text{ a un unique point fixe, et vérifie } a \neq 1}$$

2. Le coefficient de t dans une composée de fonctions affines est le produit des coefficients, et celui de f^{-1} est $\dfrac{1}{a}$. Le coefficient de $f \circ g \circ f^{-1} \circ g^{-1}$ est donc $a \cdot a' \cdot \dfrac{1}{a} \cdot \dfrac{1}{a'} = 1$.

3. Si f et g sont dans Γ, alors $c = f \circ g \circ f^{-1} \circ g^{-1}$ est dans Γ et a pour coefficient 1 : par la question 1, $c = \mathrm{id}$, c'est-à-dire $f \circ g = g \circ f$.

4. On a $f(g(\omega)) = g(f(\omega)) = g(\omega)$: $g(\omega)$ est un point fixe de f, donc $g(\omega) = \omega$ par unicité. Ainsi ω est fixé par tout élément de Γ, l'identité comprise. Si $\Gamma = \{\mathrm{id}\}$, tout point convient.

$$\boxed{\text{les éléments de } \Gamma \text{ ont un point fixe commun}}$$

À retenir. L'hypothèse porte sur chaque élément séparément, la conclusion sur tous à la fois : c'est la structure de groupe, à travers le commutateur $f \circ g \circ f^{-1} \circ g^{-1}$, qui relie les deux.

EXERCICE 52 ⋆⋆⋆

1. L'axe des abscisses est la droite (OI), et l'axe des ordonnées est la perpendiculaire à (OI) passant par O : ce sont des droites constructibles.
Si $x = 0$, les trois points sont égaux à O. Si $x \neq 0$ et si l'un des trois points est constructible, le cercle de centre O passant par ce point est constructible ; il a pour rayon $|x|$, et il coupe les axes en $(x,0)$, $(-x,0)$, $(0,x)$ et $(0,-x)$, qui sont donc constructibles.
Si $(x,0)$ est constructible, x est l'abscisse d'un point constructible, donc $x \in K$. Réciproquement, soit $x \in K$ et M un point constructible dont x est l'abscisse ou l'ordonnée. Dans le premier cas, la perpendiculaire à l'axe des abscisses passant par M coupe cet axe en $(x,0)$; dans le second, la perpendiculaire à l'axe des ordonnées passant par M coupe cet axe en $(0,x)$, et l'on conclut par ce qui précède.

$$\boxed{x \in K \iff (x,0) \text{ constructible} \iff (0,x) \text{ constructible}, \qquad \text{et} \qquad -K = K}$$

2. Les points $(x,0)$ et $(0,y)$ sont constructibles par la question 1. La perpendiculaire à l'axe des abscisses passant par $(x,0)$ et la perpendiculaire à l'axe des ordonnées passant par $(0,y)$ se coupent en (x,y), qui est donc constructible. Si $y=0$, on a $x+y=x-y=x\in K$. Sinon, le cercle de centre $(x,0)$ passant par (x,y) a pour rayon $|y|$, et il coupe l'axe des abscisses aux points d'abscisses $x+|y|$ et $x-|y|$, c'est-à-dire $x+y$ et $x-y$.

$$\boxed{x+y\in K \qquad \text{et} \qquad x-y\in K}$$

3. Les points I et $Y(0,y)$ sont distincts et constructibles, et la droite (IY) est dirigée par le vecteur $(-1,y)$. Sa parallèle passant par $X(x,0)$ est formée des points $(x-t,ty)$, $t\in\mathbb{R}$; elle n'est pas parallèle à l'axe des ordonnées, et elle le coupe pour $t=x$, au point constructible $(0,xy)$. C'est le théorème de Thalès : le rapport des ordonnées $\dfrac{xy}{y}$ est égal au rapport des abscisses $\dfrac{x}{1}$.
De même, la droite (XJ) est dirigée par $(-x,1)$, et sa parallèle passant par I, formée des points $(1-tx,t)$, coupe l'axe des ordonnées pour $t=\dfrac{1}{x}$, au point constructible $\left(0,\dfrac{1}{x}\right)$.

$$\boxed{xy\in K \qquad \text{et} \qquad \frac{1}{x}\in K}$$

Si x ou y est nul, $xy=0$ appartient aussi à K, abscisse de O. Ainsi K est une partie de $\mathbb{R}$ qui contient 1, stable par différence et par produit : c'est un sous-anneau de $\mathbb{R}$, donc un anneau commutatif non nul, dans lequel tout élément non nul a son inverse. C'est un sous-corps de $\mathbb{R}$. Il contient 1, donc $\mathbb{Z}$, par stabilité par somme et par différence, puis tous les quotients $\dfrac{p}{q}$ avec $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$.

$$\boxed{K \text{ est un sous-corps de } \mathbb{R} \text{ contenant } \mathbb{Q}}$$

4. Comme K est un corps, $m=\dfrac{a-1}{2}$ appartient à K, et le point $M(m,0)$, milieu de $[AB]$, est constructible, de même que B. Le cercle de centre M passant par B est donc constructible, et c'est le cercle de diamètre $[AB]$, de rayon $\dfrac{a+1}{2}$. Il coupe l'axe des ordonnées aux points $(0,h)$ tels que

$$\left(\frac{a-1}{2}\right)^2+h^2=\left(\frac{a+1}{2}\right)^2, \qquad \text{c'est-à-dire} \qquad h^2=\frac{(a+1)^2-(a-1)^2}{4}=a.$$

Le point $H(0,\sqrt{a})$ est constructible ; c'est la relation $OH^2=OA\times OB$ dans le triangle AHB, rectangle en H.

$$\boxed{a\in K,\ a\geqslant 0 \implies \sqrt{a}\in K}$$

Le cas $a=0$ est immédiat.

5. D'après les questions 3 et 4, $\sqrt{5}\in K$, donc $c=\cos\dfrac{2\pi}{5}=\dfrac{\sqrt{5}-1}{4}\in K$, puis $\cos\dfrac{4\pi}{5}=2c^2-1\in K$. Les cosinus des angles $\dfrac{2k\pi}{5}$, pour $0\leqslant k\leqslant 4$, valent 1, c, $2c^2-1$, $2c^2-1$ et c, puisque $\cos\dfrac{6\pi}{5}=\cos\dfrac{4\pi}{5}$ et $\cos\dfrac{8\pi}{5}=\cos\dfrac{2\pi}{5}$. Les sinus correspondants valent $\pm\sqrt{1-\cos^2\dfrac{2k\pi}{5}}$, qui sont dans K par la question 4 et la stabilité par passage à l'opposé. On conclut par la question 2.

$$\boxed{\text{les sommets du pentagone régulier sont constructibles}}$$

Pour $k=1$, on trouve $\sin\dfrac{2\pi}{5}=\sqrt{1-c^2}=\sqrt{\dfrac{5+\sqrt{5}}{8}}$. ✓

À retenir. La structure de corps transforme une question de géométrie, qui demande quels points l'on peut construire, en une question d'algèbre, qui demande quels nombres l'on obtient à partir de 0 et de 1 par les quatre opérations et la racine carrée. C'est sous cette seconde forme que l'on démontre l'impossibilité de certaines constructions.

EXERCICE 53 ⋆⋆⋆⋆

1. Soit $x \neq 0$ dans H ; comme $-x \in H$, l'un des deux est strictement positif. La partie $H \cap]0\,,+\infty[$ est non vide et minorée par 0 : elle a une borne inférieure $\alpha \geqslant 0$ (chapitre 7).

2. *(a)* Supposons $\alpha \notin H$. Par la caractérisation de la borne inférieure, il existe $g \in H$ tel que $\alpha < g < 2\alpha$, puis, comme $\alpha < g$ et que α n'est pas atteint, $h \in H$ tel que $\alpha < h < g$. Alors $g - h \in H$ et $0 < g - h < g - \alpha < \alpha$, ce qui contredit la définition de α. Ainsi $\alpha \in H$.

(b) Soit $x \in H$ et $k = \lfloor x/\alpha \rfloor$. Alors $0 \leqslant x - k\alpha < \alpha$, et $x - k\alpha \in H$, puisque $k\alpha \in H$. Si $x - k\alpha > 0$, cela contredit la définition de α ; donc $x = k\alpha$. Réciproquement, $\alpha\mathbb{Z} \subset H$.

$$\boxed{\alpha > 0 \implies H = \alpha\mathbb{Z}}$$

3. Si $\alpha = 0$, pour tout $\varepsilon > 0$, il existe $g \in H$ tel que $0 < g < \varepsilon$. Soit $]u, v[$ un intervalle ouvert non vide, et $g \in H$ tel que $0 < g < v - u$. Avec $k = \lfloor u/g \rfloor + 1$, on a $u < kg \leqslant u + g < v$, et $kg \in H$.

$$\boxed{\alpha = 0 \implies H \text{ est dense dans } \mathbb{R}}$$

4. L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ contient 0 et la différence de deux de ses éléments : c'est un sous-groupe de $\mathbb{R}$, non réduit à $\{0\}$. S'il n'est pas dense, il est de la forme $\alpha\mathbb{Z}$ avec $\alpha > 0$, par les questions 2 et 3 ; alors $a = m\alpha$ et $b = n\alpha$, avec $n \neq 0$, et $\dfrac{a}{b} = \dfrac{m}{n}$ est rationnel. Réciproquement, si $\dfrac{a}{b} = \dfrac{p}{q}$ avec $q \in \mathbb{N}^*$, alors $a\mathbb{Z} + b\mathbb{Z} \subset \dfrac{b}{q}\mathbb{Z}$, qui ne rencontre pas $]0\,, \dfrac{|b|}{q}[$.

$$\boxed{a\mathbb{Z} + b\mathbb{Z} \text{ dense} \iff \frac{a}{b} \notin \mathbb{Q}}$$

5. Le rapport $\dfrac{1}{2\pi}$ est irrationnel, donc $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense. Soit $y \in [-1\,,1]$, $\theta = \operatorname{Arccos} y$ et $\varepsilon > 0$. Il existe n et m entiers tels que $|n + 2\pi m - \theta| < \varepsilon$, et, comme cos est 1-lipschitzienne (chapitre 9),

$$|\cos|n| - y| = |\cos(n + 2\pi m) - \cos\theta| \leqslant |n + 2\pi m - \theta| < \varepsilon,$$

où l'on a utilisé la parité et la 2π-périodicité du cosinus.

$$\boxed{\{\cos n \mid n \in \mathbb{N}\} \text{ est dense dans } [-1\,,1]}$$

À retenir. Un sous-groupe de $\mathbb{R}$ est « discret » ou dense, sans intermédiaire. Cette dichotomie explique l'exercice 21 : la somme de deux fonctions périodiques est périodique si et seulement si le groupe engendré par leurs périodes est discret.

EXERCICE 54 ⋆⋆⋆⋆

Pour $x \in G$, on note $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ le sous-groupe engendré par x (exercice 20). On a $G = \bigcup_{x \in G} \langle x \rangle$, et cette réunion ne fait intervenir qu'un nombre fini de sous-groupes distincts. Il suffit donc de montrer que chacun est fini.

▷ *Les puissances de x ne sont pas toutes distinctes.* Sinon, les sous-groupes $\langle x^m \rangle$, pour $m \geqslant 1$, seraient deux à deux distincts. En effet, si $1 \leqslant m < m'$ et $\langle x^m \rangle = \langle x^{m'} \rangle$, alors $x^m = x^{m'k}$ pour un entier k, avec $m'k \neq m$, puisque m n'est pas multiple de $m' > m$; cela contredit l'hypothèse que les puissances sont distinctes. Le groupe aurait alors une infinité de sous-groupes.

▷ *Conclusion.* Il existe donc $i < j$ tels que $x^i = x^j$, et comme à l'exercice 31, $\langle x \rangle = \{e, x, \ldots, x^{p-1}\}$, où p est l'ordre de x : chaque $\langle x \rangle$ est fini. Une réunion finie d'ensembles finis est finie (chapitre 2).

$$\boxed{G \text{ est fini}}$$

À retenir. Le seul obstacle était un élément dont toutes les puissances sont distinctes : il engendre une copie de $(\mathbb{Z}, +)$, qui possède les sous-groupes $m\mathbb{Z}$ en nombre infini.

EXERCICE 55 ⋆⋆⋆⋆

1. Soit $g \in G$, et $gB^{-1} = \{gb^{-1} \mid b \in B\}$. L'application $b \mapsto gb^{-1}$ est injective, donc gB^{-1} a $|B|$ éléments. Les parties A et gB^{-1} de G vérifient $|A| + |gB^{-1}| > |G|$: elles ne sont pas disjointes, sinon leur réunion aurait plus d'éléments que G (chapitre 2, lemme 4). Il existe donc $a \in A$ et $b \in B$ tels que $a = gb^{-1}$, soit $g = ab$.

$$\boxed{G = AB}$$

2. Dans $G = \mathbb{U}_2 = \{1, -1\}$, avec $A = B = \{1\}$, on a $|A| + |B| = 2 = |G|$, mais $AB = \{1\} \neq G$. Plus généralement, si H est un sous-groupe de G à $\dfrac{|G|}{2}$ éléments, $A = B = H$ donne $AB = H \neq G$.

EXERCICE 56 ⋆⋆⋆⋆

On note $n = |G|$, $z = |Z(G)|$, et, pour $x \in G$, $C(x) = \{y \in G \mid xy = yx\}$, qui est un sous-groupe contenant $Z(G)$ et x, par le même calcul qu'à l'exercice 14.

1. Comme G n'est pas abélien, il existe $x \notin Z(G)$. Alors $C(x) \neq G$, puisque x ne commute pas avec tout, et $C(x) \neq Z(G)$, puisque $x \in C(x)$. Par le théorème de Lagrange, appliqué à $Z(G) \subset C(x)$ puis à $C(x) \subset G$, z divise $|C(x)|$ et $|C(x)|$ divise n, les inclusions étant strictes : $|C(x)| \geqslant 2z$ et $|C(x)| \leqslant \dfrac{n}{2}$.

$$\boxed{n \geqslant 4z}$$

2. Le nombre de couples qui commutent est $\displaystyle\sum_{x \in G} |C(x)|$. Pour $x \in Z(G)$, $|C(x)| = n$; pour $x \notin Z(G)$, $|C(x)| \leqslant \dfrac{n}{2}$. Ainsi

$$\sum_{x \in G} |C(x)| \leqslant zn + (n - z)\frac{n}{2} = \frac{n^2}{2} + \frac{zn}{2} \leqslant \frac{n^2}{2} + \frac{n^2}{8} = \frac{5n^2}{8}.$$

$$\boxed{\frac{|\{(x, y) \in G^2 \mid xy = yx\}|}{|G|^2} \leqslant \frac{5}{8}}$$

Pour $\mathfrak{S}_3$, on trouve $6 + 3 \times 2 + 2 \times 3 = 18$ couples, soit une proportion $\dfrac{18}{36} = \dfrac{1}{2}$. La borne est atteinte par le groupe des huit isométries du carré, dont le centre a deux éléments.

EXERCICE 57 ⋆⋆⋆⋆

1. La relation est définie par une égalité d'ensembles : elle est réflexive, symétrique et transitive. Pour $h \in H$, $hHh^{-1} = H$, puisque H est un sous-groupe, d'où

$$(xh)H(xh)^{-1} = x\,(hHh^{-1})\,x^{-1} = xHx^{-1} :$$

$x \sim xh$. Chaque classe de $\sim$ est donc une réunion de classes xH de l'exercice 31, et il y a au plus autant de classes de $\sim$ que de classes xH, c'est-à-dire $\dfrac{|G|}{|H|}$.

$$\boxed{\text{nombre de classes} \leqslant \frac{|G|}{|H|}}$$

2. La réunion des xHx^{-1} ne dépend que de la classe de x : c'est une réunion d'au plus $k = \dfrac{|G|}{|H|}$ ensembles. Chacun a $|H|$ éléments, l'application $h \mapsto xhx^{-1}$ étant injective, et tous contiennent e. Ainsi

$$\left| \bigcup_{x \in G} xHx^{-1} \right| \leqslant k(|H| - 1) + 1 = |G| - k + 1 < |G|,$$

puisque $k \geqslant 2$, H étant strict.

$$\boxed{\bigcup_{x \in G} xHx^{-1} \neq G}$$

EXERCICE 58 ⋆⋆⋆⋆

Fixons $x \in A$, et posons $S = \{y \in A \mid xy = yx\}$ et $T = \{y \in A \mid xy = -yx\}$. Ce sont deux sous-groupes de $(A, +)$, qui contiennent 0 et sont stables par différence, par distributivité. L'hypothèse dit que $A = S \cup T$. Par l'exercice 18, question 2, $S = A$ ou $T = A$.

Si $T = A$, alors $y = 1$ donne $x = -x$, donc $x + x = 0$; pour tout y, $y(x + x) = 0$, soit $yx = -yx$, et $xy = -yx = yx$. Dans les deux cas, x commute avec tout élément de A.

$$\boxed{A \text{ est commutatif}}$$

À retenir. Le résultat de groupes « un groupe n'est pas réunion de deux sous-groupes stricts » transforme une alternative, valable pour chaque couple, en une propriété uniforme.

EXERCICE 59 ⋆⋆⋆⋆

Supposons qu'il existe un isomorphisme $f : (\mathbb{K}, +) \to (\mathbb{K}^*, \cdot)$.

▷ *Si* $1 \neq -1$. L'élément -1 de $\mathbb{K}^*$ vérifie $(-1)^2 = 1$ et $-1 \neq 1$. Son antécédent a est non nul et vérifie $f(a + a) = (-1)^2 = 1 = f(0)$, donc $a + a = 0$ par injectivité. Alors $(1 + 1)a = 0$ avec $a \neq 0$, d'où $1 + 1 = 0$, soit $1 = -1$: contradiction.

▷ *Si* $1 = -1$. Alors $x + x = 0$ pour tout x, donc tout $y = f(x)$ de $\mathbb{K}^*$ vérifie $y^2 = f(x + x) = 1$. Ainsi $(y-1)^2 = y^2 - 2y + 1 = y^2 + 1 = 0$, et $y = 1$. Le groupe $\mathbb{K}^*$ serait réduit à $\{1\}$, donc $\mathbb{K} = \{0, 1\}$ aurait deux éléments, et f ne pourrait pas être une bijection.

$$\boxed{(\mathbb{K}, +) \text{ et } (\mathbb{K}^*, \cdot) \text{ ne sont jamais isomorphes}}$$

On retrouve, pour $\mathbb{K} = \mathbb{R}$, la question (a) de l'exercice 27, et le corps à deux éléments de l'exercice 43 montre que les corps où $1 = -1$ existent bien : le second cas n'est pas vide, il faut le traiter à part.