

Groupes, anneaux et corps

Corrigé de l'exercice 1 : Propriétés de lois de composition usuelles

1. La réunion est associative et commutative. De plus, $A \cup \emptyset = A$ pour toute partie A , donc $\emptyset$ est neutre. Si $A \cup B = \emptyset$, alors $A \subset A \cup B = \emptyset$, donc $A = \emptyset$. **Ainsi, $\cup$ est associative, commutative, de neutre $\emptyset$, et $\emptyset$ est le seul élément inversible.**
2. De même, l'intersection est associative et commutative, et $A \cap E = A$ pour tout $A \subset E$. Si $A \cap B = E$, alors $E \subset A$, donc $A = E$. **Par conséquent, $\cap$ a pour neutre E , et E est le seul inversible.**
3. D'abord, $\max(\max(m, n), p)$ et $\max(m, \max(n, p))$ valent toutes deux le plus grand des trois entiers : la loi est associative. Elle est évidemment commutative. Ensuite, $\max(m, 0) = m$ car $m \geq 0$, donc 0 est neutre. Enfin, $\max(m, n) = 0$ impose $m = 0$. **Le seul inversible est donc 0.**
4. La soustraction n'est pas associative : $(1 - 1) - 1 = -1$ mais $1 - (1 - 1) = 1$. Elle n'est pas commutative : $1 - 0 \neq 0 - 1$. Supposons qu'il existe un neutre e . Alors $x - e = x$ donne $e = 0$, puis $e - x = x$ donne $-x = x$ pour tout x , ce qui est faux pour $x = 1$. **La soustraction n'a donc pas de neutre.**
5. La composition est associative, de neutre $\text{id}_{\mathbb{R}}$. En revanche, avec $f(x) = x + 1$ et $g(x) = 2x$, on trouve $f \circ g(x) = 2x + 1$ et $g \circ f(x) = 2x + 2$. Elle n'est donc pas commutative. Enfin, f est inversible s'il existe g telle que $f \circ g = g \circ f = \text{id}$, ce qui caractérise les bijections. **Les inversibles de $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$ sont les bijections de $\mathbb{R}$ dans $\mathbb{R}$.**

Corrigé de l'exercice 2 : Parties stables

1. Pour l'addition, $1 + 1 = 2$ n'est pas impair : I n'est pas stable. Pour la multiplication, $(2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ est impair. **Donc I est stable par $\times$ mais pas par $+$.**
2. Une somme de réels négatifs est négative, donc $\mathbb{R}_-$ est stable par addition. En revanche, $(-1) \times (-1) = 1 \notin \mathbb{R}_-$. **Ainsi, $\mathbb{R}_-$ est stable par $+$, pas par $\times$.**
3. Si $z^n = 1$ et $w^n = 1$, alors $(zw)^n = z^n w^n = 1$, car la multiplication des complexes est commutative. **L'ensemble $\mathbb{U}_n$ est stable par multiplication.**
4. Le complexe 2 est de module 2 , mais $2 \times 2 = 4$ est de module 4 . **Ce cercle n'est pas stable par multiplication.**
5. Si f et g sont paires, alors $(fg)(-x) = f(-x)g(-x) = f(x)g(x)$: le produit est pair. Si f et g sont impaires, alors $(fg)(-x) = (-f(x))(-g(x)) = (fg)(x)$: le produit est pair. Par exemple, $x \rightarrow x$ est impaire, mais son carré $x \rightarrow x^2$ ne l'est pas, puisqu'il vaut 1 en 1 et en -1 . **Les fonctions paires forment une partie stable, les fonctions impaires non.**
6. Soient f et g injectives. Si $g \circ f(x) = g \circ f(y)$, l'injectivité de g donne $f(x) = f(y)$, puis celle de f donne $x = y$. **Les injections forment donc une partie stable par composition.**

Corrigé de l'exercice 3 : Les groupes $\mathbb{U}$, $\mathbb{U}_n$, $\mathbb{C}^*$ et $\mathbb{R}_+^*$

1. On applique la caractérisation des sous-groupes. D'abord, $\mathbb{U} \subset \mathbb{C}^*$ et $|1| = 1$. Ensuite, pour $z, w \in \mathbb{U}$, on a $|z w^{-1}| = |z| / |w| = 1$. De même, $\mathbb{R}_+^* \subset \mathbb{C}^*$, $1 > 0$, et $x / y > 0$ pour $x, y > 0$. **Ainsi, $\mathbb{U}$ et $\mathbb{R}_+^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.**
2. Écrivons $m = nq$ avec $q \in \mathbb{N}^*$. Si $z^n = 1$, alors $z^m = (z^n)^q = 1$, donc $\mathbb{U}_n \subset \mathbb{U}_m$. Par ailleurs, $\mathbb{U}_n$ contient 1 et, pour $z, w \in \mathbb{U}_n$, $(zw^{-1})^n = z^n (w^n)^{-1} = 1$. **Par conséquent, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}_m$.**
3. Si $z^3 = 1$ et $z^4 = 1$, alors $z = z^4 (z^3)^{-1} = 1$. Donc $\mathbb{U}_3 \cap \mathbb{U}_4 = \{1\}$.
Considérons ensuite ij , produit de deux éléments de la réunion. On calcule

$(ij)^3 = i^3 j^3 = -i \neq 1$ et $(ij)^4 = i^4 j^4 = j \neq 1$. Ainsi, $ij \notin \mathbb{U}_3 \cup \mathbb{U}_4$. **La réunion n'est pas stable : ce n'est pas un sous-groupe de $\mathbb{U}$.** Sur la figure de l'énoncé, $ij = e^{7i\pi/6}$ tombe en effet entre j^2 et -1 , hors des points marqués.

4. D'abord, φ est un morphisme :

$\varphi((r, u)(r', u')) = \varphi(rr', uu') = rr'uu' = (ru)(r'u')$. Ensuite, si $ru = 1$, on prend le module : $r = 1$, puis $u = 1$. Le noyau est donc $\{(1, 1)\}$, et φ est injective. Enfin, tout $z \in \mathbb{C}^*$ s'écrit $z = |z| \times \frac{z}{|z|}$, avec $|z| > 0$ et $\left| \frac{z}{|z|} \right| = 1$. **Donc φ est un isomorphisme de $\mathbb{R}_+^* \times \mathbb{U}$ sur $\mathbb{C}^*$.**

Point de méthode : pour montrer qu'une réunion n'est pas un sous-groupe, cherchez deux éléments pris dans des morceaux différents et regardez leur produit.

Corrigé de l'exercice 4 : Montrer qu'une partie est un sous-groupe

- On a $0 = 5 \times 0 \in 5\mathbb{Z}$, et $5a - 5b = 5(a - b) \in 5\mathbb{Z}$. **Donc $5\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.**
- On a $H \subset \mathbb{Q}^*$ et $1 = 2^0 \in H$. Pour $k, l \in \mathbb{Z}$, $2^k (2^l)^{-1} = 2^{k-l} \in H$. **Ainsi, H est un sous-groupe de $(\mathbb{Q}^*, \times)$.**
- D'abord, $1^2 = 1 \in \mathbb{Q}$, donc $1 \in H$. Soient ensuite $x, y \in H$. Alors $(xy^{-1})^2 = x^2 / y^2$ est un quotient de deux rationnels, le dénominateur étant non nul. De plus, $xy^{-1} \neq 0$. **Par conséquent, H est un sous-groupe de $(\mathbb{R}^*, \times)$.** Il contient par exemple $\sqrt{2}$ et $\sqrt{3}$.
- On a $0, 1 \in \mathbb{N}$ mais $0 - 1 = -1 \notin \mathbb{N}$. **Donc $\mathbb{N}$ n'est pas un sous-groupe de $\mathbb{Z}$.**
- Le complexe $z = e^{i\pi/3}$ a pour partie réelle $1/2 > 0$. Cependant, $z^2 = e^{2i\pi/3}$ a pour partie réelle $-1/2$. **Ainsi, H n'est pas stable, donc ce n'est pas un sous-groupe.**
- D'abord, $\text{id}(0) = 0$. Soient ensuite $f, g \in H$. Comme $g(0) = 0$, on a $g^{-1}(0) = 0$. Donc $f \circ g^{-1}(0) = f(0) = 0$. **Par conséquent, H est un sous-groupe de $S_{\mathbb{R}}$.**

Corrigé de l'exercice 5 : Intersection et réunion de sous-groupes

1. Le neutre e appartient à H et à K . Si $x, y \in H \cap K$, alors $x \cdot y^{-1}$ appartient à H (sous-groupe) et à K (sous-groupe). **Donc $H \cap K$ est un sous-groupe de G .**
2. Si $H \subset K$, alors $H \cup K = K$ est un sous-groupe ; de même si $K \subset H$.
Réciproquement, supposons que $H \cup K$ est un sous-groupe, et qu'aucune inclusion n'a lieu. On choisit alors $h \in H \setminus K$ et $k \in K \setminus H$. Le produit $h \cdot k$ appartient à $H \cup K$. S'il est dans H , alors $k = h^{-1} \cdot (h \cdot k) \in H$, ce qui est exclu. S'il est dans K , alors $h = (h \cdot k) \cdot k^{-1} \in K$, ce qui est également exclu. **C'est absurde : donc $H \cup K$ est un sous-groupe si et seulement si $H \subset K$ ou $K \subset H$.**
3. Soit $x \in 4\mathbb{Z} \cap 6\mathbb{Z}$. On écrit $x = 4a$. Comme 3 divise $x = 4a$ et que 3 est premier avec 4, le lemme de Gauss donne $3 \mid a$. Donc $12 \mid x$. Réciproquement, un multiple de 12 est multiple de 4 et de 6. **Ainsi, $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$.** Enfin, $2 \notin 3\mathbb{Z}$ et $3 \notin 2\mathbb{Z}$: aucune inclusion n'a lieu. **D'après la question 2, $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe.**

Corrigé de l'exercice 6 : Le groupe produit $U_2 \times U_2$

1. On calcule composante par composante. Par exemple, $ab = (1 \times (-1), (-1) \times 1) = (-1, -1) = c$. De même, $ac = (-1, 1) = b$ et $bc = (1, -1) = a$. On obtient la table de gauche de la figure ci-dessous.
2. Pour $x = (x_1, x_2) \in G$, on a $x^2 = (x_1^2, x_2^2) = (1, 1) = e$, car $(\pm 1)^2 = 1$. De plus, $xy = (x_1 y_1, x_2 y_2) = (y_1 x_1, y_2 x_2) = yx$. **Ainsi, tout élément de G vérifie $x^2 = e$, et G est abélien.**
3. La table de U_4 figure à droite. Supposons qu'il existe un isomorphisme $f : U_4 \rightarrow G$. Alors $f(i^2) = f(i)^2 = e = f(1)$, d'après la question 2. Par injectivité, $i^2 = 1$, ce qui est faux puisque $i^2 = -1$. **Les groupes G et U_4 ne sont donc pas isomorphes.**

×	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\mathbb{U}_2 \times \mathbb{U}_2 : x^2 = e \text{ pour tout } x$$

×	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

$$\mathbb{U}_4 : i^2 = -1 \neq 1$$

Sur la figure, la diagonale de la table de G ne contient que e , contrairement à celle de $\mathbb{U}_4$. C'est exactement l'invariant utilisé.

4. Les parties $\{e\}$ et G sont des sous-groupes. Pour $x \in \{a, b, c\}$, la partie $\{e, x\}$ est un sous-groupe : elle contient e , et $x^{-1} = x$, $x^2 = e$. Soit enfin H un sous-groupe contenant deux éléments distincts de $\{a, b, c\}$. Leur produit est alors le troisième, d'après la question 1. Donc $H = G$. **Les sous-groupes de G sont $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$ et G .**

Corrigé de l'exercice 7 : Le groupe symétrique S_3

- On a $\rho^2(1) = \rho(2) = 3$, $\rho^2(2) = 1$ et $\rho^2(3) = 2$. Ensuite, $\rho^3(1) = \rho(3) = 1$, et de même pour 2 et 3 : $\rho^3 = \text{id}$. Les permutations ρ et ρ^2 n'ont aucun point fixe. Chaque transposition τ_{ij} a exactement un point fixe, différent pour chacune. Les six permutations citées sont donc distinctes. **Comme S_3 a $3! = 6$ éléments, on a bien**

$$S_3 = \{\text{id}, \rho, \rho^2, \tau_{12}, \tau_{13}, \tau_{23}\}.$$
- On calcule $\tau_{12} \circ \tau_{13} : 1 \rightarrow 3, 2 \rightarrow 1, 3 \rightarrow 2$. C'est ρ^2 . Puis $\tau_{13} \circ \tau_{12} :$
 $1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 1$. C'est ρ . **Comme $\rho \neq \rho^2$, le groupe S_3 n'est pas abélien.**

3. On a $\text{id} = \rho^0 \in A$. Comme $\rho^3 = \text{id}$, les exposants se lisent modulo 3. Ainsi, pour $k, l \in \{0, 1, 2\}$, $\rho^k \circ (\rho^l)^{-1} = \rho^{k-l}$, qui est l'un des éléments id, ρ, ρ^2 . **Donc A est un sous-groupe de S_3 , à trois éléments.**
4. D'abord, $\text{id} \in H$. Si $\sigma, \sigma' \in H$, alors $\sigma'^{-1}(3) = 3$, donc $\sigma \circ \sigma'^{-1}(3) = \sigma(3) = 3$. C'est donc un sous-groupe. Un élément de H fixe 3 et permute $\{1, 2\}$. **Par conséquent, $H = \{\text{id}, \tau_{12}\}$.**
5. Dans S_n , on a $\tau_{12} \circ \tau_{13}(1) = \tau_{12}(3) = 3$, tandis que $\tau_{13} \circ \tau_{12}(1) = \tau_{13}(2) = 2$. **Ces deux permutations ne commutent pas, donc S_n n'est pas abélien pour $n \geq 3$.**

Corrigé de l'exercice 8 : Les sous-groupes de $\mathbb{Z}$

1. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$, et $n = 0$ convient.
2. Comme $H \neq \{0\}$, il contient un entier $x \neq 0$. Il contient aussi $-x$, et l'un des deux est strictement positif. Donc $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$: elle possède un plus petit élément n . Ensuite, $0 \in H$ et, si $kn \in H$, alors $(k+1)n = kn + n \in H$. Par récurrence, $kn \in H$ pour tout $k \in \mathbb{N}$. En passant à l'opposé, $-kn \in H$. **Ainsi, $n\mathbb{Z} \subset H$.**
3. Soit $x \in H$. La division euclidienne donne $x = qn + r$ avec $0 \leq r < n$. Or $r = x - qn$ est la différence de deux éléments de H , donc $r \in H$. Si l'on avait $r > 0$, r serait un élément de $H \cap \mathbb{N}^*$ strictement inférieur à n , ce qui contredit la minimalité. Donc $r = 0$ et $x \in n\mathbb{Z}$. Par conséquent, $H = n\mathbb{Z}$. Pour l'unicité, si $n\mathbb{Z} = m\mathbb{Z}$ avec $n, m \in \mathbb{N}$, alors $m \mid n$ et $n \mid m$, donc $n = m$. **Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$.**
4. On a $0 = 4 \times 0 + 6 \times 0 \in K$, et $(4u + 6v) - (4u' + 6v') = 4(u - u') + 6(v - v') \in K$. Donc K est un sous-groupe. Tous ses éléments sont pairs, donc $K \subset 2\mathbb{Z}$. De plus, $2 = 4 \times (-1) + 6 \times 1 \in K$, donc $2\mathbb{Z} \subset K$. **Ainsi, $K = 2\mathbb{Z}$ et $n = 2$.**

Point de méthode : le plus petit élément strictement positif d'un sous-groupe de $\mathbb{Z}$ est le bon candidat ; la division euclidienne fait ensuite tout le travail.

Corrigé de l'exercice 9 : Morphismes usuels et noyaux

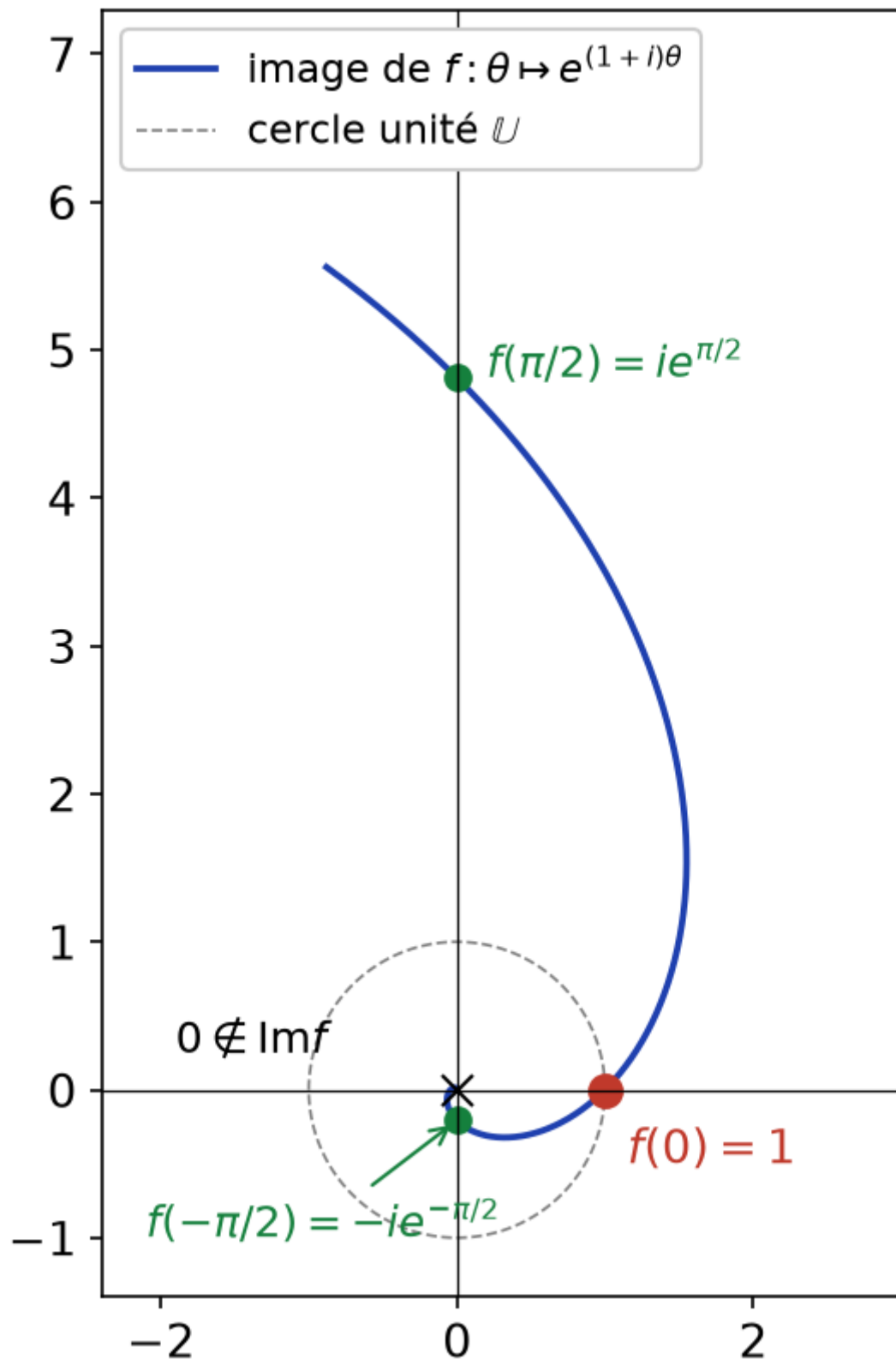
1. On a $|zz'| = |z||z'|$, donc f_1 est un morphisme. Son noyau est $\left\{z, |z| = 1\right\} = \mathbb{U}$. Comme $\ker f_1 = \mathbb{U} \neq \{1\}$, f_1 n'est pas injectif.
2. On a $e^{2i\pi(t+t')} = e^{2i\pi t} e^{2i\pi t'}$. Ensuite, $e^{2i\pi t} = 1$ si et seulement si $2\pi t \in 2\pi\mathbb{Z}$, c'est-à-dire $t \in \mathbb{Z}$. Donc $\ker f_2 = \mathbb{Z}$, et f_2 n'est pas injectif.
3. Comme $\mathbb{C}^*$ est commutatif, $(zz')^4 = z^4 z'^4$. Le noyau est l'ensemble des z tels que $z^4 = 1$. Ainsi, $\ker f_3 = \mathbb{U}_4 = \{1, i, -1, -i\}$, et f_3 n'est pas injectif.
4. On a $i^k + 1 = i^k i^1$. Ensuite, $i^k = e^{ik\pi/2} = 1$ si et seulement si $k\pi/2 \in 2\pi\mathbb{Z}$, soit $4 \mid k$. Donc $\ker f_4 = 4\mathbb{Z}$ et f_4 n'est pas injectif. Enfin, i^k ne dépend que du reste de k modulo 4. Par conséquent, $\text{Im } f_4 = \{1, i, -1, -i\} = \mathbb{U}_4$.
5. On a $(xy)^3 = x^3 y^3$. La fonction cube est strictement croissante sur $\mathbb{R}$, donc $x^3 = 1$ équivaut à $x = 1$: $\ker f_5 = \{1\}$ et f_5 est injectif. De plus, tout $y \in \mathbb{R}^*$ possède une racine cubique réelle, non nulle, d'où la surjectivité. Ainsi, f_5 est un automorphisme de $(\mathbb{R}^*, \times)$.

Corrigé de l'exercice 10 : Une spirale et un morphisme injectif

1. Par la propriété de l'exponentielle complexe, $f(\theta + \theta') = e^{(1+i)\theta + (1+i)\theta'} = f(\theta) f(\theta')$. De plus, $f(\theta) \neq 0$. Donc f est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.
2. Si $f(\theta) = 1$, on prend le module : $|f(\theta)| = e^\theta = 1$, donc $\theta = 0$. Réciproquement, $f(0) = 1$. Ainsi, $\ker f = \{0\}$: le morphisme f est injectif.
3. L'image d'un groupe par un morphisme est un sous-groupe du groupe d'arrivée. Donc $\text{Im } f$ est un sous-groupe de $\mathbb{C}^*$. Supposons $-1 = f(\theta)$. Alors $e^\theta = |-1| = 1$, donc $\theta = 0$ et $f(\theta) = 1 \neq -1$. Par conséquent, $-1 \notin \text{Im } f$, et f n'est pas surjectif.
4. D'une part, $f(\theta) \in \mathbb{U}$ équivaut à $e^\theta = 1$, soit $\theta = 0$: $\text{Im } f \cap \mathbb{U} = \{1\}$. D'autre part, $f(\theta)$ est un réel strictement positif si et seulement si $e^{i\theta} = f(\theta) / e^\theta$ est à la fois dans $\mathbb{U}$ et dans $\mathbb{R}_+^*$, c'est-à-dire $e^{i\theta} = 1$. Cela équivaut à $\theta \in 2\pi\mathbb{Z}$. Donc

$$\operatorname{Im} f \cap \mathbb{R}_+^* = \left\{ e^{2k\pi}, k \in \mathbb{Z} \right\}.$$

5. Le complexe $f(\theta)$ a pour module e^θ et pour argument θ . En coordonnées polaires, l'image est donc la courbe $r = e^\theta$: c'est une spirale logarithmique. Quand $\theta \rightarrow -\infty$, elle s'enroule autour de l'origine sans l'atteindre ; quand $\theta \rightarrow +\infty$, elle s'éloigne à l'infini. **La figure ci-dessous représente cette spirale, qui coupe le cercle unité au seul point 1.**



On lit aussi sur la figure que la demi-droite $\mathbb{R}_+^*$ est coupée en une suite de points $e^{2k\pi}$, conformément à la question 4.

Corrigé de l'exercice 11 : Image directe et image réciproque par un morphisme

1. D'abord, $e' = f(e) \in f(H)$. Soient ensuite $y_1 = f(x_1)$ et $y_2 = f(x_2)$ avec $x_1, x_2 \in H$. Alors $y_1 \diamond y_2^{-1} = f(x_1) \diamond f(x_2^{-1}) = f(x_1 \cdot x_2^{-1})$, et $x_1 \cdot x_2^{-1} \in H$. **Donc $f(H)$ est un sous-groupe de G' .**
2. Comme $f(e) = e' \in H'$, on a $e \in f^{-1}(H')$. Si $f(x)$ et $f(y)$ sont dans H' , alors $f(x \cdot y^{-1}) = f(x) \diamond f(y)^{-1} \in H'$. Enfin, si $x \in \ker f$, alors $f(x) = e' \in H'$. **Ainsi, $f^{-1}(H')$ est un sous-groupe de G qui contient $\ker f$.**
3. On a $|z^2| = |z|^2$, donc $z^2 \in \mathbb{U}$ équivaut à $|z| = 1$: $f^{-1}(\mathbb{U}) = \mathbb{U}$. Ensuite, $z^2 \in \{-1, 1\}$ équivaut à $(z^2)^2 = 1$, soit $z^4 = 1$: $f^{-1}(\{-1, 1\}) = \mathbb{U}_4$. Pour $z = e^{2ik\pi/6}$, on a $z^2 = e^{2ik\pi/3}$. Quand k décrit $\{0, \dots, 5\}$, on obtient tout $\mathbb{U}_3$. Enfin, le carré d'un réel non nul est strictement positif, et tout $y > 0$ vaut $(\sqrt{y})^2$. **Donc $f^{-1}(\mathbb{U}) = \mathbb{U}$, $f^{-1}(\{-1, 1\}) = \mathbb{U}_4$, $f(\mathbb{U}_6) = \mathbb{U}_3$ et $f(\mathbb{R}^*) = \mathbb{R}_+^*$.**

Corrigé de l'exercice 12 : Automorphismes intérieurs et centre d'un groupe

1. Pour $x, y \in G$, $\varphi_a(x)\varphi_a(y) = a x a^{-1} a y a^{-1} = a xy a^{-1} = \varphi_a(xy)$. C'est donc un morphisme. Ensuite, $\varphi_{a^{-1}}(\varphi_a(x)) = a^{-1} a x a^{-1} a = x$, et de même $\varphi_a \circ \varphi_{a^{-1}} = \text{id}_G$. **Ainsi, φ_a est un automorphisme de G , de réciproque $\varphi_{a^{-1}}$.**
2. On calcule $\varphi_a(\varphi_b(x)) = a b x b^{-1} a^{-1} = (ab) x (ab)^{-1} = \varphi_{ab}(x)$. D'après la question 1, $\varphi_a \in S_G$. **Par conséquent, $\Phi(ab) = \Phi(a) \circ \Phi(b)$: Φ est un morphisme de $(G, \cdot)$ dans $(S_G, \circ)$.**
3. On a $\Phi(a) = \text{id}_G$ si et seulement si $axa^{-1} = x$ pour tout x , c'est-à-dire $ax = xa$ pour tout x . **Donc $\ker \Phi = Z(G)$, et le centre est un sous-groupe de G , comme tout noyau.**
4. Le neutre id est dans le centre. Montrons qu'aucun autre élément n'y est. D'abord, $\tau_{12} \circ \rho(1) = 1$ et $\rho \circ \tau_{12}(1) = 3$. Ensuite, $\tau_{13} \circ \rho(1) = 2$ et $\rho \circ \tau_{13}(1) = 1$. De

même, $\tau_{23} \circ \rho(1) = 3$ et $\rho \circ \tau_{23}(1) = 2$. Aucune transposition ne commute donc avec ρ , et ρ n'est pas central. Enfin, si $\rho^2 = \rho^{-1}$ commuterait avec τ_{12} , son inverse ρ commuterait aussi avec τ_{12} : c'est exclu. **Ainsi, $Z(S_3) = \{\text{id}\}$, et ϕ est injectif pour $G = S_3$.**

Corrigé de l'exercice 13 : Isomorphismes et non-isomorphismes

1. L'exponentielle vérifie $e^x + y = e^x e^y$. Elle est continue et strictement croissante, de limites 0 en $-\infty$ et $+\infty$ en $+\infty$. C'est donc une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$, de réciproque $\ln$. **Ainsi, $\exp$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$.**
2. Supposons que $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$ soit un isomorphisme. Par surjectivité, il existe z tel que $f(z) = -1$. Or z possède une racine carrée $w \in \mathbb{C}^*$. On obtient alors $-1 = f(w^2) = f(w)^2 > 0$, ce qui est absurde. **Il n'existe donc aucun isomorphisme de $\mathbb{C}^*$ sur $\mathbb{R}^*$.**
3. Supposons que $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}_+^*, \times)$ soit un isomorphisme. Il existe $a \in \mathbb{Q}$ tel que $f(a) = 2$. Alors $2 = f\left(\frac{a}{2} + \frac{a}{2}\right) = f\left(\frac{a}{2}\right)^2$. Le rationnel positif $f(a/2)$ vaudrait donc $\sqrt{2}$, qui est irrationnel. **Ces deux groupes ne sont pas isomorphes.**
4. Supposons que $f : \mathbb{Z} \rightarrow \mathbb{Q}$ soit un isomorphisme, et posons $q = f(1)$. Comme f est un morphisme, $f(n) = nq$ pour tout $n \in \mathbb{Z}$. De plus, $q \neq 0$, sinon f serait nul. Par surjectivité, il existe n tel que $nq = q/2$, soit $n = 1/2$, qui n'est pas entier. **Donc $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.**
5. Supposons que $f : (\mathbb{R}^*, \times) \rightarrow (\mathbb{R}, +)$ soit un isomorphisme. Alors $f(1) = 0$ et $2f(-1) = f((-1)^2) = f(1) = 0$. Donc $f(-1) = 0 = f(1)$, ce qui contredit l'injectivité. **Ces groupes ne sont pas isomorphes.**

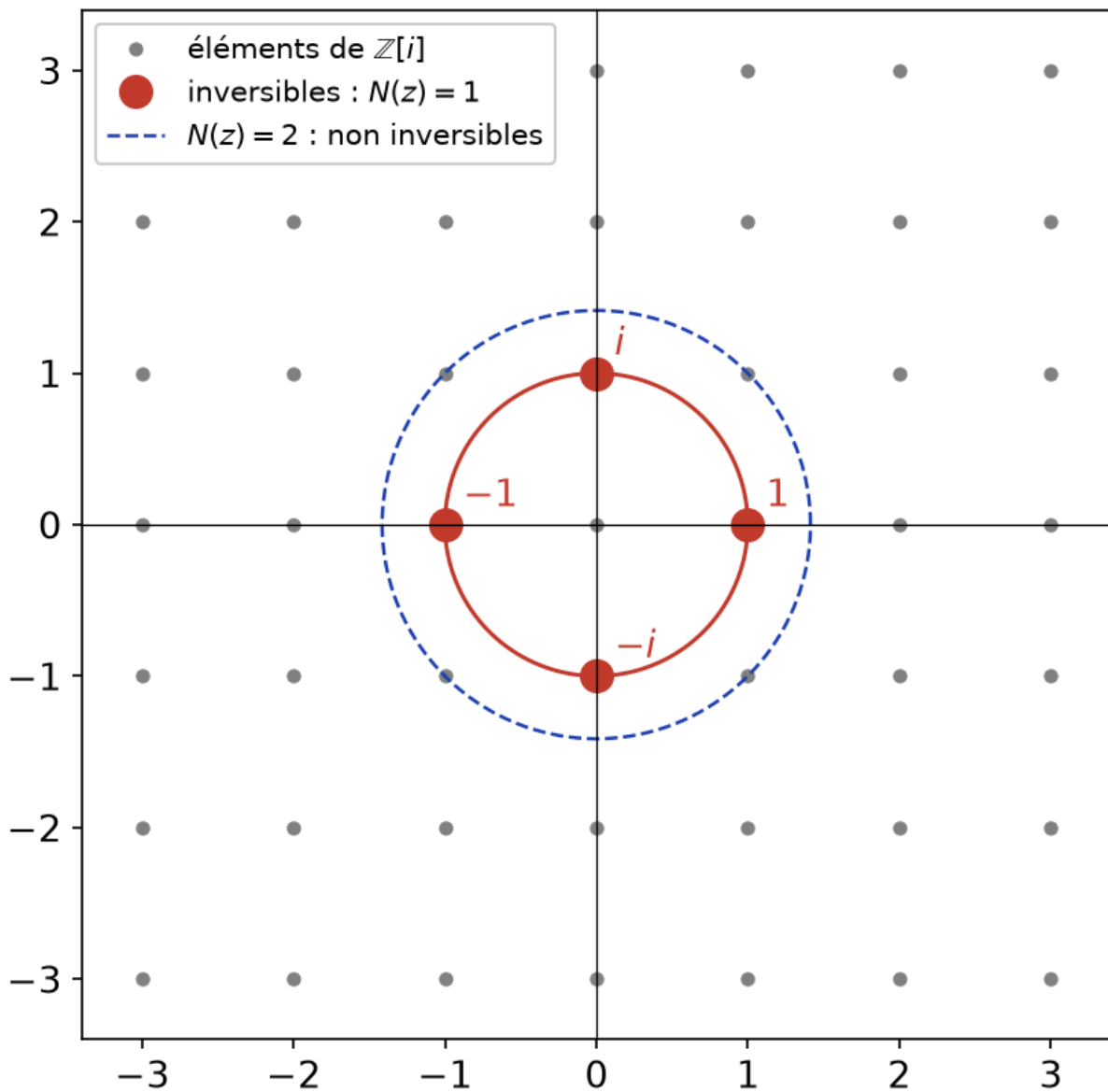
Point de méthode : pour séparer deux groupes, trouvez une équation ($x^2 = e$, $x = y^2$, $x = 2y$...) dont le nombre de solutions n'est pas le même des deux côtés.

Corrigé de l'exercice 14 : Sous-anneaux de $\mathbb{C}$

- On a $1 = 1 + 0i$. La différence de deux entiers de Gauss en est un, et
 $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ aussi. **Donc $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.**
- On a $1 = 1 / 10^0$. Ensuite, $\frac{k}{10^n} - \frac{k'}{10^m} = \frac{k 10^m - k' 10^n}{10^{n+m}}$ et $\frac{k}{10^n} \times \frac{k'}{10^m} = \frac{kk'}{10^{n+m}}$.
Ainsi, $\mathbb{D}$ est un sous-anneau de $\mathbb{C}$.
- On a $1 = 1 + 0\sqrt{2}$, la différence est stable, et
 $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. **Donc $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau.**
- On a $1 = 1 + 2i \times 0$ et $(a + 2ib) - (c + 2id) = (a - c) + 2i(b - d)$. Enfin,
 $(a + 2ib)(c + 2id) = (ac - 4bd) + 2i(ad + bc)$. **Par conséquent, B est un sous-anneau de $\mathbb{C}$.**
- D'abord, $1 \notin 2\mathbb{Z}$. Ensuite, 1 et -1 sont dans le disque, mais pas $1 - (-1) = 2$. Enfin, 1 et $-i$ sont dans $\mathbb{R} \cup i\mathbb{R}$, mais $1 - (-i) = 1 + i$ n'est ni réel ni imaginaire pur. **Aucune de ces trois parties n'est un sous-anneau.**

Corrigé de l'exercice 15 : Le groupe des inversibles de $\mathbb{Z}[i]$

- Pour $z = a + ib$, $N(z) = a^2 + b^2$ est un entier naturel. De plus,
 $N(zw) = |zw|^2 = |z|^2 |w|^2 = N(z) N(w)$. **La norme N est donc multiplicative et à valeurs dans $\mathbb{N}$.**
- Si $zw = 1$ avec $w \in \mathbb{Z}[i]$, alors $N(z) N(w) = N(1) = 1$. Ce sont deux entiers naturels de produit 1. **Donc $N(z) = 1$.**
- L'équation $a^2 + b^2 = 1$ en entiers impose $\{a^2, b^2\} = \{0, 1\}$. On trouve
 $z \in \{1, -1, i, -i\}$. Réciproquement, $1 \times 1 = 1$, $(-1)(-1) = 1$ et $i \times (-i) = 1$.
Ainsi, $\mathbb{Z}[i]^\times = \{1, -1, i, -i\} = \mathbb{U}_4$. La figure suivante montre ces quatre points, seuls points du réseau situés sur le cercle unité.



4. L'anneau $\mathbb{Z}[i]$ est commutatif et non nul. Si $zw = 0$ dans $\mathbb{Z}[i]$, cette égalité a lieu dans le corps $\mathbb{C}$, donc $z = 0$ ou $w = 0$. Il est donc intègre. En revanche, $N(1+i) = 2 \neq 1$, donc $1+i$ est non nul mais pas inversible. **L'anneau $\mathbb{Z}[i]$ est intègre, mais ce n'est pas un corps.**

Corrigé de l'exercice 16 : Diviseurs de zéro dans un anneau de fonctions

1. Les fonctions f et g sont non nulles, car $f(1) = 1$ et $g(-1) = 1$. Pour $x \geq 0$, $g(x) = 0$; pour $x \leq 0$, $f(x) = 0$. Donc $f(x)g(x) = 0$ pour tout x . **Ainsi, $fg = 0$ avec $f \neq 0$ et $g \neq 0$: l'anneau A n'est pas intègre.**
2. Si $hk = 1$, alors $h(x)k(x) = 1$ pour tout x , donc h ne s'annule pas. Réciproquement, si h ne s'annule jamais, la fonction $1/h$ est un inverse. **Donc $A^\times$ est l'ensemble des fonctions qui ne s'annulent pas.**
3. Si $h(x_0) = 0$, posons $k(x_0) = 1$ et $k(x) = 0$ pour $x \neq x_0$. Alors $k \neq 0$ et $hk = 0$. Réciproquement, si h ne s'annule pas, elle est inversible, et $hk = 0$ donne $k = h^{-1}(hk) = 0$. **Ainsi, h est un diviseur de zéro si et seulement si elle s'annule au moins une fois.**
4. L'égalité $e^2 = e$ signifie $e(x)^2 = e(x)$, soit $e(x) \in \{0, 1\}$ pour tout x . **Les solutions sont les fonctions indicatrices 1_B , où B est une partie de $\mathbb{R}$.**
5. La fonction constante 1 est continue, et la différence et le produit de deux fonctions continues sont continus. Donc $\mathcal{C}(\mathbb{R}, \mathbb{R})$ est un sous-anneau. Or f et g sont continues, et $fg = 0$: ce sous-anneau n'est pas intègre. Enfin, un inversible h de cet anneau ne s'annule pas. **D'après le théorème des valeurs intermédiaires, un inversible de $\mathcal{C}(\mathbb{R}, \mathbb{R})$ garde un signe constant.**

Corrigé de l'exercice 17 : Formule du binôme et matrices carrées d'ordre 2

1. La formule du produit donne $N^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. De plus, $(\lambda I)N = \lambda N = N(\lambda I)$. **Ainsi, $N^2 = 0$ et N commute avec λI .**
2. On écrit $A = 3I + N$, où $3I$ et N commutent. La formule du binôme s'applique, et $N^k = 0$ pour $k \geq 2$. Pour $n \geq 1$, il reste

$$A^n = \binom{n}{0} (3I)^n + \binom{n}{1} (3I)^{n-1} N = 3^n I + n 3^{n-1} N.$$

Donc $A^n = \begin{pmatrix} 3^n & n 3^{n-1} \\ 0 & 3^n \end{pmatrix}$ pour $n \geq 1$, et $A^0 = I$. Par exemple, $A^2 = \begin{pmatrix} 9 & 6 \\ 0 & 9 \end{pmatrix}$, ce que confirme un calcul direct.

3. On a $N + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, donc $(N + B)^2 = I$. Par ailleurs,
 $N^2 = B^2 = 0$ et $NB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Donc
 $N^2 + 2NB + B^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq I$. En fait,
 $BN = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq NB$. **Le développement correct est**
 $(N + B)^2 = N^2 + NB + BN + B^2 = I$: **la formule du binôme échoue car N et B ne commutent pas.**

Corrigé de l'exercice 18 : Éléments nilpotents d'un anneau

- Comme 1 et a commutent, la factorisation de $1 - a^p$ donne
 $(1 - a)(1 + a + \dots + a^{p-1}) = 1 - a^p = 1$. Le produit dans l'autre ordre vaut aussi 1.
Donc $1 - a$ est inversible, d'inverse $\sum_{k=0}^{p-1} a^k$.
- Posons $n = p + q - 1$. Comme $ab = ba$, la formule du binôme donne
 $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$. Si $k \geq p$, alors $a^k = 0$. Si $k \leq p - 1$, alors
 $n - k \geq q$, donc $b^{n-k} = 0$. Tous les termes sont nuls. **Ainsi, $(a + b)^{p+q-1} = 0$: $a + b$ est nilpotent.**
- Comme a et b commutent, une récurrence immédiate donne $(ab)^k = a^k b^k$. **En particulier, $(ab)^p = a^p b^p = 0$, donc ab est nilpotent.**
- Supposons A intègre et $a^p = 0$, avec p minimal. Si $p \geq 2$, alors $a \times a^{p-1} = 0$, donc $a = 0$ ou $a^{p-1} = 0$. Dans les deux cas, cela contredit la minimalité de p , car $a = 0$ donne $a^1 = 0$. Donc $p = 1$. **Dans un anneau intègre, 0 est le seul nilpotent.**
- D'après l'exercice 17, $N^2 = B^2 = 0$, mais $(N + B)^2 = I$. Par récurrence,
 $(N + B)^{2k} = I$ et $(N + B)^{2k+1} = N + B$, qui sont non nulles. **Donc $N + B$ n'est pas nilpotente : l'hypothèse de commutation est indispensable.**

Corrigé de l'exercice 19 : Morphismes d'anneaux

1. L'application χ est un morphisme de groupes additifs, car $(m+n) \cdot 1_A = m \cdot 1_A + n \cdot 1_A$. Par distributivité et règle des signes, $(m \cdot 1_A)(n \cdot 1_A) = (mn) \cdot 1_A$. Enfin, $\chi(1) = 1_A$. C'est donc un morphisme d'anneaux. Soit maintenant f un morphisme d'anneaux de $\mathbb{Z}$ dans A . C'est un morphisme de groupes additifs avec $f(1) = 1_A$, donc $f(n) = f(n \cdot 1) = n \cdot f(1) = n \cdot 1_A$. **Ainsi, χ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A .**

2. Supposons $a + b\sqrt{2} = a' + b'\sqrt{2}$. Si $b \neq b'$, alors $\sqrt{2} = \frac{a-a'}{b'-b}$ serait rationnel. Donc $b = b'$, puis $a = a'$. L'application σ est donc bien définie. Ensuite, $\sigma(1) = 1$, et σ est clairement additive. Pour le produit, avec $z = a + b\sqrt{2}$ et $w = c + d\sqrt{2}$:

$$\sigma(zw) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = \sigma(z)\sigma(w).$$

Enfin, $\sigma \circ \sigma = \text{id}$, donc σ est bijective. **Par conséquent, σ est un automorphisme de l'anneau $\mathbb{Z}[\sqrt{2}]$.**

3. Dans B , on a $1_B \neq 0_B$, sinon tout $b = b \times 1_B$ serait nul. Soit $x \in \ker f$ avec $x \neq 0$. Alors x est inversible dans le corps K , et $1_B = f(1_K) = f(x)f(x^{-1}) = 0_B$, ce qui est absurde. Donc $\ker f = \{0\}$. **Un morphisme d'anneaux défini sur un corps est toujours injectif.**
4. Soit f un morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Q}$. Comme à la question 1, $f(n) = n$ pour tout $n \in \mathbb{Z}$. Pour $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, on a $q f(p/q) = f(q) f(p/q) = f(p) = p$. Donc $f(p/q) = p/q$. **Le seul morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Q}$ est l'identité.**

Corrigé de l'exercice 20 : Le corps $\mathbb{Q}[\sqrt{2}]$

1. Si $a + b\sqrt{2} = a' + b'\sqrt{2}$ avec $b \neq b'$, alors $\sqrt{2} = (a - a') / (b' - b) \in \mathbb{Q}$, ce qui est faux. **Donc $b = b'$ et $a = a'$: l'écriture est unique.**
2. On a $1 \in K$, et la différence de deux éléments de K est dans K . De plus, $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, à coefficients rationnels. **Ainsi, K est un sous-anneau de $\mathbb{R}$.**

3. Soit $z = a + b\sqrt{2} \neq 0$. Si l'on avait $a - b\sqrt{2} = 0$, alors soit $b \neq 0$ et $\sqrt{2} = a/b$ serait rationnel, soit $b = 0$, puis $a = 0$ et $z = 0$. Donc $a - b\sqrt{2} \neq 0$, et $a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) \neq 0$. On en déduit

$$\frac{1}{z} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in K.$$

Comme K est commutatif et non nul, c'est un corps, sous-corps de $\mathbb{R}$.

4. Pour $3 + 2\sqrt{2}$, on a $a^2 - 2b^2 = 9 - 8 = 1$. Pour $1 + \sqrt{2}$, on trouve $1 - 2 = -1$. Pour $2 + \sqrt{2}$, on trouve $4 - 2 = 2$. **Les inverses sont $3 - 2\sqrt{2}$, $\sqrt{2} - 1$ et $1 - \frac{\sqrt{2}}{2}$.**

Vérifions le dernier : $(2 + \sqrt{2})(1 - \frac{\sqrt{2}}{2}) = 2 - \sqrt{2} + \sqrt{2} - 1 = 1$.

5. Supposons $\sqrt{3} = a + b\sqrt{2}$ avec a, b rationnels. En élevant au carré, $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. Par unicité de l'écriture, $2ab = 0$. Si $b = 0$, alors $a^2 = 3$, et $\sqrt{3}$ serait rationnel. Si $a = 0$, alors $2b^2 = 3$, donc $(2b)^2 = 6$, et $\sqrt{6}$ serait rationnel. **Les deux cas sont impossibles, donc $\sqrt{3} \notin K$.**

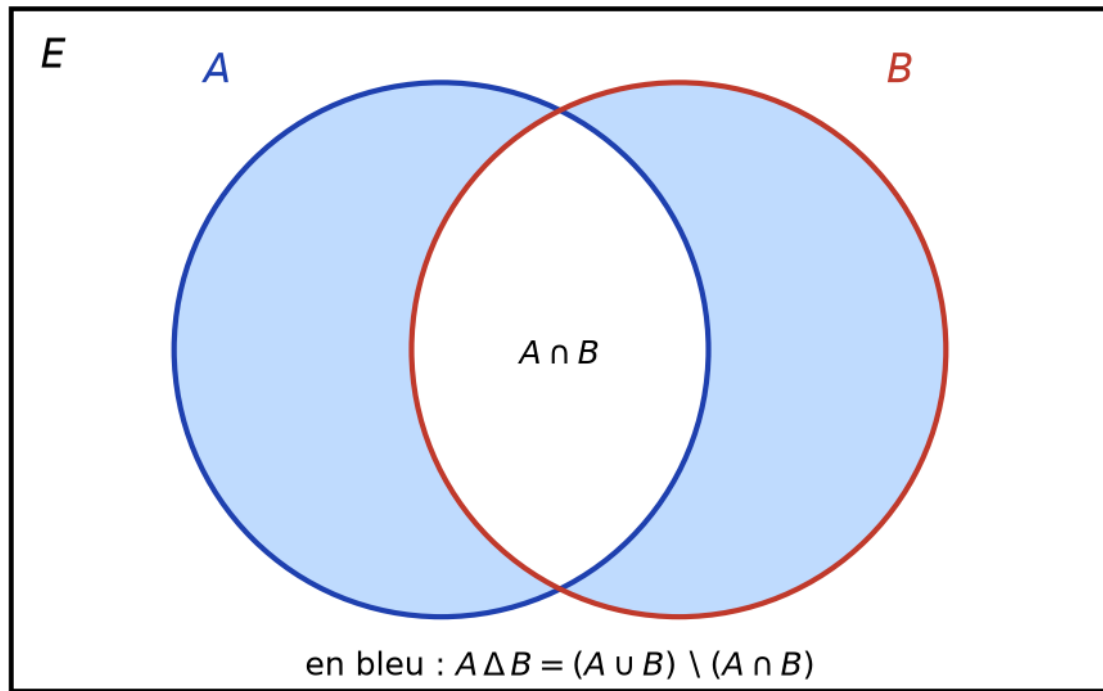
Corrigé de l'exercice 21 : Un anneau intègre fini est un corps

- Si $ax = ay$, alors $a(x - y) = 0$. Comme $a \neq 0$ et que A est intègre, $x - y = 0$. **Donc m_a est injective.**
- Une application injective d'un ensemble fini dans lui-même est bijective. Il existe donc $b \in A$ tel que $m_a(b) = ab = 1$, et $ba = 1$ par commutativité. Tout élément non nul est donc inversible. **Ainsi, un anneau intègre fini est un corps.**
- Si m_a est injective, elle est bijective comme à la question 2, et a est inversible. Sinon, il existe $x \neq y$ tels que $ax = ay$. En posant $b = x - y \neq 0$, on obtient $ab = 0$. **Tout élément d'un anneau commutatif fini est donc inversible ou diviseur de zéro.**
- Non : l'anneau $\mathbb{Z}$ est intègre et infini, mais 2 n'y est pas inversible. **L'hypothèse de finitude est essentielle.**

Point de méthode : sur un ensemble fini, injectif équivaut à bijectif ; c'est l'argument clé chaque fois que l'on veut produire un inverse sans le calculer.

Corrigé de l'exercice 22 : Anneau de Boole et différence symétrique

1. D'une part, $(x + x)^2 = x + x$ par hypothèse. D'autre part, en développant, $(x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$. On simplifie par $x + x$ dans le groupe $(A, +)$. **On obtient $x + x = 0$, c'est-à-dire $-x = x$.**
2. On développe $(x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Or $(x + y)^2 = x + y$, donc $xy + yx = 0$. D'après la question 1, $xy = -(yx) = yx$. **L'anneau A est donc commutatif.**
3. On a $x(1 - x) = x - x^2 = 0$. Si A est intègre, alors $x = 0$ ou $x = 1$ pour tout x . Comme A n'est pas réduit à $\{0\}$, on a $1 \neq 0$, donc $A = \{0, 1\}$. Réciproquement, dans $\{0, 1\}$, le seul produit de deux éléments non nuls est $1 \times 1 = 1 \neq 0$. **Ainsi, A est intègre si et seulement si $A = \{0, 1\}$.**
4. La loi Δ est associative (admis) et commutative, car sa définition est symétrique. Ensuite, $X \Delta \emptyset = X$, donc $\emptyset$ est neutre. De plus, $X \Delta X = X \setminus X = \emptyset$: chaque partie est sa propre opposée. Donc $(\mathcal{P}(E), \Delta)$ est un groupe abélien. Par ailleurs, $\cap$ est associative, commutative, de neutre E , et distributive sur Δ (admis). Enfin, $X \cap X = X$, et $E \neq \emptyset$. **Par conséquent, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.** La figure ci-dessous représente $A \Delta B$: c'est la réunion privée de l'intersection.



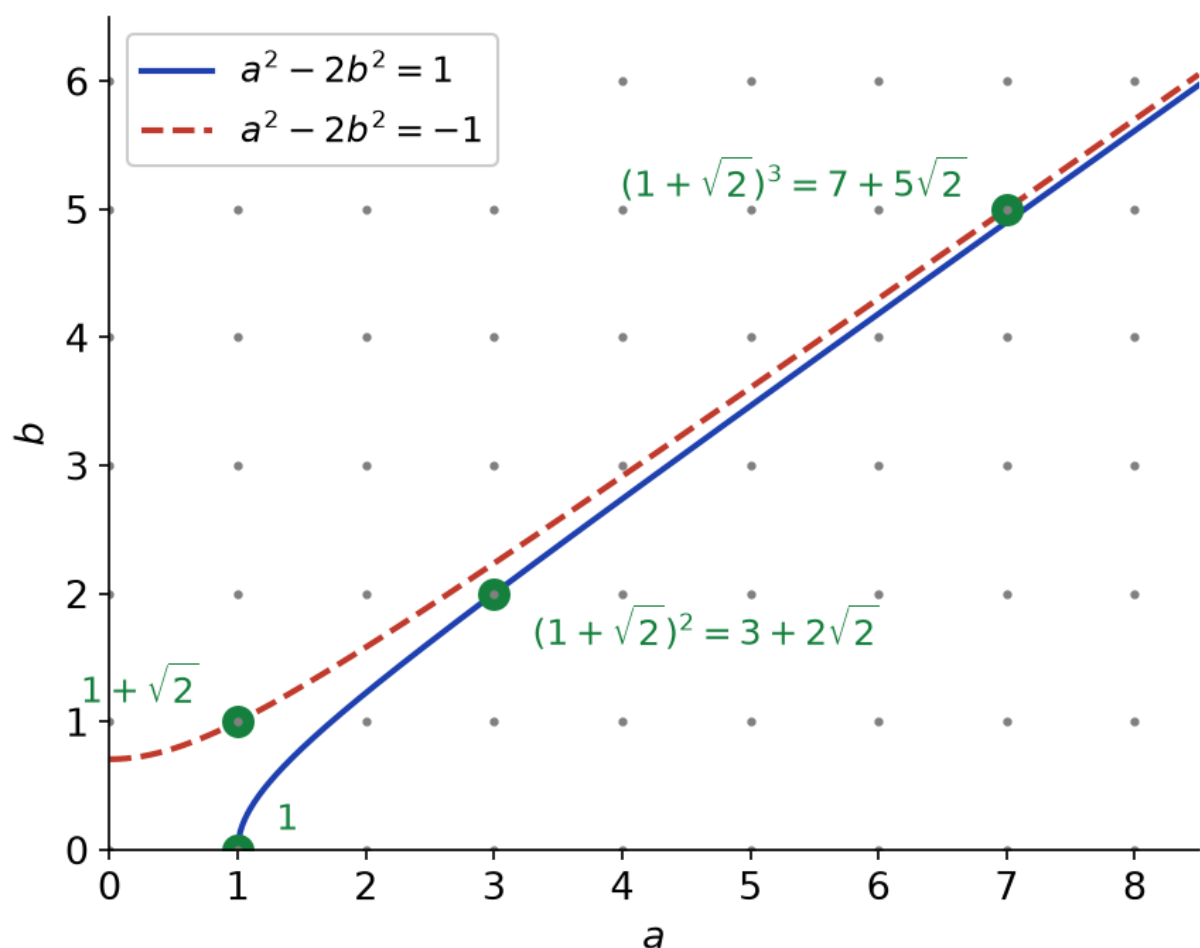
5. Si $X \cap Y = E$, alors $E \subset X$, donc $X = E$: le seul inversible est E . D'après la question 3, l'anneau est intègre si et seulement si $\mathcal{P}(E) = \{\emptyset, E\}$. Cela se produit exactement quand E est un singleton. D'ailleurs, si $a \neq b$ dans E , on a $\{a\} \cap \{b\} = \emptyset$. **Ainsi, les inversibles se réduisent à $\{E\}$, et l'anneau est intègre si et seulement si E a un seul élément.**

Corrigé de l'exercice 23 : Problème : unités de $\mathbb{Z}[\sqrt{2}]$ et équation de Pell-Fermat

- Pour $z = a + b\sqrt{2}$, on a $N(z) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$. Comme σ est un morphisme d'anneaux et que A est commutatif,
 $N(zw) = zw \sigma(z)\sigma(w) = N(z) N(w)$. **La norme est donc multiplicative.**
- Si $zw = 1$, alors $N(z) N(w) = N(1) = 1$. Ce sont deux entiers de produit 1, donc $N(z) = \pm 1$. Réciproquement, si $N(z) = \pm 1$, alors $z \times N(z)\sigma(z) = N(z)^2 = 1$, et $N(z)\sigma(z) \in A$. **Ainsi, $z \in A^\times$ si et seulement si $N(z) = \pm 1$.**

3. On a $N(\varepsilon) = 1 - 2 = -1$, donc ε est inversible. Ensuite, $\varepsilon^2 = 1 + 2\sqrt{2} + 2 = 3 + 2\sqrt{2}$ et $\varepsilon^3 = (3 + 2\sqrt{2})(1 + \sqrt{2}) = 7 + 5\sqrt{2}$. Pour $m \in \mathbb{N}$, écrivons $\varepsilon^{2m} = a_m + b_m\sqrt{2}$. Alors $a_m^2 - 2b_m^2 = N(\varepsilon)^{2m} = 1$. Comme $\varepsilon > 1$, les réels ε^{2m} sont deux à deux distincts. Par unicité de l'écriture, les couples (a_m, b_m) le sont aussi. **L'équation $a^2 - 2b^2 = 1$ a donc une infinité de solutions entières.**
4. On a $u\sigma(u) = N(u) = \pm 1$, donc $|\sigma(u)| = 1/u < 1$. Ensuite, $a = \frac{u + \sigma(u)}{2} > \frac{1-1}{2} = 0$ et $b\sqrt{2} = \frac{u - \sigma(u)}{2} > \frac{1-1}{2} = 0$. Les entiers a et b sont strictement positifs, donc $a \geq 1$ et $b \geq 1$. **Par conséquent,**
 $u = a + b\sqrt{2} \geq 1 + \sqrt{2} = \varepsilon$.
5. D'abord, les ε^n sont des inversibles strictement positifs, car $A^\times$ est un groupe. Réciproquement, soit $u \in A^\times$ avec $u > 0$. Comme $\varepsilon > 1$, il existe $n \in \mathbb{Z}$ tel que $\varepsilon^n \leq u < \varepsilon^{n+1}$: il suffit de prendre $n = \lfloor \ln u / \ln \varepsilon \rfloor$. Posons $v = u\varepsilon^{-n}$. C'est un inversible de A , et $1 \leq v < \varepsilon$. Si l'on avait $v > 1$, la question 4 donnerait $v \geq \varepsilon$, ce qui est faux. Donc $v = 1$. **Les inversibles strictement positifs de A sont exactement les ε^n , $n \in \mathbb{Z}$.**
6. Soit $(a, b) \in \mathbb{N}^2$ tel que $a^2 - 2b^2 = 1$. Alors $u = a + b\sqrt{2} \geq 1$ et $N(u) = 1$. D'après les questions 2 et 5, $u = \varepsilon^n$ avec $n \geq 0$. De plus, $1 = N(u) = (-1)^n$, donc n est pair. Réciproquement, $\varepsilon^{2m} = (3 + 2\sqrt{2})^m$ se développe à coefficients entiers positifs et a pour norme 1. **Les solutions dans $\mathbb{N}^2$ sont les couples (a, b) tels que $a + b\sqrt{2} = (3 + 2\sqrt{2})^m$, $m \in \mathbb{N}$: $(1, 0)$, $(3, 2)$, $(17, 12)$, $(99, 70)$, etc.** On vérifie par exemple que $17^2 - 2 \times 12^2 = 289 - 288 = 1$.

La figure suivante place les premières puissances de ε : elles alternent entre les deux hyperboles, selon la parité de l'exposant, car $N(\varepsilon^n) = (-1)^n$.



7. Notons $\psi(n, s) = s \varepsilon^n$. Cet élément est inversible, car s et ε le sont. Ensuite, $\psi((n, s)(n', s')) = ss' \varepsilon^{n+n'} = \psi(n, s) \psi(n', s')$: c'est un morphisme. Si $s \varepsilon^n = 1$, alors $s = 1$ car $\varepsilon^n > 0$, puis $\varepsilon^n = 1$ donne $n = 0$. Le noyau est trivial, donc ψ est injectif. Enfin, soit $u \in A^\times$. Si $u > 0$, la question 5 donne $u = \varepsilon^n = \psi(n, 1)$. Si $u < 0$, alors $-u$ est un inversible positif, et $u = -\varepsilon^n = \psi(n, -1)$. **Donc ψ est un isomorphisme de $\mathbb{Z} \times \mathbb{U}_2$ sur $A^\times = \left\{ \pm [\text{varsilon?}]^n, n \in \mu\mathbb{Z} \right\}$.**

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en maths sup

- Le cours : [groupes, anneaux et corps, cours de maths sup](#)
- Les énoncés : [exercices de maths sup sur groupes, anneaux et corps](#)
- À maîtriser avant : [Logique, ensembles, applications et relations](#), [Nombres complexes et exponentielle complexe](#)
- Chapitre précédent : [Arithmétique dans l'ensemble des entiers relatifs](#)
- Chapitre suivant : [Calcul matriciel et systèmes linéaires](#)
- Tester vos connaissances : [QCM de maths sup par chapitre](#)
- Le sommaire : [tous les chapitres de maths sup](#) et les [chapitres de maths spé](#)