Lois de composition interne et groupes abstraits

1 ☆☆☆

Étudier la loi $(a, b) \mapsto a^2 + b^2$ dans $\mathbb{R}$.

2 ☆☆☆

Soit $\lambda \in \mathbb{R}$. Étudier la loi $(a, b) \mapsto \lambda(a + b)$ sur $\mathbb{Z}$.

3 ☆☆☆

Étant donnés deux vecteurs $u_1 = (x_1, y_1, z_1)$ et $u_2 = (x_2, y_2, z_2)$ de $\mathbb{R}^3$, on définit le produit vectoriel :

$$u \wedge v = (y_1 z_2 - y_2 z_1, z_1 x_2 - z_2 x_1, x_1 y_2 - x_2 y_1).$$

Étudier la loi $\wedge$ sur $\mathbb{R}^3$.

4 ★★☆☆ ♡

Soit $(E, *)$ un monoïde. On dit qu'un élément $x \in E$ est :

- régulier à gauche lorsque : $\forall y, z \in E, (x * y = x * z \Rightarrow y = z)$.
- régulier à droite lorsque : $\forall y, z \in E, (y * x = z * x \Rightarrow y = z)$.

1. Montrer qu'un élément inversible de $(E, *)$ est régulier à gauche et à droite.
2. Soit F un ensemble non vide. On considère l'ensemble $E = F^F$ muni de la loi $\circ$ et on fixe $f \in E$.
 - (a) Montrer que f est régulier à gauche **ssi** f est injective.
 - (b) Montrer que f est régulier à droite **ssi** f est surjective.

5 ☆☆☆

Pour tout $(x, y) \in \mathbb{R}^2$, on pose $x * y = \sqrt[3]{x^3 + y^3}$.

1. Montrer que $(\mathbb{R}, *)$ est un groupe.
2. Qu'en est-il si $x * y = \sqrt[n]{x^n + y^n}$ avec $n \in \mathbb{N}^*$?

6 ★☆☆ ♡

On définit la loi $\star$ sur $\mathbb{R}$ en posant : $x \star y = x + y - xy$.

1. Étudier la loi $\star$. $(\mathbb{R}, \star)$ est-il un groupe ?
2. Montrer que $(\mathbb{R} \setminus \{1\}, \star)$ est un groupe abélien.
3. Pour tout $x \in \mathbb{R}$ et tout $n \in \mathbb{N}$, calculer $x^{(n)} = x \star \dots \star x$.

7 ★☆☆ ⊕

Montrer que $] -1, 1[$ muni de la loi définie par $x * y = \frac{x + y}{1 + xy}$ est un groupe abélien.

Groupes et sous-groupes

8 ☆☆☆ ♡

Montrer que l'ensemble des fonctions impaires de $\mathbb{R}$ dans $\mathbb{R}$ est un groupe pour l'addition usuelle.

9 ☆☆☆

Soit $n \in \mathbb{N}^*$. Montrer que l'ensemble des permutations de $\llbracket 1, n \rrbracket$ admettant 1 comme point fixe est un groupe.

10 ☆☆☆

Montrer que $\mathcal{M}_n(\mathbb{Z})$ est un groupe pour la loi $+$.

11 ☆☆☆ ⊕

Les ensembles suivants sont-ils des groupes pour la loi $\times$ usuelle (les deux derniers s'appuient sur le chapitre sur le déterminant) : $\text{GL}_n(\mathbb{R})$, $\text{GL}_n(\mathbb{Q})$, $\text{GL}_n(\mathbb{Z})$, $\text{GL}_n(\{0, 1\})$, $\{M \in \mathcal{M}_n(\mathbb{R}), \det(M) = 1\}$.

12 ★★★ ↗

Montrer que l'ensemble $\{x + y\sqrt{3}, x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\}$ est un sous-groupe de $(\mathbb{R}^{++}, \times)$.

13 ★☆☆ ↗ ⊕

On considère les applications de $\mathbb{R} \setminus \{0, 1\}$ dans lui-même définies par : $f_1(x) = x$, $f_2(x) = \frac{1}{1-x}$, $f_3(x) = \frac{x-1}{x}$, $f_4(x) = \frac{1}{x}$, $f_5(x) = 1-x$, $f_6(x) = \frac{x}{x-1}$. Et on pose $G = \{f_i, i \in \llbracket 1, 6 \rrbracket\}$.

1. Montrer que $(G, \circ)$ est un groupe. Est-il abélien ?
2. Quels sont les sous-groupes de G ?

14 ☆☆☆ ♥

Soit G un groupe. On appelle *centre* de G l'ensemble : $\mathcal{Z}(G) = \{x \in G, \forall y \in G, xy = yx\}$.

1. Montrer que $\mathcal{Z}(G)$ est un sous-groupe de G .
2. A quelle condition sur G a-t-on $\mathcal{Z}(G) = G$?
3. Identifier $\mathcal{Z}(S_3)$ où S_3 est groupe symétrique usuel.

15 ★☆☆ ♥

1. Soient n et m des entiers premiers entre eux supérieurs ou égaux à 2. Montrer que $\mathbb{U}_n \cup \mathbb{U}_m$ n'est pas un sous-groupe de $(\mathbb{C}^*, \times)$.

2. Montrer que l'ensemble $U = \bigcup_{n=1}^{+\infty} \mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

16 ★☆☆ ♥

Soient H, K deux sous-groupes d'un groupe G .

Montrer que $H \cup K$ est un sous-groupe de G ssi $H \subset K$ ou $K \subset H$.

17 ★☆☆ ⊕

Soient H, K deux sous-groupes d'un groupe G . On pose $HK = \{hk, h \in H, k \in K\}$.

Montrer que HK est un sous-groupe de G ssi $HK = KH$.

18 ☆☆☆ ⊕

Soit H un sous-groupe d'un groupe $(G, *)$. Pour tout $g \in G$, on appelle CLASSE À GAUCHE de g modulo H l'ensemble $g * H = \{g * h, h \in H\}$.

Montrer que les classes à gauche modulo H forment une partition de G .

19 ★☆☆ ♥

Soit G un groupe tel que $\forall x \in G, x^2 = e$.

1. Identifier l'inverse d'un élément quelconque de G .
2. Montrer que G est abélien.
3. ★★★ ♥ On suppose que G est fini et contient au moins trois éléments distincts.
 - (a) On suppose qu'il existe un sous-groupe H de G , strict ($\{e\} \neq H \neq G$) et fini de cardinal p . Soit $g \in G \setminus H$. On note usuellement $gH = \{gh, h \in H\}$. Montrer que $H \cup gH$ est un sous-groupe de G de cardinal $2p$.
 - (b) Justifier l'existence d'un sous-groupe de G de cardinal 2 et en conclure que le cardinal de G est une puissance de 2.

Morphismes de groupes

20 ☆☆☆

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

21 ☆☆☆ ⊕ ♥

1. Soit $G = \{-1, 1\}^2$. Pour tous $(x, y), (x', y') \in G$, on pose $(x, y) \times (x', y') = (xx', yy')$. Justifier que $(G, \times)$ est un groupe et proposer un tableau à double entrée décrivant la loi $\times$.
2. Montrer que $\mathbb{U}_4$ et G ne sont pas isomorphes.

22 ★☆☆ ♥

Soit G un groupe. Pour $a \in G$, on pose : $\forall b \in G, \tau_a(b) = aba^{-1}$.

1. Montrer que τ_a est un automorphisme de G .
2. Montrer que $\tau : a \mapsto \tau_a$ est un morphisme de G dans $(\mathcal{S}(G), \circ)$, l'ensemble des permutations de G .
3. Montrer que $\text{Ker}(\tau) = \mathcal{Z}(G)$ où $\mathcal{Z}(G) = \{a \in G, \forall b \in G, ab = ba\}$.

Anneaux et sous-anneaux

23 ☆☆☆

L'ensemble $\mathbb{D}$ des nombres décimaux est-il un anneau pour les lois $+$ et $\times$ usuelles ? Un corps ?

24 ★☆☆ ♥

Soit $r \in \mathbb{R}$. Montrer que $\mathbb{Z}[r] = \{a + br, a, b \in \mathbb{Z}\}$ est un anneau pour les lois $+$ et $\times$ usuelles **ssi** il existe un polynôme unitaire du second degré et à coefficients entiers ayant r pour racine.

25 ☆☆☆

Montrer que $\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3}, a, b, c \in \mathbb{Z}\}$ est un groupe pour la loi $+$ usuelle sur $\mathbb{R}$. Est-ce un anneau pour les lois $+$ et $\times$ usuelles ?

26 ☆☆☆

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux non réduits à leur élément nul. Pour tout $(a_1, b_1), (a_2, b_2) \in A \times B$, on pose :

- $\triangleright (a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2)$;
- $\triangleright (a_1, b_1) \times (a_2, b_2) = (a_1 \times_A a_2, b_1 \times_B b_2)$.

Montrer que $(A \times B, +, \times)$ est un anneau non intègre.

27 ☆☆☆ ⊕ ♥

Soit $(A, +, \times)$ un anneau tel que $\forall a \in A, a^2 = a$.

Montrer que, pour tout $a \in A, 2a = 0$ et en déduire que A est nécessairement commutatif.

Morphismes d'anneaux

28 ☆☆☆ ♥

Notons $S = \mathbb{C}^{\mathbb{N}}$.

1. Justifier que S est un anneau pour les lois usuelles $+$ et $\times$.
2. Montrer que l'ensemble B des suites complexes bornées est un sous-anneau de S .
3. L'ensemble D des suites complexes divergentes est-il un sous-anneau de A ?
4. Montrer que l'ensemble C des suites complexes convergentes est un sous-anneau de S .
5. Montrer que l'application $\lim : C \rightarrow \mathbb{C}$ est un morphisme d'anneaux non injectif.

29 ★☆☆ ⊕

Soit $(A, +, \times)$ un anneau. On pose, pour $x, y \in A, x \perp y = x + y + 1$ et $x * y = x \times y + x + y$.

Montrer que $(A, \perp, *)$ est un anneau isomorphe à $(A, +, \times)$.

30 ★★☆☆ ♥ Indicatrice d'Euler

Pour $n \in \mathbb{N}^*$, $\bar{x}^{[n]}$ désigne la classe d'un entier x pour la relation de congruence modulo n , on note $(\mathbb{F}_n, +, \times)$ l'anneau usuel associée à cette relation de congruence et on pose $\varphi(n) = |\mathbb{F}_n^\times|$.

1. Calculer, pour $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha)$.
2. Soient $n, m \in \mathbb{N}^*$ premiers entre eux. On note $f : \mathbb{F}_{nm} \rightarrow \mathbb{F}_n \times \mathbb{F}_m$ l'application définie par $f(\bar{x}^{[nm]}) = (\bar{x}^{[n]}, \bar{x}^{[m]})$. Montrer que f est bien définie et réalise un isomorphisme d'anneaux. En déduire que $\varphi(nm) = \varphi(n)\varphi(m)$.
3. Exprimer $\varphi(n)$ selon la décomposition primaire de n .

Groupe des inversibles

31 ☆☆☆ ♥

Soit $n \in \mathbb{N}^*$. On rappelle que la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. Pour tout $k \in \mathbb{Z}$, on note $\bar{k}$ la classe d'équivalence de k et on note $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \mathbb{Z}\}$. Enfin, si $k, h \in \mathbb{Z}$, on pose $\bar{k} + \bar{h} = \overline{k+h}$ et $\bar{k} \times \bar{h} = \overline{k \times h}$.

1. Justifier que $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \llbracket 0, n-1 \rrbracket\}$.
2. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
3. Étudier l'intégrité de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ dans les cas $n = 2$, $n = 3$ et $n = 4$.
4. Montrer qu'un élément k de $\mathbb{Z}/n\mathbb{Z}$ est inversible **ssi** $k \wedge n = 1$.
5. *Application.* Résoudre l'équation d'inconnue $n \in \mathbb{Z} : 26n \equiv 9 \pmod{45}$.

32 ★☆☆

On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, (a, b) \in \mathbb{K}^2\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
2. Pour tout $(a, b) \in \mathbb{Z}^2$, on pose $N(a + b\sqrt{2}) = a^2 - 2b^2$.
 - (a) Montrer que $\forall x_1, x_2 \in \mathbb{Z}[\sqrt{2}], N(x_1 x_2) = N(x_1)N(x_2)$.
 - (b) En déduire que $a + b\sqrt{2}$ est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$ **ssi** a et b sont des entiers satisfaisant à une équation de Pell-Fermat : $a^2 - 2b^2 = \pm 1$.
 - (c) Justifier que $\sqrt{2}$ n'est pas inversible, que $3 + 2\sqrt{2}$ est inversible et expliciter son inverse.

33 ★★☆☆ ⊕ ♥

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

1. Montrer que, si a est un élément nilpotent de A , alors $1 - a$ est inversible.
2. Soient $a, b \in A$. On suppose $1 - ab$ inversible.
 - (a) On suppose également ab nilpotent. Montrer que $1 - ba$ est inversible et expliciter son inverse sans symbole somme.
 - (b) Montrer que ce dernier résultat tient encore si l'on ne suppose plus ab nilpotent.

Corps

34 ☆☆☆ ♥

Montrer que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ est un corps pour les lois usuelles.

35 ★☆☆

Montrer que $\mathbb{Q}$ n'a pas de sous-corps strict (pour les lois usuelles).

36 ★☆☆ ⊕ ♥

Montrer qu'un anneau intègre fini et commutatif est un corps.

Indications

6 - indication 3. Conjecturer.

7 - indication Loi de composition interne : fixer un paramètre et faire une étude de fonction avec l'autre paramètre comme variable.

11 - indication Formule de la comatrice pour l'inversion pour les deux derniers.

12 - indication Observer que, en notant $a = x + \sqrt{3}y$ avec $x \in \mathbb{N}$ et $y \in \mathbb{Z}$, si $a \in G$, alors $|y\sqrt{3}| \leq x$.

13 - indication 1. Groupe « très fini » : dresser le tableau de la loi. 2. Inutile de tester les cardinaux 4 et 5 : théorème de Lagrange, MP.

15 - indication 1. Théorème de Bézout. 2. Stabilité par $\times$: élever à une « grande puissance ».

17 - indication Penser que l'inversion d'un produit renverse l'ordre des termes.

18 - indication Observer la relation binaire sur $G : \forall g_1, g_2 \in G, g_1 \sim g_2 \iff g_1 * g_2^{-1} \in H$.

19 - indication 3.a. Stabilité par $*$: distinguer les cas $x, y \in H, x \in H$ et $y \in gH$... Puis justifier que H et gH ont même cardinal.
3.b. Raisonner par l'absurde et appliquer 3.a.

21 - indication 2. Observer le carré des éléments de G .

27 - indication Développer le carré d'une somme.

29 - indication Observer $\varphi : x \mapsto x - 1$.

33 - indication Observer $1 + a + a^2 + \dots$

36 - indication Si a est non nul, observer la fonction $\varphi : x \mapsto ax$.

Solutions

1 - solution Ici, non associative, commutative, pas d'élément neutre.

2 - solution Ici **ssi** $\lambda \in \mathbb{Z}$. Supposons $\lambda \in \mathbb{Z}$ pour la suite.
Celle ici est clairement commutative pour toute valeur de $\lambda \in \mathbb{Z}$.

- > Si $\lambda = 1$, $*$ est l'addition usuelle : $(\mathbb{Z}, +)$ est un groupe.
- > Sinon, pas d'élément neutre, pas d'associativité.

3 - solution Ici, non associative, non commutative (anticommutative, en fait), pas de neutre.

4 - solution 1. Il suffit d'appliquer l'inverse à gauche ou à droite...

2. (a) $\Rightarrow$ Supposons f régulier à gauche. Soit $x_1, x_2 \in F$. Supposons $f(x_1) = f(x_2)$. Observons les fonctions constantes $g : x \mapsto x_1$ et $h : x \mapsto x_2$. On a $f \circ g = f \circ h$, donc $g = h$, donc $x_1 = x_2$.
 $\Leftarrow$ Supposons f injective. Soient $g, h \in E$. Supposons $f \circ g = f \circ h$. Soit $x \in F$. Alors $f(g(x)) = f(h(x))$. Par injectivité de f , $g(x) = h(x)$. Ceci étant vrai pour tout $x \in F$, on a donc $g = h$. Donc f est régulière à gauche.
- (b) $\Rightarrow$ Supposons f régulier à droite. Soit $y \in F$. Supposons par l'absurde que y n'admette aucun antécédent. Fixons x_1 et x_2 deux éléments de F distincts et définissons g et h en posant $g(x) = h(x) = x$ si $x \neq y$ et $g(y) = x_1$ et $h(y) = x_2$. On a $g \circ f = h \circ f$, donc nécessairement $g = h$ et $x_1 = x_2$, ce qui est absurde. Donc f est surjective.
 $\Leftarrow$ Supposons f surjective. Soient $g, h \in E$. Supposons $g \circ f = h \circ f$. Soit $x \in F$. Par surjectivité de f , il existe $t \in F$ tel que $x = f(t)$. Alors $g(x) = g(f(t)) = h(f(t)) = h(x)$. Donc $g = h$. Donc f est régulière à droite.

5 - solution 1. On vérifie que :

- > la loi est interne puisque la racine cubique est définie sur $\mathbb{R}$.
- > Associativité. Dès que $t \in \mathbb{R}$, $\sqrt[3]{t^3} = t$. Donc pour $x, y, z \in \mathbb{R}$, $x * (y * z) = \sqrt[3]{x^3 + y^3 + z^3} = (x * y) * z$.
- > Neutre : 0.
- > Inversible : tout élément x est inversible d'inverse $-x$.
- > Commutativité directement issue de la commutativité de $+$ dans $\mathbb{R}$.

2. Si n est impair, les mêmes arguments fonctionnent.

Mais si n est pair, seul 0 est inversible car $\forall x, y \in \mathbb{R}^*$, $x^n + y^n > 0$ donc $x * y \neq 0$. Donc $(\mathbb{R}, *)$ n'est pas un groupe.

6 - solution 1. On vérifie :

- > $*$ est une loi : immédiat puisque si $x, y \in \mathbb{R}$, $x * y \in \mathbb{R}$;
- > $*$ est associative puisque si $x, y, z \in \mathbb{R}$:

$$(x*y)*z = (x+y-xy)*z = x+y-xy+z-(x+y-xy)z = x+y+z-xy-xz-yz+xyz = x*(y+z-yz) = x*(y*z).$$

- > commutative puisque l'expression de $x * y$ est symétrique en x et y ;
- > de neutre 0.

Cependant, 1 n'a pas d'inverse puisque $1 * y = 0 \iff 1 = 0$, impossible. Donc $(\mathbb{R}, *)$ n'est pas un groupe.

2. Il faut montrer que sur $\mathbb{R} \setminus \{1\}$, les points précédents sont encore vérifiés (et que tout élément est inversible).

- > $*$ est une loi : immédiat puisque si $x, y \in \mathbb{R} \setminus \{1\}$, $x * y - 1 = x + y - xy - 1 = (x - 1)(1 - y) \neq 0$ donc $x * y \in \mathbb{R} \setminus \{1\}$;
- > $*$ est associative et commutative par héritage de ces propriétés vues sur $\mathbb{R}$;
- > de neutre 0 pour la même raison;
- > si $x \in \mathbb{R} \setminus \{1\}$, alors $x * y = 0 \iff x + y - xy = 0 \iff y(1 - x) = x$, équation qui a toujours une (unique) solution.

3. Récurrence : $x^{(n)} = \sum_{k=1}^n \binom{n}{k} (-1)^{k-1} x^k$. Calcul : $x^{(n)} = 1 - (1 - x)^n$ (plus facile à démontrer par récurrence...).

7 - solution > $*$ est interne. Soit $x \in]-1, 1[$. Posons $f(y) = \frac{x+y}{1+xy}$. f est bien définie sur $] -1, 1[$, puisque si $y \in] -1, 1[$, $-xy < |xy| = |x||y| < 1$, donc $1 + xy > 0$. f est alors dérivable sur $] -1, 1[$ en tant qu'quotient de polynôme dont le dénominateur ne s'annule pas et $\forall y \in] -1, 1[$, $f'(y) = \frac{1+xy-x(x+y)}{(1+xy)^2} = \frac{(1-x)(1+x)}{(1+xy)^2} > 0$. Ainsi, f est strictement croissante, de limite -1 en -1 et 1 en 1 . Bref, $\forall y \in] -1, 1[$, $\frac{x+y}{1+xy} \in] -1, 1[$.

➤ $\star$ est associative. Soient $x, y, z \in]-1, 1[$:

$$\diamond (x \star y) \star z = \frac{(x \star y) + z}{1 + (x \star y)z} = \frac{\frac{x+y}{1+x+y} + z}{1 + \frac{x+y}{1+x+y}z} = \frac{x+y+z(1+xy)}{1+xy+(x+y)z} = \frac{x+y+z+xyz}{1+xy+yz+xz}.$$

$$\diamond x \star (y \star z) = \frac{x + y \star z}{1 + x(y \star z)} = \frac{x + \frac{y+z}{1+y+z}}{1 + x \frac{y+z}{1+y+z}} = \frac{x(1+y+z) + y + z}{1 + yz + x(y+z)} = \frac{x+y+z+xyz}{1+xy+yz+xz}.$$

On constate que $(x \star y) \star z = x \star (y \star z)$.

➤ $\star$ possède un élément neutre : 0.

➤ $\star$ est évidemment commutative puisque $+$ et $\times$ sont commutatives sur $\mathbb{R}$.

8 - solution Il suffit de montrer que c'est un sous-groupe de $(\mathbb{R}^{\mathbb{R}}, +)$.

9 - solution C'est un sous-groupe de $\mathcal{S}_n$.

10 - solution C'est un sous-groupe de $\mathcal{M}_n(\mathbb{R})$.

11 - solution ➤ $GL_n(\mathbb{R})$: oui, cours.

➤ $GL_n(\mathbb{Q})$ est un sous-groupe de $GL_n(\mathbb{R})$.

➤ $GL_n(\mathbb{Z})$: pas stable par inversion. Par exemple, $2I_n \in GL_n(\mathbb{Z})$ mais son inverse, $\frac{1}{2}I_n$, n'est pas dans $GL_n(\mathbb{Z})$.

➤ $GL_n(\{0, 1\})$ et $\{M \in \mathcal{M}_n(\mathbb{R}), \det(M) = 1\}$ sont des sous-groupes de $GL_n(\mathbb{R})$, en utilisant la formule de la comatrice pour l'inversion.

12 - solution Notons G cet ensemble.

➤ Déjà, $G \subset \mathbb{R}^{+*}$. Soit $a \in G$: il existe $(x, y) \in \mathbb{N} \times \mathbb{Z}$ tel que $a = x + y\sqrt{3}$ et $x^2 - 3y^2 = 1$. Forcément, $x \neq 0$. Et comme $x \in \mathbb{N}$, $x \in \mathbb{N}^*$. Alors $3y^2 = x^2 - 1$. Alors $3y^2 \leq x^2$ donc $-y\sqrt{3} \leq |y\sqrt{3}| \leq x$ donc $a \geq 0$.

Et, évidemment, $a \neq 0$ sinon $\sqrt{3}$ serait rationnel... Ainsi, $a \in \mathbb{R}^{+*}$.

➤ $1 = 1 + 0\sqrt{3} \in G$.

➤ G est $\times$ -stable.

Soient $a, b \in G$. On écrit $a = x + y\sqrt{3}$ et $b = z + t\sqrt{3}$ avec $x, z \in \mathbb{N}$, $y, t \in \mathbb{Z}$ et $x^2 - 3y^2 = 1 = z^2 - 3t^2$.

Alors $ab = (x + y\sqrt{3})(z + t\sqrt{3}) = (xz + 3yt) + (yz + xt)\sqrt{3}$.

◆ On a évidemment $yz + xt \in \mathbb{Z}$.

◆ On a aussi évidemment $xz + 3yt \in \mathbb{Z}$. Et, comme précédemment, vu que $|y\sqrt{3}| \leq x$ et $|t\sqrt{3}| \leq z$, on a $-3yt \leq |3yt| \leq xz$, donc $xz + 3yt \geq 0$. Ainsi $xz + 3yt \in \mathbb{N}$.

◆ $(xz + 3yt)^2 - 3(yz + xt)^2 = (x^2 - 3y^2)(z^2 - 3t^2) = 1$.

➤ L'inverse de $a = x + y\sqrt{3}$ dans $\mathbb{R}^{+*}$ est $x - y\sqrt{3}$, qui est bien dans G .

13 - solution 1. Posons $E = \mathbb{R} \setminus \{0, 1\}$. On sait que $(E^E, \circ)$ est un groupe non abélien. On commence donc par montrer que $(G, \circ)$ est un sous-groupe de $(E^E, \circ)$.

➤ $f_1 = \text{Id}_E \in G$.

➤ G est stable par $\circ$ et par inversion en observant le tableau de la loi :

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

Tous les éléments du tableau sont des éléments de G donc G est stable par $\circ$; et f_1 est présent sur chaque ligne et chaque colonne donc G est stable par inversion.

Donc $(G, \circ)$ est un groupe.

Par contre, $f_2 \circ f_4 = f_6 \neq f_5 = f_4 \circ f_2$ donc G n'est pas abélien.

2. Les sous-groupes : on les construit par cardinaux croissants.

➤ $\{f_1\}$ est le seul sous-groupe de cardinal 1.

➤ Un sous-groupe de cardinal > 1 contient f_1 et d'autres éléments.

◆ $\{f_1, f_4\}$ est un sous-groupe.

◆ $\{f_1, f_5\}$ est un sous-groupe.

◆ $\{f_1, f_6\}$ aussi.

◇ Par contre, s'il contient f_2 ou f_3 , il contient leur carré donc l'autre...

- De cardinal 3 : $\{f_1, f_2, f_3\}$ est le seul sous-groupe de cardinal 3. En effet, s'il contient deux des trois f_4, f_5, f_6 , il contient forcément f_2 .
- Théorème de Lagrange : pas de sous-groupe de cardinal 4, 5.
- G est le seul sous-groupe de cardinal 6.

14 - solution

1. On vérifie les trois points usuels.

- Le neutre e commute évidemment avec tous les éléments de G donc $e \in \mathcal{Z}(G)$.
- $\mathcal{Z}(G)$ est stable par $*$. Soient $x, y \in \mathcal{Z}(G)$, alors pour tout $z \in G$, $(xy)z = x(yz) = x(z y) = (xz)y = z(xy)$. Donc $xy \in \mathcal{Z}(G)$.
- $\mathcal{Z}(G)$ est stable par inversion. Soit $x \in \mathcal{Z}(G)$, montrons que $x^{-1} \in \mathcal{Z}(G)$. Soit donc $z \in G$. Comme $x \in \mathcal{Z}(G)$, on a en particulier $xz^{-1} = z^{-1}x$. De fait, $(xz^{-1})^{-1} = (z^{-1}x)^{-1}$, soit $zx^{-1} = x^{-1}z$. Ainsi $x^{-1} \in \mathcal{Z}(G)$.

Ainsi, $\mathcal{Z}(G)$ est un sous-groupe de G .

2. $\mathcal{Z}(G) = G$ ssi tout élément de G commute avec tous les autres éléments de G i.e. G est abélien.
3. $\mathcal{Z}(S_3) = \{\text{Id}\}$.

15 - solution

1. Raisonnons par l'absurde en supposant que $\mathbb{U}_m \cup \mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$. Alors $\frac{u}{n} + \frac{v}{m} = \frac{1}{mn}$. On peut donc écrire $e^{i\frac{2u\pi}{n}} e^{i\frac{2v\pi}{m}} = e^{i\frac{2\pi}{nm}}$. Et comme les deux termes du produit sont dans $\mathbb{U}_m \cup \mathbb{U}_n$, on a forcément $e^{i\frac{2\pi}{nm}} \in \mathbb{U}_m \cup \mathbb{U}_n$, ce qui est absurde puisque $(e^{i\frac{2\pi}{nm}})^n = e^{i\frac{2\pi}{m}} \neq 1$ car $m \neq 1$.

On montrerait plus généralement que $\mathbb{U}_m \cup \mathbb{U}_n$ est un sous-groupe de $\mathbb{C}^*$ ssi $m \mid n$ ou $n \mid m$.

2. ➤ 1 est dans $\mathbb{U}_1$, donc dans U .
- Stabilité par $\times$. Soient $a, b \in U$. Il existe $m, n \in \mathbb{N}^*$ tels que $a \in \mathbb{U}_m$ et $b \in \mathbb{U}_n$. Alors :

$$(ab)^{n+m} = (a^m)^n (b^n)^m = 1,$$

donc $ab \in \mathbb{U}_{m+n} \subset U$.

- Stabilité par inversion : immédiate.

Donc U est un sous-groupe de $(\mathbb{C}^*, \times)$.

16 - solution

⇐ Évident.

⇒ Supposons que $H \cap K$ soit un groupe. Supposons par l'absurde que $H \not\subset K$ et $K \not\subset H$. Alors il existe $h \in H \setminus K$ et $k \in K \setminus H$. Et forcément, $h, k \in H \cup K$ donc $hk \in H \cup K$.

- Si $hk \in H$, alors $h = \underbrace{h^{-1}}_{\in H} (\underbrace{hk}_{\in H}) \in H$, absurde.
- Si $hk \in K$, alors $h = (\underbrace{hk}_{\in K}) \underbrace{k^{-1}}_{\in K} \in K$, absurde.

Bref, dans tous les cas on a obtenu une contradiction.

17 - solution

⇒ Supposons que HK est un sous-groupe de G . Montrons que $HK = KH$.

- Soit $x \in HK$. Comme HK est un sous-groupe de G , $x^{-1} \in HK$. Donc il existe $h \in H$ et $k \in K$ tels que $x^{-1} = hk$. Et alors $x = k^{-1}h^{-1} \in KH$.
- Soit $x \in KH$. Soient $h \in H$ et $k \in K$ tels que $x = kh$. On écrit $x = (\underbrace{ek}_{\in HK})(\underbrace{he}_{\in HK}) \in HK$ puisque HK est un groupe.

⇐ Supposons que $HK = KH$. Montrons que HK est un sous-groupe de G .

- $e = \underbrace{e}_{\in H} * \underbrace{e}_{\in K} \in HK$.
- Soient $x, x' \in HK$. Montrons $xx' \in HK$. Soient $h, h' \in H$ et $k, k' \in K$ tels que $x = hk$ et $x' = h'k'$. Alors $xx' = kh'k'$. Or, $kh' \in KH = HK$, donc il existe $h'' \in H$ et $k'' \in K$ tels que $kh' = h''k''$. Ainsi $xx' = \underbrace{hh''}_{\in H} \underbrace{k''k'}_{\in K} \in HK$.
- Soit $x \in HK$. Soient $h \in H$ et $k \in K$ tels que $x = hk$. Alors $x^{-1} = k^{-1}h^{-1} \in KH = HK$.

18 - solution

On définit la relation binaire sur G : $\forall g_1, g_2 \in G, g_1 \sim g_2 \iff g_1 * g_2^{-1} \in H$.

C'est une relation d'équivalence. Ses classes d'équivalence sont exactement les classes à gauche, et forment donc une partition de G .

19 - solution

1. Si $x \in G$, $xx = e$ donc $x^{-1} = x$.
2. Soient $x, y \in G$. Selon la question 1, $(xy)^{-1} = xy$, soit $y^{-1}x^{-1} = xy$, soit $yx = xy$.
3. (a) On vérifie les trois points.
 - $e \in H$ donc $e \in H \cup gH$.
 - Stabilité par inversion : immédiat puisque $x^{-1} = x$...
 - Stabilité par $*$: soient $x, y \in H \cup gH$.
 - ◆ Si $x, y \in H$, évidemment $xy \in H \subset H \cup gH$.
 - ◆ Si $x \in H$ et $y \in gH$, on écrit $y = gy'$ avec $y' \in H$, et alors par commutativité de G :

$$xy = xgy' = gxy' \in gH \subset H \cup gH.$$

- ◆ Si $x \in gH$ et $y \in H$, on fait de même.
- ◆ Si $x, y \in gH$, il existe $x', y' \in H$ tels que $x = gx'$ et $y = gy'$. Alors :

$$xy = gx'gy' = g^2x'y' = gx'y' \in gH \subset H \cup gH.$$

Bref, $H \cup gH$ est stable par $*$.

Ainsi, $H \cup gH$ est un sous-groupe de G .

Le cardinal de gH est le même que celui de H par bijectivité de $h \mapsto gh$. De plus, $H \cap gH = \emptyset$, sinon il existerait $x, x' \in H$ tels que $x = gx'$, soit $g = xx' \in H$, ce qui est absurde. Ainsi, le cardinal de $H \cup gH$ est bien $2p$.

- (b) Il existe $g \in G \setminus \{e\}$. Alors $H_1 = \{e, g\}$ est un sous-groupe de G de cardinal 2. Raisonons ensuite par l'absurde en supposant que le cardinal de G n'est pas une puissance de 2.
 - On considère le H_1 précédent, de cardinal 2. $H_1 \neq G$, sinon $\text{Card}(G)$ est une puissance de 2.
 - On applique le procédé de la question précédente : $H_2 = H_1 \cup g_1H_1$, sous-groupe de cardinal 2^2 . $H_2 \neq G$...
 - Et ainsi de suite. On construit ainsi une suite de sous-groupes (H_k) de G , de cardinal 2^k , qui tend vers $+\infty$. Absurde, puisque G est fini.

Donc $\text{Card}(G)$ est une puissance de 2.

20 - solution

Analyse. Si φ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$, alors $\varphi(0) = 0$. Posons $a = \varphi(1)$.
Récurrence : $\forall n \in \mathbb{N}$, $\varphi(n) = an$ Et pour $n \in \mathbb{Z}^-$, $\varphi(n) = -\varphi(-n) = an$.
Synthèse. Pour tout $a \in \mathbb{Z}$, $k \mapsto ak$ est bien un morphisme de groupes...

21 - solution

1. C'est un groupe puisque c'est un groupe produit. Et le tableau de la loi :

$\searrow$	(1, 1)	(1, -1)	(-1, 1)	(-1, -1)
(1, 1)	(1, 1)	(1, -1)	(-1, 1)	(-1, -1)
(1, -1)	(1, -1)	(1, 1)	(-1, -1)	(-1, 1)
(-1, 1)	(-1, 1)	(-1, -1)	(1, 1)	(1, -1)
(-1, -1)	(-1, 1)	(-1, -1)	(1, 1)	(1, 1)

2. On constate que $\forall x \in G$, $x^2 = (1, 1)$. Donc si $f : G \mapsto \mathbb{U}_4$ est un isomorphisme de groupes, alors :

$$f(x)^2 = f(x^2) = f((1, 1)) = 1.$$

Donc le carré de tout élément de $\mathbb{U}_4$ est le neutre 1, ce qui n'est pas le cas puisque $i^2 = -1 \neq 1$.

22 - solution

1. Soit $a \in G$.

- $\tau_a : G \mapsto G$ puisque G est un groupe.
- Soit $b_1, b_2 \in G$. $\tau_a(b_1b_2) = ab_1b_2a^{-1} = ab_1a^{-1}ab_2a^{-1} = \tau_a(b_1)\tau_a(b_2)$.

Donc τ_a est un morphisme de groupe. Montrons qu'il est bijectif.

M1 On prouve successivement injectivité et surjectivité.

- ◆ Montrons que τ_a est injectif. Soit $b \in \text{Ker}(\tau_a)$. Alors $\tau_a(b) = e \iff aba^{-1} = e \iff b = a^{-1}ea = e$.
 Donc $\text{Ker}(\tau_a) = \{e\}$ et τ_a est injectif.

- ◆ Montrons que τ_a est surjectif. Soit $c \in G$. En posant $b = a^{-1}ca$, on a directement $\tau_a(b) = c$ donc τ_a est surjectif.

M2 On peut simplement résoudre l'équation $\tau_a(b) = c$.

Soit donc $c \in G : \tau_a(b) = c \iff aba^{-1} = c \iff b = a^{-1}ca$.

L'équation admet toujours une unique solution, donc τ_a est bijective.

M3 On peut observer que $\tau_a \circ \tau_{a^{-1}} = \text{Id}_G$ donc d'après le théorème de neutralisation, τ_a est bijective.

2. D'après la question 1, $\tau : G \rightarrow \mathcal{S}(G)$. Il reste à prouver que τ est un morphisme.

Soient $a_1, a_2 \in G$. $\tau(a_1 a_2)$ est définie par :

$$\forall b \in G, \tau(a_1 a_2)(b) = \tau_{a_1 a_2}(b) = a_1 a_2 b (a_1 a_2)^{-1} = a_1 a_2 b a_2^{-1} a_1^{-1} = \tau_{a_1}(\tau_{a_2}(b)).$$

Ainsi, $\tau(a_1 a_2) = \tau(a_1) \circ \tau(a_2)$.

3. Soit $a \in G$. $a \in \text{Ker}(\tau) \iff \tau(a) = \text{Id}_G \iff \forall b \in G, a b a^{-1} = b \iff \forall b \in G, a b = b a \iff a \in \mathcal{Z}(G)$.

23 - solution Oui. Non car $3 \in \mathbb{D}$ mais $\frac{1}{3} \notin \mathbb{D}$.

24 - solution $\triangleright \implies$ Supposons que $\mathbb{Z}[r]$ soit un anneau. Alors $r \in \mathbb{Z}[r]$, donc $r^2 \in \mathbb{Z}[r]$ donc il existe $a, b \in \mathbb{Z}$ tels que $r^2 = a + br$. Ainsi, r est racine du polynôme unitaire du second degré à coefficients entiers $P(X) = X^2 - bX - a$.

$\triangleright \implies$ Supposons qu'il existe $a, b \in \mathbb{Z}$ tels que $r^2 + ar + b = 0$. Montrons que $\mathbb{Z}[r]$ est un sous-anneau de $\mathbb{R}$ en vérifiant les trois points.

H1 $1 = 1 + 0r \in \mathbb{Z}[r]$.

H2 Soit $(x_1, x_2) \in \mathbb{Z}[r]$. Il existe donc $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1 r$ et $x_2 = a_2 + b_2 r$. Alors $x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2)r \in \mathbb{Z}[r]$, car $a_1 - a_2, b_1 - b_2 \in \mathbb{Z}$.

H3 Soit $(x_1, x_2) \in \mathbb{Z}[r]$. Il existe donc $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1 r$ et $x_2 = a_2 + b_2 r$. Alors :

$$\begin{aligned} x_1 x_2 &= a_1 a_2 + (a_1 b_2 + a_2 b_1)r + b_1 b_2 r^2 \\ &= (a_1 a_2 - b b_1 b_2) + (a_1 b_2 + a_2 b_1 - a b_1 b_2)r \in \mathbb{Z}[\sqrt{2}], \text{ car } a_1 a_2 - b b_1 b_2, a_1 b_2 + a_2 b_1 - a b_1 b_2 \in \mathbb{Z}. \end{aligned}$$

Donc $\mathbb{Z}[r]$ est un sous-anneau de $\mathbb{R}$, donc c'est un anneau.

25 - solution $\triangleright$ On vérifie les deux points.

H1 $0 = 0 + 0\sqrt{2} + 0\sqrt{3} \in \mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

H2 Soit $(x_1, x_2) \in \mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

Il existe donc $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1\sqrt{2} + c_1\sqrt{3}$ et $x_2 = a_2 + b_2\sqrt{2} + c_2\sqrt{3}$.

Alors $x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} + (c_1 - c_2)\sqrt{3} \in \mathbb{Z}[\sqrt{2}, \sqrt{3}]$, car $a_1 - a_2, b_1 - b_2, c_1 - c_2 \in \mathbb{Z}$.

Donc $(\mathbb{Z}[\sqrt{2}, \sqrt{3}], +)$ est un sous-groupe de $(\mathbb{R}, +)$, donc c'est un groupe.

$\triangleright (\mathbb{Z}[\sqrt{2}, \sqrt{3}], +, \times)$ n'est un anneau car ce n'est pas un sous-anneau de $(\mathbb{R}, +, \times)$.

En effet : $\sqrt{2}, \sqrt{3} \in \mathbb{Z}[\sqrt{2}, \sqrt{3}]$, mais $\sqrt{2} \times \sqrt{3} = \sqrt{6} \notin \mathbb{Z}[\sqrt{2}, \sqrt{3}]$. Justifions-le par l'absurde : supposons donc qu'il existe $a, b \in \mathbb{Z}$ tels que $\sqrt{6} = a\sqrt{2} + b\sqrt{3}$. Il est clair que $a \neq 0$ et $b \neq 0$ (raisonnement par l'absurde immédiat).

Alors $6 = 2a^2 + 3b^2 + ab\sqrt{6}$, soit $6 - 2a^2 - 3b^2 = ab\sqrt{6}$ ou encore $\sqrt{6} = \frac{6 - 2a^2 - 3b^2}{ab}$. Ainsi, $\sqrt{6}$ serait rationnel, ce qui est absurde.

26 - solution Anneau : cf. groupe produit...

Non intègre : $(0_A, 1_B) \times (1_A, 0_B) = (0_A, 0_B)$ donc $A \times B$ n'est jamais intègre.

27 - solution $\triangleright$ Soit $a \in A$. a et 1 commutent forcément puisque 1 commute avec tout élément de A , donc $(a+1)^2 = a^2 + 2a + 1$. Or, $(a+1)^2 = a+1$ et $a^2 = a$, donc $2a = 0$.

$\triangleright$ Soient alors $a, b \in A$. On a $(a+b)^2 = a^2 + b^2 + ab + ba$. Or, $(a+b)^2 = a+b$, $a^2 = a$ et $b^2 = b$, donc $0 = ab + ba$, soit $ab = -ba$. Selon la question 1, $2ba = 0$ donc $-ba = ba$. Finalement, $ab = ba$. Ainsi, A est commutatif.

28 - solution 1. Élément neutre pour l'addition : la suite constante nulle ; élément neutre pour la multiplication : la suite $\mathbb{1}$.

2. ...

3. Non : la suite constante égale à 1 n'est pas dans D !

4. ...

5. Opérations algébriques : $\lim(u+v) = \lim(u) + \lim(v)$; $\lim(uv) = \lim(u)\lim(v)$; $\lim(\mathbb{1}) = 1$. Non injectif car $(1/n)$ et $(-1/n)$ convergent toutes deux vers 0 mais ne sont pas égales.

29 - solution $\triangleright (A, \perp, *)$ est un anneau. Son neutre pour $\perp$ est -1 ; son neutre pour $*$ est 0.

$\triangleright \varphi : x \mapsto x - 1$ est un isomorphisme d'anneaux.

30 - solution

1. $\mathbb{F}_n^\times$ désigne l'ensemble des nombres premiers avec n . Or, pour $k \in \llbracket 0, p^\alpha - 1 \rrbracket$:

$$k \wedge p^\alpha = 1 \iff k \wedge p = 1.$$

Les éléments non inversibles de $\mathbb{F}_{p^\alpha}$ sont donc les multiples de p : $0, p, 2p, (p^\alpha - 1)p$. Il y en a $p^{\alpha-1}$. Donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

2. $\triangleright$ Soient $x, y \in \mathbb{Z}$ tels que $\bar{x}^{[nm]} = \bar{y}^{[nm]}$. On a donc $x \equiv y \pmod{nm}$, donc $x \equiv y \pmod{n}$, soit $\bar{x}^{[n]} = \bar{y}^{[n]}$. Et, de même, $\bar{x}^{[m]} = \bar{y}^{[m]}$. Ainsi f est bien définie.

$\triangleright f$ est un morphisme d'anneaux car :

$$\diamond f(\bar{1}^{[nm]}) = (\bar{1}^{[n]}, \bar{1}^{[m]});$$

$$\diamond \text{ si } h, k \in \mathbb{Z}, f(\overline{h+k}^{[nm]}) = f(\overline{h}^{[nm]}) + f(\overline{k}^{[nm]});$$

$$\diamond \text{ si } h, k \in \mathbb{Z}, f(\overline{hk}^{[nm]}) = f(\overline{h}^{[nm]})f(\overline{k}^{[nm]}).$$

$\triangleright \text{Ker}(f) = \{\bar{0}^{[nm]}\}$ donc f est injective (lemme de Gauss).

$\triangleright |\mathbb{F}_{nm}| = nm = |\mathbb{F}_n| |\mathbb{F}_m|$ donc f est bijective.

Donc f est un isomorphisme d'anneaux.

On en déduit que $\mathbb{F}_{nm}^\times = f^{-1}(\mathbb{F}_n^\times \times \mathbb{F}_m^\times)$, donc $\varphi(nm) = \varphi(n)\varphi(m)$.

3. $\varphi(n) = \prod_{p \in \mathbb{P}} (p^{v_p(n)-1}(p-1))$.

31 - solution

1. Cours.

2. Le neutre pour $+$ est $\bar{0}$, celui pour la loi $\times$ est $\bar{1}$.

3. Intègre si $n = 2$ et $n = 3$. Pas intègre si $n = 4$ car $\bar{2} \times \bar{2} = \bar{4} = \bar{0}$.

4. Théorème de Bézout.

5. Algorithme étendu d'Eulcide : on trouve $-19 \times 26 + 11 \times 45 = 1$. Donc l'inverse de 26 dans $\mathbb{Z}/45\mathbb{Z}$ est -19 qui est congru à 26 modulo 45. Autrement dit, 26 est son propre inverse. Alors : $26n \equiv 9 \pmod{45} \iff n \equiv 9 \times 26 \pmod{45} \iff n \equiv 234 \pmod{45} \iff n \equiv 9 \pmod{45}$.

L'ensemble des solutions est $\{9 + 45k, k \in \mathbb{Z}\}$.

32 - solution

1. On montrer que

H1 $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

H2 Soit $(x_1, x_2) \in \mathbb{Z}[\sqrt{2}]$. Il existe donc $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1\sqrt{2}$ et $x_2 = a_2 + b_2\sqrt{2}$. Alors $x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, car $a_1 - a_2, b_1 - b_2 \in \mathbb{Z}$.

H3 Soit $(x_1, x_2) \in \mathbb{Z}[\sqrt{2}]$. Il existe donc $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1\sqrt{2}$ et $x_2 = a_2 + b_2\sqrt{2}$. Alors $x_1x_2 = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, car $a_1a_2 + 2b_1b_2, a_1b_2 + a_2b_1 \in \mathbb{Z}$.

2. (a) Soient $x_1, x_2 \in \mathbb{Z}[\sqrt{2}]$. Il existe donc $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x_1 = a_1 + b_1\sqrt{2}$ et $x_2 = a_2 + b_2\sqrt{2}$. Alors :

$$\begin{aligned} N(x_1x_2) &= N((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) \\ &= (a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2 \\ &= a_1^2a_2^2 - 2a_1^2b_2^2 - 2a_2^2b_1^2 + 4b_1^2b_2^2 \\ &= (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) \\ &= N(x_1)N(x_2) \end{aligned}$$

(b) Par double implication.

$\triangleright$ Si $x = a + b\sqrt{2}$ vérifie $N(x) = \pm 1$, alors $x^{-1} = \frac{a-b\sqrt{2}}{N(x)} = \pm(a - b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$ donc x est inversible dans $(\mathbb{Z}, +, \times)$.

$\triangleright$ Réciproquement, si x est inversible dans $\mathbb{Z}[\sqrt{2}]$, alors il existe $x_2 \in \mathbb{Z}[\sqrt{2}]$ tel que $xx_2 = 1$. *A fortiori*, $N(xx_2) = N(x)N(x_2) = 1$, donc $N(x)$ est inversible dans $(\mathbb{Z}, \times)$, donc $N(x) = \pm 1$.

(c) $\triangleright N(\sqrt{2}) = -2 \neq \pm 1$ donc $\sqrt{2}$ n'est pas inversible.

$\triangleright N(3 + 2\sqrt{2}) = 9 - 8 = 1$ donc $3 + 2\sqrt{2}$ est inversible.

$\triangleright \frac{1}{3+2\sqrt{2}} = 3 - 2\sqrt{2}$.

33 - solution

1. Soit $a \in A$ nilpotent. Soit $n \in \mathbb{N}$ tel que $a^n = 0$. Posons $x = \sum_{k=0}^{n-1} a^k$.

On calcule $(1-a)x = \sum_{k=0}^{n-1} (a^k - a^{k+1}) = 1 - a^n = 1$. Et de même $x(1-a) = 1$. Donc $1-a$ est inversible d'inverse

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

2. (a) Comme ab est nilpotent, il existe $n \in \mathbb{N}$ tel que $(ab)^n = 0$. Alors $(ba)^{n+1} = b(ab)^n a = 0$. Donc d'après la question 1, $1 - ba$ est inversible et $(1 - ba)^{-1} = \sum_{k=0}^n (ba)^k = 1 + b \left(\sum_{k=0}^{n-1} (ab)^k \right) a = 1 + b(1 - ab)^{-1}a$.
- (b) Posons $x = 1 + b(1 - ab)^{-1}a$. On vérifie :
- $(1 - ba)x = 1 - ba + b(1 - ab)^{-1}a - bab(1 - ab)^{-1}a = 1 - ba + b(1 - ab)(1 - ab)^{-1}a = 1 - ba + ba = 1$;
 - $x(1 - ba) = 1$ de même.
- Ainsi, $1 - ba$ est inversible d'inverse $1 + b(1 - ab)^{-1}a$.

34 - solution On montre facilement avec la caractérisation que $\mathbb{Q}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$. De plus, il hérite de la commutativité et de l'intégrité de celle de $\mathbb{R}$.

Soit $x \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$. On pose $a, b \in \mathbb{Q}^*$ tels que $x = a + b\sqrt{2}$. Alors $a^2 - 2b^2 = (a - b\sqrt{2})(a + b\sqrt{2}) \neq 0$ et on peut écrire :

$$\frac{1}{x} = \frac{a}{a^2 - 2b^2} + \sqrt{2} \frac{b}{a^2 - 2b^2} \in \mathbb{Q}[\sqrt{2}].$$

Ainsi, tout élément non nul de $\mathbb{Q}[\sqrt{2}]$ est inversible dans $\mathbb{Q}[\sqrt{2}]$, donc $\mathbb{Q}[\sqrt{2}]$ est un corps.

35 - solution Soit K un corps contenu dans $\mathbb{Q}$.

- $1 \in K$ puisque K est un sous-anneau de $\mathbb{Q}$.
- $0 = 1 - 1 \in K$ pour la même raison.
- Pour tout $n \in \mathbb{N}^*$, $n = \sum_{k=1}^n 1 \in K$.
- Pour tout $n \in \mathbb{N}$, $-n \in K$, donc $\forall n \in \mathbb{Z}$, $n \in K$.
- Pour tout $n \in \mathbb{Z}^*$, $n \in K \setminus \{0\} = K^\times$, donc $\frac{1}{n} \in K$.
- Enfin, dès que $(n, m) \in \mathbb{Z} \times \mathbb{N}^*$, $n \in K$ et $\frac{1}{m} \in K$ selon précédemment, donc $\frac{n}{m} = n \times \frac{1}{m} \in K$.

On en conclut que $\mathbb{Q} \subset K$ et donc que $K = \mathbb{Q}$.

36 - solution Il reste à montrer que tout élément non nul de cet anneau est inversible. Soit a un élément non nul. $\varphi : x \mapsto ax$ est injective, car $\text{Ker}(\varphi) = \{0\}$. Comme A est fini, φ est forcément bijective donc 1 admet un antécédent, d'où le résultat.