Groupes, anneaux, corps

Solution 1.

Tout d'abord, $S(x)$ est bien une partie de $S(E)$.
Ensuite, $\mathrm{Id}_E \in S(x)$ puisque $\mathrm{Id}_E(x) = x$.
Enfin, soient $\sigma, \sigma' \in S(x)$. Montrons que $\sigma^{-1} \circ \sigma' \in S(x)$. On a $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x)$ car $\sigma'(x) = x$. Or $\sigma(x) = x$ donc, en composant par σ^{-1}, $\sigma^{-1}(x) = x$. Donc $\sigma^{-1} \circ \sigma'(x) = \sigma^{-1}(x) = x$ et $\sigma^{-1} \circ \sigma' \in S(x)$.
$S(x)$ est bien un sous-groupe de $(S(E), \circ)$.
Remarque. $S(x)$ est appelé le stabilisateur de x. ■

Solution 2.

1. Soient (x, y) et (x', y') dans G. Comme $x, x' \in \mathbb{R}^*$, $xx' \in \mathbb{R}^*$ et il est évident que $xy' + y \in \mathbb{R}$. Donc $(x, y) * (x', y') \in G$.
Soient (x, y), (x', y') et (x'', y'') dans G. On voit facilement que :
$$\begin{aligned}((x, y) * (x', y')) * (x'', y'') &= (x, y) * ((x', y') * (x'', y''))\\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

2. G possède un élément neutre à savoir $(1, 0)$. Soit $(x, y) \in G$ et cherchons $(x', y') \in G$ tel que $(x, y) * (x', y') = (1, 0)$. Ceci équivaut à résoudre
$$\begin{cases} xx' = 1 \\ xy' + y = 0 \end{cases} \iff \begin{cases} x' = \dfrac{1}{x} \\ y' = -\dfrac{y}{x} \end{cases} \text{ car } x \neq 0$$
Donc (x, y) admet pour inverse à droite $\left(\dfrac{1}{x}, -\dfrac{y}{x}\right)$. On vérifie facilement que c'est aussi l'inverse à gauche, donc l'inverse.
En conclusion, $(G, *)$ est bien un groupe. On voit qu'il n'est pas commutatif car $(1, 1) * (2, 2) = (2, 4)$ et $(2, 2) * (1, 1) = (2, 3)$.

3. A partir des premières valeurs de n, on conjecture $(x, y)^{*n} = (x^n, y + yx + \cdots + yx^{n-1})$.
Initialisation : La formule est clairement vraie pour $n = 0$.
Hérédité : On suppose $(x, y)^{*n} = (x^n, y + yx + \cdots + yx^{n-1})$ pour un certain n. Alors
$$\begin{aligned}(x, y)^{*(n+1)} &= (x, y) * (x, y)^{*n}\\ &= (x, y) * (x^n, y + yx + \cdots + yx^{n-1})\\ &= (x^{n+1}, y + yx + \cdots + yx^n)\end{aligned}$$
On conclut par récurrence.
En outre, en utilisant la somme des termes d'une suite géométrique, on a :
$$(x, y)^{*n} = \begin{cases} \left(x^n, y \cdot \dfrac{1 - x^n}{1 - x}\right) \text{ si } x \neq 1 \\ (x, ny) \text{ sinon} \end{cases}$$

Solution 3.

1. Soient $x, y \in G$. Comme th induit une bijection de $\mathbb{R}$ sur $]-1, 1[$, il existe $a, b \in \mathbb{R}$ tels que $x = \operatorname{th} a$ et $y = \operatorname{th} b$. Alors $x * y = \operatorname{th}(a + b) \in]-1, 1[$.
Soient maintenant $x, y, z \in G$. De la même façon, il existe $a, b, c \in \mathbb{R}$ tels que $x = \operatorname{th} a$, $y = \operatorname{th} b$ et $z = \operatorname{th} c$. On voit alors facilement que
$$(x * y) * z = x * (y * z) = \operatorname{th}(a + b + c)$$
En conclusion, $*$ est une loi interne associative sur G.

2. Il est clair que 0 est l'élément neutre de $(G, *)$ et que tout $x \in G$ admet $-x$ pour inverse. G est donc un groupe.
   L'expression de $x * y$ est symétrique en x et y : le groupe est donc commutatif.

3. Soit $x \in G$ et $a \in \mathbb{R}$ tel que $x = \operatorname{th} a$. On a donc $x^{*n} = \operatorname{th}(na)$.
   Or $a = \operatorname{argth} x = \dfrac{1}{2} \ln\left(\frac{1+x}{1-x}\right)$. Par conséquent,

$$\operatorname{th}(na) = \frac{\left(\frac{1+x}{1-x}\right)^{\frac{n}{2}} - \left(\frac{1+x}{1-x}\right)^{-\frac{n}{2}}}{\left(\frac{1+x}{1-x}\right)^{\frac{n}{2}} + \left(\frac{1+x}{1-x}\right)^{-\frac{n}{2}}} = \frac{(1+x)^n - (1-x)^n}{(1+x)^n + (1-x)^n}$$

Remarque. On a en fait montré que th était un morphisme de $(\mathbb{R}, +)$ sur $(G, *)$. ■

Solution 4.

1. Notons e l'élément neutre de G. Comme H et K sont des sous-groupes de G, ils contiennent tous deux l'élément neutre e. Donc $e \in H \cap K$.
   Soit $h, k \in H \cap K$. Comme H est un sous-groupe de G, $h^{-1}k \in H$. De même, $h^{-1}k \in K$. Par conséquent, $h^{-1}k \in H \cap K$. En conclusion, $H \cap K$ est un sous-groupe de G.

2. Si $H \subset K$ ou $K \subset H$, on a $H \cup K = K$ ou $H \cup K = H$. Donc $H \cup K$ est bien un sous-groupe de G.
   Réciproquement, supposons que $H \cup K$ est un sous-groupe de G. Supposons de plus que $H \not\subset K$ et montrons que $K \subset H$. Comme $H \not\subset K$, il existe $h_0 \in H \setminus K$. Soit maintenant $k \in K$. Comme $h_0, k \in H \cup K$ et que $H \cup K$ est un sous-groupe de G, $h_0 k \in H \cup K$. On ne peut avoir $h_0 k \in K$ car sinon $h_0 = (h_0 k)k^{-1} \in K$, ce qui n'est pas. Donc $h_0 k \in H$. Or $k = h_0^{-1}(h_0 k) \in H$. Ceci étant vrai pour tout élément k de K, on a donc $K \subset H$.

Solution 5.

On remarque que pour tout $x \in G$, $x^{-1} = x$. Soient $x, y \in G$. On a donc $(xy)^{-1} = xy$. Mais on a aussi $(xy)^{-1} = y^{-1}x^{-1} = yx$. Par conséquent, $yx = xy$. Ceci étant valable pour tous $x, y \in G$, G est commutatif.

Solution 6.

Notons e l'élément neutre de G. Il est clair que $e \in Z(G)$. Soit $(x, y) \in Z(G)^2$. Alors, pour tout $a \in G$, $xya = xay = axy$, donc xy commute avec tout élément a de G. Ainsi G est stable par produit. De plus, pour tout $a \in G$, $ax = xa$. En mutipliant cette relation à gauche et à droite par x^{-1}, on obtient $x^{-1}a = ax^{-1}$ pour tout élément a de G. Ainsi $Z(G)$ est stable par passage à l'inverse. Donc $Z(G)$ est un sous-groupe de G.

Solution 7.

Pour tout $a \in \mathbb{R}$, $a * 0 = 0 * a = a$ donc 0 est élément neutre. Mais pour tout $a \in \mathbb{R}$, $(-1) * a = -1 \neq 0$ donc -1 n'admet pas d'inverse pour la loi $*$. $(\mathbb{R}, *)$ n'est donc pas un groupe.

Solution 8.

1. Il suffit de chosir $n = \left\lfloor \dfrac{\beta}{\alpha} \right\rfloor$.

2. Comme $G \neq \{0\}$ et $0 \in G$, G contient un élément non nul a. Si $a > 0$, $G \cap \mathbb{R}_+^*$ est non vide. Sinon, G étant un groupe, $-a \in G$ et à nouveau $G \cap \mathbb{R}_+^*$ est non vide.
   De plus, $G \cap \mathbb{R}_+^*$ est minorée par 0. Ainsi $G \cap \mathbb{R}_+^*$ admet une borne inférieure.

3. **a.** Comme $a = \inf G \cap \mathbb{R}_+^*$ et que $a > 0$, il existe $x \in G \cap \mathbb{R}_+^*$ tel que $a \leqslant x < a + a = 2a$. Comme on a supposé $a \notin G$, on a en fait $a < x < 2a$. Puisque $x - a > 0$, il existe $y \in G \cap \mathbb{R}_+^*$ tel que $a \leqslant y < a + (x - a) = x$. A nouveau $a \notin G$ donc $a < y < x < 2a$. Les réels x et y sont bien deux éléments distincts de $]a, 2a[$.
   b. Comme $a < y < x < 2a$, $0 < x - y < a$. Comme G est un sous-groupe de $\mathbb{R}$, $y - x \in G$. On a donc $y - x \in G \cap \mathbb{R}_+^*$ et $y - x < a$, ce qui contredit le fait que $a = \inf G \cap \mathbb{R}_+^*$. On a donc $a \in G$.
   c. Comme G est un sous-groupe de $\mathbb{R}$, $na \in G$ pour tout $n \in \mathbb{Z}$. On a donc $a\mathbb{Z} \subset G$.
   d. D'après la question **1**, il existe $n \in \mathbb{Z}$ tel que $na \leqslant z < (n+1)a$. Comme z et a sont des éléments du sous-groupe G, $z - na$ est également un élément de G. Or $0 \leqslant z - na < a$ et $a = \inf G \cap \mathbb{R}_+^*$. On a donc nécessairement $z - na = 0$ i.e. $z = na$.
   e. Les deux questions précédentes montrent que $G \subset a\mathbb{Z}$. Par double inclusion, $G = a\mathbb{Z}$.

4. **a.** Comme $\inf G \cap \mathbb{R}_+^* = 0$, il existe $\varepsilon' \in G \cap \mathbb{R}_+^*$ tel que $0 < \varepsilon' < \varepsilon$. D'après la question **1**, il existe $n \in \mathbb{Z}$ tel que $n\varepsilon' \leqslant t < (n+1)\varepsilon'$. Posons $g = n\varepsilon'$. $g \in G$ puisque $\varepsilon' \in G$. De plus, $0 \leqslant t - g < \varepsilon' < \varepsilon$ donc $|g - t| < \varepsilon$.
   b. On a prouvé que pour tout élément t de $\mathbb{R}$ et tout $\varepsilon > 0$, il existe un élément de G dans $]t - \varepsilon, t + \varepsilon[$: ceci signifie que G est dense dans $\mathbb{R}$.

Solution 9.

Première méthode :
Notons p le produit recherché et e l'élément neutre de G. Dans le produit, les éléments x de G tels que $x \neq x^{-1}$ i.e. $x^2 \neq e$ se simplifient avec leur inverse. Notons $A = \{x \in G \mid x^2 = e\}$. On a donc $p = \prod_{x \in A} x$. Les éléments de A sont d'ordre 1 ou 2. Comme l'ordre de G est impair, les éléments de A sont tous d'ordre 1, autrement dit $A = \{e\}$ et $p = e$.
Seconde méthode :
L'application $x \mapsto x^{-1}$ est une permutation de G. Ainsi $p = \prod_{x \in G} x = \prod_{x \in G} x^{-1}$. D'où $p^2 = e$. p est donc d'ordre 1 ou 2. Comme G est d'ordre impair, p est d'ordre 1 i.e. $p = e$.

Solution 10.

Associativité :
Soient $x, y, z \in H$.

$$\begin{aligned}
x.(y.z) &= f\left(f^{-1}(x) * f^{-1}(y.z)\right) \\
&= f\left(f^{-1}(x) * \left(f^{-1}(y) * f^{-1}(z)\right)\right) \\
&= f\left(\left(f^{-1}(x) * f^{-1}(y)\right) * f^{-1}(z)\right) \text{ par associativité de } * \\
&= f\left(f^{-1}(x.y) * f^{-1}(z)\right) \\
&= (x.y).z
\end{aligned}$$

Elément neutre :
Notons e l'élément neutre de $(G, *)$. Pour tout $x \in H$

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

Donc $(H, .)$ admet un élément neutre, à savoir $f(e)$.
Inversibilité :
Soit $x \in H$.

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

Ainsi tout élément x de G est inversible (d'inverse $\left(f^{-1}(x)\right)^{-1}$).
Remarque. On a des résultats pour les anneaux et les corps. La bijection f permet de «transporter» la structure de G sur H. ■

Solution 11.

Associativité :
Soient $x', y', z' \in H$. Comme f est surjective, x', y', z' admmettent des antécédents x, y, z par f dans G.

$$\begin{aligned} x'.(y'.z') &= f(x).\left(f(y).f(z)\right) \\ &= f(x).f(y*z) \\ &= f\left(x*(y*z)\right) \\ &= f((x*y)*z) \text{par associativité de } * \\ &= f(x*y).f(z) \\ &= \left(f(x).f(y)\right).f(z) \\ &= (x'.y').z' \end{aligned}$$

Elément neutre :
Notons e l'élément neutre de G. Soit $x' \in G$. Comme f est surjective, x' admet un antécédent x par f dans G

$$\begin{aligned} x'.f(e) = f(x).f(e) = f(x*e) = f(x) = x' \\ f(e).x' = f(e).f(x) = f(e*x) = f(x) = x' \end{aligned}$$

Ainsi $(H, .)$ admet un élément neutre, à savoir $f(e)$.
Inversibilité :
Soit $x' \in G$. Comme f est surjective, x' admet un antécédent x par f dans G.

$$\begin{aligned} x'.f(x^{-1}) = f(x).f(x^{-1}) = f(x*x^{-1}) = f(e) \\ f(x^{-1}).x' = f(x^{-1}).f(x) = f(x^{-1}*x) = f(e) \end{aligned}$$

Ainsi tout élément de G est inversible.

Puisque G et H sont des groupes, f est un morphisme de groupes.
Remarque. On a des résultats pour les anneaux et les corps. La surjection f permet de «transporter» la structure de G sur H. ■

Solution 12.

Notons e l'élément neutre de G.
Pour tout $x \in G$, $x = e^{-1}xe$ donc $x \sim x$. Ainsi $\sim$ est réflexive.
Soit $(x, y) \in G^2$ tel que $x \sim y$. Il existe donc $g \in G$ tel que $y = g^{-1}xg$. Mais alors $x = gyg^{-1} = \left(g^{-1}\right)^{-1} x \left(g^{-1}\right)$ donc $y \sim y$. Ainsi $\sim$ est symétrique.
Soit $(x, y, z) \in G^3$ tel que $x \sim y$ et $y \sim z$. Il existe donc $(g, h) \in G^2$ tel que $y = g^{-1}xg$ et $z = h^{-1}yh$. Mais alors $z = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh)$ donc $x \sim z$. Ainsi $\sim$ est transitive.
Finalement, $\sim$ est bien une relation d'équivalence.

Solution 13.

Notons e l'élément neutre de G.
Pour tout $x \in G$, $x = xe$ et $e \in H$ car H est un sous-groupe de G donc $x \sim x$. Ainsi $\sim$ est réflexive.
Soit $(x, y) \in G^2$ tel que $x \sim y$. Il existe donc $h \in H$ tel que $y = xh$. Mais alors $x = yh^{-1}$ et $h^{-1} \in H$ car H est un sous-groupe de G donc $y \sim y$. Ainsi $\sim$ est symétrique.
Soit $(x, y, z) \in G^3$ tel que $x \sim y$ et $y \sim z$. Il existe donc $(h, k) \in H^2$ tel que $y = xh$ et $z = yk$. Mais alors $z = xhk$ et $hk \in H$ car H est

un sous-groupe de G donc $x \sim z$. Ainsi $\sim$ est transitive.
Finalement, $\sim$ est bien une relation d'équivalence.
Remarque. On montrerait de la même manière que la relation binaire $\sim$ définie par

$$\forall(x,y) \in G^2,\ x \sim y \iff \exists h \in H,\ y = hx$$

est également une relation d'équivalence. ■

Solution 14.

1. On rappelle que $S(\mathbb{C})$ désigne l'ensemble des bijections de $\mathbb{C}$ dans $\mathbb{C}$. On va montrer que G est un sous-groupe de $S(\mathbb{C})$.
   - Montrons que $G \subset S(\mathbb{C})$. Soit $f \in G$. Il existe donc $(a,b) \in \mathbb{C}^* \times \mathbb{C}$ tel que $f(z) = az + b$ pour tout $z \in \mathbb{C}$. On montre alors que f est bijective en vérifiant que $z \mapsto \frac{1}{a}(z-b)$ est sa bijection réciproque.
   - Clairement, $\mathrm{Id}_{\mathbb{C}} \in G$, puisque $\mathrm{Id}_{\mathbb{C}}$ est par exemple la translation de vecteur nul ou une rotation d'angle nul (et de centre quelconque).
   - Montrons que G est stable par composition. Soit $(f,g) \in G^2$. Il existe donc $(a,b,c,d) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}^* \times \mathbb{C}$ tel que $f(z) = az+b$ et $g(z) = cz + d$ pour tout $z \in \mathbb{C}$. Alors $g \circ f(z) = caz + cb + d$ pour tout $z \in \mathbb{C}$. $g \circ f$ est bien une translation ou une similitude directe puisque $ca \neq 0$.
   - Montrons que G est stable par inversion. Soit $f \in G$. Il existe donc $(a,b) \in \mathbb{C}^* \times \mathbb{C}$ tel que $f(z) = az + b$ pour tout $z \in \mathbb{C}$. On a montré précédemment que $f^{-1}(z) = \frac{1}{a}z - \frac{b}{a}$ pour tout $z \in \mathbb{C}$. Ceci montre que f^{-1} est bien une translation ou une similitude directe puisque $\frac{1}{a} \neq 0$.

   On a donc montré que G était un sous-groupe de $S(\mathbb{C})$ et donc un groupe.
2. - A nouveau, $\mathrm{Id}_{\mathbb{C}} \in H$, puisque $\mathrm{Id}_{\mathbb{C}}$ est par exemple la translation de vecteur nul ou une rotation d'angle nul (et de centre quelconque).
   - Montrons que H est stable par composition. Soit $(f,g) \in H^2$. Il existe donc $(a,b,c,d) \in \mathbb{U} \times \mathbb{C} \times \mathbb{U} \times \mathbb{C}$ tel que $f(z) = az+b$ et $g(z) = cz+d$ pour tout $z \in \mathbb{C}$. Alors $g \circ f(z) = caz+cb+d$ pour tout $z \in \mathbb{C}$. $g \circ f$ est bien une translation ou une rotation puisque $ca \in \mathbb{U}$.
   - Montrons que H est stable par inversion. Soit $f \in H$. Il existe donc $(a,b) \in \mathbb{U} \times \mathbb{C}$ tel que $f(z) = az + b$ pour tout $z \in \mathbb{C}$. On a montré précédemment que $f^{-1}(z) = \frac{1}{a}z - \frac{b}{a}$ pour tout $z \in \mathbb{C}$. Ceci montre que f^{-1} est bien une translation ou une rotation puisque $ca \in \mathbb{U}$.

   On a donc montré que H était un sous-groupe de G.

Solution 15.

1. Pour tout $g, h \in G$ on a

$$(\varphi_{g^{-1}} \circ \varphi_g)(h) = g^{-1}(gh) = (g^{-1}g)h = h\,,$$
$$(\varphi_g \circ \varphi_{g^{-1}})(h) = g(g^{-1}h) = (gg^{-1})h = h\,.$$

   Cela signifie que l'application φ_g est bijective, $\varphi_{g^{-1}}$ étant son inverse.
2. $\forall g, g', h \in G$ on a

$$(\varphi_{gg'})(h) = (gg')h = g(g'h) = (\varphi_g \circ \varphi_{g'})(h),$$

   d'où $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$.
   Soit $g \in \operatorname{Ker}\varphi$. Alors $\varphi_g = \mathrm{Id}_G$, c'est-à-dire $gh = h$ pour tout $h \in G$. En particulier $g = ge_G = e_G$. Ainsi $\operatorname{Ker}\varphi = \{e_G\}$, c'est-à-dire φ est un morphisme injectif.

SOLUTION 16.

1. On a pour tous $x, y \in G$,
$$\varphi(x)\varphi(y) = axa^{-1}aya^{-1} = axya^{-1} = \varphi_a(xy).$$
Ainsi φ_a est bien un endomorphisme de G.
Pour $x, y \in G$,
$$y = \varphi_a(x) \iff y = axa^{-1} \iff a^{-1}ya = x \iff x = \varphi_{a^{-1}}(y)$$
Ainsi νa_a est bien bijectif : c'est un automorphisme de G. On a en fait aussi prouvé que $\varphi_a^{-1} = \varphi_{a^{-1}}$.

2. Comme pour tout $a \in G$, φ_a est bijectif, $\mathfrak{I}(G) \subset \mathcal{A}ut(G)$. On a $\mathrm{Id}_G = \varphi_e \in \mathfrak{I}(G)$.
De plus, on vérifie que pour $a, b \in G$, $\varphi_a \circ \varphi_b = \varphi_{ab} \in \mathfrak{I}(G)$.
Enfin, on a vu à la question précédente que pour $a \in G$, $\varphi_a^{-1} = \varphi_{a^{-1}} \in \mathfrak{I}(G)$.
Par conséquent, $\mathfrak{I}(G)$ est un sous-groupe de $(\mathcal{A}ut(G), \circ)$.

3. On a montré à la question précédente que $\varphi_a \circ \varphi_b = \varphi_{ab}$ i.e. $\varphi(a) \circ \varphi(b) = \varphi(ab)$. Ainsi φ est un morphisme de groupes.

SOLUTION 17.

Si f est un automorphisme, c'est en particulier un morphisme. Donc pour tous $a, b \in G$, $f(ab) = f(a)f(b)$ i.e.
$$(ab)^{-1} = a^{-1}b^{-1} \iff (ab)^{-1} = (ba)^{-1} \iff ab = ba$$
Ainsi G est commutatif.
Réciproquement si G est commutatif, le raisonnement inverse nous montre que f est un morphisme. De plus, $f \circ f = \mathrm{Id}_G$, donc f est bijectif (d'application réciproque lui-même). f est bien un automorphisme.

SOLUTION 18.

Soit $r \in \mathbb{Q}$. Montrons que $f(r) = 0$. Soit $n \in \mathbb{N}^*$. On a
$$f(r) = f\left(n\frac{r}{n}\right) = nf\left(\frac{r}{n}\right)$$
Or $f(r)$, n et $f\left(\frac{r}{n}\right)$ sont des entiers. Donc $f(r)$ est divisible par n.
Ainsi $f(r)$ est divisible par tout entier $n \in \mathbb{N}^*$. On a forcément $f(r) = 0$. En conclusion, le seul morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est le morphisme nul.

SOLUTION 19.

Il est clair que les homothéties sont bien des endomorphismes de $(\mathbb{R}, +)$.
Soit maintenant f est un endomorphisme de $(\mathbb{R}, +)$. On a donc pour tous $x, y \in \mathbb{R}$, $f(x+y) = f(x) + f(y)$. On montre par récurrence que $f(nx) = nf(x)$ pour tout $x \in \mathbb{R}$ et pour tout $n \in \mathbb{N}$ puis pour tout $n \in \mathbb{Z}$ en passant à l'opposé. Soit maintenant r un rationnel. Il existe donc deux entiers p et q avec $q \neq 0$ tels que $r = \frac{p}{q}$. On a d'une part
$$f(p) = f(qr) = qf(r)$$
et d'autre part
$$f(p) = pf(1)$$
Donc $f(r) = rf(1)$. Posons donc $\lambda = f(1)$. Soit maintenant $x \in \mathbb{R}$. On sait que x est limite d'une suite de rationnels (r_n). Or f étant continue sur $\mathbb{R}$ et donc en x, la suite $(f(r_n))$ tend vers $f(x)$. Or $f(r_n) = \lambda r_n$ pour tout $n \in \mathbb{N}$.Par passage à la limite, on a donc $f(x) = \lambda x$.

Solution 20.

Évidemment 0 et 1 sont dans $\mathbb{D}$.
Soient $k, \ell \in \mathbb{Z}$ et $n, m \in \mathbb{N}$.Stabilité par produit.

$$\frac{k}{10^n} \times \frac{\ell}{10^m} = \frac{k\ell}{10^{n+m}} \in \mathbb{D}.$$

Stabilité par addition. On peut supposer $n \geqslant m$. Alors

$$\frac{k}{10^n} + \frac{\ell}{10^m} = \frac{k + 10^{n-m}\ell}{10^n} \in \mathbb{D}.$$

Ce n'est pas un sous-corps car $\dfrac{3}{10^0}$ ne possède pas d'inverse dans $\mathbb{D}$.

Solution 21.

Soit A un anneau commutatif intègre fini. Pour montrer que A est un corps, il suffit de montrer que tout élément non nul est inversible. Soit donc $a \in A^*$. Posons $\varphi : \left\{ \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array} \right.$. Soit $x, y \in A$ tels que $\varphi(x) = \varphi(y)$ i.e. $a(x - y) = 0$. Par intégrité de A, on a donc $x = y$. Ainsi φ est injective. Comme l'ensemble de départ et l'ensemble d'arrivée de φ ont le *même nombre fini* d'éléments, φ est bijective donc surjective. En particulier, il existe $x \in A$ tel que $\varphi(x) = 1$. Ainsi a admet x pour inverse.

Solution 22.

1. On vérifie que $\mathbb{Z}[i]$ est un sous anneau de $\mathbb{C}$.
   - $1 = 1 + 0i \in \mathbb{Z}[i]$
   - $\forall z, z' \in \mathbb{Z}, z - z' \in \mathbb{Z}[i]$,
   - $\forall z, z' \in \mathbb{Z}, zz' \in \mathbb{Z}[i]$.
2. Posons $N(z) = z\bar{z}$. Pour $z = a + ib \in \mathbb{Z}[i]$, $N(z) = a^2 + b^2 \in \mathbb{N}$. Pour $z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$. Soit $z \in (\mathbb{Z}[i])^*$. Il existe donc $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. On a alors $N(z)N(z') = 1$ et $N(z), N(z') \in \mathbb{N}$. Ceci implique que $N(z) = 1$. Si $z = a + ib$, on a donc $a^2 + b^2 = 1$. Les seuls couples d'entiers (a, b) possibles sont $(1, 0)$, $(-1, 0)$, $(0, 1)$ et $(0, -1)$, ce qui correspond à $z = \pm 1$ ou $z = \pm i$. Réciproquement on vérifie que ces éléments sont bien inversibles dans $\mathbb{Z}[i]$.

Solution 23.

1. Supposons $x \times y$ nilpotent. Il existe donc $n \in \mathbb{N}$ tel que $(x \times y)^n = 0$. Alors

   $$(y \times x)^{n+1} = y \times (x \times y)^n \times x = y \times 0_A \times x = 0_A$$

   de sorte que $y \times x$ est nilpotent.
2. Supposons que x et y commutent et que l'un d'entre eux est nilpotent. Puisque x et y commutent, on peut supposer x nilpotent. Il existe donc $n \in \mathbb{N}$ tels que $x^n = 0$. Comme x et y commutent,

   $$(x \times y)^n = x^n \times y^n = 0_A \times y^n = 0_A$$

   de sorte que $x \times y$ est nilpotent.

3. Supposons x et y nilpotents. Il existe donc $(n,p) \in \mathbb{N}^2$ tel que $x^n = 0_A$ et $y^p = 0_A$. Posons $q = n+p$. Alors

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

Soit alors $k \in [\![0, q]\!]$.

- Si $k \geqslant n$, alors $x^k = 0_A$ puis $\binom{q}{k} x^k \times y^{q-k} = 0_A$.
- Si $k < n$, alors $q-k > q-n = p$ donc $y^k = 0_A$ puis $\binom{q}{k} x^k \times y^{q-k} = 0_A$.

Ainsi $(x+y)^q = 0_A$ de sorte que $x+y$ est bien nilpotent.

4. Supposons x nilpotent. Il existe donc $n \in \mathbb{N}$ tel que $x^n = 0_A$. On écrit :

$$1_A = 1_A^n - x^n = (1_A - x) \times \left(\sum_{k=0}^{n-1} x^k\right) = \left(\sum_{k=0}^{n-1} x^k\right) \times (1_A - x)$$

Ainsi $1_A - x$ est inversible d'inverse $\sum_{k=0}^{n-1} x^k$.

Solution 24.

1. Soit $x \in A$. D'une part,

$$(x+1)^2 = x^2 + 2x + 1 = 3x + 1$$

D'autre part,

$$(x+1)^2 = x + 1$$

D'où $2x = 0$.

2. Soient $x, y \in A$. D'une part,

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

D'autre part,

$$(x+y)^2 = x + y$$

D'où $xy + yx = 0$. Donc $2xy + yx = xy$. Or $2xy = 0$ d'après la question précédente donc $yx = xy$. Ceci étant valable pour tous $x, y \in A$, l'anneau est commutatif.

Solution 25.

1. On peut par exemple utiliser les fonctions indicatrices pour montrer l'associativité de Δ. Soit $(A, B, C) \in \mathcal{P}(E)^3$. On montre que :

$$\mathbb{1}_{(A\Delta B)\Delta C} = \mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C - 2(\mathbb{1}_A\mathbb{1}_B + \mathbb{1}_A\mathbb{1}_C + \mathbb{1}_B\mathbb{1}_C) + 4\mathbb{1}_A\mathbb{1}_B\mathbb{1}_C$$

La dernière expression est invariante par permutation de A, B et C. Par conséquent,

$$\mathbb{1}_{(A\Delta B)\Delta C} = \mathbb{1}_{(B\Delta C)\Delta A}$$

Finalement, $(A\Delta B)\Delta C = (B\Delta C)\Delta A = A\Delta(B\Delta C)$. La loi Δ possède un élément neutre en la personne de l'ensemble vide $\varnothing$. Tout élément $A \in \mathcal{P}(E)$ possède un inverse pour Δ à savoir $\overline{A}$. La loi Δ est clairement commutative. En conclusion, $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.
L'intersection $\cap$ est clairement associative. Elle possède un élément neutre, à savoir E. On peut à nouveau montrer la distributivité de $\cap$ sur Δ en utilisant les fonctions indicatrices. Enfin, $\cap$ est commutative donc $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

2. Soit $A \in \mathcal{P}(E)$. A est inversible pour $\cap$ *si et seulement si* il existe $B \in \mathcal{P}(E)$ tel que $A \cap B = E$. On a donc nécessairement $A = E$. Or E possède un inverse pour $\cap$, à savoir E lui-même. On en déduit que le seul élément inversible pour $\cap$ est E.

3. Pour tout $A \in \mathcal{P}(E)$, $A \cap \overline{A} = \varnothing$. Comme E est non vide, $\mathcal{P}(E)$ possède des éléments A non nuls (i.e. des parties non vides de E). Donc l'anneau $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre.

Solution 26.

On montre que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.

- $1 = 1 + 0\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- Soient $x = a + b\sqrt{3}$ et $x' = a' + b'\sqrt{3}$ des éléments de $\mathbb{Q}[\sqrt{3}]$. Alors $x - x' = (a - a') + (b - b')\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- On a également $xx' = (aa' + 3bb') + (ab' + a'b)\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$.
- Supposons $x \neq 0$. On a alors
$$\frac{1}{x} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$$
Mais il aurait fallu montrer auparavant que $a^2 - 3b^2 \neq 0$. Supposons $a^2 - 3b^2 = 0$. En notant $a = \frac{p}{q}$ et $b = \frac{r}{s}$ avec p, q, r, s entiers, on a donc $p^2s^2 - 3r^2q^2 = 0$. Il existe donc des entiers m et n tels que $m^2 = 3n^2$. Quitte à les diviser par leur pgcd, on peut les supposer premiers entre eux. On a alors toujours la relation $m^2 = 3n^2$. En particulier, 3 divise m^2. Mais 3 étant premier 3 divise m. Il existe donc $k \in \mathbb{Z}$ tel que $m = 3k$. On en déduit $9k^2 = 3n^2$ i.e. $3k^2 = n^2$ donc 3 divise n^2 et donc n. Ceci contredit le fait que m et n sont premiers entre eux. Finalement $a^2 - 3b^2 \neq 0$.

Solution 27.

1. Soit $(x, y) \in A^2$ tel que $\varphi(x) = \varphi(y)$. Alors $ax = ay$ i.e. $a(x - y) = 0$. Puisque A est intègre et que $a \neq 0$, $x - y = 0$ i.e. $x = y$. Ainsi φ est injective. Puisque A est de cardinal fini et que φ est une application de A dans A, φ est également bijective.

2. Soit a un élément non nul de A. Puisque l'application φ définie à la question précédente est bijective, elle est a fortiori surjective. Il existe donc $b \in A$ tel que $\varphi(b) = 1$ i.e. $ab = 1$. Ceci prouve que a est inversible.
Ainsi tout élément non nul de A est inversible : A est un corps.

Solution 28.

1. Comme f est un morphisme de corps, on a $f(1) = 1$. De plus, pour $n \in \mathbb{Z}$,
$$f(n) = f(n1) = nf(1) = n1 = n$$
Soit $r = \dfrac{p}{q} \in \mathbb{Q}$. Alors $f(p) = f(qr) = qf(r)$. Or $p \in \mathbb{Z}$ donc $f(p) = p$. Par conséquent, $f(r) = \dfrac{p}{q} = r$.

2. Soit $x \geqslant 0$. Il existe $a \in \mathbb{R}$ tel que $x = a^2$. Alors $f(x) = f(a^2) = f(a)^2 \geqslant 0$.
Soit $x \leqslant y$. Alors $f(y) - f(x) = f(y - x) \geqslant 0$ car $y - x \geqslant 0$. Donc $f(x) \leqslant f(y)$. Ainsi f est croissant.

3. Soit $x \in \mathbb{R}$. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe deux suites de rationnels (r_n) et $r'_n)$ convergeant respectivement vers x par valeurs inférieures et par valeurs supérieures. Ainsi, $\forall n \in \mathbb{N}$,
$$r_n \leqslant x \leqslant r'_n$$
Par croissance de f et en utilisant la première question,
$$r_n = f(r_n) \leqslant f(x) \leqslant f(r'_n) = r'_n$$
Par passage à la limite, on obtient $f(x) = x$. Ceci étant valable pour tout $x \in \mathbb{R}$, $f = \mathrm{Id}_{\mathbb{R}}$.

Solution 29.

1. Tout d'abord $1 = 1 + 0\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$.
Soient $z_1 = a_1 + b_1\sqrt{3}$ avec $(a_1, b_1) \in \mathbb{Z}^2$ et $z_2 = a_2 + b_2\sqrt{3}$ avec $(a_2, b_2) \in \mathbb{Z}^2$. Alors

$$z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

et

$$z_1 z_2 = (a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$

$\mathbb{Z}[\sqrt{3}]$ est donc un sous-anneau de $\mathbb{R}$.

2. **a.** On reprend les notations de l'énoncé. On a donc $p^2 = 3q^2$. Ainsi 3 divise p^2. Comme 3 est premier, 3 divise p. Il existe donc $k \in \mathbb{Z}$ tel que $p = 3k$. On a alors $9k^2 = 3q^2$ i.e. $3k^3 = q^2$. On prouve comme précédement que 3 divise q. Ainsi p et q ont un facteur premier commun, ce qui contredit $p \wedge q = 1$. En conclusion, $\sqrt{3} \notin \mathbb{Q}$.

   b. On vérifie aisément que pour tout $(a, b, c, d) \in \mathbb{Z}^4$, $f((a, b) + (c, d)) = f((a, b)) + f((c, d))$, ce qui prouve que f est bien un morphisme de groupes.
Soit $(a, b) \in \operatorname{Ker} f$. On a donc $a + b\sqrt{3} = 0$. Si on avait $b \neq 0$, $\sqrt{3}$ serait rationnel, ce qui n'est pas. Ainsi $b = 0$ puis $a = 0$. On a donc montré que $\operatorname{Ker} f = \{(0, 0)\}$. Ainsi f est injective. f est surjective par définition de $\mathbb{Z}[\sqrt{3}]$.

3. **a.** Puisque $1 = 1 + 0\sqrt{3}$, $g(1) = \tilde{1} = 1 - 0\sqrt{3} = 1$.
Soient $z_1 = a_1 + b_1\sqrt{3}$ avec $(a_1, b_1) \in \mathbb{Z}^2$ et $z_2 = a_2 + b_2\sqrt{3}$ avec $(a_2, b_2) \in \mathbb{Z}^2$. Alors $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{3}$ et donc

$$g(z_1 + z_2) = \widetilde{z_1 + z_2} = (a_1 + a_2) - (b_1 + b_2)\sqrt{3} = (a_1 - b_1\sqrt{3}) + (a_2 - b_2\sqrt{3}) = \tilde{z}_1 + \tilde{z}_2 = g(z_1) + g(z_2)$$

   De plus, $z_1 z_2 = (a_1 a_2 + 3b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{3}$ donc

$$g(z_1 z_2) = \widetilde{z_1 z_2} = (a_1 a_2 + 3b_1 b_2) - (a_1 b_2 + a_2 b_1)\sqrt{3} = (a_1 - b_1\sqrt{3})(a_2 - b_2\sqrt{3}) = \tilde{z}_1 \tilde{z}_2 = g(z_1)g(z_2)$$

   Ainsi f est un endomorphisme d'anneau.
De plus, $f \circ f = \operatorname{Id}_{\mathbb{Z}[\sqrt{3}]}$ donc f est bijectif : c'est un automorphisme d'anneau.

   b. On a $N(xy) = xy\widetilde{xy} = x\tilde{x}y\tilde{y} = N(x)N(y)$.

   c. Si x est inversible, il existe $y \in \mathbb{Z}[\sqrt{3}]$ tel que $xy = 1$. On a donc $N(x)N(y) = N(1) = 1$. Or $N(x)$ et $N(y)$ sont des entiers donc $N(x) = \pm 1$.
Si $N(x) = 1$, alors $x\tilde{x} = 1$, ce qui prouve que x est inversible d'inverse $\tilde{x}$. Si $N(x) = -1$, alors $x(-\tilde{x}) = 1$, ce qui prouve que x est inversible d'inverse $-\tilde{x}$.