Chapitre 11

Structures algébriques

11.1 Lois de composition

► Solution 11.1.1

1. Dans (H), on pose $x = v = e$ et $y = u = f$.
   On obtient donc $(e \star f) \bullet (f \star e) = (e \bullet f) \star (f \bullet e)$.
   Avec les définitions de e et f, on trouve $f \bullet f = e \star e$, puis $f = e$.

2. Dans (H), on pose $y = u = e$, et on laisse x et v quelconques.
   $\forall (x, v) \in E^2, (x \star e) \bullet (e \star v) = (x \bullet e) \star (e \bullet v)$.
   Sachant que e est neutre pour les deux lois, on en déduit :
   $\forall (x, v) \in E^2, x \bullet v = x \star v$: Les lois $\star$ et $\bullet$ sont donc identiques.

3. On a maintenant : $\forall (x, y, u, v) \in E^4$, $(x \star y) \star (u \star v) = (x \star u) \star (y \star v)$ (K).
   Dans cette égalité, on choisit $y = e$, les trois autres étant quelconques.
   On en déduit : $\forall (x, u, v) \in E^3$, $(x \star e) \star (u \star v) = (x \star u) \star (e \star v)$, c'est-à-dire :
   $\forall (x, u, v) \in E^3$, $x \star (u \star v) = (x \star u) \star v$: la loi $\star$ est associative.
   Enfin, dans (K), on pose $x = v = e$, les deux autres étant quelconques.
   On en déduit : $\forall (y, u) \in E^2$, $(e \star y) \star (u \star e) = (e \star u) \star (y \star e)$, c'est-à-dire :
   $\forall (y, u) \in E^2, y \star u = u \star y$: la loi $\star$ est commutative.

► Solution 11.1.2

Pour tous réels x, y, z, on a :

$$\begin{aligned}(x \star y) \star z &= [kxy + k'(x + y)] \star z \\ &= k\,[kxy + k'(x + y)]\, z + k'\,[kxy + k'(x + y) + z] \\ &= k^2xyz + kk'(xy + xz + yz) + k'\,[k'(x + y) + z]\end{aligned}$$

On remarque que la loi $\star$ est commutative.

On peut donc écrire $x \star (y \star z) = (y \star z) \star x = (z \star y) \star x$.

On obtient donc $x \star (y \star z)$ en échangeant x et z dans l'expression de $(x \star y) \star z$.

Ainsi $x \star (y \star z) = k^2zyx + kk'(zy + zx + yx) + k'\,[k'(z + y) + x]$.

On en déduit : $(x \star y) \star z - x \star (y \star z) = k'(k' - 1)(x - z)$.

La loi $\star$ est associative $\Leftrightarrow$ cette dernière quantité est nulle pour tous x, z.

Conclusion : la loi $\star$ est associative $\Leftrightarrow$ $k' \in \{0, 1\}$.

▶ Solution 11.1.3

1. La symétrie de la définition prouve que la loi $\star$ est commutative.
2. Pour toute partie A de E, on a : $A \cap \emptyset = \emptyset \Rightarrow A \star \emptyset = A \cup \emptyset = A$.
   Autrement dit, $\emptyset$ est neutre pour la loi $\star$.
3. On remarque que pour toutes parties A, B de E, on a $A \star B \supset A \cup B$.
   On ne peut donc avoir $A \star B = \emptyset$ que si $A = B = \emptyset$.
   $\emptyset$ est donc le seul élément de $\mathcal{P}(E)$ à avoir un inverse (il est son propre inverse.)
4. Soient A, B, C trois parties quelconques de E.
   - Si A, B, C sont deux à deux disjointes, alors
     $$\begin{aligned} A \star (B \star C) &= A \star (B \cup C) = A \cup (B \cup C) \\ &= (A \cup B) \cup C = (A \star B) \cup C = (A \star B) \star C \end{aligned}$$
   - Si $A \cap B \neq \emptyset$ alors $A \cap (B \star C) \neq \emptyset$ car $B \star C \supset B$.
     On en déduit : $A \star (B \star C) = E$ et $(A \star B) \star C = E \star C = E$.
   - De même, si $A \cap C \neq \emptyset$ ou si $B \cap C \neq \emptyset$ alors $A \star (B \star C) = (A \star B) \star C = E$.
   - Dans tous les cas, on a donc $A \star (B \star C) = (A \star B) \star C$: la loi $\star$ est associative.

▶ Solution 11.1.4

1. La symétrie de la définition prouve que la loi $\star$ est commutative.
2. Pour tout $A \subset E$, on a : $A \star E = (A \cap E) \cup (\overline{A} \cap \overline{E}) = A \cup (\overline{A} \cap \emptyset) = A \cup \emptyset = A$.
   Autrement dit, E est neutre pour la loi $\star$.
3. Soit A une partie de E. On constate que $A \star A = (A \cap A) \cup (\overline{A} \cap \overline{A}) = A \cup \overline{A} = E$.
   Tout élément de A est donc son propre symétrique pour la loi $\star$.
4. On remarque que pour toutes parties X, Y de E, on a :
   $$\begin{aligned} X \star Y &= (X \cap Y) \cup (\overline{X} \cap \overline{Y}) = (X \cup \overline{X}) \cap (X \cup \overline{Y}) \cap (Y \cup \overline{X}) \cap (Y \cup \overline{Y}) \\ &= E \cap (X \cup \overline{Y}) \cap (Y \cup \overline{X}) \cap E = (X \cup \overline{Y}) \cap (Y \cup \overline{X}) \end{aligned}$$
   Soient A, B, C trois parties quelconques de E.
   On utilise les deux définitions possibles de $\star$ pour évaluer $(A \star B) \star C$. On trouve :
   $$\begin{aligned} (A \star B) \star C &= \Big[\Big[(A \cup \overline{B}) \cap (\overline{A} \cup B)\Big] \cup \overline{C}\Big] \cap \Big[\overline{(A \cap B) \cup (\overline{A} \cap \overline{B})} \cup C\Big] \\ &= (A \cup \overline{B} \cup \overline{C}) \cap (\overline{A} \cup B \cup \overline{C}) \cap \Big[\Big[(\overline{A} \cup \overline{B}) \cap (A \cup B)\Big] \cup C\Big] \\ &= (A \cup \overline{B} \cup \overline{C}) \cap (\overline{A} \cup B \cup \overline{C}) \cap (\overline{A} \cup \overline{B} \cup C) \cap (A \cup B \cup C) \end{aligned}$$
   Puisque la loi $\star$ est commutative, on a $A \star (B \star C) = A \star (C \star B) = (C \star B) \star A$.
   Pour obtenir $A \star (B \star C)$, il suffit donc d'échanger A et C dans l'expression de $(A \star B) \star C$.
   Or on voit que cette expression est invariante dans cet échange.
   On en déduit $A \star (B \star C) = (A \star B) \star C$: la loi $\star$ est associative.

▶ Solution 11.1.5

1. Soit a un élément régulier de E.
   Par définition, pour tous x, y de E, on a : $\begin{cases} x \star a = y \star a \Rightarrow x = y \\ a \star x = a \star y \Rightarrow x = y \end{cases}$
   Les applications $\begin{cases} d_a : x \mapsto x \star a \\ g_a : x \mapsto a \star x \end{cases}$ sont donc injectives de E dans E.
   Or E est un ensemble fini. Ces deux applications sont donc bijectives.
   En particulier, il existe a' dans E tel que $d_a(a') = e$, c'est-à-dire tel que $a' \star a = e$.
   De même, il existe a'' dans E tel que $g_a(a'') = e$, c'est-à-dire tel que $a \star a'' = e$.

On peut alors écrire, en utilisant l'associativité :

$$\begin{cases} a' \star (a \star a'') = a' \star e = a' \\ a' \star (a \star a'') = (a' \star a) \star a'' = e \star a'' = a'' \end{cases}$$

Ainsi $a' = a''$ donc $a' \star a = a \star a' = e$.
Conclusion : a' est l'inverse de a pour la loi $\star$.

2. On se place par exemple dans $\mathbb{Z}$ muni de la multiplication.
Cette loi est associative et tout élément non nul est régulier (simplifiable).
Pourtant seuls 1 et -1 possèdent un inverse dans $\mathbb{Z}$ pour cette loi.

► Solution 11.1.6

L'hypothèse sur a signifie : $\forall\, x \in E, \exists\, y \in E, aya = x$.
En particulier, il existe un élément b de E tel que $aba = a$.
Soit x un élément quelconque de E.
Toujours par hypothèse, il existe y dans E tel que $aya = x$.
En utilisant l'associativité de la loi, on constate alors que :

$$\begin{cases} x(ba) = (aya)(ba) = (ay)(aba) = (ay)a = x \\ (ab)x = (ab)(aya) = (aba)(ya) = a(ya) = x \end{cases}$$

Autrement dit, ab est neutre "à gauche" et ba est neutre "à droite".
En particulier $(ab)(ba) = ab$ et $(ab)(ba) = ba$.
Conclusion : l'élément $e = ab = ba$ est neutre dans E.

► Solution 11.1.7

1. Par hypothèse, les applications $\begin{cases} g_a : x \mapsto a \star x \\ d_b : x \mapsto x \star b \end{cases}$ sont injectives.
Or E est un ensemble fini.
Ces deux applications sont donc bijectives.
En particulier, il existe e dans E tel que $g_a(e) = a$.
De même, il existe f dans E tel que $d_b(f) = b$.
Avec ces notations, on a donc $a \star e = a$ et $f \star b = b$.

2. Pour tout x de E, en utilisant l'associativité de la loi $\star$, on a :

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

On en déduit $e \star x = x$.
De la même manière :

$$(x \star f) \star b = x \star (f \star b) = x \star b$$

Donc $x \star f = x$.

3. Ce qui précède montre que e est neutre "à gauche" et f est neutre "à droite".
En particulier $e \star f = f$ (e neutre à gauche.)
De la même manière : $e \star f = e$ (f neutre à droite.)
Conclusion : l'élément $e = f$ est neutre dans E pour la loi $\star$.

▶ Solution 11.1.8

Soient $\mathcal{R}$, $\mathcal{S}$ et $\mathcal{T}$ trois relations sur E.

On pose $\mathcal{U} = \mathcal{R} \star \mathcal{S}$ et $\mathcal{V} = \mathcal{S} \star \mathcal{T}$.

Il faut montrer $(\mathcal{R} \star \mathcal{S}) \star \mathcal{T} = \mathcal{R} \star (\mathcal{S} \star \mathcal{T})$, c'est-à-dire $\mathcal{U} \star \mathcal{T} = \mathcal{R} \star \mathcal{V}$.

Soient a, b deux éléments quelconques de E.

Il faut prouver l'équivalence $a\,(\mathcal{U} \star \mathcal{T})\,b \Leftrightarrow a\,(\mathcal{R} \star \mathcal{V})\,b$. Or :

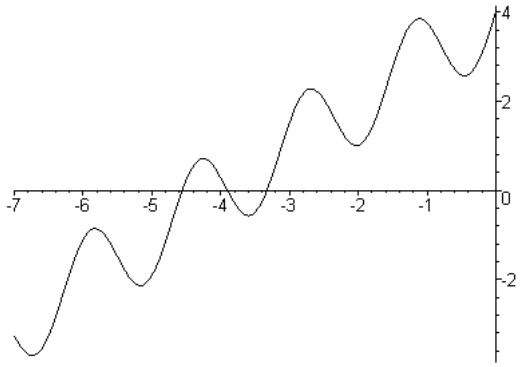
$$\begin{aligned} a\,(\mathcal{U} \star \mathcal{T})\,b &\Leftrightarrow \exists\, x \in E, a\,\mathcal{U}\,x \text{ et } x\,\mathcal{T}\,b \\ &\Leftrightarrow \exists\, x \in E, \exists\, y \in E, a\,\mathcal{R}\,y, y\,\mathcal{S}\,x, x\,\mathcal{T}\,b \\ &\Leftrightarrow \exists\, y \in E, a\,\mathcal{R}\,y, y\,\mathcal{V}\,b \\ &\Leftrightarrow a\,(\mathcal{R} \star \mathcal{V})\,b \end{aligned}$$

Conclusion : la loi $\star$ est associative.

Remarque : la relation "égalité" est neutre pour la loi $\star$.

▶ Solution 11.1.9

1. Par symétrie de la définition, la loi $\star$ est évidemment commutative.
   D'autre part, il est clair que 0 est neutre : $\forall\, x \in E, x \star 0 = x$.
2. Chercher les inverses éventuels d'un réel a, c'est résoudre l'équation $a \star x = 0$.
   Mais $a \star x = 0 \Leftrightarrow a + x + \sin(ax) = 0$.
   Posons par exemple $a = 4$, et soit f l'application définie par $f(x) = 4 + x + \sin(4x)$.
   Voici la courbe représentative de f :



   Graphiquement, on voit que f possède trois racines distinctes $\alpha < \beta < \gamma$.
   Cela signifie que α, β, γ sont trois inverses de $a = 4$. Plus précisément :
   - $f(-\frac{3}{2}\pi) = 4 - \frac{3}{2}\pi \approx 0 - .712388981 < 0$
   - $f(-\frac{4}{3}\pi) = 4 - \frac{4}{3}\pi + \frac{1}{2}\sqrt{3} \approx 0.6772352000 > 0$
   - $f(-\frac{7}{6}\pi) = 4 - \frac{7}{6}\pi - \frac{1}{2}\sqrt{3} \approx -0.5312168350 < 0$
   - $f(-\pi) = 4 - \pi \approx 0.858407346 > 0$.

   On en déduit $-\frac{3}{2}\pi < \alpha < -\frac{4}{3}\pi < \beta < -\frac{7}{6}\pi < \gamma < -\pi$.
   On montre que : $\alpha \approx -4.562912597$, $\beta \approx -3.902602873$ et $\gamma \approx -3.326370012$.
3. On sait que si une loi sur E est associative et s'il y a un élément neutre, alors l'inverse d'un élément a, s'il existe, est unique.
   Rappelons la démonstration. Si a' et a'' sont deux inverses de a, on a :
   $a' \star (a \star a'') = (a' \star a) \star a''$ donc $a' \star e = e \star a''$ donc $a' = a''$.

Dans notre exemple, le fait que $a = 4$ ait plusieurs inverses montre que $\star$ n'est pas associative, mais cette "méthode" est évidemment une farce. Il est en effet bien plus rapide d'exhiber trois éléments x, y, z tels que $x \star (y \star z) \neq (x \star y) \star z$.

Posons par exemple $x = 2$, $y = \pi$ et $z = 1$. On constate que :

$$\begin{aligned} x \star (y \star z) &= 2 \star (\pi \star 1) = 2 \star (\pi + 1) \\ &= 3 + \pi + \sin(2(\pi + 1)) = 3 + \pi + \sin 2 \end{aligned}$$

D'autre part :

$$\begin{aligned} (x \star y) \star z &= (2 \star \pi) \star 1 = (2 + \pi) \star 1 \\ &= 3 + \pi + \sin((2 + \pi)1) = 3 + \pi - \sin 2 \neq x \star (y \star z) \end{aligned}$$

► Solution 11.1.10

1. Soit E un ensemble fini de cardinal $n \geqslant 1$.
   Une loi sur E est une application de $E \times E$ sur E.
   Or $\text{card}(E \times E) = n^2$. Il y a donc n^{n^2} possibilités.
   Par exemple il y a $5^{25} = 298023223876953125$ lois sur un ensemble à 5 éléments.

2. Posons $E = \{x_1, x_2, \ldots, x_n\}$. On définit une loi $\star$ commutative sur E en se donnant les $x_i \star x_j$ dans E avec $1 \leqslant i \leqslant j \leqslant n$.
   Comme il y a $\frac{n(n+1)}{2}$ tels couples (i, j), il y a $n^{\frac{n(n+1)}{2}}$ lois commutatives sur E.
   Il y a par exemple $5^{15} = 30517578125$ lois commutatives sur un ensemble à 5 éléments.

► Solution 11.1.11

1. On peut citer $E = \mathcal{P}(F)$ muni de la loi "réunion" ou de la loi "intersection".
   On peut également citer $E = \mathbb{Z}$ muni de la loi "pgcd" ou de la loi "ppcm"

2. – Pour tout x de E on a $x \star x = x$ c'est-à-dire $x \mathcal{R} x$: la relation $\mathcal{R}$ est réflexive.
   – Soient x, y dans E tels que $x \mathcal{R} y$ et $y \mathcal{R} x$. Alors $x \star y = y$ et $y \star x = x$.
   Or la loi $\star$ est commutative.
   On en déduit $x = y$: la relation $\mathcal{R}$ est antisymétrique.
   – Soient x, y, z dans E tels que $x \mathcal{R} y$ et $y \mathcal{R} z$.
   On a donc $x \star y = y$ et $y \star z = z$.
   La loi $\star$ étant associative, on en déduit

$$x \star z = x \star (y \star z) = (x \star y) \star z = y \star z = z$$

   Autrement dit $x \mathcal{R} z$: la relation $\mathcal{R}$ est transitive.
   – Conclusion : $\mathcal{R}$ est une relation d'ordre sur E

3. On montre tout d'abord que $x \star y$ est un majorant de $\{x, y\}$.
   Par symétrie, il suffit de vérifier que $x \mathcal{R} (x \star y)$.
   Cela résulte de $x \star x = x$. En effet : $x \star (x \star y) = (x \star x) \star y = x \star y$.
   Enfin soit z un majorant de x et de y, c'est-à-dire tel que $x \star z = z$ et $y \star z = z$.
   Il reste à montrer que z est un majorant de $x \star y$.
   En effet $(x \star y) \star z = x \star (y \star z) = x \star z = z$.
   Conclusion :
   Pour tous x, y dans E, $x \star y$ est la borne supérieure de $\{x, y\}$ pour la relation $\mathcal{R}$.

► Solution 11.1.12

1. Soient a, b deux éléments quelconques de E.
   La première partie de l'hypothèse donne $b \star a \leqslant b$ et $b \star a \leqslant a$.
   Avec $x = b \star a$, la deuxième hypothèse donne alors $b \star a \leqslant a \star b$.
   En échangeant les rôles de a et b, on a alors $a \star b \leqslant b \star a$ donc $a \star b = b \star a$.
   Conclusion : la loi $\star$ est commutative.

2. Soit a un élément de E.
   La première partie de l'hypothèse donne $a \star a \leqslant a$.
   Avec $x = a = b$, la deuxième hypothèse donne alors $a \leqslant a \star a$.
   Conclusion : pour tout a de E, on a : $a \star a = a$.

3. Soient a, b, c trois éléments quelconques de E, avec $a \leqslant b$.
   On sait que $a \star c \leqslant a \leqslant b$.
   D'autre part $a \star c \leqslant c$.
   Les inégalités $\begin{cases} a \star c \leqslant b \\ a \star c \leqslant c \end{cases}$ donnent alors $a \star c \leqslant b \star c$.

   Soient a, b, c, d quatre éléments quelconques de E, avec $\begin{cases} a \leqslant b \\ c \leqslant d \end{cases}$

   D'après ce qui précède, on a $\begin{cases} a \star c \leqslant b \star c \\ c \star b \leqslant d \star b \end{cases}$
   On en déduit $a \star c \leqslant b \star d$, ce qu'il fallait démontrer.

4. Soient a, b, c trois éléments quelconques de E.
   On a $(a \star b) \star c \leqslant a \star b \leqslant a$.
   De même on a les inégalités $(a \star b) \star c \leqslant b$.
   On a aussi $(a \star b) \star c \leqslant c$.
   Ainsi $\begin{cases} (a \star b) \star c \leqslant b \\ (a \star b) \star c \leqslant c \end{cases} \Rightarrow (a \star b) \star c \leqslant b \star c$.
   Les inégalités $\begin{cases} (a \star b) \star c \leqslant a \\ (a \star b) \star c \leqslant b \star c \end{cases}$ donnent finalement $(a \star b) \star c \leqslant a \star (b \star c)$.
   En utilisant ce résultat et la commutativité de la loi $\star$, on peut alors écrire :

$$a \star (b \star c) = (b \star c) \star a = (c \star b) \star a \leqslant c \star (b \star a) = (a \star b) \star c$$

   Finalement on voit que $a \star (b \star c) = (a \star b) \star c$: la loi $\star$ est associative.

▶ Solution 11.1.13

1. Soit a un élément de E pour lequel les applications g_a et d_a sont surjectives.
   Il existe donc e dans E tel que $d_a(e) = a$, c'est-à-dire $e \star a = a$.
   De même, il existe f dans E tel que $g_a(f) = a$, c'est-à-dire $a \star f = a$.
   Soit x un élément quelconque de E.
   Par hypothèse, il existe y, z dans E tels que $\begin{cases} d_a(y) = x \\ g_a(z) = x \end{cases}$ c'est-à-dire $\begin{cases} y \star a = x \\ a \star z = x \end{cases}$
   On en déduit : $x \star f = (y \star a) \star f = y \star (a \star f) = y \star a = x$.
   De même : $e \star x = e \star (a \star z) = (e \star a) \star z = a \star z = x$.
   Ainsi, pour tout x de E, on a $x \star f = x$ et $e \star x = x$.
   En particulier avec $x = e$ puis $x = f$ on trouve $e \star f = e$ puis $e \star f = f$.
   On a donc $e = f$, et $x \star e = e \star x = x$ pour tout x de E.
   L'élément e est donc le neutre.

2. On sait qu'il existe un élément neutre e dans E pour la loi $\star$.
   Soit a un élément quelconque de E.
   Puisque d_a est surjective, il existe a' dans E tel que $d_a(a') = e$ c'est-à-dire $a' \star a = e$.
   Puisque g_a est surjective, il existe a'' dans E tel que $g_a(a'') = e$ c'est-à-dire $a \star a'' = e$.
   On a alors $\begin{cases} a' \star (a \star a'') = a' \star e = a' \\ a' \star (a \star a'') = (a' \star a) \star a'' = e \star a'' = a'' \end{cases}$
   Ainsi l'élément $a' = a''$ vérifie $a' \star a = a \star a' = e$: il est l'inverse de a.
   Conclusion : tout élément de E possède un inverse pour la loi $\star$.

▶ Solution 11.1.14

Soit a un élément de E.
La suite de terme général a^n est à valeurs dans l'ensemble fini E.
Il existe donc nécessairement deux entiers p et $q > p$ tels $a^q = a^p$.
Posons $r = q - p > 0$. On a $a^p = a^{p+r}$.
On en déduit $\forall\, m \geqslant p, a^m = a^{m+r}$ (on a multiplié par a^{m-p}).
Autrement dit, la suite des a^n est r-périodique, à partir de a^p.
On peut donc écrire : $\forall\, m \geqslant p, \forall\, n \geqslant 0, a^{m+nr} = a^m$.
Si on choisit n tel que $nr \geqslant p$ puis $m = nr$, on en déduit : $a^{2m} = a^m$.
On a ainsi trouvé un élément $x = a^m$ tel que $x^2 = x$.

11.2 Groupes et sous-groupes

▶ Solution 11.2.1

1. L'hypothèse $(yx)^{-1} = y^{-1}x$ s'écrit $x^{-1}y^{-1} = y^{-1}x$.
   On obtient $yx^{-1} = xy$ en multipliant par y à droite et à gauche.
   On en déduit : $x^2y^2 = x(xy)y = x(yx^{-1})y = (xy)(x^{-1}y) = (xy)(xy)^{-1} = e$.
   Mais l'égalité $x^2y^2 = e$ signifie que $(x^2)^{-1} = y^2$, ce qu'il fallait prouver.
2. On trouve successivement :
   $$\begin{aligned} x^4 &= x^2x^2 = (y^2)^{-1}x^2 = y^{-1}(y^{-1}x)x = y^{-1}(x^{-1}y^{-1})x \\ &= (y^{-1}x^{-1})(y^{-1}x) = (xy)^{-1}(y^{-1}x) = (x^{-1}y)(y^{-1}x) = e \end{aligned}$$
   On a donc obtenu $x^4 = e$. Il en découle $y^4 = (y^2)^2 = (x^2)^{-2} = (x^4)^{-1} = e$.

▶ Solution 11.2.2

Dire que l'application $x \to x^{-1}$ est un morphisme, c'est dire que :

$$\forall\, (x, y) \in G^2, x^{-1}y^{-1} = (xy)^{-1} = y^{-1}x^{-1}$$

Mais pour tout a de G, l'application $a \mapsto a^{-1}$ est une permutation du groupe G.
On obtient donc une proposition équivalente si on remplace x^{-1} par x et y^{-1} par y :

$$\forall\, (x, y) \in G^2, xy = yx$$

Ainsi l'application $x \to x^{-1}$ est un morphisme $\Leftrightarrow$ la loi de G est commutative.

▶ Solution 11.2.3

– Puisque la loi $\star$ est commutative, il en est de même de la loi $\mathcal{T}$.
En effet, pour tous a, b de G : $a\mathcal{T}b = a \star b \star \alpha = b \star a \star \alpha = b\mathcal{T}a$.

– Pour tous a, b, c de E, on a : $a\mathcal{T}(b\mathcal{T}c) = a\mathcal{T}(b \star c \star \alpha) = a \star b \star c \star \alpha \star \alpha$.
De même : $(a\mathcal{T}b)\mathcal{T}c = (a \star b \star \alpha)\mathcal{T}c = a \star b \star \alpha \star c \star \alpha = a \star b \star c \star \alpha \star \alpha$.
La loi $\mathcal{T}$ est donc asscociative.

– On constate que α' est neutre pour la loi $\mathcal{T}$.
En effet, pour tout a de E : $a\mathcal{T}\alpha' = a \star \alpha \star \alpha' = a \star e = a$.

– Soit a un élément quelconque de G.
On constate que $b = a' \star \alpha' \star \alpha'$ est inverse de a pour la loi $\mathcal{T}$.
En effet $a\mathcal{T}b = a \star a' \star \alpha' \star \alpha' \star \alpha = e \star \alpha' \star e = \alpha'$.

– Conclusion : muni de la loi $\mathcal{T}$, l'ensemble G est un groupe abélien.

► Solution 11.2.4

Considérons l'application φ défini sur $\mathbb{R}$ par $\varphi(x) = x^{1/3}$.
Pour tous réels x, y on a : $(x+y)^{1/3} = x^{1/3} \star y^{1/3}$ c'est-à-dire $\varphi(x+y) = \varphi(x) \star \varphi(y)$.
L'application φ, qui est bijective, est donc un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}, \star)$.
On en déduit que $(\mathbb{R}, \star)$ est muni d'une structure de groupe commutatif.
Plus précisément, le neutre de $(\mathbb{R}, \star)$ est 0 et le symétrique de x pour la loi $\star$ est $-x$.

► Solution 11.2.5

– Soit a fixé dans G : il existe α, β dans G tels que $a = a\alpha = \beta a$.
Soit b quelconque dans G : il existe x, y dans G tels que $b = ax = ya$.
On en déduit : $\begin{cases} b\alpha = (ya)\alpha = y(a\alpha) = ya = b \\ \beta b = \beta(ax) = (\beta a)x = ax = b \end{cases}$
En particulier, en choisissant $b = \beta$ puis $b = \alpha$: $\beta\alpha = \beta = \alpha$.
Ainsi l'élément $e = \alpha = \beta$ vérifie $\forall\, b \in G, eb = be = b$: e est élément neutre.

– Soit a un élément de G. On sait qu'il existe u, v dans G tels que $e = ua = av$.
On a alors $u(av) = ue = u$ et $u(av) = (ua)v = ev = v$. Donc $u = v$.
L'élément $u = v$ vérifie donc $ua = au = e$: u est l'inverse de a.

– Conclusion : l'ensemble G est donc muni d'une structure de groupe.

► Solution 11.2.6

– Soit a dans G. Pour tous, x, y de G, on a : $y = \varphi_a(x) = axa^{-1} \Leftrightarrow x = a^{-1}ya = \varphi_{a^{-1}}(y)$.
Ainsi φ_a est une bijection de G et la bijection réciproque est $\varphi_{a^{-1}}$.

– Soit a dans G. Pour tous x, y de G, $\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_b(x)$.
Ainsi φ_a est un automorphisme du groupe G.

– Soient a, b deux éléments de G.
Pour tout x de G, $(\varphi_b \circ \varphi_a)(x) = \varphi_b(axa^{-1}) = b(axa^{-1})b^{-1} = (ba)x(ba)^{-1} = \varphi_{ba}(x)$.
Autrement dit $\varphi_b \circ \varphi_a = \varphi_{ba}$: l'application $\varphi : a \mapsto \varphi_a$ est donc un morphisme du groupe G dans le groupe $\mathrm{Aut}(G)$ des automorphismes de G.

– Le noyau de φ est formé des éléments a de G tels que $\varphi_a = \mathrm{id}_G$.
Or $\varphi_a = \mathrm{id}_G \Leftrightarrow \forall\, x \in G, x = axa^{-1} \Leftrightarrow \forall\, x \in G, xa = ax$.

Le noyau de φ est donc l'ensemble des éléments de G qui commutent avec tous les éléments de G (on parle du *centre* de G.)

Remarque : les automorphismes φ_a sont appelés *automorphismes intérieurs* de G.

▶ Solution 11.2.7

Rappelons que dans un groupe d'ordre n, on a $x^n = e$ pour tout x de G.

Par hypothèse, il existe deux entiers u et v tels que $un + vk = 1$ (identité de Bezout.)

Pour tout y de G, on a donc $y = y^{un+vk} = (y^n)^u(y^v)^k = (y^v)^k = x^k$ avec $x = y^v$.

Ainsi l'application $x \to x^k$ est surjective de G dans lui-même.

Comme G est un ensemble fini, c'est une permutation de G.

▶ Solution 11.2.8

Soit $G = \{e, a, b, c\}$ un groupe d'ordre 4, de neutre e.

Si on montre par exemple $ab = ba$, on aura prouvé que G est commutatif.

L'égalité $ab = b$ est impossible car elle impliquerait $a = e$ par simplification.

Il en est de même de l'égalité $ab = a$.

On a donc $ab \in \{e, c\}$, et de même $ba \in \{e, c\}$.

– Si $ab = e$ ou si $ba = e$, alors b est l'inverse de a. Il en découle $ba = ab = e$.

– Le seul cas restant est donc $ab = ba = c$.

Conclusion : G est un groupe abélien.

Remarque : à un isomorphisme près, il n'y a que deux groupes d'ordre 4, qu'on note $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ avec des notations classiques.

▶ Solution 11.2.9

La réponse est négative car la loi $\star$ n'est pas associative.

En effet : $x \star (y \star z) = x \star t = z$ et $(x \star y) \star z = t \star z = x$.

On vérifie cependant que e est élément neutre, et que tout élément de l'ensemble est inversible (car égal à son propre inverse.)

▶ Solution 11.2.10

On a $a^2b = a(ab) = a(ba^3) = (ab)a^3 = (ba^3)a^3 = b(a^5)a = ba$.

De même, on a les égalités :

$$\begin{aligned} ab^3 &= (ab)b^2 = (ba^3)b^2 = ba(a^2b)b = ba(ba)b = b(ab)ab \\ &= b(ba^3)ab = b^2a^2(a^2b) = b^2a^2(ba) = b^2(a^2b)a \\ &= b^2(ba)a = b^3a^2 \end{aligned}$$

▶ Solution 11.2.11

Remarque : Les parenthèses dans les hypothèses de l'énoncé sont rendues nécessaires par le fait qu'on ne sait pas si la loi multiplicative de E est associative.

En particulier, b^2b signifie $(bb)b$, qui peut être différent de $b(bb)$.

– La première hypothèse indique que l'application $a \mapsto a^2$ est constante.
Notons e cette constante et montrons que e est neutre pour la loi $\star$.
Remarquons que la loi $\star$ s'écrit maintenant : $a \star b = a(eb)$.

Les hypothèses deviennent donc : $\forall\,(a,b,c)\in E^3,\begin{cases} ae=a & (1)\\ e(bc)=cb & (2)\\ (ac)(bc)=ab & (3)\end{cases}$

On constate tout d'abord que $e^2e=e^2=e$

Pour tout élément a de G, on a donc : $a\star e=a(e^2e)=ae=a$.

De même, avec l'hypothèse (2) : $e\star a=e(ea)=ae=a$.

– Montrons que $\star$ est associative. Soient a,b,c trois éléments de G. On a :

$$\begin{aligned} a\star(b\star c) &= a\star(b(ec))=a\,(e\,(b(ec)))\\ &= a\,((ec)b) \quad \text{(hypothèse 2)}\end{aligned}$$

De même :

$$\begin{aligned} (a\star b)\star c) &= (a(eb))\,(ec)=(a(eb))\,((ec)e) \quad \text{(hypothèse 1)}\\ &= (a(eb))\,(((ec)b)\,(eb)) \quad \text{(hypothèse 3)}\\ &= a\,((ec)b) \quad \text{(hypothèse 3)}\end{aligned}$$

– Montrons que l'inverse d'un élément a de G pour la loi $\star$ est ea.

On a en effet :

$a\star(ea)=a\,(e(ea))=a(ae)=a(a)=e$

$(ea)\star a=(ea)(ea)=(ea)^2=e$

– La loi $\star$ est donc associative, il existe un neutre et tout élément possède un inverse : l'ensemble E muni de la loi $\star$ est donc un groupe.

– Inversement, soit $(G,\star)$ un groupe de neutre e (on note z^{-1} l'inverse de z.)

On définit une loi sur G en posant : $\forall\,(x,y)\in G, xy=x\star y^{-1}$.

On constate que, pour tous éléments a,b,c de G :

$$\begin{aligned} a^2 &= a\star a^{-1}=e=b^2\\ a(b^2) &= ae=a\star e^{-1}=a\star e=a\\ a^2(bc) &= e(bc)=e\star(bc)^{-1}=(bc)^{-1}=(b\star c^{-1})^{-1}=c\star b^{-1}=cb\\ (ac)(bc) &= (a\star c^{-1})\star\left(b\star c^{-1}\right)^{-1}=(a\star c^{-1})\star(c\star b^{-1})\\ &= a\star(c^{-1}\star c)\star b^{-1}=a\star e\star b^{-1}=a\star b^{-1}=ab\end{aligned}$$

Enfin, on a bien : $\forall\,(a,b)\in G^2,\ a(b^2b)=a(eb)=a(e\star b^{-1})=a(b^{-1})=a\star\left(b^{-1}\right)^{-1}=a\star b$.

▶ Solution 11.2.12

1. La loi $\star$ est visiblement commutative.

   Pour tous réels x,y,z, on a :

   $$(x\star y)\star z=(x+y-xy)+z-(x+y-xy)z=x+y+z-xy-xz-yz+xyz$$

   De même, en utilisant la commutativité :

   $$x\star(y\star z)=(z\star y)\star x=z+y+x-zy-zx-yx+zyx=(x\star y)\star z$$

   La loi $\star$ est donc associative. De plus il est clair que 0 est élément neutre.

   Soit x et x' deux réels. x' est inverse de x si et seulement si $x'\star x=0$.

   Or $x'\star x=0\ \Leftrightarrow\ x'(x-1)=x$, qui ne possède pas de solution x' si $x=1$.

   On en déduit que $(\mathbb{R},\star)$ n'est pas un groupe (1 n'a pas d'inverse.)

2. Remarquons que pour tous réels x et y, on a : $1-x\star y=1-x-y+xy=(1-x)(1-y)$.

   Il en découle que si $x\neq 1$ et $y\neq 1$ alors $x\star y\neq 1$.

Autrement dit $\mathbb{R}-\{1\}$ est stable pour la loi $\star$.
On note encore $\star$ la restriction de cette loi à $\mathbb{R}-\{1\}$.
Cette restriction est toujours associative et commutative, et 0 est encore élément neutre.
Un calcul précédent montre que pour tout $x \neq 1$: $x' \star x = 0 \Leftrightarrow x' = \dfrac{x}{x-1}$.
Cet élément x', qui est distinct de 1, est donc l'inverse de x dans $(\mathbb{R}-\{1\},\star)$.
Conclusion : $(\mathbb{R}-\{1\},\star)$ est un groupe abélien.
Remarque : on obtient une démonstration plus rapide en notant que l'égalité

$$\forall\, x,y \in \mathbb{R},\ 1-x\star y = 1-x-y+xy = (1-x)(1-y)$$

s'écrit (remplacer x par $1-x$ et y par $1-y$)

$$\forall\, x,y \in \mathbb{R},\ 1-(1-x)\star(1-y) = (1-(1-x))\,(1-(1-y)) = xy$$

ou encore $\varphi(xy) = \varphi(x)\star\varphi(y)$ avec $\varphi : t \mapsto 1-t$.
L'application φ, qui est bijective de $\mathbb{R}-\{1\}$ sur $\mathbb{R}^*$ est donc un isomorphisme de $(\mathbb{R}^*,\times)$ sur $(\mathbb{R}-\{1\},\star)$.
Ainsi $(\mathbb{R}-\{1\},\star)$ est un groupe abélien.

3. On sait qu'on a l'égalité $1-x\star y = (1-x)(1-y)$ c'est-à-dire $\varphi(x\star y) = \varphi(x)\varphi(y)$.
On en déduit $\varphi(x^{(n)}) = (\varphi(x))^n$ (récurrence évidente).
Autrement dit : $\forall\, x \in \mathbb{R}, \forall\, n \in \mathbb{N}, 1-x^{(n)} = (1-x)^n$.
Conclusion : $\forall\, x \in \mathbb{R}, \forall\, n \in \mathbb{N}, x^{(n)} = 1-(1-x)^n$.

▶ Solution 11.2.13

Remarquons que $x\star y$ est défini pour tous x,y de $]-1,1[$, car $1+xy>0$.
Il faut cependant vérifier que $x\star y$ est encore un élément de $]-1,1[$. Or :

$$\begin{cases} 1-x\star y = \dfrac{1+xy-x-y}{1+xy} = \dfrac{(1-x)(1-y)}{1+xy} > 0 \\ 1+x\star y = \dfrac{1+xy+x+y}{1+xy} = \dfrac{(1+x)(1+y)}{1+xy} > 0 \end{cases}$$

En en déduit l'encadrement : $-1 < x\star y < 1$.
Il est clair que la loi $\star$ est commutative et que 0 est élément neutre.
Soient x,y,z trois éléments de $]-1,1[$.

On a : $x\star(y\star z) = \dfrac{x+y\star z}{1+x(y\star z)} = \dfrac{x+\dfrac{y+z}{1+yz}}{1+x\dfrac{y+z}{1+yz}} = \dfrac{x+y+z+xyz}{1+xy+xz+yz}$.

En utilisant la commutativité, $(x\star y)\star z = z\star(y\star x)$.
or l'expression donnant $x\star(y\star z)$ est inchangée quand on permute x et z.
On en déduit que $x\star(y\star z) = (x\star y)\star z$: la loi $\star$ est associative.
Enfin, il est clair que l'inverse de tout x de $]-1,1[$ est $-x$.
Conclusion : $(]-1,1[,\star)$ est un groupe abélien.
Remarque :
On peut connaître l'application th (tangente hyperbolique), bijective de $\mathbb{R}$ sur $]-1,1[$.
On sait que pour tous réels x,y on a : $\operatorname{th}(x+y) = \dfrac{\operatorname{th}(x)+\operatorname{th}(y)}{1+\operatorname{th}(x)\operatorname{th}(y)} = \operatorname{th}(x)\star\operatorname{th}(y)$.
L'application th est donc un isomorphisme du groupe $(\mathbb{R},+)$ sur le groupe $(]-1,1[,\star)$.

▶ Solution 11.2.14

On a les égalités :
$ab^3 = (ab)b^2 = (b^4a)b^2 = b^4(ab)b = b^4(b^4a)b = b^2b^6(ab) = b^2(b^4a) = b^6a = a.$
On en déduit $b^3 = e$ après simplification par a (on est dans un groupe.)
Il en découle $ab = b^4a = b^3(ba) = ba.$
Autre méthode : l'hypothèse $ab = b^4a$ s'écrit $b = a^{-1}b^4a$ et donne
$b^3 = (a^{-1}b^4a)^3 = a^{-1}(b^4)^3a = a^{-1}(b^3)^4a = a^{-1}ea = a^{-1}a = e$

▶ Solution 11.2.15

Soient x et y deux éléments quelconques de G.
Il s'agit de prouver $x^{n-1}y = yx^{n-1}$.
Par hypothèse, il existe un élément z de G tel que $y = z^n$.
On a alors les égalités :

$$\begin{aligned} x^{n-1}y &= x^{-1}x^ny = x^{-1}x^nz^n \\ &= x^{-1}(xz)^n \quad \text{(en utilisant le morphisme } t \mapsto t^n\text{)} \\ &= x^{-1}x(zx)^{n-1}z = (zx)^{n-1}z = (zx)^nx^{-1} \\ &= z^nx^nx^{-1} \quad \text{(en utilisant encore le morphisme } t \mapsto t^n\text{)} \\ &= z^nx^{n-1} = yx^{n-1} \end{aligned}$$

Ce qui établit le résultat demandé.

▶ Solution 11.2.16

L'hypothèse dit que pour tout a de G, les applications $x \mapsto x \star a$ et $x \mapsto a \star x$ sont injectives.
Puisque G est fini ces applications sont donc bijectives.
On peut alors terminer la démonstration comme dans 4.2.5.

▶ Solution 11.2.17

Cet exercice peut être considéré comme une question de cours.
Soit a un élément de G, distinct du neutre e ($\text{card}(G) \geqslant 2$).
L'ensemble $(a) = \{a^n, n \in \mathbb{Z}\}$ des puissances entières de a est un sous-groupe de G.
On sait que l'ordre (le cardinal) d'un sous-groupe d'un groupe fini divise l'ordre de ce groupe.
On en déduit que l'ordre de (a) (qui est au moins égal à 2, car il contient $e = a^0$ et $a = a^1$) divise l'ordre p (premier) de G et est donc égal à p.
Ainsi $(a) = G$, ce qui signifie effectivement que G est cyclique (et qu'il est d'ailleurs engendré par chacun de ses éléments différent du neutre.)

▶ Solution 11.2.18

Soient x, y deux éléments de G. On a $e = (xy)^2 = xyxy$.
On multiplie cette égalité à gauche par x puis à droite par y.
On en déduit $x = x^2yxy = yxy$, puis $xy = yxy^2 = yx$: le groupe G est donc commutatif.

▶ Solution 11.2.19

Soient x, y deux éléments de G. On a $(xy)^2 = x^2y^2$ donc $xyxy = xxyy$.
On simplifie par x à gauche et on obtient : $yxy = xyy$.
On simplifie par y à droite et on obtient : $yx = xy$: le groupe G est donc commutatif.

▶ Solution 11.2.20

1. Cette question a déjà fait l'objet de l'exercice 4.2.18.

2. Il est clair que tout x de G appartient à $\overline{x}$: la relation $\mathcal{R}$ est réflexive.
   Soient x, y dans G tel que $y\,\mathcal{R}\,x$ c'est-à-dire $y = x$ ou $y = ax$.
   Si $y = ax$ alors $ay = a^2x = x$. Dans tous les cas, on a donc $x = y$ ou $x = ay$.
   Ainsi $y\,\mathcal{R}\,x \Leftrightarrow x\,\mathcal{R}\,y$: la relation $\mathcal{R}$ est symétrique.
   Soient x, y, z trois éléments de G tels que $x\,\mathcal{R}\,y$ et $y\,\mathcal{R}\,z$.
   On a donc ($x = y$ ou $x = ay$) et ($y = z$ ou $y = az$).
   Dans tous les cas, sachant que $a^2 = e$, on trouve $x = z$ ou $x = az$ c'est-à-dire $x\,\mathcal{R}\,z$.
   On en déduit que $\mathcal{R}$ est transitive. C'est donc une relation d'équivalence.

3. On sait que les différentes classes d'équivalence $\overline{x}$ forment une partition de G.
   Or chacune de ces classes est de cardinal 2 : en effet $a \neq e \Rightarrow x \neq ax$.
   Il s'ensuit que $\text{Card}(G)$ est pair et que $\text{Card}(H) = \dfrac{1}{2}\text{Card}(G)$.

4. Soient α et β deux éléments de H.
   Il existe donc x, y dans G tels que $\alpha = \overline{x} = \overline{x'}$ et $\beta = \overline{y} = \overline{y'}$ avec $x' = ax$ et $y' = ay$.
   On constate que les éléments xy, $x'y$, xy' et $x'y'$ sont en relation par $\mathcal{R}$.
   En effet chacun d'eux vaut xy ou axy (conséquence de la commutativité et de $a^2 = e$.)
   La définition $\alpha \star \beta = \overline{xy}$ ne dépend donc pas du choix de x dans α et y dans β.
   L'application $\varphi : x \mapsto \overline{x}$ est une surjection de G sur H.
   De plus elle vérifie : $\forall\,(x, y) \in G^2, \varphi(xy) = \varphi(x) \star \varphi(y)$.
   φ est donc un morphisme surjectif du groupe $(G, \cdot)$ sur $(H, \star)$.
   Il en découle que $(H, \star)$ est un groupe commutatif (résultat classique).
   Plus précisément, le neutre est $\overline{e} = \{e, a\}$ et le symétrique de $\overline{x}$ est $\overline{x^{-1}}$.
   Enfin on contaste que : $\forall\, x \in G, \overline{x} \star \overline{x} = \overline{x^2} = \overline{e}$ (le neutre de H).
   Le groupe H satisfait donc aux mêmes hypothèses que G (tout élément est *involutif*).

5. Si G est réduit à son neutre $\{e\}$, alors son cardinal est $1 = 2^0$.
   Sinon, avec les notations précédentes, $\text{Card}(G) = 2\text{Card}(H)$.
   Si H se réduit à son neutre, alors $\text{Card}(G) = 2$.
   Sinon on construit un groupe K à partir de H comme on a construit H à partir de G.
   Ce procédé peut continuer tant que le groupe obtenu est de cardinal $\geqslant 2$.
   Puisque les cardinaux diminuent de moitié à chaque étape, le procédé est fini.
   On forme donc une suite finie de groupes $G_0 = G, G_1, G_2, \ldots, G_{n-1}, G_n$ avec à chaque étape $\text{Card}(G_k) = 2\text{Card}(G_{k+1})$ et finalement $\text{Card}(G_n) = 1$.
   Il en découle $\text{Card}(G_n) = 2^n$.
   Le cardinal de G est donc bien une puissance de 2.

▶ Solution 11.2.21

Montrons que e est neutre dans G.
Pour cela, soit x dans G. Il faut prouver $ex = x$.
On sait qu'il existe x' tel que $xx' = e$.
De même, il existe x'' tel $x'x'' = e$.
On peut alors écrire : $ex = (ex)(\underbrace{x'x''}_{=e}) = e(\underbrace{xx'}_{=e})x'' = ex''$.
On en déduit : $x'(ex) = x'(ex'')$ puis $(x'e)x = (x'e)x''$ ou encore $x'x = x'x'' = e$.
Il en découle $x(x'x) = xe = e$ puis $(xx')x = e$ c'est-à-dire $ex = e$.

On voit donc que e est neutre dans G, et que x' est l'inverse de x car $x'x = xx' = e$.
Conclusion : G est muni d'une structure de groupe.

► Solution 11.2.22

Soient x, y deux éléments quelconques de G.
Par hypothèse, on a l'égalité $(xy)^{k+1} = x^{k+1}y^{k+1}$.
Mais cette égalité s'écrit aussi $x(yx)^k y = x(x^k y^k)y$.
On simplifie par x à gauche et par y à droite : $(yx)^k = x^k y^k$ donc $(yx)^k = (xy)^k$.
Le même raisonnement (remplacer k par $k-1$) conduit à $(yx)^{k-1} = (xy)^{k-1}$.
Par passage aux inverses, on en déduit $(yx)^{1-k} = (xy)^{1-k}$.
Par produit terme à terme les égalités $\begin{cases}(yx)^k = (xy)^k \\ (yx)^{1-k} = (xy)^{1-k}\end{cases}$ donnent $yx = xy$.
Le groupe G est donc abélien.

► Solution 11.2.23

Il suffit de montrer que l'inverse d'un élément x de H est encore dans H.
Puisque H est stable, la suite des puissances $(x^n)_{n\geqslant 0}$ est incluse dans H.
Mais puisque H est fini, l'application $n \mapsto x^n$ ne peut pas être injective.
Il existe donc deux entiers n, p, avec $p > n$, tels que $x^n = x^p$.
On simplifie par x^n (dans le groupe G) et on trouve $x^{p-n} = e$.
Il en découle que e est dans H et que x^{p-n-1} (qui est lui aussi dans H) est l'inverse de x.
Conclusion : H est un sous-groupe de G.

► Solution 11.2.24

1. Il est clair que chacune des applications f_k est une bijection de $(\mathbb{R} - \{0,1\})$ sur lui-même.
   On forme la table des $f_i \circ f_j$. La plupart des résultats ci-dessous sont évidents.

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

   On constate que G est stable pour la loi $\circ$.
   Enfin tout élément de G a un symétrique dans G. Plus précisément, les applications f_1, f_4, f_5 et f_6 sont involutives et sont donc leur propre inverse, alors que les applications f_2 et f_3 sont inverses l'une de l'autre.
   G est donc un sous-groupe du groupe des bijections de $\mathbb{R} - \{0,1\}$ dans lui-même.

2. Les sous-groupes de G sont nécessairement d'ordre 1, 2, 3 ou 6.
   Le seul sous-groupe d'ordre 1 est $\{f_1\}$.
   Le seul sous-groupe d'ordre 6 est G lui-même.
   Les sous-groupes d'ordre 2 sont $\{f_1, f_4\}$, $\{f_1, f_5\}$ et $\{f_1, f_6\}$.
   Le seul sous-groupe d'ordre 3 est $\{f_1, f_2, f_3 = f_2^2\}$.

► Solution 11.2.25

Il est évident que si $H \subset K$ ou $K \subset H$, alors $H \cup K$ est un sous-groupe de G.
Réciproquement, on suppose que $H \cup K$ est un sous-groupe de G.
Supposons de plus $H \not\subset K$. Alors on doit montrer $K \subset H$.
Par hypothèse il existe un élément a tel que $a \in H, a \notin K$.
Soit x un élément quelconque de K.
Puisque x et a sont dans le sous-groupe $H \cup K$, il en est de même de xa.
Or $xa \in K$ impliquerait $a = x^{-1}(xa) \in K$, ce qui n'est pas.
Ainsi $xa \in H$, ce qui prouve $x = (xa)a^{-1} \in H$.
On a donc l'inclusion $K \subset H$, ce qui achève la démonstration.

► Solution 11.2.26

– On suppose que HK est un sous-groupe de G. Soit x dans HK : x^{-1} est encore dans HK.
Ainsi $\exists\,(h,k) \in (H,K)$ tel que $x^{-1} = hk$. On a alors $x = (hk)^{-1} = k^{-1}h^{-1}$, donc $x \in KH$.
On a ainsi prouvé $HK \subset KH$.
De même soit y dans KH. On écrit $y = kh$ avec $k \in K$ et $h \in H$.
$y^{-1} = h^{-1}k^{-1}$ est dans le sous-groupe HK. Il en est donc de même de y.
Ainsi on a l'inclusion $KH \subset HK$ et finalement l'égalité $HK = KH$.

– Réciproquement on suppose que $HK = KH$. Montrons que HK est un sous-groupe de G.
Soient $a = h_1k_1$ et $b = h_2k_2$ dans HK ($h_1 \in H, h_2 \in H, k_1 \in K, k_2 \in K$).
On doit prouver que $b^{-1}a$ appartient encore à HK. Or $b^{-1}a = k_2^{-1}h_2^{-1}h_1k_1$.
L'élément k_2^{-1} est dans K et $h_2^{-1}h_1$ est dans H.
Puisque $KH = HK$, il existe donc h_3 dans H et k_3 dans K tels que $(k_2^{-1})(h_2^{-1}h_1) = h_3k_3$.
On peut donc écrire $b^{-1}a = h_3k_3k_1$, avec h_3 dans H et k_3k_1 dans K.
Il en découle que $b^{-1}a$ est dans HK. Ainsi HK est un sous-groupe de G.

► Solution 11.2.27

Tout d'abord $H \neq \emptyset$. Soient a et b deux éléments de H.
Il existe i, j dans I tels que $a \in H_i$ et $b \in H_j$. Soit $k \in I$ tel que $H_i \cup H_j \subset H_k$.
Puisque a et b sont dans le sous-groupe H_k, il en est de même de $b^{-1}a$.
Mais $b^{-1}a \in H_k \Rightarrow b^{-1}a \in H$: ainsi H est un sous-groupe de G.

► Solution 11.2.28

$\text{card}\,(H \cup K) = 2n - 1$. Il existe donc a dans $G \setminus (H \cup K)$ tel que $G = H \cup K \cup \{a\}$.
Soient x dans H et y dans K, distincts de e (donc distincts l'un de l'autre).
On ne peut avoir $xy \in H$, car il en découlerait $y = x^{-1}(xy) \in H$.
De même $xy \notin K$. On en déduit $xy = a$, et pour la même raison $yx = a$.
Pour tout élément x' de H, et avec le même y de K, on a alors $x'y = a$.
Ainsi $xy = x'y$ puis $x = x'$. $H - \{e\}$ est donc un singleton (idem pour K). Donc $n = 2$.
Si on note $H = \{e, x\}$ et $K = \{e, y\}$, on en déduit la table du groupe $G = \{e, a, x, y\}$:

$\star$	e	a	x	y
e	e	a	x	y
a	a	e	y	x
x	x	y	e	a
y	y	x	a	e

11.3 Structures d'anneau et de corps

▶ Solution 11.3.1

Tout d'abord C est non vide car il contient le neutre multiplicatif de A.

Soient a et b deux éléments de C, et x un élément quelconque de A.

On a $\begin{cases}(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)\\(a-b)x = ax - bx = xa - xb = x(a-b)\end{cases}$

Cela prouve $\begin{cases}ab \in C\\a-b \in C\end{cases}$. L'ensemble C est donc un sous-anneau de A.

▶ Solution 11.3.2

1. Soient x, y, z trois éléments quelconques de A.
   Il faut prouver $(xy+yx)z = z(xy+yx)$.
   On utilise l'hypothèse avec $a = x+y$ et $b = z$. On a donc :

$$\begin{aligned}(a^2-a)z &= ((x+y)^2 - x - y))z = (x^2+xy+yx+y^2-x-y)z\\&= (x^2-x)z + (xy+yx)z + (y^2-y)z\\&= z(x^2-x) + (xy+yx)z + z(y^2-y) \quad \text{(en utilisant l'hypothèse)}\end{aligned}$$

   Par un calcul analogue : $(a^2-a)z = z(a^2-a) = z(x^2-x) + z(xy+yx) + z(y^2-y)$.
   Par comparaison des deux expressions de $(a^2-a)z$, on a bien $(xy+yx)z = z(xy+yx)$.

2. Soient x et y deux éléments de A.
   En utilisant ce qui précède, on peut écrire : $(xy+yx)x = x(xy+yx)$ donc $yx^2 = x^2y$.
   On a alors : $xy = x^2y - (x^2-x)y = yx^2 - y(x^2-x) = yx$.
   Conclusion : L'anneau A est commutatif.

▶ Solution 11.3.3

Soit b un élément quelconque de A.

On doit montrer que $x = ab - ba$ est nul.

On constate que $\begin{cases}ax = a^2b - aba = ab - aba\\xa = aba - ba^2 = aba - ba\end{cases}$

Par addition, il en résulte $ax + xa = ab - ba = x$.

Mais $x = ax + xa \Rightarrow ax = a^2x + axa = ax + axa \Rightarrow axa = 0$.

On en déduit $0 = x(axa) = (xa)^2$ et donc $xa = 0$ (pas de nilpotent sauf 0.)

De même $0 = (axa)x = (ax)^2 \Rightarrow ax = 0$.

On trouve finalement $x = ax + xa = 0$ c'est-à-dire $ab = ba$.

▶ Solution 11.3.4

1. On peut considérer $\mathbb{Z}_2 = \{0,1\}$ avec les lois

$+$	0	1
0	0	1
1	1	0

et

$\times$	0	1
0	0	0
1	0	1

   On peut aussi considérer les anneaux produits $B = \mathbb{Z}_2^n$ où $\mathbb{Z}_2$ a le sens précédent.
   Il y a encore l'anneau $A = (\mathcal{P}(E), \Delta, \cap)$, où Δ est la différence symétrique.

2. Soit a un élément de A. On a $(a+a)^2 = a+a$, donc $a^2+2a+a^2 = a+a$ donc $2a = 0$.
   Remarque : ce résultat peut aussi s'écrire : $\forall\, a \in A, a = -a$.
   Pour tous x, y de A, on a : $\begin{cases} (x+y)^2 = x+y \\ (x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y \end{cases}$.
   Il en découle $xy+yx = 0$, c'est-à-dire $yx = -xy = xy$: l'anneau A est commutatif.

3. Rappel : dans un anneau non réduit à $\{0\}$, les deux éléments 0 (le neutre additif) et 1 (le neutre multiplicatif) sont distincts.
   Supposons $A = \{0, 1, a\}$. Alors $a+1$ n'est ni égal à 0 (car sinon $a = -1 = 1$) ni égal à 1 (car $a \neq 0$) ni égal à a (car $1 \neq 0$).
   On aboutit à une impossibilité : A ne peut pas être de cardinal 3.

4. On suppose donc que A est fini et qu'il est au moins de cardinal 4.
   Soient x un élément de A, non nul et distinct de 1.
   On a $x(x+1) = x^2+x = x+x = 0$, alors que ni x ni $x+1$ ne sont nuls.
   On constate donc que l'anneau A possède des diviseurs de zéro.

5. Soit $A = \{0, 1, a, b\}$ un anneau de Boole de cardinal 4.
   On sait que $1+a \notin \{0, 1, a\}$. Donc $a+1 = b$.
   De même $b+1 = a$. On en déduit $a+b = 2a+1 = 1$.
   Enfin $ab = a(a+1) = 0$ et $ba = b(a+1) = 0$.
   On en déduit les tables des lois de A :

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

et

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	a	0
b	0	b	0	b

   On définit $\varphi : \mathbb{Z}_2^2 \to A$ en posant $\varphi(0,0) = 0, \varphi(1,1) = 1, \varphi(1,0) = a, \varphi(0,1) = b$.
   On constate alors que φ est un isomorphisme d'anneaux.
   Il n'y a donc qu'un seul anneau de Boole à quatre éléments : c'est $\mathbb{Z}_2^2$.

6. $(A, +)$ est un groupe fini dans lequel tout élément est son propre inverse.
   Il en découle que $\text{card}(A)$ est une puissance de 2.
   On pourra se reporter à la solution de l'exercice 4.2.20.

► Solution 11.3.5

Remarque : par convention, les anneaux intègres et les corps sont commutatifs.

Soit a un élément non nul de A. On doit montrer que a est inversible.

Puisque A est intègre, a est simplifiable.

L'application $x \mapsto ax$ est donc injective de A dans A.

Puisque A est fini, cette application est bijective.

En particulier, il existe b dans A tel que $ba = 1$: cet élément est l'inverse de a.

Conclusion : A est un corps (tous ses éléments non nuls sont inversibles).

► Solution 11.3.6

Supposons par exemple $x^n = 0$, avec $n \geqslant 1$.

Alors $(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1-x^n = 1$.

Ainsi $1-x$ est inversible et son inverse est $y = 1+x+x^2+\cdots+x^{n-1}$.

► Solution 11.3.7

1. Tout d'abord $A \neq \emptyset$ car il contient 1 (le neutre multiplicatif de $\mathbb{R}$).
   Soient $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ dans A, avec $(a, b, c, d) \in \mathbb{Z}^4$.
   On a $x - y = (a - c) + (b - d)\sqrt{2}$, avec $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$. Donc $x - y \in A$.
   De même $xy = \alpha + \beta\sqrt{2}$ avec $\alpha = ac + 2bd \in \mathbb{Z}$ et $\beta = ad + bc \in \mathbb{Z}$. Donc $xy \in A$.
   Conclusion : A est un sous-anneau de $\mathbb{R}$.
   Bien sûr A est intègre car $\mathbb{R}$ l'est lui-même...
2. Avec les notations ci-dessus :
   $$\begin{aligned} N(xy) &= \alpha^2 - 2\beta^2 = (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2 \\ &= (a^2 - 2b^2)(c^2 - 2d^2) = N(x)N(y) \end{aligned}$$
3. Notons toujours $x = a + b\sqrt{2}$, avec $(a, b) \in \mathbb{Z}^2$.
   On suppose que x est inversible dans A, d'inverse y. Remarquons que $N(1) = 1$.
   L'égalité $N(x)N(y) = N(xy)$ donne ici $N(x)N(y) = 1$.
   Ainsi $N(x)$ est un élément inversible de $\mathbb{Z}$. Donc $N(x) = \pm 1$.
   Réciproquement, supposons $N(x) = \varepsilon$ avec $\varepsilon = \pm 1$. Posons $y = a - b\sqrt{2} \in A$.
   On constate alors $xy = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = \varepsilon$.
   Il en découle que $x(\varepsilon y) = 1$. Ainsi εy est l'inverse de x dans A.
4. Une généralisation évidente de la question (2) donne, pour tout n de $\mathbb{Z}$:
   $$N(\pm(1 + \sqrt{2})^n)) = N((1 + \sqrt{2})^n)) = \Big(N(1 + \sqrt{2})\Big)^n = (-1)^n = \pm 1$$
   Les éléments $\pm(1 + \sqrt{2})^n)$ sont donc inversibles dans A.
   Plus précisément, l'inverse de $1 + \sqrt{2}$ est $-1 + \sqrt{2}$.
   l'inverse de $\varepsilon(1 + \sqrt{2})^n$ est donc $\varepsilon(-1 + \sqrt{2})^n$.
5. Soit $x = a + b\sqrt{2}$ un élément inversible de A (avec bien sûr $(a, b) \in \mathbb{Z}^2$).
   (a) On doit montrer que x est de la forme $\pm(1 + \sqrt{2})^n$, avec $n \in \mathbb{Z}$.
   Puisque le résultat est demandé au signe près, on peut toujours supposer $b \geqslant 0$.
   Ensuite, on sait que l'inverse de $x = a + b\sqrt{2}$ est $y = -a + b\sqrt{2}$.
   Comme l'ensemble des résultats attendus est invariant par passage à l'inverse (n est entier relatif) on peut partir indifféremment de x ou de y.
   Dans la pratique, cela revient à dire qu'on peut choisir $a \geqslant 0$.
   Remarquons cependant que l'égalité $a^2 - 2b^2 = \pm 1$ est incompatible avec $a = 0$.
   On peut donc partir de $x = a + b\sqrt{2}$, avec $a \in \mathbb{N}^*$, $b \in \mathbb{N}$, et $a^2 - 2b^2 = \pm 1$.

   (b) On va montrer que x est de la forme $(1 + \sqrt{2})^n$, avec $n \in \mathbb{N}^*$.
   Remarquons que si $b = 0$ alors nécessairement $a^2 = 1$ et $a = 1$.
   Dans ce cas $x = 1 = (1 + \sqrt{2})^0$ est de la forme voulue.
   On suppose donc $b \geqslant 1$.
   Soit $x_1 = \dfrac{x}{1 + \sqrt{2}} = (a + b\sqrt{2})(\sqrt{2} - 1) = a_1 + b_1\sqrt{2}$, où $\begin{cases} a_1 = -a + 2b \\ b_1 = a - b \end{cases}$
   Remarquons que $a^2 = 2b^2 \pm 1 \Rightarrow \begin{cases} a^2 = b^2 + (b^2 \pm 1) \geqslant b^2 \\ a^2 = 2b^2 \pm 1 < 4b^2 \end{cases}$
   On en déduit les inégalités : $0 < b \leqslant a < 2b$.
   Il en découle : $a_1 = 2b - a \in]0, a]$ et $b_1 = a - b \in [0, b[$.
   Si $b_1 = 0$, alors $a_1 = 1$ (conséquence toujours de $a_1^2 - 2b_1^2 = \pm 1$) donc $x_1 = 1$.
   Dans ce cas $x = 1 + \sqrt{2}$ est bien de la forme attendue.

Sinon on peut construire $x_2 = \dfrac{x_1}{1+\sqrt{2}}$ comme on a construit x_1 à partir de x.

On forme ainsi une suite $x_0 = x, x_1, x_2, \dots, x_k = a_k + b_k\sqrt{2}$, avec les conditions :

$$a_{k+1} = 2b_k - a_k \in]0, a_k] \quad \text{et} \quad b_{k+1} = a_k - b_k \in [0, b_k[$$

Passer de x_k à $x_{k+1} = \dfrac{x_k}{1+\sqrt{2}}$ est possible (avec les conditions ci-dessus) si $x_k \neq 1$.

Ces conditions (notamment la décroissance stricte des b_k) montrent que la suite des x_k est finie. Ainsi il existe un premier entier n tel que $x_n = 1$.

Par construction, on a alors $1 = x_n = \dfrac{x}{(1+\sqrt{2})^n}$, c'est-à-dire $x = (1+\sqrt{2})^n$.

Conclusion : Les éléments inversibles de A sont les $\pm(1+\sqrt{2})^n$, avec $n \in \mathbb{Z}$.