TD 15 : Structures algébriques

▶ Lois de composition interne

Exercice 15.1 PD
Soit $(E, \leqslant)$ un ensemble totalement ordonné. Alors pour tout $(x, y) \in E^2$, $\max(x, y)$ est bien défini. On définit ainsi une loi de composition interne, notée max sur E.

1. Montrer que la loi max est associative et commutative.
2. Donner une condition nécessaire et suffisante pour que $(E, \max)$ possède un élément neutre.
3. Lorsque cette condition est vérifiée, quels sont les éléments inversibles de E ?

Exercice 15.2 **Éléments réguliers** AD
Soit E un ensemble muni d'une loi de composition interne $\star$, associative, et possédant un élément neutre e. Un élément $x \in E$ est dit régulier à gauche si $\forall (y, z) \in E^2, x*y = x*z \Rightarrow y = z$ et régulier à droite si $\forall (y, z) \in E^2,\ y*x = z*x \Rightarrow y = z$.

1. Quels sont les éléments réguliers (à droite ou à gauche) de $(\mathbf{Z}, \times)$?
2. Soit A un ensemble. Montrer que dans $(\mathcal{F}(A, A), \circ)$, un élément f est régulier à droite si et seulement si f est surjective. Donner une condition nécessaire et suffisante pour que f soit régulier à gauche.

▶ Groupes

Exercice 15.3 PD
On définit une loi de composition interne $\star$ sur $\mathbf{R}$ par : $\forall (x, y) \in \mathbf{R}^2,\ x \star y = \sqrt[3]{x^3 + y^3}$.
Montrer que $(\mathbf{R}, \star)$ est un groupe abélien.

Exercice 15.4 F
Soit E un ensemble muni d'une loi de composition interne associative $\star$, possédant un élément neutre e, et telle que $\forall x \in E,\ x \star x = e$.
Prouver que $(E, \star)$ est un groupe commutatif.

Exercice 15.5 **Centre d'un groupe** PD
Soit G un groupe. On appelle centre de G l'ensemble $\mathcal{Z}(G) = \{x \in G,\ \forall y \in G,\ xy = yx\}$ des éléments commutant avec tous les éléments de G. Montrer que $\mathcal{Z}(G)$ est un sous-groupe de G. À quelle condition a-t-on $\mathcal{Z}(G) = G$?

Exercice 15.6 **Divers sous-groupes** PD
Dans chacun des cas suivants, déterminer si H est ou non un sous-groupe de G.
La loi de composition de G n'est volontairement pas précisée, et je vous laisse le soin de deviner de laquelle il est question, sachant qu'à chaque fois il s'agit de la seule loi de groupe que vous connaissiez sur G.

1. $G = \mathbf{C}^*$, $H = \bigcup_{n \in \mathbf{N}^*} \mathbf{U}_n$
2. $G = \mathcal{M}_n(\mathbf{C})$, H l'ensemble des matrices triangulaires supérieures de G.
3. $G = GL_2(\mathbf{R})$, H l'ensemble des éléments de G dont tous les coefficients sont dans $\mathbf{Z}$.
4. $G = GL_n(\mathbf{R})$, H l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux valent 1.
5. $G = \mathfrak{S}_n$, $H = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = 2\}$

Exercice 15.7 AD
Donner les tables de multiplication de $\mathbf{U}_4$ et $\mathbf{U}_2 \times \mathbf{U}_2$. Prouver alors que ces deux groupes ne sont pas isomorphes (c'est-à-dire qu'il n'existe pas d'isomorphisme entre ces groupes), bien que de même cardinal.

Exercice 15.8 D
Soit G un groupe non réduit à un élément tel que pour tout $g \in G$, $g^2 = e$.

1. Montrer que tout élément est égal à son propre inverse. En déduire que G est abélien.
2. Montrer que G possède au moins un sous-groupe de cardinal 2.
3. On suppose que G contient au moins trois éléments. Soit H un sous-groupe fini de G, différent de $\{e\}$ ou de G, et soit $g \in G \setminus H$. On pose alors $gH = \{gh,\ h \in H\}$.
   (a) Montrer que $H \cup gH$ est un sous-groupe de cardinal $2|H|$.
   (b) Montrer que si G est fini, alors son cardinal est une puissance de 2.

Exercice 15.9 **Un cas particulier du théorème de Lagrange** AD
Soit G un groupe commutatif fini, de cardinal n.

1. Soit $g \in G$. Montrer que $x \mapsto gx$ est une bijection de G sur lui-même.
2. Soit $g \in G$. En calculant de deux manières le produit $\prod_{x \in G} (gx)$, montrer que $g^n = 1_G$.
3. Déterminer tous les sous-groupes finis de $(\mathbf{C}^*, \times)$.

Exercice 15.10 **Union de sous-groupes** AD

1. Donner un exemple de deux sous-groupes de $(\mathbf{R}^*, \times)$ dont l'union n'est pas un sous-groupe.
2. Soit G un groupe, H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe si et seulement si $H \subset K$ ou $K \subset H$.
3. Soit $(H_n)_{n\in\mathbf{N}}$ une suite croissante de sous-groupes de G. Montrer que $\bigcup_{n\in\mathbf{N}} H_n$ est un sous-groupe de G.

Exercice 15.11 **Opérations sur les sous-groupes** AD

Soit G un groupe, H et K deux sous-groupes de G. On note $HK = \{h \cdot k,\ (h,k) \in H \times K\}$

1. Montrer que $H \cap K$ est un sous-groupe de G.
2. Si G est abélien, montrer que HK est un sous-groupe de G.
3. ($\star$) Prouver que HK est un sous-groupe de G si et seulement si $HK = KH$.

Exercice 15.12 Dans cet exercice, on note G l'ensemble des similitudes directes du plan, qu'on assimile à l'ensemble des fonctions $f : \mathbf{C} \to \mathbf{C}$ telles qu'il existe $(a,b) \in \mathbf{C}^* \times \mathbf{C}$ tels que $\forall z \in \mathbf{C}$, $f(z) = az + b$. AD

1. Montrer que $(G, \circ)$ est un groupe, et qu'il n'est pas abélien.
2. Soit $z_0 \in \mathbf{C}$. On pose $G_{z_0} = \{g \in G \mid g(z_0) = z_0\}$.
   Montrer que G_{z_0} est un sous-groupe de G, isomorphe à $\mathbf{C}^*$. Est-il abélien ?

Exercice 15.13 Soit G un groupe abélien fini avec un seul élément f d'ordre 2 (c'est-à-dire tel que $f^2 = e$ et $f \neq e$). Montrer que $\prod_{g\in G} g = f$. PD

Exercice 15.14 Soit G un groupe, et soit $x \in G$. On dit que x est d'ordre fini s'il existe $n \in \mathbf{N}^*$ tel que $x^n = e_G$. AD

1. Montrer que si G est abélien, et que x et y sont d'ordre fini, alors xy est encore d'ordre fini.
2. Le résultat de la question précédente reste-t-il vrai si G n'est plus abélien ?

Exercice 15.15 **Conjugaison dans un groupe** AD

Soit G un groupe. Pour $a \in G$, on pose $\tau_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & aga^{-1} \end{array}\right.$.

1. Montrer que τ_a est un morphisme bijectif de G dans lui-même (on parle alors d'automorphisme).
2. On pose $\mathscr{C}(G) = \{\tau_a,\ a \in G\}$. Montrer qu'il s'agit d'un sous-groupe de $(\mathfrak{S}(G), \circ)$.
3. Montrer que l'application $\varphi : G \to \mathfrak{S}(G)$ qui à $a \in G$ associe τ_a est un morphisme de groupes. Quel est son noyau ?

Exercice 15.16 Soit $f : G_1 \to G_2$ un morphisme de groupes. PD

1. Prouver que pour tout sous-groupe H_1 de G_1, $f(H_1)$ est un sous-groupe de G_2.
2. Prouver que pour tout sous-groupe H_2 de G_2, $f^{-1}(H_2)$ est un sous-groupe de G_1. En déduire que $\operatorname{Ker} f$ est un sous-groupe de G_1.

Exercice 15.17 Soient $m, n \in \mathbf{N}^*$. On note alors $f : \left|\begin{array}{ccc} \mathbf{U}_{mn} & \longrightarrow & \mathbf{U}_m \times \mathbf{U}_n \\ z & \longmapsto & (z^n, z^m) \end{array}\right.$. AD

1. Montrer que f est un morphisme de groupes.
2. Déterminer un entier k tel que $\operatorname{Ker} f = \mathbf{U}_k$.
3. Déterminer une condition nécessaire et suffisante pour que f soit un isomorphisme.

Exercice 15.18 Déterminer tous les morphismes de groupe de $(\mathbf{Z}, +)$ dans $(\mathbf{Z}, +)$. De $(\mathbf{Q}, +)$ dans $(\mathbf{Z}, +)$. AD

Exercice 15.19 Soit $(G, *)$ un groupe, et soit A une partie non vide **finie** de G, stable par $*$. Prouver que A est un sous-groupe de G. D

Exercice 15.20 Soit G un groupe possédant exactement deux sous-groupes. D

Montrer qu'il existe $x \in G$ tel que $G = \langle x \rangle$, que G est fini, et que son cardinal est premier.

▶ Anneaux, corps

Exercice 15.21 Montrer que $\mathbf{Z}\left[\sqrt{2}\right] = \left\{x + y\sqrt{2},\ (x,y) \in \mathbf{Z}^2\right\}$ est un anneau. AD

Prouver que $\mathbf{Q}\left(\sqrt{2}\right) = \left\{x + y\sqrt{2},\ (x,y) \in \mathbf{Q}^2\right\}$ est un corps.

Plus généralement, prouver que pour tout $d \in \mathbf{N}^*$, $\mathbf{Q}(\sqrt{n}) = \{a + h\sqrt{d},\ (a,b) \in \mathbf{Q}^2\}$ est un corps. Donner une condition nécessaire et suffisante pour que $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}$.

Exercice 15.22 Soit $\mathbb{D}$ l'ensemble des nombres décimaux. Montrer que $(\mathbb{D}, +, \times)$ est un anneau. Est-ce un corps ? F

Exercice 15.23 **Produit direct d'anneaux** PD

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. On munit $A \times B$ de deux lois de composition $\oplus$ et $\otimes$ définies par :

$$(a, b) \oplus (a', b') = (a +_A a', b +_B b') \text{ et } (a, b) \otimes (a', b') = (a \times_A a', b \times_B b').$$

Montrer que $(A \times B, \oplus, \otimes)$ est un anneau, commutatif si A et B le sont. Cet anneau est-il intègre ?

Exercice 15.24 Parmi les ensembles suivants, lesquels sont des sous-anneaux de $\mathbf{R}^{\mathbf{N}}$, l'anneau des suites réelles ? PD

1. l'ensemble des suites de limite nulle
2. l'ensemble des suites croissantes
3. l'ensemble des suites convergentes
4. l'ensemble des suites divergentes
5. l'ensemble des suites bornées
6. l'ensemble des suites (u_n) telles que $\lim\limits_{n\to+\infty} u_n = +\infty$
7. l'ensemble des suites stationnaires
8. l'ensemble des suites nulles à partir d'un certain rang

Exercice 15.25 Soient $k, \mathbf{K}$ deux corps, et soit $f : k \to \mathbf{K}$ un morphisme d'anneaux. Montrer que f est injectif. F

Exercice 15.26 Soit $(A, +, \times)$ un anneau commutatif. Pour $a \in A$, on appelle racine carrée de a tout élément dont le carré vaut a. AD

1. Prouver que si A est intègre, alors tout élément de A admet au plus deux racines carrées.
2. En revanche, prouver que dans $(\mathcal{F}(\mathbf{R}, \mathbf{R}), +, \times)$, la fonction constante $x \mapsto 1$ possède une infinité de racines carrées.

Exercice 15.27 Soit A un anneau commutatif et E un ensemble non vide. À quelle condition $\mathcal{F}(E, A)$ est-il intègre ? PD

Exercice 15.28 Soit $(A, +, \times)$ un anneau. Un élément $a \in A$ est dit nilpotent s'il existe $n \in \mathbf{N}$ tel que $a^n = 0_A$.

1. Soient x, y deux éléments nilpotents de A, qui commutent. Montrer que xy et $x + y$ sont nilpotents.
2. Montrer que si $x \in A$ est nilpotent, alors $1_A - x \in A^\times$.

Exercice 15.29 Montrer qu'un anneau intègre fini est un corps. D

Exercice 15.30 **Idéaux premiers (D'après oral ENS)** TD

Soit A un anneau commutatif non nul. On appelle idéal de A tout sous-groupe I de $(A, +)$ tel que $\forall (a, x) \in A \times I,\ ax \in I$.

1. Montrer que pour tout $x \in A$, $xA = \{ax, a \in A\}$ est un idéal de A.
2. Un idéal I est dit maximal si tout idéal de A, différent de A, et qui contient I est égal à I lui-même.
   Et un idéal I différent de A est dit premier si $\forall (a, b) \in A^2,\ ab \in I \Rightarrow a \in I$ ou $b \in I$.
   (a) Montrer qu'un idéal I est maximal si et seulement si pour tout $x \in A \setminus I$, $I + xA = A$ (où $I + aA$ est l'ensemble des éléments qui s'écrivent comme somme d'un élément de I et d'un élément de aA).
   (b) Prouver qu'un idéal maximal est premier.
3. Montrer que A est un corps si et seulement si tout idéal de A autre que A est premier.

Exercice 15.31 **Endomorphismes de l'anneau R.** AD

Soit $f : \mathbf{R} \to \mathbf{R}$ un morphisme d'anneaux.

1. Montrer que $f_{|\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$.
2. Prouver que f est croissant.
3. En déduire que $f = \mathrm{id}_{\mathbf{R}}$.

CORRECTION DES EXERCICES DU TD 15

SOLUTION DE L'EXERCICE 15.1

1. C'est trivial.

2. Supposons que E contienne un élément neutre e pour max. Alors, pour tout $x \in E$, $\max(x, e) = x$, et donc $e \leqslant x$.
Donc un élément neutre est forcément un minorant de E, et étant dans E, c'est le plus petit élément de E.
Inversement, si E possède un plus petit élément e, alors pour tout $x \in E$, $\max(x, e) = x$, et donc e est élément neutre.
Ainsi, $(E, \max)$ possède un élément neutre si et seulement si il possède un plus petit élément.

3. L'élément neutre est bien entendu inversible, égal à son propre inverse.
Soit $x \in E$ un élément inversible. Alors il existe $y \in E$ tel que $\max(x, y) = e$.
Donc soit $x = e$, soit $y = e$.
Mais si $y = e$, alors y est l'inverse de x, et donc $x = y^{-1} = e^{-1} = e$.
Donc e est l'unique élément inversible de E.

SOLUTION DE L'EXERCICE 15.2

1. Notons que $\mathbf{Z}$ étant commutatif, les éléments réguliers à droite et réguliers à gauche sont les mêmes.
Supposons donc que x soit régulier, et soient $y, z \in \mathbf{Z}$ tels que $xy = xz$.
Alors $x(y - z) = 0$. Et donc soit $x = 0$, soit $y - z = 0 \Leftrightarrow y = z$.
Il est clair que 0 n'est pas régulier car $0 \cdot 1 = 0 \cdot 2$. Donc tout élément non nul de $\mathbf{Z}$ est régulier.

2. Supposons que f soit surjective, et soient $g, h \in \mathcal{F}(A, A)$ telles que $g \circ f = h \circ f$.
Soit alors $y \in A$. Par surjectivité de f, il existe $x \in A$ tel que $y = f(x)$.
Et alors $g(y) = g(f(x)) = h(f(x)) = h(y)$. Ceci étant vrai quel que soit $y \in A$, on en déduit que $g = h$, donc que f est régulier à droite.

En revanche, si f n'est pas surjective, alors il existe $y \in A$ qui ne possède pas d'antécédent par f. Et alors deux fonctions g et h qui diffèrent uniquement en y vérifient $\forall x \in A,\ g(f(x)) = h(f(x))$ car $f(x) \neq y$.
Pourtant $h \neq g$ par hypothèse, donc f n'est pas régulier à droite.

> **Autrement dit**
> On suppose que $g(x) = h(x)$ pour tout $x \neq y$ et que $g(y) \neq h(y)$.

Si f est injective, soient alors g et h deux fonctions telles que $f \circ g = f \circ h$.
Alors pour tout $x \in A$, $f(g(x)) = f(h(x))$, et donc $g(x) = h(x)$. Donc $g = h$: f est régulier à gauche.
Inversement, soit f une fonction régulière à gauche pour la composition, et soient $x_1, x_2 \in A$ tels que $f(x_1) = f(x_2)$.
Soient alors g et h les fonctions constantes égales respectivement à x_1 et x_2.
On a donc $f \circ g = f \circ h$. Et donc $g = h$, de sorte que $x_1 = x_2$.

SOLUTION DE L'EXERCICE 15.3

Commençons par prouver l'associativité de la loi $\star$: soient x, y, z trois réels. Alors

$$x \star (y \star z) = \sqrt[3]{x^3 + \left(\sqrt[3]{y^3 + z^3}\right)^3} = \sqrt[3]{x^3 + y^3 + z^3}.$$

Et d'autre part,

$$(x \star y) \star z = \sqrt[3]{\left(\sqrt[3]{x^3 + y^3}\right)^3 + z^3} = \sqrt[3]{x^3 + y^3 + z^3} = x \star (y \star z).$$

Donc $\star$ est une loi de composition associative.
Notons qu'elle est clairement commutative, puisque la somme dans $\mathbf{R}$ est commutative, et donc $x^3 + y^3 = y^3 + x^3$.

0 est l'élément neutre pour $\star$, puisque pour tout $x \in \mathbf{R}$, $x \star 0 = \sqrt[3]{x^3} = x$. Et par commutativité, $0 \star x = x \star 0 = x$.
Enfin, tout élément admet bien un inverse, qui est $-x$, puisque

$$x \star (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0.$$

Et par commutativité, $(-x) \star x = 0$.
Ainsi, $(\mathbf{R}, \star)$ est bien un groupe.

> **Remarque**
> Bien que l'élément neutre soit le même que celui du groupe $(\mathbf{R}, +)$, et que l'inverse d'un élément x soit également le même que dans $(\mathbf{R}, +)$, il ne s'agit pas du même groupe, car en général,
> $$x \star y \neq x + y.$$
> Par exemple
> $$1 \star 1 = \sqrt[3]{2} \neq 2 = 1 + 1.$$

Solution de l'exercice 15.4

Il s'agit donc de prouver que tout élément est inversible, ainsi que la commutativité de $\star$.
Mais puisque pour tout $x \in E$, $x \star x = e$, x est inversible, égal à son propre inverse.
Donc $(E, \star)$ est un groupe.
Et pour $(x, y) \in E^2$, on a $x \star y = (x \star y)^{-1} = y^{-1} \star x^{-1} = y \star x$.
Donc $\star$ est commutative.

Solution de l'exercice 15.5

Pour tout $x \in G$, $ex = xe = x$, donc $e \in \mathcal{Z}(G)$.
Soit $g \in \mathcal{Z}(G)$, et soit $x \in G$. Alors $gx^{-1} = x^{-1}g$, et donc en passant à l'inverse, $xg^{-1} = g^{-1}x$, de sorte que x et g^{-1} commutent. Ceci étant vrai pour tout $x \in G$, $g^{-1} \in \mathcal{Z}(G)$.
Enfin, si $g, h \in \mathcal{Z}(G)$, alors pour tout $x \in G$,

$$ghx = g(hx) = g(xh) = (gx)h = xgh.$$

Donc gh et x commutent, de sorte que $gh \in \mathcal{Z}(G)$.
Et donc nous avons bien vérifié les quatre points caractérisant un sous-groupe, $\mathcal{Z}(G)$ est un sous-groupe de G.
On a alors $\mathcal{Z}(G) = G$ si et seulement si

$$\forall g \in G,\ g \in \mathcal{Z}(G) \Leftrightarrow \forall (g, h) \in G^2,\ hg = gh.$$

Soit encore si et seulement si G est abélien.

Solution de l'exercice 15.6

1. 1 (qui est l'élément neutre de $\mathbf{C}^*$) est dans tous les $\mathbf{U}_n$, donc dans leur union.
Soient $x, y \in \bigcup_{n \in \mathbf{N}^*} \mathbf{U}_n$.
Alors il existe $n \in \mathbf{N}^*$ tel que $x^n = 1$ et il existe $p \in \mathbf{N}^*$ tel que $y^p = 1$.
Mais alors $(xy)^{np} = x^{np} y^{np} = (x^n)^p\,(y^p)^n = 1^p 1^n = 1$.
Donc $xy \in H$.
De plus, si $x \in H$, alors il existe $n \in \mathbf{N}^*$ tel que $x^n = 1$, et donc $\left(\frac{1}{x}\right)^n = 1$, donc $\frac{1}{x} \in \mathbf{U}_n \subset H$.
Ainsi, H est un sous-groupe de G.

> **Danger !**
> n et p n'ont aucune raison d'être égaux.

2. La matrice nulle est dans H.
La somme[1] de deux matrices triangulaires supérieures est encore triangulaire supérieure.
Et si $M \in H$, alors $-M$ (qui est l'inverse de M pour l'addition) est encore dans H.
Donc H est un sous-groupe de $\mathcal{M}_n(\mathbf{C})$.

[1] Ici, $\mathcal{M}_n(\mathbf{C})$ est bien muni de la somme.

3. $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ est dans H, mais son inverse, $\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$ n'est pas dans H, donc H n'est pas un sous-groupe de G.

> **Remarque**
> Si on ajoute la condition que $\det A = \pm 1$, alors H devient un sous-groupe de G.

4. La matrice I_n est dans H.
Le produit de deux matrices de H est dans H.
Et si $M \in H$, alors son inverse est triangulaire supérieure, et ses coefficients diagonaux sont les inverses de ceux de M, donc valent tous 1.
Donc $M^{-1} \in H$: H est un sous-groupe de G.

5. $\mathrm{id}(1) = 1 \neq 2$, donc id, qui est l'élément neutre de $\mathfrak{S}_n$ n'est pas dans H : H n'est pas un sous-groupe de G.

Solution de l'exercice 15.7

Pour $\mathbf{U}_4 = \{1, -1, i, -i\}$, il n'y a pas de difficulté :

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Puisque $\mathbf{U}_2 = \{-1, 1\}$, le groupe $\mathbf{U}_2 \times \mathbf{U}_2$ contient 4 éléments : $(1,1), (-1,-1), (1,-1), (-1,1)$, et on a alors

$\times$	$(1,1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$
$(1,1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$

En particulier, pour tout x dans $\mathbf{U}_2 \times \mathbf{U}_2$, on a $x^2 = (1,1)$ l'élément neutre.
Supposons par l'absurde qu'il existe un isomorphisme $\varphi : \mathbf{U}_2 \times \mathbf{U}_2 \to \mathbf{U}_4$.
Alors pour tout $y \in \mathbf{U}_4$, il existe un unique $x \in \mathbf{U}_2 \times \mathbf{U}_2$ tel que $y = \varphi(x)$. Et alors $y^2 = \varphi(x)^2 = \varphi\left(x^2\right) = \varphi((1,1)) = 1$.
Autrement dit, le carré de tout élément de $\mathbf{U}_4$ est égal à 1. Ceci est manifestement faux, puisque $i^2 = -1 \neq 1$.
Par conséquent, il n'existe pas d'isomorphisme de $\mathbf{U}_2 \times \mathbf{U}_2 \to \mathbf{U}_4$.

Rappel
Un morphisme envoie toujours l'élément neutre sur l'élément neutre.

SOLUTION DE L'EXERCICE 15.8

1. Pour tout $x \in G$, $xx = x^2 = e$, et donc $x^{-1} = x$.

2. Soient $x, y \in G$. Alors $xy = (xy)^{-1}$. Mais $(xy)^{-1} = y^{-1}x^{-1}$, qui par la question précédente vaut yx. Et donc $xy = yx$, si bien que G est abélien.

3. Il existe $x \in G$ tel que $x \neq e$. Et alors $\{e, x\}$ est un sous-groupe de G, de cardinal 2.

4.a. Notons qu'un tel sous-groupe H existe par la question précédente.
Puisque $e \in H$, $e \in H \cup gH$.
Soient $g_1, g_2 \in H \cup gH$. Soit $g_1 \in H$, soit il existe $h_1 \in H$ tel que $g_1 = gh_1$.
De même, soit $g_2 \in H$, soit il existe $h_2 \in H$ tel que $g_2 = gh_2$.

Montrons que $g_1g_2 \in H \cup gH$ est stable par produit, puisque tout élément étant égal à son propre inverse, on aura donc, $g_1g_2^{-1} = g_1g_2 \in H \cup gH$.

► Si $g_1, g_2 \in H$. Alors $g_1g_2 \in H$ par définition d'un sous-groupe.
► Si $g_1 \in H$ et $g_2 \notin H$. Alors $g_1g_2 = g_1gh_2 = g\underbrace{(g_1h_2)}_{\in H} \in gH \subset H \cup gH$.
► Si $g_1 \notin H$ et $g_2 \in H$. Alors $g_1g_2 = g\underbrace{(h_1g_2)}_{\in H}$.
► Si $g_1 \notin H$ et $g_2 \notin H$. Alors $g_1g_2 = gh_1gh_2 = g^2h_1h_2 = h_1h_2 \in H \subset H \cup gH$.
Donc nous avons bien prouvé que pour tout $g_1, g_2 \in H \cup gH$, $g_1g_2 \in H \cup gH$, qui est donc un sous-groupe de G.
Puisque la translation à gauche par g est bijective, $h \mapsto gh$ est une bijection de H sur gH, qui a donc même cardinal que H.
Par ailleurs, H et gH sont disjoints. En effet, supposons par l'absurde qu'il existe $x \in H \cup gH$.
Alors $x \in H$ et il existe $h \in H$ tel que $x = gh$. Et alors $g = xh^{-1} \in H$, ce qui est absurde puisqu'on a supposé $g \notin H$.
Donc $H \cup gH$ est de cardial $\mathrm{Card}(H) + \mathrm{Card}(gH) = 2\mathrm{Card}(H)$.

4.b. Supposons par l'absurde que $\mathrm{Card}(G)$ ne soit pas une puissance de 2.
Soit alors H_1 un sous-groupe de G de cardinal 2. Alors $H_1 \neq G$, et donc il existe $g_1 \in G \setminus H_1$.
Donc $H_2 = H_1 \cup g_1H_1$ est un sous-groupe de G de cardinal 4.
Mais alors $H_2 \neq G$ puisque G n'est pas de cardial 4. Donc il existe $g_2 \in G \setminus H_2$. Et alors $H_3 = H_2 \cup g_2H_2$ est un sous-groupe de G de cardinal 8.
Mais H_3 n'est pas égal à G, etc.
On construit donc par récurrence une suite de sous-groupes $(H_k)_{k \geqslant 1}$ tels que H_k soit de cardinal 2^k.

Mais si k est suffisamment grand, $2^k > \text{Card}(G)$, ce qui est absurde.
Donc $\text{Card}(G)$ est nécessairement une puissance de 2.

Solution de l'exercice 15.9

1. Notons $f_g : x \mapsto gx$, et $f_{g^{-1}} : x \mapsto g^{-1}x$. Alors, pour tout $x \in G$,

$$\left(f_g \circ f_{g^{-1}}\right)(x) = g(g^{-1}x) = x \text{ et de même } \left(f^{g^{-1}} \circ f_g\right)(x) = g^{-1}(gx) = x.$$

Donc non seulement f_g est bijective, mais en plus, nous savons que son inverse est $f_{g^{-1}}$.

2. D'une part, f_g étant bijective, on a, avec le changement de variable $y = gx$,

$$\prod_{x\in G}(gx) = \prod_{y\in G} y.$$

D'autre part, G étant commutatif, on a

$$\prod_{g\in G}(gx) = g^n \prod_{x\in G} x.$$

Détaillons un poil ce calcul pour bien voir où l'hypothèse de commutativité est indispensable : notons $G = \{g_1, g_2, \dots, g_n\}$. Alors

$$\begin{aligned}\prod_{x\in G}(gx) &= \prod_{i=1}^{n}(gx_i)\\ &= (gx_1)(gx_2)\cdots(gx_n) = gx_1gx_2\cdots gx_n\\ &= ggx_1x_2gx_3\cdots gx_n\\ &= \cdots = \underbrace{g\cdots g}_{n \text{ fois}}(x_1x_2\cdots x_n)\\ &= g^n \prod_{x\in G} x.\end{aligned}$$

En notant $A = \prod_{x\in G} x$, on a donc $g^nA = A$, et donc en multipliant à droite par A^{-1}, $g^n = 1_G$.

Explication

La bijectivité nous dit que les gx, quant x parcourt G, prennent une et une seule fois chaque valeur dans G.
Et donc le produit des gx est le même que le produit des $x, x \in G$.
Remarquons au passage que cette notation produit n'a de sens que parce que le groupe est commutatif, sans cela, on ne saurait pas dans quel ordre a lieu le produit.

L'associativité nous permet de nous passer des parenthèses.
La commutativité sert ici : on peut permuter l'ordre de deux facteurs.

3. D'après la question précédente, un sous-groupe de cardinal n de $(\mathbf{C}^*, \times)$, qui sera forcément commutatif car $(\mathbf{C}^*, \times)$ l'est, est formé d'éléments z tels que $z^n = 1$.
Par conséquent, il est formé de racines $n^{\text{èmes}}$ de l'unité.
Autrement dit, si G est un sous-groupe de $(\mathbf{C}^*, \times)$ de cardinal n, alors $G \subset \mathbf{U}_n$.
Mais $\mathbf{U}_n$ est lui-même de cardinal n, et donc $G = \mathbf{U}_n$.
Donc pour tout $n \in \mathbf{N}^*$, $(\mathbf{C}^*, \times)$ possède un unique sous-groupe de cardinal n, qui est $\mathbf{U}_n$.

Solution de l'exercice 15.10

1. $\{-1, 1\}$ et $\mathbf{R}_+^*$ sont deux sous-groupes de $\mathbf{R}^*$, dont l'union n'est clairement pas un sous-groupe par exemple car elle contient -1, elle contient 2, mais ne contient pas leur produit.

2. Il est évident que si $H \subset K$, alors $H \cup K = K$ est un sous-groupe de G, et de même si $K \subset H$.

Supposons à présent que $H \not\subset K$ et $K \not\subset H$.
Il existe alors $h \in H$ tel que $h \notin K$, et il existe $k \in K$ tel que $k \notin H$.
Considérons de tels h et k.
Si on avait $h \cup k \in H$, alors il viendrait $k = h^{-1}(hk) \in H$ car $h \in H$ et $hk \in K$. C'est absurde car $k \notin H$, et donc $hk \notin H$. Et de même, si on avait $hk \in K$, alors $h = (hk)k^{-1} \in K$, ce qui est absurde.
Donc nous avons prouvé que $hk \notin H \cup K$, si bien que $H \cup K$ n'est pas stable par produit[2].

Ainsi, si $H \cup K$ est un sous-groupe de G, alors soit $H \subset K$, soit $K \subset H$. L'implication réciproque ayant déjà été prouvée, on a bien l'équivalence souhaitée.

[2] Notons que h et k sont tous deux dans $H \cup K$.

3. Notons que la croissance de la suite (H_n) s'entend par rapport à la relation d'ordre[3] donnée par l'inclusion.
Donc pour tout $n \in \mathbf{N}$, $H_n \subset H_{n+1}$.

[3] Partielle.

Puisque H_0 est un sous-groupe de G, $e \in H_0 \subset \bigcup_{n\in\mathbf{N}} H_n$.
Soient $x, y \in \bigcup_{n\in\mathbf{N}} H_n$, et soient n_0, n_1 tels que $x \in H_{n_0}, y \in H_{n_1}$.
Soit alors $k = \max(n_0, n_1)$. Puisque $n_0 \leqslant k$, $H_{n_0} \subset H_k$ et de même, $H_{n_1} \subset H_k$.
Donc $x, y \in H_n$, si bien que par stabilité de H_n par produit, $xy \in H_k \subset \bigcup_{n\in\mathbf{N}} H_n$.
Et donc $\bigcup_{n\in\mathbf{N}} H_n$ est stable par produit.
Enfin, $x^{-1} \in H_{n_0} \subset \bigcup_{n\in\mathbf{N}} H_n$, et donc $\bigcup_{n\in\mathbf{N}} H_n$ est stable par inverse.
C'est donc un sous-groupe de G.

SOLUTION DE L'EXERCICE 15.11

1. C'est du cours, mais reprouvons-le tout de même :

- ▶$e_G \in H$ car H est un sous-groupe, et de même, $e_G \in K$. Donc $e_G \in H \cap K$.
- ▶soient $g_1, g_2 \in H \cap K$. Alors $g_1 g_2 \in H$ car H est un sous-groupe, et de même, $g_1 g_2 \in K$, donc $g_1 g_2 \in H \cap K$: $H \cap K$ est stable par produit.
- ▶enfin, si $g \in H \cap K$, alors $g^{-1} \in H$, puisque H est un sous-groupe, et de même $g^{-1} \in K$, donc $g^{-1} \in H \cap K$.

Et donc $H \cap K$ est un sous-groupe de G.

2. Si l'un des deux sous-groupes est inclus dans l'autre, alors il est évident que $H \cup K$ est un sous-groupe[4].
Inversement supposons que $H \cup K$ soit un sous-groupe de G, et supposons que $H \not\subset K$ et $K \not\subset H$.
Alors il existe $h \in H \setminus K$ et il existe $k \in K \setminus H$.
Alors $hk \in H \cup K$.
▶ **Si** $hk \in H$: alors $h^{-1} \in H$ et donc $k = h^{-1}(hk) \in H$, ce qui est absurde.
▶ **Si** $hk \in K$: alors $k^{-1} \in K$ et donc $h = (hk)k^{-1} \in K$, ce qui est absurde.
Dans tous les cas, on aboutit à une contradiction, et donc $H \cup K$ sous-groupe de G implique $H \subset K$ ou $K \subset H$.

[4] Puisqu'il est égal soit à H soit à K.

Rédaction
Attention aux quantificateurs : il existe un élément dans H pas dans K, mais ce n'est pas le cas de tous les éléments de H (ne serait-ce que parce que e_G est dans H et dans K).

3. Déjà, $e_G = \underbrace{e_G}_{\in H}\underbrace{e_G}_{\in K} \in HK$.
Soient $x, y \in HK$. Alors il existe $(h, h') \in H^2$ et $(k, k') \in K^2$ tels que $x = hk$ et $y = h'k'$.
Et alors $xy = (hk)(h'k') = hkh'k' = hh'kk' = \underbrace{hh'}_{\in H}\underbrace{kk'}_{\in K} \in HK$.
Et avec les mêmes notations, $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} = \underbrace{h^{-1}}_{\in H}\underbrace{k^{-1}}_{\in K} \in HK$.
Donc HK est un sous-groupe de G.

4. Supposons que $KH = HK$. Prouvons qu'alors HK est un sous-groupe de G.
Il contient évidemment $e_G = e_G \cdot e_G$.
Soient $x, y \in HK$. Alors il existe $h_1, h_2 \in H$ et $k_1, k_2 \in K$ tels que $x = h_1 k_1$ et $y = h_2 k_2$.
Et alors $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$.
Mais $(k_1 k_2^{-1}) h_2^{-1} \in KH = HK$. Donc il existe $h \in H$ et $k \in K$ tels que $(k_1 k_2^{-1}) h_2^{-1} = hk$.
Et alors $xy^{-1} = h_1 hk = (h_1 h)k \in HK$. Donc HK est un sous-groupe de G.

Inversement, supposons que HK soit un sous-groupe de G.
Alors $K \subset HK$ (puisque $h \in H$ s'écrit $h \cdot e_G$) et $H \subset HK$, par stabilité de HK par produit, $KH \subset HK$. Inversement, soit $x \in HK$. Alors $x^{-1} \in HK$. Et donc il existe $h \in H$ et $k \in K$ tels que $x^{-1} = hk$, de sorte que $x = k^{-1}h^{-1} \in KH$. Donc $KH = HK$.

SOLUTION DE L'EXERCICE 15.12

1. Puisque les similitudes directes sont des bijections de $\mathbf{C}$ dans $\mathbf{C}$, nous allons prouver que G est un sous-groupe du groupe $\mathfrak{S}(\mathbf{C})$ des bijections de $\mathbf{C}$ dans $\mathbf{C}$.
G contient évidemment $\mathrm{id}_{\mathbf{C}} : z \mapsto z$.
Il est évident que la composée de deux similitudes directes est encore une similitude directe, donc G est stable par produit. Et si $f : z \mapsto az + b$ est une similitude directe, alors

Rappel
Il a été prouvé en cours que l'ensemble des permutations d'un ensemble est un groupe pour la composition.

$f^{-1} : z \mapsto \dfrac{z-b}{a}$ est également une similitude directe.
Donc G est stable par passage à l'inverse, et donc est un sous-groupe de $(\mathfrak{S}(\mathbf{C}), \circ)$.
Il ne s'agit pas d'un groupe abélien, par exemple car $f : z \mapsto -z$ et $g : z \mapsto z+1$ ne commutent pas :

$$f \circ g : z \mapsto -z-1 \text{ et } g \circ f : z \mapsto -z-1.$$

2. Donc G_{z_0} est l'ensemble des similitudes qui ont z_0 pour point fixe.
C'est bien le cas de l'identité, si f et g ont z_0 pour point fixe, alors $g(z_0) = z_0 \Leftrightarrow g^{-1}(z_0) = z_0$, si bien que $(f \circ g^{-1})(z_0) = f(z_0) = z_0$ et donc $f \circ g^{-1} \in G_{z_0}$.
Ainsi, G_{z_0} est un sous-groupe de G.
Soit alors $\varphi : \left| \begin{array}{ccc} \mathbf{C}^* & \longrightarrow & G_{z_0} \\ \alpha & \longmapsto & z \mapsto \alpha(z-z_0)+z_0 \end{array} \right.$.
Nous savons que toute similitude directe qui possède z_0 comme point fixe est de la forme $z \mapsto re^{i\theta}(z-z_0)+z_0$ où r est le rapport et θ l'angle de la similitude.
Donc φ est surjective, et même bijective puisque l'écriture d'une similitude sous la forme $z \mapsto az+b$ est unique.
Reste donc à voir qu'ils s'agit d'un morphisme de groupes.
Soient $\alpha_1, \alpha_2 \in \mathbf{C}^*$. Notons $f_1 = \varphi(\alpha_1) : z \mapsto \alpha_1(z-z_0)+z_0$ et $f_2 = \varphi(\alpha_2) : z \mapsto \alpha_2(z-z_0)+z_0$.
Alors $f_1 \circ f_2$ est une fonction affine, qui possède z_0 comme point fixe (car il est point fixe de z_1 et de z_2), et qui possède $\alpha_1\alpha_2$ comme coefficient dominant.
Donc pour tout $z \in \mathbf{C}$, $(f_1 \circ f_2)(z) = \alpha_1\alpha_2(z-z_0)+z_0$, c'est donc $\varphi(\alpha_1\alpha_2)$.

Alternative
Si vous n'êtes pas convaincu, faire le calcul !

Et donc f est un morphisme de groupes, c'est donc un isomorphisme de groupes.

Solution de l'exercice 15.14

1. Si G est abélien, alors les puissances de x et de y commutent.
Donc en particulier, si n, p sont deux entiers strictement positifs tels que $x^n = y^p = e_G$, alors $(xy)^{np} = x^{np}y^{np} = (x^n)^p\,(y^p)^n = e_G$.
Et donc xy est d'ordre fini.

2. Le résultat n'est plus vrai si G n'est pas abélien. Par exemple, dans le groupe des similitudes directes du plan[5], une rotation d'angle π est d'ordre fini, puisqu'élevée au carré, elle est égale à l'identité.
En revanche, la composée de deux rotations d'angle π, de centre distincts est une translation de vecteur non nul.
En effet, si $\alpha \neq \beta$ sont deux complexes, si $f : z \mapsto -z+\alpha$ et $g : z \mapsto -z+\beta$ sont deux rotations d'angle π, alors $g \circ f : z \mapsto z+(\beta-\alpha)$.
Or, une translation τ de vecteur non nul $\vec{u}$ n'est jamais d'ordre fini puisque pour tout $n \in \mathbf{N}^*$, τ^n est[6] la translation de vecteur $n\vec{u} \neq \vec{0}$.

[5] Voir l'exercice précédent.

[6] Passer par les complexes si vous avez besoin de vous en convaincre.

Solution de l'exercice 15.15

1. Soient $(g,h) \in G^2$. Alors

$$\tau_a(g)\tau_a(h) = aga^{-1}aha^{-1} = agha^{-1} = \tau_a(h).$$

Donc τ_a est un morphisme de G dans lui-même.
Pour montrer la bijectivité , il y a deux options :

- ▶soit prouver injectivité et surjectivité
- ▶soit exhiber la bijection réciproque si on la voit.

Ici, la seconde option est de loin la plus facile, puisque pour tout $g \in G$,

$$(\tau_{a^{-1}} \circ \tau_a)(g) = a^{-1}\tau_a(g)a = a^{-1}aga^{-1}a = g = \mathrm{id}_G(g).$$

Et de même, $\tau_a \circ \tau_{a^{-1}} = \mathrm{id}$, donc $\tau_{a^{-1}}$ est la bijection réciproque de τ_a.

Prouvons tout de même injectivité et surjectivité.
Pour l'injectivité, soit $g \in \mathrm{Ker}\,\tau_a$.
Alors $aga^{-1} = e \Leftrightarrow ag = ea \Leftrightarrow g = e$.
Donc τ_a est injectif.

Soit à présent $y \in G$. Alors $y = a(a^{-1}ya)a^{-1} = \tau_a\left(a^{-1}ya\right)$, et donc τ_a est surjectif.
On en déduit donc que τ_a est bijectif.

Méthode
Pour prouver l'injectivité d'un morphisme, il suffit de prouver que son noyau est réduit à l'élément neutre.
Et puisqu'on a toujours $\{e_G\} \subset \mathrm{Ker}\,\varphi$, il suffit de prouver l'inclusion réciproque, c'est à dire

$$x \in \mathrm{Ker}\,\varphi \Rightarrow x = e_G.$$

Remarque
Notons que nous venons de trouver l'unique antécédent de y, et donc la bijection réciproque de τ_a.

2. Nous venons de prouver que les τ_a sont des éléments de $\mathfrak{S}(G)$, car bijectifs.
On a $\tau_e = \mathrm{id}_G \in \mathscr{C}(G)$.
Et pour $(a,b) \in G^2$ et $g \in G$, on a

$$\left(\tau_a \circ \tau_b^{-1}\right)(g) = (\tau_a \circ \tau_{b^{-1}})(g) = \tau_a\left(b^{-1}gb\right) = ab^{-1}g\left(ab^{-1}\right)^{-1}(g).$$

Et donc $\tau_a \circ \tau_{b^{-1}} = \tau_{ab^{-1}} \in \mathscr{C}(G)$.
Ainsi, $\mathscr{C}(G)$ est bien un sous-groupe de $(\mathfrak{S}(G), \circ)$.

3. Le calcul réalisé à l'instant prouve que pour $(a,b) \in G^2$, $\tau_a \circ \tau_b = \tau_{ab}$, soit encore que $\varphi(ab) = \varphi(a) \circ \varphi(b)$, et donc φ est un morphisme de groupes.

SOLUTION DE L'EXERCICE 15.16

1. Soit H_1 un sous-groupe de G_1, et soient $y_1, y_2 \in f(H_1)$. Alors il existe deux éléments $x_1, x_2 \in H_1$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
Et alors $y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1 x_2^{-1})$. Puisque H_1 est un sous-groupe de G_1, $x_1 x_2^{-1} \in H_1$ et donc $y_1 y_2^{-1} \in f(H_1)$, de sorte que $f(H_1)$ est un sous-groupe de G_2.

2. Soit H_2 un sous-groupe de G_2, et soient $x_1, x_2 \in f^{-1}(H_2)$.
Alors $f(x_1) \in H_2$ et $f(x_2) \in H_2$.
Donc $f(x_1 x_2^{-1}) = f(x_1)f(x_2)^{-1} \in H_2$, de sorte que $x_1 x_2^{-1} \in f^{-1}(H_2)$.
Donc $f^{-1}(H_2)$ est un sous-groupe de G_2.

En particulier, $\mathrm{Ker}\, f = f^{-1}(\{e_{G_2}\})$, et $\{e_{G_2}\}$ est un sous-groupe de G_2, donc $\mathrm{Ker}\, f$ est un sous-groupe de G_1.

SOLUTION DE L'EXERCICE 15.17

1. Commençons par noter que si $z \in \mathbf{U}_{mn}$, alors $(z^n)^m = z^{mn} = 1$, si bien que $z^n \in \mathbf{U}_m$. Et de même, $z^m \in \mathbf{U}_n$, donc la définition de f est correcte.
Soient alors $z_1, z_2 \in \mathbf{U}_{mn}$. On a alors

$$f(z_1z_2) = ((z_1z_2)^n, (z_1z_2)^m) = \left(z_1^n z_2^n, z_1^m z_2^m\right) == (z_1^n, z_1^m)(z_2^n, z_2^m) = f(z_1)f(z_2).$$

Remarque
Les deux derniers produits ont lieu dans le produit direct $\mathbf{U}_m \times \mathbf{U}_n$.

2. Soit $z \in \mathbf{U}_{mn}$. Alors $z \in \mathrm{Ker}(f) \Leftrightarrow f(z) = (1,1) \Leftrightarrow z^n = z^m = 1$.
Ainsi, $\mathrm{Ker}\, f = \mathbf{U}_n \cap \mathbf{U}_m$.

Notons alors d le pgcd de m et n, de sorte que d divise à la fois m et n.
Alors si $z \in \mathbf{U}_d$, on a $z^m = \left(z^d\right)^{\frac{m}{d}} = 1$ et de même $z^n = 1$.
Ainsi, $\mathbf{U}_d \subset \mathbf{U}_m \cap \mathbf{U}_n$.
D'autre part, par Bézout, il existe $u, v \in \mathbf{Z}$ tels que $mu + nv = d$.
Et alors si $z \in \mathbf{U}_m \cap \mathbf{U}_n$, alors $z^d = z^{mu+nv} = (z^m)^u (z^n)^v = 1$, et donc $\mathbf{U}_m \cap \mathbf{U}_n \subset \mathbf{U}_d$.
Par double inclusion, $\mathrm{Ker}\, f = \mathbf{U}_m \cap \mathbf{U}_n = \mathbf{U}_d$.

3. Par la question précédente, f est injective si et seulement si $\mathrm{Ker}\, f = \{1\}$, donc si et seulement si $\mathbf{U}_d = \{1\}$, soit si et seulement si m et n sont premiers entre eux.
Donc déjà, si f est un isomorphisme, alors m et n sont premiers entre eux.

Et inversement, si m et n sont premiers entre eux, alors f est injective. Et de plus puisque $\mathbf{U}_{mn}$ et $\mathbf{U}_m \times \mathbf{U}_n$ sont tous deux de cardinal mn, f est bijective, donc est un isomorphisme.

Cardinal
C'est un résultat qui sera prouvé plus tard, et qu'on formalisera en temps voulu. Mais il doit être assez intuitif pour l'instant : si $f : E \to F$ est une injection entre deux ensembles finis de même cardinal, alors f prend au maximum une fois chaque valeur, et donc doit prendre toutes les valeurs. Autrement dit doit être surjective (et donc bijective).

Si on veut éviter cet argument de cardinal, il est également possible de prouver «à la main» que f est surjective.
Notons alors $\zeta = \exp\left(\frac{2i\pi}{mn}\right)$.
Alors $\mathbf{U}_{mn} = \{\zeta^k, k \in \mathbf{Z}\}$, $\mathbf{U}_m = \{\zeta^{nk}, k \in \mathbf{Z}\}$ et $\mathbf{U}_n = \{\zeta^{mk}, k \in \mathbf{Z}\}$.
Soit donc $(z_1, z_2) \in \mathbf{U}_n \times \mathbf{U}_m$, et soient $a, b \in \mathbf{Z}$ tels que $z_1 = \zeta^{na}$ et $z_2 = \zeta^{mb}$.
Partons alors de deux entiers[7] u, v tels que $1 = mu + nv$, et soit $k = bmu + anv$. Alors $k \equiv anv\ [m]$, et puisque $1 = mu + nv$, $nv \equiv 1\ [m]$, si bien que $anv \equiv a\ [m]$.
Donc $\left(\zeta^k\right)^n = (\zeta^a)^n = \zeta^{na} = z_1$.
Et de même, $\left(\zeta^k\right)^m = \zeta^{mb} = z_2$.

Et ainsi, $f\left(\zeta^k\right) = (z_1, z_2)$, si bien que f est surjectif.

[7] Qui existent par le théorème de Bézout.

Solution de l'exercice 15.18

Soit $\varphi : \mathbf{Z} \to \mathbf{Z}$ un morphisme de groupes. Alors $\varphi(0) = 0$.
Notons $k = \varphi(1)$. Alors $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = k + k = 2k$.
Puis $\varphi(3) = \varphi(2+1) = \varphi(2) + \varphi(1) = 2k + k = 3k$.
Une récurrence facile prouve alors que pour tout $n \in \mathbf{N}$, $\varphi(n) = nk$.
Et pour $n \in \mathbf{Z}$ négatif, $\varphi(n) = -\varphi(-n)$, où $-n \in \mathbf{N}$ et donc $\varphi(n) = -(-nk) = nk$.
Inversement, il est facile de constater que pour $k \in \mathbf{Z}$ fixé, $\varphi : n \mapsto nk$ est bien un morphisme de $(\mathbf{Z}, +)$ dans lui-même car

$$\forall (p,q) \in \mathbf{Z}^2, \varphi(p+q) = (p+q)k = pk + qk = \varphi(p) + \varphi(q).$$

Donc les morphismes de $(\mathbf{Z}, +)$ dans lui-même sont les $n \mapsto kn$, $k \in \mathbf{Z}$.

Soit à présent $\varphi : \mathbf{Q} \to \mathbf{Z}$ un morphisme. Soit alors $r \in \mathbf{Q}$ non nul, et soit $n \in \mathbf{N}$.
Alors $\varphi(r) = \varphi\left(\frac{r}{n} + \frac{r}{n} + \cdots + \frac{r}{n}\right) = \varphi\left(\frac{r}{n}\right) + \cdots + \varphi\left(\frac{r}{n}\right) = n\varphi\left(\frac{r}{n}\right)$.
Or, $\varphi(r)$, $\varphi\left(\frac{r}{n}\right)$ et n sont tous des entiers, donc n divise $\varphi(r)$, et ce quel que soit $n \in \mathbf{N}$.
Le seul entier étant divisible par tous les autres est 0, et donc $\varphi(r) = 0$ pour tout $r \in \mathbf{Q}$: φ est le morphisme nul.

Solution de l'exercice 15.19

> **⚠ Attention !**
> On ne sait pas encore si $a^0 = e_G$ est dans A.

Soit $a \in A$. Puisque A est stable par $*$, pour tout $n \in \mathbf{N}^*$, $a^n \in A$.
Mais A étant fini, ces puissances ne sauraient être toutes distinctes : il existe deux entiers distincts n et p tels que $a^n = a^p$.
Quitte à échanger n et p, supposons que $p > n$. Alors $a^n = a^p \Leftrightarrow a^{p-n} = e_G$.
Donc déjà, $e_G \in A$ car $p - n \in \mathbf{N}^*$. Et donc $\{a^k, k \in \mathbf{N}\} \subset A$.
De plus, $a * a^{p-n-1} = e_G$, de sorte que $a^{p-n-1} = a^{-1}$.
Or, $p - n - 1 \geqslant 0$, donc $a^{-1} \in A$.
Ainsi, nous avons prouvé que A contient l'élément neutre, et est stable par passage à l'inverse : si $a \in A$, alors $a^{-1} \in A$.
Puisque A est de plus stable par $*$, il s'agit d'un sous-groupe de G.

Solution de l'exercice 15.20

> **Remarque**
> Nous avons prouvé mieux que ce qui était demandé : non seulement il existe $g \in G$ tel que $G = \langle g \rangle$, mais en plus tout élément g différent de e possède cette propriété.

Notons e le neutre de G. Alors $G \neq \{e\}$, car sinon G serait l'unique sous-groupe de G.
Donc G et $\{e\}$ sont deux sous-groupes distincts de G, qui sont donc nécessairement les deux seuls sous-groupes de G.
Soit $g \in G \setminus \{e\}$, de sorte que $\langle g \rangle \neq \{e\}$.
Alors $\langle g \rangle$ est un sous-groupe de G, donc nécessairement égal à G.

Notons que $\langle x \rangle$ étant toujours un sous-groupe abélien de G (car deux puissances de g commutent entre elles), ceci prouve que G est un groupe abélien.

Soit donc $g \in G \setminus \{e\}$ fixé, de sorte que $G = \langle g \rangle = \{g^n, n \in \mathbf{Z}\}$.
Si $g^2 = e$, alors $G = \{e, g\}$ est fini, de cardinal 2.
Sinon, $\langle g^2 \rangle$ est un sous-groupe de G, différent de $\{e\}$, donc encore égal à G tout entier.
Donc en particulier, il existe $k \in \mathbf{Z}$ tel que $g = g^{2k}$, et alors $g^{2k-1} = e$.
Quitte à changer g en g^{-1}, supposons que $2k - 1 > 0$.
Alors pour tout $n \in \mathbf{Z}$, si $n = (2k-1)q + r$ est la division euclidienne de n par $2k-1$, avec $0 \leqslant r \leqslant 2k-2$, il vient $g^n = g^{q(2k-1)+r} = \left(g^{2k-1}\right)^q g^r = g^r$.
Et donc $\langle g \rangle = \{g^r, r \in [\![0, 2k-2]\!]\}$ est fini, de cardinal au plus égal à $2k-2$.

Notons $p = \mathrm{Card}(G)$. Alors pour tout $k \in [\![1, p-1]\!]$, $\langle g^k \rangle$ est un sous-groupe de G, donc soit égal à $\{e\}$, soit égal à G.
Si $\langle g^k \rangle = \{e\}$, alors $g^k = e$. Mais alors comme précédemment, $G = \{g^r, 0 \leqslant r < k\}$ est de cardinal inférieur ou égal à k et donc de cardinal inférieur strict à p, ce qui est absurde.
Prouvons que $g^p = e$. En effet, les éléments $e, g, \ldots, g^{p-1}$ sont deux à deux distincts, car si on avait $g^k = g^\ell$ avec $0 \leqslant k \leqslant \ell < p$, alors $g^{\ell-k} = e$, avec $\ell - k \in [\![1, p-1]\!]$, et nous venons de prouver que ceci est impossible.
Donc $G = \{e, g, g^2, \ldots, g^{p-1}\}$. Et puisque $g^p \in G$, il existe $k \in [\![0, p-1]\!]$ tel que $g^p = g^k$.
Et encore une fois, si on avait $k \neq 0$, alors $g^{p-k} = e$, avec $p - k \in [\![1, p-1]\!]$.
Donc on a bien $g^p = e$.

Supposons que p ne soit pas premier, et soient $a, b \in \mathbf{N}$ tels que $p = ab$, avec $a > 1$ et $b > 1$.
Alors $(g^a)^b = g^{ab} = g^p = e$, et donc $\langle g^a \rangle = \{e, g^a, \dots, g^{a(b-1)}\}$ est un sous-groupe de G de cardinal b, donc qui n'est égal ni à $\{e\}$ ni à G.
C'est absurde puisque G ne possède que deux sous-groupes. Et donc p est premier.

SOLUTION DE L'EXERCICE 15.21

Il est clair que $1 \in \mathbf{Z}\left[\sqrt{2}\right]$ car $1 = 1 + 0\sqrt{2}$. Soient $(x, y) \in \mathbf{Z}\left[\sqrt{2}\right]^2$. Alors il existe quatre entiers a, b, c, d tels que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$.
Et donc $x - y = \underbrace{a - c}_{\in \mathbf{Z}} + \underbrace{(b - d)}_{\in \mathbf{Z}}\sqrt{2} \in \mathbf{Z}\left[\sqrt{2}\right]$.

> **Méthode**
> Pour montrer qu'un ensemble est muni d'une structure d'anneau, toujours commencer par se demander s'il ne pourrait pas s'agir d'un sous-anneau d'un ensemble déjà connu.
> En effet, il y a bien moins de propriétés à prouver pour un sous-anneau que pour un anneau.

De même, $xy = \underbrace{ac + 2bd}_{\in \mathbf{Z}} + \underbrace{(ad + bc)}_{\in \mathbf{Z}}\sqrt{2} \in \mathbf{Z}\left[\sqrt{2}\right]$.
Donc $\mathbf{Z}\left[\sqrt{2}\right]$ est un sous-anneau de $(\mathbf{R}, +, \times)$, et en particulier est un anneau.

Les mêmes types de calculs, en remplaçant $\mathbf{Z}$ par $\mathbf{Q}$ prouvent que $\mathbf{Q}\left(\sqrt{2}\right)$ est un anneau.
De plus, soit x un élément non nul de $\mathbf{Q}\left(\sqrt{2}\right)$.
Alors il existe deux rationnels a et b tels que $x = a + b\sqrt{2}$.
Et alors l'inverse[8] de x

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbf{Q}\left(\sqrt{2}\right).$$

Et donc tout élément non nul est inversible : $\mathbf{Q}\left(\sqrt{2}\right)$ est bien un corps.

Le même raisonnement prouve que pour $d \in \mathbf{N}^*$, $\mathbf{Q}(\sqrt{d})$ est un sous-anneau de $\mathbf{R}$ dans lequel tout élément est inversible., et donc est un corps.

Si $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}$, alors $\sqrt{d} \in \mathbf{Q}$. Il est alors classique que ceci est le cas si et seulement si $\sqrt{d} \in \mathbf{N}$, c'est-à-dire si et seulement si d est un carré parfait.
Et inversement, si d est un carré parfait, alors il est facile de voir que $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}$.

[8] Dans le corps $\mathbf{R}$.

SOLUTION DE L'EXERCICE 15.22

Rappelons que $\mathbb{D} = \left\{\frac{n}{10^k},\ (n, k) \in \mathbf{Z} \times \mathbf{N}\right\}$.

Nous allons prouver qu'il s'agit d'un sous-anneau de $\mathbf{Q}$.
On a $1 = \frac{1}{10^0} \in \mathbb{D}$.
Soient x, y deux nombre décimaux. Alors il existe des $(k_1, k_2) \in \mathbf{Z}^2$ et $(n_1, n_2) \in \mathbf{N}^2$ tels que $x = \frac{k_1}{10^{n_1}}$ et $y = \frac{k_2}{10^{n_2}}$. Et alors

$$x - y = \frac{k_1}{10^{n_1}} - \frac{k_2}{10^{n_2}} = \frac{10^{n_2}k_1 - 10^{n_1}k_2}{10^{n_1+n_2}} \in \mathbb{D}.$$

Et de même, $xy = \frac{k_1 k_2}{10^{n_1+n_2}} \in \mathbb{D}$.
Donc il s'agit d'un sous-anneau de $\mathbf{Q}$.
Il ne s'agit pas d'un corps, car bien que $3 \in \mathbb{D}$, $\frac{1}{3}$ n'est pas décimal, puisque les diviseurs premiers du dénominateur d'un nombre décimal ne peuvent qu'être 2 et/ou 5.

SOLUTION DE L'EXERCICE 15.23

Ici, pas question de prouver qu'il s'agit d'un sous-anneau de quelque chose déjà connu, il va donc tout falloir reprouver.
Avec tout de même une bonne nouvelle : il a déjà été prouvé en cours que $(A \times B, \oplus)$ est un groupe[9], abélien car A et B le sont.
Il reste donc à prouver que $\otimes$ est associative, qu'elle possède un élément neutre (qui est $(1_A, 1_B)$), et qu'elle est distributive par rapport à $\oplus$.

[9] C'est celui que nous avons appelé produit direct de A et B.

Prouvons juste ce dernier point, en traitant par exemple le cas de la distributivité à gauche : soient (x_A, x_B), (y_A, y_B) et (z_A, z_B) trois éléments de $A \times B$. Alors

$$\begin{aligned}(x_A, x_B) \otimes ((y_A, y_B) \otimes (z_A, z_B)) &= (x_A, x_B) \otimes ((y_A +_A z_A, y_B +_B z_B)) \\ &= (x_A \times_A (y_A +_A z_A), x_B \times_B (y_B +_B z_B)) \\ &= (x_A \times_A y_A +_A x_A \times_A z_A, x_B \times_B y_B +_B x_B \times_B z_B) \\ &= (x_A \times_A y_A, x_B \times_B y_B) \oplus (x_A \times_A z_A, x_B \times_B z_B) \\ &= ((x_A, y_A) \otimes (x_B, y_B)) \oplus ((x_A, y_A) \otimes (z_A, z_B))\,.\end{aligned}$$

$\times_A$ est ditributive par rapport à $+_A$, et idem dans B.

On prouverait de même la distributivité à droite.
Bref, $A \times B$ est un anneau, et il est facile de constater qu'il est commutatif si A et B le sont, et même qu'il s'agit là d'une condition nécessaire et suffisante.
En revanche, même si A et B sont intègres, dès que A et B sont non nuls, on a $A \times B$ qui n'est pas intègre.
En effet, pour $a \in A \setminus \{0_1\}$ et $b \in B \setminus \{0_B\}$, $(a, 0_B) \otimes (0_A, b) = (0_A, 0_B)$, sans qu'aucun des deux facteurs ne soit nul.

Enfin, si A est nul, alors tout élément de $A \times B$ est de la forme $(0_A, b)$, avec $b \in B$.
Donc si B est intègre, alors $(0_A, b_1) \otimes (0_A, b_2) = (0_A, 0_B) \Leftrightarrow b_1 b_2 = 0_B \Leftrightarrow b_1 = 0_B$ **ou** $b_2 = 0_B$.
Donc $A \times B$ est intègre.
En revanche, si B n'est pas intègre, et que a, b sont deux diviseurs de zéro tels que $ab = 0_B$, alors $(0_A, a) \otimes (0_A, b) = (0_A, 0_B)$, et donc $(0_A, a)$ est un diviseur de zéro dans $A \times B$, qui n'est donc pas intègre.

Solution de l'exercice 15.24

1. Non, car la suite constante égale à 1 n'est pas dedans.
2. Non, car l'opposée d'une suite strictement croissante n'est plus croissante.
3. Oui.
4. Non : la suite nulle n'est pas divergente.
5. Oui : la suite constante égale à 1 est bornée.
   Et si (u_n) et (v_n) sont deux suites bornées, soient $K_1, K_2 \in \mathbf{R}$ tels que $\forall n \in \mathbf{N}$, $|u_n| \leqslant K_1$ et $|v_n| \leqslant K_2$.
   Alors pour tout $n \in \mathbf{N}$, $|u_n - v_n| \leqslant |u_n| + |v_n| \leqslant K_1 + K_2$.
   Et de même, $|u_n v_n| \leqslant K_1 K_2$.
   Donc $(u_n - v_n)$ et $(u_n v_n)$ sont bornées.
6. Non : l'opposé d'une suite qui tend vers $+\infty$ tend vers $-\infty$.
7. Oui : la suite constante égale à 1 est stationnaire[10].
   Si (u_n) et (v_n) sont stationnaires, alors il existe $n_0 \in \mathbf{N}$ et $n_1 \in \mathbf{N}$ tels que $n \geqslant n_0 \Rightarrow u_n = u_{n_0}$ et $n \geqslant n_1 \Rightarrow v_n = v_{n_1}$.
   Mais alors pour $n \geqslant \max(n_0, n_1)$, on a $u_n - v_n = u_{n_0} - v_{n_1}$, et donc $(u_n - v_n)$ est stationnaire.
   De même, pour $n \geqslant \max(n_0, n_1)$, $u_n v_n = u_{n_0} v_{n_1}$.
   Donc on a bien un sous-anneau de $\mathbf{R}^{\mathbf{N}}$.
8. Non, la suite constante égale à 1 n'est pas dedans.

[10] Puisque constante.

Solution de l'exercice 15.25

Puisqu'un morphisme d'anneaux est en particulier un morphisme de groupes additifs, il est injectif si et seulement si son noyau ne contient que 0_k.

Mais si $x \in k \setminus \{0_k\}$, alors x est inversible, et donc $f(x)$ est inversible d'inverse $f(x)^{-1}$, et en particulier $f(x) \neq 0$. On en déduit que $x \notin \operatorname{Ker} f$.
Et donc $\operatorname{Ker} f \subset \{0_k\}$. L'inclusion réciproque étant triviale, on a donc $\operatorname{Ker} f = \{0_k\}$, et donc f est injectif.

Rappel

Un morphisme d'anneaux $f : A \to B$ envoie les inversibles de A sur des inversibles de B.

Solution de l'exercice 15.26

1. Supposons A intègre, et soit $a \in A$ possédant une racine carrée b : $a = b^2$.
   Si c est une racine carrée de a, on a donc $c^2 = b^2 \Leftrightarrow c^2 - b^2 = 0_A$.
   Soit encore[11], $(c - b)(c + b) = 0_A$.
   Puisque A est intègre, on a donc $c - b = 0_A$ ou $c + b = 0_A$, et donc $c = b$ ou $c = -b$.

[11] Et là, l'hypothèse que A est commutatif est importante.

Donc a possède au plus deux racines carrées.

Bien entendu, vous connaissez bien l'anneau intègre $\mathbf{R}$: nous ne venons pas de dire que tout élément de A possède exactement deux racines carrées, mais bien au plus deux.

2. Pour $a \in \mathbf{R}$, la fonction définie par $f_a(x) = \begin{cases} 1 & \text{si } x \leqslant a \\ -1 & \text{si } x > a \end{cases}$ est telle que $f_a \times f_a = \tilde{1}$, et donc est une racine carrée de $\tilde{1}$.
Et donc, cette dernière possède une infinité de racines carrées.

SOLUTION DE L'EXERCICE 15.27

Nous allons prouver que $\mathcal{F}(E,A)$ est intègre si et seulement si E est un singleton et que A est intègre.
Si $E = \{x\}$ est un singleton et que A est intègre, soient alors $f, g \in \mathcal{F}(E,A)$ telles que $f \times g = \widetilde{0}$, la fonction nulle.
Alors $f(x)g(x) = 0_A$, et donc par intégrité de A, $f(x) = 0_A$ ou $g(x) = 0_A$.
Mais alors f est la fonction nulle[12], ou g est la fonction nulle. Donc $\mathcal{F}(E,A)$ est intègre.

[12] Qui est le neutre additif de $\mathcal{F}(E,A)$.

En revanche, si $\text{Card}(E) \geqslant 2$, alors soient x, y deux éléments distincts de $\mathcal{F}(E,A)$. Alors les fonctions $f : \left| \begin{array}{ccc} E & \longrightarrow & A \\ t & \longmapsto & \begin{cases} 1_A & \text{si } t = x \\ 0_A & \text{sinon} \end{cases} \end{array} \right.$ et $g : \left| \begin{array}{ccc} E & \longrightarrow & A \\ t & \longmapsto & \begin{cases} 1_A & \text{si } t = y \\ 0_A & \text{sinon} \end{cases} \end{array} \right.$ sont non nulles mais vérifient $f \times g = \widetilde{0}$.
Donc $\mathcal{F}(E,A)$ n'est pas intègre.

Et si A n'est pas intègre, soient alors x, y deux diviseurs de zéro tels que $xy = 0_A$. Alors les fonctions constantes égales respectivement à x et y ne sont pas nulles, mais leur produit l'est, donc sont des diviseurs de zéro.

SOLUTION DE L'EXERCICE 15.28

1. Notons n et p deux entiers tels que $x^n = y^p = 0_A$.
Puisque x et y commutent, $(xy)^n = x^n y^n = 0_A y^n = 0_A$. Et donc xy est nilpotent.

Par la formule du binôme de Newton[13], on a

$$\begin{aligned}(x+y)^{n+p} &= \sum_{k=0}^{n+p} \binom{n+p}{k} x^k y^{n+p-k} \\ &= \sum_{k=0}^{n} \binom{n+p}{k} x^k y^{n+p-k} + \sum_{k=n+1}^{n+p} \binom{n+p}{k} x^k y^{n+p-k} \\ &= \sum_{k=0}^{n} \binom{n+p}{k} x^k 0_A + \sum_{k=n+1}^{n+p} \binom{n+p}{k} 0_A y^{n+p-k} = 0_A.\end{aligned}$$

[13] Et là aussi, l'hypothèse que x et y commutent est indispensable.

Détails
Si $k \leqslant n$, $n+p-k \geqslant p$, et donc $y^{n+p-k} = 0_A$.
Et si $k \geqslant n$, $x^k = 0_A$.

Et donc $x + y$ est nilpotent.

2. Soit $n \in \mathbf{N}$ tel que $x^n = 0_A$. Alors, $1_A = 1_A - x^n = 1_A^n - x^n$, et donc, par la troisième identité remarquable généralisée, qui s'applique puisque 1_A et x commutent,

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

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

SOLUTION DE L'EXERCICE 15.29

Soit $(A, +, \times)$ un anneau intègre de cardinal n.
Pour prouver que A est un corps, il suffit de prouver que tout élément non nul de A admet un inverse.
Soit donc $x \neq 0_A$.

Rappel
Par définition, un anneau intègre est commutatif et n'est pas l'anneau nul.

Alors l'application $f : \left|\begin{array}{ccc} A & \longrightarrow & A \\ y & \longmapsto & xy \end{array}\right.$ est injective.
En effet, si $f(y_1) = f(y_2)$, alors

$$xy_1 = xy_2 \Leftrightarrow xy_1 - xy_2 = 0 \Leftrightarrow x(y_1 - y_2) = 0_A.$$

Mais A étant intègre, et x étant non nul, il vient nécessairement $y_1 - y_2 = 0_A \Leftrightarrow y_1 = y_2$.

Or, A étant de cardinal fini, f est injective si et seulement si elle est bijective[14].
En particulier, 1_A admet un antécédent par f : il existe $y \in A$ tel que $xy = 1_A$. Puisque A est commutatif, on a alors $yx = 1_A$, et donc y est l'inverse de x.
Par conséquent, tout élément non nul de A est inversible : A est un corps.

[14] Ce résultat plutôt intuitif sera prouvé bien plus tard.

Alternative : soit $x \in A \setminus \{0_A\}$. Puisque A est fini, les x^k, $k \in \mathbf{N}$ ne peuvent pas être deux à deux distincts.
Et donc il existe $k < k'$ deux entiers distincts tels que $x^k = x^{k'}$.
Soit encore $x^k - x^{k'} = 0_A \Leftrightarrow x^k \left(1_A - x^{k'-k}\right) = 0_A$.
Puisque A est intègre et x non nul, $x^k \neq 0_A$, si bien que

$$1_A - x^{k'-k} = 0_A \Leftrightarrow x^{k'-k} = 1_A \Leftrightarrow xx^{k'-k-1} = 1_A.$$

Donc x est inversible, et $x^{-1} = x^{k'-k-1}$.
Et tout élément non nul de A étant inversible, A est un corps.

Solution de l'exercice 15.30

1. Soit $x \in A$. Alors $0_A = x0_A \in xA$, qui est donc non vide.
Soient xu, xv deux éléments de xA. Alors $xu - xv = x(u - v)$, qui est un élément de xA.
Donc déjà xA est un sous-groupe de $(A, +)$.
Si $u \in xA$, alors il existe $v \in A$ tel que $u = xv$. Et alors pour $y \in A$, $yu = yxv = x(yv) \in xA$.
Donc xA est un idéal de A.

2.a. Il s'agit de remarquer que si I et J sont deux idéaux, alors $I + J = \{x + y,\ (x, y) \in I \times J\}$ est encore un idéal de A.
En effet, si $x + y$ et $x' + y'$ sont deux éléments de $I + J$, avec $(x, x') \in I^2$ et $(y, y') \in J^2$, alors

$$(x + y) - (x' + y') = (x - x') + (y - y') \in I + J$$

car I et J sont des sous-groupes.
Et pour $a \in A$, et $x + y \in I + J$, on a $ax \in I$ car I est un idéal et de même $ay \in J$, donc $a(x + y) = ax + ay \in I + J$.
Donc $I + J$ est un idéal de A.

Soit donc I un idéal maximal, et soit $x \in A \setminus I$. Alors $I + xA$ est un idéal de A, qui contient I, et qui contient même strictement I, puisqu'il contient x, qui n'est pas dans I.
Par maximalité de I, ceci signifie donc que $I + xA = A$.

Et inversement, supposons que pour tout $x \in A \setminus I$, $I + xA = A$.
Soit alors J un idéal de A, différent de A, et contenant I. Supposons que $J \neq I$. Alors il existe $x \in J \setminus I$, pour lequel $I + xA = A$.
Mais $I + xA \subset J$, donc $A \subset J$, et donc $J = A$.
Ceci est absurde, et donc c'est que $J = I$, ce qui prouve que I est maximal.

2.b. Soit I un idéal maximal, et soient $(a, b) \in A^2$ tels que $ab \in I$. Supposons que $a \notin I$.
Alors $I + aA = A$ par la question précédente.
Et donc en particulier, $1 \in A$, et donc il existe $x \in I$ et $y \in A$ tels que $x + ay = 1$. Après multiplication par b, on a donc $bx + bay = b$.
Mais $x \in I$, donc $bx \in I$, par définition d'un idéal. Et $ab \in I$, donc $yab \in I$.
Et, donc par stabilité de I pour la somme[15], $b = bx + aby \in I$.
On prouve de la même manière que si $ab \in I$ et $b \notin I$, alors $a \in I$.
Et donc I est bien un idéal premier de A.

[15] Rappelons que c'est un sous-groupe de $(A, +)$.

3. Supposons que A soit un corps, et soit I un idéal de A.
Si $I = \{0\}$, alors I est premier car A est intègre : $ab = 0 \Rightarrow a = 0$ ou $b = 0$.
En revanche, si $I \neq \{0\}$, alors il existe $x \in I$ non nul.

Et donc $1 = xx^{-1} \in I$. Et donc pour tout $a \in A$, $a \times 1 = a \in I$. Et ainsi, $I = A$.
Or, il est évident que A est premier.

> **Remarque**
> Nous venons au passage de prouver qu'un idéal qui contient 1 est nécessairement A tout entier.

Inversement, supposons que tout idéal de A autre que A soit premier.
Puisque $\{0\}$ est un idéal, il est premier, et donc A est intègre.
Soit $a \in A$. Alors l'idéal a^2A est alors soit égal à A tout entier, soit premier.
Dans le premier cas, cela signifie qu'il existe $b \in A$ tel que $a^2b = 1$, et donc a est inversible.
Dans le second cas, puisque $a^2 \in I$, $a \in I$ (ou $a \in I$). Et donc il existe $b \in I$ tel que $a^2b = a \Leftrightarrow a(ab-1) = 0$.
Puisque A est intègre, si $a \neq 0$, alors $ab = 1$, et donc a est inversible.
Par conséquent, tout élément non nul de A est inversible : A est un corps.

> **Détails**
> Sans récurrence, ceci tient au fait que pour un morphisme de groupes, pour tout x et pour tout $n \in \mathbf{Z}$, $f(x^n) = f(x)^n$.
> Ici le groupe est un groupe additif, et donc on note $n \cdot 1$ au lieu de 1^n.

SOLUTION DE L'EXERCICE 15.31

1. Par définition, $f(1) = 1$.
Et donc pour tout $n \in \mathbf{Z}$, $f(n) = nf(1) = n$.
Soit alors $\frac{p}{q} \in \mathbf{Q}$, avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$. Alors

$$f\left(\frac{p}{q}\right) = f\left(p\frac{1}{q}\right) = f(p)f\left(\frac{1}{q}\right) = \frac{f(p)}{f(q)} = \frac{p}{q}.$$

Et donc pour tout $r \in \mathbf{Q}$, $f(r) = r$, si bien que $f_{|\mathbf{Q}} = \mathrm{id}_{\mathbf{Q}}$.

2. Soient $x, y \in \mathbf{R}$ tels que $x \leqslant y$.
On souhaite alors prouver que $f(x) \leqslant f(y)$.
Mais puisque f est un morphisme,

$$f(x) \leqslant f(y) \Leftrightarrow 0 \leqslant f(y) - f(x) \Leftrightarrow 0 \leqslant f(y-x).$$

Puisque $y - x \geqslant 0$, $y - x = \sqrt{y-x}^2$, et donc

$$f(y-x) = f\left(\sqrt{y-x}^2\right) = f\left(\sqrt{y-x}\right)^2 \geqslant 0.$$

Et donc on a bien $f(y-x) \geqslant 0$ et donc $f(x) \leqslant f(y)$.
Ainsi, f est croissant.

3. Soit $x \in \mathbf{R}$. Alors il existe deux suites (a_n), (b_n) de rationnels, convergeant toutes deux vers x, telles que pour tout $n \in \mathbf{N}$, $a_n \leqslant x \leqslant b_n$.
Et alors par croissance de f, pour tout $n \in \mathbf{N}$, $f(a_n) \leqslant f(x) \leqslant f(b_n)$, si bien que par la question 1, $a_n \leqslant f(x) \leqslant b_n$.
Par passage à la limite, $x \leqslant f(x) \leqslant x$, et donc $f(x) = x$.
Ainsi, pour tout $x \in \mathbf{R}$, $f(x) = x$, et donc $f = \mathrm{id}_{\mathbf{R}}$.

> **Détails**
> Il suffit de prendre a_n (resp. b_n) l'approximation décimale par défaut (resp. par excès) de x à 10^{-n} près.