

1 Groupes

Exercice 1 ★★ Un exemple de groupes –

On définit, pour (x, y) et (x', y') dans $\mathbb{R}^* \times \mathbb{R}$,

$$(x, y) \star (x', y') = (xx', xy' + y).$$

1. Démontrer que $(\mathbb{R}^* \times \mathbb{R}, \star)$ est un groupe. Est-il commutatif ?
2. Simplifier $(x, y)^n$ pour tout $(x, y) \in \mathbb{R}^* \times \mathbb{R}$ et tout $n \in \mathbb{N}^*$.

[Indication ▼](#) [Correction ▼](#)

[3213]

Exercice 2 ★ Sous-groupes ou non ? –

Dans les questions suivantes, déterminer si la partie H est un sous-groupe du groupe G .

1. $G = (\mathbb{Z}, +)$; $H = \{\text{nombre pairs}\}$.
2. $G = (\mathbb{Z}, +)$; $H = \{\text{nombre impairs}\}$.
3. $G = (\mathbb{R}, +)$; $H = [-1, +\infty[$.
4. $G = (\mathbb{R}^*, \times)$; $H = \mathbb{Q}^*$.
5. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G; f(x) = x\}$ où E est un ensemble et $x \in E$.
6. $G = (\{\text{bijections de } E \text{ dans } E\}, \circ)$; $H = \{f \in G; f(x) = y\}$ où E est un ensemble et $x, y \in E$ avec $x \neq y$.

[Indication ▼](#) [Correction ▼](#)

[2578]

Exercice 3 ★★ Quelques exemples de sous-groupes –

Démontrer pour chaque question que H est un sous-groupe de G .

1. $G = (\mathbb{C}^*, \times)$ et $H = \{z \in \mathbb{C}^*; \exists n \in \mathbb{N}^*, z^n = 1\}$.
2. $G = (\mathbb{R}^*, \times)$ et $H = \{a + b\sqrt{2}; a, b \in \mathbb{Q}, (a, b) \neq (0, 0)\}$.

[Indication ▼](#) [Correction ▼](#)

[13214]

Exercice 4 ★★★ Quelques sous-groupes usuels –

Soit (G, \cdot) un groupe. Démontrer que les parties suivantes sont des sous-groupes de G :

1. $C(G) = \{x \in G; \forall y \in G, xy = yx\}$ ($C(G)$ s'appelle le centre de G);
2. $aHa^{-1} = \{aha^{-1}; h \in H\}$ où $a \in G$ et H est un sous-groupe de G .
3. On suppose de plus que G est commutatif. On dit que x est un élément de torsion de G s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Démontrer que l'ensemble des éléments de torsion de G est un sous-groupe de G .

[Indication ▼](#) [Correction ▼](#)

[1302]

Exercice 5 ★★★ Sous-groupe d'une courbe –

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

[Indication ▼](#) [Correction ▼](#)

[1304]

Exercice 6 ★★★★★ Sous-groupe engendré par une partie –

Dans cet exercice, G désigne un groupe.

1. Soit $(H_i)_{i \in I}$ une famille quelconque de sous-groupes de G . Démontrer que $\bigcap_{i \in I} H_i$ est un sous-groupe de G .
2. Soit X une partie de G . On note $\langle X \rangle$ l'intersection de tous les sous-groupes de G contenant X . Démontrer que $\langle X \rangle$ est le plus petit sous-groupe de G contenant X .
3. Démontrer que

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}; n \in \mathbb{N}, x_i \in X, \varepsilon_i = \pm 1 \text{ pour } i = 1, \dots, n\}$$

(avec la convention qu'un produit vide vaut 1_G).

[Indication ▼](#) [Correction ▼](#)

[3215]

Exercice 7 ★ Intersection de deux sous-groupes –

Soit G un groupe et H_1, H_2 deux sous-groupes de G . Démontrer que $H_1 \cap H_2$ est un sous-groupe de G .

[Indication ▼](#) [Correction ▼](#)

[3216]

Exercice 8 ★ Produit de groupe et sous-groupe du produit –

Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

[Indication ▼](#) [Correction ▼](#)

[1305]

Exercice 9 ★★ Union de deux sous-groupes –

Soit G un groupe et H, K deux sous-groupes de G . Démontrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

[Indication ▼](#) [Correction ▼](#)

[1306]

Exercice 10 ★★★ Produit de deux sous-groupes –

Soit (G, \cdot) un groupe et A, B deux sous-groupes de G . On note $AB = \{ab; a \in A, b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

[Indication ▼](#) [Correction ▼](#)

[1307]

Exercice 11 ★★★★★ Théorème de Lagrange –

Soit (G, \cdot) un groupe fini et H un sous-groupe de G .

1. Montrer que pour tout $a \in G, H$ et $aH = \{ah; h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \emptyset$.
3. En déduire que le cardinal de H divise le cardinal de G .

[Indication ▼](#) [Correction ▼](#)

[1309]

Exercice 12 ★ Des propriétés bien connues –

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1. $\ln(xy) = \ln(x) + \ln(y)$;
2. $|zz'| = |z||z'|$;
3. $\sqrt{xy} = \sqrt{x}\sqrt{y}$;
4. $e^{x+y} = e^x e^y$;

[Indication ▼](#) [Correction ▼](#)

[1310]

Exercice 13 ★ Exponentielle complexe –

Justifier que \exp est un morphisme de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \cdot) . Quel est son image ? Son noyau ?

[Indication ▼](#) [Correction ▼](#)

[1313]

Exercice 14 ★★ Morphismes de \mathbb{Z} dans \mathbb{Z} –

Déterminer tous les morphismes de $(\mathbb{Z}, +)$ dans lui-même. Lesquels sont injectifs ? surjectifs ?

[Indication ▼](#) [Correction ▼](#)

[1311]

Exercice 15 ★★ Morphismes que $(\mathbb{Q}, +)$ –

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

Exercice 16 ★★ Morphisme entre groupes de torsion et groupes sans torsion –

Dans un groupe (G, \cdot) , un élément x est dit de torsion s'il existe $n \geq 1$ tel que $x^n = e$. On dit que G est de torsion si tous ses éléments sont de torsion. On dit que G est sans torsion si son seul élément de torsion est l'élément neutre. Soit G_1 un groupe de torsion et G_2 un groupe sans torsion. Déterminer tous les morphismes de groupe de G_1 dans G_2 .

Indication ▼ Correction ▼

[2640]

Exercice 17 ★★ Groupes non isomorphes –

Démontrer que les groupes multiplicatifs (\mathbb{R}^*, \cdot) et (\mathbb{C}^*, \cdot) ne sont pas isomorphes.

Indication ▼ Correction ▼

[1312]

Exercice 18 ★★★ Groupes non isomorphes –

Démontrer que les groupes (\mathbb{R}^*, \times) et (\mathbb{Q}^*, \times) ne sont pas isomorphes.

Indication ▼ Correction ▼

[2974]

Exercice 19 ★★★ Automorphisme intérieur –

Soit (G, \cdot) un groupe. Pour $a \in G$, on note $\tau_a : G \rightarrow G$ défini par $\tau_a(x) = axa^{-1}$.

1. Démontrer que τ_a est un endomorphisme de G .
2. Vérifier que, pour tous $a, b \in G$, $\tau_a \circ \tau_b = \tau_{ab}$.
3. Montrer que τ_a est bijective et déterminer son inverse.
4. En déduire que $\Theta = \{\tau_a; a \in G\}$ muni du produit de composition est un groupe.

Indication ▼ Correction ▼

[1314]

Exercice 20 ★★★★★ Somme des valeurs –

Soit f un morphisme non constant d'un groupe fini (G, \cdot) dans (\mathbb{C}^*, \cdot) . Calculer $\sum_{x \in G} f(x)$.

Indication ▼ Correction ▼

[1315]

2 Anneaux

Exercice 21 ★ Anneau de matrices –

Soit A l'ensemble des matrices s'écrivant $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ avec a et b des entiers relatifs.

1. Démontrer que A est un anneau pour les lois d'addition et de produits de matrices.
2. Déterminer les éléments inversibles de A .

Indication ▼ Correction ▼

[1319]

Exercice 22 ★★ Anneau des entiers de Gauss –

On appelle ensemble des entiers de Gauss noté $\mathbb{Z}[i]$ l'ensemble des nombres complexes qui s'écrivent $a + ib$, avec a et $b \in \mathbb{Z}$.

1. Démontrer que $\mathbb{Z}[i]$ est un anneau.
2. Pour tout nombre complexe z , on note $N(z) = z\bar{z}$.

Démontrer que, pour tous nombres complexes z et z' , $N(z)N(z') = N(zz')$. Démontrer que, pour tout entier de Gauss z , $N(z)$ est un entier naturel. Soit z un entier de Gauss inversible. Déduire des questions précédentes que $N(z) = 1$. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

3. Démontrer que, pour tous nombres complexes z et z' , $N(z)N(z') = N(zz')$.

4. Démontrer que, pour tout entier de Gauss z , $N(z)$ est un entier naturel.
5. Soit z un entier de Gauss inversible. Dédurre des questions précédentes que $N(z) = 1$.
6. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

[Indication ▼](#) [Correction ▼](#)

[3220]

Exercice 23 ★★ Endomorphisme de groupes –

Soit $(G, +)$ un groupe commutatif. On note $\text{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : G \rightarrow G, x \mapsto f(x) + g(x)$. Démontrer que $(\text{End}(G), +, \circ)$ est un anneau.

[Indication ▼](#) [Correction ▼](#)

[1359]

Exercice 24 ★★ Rationnels à dénominateur impair –

Soit $A = \left\{ \frac{m}{n}; m \in \mathbb{Z}, n \in 2\mathbb{N} + 1 \right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair). Démontrer que $(A, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

[Indication ▼](#) [Correction ▼](#)

[1356]

Exercice 25 ★★★ Décimaux –

Soit \mathbb{D} l'ensemble des nombres décimaux,

$$\mathbb{D} = \left\{ \frac{n}{10^k}; n \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Démontrer que $(\mathbb{D}, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

[Indication ▼](#) [Correction ▼](#)

[1357]

Exercice 26 ★★ Centre d'un anneau –

Soit A un anneau. On appelle centre de A et l'on note $C(A)$ l'ensemble des éléments $a \in A$ tels que, pour tout $b \in A$, $ab = ba$. Démontrer que $C(A)$ est un sous-anneau de A .

[Indication ▼](#) [Correction ▼](#)

[3222]

Exercice 27 ★ Anneau des fonctions de \mathbb{R} dans \mathbb{R} –

L'anneau des fonctions de \mathbb{R} dans \mathbb{R} est-il intègre ?

[Indication ▼](#) [Correction ▼](#)

[3223]

Exercice 28 ★ Éléments nilpotents –

Un élément x d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. Montrer que $1_A - x$ est inversible.
4. Dans cette question, on ne suppose plus que A est commutatif. Soit $u, v \in A$ tels que uv est nilpotent.

Montrer que vu est nilpotent.

[Indication ▼](#) [Correction ▼](#)

[1354]

Exercice 29 ★ Anneau de Boole –

On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.

1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.
3. On suppose que A est intègre. Montrer que A contient exactement deux éléments.

[Indication ▼](#) [Correction ▼](#)

[1355]

3 Corps

Exercice 30 $\mathbb{Q}(i)$ –

Montrer que $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$ est un corps.

[Indication ▼](#) [Correction ▼](#)

[3224]

Exercice 31 $\mathbb{Q}[\sqrt{d}]$ –

Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d}; (a, b) \in \mathbb{Q}^2\}.$$

Démontrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.

[Indication ▼](#) [Correction ▼](#)

[1382]

Exercice 32 Un corps de matrices –

Soit $\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : (a, b) \in \mathbb{R}^2 \right\}$.

1. Démontrer que $(\mathcal{C}, +, \times)$ est un corps.
2. Démontrer que \mathcal{C} est isomorphe à \mathbb{C} .

[Indication ▼](#) [Correction ▼](#)

[3218]

Exercice 33 Anneau intègre fini –

Soit A un anneau intègre commutatif fini. Démontrer que A est un corps.

[Indication ▼](#) [Correction ▼](#)

[1361]

Indication pour l'exercice 1 ▲

1. Il faut vérifier les trois propriétés de la définition d'un groupe.
 2. Calculer ce que cela vaut pour $n = 2$, $n = 3$, puis faire une récurrence.
-

Indication pour l'exercice 2 ▲

Appliquer le théorème de caractérisation des sous-groupes. Pour prouver qu'une partie n'est pas un sous-groupe, elle peut ne pas contenir l'élément neutre, ou ne pas être stable par multiplication, ou...

Indication pour l'exercice 3 ▲

Il faut vérifier que les 3 propriétés d'un sous-groupe sont satisfaites. Pour le deuxième point, la quantité conjuguée pourra être utile.

Indication pour l'exercice 4 ▲

Appliquer le théorème de caractérisation des sous-groupes.

Indication pour l'exercice 5 ▲

Pour la stabilité par le passage à l'inverse, utiliser la quantité conjuguée. Pour la stabilité pour le produit, tout développer et factoriser habilement...

Indication pour l'exercice 6 ▲

1. Vérifier les propriétés d'un sous-groupe.
2. La moitié de la question vient de la question précédente. Il faut encore prouver que c'est le plus petit, en remarquant qu'un sous-groupe de G contenant X contient $\langle X \rangle$.
3. Poser

$$H = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : n \in \mathbb{N}, x_i \in X, \varepsilon_i = \pm 1\}$$

et vérifier successivement que H contient X , H est un sous-groupe de G , puis que $H \subset \langle X \rangle$.

Indication pour l'exercice 7 ▲

Vérifier les hypothèses du théorème de caractérisation des sous-groupes.

Indication pour l'exercice 8 ▲

Penser à un contre-exemple avec \mathbb{Z}^2 .

Indication pour l'exercice 9 ▲

Indication pour l'exercice 10 ▲

Pour montrer que AB sous-groupe entraîne $AB = BA$, on pourra utiliser la stabilité par x^{-1} .

Indication pour l'exercice 11 ▲

1. Construire une bijection.
 - 2.
 3. Réaliser une partition de G .
-

Indication pour l'exercice 12 ▲

Il faut trouver le bon groupe. Attention à ce qu'il s'agisse bien d'un groupe!

Indication pour l'exercice 13 ▲

Pour le noyau, on pourra chercher les solutions de $\exp(z) = 1$ en posant $z = a + ib$.

Indication pour l'exercice 14 ▲

Il suffit de connaître l'image de 1.

Indication pour l'exercice 15 ▲

Démontrer et utiliser que si f est un tel morphisme et p et q sont des entiers naturels, $f(p) = pf(1)$ et $f\left(\frac{1}{q}\right) = \frac{1}{q}f(1)$.

Indication pour l'exercice 16 ▲

Seul le morphisme qui à x associe l'élément neutre de G_2 convient.

Indication pour l'exercice 17 ▲

Raisonnement par l'absurde, supposer l'existence d'un isomorphisme f de (\mathbb{C}^*, \cdot) dans (\mathbb{R}^*, \cdot) et travailler à partir de $f(i)$.

Indication pour l'exercice 18 ▲

On pourra procéder par l'absurde et considérer f un isomorphisme de (\mathbb{R}^*, \times) sur (\mathbb{Q}, \times) puis a tel que $f(a) = 2$. Conclure en utilisant que $\sqrt{2}$ n'est pas rationnel.

Indication pour l'exercice 19 ▲

1. Vérifier la définition.
 - 2.
 3. Utiliser la question précédente avec $b = a^{-1}$.
 4. Démontrer qu'il s'agit d'un sous-groupe de (S_G, \circ) .
-

Indication pour l'exercice 20 ▲

Partir de $a \in G$ tel que $f(a) \neq 1$ et calculer $\sum_{x \in G} f(ax)$.

Indication pour l'exercice 21 ▲

1. Démontrer que c'est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.
 2. Faire un raisonnement par analyse-synthèse : si M est inversible, que doivent forcément vérifier ses coefficients. Attention ! Il ne faut pas oublier que les coefficients de M sont des entiers.
-

Indication pour l'exercice 22 ▲

1. C'est un sous-anneau d'un anneau bien connu.
2. Utiliser une propriété bien connue du module.
Quand est-ce que le produit de deux entiers naturels peut-il être égal à 1 ? Quand est-ce que la somme de deux entiers naturels peut-elle être égale à 1 ?
3. Utiliser une propriété bien connue du module.
- 4.
5. Quand est-ce que le produit de deux entiers naturels peut-il être égal à 1 ?
6. Quand est-ce que la somme de deux entiers naturels peut-elle être égale à 1 ?

Indication pour l'exercice 23 ▲

Vérifier tous les points de la définition d'un anneau.

Indication pour l'exercice 24 ▲

Démontrer que c'est un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour déterminer les éléments inversibles, partir de $x = \frac{m}{n} \in A$ qu'on suppose inversible, écrire que $xy = 1$ pour un certain $y \in A$, et en déduire une condition nécessaire sur m . Démontrer ensuite que cette condition est suffisante.

Indication pour l'exercice 25 ▲

Démontrer qu'il s'agit d'un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour déterminer les éléments inversibles, partir de $x = \frac{n}{10^k} \in \mathbb{D}$ inversible, écrire $xy = 1$ avec $y \in \mathbb{D}$, et obtenir une condition nécessaire sur n . Prouver ensuite que cette condition est suffisante.

Indication pour l'exercice 26 ▲

Il suffit de vérifier les hypothèses du théorème de caractérisation des sous-anneaux.

Indication pour l'exercice 27 ▲

Trouver deux fonctions non identiquement nulles dont le produit est nulle.

Indication pour l'exercice 28 ▲

Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Calculer $(xy)^p$ avec $p \geq \min(n, m)$.
 2. Calculer $(x+y)^{n+m}$.
 3. Calculer $(1-x)(1+x+\cdots+x^p)$.
 4. Si $(uv)^n = 0$, montrer que $(vu)^{n+1} = 0$.
-

Indication pour l'exercice 29 ▲

-
1. Appliquer la propriété à $x+x$
 2. Fixer $x, y \in A$ et appliquer la propriété à $x+y$.
 3. Pour $x, y \in A$, calculer $xy(x+y)$.
-

Indication pour l'exercice 30 ▲

Montrer que c'est un sous-anneau de \mathbb{C} , et que tous les éléments non nuls de $\mathbb{Q}(i)$ sont inversibles (dans $\mathbb{Q}(i)$).

Indication pour l'exercice 31 ▲

Démontrer que c'est un sous-corps de $(\mathbb{R}, +, \times)$.

Indication pour l'exercice 32 ▲

-
1. On pourra commencer par démontrer que \mathcal{C} est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.
 2. Considérer $\phi \left(\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \right) = a + ib$.
-

Indication pour l'exercice 33 ▲

Prendre $a \in A$ non nul et considérer $x \mapsto ax$.

Correction de l'exercice 1 ▲

1. On n'a pas affaire à une loi "classique" et donc on ne peut pas démontrer qu'on a un sous-groupe d'un groupe connu. Il faut donc vérifier à la main les trois propriétés d'un groupe ainsi que le fait qu'il s'agit bien d'une loi interne.

Si (x, y) et (x', y') sont dans $\mathbb{R}^* \times \mathbb{R}$, alors $xx' \in \mathbb{R}^*$ et $xy' + y \in \mathbb{R}$ et donc il s'agit bien d'une loi interne. La loi \star est associative : en effet, si (x, y) , (x', y') et (x'', y'') sont dans $\mathbb{R}^* \times \mathbb{R}$, alors d'une part

$$\begin{aligned}((x, y) \star (x', y')) \star (x'', y'') &= (xx', xy' + y) \star (x'', y'') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

et d'autre part

$$\begin{aligned}(x, y) \star ((x', y') \star (x'', y'')) &= (x, y) \star (x'x'', x'y'' + y') \\ &= (xx'x'', x(x'y'' + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y).\end{aligned}$$

La loi possède un élément neutre, qui est $(1, 0)$. Il est en effet facile de vérifier que

$$(x, y) \star (1, 0) = (1, 0) \star (x, y) = (x, y).$$

Tout élément (x, y) possède un inverse. Expliquons comment le trouver. Il n'est pas très difficile de remarquer qu'il doit s'écrire sous la forme $(1/x, a)$. De

$$(x, y) \star (1/x, a) = (1, xa + y)$$

on voit qu'on doit avoir $xa + y = 0$ et donc $a = -y/x$. On vérifie alors que $(1/x, -y/x)$ est un inverse de (x, y) :

$$(x, y) \star (1/x, -y/x) = (1/x, -y/x) \star (x, y) = (1, 0).$$

Le groupe n'est pas commutatif. En effet on a

$$(1, 1) \star (2, 1) = (2, 2)$$

alors que

$$(2, 1) \star (1, 1) = (2, 3).$$

2. Si (x, y) et (x', y') sont dans $\mathbb{R}^* \times \mathbb{R}$, alors $xx' \in \mathbb{R}^*$ et $xy' + y \in \mathbb{R}$ et donc il s'agit bien d'une loi interne.

3. La loi \star est associative : en effet, si (x, y) , (x', y') et (x'', y'') sont dans $\mathbb{R}^* \times \mathbb{R}$, alors d'une part

$$\begin{aligned}((x, y) \star (x', y')) \star (x'', y'') &= (xx', xy' + y) \star (x'', y'') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

et d'autre part

$$\begin{aligned}(x, y) \star ((x', y') \star (x'', y'')) &= (x, y) \star (x'x'', x'y'' + y') \\ &= (xx'x'', x(x'y'' + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y).\end{aligned}$$

4. La loi possède un élément neutre, qui est $(1, 0)$. Il est en effet facile de vérifier que

$$(x, y) \star (1, 0) = (1, 0) \star (x, y) = (x, y).$$

5. Tout élément (x, y) possède un inverse. Expliquons comment le trouver. Il n'est pas très difficile de remarquer qu'il doit s'écrire sous la forme $(1/x, a)$. De

$$(x, y) \star (1/x, a) = (1, xa + y)$$

on voit qu'on doit avoir $xa + y = 0$ et donc $a = -y/x$. On vérifie alors que $(1/x, -y/x)$ est un inverse de (x, y) :

$$(x, y) \star (1/x, -y/x) = (1/x, -y/x) \star (x, y) = (1, 0).$$

6. On remarque que

$$(x, y)^2 = (x^2, xy + y) \text{ et } (x, y)^3 = (x^3, x^2y + xy + y).$$

On prouve alors par récurrence sur $n \in \mathbb{N}^*$ que

$$(x, y)^n = (x^n, x^{n-1}y + x^{n-2}y + \dots + xy + y).$$

Correction de l'exercice 2 ▲

1. H est un sous-groupe de G . En effet, $0 \in H$, si $x, y \in H$, alors $-x$ et $x + y$ sont deux entiers pairs et donc $-x \in H$, $x + y \in H$. Le théorème de caractérisation des sous-groupes nous dit que H est un sous-groupe de G .

2. $0 \notin H$ et donc H n'est pas un sous-groupe de G .

3. $2 \in H$ et $-2 \notin H$: H n'est pas un sous-groupe de G .

4. $1 \in H$. Si $x = p/q$ et $y = p'/q'$ sont deux rationnels non-nuls, alors $1/x = q/p$ et $x \times y = \frac{p \times p'}{q \times q'}$ sont deux rationnels non nuls. H est un sous-groupe de G .

5. Id_E , l'élément neutre de G , est élément de H . De plus, si $f, g \in H$, alors

$$f(x) = x \implies f^{-1}(f(x)) = f^{-1}(x) \implies f^{-1}(x) = x$$

et

$$f \circ g(x) = f(g(x)) = f(x) = x.$$

Ainsi, f^{-1} et $f \circ g$ sont éléments de H , et H est un sous-groupe de G .

6. L'élément neutre de G , Id_E , n'est pas élément de H qui n'est donc pas un sous-groupe de G .

Correction de l'exercice 3 ▲

1. On commence par vérifier que $H \subset G$ (c'est-à-dire que $0 \notin H$). On vérifie ensuite que $1 \in H$ puisque $1^1 = 1$. Soit $z_1, z_2 \in H$. Alors il existe $n_1 \in \mathbb{N}$ et $n_2 \in \mathbb{N}$ tels que $z_1^{n_1} = 1$ et $z_2^{n_2} = 1$ (attention ! on n'a pas forcément $n_1 = n_2$). Mais alors

$$(z_1 z_2)^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{n_1} = 1^{n_2} 1^{n_1} = 1.$$

Ainsi, $z_1 z_2 \in H$. De plus,

$$\left(\frac{1}{z_1}\right)^{n_1} = \frac{1}{z_1^{n_1}} = 1$$

et donc $1/z_1 \in H$. Ainsi, H est bien un sous-groupe de G .

2. $1 = 1 + 0\sqrt{2} \in H$ (attention ! la condition $(a, b) \neq (0, 0)$ signifie qu'on ne peut pas avoir $a = 0$ ET $b = 0$ en même temps, mais il est tout à fait possible de prendre $a = 1$ et $b = 0$). Si $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ sont éléments de H , alors

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2} \sqrt{2}$$

est lui aussi un élément de H (on n'a $a^2 - 2b^2 \neq 0$ si $(a, b) \neq (0, 0)$ car $\sqrt{2}$ est irrationnel). De même, $xy \in H$ puisque

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2}$$

est un élément de H . Remarquons que l'on ne peut pas avoir $ac + 2bd = 0$ et $ad + bc = 0$, sinon on aurait $xy = 0$ et donc ou bien $x = 0$ ou bien $y = 0$ ce qui n'est pas le cas. Ainsi H est un sous-groupe de G .

Correction de l'exercice 4 ▲

Il suffit, pour chaque cas, d'appliquer le théorème de caractérisation des sous-groupes.

1. e est élément de $C(G)$ car $ey = ye = y$ pour tout $y \in G$. Soient $x_1, x_2 \in C(G)$. Alors, pour tout $y \in G$, on a

$$x_1x_2y = x_1(x_2y) = (x_1y)x_2 = yx_1x_2$$

et donc $x_1x_2 \in C(G)$. Enfin, si $x \in C(G)$, alors pour tout $y \in G$,

$$xy = yx \implies xyx^{-1} = yxx^{-1} = y \implies x^{-1}xyx^{-1} = x^{-1}y \implies yx^{-1} = x^{-1}y$$

où on a multiplié à droite puis à gauche par x^{-1} . On en déduit que $x^{-1} \in C(G)$ qui est donc un sous-groupe de G .

2. Puisque H est un sous-groupe de G , $e \in H$ et donc $aea^{-1} \in aHa^{-1}$. Mais $aea^{-1} = e$ et donc $e \in aHa^{-1}$. Soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a

$$xy = aha^{-1}ah'a^{-1} = ah'h'a^{-1} \in aHa^{-1}$$

puisque $hh' \in H$ (H est un sous-groupe de G). Enfin, si on choisit $h' = h^{-1}$, le calcul précédent montre que

$$xy = yx = e$$

et donc $x^{-1} = y \in aHa^{-1}$ puisque $h^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G .

3. Notons T l'ensemble des éléments de torsion de G . On a $e^1 = e$, donc $e \in T$. De plus, si $x, y \in T$, avec respectivement $x^n = e$ et $y^m = e$, il suffit de remarquer que

$$(y^{-1})^m = (y^m)^{-1} = e^{-1} = e$$

puis d'utiliser le fait que x et y^{-1} commutent pour prouver que

$$(xy^{-1})^{nm} = (x^n)^m ((y^{-1})^m)^n = e.$$

Ainsi, xy^{-1} est élément de T , et T est bien un sous-groupe de G .

Correction de l'exercice 5 ▲

La première chose à remarquer est que $H \subset \mathbb{R}_+^*$. Pour $x + y\sqrt{3} \in H$, puisque $x^2 - 3y^2 > 0$ et $x \in \mathbb{N}$, on a $x > \sqrt{3}|y|$ et donc $x + y\sqrt{3} > 0$. On remarque ensuite que $1 = 1 + 0\sqrt{3}$ est bien un élément de H . Soient $a = x + y\sqrt{3}$ et $b = u + v\sqrt{3}$ deux éléments de H . Alors :

$$(x + y\sqrt{3})(u + v\sqrt{3}) = (xu + 3yv) + \sqrt{3}(xv + yu).$$

On remarque ensuite que

$$\begin{aligned} (xu + 3yv)^2 - 3(xv + yu)^2 &= x^2u^2 + 9y^2v^2 - 3x^2v^2 - 3y^2u^2 \\ &= x^2(u^2 - 3v^2) + 3y^2(3v^2 - u^2) \\ &= x^2 - 3y^2 \\ &= 1. \end{aligned}$$

De plus, il est clair que $xu + 3yv$ et $xv + yu$ sont éléments de \mathbb{Z} . Il reste à voir que $xu + 3yv$ est élément de \mathbb{N} . Mais c'est clair car $x \geq \sqrt{3}|y|$ et $u \geq \sqrt{3}|v|$. Ainsi, $ab \in H$. Démontrons finalement que H est bien stable par passage à l'inverse. On a

$$\frac{1}{a} = \frac{1}{x + y\sqrt{3}} = \frac{x - y\sqrt{3}}{x^2 - 3y^2} = x - y\sqrt{3} \in H$$

puisque $x^2 - 3y^2 = 1$. Ainsi, H est bien un sous-groupe de (\mathbb{R}_+^*, \times) .

Correction de l'exercice 6 ▲

1. Notons $H = \bigcap_{i \in I} H_i$.

$1_G \in H$ puisque 1_G appartient à tous les H_i . Soit $x, y \in H$. Pour tout $i \in I$, $x \in H_i$ et $y \in H_i$. Puisque H_i est un sous-groupe de G , on a $xy \in H_i$ et comme c'est vrai pour tout $i \in I$, $xy \in H$. Soit $x \in H$. Pour tout $i \in I$, $x \in H_i$ et donc $x^{-1} \in H_i$ puisque H_i est un sous-groupe de G . Puisque c'est vrai pour tout $i \in I$, $x^{-1} \in H$.

Finalement, on a prouvé que H est un sous-groupe de G .

2. $1_G \in H$ puisque 1_G appartient à tous les H_i .

3. Soit $x, y \in H$. Pour tout $i \in I$, $x \in H_i$ et $y \in H_i$. Puisque H_i est un sous-groupe de G , on a $xy \in H_i$ et comme c'est vrai pour tout $i \in I$, $xy \in H$.

4. Soit $x \in H$. Pour tout $i \in I$, $x \in H_i$ et donc $x^{-1} \in H_i$ puisque H_i est un sous-groupe de G . Puisque c'est vrai pour tout $i \in I$, $x^{-1} \in H$.

5. Notons $(H_i)_{i \in I}$ la famille des sous-groupes de G qui contiennent X , de sorte que $\langle X \rangle = \bigcap_{i \in I} H_i$. Alors, d'après la question précédente, $\langle X \rangle$ est bien un sous-groupe de G . Puisque $X \subset H_i$ pour tout $i \in I$, $X \subset \langle X \rangle$. Puisque $\langle X \rangle$ est contenu dans tout sous-groupe de G contenant X , $\langle X \rangle$ est bien le plus petit sous-groupe de G contenant X .

6. Posons

$$H = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : n \in \mathbb{N}, x_i \in X, \varepsilon_i = \pm 1 \text{ pour } i = 1, \dots, n\}.$$

On commence par remarquer que H est un sous-groupe de G . En effet,

$1_G \in H$ (cas du produit vide) si $x, y \in H$, on écrit $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ et $y = y_1^{\nu_1} \cdots y_m^{\nu_m}$. Alors

$$xy = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_1^{\nu_1} \cdots y_m^{\nu_m}$$

est bien dans H . si $x \in H$, on écrit $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ d'où

$$x^{-1} = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$$

qui est bien élément de H puisque $-\varepsilon_i \in \{-1, 1\}$.

On remarque ensuite que $X \subset H$ (cas du produit avec un seul élément). On obtient donc $\langle X \rangle \subset H$. Reste à démontrer l'inclusion réciproque. Pour cela, on va prouver par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

$$\mathcal{P}_n = \text{"tout } x \in G \text{ qui s'écrit } x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \text{ avec } x_i \in X, \varepsilon_i = \pm 1 \text{ appartient à } \langle X \rangle\text{"}.$$

Initialisation : soit $x \in G$ tel que $x = x_1$ ou $x = x_1^{-1}$ avec $x_1 \in X$. Alors si $x = x_1$, $x \in \langle X \rangle$. Si $x = x_1^{-1}$, alors, comme $x_1 \in \langle X \rangle$ et que $\langle X \rangle$ est un sous-groupe de G , on a $x = x_1^{-1} \in \langle X \rangle$. **Hérédité :** soit $n \in \mathbb{N}^*$ tel que \mathcal{P}_n est vraie. Soit $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} x_{n+1}^{\varepsilon_{n+1}}$. Alors par hypothèse de récurrence, $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \langle X \rangle$ et comme dans l'initialisation, $x_{n+1}^{\varepsilon_{n+1}} \in \langle X \rangle$. Puisque $\langle X \rangle$ est un groupe,

$$x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} x_{n+1}^{\varepsilon_{n+1}} \in \langle X \rangle.$$

On a donc prouvé par récurrence que pour tout $n \in \mathbb{N}^*$, \mathcal{P}_n est vraie. Ceci signifie exactement que $H \subset \langle X \rangle$. On a donc prouvé, par double inclusion, que $H = \langle X \rangle$.

7. $1_G \in H$ (cas du produit vide)

8. si $x, y \in H$, on écrit $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ et $y = y_1^{\nu_1} \cdots y_m^{\nu_m}$. Alors

$$xy = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} y_1^{\nu_1} \cdots y_m^{\nu_m}$$

est bien dans H .

9. si $x \in H$, on écrit $x = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ d'où

$$x^{-1} = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$$

qui est bien élément de H puisque $-\varepsilon_i \in \{-1, 1\}$.

Correction de l'exercice 7 ▲

On va vérifier les hypothèses du théorème de caractérisation des sous-groupes.

On sait que $1_G \in H_1$ (puisque H_1 est un sous-groupe de G) et que $1_G \in H_2$ (puisque H_2 est un sous-groupe de G). Donc $1_G \in H_1 \cap H_2$. Soit $x, y \in H_1 \cap H_2$. Alors, $x \in H_1$, $y \in H_1$ et donc puisque H_1 est un sous-groupe de G , $xy \in H_1$. De la même façon, on prouve que $xy \in H_2$ et donc que $xy \in H_1 \cap H_2$. Soit $x \in H_1 \cap H_2$. Alors, $x \in H_1$ et puisque H_1 est un sous-groupe de G , $x^{-1} \in H_1$. De même, $x^{-1} \in H_2$ et finalement $x^{-1} \in H_1 \cap H_2$.

Correction de l'exercice 8 ▲

Non, ce n'est pas le cas. Prenons $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ et $H = \{(x, x); x \in \mathbb{Z}\}$. H est clairement un sous-groupe de \mathbb{Z}^2 , et H ne s'écrit pas $H = A \times B$, sinon on aurait $A = B = \mathbb{Z}$ ce qui n'est pas le cas.

Correction de l'exercice 9 ▲

Si $H \subset K$, alors $H \cup K = K$ qui est un sous-groupe de G . De même, si $K \subset H$, $H \cup K = H$ qui est un sous-groupe de G . Supposons maintenant que $H \cup K$ est un sous-groupe de G et que ni $H \subset K$, ni $K \subset H$. Alors on peut trouver $x \in H \setminus K$ et $y \in K \setminus H$. Puisque $H \cup K$ est un groupe et que $x, y \in H \cup K$, on a $xy \in H \cup K$. Mais si $xy \in H$, alors $y = x^{-1}(xy)$ est le produit de deux éléments de H , qui est un sous-groupe de G , et donc $y \in H$ ce qui est une contradiction. On obtient de même une contradiction dans l'autre cas possible $xy \in K$. L'hypothèse de départ est donc fautive, et on a bien $H \subset K$ ou $K \subset H$.

Correction de l'exercice 10 ▲

Supposons d'abord que $AB = BA$. Alors AB est un sous-groupe de G car :

1. $e \in AB$, car $e = ee$ avec $e \in A$ et $e \in B$ (ce sont des sous-groupes);

2. AB est stable par passage au produit. En effet, si $x = ab \in AB$ et $y = a'b' \in AB$, alors $xy = aba'b'$. Or, ba' est un élément de BA , c'est donc aussi un élément de AB et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que

$$xy = aa''b''b' \in AB$$

puisque $aa'' \in A$ et $b''b' \in B$.

3. AB est stable par passage à l'inverse. En effet, si $x = ab \in AB$, alors $x^{-1} = b^{-1}a^{-1}$ est élément de BA et $BA = AB$. Réciproquement, supposons que AB est un sous-groupe de G et prouvons que $AB = BA$. Soit d'abord $x = ab \in AB$. Alors $x^{-1} = b^{-1}a^{-1} \in AB$ puisque AB est un groupe et donc $b^{-1}a^{-1} = a'b'$ avec $a' \in A$ et $b' \in B$. On passe à l'inverse :

$$ab = b'^{-1}a'^{-1} \in BA.$$

Pour l'autre inclusion, considérons $y = ba \in BA$. Alors $y^{-1} = a^{-1}b^{-1} \in AB$, et donc $y = (y^{-1})^{-1} \in AB$ puisque AB est un groupe. .

Correction de l'exercice 11 ▲

1. Soit $f : H \rightarrow aH$ définie par $f(h) = ah$. Il s'agit clairement d'une surjection de H sur aH . De plus, si $ah_1 = ah_2$, alors $h_1 = h_2$ car a est inversible, et donc f est aussi injective. f est donc une bijection de H sur aH ; ces deux ensembles ont le même nombre d'éléments.

2. Supposons que $aH \cap bH \neq \emptyset$ et prouvons que $aH = bH$. Par symétrie, il suffit de prouver que $aH \subset bH$. Soit $x \in aH \cap bH$, $x = ah_1 = bh_2$. Prenons $y = ah \in aH$. Alors $a = bh_2h_1^{-1}$ et donc $y = bh_2h_1^{-1}h \in bH$.

3. La réunion des ensembles aH est clairement égale à G (si $x \in G$, il est dans xH). On ne garde que les aH deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de G avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de H . Si k est le nombre d'ensembles nécessaires pour réaliser cette partition, on a

$$k \text{ card}(H) = \text{card}(G)$$

et donc le cardinal de H divise celui de G .

Correction de l'exercice 12 ▲

1. La fonction \ln est un morphisme du groupe (\mathbb{R}_+^*, \times) dans le groupe $(\mathbb{R}, +)$.
 2. La fonction $|\cdot|$ est un morphisme de groupes de (\mathbb{C}^*, \times) dans lui-même, ou de (\mathbb{C}^*, \times) dans (\mathbb{R}^*, \times) , ou de (\mathbb{C}^*, \times) dans (\mathbb{R}_+^*, \times) . Attention, même si la propriété est vraie pour $z = 0$, il faut exclure 0 (car il n'est pas inversible pour la multiplication).
 3. La fonction $\sqrt{\cdot}$ est un morphisme du groupe (\mathbb{R}_+^*, \times) dans lui-même.
 4. La fonction \exp est un morphisme de groupe de $(\mathbb{R}, +)$ dans (\mathbb{R}_+^*, \times) .
-

Correction de l'exercice 13 ▲

On sait que, pour tous $z, w \in \mathbb{C}$, on a

$$\exp(z+w) = \exp(z)\exp(w).$$

Ceci signifie exactement que \exp est un morphisme de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \cdot) (la fonction exponentielle ne prend jamais la valeur zéro). De plus, soit $w \in \mathbb{C}^*$, $w = re^{i\theta}$ avec $r > 0$. Soit $a = \ln r$ et posons $z = a + i\theta$. Alors

$$\exp(z) = \exp(a)\exp(i\theta) = re^{i\theta} = w.$$

L'exponentielle est un morphisme surjectif de $(\mathbb{C}, +)$ dans (\mathbb{C}^*, \cdot) . Déterminons son noyau. Si $\exp(z) = 1$, posons $z = x + iy$. Alors

$$\exp(z) = \exp(x)\exp(iy) = 1 = 1\exp(i0).$$

Ceci est équivalent à $x = 0$ et il existe $k \in \mathbb{Z}$ tel que $y = k2\pi$. On a donc

$$\ker(\exp) = \{2ik\pi; k \in \mathbb{Z}\}.$$

Correction de l'exercice 14 ▲

Soit f un morphisme de $(\mathbb{Z}, +)$. Prouvons par récurrence que pour tout $n \geq 1$, on a $f(n) = nf(1)$. C'est vrai pour $n = 1$, et si c'est vrai pour n , alors

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1).$$

De plus, pour $n \leq 0$, on a $-n \geq 0$ et donc $f(-n) = -nf(1)$. On en déduit :

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = f(n) - nf(1).$$

Ainsi, on a toujours $f(n) = nf(1)$, quel que soit $n \in \mathbb{Z}$. Caractérisons maintenant les morphismes surjectifs. Supposons donc que f est surjectif. Tout élément de $\mathbb{Z} = f(\mathbb{Z})$ est un multiple de $f(1)$. Or, les seuls éléments de \mathbb{Z} qui divisent tous les autres entiers sont 1 et -1 . On en déduit que $f(1) = 1$ ou $f(1) = -1$, et donc que $f(n) = n$ ou $f(n) = -n$. Réciproquement, ces deux applications sont clairement des morphismes surjectifs de $(\mathbb{Z}, +)$. Déterminons enfin les morphismes injectifs. Soit f un morphisme et $n \in \ker(f)$. Alors $f(n) = nf(1) = 0$. Si $f(1) \neq 0$, alors $f(n) = 0 \iff n = 0$ et f est injectif, et si $f(1) = 0$, alors f n'est pas injectif. Donc tous les morphismes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$ sont injectifs sauf l'application identiquement nulle.

Correction de l'exercice 15 ▲

Soit f un tel morphisme de groupe. On va commencer par démontrer que pour p et q des entiers naturels, on a $f(p) = pf(1)$ et $f\left(\frac{1}{q}\right) = \frac{1}{q}f(1)$. La première des deux propriétés se démontre aisément par récurrence. Pour la deuxième, on écrit que

$$f(1) = f\left(\frac{1}{q} + \cdots + \frac{1}{q}\right) = qf\left(\frac{1}{q}\right).$$

Notons ensuite $a = f(1)$. Alors a/q est un entier pour tout entier q , et donc $a = 0$. On en déduit que $f(p) = f(1/q) = 0$ pour tous les entiers p et q , puis que $f(p/q) = pf(1/q) = 0$. Finalement, on trouve que f est le morphisme nul.

Correction de l'exercice 16 ▲

Remarquons d'abord que le morphisme qui à tout x de G_1 associe l'élément neutre e de G_2 convient. Réciproquement, soit x un élément de G_1 et notons $y = f(x)$. Puisque x est un élément de torsion, il existe $n \geq 1$ tel que $x^n = e$. Mais alors,

$$y^n = (f(x))^n = f(x^n) = f(e) = e.$$

Comme G_2 est sans torsion, on a $y = e$ et donc $f(x) = e$ pour tout $x \in G_1$.

Correction de l'exercice 17 ▲

Supposons que ces deux groupes sont isomorphes et soit f un isomorphisme de (\mathbb{C}^*, \cdot) dans (\mathbb{R}^*, \cdot) . Posons $a = f(i)$. Alors

$$f(i^4) = a^4 = 1$$

et donc $a^2 = 1$ puisque $a^2 > 0$. D'où $1 = a^2 = f(i^2) = f(-1)$ et $1 = f(1)$. f ne peut pas être injectif, on a obtenu une contradiction.

Correction de l'exercice 18 ▲

Procédons par l'absurde et supposons qu'il existe $f : (\mathbb{R}^*, \times) \rightarrow (\mathbb{Q}^*, \times)$ un isomorphisme. En particulier, il existe $a \in \mathbb{R}^*$ tel que $f(a) = 2$. Si $a > 0$, alors il existe un réel b tel que $a = b^2$. On a alors $2 = f(a) = f(b) \times f(b)$ et donc $\sqrt{2} = \pm f(b)$. Mais ceci contredit que $\sqrt{2}$ est irrationnel. Si $a < 0$, alors il existe un réel b tel que $a = -b^2$. On a alors $2 = f(a) = f(-1)f(b) \times f(b)$. Mais $f(-1)^2 = f(-1 \times -1) = f(1) = 1$ et donc $f(-1) = \pm 1$. Comme f est un isomorphisme et $f(1) = 1$, on a $f(-1) = -1$. On obtient alors $2 = -f(b)^2$, ce qui est impossible puisque $2 > 0$ et $-f(b)^2 < 0$. Dans les deux cas, on a obtenu une contradiction et l'existence d'un tel isomorphisme est impossible. On aurait aussi pu utiliser des arguments de cardinalité : \mathbb{Q}^* est dénombrable, et \mathbb{R}^* ne l'est pas. Donc il ne peut pas exister de bijection entre ces deux ensembles.

Correction de l'exercice 19 ▲

1. Il suffit d'appliquer la définition : pour tous $x, y \in G$, on a

$$\tau_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \tau_a(x)\tau_a(y).$$

2. Soit $x \in G$. On a

$$\tau_a \circ \tau_b(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1}$$

tandis que

$$\tau_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1}.$$

On a donc $\tau_a \circ \tau_b = \tau_{ab}$.

3. Soit $a \in G$. On pourrait prouver que τ_a est injectif en calculant son noyau, puisqu'il est surjectif, mais c'est plus facile d'appliquer la question précédente. Avec $b = a^{-1}$, elle donne

$$\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_e = Id_G$$

et en inversant le rôle joué par a et b , on a aussi

$$\tau_{a^{-1}} \circ \tau_a = Id_G.$$

Ainsi, τ_a est inversible d'inverse $\tau_{a^{-1}}$.

4. On va prouver que $\Theta = \{\tau_a; a \in G\}$ est un sous-groupe de (S_G, \circ) . Il est non-vide parce qu'il contient τ_e . Si $\tau_a, \tau_b \in \Theta$, alors

$$(\tau_a)^{-1} = \tau_{a^{-1}} \in \Theta$$

et

$$\tau_a \circ \tau_b = \tau_{ab} \in \Theta.$$

Ainsi, (Θ, \circ) est bien un sous-groupe de (S_G, \circ) .

Correction de l'exercice 20 ▲

Puisque f n'est pas constante, il existe $a \in G$ tel que $f(a) \neq 1$. Maintenant, l'application $x \mapsto ax$ est une permutation de G : en effet, pour tout $y \in G$, il existe un unique $x \in G$ tel que $y = ax$ (x est égal à $a^{-1}y$). On en déduit que

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(x).$$

Mais d'autre part, puisque f est un morphisme de groupes, on a aussi

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(a)f(x) = f(a) \sum_{x \in G} f(x).$$

Ainsi, il vient

$$(f(a) - 1) \times \sum_{x \in G} f(x) = 0.$$

Puisque $f(a) \neq 1$, on en déduit que $\sum_{x \in G} f(x) = 0$.

Correction de l'exercice 21 ▲

1. Il suffit de démontrer que A est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$. Pour cela, on remarque que

$I_2 \in A$ (choisir $a = 1$ et $b = 0$). Si $M = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}$ sont dans A , alors

$$M - M' = \begin{pmatrix} a - a' & b - b' \\ 0 & a - a' \end{pmatrix}$$

et

$$MM' = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix}$$

sont dans A .

2. $I_2 \in A$ (choisir $a = 1$ et $b = 0$).

3. Si $M = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ et $M' = \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}$ sont dans A , alors

$$M - M' = \begin{pmatrix} a - a' & b - b' \\ 0 & a - a' \end{pmatrix}$$

et

$$MM' = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix}$$

sont dans A .

4. Soit $M = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ inversible dans A . Alors il existe $M' = \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}$ tel que $MM' = I_2$. On obtient $aa' = 1$, et comme a et a' sont dans \mathbb{Z} , on doit avoir $a = \pm 1$. Dans ce cas, on aura $a' = a$. De plus, on doit aussi avoir $ab' + ba' = 0$ ce qui entraîne $b' = -b$. Réciproquement, soit $M \in A$ qui s'écrit

$$M = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

avec $a = \pm 1$. Posons

$$M' = \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix}.$$

Alors

$$MM' = \begin{pmatrix} a^2 & ab - ba \\ 0 & a^2 \end{pmatrix} = I_2.$$

Ainsi, M' est inversible. On a donc démontré que les éléments inversibles de A sont ceux pour lesquels $a = 1$ ou $a = -1$.

Correction de l'exercice 22 ▲

1. On va prouver que $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} . En effet,

$1 = 1 + 0i \in \mathbb{Z}[i]$; Soit $z = a + ib$ et $z' = a' + ib' \in \mathbb{Z}[i]$. Alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$$

(puisque $a - a'$ et $b - b' \in \mathbb{Z}$) et

$$zz' = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$$

(puisque $aa - bb'$ et $ab' + a'b \in \mathbb{Z}$).

2. $1 = 1 + 0i \in \mathbb{Z}[i]$;

3. Soit $z = a + ib$ et $z' = a' + ib' \in \mathbb{Z}[i]$. Alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$$

(puisque $a - a'$ et $b - b' \in \mathbb{Z}$) et

$$zz' = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$$

(puisque $aa - bb'$ et $ab' + a'b \in \mathbb{Z}$).

4. On remarque que $N(z) = |z|^2$. Puisque $|zz'| = |z| \cdot |z'|$, en mettant au carré cette égalité, on a le résultat demandé. Si $z = a + ib$, alors $N(z) = a^2 + b^2$ et a^2, b^2 sont des entiers naturels, donc $N(z)$ aussi. Soit z un entier de Gauss inversible et soit z' son inverse. Alors on sait que $zz' = 1$ et donc $N(z) \times N(z') = 1$. Or le produit de deux entiers naturels est égal à 1 si et seulement si ces deux entiers sont égaux à 1. Donc $N(z) = 1$. Soit $z = a + ib \in \mathbb{Z}[i]$ inversible. Alors $N(z) = 1$, et donc $a^2 + b^2 = 1$. Or, puisque a^2 et b^2 sont des entiers naturels, ceci n'est possible que dans quatre cas : $(a, b) = (1, 0)$, $(a, b) = (-1, 0)$, $(a, b) = (0, 1)$, et $(a, b) = (0, -1)$. Réciproquement, il est facile de vérifier que $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$, d'inverse respectif $1, -1, -i$ et i . Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$.

5. On remarque que $N(z) = |z|^2$. Puisque $|zz'| = |z| \cdot |z'|$, en mettant au carré cette égalité, on a le résultat demandé.

6. Si $z = a + ib$, alors $N(z) = a^2 + b^2$ et a^2, b^2 sont des entiers naturels, donc $N(z)$ aussi.

7. Soit z un entier de Gauss inversible et soit z' son inverse. Alors on sait que $zz' = 1$ et donc $N(z) \times N(z') = 1$. Or le produit de deux entiers naturels est égal à 1 si et seulement si ces deux entiers sont égaux à 1. Donc $N(z) = 1$.

8. Soit $z = a + ib \in \mathbb{Z}[i]$ inversible. Alors $N(z) = 1$, et donc $a^2 + b^2 = 1$. Or, puisque a^2 et b^2 sont des entiers naturels, ceci n'est possible que dans quatre cas : $(a, b) = (1, 0)$, $(a, b) = (-1, 0)$, $(a, b) = (0, 1)$, et $(a, b) = (0, -1)$. Réciproquement, il est facile de vérifier que $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$, d'inverse respectif $1, -1, -i$ et i . Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$.

Correction de l'exercice 23 ▲

On remarque d'abord que $+$ et \circ sont bien des lois de composition interne sur $\text{End}(G)$. Ensuite, on vérifie tous les points de la définition d'un anneau.

1. $(\text{End}(G), +)$ est un groupe commutatif. En effet, la loi $+$ est associative et commutative, l'application $0_G : G \rightarrow G, g \mapsto 0$ est un élément neutre pour la loi $+$, et tout élément $f \in \text{End}(G)$ admet un inverse $-f : G \rightarrow G, x \mapsto -f(x)$.

2. La loi \circ est associative.

3. La loi \circ possède un élément neutre, qui est l'application identité.

4. La loi \circ est distributive par rapport à la loi $+$: pour tous $f, g, h \in \text{End}(G)$ et tout $x \in G$,

$$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x)$$

et

$$(f \circ (g + h))(x) = f((g + h)(x)) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = (f \circ g + f \circ h)(x).$$

Ainsi, $(\text{End}(G), +, \circ)$ est un anneau.

Correction de l'exercice 24 ▲

On va démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour cela, soient $x = \frac{m}{n}$ et $y = \frac{m'}{n'}$ $\in A$. Alors :

$$x - y = \frac{mn' - m'n}{nn'} \text{ et } xy = \frac{mm'}{nn'}.$$

Comme nn' , produit de deux nombres impairs, est impair, et que A est non vide puisqu'il contient 1, on en déduit que A est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons ensuite les inversibles de A . Soit $x = \frac{m}{n} \in A$ inversible, et soit $y = \frac{m'}{n'} \in A$ tel que $xy = 1$. On en déduit que $mm' = nn'$. En particulier, m est nécessairement impair. Réciproquement, si $x = \frac{m}{n}$ avec m impair, alors $y = \frac{n}{m}$ est dans A (si jamais $m < 0$, il suffit d'écrire $y = \frac{-n}{-m}$ pour vérifier qu'il est bien dans A), et $xy = 1$. Ainsi, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m \in \mathbb{Z}$, $n \in \mathbb{N}^*$, et m, n impairs.

Correction de l'exercice 25 ▲

On va prouver que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$. On remarque d'abord que $\mathbb{D} \subset \mathbb{Q}$, puis que $1 \in \mathbb{D}$. De plus, soient $x = \frac{n}{10^k}$ et $y = \frac{m}{10^l}$ deux éléments de \mathbb{D} . Alors

$$x - y = \frac{n10^l - m10^k}{10^{k+l}} \text{ et } xy = \frac{nm}{10^{k+l}}$$

sont clairement des éléments de \mathbb{D} , et $(\mathbb{D}, +, \times)$ est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons ensuite les inversibles de $(\mathbb{D}, +, \times)$. Soit $x = \frac{n}{10^k}$ inversible, d'inverse $y = \frac{m}{10^l}$. Alors

$$xy = 1 \iff nm = 10^{k+l}.$$

On en déduit que les seuls diviseurs premiers de n sont 2 et 5, autrement dit que n s'écrit $\pm 2^p 5^q$ pour $p, q \in \mathbb{N}$. Réciproquement, soit $x = \frac{\pm 2^p 5^q}{10^k}$ et montrons que x est inversible dans \mathbb{D} . Posons $y = \frac{\pm 10^k}{2^p 5^q}$. Il suffit de vérifier que y est élément de \mathbb{D} . Mais on peut aussi écrire

$$y = \frac{\pm 10^k 2^q 5^p}{2^{p+q} 5^{p+q}} = \frac{\pm 10^k 2^q 5^p}{10^{p+q}} \in \mathbb{D}.$$

Ainsi, les inversibles de $(\mathbb{D}, +, \times)$ sont les éléments $\frac{\pm 2^p 5^q}{10^k}$, avec $p, q, k \in \mathbb{N}$.

Correction de l'exercice 26 ▲

Il suffit de vérifier le théorème de caractérisation des sous-anneaux.

$1 \in C(A)$, puisque $1a = a1 = a$ pour tout $a \in A$. Soit $a, a' \in C(A)$ et soit $b \in A$. Alors

$$(a - a')b = ab - a'b = ba - ba' = b(a - a')$$

(on a utilisé deux fois la distributivité) et donc $a - a' \in C(A)$. Soit $a, a' \in C(A)$ et soit $b \in A$. Alors

$$(aa')b = a(a'b) = a(ba') = (ab)a' = (ba)a' = b(aa')$$

(on a utilisé plusieurs fois l'associativité) et donc $aa' \in C(A)$.

Correction de l'exercice 27 ▲

Non, cet anneau n'est pas intègre. Il suffit de trouver deux fonctions non identiquement nulles dont le produit est nul. Par exemple, si $f = 1$ sur $] -\infty, 0]$ et 0 sur $]0, +\infty[$, et si $g = 0$ sur $] -\infty, 0]$ et 1 sur $]0, +\infty[$, alors ni f ni g n'est nulle et pourtant $fg = 0$.

Correction de l'exercice 28 ▲

Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.

2. Remarquons d'abord que pour $p \geq n$, on a $x^p = x^{p-n} x^n = 0$. D'après la formule du binôme, $(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$. Mais, pour $k \geq n$, $x^k = 0 \implies x^k y^{n+m-k} = 0$. D'autre part, pour $k < n$, on a $n+m-k \geq m$ et donc $y^{n+m-k} = 0 \implies x^k y^{n+m-k} = 0$. Ainsi, $(x+y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n+m-1$.

3. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)

$$1 - x^p = (1 - x)(1 + x + \dots + x^{p-1}).$$

Si on l'applique pour $p = n$, alors on obtient

$$1 = (1 - x)(1 + x + \dots + x^{n-1})$$

ce qui implique que $1 - x$ est inversible d'inverse $1 + x + \dots + x^{n-1}$.

4. Soit $n \geq 1$ tel que $(uv)^n = 0$. Alors

$$(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0.$$

Ainsi, vu est nilpotent.

Correction de l'exercice 29 ▲

1. On applique la propriété à l'élément $x+x$. Il vient

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

Après simplification, on trouve $x+x=0$, soit $x=-x$.

2. Soient $x, y \in A$. On doit prouver $xy = yx$. Appliquons la propriété à l'élément $x+y$. On a

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

Après simplification, on trouve $xy + yx = 0$ soit $xy = -yx$, soit $xy = yx$ en appliquant le résultat de la question précédente.

3. Soit $x, y \in A$ avec $x \neq 0$ et $y \neq 0$. Alors

$$\begin{aligned} xy(x+y) &= xyx + yx^2 \\ &= x^2y + x^2y \text{ par commutativité de } A \\ &= xy + xy \text{ par définition d'un anneau de Boole} \\ &= 0 \text{ par la relation démontrée à la première question.} \end{aligned}$$

Puisque A est intègre et que ni x ni y n'est nul, on en déduit que $x+y=0$, soit $x=-y=y$. Ainsi, A ne possède qu'un seul élément non nul, et il contient exactement deux éléments.

Correction de l'exercice 30 ▲

On va commencer par démontrer que $\mathbb{Q}(i)$ est un sous-anneau de \mathbb{C} . Pour cela, on remarque que $1 \in \mathbb{Q}(i)$ si $z = a+ib$ et $z' = a'+ib' \in \mathbb{Q}(i)$, alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Q}(i)$$

et

$$zz' = (a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b) \in \mathbb{Q}(i).$$

Ensuite, soit $z = a + ib \in \mathbb{Q}(i)$, $z \neq 0$. Alors

$$\frac{1}{z} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i \frac{-b}{a^2 + b^2} \in \mathbb{Q}(i).$$

Ainsi, $1/z$ est dans $\mathbb{Q}(i)$ et donc tout élément non nul de $\mathbb{Q}(i)$ admet un inverse dans $\mathbb{Q}(i)$. Ceci achève de prouver que $\mathbb{Q}(i)$ est un corps.

Correction de l'exercice 31 ▲

On va démontrer qu'il s'agit d'un sous-corps de $(\mathbb{R}, +, \times)$. Remarquons d'abord qu'il est bien contenu dans \mathbb{R} et que $0, 1 \in \mathbb{Q}[\sqrt{d}]$. Soient $x, y \in \mathbb{Q}[\sqrt{d}]$. On les écrit $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$. Alors :

$$\begin{aligned} x - y &= (a - a') + (b - b')\sqrt{d} \\ xy &= (aa' + dbb') + (ab' + a'b)\sqrt{d} \end{aligned}$$

ce qui prouve que $x - y$ et $xy \in \mathbb{Q}[\sqrt{d}]$. D'autre part, si $x \neq 0$, alors

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

et donc $\frac{1}{x} \in \mathbb{Q}[\sqrt{d}]$. Remarquons qu'il était possible de multiplier par la quantité conjuguée qui est non-nulle car $\sqrt{d} \notin \mathbb{Q}$. Finalement, on a bien prouvé que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$.

Correction de l'exercice 32 ▲

1. On va commencer par démontrer que \mathcal{C} est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$. Pour cela, on remarque que

la matrice I_2 est bien élément de \mathcal{C} (prendre $a = 1, b = 0$). Soit A, A' deux matrices de \mathcal{C} , écrivons les

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, A' = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}.$$

Alors

$$A + A' = \begin{pmatrix} (a + a') & -(b + b') \\ (b + b') & (a + a') \end{pmatrix} \in \mathcal{C}$$

et

$$A \times A' = \begin{pmatrix} aa' - bb' & -(ab' + a'b) \\ ab' + a'b & aa' - bb' \end{pmatrix} \in \mathcal{C}.$$

De plus, $(\mathcal{C}, +, \times)$ est bien un anneau commutatif car le calcul précédent montre facilement que $A \times A' = A' \times A$. Pour conclure, il faut encore démontrer que si on choisit $A \in \mathcal{C}$, $A \neq 0$, alors A est inversible et $A^{-1} \in \mathcal{C}$. Notons toujours

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Il est facile de voir que A est inversible (par exemple par ce que son déterminant est $a^2 + b^2 \neq 0$). De plus, l'inverse de A est

$$A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

et cette matrice est bien dans \mathcal{C} (choisir $a' = a/(a^2 + b^2)$ et $b' = -b/(a^2 + b^2)$). Ainsi, on a bien démontré que \mathcal{C} est un corps.

2. la matrice I_2 est bien élément de \mathcal{C} (prendre $a = 1, b = 0$).

3. Soit A, A' deux matrices de \mathcal{C} , écrivons les

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, A' = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}.$$

Alors

$$A + A' = \begin{pmatrix} (a+a') & -(b+b') \\ (b+b') & (a+a') \end{pmatrix} \in \mathcal{C}$$

et

$$A \times A' = \begin{pmatrix} aa' - bb' & -(ab' + a'b) \\ ab' + a'b & aa' - bb' \end{pmatrix} \in \mathcal{C}.$$

4. Considérons $\phi(A) = a + ib$, où on a toujours noté

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

On a bien $\phi(I_2) = 1$. De plus, soit

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, A' = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}.$$

Alors d'après le calcul de $A + A'$ fait ci-dessus,

$$\phi(A + A') = (a + a') + i(b + b') = \phi(A) + \phi(A')$$

et de même, d'après le calcul de $A \times A'$,

$$\phi(AA') = (aa' - bb') + i(ab' + a'b) = (a + ib) \times (a' + ib') = \phi(A)\phi(A').$$

Ainsi, ϕ est bien un morphisme d'anneaux (ou de corps). C'est même un isomorphisme : si $A \in \ker(\phi)$, $\phi(A) = 0 \iff A = 0$ et donc $\ker(\phi) = \{0\}$. De plus, $\text{Im}(\phi) = \mathbb{C}^*$, puisque si $z = a + ib \in \mathbb{C}^*$, $z = \phi(A)$ où $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Ainsi, les corps \mathcal{C} et \mathbb{C} sont isomorphes.

Correction de l'exercice 33 ▲

Fixons $a \in A$ non nul et considérons le morphisme de groupes $(A, +) \rightarrow (A, +)$, $x \mapsto ax$. Alors ce morphisme de groupes est injectif, car son noyau est réduit à $\{0_A\}$ puisque A est intègre. Puisque A est fini, ce morphisme est nécessairement bijectif, et donc il existe $x \in A$ tel que $ax = 1_A$. Par commutativité de A , on a aussi $xa = 1_A$ et donc a admet un inverse : A est un corps. Remarquons que l'on peut se passer de l'hypothèse que A est commutatif, par exemple en faisant le même raisonnement avec $x \mapsto xa$, et en prouvant que l'inverse à droite et l'inverse à gauche coïncident.
