

TD 14 : GROUPES, ANNEAUX, CORPS

► Lois de composition interne

EXERCICE 14.1 Soit (E, \leq) 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 .

PD

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 14.2 Éléments réguliers

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 $\forall (y, z) \in E^2, x \star y = x \star z \Rightarrow y = z$ et régulier à droite si $\forall (y, z) \in E^2, y \star x = z \star x \Rightarrow y = z$.

AD

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 14.3 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.

PD

EXERCICE 14.4 Centre d'un groupe

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 $\mathcal{Z}(G) = G$?

PD

EXERCICE 14.5 Divers sous-groupes

Dans chacun des cas suivants, déterminer si H est ou non un sous-groupe de G .

PD

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

EXERCICE 14.6 Donner les tables de multiplication de U_4 et $U_2 \times U_2$. 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.

AD

EXERCICE 14.7 Soit G un groupe tel que $\forall x \in G, x^2 = 1_G$. Montrer que G est abélien, et que tout élément de G est égal à son propre inverse.

PD

EXERCICE 14.8 Un cas particulier du théorème de Lagrange

Soit G un groupe commutatif fini, de cardinal n .

AD

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 14.9 Opérations sur les sous-groupes

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

AD

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

EXERCICE 14.10 Soit G un groupe. On définit une relation binaire sur G par $x \sim y \Leftrightarrow \exists g \in G, x = g^{-1}yg$.

AD

1. Montrer que \sim est une relation d'équivalence sur G .
2. Déterminer le cardinal de la classe d'équivalence de 1_G .
3. Si G est abélien, prouver que les classes d'équivalence sont des singletons.

4. Montrer que si $x \sim y$ et s'il existe $n \in \mathbf{N}$ tel que $x^n = 1_G$, alors $y^n = 1_G$.

EXERCICE 14.11 On note s la conjugaison complexe, c'est-à-dire la fonction de \mathbf{C} dans \mathbf{C} définie par $\forall z \in \mathbf{C}, s(z) = \bar{z}$. On rappelle qu'une similitude directe est une application $f : \mathbf{C} \rightarrow \mathbf{C}$ telle qu'il existe $(a, b) \in \mathbf{C}^* \times \mathbf{C}$ tel que $\forall z \in \mathbf{C}, f(z) = az + b$. On appelle similitude indirecte toute application de la forme $f \circ s$ où f est une similitude directe. On note G l'ensemble des similitudes, directes ou indirectes.

1. Montrer que G , muni de la composition \circ est un groupe.
2. Montrer que l'ensemble H des similitudes directes est un sous-groupe de G . Est-ce que l'ensemble des similitudes indirectes est aussi un sous-groupe de G ?
3. Pour $z_0 \in \mathbf{C}$, on note $G_{z_0} = \{g \in H, g(z_0) = z_0\}$. Montrer que G_{z_0} est un sous-groupe de G .
4. Montrer que si z_0 et z_1 sont distincts, alors $G_{z_0} \cap G_{z_1} = \{\text{id}_{\mathbf{C}}\}$.

EXERCICE 14.12 Conjugaison dans un groupe

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

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

EXERCICE 14.13 Soit $f : G_1 \rightarrow G_2$ un morphisme de groupes.

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 $\text{Ker } f$ est un sous-groupe de G_1 .

EXERCICE 14.14 Déterminer tous les morphismes de groupe de $(\mathbf{Z}, +)$ dans $(\mathbf{Z}, +)$. De $(\mathbf{Q}, +)$ dans $(\mathbf{Z}, +)$.

EXERCICE 14.15 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 .

► Anneaux, corps

EXERCICE 14.16 Montrer que $\mathbf{Z}[\sqrt{2}] = \{x + y\sqrt{2}, (x, y) \in \mathbf{Z}^2\}$ est un anneau.

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

EXERCICE 14.17 Soit \mathbb{D} l'ensemble des nombres décimaux. Montrer que $(\mathbb{D}, +, \times)$ est un anneau. Est-ce un corps ?

EXERCICE 14.18 Produit direct d'anneaux

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

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

EXERCICE 14.20 Soit $(A, +, \times)$ un anneau commutatif. Pour $a \in A$, on appelle racine carrée de a tout élément dont le carré vaut a .

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

EXERCICE 14.22 Montrer qu'un anneau commutatif intègre fini est un corps.

EXERCICE 14.23 Idéaux premiers (D'après oral ENS)

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 $I + xA$ est l'ensemble des éléments qui s'écrivent comme somme d'un élément de I et d'un élément de xA).
 - (b) Prouver qu'un idéal maximal est premier.
3. Montrer que A est un corps si et seulement si tout idéal de A est premier.

CORRECTION DES EXERCICES DU TD 14

SOLUTION DE L'EXERCICE 14.1

- C'est trivial.
- Supposons que E contienne un élément neutre e pour \max . Alors, pour tout $x \in E$, $\max(x, e) = x$, et donc $e \leq x$.
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.
- L'élément neutre est bien entendu inversible, égal à son propre inverse.
Un élément inversible $x \in E$ devra être tel qu'il existe $y \in E$ tel que $\max(x, y) = e$.
Donc soit $x = e$, soit $y = e$.
Mais si $y = e$ est l'inverse de x , alors $x = e^{-1} = e$.
Donc e est l'unique élément inversible de E .

SOLUTION DE L'EXERCICE 14.2

- 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.
- 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 14.3

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.

SOLUTION DE L'EXERCICE 14.4

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 14.5

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 .

2. La matrice nulle est dans H .

La somme¹ 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 $\mathcal{M}_n(\mathbf{C})$.

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 .

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. $\text{id}(1) = 1 \neq 2$, 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 14.6

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

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

$$1 \star 1 = \sqrt[3]{2} \neq 2 = 1 + 1.$$

Danger !

n et p n'ont aucune raison d'être égaux.

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

Remarque

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

Puisque $U_2 = \{-1, 1\}$, le groupe $U_2 \times U_2$ 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 $U_2 \times U_2$, on a $x^2 = (1, 1)$ l'élément neutre.

Supposons par l'absurde qu'il existe un isomorphisme $\varphi : U_2 \times U_2 \rightarrow U_4$.

Alors pour tout $y \in U_4$, il existe un unique $x \in U_2 \times U_2$ tel que $y = \varphi(x)$. Et alors $y^2 = \varphi(x)^2 = \varphi(x^2) = \varphi((1, 1)) = 1$.

Autrement dit, le carré de tout élément de 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 $U_2 \times U_2 \rightarrow U_4$.

SOLUTION DE L'EXERCICE 14.7

Soient $x, y \in G$. Alors $(xy)^2 = e$, soit encore $xyxy = e$. Multiplions alors cette relation à gauche par x et à droite par y , de sorte que

$$x^2 y x y^2 = xy \Leftrightarrow yx = xy.$$

Donc G est abélien.

Et si $x \in G$, multiplions $x^2 = e$ par $x^{-1} : x = x^{-1}$.

Donc tout élément de G est égal à son inverse.

SOLUTION DE L'EXERCICE 14.8

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

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

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

$$\begin{aligned} \prod_{x \in G} (gx) &= \prod_{i=1}^n (gx_i) \\ &= (gx_1)(gx_2) \cdots (gx_n) = gx_1 gx_2 \cdots gx_n \\ &= g g x_1 x_2 g x_3 \cdots g x_n \\ &= \cdots = \underbrace{g \cdots g}_{n \text{ fois}} (x_1 x_2 \cdots x_n) \\ &= g^n \prod_{x \in G} x. \end{aligned}$$

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

3. D'après la question précédente, un sous-groupe de cardinal n de (\mathbb{C}^*, \times) , qui sera forcément commutatif car (\mathbb{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 (\mathbb{C}^*, \times) de cardinal n , alors $G \subset U_n$.

Mais U_n est lui-même de cardinal n , et donc $G = U_n$.

Donc pour tout $n \in \mathbb{N}^*$, (\mathbb{C}^*, \times) possède un unique sous-groupe de cardinal n , qui est U_n .

Rappel

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

Explication

La bijectivité nous dit que les gx , quand x parcourt G , prennent une et une seule fois chaque valeur dans G . Et donc le produit de 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.

SOLUTION DE L'EXERCICE 14.9

- 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 .

- Si l'un des deux sous-groupes est inclus dans l'autre, alors il est évident que $H \cup K$ est un sous-groupe².

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 $K \subset H$.

- 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 $xy = (hk)(h'k') = hkh'k' = \underbrace{hh'}_{\in H} \underbrace{kk'}_{\in K} \in HK$.

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 .

- 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 .

Puisque K et H sont des sous-groupes de HK , KH est inclus dans 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 14.10

- Soit $x \in G$. Alors $x = 1_G^{-1} x 1_G$, donc $x \sim x$: \sim est réflexive.
Soient $(x, y) \in G^2$ tels que $x \sim y$. Alors il existe $g \in G$ tel que $x = g^{-1} y g$. Et alors, en multipliant à gauche par g et à droite par g^{-1} , il vient $y = g x g^{-1} = (g^{-1})^{-1} x g^{-1}$, de sorte que $y \sim x$. Donc \sim est symétrique.
Soient $(x, y, z) \in G^3$ tels que $x \sim y$ et $y \sim z$. Alors il existe deux éléments g et h de G tels que $x = g^{-1} y g$ et $y = h^{-1} z h$.
Et donc $x = g^{-1} h^{-1} z h g = (hg)^{-1} z (hg)$, et donc $x \sim z$: la relation \sim est transitive.
- Un élément $x \in G$ est dans la classe d'équivalence de 1_G si et seulement si il existe $g \in G$ tel que $x = g^{-1} 1_G g = g^{-1} g = 1_G$.
Et donc $1_G = \{1_G\}$.
- Supposons G abélien, et soient $(x, y) \in G^2$ tels que $x \sim y$.
Alors il existe $g \in G$ tel que $x = g^{-1} y g = y g^{-1} g = y$.
Donc la classe d'équivalence de x est réduite à x : c'est un singleton.
- Soient x et y deux éléments de G tels que $x \sim y$, et soit $g \in G$ tel que $y = g^{-1} x g$.
Alors

$$y^n = (g^{-1} x g)^n = g^{-1} x \underbrace{g g^{-1}}_{=1_G} x g \cdots g^{-1} x g = g^{-1} x^n g = g^{-1} 1_G g = 1_G.$$

² 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).

Rédaction

Attention à ne pas oublier le quantificateur existentiel devant g , et ne pas perdre de vue qu'il dépend des éléments x et y .

SOLUTION DE L'EXERCICE 14.11

1. Une similitude directe est une bijection, et s aussi, donc une similitude indirecte est une bijection.

Donc nous allons prouver que G est un sous-groupe de l'ensemble des bijections de \mathbb{C} dans lui-même.

L'identité $\text{id}_{\mathbb{C}}$ est une similitude directe, donc dans G .

Soient $f, g \in G^2$.

► Si f et g sont des similitudes directes, alors leur composée l'est aussi.

► Si $f : z \mapsto az + b$ est directe et $g : z \mapsto c\bar{z} + d$ est indirecte, alors pour tout $z \in \mathbb{C}$,

$$(f \circ g)(z) = a(c\bar{z} + d) + b = \underbrace{ac}_{\neq 0} \bar{z} + (ad + b)$$

donc $f \circ g$ est une similitude indirecte.

► Si $f : z \mapsto a\bar{z} + b$ est directe et $g : z \mapsto cz + d$ est directe, alors pour tout $z \in \mathbb{C}$,

$$(f \circ g)(z) = a(\overline{cz + d}) + b = \underbrace{a\bar{c}}_{\neq 0} \bar{z} + a\bar{d} + b$$

donc $f \circ g$ est une similitude indirecte.

► Si $f : z \mapsto a\bar{z} + b$ et $g : z \mapsto c\bar{z} + d$ sont indirectes, alors pour tout $z \in \mathbb{C}$,

$$(f \circ g)(z) = a(\overline{c\bar{z} + d}) + b = a\bar{c}z + a\bar{d} + b$$

donc $f \circ g$ est une similitude directe.

Donc G est stable par composition.

Enfin, si $f : z \mapsto az + b$ est une similitude directe, alors $f^{-1} : z \mapsto \frac{z-b}{a}$ est une similitude directe.

Et si $f : z \mapsto a\bar{z} + b$ est indirecte, alors $f^{-1} : z \mapsto \frac{\bar{z}-\bar{b}}{a}$ est une similitude indirecte.

Donc G est stable par passage à l'inverse, et donc est un sous-groupe de l'ensemble des bijections de \mathbb{C} dans \mathbb{C} . Et en particulier, est un groupe.

2. Ceci vient quasiment d'être prouvé : l'identité est une similitude directe, la composée de deux similitudes directes est directe, et l'inverse d'une similitude directe est directe.

Donc H est un sous-groupe de G .

Ce n'est pas le cas de l'ensemble des similitudes indirectes, qui ne contient pas l'identité.

3. Notons que G_{z_0} est l'ensemble des éléments de H qui possèdent z_0 comme point fixe. L'identité est bien dans G_{z_0} . Si f, g sont dans G_{z_0} , alors $(f \circ g)(z_0) = f(g(z_0)) = f(z_0) = z_0$.

Donc $f \circ g \in G_{z_0}$.

Enfin, si $f(z_0) = z_0$, alors $f^{-1}(z_0) = z_0$, donc $f^{-1} \in G_{z_0}$.

Donc G_{z_0} est un sous-groupe de H , donc de G .

4. Soient z_0, z_1 distincts, et soit $f \in G_{z_0} \cap G_{z_1}$.

Puisque f est directe, elle est de la forme $z \mapsto az + b$.

$$\text{Mais alors on a } \begin{cases} az_0 + b = z_0 \\ az_1 + b = z_1 \end{cases}.$$

Si $a = 1$, alors $b = 0$, donc $f = \text{id}_{\mathbb{C}}$.

Et si $a \neq 1$, alors $z_0 = \frac{b}{a-1} = z_1$, ce qui est impossible.

Notons que ceci n'est plus vrai pour les similitudes indirectes, qui peuvent avoir une infinité de points fixes, c'est par exemple le cas de $z \mapsto \bar{z}$, qui laisse invariants tous les points de \mathbb{R} .

Remarque

Nous venons de prouver un résultat plutôt intuitif : une fonction affine qui possède deux points fixes (i.e. une droite qui rencontre deux fois la droite d'équation $y = x$) est nécessairement l'identité.

SOLUTION DE L'EXERCICE 14.12

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 $g \in G$,

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

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

Prouvons tout de même injectivité et surjectivité.

Pour l'injectivité, soit $g \in \text{Ker } \tau_a$.

Alors $aga^{-1} = e \Leftrightarrow ag = ea \Leftrightarrow g = e$.

Donc τ_a est injectif.

Soit à présent $y \in G$. Alors $y = a(a^{-1}ya)a^{-1} = \tau_a(a^{-1}ya)$, et donc τ_a est surjectif.

On en déduit donc que τ_a est bijectif.

2. Nous venons de prouver que les τ_a sont des éléments de $\mathfrak{S}(G)$, car bijectifs.

On a $\tau_e = \text{id}_G \in \mathcal{C}(G)$.

Et pour $(a, b) \in G^2$ et $g \in G$, on a

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

Et donc $\tau_a \circ \tau_{b^{-1}} = \tau_{ab^{-1}} \in \mathcal{C}(G)$.

Ainsi, $\mathcal{C}(G)$ 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 14.13

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_1 .

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

SOLUTION DE L'EXERCICE 14.14

Soit $\varphi : \mathbf{Z} \rightarrow \mathbf{Z}$ 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 $\varphi : \mathbf{Q} \rightarrow \mathbf{Z}$ un morphisme. Soit alors $r \in \mathbf{Q}$ non nul, et soit $n \in \mathbf{N}$.

$$\text{Alors } \varphi(r) = \varphi\left(\frac{r}{n} + \frac{r}{n} + \cdots + \frac{r}{n}\right) = \varphi\left(\frac{r}{n}\right) + \cdots + \varphi\left(\frac{r}{n}\right) = n\varphi\left(\frac{r}{n}\right).$$

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.

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 $\{e_G\} \subset \text{Ker } \varphi$, il suffit de prouver l'inclusion réciproque, c'est à dire

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

Remarque

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

SOLUTION DE L'EXERCICE 14.15

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 $p - n \in \mathbf{N}^*$.

De plus, $a * a^{p-n-1} = e_G$, de sorte que $a^{p-n-1} = a^{-1}$.

Or, $p - n - 1 \geq 0$, 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 14.16

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

Et donc $x - y = \underbrace{a - c}_{\in \mathbf{Z}} + \underbrace{(b - d)}_{\in \mathbf{Z}} \sqrt{2} \in \mathbf{Z}[\sqrt{2}]$.

De même, $xy = \underbrace{ac + 2bd}_{\in \mathbf{Z}} + \underbrace{(ad + bc)}_{\in \mathbf{Z}} \sqrt{2} \in \mathbf{Z}[\sqrt{2}]$.

Donc $\mathbf{Z}[\sqrt{2}]$ 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 $\mathbf{Q}(\sqrt{2})$ est un anneau.

De plus, soit x un élément non nul de $\mathbf{Q}(\sqrt{2})$.

Alors il existe deux rationnels a et b tels que $x = a + b\sqrt{2}$.

Et alors l'inverse³ de x

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

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

SOLUTION DE L'EXERCICE 14.17

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, $xy = \frac{k_1k_2}{10^{n_1+n_2}} \in \mathbb{D}$.

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 14.18

Ici, pas question de prouver qu'il s'agit d'un sous-anneau de quelque chose déjà connu, il va donc tout falloir prouver.

Avec tout de même une bonne nouvelle : il a déjà été prouvé en cours que $(A \times B, \oplus)$ est un groupe⁴, 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 .

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

$$(x_A, x_B) \otimes ((y_A, y_B) \otimes (z_A, z_B)) = (x_A, x_B) \otimes ((y_A +_A z_A, y_B +_B z_B))$$

⚠ Attention !

On ne sait pas encore si $a^0 = e_G$ est dans A .

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.

³ Dans le corps \mathbf{R} .

⁴ C'est celui que nous avons appelé produit direct de A et B .

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

\times_A est distributive 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 $a \in A \setminus \{0_A\}$ 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 14.19

- Non, car la suite constante égale à 1 n'est pas dedans.
- Non, car l'opposée d'une suite strictement croissante n'est plus croissante.
- Oui.
- Non : la suite nulle n'est pas divergente.
- Oui : la suite constante égale à 1 est bornée, et la différence et le produit de suites bornées sont bornées.
- Non : l'opposé d'une suite qui tend vers $+\infty$ tend vers $-\infty$.
- Oui : la suite constante égale à 1 est stationnaire⁵.
Si (u_n) et (v_n) sont stationnaires, alors il existe $n_0 \in \mathbf{N}$ et $n_1 \in \mathbf{N}$ tels que $n \geq n_0 \Rightarrow u_n = u_{n_0}$ et $n \geq n_1 \Rightarrow v_n = v_{n_1}$.
Mais alors pour $n \geq \max(n_0, n_1)$, on a $u_n - v_n = u_{n_0} - v_{n_1}$, et donc $(u_n - v_n)$ est stationnaire.
De même, pour $n \geq \max(n_0, n_1)$, $u_n v_n = u_{n_0} v_{n_1}$.
Donc on a bien un sous-anneau de $\mathbf{R}^{\mathbf{N}}$.
- Non, la suite constante égale à 1 n'est pas dedans.

⁵ Puisque constante.

SOLUTION DE L'EXERCICE 14.20

- 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 $c^2 = a \Leftrightarrow c^2 - b^2 = 0_A$.
Soit encore⁶, $(c - b)(c + b) = 0_A$.
Puisque A est intègre, on a donc $c - b = 0_A$ ou $c + b = 0_A$, et donc $c = b$ ou $c = -b$.
Donc a possède au plus deux racines carrées.
- Pour $a \in \mathbf{R}$, la fonction définie par $f_a(x) = \begin{cases} 1 & \text{si } x \leq a \\ -1 & \text{si } x > a \end{cases}$ 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.

⁶ Et là, l'hypothèse que A est commutatif est importante.

Bien entendu

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

SOLUTION DE L'EXERCICE 14.21

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 $f \times g = \tilde{0}$, 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 nulle⁷, ou g est la fonction nulle. Donc $\mathcal{F}(E, A)$ est intègre.

⁷ Qui est le neutre additif de $\mathcal{F}(E, A)$.

En revanche, si $\text{Card}(E) \geq 2$, alors soient x, y deux éléments distincts de $\mathcal{F}(E, A)$. Alors les

fonctions $f : \begin{cases} E \longrightarrow A \\ t \longmapsto \begin{cases} 1_A & \text{si } t = x \\ 0_A & \text{sinon} \end{cases} \end{cases}$ et $g : \begin{cases} E \longrightarrow A \\ t \longmapsto \begin{cases} 1_A & \text{si } t = y \\ 0_A & \text{sinon} \end{cases} \end{cases}$ sont non nulles

mais vérifient $f \times g = \tilde{0}$.

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 14.22

Soit $(A, +, \times)$ un anneau commutatif 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 $x \neq 0_A$.

Alors l'application $f : \begin{cases} A \longrightarrow A \\ y \longmapsto xy \end{cases}$ 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 bijective⁸.

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.

⁸ Ce résultat plutôt intuitif sera prouvé bien plus tard.

SOLUTION DE L'EXERCICE 14.23

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 somme⁹, $b = bx + aby \in I$.

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 .

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.

Inversement, supposons que tout idéal de 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.

⁹ Rappelons que c'est un sous-groupe de $(A, +)$.

Remarque

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