

Chapter 20 Groupes

Exercice 1 (20.1) Étude de lois de composition

Indiquer, parmi les applications suivantes, lesquelles sont des lois de composition interne. Lorsque c'est le cas, préciser l'éventuelle associativité ou commutativité.

$$\perp : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \\ (x, y) \mapsto x - y$$

$$\square : \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} \rightarrow \mathbb{R}^{\mathbb{N}} \\ ((u_n), (v_n)) \mapsto (u_0, v_0, u_1, v_1, u_2, v_2, \dots)$$

$$\top : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \\ (x, y) \mapsto \frac{x+y}{4}$$

$$\triangle : [0, 1] \times [0, 1] \rightarrow [0, 1] \\ (x, y) \mapsto e^{x+y}$$

Solution 1 (20.1)

- La loi \perp est une loi de composition interne sur \mathbb{R} . Elle n'est pas associative car $1 \perp (1 \perp 1) = 1$ qui est différent de $(1 \perp 1) \perp 1 = -1$. Elle n'est pas commutative car $3 \perp 1 = 2$ qui est différent de $1 \perp 3 = -2$.
- La loi \top est une loi de composition interne \mathbb{R} . Elle n'est pas associative car $1 \top (2 \top 3) = \frac{9}{16}$ qui est différent de $(1 \top 2) \top 3 = \frac{12}{16}$. Elle est commutative car pour $x, y \in \mathbb{R}$, $x \top y = \frac{x+y}{4} = \frac{y+x}{4} = y \top x$.
- La loi \square est une loi de composition interne sur $\mathbb{R}^{\mathbb{N}}$. Elle n'est ni associative, ni commutative. En effet, en notant $\tilde{1} = (1)_{n \in \mathbb{N}}$, $\tilde{2} = (2)_{n \in \mathbb{N}}$ et $\tilde{3} = (3)_{n \in \mathbb{N}}$, on a

$$\tilde{1} \square \tilde{2} = (1, 2, 1, 2, 1, 2, 1, 2, \dots) \quad \text{et} \quad \tilde{2} \square \tilde{1} = (2, 1, 2, 1, 2, 1, 2, 1, \dots)$$

qui sont différents. De plus

$$(\tilde{1} \square \tilde{2}) \square \tilde{3} = (1, 3, 2, 3, 1, 3, 2, 3, 1, 3, 2, 3, 1, 3, 2, \dots)$$

$$\text{et} \quad \tilde{1} \square (\tilde{2} \square \tilde{3}) = (1, 2, 1, 3, 1, 2, 1, 3, 1, 2, 1, 3, 1, 2, 1, 3, \dots)$$

- \triangle n'est pas une loi de composition interne : $1 \triangle 1 = e^2 \notin [0, 1]$.

Exercice 2 (20.1) *Propriétés de lois de composition*

Étudier les lois de composition interne suivantes : commutativité, élément neutre éventuel, éléments inversibles.

$$\begin{aligned} \star : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) &\rightarrow \mathcal{P}(\mathbb{N}) \\ (A, B) &\mapsto A \cap B \end{aligned}$$

$$\begin{aligned} \square : \mathbb{R}_+ &\rightarrow \mathbb{R}_+ \\ (x, y) &\mapsto \max(x, y) \end{aligned}$$

$$\begin{aligned} \triangle : (\mathbb{R}^\star \times \mathbb{R})^2 &\rightarrow \mathbb{R}^\star \times \mathbb{R} \\ ((x, y), (x', y')) &\mapsto (xx', xy' + x'y) \end{aligned}$$

Solution 2 (20.1)

- La loi \star est commutative ($A \cap B = B \cap A$) et a pour élément neutre \mathbb{N} ($A \cap \mathbb{N} = A$). Le seul élément ayant un symétrique est \mathbb{N} car si $A \star B \subset A$ donc $A \star B = \mathbb{N}$ implique $A = \mathbb{N}$.
- La loi \square est commutative et admet pour élément neutre 0. Seul 0 admet un symétrique (lui-même).
- La loi \triangle est commutative et admet pour élément neutre $(1, 0)$. De plus,

$$(x, y) \triangle (x', y') = (1, 0) \iff xx' = 1 \text{ et } xy' + x'y = 0 \iff x' = \frac{1}{x} \text{ et } y' = -\frac{x'y}{x} = -\frac{y}{x^2}.$$

La loi \triangle étant commutative, on voit que tout élément $(x, y) \in \mathbb{R}^\star \times \mathbb{R}$ admet un symétrique pour \triangle qui est $\left(\frac{1}{x}, -\frac{y}{x^2}\right)$.

Exercice 3 (20.2)

Sur $G = \mathbb{R}^* \times \mathbb{R}$, on définit la loi \square par $(x, y) \square (x', y') = (xx', xy' + y)$.

1. Montrer que (G, \square) est un groupe.
2. Montrer que $H =]0, +\infty[\times \mathbb{R}$ est un sous-groupe de (G, \square) .

Solution 3 (20.2)

1. Soit $(a, b, c) \in G^3$. On note $a = (x, y)$, $b = (x', y')$ et $c = (x'', y'')$.

- La loi \square est une loi de composition interne sur G puisque

$$a \square b = (xx', xy' + y) \quad \text{et} \quad xx' \in \mathbb{R}^* \quad \text{et} \quad xy' + y \in \mathbb{R}.$$

- La loi \square est associative

$$\begin{aligned} a \square (b \square c) &= (x, y) \square (x'x'', x'y'' + y') = (xx'x'', x(x'y'' + y') + y) = (xx'x'', xx'y'' + xy' + y) \\ \text{et } (a \square b) \square c &= (xx', xy' + y) \square (x'', y'') = (xx'x'', xx'y'' + xy' + y) \end{aligned}$$

On a bien $a \square (b \square c) = (a \square b) \square c$.

- Déterminons l'élément neutre pour \square :

$$a \square b = a \iff xx' = x \quad \text{et} \quad xy' + y = y \iff xx' = x \quad \text{et} \quad xy' = 0.$$

On peut donc choisir $e = (1, 0)$ et on a bien $a \square e = a$. Un calcul direct donne $e \square a = (1 \times x, 1 \times y + 0) = a$. Donc e est bien élément neutre pour \square .

- Déterminons l'inverse de a :

$$a \square b = e \iff xx' = 1 \quad \text{et} \quad xy' + y = 0 \iff x' = \frac{1}{x} \quad \text{et} \quad y' = -\frac{y}{x}.$$

En posant $a' = \left(\frac{1}{x}, -\frac{y}{x}\right)$, on a bien $a \square a' = e$. On vérifie directement

$$a' \square a = \left(\frac{1}{x}x, \frac{1}{x}y + \frac{-y}{x}\right) = (1, 0) = e.$$

donc l'élément a est symétrisable et sont symétrique et $a' = (1/x, -y/x)$.

2. On a clairement $H \subset G$ et $e = (1, 0) \in H$.

Soit $(a, b) \in G^2$. On note $a = (x, y)$, $b = (x', y')$.

On a $a \square b = (xx', xy' + y) \in H$ car $x > 0$ et $x' > 0$ donc $xx' > 0$. Ainsi H est stable par \square .

De plus $a^{-1} = (1/x, -y/x) \in H$ car $x > 0$ donc $1/x > 0$. Ainsi H est stable par passage au symétrique pour \square .

Conclusion

H est un sous-groupe de (G, \square) .

Exercice 4 (20.2)

Soit (G, \cdot) un groupe dont on note e l'élément neutre.

Soit $a, b, c \in G$. On suppose que $b^6 = e$ et $ab = b^4a$. Montrer les égalités $b^3 = e$ et $ab = ba$.

Solution 4 (20.2)

- On a $ab^2 = (ab)b = (b^4a)b = b^4(ab) = b^4(b^4a) = b^8a = b^2a$ car $b^6 = e$.

Puisque a et b^2 commutent, on a $ab = b^4a = ab^4 = (ab)b^3$, en multipliant à gauche par $b^{-1}a^{-1}$ on obtient $b^3 = e$ et finalement $ab = b^4a = b^3ba = eba = ba$.

- (Variante) Puisque $ab = b^4a$, on a $b = a^{-1}b^4a$, d'où

$$b^3 = (a^{-1}b^4a)(a^{-1}b^4a)(a^{-1}b^4a) = a^{-1}b^{12}a = a^{-1}ea = a^{-1}a = e.$$

On a donc $b^3 = e$ et par conséquent $ab = b^4a = b^3ba = eba = ba$.

Exercice 5 (20.2)

Soit (G, \cdot) un groupe tel que $x^2 = e$ pour tout $x \in G$. Montrer que G est commutatif.

Solution 5 (20.2)

- Soit $(x, y) \in G^2$.

La relation $x^2 = e$ signifie $x^{-1} = x$. Ceci est valable pour tout élément de G .

En particulier, $y^{-1} = y$ et $(xy)^{-1} = xy$. Finalement,

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

- (Variante) On a $(xy)^2 = e$, c'est-à-dire $xyxy = e$. En multipliant à gauche par x et à droite par y , il vient $x^2yxy^2 = xy$ d'où $yx = xy$.

Exercice 6 (20.2) Étude des groupes à faibles cardinaux

1. (a) Soit (G, \cdot) un groupe à deux éléments. Construire la table de multiplication de G .
 (b) Soit (G, \cdot) et (G', \cdot) deux groupes à deux éléments. Construire un isomorphisme de groupes de G dans G' .

Ainsi, tous les groupes à deux éléments sont isomorphes. On dit qu'il n'y a qu'un groupe à deux éléments à isomorphisme près.

2. Soit (G, \cdot) un groupe à trois éléments. Construire la table de multiplication de G . En déduire qu'il n'y a qu'un groupe à trois éléments à isomorphisme près.
3. Montrer que \mathbb{U}_4 et $\mathbb{U}_2 \times \mathbb{U}_2$ (muni de la loi de groupe produit) ne sont pas isomorphes (il y a donc plusieurs «types» de groupes à quatre éléments).

Solution 6 (20.2)

1. Notons $G = \{e, a\}$ où e est l'élément neutre de G . On a donc $ee = e$, $ea = a$ et $ae = a$. Reste à déterminer aa . Si $aa = a$, alors en multipliant à gauche par a^{-1} , on obtient $ea = e$ d'où $a = e$ ce qui est manifestement faux. On a donc nécessairement $a \cdot a = e$. D'où la table de multiplication de G donnée par

	e	a
e	e	a
a	a	e

Notons $G' = \{e', a'\}$ un autre groupe à deux éléments où e' est élément neutre. Soit $f : G \rightarrow G'$ définie par $f(e) = e'$ et $f(a) = a'$. La fonction f est clairement bijective. Reste à vérifier que c'est un morphisme de groupe:

$$\begin{array}{ll}
 f(ee) = f(e) = e' & \text{et } f(e)f(e) = e'e' = e' \\
 f(ae) = f(a) = a' & \text{et } f(a)f(e) = a'e' = a' \\
 f(ea) = f(a) = a' & \text{et } f(e)f(a) = e'a' = a' \\
 f(aa) = f(e) = e' & \text{et } f(a)f(a) = a'a' = e'
 \end{array}$$

On a donc bien, pour tout $x, y \in G$, $f(xy) = f(x)f(y)$. Les groupes G et G' sont donc isomorphes.

2. Soit $G = \{e, a, b\}$ un groupe à trois éléments où e est l'élément neutre de G . Nous devons déterminer ab , ba , a^2 et b^2 .

Si $ab = a$, en multipliant à gauche par a^{-1} , on obtient $b = e$, ce qui est exclus, donc $ab \neq a$. Un raisonnement analogue montre que $ab \neq b$. Ainsi $ab = e$ donc $b = a^{-1}$ et on a aussi $ba = e$.

Si $a^2 = a$, en multipliant à gauche par a^{-1} , on obtient $a = e$, ce qui est exclus, donc $a^2 \neq a$. Si $a^2 = e$, alors $a^2 = ab$ et l'on obtient $a = b$: impossible, donc $a^2 \neq e$. Nécessairement $a^2 = b$.

De manière analogue, $b^2 = a$. D'où la table de multiplication de G donnée par

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

On reconnaît la table de multiplication de $\mathbb{U}_3 = \{1, j, \bar{j}\}$ puisque $j^2 = \bar{j} = j^{-1}$.

Comme précédemment, un groupe $G' = \{ e', a', b' \}$ aurait une table de multiplication analogue et on montre que l'application $f : G \rightarrow G'$ telle que $f(e) = e'$, $f(a) = a'$ et $f(b) = b'$ est un isomorphisme entre G et G' .

3. On a $\mathbb{U}_4 = \{ 1, i, -1, -i \} = \{ 1, i, i^2, i^3 \}$.

On note $\mathbb{U}_2 \times \mathbb{U}_2 = \{ e, a, b, ab \}$ où $e = (1, 1)$, $a = (-1, 1)$, $b = (1, -1)$ et donc $ab = ba = (-1, -1)$.

Supposons qu'il existe f un isomorphisme de \mathbb{U}_4 sur $\mathbb{U}_2 \times \mathbb{U}_2$. Alors

$$f(i \cdot i) = f(i) \cdot f(i) = e$$

car pour tout $x \in \mathbb{U}_2 \times \mathbb{U}_2$, on a $x^2 = e$. On a donc $f(-1) = e$. Or f étant un morphisme de groupe, $f(1) = e$ et comme f est injective on obtient $-1 = 1$ ce qui est exclus.

Conclusion

Les groupe \mathbb{U}_4 et $\mathbb{U}_2 \times \mathbb{U}_2$ ne sont pas isomorphes.

On peut montrer que tout groupe à 5 éléments est isomorphe à \mathbb{U}_5 . Remarquez que tous ces groupes sont commutatifs.

À isomorphisme près, il existe deux groupes à 6 éléments \mathbb{U}_6 et S_3 (le groupe des permutations de $\llbracket 1, 3 \rrbracket$). S_3 est le plus petit groupe non commutatif.

Exercice 7 (20.2)

Soit l'ensemble

$$\mathcal{J} = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \mid x \in \mathbb{R}^* \right\}.$$

Montrer que, muni de la multiplication usuelle des matrices, \mathcal{J} est un groupe abélien.

Solution 7 (20.2)

Soit $A = \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in \mathcal{J}$ et $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in \mathcal{J}$. On a

$$AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in \mathcal{J}$$

car $xy \neq 0$.

La multiplication matricielle induit donc une loi de composition interne sur \mathcal{J} . La multiplication matricielle étant associative sur $\mathcal{M}_2(\mathbb{R})$, elle reste associative sur \mathcal{J} .

On vérifie que la matrice $J = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ est élément neutre pour la multiplication dans \mathcal{J} :

$$AJ = \begin{pmatrix} 2\frac{1}{2}x & 2\frac{1}{2}x \\ 2\frac{1}{2}x & 2\frac{1}{2}x \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix} = A.$$

De même, $JA = A$.

En posant $A' = \begin{pmatrix} \frac{1}{2x} & \frac{1}{2x} \\ \frac{1}{2x} & \frac{1}{2x} \end{pmatrix}$, on vérifie

$$A' \in \mathcal{J} \quad \text{et} \quad AA' = J \quad \text{et} \quad A'A = J.$$

Donc A admet un symétrique dans \mathcal{J} qui est A' .

Conclusion

\mathcal{J} est un groupe lorsqu'il est muni de la multiplication matricielle.

Par contre, ce n'est pas un sous-groupe de $\mathcal{M}_2(\mathbb{R})$ (qui n'est pas un groupe pour la multiplication) et ce n'est pas un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ (aucune matrice de \mathcal{J} n'appartient à $\mathbf{GL}_2(\mathbb{R})$).

Exercice 8 (20.2)

Supprimé car doublon.

Solution 8 (20.2)

Exercice 9 (20.2) *Un exemple de sous-groupe*

On pose $\mathbb{Z}[\sqrt{7}] = \left\{ a + b\sqrt{7} \mid (a, b) \in \mathbb{Z}^2 \right\}$.
Montrer que $\mathbb{Z}[\sqrt{7}]$ est un sous-groupe de $(\mathbb{R}, +)$.

Solution 9 (20.2)

Notons $H = \mathbb{Z}[\sqrt{7}]$.

- On a clairement $H \subset \mathbb{R}$.
- L'élément neutre de $(\mathbb{R}, +)$ est $0 = 0 + 0\sqrt{7}$ appartient à H .
- Soit $(x, y) \in H^2$. On note $x = a + b\sqrt{7}$ et $y = a' + b'\sqrt{7}$ avec $a, b, a', b' \in \mathbb{Z}$. On a

$$x + y = a + b\sqrt{7} + a' + b'\sqrt{7} = (a + a') + (b + b')\sqrt{7}$$

donc $x + y \in H$ car $a + a' \in \mathbb{Z}$ et $b + b' \in \mathbb{Z}$.

L'opposé de x est $-x = (-a) + (-b)\sqrt{7} \in H$ car $-a \in \mathbb{Z}$ et $-b \in \mathbb{Z}$.

Conclusion

$\mathbb{Z}[\sqrt{7}]$ est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 10 (20.2)

Montrer que

$$\left\{ \frac{1}{\sqrt{1-x^2}} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \mid x \in]-1, 1[\right\}$$

est un groupe pour la multiplication matricielle.

Solution 10 (20.2)

Notons

$$G = \left\{ \frac{1}{\sqrt{1-x^2}} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \mid x \in]-1, 1[\right\}$$

On va montrer que G est un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ muni de la multiplication matricielle. Ainsi, G sera un groupe pour cette même loi (ou plus précisément pour la loi induite sur G).

Soit $A = \frac{1}{\sqrt{1-x^2}} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \in G$ et $B = \frac{1}{\sqrt{1-y^2}} \begin{pmatrix} 1 & y \\ y & 1 \end{pmatrix} \in G$ avec $x, y \in]-1, 1[$.

- On a $\det(A) = \frac{1}{1-x^2} - \frac{x^2}{1-x^2} = 1 \neq 0$ donc A est inversible. On a bien $G \subset \mathbf{GL}_2(\mathbb{R})$.
- L'élément neutre de $\mathbf{GL}_2(\mathbb{R})$ est $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartient clairement à G (c'est le cas $x = 0$).
- Un calcul direct donne

$$AB = \frac{1}{\sqrt{1-x^2}} \frac{1}{\sqrt{1-y^2}} \begin{pmatrix} 1+xy & x+y \\ x+y & 1+xy \end{pmatrix} = \frac{1+xy}{\sqrt{1-x^2}\sqrt{1-y^2}} \begin{pmatrix} 1 & \frac{x+y}{1+xy} \\ \frac{x+y}{1+xy} & 1 \end{pmatrix}.$$

Posons $z = \frac{x+y}{1+xy}$, alors

$$1 - z^2 = 1 - \frac{x^2 + y^2 + 2xy}{1 + 2xy + x^2y^2} = \frac{1 + 2xy + x^2y^2 - x^2 - y^2 - 2xy}{1 + 2xy + x^2y^2} = \frac{1 + x^2y^2 - x^2 - y^2}{1 + 2xy + x^2y^2} = \frac{(1-x^2)(1-y^2)}{(1+xy)^2}.$$

Cela montre que $1 - z^2 > 0$ car $1 - x^2 > 0$ et $1 - y^2 > 0$, d'où $z \in]-1, 1[$. De plus, comme $1 + xy > 0$, on a

$$\frac{1}{\sqrt{1-z^2}} = \frac{1+xy}{\sqrt{1-x^2}\sqrt{1-y^2}}$$

et par conséquent $AB = \frac{1}{\sqrt{1-z^2}} \begin{pmatrix} 1 & z \\ z & 1 \end{pmatrix} \in G$.

Ainsi, G est stable par multiplication.

- L'inverse de A est la matrice

$$\frac{1}{\det(A)} \begin{pmatrix} \frac{1}{\sqrt{1-x^2}} & \frac{-x}{\sqrt{1-x^2}} \\ \frac{-x}{\sqrt{1-x^2}} & \frac{1}{\sqrt{1-x^2}} \end{pmatrix} = \frac{1}{\sqrt{1-(-x)^2}} \begin{pmatrix} 1 & -x \\ -x & 1 \end{pmatrix}$$

avec $-x \in]-1, 1[$. Ainsi $A^{-1} \in G$.

Conclusion

G est un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ et donc un groupe (pour la multiplication matricielle).

Exercice 11 (20.2)

Pour la multiplication usuelle des matrices carrées, les ensembles suivants sont-ils des groupes.

1. $\text{GL}_2(\mathbb{R}) \cap \mathcal{M}_2(\mathbb{Z})$.
2. $\{ M \in \mathcal{M}_2(\mathbb{Z}) \mid \det M = 1 \}$.

Solution 11 (20.2)

Le premier ensemble n'est pas un groupe car, par exemple, la matrice $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ ne peut avoir pour inverse que $\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ qui n'appartient pas à l'ensemble. Notons $G = \{ M \in \mathcal{M}_2(\mathbb{Z}) : \det M = 1 \}$ et montrons que G est un sous-groupe de $GL(2, \mathbb{R})$.

- la matrice identité appartient à G .
- si $A, B \in G$ alors $AB \in \mathcal{M}_2(\mathbb{Z})$ et $\det AB = \det A \times \det B = 1 \times 1 = 1$, et donc $AB \in G$.
- Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ($a, b, c, d \in \mathbb{Z}$) alors $\frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ appartient à G et est l'inverse de A .

Exercice 12 (20.2)

Soit (G, \star) un groupe. On appelle centre de G l'ensemble

$$Z(G) = \{ x \in G \mid \forall g \in G, x \star g = g \star x \}.$$

Montrer que $Z(G)$ est un sous-groupe de G .

Solution 12 (20.2)

On a clairement $Z(G) \subset G$. On note e l'élément neutre de G .

- Pour tout $g \in G$, $e \star g = g$ et $g \star e = g$ donc $e \star g = g \star e$. Ainsi $e \in Z(G)$.
- Soit $(x, y) \in Z(G)^2$.

Pour tout $g \in G$,

$$\begin{aligned} (x \star y) \star g &= x \star (y \star g) && \text{car } \star \text{ est associative} \\ &= x \star (g \star y) && \text{car } y \in Z(G) \\ &= (x \star g) \star y && \text{car } \star \text{ est associative} \\ &= (g \star x) \star y && \text{car } x \in Z(G) \\ &= g \star (x \star y) && \text{car } \star \text{ est associative.} \end{aligned}$$

On a donc montré que $x \star y \in Z(G)$.

- Pour tout $g \in G$, on a la relation $x \star g = g \star x$. En multipliant à gauche par x^{-1} , on obtient

$$g = x^{-1} \star g \star x$$

puis en multipliant à droite par x^{-1} , on obtient

$$g \star x^{-1} = x^{-1} \star g.$$

Ceci étant vrai pour tout $g \in G$, on a donc $x^{-1} \in Z(G)$.

Conclusion

$Z(G)$ est un sous-groupe de G .

Exercice 13 (20.2)

Soient G un groupe commutatif d'élément neutre e et $n \in \mathbb{N}$. On pose

$$B = \{ a \in G \mid a^n = e \}.$$

Montrer que B est un sous-groupe de G .

Solution 13 (20.2)

Exercice 14 (20.2)

Soit G un groupe commutatif d'élément neutre e . On pose

$$B = \{ a \in G \mid \exists n \in \mathbb{N}^*, a^n = e \}.$$

Montrer que B est un sous-groupe de G .

Solution 14 (20.2)

Exercice 15 (20.2)

Soit G un groupe abélien fini (loi notée multiplicativement), de cardinal $n \geq 2$, de neutre e , et a , un élément de G .

1. En considérant l'ensemble des a^k , $k = 0, \dots, n$, montrer qu'il existe $d \in \llbracket 1, n \rrbracket$ tel que $a^d = e$.
2. Justifier l'existence de ω , le plus petit entier supérieur ou égal à 1 vérifiant $a^\omega = e$. ω s'appelle l'**ordre** de l'élément a .
3. Vérifier que

$$\langle a \rangle = \{ e, a, a^2, \dots, a^{\omega-1} \}$$

est un sous-groupe de G à ω éléments.

Solution 15 (20.2)

Exercice 16 (20.2)

1. Soit $(G, +)$ un groupe commutatif ; soient A et B deux parties de G . On définit la somme de A et B , notée $A + B$, par $A + B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a + b \}$.

Montrer que si A et B sont deux sous-groupes de G , $A + B$ est un sous-groupe de G .

On suppose que A et $A + B$ sont deux sous-groupes de G ; B est-il un sous-groupe de G ?

2. Soit (G, \cdot) un groupe (non commutatif) ; soient A et B deux parties de G . On définit le produit de A et B , noté $A.B$, par $A.B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a.b \}$.

Montrer les équivalences $(A.B \text{ est un sous-groupe de } G) \iff (A.B = B.A) \iff (B.A \subset A.B)$.

Donner un exemple (en précisant G, A, B) où $A.B$ n'est pas un groupe.

Solution 16 (20.2)

Exercice 17 (20.2)

Soient $n \in \mathbb{N}^*$ et $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$. Montrer que f est un endomorphisme du groupe $(\mathbb{R}^*, .)$.

$$x \mapsto x^n$$

Déterminer son image et son noyau.

Solution 17 (20.2)

Exercice 18 (20.2)

Soit $f : \mathbb{R} \rightarrow \mathbb{C}^*$ l'application qui à tout $x \in \mathbb{R}$ associe $e^{ix} \in \mathbb{C}^*$.

1. Montrer que f est un homomorphisme de groupes.
2. Calculer son noyau et son image.
3. f est-elle injective ?

Solution 18 (20.2)

Exercice 19 (20.2)

Traduire en termes d'homomorphisme de groupes les propriétés traditionnelles suivantes

1. $\ln(xy) = \ln x + \ln y$;

2. $|zw| = |z||w|$;

3. $(xy)^{\frac{1}{2}} = x^{\frac{1}{2}}y^{\frac{1}{2}}$;

4. $e^{z+w} = e^z e^w$;

5. $\overline{z + w} = \bar{z} + \bar{w}$;

6. $\overline{zw} = \bar{z}\bar{w}$.

Solution 19 (20.2)

Exercice 20 (20.2)

Soit $(G, .)$ un groupe. Pour $a \in G$ fixé, on considère l'application

$$\begin{aligned} f_a : G &\rightarrow G \\ x &\mapsto a.x.a^{-1} \end{aligned} .$$

1. Montrer que f_a est un automorphisme de $(G, .)$.
2. On note $I = \{ f_a \mid a \in G \}$. Montrer que (I, \circ) est un groupe où \circ est la loi de composition des applications de G dans G .
3. Soit

$$\begin{aligned} \phi : G &\rightarrow I \\ a &\mapsto f_a \end{aligned} .$$

Montrer que ϕ est un morphisme de $(G, .)$ dans (I, \circ) .

Solution 20 (20.2)

Exercice 21 (20.2)

Soit $f : (\mathbb{R}, +) \rightarrow (\mathbb{C}^*, \cdot)$ l'application qui à tout $x \in \mathbb{R}$ associe $e^{ix} \in \mathbb{C}^*$.

Montrer que f est un morphisme de groupes. Calculer son noyau et son image. f est-elle injective ?

Solution 21 (20.2)

Pour $x, y \in \mathbb{R}$,

$$f(x + y) = e^{i(x+y)} = e^{ix+iy} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y).$$

Donc f est un morphisme de groupes. De plus pour $x \in \mathbb{R}$,

$$x \in \ker f \iff f(x) = 1 \iff e^{ix} = 1 \iff x \equiv 0 \pmod{2\pi} \iff x \in 2\pi\mathbb{Z}.$$

On a donc $\ker f = 2\pi\mathbb{Z} = \{ 2k\pi \mid k \in \mathbb{Z} \}$. Le noyau n'est pas réduit à un seul élément, f n'est donc pas injective.

Le cours sur les nombres complexes nous permet d'affirmer $\text{Im } f = \{ e^{ix} \mid x \in \mathbb{R} \} = \mathbb{U} = \{ z \in \mathbb{C}^* \mid |z| = 1 \}$.

Exercice 22 (20.2)

Pour tout couple (a, b) de \mathbb{R}^2 , on pose la matrice

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

Soit

$$\mathcal{G} = \{ M_{a,b} \mid (a, b) \in \mathbb{R}^2 \setminus \{ (0, 0) \} \} \quad \text{et} \quad f : \begin{array}{ccc} \mathcal{G} & \rightarrow & \mathbb{R}^\star \\ M_{a,b} & \mapsto & a^2 + b^2 \end{array}.$$

1. Montrer que \mathcal{G} est un groupe pour la loi usuelle de multiplication des matrices carrées.
2. Montrer que f est un morphisme du groupe (\mathcal{G}, \times) dans le groupe $(\mathbb{R}^\star, \times)$.

Exercice 23 (20.2)

Soit (G, \cdot) un groupe (quelconque). On note $C(G)$ l'ensemble des caractères de G , c'est-à-dire l'ensemble des morphismes de G vers le groupe multiplicatif \mathbb{C}^\star .

1. Montrer que $C(G)$ est un groupe commutatif pour la loi naturelle. On l'appelle *groupe des caractères* de G .
2. Montrer que $C(\mathbb{Z})$ est isomorphe à \mathbb{C}^\star .
3. Soient $n \in \mathbb{N}$ et $\omega = e^{2i\pi/n}$. Montrer que $F : \begin{array}{ccc} C(\mathbb{U}_n) & \rightarrow & \mathbb{U}_n \\ f & \mapsto & f(\omega) \end{array}$ est un isomorphisme de groupes.
4. Soit $G = G_1 \times G_2$ un groupe produit. En introduisant, pour $f_1 \in C(G_1)$ et $f_2 \in C(G_2)$, l'application

$$f : \begin{array}{ccc} G & \rightarrow & \mathbb{C}^\star \\ (g_1, g_2) & \mapsto & f_1(g_1)f_2(g_2) \end{array},$$

montrer que $C(G)$ est isomorphe à $C(G_1) \times C(G_2)$.

Solution 23 (20.2)

Exercice 24 (20.2)

Montrer que si f est une bijection de X sur Y , alors $F : \mathfrak{S}(X) \rightarrow \mathfrak{S}(Y)$ est un isomorphisme.

$$\sigma \mapsto f\sigma f^{-1}$$
Solution 24 (20.2)

Exercice 25 (20.2)

Le but de cet exercice est de montrer que les groupes $(\mathbb{R}^\star, \times)$ et $(\mathbb{C}^\star, \times)$ ne sont pas isomorphes. Supposons qu'il existe un isomorphisme ϕ de $(\mathbb{R}^\star, \times)$ sur $(\mathbb{C}^\star, \times)$.

1. Montrer que $\phi(-1) = -1$.
2. Montrer que si $\alpha = \phi^{-1}(i)$, alors $\alpha^2 = -1$.
3. Conclure.

Solution 25 (20.2)

Exercice 26 (20.2)

Soient p, q deux entiers naturels premiers entre eux et $n = pq$. Soit (G, \cdot) un groupe fini commutatif vérifiant $x^n = 1$ pour tout $x \in G$. On forme

$$M = \{ x \in G \mid x^p = 1 \} \quad \text{et} \quad N = \{ x \in G \mid x^q = 1 \}.$$

1. Montrer que M et N sont des sous-groupes de (G, \cdot) .
2. Vérifier $M \cap N = \{ 1 \}$.
3. Établir que l'application

$$\begin{aligned} f : M \times N &\rightarrow G \\ (x, y) &\mapsto xy \end{aligned}$$

est un isomorphisme de groupes.

Solution 26 (20.2)

Anneaux, corps

Exercice 27 (20.3) *Études d'inversibilités dans un anneau*

Soit $(A, +, \cdot)$ un anneau.

1. Soit $a \in A$ tel que $a^2 = 0$. Démontrer que $1 - a$ et $1 + a$ sont inversibles et expliciter leurs inverses.
2. Généraliser pour $a \in A$ tel qu'il existe $n \in \mathbb{N}^*$ pour lequel $a^n = 0$.

Solution 27 (20.3)

Exercice 28 (20.3) *Éléments nilpotents*

Soit $(A, +, \cdot)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

1. Démontrer que si xy est nilpotent, alors yx l'est aussi.
2. Démontrer que si x et y sont nilpotents et commutent, alors, xy et $x + y$ sont nilpotents.

Solution 28 (20.3)

Exercice 29 (20.3) *Étude d'un ensemble de fonctions*

Soit A l'ensemble des fonctions définies sur \mathbb{R} telles que $f(0) = f(1)$. Démontrer que A est un anneau.

Solution 29 (20.3)

Exercice 30 (20.3)

Soit a un élément d'un ensemble X . Montrer que l'application

$$\begin{aligned} E_a : \mathcal{F}(X, \mathbb{R}) &\rightarrow \mathbb{R} \\ f &\mapsto f(a) \end{aligned}$$

est un morphisme d'anneaux.

Solution 30 (20.3)

Exercice 31 (20.4)

Montrer que $\mathbb{Q}[i\sqrt{3}] = \left\{ a + bi\sqrt{3} \mid (a, b) \in \mathbb{Q}^2 \right\}$ est un corps.

Solution 31 (20.4)

Exercice 32 (20.6) *Nilradical d'un anneau*

On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A , c'est-à-dire des $x \in A$ tels qu'il existe $n \in \mathbb{N}^*$ vérifiant $x^n = 0_A$.
Montrer que N est un idéal de A .

Solution 32 (20.6)