Chapter 13 Groupes

13.1 loi de composition

Solution 13.1
Solution 13.2 *Étude de lois de composition*

- La loi $\perp$ est une loi de composition interne sur $\mathbb{R}$. Elle n'est pas associative car $1\perp(1\perp 1) = 1$ qfui 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

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

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

Solution 13.3 *Propriétés de lois de composition*

- 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 $\left(\frac{1}{x}, -\frac{y}{x^2}\right)$.

13.2 La structure de groupes

Solution 13.4 *Addition des vitesses en théorie de la relativité*
Solution 13.5
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 $\mathscr{M}_2(\mathbb{R})$, 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

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

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 $\mathscr{M}_2(\mathbb{R})$ (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 $\mathbf{GL}_2(\mathbb{R})$).

Solution 13.6

- 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 $yx = xy$.

Solution 13.7

- 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 $ab = b^4a = b^3ba = eba = ba$.

13.3 Sous-groupes

Solution 13.8

Solution 13.9

On a clairement $0 \in H$ (avec $a = 0$ et $n = 12$ par exemple).

Soit $(x, y) \in H^2$. Il existe $a, b \in \mathbb{Z}$ et $n, m \in \mathbb{N}$ tels que $x = \frac{a}{3^n}$ et $y = \frac{b}{3^m}$. On a donc

$$x + y = \frac{a}{3^n} + \frac{b}{3^m} = \frac{a3^m + b3^n}{3^{n+m}} \qquad a3^m + b3^n \in \mathbb{Z} \qquad n + m \in \mathbb{N};$$

donc $x + y \in H$.

De plus, $-x = \frac{-a}{3^n}$, $-a \in \mathbb{Z}$ et $n \in \mathbb{N}$ donc $-x \in H$.

Solution 13.10

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

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

- La loi $\square$ est associative

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

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

- Déterminons l'élément neutre pour $\square$:

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

  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:

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

  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 $(G, \square)$.

Solution 13.11 *Un exemple de sous-groupe*

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 $(\mathbb{R}, +)$.

Solution 13.12

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 $g \in G$,

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

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.

Solution 13.13

- On a clairement $B \subset G$.
- On a bien $e \in B$ puisque $e^n = e$.

- Soit $(x, y) \in B^2$. On a donc $x^n = e$ et $y^n = e$. Puisque G est commutatif, $(xy)^n = x^n y^n = e$, d'où $xy \in B$.

  Deplus, $\left(x^{-1}\right)^n = (x^n)^{-1} = e^{-1} = e$, donc $x^{-1} \in B$.

  Ainsi, B est stable par produit et par passage à l'inverse.

Conclusion

B est un sous-groupe de G.

Solution 13.14

- On a clairement $B \subset G$.
- On a bien $e \in B$ puisque $e^1 = e$.
- Soit $(x, y) \in B^2$. Il existe $p, q \in \mathbb{N}^\star$ tel que $x^p = e$ et $y^q = e$ (il n'y a aucune raison pour que $p = q$). On a donc $x^{pq} = (x^p)^q = e^q = e$ et $y^{pq} = (y^q)^p = e^p = e$. Puisque G est commutatif, $(xy)^{pq} = x^{pq} y^{pq} = e$, d'où $xy \in B$.

  Deplus, $\left(x^{-1}\right)^p = (x^p)^{-1} = e^{-1} = e$, donc $x^{-1} \in B$.

  Ainsi, B est stable par produit et par passage à l'inverse.

Conclusion

B est un sous-groupe de G.

Solution 13.15

Supposons que A et B soient des sous-groupes de G et notons $H = A + B$. Par définition de H, nous avons bien $H \subset G$.

Notons 0 l'élément neutre de G. On a alors $0 \in A$ et $0 \in B$ car A et B sont des sous-groupes de G, d'où $0 + 0 = 0 \in H$.

Soit $(x, y) \in H^2$. Il existe $(a, b) \in A \times B$ et $(a', b') \in A \times B$ tels que $x = a + b$ et $y = a + b$. Puisque A et B sont stables par la loi $+$, $a + a' \in A$ et $b + b' \in B$. Par coséquent

$$x + y = (a + b) + (a' + b') = (a + a') + (b + b') \in H.$$

De plus, A et B étant stable par passage à l'opposé (le symétrique pour la loi $+$), on a également $-a \in A$ et $-b \in B$, d'où

$$-x = -(a + b) = (-a) + (-b) \in H.$$

Conclusion

$H = A + B$ est un sous-groupe de G.

Réciproquement, avec $G = \mathbb{Z}$, $A = \mathbb{Z}$ et $B = \{ 5 \}$, on a $A + B = \mathbb{Z}$. Ainsi, A et $A + B$ sont deux sous-groupes de G, mais pas B.

Solution 13.16

Notons e l'élément neutre de G pour la loi $\cdot$. Commençons par remarquer que l'on a toujours $A \cdot B \subset G$ et $B \cdot A \subset G$.

- Supposons que $A \cdot B$ est un sous-groupe de G.

  Nous allons montrer que $A \cdot B = B \cdot A$ par double inclusion.

Soit $x \in A \cdot B$. Puisque $A \cdot B$ est un sous-groupe de G, alors $x^{-1} \in A \cdot B$, donc il existe $(a, b) \in A \times B$

$$x^{-1} = a \cdot b \quad \text{et} \quad x = b^{-1} \cdot a^{-1}.$$

Puisque A et B sont des sous-groupes de G, $b^{-1} \in B$ et $a^{-1} \in A$ et donc $x \in B \cdot A$. On a donc montré $A \cdot B \subset B \cdot A$.

Réciproquement, soit $x \in B \cdot A$. Il existe $(a, b) \in A \times B$ tels que $x = b \cdot a$. On peut donc écrire

$$x = b \cdot a = (e \cdot b) \cdot (a \cdot e)$$

Et comme $e \cdot b \in A \cdot B$ et $a \cdot e \in A \cdot B$ et $A \cdot B$ est un groupe, alors $x = b \cdot a \in A \cdot B$.

- Trivialement, si $A \cdot B = B \cdot A$, alors $B \cdot A \subset A \cdot B$.
- Supposons $B \cdot A \subset A \cdot B$.

  Notons $H = A \cdot B$. On a clairement $H \subset G$ et $e \in H$ puisque $e \in A$ et $e \in B$.

  Soit $(x, y) \in H^2$. Il existe $(a, b) \in A \times B$ et $(a', b') \in A \times B$ tel que $x = ab$ et $y = a'b'$. On a donc

  $$x \cdot y = a \cdot b \cdot a' \cdot b'$$

  Or $b \cdot a' \in B \cdot A$ donc $b \cdot a' \in A \cdot B$: il existe $(u, v) \in A \times B$ tel que $(b \cdot a' = u \cdot v$. On peut donc écrire

  $$x \cdot y = a \cdot (b \cdot a') \cdot b' = (a \cdot u) \cdot (v \cdot b') \in H.$$

  puisque $a \cdot u \in A$ et $v \cdot b' \in B$.

  De plus, $x^{-1} = b^{-1} \cdot a^{-1} \in B \cdot A$ et donc $x^{-1} \in A \cdot B = H$.

  Nous avons donc montré que H est un sous-groupe de G.

Conclusion

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

Solution 13.17

1. Les a^k avec $k \in [\![0, n]\!]$ sont des éléments de G. Il y a $n+1$ valeurs de k différentes et G est un ensemble à n éléments. D'après le principe des tiroirs et des chaussettes, il existe deux valeurs distinctes $p, q \in [\![0, n]\!]$ telles que $a^p = a^q$.

   (Autrement dit, l'application $[\![0, n]\!] \to G, k \mapsto a^k$ n'est pas injective).

   Quitte à échanger p et q, on peut supposer $0 \leq p < q \leq n$. On pose $d = q - p$, alors $a^d = a^q a^{-p} = e$ et $d \in [\![1, n]\!]$.

2. L'ensemble $W = \left\{ k \in \mathbb{N}^\star, a^k = e \right\}$ est une partie non vide de $\mathbb{N}^\star$ (elle contient d) minorée par 1. Elle admet donc un plus petit élément ω. On a bien $\omega \geq 1$. De plus, $\omega \leq d \leq n$.

3. On a clairement $e \in H$ et $H \subset G$ par définition de H.

   Soit $n \in \mathbb{Z}$, on effectue la division euclidienne de n par ω:

   $$n = \omega q + r \quad \text{et} \quad 0 \leq r < \omega.$$

   On a alors $a^n = a^{\omega q + r} = (a^\omega)^q\, a^r = e^q a^r = a^r \in H$. En particulier, si $x, y \in H$, il existe $p, q \in [\![0, \omega - 1]\!]$ tel que $x = a^p$ et $y = a^q$. D'après la remarque précédente, on a donc

   $$xy = a^{p+q} \in H \quad \text{et} \quad x^{-1} = a^{-p} \in H.$$

Conclusion

L'ensemble H est un sous-groupe de G.

De plus, un raisonnement analogue à la question 1 avec $0 \leq p < q \leq \omega - 1$. monter que les éléments a^k avec $k = 0, \dots, \omega - 1$ sont distincts. Ainsi

$$\text{card } H = \omega.$$

Solution 13.18 *Théorème de Lagrange*

13.4 Morphismes de groupes

Solution 13.19

1. ln est un morphisme du groupe $(\mathbb{R}_+^\star, .)$ dans le groupe $(\mathbb{R}, +)$.
2. $z \mapsto |w|$ est un morphisme du groupe $(\mathbb{C}^\star, .)$ dans le groupe $(\mathbb{C}, .)$.
3. $x \mapsto x^{1/2}$ est un morphisme du groupe $(\mathbb{R}_+^\star, .)$ dans le groupe $(\mathbb{R}_+^\star, .)$.
4. exp est un morphisme du groupe $(\mathbb{C}, +)$ dans le groupe $(\mathbb{C}^\star, .)$.
5. $z \mapsto \bar{z}$ est un morphisme du groupe $(\mathbb{C}, +)$ dans le groupe $(\mathbb{C}, +)$.
6. $z \mapsto \bar{z}$ est un morphisme du groupe $(\mathbb{C}, .)$ dans le groupe$(\mathbb{C}, .)$.

Solution 13.20

1. Soit $x, y \in G$, alors

$$f_a(xy) = axya^{-1}$$
$$\text{et } \ f_a(x)f_a(y) = axa^{-1}aya^{-1} = axeya^{-1} = axya^{-1}$$

et donc $f_a(xy) = f_a(x)f_a(y)$.

L'application f_a est donc un endomorphisme de G.

De plus, pour $x \in G$ et $y \in G$, on a

$$f(x) = y \iff axa^{-1} = y \iff x = a^{-1}ya.$$

Ainsi, y a un unique antécédent par f qui est $a^{-1}ya$: l'application f est bijective. On peut remarquer que sa réciproque est $f_{a^{-1}}$.

Conclusion

L'application f_a est un automorphisme de $(G, .)$.

2. Nous allons montrer que I est un sous-groupe de $(S(G), \circ)$, le groupe des permutation de G. Ainsi, I sera un groupe lorsqu'il est muni de la loi $\circ$.

   - $I \subset S(G)$ puisque nous avons montrer au dessus que toute élément de I est une bijection.
   - En notant e l'élément neutre de G, on a $\text{Id}_G = f_e \in I$.

- Soit f_a et f_b deux éléments de I. Pour $x \in G$,

$$f_a \circ f_b(x) = a\left(bxb^{-1}\right)a^{-1} = (ab)\,x\left(b^{-1}a^{-1}\right) = (ab)\,x\,(ab)^{-1}.$$

Ce qui montrer que $f_a \circ f_b = f_{ab} \in I$. Ainsi I est stable par $\circ$.

De plus, nous avons vu au dessus que $\left(f_a\right)^{-1} = f_{a^{-1}}$ et donc $\left(f_a\right)^{-1} \in I$.

Conclusion

I est un sous-groupe de $(S(G), \circ)$ et donc un groupe pour la loi (induite) $\circ$.

3. Soit $(a, b) \in G^2$. Nous avons vu au dessus

$$\varphi(a) \circ \varphi(b) = f_a \circ f_b = f_{ab} = \varphi(ab).$$

Autrement dit, φ est un morphisme de $(G, .)$ dans $(I, \circ)$.

Solution 13.21

Soit $x, y \in \mathbb{R}^\star$, alors

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

Donc f est un morphisme de $\mathbb{R}^\star$ dans lui-même.

De plus,

$$f(x) = 1 \iff x^n = 1.$$

- Si n est un entier pair $\ker(f) = \{ -1, 1 \}$.
- Si n est un entier impair $\ker(f) = \{ 1 \}$.

Une étude de fonction rapide donne

- Si n est un entier pair $\operatorname{Im}(f) =]0, +\infty[$.
- Si n est un entier impair $\operatorname{Im}(f) = \mathbb{R}^\star$.

Solution 13.22

1. Soit $x, y \in \mathbb{R}$.

$$f(x)f(y) = e^{ix}e^{iy} = (\cos x + i \sin x)(\cos y + i \sin y) = (\cos x \cos y - \sin x \sin y) + i(\sin x \cos y + \cos x \sin y)$$

On reconnait alors les formules d'additions, d'où

$$f(x)f(y) = \cos(x+y) + i\sin(x+y) = e^{i(x+y)} = f(x+y).$$

2.
- On a

$$x \in \ker(f) \iff f(x) = 1 \iff e^{ix} = 1 \iff \exists k \in \mathbb{Z}, x = 2k\pi.$$

Autrement dit, $\ker(f) = 2\pi\mathbb{Z} = \{ 2k\pi \mid k \in \mathbb{Z} \}$.
- $\operatorname{Im}(f) = \left\{ e^{ix} \,\middle|\, x \in \mathbb{R} \right\} = \mathbb{U} = \left\{ z \in \mathbb{C}^\star \,\middle|\, |z| = 1 \right\}$.

3. L'application f n'est pas injective puisque $\ker(f) \neq \{ 0 \}$.

Solution 13.23 *Étude des groupes à faibles cardinaux*

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 $G' = \left\{ e', a' \right\}$ un autre groupe à deux éléments où e' est élément neutre. Soit $f : G \to G'$ 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:

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

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

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

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

   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 élément $\mathbb{U}_6$ et S_3 (le groupe des permutations de $[\![1,3]\!]$). S_3 est le plus petit groupe non commutatif.

Solution 13.24

Solution 13.25

Vu en cours!

Solution 13.26

1. Dans $(\mathscr{F}G, \mathbb{C}, +, .)$, l'anneau des fonctions de G dans $\mathbb{C}$, l'ensemble des éléments inversibles (pour la multiplication) est $\mathscr{F}(G, \mathbb{C}^\star)$, autrement dit l'ensemble des fonctions qui ne s'annule pas. Nous allons donc montrer que $\widehat{G}$ est un sous-groupe de $\left(\mathscr{F}(G, \mathbb{C}^\star), .\right)$.

   L'application $e : G \to \mathbb{C}^\star, x \mapsto 1$ est bien un morphisme puisque, pour $x, y \in G$,

$$e(x.y) = 1 \qquad \text{et} \qquad e(x).e(y) = 1.1 = 1.$$

   Soit $f, g \in \widehat{G}$. Montrons que fg est un morphisme de G dans $\mathbb{C}^\star$. Pour $x, y \in G$,

$$\begin{aligned}
(fg)(xy) &= f(xy)g(xy) && \text{part définition du produit de deux fonctions} \\
&= f(x)f(y)g(x)g(y) && \text{car } f \text{ et } g \text{ sont des morphismes de } G \text{ dans } \mathbb{C}^\star \\
&= f(x)g(x)f(y)g(y) && \text{car le produit dans } \mathbb{C}^\star \text{ est commutatif} \\
&= (fg)(x)(fg)(y) && \text{part définition du produit de deux fonctions.}
\end{aligned}$$

   On a donc bien $fg \in \widehat{G}$.

   De plus, pour $x, y \in G$,

$$\begin{aligned}
f^{-1}(xy) &= \frac{1}{f(xy)} && 1/f \text{ est l'inverse de } f \text{ pour la multiplication} \\
&= \frac{1}{f(x)f(y)} && \text{car } f \text{ est un morphisme de } G \text{ dans } \mathbb{C}^\star \\
&= \frac{1}{f(x)}\frac{1}{f(y)} && \text{ce sont des calculs dans } \mathbb{C}^\star \\
&= f^{-1}(x)f^{-1}(y) && \text{On retrouve l'inverse de } f \text{ pour la multiplication.}
\end{aligned}$$

   On a donc bien $f^{-1} \in \widehat{G}$.

Conclusion

L'ensemble $\widehat{G}$ muni de la multiplication des fonctions est un sous-groupe de $\mathscr{F}(G, \mathbb{C}^\star)$ et donc un groupe.

2. Un morphisme de $(\mathbb{Z}, +)$ dans $\mathbb{C}$ est entièrement déterminer par sa valeur en 1. En effet, si $f \in \widehat{\mathbb{Z}}$, alors pour $n \in \mathbb{Z}$,

$$f(n) = f(n.1) = f(\underbrace{1 + 1 + \cdots + 1}_{n}) = \underbrace{f(1) \cdot f(1) \cdot \cdots \cdot f(1)}_{n} = f(1)^n.$$

   Ainsi,

$$\begin{array}{rccc}
\varphi : & \widehat{\mathbb{Z}} & \to & \mathbb{C}^\star \\
& f & \mapsto & f(1)
\end{array}$$

est injective. De plus, si $f, g \in \widehat{\mathbb{Z}}$, alors $\varphi(fg) = (fg)(1) = f(1)g(1) = \varphi(f)\varphi(g)$. Donc φ est un morphisme du groupe $\widehat{\mathbb{Z}}$ dans le groupe $\mathbb{C}^\star$.

Enfin, si $a \in \mathbb{C}^\star$, alors $f : n \mapsto a^n$ est un morphimse de $\mathbb{Z}$ dans $\mathbb{C}^\star$, et on a bien $\varphi(f) = a$. Donc φ est surjective.

Conclusion

L'application φ est un isomorphisme du groupe $\widehat{\mathbb{Z}}$ dans le groupe $\mathbb{C}^\star$.

Remarque. Pour l'injectivité, on aurait pu aussi étudier $\ker \varphi = \{ e \}$ où $e : x \mapsto 1$.

3. On remarque que si $f \in \widehat{\mathbb{U}_n}$ et $k \in \mathbb{Z}$,

$$f\left(e^{2ik\pi/n}\right) = f\left(\omega^k\right) = f(\omega)^k .$$

Un élément de $\widehat{\mathbb{U}_n}$ est donc entièrement caractériser par sa valeur en ω. La suite de la démonstration est analogue à la question précédente.

4. On note

$$\begin{array}{rccc} T : & \widehat{G_1} \times \widehat{G_2} & \to & \widehat{G} \\ & (f_1, f_2) & \mapsto & f \end{array}$$

où $f(x_1, x_2) = f_1(x_1)f_2(x_2)$.

Soit $(f_1, f_2) \in \widehat{G_1} \times \widehat{G_2}$ et $(g_1, g_2) \in \widehat{G_1} \times \widehat{G_2}$. On pose $f = T(f_1, f_2)$ et $g = T(g_1, g_2)$. Pour $(x_1, x_2) \in G_1 \times G_2$,

$$T\left((f_1, f_2).(g_1, g_2)\right)(x_1, x_2) = T\left(f_1g_1, f_2g_2\right)(x_1, x_2) = \left(f_1g_1\right)(x_1)\left(f_2g_2\right)(x_2) = f_1(x_1)g_1(x_1)f_2(x_2)g_2(x_2) = f$$

Ceci étant vrai pour tout $(x_1, x_2) \in G$, on a

$$T\left((f_1, f_2).(g_1, g_2)\right) = fg = T\left(f_1, f_2\right) T\left(g_1, g_2\right),$$

donc T est un morphisme de groupe.

Étudions le noyau de T. Supposons que $T(f_1, f_2) = e_{\widehat{G}} : x \mapsto 1$. On a alors,

$$\forall (x_1, x_2) \in G_1 \times G_2, f_1(x_1)f_2(x_2) = 1.$$

En particulier, avec $x_1 = e_{G_1}$ (l'élément neutre de G_1), on a $f_1(e_{G_1}) = 1$ et on obtient

$$\forall x_2 \in G_2 f_2(x_2) = 1$$

et donc $f_2 = e_{\widehat{G_2}} : x \mapsto 1$. *Mutatis mutandis*, en spécialisant avec $x_2 = e_{G_2}$, on obtient $f_1 = e_{\widehat{G_1}}$. Finalement $(f_1, f_2) = \left(e_{\widehat{G_1}}, e_{\widehat{G_2}}\right)$ qui est l'élément neutre du groupe produit $\widehat{G_1} \times \widehat{G_2}$.

Nous avons donc montrer $\ker(T) \subset \left\{ \left(e_{\widehat{G_1}}, e_{\widehat{G_2}}\right) \right\}$, l'inclusion réciproque étant automatique. Donc T est injective.

Soit $f \in \widehat{G}$. On définit

$$\begin{array}{rccc} f_1 : & G_1 & \to & \mathbb{C}^\star \\ & x_1 & \mapsto & f(x_1, e_{G_2}) \end{array} \quad \text{et} \quad \begin{array}{rccc} f_2 : & G_2 & \to & \mathbb{C}^\star \\ & x_2 & \mapsto & f(e_{G_1}, x_2) \end{array}$$

On a alors $T(f_1, f_2) = f$ puisque pour $(x_1, x_2) \in G_1 \times G_2$,

$$f_1(x_1)f_2(x_2) = f(x_1, e_{G_2})f(e_{G_1}, x_2) = f\left(x_1e_{G_1}, e_{G_2}x_2\right) = f\left(x_1, x_2\right).$$

Reste à vérifier (facile) que $f_1 \in \widehat{G_1}$ et $f_2 \in \widehat{G_2}$. Ce qui montre que T est surjective.

Conclusion

L'application T est un isomorphisme de $\widehat{G_1} \times \widehat{G_2}$ dans $\hat{G}$.

Solution 13.27

1. On a
$$\varphi(-1)^2 = \varphi((-1)^2) = \varphi(1) = 1$$
donc $\varphi(-1) = \pm 1$. Or φ est injective et $\varphi(1) = 1$. On a nécessairement $\varphi(-1) = -1$.

2. On a $\varphi(\alpha) = i$ donc $\varphi(\alpha^2) = i^2 = -1$. D'après la questions précédente $\alpha^2 = -1$.

3. On obtient donc $\alpha \in \mathbb{R}^\star$ tel que $\alpha^2 = -1$: impossible.
Un tel isomorphisme n'exite donc pas.

Solution 13.28

1. Voir l'exercice ??? en début de fiche.

2. On a déjà $\{ 1 \} \subset M \cap N$ car M et N sont des sous-groupes de G.
Soit $x \in M \cap N$. On a donc $x^p = 1$ et $x^q = 1$. Comme p et q sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$, d'où
$$x = x^1 = x^{up+vq} = x^{up}x^{vq} = (x^p)^u (x^q)^v = 1^u 1^v = 1.$$
On a donc bien $M \cap N \subset \{ 1 \}$ et le résultat par double inclusion.

3. Soit $a = (x_1, y_1) \in M \times N$ et $b = (x_2, y_2) \in M \times N$, alors
$$f(ab) = f\left((x_1, y_1) \cdot (x_2, y_2)\right) = f\left(x_1x_2, y_1y_2\right) = x_1x_2y_1y_2$$
$$\text{et } \; f(a)f(b) = f(x_1, y_1)f(x_2, y_2) = x_1y_1x_2y_2$$
et puisque G est un groupe commutatif, on a bien $f(ab) = f(a)f(b)$. Ainsi, f est un morphisme de groupes.
Pour montrer que f est injective, nous allons montrer $\ker(f) = \{ (1, 1) \}$. Soit $(x, y) \in \ker(f)$. On a donc $x \in M$, $y \in N$ et $f(x, y) = xy = 1$. Nous allons exploiter la relation $up + vq = 1$.
$$1 = (xy)^{vq} = x^{vq}y^{vq} = x^1x^{-up} \cdot y^{vq} = x \cdot 1 \cdot 1 = x.$$
D'où $x = 1$ puis $y = xy = 1$. On a donc $(x, y) = (1, 1)$ et $\ker(f) = \{ (1, 1) \}$. L'application f est donc injective.
Enfin, pour $z \in G$, on a $z^n = 1$, ou encore $(z^p)^q = 1$. Donc $z^p \in N$ et même $z^{pu} \in N$. De même $z^{vq} \in M$. On peut écrire
$$z = z^1 = z^{up+vq} = z^{vq} \cdot z^{up}$$
Autrement dit, $(z^{vq}, z^{up}) \in M \times N$ et
$$f\left(z^{vq}, z^{up}\right) = z.$$
donc z admet un antécédent par f. On a donc montrer que f est aussi surjective.

Conclusion

L'application f est un isomorphisme du groupe produit $M \times N$ sur le groupe G.

Solution 13.29
Solution 13.30 *Lemme des 5*

13.5 Générateurs

Solution 13.31
Solution 13.32
Solution 13.33
Solution 13.34