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.

$$\perp : \begin{array}{rcl} \mathbb{R}\times\mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & x-y \end{array} \qquad \top : \begin{array}{rcl} \mathbb{R}\times\mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & \frac{x+y}{4} \end{array}$$

$$\square : \begin{array}{rcl} \mathbb{R}^{\mathbb{N}}\times\mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ \big((u_n),(v_n)\big) & \mapsto & (u_0, v_0, u_1, v_1, u_2, v_2, \dots) \end{array} \qquad \triangle : \begin{array}{rcl} [0,1]\times[0,1] & \to & [0,1] \\ (x,y) & \mapsto & \mathrm{e}^{x+y} \end{array}.$$

Solution 1 (20.1)

- La loi $\perp$ est une loi de composition interne sur $\mathbb{R}$. Elle n'est pas associative car $1\perp(1\perp1) = 1$ qfui est différent de $(1\perp1)\perp1 = -1$. Elle n'est pas commutative car $3\perp1 = 2$ qui est différent de $1\perp3 = -2$.
- La loi $\top$ est une loi de composition interne $\mathbb{R}$. Elle n'est pas associative car $1\top(2\top3) = \frac{9}{16}$ qui est différent de $(1\top2)\top3 = \frac{12}{16}$. 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 : $1 \triangle 1 = e^2 \notin [0,1]$.

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

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

$$\star : \begin{array}{rcl} \mathfrak{P}(\mathbb{N}) \times \mathfrak{P}(\mathbb{N}) & \to & \mathfrak{P}(\mathbb{N}) \\ (A, B) & \mapsto & A \cap B \end{array} \qquad \square : \begin{array}{rcl} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ (x, y) & \mapsto & \max(x, y) \end{array}$$

$$\triangle : \begin{array}{rcl} \left(\mathbb{R}^\star \times \mathbb{R}\right)^2 & \to & \mathbb{R}^\star \times \mathbb{R} \\ \big((x, y), (x', y')\big) & \mapsto & \left(xx', xy' + x'y\right) \end{array}$$

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 $G = \mathbb{R}^\star \times \mathbb{R}$, 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

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

   - 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 $(G, \square)$.

Exercice 4 (20.2)

Soit $(G,.)$ 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

$$\begin{array}{c|cc} & e & a \\ \hline e & e & a \\ a & a & e \end{array}$$

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

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$

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.

Exercice 7 (20.2)

Soit l'ensemble
$$\mathcal{J} = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \;\middle|\; x \in \mathbb{R}^\star \right\}.$$
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
$$A' \in \mathcal{J} \qquad \text{et} \qquad AA' = J \qquad \text{et} \qquad A'A = J.$$
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 $\mathcal{M}_2(\mathbb{R})$ (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 $\mathbb{Z}[\sqrt{7}] = \left\{ a + b\sqrt{7} \;\middle|\; (a, b) \in \mathbb{Z}^2 \right\}$.
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

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

est un groupe pour la multiplication matricielle.

Solution 10 (20.2)

Notons

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

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 précisement 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

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

Cela montre que $1 - z^2 > 0$ car $1 - x^2 > 0$ et $1 - y^2 > 0$, d'où $z \in]-1, 1[$. Deplus, 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. $\mathbf{GL}_2(\mathbb{R}) \cap \mathscr{M}_2(\mathbb{Z})$.
2. $\left\{ M \in \mathscr{M}_2(\mathbb{Z}) \,\middle|\, \det M = 1 \right\}$.

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 $g \in G$,

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

  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.

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)

- 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.

Exercice 14 (20.2)

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

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

Montrer que B est un sous-groupe de G.

Solution 14 (20.2)

Solution 14 (20.2)

- 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.

Exercice 15 (20.2)

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

1. En considérant l'ensemble des a^k, $k = 0, \dots, n$, montrer qu'il existe $d \in [\![1, n]\!]$ 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
$$< a >= \left\{ e, a, a^2, \dots, a^{\omega-1} \right\}$$
est un sous-groupe de G à ω éléments.

Solution 15 (20.2)

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 $e \in < a >$ et $< a > \subset G$ par définition de $< a >$.

   Soit $n \in \mathbb{Z}$, on effectue la division euclidienne de n par ω:
$$n = \omega q + r \qquad \text{et} \qquad 0 \leq r < \omega.$$
   On a alors $a^n = a^{\omega q + r} = (a^\omega)^q a^r = e^q a^r = a^r \in < a >$. En particulier, si $x, y \in < a >$, 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
$$xy = a^{p+q} \in < a > \qquad \text{et} \qquad x^{-1} = a^{-p} \in < a > .$$

   Conclusion

   L'ensemble $< a >$ 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
$$\text{card} < a >= \omega.$$

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

$$A + B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a + b \} .$$

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

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

2.
ATTENTION : erreur d'énoncé... A et B sont deux sous-groupes!!!!
Soit $(G, \cdot)$ un groupe (non commutatif) ; soient A et B deux sous-groupes de G. On définit le produit de A et B, noté $A \cdot B$, par

$$A \cdot B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a.b \} .$$

Montrer les équivalences

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

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

Solution 16 (20.2)

1.

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.

2.

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

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

Exercice 17 (20.2)

Soient $n \in \mathbb{N}^\star$ et $f : \begin{array}{ccc} \mathbb{R}^\star & \to & \mathbb{R}^\star \\ x & \mapsto & x^n \end{array}$. Montrer que f est un endomorphisme du groupe $(\mathbb{R}^\star, .)$.
Déterminer son image et son noyau.

Solution 17 (20.2)
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 $\operatorname{Im}(f) = \mathbb{R}^\star$.

Exercice 18 (20.2)

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

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)

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

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

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. $\mathrm{e}^{z+w} = \mathrm{e}^{z}\,\mathrm{e}^{w}$;
5. $\overline{z+w} = \bar{z} + \bar{w}$;
6. $\overline{zw} = \bar{z}\bar{w}$.

Solution 19 (20.2)

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$(\mathbb{C}, .)$.

Exercice 20 (20.2)

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

$$f_a : \begin{array}{rcl} G & \to & G \\ x & \mapsto & a.x.a^{-1} \end{array}.$$

1. Montrer que f_a est un automorphisme de $(G, .)$.

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

3. Soit

$$\phi : \begin{array}{rcl} G & \to & I \\ a & \mapsto & f_a \end{array}.$$

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

Solution 20 (20.2)

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

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

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 $\mathrm{Id}_G = f_e \in I$.
- 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

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

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

Exercice 21 (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

$$\mathcal{G} = \left\{ M_{a,b} \,\middle|\, (a, b) \in \mathbb{R}^2 \setminus \{ (0,0) \} \right\} \qquad \text{et} \qquad f : \begin{array}{ccc} \mathcal{G} & \to & \mathbb{R}^\star \\ M_{a,b} & \mapsto & a^2 + b^2 \end{array}.$$

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 $\left(\mathbb{R}^\star, \times\right)$.

Solution 21 (20.2)

1. Pour montrer que $\mathcal{G}$ est un groupe pour la multiplication des matrices carrées, il suffit de montrer que c'est un sous-groupe de $\left(\mathbf{GL}_2(\mathbb{R}), \times\right)$.

   - Pour $(a, b) \neq (0, 0)$,
   $$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 \neq 0$$
   ce qui montre que $M_{a,b}$ est inversible. On a donc bien $\mathcal{G} \subset \mathbf{GL}_2(\mathbb{R})$.
   - On a $I_2 = M_{1,0} \in \mathcal{G}$.
   - Soit $(a, b) \in \mathbb{R}^2 \setminus \{ (0,0) \}$ et $(c, d) \in \mathbb{R}^2 \setminus \{ (0,0) \}$.
   $$M_{a,b}M_{c,d} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{pmatrix} = M_{u,v}.$$
   avec $u = ac - bd$ et $v = bc + ad$. Remarquons que $M_{u,v}$ est le produit de deux matrices inversibles, donc elle est aussi inversible et nécessairement $(u, v) \neq (0, 0)$.
   - L'inverse de la matrice $M_{a,b}$ est
   $$M_{a,b}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = M_{a',b'}$$
   avec $a' = \frac{a}{a^2+b^2}$ et $b' = \frac{-b}{a^2+b^2}$ et $(a', b') \neq (0, 0)$ donc $M_{a,b}^{-1} \in \mathcal{G}$.

   Conclusion

   $\mathcal{G}$ est un sous-groupe de $\mathbf{GL}_2(\mathbb{R})$ et donc un groupe lorsqu'il est muni de la multiplication des matrice carrées.

2. Soit $(a, b) \in \mathbb{R}^2 \setminus \{ (0,0) \}$ et $(c, d) \in \mathbb{R}^2 \setminus \{ (0,0) \}$. On note $(u, v) = (ac - bd, bc + ad)$, de sorte que $M_{a,b}M_{c,d} = M_{u,v}$. On a
$$f\left(M_{a,b}\right) f\left(M_{c,d}\right) = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac)^2 + (bc)^2 + (ad)^2 + (bd)^2$$
$$\text{et } f\left(M_{a,b}M_{c,d}\right) = \left(u^2 + v^2\right) = (ac)^2 - \cancel{2acbd} + (bd)^2 + (bc)^2 + \cancel{2bcad} + (ad)^2$$

et donc $f\left(M_{a,b}M_{c,d}\right) = f\left(M_{a,b}\right) f\left(M_{c,d}\right)$

Conclusion

L'application f est un morphisme du groupe $(\mathcal{G}, \times)$ dans le groupe $\left(\mathbb{R}^{\star}, \times\right)$.

Exercice 22 (20.2)

Soit $(G, .)$ 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 $F : \begin{array}{ccc} C(\mathbb{U}_n) & \to & \mathbb{U}_n \\ f & \mapsto & f(\omega) \end{array}$ 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
$$f : \begin{array}{ccc} G & \to & \mathbb{C}^\star \\ (x_1, x_2) & \mapsto & f_1(x_1)f_2(x_2) \end{array},$$
montrer que $C(G)$ est isomorphe à $C(G_1) \times C(G_2)$.

Solution 22 (20.2)

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 $C(G)$ 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 $x, y \in G$,
$$e(x.y) = 1 \quad \text{et} \quad e(x).e(y) = 1.1 = 1.$$
   Soit $f, g \in C(G)$. 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 $fg \in C(G)$.

   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 $f^{-1} \in C(G)$.

   Conclusion

   L'ensemble $C(G)$ 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 $f \in C(\mathbb{Z})$, 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,

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

est injective. De plus, si $f, g \in C(\mathbb{Z})$, alors $\phi(fg) = (fg)(1) = f(1)g(1) = \phi(f)\phi(g)$. Donc ϕ est un morphisme du groupe $C(\mathbb{Z})$ 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 $\phi(f) = a$. Donc ϕ est surjective.

Conclusion

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

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

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

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

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

4. On note

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

où $f(x_1, x_2) = f_1(x_1) f_2(x_2)$.

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

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

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 $T(f_1, f_2) = e_{C(G)} : x \mapsto 1$. 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 $f_2 = e_{C(G_2)} : x \mapsto 1$. *Mutatis mutandis*, en spécialisant avec $x_2 = e_{G_2}$, on obtient $f_1 = e_{C(G_1)}$. Finalement $(f_1, f_2) = \left(e_{C(G_1)}, e_{C(G_2)}\right)$ qui est l'élément neutre du groupe produit $C(G_1) \times C(G_2)$.

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

Soit $f \in C(G)$. On définit

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

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

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

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

Conclusion

L'application T est un isomorphisme de $C(G_1) \times C(G_2)$ dans $C(G)$.

Exercice 23 (20.2)

Montrer que si f est une bijection de X sur Y, alors $F : \begin{array}{ccc} \mathfrak{S}(X) & \to & \mathfrak{S}(Y) \\ \sigma & \mapsto & f\sigma f^{-1} \end{array}$ est un isomorphisme.

Solution 23 (20.2)

Vu en cours!

Exercice 24 (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 24 (20.2)

1. On a

$$\phi(-1)^2 = \phi((-1)^2) = \phi(1) = 1$$

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

2. On a $\phi(\alpha) = i$ donc $\phi(\alpha^2) = i^2 = -1$. 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.

Exercice 25 (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

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

est un isomorphisme de groupes.

Solution 25 (20.2)

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

$$\begin{aligned} f(ab) &= f\left((x_1, y_1) \cdot (x_2, y_2)\right) = f\left(x_1x_2, y_1y_2\right) = x_1x_2y_1y_2 \\ \text{et} \quad f(a)f(b) &= f(x_1, y_1)f(x_2, y_2) = x_1y_1x_2y_2 \end{aligned}$$

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.

Anneaux, corps

Exercice 26 (20.3) *Études d'inversibilités dans un anneau*

Soit $(A, +, .)$ 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 $n \in \mathbb{N}^{\star}$ pour lequel $a^n = 0$.

Solution 26 (20.3)

Exercice 27 (20.3) *Éléments nilpotents*

Soit $(A, +, .)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe $n \in \mathbb{N}^\star$ 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 27 (20.3)

Exercice 28 (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 28 (20.3)

Exercice 29 (20.3)

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

$$E_a : \begin{array}{ccc} \mathscr{F}(X, \mathbb{R}) & \to & \mathbb{R} \\ f & \mapsto & f(a) \end{array}$$

est un morphisme d'anneaux.

Solution 29 (20.3)

Exercice 30 (20.4)

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

Solution 30 (20.4)

Exercice 31 (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 $n \in \mathbb{N}^\star$ vérifiant $x^n = 0_A$.
Montrer que N est un idéal de A.

Solution 31 (20.6)