Groupes et Morphismes de Groupes

1 Lois de composition interne

Exercice 1
Les propositions suivantes sont-elles vraies ou fausses ? Justifier votre réponse.

1. La soustraction est un LCI dans $\mathbb{Z}$.
2. 0 est l'élément neutre de la soustraction dans $\mathbb{Z}$.
3. La soustraction dans $\mathbb{Z}$ est associative.
4. 0 est l'élément neutre pour l'addition dans $\mathbb{N}$.
5. L'addition est associative dans $\mathbb{N}$.
6. L'addition est une LCI dans l'ensemble des nombres entiers pairs.
7. L'addition est une LCI dans l'ensemble des nombres entiers impairs.

Solution

1. Oui. $a-b \in \mathbb{Z}$
2. Non car pas neutre à gauche.
3. Non car $a-(b-c)=a-b+c=(a-b)-(-c)$.
4. Oui $a+0=0+a=a$
5. Oui.
6. Oui car la somme de deux entiers pairs est paire.
7. Non car la somme de deux entiers impairs est paire.

Exercice 2
Préciser pour chacune des LCI $\star$ définies ci-dessous si elle est associative, commutative, possède un élément neutre.

1. $\forall x, y \in \mathbb{R}^2, x \star y = \sqrt{x^2+y^2}$
2. $\forall x, y \in \mathbb{R}^2, x \star y = \ln\left(\mathrm{e}^x + \mathrm{e}^y\right)$

Solution

1. Elle est clairement commutative.
   Elle est associative :
   $(x \star y) \star z = \left(\sqrt{x^2+y^2}\right) \star z = \sqrt{\left(\sqrt{x^2+y^2}\right)^2 + z^2} = \sqrt{x^2+y^2+z^2} = \sqrt{x^2 + \left(\sqrt{y^2+z^2}\right)^2} = x \star (y \star z)$
   (cela provient du fait que $x^2+y^2 \geq 0$).
   Le seul élément neutre qui peut venir à l'esprit est 0, mais il n'est pas neutre pour les nombres négatifs : $x \star 0 = \sqrt{x^2} = |x| \neq x$.
   Si on n'a pas l'intuition, on peut le chercher : soit e un éventuel élément neutre et $x \in \mathbb{R}$. Alors
   $$x \star e = x \Leftrightarrow \sqrt{x^2+e^2} = x \Rightarrow x^2+e^2 = x^2 \Rightarrow e^2 = 0$$
   Le seul élément neutre possible est donc 0 , mais il n'en est pas un.
2. Elle est clairement commutative.
   Elle est associative :
   $(x \star y) \star z = \left(\ln\left(\mathrm{e}^x+\mathrm{e}^y\right)\right) \star z = \ln\left(\mathrm{e}^{\ln\left(\mathrm{e}^x+\mathrm{e}^y\right)} + \mathrm{e}^z\right) = \ln\left(\mathrm{e}^x + \mathrm{e}^{\bar{y}} + \mathrm{e}^z\right) = \ln\left(\mathrm{e}^x + \mathrm{e}^{\ln\left(\mathrm{e}^y+\mathrm{e}^z\right)}\right) = x \star (y \star z)$
   (les fonctions exponentielle et logarithme népérien sont bijections réciproques l'une de l'autre).
   Si y est l'élément neutre alors $x \star y = x \Leftrightarrow \ln\left(\mathrm{e}^x+\mathrm{e}^y\right) = x = \ln\left(\mathrm{e}^x\right) \Leftrightarrow \mathrm{e}^x + \mathrm{e}^y = \mathrm{e}^x \Leftrightarrow \mathrm{e}^y = 0$.
   $e^y = 0$ est faut pour tout $y \in \mathbb{R}$, donc il n'y a pas d'élément neutre.

Exercice 3
Pour tout $(x;y) \in [0;1]^2$, on pose :

$$x \star y = x + y - xy$$

1. Montrer que $([0;1];\star)$ est un magma commutatif et associatif.
2. Montrer que $([0;1];\star)$ possède un elément neutre.
3. Quels sont les éléments inversibles de $([0;1];\star)$?

Solution

1. Magma : Si $0 \leqslant x \leqslant 1$ et $0 \leqslant y \leqslant 1$, alors $0 \leqslant 1-x \leqslant 1$ et $0 \leqslant 1-y \leqslant 1$.
   D'où $0 \leqslant (1-x)(1-y) = 1-(x+\ y-xy) \leqslant 1$.
   Ainsi $-1 \leqslant (-(x+y-xy) \leqslant 0$ et $0 \leqslant x+y = xy \leqslant 1$.
   Commutatif : Évident.
   Associatif : $x\star(y\star z) = x+(y\star z)-x(y\star z) = x+(y+z-yz)-x(y+z-yz) = x+y+z-xy-xz-yz+xyz$, et $(x\star y)\star z = (x\star y)+z-(x\star y)z = (x+y-xy)+z-(x+y-xy)z = x+y+z-xy-xz-yz+xyz$.
2. Pour qu'un élément neutre e existe, il doit vérifier que pour tout $x \in [0;1], x\star e = x = x+e-xe$. D'où nécessairement, pour tout $x, e(x-1) = 0$. Donc $e = 0$. On vérifie aisément que 0 est bien un élément neutre.
3. Deux éléments x, y sont inverses l'un de l'autre si et seulement si $x \star y = 0 = x+y-xy$, c'est-â-dire $y(x-1) = x$.
   Si $x = 1$, ceci est impossible.
   Si $x \neq 1$, nous avons $y = \dfrac{x}{x-1} \leqslant 0$. Le seul elément inversible de $[0;1]$ est donc 0 .

Exercice 4
Soit E un ensemble muni d'une loi de composition interne associative $\star$ et d'un élément neutre.
Un élément de E est dit idempotent si $x \star x = x$.

1. Montrer que si x et y sont idempotents et commutent, alors $x \star y$ est idempotent.
2. Montrer que si x est idempotent et inversible alors x^{-1} est idempotent.

Solution

1. $(x\star y)\star(x\star y) = (x\star x)\star(y\star y)($ associative et commute). C'est égal à $x\star y$. Donc $(x\star y)$ est idempotent.
2. Nous savons que si x et y sont inversibles alors $x\star y$ aussi et l'inverse est $y^{-1}\star x^{-1}$, en prenant $y = x$ et en utilisant le fait que $x\star x = x$, nous avons $x^{-1} = (x\star x)^{-1} = x^{-1}\star x^{-1}$ et l'inverse est bien idempotent.
   On peut aussi observer que si $x\star x = x$ en composant à droite par x^{-1}, on a $x\star x\star x^{-1} = x\star x^{-1}$ donc $x = e$ donc si x et y sont idempotent et inversibles $x = y = e$ donc $x\star y$ est idempotent.

Exercice 5
Soit E un ensemble muni d'une loi de composition interne $\star$ associative.
Pour tout a de E, on définit les applications g_a et d_a de E dans E : $\forall x \in E, d_a(x) = x\star a$ et $g_a(x) = a\star x$.

1. Montrer que s'il existe a dans E tel que g_a et d_a soient surjectives, alors E possède un élément neutre pour la loi $\star$.
2. Montrer que si pour tout a de E, les applications g_a et d_a sont surjectives, alors tout élément de E possède un inverse pour la loi $\star$.

Solution

1. Puisque g_a et d_a sont surjective, il existe e et f tels que $e\star a = a = a\star f$.
   — Montrer que $e = f$. Toujours par surjectivité, il existe y et z tels que $y\star a = e$ et $a\star z = f$. Nous avons alors

   $$\begin{aligned} e\star f &= (y\star a)\star f = y\star(a\star f) = y\star a \\ &= e \\ e\star f &= e\star(a\star z) = (e\star a)\star z = a\star z \\ &= f \end{aligned}$$

   D'où l'égalité.

— Montrons maintenant que $\forall x \in E, x \star f = f \star x = x$.
Par surjectivité des applications, il existe y et z tels que $y \star a = x = a \star z$. Nous avons alors

$$x \star f = (y \star a) \star f = y \star (a \star f) = y \star a = x$$
$$f \star x = f \star (a \star z) = (f \star a) \star z = a \star z = x$$

Donc f est bien un élément neutre pour la loi $\star$.

2. Si les applications sont surjectives, pour tout a, alors nous venons de voir qu'il existe un élément neutre f.
Ainsi, pour tout a, par surjectivité, il existe a_d et a_g tels que $a_g \star a = f = a \star a_d$.
Il ne reste donc plus qu'à montrer que $a_d = a_g$:

$$a_g = a_g \star f = a_g \star (a \star a_d) = (a_g \star a) \star a_d = f \star a_d = a_d$$

---

2 Groupes, Sous-Groupes

Exercice 6
Sur $G = \mathbb{R}_+^* \times \mathbb{R}$, on definit l'opération $\star$ par :

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

Montrer que $(G; \star)$ est un groupe.
Solution

— Si $(x; x') \in \left(\mathbb{R}_+^+\right)^2$, alors $xx' \in \mathbb{R}_+$. Il est évident que pour tout $(x; y)$ et $(x'; y')$ de $G, xy' + y \in \mathbb{R}$. Donc la loi $\star$ est bien une loi de composition interne.
— Nous avons $(1; 0) \in G$ et pour tout $(x; y) \in G, (x; y) \star (1; 0) = (x \times 1; x \times 0 + y) = (x; y)$ et $(1; 0) \star (x; y) = (1 \times x; 1 \times y + 0) = (x; y)$. Donc $(1; 0)$ est un élément neutre pour $\star$.
— Soit $(x; y) \in G$, alors $(x'; y') = \left(\frac{1}{x}; -\frac{y}{x}\right) \in G(x > 0)$. Et nous avons $(x; y) \star (x'; y') = \left(\frac{x}{x}; \frac{-xy + yx}{x}\right) = (1; 0)$. De même $(x'; y') \star (x; y) = (1; 0)$. Donc tout élément de G est inversible.
— Enfin, pour tout $(x; y), (x'; y'), (x''; y'')$ de G nous avons $(x; y) \star ((x'; y') \star (x''; y'')) = (x; y) \star (x'y'; x'y'' + y') = (xx'x''; x'y'' + xy' + y)$ $((x; y) \star (x'; y')) \star (x''; y') = (x'; x' + y) \star (x''; y'') = (xx'x''; xx'y'' + xy' + y)$

Donc $(G; \star)$ est un groupe.

Exercice 7
Soit les quatre fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$:

$$f_1(x) = x \quad ; \quad f_2(x) = \frac{1}{x} \quad ; \quad f_3(x) = -x \quad ; \quad ; f_4(x) = -\frac{1}{x}$$

Montrer que $G = \{f_1; f_2; f_3; f_4\}$ muni de la loi $\circ$ est un groupe.
Solution
f_1 est l'identité, donc l'ensemble possède déjà un elément neutre. Ensuite, $f_2 \circ f_3 = f_3 \circ f_2 = f_4 \in G, f_2 \circ f_4 = f_4 \circ f_2 = f_3 \in G, f_3 \circ f_4 = f_4 \circ f_3 = f_2, f_2 \circ f_2 = f_1 = f_3 \circ f_3 = f_4 \circ f_4 \in G$.
Donc nous avons bien une lci et $(G; \circ)$ est bien un magma.
Nous venons de voir que tout elément était son propre inverse et nous savons déja que la loi $\circ$ est associative.
Donc $(G; \circ)$ est bien un groupe.
La loi est donc associative.
Donc $(G; \star)$ est un groupe.

Exercice 8
Quel est le plus petit sous-groupe de $(\mathbb{R}; +)$ (respectivement de $(\mathbb{R}^*; \times)$) contenant 1 ? Contenant 2 ?
Solution
Un sous-groupe de $(\mathbb{R}; +)$ contenant 1 doit nécessairement contenir l'élément neutre 0 , mais aussi $1 + 1 = 2$, puis 3 , etc, donc $\mathbb{N}$, mais aussi tous les opposés, done $\mathbb{Z}$. Or $\mathbb{Z}$ étant un sous-groupe, on a trouvé le plus petit.
Avec le même raisonnement, on montre que le plus petit sous-groupe contenant 2 est $2\mathbb{Z}$.
Pour les sous-groupes de $(\mathbb{R}^*; x)$, on doit contenir 1 et son inverse : 1 . Donc en fait le groupe réduit à l'élément neutre $\{1\}$ est le plus petit.
S'il contient 2, il contient aussí l'element neutre $1 = 2^0$, mais aussi $2 \times 2 = 4 = 2^2, 4 \times 2 = 2^3$, etc. C'est-ì-dire $\left\{2^k / k \in \mathbb{N}\right\}$.
Il doit aussi contenir les inverses de tous ces nombres. Finalement le plus petit sous-groupe de $(\mathbb{R}^*; x)$ est $\left\{2^k / k \in \mathbb{Z}\right\}$ (à condition d'avoir vérifié, bien évidemment, que c'est un sous-groupe).

Exercice 9
Les ensembles suivants, munis de l'addition des réels sont-ils des groupes ? Justifier.

1. $\{a\sqrt{2}/a \in \mathbb{N}\}$
2. $\{a\sqrt{2}+b\sqrt{3}/a, b \in \mathbb{Z}\}$
3. $\{a\sqrt{2}+b\sqrt{3}/a \in \mathbb{Z}, b \in \mathbb{N}\}$

Solution

1. L'élément neutre étant 0 , les éléments ne sont pas inversibles (car si $a \in \mathbb{N}^*, -a \notin \mathbb{N}$).
2. Si $x = a\sqrt{2}+b\sqrt{3}$ et $y = d'\sqrt{2}+b'\sqrt{3}$, alors $x+y = (a+a')\sqrt{2}+(b+b')\sqrt{3} \in G$. Nous avons donc stabilité par addition qui conserve sa propriété d'associativité. L'élément neutre est $0 = 0\sqrt{2}+0\sqrt{3}$, l'inverse est $-a\sqrt{2}-\ b\sqrt{3}$. C'est donc bien un groupe.
   Autre Méthode
   On peut aussi montrer que pour tout $a\sqrt{2}+b\sqrt{3}$ et $a'\sqrt{2}+b'\sqrt{3}$ avec $(a, b, a', b') \in \mathbb{R}^4$,
   $(a\sqrt{2}+b\sqrt{3})-(a'\sqrt{2}+b'\sqrt{3}) = (a-a')\sqrt{2}+(b-b')\sqrt{3}$.
   Or $(a-a') \in \mathbb{Z}$ et $(b-b') \in \mathbb{Z}$ donc il appartient bien à $\{a\sqrt{2}+b\sqrt{3}/a, b \in \mathbb{Z}\}$. Donc c'est un sous-groupe de $(\mathbb{R}, +)$
3. Cette fois ce n'est pas un groupe puisque l'inverse n'est pas dans l'ensemble (si $b \in \mathbb{N}$, alors $-b \notin \mathbb{N}$).

Exercice 10
Les ensembles suivants, munis de la multiplication des réelles sont-ils des groupes ? Justifier.

1. $\left\{1, -1, \frac{1}{2}, 2\right\}$
2. $\{a2^n, a \in \{-1, 1\}, n \in \mathbb{Z}\}$
3. $\left\{a+b\sqrt{2}, a, b \in \mathbb{Q}^*\right\}$

Solution

1. La loi n'est pas interne : tout produit entre deux éléments distincts de l'ensemble est bien dans l'ensemble, mais $2 \times 2 = 4$ n'est pas dans l'ensemble.
2. La loi est bien interne : $a_1 2^{m_1} a_2 2^{m_2} = (a_1 a_2) 2^{m_1+m_2}$ avec $a_1 a_2 = \pm 1$ et $n_1 + n_2 \in \mathbb{Z}$, elle est associative. L'élément neutre est $1 = 1 \times 2^0$. L'inverse de $a2^n$ est $a2^{-n}$ avec $-n \in \mathcal{Z}$. Donc c'est bien un groupe.
3. L'élément neutre n'est pas dans l'ensemble : $1 = 1 + 0 \times \sqrt{2}$ or on doit avoir $b \in Q^*$et $1 = a + b\sqrt{2} \Leftrightarrow \sqrt{2} = \frac{1-a}{b} \in \mathbb{Q}$($b$ est non nul), ce qui est absurde car $\sqrt{2}$ est irrationnel.

Exercice 11
Soit S un sous-groupe d'un groupe G et $a \in G$. Montrer que $a^{-1}Sa = \left\{c = a^{-1}ba/b \in S\right\}$ est un sous-groupe de G, dit conjugué de S.
Solution

— G étant un groupe, il est clair que $a^{-1}Sa \subset G$.
— Nous avons $1_G = a^{-1}1_G a \in a^{-1}Sa$.
— Si $d = a^{-1}ba$ et $e = a^{-1}ca$ sont deux éléments de $a^{-1}Sa$, alors

$$de^{-1} = a^{-1}ba\left(a^{-1}ca\right)^{-1} = a^{-1}ba\left(a^{-1}c^{-1}a\right) = a^{-1}\left(bc^{-1}\right)a \in a^{-1}Sa$$

Car S étant un sous-groupe, $bc^{-1} \in S$

Exercice 12
Soit G un groupe et $A \subset G$, non vide. On pose :

$$N(A) = \left\{x \in G/x^{-1}Ax = A\right\}$$

Montrer que $N(A)$ est un sous-groupe de G.
Solution
Version sûr de ce que l'on fait

— $-1^{-1}A1 = 1A1 = A$, donc $1 \in N(A)$.
— Soit x et y deux éléments de $N(A)$. Nous avons $(xy)^{-1} = y^{-1}x^{-1}$, d'où $(xy)^{-1}A(xy) = y^{-1}x^{-1}Axy = y^{-1}Ay = A$. Donc $xy \in N(A)$.
— Si $x \in N(A)$, alors $x^{-1}Ax = A$. En multipliant par x à gauche et x^{-1} à droite, nous avons $A = xAx^{-1} = \left(x^{-1}\right)^{-1}Ax^{-1}$. Donc $x^{-1} \in N(A)$.

Version on détaille

— Soit $y \in A$, montrons que $y \in 1^{-1}A1.y = 1^{-1}y1 \in 1^{-1}A1$.
Soit $y \in 1^{1-}A1$, montrons que $y \in A$. Il existe $x \in A$ tel que $y = 1^{-1}x1 = x \in A$.
Donc $A = 1^{-1}A1$ et $1 \in N(A)$.

— Soit $x \in N(A)$. Montrons que $xAx^{-1} = A$.
Soit $z \in A$. Puisque $A = x^{-1}Ax$, il existe $y \in A$ tel que $z = x^{-1}yx$. D'où $z = xyx^{-1} \in xAx^{-1}$.
Soit $z \in xAx^{-1}$. Il existe $y \in A$ tel que $z = xyx^{-1}$. Or $A = x^{-1}Ax$, donc il existe $t \in A$ tel que $y = x^{-1}tx$.
Ainsi, $z = xx^{-1}txx^{-1} = t =\in A$.
Donc $A = xAx^{-1}$ et $x^{-1} \in N(A)$.

— Soit x et y deux éléments de $N(A)$. Nous avons $x^{-1}Ax = A = y^{-1}Ay$. Montrons que $(xy)^{-1}A(xy) = A$.
Soit $z \in (xy)^{-1}$ Axy.
Il existe $t \in A$ tel que $z = (xy)^{-1}t(xy) = y^{-1}x^{-1}txy$.
Or $A = x^{-1}Ax$, donc $x^{-1}tx \in x^{-1}Ax = A$.
De même, un posant $u = x^{-1}tx \in A$, nous avons $y^{-1}uy \in y^{-1}Ay = A$. donc finalement $z \in A$.
Soit $z \in A$. Puisque $A = y^{-1}Ay$, il existe $t \in A$ tel que $z = y^{-1}ty$.
Mais de même, il existe $u \in A$ tel que $t = x^{-1}ux$. D'où $z = y^{-1}x^{-1}uxy = (xy)^{-1}u(xy)$.
Donc $z \in (xy)^{-1}A(xy)$.
Donc $A = (xy)^{-1}A(xy)$ et $xy \in N(A)$.

Donc $N(A)$ est bien un sous-groupe de G.

Exercice 13

Soit E un ensemble, $(G;-)$ un groupe et f une bijection de E vers F. Pour $(x;y) \in E^2$, on pose $xy = f^{-1}(f(x)f(y))$.
Montrer que la loi de composition interne ainsi définie sur E munit E d'une structure de groupe.

Solution

— Soit x, y, z trois éléments de E. Alors $x(yz) = xf^{-1}(f(y)f(z)) = f^{-1}\left(f(x)f \circ f^{-1}(f(y)f(z))\right) = f^{-1}(f(x)f(y)f(z)) = f^{-1}\left(f \circ f^{-1}(f(x)f(y))f(z)\right) = f^{-1}(f(x)f(y))z = (xy)z$. La loi est associative.

— Si e est un élément neutre alors nécessairement, $x = xe = f-1(f(x)f(e))$. En composant par f, nous avons $f(x) = f(x)f(e)$. Or $f(x) \in G$, groupe, donc est inversible et $1_G = f(e)$. Par bijectivité de f, nous avons $e = f^{-1}(1_G)$. On vérifie alors aisément que $e = f^{-1}(1_G)$ est un élément neutre pour la loi (à droite ET à gauche).

— Soit $x \in E$. Posons alors $x^{-1} = f^{-1}\left(f(x)^{-1}\right)$. Ainsi $xx^{-1} = f^{-1}\left(f(x)f\left(x^{-1}\right)\right) = f^{-1}\left(f(x)f(x)^{-1}\right) = f^{-1}(1_G) =$ e. De même pour $x^{-1}x$. Ainsi tout élément de E est inversible.

Donc E est bien muni d'une structure de groupe.

Exercice 14

Soit $(E;\star)$ et $(F;\cdot)$ deux groupes. On munit l'ensemble produit $E \times F$ de la loi de composition $\otimes$ définie par :

$$\forall (x;y), (x';y') \in E \times F, (x;y) \otimes (x';y') = (x \star x'; y \cdot y')$$

1. Montrer que $(E \times F; \otimes)$ est un groupe.
2. Soit E' un sous-groupe de E et F' un sous-groupe de F. Montrer que $E' \times F'$ est un sous-groupe de $E \times F$, muni de la loi $\otimes$.

Solution

1. C'est la loi produit, donc la démonstration est faite dans le cours.
2. Nous avons bien $E' \times F' \subset E \times F$. Puisque E' et F' sont des sous-groupes, ils contiennent respectivement les neutres de E et F, donc $E' \times F'$ contient le neutre de $E \times F$. Enfin, par construction, si $(x;y) \in E' \times F'$ et $(x';y') \in E' \times F'$, alors $(x;y) \otimes \left(x'^{-1}; y'^{-1}\right) = \left(x \star x'^{-1}; y \cdot y'^{-1}\right) \in E' \times F'$ car E' et F' sont des sous-groupes. Plus simplement, d'après la question précédente, $E' \times F'$ est un groupe inclu dans $E \times F$, donc c'est un sousgroupe.

Exercice 15

Soit $G =]-1, 1[$ muni de la loi $\star$ définie par : $x \star y = \dfrac{x+y}{1+xy}$. Montrer que $(G, \star)$ est un groupe abélien.

Solution

— La loi $\star$ est clairement commutative.

— LCI Pour tout $y \in G$, la fonction $f : x \mapsto x \star y$ est strictement croissante $\left(f'(x) = \dfrac{1-y^2}{(1+xy)^2} > 0\right)$ et $f(-1) = -1$ et $f(1) = 1$, donc pour tout $x \in G, f(x) \in G$. La loi est donc bien une lci.
Autre méthode : nous avons $1+xy > 0$, donc $x \star y \in]-1;1[\Leftrightarrow -1-xy < x+y < 1+xy \Leftrightarrow 0 < 1+x+xy$ et $1+ xy - x - y > 0$. Or $(1+x) > 0$ et $(1+y) > 0$, donc $(1+x)(1+y) > 0$, d'où $1+x+y+xy > 0$.
De même avec $(1-) > 0$ et $1-y > 0$.

— Associative
Soit $x, y, z \in G$,

$$x \star (y \star z) = x \star \left(\frac{y+z}{1+yz}\right) = \frac{x + \frac{y+z}{1+yz}}{1 + x\left(\frac{y+z}{1+yz}\right)}$$
$$= \frac{x+y+z+xyz}{1+yz+xy+xz}$$

Cette dernière expression est invariante par permutation sur x, y et z, donc $x \star (y \star z) = z \star (y \star x)$. Et par commutativité, cette dernière expression est égale à $(x \star y) \star z$

— Élément neutre
0 est clairement l'élément neutre : $x \star 0 = 0 \star x = \dfrac{x}{1} = x$.

— Inversible
L'inverse de x est alors tout simplement $-x \in G : x \star (-x) = \dfrac{x-x}{1-x^2} = 0$.

Exercice 16
Soit G un groupe et H et K deux sous-groupes de G.

1. Montrer que $H \cap K$ est un sous-groupe de G.
2. Montrer que ($H \cup K$ est un sous-groupe de G) $\Longleftrightarrow$ ($H \subset K$ ou $K \subset H$).

Solution

1. Si H et K sont des sous-groupes, ils contiennent l'élément neutre, donc $H \cap K$ aussi. Si x et y sont dans l'intersection, alors x et y sont dans K, donc $xy^{-1} \in K$; de même $xy^{-1} \in H$. Donc $xy^{-1} \in H \cap K$ et nous avons bien la stabilité par produit et passage à l'inverse.
2. La réciproque est claire : si l'un des deux contient l'autre, l'union est égale à l'autre, donc est un sous-groupe. Démontrons le sens direct par contraposée. Si H n'est pas inclus dans K et K pas inclus dans H, alors $H \cap \bar{K} \neq \emptyset$ et $\bar{H} \cap K \neq \emptyset$. Prenons $x \in H \cap \bar{K}$ et $y \in \bar{H} \cap K$. Ces deux éléments sont dans $H \cup K$. Puisque $x \in H$ et que H est un sous-groupe, alors x^{-1} est aussi dans H. Supposons que $xy \in H$, alors $y = x^{-1}xy \in H$, ce qui est impossible, donc $xy \notin H$. De même $xy \notin K$. Finalement $xy \notin H \cup K$ et $H \cup K$ n'est pas stable pour la loi du groupe, donc n'est pas un sous-groupe de G.

Exercice 17

1. Soit $n \in \mathbb{N}$. Montrer que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
2. Montrer que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$.
3. Soit $a, b \in \mathbb{Z}$. On note $a\mathbb{Z} + b\mathbb{Z} = \{au + bv; u, v \in \mathbb{Z}\}$. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
   En particulier, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ pour un certain $d \in \mathbb{Z}$. Montrer alors que $d = a \wedge b$.

Solution
L'ensemble $\mathbb{Z}$ est bien évidemment muni de sa loi $+$ pour devenir un groupe. On rappelle que $n\mathbb{Z} = \{kn/k \in \mathbb{Z}\}$.

1. L'élément neutre $0 = 0 \times n$ est dans $n\mathbb{Z}$. Si $x = kn$ et $y = k'n$ sont dans $n\mathbb{Z}$, alors $x - y = (k - k')\,n$ est aussi dans $n\mathbb{Z}$.
2. Soit G un sous groupe de $\mathbb{Z}$. Il contient donc $0.\mathrm{Si}G = \{0\}$, alors $G = 0\mathbb{Z}$. Sinon, il contient un élément $x \neq 0$. Mais puisque c'est un groupe, il contient aussi $-x$. Ainsi $G \cap \mathbb{N}^*$ est une partie de $\mathbb{N}$ non vide et contient donc un plus petit élément que l'on note n. Montrons alors que $G = n\mathbb{Z}$ par double inclusion :
   — Soit $x \in G$. Si $x = 0$, alors $x \in n\mathbb{Z}$. Sinon, comme précédemment, $|x| \in G$. De plus, en effectuant la division euclidienne de $|x|$ par n, nous avons $|x| = nq + r$ avec $0 \leq r < n$. Or $|x| \in G$ et $n \in G$, d'où par stabilité, $nq \in G$ et $r = x - nq \in G$. Or n était le plus petit élément strictement positif de G. Ainsi $r = 0$ et $x = nq \in n\mathbb{Z}$.
   — Soit $x = nk \in n\mathbb{Z}$. Alors par stabilité, puisque $n \in G, nk$ et donc x est dans G.
   Nous avons donc montré que tout sous groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$. Or nous avons montré à la question précédente que tous les ensembles $n\mathbb{Z}$ étaient des sous-groupes de $\mathbb{Z}$. Finalement, les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$.
3. Nous avons $0 = a \times 0 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$. Soit $x = ak_1 + bk_2 \in a\mathbb{Z} + b\mathbb{Z}$ et $y = ak_1' + bk_2' \in a\mathbb{Z} + b\mathbb{Z}$. Alors $x - y = a\,(k_1 - k_1') + b\,(k_2 - k_2') \in a\mathbb{Z} + b\mathbb{Z}$. Donc $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$, donc s'écrit $d\mathbb{Z}$. On en déduit qu'il existe k et k' tels que $ak + bk' = d$ (car $d \in d\mathbb{Z}$). Donc $a \wedge b \mid d$. De plus, d'après la relation de Bézout, il existe u et v tels que $au + bv = a \wedge b$, donc $a \wedge b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Donc il existe $k \in \mathbb{Z}$ tel que $dk = a \wedge b$. Donc $d \mid a \wedge b$. Finalement $d = a \wedge b$.

---

document
Exercice 18

Soit H un groupe abélien. Un élément $x \in H$ est dit d'ordre fini lorsqu'il existe $n \in \mathbb{N}$ tel que la somme $x + \cdots + x$ (n fois) soit égale à 0 . Montrer que l'ensemble des éléments d'ordre fini est un sous-groupe abélien de H. Notons G l'ensemble des éléments d'ordre fini de H.

Solution

— Inclusion : Nous avons clairement $G \subset H$.
— Élément neutre : Nous avons $0 = 0$, donc $0 \in G$.
— Stabilité par passage à l'inverse : Soit $x \in G$. Il existe n tel que $x + \cdots + x = 0(n$ fois $)$. D'où $(-x) + \cdots + (-x) = -(x + \cdots + x) = -0 = 0$.
— Stabilité par somme : Soit x et y dans G. Il existe n_x et n_y tels que $x + \cdots + x = 0$ (n_x fois) et $y + \cdots + y = 0$ (n_y fois). Alors, par commutativité de $+(H$ est un groupe abélien), nous avons $(x + y)$ $y \in G$.

Donc $x + y \in G$. G est un sous-groupe de H et comme H est commutatif, G aussi.

Exercice 19

Décrire tous les homomorphismes de groupes de $\mathbb{Z}$ dans $\mathbb{Z}$.
Déterminer ceux qui sont injectifs et ceux qui sont surjectifs.

Solution

Soit $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ un morphisme de groupe. Comme tout morphisme f vérifie $f(0) = 0$. Notons $a = f(1)$. Alors

$$f(2) = f(1 + 1) = f(1) + f(1) = a + a = 2.a.$$

De même, pour $n \geq 0$:

$$f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = n \cdot f(1) = n \cdot a.$$

Enfin comme

$$0 = f(0) = f(1 + (-1)) = f(1) + f(-1) = a + f(-1),$$

alors $f(-1) = -a$ et pour tout $n \in \mathbb{Z}$:

$$f(n) = \text{ n.a.}$$

Donc tous les morphismes sont de la forme $n \mapsto n.a$, avec $a \in \mathbb{Z}$. Un morphisme $n \mapsto n.a$ est injectif si et seulement si $a \neq 0$, et surjectif si et seulement si $a = \pm 1$.

Exercice 20

1. Soit G un groupe, pour tout $h \in G$, on définit l'application

$$\phi_h : \quad \begin{aligned} G &\to G \\ g &\mapsto hgh^{-1} \end{aligned}$$

   (a) Montrer que, pour tout $h \in G$, l'application ϕ_h est un automorphisme de groupe ($\phi_h \in \operatorname{Aut}(G)$).
   (b) Considérons l'application :

$$\phi : G \mapsto \phi_h$$

   Montrer que ϕ est un morphisme de groupe.
   (c) On suppose que $(G, \cdot)$ est commutatif. Déterminer le noyau de ϕ.

Solution

1. Il faut montrer que ϕ_h est un morphisme de G dans G, bijectif.
   $\forall g \in G, \phi_h(e) = heh^{-1} = e$ donc le neutre a pour image le neutre.
   $\forall (g, g') \in G^2, \phi_h(gg') = hgg'h^{-1} = hgh^{-1}hg'h^{-1} = \phi_h(g)\phi_h(g')$ donc il s'agit bien d'un morphisme.
   On remarque que $\phi_{h^{-1}} \circ \phi_h(g) = \phi_{h^{-1}}(hgh^{-1}) = h^{-1}hgh^{-1}h = g$
   Donc phi_h admet une réciproque $\phi_{h^{-1}}$ donc ϕ_h est bijective.
2. On a $\phi_{hh'}(g) = hh'gh^{-1}h'^{-1} = \phi_h \circ \phi_{h'}(g)$ et $\phi_e = Id$ donc on a bien un morphisme.
3. Si G est commutatif, $\phi_h = Id$ donc le noyau est G.

Exercice 21

On note $\mathbb{C}^*$ l'ensemble des nombres complexes non nuls.

1. Montrer que l'application
   $$\begin{array}{ccc} f & \mathbb{C}^* & \to & \mathbb{R}^* \\ & z & \mapsto & |z| \end{array}$$
   est un morphisme de groupes. On note U le noyau du morphisme ci-dessus.

2. Construire un isomorphisme de groupes de $\mathbb{C}^*$ vers le groupe produit $\mathbb{R}^* \times U$.

Solution

1. Soit $(z,z') \in \mathbb{C}^{*2}, f(\frac{z}{z'}) = \left|\frac{z}{z'}\right| = \frac{|z|}{|z'|} = \frac{f(z)}{f(z')}$
2. On pose $\begin{array}{cccc} \psi & \mathbb{C}^* & \to & \mathbb{R}^* \times U \\ & z & \mapsto & (|z|, e^{iarg(z)} \end{array}$

   On démontre aisément que c'est un isomorphisme

Exercice 22

Soit $(G,\star)$ un groupe, pour tout $h \in G$, on définit l'application

$$\begin{array}{ll} \phi_h : & G \to G \\ & g \mapsto \quad h \star g \star h^{-1} \end{array}$$

1. Montrer que, pour tout $h \in G$, l'application ϕ_h est un automorphisme de groupe ($\phi_h \in Aut(G)$).
2. Déterminer son inverse ϕ_h^{-1}.
3. Montrer que $\phi_h \circ \phi_k = \phi_{h\star k}$, pour tout $h, k \in G$.
4. Considerons l'application :

$$\begin{array}{ll} \phi : & G \to \mathrm{Aut}(G) \\ & g \mapsto \phi_g \end{array}$$

   Montrer que ϕ est un morphisme de groupe.
5. On suppose que $(G,\cdot)$ est commutatif. Déterminer le noyau de ϕ.

Solution

1. • Bijection ?

   Soit $g' \in G$, on résout pour $g \in G$, $\begin{array}{l} g' = \phi_h(g) \Leftrightarrow h \star g \star h^{-1} = g' \\ \Leftrightarrow h^{-1} \star h \star g \star h^{-1} \star h = h^{-1} \star g' \star h \\ \Leftrightarrow g = h^{-1} \star g' \star h \end{array}$

   On a donc obtenu un antécédent unique de g' par ϕ_h. Donc il s'agit bien d'une bijection.

   • Morphisme ?

   $\forall (g,g') \in G^2,\ \phi_h(g \star g') = h \star g \star g' \star h^{-1}$
   $= h \star g \star \left(h^{-1} \star h\right) \star g' \star h^{-1} = \left(h \star g \star h^{-1}\right) \star \left(h \star g' \star h^{-1}\right) = \ \phi_h(g)\ \star \phi_h(g')$

   Il s'agit bien d'un morhpisme de groupe.

   • On aurait pu montrer séparément l'injectivité :

   Si e est le neutre, on a $\begin{array}{l} \phi_h(g) = e \Leftrightarrow\ h \star g \star h^{-1} = e \Leftrightarrow\ h^{-1} \star h \star g \star h^{-1} \star h = h^{-1} \star e \star h \\ \Leftrightarrow\ g = e \end{array}$

   Donc $ker(\phi) = \{e\}$
2. On résout d'abord la question 3)

   $\forall (h,h') \in G,\ \forall g \in G,\ \phi_{h\star h'}(g) = h \star h' \star g \star (h \star h')^{-1} = h \star h' \star g \star h'^{-1} \star h^{-1}$
   $= h \star \left(h' \star g \star h'^{-1}\right) \star h^{-1} = \phi_h(\phi_{h'}(g)) = (\phi_h \circ \phi_{h'})(g)$

   donc $\phi_{h\star h'} = \phi_h \circ \phi_{h'}$

   Donc ϕ est un morphisme de groupe.

   on en déduit la question 2 : D'après la relation précédente, $\phi_h^{-1} = \phi_{h^{-1}}$ car $\phi_{h\star h^{-1}} = \phi_e = Id$ évidemment.
3.
5. Si G est commutatif, $\forall (h,g) \in G^2,\ \phi_h(g) = h \star g \star h^{-1} = g \star h \star h^{-1} = g$

   Donc toute application ϕ_h est l'identité donc $Ker(\phi) = G$

Exercice 23

Soit G un groupe. Montrer que l'application $g \mapsto g^{-1}$ est un morphisme de groupes $G \to G$, si et seulement si, G est abélien.

Solution

On pose $\phi : \begin{array}{ccc} G & \to & G \\ g & \mapsto & g^{-1} \end{array}$

Si G est abélien alors si alors

$\forall (g,g') \in G^2, \phi(gg') = (gg')^{-1} = g'^{-1}g^{-1} = g^{-1}g'^{-1} = \phi(g)\phi(g')$ donc ϕ est un morphisme.

Si ϕ est un morphisme : $\forall (g,g') \in G^2, (gg')^{-1} = g^{-1}g'^{-1}$

Si on prend l'inverse : $gg' = (g^{-1}g'^{-1})^{-1} = (g'^{-1})^{-1}(g^{-1})^{-1} = g'g$ donc G est abélien.

Exercice 24

Les applications f_1 et f_2, sont-elles des morphismes de groupes ? Si c'est le cas, déterminer le noyau et l'image.

$$f_1 : \left(\mathbb{Z}^2, +\right) \to (\mathbb{Z}, +), (a,b) \mapsto a - b$$
$$f_2 : \left(\mathbb{Z}^3, +\right) \to \left(\mathbb{Q}, +\right), (a,b,c) \mapsto 2^a 3^b 5^c$$

Solution

1. Soit $((a,b),(c,d)) \in \left(\mathbb{Z}^2\right)^2$ alors $f_1((a,b)+(c,d)) = f_1((a+c, b+d)) = (a+c)-(b+d) = (a-b)+(c-d) = f_1((a,b)) - f_1((c,d))$.
   C'est donc un morphisme.
   L'image est $\mathbb{Z}$ car il est surjectif ($f_1(n,0) = n$)
   Le noyau est l'ensemble des couples (a,b) tels que $a = b$ donc il est isomorphe à $\mathbb{Z}$.
2. Soit $((a,b,c),(d,e,f)) \in \left(\mathbb{Z}^3\right)^2$ alors $f_1((a,b,c)+(d,e,f)) = f_1((a+d, b+e, c+f)) = 2^{a+d}3^{b+e}5^{c+f} = 2^a 3^b 5^c 2^d 3^e 5^f = f_2(a,b,c)f_2(d,e,f)$. Donc il s'agit d'un morphisme.
   L'image est l'ensemble des rationnels donc la décomposition en fraction irréductible contient uniquement des 2, 3 et 5 lors de la décomposition.
   Le noyau est l'antécédent de 1 donc (0,0,0). Donc le morphisme est injectif.

Exercice 25

Soit a un élément d'un groupe $(G, \star)$.

1. Montrer que l'application $f : k \mapsto a^k$ définit un morphisme du groupe $(\mathbb{Z}, +)$ vers $(G, \star)$.
2. Déterminer l'image et le noyau de f.

Solution

1. $\forall (m,n) \in \mathbb{Z}^2, f(m+n) = a^{m+n} = a^m a^n = f(m)f(n)$ donc f est un morphisme.
2. L'image est le sous-groupe généré par a.
   Le noyau est un sous-groupe de $\mathbb{Z}$ donc de type $n\mathbb{Z}$

Exercice 26

Soient $n \in \mathbb{N}^*$ et $f : \mathbb{R}^* \to \mathbb{R}^*$ définie par $f(x) = x^n$.

1. Montrer que f est un morphisme du groupe $(\mathbb{R}^*, \times)$ dans lui même.
2. Déterminer l'image et le noyau de f.

Solution

1. $\forall (x,y) \in \mathbb{R}_*^2, f(xy) = (xy)^n = x^n y^n = f(x)f(y)$ donc f est un morphisme de groupe.
2. Soit $z \in \mathbb{R}_+^*$, alors $z = x^n \Leftrightarrow \ln z = n \ln x$
   donc $x = e^{\frac{\ln z}{n}} = z^{\frac{1}{n}}$ est un antécédent de z donc tout élément de $\mathbb{R}_+^*$, admet un antécédent.
   Si n est est pair, $\forall x \in \mathbb{R}^*, x^n \geqslant 0$, donc l'image par le morphisme est $\mathbb{R}_+^*$.
   Le noyau est $\{-1; 1\}$
   Si n est impair, soit $z \in \mathbb{R}_-^*$, alors $-(-z)^{\frac{1}{n}}$ est un antécédent de z donc l'image par le morphisme est $\mathbb{R}^*$.
   Le noyau est $\{1\}$
