Groupes 1

Exercices axés sur le calcul

Exercice 1 *Image par un morphisme de l'itéré d'un élément*

Soit G et G' deux groupes notés additivement. Pour $n \in \mathbb{Z}$ et $x \in G$, on désigne par nx l'itéré de x d'ordre n dans le groupe G.
Soit f un morphisme de G dans G'.

1) Montrer que pour $x \in G$ et tout $n \in \mathbb{N}$, on a $f(nx) = nf(x)$.
2) Montrer l'égalité précédente est encore vraie quand $n \in \mathbb{Z}$.
3) Que deviennent ces égalités en notations multiplicatives ?

Exercice 2 *Classique*

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ vers $(\mathbb{R}, +)$.
Montrer que pour tout $r \in \mathbb{Q}$, $f(r) = rf(1)$.

Exercice 3

Soit $\sigma \in \mathfrak{S}_9$ définie par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$.

1) Décomposer σ en produit de cycles à supports disjoints.
2) Déterminer la signature et l'ordre de σ.

Exercice 4

On rappelle que pour tout a réel, $b = \sqrt[3]{a}$ désigne l'unique réel b tel que $a = b^3$.
On munit $\mathbb{R}$ de la loi $\star$ définie par :

$$x \star y = \sqrt[3]{x^3 + y^3}.$$

1) Montrer que $(\mathbb{R}, \star)$ est un groupe abélien.
2) Montrer qu'il est isomorphe à $(\mathbb{R}, +)$.

Exercice 5 *Automorphismes intérieurs*

Soit $(G,*)$ un groupe. Pour $a \in G$, on note a^{-1} son symétrique pour la loi $*$ et τ_a l'application de G vers G définie par $x \mapsto a * x * a^{-1}$.

1) Montrer que τ_a est un automorphisme du groupe $(G,*)$ (c'est-à-dire un isomorphisme du groupe dans lui-même).

2) Vérifier que :

$$\forall a,b \in G, \quad \tau_a \circ \tau_b = \tau_{a*b}$$

3) En déduire que $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

D'après Mines-Télécom

Exercice 6 *Centre d'un groupe*

1) Soit $(G,*)$ un groupe. On note :

$$Z(G) = \{x \in G \mid \forall y \in G,\ x \cdot y = y \cdot x\}.$$

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

2) Montrer que l'ensemble des matrices de la forme $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ avec x, y et $z \in \mathbb{R}$ est un groupe pour le produit matriciel. Trouver le centre de ce groupe.

Exercice 7

On considère l'intervalle $I = [0,1[$. Pour x et y dans I, on pose

$$x \star y = x + y - \lfloor x + y \rfloor$$

1) Montrer que $(I,\star)$ est un groupe abélien.

2) Résoudre l'équation $x \star x = 0$ d'inconnue $x \in I$.
En déduire qu'il existe un unique $d \in I$ qui soit d'ordre 2 dans $(I,\star)$.

3) Pour $n \in \mathbb{N}^*$, préciser, s'il en existe, les éléments d'ordre n de I.

Exercices axés sur le raisonnement

Exercice 8 *Classique*

Montrer que la réunion de deux sous-groupes est un sous-groupe si et seulement si l'un des deux sous-groupes est inclus dans l'autre.

Exercice 9

Soit $(G,*)$ un groupe d'élément neutre e et f l'application de G dans lui-même qui associe à tout x son symétrique x^{-1} pour la loi $*$.
Montrer que f est un automorphisme du groupe $(G,*)$si, et seulement si, le groupe $(G,*)$ est commutatif.

Exercice 10

On note $\mathrm{GL}_2(\mathbb{Z})$ l'ensemble des matrices carrées de taille 2 à coefficients dans $\mathbb{Z}$ dont le déterminant vaut 1 ou -1.

1) Soit M une matrice carrée d'ordre 2 à coefficients entiers et inversible.
   Montrer que si M^{-1} est à coefficients entiers alors $\det(M) = \pm 1$.
2) Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est un groupe pour la multiplication.
3) On pose $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.
   Calculer l'ordre de A, de B et de AB. Que peut-on en conclure ?

Exercice 11

Soit H et K deux groupes notés multiplicativement.

1) Soit h un élément de H et k un élément de K. On suppose ces éléments d'ordres finis.
   On note p l'ordre de h, q celui de k et $r = \mathrm{ppcm}(p,q)$.
   Montrer que (h,k) est un élément d'ordre r dans le groupe $H \times K$.
2) On suppose que H et K sont des groupes cycliques.
   Montrer que le groupe produit $H \times K$ est cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 12

Soit G un sous-groupe fini de $(\mathbb{C}^*,\times)$.

1) Montrer que $G \subset \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
2) Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $G = \mathbb{U}_p$ (ensemble des racines p-ièmes de 1).

Exercice 13 ⋆⋆ *Groupes des éléments d'ordre fini de $\mathbb{C}^*$*

On note $\mathbb{U}_\infty = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^*,\ z^n = 1\}$.

1) Montrer que $\mathbb{U}_\infty$ est infini.
2) Montrer $\mathbb{U}_\infty$ est un sous-groupe de $\left(\mathbb{C}^*,\times\right)$.
3) Montrer que $\mathbb{U}_\infty$ n'est pas engendré par une partie finie.

Exercice 14 ★★

Soit G un groupe fini noté multiplicativement, H et K deux sous-groupes de G.
On note $f\ :\ H \times K \to G, (h,k) \mapsto hk$ et :

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

1) Quelle est l'image de f ? Déterminer le nombre d'antécédents par f que possède un élément de cette image.

2) En déduire que :

$$\mathrm{Card}(HK)\mathrm{Card}(H \cap K) = \mathrm{Card}(H)\mathrm{Card}(K)$$

Exercice 15 *Sous-groupe d'un groupe cyclique*

On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique : on introduit un groupe cyclique $(G,*)$, a un générateur de G et H un sous-groupe de $(G,*)$.

1) Justifier l'existence d'un plus petit entier naturel non nul tel que $a^n \in H$.

2) Établir qu'alors H est le groupe engendré par a^n.

Exercice 16

Soit $n \in \mathbb{N} \setminus \{0,1\}$ et $(G,*)$ un groupe de cardinal $2n$.
Soit A et B deux sous-groupes de G de cardinal n tels que $A \cap B = \{e\}$.

1) Montrer qu'il existe $c \in G$ tel que $A \cup B \cup \{c\} = G$.

2) Montrer que

$$\forall a \in A \setminus \{e\}, \forall b \in B \setminus \{e\}, \quad a * b = c$$

En déduire $n = 2$.

Exercice 17 ★

1) Soit f un homomorphisme de groupes de G dans G' et x un élément de G d'ordre fini p.
Que peut-on dire de l'ordre de $f(x)$ dans G' ?

2) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

3) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 18 ★

Montrer qu'il existe un multiple de 23 dont l'écriture décimale ne comporte que des 1.

D'après TPE Mines-Ponts

Exercices avec questions ouvertes

Exercice 19 *Caractérisation des groupes finis par le nombre de sous-groupes*

Soit $(G, *)$ un groupe.

1) Justifier que si G est fini alors G possède un nombre fini de sous-groupes.

2) Réciproquement, on suppose que G possède un nombre fini de sous-groupes.
Tous les éléments de G sont-ils d'ordre fini ?
L'ensemble G est-il fini ?

Exercice 20

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 21

Soit n un entier naturel supérieur à 4 et $\sigma \in \mathfrak{S}_n$.
Existe-t-il un lien entre la parité de l'ordre de σ et sa signature ?

Exercice 22 *Classique*

Quels sont les morphismes de groupes continus de $(\mathbb{R}, +, \times)$ dans lui-même ?
Indication : Utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.

Corrections

Exercices axés sur le calcul

Exercice 1

On raisonne par récurrence.

1) Soit $x \in G$. Pour $n \in \mathbb{N}$, on a appelle $\mathcal{P}_n$ la proposition « $f(nx) = nf(x)$ ».
Par définition, $0x = 0_G$ et $0f(x) = 0_{G'}$. Par ailleurs $f(0_G) = 0_{G'}$ car f est un morphisme.
Donc $\mathcal{P}_0$ est vraie.
Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie. On a alors :

$$\begin{aligned} f\big((n+1)x\big) &= f(nx + x) && \text{car } f \text{ est un morphisme} \\ &= f(nx) + f(x) && \text{d'après } \mathcal{P}_n \\ &= nf(x) + f(x) && \text{par définition} \\ &= (n+1)f(x) \end{aligned}$$

ce qui montre que $\mathcal{P}_{n+1}$ est vraie.
On a montré par récurrence que

$$\forall n \in \mathbb{N}, \quad f(nx) = nf(x)$$

2) Soit $x \in G$ et $n \in \mathbb{Z} \setminus \mathbb{N}$. Puisque f est un morphisme on a $f(nx) = -f(-nx)$.
Or $-nx = (-n)x$ et $-n \in \mathbb{N}$ donc $f(-nx) = (-n)f(n)$.
Finalement $f(nx) = -(-n)f(x) = nf(x)$.
On a montré

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f(nx) = nf(x).$$

3) En notations multiplicatives, on obtient :

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f\left(x^n\right) = \left(f(x)\right)^n.$$

Exercice 2

Soit $r \in \mathbb{Q}$. On choisit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $r = p/q$.
En utilisant les images des itérés d'un élément par un morphisme (voir exercice 1) on a :

$$\begin{aligned} qf(r) &= qf\left(\tfrac{p}{q}\right) && f(qx) = qf(x) \text{ car } f \text{ est un morphisme} \\ &= f\left(q\tfrac{p}{q}\right) && q\tfrac{p}{q} = p = p \cdot 1 \\ &= pf(1) \end{aligned}$$

En divisant l'égalité par q, on obtient $f(r) = rf(1)$.

Exercice 3

1) En étudiant les images successives de chacun des éléments de $[\![1, 9]\!]$, on obtient :
$\sigma(1) = 3, \sigma(3) = 8, \sigma(8) = 1$. De même $\sigma(2) = 7, \sigma(7) = 2$.
Et $\sigma(4) = 9, \sigma(9) = 6, \sigma(6) = 5, \sigma(5) = 4$.
Donc

$$\sigma = \langle 1, 3, 8\rangle \circ \langle 2, 7\rangle \circ \langle 4, 9, 5, 7\rangle$$

2) • ***Signature***

La transposition $\tau = \langle 2, 7\rangle$ est de signature -1. Le cycle $c_3 = \langle 1, 3, 8\rangle$ est de signature $+1$ et le cycle $c_4 = \langle 4, 9, 5, 7\rangle$ est de signature -1.
La signature étant un homomorphisme de groupe, on a

$$\varepsilon(\sigma) = \varepsilon(\tau)\varepsilon(c_3)\varepsilon(c_4) = (-1) \cdot 1 \cdot (-1) = 1.$$

• ***Ordre***

Deux cycles de supports disjoints commutant pour la composition, on a pour tout $p \in \mathbb{N}$:

$$\sigma^p = \tau^p \circ c_3^p \circ c_4^p$$

La transposition $\tau = \langle 2, 7\rangle$ est d'ordre 2. Le cycle $c_3 = \langle 1, 3, 8\rangle$ est d'ordre 3 et le cycle $c_4 = \langle 4, 9, 5, 7\rangle$ est d'ordre 4.
On en déduit que l'ordre de σ est égal à $\mathrm{ppcm}(2, 3, 4) = 12$.

Remarque
On peut déterminer $\varepsilon(\sigma)$ en calculant le nombre d'inversions de σ. On trouve qu'il y a 22 couples (i,j) tels que $i < j$ et $\sigma(i) > \sigma(j)$. Donc $\varepsilon(\sigma) = (-1)^{22} = 1$. Mais il est plus rapide d'utiliser la décomposition en cycles. Quant à déterminer l'ordre de σ en calculant successivement σ^2, σ^3, etc., ce serait déraisonnable.

Exercice 4

1) • Montrons que la loi $\star$ est associative :
Soit x, y et z trois réels.

$$\begin{aligned}(x\star y)\star z &= \sqrt[3]{(x\star y)^3+z^3}\\ &= \sqrt[3]{(x^3+y^3)+z^3} && x\star y=\sqrt[3]{x^3+y^3} \text{ et } \left(\sqrt[3]{t}\right)^3=t\\ &= \sqrt[3]{x^3+(y^3+z^3)} && \text{par associativité de } +\\ &= \sqrt[3]{x^3+(y\star z)^3} && y\star z=\sqrt[3]{y^3+z^3}\\ &= x\star(y\star z).\end{aligned}$$

• De la même façon, la commutativité de $+$ entraîne celle de $\star$.
• Pour tout $x \in \mathbb{R}$, $0\star x = x\star 0 = \sqrt[3]{x^3+0^3} = \sqrt[3]{x^3} = x$. Donc 0 est neutre pour $\star$.
• Pour tout $x \in \mathbb{R}$, $(-x)\star x = x\star(-x) = \sqrt[3]{x^3+(-x)^3} = \sqrt[3]{x^3-x^3} = \sqrt[3]{0} = 0$. Donc tout réel admet un symétrique pour $\star$.

On a montré que $(\mathbb{R},\star)$ est un groupe abélien.

2) Notons $f : t \mapsto t^3$. On a

$$\forall x,y\in\mathbb{R},\quad f(x\star y)=(x\star y)^3=x^3+y^3=f(x)+f(y).$$

Donc f est un morphisme de groupes de $(\mathbb{R},\star)$ dans $(\mathbb{R},+)$.
Or f est bijective donc on a prouvé que $(\mathbb{R},\star)$ est isomorphe à $(\mathbb{R},+)$.

Exercice 5

1) Soit $a \in G$. Montrons que τ_a est un morphisme de groupes :
Soit x et y dans G.

$$\begin{aligned}\tau_a(x)*\tau_a(y) &= (a*x*a^{-1})*(a*y*a^{-1})\\ &= a*x*(a^{-1}*a)*y*a^{-1} && \text{par associativité}\\ &= a*(x*y)*a^{-1} && a^{-1}*a=e \text{ (élément neutre)}\\ &= \tau_a(x*y).\end{aligned}$$

Montrons que τ_a est une permutation de G :
Soit x et y dans G.

$$\begin{aligned}y=\tau_a(x) &\iff y=a*x*a^{-1}\\ &\iff y*a=a*x\\ &\iff a^{-1}*y*a=x.\end{aligned}$$

Donc tout élément de G a un unique antécédent dans G par τ_a. Donc τ_a est bijection de G dans lui-même.

Remarque
On peut même préciser que $\tau_a^{-1} = \tau_{a^{-1}}$.

On a montré que τ_a est un automorphisme du groupe $(G, *)$.

2) Soit a et b dans G. On a pour tout $x \in G$:

$$\begin{aligned} \tau_a \circ \tau_b(x) &= \tau_a\left(\tau_b(x)\right) \\ &= a * (b * x * b^{-1}) * a^{-1} \\ &= (a * b) * x * \left(b^{-1} * a^{-1}\right) \\ &= \tau_{a*b}(x) \end{aligned} \quad (a * b)^{-1} = b^{-1} * a^{-1}$$

Donc $\tau_a \circ \tau_b = \tau_{a*b}$.

3) En notant $\mathfrak{S}(G)$ l'ensemble des permutations de G, on vient de montrer que $a \mapsto \tau_a$ est un homomorphisme de groupes de $(G, *)$ dans $\left(\mathfrak{S}(G), \circ\right)$. Puisqu'on a un homomorphisme, l'image du groupe G est un sous-groupe de $\mathfrak{S}(G)$. Donc $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

Remarque
$a \mapsto \tau_a$ étant un homomorphisme de groupes, on retrouve $\tau_a^{-1} = \tau_{a^{-1}}$.

Exercice 6

1) Par définition, $Z(G)$ est une partie de G.

- En notant e l'élément neutre de G, on a pour tout $y \in G$, $e * y = y * e$ donc $e \in Z(G)$.
- Soit x_1 et x_2 deux éléments de $Z(G)$. On a pour tout $y \in G$:

$$\begin{aligned} (x_1 * x_2) * y &= x_1 * (x_2 * y) \\ &= x_1 * (y * x_2) \\ &= (x_1 * y) * x_2 \\ &= (y * x_1) * x_2 \\ &= y * (x_1 * x_2) \end{aligned}$$

  Donc $x_1 * x_2 \in Z(G)$.
- Soit x un élément de $Z(G)$. On a pour tout $y \in G$, $x * y = y * x$. En multipliant à gauche et à droite par le l'inverse x^{-1} de x, on obtient $e * y * x^{-1} = x^{-1} * y * e$ donc $y * x^{-1} = x^{-1} * y$. Donc $x^{-1} \in Z(G)$.

On a montré que $Z(G)$ est un sous-groupe de G.

2) Notons $\mathcal{G}$ l'ensemble des matrices de la forme $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ avec x, y et $z \in \mathbb{R}$.

- $\mathcal{G}$ contient l'élément neutre I_3.