

Feuille d'exercices n°79

Exercice 1 (*)

Décrire les groupes d'ordre 3. Donner deux exemples de tels groupes.

Corrigé : Soit G un groupe d'ordre 3. Il existe un élément $x \in G \setminus \{e\}$. On a $o(x)$ diviseur de 3 et $o(x) = \text{Card } \langle x \rangle > 1$ puisque $\{e, x\} \subset \langle x \rangle$. On en déduit $G = \langle x \rangle$ et on conclut

Les groupes d'ordre 3 sont isomorphes à $\mathbb{Z}/3\mathbb{Z}$.

Les groupes $\mathbb{Z}/3\mathbb{Z}$ et $\mathcal{A}_3$ sont d'ordre 3.

Exercice 2 (*)

Déterminer deux groupes d'ordre 6 non isomorphes.

Corrigé : Le groupe S_3 est d'ordre 6 et n'est pas abélien puisque

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \neq \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$$

S'il n'est pas abélien, il n'est pas cyclique. Ainsi

Les groupes S_3 et $\mathbb{Z}/6\mathbb{Z}$ sont d'ordre 6 mais non isomorphes.

Exercice 3 (*)

Déterminer tous les automorphismes du groupe $(\mathbb{Z}, +)$.

Corrigé : Soit φ un automorphisme. On a $\text{Im } \varphi = \mathbb{Z}$ d'où l'existence de $k \in \mathbb{Z}$ tel que $1 = \varphi(k)$. Par propriété de morphisme, on a $\varphi(k) = k\varphi(1)$ d'où $\varphi(1)|1$ ce qui impose $\varphi(1) \in \{\pm 1\}$ et par conséquent $\varphi = \pm \text{id}$. Réciproquement, de telles applications sont des automorphismes de $(\mathbb{Z}, +)$. On conclut

Les automorphismes de $(\mathbb{Z}, +)$ sont id et $-\text{id}$.

Variante : Comme on a $\varphi(k) = k\varphi(1)$ pour $k \in \mathbb{Z}$, il s'ensuit $\text{Im } \varphi = \varphi(1)\mathbb{Z}$ et comme φ est un automorphisme, on a donc $\text{Im } \varphi = \mathbb{Z}$ d'où $\varphi(1)\mathbb{Z} = \mathbb{Z}$ ce qui prouve que $\varphi(1)$ et 1 sont associés d'où $\varphi(1) = \pm 1$. On conclut comme précédemment.

Exercice 4 (*)

Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ sont-ils isomorphes ?

Corrigé : Soit $\varphi : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \times)$ un isomorphisme de groupes. Par surjectivité, il existe x réel tel que $\varphi(x) = -1$ et par suite

$$\varphi(x) = \varphi\left(2\frac{x}{2}\right) = \left(\varphi\left(\frac{x}{2}\right)\right)^2 = -1$$

ce qui est absurde. On conclut

Les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ne sont pas isomorphes.

Exercice 5 (*)

Soient $(G, \times)$, $(G', \times)$ des groupes, $C = \{aba^{-1}b^{-1}, (a, b) \in G^2\}$ et $\varphi : G \rightarrow G'$ un morphisme de groupes. Montrer

$$(\varphi(G), \times) \text{ abélien} \iff \langle C \rangle \subset \text{Ker } \varphi$$

Corrigé : Pour $(a, b) \in G^2$, on a par morphisme de groupes

$$\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = e' \iff \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$$

Ainsi

$$(\varphi(G), \times) \text{ abélien} \iff C \subset \text{Ker } \varphi$$

Comme $\text{Ker } \varphi$ est un sous-groupe de G , on a $C \subset \text{Ker } \varphi \iff \langle C \rangle \subset \text{Ker } \varphi$. Ainsi

$$\boxed{(\varphi(G), \times) \text{ abélien} \iff \langle C \rangle \subset \text{Ker } \varphi}$$

Vocabulaire : Les éléments de la partie C sont appelés *commutateurs* de G .

Exercice 6 (*)

Soit $n \geq 2$. Calculer

$$\sum_{\sigma \in S_n} \varepsilon(\sigma)$$

Corrigé : Soit τ une transposition de S_n . L'application $\varphi : S_n \rightarrow S_n, \sigma \mapsto \tau \circ \sigma$ est une permutation de S_n (c'est une involution). Par conséquent, on a

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) = \sum_{\sigma \in S_n} \varepsilon(\tau \circ \sigma) = \sum_{\sigma \in S_n} \varepsilon(\tau)\varepsilon(\sigma)$$

Or, la signature d'une transposition est égale à -1 et par conséquent

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) = - \sum_{\sigma \in S_n} \varepsilon(\sigma)$$

Ainsi

$$\boxed{\sum_{\sigma \in S_n} \varepsilon(\sigma) = 0}$$

Variante : Pour $A \in \mathcal{M}_n(\mathbb{R})$, on a $\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n a_{i, \sigma(i)}$. Ainsi, notant J la matrice de $\mathcal{M}_n(\mathbb{R})$ constituée de 1, on a

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) = \det J$$

La matrice J contient (au moins) deux colonnes identiques et n'est donc pas inversible. On retrouve alors le résultat précédent.

Exercice 7 (**)

1. Déterminer les morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
2. Déterminer les morphismes de groupes de $\mathbb{Z}/6\mathbb{Z}$ vers $\mathbb{Z}/8\mathbb{Z}$.

Corrigé : Soit $\varphi : (\mathbb{Z}/n\mathbb{Z}, +) \rightarrow (G, +)$ un morphisme de groupes. On a $\varphi(\bar{k}) = k\varphi(\bar{1})$ pour tout $k \in \mathbb{Z}$ ce qui signifie que φ est caractérisé par $\varphi(\bar{1})$.

1. Le groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est d'ordre 8. On a $o(\varphi(\bar{1})) \mid 3$ et $o(\varphi(\bar{1})) \mid 8$ d'où $o(\varphi(\bar{1})) \mid 3 \wedge 8 = 1$, i.e. $\varphi(\bar{1}) = \hat{0}$. Ainsi

Le morphisme nul est l'unique morphisme de $\mathbb{Z}/3\mathbb{Z}$ vers $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

2. On a $o(\varphi(\bar{1})) \mid 6 \wedge 8 = 2$. Ainsi, on a $2\varphi(\bar{1}) = \widehat{0}$ d'où $\varphi(\bar{1}) \in \{\widehat{0}, \widehat{4}\}$ d'où les morphismes candidats : le morphisme nul et $\bar{x} \mapsto \widehat{4x}$ qui est bien défini puisque pour $\bar{x} \in \mathbb{Z}/6\mathbb{Z}$ et $x \in \bar{x}$, on envoie $\bar{x} = x\bar{1} \mapsto x\widehat{4} = \widehat{4x}$ et le choix du représentant n'influe pas. La synthèse est immédiate et on conclut

Les morphismes de groupes de $\mathbb{Z}/6\mathbb{Z}$ vers $\mathbb{Z}/8\mathbb{Z}$ sont le morphisme nul et $\bar{x} \mapsto \widehat{4x}$.

Exercice 8 (**)

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

Corrigé : Soit $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$ un morphisme de groupes. Pour x rationnel, on a

$$\forall n \in \mathbb{N}^* \quad f(x) = f\left(n \frac{x}{n}\right) = nf\left(\frac{x}{n}\right)$$

ce qui prouve que $f(x)$ est un entier naturel divisible par tout entier non nul d'où $f(x) = 0$. Ainsi

L'unique morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est le morphisme nul.

Variante : Soit $f : (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$ un morphisme de groupes. L'ensemble $\text{Im } f$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il existe $n \in \mathbb{N}$ tel que $\text{Im } f = n\mathbb{Z}$. Supposons $n \neq 0$. Comme $n \in \text{Im } f$, il existe $x \in \mathbb{Q}$ tel que $f(x) = n$. Puis

$$2f\left(\frac{x}{2}\right) = f(x) = n \implies f\left(\frac{x}{2}\right) = \frac{n}{2} \in \text{Im } f$$

ce qui contredit $\text{Im } f = n\mathbb{Z}$.

Exercice 9 (**)

Soit $n \geq 3$. Montrer que S_n est engendré par les permutations suivantes :

1. $(1 \ 2), \dots, (1 \ n)$;
2. $(1 \ 2), (2 \ 3), \dots, (n-1 \ n)$;
3. $(1 \ 2), (2 \ 3 \ \dots \ n)$.

Corrigé : 1. Soit $(i, j) \in \llbracket 2; n \rrbracket^2$ avec $i \neq j$. On observe

$$(i \ j) = (1 \ i) (1 \ j) (1 \ i)$$

Toute transposition est donc engendré par $\{(1, k), k \in \llbracket 2; n \rrbracket\}$ et comme les transpositions engendrent S_n , on conclut

$$S_n = \langle \{(1 \ k), k \in \llbracket 2; n \rrbracket\} \rangle$$

Remarque : On a utilisé le fait que les 2-cycles sont conjuguées pour avoir l'intuition de cette décomposition.

2. Soit $H = \langle \{(1 \ 2), (2 \ 3), \dots, (n-1 \ n)\} \rangle$. On montre par récurrence $(1 \ k) \in H$ pour $k \in \llbracket 2; n \rrbracket$. L'initialisation est vraie pour $k = 2$. On suppose la propriété vraie au rang $k \in \llbracket 2; n-1 \rrbracket$ fixé. On a

$$(1 \ k+1) = (1 \ k) (k \ k+1) (1 \ k) \in H$$

d'où l'hérédité et d'après le résultat de la première question, on conclut

$$S_n = \langle \{(1 \ 2), (2 \ 3), \dots, (n-1 \ n)\} \rangle$$

3. On observe

$$\forall k \in \llbracket 2; n-1 \rrbracket \quad (2 \ 3 \ \dots \ n) (1 \ k) (2 \ 3 \ \dots \ n)^{-1} = (1 \ k+1)$$

Par récurrence, on trouve $(1 \ k) \in \langle \{(1 \ 2), (2 \ 3 \ \dots \ n)\} \rangle$ pour tout $k \in \llbracket 2; n \rrbracket$ et avec le résultat de la première question, on conclut

$$S_n = \langle \{(1 \ 2), (2 \ 3 \ \dots \ n)\} \rangle$$

Exercice 10 (**)

Soit n entier avec $n \geq 2$ et d un diviseur de n . Montrer qu'il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d .

Corrigé : Soit d diviseur de n . L'ensemble $\{\bar{0}\}$ est l'unique sous-groupe d'ordre 1 de $\mathbb{Z}/n\mathbb{Z}$. On suppose $d > 1$. On a $n = cd$ avec c entier non nul puis $d\bar{c} = \bar{0}$ et $\ell\bar{c} \neq \bar{0}$ pour $\ell \in \llbracket 1; d-1 \rrbracket$ puisque les $\bar{k}$ pour $k \in \llbracket 0; n-1 \rrbracket$ sont deux à deux distincts. On en déduit $o(\bar{c}) = d$ et par conséquent $\langle \bar{c} \rangle$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d décrit par

$$\langle \bar{c} \rangle = \{k\bar{c}, k \in \mathbb{Z}\} = \{\bar{0}, \bar{c}, \dots, (d-1)\bar{c}\}$$

Montrons l'unicité de ce sous-groupe. Soit H sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d . Pour $\bar{x} \in H$ et $x \in \bar{x}$, on a $d\bar{x} = \bar{0}$ d'où $dx \equiv 0 [n]$, i.e. $dx = kn$ avec $k \in \mathbb{Z}$ puis $dx = kdc$ autrement dit $x = kc$ d'où $\bar{x} \in \langle \bar{c} \rangle$. Il s'ensuit que $H \subset \langle \bar{c} \rangle$ et par égalité des cardinaux, on conclut que $H = \langle \bar{c} \rangle$. Ainsi

Pour d diviseur de n , il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d .

Exercice 11 (**)

Dénombrer les p -cycles de S_n .

Corrigé : Choisir un p -cycle, c'est d'abord choisir une p -liste $(i_1, \dots, i_p)$ d'éléments de $\llbracket 1; n \rrbracket$ et ensuite tenir compte du fait que pour $c = (1 \ \dots \ p)$, on a

$$\forall k \in \llbracket 0; p-1 \rrbracket \quad (i_{c^k(1)} \ \dots \ i_{c^k(p)}) = (i_1 \ \dots \ i_p)$$

ce qui signifie que chaque p -cycle est donc compté p fois. On conclut

$$\text{Il y a } \frac{n!}{p(n-p)!} \text{ } p\text{-cycles dans } S_n.$$

Variante : Choisir un p -cycle, c'est d'abord choisir p éléments de $\llbracket 1; n \rrbracket$, puis considérer le minimum du support comme début du cycle et choisir une permutation des $(p-1)!$ éléments restants ce qui fait

$$\binom{n}{p}(p-1)! \text{ choix de } p\text{-cycle dans } S_n$$

Exercice 12 (**)

Soit n entier non nul. Pour $\sigma \in S_n$, on pose $M_\sigma = (\delta_{i, \sigma(j)})_{(i,j) \in \llbracket 1; n \rrbracket^2} \in \mathcal{M}_n(\mathbb{R})$ et $f_\sigma \in \mathcal{L}(\mathbb{R}^n)$ l'application canoniquement associée. Déterminer la nature de l'application de $\frac{1}{n!} \sum_{\sigma \in S_n} f_\sigma$ et préciser son noyau et son image.

Corrigé : Notons $f = \frac{1}{n!} \sum_{\sigma \in S_n} f_\sigma$ puis $M = \text{mat}_{\mathcal{C}} f$ avec $\mathcal{C}$ base canonique de $\mathbb{R}^n$. Notant $M = (m_{i,j})_{1 \leq i,j \leq n}$, on a

$$\forall (i,j) \in \llbracket 1; n \rrbracket^2 \quad m_{i,j} = \frac{1}{n!} \sum_{\sigma \in S_n} \delta_{i,\sigma(j)} = \frac{1}{n!} \text{Card} \{ \sigma \in S_n \mid \sigma(j) = i \} = \frac{(n-1)!}{n!} = \frac{1}{n}$$

Notant $J \in \mathcal{M}_n(\mathbb{R})$ la matrice constituée de 1, on a $M = \frac{1}{n}J$ et $J^2 = nJ$ d'où $M^2 = M$. Sans difficulté, on trouve $\text{Ker } M : \sum_{i=1}^n x_i = 0$ et $\text{Im } M = \text{Vect}(u)$ avec $u = (1, \dots, 1)$ et on conclut

L'application f est le projecteur sur $\text{Vect}(u)$ parallèlement à l'hyperplan $\sum_{i=1}^n x_i = 0$.

Variante : Notons $E = \mathbb{R}^n$, $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ da base canonique. Soit $\sigma \in S_n$. Pour $x = \sum_{i=1}^n x_i e_i \in E$,

on a
$$f_\sigma(x) = f_\sigma \left(\sum_{i=1}^n x_i e_i \right) = \sum_{i=1}^n x_i f_\sigma(e_i) = \sum_{i=1}^n x_i e_{\sigma(i)} = \sum_{i=1}^n x_{\sigma^{-1}(e_i)} e_i$$

Ainsi
$$f(x) = \frac{1}{n!} \sum_{\sigma \in S_n} \sum_{i=1}^n x_{\sigma^{-1}(e_i)} e_i = \sum_{i=1}^n \left(\sum_{\sigma \in S_n} x_{\sigma^{-1}(e_i)} \right) e_i$$

Or
$$\sum_{\sigma \in S_n} x_{\sigma^{-1}(e_i)} = \sum_{j=1}^n \sum_{\sigma \in S_n \mid \sigma(j)=i} x_j = \sum_{j=1}^n x_j \text{Card} \{ \sigma \in S_n \mid \sigma(j) = i \} = (n-1)! \sum_{j=1}^n x_j$$

Ainsi
$$f(x) = \frac{1}{n} \left(\sum_{j=1}^n x_j \right) \left(\sum_{i=1}^n e_i \right)$$

On retrouve le résultat précédent.

Exercice 13 (**)

Soit $(G, \times)$ un groupe fini d'ordre n . Montrer que

1. $(G, \times)$ est isomorphe à un sous-groupe de $(S_n, \circ)$;
2. $(G, \times)$ est isomorphe à un sous-groupe de $(\mathcal{A}_{n+2}, \circ)$;

Corrigé : 1. Soit $a \in G$ et $\varphi_a : G \rightarrow G, x \mapsto ax$. L'application φ_a est une permutation de G (d'application réciproque $\varphi_{a^{-1}}$). Considérons l'application $\Phi : G \rightarrow S(G), a \mapsto \varphi_a$. Pour $(a, b) \in G^2$, on a

$$\forall x \in G \quad \Phi(ab)(x) = \varphi_{ab}(x) = abx = \varphi_a \circ \varphi_b(x) = \Phi(a) \circ \Phi(b)(x)$$

autrement dit

$$\Phi(ab) = \Phi(a) \circ \Phi(b)$$

ce qui prouve que Φ est un morphisme de groupes. Puis, pour $a \in G$, on trouve

$$\Phi(a) = \text{id} \iff \forall x \in G \quad ax = x \iff a = 1$$

d'où l'injectivité de Φ . Par conséquent, on a

$$G \simeq \Phi(G) \quad \text{avec} \quad \Phi(G) \text{ sous-groupe de } S(G)$$

Comme $S(G)$ est isomorphe à S_n , on obtient

Le groupe $(G, \times)$ est isomorphe à un sous-groupe de $(S_n, \circ)$.

Remarque : Ce résultat s'intitule *théorème de Cayley*.

2. Pour $\sigma \in S_n$, on identifie σ à une permutation de S_{n+2} qui fixe $n+1$ et $n+2$. Notons $\tau = (n+1 \ n+2)$. On définit

$$\forall \sigma \in S_n \quad \Psi(\sigma) = \begin{cases} \sigma & \text{si } \varepsilon(\sigma) = 1 \\ \sigma \circ \tau & \text{sinon} \end{cases}$$

On pose $\forall \sigma \in S_n \quad \nu(\sigma) = \mathbb{1}_{\varepsilon^{-1}(\{-1\})}(\sigma)$

Ainsi $\forall \sigma \in S_n \quad \Psi(\sigma) = \sigma \circ \tau^{\nu(\sigma)}$

L'application Ψ ainsi définie est clairement à valeurs dans $\mathcal{A}_{n+2}$. On observe l'égalité

$$\forall (\sigma, \gamma) \in S_n^2 \quad \nu(\sigma) + \nu(\gamma) \equiv \nu(\sigma \circ \gamma) \pmod{2}$$

d'où $\forall (\sigma, \gamma) \in S_n^2 \quad \tau^{\nu(\sigma)+\nu(\gamma)} = \tau^{\nu(\sigma \circ \gamma)}$

Pour $\sigma \in S_n$, les supports de τ et σ étant disjoints, ces permutations commutent. Il en résulte que Ψ est un morphisme de groupe :

$$\begin{aligned} \forall (\sigma, \gamma) \in S_n^2 \quad \Psi(\sigma \circ \gamma) &= \sigma \circ \gamma \circ \tau^{\nu(\sigma \circ \gamma)} = \sigma \circ \gamma \circ \tau^{\nu(\sigma)+\nu(\gamma)} \\ &= \sigma \circ \tau^{\nu(\sigma)} \circ \gamma \circ \tau^{\nu(\gamma)} = \Psi(\sigma) \circ \Psi(\gamma) \end{aligned}$$

Soit $\sigma \in S_n$ tel que $\Psi(\sigma) = \text{id}$. On a $\Psi(\sigma)(n+1) = n+1$ d'où $\varepsilon(\sigma) = 1$ puis $\sigma = \text{id}$ ce qui prouve l'injectivité de Ψ . Comme G est isomorphe à un sous-groupe de S_n lui-même isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$ via le morphisme Ψ , on conclut

Le groupe G est isomorphe à un sous-groupe de $\mathcal{A}_{n+2}$.