ISM MP, Mathématiques
Année 2025/2026

Feuille d'exercices n°81

Exercice 1 (***)

Soit G un groupe fini vérifiant $\forall x \in \mathrm{G} \quad x^2 = e$

1. Montrer que G est un groupe abélien.
2. On suppose que G est fini non réduit à $\{e\}$.
   (a) Justifier l'existence de $n = \min\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\}$ entier non nul.
   (b) Soit $(x_1, \dots, x_n) \in \mathrm{G}^n$ tel que $\mathrm{G} = \langle x_1, \dots, x_n\rangle$. On pose
   $$\varphi : (\mathbb{Z}/2\mathbb{Z})^n \to \mathrm{G},\ (\overline{\alpha_1}, \dots, \overline{\alpha_n}) \mapsto x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{avec} \quad \alpha_i \in \{0, 1\}$$
   Justifier que φ est bien définie et vérifier que φ est un morphisme de de groupes.
   (c) Conclure que $\mathrm{G} \simeq (\mathbb{Z}/2\mathbb{Z})^n$

Corrigé : 1. Soit $(x, y) \in \mathrm{G}^2$. On a
$$(xy)^2 = e \iff xyxy = e \iff yxy = x \iff xy = yx$$
Ainsi $\boxed{\text{Le groupe G est abélien.}}$

2.(a) L'ensemble $\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\}$ est non vide puisque $\langle \mathrm{G}\rangle = \mathrm{G}$ et il s'agit d'une partie non vide de $\mathbb{N}$ qui admet donc un plus petit élément n. Enfin, comme $\langle \varnothing\rangle = \{e\} \neq \mathrm{G}$ et que l'ensemble vide est l'unique partie de cardinal nul, on conclut
$$\boxed{\text{Il existe } n = \min\{\text{Card P, P} \subset \mathrm{G} \text{ tel que } \langle \mathrm{P}\rangle = \mathrm{G}\} \text{ entier non nul.}}$$

2.(b) Soit $(\alpha_i)_{i\in[\![1\,;n]\!]}$ et $(\beta_i)_{i\in[\![1\,;n]\!]}$ dans $\mathbb{Z}^n$ tel que $\overline{\alpha_i} = \overline{\beta_i}$ pour tout $i \in [\![1\,;\,n]\!]$. Il s'ensuit
$$x_1^{\alpha_1} \dots x_n^{\alpha_n} = x_1^{\beta_1} \dots x_n^{\beta_n}$$
ce qui prouve que l'application φ est bien définie et ne dépend pas du choix des représentants des classes $\overline{\alpha_i}$. Puis, par commutativité, on a
$$\begin{aligned}\varphi\left((\overline{\alpha_1}, \dots, \overline{\alpha_n}) + (\overline{\beta_1}, \dots, \overline{\beta_n})\right) &= \varphi\left(\overline{\alpha_1 + \beta_1}, \dots, \overline{\alpha_n + \beta_n}\right)\\ &= x_1^{\alpha_1+\beta_1} \dots x_n^{\alpha_n+\beta_n} = x_1^{\alpha_1} \dots x_n^{\alpha_n} x_1^{\beta_1} \dots x_n^{\beta_n}\\ &= \varphi(\overline{\alpha_1}, \dots, \overline{\alpha_n})\varphi(\overline{\beta_1}, \dots, \overline{\beta_n})\end{aligned}$$
Ainsi $\boxed{\text{L'application } \varphi \text{ est un morphisme de groupes.}}$

2.(c) On note $\mathrm{H} = \left\{x_1^{\alpha_1} \dots x_n^{\alpha_n}, (\alpha_i)_{i\in[\![1\,;n]\!]} \in \mathbb{Z}^n\right\}$. L'ensemble H est clairement un sous-groupe de G contenant $\{x_1, \dots, x_n\}$ d'où $\mathrm{G} \subset \mathrm{H}$ et on a clairement $\mathrm{H} \subset \mathrm{G}$ d'où l'égalité $\mathrm{G} = \mathrm{H}$. Par définition, on a $\mathrm{Im}\,\varphi = \mathrm{H}$ d'où la surjectivité de φ. Enfin, soit $(\alpha_i)_{i\in[\![1\,;n]\!]} \in \mathbb{Z}^n$ tel que $(\overline{\alpha_i})_{i\in[\![1\,;n]\!]} \in \mathrm{Ker}\,\varphi$. Supposons α_{i_0} impair avec $i_0 \in [\![1\,;\,n]\!]$. Il vient par commutativité
$$x_{i_0} = \prod_{i\in[\![1\,;n]\!]\setminus\{i_0\}} x_i^{\alpha_i}$$
Ceci contredirait la minimalité de n, cardinal d'une famille génératrice minimale. On en déduit que tous les α_i sont pairs d'où

$$\text{Ker } \varphi = \{(\bar{0}, \dots, \bar{0})\}$$

Le morphisme de groupes φ est donc un isomorphisme et on conclut

$$\boxed{\text{G} \simeq (\mathbb{Z}/2\mathbb{Z})^n}$$

Remarque : On peut observer que le cardinal d'une famille génératrice minimale vérifie $n = \log_2 \text{Card G}$.

Exercice 2 (***)

Soient p et q des entiers non nuls premiers entre eux. Montrer que l'application $\varphi : \mathbb{U}_p \times \mathbb{U}_q \to \mathbb{U}_{pq}, (x, y) \mapsto xy$ est un isomorphisme de groupes.

Corrigé : L'application est bien définie puisque pour $(x, y) \in \mathbb{U}_p \times \mathbb{U}_q$, on a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$ et est clairement un morphisme puisque

$$\forall (x, x') \in \mathbb{U}_p^2 \qquad \forall (y, y') \in \mathbb{U}_q^2 \qquad \varphi(xx', yy') = xx'yy' = xyx'y' = \varphi(x, y)\varphi(x', y')$$

On pose $\alpha = \mathrm{e}^{\frac{2\mathrm{i}\pi}{p}} \qquad \beta = \mathrm{e}^{\frac{2\mathrm{i}\pi}{q}} \qquad \gamma = \mathrm{e}^{\frac{2\mathrm{i}\pi}{pq}}$

L'application φ réalise la transformation suivante :

$$\forall (k, \ell) \in \mathbb{Z}^2 \qquad \varphi(\alpha^k, \beta^\ell) = \gamma^{qk+\ell p}$$

Posons $\psi : \begin{cases} \mathbb{Z}^2 & \longrightarrow \mathbb{Z} \\ (k, \ell) & \longmapsto qk + p\ell \end{cases}$

L'application ψ est clairement un morphisme de groupes donc Im ψ est un sous-groupe de $\mathbb{Z}$. Or, d'après le théorème de Bézout, comme $p \wedge q = 1$, il s'ensuit que $1 \in \text{Im } \psi$ d'où Im $\psi = \mathbb{Z}$ et la surjectivité de φ s'ensuit. On a donc une surjection entre deux ensembles de même cardinaux d'où la bijectivité de φ et on conclut

$$\boxed{\text{L'application } \varphi \text{ est un morphisme de groupes.}}$$

Variante : Déterminons Ker φ, ou de manière équivalente les couples $(k, \ell) \in \mathbb{Z}^2$ tels que $qk + p\ell \equiv 0\ [qp]$, c'est-à-dire $qk + p\ell = rpq$ avec $r \in \mathbb{Z}$. En isolant les facteurs en q puis les facteurs en p, on en déduit à l'aide du théorème de Gauss que $p|qk$ donc $p|k$ puis $q|p\ell$ donc $q|\ell$ et par conséquent $\alpha^k = 1$ et $\beta^\ell = 1$, autrement dit

$$\text{Ker } \varphi = \{(1, 1)\}$$

d'où l'injectivité de φ entre deux ensembles de même cardinal et on conclut comme précédemment. On peut aussi utiliser la relation de Bézout pour établir la surjectivité plutôt que passer par l'argument sur les cardinaux. Enfin, cet exercice est un jumeau du théorème chinois qui fournit directement

$$qk + p\ell \equiv 0\ [pq] \iff \begin{cases} qk + p\ell \equiv 0\ [p] \\ qk + p\ell \equiv 0\ [q] \end{cases}$$

avec l'isomorphisme d'anneaux $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Exercice 3 (***)

Soit φ un morphisme d'un groupe fini $(\mathrm{G}, \times)$ vers un autre groupe. Établir

$$\mathrm{Card}\ \mathrm{G} = \mathrm{Card}\ \mathrm{Ker}\ \varphi \times \mathrm{Card}\ \mathrm{Im}\ \varphi$$

Corrigé : On définit la relation binaire $\mathcal{R}$ par

$$\forall (x,y) \in \mathrm{G}^2 \qquad x \mathcal{R} y \iff \varphi(x) = \varphi(y)$$

On vérifie sans difficulté que $\mathcal{R}$ est une relation d'équivalence. L'ensemble des classes d'équivalence est exactement le cardinal de Im φ. Pour $(x,y) \in \mathrm{G}^2$, par propriété de morphisme de groupes, on a

$$\begin{aligned} x \mathcal{R} y &\iff \varphi(x) = \varphi(y) \iff \varphi(y)^{-1}\varphi(x) = 1 \\ &\iff \varphi(y^{-1}x) = 1 \iff x^{-1}y \in \mathrm{Ker}\ \varphi \iff y \in x\,\mathrm{Ker}\ \varphi \end{aligned}$$

Ainsi, une classe d'équivalence pour $\mathcal{R}$ est de la forme $x\,\mathrm{Ker}\ \varphi$. Or, l'application $\mathrm{G} \to \mathrm{G}, u \mapsto xu$ est une permutation de G ce qui prouve que les classes d'équivalence sont toutes en bijection avec Ker φ. Notant $x_1, \dots, x_p$ des représentants des classes d'équivalence, la famille $\overline{x_1}, \dots, \overline{x_p}$ est une partition de G d'où

$$\mathrm{Card}\ \mathrm{G} = \mathrm{Card} \bigsqcup_{i=1}^{p} \overline{x_i} = \sum_{i=1}^{p} \mathrm{Card}\ \overline{x_i} = p\,\mathrm{Card}\ \mathrm{Ker}\ \varphi$$

On conclut $\boxed{\mathrm{Card}\ \mathrm{G} = \mathrm{Card}\ \mathrm{Ker}\ \varphi \times \mathrm{Card}\ \mathrm{Im}\ \varphi}$

Remarque : C'est exactement la démonstration du théorème de Lagrange.

Exercice 4 (***)

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

1. G est isomorphe à un sous-groupe de S_n ;
2. G est isomorphe est à un sous-groupe de $\mathcal{O}_n(\mathbb{R})$.

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

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

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

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

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

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

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

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

$$\boxed{\text{Le groupe G est isomorphe à un sous-groupe de } \mathrm{S}_n.}$$

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

2. On pose $$\forall \sigma \in \mathrm{S}_n \qquad \chi(\sigma) = \left(\delta_{i,\sigma(j)}\right)_{1 \leqslant i,j \leqslant n}$$

Pour $\sigma \in \mathrm{S}_n$, les colonnes de $\chi(\sigma)$ forment clairement une base orthonormée :

$$\forall (j,k) \in [\![1\,;\, n]\!]^2 \qquad \sum_{i=1}^{n} \delta_{i,\sigma(j)}\delta_{i,\sigma(k)} = \delta_{\sigma(j),\sigma(k)} = \delta_{j,k}$$

Soit $(\sigma,\gamma) \in \mathrm{S}_n^2$. On a

$$\forall (i,j) \in [\![1\,;\, n]\!]^2 \qquad (\chi(\sigma)\chi(\gamma))_{i,j} = \sum_{k=1}^{n} \delta_{i,\sigma(k)}\delta_{k,\gamma(j)} = \delta_{i,\sigma(\gamma(j))} = \chi(\sigma\circ\gamma)_{i,j}$$

Autrement dit $\qquad \forall (\sigma,\gamma) \in \mathrm{S}_n^2 \qquad \chi(\sigma\circ\gamma) = \chi(\sigma)\chi(\gamma)$

Ainsi, l'application χ est un morphisme du groupe $(\mathrm{S}_n, \circ)$ vers le groupe $(\mathcal{O}_n(\mathbb{R}), \times)$. Puis, pour $\sigma \in \mathrm{S}_n$, on a

$$\begin{aligned} \chi(\sigma) = \mathrm{I}_n &\iff \forall (i,j) \in [\![1\,;\, n]\!]^2 \qquad \delta_{i,\sigma(j)} = \delta_{i,j} \\ &\iff \forall j \in [\![1\,;\, n]\!] \qquad j = \sigma(j) \iff \sigma = \mathrm{id} \end{aligned}$$

Ainsi, le morphisme χ est injectif. Comme le groupe G est isomorphe à un sous-groupe de S_n, on conclut

$$\boxed{\text{Le groupe G est isomorphe à un sous-groupe de } \mathcal{O}_n(\mathbb{R}).}$$

Exercice 5 (***)

Soit $(\mathrm{G}, \times)$ un groupe cyclique de cardinal n. Montrer que le cardinal de $(\mathrm{Aut}(\mathrm{G}), \circ)$ est $\varphi(n)$.

Corrigé : Soit $a \in \mathrm{G}$ tel que $\mathrm{G} = \langle a \rangle$. Soit $f \in \mathrm{Aut}(\mathrm{G})$. Comme f est un morphisme de groupes, on a $f(\mathrm{G}) = \langle f(a) \rangle$ et $f(a) \in \langle a \rangle$ d'où $f(a) = a^\ell$ avec $\ell \in [\![0\,;\, n-1]\!]$. Cet entier ℓ caractérise f. L'application $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathrm{G}, k \mapsto a^k$ est un isomorphisme (voir preuve du théorème décrivant les groupes monogènes). Il s'ensuit

$$f(\mathrm{G}) = \mathrm{G} \iff \langle f(a) \rangle = \langle a \rangle \iff \left\langle a^\ell \right\rangle = \langle a \rangle \iff \left\langle \bar{\ell} \right\rangle = \langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z} \iff \ell \wedge n = 1$$

Ainsi $\qquad \mathrm{Card}\ \mathrm{Aut}(\mathrm{G}) = \mathrm{Card}\ \{\ell \in [\![0\,;\, n-1]\!] \mid \ell \wedge n = 1\}$

Et on conclut $\qquad \boxed{\mathrm{Card}\ \mathrm{Aut}(\mathrm{G}) = \varphi(n)}$

Exercice 6 (***)

Décrire les groupes d'ordre 4.

Corrigé : Si G est monogène, c'est fini. Supposons qu'il ne le soit pas. Comme l'ordre d'un élément divise l'ordre du groupe, on en déduit que $x^2 = e$ pour tout $x \in \mathrm{G}$. Si G contient un unique élément x d'ordre 2, alors $\mathrm{G} = \{e, x\}$ ce qui est contradictoire. Donc G contient au moins deux éléments distincts x et y d'ordre 2, d'où $\{e, x, y\} \subset \mathrm{G}$. Si $xy = e$, on aurait $x^2y = y = x$ ce qui est faux. De même, on n'a pas $xy = x$ ni $xy = y$. Par stabilité par composition, on a

$$\{e, x, y, xy\} \subset \mathrm{G}$$

et l'inclusion est une égalité pour raison de cardinal. On a

$$(xy)^2 = e \iff xyxy = e \iff x^2yxy = x \iff yxy = x \iff y^2xy = yx \iff xy = yx$$

On remarque qu'on peut écrire $\qquad \mathrm{G} = \left\{ x^k y^\ell, (k,\ell) \in \{0,1\}^2 \right\}$

Enfin, on considère l'application : $\varphi : \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow \mathrm{G} \\ (\bar{k}, \bar{\ell}) \longmapsto x^k y^\ell \end{cases}$

C'est un morphisme surjectif. Déterminons $\mathrm{Ker}\,\varphi$. Soit $(k, \ell) \in \{0,1\}^2$ tel que $\varphi(\bar{k}, \bar{\ell}) = e$. On vérifie alors $\varphi(\bar{k}, \bar{\ell}) \neq e$ pour $(\bar{k}, \bar{\ell}) \neq (\bar{0}, \bar{0})$ d'où l'injectivité de φ. Il s'agit donc d'un isomorphisme et on conclut

$$\boxed{\mathrm{G} \simeq \mathbb{Z}/4\mathbb{Z} \quad \text{ou} \quad \mathrm{G} \simeq (\mathbb{Z}/2\mathbb{Z})^2}$$

Exercice 7 (***)

Montrer qu'un groupe est fini si et seulement si l'ensemble de ses sous-groupes est fini.

Corrigé : Si G est fini, l'ensemble $\mathcal{P}(\mathrm{G})$ des parties de G est fini (de cardinal égal $2^{\mathrm{Card\ G}}$) donc l'ensemble de ses sous-groupes également. Supposons désormais que l'ensemble des sous-groupes de G est fini. On a $\mathrm{G} = \bigcup_{x \in \mathrm{G}} \langle x \rangle$ et par hypothèse, il existe F une partie finie de G tel que $\mathrm{G} = \bigcup_{x \in \mathrm{F}} \langle x \rangle$. Supposons qu'il existe $x \in \mathrm{F}$ tel que $\langle x \rangle$ soit infini. Dans ce cas, on a $\langle x \rangle \simeq \mathbb{Z}$. Or, le groupe $\mathbb{Z}$ admet une infinité de sous-groupes que sont les $n\mathbb{Z}$ avec n entier. Par isomorphisme, le groupe $\langle x \rangle$ admet donc une infinité de sous-groupes et par conséquent, G également, ce qui est absurde. Ainsi, pour tout $x \in \mathrm{F}$, on a $\langle x \rangle$ fini et $\mathrm{G} = \bigcup_{x \in \mathrm{F}} \langle x \rangle$ est donc fini lui-aussi. On conclut

$$\boxed{\text{Un groupe est fini si et seulement si l'ensemble de ses sous-groupes est fini.}}$$

Exercice 8 (****)

Montrer que les groupes $(\mathbb{Z}^n, +)$ avec n entier non nul sont deux à deux non isomorphes.

Corrigé : Soit n entier non nul. On note $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, etc.. On a clairement

$$\mathbb{Z}^n = \langle e_1, \ldots, e_n \rangle$$

On pose $$p = \min \{\mathrm{Card\ A}, \mathrm{A\ fini} \mid \langle \mathrm{A} \rangle = \mathbb{Z}^n\}$$

Le minimum est bien défini puisque l'ensemble concerné est une partie non vide (contient $(e_1, \ldots, e_n)$) de $\mathbb{N}$. On a également $p \leqslant n$. Montrons qu'il s'agit d'une égalité. Supposons $p < n$ (cas $n = 1$ trivial) et soit $(x_1, \ldots, x_p)$ une famille génératrice de $\mathbb{Z}^n$. Ainsi

$$\forall k \in [\![1\,;\, n]\!] \qquad \exists (\alpha_{k,j})_{j \in [\![1\,;\, p]\!]} \in \mathbb{Z}^p \quad \mid \quad e_k = \sum_{j=1}^{p} \alpha_{k,j} x_j$$

On pose $$\mathrm{A} = \begin{pmatrix} \alpha_{1,1} & \ldots & \alpha_{1,p} \\ \vdots & & \vdots \\ \alpha_{n,1} & \ldots & \alpha_{n,p} \end{pmatrix} \in \mathscr{M}_{n,p}(\mathbb{R})$$

On a $\mathrm{rg\ A} \leqslant \min(n, p) = p$ ce qui signifie que la famille des lignes est liée. On peut donc trouver un indice $k_0 \in [\![1\,;\, n]\!]$ et des réels $(\mu_i)_{i \in [\![1\,;\, n]\!] \setminus \{k_0\}}$ tels que $\mathrm{L}_{k_0} = \sum_{i \in [\![1\,;\, n]\!] \setminus \{k_0\}} \mu_i \mathrm{L}_i$, autrement dit

$$(0,\dots,\underbrace{1}_{\text{indice } k_0},0,\dots)=e_{k_0}=\sum_{i\in[\![1\,;n]\!]\setminus\{k_0\}}\mu_i e_i=(\dots,\underbrace{0}_{\text{indice } k_0},\dots)$$

ce qui absurde. On conclut que $p=n$ ce qui signifie que l'entier n est le cardinal minimal d'une famille génératrice de $\mathbb{Z}^n$. Soient n,m entier et $\varphi:(\mathbb{Z}^n,+)\to(\mathbb{Z}^m,+)$ un isomorphisme. Par surjectivité, on voit que l'application φ envoie une famille génératrice sur une famille génératrice. On en déduit que $m\leqslant n$ et considérant l'isomorphisme réciproque, on obtient $n\leqslant m$. Par conséquent, le cas $n=m$ est l'unique situation d'isomorphisme et on conclut

Les groupes $(\mathbb{Z}^n,+)$ avec n entier non nul sont deux à deux non isomorphes.

Variante : Soit n entier non nul. Pour $(x,y)\in(\mathbb{Z}^n)^2$, on définit la relation binaire $x\mathcal{R}y$ par $x-y\in 2\mathbb{Z}^n$. On vérifie sans difficulté qu'il s'agit d'une relation d'équivalence et on note $\mathbb{Z}^n/2\mathbb{Z}^n$ l'ensemble des classes d'équivalence pour cette relation. On montre aisément l'isomorphisme $\mathbb{Z}^n/2\mathbb{Z}^n\simeq(\mathbb{Z}/2\mathbb{Z})^n$. Pour m et n entiers non nuls, si $\mathbb{Z}^n\simeq\mathbb{Z}^m$ alors il s'ensuit

$$(\mathbb{Z}/2\mathbb{Z})^n\simeq\mathbb{Z}^n/2\mathbb{Z}^n\simeq\mathbb{Z}^m/2\mathbb{Z}^m\simeq(\mathbb{Z}/2\mathbb{Z})^m$$

En considérant les cardinaux, il vient $2^n=2^m$ d'où $n=m$.