ISM MP, Mathématiques
Année 2024/2025

Feuille d'exercices n°81

Exercice 1 (***)

Soit $(\mathrm{G}, \times)$ un groupe. Pour $a \in \mathrm{G}$, on note

$$\forall x \in \mathrm{G} \qquad \varphi_a(x) = axa^{-1}$$

1. Montrer que φ_a est un automorphisme de G pour tout $a \in \mathrm{G}$.
2. Montrer que $\mathcal{I} = \{\varphi_a, a \in \mathrm{G}\}$ est un sous-groupe du groupe des automorphismes de G.
3. Montrer que si $(\mathcal{I}, \circ)$ est monogène, alors $(\mathrm{G}, \times)$ est commutatif.

Corrigé : 1. Soit $a \in \mathrm{G}$. On a

$$\forall (x, y) \in \mathrm{G}^2 \qquad \varphi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)$$

Puis

$$y = \varphi_a(x) \iff y = axa^{-1} \iff x = a^{-1}ya$$

Ainsi

$$\boxed{\text{L'application } \varphi_a \text{ est un automorphisme de G pour tout } a \in \mathrm{G}.}$$

2. D'après le calcul précédent, pour $b \in \mathrm{G}$, on a $(\varphi_b)^{-1} = \varphi_{b^{-1}}$ puis

$$\forall (a, b) \in \mathrm{G}^2 \qquad \varphi_a \circ (\varphi_b)^{-1} = \varphi_{ab^{-1}} \in \mathcal{I}$$

et $\mathrm{id} = \varphi_e \in \mathcal{I}$ d'où

$$\boxed{\text{L'ensemble } \mathcal{I} \text{ est un sous-groupe du groupe des automorphismes de G.}}$$

3. Si $(\mathcal{I}, \circ)$ est monogène, alors il existe $a \in \mathrm{G}$ tel que

$$\mathcal{I} = \langle \varphi_a \rangle = \{\varphi_{a^k}, k \in \mathbb{Z}\}$$

Soit $(b, c) \in \mathrm{G}^2$. Il existe $(p, q) \in \mathbb{Z}^2$ tel que $\varphi_b = \varphi_{a^p}$ et $\varphi_c = \varphi_{a^q}$. Puis

$$\begin{aligned} bcb^{-1}c^{-1} &= \varphi_b(c)c^{-1} = \varphi_{a^p}(c)c^{-1} = a^pca^{-p}c^{-1} \\ &= a^p\varphi_c(a^{-p}) = a^p\varphi_{a^q}(a^{-p}) = a^pa^qa^{-p}a^{-q} = a^{p+q-p-q} = e \end{aligned}$$

Ainsi

$$\boxed{\text{Le groupe } (\mathrm{G}, \times) \text{ est commutatif.}}$$

Remarque : On peut alors observer que $\mathcal{I} = \{\mathrm{id}\}$.

Exercice 2 (***)

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

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 3 (***)

Soient $(\mathrm{G}_1, \times)$ et $(\mathrm{G}_2, \times)$ deux groupes cycliques.

1. Pour $(x, y) \in \mathrm{G}_1 \times \mathrm{G}_2$, déterminer l'ordre de (x, y) en fonction de $o(x)$ et $o(y)$.
2. Déterminer une condition nécessaire et suffisante pour avoir $\mathrm{G}_1 \times \mathrm{G}_2$ cyclique.

Corrigé : 1. On notera $o(x, y)$ l'ordre de (x, y). Soit k entier non nul tel que $(x, y)^k = (e_1, e_2)$, ce qui équivaut à $(x^k, y^k) = (e_1, e_2)$. Un tel entier existe comme par exemple $o(x)o(y)$. Puis, comme $(x^k, y^k) = (e_1, e_2)$, il vient $o(x)|k$ et $o(y)|k$. Or, on veut l'entier minimal vérifiant ces conditions et on conclut

$$\boxed{o(x, y) = o(x) \vee o(y)}$$

2. Notons $n = \mathrm{Card}\ \mathrm{G}_1$ et $m = \mathrm{Card}\ \mathrm{G}_2$. Supposons $\mathrm{G}_1 \times \mathrm{G}_2$ cyclique. Il existe donc un élément (x, y) tel $o(x, y) = nm$. Or, on a $o(x, y) = o(x) \vee o(y)$. Puis

$$(o(x) \wedge o(y))(o(x) \vee o(y)) = o(x)o(y) \quad \Longrightarrow \quad o(x) \vee o(y) | o(x)o(y)$$

et enfin $o(x)|n$ et $o(y)|m$. Ainsi, on a

$$nm = o(x, y) = o(x) \vee o(y) | o(x)o(y) | nm$$

d'où $o(x) \vee o(y) = o(x)o(y) = nm$ et $o(x) = n$, $o(y) = m$. Il en résulte que x et y sont des générateurs respectifs de G_1 et G_2 et les ordres n et m sont premiers entre eux. Réciproquement, supposons $n \wedge m = 1$. Alors, considérant x et y générateurs respectifs de G_1 et G_2, on a

$$o(x, y) = o(x) \vee o(y) = n \vee m = nm$$

ce qui prouve que $\mathrm{G}_1 \times \mathrm{G}_2$ est cyclique. On conclut

$$\boxed{\mathrm{G}_1 \times \mathrm{G}_2 \text{ cyclique} \iff \mathrm{Card}\ \mathrm{G}_1 \wedge \mathrm{Card}\ \mathrm{G}_2 = 1}$$

Exercice 4 (***)

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

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

Exercice 5 (***)

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 $x^2 y = y = x$ 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 $\mathrm{G} = \left\{x^k y^\ell, (k, \ell) \in \{0, 1\}^2\right\}$

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 6 (***)

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

Un groupe est fini si et seulement si l'ensemble de ses sous-groupes est fini.

Exercice 7 (****)

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

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

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 $n = m$.