Annales
corrigées et commentées

Concours 2020-2025

AGREG INTERNE

Les épreuves écrites de Maths

Adrien Fontaine
Alexandre Gélin
Axel Rogue

ellipses

1 | 2025 Épreuve 1 – Énoncé

Notations et rappels

On désigne par $\mathbb{N}$ l'ensemble des entiers naturels et par $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls. On désigne par $\mathbb{Z}$ l'anneau des entiers relatifs. On désigne respectivement par $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ les corps des nombres rationnels, des nombres réels et des nombres complexes. Pour k et n dans $\mathbb{Z}$ avec $k \leqslant n$, on désigne par $[\![k, n]\!]$ l'ensemble des entiers relatifs ℓ tels que $k \leqslant \ell \leqslant n$.

Pour $n \in \mathbb{N}^*$, on note $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$ le groupe multiplicatif des racines n-ièmes de l'unité dans $\mathbb{C}$. On rappelle qu'il s'agit d'un groupe cyclique d'ordre n. On dit que $z \in \mathbb{U}_n$ est une *racine primitive* n-ième de l'unité si z engendre le groupe $\mathbb{U}_n$.

Pour un corps $\mathbb{K}$ et un entier naturel non nul k, on note $\mathrm{GL}_k(\mathbb{K})$ le groupe des matrices inversibles de taille $k \times k$ et à coefficients dans $\mathbb{K}$. On désigne par I_k la matrice identité de taille k de $\mathrm{GL}_k(\mathbb{K})$. On note $\mathrm{O}_2(\mathbb{R})$ le groupe des matrices orthogonales de taille 2, c'est l'ensemble des matrices $M \in \mathcal{M}_2(\mathbb{R})$ telles que $M^T M = \mathrm{I}_2$, où M^T est la transposée de la matrice M.

Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ de caractéristique différente de 2. Pour u endomorphisme de E, le polynôme caractéristique de u est noté $\chi_u(X) = \det\left(X\,\mathrm{Id}_E - u\right)$ où Id_E est l'endomorphisme identité de E.

Définition 1. *Soient $\mathbb{K}$ un corps et k un entier naturel non nul. Soit $A \in \mathrm{GL}_k(\mathbb{K})$. On dira que A est d'*ordre fini *s'il existe $n \in \mathbb{N}^*$ tel que $A^n = \mathrm{I}_k$, son* ordre *est alors le plus petit entier naturel non nul r tel que $A^r = \mathrm{I}_k$.*

Ce sujet est formé de deux exercices préliminaires et de six parties. Son but est d'étudier les matrices d'ordre fini dans $\mathrm{GL}_k(\mathbb{K})$ pour les corps $\mathbb{K} = \mathbb{C}, \mathbb{R}$ et $\mathbb{Q}$, de déterminer les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$ et d'étudier un exemple dans $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ où p est un nombre premier.

Exercice préliminaire 1

Soient $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension finie. On considère un endomorphisme u de E. On désigne par $\mathbb{K}[X]$ la $\mathbb{K}$-algèbre des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$ et par $\mathrm{End}(E)$ *la $\mathbb{K}$-algèbre des endomorphismes de E.*

1. Montrer qu'il existe un unique morphisme de $\mathbb{K}$-algèbres $\theta_u : \mathbb{K}[X] \to \mathrm{End}(E)$ envoyant X sur u.

Pour tout polynôme $P \in \mathbb{K}[X]$, on note $P(u) = \theta_u(P)$. L'image de θ_u est notée $\mathbb{K}[u]$.

2. Montrer que le morphisme θ_u n'est pas injectif.
3. En déduire l'existence d'un unique polynôme unitaire $\mu_u \in \mathbb{K}[X]$ tel que pour tout polynôme $P \in \mathbb{K}[X]$, $\theta_u(P)$ est l'endomorphisme nul de E si et seulement si μ_u divise P.

Définition 2. *Ce polynôme μ_u est appelé le* polynôme minimal *de u.*

4. Soit d le degré de μ_u. Montrer que $\left(\mathrm{Id}_E, u, \dots, u^{d-1}\right)$ est une base de $\mathbb{K}[u]$.

On rappelle le théorème de Cayley-Hamilton :

Théorème 3. *Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension finie, alors μ_u divise χ_u.*

Exercice préliminaire 2

Définition 4. *L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui à tout entier naturel non nul n associe le cardinal des entiers $k \in [\![1, n]\!]$ premiers avec n est appelée* fonction indicatrice d'Euler.

5. Soit n un entier naturel non nul. Montrer que la valeur de $\varphi(n)$ est égale au nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
6. Montrer que si p est un nombre premier et $\alpha \in \mathbb{N}^*$, alors on a la relation $\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1}$.
7. Dans $\mathbb{N}^*$, résoudre l'inéquation $\varphi(n) \leqslant 2$.
   Indication : on pourra décomposer n en produit de nombres premiers ; on rappelle que si m et n sont deux entiers naturels non nuls premiers entre eux, alors on a l'égalité
   $$\varphi(mn) = \varphi(m)\varphi(n).$$

I. Décomposition de $X^n - 1$ en produit d'irréductibles

Dans toute cette partie, n désigne un entier naturel non nul. On note $\omega_n = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$.

8. Dans $\mathbb{C}[X]$, exprimer à l'aide de ω_n la décomposition du polynôme $X^n - 1$ en facteurs irréductibles. En déduire que $X^n - 1$ est à racines simples dans $\mathbb{C}$.
9. (a) Quelles sont, en fonction de n, les racines n-ièmes de l'unité appartenant à $\mathbb{R}$?
   (b) Soit θ un nombre réel non nul qui n'est pas de la forme $m\pi$ avec m un entier relatif. Justifier que le polynôme de $\mathbb{C}[X]$ de degré 2 donné par $P_\theta = \left(X - \mathrm{e}^{\mathrm{i}\theta}\right)\left(X - \mathrm{e}^{-\mathrm{i}\theta}\right)$ est un polynôme de $\mathbb{R}[X]$ qui est irréductible dont on donnera les coefficients.
   (c) En fonction de n, donner la décomposition en facteurs irréductibles du polynôme $X^n - 1$ dans $\mathbb{R}[X]$.
10. (a) Soit $m \in \mathbb{N}^*$. Démontrer que ω_n^m est une racine primitive n-ième de l'unité si et seulement si m et n sont premiers entre eux.
    (b) Montrer que le nombre de racines primitives n-ièmes de l'unité est $\varphi(n)$.

Définition 5. *Pour n entier naturel non nul, on note*

$$\Phi_n = \prod_{\substack{1 \leqslant m \leqslant n \\ m \wedge n = 1}} \left(X - \omega_n^m\right).$$

*Ce polynôme est appelé le n-*ième polynôme cyclotomique.

11. (a) Justifier que $\mathbb{U}_n = \bigcup_{d|n} \mathbb{A}_d$, où $\mathbb{A}_d$ désigne l'ensemble des racines primitives d-ièmes de l'unité. Montrer que cette union est disjointe. En déduire que
$$X^n - 1 = \prod_{d|n} \Phi_d.$$
(b) Déterminer Φ_n pour $1 \leqslant n \leqslant 6$.
(c) Soient $B \in \mathbb{Z}[X]$ un polynôme unitaire et $A \in \mathbb{Z}[X]$. Montrer qu'il existe $Q, R \in \mathbb{Z}[X]$ tels que $A = BQ + R$ avec $\deg R < \deg B$ ou $R = 0$.
Indication : on pourra faire une preuve par récurrence sur le degré de A.
(d) En déduire que pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

Dans la suite du sujet, on admet que pour tout $n \in \mathbb{N}^*$, le polynôme Φ_n est un polynôme irréductible de $\mathbb{Q}[X]$. La décomposition de $X^n - 1$ en facteurs irréductibles dans $\mathbb{Q}[X]$ est donc donnée par
$$X^n - 1 = \prod_{d|n} \Phi_d.$$

II. Un lemme sur les matrices d'ordre fini

Dans cette partie, $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. On considère une matrice $A \in \mathrm{GL}_k(\mathbb{K})$ d'ordre fini ; son ordre est noté r.

12. Montrer que A est diagonalisable sur $\mathbb{C}$ et que ses valeurs propres sont des racines de l'unité.
13. Montrer que le polynôme minimal μ_A de A s'écrit sous la forme $\mu_A = P_1 \cdots P_q$, où les P_j sont des polynômes irréductibles unitaires de $\mathbb{K}[X]$ deux à deux distincts.

III. Endomorphismes cycliques et décomposition de Frobenius

Dans cette partie, on fixe un corps $\mathbb{K}$, un $\mathbb{K}$-espace vectoriel E de dimension finie $k \geqslant 1$ et u un endomorphisme de E. On note
$$\mu_u = P_1^{m_1} \cdots P_q^{m_q}$$
la décomposition en facteurs irréductibles du polynôme minimal de u dans $\mathbb{K}[X]$; les P_i sont des polynômes irréductibles unitaires de $\mathbb{K}[X]$ deux à deux distincts et les m_i sont des entiers naturels non nuls.

Définition 6. *On associe à tout polynôme unitaire P, de degré n et noté*
$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$
de $\mathbb{K}[X]$, sa matrice compagnon définie par
$$C_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

14. Soit P un polynôme unitaire de $\mathbb{K}[X]$. Démontrer que le polynôme caractéristique de C_P est égal à P.
Indication : on pourra procéder par récurrence sur l'entier $n \geqslant 1$.

15. Soit $x \in E$. On note
$$I_x = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0\}.$$
(a) Justifier qu'il existe un unique polynôme unitaire μ_x de $\mathbb{K}[X]$ tel que $I_x = \mu_x \mathbb{K}[X]$ et que l'on a $\mu_x \mid \mu_u$.
(b) Justifier que $E = \bigoplus_{i=1}^{q} \operatorname{Ker}\left(P_i^{m_i}(u)\right)$ et que les sous-espaces $N_i = \operatorname{Ker}\left(P_i^{m_i}(u)\right)$ sont stables par u.
(c) Pour tout $i \in [\![1, q]\!]$, on note u_i l'endomorphisme induit par u sur N_i. Montrer que
$$\mu_{u_i} = P_i^{m_i}.$$
En déduire qu'il existe $x_i \in E$ tel que $\mu_{x_i} = \mu_{u_i}$, puis qu'il existe $x \in E$ tel que $\mu_x = \mu_u$.

Définition 7. *Soit u un endomorphisme de E. On dit que u est* cyclique *s'il existe un vecteur $x_0 \in E$ tel que la famille $\left(x_0, u(x_0), \ldots, u^{k-1}(x_0)\right)$ soit une base de E.*

16. Soit u un endomorphisme de E. Montrer que les énoncés suivants sont équivalents :
i) L'endomorphisme u est cyclique.
ii) Il existe une base $\mathcal{B}$ de E telle que $\operatorname{Mat}_{\mathcal{B}}(u)$ soit la matrice compagnon d'un certain polynôme.
iii) $\chi_u = \mu_u$.

17. Soit u un endomorphisme cyclique de E. On note $\operatorname{Com}(u) = \{v \in \operatorname{End}(E) \mid v \circ u = u \circ v\}$ l'ensemble des endomorphismes qui commutent avec u. Justifier que $\operatorname{Com}(u) = \mathbb{K}[u]$.

18. *Dans cette question, on suppose que μ_u est irréductible sur $\mathbb{K}$.* Pour $x \in E$, on note
$$E_x = \{P(u)(x) \mid P \in \mathbb{K}[X]\}.$$
(a) Montrer que E_x est stable par u pour tout x dans E. Montrer que si x est non nul, l'endomorphisme v induit par u sur E_x est cyclique, de polynôme minimal égal à μ_u. En déduire la dimension de E_x.
(b) Soient F un sous-espace de E stable par u et $x \in E$. Montrer que $E_x \subseteq F$ ou $E_x \cap F = \{0\}$.
(c) Montrer qu'il existe des vecteurs $x_1, \ldots, x_p$ de E tels que
$$E = \bigoplus_{i=1}^{p} E_{x_i}.$$

19. *Dans cette question, on suppose que μ_u est sans facteurs carrés, c'est-à-dire que sa décomposition en produit de polynômes irréductibles unitaires est de la forme $\mu_u = P_1 \cdots P_q$ où les P_i sont 2 à 2 distincts.*
(a) Déduire de la question précédente qu'il existe des vecteurs $x_1, \ldots, x_p$ de E tels que
$$E = \bigoplus_{i=1}^{p} E_{x_i},$$
puis qu'il existe une base $\mathcal{B}$ de E telle que la matrice de u dans $\mathcal{B}$ est diagonale par blocs

de la forme

$$\mathrm{Diag}\big(C_{P_1},\dots,C_{P_1},\dots,C_{P_q},\dots,C_{P_q}\big),$$

où chaque bloc C_{P_j} est présent un certain nombre de fois, noté ℓ_j.

(b) Montrer que $\chi_u = P_1^{\ell_1}\cdots P_q^{\ell_q}$.

IV. Matrices complexes ou réelles d'ordre fini

20. *Dans cette question, on prend $\mathbb{K}=\mathbb{C}$ et $A\in \mathrm{GL}_k(\mathbb{C})$ est une matrice d'ordre fini. Par conséquent, il existe un entier n de $\mathbb{N}^*$ tel que $A^n = \mathrm{I}_k$.*

(a) Justifier que A est diagonalisable et que ses valeurs propres sont des racines n-ièmes de l'unité.

(b) On note $\lambda_1,\dots,\lambda_k$ les valeurs propres de A et pour $j\in[\![1,k]\!]$, on note n_j l'ordre de λ_j dans le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité. Exprimer l'ordre de A dans le groupe $\mathrm{GL}_k(\mathbb{K})$ en fonction des n_j.

(c) Montrer que pour tout $r\in\mathbb{N}^*$, il existe une matrice $A_r\in\mathrm{GL}_k(\mathbb{C})$ d'ordre exactement r.

Définition 8. *Pour $\theta\in\mathbb{R}$, on note $R_\theta = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\in\mathrm{GL}_2(\mathbb{R})$ la matrice de la rotation plane d'angle θ.*

21. Dans le cas où θ n'est pas congru à 0 modulo π, déterminer le polynôme minimal de R_θ et en déduire que R_θ est semblable à $\begin{pmatrix}0 & -1\\ 1 & 2\cos\theta\end{pmatrix}$.

22. Soit $A\in\mathrm{GL}_k(\mathbb{R})$ une matrice d'ordre fini. Justifier que le polynôme minimal μ_A de A est de la forme

$$\mu_A = (X-1)^{\varepsilon_1}(X+1)^{\varepsilon_2}P_{\theta_1}\cdots P_{\theta_q}$$

où ε_1 et ε_2 sont des éléments de $\{0,1\}$, $P_{\theta_j}=X^2-2\cos(\theta_j)X+1$ et les θ_j sont des éléments de $2\pi\mathbb{Q}\setminus\pi\mathbb{Z}$ qui sont deux à deux distincts.

23. Soit $A\in\mathrm{GL}_k(\mathbb{R})$. Montrer que A est d'ordre fini si et seulement si A est semblable à une matrice diagonale par blocs de la forme

$$\mathrm{Diag}\big(\mathrm{I}_{k_1},-\mathrm{I}_{k_2},R_{\theta_1},\dots,R_{\theta_1},\dots,R_{\theta_q},\dots,R_{\theta_q}\big),$$

où chaque bloc R_{θ_j} apparaît ℓ_j fois, avec $k=k_1+k_2+2(\ell_1+\cdots+\ell_q)$ et les θ_j sont des éléments de $2\pi\mathbb{Q}\setminus\pi\mathbb{Z}$ qui sont deux à deux distincts. Certains blocs peuvent ne pas apparaître dans cette écriture.

24. Soit $A\in\mathrm{GL}_k(\mathbb{R})$ une matrice d'ordre fini. En gardant les notations de la question précédente, et en écrivant $\theta_j = 2\pi\dfrac{a_j}{b_j}$ où a_j et b_j sont premiers entre eux, exprimer l'ordre de A en fonction des b_j.

Indication : on pourra distinguer les cas $k_2>0$ et $k_2=0$.

25. On considère le cas $k = 2$. Montrer que A est d'ordre fini si et seulement si A est semblable à $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ ou à une matrice R_θ avec $\theta \in 2\pi\mathbb{Q}$.
26. Montrer que pour tout $r \in \mathbb{N}^*$, il existe une matrice de $\mathrm{GL}_2(\mathbb{R})$ d'ordre exactement r.
27. Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$.
    (a) Pour u et v des éléments de $\mathbb{R}^2$, on pose
    $$\big(u, v\big)_G = \frac{1}{|G|}\sum_{A\in G}\langle Au, Av\rangle,$$
    où $\langle\cdot,\cdot\rangle$ désigne le produit scalaire canonique de $\mathbb{R}^2$. Montrer que $\big(\cdot,\cdot\big)_G$ est un produit scalaire sur $\mathbb{R}^2$ et que pour tout u et v de $\mathbb{R}^2$ et pour tout A de G, on a $\big(u, v\big)_G = \big(Au, Av\big)_G$.
    (b) On note S l'élément de $\mathcal{M}_2(\mathbb{R})$ qui est la matrice du produit scalaire $\big(\cdot,\cdot\big)_G$ dans la base canonique de $\mathbb{R}^2$. Justifier qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ telle que $S = P^TP$, puis montrer que pour tout $A \in G$, on a $PAP^{-1} \in \mathrm{O}_2(\mathbb{R})$.

Ainsi, le sous-groupe G est conjugué — en conséquence isomorphe — à un sous-groupe de $\mathrm{O}_2(\mathbb{R})$.

28. On note $\mathrm{SO}_2(\mathbb{R})$ le sous-groupe de $\mathrm{O}_2(\mathbb{R})$ constitué des matrices de déterminant 1, qui sont les matrices de rotation plane. Montrer que si G est un sous-groupe fini d'ordre n de $\mathrm{SO}_2(\mathbb{R})$, alors G est un groupe cyclique, engendré par la matrice $R_{\frac{2\pi}{n}}$.
29. Soit n un entier naturel non nul. On considère le sous-groupe D_n de $\mathrm{O}_2(\mathbb{R})$ engendré par les matrices
    $$A = R_{\frac{2\pi}{n}} = \begin{pmatrix}\cos\left(\dfrac{2\pi}{n}\right) & -\sin\left(\dfrac{2\pi}{n}\right)\\ \sin\left(\dfrac{2\pi}{n}\right) & \cos\left(\dfrac{2\pi}{n}\right)\end{pmatrix}, \qquad B = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$
    Montrer que l'on a
    $$D_n = \big\{\mathrm{I}_2, A, \ldots, A^{n-1}, B, BA, \ldots, BA^{n-1}\big\}.$$
    Indication : on pourra d'abord montrer que $AB = BA^{-1}$.

Définition 9. *Ce groupe D_n est appelé n-*ième groupe diédral.

30. *Dans cette question, G est un sous-groupe fini de* $\mathrm{O}_2(\mathbb{R})$ *non inclus dans* $\mathrm{SO}_2(\mathbb{R})$.
    (a) Montrer que $G \cap \mathrm{SO}_2(\mathbb{R})$ est un sous-groupe d'indice 2 de G.
    (b) Montrer que G contient une matrice de la forme
    $$S_\theta = \begin{pmatrix}\cos(\theta) & \sin(\theta)\\ \sin(\theta) & -\cos(\theta)\end{pmatrix},$$
    où θ est un nombre réel.
    (c) Montrer qu'il existe $P \in \mathrm{SO}_2(\mathbb{R})$ telle que $P^{-1}S_\theta P = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.
    (d) En déduire qu'il existe un entier n tel que G est conjugué dans $\mathrm{SO}_2(\mathbb{R})$ au groupe diédral D_n.

Ainsi, tout sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$ *est isomorphe, soit à un groupe cyclique* $\mathbb{Z}/n\mathbb{Z}$*, soit à un groupe diédral D_n.*

V. Matrices rationnelles d'ordre fini

31. Soit $A \in \mathrm{GL}_k(\mathbb{Q})$ une matrice d'ordre fini. Par conséquent, il existe un entier n de $\mathbb{N}^*$ tel que $A^n = \mathrm{I}_k$. Justifier que le polynôme minimal μ_A de A est de la forme

$$\mu_A = \Phi_{d_1} \cdots \Phi_{d_q}$$

où $q \geqslant 1$ et les d_i sont des entiers 2 à 2 distincts qui divisent n.

32. Justifier que A est semblable à une matrice diagonale par blocs de la forme

$$\mathrm{Diag}\big(C_{\Phi_{d_1}}, \ldots, C_{\Phi_{d_1}}, \ldots, C_{\Phi_{d_q}}, \ldots, C_{\Phi_{d_q}}\big),$$

où chaque bloc $C_{\Phi_{d_j}}$ est présent ℓ_j fois, avec ℓ_j la multiplicité de Φ_{d_j} dans le polynôme caractéristique de A.

33. (a) Justifier que pour tout entier naturel non nul d, l'ordre de la matrice C_{Φ_d} dans le groupe multiplicatif $\mathrm{GL}_k(\mathbb{Q})$ est d.

(b) En déduire que $A \in \mathrm{GL}_k(\mathbb{Q})$ est d'ordre fini si et seulement si A est semblable à une matrice de la forme

$$\mathrm{Diag}\big(C_{\Phi_{d_1}}, \ldots, C_{\Phi_{d_1}}, \ldots, C_{\Phi_{d_q}}, \ldots, C_{\Phi_{d_q}}\big),$$

où chaque bloc $C_{\Phi_{d_j}}$ est présent ℓ_j fois et $\ell_1\varphi(d_1) + \cdots + \ell_q\varphi(d_q) = k$.

(c) Lorsque $A \in \mathrm{GL}_k(\mathbb{Q})$ est d'ordre fini, exprimer son ordre en fonction des entiers d_j.

(d) On prend $k = 4$. Exhiber une matrice $A \in \mathrm{GL}_4(\mathbb{Q})$ d'ordre 12.

(e) Montrer que l'ordre maximal d'une matrice A de $\mathrm{GL}_k(\mathbb{Q})$ est inférieur ou égal à

$$\mathrm{PPCM}\big\{m,\ \varphi(m) \leqslant k\big\}.$$

34. *Dans cette question, on fixe $k = 2$.*

(a) Montrer que $A \in \mathrm{GL}_2(\mathbb{Q})$ est d'ordre fini si et seulement si A est semblable à l'une des 6 matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

On précisera l'ordre de chacune de ces matrices.

(b) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$. En s'appuyant sur les résultats de la quatrième partie, montrer que G est isomorphe à l'un des groupes suivants :

$$\{\mathrm{I}_2\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad D_2, \quad D_3, \quad D_4, \quad D_6.$$

VI. Matrices d'ordre fini dans $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$

Dans cette partie, on fixe un nombre premier p et on considère le groupe $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$. On rappelle que l'on peut faire agir le groupe $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ sur lui-même par conjugaison en posant $P\cdot M = PMP^{-1}$; ainsi, l'orbite $\mathcal{O}_M$ de M est alors sa classe de similitude et son stabilisateur est

$$\mathrm{Stab}(M) = \left\{P \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right) \;\middle|\; PMP^{-1} = M\right\}.$$

On a alors l'égalité de cardinaux

$$\frac{\left|\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)\right|}{|\mathrm{Stab}(M)|} = |\mathcal{O}_M|.$$

35. Déterminer le cardinal de $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$.

36. Soit $M \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$. Justifier que l'algèbre $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$ des polynômes en M à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ est de cardinal 1, p ou p^2.

37. En déduire que l'ordre de toute matrice de $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ est majoré par p^2-1.

38. Soit $M \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$. *On suppose dans cette question que le polynôme minimal de M est de degré* 2.
    (a) Justifier que $\mathrm{Stab}(M) = \left(\mathbb{Z}/p\mathbb{Z}\right)[M] \cap \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$.
    (b) Montrer que si $M \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ n'admet pas de valeur propre dans $\mathbb{Z}/p\mathbb{Z}$, alors on a l'égalité $|\mathrm{Stab}(M)| = p^2-1$.
    (c) Montrer que si M admet une unique valeur propre dans $\mathbb{Z}/p\mathbb{Z}$, alors on a
    $$|\mathrm{Stab}(M)| = p^2 - p.$$

À partir de maintenant et jusqu'à la fin du sujet, on prend $p=3$ et on détermine les ordres des éléments de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$, ainsi que le nombre de matrices ayant un ordre donné.

39. Justifier que les ordres possibles pour une matrice de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ sont 1, 2, 3, 4, 6 et 8.

40. *Éléments d'ordre* 6.
    (a) Justifier que le polynôme X^6-1 est scindé dans $\mathbb{Z}/3\mathbb{Z}$.
    (b) En déduire que $M \in \mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ est d'ordre 6 si et seulement si M est semblable à $\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$.
    (c) Dénombrer les matrices d'ordre 6.

41. *Éléments d'ordre* 3. Adapter la méthode de la question précédente.

42. *Éléments d'ordre* 8.
    (a) Montrer que la décomposition en facteurs irréductibles de X^8-1 dans $\left(\mathbb{Z}/3\mathbb{Z}\right)[X]$ est
    $$X^8-1 = (X-1)(X+1)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

(b) En déduire une condition nécessaire et suffisante sur le polynôme minimal d'une matrice de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ pour qu'elle soit d'ordre 8.

(c) Exhiber alors une matrice $M \in \mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ d'ordre 8.

(d) Dénombrer les matrices d'ordre 8.

43. *Éléments d'ordre* 4. Adapter la méthode de la question précédente.

44. *Éléments d'ordre* 2.

(a) Justifier qu'une matrice d'ordre 2 autre que $-\mathrm{I}_2$ est semblable à $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(b) Déterminer $|\mathrm{Stab}(M)|$ et en déduire le nombre d'éléments d'ordre 2 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

——— FIN DU SUJET ———

1 | 2025 Épreuve 1 – Corrigé

Exercice préliminaire 1

1. On suppose qu'il existe un morphisme d'algèbres θ_u de $\mathbb{K}[X]$ vers $\mathrm{End}(E)$ tel que $\theta_u(X) = u$.
   Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ où $d \in \mathbb{N}$ et $a_0, \dots, a_d \in \mathbb{K}$. Alors, par définition d'un morphisme d'algèbres, on a
   $$\theta_u(P) = \theta_u\left(\sum_{k=0}^{d} a_k X^k\right) = \sum_{k=0}^{d} a_k \theta_u\big(X^k\big) = \sum_{k=0}^{d} a_k \big(\theta_u(X)\big)^k = \sum_{k=0}^{d} a_k u^k.$$
   Il n'y a qu'une seule image possible pour chaque $P \in \mathbb{K}[X]$, ce qui prouve (sous réserve d'existence) l'unicité de θ_u.
   Réciproquement, pour tout polynôme $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$ avec $d \in \mathbb{N}$ et $a_0, \dots, a_d \in \mathbb{K}$, on pose $\theta_u(P) = \sum_{k=0}^{d} a_k u^k$. On vérifie que cela définit un morphisme d'algèbres de $\mathbb{K}[X]$ dans $\mathrm{End}(E)$.
   - Tout d'abord, $\mathrm{End}(E)$ étant une algèbre, θ_u est bien à valeurs dans $\mathrm{End}(E)$.
   - $\theta_u(1) = u^0 = \mathrm{Id}_E$.
   - Pour tous polynômes $P, Q \in \mathbb{K}[X]$ et tout $\lambda \in \mathbb{K}$, en prenant d un entier supérieur à $\deg(P)$ et à $\deg(Q)$ et en notant $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{k=0}^{d} b_k X^k$ avec $a_0, b_0, \dots, a_d, b_d \in \mathbb{K}$, on a
     $$\theta_u\big(\lambda P + Q\big) = \sum_{k=0}^{d} \big(\lambda a_k + b_k\big) u^k = \lambda \sum_{k=0}^{d} a_k u^k + \sum_{k=0}^{d} b_k u^k = \lambda \theta_u(P) + \theta_u(Q).$$
   - Avec les mêmes notations,
     $$\theta_u\big(PQ\big) = \sum_{k=0}^{d} \left(\sum_{j=0}^{d} a_k b_j u^{k+j} \right) = \sum_{k=0}^{d} \left(\sum_{j=0}^{d} a_k u^k \circ b_j u^j \right) = \left(\sum_{k=0}^{d} a_k u^k \right) \circ \left(\sum_{j=0}^{d} b_j u^j \right),$$
     donc $\theta_u\big(PQ\big) = \theta_u(P) \circ \theta_u(Q)$.

   Ceci achève de démontrer que θ_u est un morphisme d'algèbres. Par définition, $\theta_u(X) = u$. On a donc bien existence et unicité de θ_u.

Commentaire

Dans ces questions où l'on cherche à prouver existence et unicité, il est très souvent pertinent de commencer par l'unicité, car lors du raisonnement par analyse-synthèse, la démonstration de l'unicité va permettre de trouver l'expression de l'objet recherché et il n'y a ensuite plus qu'à vérifier que cette expression convient pour justifier l'existence.

Commentaire

Le fait que pour une $\mathbb{K}$-algèbre B et $b \in B$, il existe un unique morphisme φ_b d'algèbre de $\mathbb{K}[X]$ vers B vérifiant $\varphi_b(X) = b$ est un résultat classique, conséquence de la propriété universelle des algèbres. On appelle φ_b le *morphisme d'évaluation* en b.
Il ne s'agit cependant pas d'un résultat trivial et puisqu'il s'agit d'une question visiblement typée « question de cours », il faut ici détailler le raisonnement pour mettre le correcteur en confiance dès la première question.

2. Puisque θ_u est un morphisme d'algèbres, c'est en particulier une application $\mathbb{K}$-linéaire. Or $\mathbb{K}[X]$ est un $\mathbb{K}$-espace vectoriel de dimension infinie, alors que $\mathrm{End}(E)$ est de dimension finie, à savoir $\dim(E)^2$, E étant de dimension finie. Donc θ_u n'est pas injective.
3. Comme θ_u est un morphisme d'algèbres, c'est en particulier un morphisme d'anneaux.

Commentaire

Le noyau de tout morphisme d'anneaux est un idéal de l'anneau de départ.
On rappelle ci-après la définition d'un idéal et de deux types d'idéaux particuliers.

- ⋆ Dans un anneau commutatif unitaire A, on dit qu'une partie I de A est un idéal si :
  - (i) $(I,+)$ est un sous-groupe de $(A,+)$,
  - (ii) pour tout $x \in I$ et tout $a \in A$, $a \cdot x \in I$.
- ⋆ Un idéal I est dit
  - *premier* si $I \neq A$ et que pour tout $x, y \in A$, $x \cdot y \in I \implies x \in I$ ou $y \in I$.
  - *principal* s'il existe $x \in I$ tel que $I = xA = \{x \cdot a \mid a \in A\}$.

Le noyau de θ_u constitue donc un idéal de $\mathbb{K}[X]$. Or $\mathbb{K}[X]$ est un anneau principal, à savoir que chacun de ses idéaux peut-être engendré par un seul élément. On note $P_u \in \mathbb{K}[X]$ l'élément tel que $\mathrm{Ker}(\theta_u) = P_u\mathbb{K}[X]$. Alors P_u n'est pas nul, sans quoi le noyau de θ_u serait réduit à $\{0_{\mathbb{K}[X]}\}$ et l'application θ_u serait injective, ce qui est impossible d'après la question précédente. En divisant P_u par son coefficient dominant, ce qui est possible car $\mathbb{K}$ est un corps, on obtient un polynôme μ_u unitaire tel que $\mathrm{Ker}(\theta_u) = \mu_u\mathbb{K}[X]$, et pour tout $P \in \mathbb{K}[X]$,

$$\theta_u(P) = 0 \iff P \in \mathrm{Ker}(\theta_u) \iff P \in \mu_u\mathbb{K}[X] \iff \mu_u \text{ divise } P.$$

Il reste à justifier l'unicité de μ_u. On suppose qu'il existe un autre $Q_u \in \mathbb{K}[X]$ unitaire tel que pour tout polynôme $P \in \mathbb{K}[X]$, on ait $\theta_u(P) = 0$ si et seulement si Q_u divise P. On a alors en particulier que Q_u divise μ_u et que μ_u divise Q_u, ce qui implique que $\deg(Q_u) = \deg(\mu_u)$ et donc qu'il existe $\lambda \in \mathbb{K}$ tel que $Q_u = \lambda\mu_u$. En observant que les coefficients dominants de Q_u et de μ_u sont égaux à 1, on obtient $\lambda = 1$ et donc $Q_u = \mu_u$. D'où l'unicité de μ_u.

4. Si u est l'endomorphisme nul, alors l'algèbre $\mathbb{K}[u]$ est réduite à l'endomorphisme nul, le polynôme minimal de u est 1, de degré 0, et la famille vide est bien une base de $\mathbb{K}[u]$.
Si u n'est pas l'endomorphisme nul, on commence par remarquer que comme les polynômes constants non nuls ne sont pas annulateurs de u, alors $\deg(\mu_u) \geqslant 1$.
On montre que la famille $\left(\mathrm{Id}_E, u, \ldots, u^{d-1}\right)$ est libre.

Soient $\lambda_0,\dots,\lambda_{d-1}\in\mathbb{K}$ tels que $\sum_{k=0}^{d-1}\lambda_k u^k=0$. Autrement dit, en notant $P=\sum_{k=0}^{d-1}\lambda_k X_k$, on obtient que $\theta_u(P)=0$. D'après la question précédente, μ_u divise alors P. Or P est de degré strictement inférieur à μ_u, ce qui implique que $P=0$, et donc que $\lambda_0=\cdots=\lambda_{d-1}=0$.
La famille $\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ est donc libre.

Soient $P\in\mathbb{K}[X]$ et $w=P(u)$. On note respectivement Q et R le quotient et le reste de la division euclidienne de P par μ_u. On a alors

$$w=P(u)=Q(u)\circ\mu_u(u)+R(u)=Q(u)\circ 0_{\mathbb{K}[u]}+R(u)=R(u).$$

Comme $\deg(R)<\deg(\mu_u)=d$, alors $R(u)\in\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$. On en déduit ainsi que $w\in\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ et donc $\mathbb{K}[u]\subset\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$. L'inclusion réciproque est évidente, donc $\mathbb{K}[u]=\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ et $\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ est génératrice de $\mathbb{K}[u]$.
Finalement, on a bien montré que $\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ est une base de $\mathbb{K}[u]$.

Commentaire

Pour montrer le caractère générateur, on peut aussi procéder par récurrence forte en montrant que $\forall n\in\mathbb{N},\ u^n\in\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$.
Le résultat est évident pour $n\in[\![0,d-1]\!]$.
Soit $n\in\mathbb{N}$ tel que pour tout $k\in[\![0,n]\!]$, on ait $u^k\in\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$.
D'après la question précédente, $\theta_u\left(X^{n+1-d}\mu_u\right)=0$, *i.e.* $u^{n+1-d}\mu_u(u)=0$.
Comme μ_u est de degré d, le polynôme $X^{n+1-d}\mu_u$ est de degré $n+1$ et on en déduit que u^{n+1} est une combinaison linéaire de $u^0,\dots,u^n$, qui sont dans $\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$ par hypothèse de récurrence. Donc $u^{n+1}\in\mathrm{Vect}\left(\mathrm{Id}_E,u,\dots,u^{d-1}\right)$.
Ceci termine la preuve de l'hérédité et on conclut comme précédemment.

Commentaire

L'énoncé rappelle à ce moment le théorème de Cayley-Hamilton. On en profite pour mentionner les autres résultats fondamentaux de réduction concernant le polynôme minimal :

- ⋆ Les valeurs propres sont exactement les racines du polynôme minimal. Autrement dit, le polynôme caractéristique et le polynôme minimal ont les mêmes racines.
- ⋆ Un endomorphisme (ou sa matrice) est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples.
- ⋆ Un endomorphisme (ou sa matrice) est trigonalisable si et seulement si son polynôme minimal est scindé. C'est toujours le cas lorsque le corps de base est algébriquement clos, comme $\mathbb{C}$.

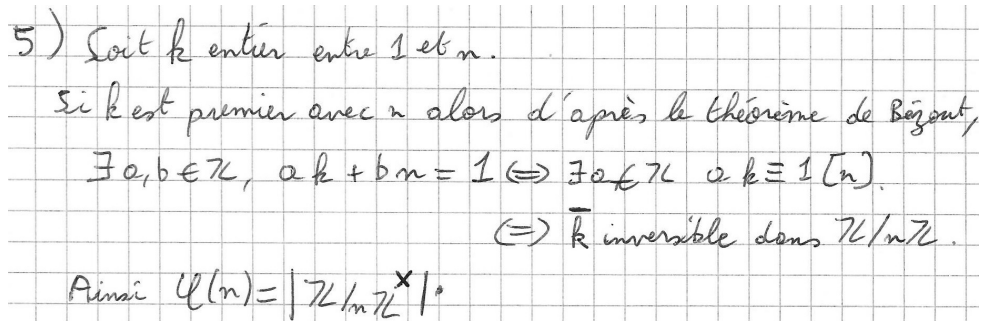
Exercice préliminaire 2

5. Soit $k\in[\![1,n]\!]$. Alors, en utilisant le théorème de Bézout,

$$\begin{aligned} k \text{ est premier avec } n &\iff \text{il existe } a,b\in\mathbb{Z} \text{ tels que } ak+bn=1\\ &\iff \text{il existe } a\in\mathbb{Z} \text{ tel que } ak\equiv 1\ [n]\\ &\iff \text{la classe de } k \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

Comme l'intervalle d'entiers $[\![1,n]\!]$ fournit exactement un représentant de chaque classe de $\mathbb{Z}/n\mathbb{Z}$, alors il y a autant d'inversibles de $\mathbb{Z}/n\mathbb{Z}$ que d'entiers de $[\![1,n]\!]$ premiers avec n, et donc la valeur de $\varphi(n)$ est bien égale au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Analyse d'un extrait de copie



L'idée est comprise mais la rédaction souffre de plusieurs problèmes :

- ⋆ L'enchaînement « si ... alors ... $\iff$ ... » est une erreur de logique, en plus d'être grammaticalement incorrect. Si l'on souhaite raisonner par équivalences, on ne doit pas commencer par une supposition.
- ⋆ L'argument manquant, à savoir que $[\![1,n]\!]$ fournit exactement un représentant de chaque classe de $\mathbb{Z}/n\mathbb{Z}$, est important. L'équivalence serait aussi vraie pour $k \in [\![1,42n]\!]$, mais on ne pourrait pas en déduire $\varphi(n)$.

On peut en revanche remarquer l'usage pertinent de la notation $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ pour désigner le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

6. Soient p un nombre premier et $\alpha \in \mathbb{N}^*$. Les entiers de $[\![1,p^\alpha]\!]$ qui ne sont pas premiers avec p^α sont ceux qui ont un facteur premier commun avec p^α, c'est-à-dire ceux qui sont multiples de p puisque p est premier. Il y a ainsi $\dfrac{p^\alpha}{p} = p^{\alpha-1}$ entiers de $[\![1,p^\alpha]\!]$ qui ne sont pas premiers avec p^α, et donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
7. On commence par traiter le cas $n=1$: on remarque que $\varphi(1)=1$. Puis pour tout entier $n \geqslant 2$, d'après le théorème de décomposition en facteurs premiers, il existe $r \in \mathbb{N}^*$, des nombres premiers distincts $p_1,\dots,p_r$ et des entiers strictement positifs $\alpha_1,\dots,\alpha_r$ tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
   Comme les p_i sont deux à deux distincts, les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux et on en déduit par multiplicativité de la fonction φ que
   $$\varphi(n) = \varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}).$$
   Il s'agit d'un produit d'entiers strictement positifs. Ainsi $\varphi(n) \leqslant 2$ si et seulement si pour tout $i \in [\![1,r]\!]$, $\varphi(p_i^{\alpha_i}) = 1$, sauf éventuellement un des facteurs qui vaut 2.
   Selon la question précédente, pour tout $i \in [\![1,r]\!]$, on a $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1} = p_i^{\alpha_i-1}(p_i-1)$.
   On résout alors $\varphi(p^\alpha) = 1$, *i.e.* $p^{\alpha-1}(p-1) = 1$. Comme $p \geqslant 2$, alors $\alpha - 1 = 0$, *i.e.* $\alpha = 1$. Et $p-1=1 \implies p=2$. Finalement, comme $\varphi(2)=1$, alors on obtient $\varphi(p^\alpha) = 1 \iff p^\alpha = 2$.

On résout ensuite $\varphi(p^\alpha) = 2$, *i.e.* $p^{\alpha-1}(p-1) = 2$. Deux possibilités :

- Si $p-1 = 2$, *i.e.* $p = 3$, alors $\alpha - 1 = 0$, *i.e.* $\alpha = 1$, et finalement $p^\alpha = 3$.
- Si $p-1 = 1$, *i.e.* $p = 2$, alors $\alpha - 1 = 1$, *i.e.* $\alpha = 2$, et finalement $p^\alpha = 2^2 = 4$.

Finalement, comme $\varphi(3) = \varphi(4) = 2$, alors on obtient $\varphi(p^\alpha) = 2 \iff p^\alpha = 3$ ou $p^\alpha = 4$.

En conclusion, 1 est solution triviale de $\varphi(n) \leqslant 2$, les solutions de la forme p^α sont 2, 3 et 4, et la seule autre solution que l'on peut reconstruire par multiplicativité, avec $n = p_1^{\alpha_1} p_2^{\alpha_2}$ où $p_1^{\alpha_1}$ et $p_2^{\alpha_2}$ sont premiers entre eux et tels que $\varphi(p_1^{\alpha_1}) = 1$ et $\varphi(p_2^{\alpha_2}) = 2$ est $n = 2 \times 3 = 6$.

Finalement l'ensemble des solutions de l'inéquation $\varphi(n) \leqslant 2$ est donné par $\{1, 2, 3, 4, 6\}$.

I. Décomposition de $X^n - 1$ en produit d'irréductibles

8. Pour $k \in [\![1, n]\!]$, on a $\omega_n^k = \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$ et les complexes obtenus sont deux à deux distincts puisque leurs arguments sont des éléments deux à deux distincts de $]0, 2\pi]$. Or ω_n^k est une racine n-ième de l'unité, donc $X - \omega_n^k$ est un facteur irréductible (car de degré 1) de $X^n - 1$. Cela donne n facteurs irréductibles distincts de degré 1 de $X^n - 1$, polynôme unitaire de degré n.

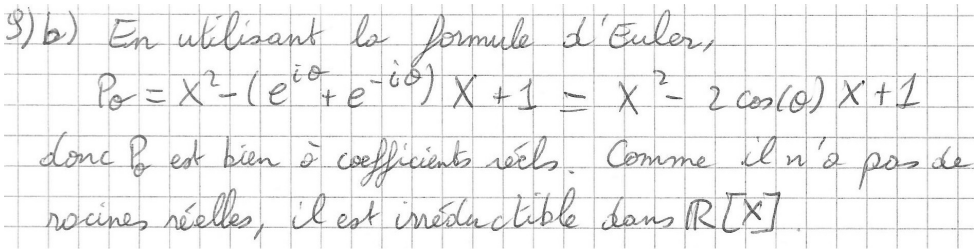
   On a donc trouvé tous les facteurs irréductibles de $X^n - 1$ et finalement $X^n - 1 = \prod_{k=1}^{n} (X - \omega_n^k)$.

   Ainsi $X^n - 1$ possède n racines distinctes, toutes de multiplicité 1, il est bien à racines simples dans $\mathbb{C}$.

9. (a) Dans $\mathbb{R}$, il y a deux racines n-ièmes de l'unité si n est pair (1 et -1) et une seule si n est impair, à savoir 1.

   (b) On remarque grâce à la formule d'Euler que
   $$P_\theta = X^2 - \left(\mathrm{e}^{\mathrm{i}\theta} + \mathrm{e}^{-\mathrm{i}\theta}\right) X + \mathrm{e}^{\mathrm{i}\theta}\,\mathrm{e}^{-\mathrm{i}\theta} = X^2 - 2\cos(\theta) X + 1.$$
   P_θ est bien dans $\mathbb{R}[X]$. Comme θ n'est pas multiple de π, $\mathrm{e}^{\mathrm{i}\theta}$ et $\mathrm{e}^{-\mathrm{i}\theta}$ ne sont pas réels. P_θ est donc un polynôme réel de degré 2 sans racines réelles, ce qui justifie bien qu'il est irréductible.

Analyse d'un extrait de copie



L'irréductibilité du polynôme n'est pas bien justifiée par le candidat pour deux raisons :

- ⋆ Il faut rappeler que θ n'est pas multiple de π pour bien justifier que les racines ne sont pas réelles.
- ⋆ Le fait que P_θ soit de degré 2 est crucial. En effet, un polynôme de degré 3 ou plus sans racine réelle n'est jamais irréductible dans $\mathbb{R}[X]$. Par exemple, $X^4 + X^3 + 3X^2 + X + 2$ n'a pas de racines réelles, mais se factorise en $(X^2 + 1)(X^2 + X + 2)$.

(c) Si n est impair, en posant $r = \dfrac{n-1}{2}$, on a grâce à la question **8** et au changement d'indice $j = n-k$ dans le second produit, que

$$\begin{aligned} X^n - 1 &= \left(\prod_{k=1}^{r}\left(X-\omega_n^k\right)\right)\left(\prod_{k=r+1}^{n-1}\left(X-\omega_n^k\right)\right)\left(X-\omega_n^n\right) \\ &= (X-1)\left(\prod_{k=1}^{r}\left(X-\omega_n^k\right)\right)\left(\prod_{j=1}^{r}\left(X-\omega_n^{-j}\right)\right) = (X-1)\prod_{k=1}^{r}\left(X-\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}\right)\left(X-\mathrm{e}^{-\frac{2\mathrm{i}k\pi}{n}}\right) \\ &= (X-1)\prod_{k=1}^{r}\left(X^2-2\cos\left(\frac{2k\pi}{n}\right)X+1\right). \end{aligned}$$

Pour tout $k \in \left[\!\left[1, \dfrac{n-1}{2}\right]\!\right]$, comme $\dfrac{2k}{n}$ n'est pas entier, alors la question précédente assure que $X^2-2\cos\left(\dfrac{2k\pi}{n}\right)X+1$ est irréductible et on a bien obtenu la décomposition en facteurs irréductibles de X^n-1 dans $\mathbb{R}[X]$.

Si n est pair, on procède de manière similaire pour obtenir que, en posant $r = \dfrac{n}{2}$, on a la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ suivante :

$$X^n - 1 = (X-1)(X+1)\prod_{k=1}^{r-1}\left(X^2-2\cos\left(\frac{2k\pi}{n}\right)X+1\right).$$

10. (a) On raisonne par double implication.

Si n et m sont premiers entre eux, d'après le théorème de Bézout, il existe $a, b \in \mathbb{Z}$ tels que $an+bm=1$. Ainsi pour tout $k \in [\![1, n-1]\!]$,

$$\left(\omega_n^m\right)^{bk} = \mathrm{e}^{\frac{2\mathrm{i}bkm\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}k(1-an)\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \neq 1.$$

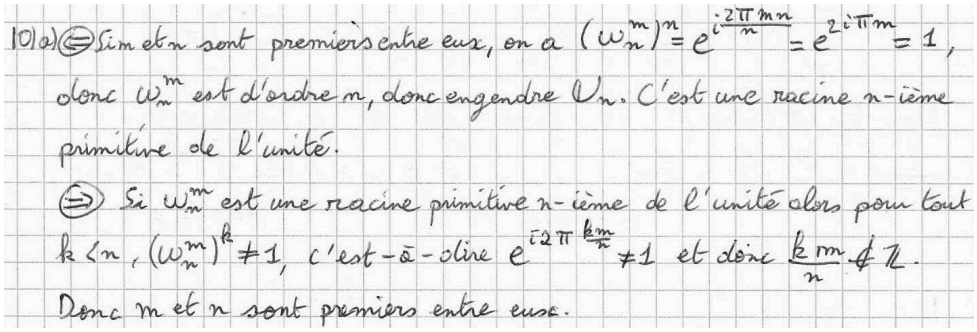
Donc $\left(\omega_n^m\right)^k \neq 1$. De plus, on a $\left(\omega_n^m\right)^n = 1$, donc ω_n^m est un élément d'ordre n de $\mathbb{U}_n$, et comme $\mathbb{U}_n$ est cyclique d'ordre n, alors ω_n^m engendre bien $\mathbb{U}_n$. C'est donc une racine primitive de l'unité.

Pour la réciproque, on procède par contraposition. Si n et m ne sont pas premiers entre eux, alors ils ont un diviseur commun $d \geqslant 2$. En notant $k = \dfrac{n}{d}$ et $k' = \dfrac{m}{d}$, on a $k < n$ et

$$\left(\omega_n^m\right)^k = \mathrm{e}^{\frac{2\mathrm{i}km\pi}{n}} = \mathrm{e}^{\frac{2\mathrm{i}m\pi}{d}} = \mathrm{e}^{2\mathrm{i}k'\pi} = 1.$$

Ainsi ω_n^m n'est pas d'ordre n, donc n'engendre pas $\mathbb{U}_n$. Ce n'est pas une racine primitive de l'unité et on a bien démontré l'équivalence demandée.

Analyse d'un extrait de copie


10) a) ⟸ Si m et n sont premiers entre eux, on a $(\omega_n^m)^n = e^{i\frac{2\pi mn}{n}} = e^{2i\pi m} = 1$, donc ω_n^m est d'ordre n, donc engendre U_n. C'est une racine n-ième primitive de l'unité.
⟹ Si ω_n^m est une racine primitive n-ième de l'unité alors pour tout $k < n$, $(\omega_n^m)^k \neq 1$, c'est-à-dire $e^{i2\pi\frac{km}{n}} \neq 1$ et donc $\frac{km}{n} \notin \mathbb{Z}$.
Donc m et n sont premiers entre eux.

- ⋆ Dans la première implication, $\omega_n^n = 1$ ne suffit pas à justifier que l'ordre de ω_n est n, mais seulement qu'il est au plus n (et plus précisément que c'est un diviseur n). C'est pour cela qu'il est important de préciser que ω_n^k n'est pas 1 pour $k < n$, et donc que l'ordre de ω_n ne peut pas être strictement inférieur à n.
- ⋆ Dans la seconde, le candidat passe trop rapidement sur l'implication suivante :

$$\forall k \in [\![1, n-1]\!],\ \frac{km}{n} \notin \mathbb{Z} \implies m \text{ et } n \text{ sont premiers entre eux.}$$

Le correcteur peut avoir l'impression que le candidat essaie de masquer qu'il n'a pas totalement compris le raisonnement et pénaliser une telle rédaction.

(b) D'après la question **8**, les racines n-ièmes de l'unité sont les ω_n^k pour $k \in [\![1, n]\!]$. La question précédente justifie que celles qui sont des racines primitives n-ièmes de l'unité sont celles pour lesquelles k et n sont premiers entre eux. Il y a donc autant de racines primitives n-ièmes de l'unité que d'entiers de $[\![1, n]\!]$ premiers avec n, c'est-à-dire $\varphi(n)$.

11. (a) Pour tout entier $d \in \mathbb{N}$ qui divise n, on note k l'entier tel que $n = kd$. Ainsi pour tout $\omega \in \mathbb{A}_d$, on a $\omega^n = \left(\omega^d\right)^k = 1^k = 1$, de sorte que $\omega \in \mathbb{U}_n$. D'où $\bigcup_{d|n} \mathbb{A}_d \subset \mathbb{U}_n$.

Réciproquement, si $\omega \in \mathbb{U}_n$, alors d'après le théorème de Lagrange, l'ordre de ω divise n, l'ordre de $\mathbb{U}_n$. Donc ω est d'ordre d pour un certain entier d qui divise n. Ainsi ω est une racine d-ième de l'unité et comme ω est d'ordre d, alors elle engendre $\mathbb{U}_d$, c'est-à-dire que $\omega \in \mathbb{A}_d$. On en déduit que $\mathbb{U}_n \subset \bigcup_{d|n} \mathbb{A}_d$ et finalement $\bigcup_{d|n} \mathbb{A}_d = \mathbb{U}_n$.

L'ordre d'un élément étant unique, les ensembles $\mathbb{A}_d$ sont deux à deux disjoints. Ainsi d'après la question **8**,

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \left(\prod_{\omega \in \mathbb{A}_d} (X - \omega). \right).$$

Enfin d'après la question **10**, les éléments de $\mathbb{A}_d$ sont les ω_d^m avec $m \in [\![1, d]\!]$ et m et d premiers entre eux. On en déduit donc que

$$\prod_{\omega \in \mathbb{A}_d} (X - \omega) = \prod_{\substack{1 \leqslant m \leqslant d \\ m \wedge d = 1}} \left(X - \omega_d^m\right) = \Phi_d,$$

ce qui finalement aboutit à $X^n - 1 = \prod_{d|n} \Phi_d$.

(b) On détermine Φ_n pour chaque $n \in [\![1,6]\!]$:

- 1 est l'unique racine première de 1. Donc $\Phi_1 = X-1$.
- Les racines carrées de 1 sont 1 et -1, et seule -1 est primitive. Donc $\Phi_2 = X+1$.
- Les racines cubiques de 1 sont 1, $j = \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ et $j^2 = \overline{j}$, et seules j et j^2 sont primitives. Donc $\Phi_3 = \big(X-j\big)\big(X-\overline{j}\big) = X^2+X+1$.
- Les racines quatrièmes de 1 sont 1, -1, i et $-\mathrm{i}$, et seules i et $-\mathrm{i}$ sont primitives. Donc $\Phi_4 = \big(X-\mathrm{i}\big)\big(X+\mathrm{i}\big) = X^2+1$.
  On aurait aussi pu remarquer que $\big(X-1\big)\big(X+1\big)\big(X^2+1\big) = X^4-1 = \Phi_1\Phi_2\Phi_4$ pour en déduire que $\Phi_4 = X^2+1$.
- Les racines cinquièmes de 1 sont les $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{5}}$ pour $k \in [\![0,4]\!]$, toutes primitives sauf 1.
  Donc $\Phi_5 = \displaystyle\prod_{k=1}^{5}\Big(X-\mathrm{e}^{\frac{2\mathrm{i}k\pi}{5}}\Big) = \Big(X^2-2\cos\Big(\frac{2\pi}{5}\Big)X+1\Big)\Big(X^2-2\cos\Big(\frac{4\pi}{5}\Big)X+1\Big)$.
  En remarquant que $X^5-1 = \big(X-1\big)\big(X^4+X^3+X^2+X+1\big)$, on obtient de surcroît l'écriture $\Phi_5 = X^4+X^3+X^2+X+1$.
- Les racines sixièmes de 1 sont $1, \mathrm{e}^{\frac{\mathrm{i}\pi}{3}}, j, -1, j^2, \mathrm{e}^{\frac{5\mathrm{i}\pi}{3}}$, et seules $\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}$ et $\mathrm{e}^{\frac{5\mathrm{i}\pi}{3}}$ sont primitives. Donc $\Phi_6 = \Big(X-\mathrm{e}^{\frac{\mathrm{i}\pi}{3}}\Big)\Big(X-\mathrm{e}^{\frac{5\mathrm{i}\pi}{3}}\Big) = X^2-2\cos\Big(\frac{\pi}{3}\Big)X+1 = X^2-X+1$.

(c) Si B est constant (donc égal à 1 car unitaire), alors on peut prendre $R=0$ et $Q=A$. Pour faciliter la suite de la démonstration, on décide d'utiliser la convention $\deg(0) = -\infty$ (très répandue), de sorte que le cas $R=0$ soit inclus dans la condition $\deg(R) < \deg(B)$.
On suppose désormais que B n'est pas constant, de sorte que $d_B = \deg(B) \geqslant 1$.
On procède par récurrence sur le degré de A. Pour tout $d \in \mathbb{N}$, on pose H_d : « Pour tout polynôme A de degré inférieur ou égal à d, alors il existe un couple $(Q,R) \in \mathbb{Z}[X]^2$ tel que $A = QB+R$ et $\deg(R) < \deg(B)$. »

Initialisation : Si $d < d_B$, *i.e.* $\deg(A) < \deg(B)$, alors on peut prendre $Q=0$ et $R=A$.
On a bien Q et R dans $\mathbb{Z}[X]$ et $\deg(R) = \deg(A) < \deg(B)$.

Hérédité : Soit $d \in \mathbb{N}$ fixé avec $d \geqslant d_B - 1$. On suppose que H_d est vraie.
Soit A de degré $d+1$. Alors $\deg(A) = d+1 \geqslant d_B = \deg(B)$.
On note $A = \displaystyle\sum_{k=0}^{d+1} a_k X^k$ avec $a_{d+1} \neq 0$ et $B = \sum_{k=0}^{d_B} b_k X^k$ avec $b_{d_B} = 1$ car B est unitaire.
On définit $Q_1 = a_{d+1}X^{d+1-d_B}$. Alors A et $-Q_1B$ sont de même degré et ont des coefficients dominants opposés. Donc $A - Q_1B$ est de degré inférieur ou égal à d.
Par hypothèse de récurrence, il existe Q_2 et R des polynômes de $\mathbb{Z}[X]$ tels que

$$A - Q_1B = Q_2B + R \quad \text{et} \quad \deg(R) < \deg(B).$$

On a donc

$$A = \big(Q_1+Q_2\big)B + R \quad \text{et} \quad \deg(R) < \deg(B),$$

avec $Q_1+Q_2 \in \mathbb{Z}[X]$, ce qui démontre que H_{d+1} est vraie.

Conclusion : Par récurrence, pour tout polynôme A il existe des polynômes Q et R à coefficients entiers tels que $A = BQ+R$ et $\deg(R) < \deg(B)$.

Commentaire

On ne peut pas se contenter de répondre qu'il s'agit de la division euclidienne dans $\mathbb{Z}[X]$. En effet, la théorie classique de la division euclidienne ne s'applique que lorsqu'on l'effectue dans $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps.
Dire qu'il s'agit d'un cas particulier de division euclidienne dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ n'est pas suffisant non plus, car ceci ne justifie pas que les polynômes Q et R obtenus sont à coefficients entiers.

(d) On procède par récurrence forte. Pour tout $n \in \mathbb{N}^*$, on pose H_n : « Φ_n est un polynôme unitaire de $\mathbb{Z}[X]$. »

Initialisation : Comme vu à la question **11.b**, Φ_1 est unitaire et dans $\mathbb{Z}[X]$.

Hérédité : Soit $n \in \mathbb{N}$ avec $n \geqslant 2$. On suppose que H_k est vraie pour tout $k \in [\![1, n-1]\!]$.
D'après la question **11.a**, on a

$$X^n - 1 = \Phi_n B \text{ avec } B = \prod_{\substack{d|n \\ d<n}} \Phi_d.$$

Par hypothèse de récurrence, B est un produit de polynômes unitaires et à coefficients entiers, donc est lui-même unitaire et à coefficients entiers. La question précédente assure alors de l'existence de Q et R dans $\mathbb{Z}[X]$ tels que $X^n - 1 = QB + R$ avec $\deg(R) < \deg(B)$. On en déduit que $\Phi_n B = QB + R$, et donc que $R = B\big(\Phi_n - Q\big)$. En passant aux degrés, on a $\deg(R) = \deg(B) + \deg\big(\Phi_n - Q\big)$. Comme $\deg(R) < \deg(B)$, cela implique que $\deg\big(\Phi_n - Q\big) < 0$, c'est-à-dire que $\Phi_n - Q = 0$. Ainsi $\Phi_n = Q \in \mathbb{Z}[X]$, et comme $X^n - 1$ est unitaire, alors Q est unitaire, ce qui finit de démontrer H_n.

Conclusion : Par récurrence, pour tout $n \in \mathbb{N}^*$, Φ_n est un polynôme unitaire de $\mathbb{Z}[X]$.

Commentaire

Bien que l'énoncé ne demande pas de montrer que le polynôme Φ_n est unitaire, il est nécessaire de l'introduire dans la récurrence afin de pouvoir appliquer la question **11.c**, qui requiert que le polynôme par lequel on divise soit unitaire.

II. Un lemme sur les matrices d'ordre fini

12. Comme A est d'ordre r, alors $A^r = \mathrm{I}_k$, de sorte que $X^r - 1$ est un polynôme annulateur de A. Il s'agit donc d'un multiple de μ_A, polynôme minimal de A. Or $X^r - 1$ est scindé à racines simples sur $\mathbb{C}$, donc μ_A est également scindé à racines simples et on en déduit que A est diagonalisable sur $\mathbb{C}$. De plus, ses valeurs propres sont toutes des racines de $X^r - 1$, donc ce sont des racines de l'unité.

13. On sait que μ_A divise $X^r - 1$, donc μ_A se décompose dans $\mathbb{K}[X]$ en un produit de facteurs irréductibles, qui sont des facteurs irréductibles de $X^r - 1$ dans $\mathbb{K}[X]$. Ces facteurs sont nécessairement deux à deux distincts, sans quoi μ_A aurait une racine double dans $\mathbb{C}$, ce qui contredit le fait que μ_A soit scindé à racines simples obtenu dans la question précédente. Enfin, les facteurs irréductibles de μ_A dans $\mathbb{K}[X]$ peuvent être choisis unitaires car μ_A est unitaire par définition.

III. Endomorphismes cycliques et décomposition de Frobenius

14. On procède par récurrence. Pour tout $n \in \mathbb{N}^*$, on pose H_n : « Si $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ avec $a_0, \ldots, a_{n-1} \in \mathbb{K}$, alors le polynôme caractéristique de C_P est P ».

Initialisation : Pour $n = 1$, on a $C_P = \begin{pmatrix} -a_0 \end{pmatrix}$, dont le polynôme caractéristique est $X + a_0$, c'est-à-dire P.

Hérédité : Soit $n \in \mathbb{N}^*$ tel que H_n soit vraie.
Soient $a_0, \ldots, a_n \in \mathbb{K}$ et $P = X^{n+1} + a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Alors en développant le déterminant de $X\mathrm{I}_{n+1} - C_p$ par rapport à la première ligne, on obtient

$$\chi_{C_P} = \begin{vmatrix} X & 0 & \ldots & 0 & a_0 \\ -1 & X & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-1} \\ 0 & \ldots & 0 & -1 & X + a_n \end{vmatrix}, \qquad \text{déterminant de taille } n+1,$$

$$= X \begin{vmatrix} X & 0 & \ldots & 0 & a_1 \\ -1 & X & \ddots & \vdots & a_2 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{n-1} \\ 0 & \ldots & 0 & -1 & X + a_n \end{vmatrix} + (-1)^{n+2} a_0 \begin{vmatrix} -1 & X & 0 & \ldots & 0 \\ 0 & -1 & X & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & -1 & X \\ 0 & \ldots & \ldots & 0 & -1 \end{vmatrix},$$

où ces deux déterminants sont de taille n.

Le second déterminant est triangulaire supérieur, donc il vaut simplement le produit des éléments diagonaux, à savoir $(-1)^n$.
Pour le premier, en posant $Q = X^n + a_n X^{n-1} + \cdots + a_1$, on reconnaît qu'il s'agit de χ_{C_Q}. Comme Q est unitaire et de degré n, alors par hypothèse de récurrence, on a $\chi_{C_Q} = Q$. D'où

$$\chi_{C_P} = X \times Q + (-1)^{2n+2} a_0 = X^{n+1} + \sum_{k=1}^{n} a_k X^k + a_0 = X^{n+1} + \sum_{k=0}^{n} a_k X^k = P.$$

On en déduit que H_{n+1} est vraie.

Conclusion : Par principe de récurrence, si P est un polynôme unitaire de $\mathbb{K}[X]$, alors le polynôme caractéristique de C_P est donné par P.

Commentaire

Les matrices compagnons peuvent servir à démontrer le théorème de Cayley-Hamilton comme cela est fait dans l'exercice préliminaire de l'Épreuve 1 de 2022.

15. (a) On montre que I_x est un idéal non trivial de $\mathbb{K}[X]$. Naturellement, I_x contient le polynôme nul. Et pour P et Q dans I_x, on a $\big(P-Q\big)(u)(x) = P(u)(x) - Q(u)(x) = 0_E - 0_E = 0_E$, donc $P - Q \in I_x$. Ainsi I_x est un sous-groupe additif de $\mathbb{K}[X]$. De plus, pour $R \in \mathbb{K}[X]$,

$$\big(RP\big)(u)(x) = \big(R(u)\circ P(u)\big)(x) = R(u)\big(P(u)(x)\big) = R(u)\big(0_E\big) = 0_E.$$

Donc $RP \in I_x$ et on a bien montré que I_x est un idéal de $\mathbb{K}[X]$. Enfin, $\mu_u(u) = 0_{\mathrm{End}(E)}$ donc I_x contient μ_u, non nul, ce qui montre que I_x n'est pas réduit au singleton $\big\{0_{\mathbb{K}[X]}\big\}$.
Comme $\mathbb{K}[X]$ est un anneau principal, il existe $\mu_x \in \mathbb{K}[X]$ tel que $I_x = \mu_x\mathbb{K}[X]$ et $\mu_x \neq 0$ puisque I_x n'est pas l'idéal nul.
Aussi, on peut supposer μ_x unitaire, quitte à le diviser par son coefficient dominant. L'unicité de μ_x s'obtient de la même manière qu'à la question **3** : deux polynômes qui engendrent I_x se divisent mutuellement, ce qui ne peut se produire que s'ils sont égaux puisqu'ils sont unitaires. Enfin, on a vu précédemment que $\mu_u \in I_x$, donc $\mu_x \mid \mu_u$.

(b) Comme les P_i sont irréductibles et deux à deux distincts, alors les $P_i^{m_i}$ sont deux à deux premiers entre eux, donc d'après le lemme des noyaux, on a

$$\bigoplus_{i=1}^{q} \mathrm{Ker}\Big(P_i^{m_i}(u)\Big) = \mathrm{Ker}\left(\left(\prod_{i=1}^{q} P_i^{m_i}\right)(u)\right) = \mathrm{Ker}\big(\mu_u(u)\big).$$

Comme $\mu_u(u) = 0_{\mathrm{End}(E)}$, alors on a $\mathrm{Ker}\big(\mu_u(u)\big) = E$ et finalement $E = \bigoplus_{i=1}^{q} \mathrm{Ker}\Big(P_i^{m_i}(u)\Big)$.
Enfin, puisque u commute avec tout polynôme en u, pour tout $x \in N_i$, on a

$$P_i^{m_i}(u)\big(u(x)\big) = u\Big(P_i^{m_i}(u)(x)\Big) = u\big(0_E\big) = 0_E,$$

donc $u(x) \in N_i$, ce qui prouve bien que les N_i sont stables par u.

(c) Pour tout $i \in [\![1,q]\!]$, on a $N_i = \mathrm{Ker}\Big(P_i^{m_i}(u)\Big)$, donc $P_i^{m_i}$ est un polynôme annulateur de u_i et on en déduit, comme μ_{u_i} et P_i sont unitaires, que $\mu_{u_i} \mid P_i^{m_i}$. Ainsi P_i est le seul facteur irréductible de μ_{u_i}, qui est donc de la forme P_i^k, avec $k \in [\![0, m_i]\!]$. S'il existe un $j \in [\![1,q]\!]$ pour lequel $\mu_{u_j} = P_j^k$ avec $k < m_j$, alors le polynôme $P_1^{m_1}\cdots P_{j-1}^{m_{j-1}} P_j^k P_{j+1}^{m_{j+1}}\cdots P_q^{m_q}$ est un polynôme non nul, de degré strictement inférieur à μ_u et annulateur de u puisqu'il annule tous les endomorphismes induits sur les sous-espaces N_i, pour tout $i \in [\![1,q]\!]$. Ceci contredit la minimalité du degré de μ_u. Ainsi pour tout $i \in [\![1,q]\!]$, on a $k = m_i$, d'où

$$\mu_{u_i} = P_i^{m_i}.$$

Pour tout $i \in [\![1,q]\!]$ et tout $x \in N_i$, d'après la question **15.a** appliquée à N_i, on sait que μ_x divise μ_{u_i}, donc que μ_x est de la forme $P_i^{m_x}$ avec $m_x \in [\![0, m_i]\!]$. Si pour tout $x \in N_i$, on avait $m_x \leqslant m_i - 1$, alors $P_i^{m_i-1}$ serait un polynôme annulateur de u_i, ce qui contrarie la minimalité de μ_{u_i}. Donc pour tout $i \in [\![1,q]\!]$, il existe $x_i \in N_i$ tel que $\mu_{x_i} = P_i^{m_i} = \mu_{u_i}$.
On définit $x = \sum_{i=1}^{q} x_i$. On sait que $\mu_x \mid \mu_u$ d'après la question **15.a**. De plus $\mu_x(u)(x) = 0_E$, donc par linéarité de u, on a

$$\sum_{i=1}^{q} \mu_x(u)(x_i) = 0_E.$$

Comme les $(N_i)_{i\in[\![1,q]\!]}$ sont stables par u, alors pour tout $i \in [\![1,q]\!]$, $\mu_x(u)(x_i) \in N_i$. Puisqu'ils sont par ailleurs en somme directe, on en déduit que pour tout $i \in [\![1,q]\!]$, $\mu_x(u)(x_i) = 0$, et donc que $\mu_x \in I_{x_i}$, ce qui donne $\mu_{x_i} \mid \mu_x$, à savoir $P_i^{m_i} \mid \mu_x$.
Enfin, puisque les polynômes $(P_i)_{i\in[\![1,q]\!]}$ sont premiers entre eux dans leur ensemble, on en déduit que $\prod_{i=1}^{q} P_i^{m_i} \mid \mu_x$, autrement dit $\mu_u \mid \mu_x$.
Ces deux polynômes étant unitaires, on aboutit finalement à $\mu_x = \mu_u$.

16. On montre que i) $\iff$ ii) puis que i) $\iff$ iii), ce qui suffit à prouver que les trois propositions sont équivalentes.
    - Si u est cyclique, il existe $x_0 \in E$ tel que $\mathcal{B} = \big(x_0, u(x_0), \dots, u^{k-1}(x_0)\big)$ soit une base de E. Alors il existe $(\lambda_j)_{j\in[\![0,k-1]\!]} \in \mathbb{K}^k$ tel que $u\big(u^{k-1}(x_0)\big) = u^k(x_0) = \sum_{j=0}^{k-1} \lambda_j u^j(x_0)$. De plus, pour tout $j \in [\![0,k-2]\!]$, on a $u\big(u^j(x_0)\big) = u^{j+1}(x_0)$. Ayant déterminé toutes les images des vecteurs de $\mathcal{B}$ par u, on constate que la matrice de u dans $\mathcal{B}$ est la matrice compagnon du polynôme $P = X^n - \sum_{j=0}^{k-1} \lambda_j X^j$. Donc i) $\implies$ ii).
    - On suppose qu'il existe une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u)$ soit la matrice compagnon d'un certain polynôme P. On note x_0 le premier élément de la base $\mathcal{B}$. Alors les coefficients de C_P indiquent que chaque autre vecteur de $\mathcal{B}$ est l'image par u de celui qui le précède dans $\mathcal{B}$ et donc par une récurrence immédiate, $\mathcal{B} = \big(x_0, u(x_0), \dots, u^{k-1}(x_0)\big)$. Ainsi ii) $\implies$ i), ce qui achève de prouver que i) $\iff$ ii).
    - Si u est cyclique, il existe $x_0 \in E$ tel que $\mathcal{B} = \big(x_0, u(x_0), \dots, u^{k-1}(x_0)\big)$ soit une base de E. Cela signifie qu'aucune combinaison linéaire non triviale de ces vecteurs n'est nulle. Autrement dit, aucun polynôme $P \in \mathbb{K}[X]$ non nul de degré inférieur ou égal à $k-1$ ne vérifie $P(u)(x_0) = 0$. Donc μ_{x_0} est de degré au moins k. Puis comme $\mu_{x_0} \mid \mu_u$, alors μ_u est degré au moins k. Or χ_u est lui aussi de degré k et on sait que $\mu_u \mid \chi_u$ (théorème de Cayley-Hamilton) et que χ_u et μ_u sont tous les deux unitaires. Ainsi $\chi_u = \mu_u$.
      Donc i) $\implies$ iii).
    - On suppose que $\chi_u = \mu_u$. D'après la question **15.c**, il existe $x_0 \in E$ tel que $\mu_{x_0} = \mu_u = \chi_u$. En particulier, μ_{x_0} est de degré k. On montre alors que $\mathcal{B} = \big(x_0, u(x_0), \dots, u^{k-1}(x_0)\big)$ est une base de E. Soient $\lambda_0, \dots, \lambda_{k-1} \in \mathbb{K}$ tels que

      $$\lambda_0 x_0 + \lambda_1 u(x_0) + \cdots + \lambda_{k-1} u^{k-1}(x_0) = 0_E.$$

      Ainsi $P = \sum_{j=0}^{k-1} \lambda_j X^j$ est un polynôme tel que $P(u)(x_0) = 0$, donc $P \in I_{x_0}$ ce qui signifie d'après la question **15.a** que P est un multiple de μ_{x_0}. Or $\deg(P) \leqslant k-1 < \deg(\mu_{x_0})$ donc P est le polynôme nul, ce qui implique que $\lambda_j = 0$ pour tout $j \in [\![0,k-1]\!]$. Ainsi la famille $\mathcal{B}$ est libre et comme il s'agit d'une famille libre à k vecteurs de E, qui est de dimension k, alors $\mathcal{B}$ est une base de E. Donc iii) $\implies$ i) et on obtient bien que i) $\iff$ iii).

17. Pour tout polynôme $P \in \mathbb{K}[X]$, on note $P = \sum_{k=0}^{d} a_k X^k$ avec $d \in \mathbb{N}$ et $a_0, \dots, a_d \in \mathbb{K}$.

Grâce à la linéarité de la composition,

$$u\circ P(u)=u\circ\left(\sum_{k=0}^{d}a_k u^k\right)=\sum_{k=0}^{d}a_k u^{k+1}=\left(\sum_{k=0}^{d}a_k u^k\right)\circ u=P(u)\circ u.$$

Donc $P(u)\in\mathrm{Com}(u)$ et on en déduit que $\mathbb{K}[u]\subset\mathrm{Com}(u)$.
Réciproquement, soit $v\in\mathrm{End}(E)$ qui commute avec u. Comme u est cyclique, on note x_0 un élément de E tel que $\big(x_0,u(x_0),\dots,u^{k-1}(x_0)\big)$ soit une base E. Ainsi, il existe $\lambda_0,\dots,\lambda_{k-1}\in\mathbb{K}$ tels que $v(x_0)=\sum_{i=0}^{k-1}\lambda_i u^i(x_0)$. On pose $P=\sum_{i=0}^{k-1}\lambda_i X^i$. On montre que $v=P(u)$.
Pour tout $j\in[\![0,k-1]\!]$, en utilisant que u et v commutent, alors

$$v\big(u^j(x_0)\big)=u^j\big(v(x_0)\big)=u^j\left(\sum_{i=0}^{k-1}\lambda_i u^i(x_0)\right)=\sum_{i=0}^{k-1}\lambda_i u^i\big(u^j(x_0)\big)=P(u)\big(u^j(x_0)\big).$$

Ainsi v et $P(u)$ coïncident sur une base de E, donc $v=P(u)$. On aboutit à $\mathrm{Com}(u)\subset\mathbb{K}[u]$ et finalement, on a bien montré que $\mathrm{Com}(u)=\mathbb{K}[u]$.

18. (a) Soit $x\in E$. Pour $P\in\mathbb{K}[X]$, $u\big(P(u)(x)\big)=Q(u)(x)$ avec $Q=XP$ et donc $u\big(P(u)(x)\big)\in E_x$. Ainsi E_x est stable par u.
On suppose désormais que x est non nul. On note d le plus grand entier naturel tel que $\big(x,v(x),\dots,v^d(x)\big)$ soit une famille libre de E_x. Ce d existe bien car $x\neq 0_E$. Alors $v^{d+1}(x)$ est une combinaison linéaire des vecteurs $x,v(x),\dots,v^d(x)$. Autrement dit, il existe un polynôme $B\in\mathbb{K}[X]$ de degré $d+1$ tel que $B(v)(x)=0_E$. Pour $P\in\mathbb{K}[X]$ quelconque, on note respectivement Q et R le quotient et le reste de sa division euclidienne par B. On a alors

$$P(v)(x)=Q(v)\big(B(v)(x)\big)+R(v)(x)=R(v)(x)\in\mathrm{Vect}\big(x,v(x),\dots,v^d(x)\big),$$

car $\deg(R)\leqslant d$. Ainsi la famille $\big(x,v(x),\dots,v^d(x)\big)$ est génératrice de E_x, et c'est bien une base de E_x. Donc l'endomorphisme v est cyclique.
Tout polynôme annulateur de u est également annulateur de v, donc $\mu_v\mid\mu_u$. Or ces deux polynômes sont unitaires et μ_u est supposé irréductible, donc $\mu_v=\mu_u$.
On sait que $\dim(E_x)=\deg(\chi_v)$, et en utilisant la question **16**, on obtient $\chi_v=\mu_v=\mu_u$. Finalement, $\dim(E_x)=\deg(\mu_u)$.

(b) Si $x=0_E$, alors $E_x=\{0_E\}$ et le résultat est immédiat. On suppose désormais x non nul. On suppose qu'il existe y non nul dans $F\cap E_x$. Comme F est stable par u, alors $u^j(y)\in F$ pour tout $j\in\mathbb{N}$ et comme F est un sous-espace vectoriel de E, la stabilité par combinaison linéaire assure que pour tout $P\in\mathbb{K}[X]$, $P(u)(y)\in F$. Autrement dit, $E_y\subset F$. Comme $y\in E_x$, on a $y=Q(u)(x)$ pour un certain polynôme Q. Ainsi pour tout $P\in\mathbb{K}[X]$, $P(u)(y)=\big(PQ\big)(u)(x)\in E_x$. D'où $E_y\subset E_x$. Or x et y étant non nuls, la question précédente affirme que E_x et E_y sont de même dimension (à savoir $\deg(\mu_u)$) et donc $E_x=E_y$, ce qui achève de démontrer que $E_x\subset F$.
Finalement on obtient bien l'alternative $E_x\subset F$ ou $E_x\cap F=\{0_E\}$.

(c) On construit la famille $(x_1,\dots,x_p)$ demandée grâce à un procédé récursif :

- Pour débuter, x_1 est n'importe quel vecteur non nul de E.
- Pour un entier $j\in\mathbb{N}^*$ fixé, on suppose qu'il existe des vecteurs $x_1,\dots,x_j$ de E tels que $E_{x_1},\dots,E_{x_j}$ soient en somme directe. Deux cas peuvent alors se produire :
  - Si $E=\bigoplus_{i=1}^{j}E_{x_i}$, alors le procédé est terminé et la famille $(x_1,\dots,x_j)$ convient.
  - Si $E\neq\bigoplus_{i=1}^{j}E_{x_i}$, alors il existe $x_{j+1}\in E\setminus\bigoplus_{i=1}^{j}E_{x_i}$. Le sous-espace $E_{x_{j+1}}$ est stable par u d'après la question **18.a**. De plus, $\bigoplus_{i=1}^{j}E_{x_i}$ est également stable par u, en tant que somme de sous-espaces stables par u. La question précédente assure alors que $\bigoplus_{i=1}^{j}E_{x_i}\bigcap E_{x_{j+1}}=\{0_E\}$ et donc que les espaces $E_{x_1},\dots,E_{x_{j+1}}$ sont en somme directe. On reprend alors au début du deuxième point.

Ce procédé s'arrête nécessairement en un nombre fini d'étapes car la dimension de l'espace $\bigoplus_{i=1}^{j}E_{x_i}$ croit strictement (de $\deg(\mu_u)$) à chaque itération et ne peut dépasser $k=\dim(E)$. Cela assure donc l'existence d'une famille $(x_1,\dots,x_p)$ telle que $\bigoplus_{i=1}^{p}E_{x_i}=E$.

19. (a) Comme $\mu_u=P_1\cdots P_q$ avec les P_i irréductibles et deux à deux distincts, la question **15.b** affirme que $E=\bigoplus_{i=1}^{q}\mathrm{Ker}(P_i)$ et pour tout $i\in[\![1,q]\!]$, $\mathrm{Ker}(P_i)$ est stable par u, ce qui induit un endomorphisme $\widetilde{u}_i$ de $\mathrm{Ker}(P_i)$ ayant P_i comme polynôme minimal. Ainsi en appliquant la question précédente à $\widetilde{u}_i$, il existe une famille de vecteurs $(y_{i,1},\dots,y_{i,a_i})$ telle que $\mathrm{Ker}(P_i)=\bigoplus_{j=1}^{a_i}E_{y_{i,j}}$.

En renommant $(x_1,\dots,x_p)$ la famille $(y_{1,1},\dots,y_{1,a_1},y_{2,1},\dots,y_{2,a_2},\dots,y_{q,1},\dots,y_{q,a_q})$, on a

$$E=\bigoplus_{i=1}^{q}\mathrm{Ker}(P_i)=\bigoplus_{i=1}^{q}\left(\bigoplus_{j=1}^{a_i}E_{y_{i,j}}\right)=\bigoplus_{i=1}^{p}E_{x_i}.$$

On peut supposer sans perte de généralité que les x_i sont non nuls, quitte à retirer ceux qui le sont, car $E_{0_E}=\{0_E\}$, qui ne contribue pas à la somme directe. On peut alors utiliser la question **18.a** qui assure que les E_{x_i} sont tous stables par u et que l'endomorphisme u_i induit par u est cyclique de polynôme minimal μ_i. Ainsi grâce à la question **16**, il existe une base $\mathcal{B}_i$ de E_{x_i} dans laquelle la matrice de u_i est la matrice compagnon de $\mu_{u_i}=P_i$. En concaténant les bases $\mathcal{B}_i$, on obtient une base $\mathcal{B}$ adaptée à la somme directe obtenue précédemment, dans laquelle la matrice de u est diagonale par blocs :

$$\mathrm{Mat}_{\mathcal{B}}(u)=\mathrm{Diag}\left(C_{P_1},\dots,C_{P_1},\dots,C_{P_q},\dots,C_{P_q}\right),$$

où pour tout $j\in[\![1,q]\!]$, le bloc C_{P_j} apparaît un nombre de fois que l'on note ℓ_j.

(b) Comme le polynôme caractéristique d'un endomorphisme est aussi celui de sa matrice dans n'importe quelle base et que $\mathrm{Mat}_{\mathcal{B}}(u)$ est diagonale par blocs, on a

$$\chi_u = \chi_{C_{P_1}} \cdots \chi_{C_{P_1}} \cdots \chi_{C_{P_q}} \cdots \chi_{C_{P_q}},$$

où chaque $\chi_{C_{P_i}}$ apparaît ℓ_i fois. Grâce à la question **14**, on obtient alors

$$\chi_u = P_1 \cdots P_1 \cdots P_q \cdots P_q = P_1^{\ell_1} \cdots P_q^{\ell_q}.$$

IV. Matrices complexes ou réelles d'ordre fini

20. (a) Comme $A^n = \mathrm{I}_k$, alors $X^n - 1$ est un polynôme annulateur de A, donc μ_a divise $X^n - 1$. Or on sait grâce à la question **8** que $X^n - 1$ est scindé à racines simples dans $\mathbb{C}$ et que ses racines sont les racines n-ièmes de l'unité. Donc μ_A est scindé à racines simples et ses racines sont des racines n-ièmes de l'unité. On en déduit que A est diagonalisable et que ses valeurs propres sont des racines n-ièmes de l'unité.

(b) D'après la question précédente, en notant $D = \mathrm{Diag}\big(\lambda_1, \ldots, \lambda_k\big)$, il existe $P \in \mathrm{GL}_k(\mathbb{C})$ telle que $A = PDP^{-1}$. On a donc, pour tout $m \in \mathbb{N}^*$, $A^m = PD^mP^{-1}$ où, puisque D est diagonale, $D^m = \mathrm{Diag}\big(\lambda_1^m, \ldots, \lambda_k^m\big)$. Ainsi

$$A^m = \mathrm{I}_k \iff PD^mP^{-1} = \mathrm{I}_k \iff \mathrm{Diag}\big(\lambda_1^m, \ldots, \lambda_k^m\big) = \mathrm{I}_k \iff \forall j \in [\![1,k]\!],\ \lambda_j^m = 1.$$

Pour tout $j \in [\![1,k]\!]$, λ_j est d'ordre n_j, donc $\lambda_j^m = 1$ si et seulement si m est un multiple de n_j. On en déduit que

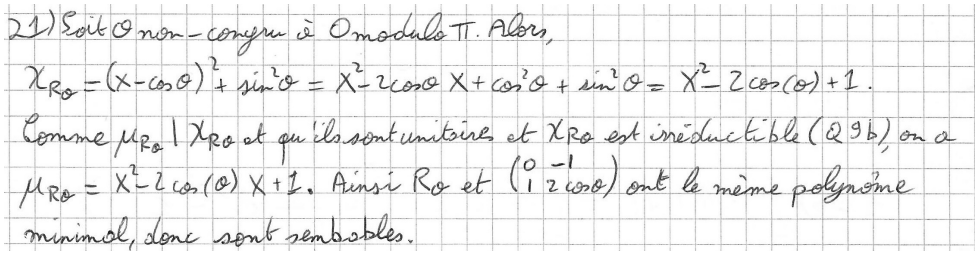
$$A^m = \mathrm{I}_k \iff \forall j \in [\![1,k]\!],\ n_j \mid m \iff \mathrm{PPCM}\big(n_1, \ldots, n_k\big) \mid m.$$

Finalement A est d'ordre $\mathrm{PPCM}\big(n_1, \ldots, n_k\big)$.

(c) Soit $r \in \mathbb{N}^*$. On définit $A_r = \mathrm{Diag}\big(\omega_r, 1, \ldots, 1\big)$, qui est bien un élément de $\mathrm{GL}_k(\mathbb{C})$ car diagonale, avec des coefficients diagonaux non nuls, donc inversible. D'après la question précédente, A_r est d'ordre $\mathrm{PPCM}\big(r, 1, \ldots, 1\big)$, c'est-à-dire r.

21. Soit $\theta \in \mathbb{R} \setminus \pi\mathbb{Z}$, de sorte que $\cos(\theta) \neq \pm 1$. Le polynôme caractéristique de R_θ est donné par $\chi_{R_\theta} = \big(X - \cos(\theta)\big)^2 + \sin^2(\theta) = X^2 - 2\cos(\theta)X + 1$. On a déjà vu à la question **9.b** que ce polynôme est irréductible dans $\mathbb{R}[X]$. Or le théorème de Cayley-Hamilton affirme que $\mu_{R_\theta} \mid \chi_{R_\theta}$. Ces deux polynômes étant unitaires, on obtient que $\mu_{R_\theta} = X^2 - 2\cos(\theta)X + 1$.
Ainsi, d'après la décomposition obtenue dans la partie III, il existe une base de $\mathbb{R}^2$ où la rotation d'angle θ a pour matrice la matrice compagnon de χ_{R_θ}, c'est-à-dire $\begin{pmatrix} 0 & -1 \\ 1 & 2\cos(\theta) \end{pmatrix}$.
Comme elles représentent la même application linéaire dans deux bases différentes, les deux matrices $\begin{pmatrix} 0 & -1 \\ 1 & 2\cos(\theta) \end{pmatrix}$ et R_θ sont donc semblables.

Analyse d'un extrait de copie


21) Soit θ non-congru à 0 modulo π. Alors,
$\chi_{R_\theta} = (X-\cos\theta)^2 + \sin^2\theta = X^2 - 2\cos\theta X + \cos^2\theta + \sin^2\theta = X^2 - 2\cos(\theta) + 1$.
Comme $\mu_{R_\theta} \mid \chi_{R_\theta}$ et qu'ils sont unitaires et χ_{R_θ} est irréductible (Q 9b), on a $\mu_{R_\theta} = X^2 - 2\cos(\theta)X + 1$. Ainsi R_θ et $\begin{pmatrix} 0 & -1 \\ 1 & 2\cos\theta \end{pmatrix}$ ont le même polynôme minimal, donc sont semblables.

La fin du raisonnement présentée ici est incorrecte : tout comme la trace, le déterminant ou encore le polynôme caractéristique, le polynôme minimal est bien le même pour deux matrices semblables, mais deux matrices peuvent avoir le même polynôme minimal sans être semblables. Tous ces objets sont des invariants de similitude incomplets.
Moins important, il est de bon ton de nommer les résultats importants comme le théorème de Cayley-Hamilton lors de leur utilisation.

22. On note n l'ordre de A. On a alors $A^n - \mathrm{I}_k = 0$, de sorte que $X^n - 1$ annule A, ce qui signifie que $\mu_a \mid X^n - 1$. On a déterminé à la question **9.c** la décomposition en facteurs irréductibles de $X^n - 1$. Elle est sans facteurs carrés et est le produit (selon les cas), de facteurs parmi

$$X-1, \qquad X+1, \qquad X^2 - 2\cos(\theta_j)X + 1, \text{ avec } \theta_j = \frac{2j\pi}{n} \text{ pour tout } j \in \left[\!\left[1, \left\lfloor \frac{n-1}{2} \right\rfloor\right]\!\right].$$

Le polynôme μ_A est donc le produit de certains de ces facteurs, où chaque facteur apparaît au plus une fois. On remarque que pour tout $j \in \left[\!\left[1, \left\lfloor \frac{n-1}{2} \right\rfloor\right]\!\right]$, on a $\frac{\theta_j}{2\pi} = \frac{j}{n} \in \mathbb{Q} \cap \left]0, \frac{1}{2}\right[$ et donc $\theta_j \in 2\pi\mathbb{Q} \cap]0, \pi[\subset 2\pi\mathbb{Q} \setminus \pi\mathbb{Z}$. On obtient bien la forme demandée pour μ_A.

Commentaire

Les θ_j ne sont pas seulement deux à deux distincts, ils sont deux à deux distincts modulo π, ce qui est plus fort et nécessaire dans la suite pour pouvoir appliquer la question **19**.

23. Si A est d'ordre fini, en reprenant les notations de la question précédente, μ_A est de la forme $(X-1)^{\varepsilon_1}(X+1)^{\varepsilon_2} P_{\theta_1} \cdots P_{\theta_q}$ où les θ_j sont dans $2\pi\mathbb{Q} \setminus \pi\mathbb{Z}$ et deux à deux distincts modulo π. En particulier, μ_A est sans facteur carré donc, d'après la question **19**, il existe une base $\mathcal{B}$ de E dans laquelle l'endomorphisme associé à A a une matrice diagonale par blocs de la forme

$$M = \mathrm{Diag}\left(C_{X-1}, \ldots, C_{X-1}, C_{X+1}, \ldots, C_{X+1}, C_{P_{\theta_1}}, \ldots, C_{P_{\theta_1}}, \ldots, C_{P_{\theta_q}}, \ldots, C_{P_{\theta_q}}\right),$$

où C_{X-1} apparaît k_1 fois, C_{X+1} apparaît k_2 fois et pour tout $i \in [\![1, q]\!]$, $C_{P_{\theta_j}}$ apparaît ℓ_j fois, k_1 ou k_2 pouvant éventuellement être nuls. En remarquant que C_{X-1} est la matrice (1) et que C_{X+1} est la matrice (-1), on obtient que

$$M = \mathrm{Diag}\left(\mathrm{I}_{k_1}, -\mathrm{I}_{k_2}, C_{P_{\theta_1}}, \ldots, C_{P_{\theta_1}}, \ldots, C_{P_{\theta_q}}, \ldots, C_{P_{\theta_q}}\right).$$

D'après la question **21**, pour tout $j \in [\![1,q]\!]$, il existe $Q_j \in \mathrm{GL}_2(\mathbb{R})$ telle que $C_{P_{\theta_j}} = Q_j R_{\theta_j} Q_j^{-1}$. On définit alors la matrice diagonale par blocs $Q = \mathrm{Diag}\big(\mathrm{I}_{k_1+k_2}, Q_1, \dots, Q_1, \dots, Q_q, \dots, Q_q\big)$ où chaque Q_j apparaît ℓ_j fois. Tous les blocs diagonaux sont inversibles, donc Q est inversible avec $Q^{-1} = \mathrm{Diag}\big(\mathrm{I}_{k_1+k_2}, \dots, Q_1^{-1}, \dots, Q_1^{-1}, \dots, Q_q^{-1}, \dots, Q_q^{-1}\big)$. Ainsi en calculant par blocs,

$$M = Q\,\mathrm{Diag}\big(\mathrm{I}_{k_1}, -\mathrm{I}_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}\big)Q^{-1}.$$

Finalement, M (et donc aussi A) est semblable à une matrice diagonale par blocs de la forme $\mathrm{Diag}\big(\mathrm{I}_{k_1}, -\mathrm{I}_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}\big)$ et comme A est une matrice de taille $k \times k$, les dimensions de la matrice donnent $k = k_1 + k_2 + 2\big(\ell_1 + \cdots + \ell_q\big)$.

Réciproquement, on suppose qu'il existe $Q \in \mathrm{GL}_k(\mathbb{R})$ telle que

$$A = Q\,\mathrm{Diag}\big(\mathrm{I}_{k_1}, -\mathrm{I}_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}\big)Q^{-1},$$

avec $k = k_1 + k_2 + 2\big(\ell_1 + \cdots + \ell_q\big)$ et les θ_j dans $2\pi\mathbb{Q} \setminus \pi\mathbb{Z}$. Alors pour tout $m \in \mathbb{N}^*$,

$$A^m = Q\,\mathrm{Diag}\Big(\mathrm{I}_{k_1}^m, \big(-\mathrm{I}_{k_2}\big)^m, R_{\theta_1}^m, \dots, R_{\theta_1}^m, \dots, R_{\theta_q}^m, \dots, R_{\theta_q}^m\Big)Q^{-1}. \tag{1.1}$$

Dans le groupe $\mathrm{GL}_2(\mathbb{R})$, I_{k_1} est d'ordre 1, $-\mathrm{I}_{k_2}$ est d'ordre 2 et les θ_j étant dans $2\pi\mathbb{Q}$, R_{θ_j} est d'ordre fini pour tout $j \in [\![1,q]\!]$. En prenant pour m le PPCM de tous ces ordres, on a alors

$$A^m = Q\,\mathrm{Diag}\big(\mathrm{I}_{k_1}, \mathrm{I}_{k_2}, \mathrm{I}_2, \dots, \mathrm{I}_2\big)Q^{-1} = Q\,\mathrm{I}_k\,Q^{-1} = \mathrm{I}_k,$$

donc A est d'ordre fini, ce qui conclut la preuve de l'équivalence.

24. En reprenant la relation (1.1), on voit que $A^m = \mathrm{I}_k$ si et seulement si tous les blocs $\big(-\mathrm{I}_{k_2}\big)^m$, $R_{\theta_1}^m, \dots, R_{\theta_q}^m$ sont égaux à une matrice identité, ce qui ne se produit que si m est un multiple des ordres de tous ces blocs. Or en notant $\theta_j = 2\pi\dfrac{a_j}{b_j}$ avec a_j et b_j premiers entre eux, $R_{\theta_j}^m$ représente la rotation du plan d'angle $2\pi\dfrac{a_j m}{b_j}$, qui est l'identité si et seulement si $\dfrac{a_j m}{b_j} \in \mathbb{Z}$. D'après le lemme de Gauss, cela équivaut à $b_j \mid m$ puisque b_j et a_j sont premiers entre eux. Ainsi R_{θ_j} est d'ordre b_j. Et finalement, selon les valeurs de k_2 :
    - Si $k_2 > 0$, $-\mathrm{I}_{k_2}$ est d'ordre 2 et donc A est d'ordre $\mathrm{PPCM}\big(2, b_1, \dots, b_q\big)$.
    - Si $k_2 = 0$, il n'y a pas de bloc $-\mathrm{I}_{k_2}$ et donc A est d'ordre $\mathrm{PPCM}\big(b_1, \dots, b_q\big)$.
25. Si $k = 2$, on applique la question **23**, dont on reprend les notations. En particulier, on a $2 = k_1 + k_2 + 2\big(\ell_1 + \cdots + \ell_q\big)$ où $k_1, k_2 \in \mathbb{N}$ et $\ell_1, \dots, \ell_q \in \mathbb{N}^*$. On a donc $q = 0$ ou $q = 1$.
    - Si $q = 1$, alors nécessairement $k_1 = k_2 = 0$ et donc A est semblable à R_{θ_1} avec $\theta_1 \in 2\pi\mathbb{Q}$.
    - Si $q = 0$, trois cas peuvent se présenter :
        - Si $k_1 = 2$ et $k_2 = 0$, A est semblable à $\mathrm{I}_2 = R_0$ où $0 \in 2\pi\mathbb{Q}$ (A est en fait I_2).
        - Si $k_1 = 1$ et $k_2 = 1$, A est semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
        - Si $k_1 = 0$ et $k_2 = 2$, A est semblable à $-\mathrm{I}_2 = R_\pi$ où $\pi = \dfrac{1}{2}2\pi \in 2\pi\mathbb{Q}$ (et A est en fait $-\mathrm{I}_2$).

    Dans tous les cas, A est semblable à une matrice R_θ avec $\theta \in 2\pi\mathbb{Q}$ ou à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

26. Soit $r \in \mathbb{N}^*$. En prenant $\theta = \dfrac{2\pi}{r}$, on a vu en question **24** que R_θ est d'ordre exactement r et il s'agit bien d'un élément de $\mathrm{GL}_2(\mathbb{R})$.

27. (a) Pour commencer, $(\cdot,\cdot)_G$ est bien à valeurs dans $\mathbb{R}$. Comme la multiplication matricielle par un vecteur et la somme sont linéaires et que le produit scalaire $\langle\cdot,\cdot\rangle$ est bilinéaire, alors $(\cdot,\cdot)_G$ est bilinéaire.
Puis pour tous $u, v \in \mathbb{R}^2$, on a $(v,u)_G = \dfrac{1}{|G|}\displaystyle\sum_{A\in G}\langle Av, Au\rangle = \dfrac{1}{|G|}\sum_{A\in G}\langle Au, Av\rangle = (u,v)_G$, donc $(\cdot,\cdot)$ est symétrique.
Enfin pour tout $u \in \mathbb{R}^2$, $(u,u)_G = \dfrac{1}{|G|}\displaystyle\sum_{A\in G}\langle Au, Au\rangle$. Comme $\langle\cdot,\cdot\rangle$ est un produit scalaire, alors pour toute matrice A, $\langle Au, Au\rangle$ est positif, donc $(u,u)_G \geqslant 0$.
De plus, en utilisant que $\langle\cdot,\cdot\rangle$ est défini positif, alors on obtient

$$(u,u)_G = 0 \implies \forall A \in G,\ \langle Au, Au\rangle = 0 \implies \forall A \in G,\ Au = 0 \implies u = 0,$$

puisque G contient I_2. Ainsi $(\cdot,\cdot)_G$ est une forme bilinéaire symétrique définie positive, c'est donc bien un produit scalaire de $\mathbb{R}^2$.
Soit $A \in G$. Comme G est un groupe, l'application $\varphi_A : \begin{cases} G & \longrightarrow & G \\ M & \longmapsto & MA \end{cases}$ est bien définie et bijective (puisqu'elle admet $\varphi_{A^{-1}}$ comme réciproque), donc pour tous $u, v \in \mathbb{R}^2$,

$$\begin{aligned}(Au, Av)_G &= \frac{1}{|G|}\sum_{M\in G}\langle MAu, MAv\rangle = \frac{1}{|G|}\sum_{\substack{N=\varphi_A(M)\\ M\in G}}\langle Nu, Nv\rangle \\ &= \frac{1}{|G|}\sum_{N\in G}\langle Nu, Nv\rangle = (u,v)_G.\end{aligned}$$

Commentaire

Il s'agit là d'un procédé classique de « moyennisation » d'un produit scalaire que l'on peut notamment retrouver dans le sujet d'Algèbre 2024 sur les représentations.

(b) Soit (X_1, X_2) une base orthonormée de $\mathbb{R}^2$ pour le produit scalaire $(\cdot,\cdot)_G$. Une telle base existe nécessairement grâce au procédé de Gram-Schmidt. On note alors $Q \in \mathrm{GL}_2(\mathbb{R})$ la matrice de passage de (X_1, X_2) à la base canonique de $\mathbb{R}^2$.
En outre, S étant la matrice d'un produit scalaire, elle est donc symétrique définie positive. La matrice Q^TSQ est symétrique car $(Q^TSQ)^T = Q^TS^T(Q^T)^T = Q^TSQ$ (puisque S est symétrique) et pour tout $u \in \mathbb{R}^2 \setminus \{0_{\mathbb{R}^2}\}$, on a $u^TQ^TSQu = (Qu)^TS(Qu) > 0$ (puisque S est définie positive). Donc Q^TSQ est symétrique définie positive et c'est aussi la matrice d'un produit scalaire de $\mathbb{R}^2$.
On remarque alors en notant (e_1, e_2) la base canonique de $\mathbb{R}^2$ que pour tous $i, j \in \{1,2\}$,

$$e_i^TQ^TSQe_j = (Qe_i)^TS(Qe_j) = X_i^TSX_j = \delta_{i,j}.$$

Le produit scalaire associé à Q^TSQ est donc le produit scalaire canonique de $\mathbb{R}^2$ et on a ainsi $Q^TSQ = \mathrm{I}_2$, d'où $S = P^TP$ en posant $P = Q^{-1}$.
Pour tout $A \in G$, on a vu à la question précédente que les produits scalaires $(\cdot,\cdot)_G$ et $\big(A\,\cdot\,, A\,\cdot\big)_G$ sont identiques, donc ont la même matrice, c'est-à-dire $S = A^TSA$. Ainsi

$$\begin{aligned}\big(PAP^{-1}\big)^TPAP^{-1} &= \big(P^{-1}\big)^TA^TP^TPAP^{-1} = \big(P^T\big)^{-1}A^TSAP^{-1}\\ &= \big(P^T\big)^{-1}SP^{-1} = \big(P^T\big)^{-1}P^TPP^{-1} = \mathrm{I}_2\,.\end{aligned}$$

D'où $PAP^{-1} \in \mathrm{O}_2(\mathbb{R})$.

28. Soit G un sous-groupe d'ordre n de $\mathrm{SO}_2(\mathbb{R})$. Si $M \in G$, alors M est une matrice de rotation plane R_θ d'angle $\theta \in \mathbb{R}$ comme rappelé par l'énoncé. De plus, d'après le théorème de Lagrange, l'ordre de M divise n, donc $M^n = R_{n\theta} = \mathrm{I}_2$, ce qui implique que $n\theta \equiv 0\ [2\pi]$ et donc que θ est de la forme $\dfrac{2k\pi}{n}$ avec $k \in \mathbb{Z}$. Ainsi G est inclus dans le groupe engendré par $R_{\frac{2\pi}{n}}$. Ces deux groupes étant de même cardinal n, alors G est exactement le groupe cyclique engendré par $R_{\frac{2\pi}{n}}$.

29. Suivant l'indication, on commence par remarquer que

$$BA^{-1} = BR_{-\frac{2\pi}{n}} = \begin{pmatrix}\cos\Big(-\dfrac{2\pi}{n}\Big) & -\sin\Big(-\dfrac{2\pi}{n}\Big)\\ -\sin\Big(-\dfrac{2\pi}{n}\Big) & -\cos\Big(\dfrac{2\pi}{n}\Big)\end{pmatrix} = \begin{pmatrix}\cos\Big(\dfrac{2\pi}{n}\Big) & \sin\Big(\dfrac{2\pi}{n}\Big)\\ \sin\Big(\dfrac{2\pi}{n}\Big) & -\cos\Big(\dfrac{2\pi}{n}\Big)\end{pmatrix} = AB.$$

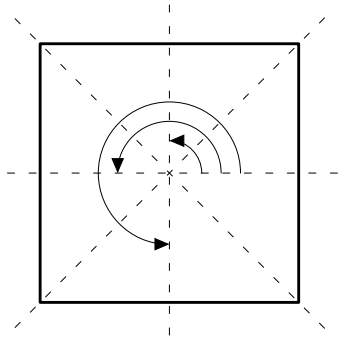
Le groupe engendré par A et B contient tous les éléments qui peuvent s'écrire sous la forme $M_1\cdots M_k$ où $k \in \mathbb{N}$ et $M_1,\dots,M_k \in \big\{A, A^{-1}, B, B^{-1}\big\}$. En remarquant que $B^{-1} = B$ et que $A^{-1} = A^{n-1}$ puisque $A^n = \mathrm{I}_2$, on se ramène aux objets de la forme $M_1\cdots M_k$ où $k \in \mathbb{N}$ et $M_1,\dots,M_k \in \big\{A, B\big\}$. Soit M un tel élément. On utilise alors la remarque initiale pour transformer, tant que c'est possible, toute occurrence du facteur AB en un facteur BA^{n-1}. Lorsque ce n'est plus possible on a alors obtenu que $M = A^r$ ou $M = BA^r$ avec $r \in \mathbb{N}$.

Comme A est d'ordre n, en notant k le reste de la division euclidienne de r par n, on obtient bien $M \in \big\{\mathrm{I}_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\big\}$ et donc $D_n \subset \big\{\mathrm{I}_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\big\}$. L'inclusion réciproque est immédiate donc $D_n = \big\{\mathrm{I}_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\big\}$.

Même si ce n'est pas précisément demandé par l'énoncé, on peut justifier que D_n est d'ordre exactement $2n$, c'est-à-dire que les éléments listés ci-dessus sont deux à deux distincts. Comme A est d'ordre n, alors $\mathrm{I}_2, A, \dots, A^{n-1}$ sont tous distincts. La matrice B étant inversible, la multiplication par B est bijective et donc $B, BA, \dots, BA^{n-1}$ sont aussi tous distincts. Enfin, les éléments de la forme A^k sont de déterminant 1 et ceux de la forme BA^k sont de déterminant -1, donc ils sont distincts.
Finalement les matrices $\mathrm{I}_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}$ sont bien deux à deux distinctes.

Commentaire

Le groupe diédral D_n ainsi défini est un groupe usuel qui peut se comprendre de manière géométrique : il s'agit de l'ensemble des isométries vectorielles du plan laissant invariant un polygone régulier à n côtés et centré en l'origine O.
Les éléments de la forme A^k sont des rotations et les éléments BA^k correspondent alors à des symétries orthogonales du plan.
Par exemple, D_4 est le groupe de symétrie d'un carré : il contient l'identité, les rotations de centre O et d'angle $\frac{\pi}{2}$, π et $\frac{3\pi}{2}$, ainsi que quatre symétries orthogonales, dont les axes respectifs sont les deux diagonales du carré et les deux médiatrices des côtés.



30. (a) On note $G_+ = G \cap \mathrm{SO}_2(\mathbb{R})$ l'ensemble des matrices de déterminant 1 de G et $G_- = G \setminus G_+$ celui des matrices de déterminant -1. Comme G_+ est l'intersection de sous-groupes de $\mathrm{GL}_2(\mathbb{R})$, c'est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. En particulier, c'est un groupe dont tous les éléments sont dans G, c'est donc un sous-groupe de G.
Comme G n'est pas inclus dans $\mathrm{SO}_2(\mathbb{R})$, G_- n'est pas vide et on peut considérer $S \in G_-$.
L'application $\psi_S : \begin{cases} G & \longrightarrow & G \\ M & \longmapsto & SM \end{cases}$ est bien définie car G est un groupe et est bijective car elle admet $\psi_{S^{-1}}$ comme réciproque $\big($sachant que $S^{-1} \in G$ car G est un groupe$\big)$.
Par multiplicativité du déterminant, on obtient $\psi_S\big(G_+\big) \subset G_-$ et $\psi_S\big(G_-\big) \subset G_+$. Or on sait que $\psi_S\big(G_+\big) \cup \psi_S\big(G_-\big) = G$ car G est bijective et que G_+ et G_- forment une partition de G. On en déduit que $\psi_S\big(G_+\big) = G_-$ et $\psi_S\big(G_-\big) = G_+$. Comme ψ_S est bijective, on en déduit que G_+ et G_- sont de même cardinal, et donc G est de cardinal double de celui de G_+. Autrement dit, G_+ est un sous-groupe d'indice 2 de G.

Commentaire

On peut aussi procéder plus rapidement en rappelant que l'application déterminant $\det : \begin{cases} (G,\circ) & \longrightarrow & \big(\{-1,1\},\times\big) \\ M & \longmapsto & \det(M) \end{cases}$ est un morphisme de groupe. Ce morphisme est surjectif puisque G contient au moins un élément de déterminant -1 par hypothèse et contient aussi I_2 qui est de déterminant 1. De plus, son noyau est G_+, ce qui montre que G_+ est un sous-groupe de G. Et par théorème d'isomorphisme, ${}^{G}\!/_{G_+} \simeq \{-1,1\}$, donc $\left|{}^{G}\!/_{G_+}\right| = 2$, ce qui prouve que G_+ est d'indice 2 dans G.

(b) Soit M un élément de G_-. Alors ses colonnes forment une base orthonormée indirecte de $\mathbb{R}^2$. Puisque sa première colonne est un élément de norme 1 de $\mathbb{R}^2$, il existe $\theta \in \mathbb{R}$ tel que cette colonne s'écrive $\begin{pmatrix}\cos(\theta)\\ \sin(\theta)\end{pmatrix}$. Et comme pour tout vecteur $u = \begin{pmatrix}a\\ b\end{pmatrix}$ du plan, l'unique vecteur v de même norme tel que (u, v) forme une base indirecte est $\begin{pmatrix}b\\ -a\end{pmatrix}$, alors la deuxième colonne de M est $\begin{pmatrix}\sin(\theta)\\ -\cos(\theta)\end{pmatrix}$ et donc $M = S_\theta$.

(c) La matrice S_θ est symétrique réelle donc diagonalisable en base orthonormée d'après le théorème spectral. Ses valeurs propres ne peuvent être que 1 ou -1 car S_θ représente une isométrie et comme son déterminant est égal à -1, on sait que S_θ a deux valeurs propres simples : 1 et -1. Puis en remarquant que

$$S_\theta \begin{pmatrix}\cos\left(\frac{\theta}{2}\right)\\ \sin\left(\frac{\theta}{2}\right)\end{pmatrix} = \begin{pmatrix}\cos(\theta)\cos\left(\frac{\theta}{2}\right)+\sin(\theta)\sin\left(\frac{\theta}{2}\right)\\ \sin(\theta)\cos\left(\frac{\theta}{2}\right)-\cos(\theta)\sin\left(\frac{\theta}{2}\right)\end{pmatrix} = \begin{pmatrix}\cos\left(\frac{\theta}{2}\right)\\ \sin\left(\frac{\theta}{2}\right)\end{pmatrix}$$

$$\text{et} \quad S_\theta \begin{pmatrix}-\sin\left(\frac{\theta}{2}\right)\\ \cos\left(\frac{\theta}{2}\right)\end{pmatrix} = \begin{pmatrix}-\cos(\theta)\sin\left(\frac{\theta}{2}\right)+\sin(\theta)\cos\left(\frac{\theta}{2}\right)\\ -\sin(\theta)\sin\left(\frac{\theta}{2}\right)-\cos(\theta)\cos\left(\frac{\theta}{2}\right)\end{pmatrix} = (-1)\begin{pmatrix}-\sin\left(\frac{\theta}{2}\right)\\ \cos\left(\frac{\theta}{2}\right)\end{pmatrix},$$

alors on a obtenu des vecteurs propres pour chacune des valeurs propres.
Ainsi en prenant $P = R_{\frac{\theta}{2}}$, on a bien que $P \in \mathrm{SO}_2(\mathbb{R})$ et $P^{-1}S_\theta P = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.

(d) Soient ι_P l'automorphisme intérieur de $\mathrm{O}_2(\mathbb{R})$ défini par $\iota_P : \left\{\begin{array}{ccc}\mathrm{O}_2(\mathbb{R}) & \longrightarrow & \mathrm{O}_2(\mathbb{R})\\ M & \longmapsto & P^{-1}MP\end{array}\right.$ et $G' = \iota_P(G)$. Alors G' est un sous-groupe de $\mathrm{O}_2(\mathbb{R})$, conjugué à G dans $\mathrm{SO}_2(\mathbb{R})$.
On montre que G' est le groupe diédral D_n avec $n = \dfrac{1}{2}|G|$.
En appliquant la question **30.a** à G', on a que $G'_+ = G' \cap \mathrm{SO}_2(\mathbb{R})$ est un sous-groupe d'indice 2 de G', donc un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$. On note n l'ordre de ce groupe G'_+.
La question **28** assure alors que $G'_+ = G' \cap \mathrm{SO}_2(\mathbb{R}) = \left\{\mathrm{I}_2, A, \ldots, A^{n-1}\right\}$ avec $A = R_{\frac{2\pi}{n}}$.
De plus, on a montré à la question précédente que G' contient la matrice B (selon la notation de la question **29**) et le même raisonnement que celui mené dans la question **30.a** montre que $G'_- = \psi_B(G'_+)$, donc les éléments de G'_- sont engendrés par A et B.
Comme $G' = G'_+ \cup G'_-$, tous les éléments de G' sont engendrés par A et B.
Le sous-groupe G' est donc contenu dans le sous-groupe engendré par A et B, à savoir D_n d'après la question **29**. Or D_n et G' sont de même cardinal, à savoir $2n$. Donc $G' = D_n$, ce qui permet de conclure que G est bien conjugué dans $\mathrm{SO}_2(\mathbb{R})$ au groupe diédral D_n.

V. Matrices rationnelles d'ordre fini

31. Il est admis par l'énoncé que la décomposition en facteurs irréductibles de $X^n - 1$ dans $\mathbb{Q}[X]$ est $X^n - 1 = \prod_{d|n} \Phi_d$. Comme A est d'ordre n, alors $X^n - 1$ est un polynôme annulateur de A et

est donc un multiple du polynôme minimal μ_A. Ses facteurs irréductibles sont donc parmi les facteurs irréductibles de X^n-1, avec au plus la même puissance que celle à laquelle ils apparaissent dans la décomposition de X^n-1, à savoir 1. Comme de plus μ_A est unitaire, on a bien $\mu_A = \Phi_{d_1}\cdots\Phi_{d_q}$ où $q \in \mathbb{N}^*$ et $d_1,\dots,d_q$ sont des diviseurs de n deux à deux distincts.

32. Pour deux diviseurs d_1 et d_2 de n distincts, les polynômes Φ_{d_1} et Φ_{d_2} sont distincts (ils n'ont pas les mêmes racines complexes). La question précédente montre donc que μ_A est sans facteurs carrés et on peut ainsi appliquer la question **19**. On obtient que A est semblable à une matrice diagonale par blocs de la forme $\mathrm{Diag}\left(C_{\Phi_{d_1}},\dots,C_{\Phi_{d_1}},\dots,C_{\Phi_{d_q}},\dots,C_{\Phi_{d_q}}\right)$ où pour tout $j \in [\![1,q]\!]$, le bloc $C_{\Phi_{d_j}}$ apparaît autant de fois que la multiplicité de Φ_{d_j} dans le polynôme caractéristique de A.

33. (a) Soit $d \in \mathbb{N}^*$. D'après la question **14**, on a que le polynôme caractéristique de C_{Φ_d} est Φ_d. Grâce au théorème de Cayley-Hamilton, on sait que $\mu_{C_{\Phi_d}} \mid \Phi_d$. Il est admis que Φ_d est irréductible dans $\mathbb{Q}[X]$ et les polynômes Φ_d et $\mu_{C_{\Phi_d}}$ sont unitaires. Alors on en déduit que le polynôme minimal de C_{Φ_d} est Φ_d.
Or X^d-1 est un multiple de Φ_d, donc X^d-1 annule C_{Φ_d} et C_{Φ_d} est donc d'ordre fini inférieur ou égal à d. Et pour tout entier $m<d$, Φ_d ne divise pas X^m-1 car la décomposition en facteurs irréductibles de X^m-1 ne fait pas apparaître Φ_d.
Finalement l'ordre de C_{Φ_d} est exactement d.

(b) Soit $A \in \mathrm{GL}_k(\mathbb{Q})$. D'après la question **32**, si A est d'ordre fini elle est semblable à une matrice diagonale par blocs $\mathrm{Diag}\left(C_{\Phi_{d_1}},\dots,C_{\Phi_{d_1}},\dots,C_{\Phi_{d_q}},\dots,C_{\Phi_{d_q}}\right)$ où $q \in \mathbb{N}^*$ et $d_1,\dots,d_q$ sont des diviseurs de n deux à deux distincts. D'après sa définition (question **10.b**), Φ_n est de degré $\varphi(n)$. En considérant la taille de la matrice A, on a $\ell_1\varphi(d_1)+\cdots+\ell_q\varphi(d_q)=k$. Réciproquement, si A est semblable à une matrice diagonale par blocs de la forme

$$D = \mathrm{Diag}\left(C_{\Phi_{d_1}},\dots,C_{\Phi_{d_1}},\dots,C_{\Phi_{d_q}},\dots,C_{\Phi_{d_q}}\right),$$

où $q \in \mathbb{N}^*$ et $d_1,\dots,d_q$ sont des diviseurs de n deux à deux distincts, alors en notant n un multiple des ordres des matrices $C_{\Phi_{d_1}},\dots,C_{\Phi_{d_q}}$, on a que $D^n = \mathrm{I}_k$ et donc $A^n = \mathrm{I}_k$, ce qui montre que A est d'ordre fini. Ceci conclut la preuve de l'équivalence.

(c) Comme à la question **24**, lorsque A est d'ordre fini, on a pour tout $n \in \mathbb{N}^*$ l'équivalence $A^n = \mathrm{I}_k$ si et seulement si n est un multiple de tous les ordres des matrices $C_{\Phi_{d_1}},\dots,C_{\Phi_{d_q}}$, c'est-à-dire un multiple de $d_1,\dots,d_q$ d'après la question **33.a**.
Ainsi l'ordre de A est $\mathrm{PPCM}(d_1,\dots,d_q)$.

(d) Grâce aux questions précédentes, la matrice diagonale par blocs $A = \mathrm{Diag}\left(C_{\Phi_3}, C_{\Phi_4}\right)$ est d'ordre $\mathrm{PPCM}(3,4) = 12$. On a déterminé à la question **11.b** que $\Phi_3 = X^2+X+1$ et $\Phi_4 = X^2+1$, donc les blocs C_{Φ_3} et C_{Φ_4} sont de taille 2×2 et ainsi A est de taille 4×4 avec

$$A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

De plus, A est bien inversible (d'inverse A^{11}) donc $A \in \mathrm{GL}_4(\mathbb{Q})$.

(e) Soit A une matrice de $\mathrm{GL}_k(\mathbb{Q})$ d'ordre fini n. D'après les questions précédentes, elle est semblable à une matrice diagonale par blocs $D = \mathrm{Diag}\left(C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_q}}, \dots, C_{\Phi_{d_q}}\right)$ où $q \in \mathbb{N}^*$, $d_1, \dots, d_q$ sont des diviseurs de n deux à deux distincts et $n = \mathrm{PPCM}\left(d_1, \dots, d_q\right)$. Or par définition des polynômes cyclotomiques, chaque Φ_{d_j} est de degré $\varphi(d_j)$ donc la matrice $C_{\Phi_{d_j}}$ est de taille $\varphi(d_j) \times \varphi(d_j)$. Comme A est de taille $k \times k$, seuls des blocs $C_{\Phi_{d_j}}$ pour des entiers d_j vérifiant $\varphi(d_j) \leqslant k$ peuvent apparaître dans D.
Ainsi $\{d_1, \dots, d_q\} \subset \{m \in \mathbb{N}^* \mid \varphi(m) \leqslant k\}$ et donc

$$n = \mathrm{PPCM}\left(d_1, \dots, d_q\right) \leqslant \mathrm{PPCM}\left(\{m \in \mathbb{N}^* \mid \varphi(m) \leqslant k\}\right).$$

34. (a) Soit A une matrice de $\mathrm{GL}_2(\mathbb{Q})$ d'ordre fini n. D'après la question précédente **33.b**, elle est semblable à une matrice diagonale par blocs $D = \mathrm{Diag}\left(C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_q}}, \dots, C_{\Phi_{d_q}}\right)$ où $q \in \mathbb{N}^*$ et chaque bloc $C_{\Phi_{d_1}}$ est présent ℓ_j fois avec $\ell_1\varphi(d_1) + \dots + \ell_q\varphi(d_q) = 2$. Ainsi seuls des entiers dont la caractéristique d'Euler est inférieure ou égale à 2 peuvent apparaître comme d_j. D'après la question **7**, cela limite les possibilités à 1, 2, 3, 4 et 6. De plus, 3, 4 et 6 sont solutions de $\varphi(n) = 2$ tandis que 1 et 2 sont solutions de $\varphi(n) = 1$. Par conséquent, A est semblable à l'une des matrices suivantes :

- C_{Φ_3}, c'est-à-dire $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, qui est d'ordre 3.
- C_{Φ_4}, c'est-à-dire $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, qui est d'ordre 4.
- C_{Φ_6}, c'est-à-dire $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, qui est d'ordre 6.
- $\mathrm{Diag}\left(C_{\Phi_1}, C_{\Phi_1}\right)$, c'est-à-dire I_2, qui est d'ordre 1.
- $\mathrm{Diag}\left(C_{\Phi_2}, C_{\Phi_2}\right)$, c'est-à-dire $-\mathrm{I}_2$, qui est d'ordre 2.
- $\mathrm{Diag}\left(C_{\Phi_1}, C_{\Phi_2}\right)$, c'est-à-dire $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, qui est d'ordre 2.

Les matrices et les ordres ont été déterminés grâce aux expressions des polynômes cyclotomiques obtenues en question **11.b** et puisque pour $d \in \mathbb{N}^*$, C_{Φ_d} est d'ordre d.
Réciproquement, les six matrices de l'énoncé sont donc bien d'ordre fini et toute matrice qui leur est semblable est également d'ordre fini, ce qui achève de démontrer l'équivalence demandée.

(b) Un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$ est aussi un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$, donc les résultats obtenus en partie IV montrent que G isomorphe soit à un groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, soit à un groupe diédral D_n avec $n \in \mathbb{N}^*$.
Pour tout $n \in \mathbb{N}^*$, les groupes $\mathbb{Z}/n\mathbb{Z}$ et D_n contiennent au moins un élément d'ordre n et on a vu à la question précédente que les ordres possibles pour les éléments de $\mathrm{GL}_2(\mathbb{Q})$ d'ordre fini sont 1, 2, 3, 4 et 6, qui sont donc les seules valeurs possibles de n.
En remarquant que D_1 est un groupe d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$ puisqu'il n'existe qu'un seul groupe d'ordre 2 à isomorphisme près, on en déduit que G est isomorphe à l'un des groupes de la liste suivante :

$$\{\mathrm{I}_2\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ D_2,\ D_3,\ D_4,\ D_6.$$

Commentaire

Bien que cela ne soit pas demandé, on peut justifier que ces neuf groupes sont deux à deux non isomorphes pour compléter le travail de classification des sous-groupes finis de $\mathrm{GL}_2(\mathbb{Q})$. Deux groupes d'ordres différents ne peuvent évidemment pas être isomorphes, ce qui laisse deux cas à étudier :

- ⋆ D_2 et $\mathbb{Z}/4\mathbb{Z}$ sont tous deux d'ordre 4 mais ne sont pas isomorphes car D_2 ne contient aucun élément d'ordre 4 (en reprenant les notations de la question **29**, I_2 est d'ordre 1 et A, B et BA sont d'ordre 2) alors que $\mathbb{Z}/4\mathbb{Z}$ en contient deux ($\overline{1}$ et $\overline{3}$).
- ⋆ D_3 et $\mathbb{Z}/6\mathbb{Z}$ sont tous deux d'ordre 6 mais ne sont pas isomorphes car $\mathbb{Z}/6\mathbb{Z}$ est abélien alors que D_3 ne l'est pas. Par exemple, $AB = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix} \neq \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix} = BA$.

VI. Matrices d'ordre fini dans $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$

35. Il existe une bijection entre les matrices inversibles et les matrices de passage depuis la base canonique de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$. Il y a donc autant d'éléments dans $\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ que de bases du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$. Pour construire une telle base, il y a p^2-1 possibilités pour le premier vecteur (tous les vecteurs de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2$ sauf le vecteur nul). Pour le second vecteur, les possibilités sont tous les vecteurs qui ne sont pas colinéaires au premier. Or pour tout vecteur $v \in \left(\mathbb{Z}/p\mathbb{Z}\right)^2$, on a $\mathrm{Vect}(v) = \{kv \mid k \in [\![0, p-1]\!]\}$ qui est de cardinal p, ce qui donne donc p^2-p possibilités pour le second vecteur. Finalement,

$$\mathrm{Card}\left(\mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)\right) = (p^2-1)(p^2-p).$$

Commentaire

Cet exercice est le cas particulier en $n=2$ d'un exercice classique : dénombrer $\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)$. Son cardinal est donné par le nombre de $\mathbb{Z}/p\mathbb{Z}$-bases de $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$. On construit par récurrence les bases $(e_1, \dots, e_n)$ de cet espace vectoriel comme ci-dessus. Si l'on a construit les vecteurs $(e_1, \dots, e_i)$, alors $\mathrm{Vect}\left((e_1, \dots, e_i)\right)$ a pour dimension i, donc est de cardinal p^i. Il y a donc $p^n - p^i$ vecteurs qui ne sont pas combinaison linéaire de $(e_1, \dots, e_i)$ et qui peuvent être le vecteur e_{i+1}.
En continuant le procédé, on trouve finalement que le cardinal de $\mathrm{GL}_n\left(\mathbb{Z}/p\mathbb{Z}\right)$ est égal à

$$\prod_{i=1}^{n}\left(p^n - p^{i-1}\right) = \prod_{i=0}^{n-1}\left(p^n - p^i\right).$$

36. Comme M est une matrice de taille 2×2, son polynôme caractéristique est de degré 2. Le théorème de Cayley-Hamilton permet donc d'affirmer que le polynôme minimal de M est de degré 0, 1 ou 2.

D'après la question **4** appliquée à l'endomorphisme associé à M dans la base canonique, on obtient que $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$ est de dimension 0, 1 ou 2 en tant que $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Il est donc de cardinal 1, p ou p^2.

37. Soit $M \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$. On note n son ordre. Alors les matrices $M^0, M, M^2, \ldots, M^{n-1}$ sont des éléments distincts de $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$. En effet, s'il existe $\ell, \ell' \in [\![0, n-1]\!]$ avec $\ell < \ell'$ tels que $M^\ell = M^{\ell'}$, alors on a $M^{\ell'-\ell} = \mathrm{I}_2$ avec $\ell' - \ell < n$, ce qui contredit la définition de l'ordre. De plus ces éléments sont non nuls car M est inversible. Or selon la question précédente, il y a au plus p^2-1 éléments non nuls dans $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$. D'où $n \leqslant p^2-1$.

38. (a) On commence par remarquer que $\mathrm{Stab}(M) = \left\{P \in \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right) \;\middle|\; PM = MP\right\}$. On sait que μ_M est de degré 2, tout comme χ_M. Comme $\mu_M \mid \chi_M$ (théorème de Cayley-Hamilton) et que μ_M et χ_M sont tous deux unitaires, on a $\mu_M = \chi_M$. En notant u l'endomorphisme associé à M dans la base canonique de $\mathbb{Z}/p\mathbb{Z}$, la question **16** assure que u est cyclique. Grâce à la question **17**, le commutant de u dans $\mathrm{End}(E)$ est $\left(\mathbb{Z}/p\mathbb{Z}\right)[u]$, ce qui signifie que l'ensemble des matrices de $\mathcal{M}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$ qui commutent avec M est $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$. Comme $\mathrm{Stab}(M)$ est l'ensemble des matrices inversibles qui commutent avec M, alors on a bien $\mathrm{Stab}(M) = \left(\mathbb{Z}/p\mathbb{Z}\right)[M] \cap \mathrm{GL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$.

(b) On suppose que M n'a pas de valeur propre dans $\mathbb{Z}/p\mathbb{Z}$. D'après la question **4** (ou plus exactement sa traduction matricielle), comme son polynôme minimal est de degré 2, alors (I_2, M) est une base de $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$. Grâce à la question précédente, il reste à déterminer pour quelles valeurs de α et β dans $\mathbb{Z}/p\mathbb{Z}$ la matrice $N = \alpha\,\mathrm{I}_2 + \beta M$ est inversible.

- Si $\alpha = \beta = 0$, alors $N = 0$, qui n'est évidement pas inversible.
- Si $\beta = 0$ et $\alpha \neq 0$, alors $N = \alpha\,\mathrm{I}_2$, qui est inversible (d'inverse $\alpha^{-1}\,\mathrm{I}_2$).
- Si $\beta \neq 0$, alors $N = \beta\left(\dfrac{\alpha}{\beta}\mathrm{I}_2 + M\right)$. On remarque que $\dfrac{\alpha}{\beta}\mathrm{I}_2 + M$ n'est pas inversible si et seulement si M admet $-\dfrac{\alpha}{\beta}$ pour valeur propre. Or on a supposé que M est sans valeur propre. Ainsi $\dfrac{\alpha}{\beta}\mathrm{I}_2 + M$ est inversible et donc N aussi.

Finalement, la matrice nulle est la seule qui n'est pas inversible, ce qui donne bien $|\mathrm{Stab}(M)| = p^2 - 1$.

(c) On reprend le raisonnement et les notations de la question précédente dans le cas où M admet une unique valeur propre $\lambda \in \mathbb{Z}/p\mathbb{Z}$. Les deux premiers cas sont identiques.

Lorsque $\beta \neq 0$, on a désormais que N n'est pas inversible si et seulement si $-\dfrac{\alpha}{\beta} = \lambda$, ce qui équivaut à $\alpha = -\beta\lambda$. Ainsi, à chaque valeur possible de β non nul dans $\mathbb{Z}/p\mathbb{Z}$, correspond un unique α tel que $\alpha\,\mathrm{I}_2 + \beta M$ n'est pas inversible.

En prenant aussi en compte le cas $\alpha = \beta = 0$, cela donne exactement p matrices de $\left(\mathbb{Z}/p\mathbb{Z}\right)[M]$ qui ne sont pas inversibles et donc $|\mathrm{Stab}(M)| = p^2 - p$.

39. En appliquant la question **37** avec $p=3$, on obtient que l'ordre des éléments de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ est majoré par 8. De plus, l'ordre de tout élément d'un groupe divise le cardinal du groupe et on sait grâce à la question **35** que $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ est de cardinal $\left(3^2-1\right)\left(3^2-3\right)=48$.

    Comme 5 et 7 ne divisent pas 48, alors $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ ne contient aucun élément d'ordre 5 ou 7. Ceci réduit bien les ordres possibles à 1, 2, 3, 4, 6 et 8.

40. (a) On rappelle que pour tout $a\in\mathbb{Z}/3\mathbb{Z}$, on a d'après la formule du binôme de Newton que

$$\left(X+a\right)^3=X^3+3aX^2+3a^2X+a^3=X^3+a^3.$$

    Or dans $\mathbb{Z}/3\mathbb{Z}$, on a $0^3=0$, $1^3=1$ et $2^3=8=2$, donc $\left(X+a\right)^3=X^3+a$. On en déduit que

$$X^6-1=\left(X^3-1\right)\left(X^3+1\right)=\left(X-1\right)^3\left(X+1\right)^3,$$

    donc X^6-1 est bien scindé.

Commentaire

Nous avons redémontré dans ce particulier deux résultats classiques dans les anneaux et corps de caractéristique finie. Soit p un nombre premier.

- ⋆ Pour un anneau commutatif A de caractéristique p, l'application $\left\{\begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & x^p \end{array}\right.$ est un morphisme d'anneaux (appelé *morphisme de Frobenius*).
  En particulier, $\left(x+y\right)^p=x^p+y^p$ pour tous x et y dans A.
- ⋆ Dans un corps K de caractéristique p, tous les éléments sont des points fixes du morphisme de Frobenius. Autrement dit, $x^p=x$ pour tout $x\in K$.

    (b) Soit $M\in\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ d'ordre 6. Alors M n'admet pas 0 comme valeur propre, sinon elle ne serait pas inversible. On peut également affirmer que M n'est pas diagonalisable. En effet, si elle l'était, elle serait semblable à une matrice de la forme $\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix}$ qui est d'ordre 1 ou 2. M serait donc également d'ordre 1 ou 2, ce qui contredirait l'hypothèse que M est d'ordre 6.
    Comme X^6-1 est un polynôme annulateur de M, c'est un multiple de son polynôme minimal μ_M. Or X^6-1 est scindé d'après la question précédente, donc μ_M est également scindé. On en déduit que M est trigonalisable. Si M admettait deux valeurs propres distinctes, elles seraient toutes deux racines du polynôme minimal et comme celui-ci est de degré au plus 2, il serait scindé à racines simples. M serait alors diagonalisable, ce qui est impossible. Donc M n'admet qu'une seule valeur propre.
    En résumé, M est trigonalisable, avec une unique valeur propre non nulle, 1 ou -1, mais n'est pas diagonalisable. Elle est donc semblable à une des quatre matrices suivantes :

$$M_1=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\qquad M_2=\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix},\qquad M_3=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix},\qquad M_4=\begin{pmatrix}-1 & -1\\ 0 & -1\end{pmatrix}.$$

    On remarque que $M_1^3=M_2^3=\mathrm{I}_2$, donc M_1 et M_2 ne sont pas d'ordre 6 et ne peuvent pas être semblables à M. Enfin, M_3 et M_4 sont semblables entre elles, car avec $P=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$ (qui est bien inversible), on a $P^{-1}M_3P=M_4$.
    Finalement, M est donc bien nécessairement semblable à M_4.

Réciproquement, si l'on détermine les puissances de M_4 aux ordres potentiels dans le groupe $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$, on a

$$M_4^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad M_4^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad M_4^4 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad M_4^6 = \mathrm{I}_2\,.$$

M_4 est donc d'ordre 6 et toute matrice qui lui est semblable l'est également, ce qui conclut la preuve de l'équivalence demandée.

(c) Ce qui précède justifie que les matrices d'ordre 6 forment exactement l'orbite de M_4 par l'action de conjugaison de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ sur lui-même. Comme M_4 a une unique valeur propre, la question **38.c** assure alors que $|\mathrm{Stab}(M_4)| = 3^2 - 3 = 6$. On utilise la formule des classes rappelée en début de partie pour obtenir que $\left|\mathcal{O}_{M_4}\right| = \dfrac{\left|\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)\right|}{|\mathrm{Stab}(M_4)|} = \dfrac{48}{6} = 8$. Il y a donc 8 matrices d'ordre 6 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

41. Comme vu en question **40.a**, $X^3 - 1 = (X-1)^3$ donc $X^3 - 1$ est scindé et n'admet qu'une unique racine (triple) : 1. Or $X^3 - 1$ étant polynôme annulateur de M, 1 est la seule valeur propre possible pour M. Pour les mêmes raisons que dans la question **40.b**, M est trigonalisable mais pas diagonalisable. Donc M est semblable à l'une des deux matrices M_1 ou M_2. Comme $P^{-1}M_1P = M_2$, alors M est forcément semblable à M_1.
Réciproquement, $M_1^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ et $M_1^3 = \mathrm{I}_2$, donc M_1 est bien d'ordre 3 et toutes les matrices qui lui sont semblables sont également d'ordre 3.
On obtient donc que les matrices d'ordre 3 constituent exactement l'orbite de M_1 par l'action de conjugaison de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ sur lui-même. La matrice M_1 ayant une unique valeur propre, le raisonnement se conclut comme en question **40.c** et il y a exactement 8 matrices d'ordre 3 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

42. (a) On a d'un côté $(X-1)(X+1)(X^2+1) = (X^2-1)(X^2+1) = X^4 - 1$ et de l'autre

$$(X^2+X+2)(X^2+2X+2) = X^4 + 3X^3 + 6X^2 + 6X + 4 = X^4 + 1,$$

de sorte que

$$(X-1)(X+1)(X^2+1)(X^2+X+2)(X^2+2X+2) = (X^4-1)(X^4+1) = X^8 - 1.$$

$X-1$ et $X+1$ sont irréductibles puisque de degré 1. En notant $A = X^2+1$, $B = X^2+X+2$ et $C = X^2+2X+2$, on a que $A(0) = 1$, $A(1) = 2$ et $A(2) = 2$, donc A n'a pas de racines. Comme il est de degré 2, il est bien irréductible. De même, $B(0) = 2$, $B(1) = 1$, $B(2) = 1$, $C(0) = 2$, $C(1) = 2$ et $C(2) = 1$, donc B et C étant aussi de degré 2 et sans racines, alors ils sont irréductibles. Finalement $(X-1)(X+1)(X^2+1)(X^2+X+2)(X^2+2X+2)$ est bien la décomposition en facteurs irréductibles de $X^8 - 1$.

(b) Soit $M \in \mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ d'ordre 8. Alors M est annulée par $X^8 - 1$, donc son polynôme minimal μ_M divise $X^8 - 1$. On peut alors remarquer que μ_M est de degré 2.

En effet, l'autre degré potentiel est 1, mais alors il serait de la forme $\mu_M = X - \lambda$, avec $\lambda \in \{1,2\}$ et on aurait donc $M = \mathrm{I}_2$ ou $M = 2\mathrm{I}_2$. Les matrices I_2 et $2\mathrm{I}_2 = -\mathrm{I}_2$ étant respectivement d'ordres 1 et 2, c'est impossible.
Ainsi μ_M est égal à un facteur irréductible de degré 2 de $X^8 - 1$ ou au produit de deux facteurs irréductibles de degré 1, c'est-à-dire que μ_M est l'un des polynômes suivants :

$$(X-1)(X+1), \qquad X^2+1, \qquad X^2+X+2, \qquad X^2+2X+2.$$

Si μ_M est $(X-1)(X+1)$ ou X^2+1, alors c'est en particulier un diviseur de X^4-1, ce qui implique que $M^4 = \mathrm{I}_2$ et donc que M est d'ordre au plus 4, ce qui est absurde. Donc μ_M est X^2+X+2 ou X^2+2X+2.
Réciproquement, si μ_M est X^2+X+2 ou X^2+2X+2, alors c'est un diviseur de X^8-1, donc l'ordre de M divise 8, mais ce n'est pas un diviseur de X^4-1, donc l'ordre de M ne divise pas 4, ce qui veut dire que M est forcément d'ordre 8.
Finalement, on a montré que M est d'ordre 8 si et seulement si son polynôme minimal est X^2+X+2 ou X^2+2X+2.

(c) On pose $M_5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. M_5 est la matrice compagnon du polynôme X^2+X+2, donc $\chi_{M_5} = X^2+X+2$ par la question **14**. Comme $\mu_{M_5} \mid \chi_{M_5}$ (théorème de Cayley-Hamilton) avec μ_{M_5} et χ_{M_5} unitaires et χ_{M_5} irréductible, on a $\mu_{M_5} = X^2+X+2$ et M_5 est d'ordre 8 d'après la question précédente.

(d) On pose $M_6 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, matrice compagnon de X^2+2X+2. De même, M_6 est d'ordre 8.
Soit M d'ordre 8 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$. Si son polynôme caractéristique est X^2+X+2, alors $\mu_M = \chi_M$ comme χ_M est irréductible. Donc d'après la question **16**, M est semblable à la matrice compagnon de χ_M, c'est-à-dire à M_5. De même, si le polynôme caractéristique de M est X^2+2X+2, alors M est semblable à M_6.
Ceci justifie que l'ensemble des matrices d'ordre 8 est $\mathcal{O}_{M_5} \cup \mathcal{O}_{M_6}$. Cette union est disjointe car M_5 et M_6 ne sont pas semblables puisqu'elles n'ont pas le même polynôme caractéristique.
Les matrices semblables à M_5 n'ont pas de valeurs propres puisque leur polynôme caractéristique n'a pas de racine. Ainsi, par la question **38.b**, on a $|\mathrm{Stab}(M_5)| = 3^2 - 1 = 8$ et donc grâce à la formule des classes, $\left|\mathcal{O}_{M_5}\right| = \dfrac{\left|\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)\right|}{|\mathrm{Stab}(M_5)|} = \dfrac{48}{8} = 6$.
De même, $\left|\mathcal{O}_{M_6}\right| = 6$ et il y a donc 12 matrices d'ordre 8 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

43. La décomposition en facteurs irréductibles de X^4-1 est $(X-1)(X+1)(X^2+1)$ (question **42.a**). Si M est une matrice d'ordre 4 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$, alors M est annulée par X^4-1, donc son polynôme minimal μ_M divise X^4-1. Comme en question **42.b**, on peut montrer que μ_M est de degré 2. Ainsi μ_M est $(X-1)(X+1)$ ou X^2+1. Or μ_M ne peut pas être $(X-1)(X+1) = X^2-1$, sinon M serait d'ordre au plus 2. Donc $\mu_M = X^2+1$.

Réciproquement une matrice dont le polynôme minimal est X^2+1 est annulée par X^4-1 mais pas par X^2-1, donc est forcément d'ordre 4. On pose $M_7 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ la matrice compagnon de X^2+1. Le même raisonnement qu'en question **42.d** montre que les matrices d'ordre 4 sont celles qui sont semblables à M_7 et que $\left|\mathcal{O}_{M_7}\right| = \dfrac{\left|\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)\right|}{|\mathrm{Stab}(M_7)|} = \dfrac{48}{8} = 6$.

Il y a donc 6 matrices d'ordre 4 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

44. (a) Soit $N \in \mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ d'ordre 2 avec $N \neq -\mathrm{I}_2$. Alors $N^2 - \mathrm{I}_2 = 0_2$, donc N est annulée par X^2-1, qui est donc un multiple de μ_N. La décomposition en facteurs irréductibles de X^2-1 est $(X-1)(X+1)$, donc les diviseurs unitaires de X^2-1 sont $X-1$, $X+1$ et X^2-1. Or μ_N ne peut pas être $X-1$ (car on aurait $N = \mathrm{I}_2$, qui n'est pas d'ordre 2) ni $X+1$ (car on aurait $N = -\mathrm{I}_2$, ce que l'on a exclu). Donc $\mu_N = X^2-1$.
Comme μ_N est scindé à racines simples, la matrice N est diagonalisable avec pour valeurs propres 1 et -1, c'est-à-dire qu'elle est semblable à $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(b) Réciproquement, les matrices semblables à M ont pour polynôme minimal X^2-1 donc sont d'ordre 2. Ainsi les matrices d'ordre 2 de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$ sont $-\mathrm{I}_2$ et les éléments de l'orbite de M. On remarque aussi que $-\mathrm{I}_2$ et M ne sont pas semblables car ces deux matrices ne partagent pas le même spectre.
On raisonne de manière similaire à la question **38.b** pour déterminer $\mathrm{Stab}(M)$.
On sait grâce à la question **38.a** que $\mathrm{Stab}(M)$ est l'ensemble des matrices inversibles de $\left\{\alpha M + \beta \mathrm{I}_2 \;\middle|\; \alpha,\beta \in \mathbb{Z}/3\mathbb{Z}\right\}$. Soient $\alpha,\beta \in \mathbb{Z}/p\mathbb{Z}$ et $N = \alpha \mathrm{I}_2 + \beta M$.

- Si $\alpha = \beta = 0$, alors $N = 0$, qui n'est évidement pas inversible.
- Si $\beta = 0$ et $\alpha \in \{-1, 1\}$, $N = \alpha \mathrm{I}_2$, qui est inversible.
- Si $\beta \neq 0$, alors $N = \beta\left(\dfrac{\alpha}{\beta}\mathrm{I}_2 + M\right)$. N est inversible si et seulement si $\dfrac{\alpha}{\beta}$ est une valeur propre de M. Comme M a deux valeurs propres, 1 et -1, c'est le cas si et seulement si $(\alpha,\beta) \in \left\{(1,1),(-1,1),(1,-1),(-1,-1)\right\}$.

Il y a donc 5 matrices non inversibles et 4 matrices inversibles dans $\left(\mathbb{Z}/3\mathbb{Z}\right)[M]$.

D'où $|\mathrm{Stab}(M)| = 4$ et d'après la formule des classes, $|\mathcal{O}_M| = \dfrac{\left|\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)\right|}{|\mathrm{Stab}(M)|} = \dfrac{48}{4} = 12$.

En ajoutant $-\mathrm{I}_2$, cela fait 13 matrices d'ordre 2 dans $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$.

Commentaire

On peut ici facilement s'assurer que les résultats des dernières questions sont cohérents en vérifiant que l'on a bien trouvé les 48 éléments de $\mathrm{GL}_2\left(\mathbb{Z}/3\mathbb{Z}\right)$. Sans oublier qu'il y a un élément d'ordre 1, on a trouvé $8+8+12+6+13+1 = 48$ éléments. Le compte est bon.

2 | 2025 Épreuve 2 – Énoncé

Notations et rappels

Dans tout le sujet, n est un entier naturel non nul. On désigne par $\mathbb{N}$ l'ensemble des entiers naturels, par $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls, par $\mathbb{R}$ le corps des nombres réels, par $\mathbb{R}_+$ l'ensemble des nombres réels positifs ou nuls, par $\mathbb{R}_+^*$ l'ensemble des nombres réels strictement positifs.

On désigne par $\mathcal{M}_n(\mathbb{R})$ le $\mathbb{R}$-espace vectoriel des matrices carrées de taille n à coefficients réels et par $\mathcal{S}_n(\mathbb{R})$ son sous $\mathbb{R}$-espace vectoriel des matrices symétriques. Si $A \in \mathcal{M}_n(\mathbb{R})$, on note A^T sa transposée et $\mathrm{Tr}(A)$ sa trace ; on note $\mathrm{Sp}(A)$ le spectre de A, qui est l'ensemble de toutes ses valeurs propres.

L'espace vectoriel $\mathbb{R}^n$ est muni de son produit scalaire usuel, noté $\langle \cdot, \cdot \rangle$. La norme euclidienne associée est notée $\|\cdot\|$. La base canonique, orthonormée pour le produit scalaire $\langle \cdot, \cdot \rangle$, est notée $\mathcal{F}$. Si $x \in \mathbb{R}^n$, on note x^T son transposé.

On note $\mathcal{S}_n^+(\mathbb{R})$ l'ensemble des matrices symétriques positives, *i.e.* l'ensemble des matrices $A \in \mathcal{S}_n(\mathbb{R})$ telles que

$$\forall x \in \mathbb{R}^n, \quad \langle Ax, x \rangle \geqslant 0.$$

On remarquera qu'une matrice $A \in \mathcal{S}_n(\mathbb{R})$ est symétrique positive si et seulement si

$$\forall x \in \mathbb{R}^n, \quad x^T A x \geqslant 0.$$

On note $\mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies positives, *i.e.* l'ensemble des matrices $A \in \mathcal{S}_n(\mathbb{R})$ telles que

$$\forall x \in \mathbb{R}^n \setminus \{0\}, \quad \langle Ax, x \rangle > 0.$$

On remarquera qu'une matrice $A \in \mathcal{S}_n(\mathbb{R})$ est symétrique définie positive si et seulement si

$$\forall x \in \mathbb{R}^n \setminus \{0\}, \quad x^T A x > 0.$$

La matrice d'un endomorphisme u d'un espace vectoriel E de dimension finie dans une base $\mathcal{B}$ est notée $\mathrm{Mat}_{\mathcal{B}}(u)$.

Soit E un espace vectoriel normé. Dans la suite, on considère E muni de la topologie induite par la norme. Pour toute partie A de E, on note $\mathring{A}$ l'intérieur de A, *i.e.* le plus grand ouvert (au sens de l'inclusion) inclus dans A, $\overline{A}$ l'adhérence de A, *i.e.* le plus petit fermé contenant A.
Le bord ∂A d'une partie $A \subset \mathbb{R}^n$ est défini par $\partial A = \overline{A} \setminus \mathring{A}$; c'est l'adhérence de A privée de l'intérieur de A. Soient A et B deux parties de E telles que $A \subset B$. A est dense dans B si $\overline{A} = B$.
Soit A une partie de E : A est une partie compacte (un compact) de E si de toute suite $(u_n)_{n\in\mathbb{N}}$ d'éléments de A on peut extraire une suite convergeant dans A.

Si $x \in \mathbb{R}^n$ et $r \in \mathbb{R}_+$, la boule ouverte, respectivement fermée, de centre x et de rayon r est notée $B(x,r)$, respectivement $\overline{B}(x,r)$. La boule unité fermée de $\mathbb{R}^n$ pour la norme $\|\cdot\|$ est notée B_2^n. La sphère unité est notée S^{n-1}.

Soit E un espace vectoriel et soit A une partie de E. A est une partie convexe si, pour tout u et pour tout v éléments de A, le segment $[u,v] = \{x \in E,\ \exists t \in [0,1] \text{ tel que } x = (1-t)u + tv\}$ est inclus dans A.

L'espérance d'une variable aléatoire X définie sur un univers probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ est notée, sous réserve d'existence, $\mathbb{E}(X)$.

Définition 1. *Une variable aléatoire X définie sur un univers probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ suit une loi de Rademacher si $X(\Omega) = \{-1, 1\}$ et que $\mathbb{P}(X=1) = \mathbb{P}(X=-1) = \dfrac{1}{2}$.*

Dans tout le sujet, on pourra utiliser librement l'inégalité suivante :

Théorème 2. ***Inégalité arithmético-géométrique.*** *Soit $m \in \mathbb{N}^*$. Soit $(x_1, \dots, x_m) \in (\mathbb{R}_+)^m$. Alors*

$$\left(\prod_{i=1}^{m} x_i\right)^{1/m} \leqslant \frac{1}{m}\sum_{i=1}^{m} x_i,$$

avec égalité si, et seulement si, $x_1 = \cdots = x_m$.

Le sujet est composé d'un vrai/faux, d'un exercice préliminaire et d'un problème en huit parties. Les résultats de l'exercice préliminaire peuvent être utilisés durant le problème.

Vrai/faux

Dire si les assertions suivantes sont vraies ou fausses. On justifiera soigneusement la réponse.

1. Si $f : \mathbb{R} \to \mathbb{R}$ est une fonction continue, la fonction $x \mapsto \displaystyle\int_0^x (x-t)f(t)\mathrm{d}t$ est deux fois dérivable sur $\mathbb{R}$ et sa dérivée seconde est f.
2. L'intégrale $\displaystyle\int_0^{+\infty} \frac{\ln(t)}{1+t^2}\mathrm{d}t$ est convergente et est nulle.
3. Il existe une probabilité $\mathbb{P}$ sur $\mathbb{N}^*$ telle que :
$$\forall k \in \mathbb{N}^*, \quad \mathbb{P}(\{k\}) = \frac{1}{k(k+1)}.$$
4. Si X et Y sont deux variables aléatoires définies sur un univers probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ suivant toutes les deux des lois de Rademacher, alors la variable aléatoire XY suit une loi de Rademacher.
5. Soit E un espace vectoriel normé. Soient A et B deux parties de E telles que $A \subset B$. On suppose que A est dense dans B et que B est dense dans E. Alors A est dense dans E.
6. La réunion de deux parties convexes de $\mathbb{R}^n$ est une partie convexe de $\mathbb{R}^n$.
7. La seule partie convexe dense de $\mathbb{R}$ est $\mathbb{R}$.

Exercice préliminaire

8. Soit Φ l'application définie sur $\mathcal{M}_n(\mathbb{R})^2$ par $\Phi(A,B) = \mathrm{Tr}\left(AB^T\right)$. Montrer que Φ est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

Dans la suite de l'exercice, $\mathcal{M}_n(\mathbb{R})$ est muni de la norme associée au produit scalaire Φ.
On considère $\mathcal{M}_n(\mathbb{R})$ comme un espace topologique avec la topologie définie par cette norme.
Dans la suite, toute partie A de $\mathcal{M}_n(\mathbb{R})$ est munie de la topologie induite de $\mathcal{M}_n(\mathbb{R})$ $\left(O$ est un ouvert de A si, et seulement si, il existe un ouvert U de $\mathcal{M}_n(\mathbb{R})$ tel que $O = U \cap A\right)$.

9. (a) Soit $A \in \mathcal{S}_n(\mathbb{R})$. Montrer que $A \in \mathcal{S}_n^+(\mathbb{R})$ si, et seulement si, $\mathrm{Sp}(A) \subset \mathbb{R}_+$.
   (b) Énoncer et démontrer une caractérisation similaire des matrices de $\mathcal{S}_n^{++}(\mathbb{R})$ à l'aide de leurs spectres.
10. Soient A une matrice de $\mathcal{S}_n^{++}(\mathbb{R})$ et $B \in \mathcal{M}_n(\mathbb{R})$ une matrice inversible.
    Montrer que $B^TAB \in \mathcal{S}_n^{++}(\mathbb{R})$.
11. Montrer que $\mathcal{S}_n^+(\mathbb{R})$ et $\mathcal{S}_n^{++}(\mathbb{R})$ sont convexes.
12. Montrer que $\mathcal{S}_n^+(\mathbb{R})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$.
13. Montrer que $\mathcal{S}_n^{++}(\mathbb{R})$ est dense dans $\mathcal{S}_n^+(\mathbb{R})$.
14. Soit $S \in \mathcal{S}_n^{++}(\mathbb{R})$. Montrer qu'il existe une unique matrice $R \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $R^2 = S$.
    On notera $R = S^{1/2}$.
15. Soit $S \in S_n^{++}(\mathbb{R})$. Justifier que $S^{1/2}$ est inversible, puis que $\left(S^{1/2}\right)^{-1} = \left(S^{-1}\right)^{1/2}$.
    On notera plus simplement $S^{-1/2}$ la matrice $\left(S^{1/2}\right)^{-1}$.

I. Jauge d'un corps convexe symétrique

Définition 3. *Soit C une partie de $\mathbb{R}^n$. On dit que C est un* corps convexe *si C est compact, convexe et que 0 appartient à l'intérieur de C, c'est-à-dire $0 \in \mathring{C}$. On dit que C est symétrique si*

$$\forall x \in \mathbb{R}^n, \quad \left(x \in C\right) \iff \left(-x \in C\right).$$

On notera que cette notion de « corps convexe » n'est aucunement liée avec la notion de corps en algèbre.

16. Montrer que si C est la boule unité d'une norme N définie sur $\mathbb{R}^n$, alors C est un corps convexe symétrique.

Le but de cette partie est de caractériser les corps convexes symétriques de $\mathbb{R}^n$ comme des boules unités d'une certaine norme sur $\mathbb{R}^n$. Pour cela, on va introduire la jauge associée à un corps convexe symétrique :

Définition 4. *Soit C un corps convexe symétrique. On définit sur $\mathbb{R}^n$ l'application J, appelée jauge de C, par :*

$$\forall x \in \mathbb{R}^n, \quad J(x) = \inf\left\{\lambda \in \mathbb{R}_+^*,\ \frac{1}{\lambda}x \in C\right\}.$$

On se donne maintenant un corps convexe symétrique C.

17. Justifier que J, la jauge de C, est bien définie et que $J(0) = 0$.
18. Soit $x \in \mathbb{R}^n$. Montrer que $J(x) = 0$ si, et seulement si, $x = 0$.
19. (a) Montrer que pour tout $x \in \mathbb{R}^n$, pour tout $\mu \in \mathbb{R}_+^*$, $J(\mu x) = \mu J(x)$.
    (b) Montrer que pour tout $x \in \mathbb{R}^n$, pour tout $\mu \in \mathbb{R}$, $J(\mu x) = |\mu| J(x)$.
20. Montrer que $C = \{x \in \mathbb{R}^n,\ J(x) \leqslant 1\}$.
21. Soient x et y deux éléments de $\mathbb{R}^n$. Soit ε un réel strictement positif. On note :

$$x' = \frac{x}{J(x)+\varepsilon} \quad \text{et} \quad y' = \frac{y}{J(y)+\varepsilon}.$$

Soient $\alpha = \dfrac{J(x)+\varepsilon}{J(x)+J(y)+2\varepsilon}$ et $z = \alpha x' + (1-\alpha) y'$.

(a) Montrer que x' et y' appartiennent à C. En déduire que $z \in C$.
(b) En déduire que $J(x+y) \leqslant J(x) + J(y)$.

22. (a) Déduire de ce qui précède que J est une norme.
    (b) Quelle est la boule unité de cette norme J ?
    (c) En déduire que $\partial C = \{x \in \mathbb{R}^n,\ J(x) = 1\}$.
23. Montrer que si N_1 et N_2 sont deux normes de $\mathbb{R}^n$ ayant la même boule unité, alors $N_1 = N_2$.

II. Généralités sur les ensembles convexes

Soit E un espace euclidien, dont on note $\langle \cdot, \cdot \rangle_E$ le produit scalaire. On note $\| \cdot \|_E$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle_E$.
Dans toute cette partie, on désigne par C un convexe compact de E.

24. Soit $a \in E$.
    (a) Montrer qu'il existe $x_a \in C$ tel que $\|a - x_a\|_E = \inf_{x \in C} \|a - x\|_E$. Justifier que si $a \notin C$, alors $\|a - x_a\|_E > 0$
    (b) Soient $x_0, x_1 \in C$ tels que $\|a - x_0\|_E = \|a - x_1\|_E = \inf_{x \in C} \|a - x\|_E$. Montrer que $x_0 = x_1$.
    Indication : on pourra raisonner par l'absurde et considérer $\dfrac{x_0 + x_1}{2}$.

Ainsi, pour tout $a \in E$, il existe un unique $x_a \in C$ tel que $\|a - x_a\|_E = \inf_{x \in C} \|a - x\|_E$.
On définit alors l'application $\pi_C : E \to C$ par la relation $\pi_C(a) = x_a$.

25. Soit $a \in E$.
    (a) Soit l'application $f : E \to \mathbb{R}$ définie par $f(x) = \langle a - \pi_C(a), x \rangle_E$.
    Soit l'ensemble $H = \{x \in E,\ f(x) = f(a)\}$. Justifier que H est un sous-espace affine de E.
    Quelles sont les dimensions possibles pour H ?
    (b) Vérifier que $f(\pi_C(a)) \leqslant f(a)$ et que cette inégalité est stricte si $a \notin C$.
    (c) Montrer que pour tout $x \in C$, $f(x) \leqslant f(\pi_C(a))$.
    Indication : on pourra considérer l'application $g : [0,1] \to \mathbb{R}_+$ qui à t associe

$$\left\| a - \big((1-t)\pi_C(a) + tx\big) \right\|_E^2.$$

(d) Soit $b \in C$ tel que pour tout $x \in C$, $\langle a-b, x-b\rangle_E \leqslant 0$. Pour tout $x \in C$, montrer que $\|a-x\|_E \geqslant \|a-b\|_E$ et en déduire que $b = \pi_C(a)$.

Ainsi, on a montré que pour tout $a \in E$, $\pi_C(a)$ est l'unique point b de C tel que pour tout $x \in C$, $\langle a-b, x-b\rangle_E \leqslant 0$.

26. (a) Soient $a, a' \in E$. Montrer que $\left\|\pi_C(a') - \pi_C(a)\right\|_E^2 \leqslant \left\langle a'-a, \pi_C(a') - \pi_C(a)\right\rangle_E$.

(b) En déduire que π_C est 1-lipschitzienne.

27. Soit $a \in \partial C$. Soit $\left(a_p\right)_{p\in\mathbb{N}}$ une suite d'éléments de $E \setminus C$ qui converge vers a.

(a) Montrer que la suite $\left(\dfrac{a_p - \pi_C(a_p)}{\left\|a_p - \pi_C(a_p)\right\|_E}\right)_{p\in\mathbb{N}}$ est une suite de E et qu'elle possède une sous-suite convergeant vers un élément y de E.

(b) Montrer que y est non nul et que pour tout $x \in C$, $\left\langle y, x-a\right\rangle_E \leqslant 0$.

III. Sur les ellipsoïdes

Définition 5. *Soit $A \in \mathcal{S}_n^{++}(\mathbb{R})$. On appelle* ellipsoïde associé à A *la partie $\mathcal{E}_A$ définie par*

$$\mathcal{E}_A = \left\{x \in \mathbb{R}^n,\ \langle Ax, x\rangle \leqslant 1\right\}.$$

Une partie $\mathcal{E}$ de $\mathbb{R}^n$ est un ellipsoïde *s'il existe $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $\mathcal{E} = \mathcal{E}_A$.*

28. Soit $r > 0$. Montrer que $\overline{B}(0,r)$ (la boule fermée de centre 0 et de rayon r) pour la norme $\|\cdot\|$ est un ellipsoïde de $\mathbb{R}^n$ et préciser une matrice $A_r \in \mathcal{S}_n^{++}$ telle que $\overline{B}(0,r) = \mathcal{E}_{A_r}$.

29. Soit $\mathcal{E}_A$ l'ellipsoïde associé à une matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

(a) Soit $B \in \mathcal{M}_n(\mathbb{R})$ une matrice inversible. Montrer que $B^{-1}\mathcal{E}_A = \left\{B^{-1}x,\ x \in \mathcal{E}_A\right\}$ est un ellipsoïde.

(b) Montrer que $\mathcal{E}_A = A^{-1/2}B_2^n$.

(c) En déduire que $\mathcal{E}_A$ est un corps convexe symétrique.

(d) Quelle est la jauge J_A associée à $\mathcal{E}_A$?

(e) Montrer que cette jauge J_A est une norme euclidienne. On donnera la matrice du produit scalaire associé à cette norme dans la base canonique de $\mathbb{R}^n$.

30. Soient $\mathcal{E}_A$ et $\mathcal{E}_B$ deux ellipsoïdes de $\mathbb{R}^n$, respectivement associés à A et $B \in \mathcal{S}_n^{++}(\mathbb{R})$. Montrer que $\mathcal{E}_A = \mathcal{E}_B$ si et seulement si $A = B$.

31. Soient $\mathcal{E}_A$ et $\mathcal{E}_B$ deux ellipsoïdes de $\mathbb{R}^n$, respectivement associés à A et $B \in \mathcal{S}_n^{++}(\mathbb{R})$. Montrer que $\mathcal{E}_A \subseteq \mathcal{E}_B$ si et seulement si pour tout $x \in E$, $\langle Bx, x\rangle \leqslant \langle Ax, x\rangle$.

Définition 6. *Soit $\mathcal{E}$ un ellipsoïde. On a montré qu'il existe une unique matrice $A \in \mathcal{S}_n^{++}(\mathbb{R})$ telle que $\mathcal{E} = \mathcal{E}_A$. On définit alors la* mesure de $\mathcal{E}$, *noté $\mu(\mathcal{E})$, par*

$$\mu(\mathcal{E}) = \frac{1}{\det(A)}.$$

32. Dans cette question uniquement, on suppose $n = 3$. Soit r un réel strictement positif. Donner une relation entre $\mu\left(\overline{B}(0,r)\right)$ et le volume de $\overline{B}(0,r)$.

33. Soit $\mathcal{E}$ un ellipsoïde de $\mathbb{R}^n$. Soit $B \in \mathcal{M}_n(\mathbb{R})$ une matrice inversible. Préciser la mesure de $B^{-1}\mathcal{E}$ en fonction de la mesure de $\mathcal{E}$.

34. Soit $(e_1,\dots,e_n)$ une base orthonormée de $\mathbb{R}^n$ et soient $a_1,\dots,a_n$ des réels strictement positifs. Soit $\mathcal{E} = \left\{ x = \sum_{i=1}^{n} x_i e_i \in \mathbb{R}^n,\ \sum_{i=1}^{n} a_i x_i^2 \leqslant 1 \right\}$. Montrer que $\mathcal{E}$ est un ellipsoïde de $\mathbb{R}^n$ et calculer sa mesure.

35. Soit $A \in \mathcal{S}_n(\mathbb{R})$.

    (a) Justifier que A admet n valeurs propres réelles (comptées avec leurs ordres de multiplicité) $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$ et qu'il existe une base orthonormée $(f_1,\dots,f_n)$ de $\mathbb{R}^n$ telle que pour tout $i \in \{1,\dots,n\}$, $Af_i = \lambda_i f_i$.

    (b) Soit $k \in [\![1,n]\!]$. Montrer que l'on a

$$\lambda_k = \sup_{V \in G_k} \min_{\substack{x \in V \\ \|x\|=1}} \langle Ax, x\rangle,$$

    où G_k désigne l'ensemble des sous-espaces vectoriels de $\mathbb{R}^n$ de dimension k.
    Indication : si $V \in G_k$, on pourra considérer l'intersection de V avec le sous-espace engendré par $f_k,\dots,f_n$.

36. Soient $\mathcal{E}$ et $\mathcal{E}'$ deux ellipsoïdes de $\mathbb{R}^n$ tels que $\mathcal{E} \subset \mathcal{E}'$. Montrer que $\mu(\mathcal{E}) \leqslant \mu(\mathcal{E}')$.

IV. Existence d'un ellipsoïde de mesure maximale

Soit C un corps convexe symétrique de $\mathbb{R}^n$.

37. Justifier que C est borné et qu'il existe un ellipsoïde $\mathcal{E}'$ tel que $C \subset \mathcal{E}'$.

38. Soit $\mathcal{A} = \{\mu(\mathcal{E}),\ \mathcal{E} \text{ ellipsoïde tel que } \mathcal{E} \subset C\}$. Montrer que $\mathcal{A}$ est non vide et majoré. En déduire qu'il admet une borne supérieure notée α.

39. Justifier qu'il existe une suite $(A_p)_{p\in\mathbb{N}^*}$ d'éléments de $\mathcal{S}_n^{++}(\mathbb{R})$ telle que, en notant $\mathcal{E}_p$ l'ellipsoïde associé à A_p, pour tout $p \in \mathbb{N}^*$, $\mathcal{E}_p \subset C$ et $\lim_{p\to+\infty} \mu(\mathcal{E}_p) = \alpha$.

40. Pour $A \in \mathcal{S}_n(\mathbb{R})$, on pose $N(A) = \sup_{\|x\|=1} |\langle Ax, x\rangle|$. Montrer que N est une norme sur $\mathcal{S}_n(\mathbb{R})$.

41. Soit $p \in \mathbb{N}^*$. On introduit $0 < \lambda_1(p) \leqslant \cdots \leqslant \lambda_n(p)$ les valeurs propres de A_p. Montrer que la suite $(\lambda_1(p))_{p\in\mathbb{N}^*}$ est minorée par un réel strictement positif, puis que la suite $(\lambda_n(p))_{p\in\mathbb{N}^*}$ est majorée.

42. En déduire que la suite $(A_p)_{p\in\mathbb{N}^*}$ est bornée pour la norme N.

43. En déduire qu'il existe $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ strictement croissante et $A \in \mathcal{S}_n^+(\mathbb{R})$ telles que

$$\lim_{p\to+\infty} A_{\varphi(p)} = A.$$

44. Montrer que $A \in \mathcal{S}_n^{++}(\mathbb{R})$.

45. En déduire qu'il existe un ellipsoïde $\mathcal{E}$ de mesure maximale inclus dans C.