

SESSION 2025

---

**AGRÉGATION**  
Concours interne et CAER

Section  
**MATHÉMATIQUES**

Première épreuve

Durée : 6 heures

---

L'usage de tout ouvrage de référence, de tout dictionnaire et de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.

Il appartient au candidat de vérifier qu'il a reçu un sujet complet et correspondant à l'épreuve à laquelle il se présente.

Si vous repérez ce qui vous semble être une erreur d'énoncé, vous devez le signaler très lisiblement sur votre copie, en proposer la correction et poursuivre l'épreuve en conséquence. De même, si cela vous conduit à formuler une ou plusieurs hypothèses, vous devez la (ou les) mentionner explicitement.

**NB : Conformément au principe d'anonymat, votre copie ne doit comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé consiste notamment en la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de la signer ou de l'identifier. Le fait de rendre une copie blanche est éliminatoire.**

**Tournez la page S.V.P.**

## INFORMATION AUX CANDIDATS

Vous trouverez ci-après les codes nécessaires vous permettant de compléter les rubriques figurant en en-tête de votre copie. Ces codes doivent être reportés sur chacune des copies que vous remettrez.

## AGRÉGATION INTERNE MATHÉMATIQUES

► Concours interne de l'Agrégation de l'enseignement public :

Concours	Section/option	Epreuve	Matière
EAI	1300A	101	0540

► Concours interne du CAER / Agrégation de l'enseignement privé :

Concours	Section/option	Epreuve	Matière
EAIH	1300A	101	0540





AGRÉGATION INTERNE ET CAERPA DE MATHÉMATIQUES  
PREMIÈRE ÉPREUVE ÉCRITE

---

## 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  $k \leq n$ , on désigne par  $\llbracket k, n \rrbracket$  l'ensemble des entiers relatifs  $\ell$  tels que  $k \leq \ell \leq n$ .

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  $M^T M = I_2$ , 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  $\chi_u(X) = \det(X \mathrm{Id}_E - u)$  où  $\mathrm{Id}_E$  est l'endomorphisme identité de  $E$ .

**Définition 1.** Soit  $\mathbb{K}$  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  $A^n = I_k$ , son ordre est alors le plus petit entier naturel non nul  $r$  tel que  $A^r = I_k$ .

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  $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$  où  $p$  est un nombre premier.

### Exercice préliminaire 1

Soit  $\mathbb{K}$  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  $\theta_u : \mathbb{K}[X] \longrightarrow \mathrm{End}(E)$  envoyant  $X$  sur  $u$ .

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

2. Montrer que le morphisme  $\theta_u$  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  $\mu_u$  divise  $P$ .

**Définition 2.** Ce polynôme  $\mu_u$  est appelé le polynôme minimal de  $u$ .

4. Soit  $d$  le degré de  $\mu_u$ . Montrer que  $(\mathrm{Id}_E, u, \dots, u^{d-1})$  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  $\mu_u$  divise  $\chi_u$ .

### Exercice préliminaire 2

**Définition 4.** L'application  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  qui à tout entier naturel non nul  $n$  associe le cardinal des entiers  $k \in \llbracket 1, n \rrbracket$  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  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ .
7. Dans  $\mathbb{N}^*$ , résoudre l'inéquation  $\varphi(n) \leq 2$ .

*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  $\varphi(mn) = \varphi(m)\varphi(n)$ .

### Première partie : décomposition de $X^n - 1$ en produit d'irréductibles

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

8. Dans  $\mathbb{C}[X]$ , exprimer à l'aide de  $\omega_n$  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  $\theta$  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  $P_\theta = (X - e^{i\theta})(X - e^{-i\theta})$  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  $\omega_n^m$  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

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

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  $\Phi_n$  pour  $1 \leq n \leq 6$ .
- (c) Soit  $B \in \mathbb{Z}[X]$  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  $\Phi_n$  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

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

## Deuxième partie : un lemme sur les matrices d'ordre fini

Dans cette partie,  $\mathbb{K} = \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$ . On considère une matrice  $A \in \text{GL}_k(\mathbb{K})$  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  $\mu_A$  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.

## Troisième partie : endomorphismes cycliques et décomposition de Frobenius

Dans cette partie, on fixe un corps  $\mathbb{K}$ , un  $\mathbb{K}$ -espace vectoriel  $E$  de dimension finie  $k \geq 1$  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  $n \geq 1$ .

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  $\mu_x$  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  $E = \bigoplus_{i=1}^q \text{Ker} \left( P_i^{m_i}(u) \right)$  et que les sous-espaces  $N_i = \text{Ker} \left( P_i^{m_i}(u) \right)$  sont stables par  $u$ .
- (c) Pour tout  $i \in \llbracket 1, q \rrbracket$ , 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  $(x_0, u(x_0), \dots, u^{k-1}(x_0))$  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  $\text{Mat}_{\mathcal{B}}(u)$  soit la matrice compagnon d'un certain polynôme.
  - iii)  $\chi_u = \mu_u$ .
17. Soit  $u$  un endomorphisme cyclique de  $E$ . On note  $\text{Com}(u) = \{v \in \text{End}(E) \mid v \circ u = u \circ v\}$  l'ensemble des endomorphismes qui commutent avec  $u$ . Justifier que  $\text{Com}(u) = \mathbb{K}[u]$ .
18. Dans cette question, on suppose que  $\mu_u$  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  $\mu_u$ . En déduire la dimension de  $E_x$ .
- (b) Soit  $F$  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  $x_1, \dots, x_p$  de  $E$  tels que

$$E = \bigoplus_{i=1}^p E_{x_i}.$$

19. Dans cette question, on suppose que  $\mu_u$  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  $x_1, \dots, x_p$  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

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

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

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

### Quatrième partie : matrices complexes ou réelles d'ordre fini

20. Dans cette question, on prend  $\mathbb{K} = \mathbb{C}$  et  $A \in \text{GL}_k(\mathbb{C})$  est une matrice d'ordre fini. Par conséquent, il existe un entier  $n$  de  $\mathbb{N}^*$  tel que  $A^n = I_k$ .
- (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  $j \in \llbracket 1, k \rrbracket$ , on note  $n_j$  l'ordre de  $\lambda_j$  dans le groupe  $\mathbb{U}_n$  des racines  $n$ -ièmes de l'unité. Exprimer l'ordre de  $A$  dans le groupe  $\text{GL}_k(\mathbb{K})$  en fonction des  $n_j$ .
  - (c) Montrer que pour tout  $r \in \mathbb{N}^*$ , il existe une matrice  $A_r \in \text{GL}_k(\mathbb{C})$  d'ordre exactement  $r$ .

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

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

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

$$\mu_A = (X - 1)^{\epsilon_1} (X + 1)^{\epsilon_2} P_{\theta_1} \cdots P_{\theta_q}$$

où  $\epsilon_1$  et  $\epsilon_2$  sont des éléments de  $\{0, 1\}$ ,  $P_{\theta_j} = X^2 - 2 \cos(\theta_j)X + 1$  et les  $\theta_j$  sont des éléments de  $2\pi\mathbb{Q} \setminus \pi\mathbb{Z}$  qui sont deux-à-deux distincts.

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

$$\text{Diag}(I_{k_1}, -I_{k_2}, R_{\theta_1}, \dots, R_{\theta_1}, \dots, R_{\theta_q}, \dots, R_{\theta_q}),$$

où chaque bloc  $R_{\theta_j}$  apparaît  $\ell_j$  fois, avec  $k = k_1 + k_2 + 2(\ell_1 + \dots + \ell_q)$  et les  $\theta_j$  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  $A \in \text{GL}_k(\mathbb{R})$  une matrice d'ordre fini. En gardant les notations de la question précédente, et en écrivant  $\theta_j = 2\pi \frac{a_j}{b_j}$  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  $R_\theta$  avec  $\theta \in 2\pi\mathbb{Q}$ .

26. Montrer que pour tout  $r \in \mathbb{N}^*$ , il existe une matrice de  $\text{GL}_2(\mathbb{R})$  d'ordre exactement  $r$ .

27. Soit  $G$  un sous-groupe fini de  $\text{GL}_2(\mathbb{R})$ .

(a) Pour  $u$  et  $v$  des éléments de  $\mathbb{R}^2$ , on pose

$$(u, v)_G = \frac{1}{|G|} \sum_{A \in G} \langle Au, Av \rangle,$$

où  $\langle -, - \rangle$  désigne le produit scalaire canonique de  $\mathbb{R}^2$ . Montrer que  $(-, -)_G$  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  $(u, v)_G = (Au, Av)_G$ .

(b) On note  $S$  l'élément de  $\mathcal{M}_2(\mathbb{R})$  qui est la matrice du produit scalaire  $(-, -)_G$  dans la base canonique de  $\mathbb{R}^2$ . Justifier qu'il existe  $P \in \text{GL}_2(\mathbb{R})$  telle que  $S = P^T P$ , puis montrer que pour tout  $A \in G$ , on a  $PAP^{-1} \in \text{O}_2(\mathbb{R})$ .

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

28. On note  $\text{SO}_2(\mathbb{R})$  le sous-groupe de  $\text{O}_2(\mathbb{R})$  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  $\text{SO}_2(\mathbb{R})$ , 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  $\text{O}_2(\mathbb{R})$  engendré par les matrices

$$A = R_{\frac{2\pi}{n}} = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Montrer que l'on a

$$D_n = \{I_2, A, \dots, A^{n-1}, B, BA, \dots, BA^{n-1}\}.$$

*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  $O_2(\mathbb{R})$  non inclus dans  $SO_2(\mathbb{R})$ .

(a) Montrer que  $G \cap SO_2(\mathbb{R})$  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  $\theta$  est un nombre réel.

(c) Montrer qu'il existe  $P \in SO_2(\mathbb{R})$  tel 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  $SO_2(\mathbb{R})$  au groupe diédral  $D_n$ .

Ainsi, tout sous-groupe fini de  $GL_2(\mathbb{R})$  est isomorphe, soit à un groupe cyclique  $\mathbb{Z}/n\mathbb{Z}$ , soit à un groupe diédral  $D_n$ .

### Cinquième partie : matrices rationnelles d'ordre fini

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

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

où  $q \geq 1$  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

$$\text{Diag}(C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_q}}, \dots, C_{\Phi_{d_q}}),$$

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

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

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

$$\text{Diag}(C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_1}}, \dots, C_{\Phi_{d_q}}, \dots, C_{\Phi_{d_q}}),$$

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

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

(d) On prend  $k = 4$ . Exhiber une matrice  $A \in GL_4(\mathbb{Q})$  d'ordre 12.

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

$$\text{ppcm}\{m, \varphi(m) \leq k\}.$$

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

(a) Montrer que  $A \in GL_2(\mathbb{Q})$  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  $GL_2(\mathbb{Q})$ . En s'appuyant sur les résultats de la quatrième partie, montrer que  $G$  est isomorphe à l'un des groupes suivants :

$$\{I_2\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad D_2, \quad D_3, \quad D_4, \quad D_6.$$

### Sixième partie : matrices d'ordre fini dans $GL_2(\mathbb{Z}/p\mathbb{Z})$

Dans cette partie, on fixe un nombre premier  $p$  et on considère le groupe  $GL_2(\mathbb{Z}/p\mathbb{Z})$ . On rappelle que l'on peut faire agir le groupe  $GL_2(\mathbb{Z}/p\mathbb{Z})$  sur lui-même par conjugaison en posant  $P \cdot M = PMP^{-1}$  ; ainsi, l'orbite  $O_M$  de  $M$  est alors sa classe de similitude et son stabilisateur est

$$\text{Stab}(M) = \{P \in GL_2(\mathbb{Z}/p\mathbb{Z}) \mid PMP^{-1} = M\}.$$

On a alors l'égalité de cardinaux

$$\frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{|\text{Stab}(M)|} = |O_M|.$$

35. Déterminer le cardinal de  $GL_2(\mathbb{Z}/p\mathbb{Z})$ .
36. Soit  $M \in GL_2(\mathbb{Z}/p\mathbb{Z})$ . Justifier que l'algèbre  $(\mathbb{Z}/p\mathbb{Z})[M]$  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  $GL_2(\mathbb{Z}/p\mathbb{Z})$  est majoré par  $p^2 - 1$ .
38. Soit  $M \in GL_2(\mathbb{Z}/p\mathbb{Z})$ . On suppose dans cette question que le polynôme minimal de  $M$  est de degré 2.
  - (a) Justifier que  $\text{Stab}(M) = \mathbb{Z}/p\mathbb{Z}[M] \cap GL_2(\mathbb{Z}/p\mathbb{Z})$ .
  - (b) Montrer que si  $M \in GL_2(\mathbb{Z}/p\mathbb{Z})$  n'admet pas de valeur propre dans  $\mathbb{Z}/p\mathbb{Z}$ , alors on a l'égalité  $|\text{Stab}(M)| = p^2 - 1$ .
  - (c) Montrer que si  $M$  admet une unique valeur propre dans  $\mathbb{Z}/p\mathbb{Z}$ , alors on a  $|\text{Stab}(M)| = p^2 - p$ .

À partir de maintenant et jusqu'à la fin du sujet, on prend  $p = 3$  et on détermine les ordres des éléments de  $GL_2(\mathbb{Z}/3\mathbb{Z})$ , ainsi que le nombre de matrices ayant un ordre donné.

39. Justifier que les ordres possibles pour une matrice de  $GL_2(\mathbb{Z}/3\mathbb{Z})$  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  $M \in GL_2(\mathbb{Z}/3\mathbb{Z})$  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  $\mathbb{Z}/3\mathbb{Z}[X]$  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  $GL_2(\mathbb{Z}/3\mathbb{Z})$  pour qu'elle soit d'ordre 8.
  - (c) Exhiber alors une matrice  $M \in GL_2(\mathbb{Z}/3\mathbb{Z})$  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  $-I_2$  est semblable à  $M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ .

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

————— FIN DU SUJET —————