Agrégation interne CAERPA 2025 épreuve 1.

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 une entier naturel non nul k, on note $\mathrm{GL}_n(\mathbb{K})$ le groupe des matrices inversibles de taille $k \times k$ à coefficients dans $\mathbb{K}$. On désigne par I_k la matrice identité de taille k de $\mathrm{GL}_n(\mathbb{K})$.

On note $\mathrm{O}_2(\mathbb{K})$ le groupe des matrice orthogonales de taille 2, c'est l'ensemble des matrices $M \in \mathcal{M}_2(\mathbb{K})$ telles que $M^{\mathrm{T}}M = I_2$, 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 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 $\mathrm{GL}_n(\mathbb{K})$ 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 $\mathbb{GL}_2(\mathbb{Q})$ 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 $\theta_u : \mathbb{K}[X] \to \mathrm{End}(E)$ envoyant X sur u.
   Démontrons l'existence et l'unicité en raisonnant par analyse-synthèse.
   Analyse.
   Soit $f : \mathbb{K}[X] \to \mathrm{End}(E)$ une application envoyant X sur u.
   Par une récurrence immédiate, si f est un morphisme de $(\mathbb{K}[X], \times)$ dans $(\mathrm{End}(E), \circ)$: $\forall k \in \mathbb{N},\ f(X^k) = u^k$ et donc, $\left(X^k\right)_{k\in\mathbb{N}}$ étant une base de $(\mathbb{K}[X], +, \cdot)$ et f étant linéaire, est nécessairement unique.
   On remarque de plus que : $\forall P \in \mathbb{K}[X],\ \theta_u(P) = P(u)$

   Synthèse.
   Notons $\theta_u : \mathbb{K}[X] \to \mathrm{End}(E)$ l'application définie par : $\forall P \in \mathbb{K}[X],\ \theta_u(P) = P(u)$.

   * $\theta_u(X) = u$.

* Soient $\lambda \in \mathbb{K}$, $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{j=0}^{q} b_j X^j$ deux éléments de $\mathbb{K}[X]$.

$$\begin{aligned}\theta_u(\lambda P + Q) &= (\lambda P + Q)(u)\\ &= \left(\lambda \sum_{i=0}^{p} a_i X^i + \sum_{j=0}^{q} b_j X^j\right)(u)\\ &= \lambda \sum_{i=0}^{p} a_i u^i + \sum_{j=0}^{q} b_j u^j\\ &= \lambda P(u) + Q(u)\end{aligned}$$

Ainsi θ_u est $\mathbb{K}$-linéaire.

* Soient $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{j=0}^{q} b_j X^j$ deux éléments de $\mathbb{K}[X]$.

$$\begin{aligned}\theta_u(P \times Q) &= (P \times Q)(u)\\ &= \left[\left(\sum_{i=0}^{p} a_i X^i\right)\left(\sum_{j=0}^{q} b_j X^j\right)\right](u)\\ &= \left(\sum_{i=0}^{p}\sum_{j=0}^{q} a_i b_j X^{i+j}\right)(u)\\ &= \sum_{i=0}^{p}\sum_{j=0}^{q} a_i b_j u^{i+j}\end{aligned}$$

et

$$\begin{aligned}\theta_u(P) \circ \theta_u(Q) &= \left(\sum_{i=0}^{p} a_i u^i\right) \circ \left(\sum_{j=0}^{q} b_j u^j\right)\\ &= \sum_{i=0}^{p} a_i u^i \left(\sum_{j=0}^{q} b_j u^j\right)\\ &= \sum_{i=0}^{p} a_i \sum_{j=0}^{q} b_j u^i \circ u^j\\ &= \sum_{i=0}^{p}\sum_{j=0}^{q} a_i b_j u^{i+j}\end{aligned}$$

Ainsi : $\theta_u(P \times Q) = \theta_u(P) \circ \theta_u(Q)$ et donc θ_u est un morphisme de $(\mathbb{K}[X], \times)$ dans $(\mathrm{End}(E), \circ)$.

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 θ_u n'est pas injectif.
$\mathbb{K}[X]$ est de dimension infinie et $\mathrm{End}(E)$ de dimension finie donc θ_u ne peut être injectif. En effet $\dim(\mathrm{End}(E)) = (\dim(E))^2$ donc $\left(\mathrm{Id}_E, u, \ldots, u^{(\dim(E))^2}\right)$ est liée donc il existe $P \in \mathbb{K}[X] \setminus \{0\}$ tel que $\theta_u(P) = P(u) = 0$ et donc $\ker(\theta_u) \neq \{0\}$, autrement dit

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 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 $(\mathrm{Id}_E, u \ldots, u^{d-1})$ est une base de $\mathbb{K}[u]$.

On rappelle le théorème de Cayley-Hamilton :

Théorème 3. *Si u est 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 si $\alpha \in \mathbb{N}^*$, alors on a la relation $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
7. Dans $\mathbb{N}^*$, résoudre l'équation $\varphi(n) \leqslant 2$.
   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 $\varphi(mn) = \varphi(m)\varphi(n)$.

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

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

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-ième 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 $P_\theta = \left(X - \mathrm{e}^{i\theta}\right)\left(X - \mathrm{e}^{-i\theta}\right)$ est un polynôme de $\mathbb{R}[X]$ qu 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 $\Phi_n = \prod_{\substack{1 \leqslant m \leqslant n \\ m \wedge n = 1}} (X - \omega_n^m)$. Ce polynôme est appelé le n-ième* polynôme cyclotomique.

11. (a) Justifier que $\mathbb{U}_n = \prod_{d|n} \mathbb{A}_d$, 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) Déterminez Φ_n pour $1 \leqslant n \leqslant 6$.
    (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 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 $X^n - 1 = \prod_{d|n} \Phi_d$.

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 $A \in \mathrm{GL}_n(\mathbb{K})$ d'ordre fini ; son ordre est noté r.

1. Montrer que A est diagonalisable sur $\mathbb{C}$ et que ses valeurs propres sont des racines de l'unité.
2.