MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE
Liberté
Égalité
Fraternité

EAI MAT 1

SESSION 2026

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.

A

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
EAH	1300A	101	0540

IMPRIMERIE NATIONALE – 26 0350 – D'après documents fournis

Notations, rappels et définitions

Soit $\mathbb{K}$ un corps, on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. On note $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$.
Pour $R \in \mathbb{K}[X]$, on notera $d^\circ(R)$ le degré de R. On dira que $R \in \mathbb{K}[X]$ est unitaire si son coefficient dominant vaut 1. Pour $R, S \in \mathbb{K}[X]$, on notera $R \wedge S$ le plus grand diviseur commun de R et S qui sera par convention unitaire.
On dit qu'une matrice M de $\mathcal{M}_n(\mathbb{Z})$ est dans $GL_n(\mathbb{Z})$ si M est inversible dans $\mathcal{M}_n(\mathbb{R})$ et M^{-1} est dans $\mathcal{M}_n(\mathbb{Z})$. On appelle I_n la matrice identité de $\mathcal{M}_n(\mathbb{K})$, qui est la matrice diagonale constituée uniquement de 1 sur la diagonale. On notera M^T la transposée d'une matrice M.
Soit $\mathbb{K}$ un corps, on note $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices de taille $n \times n$ à coefficients dans $\mathbb{K}$ et on note $GL_n(\mathbb{K})$ l'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$. On note $\mathcal{M}_n(\mathbb{Z})$ l'ensemble des matrices de $\mathcal{M}_n(\mathbb{R})$ à coefficients dans $\mathbb{Z}$. On note $O_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}),\ M^TM = I_n\}$ et $O_n(\mathbb{Q}) = \{M \in \mathcal{M}_n(\mathbb{Q}),\ M^TM = I_n\}$. On note $S_n(\mathbb{Z})$ l'ensemble des matrices A de $\mathcal{M}_n(\mathbb{Z})$ telles que $A^T = A$.
Soit $M \in \mathcal{M}_n(\mathbb{K})$, on note χ_M le polynôme caractéristique de M défini par $\chi_M(X) = \det(XI_n - M)$.
Pour i, j deux entiers strictement positifs distincts et $a \in \mathbb{K}$, l'opération élémentaire consistant à ajouter a fois la colonne i à la colonne j d'une matrice se notera $C_j \leftarrow C_j + aC_i$. De même l'opération élémentaire consistant à ajouter a fois la ligne i à la ligne j se notera $L_j \leftarrow L_j + aL_i$.
On notera $(E_{i,j})_{1 \leqslant i,j \leqslant n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$. Ainsi pour i et j dans $[\![1, n]\!]$, la matrice $E_{i,j}$ n'a que des zéros sauf au niveau de la i-ème ligne et j-ème colonne où l'on a un coefficient qui vaut 1.
Soit $M \in \mathcal{M}_n(\mathbb{Q})$. On note $\ell(M)$ le plus petit entier naturel non nul tel que $\ell(M)M$ soit dans $\mathcal{M}_n(\mathbb{Z})$.

Soit p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ et pour a dans $\mathbb{Z}$, on note $\overline{a}$ sa classe dans $\mathbb{F}_p$.
Soit $R = \sum_{k=0}^{n} r_k X^k$ dans $\mathbb{Z}[X]$, on note $\overline{R} = \sum_{k=0}^{n} \overline{r_k} X^k$ qui est un polynôme de $\mathbb{F}_p[X]$.
Soient p un nombre premier et $R = \sum_{k=0}^{n} r_k X^k$ et $S = \sum_{k=0}^{n} s_k X^k$ dans $\mathbb{Z}[X]$. On écrira $R \equiv S[p^2]$ si : $\forall k \in [\![0, n]\!],\ r_k \equiv s_k[p^2]$.
Soit $M = [m_{i,j}]_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}} \in \mathcal{M}_{r,s}(\mathbb{Z})$, on note $\overline{M} = [\overline{m_{i,j}}]_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}}$ la matrice de $\mathcal{M}_{r,s}(\mathbb{F}_p)$ obtenue par réduction modulo p de ses coefficients.
Soient p un nombre premier, $k \in \mathbb{N}^*$ et $M = [m_{i,j}]_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}}$ et $N = [n_{i,j}]_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}}$ dans $\mathcal{M}_{r,s}(\mathbb{Z})$. On écrira $M \equiv N[p^k]$ si : $\forall (i, j) \in [\![1, r]\!] \times [\![1, s]\!],\ m_{i,j} \equiv n_{i,j}[p^k]$.

Soit E un $\mathbb{K}$-espace vectoriel. On notera $\mathcal{L}(E)$ l'ensemble des endomorphismes de E. Soient $\mathcal{B}$ une base de E et $f \in \mathcal{L}(E)$. On notera $Mat_{\mathcal{B}}(f)$ la matrice de f dans la base $\mathcal{B}$ et χ_f le polynôme caractéristique de f défini par $\chi_f(X) = \det\big(XId_E - Mat_{\mathcal{B}}(f)\big)$. Soient F un espace vectoriel ayant pour base $\mathcal{C}$ et, une application linéaire de E dans F, $g \in \mathcal{L}(E, F)$. On notera $Mat_{\mathcal{B},\mathcal{C}}(g)$ la matrice de g dans les bases $\mathcal{B}$ et $\mathcal{C}$.
On rappelle qu'une forme bilinéaire symétrique $\varphi : E \times E \to \mathbb{K}$ définie sur $E \times E$ est non dégénérée si pour tout x dans E on a l'implication :

$$[\forall y \in E,\ \varphi(x, y) = 0] \Rightarrow x = 0.$$

On note $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$. Pour $m, n \in \mathbb{Z}$, tels que $m \leqslant n$, on note $[\![m, n]\!]$ l'intervalle d'entiers relatifs défini par $\{m, m + 1, ..., n - 1, n\}$.

On note $\mathcal{S}_n$ l'ensemble des permutations de $[\![1, n]\!]$.

Pour (i, j) dans $\mathbb{N}^2$, on note δ_{ij} le symbole de Kronecker défini par $\begin{cases} \delta_{ij} = 1 & si \quad i = j \\ \delta_{ij} = 0 & si \quad i \neq j \end{cases}$.

Tournez la page S.V.P. B

Objectif et structure du problème

Ce problème porte sur l'action de conjugaison de $O_n(\mathbb{Q})$ sur $S_n(\mathbb{R}) \cap \mathcal{M}_n(\mathbb{Z})$. Nous y démontrons deux résultats qui feront l'objet des deux dernières parties.

Le sujet débute par un Vrai/Faux. Il est suivi d'un problème en sept parties. Les quatre premières parties sont totalement indépendantes et peuvent être traitées individuellement.

La **partie V** reprend des résultats de la **partie I**.

La **partie VI** utilise les **partie I**, **partie II** et **partie III**.

La **partie VII** utilise toutes les parties précédentes.

Vrai ou faux ?

Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.

1. Soient p un nombre premier et $A \in \mathcal{M}_n(\mathbb{Z})$.
   Affirmation : "Dans $\mathbb{F}_p$, on a $\overline{\det(A)} = \det(\overline{A})$."
2. Soient E et F deux espaces vectoriels admettant respectivement les bases $(e_i)_{1 \leqslant i \leqslant m}$ et $(f_i)_{1 \leqslant i \leqslant n}$.
   Affirmation : "$(e_i, f_j)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ est une base de $E \times F$."
3. Soient E un espace vectoriel de dimension finie et f un endomorphisme de E diagonalisable. Soit F un sous-espace vectoriel de E.
   Affirmation : "Si F est un sous-espace stable par f, alors f induit un endomorphisme diagonalisable sur F."
4. Soient $\mathbb{K}$ un corps, R un polynôme dans $\mathbb{K}[X]$ et R' son polynôme dérivé.
   Affirmation : "Si $R' = 0$, alors R est un polynôme constant."

Partie I. Quelques résultats sur les matrices à coefficients dans $\mathbb{Z}$.

Soit $n \in \mathbb{N}^*$.

5. Soient $Q \in O_n(\mathbb{Q})$ et $A \in \mathcal{M}_n(\mathbb{Z})$ telles que $Q^T A Q$ soit dans $\mathcal{M}_n(\mathbb{Z})$.
   On rappelle que $\ell(Q)$ est le plus petit entier naturel non nul tel que $\ell(Q)Q$ soit dans $\mathcal{M}_n(\mathbb{Z})$.
   On note $\widehat{Q} = \ell(Q)Q$ et on suppose que p est un nombre premier qui divise $\ell(Q)$. Démontrer que $\widehat{Q}^T\widehat{Q} \equiv 0[p^k]$ et $\widehat{Q}^T A \widehat{Q} \equiv 0[p^k]$, pour k dans $\{1, 2\}$ où 0 désigne la matrice nulle.
6. Soit $U \in \mathcal{M}_n(\mathbb{Z})$.
   On rappelle qu'une matrice M de $\mathcal{M}_n(\mathbb{Z})$ est dans $GL_n(\mathbb{Z})$ si M est inversible dans $\mathcal{M}_n(\mathbb{R})$ et M^{-1} est dans $\mathcal{M}_n(\mathbb{Z})$.
   (a) On suppose que U est dans $GL_n(\mathbb{Z})$. Démontrer que $\det(U)$ vaut 1 ou -1.
   (b) On suppose que $\det(U)$ vaut 1 ou -1. Démontrer que U est dans $GL_n(\mathbb{Z})$.
   (c) Montrer que $\big(GL_n(\mathbb{Z}), \times\big)$, où $\times$ désigne le produit matriciel, est un groupe.
7. (a) Soit $M \in O_n(\mathbb{Z})$. Démontrer que sur chaque ligne et chaque colonne de M, on n'a qu'un et un seul coefficient non nul et que celui-ci vaut 1 ou -1.
   (b) En déduire le cardinal de $O_n(\mathbb{Z})$.
8. Soit une permutation $\sigma \in \mathcal{S}_n$. On pose $Q_\sigma = [\delta_{i,\sigma(j)}]_{1 \leqslant i,j \leqslant n}$. Démontrer que $Q_\sigma^T = Q_{\sigma^{-1}}$, puis que Q_σ est dans $O_n(\mathbb{Z})$.

9. Pour i, j des entiers naturels dans $[\![1, n]\!]$, avec $i \neq j$, on pose

$$P_{i,j} = \begin{array}{c} \\ i \to \\ \\ \\ \\ \\ j \to \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & & i & & & j & & \\ & & & \downarrow & & & \downarrow & & \end{array} \\ \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & (0) & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & & 1 & & \\ & & & & 1 & & & & \\ & & & \vdots & & \ddots & \vdots & & \\ & & & & & & 1 & & \\ & & & 1 & \cdots & & 0 & & \\ & & & & & & & 1 & \\ & & (0) & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix} \end{array}$$

la matrice ayant des coefficients nuls en dehors de la diagonale, sauf 1 en position (i, j) et (j, i) ; et, sur la diagonale, on n'a que des 1 sauf en position (i, i) et (j, j) où l'on a 0. On pose $A = [a_{ij}]_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ dans $\mathcal{M}_n(\mathbb{R})$.

(a) Démontrer qu'il existe une permutation $\sigma \in \mathcal{S}_n$ tel que $P_{i,j} = Q_\sigma$.

(b) Démontrer soigneusement que la matrice obtenue à partir de A en échangeant les lignes i et j est le résultat du produit matriciel $P_{i,j}A$.

On admettra de même que l'échange des colonnes i et j de A s'obtient en effectuant le produit matriciel $AP_{i,j}$.

10. Soient $q \in \mathbb{Z}$ et $i, j \in [\![1, n]\!]$ tels que $i \neq j$. On pose

$$T_{i,j}(q) = \begin{array}{c} \\ i \to \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & & j & & \\ & & & & \downarrow & & \end{array} \\ \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & (0) & \\ & & 1 & & -q & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & (0) & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array} = I_n - qE_{i,j},$$

la matrice ayant des coefficients nuls en dehors de la diagonale, sauf $-q$ en position (i, j) ; et, sur la diagonale, on n'a que des 1.

(a) Démontrer que $T_{i,j}(q)$ est dans $GL_n(\mathbb{Z})$.

(b) Démontrer soigneusement que la matrice obtenue à partir de A en effectuant l'opération $C_j \leftarrow C_j - qC_i$ est le résultat du produit matriciel $AT_{i,j}(q)$.

(c) Donner, sans démonstration, une matrice $S_{i,j}(q)$ dans $GL_n(\mathbb{Z})$ telle que $S_{i,j}(q)A$ est la matrice obtenue en effectuant l'opération $L_j \leftarrow L_j - qL_i$ sur la matrice A.

Tournez la page S.V.P.

Partie II. Résultant et applications

Soient des entiers naturels $m, n \in \mathbb{N}^*$, avec $m \geqslant 2$. Soient $R = \sum_{k=0}^{m} r_k X^k$ et $S = \sum_{k=0}^{n} s_k X^k$ deux polynômes de $\mathbb{K}[X]$, avec R de degré exactement m et S de degré au plus n. On pose

$$\varphi_{R,S} : \left\{ \begin{array}{ccc} \mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X] & \to & \mathbb{K}_{n+m-1}[X] \\ (G,H) & \mapsto & GR + HS \end{array} \right. .$$

On pose $D = R \wedge S$ et $d = d^\circ(D)$.
On note

$$\psi_R = \varphi_{R,R'} : \left\{ \begin{array}{ccc} \mathbb{K}_{m-2}[X] \times \mathbb{K}_{m-1}[X] & \to & \mathbb{K}_{2m-2}[X] \\ (G,H) & \mapsto & GR + HR' \end{array} \right.$$

et $\Delta(R) = \det(\psi_R)$.

11. Démontrer le lemme de Gauss ; à savoir, étant donnés trois polynômes $G, H, L \in \mathbb{K}[X]$, si $G \wedge H = 1$ et $G|HL$, alors on a $G|L$.
12. Démontrer que $\varphi_{R,S}$ est une application linéaire de $\mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X]$ dans $\mathbb{K}_{n+m-1}[X]$.
13. Soit la famille $\mathcal{U} = \big((1,0),(X,0),\dots,(X^{n-1},0),(0,1),(0,X),\dots,(0,X^{m-1})\big)$. Démontrer que $\mathcal{U}$ est une base de $\mathbb{K}_{n-1}[X] \times \mathbb{K}_{m-1}[X]$.
14. Expliciter les coefficients de $Mat_{\mathcal{U},\mathcal{V}}(\varphi_{R,S})$, avec $\mathcal{V} = (1, X, ..., X^{m+n-1})$ la base canonique de $\mathbb{K}_{n+m-1}[X]$.
15. Soient deux polynômes $R_1, S_1 \in \mathbb{K}[X]$ tels que $R = DR_1$ et $S = DS_1$.
Démontrer que $\mathrm{Ker}(\varphi_{R,S}) = \big\{(S_1W, -R_1W),\ W \in \mathbb{K}_{d-1}[X]\big\}$ et en déduire $\dim\big(\mathrm{Ker}(\varphi_{R,S})\big)$.
16. Déterminer $\mathrm{Im}(\varphi_{R,S})$.
17. Démontrer que si R a un facteur multiple dans sa décomposition en facteurs irréductibles, alors on a $\Delta(R) = 0$.
18. On suppose que $\dim \mathrm{Ker}(\psi_R) = 1$.
    (a) Démontrer qu'il existe $\lambda \in \mathbb{K}$ et $T \in \mathbb{K}[X]$ tels que $T(\lambda) \neq 0$ et $R = (X-\lambda)^2 T$.
    (b) Démontrer dans ce cas que $\mathrm{Ker}(\psi_R) = \mathrm{vect}\big((2T + (X-\lambda)T', -(X-\lambda)T)\big)$.
19. Démontrer que s'il existe deux polynômes $T, W \in \mathbb{K}[X]$, avec $d^\circ(T) \geqslant 2$ tels que $R = T^2W$, alors on a l'inégalité $\dim\big(\mathrm{Ker}(\psi_R)\big) \geqslant 2$.
20. En déduire que si $\dim \mathrm{Ker}(\psi_R) = 1$, alors il existe des scalaires $\lambda \in \mathbb{K}$, $\mu \in \mathbb{K}\backslash\{0\}$ et des polynômes $T_1, ..., T_r \in \mathbb{K}[X]$ deux à deux distincts et irréductibles tels que l'on a la décomposition $R = \mu(X-\lambda)^2 \prod_{i=1}^{r} T_i$ avec $\forall i \in [\![1, r]\!],\ T_i(\lambda) \neq 0$.

Partie III. Quelques résultats d'algèbre linéaire sur les sous-espaces stables

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 2$ et F un sous-espace vectoriel de E, de dimension $s \geqslant 1$ avec $s < n$; on fixe une base $\mathcal{B}_1 = (e_1, ..., e_s)$ de F.

On considère une forme bilinéaire symétrique $\varphi : E \times E \to \mathbb{K}$ non dégénérée (on renvoie aux notations pour la définition de ce point) qui vérifie la propriété $\forall x, y \in F,\ \varphi(x,y) = 0$. De plus, on note $F^\circ = \big\{x \in E / \ \forall y \in F,\ \varphi(x,y) = 0\big\}$.

Soit un endomorphisme $f \in \mathcal{L}(E)$ tel que F soit stable par f, c'est-à-dire que l'on a $f(F) \subset F$. On suppose que cet endomorphisme satisfait la propriété

$$\forall x, y \in E,\ \varphi\big(f(x), y\big) = \varphi\big(x, f(y)\big).$$

Enfin, on note $g : \left\{ \begin{array}{ccc} F & \to & F \\ x & \mapsto & f(x) \end{array} \right.$ l'endomorphisme induit par f sur F et $\Gamma = \chi_g$ le polynôme caractéristique de g.

21. On suppose, uniquement dans cette question, que $\text{rang}(f) = n - 1$.
Soient $u \in \text{Ker}(f) \backslash \{0\}$ et $v \in E$ tels que $\varphi(u, v) = 0$.
   (a) Démontrer que l'on a
   $$\forall x \in vect(v) + \text{Im}(f),\ \varphi(u, x) = 0.$$
   (b) En déduire que v est dans $\text{Im}(f)$.
22. En faisant intervenir une récurrence, démontrer que
$$\forall S \in \mathbb{K}[X], \forall x, y \in E,\ \varphi\big(S(f)(x), y\big) = \varphi\big(x, S(f)(y)\big).$$
23. (a) Soit $\mathcal{J}$ un sous-espace vectoriel de $\mathbb{K}^s$ tel que l'on a $\dim(\mathcal{J}) < s$. Montrer qu'il existe des éléments $a_1, ..., a_s \in \mathbb{K}$ non tous nuls tels que
$$\forall (y_1, ..., y_s) \in \mathcal{J},\ \sum_{i=1}^{s} a_i y_i = 0.$$
   (b) En déduire que l'application linéaire $\psi : \left\{ \begin{array}{ccc} E & \to & \mathbb{K}^s \\ x & \mapsto & (\varphi(x, e_1), ..., \varphi(x, e_s)) \end{array} \right.$ est surjective.
   (c) En déduire l'égalité $\dim(F^\circ) = n - s$.
24. Démontrer que l'on a
$$\forall x \in F,\ \Gamma(f)(x) = 0.$$
25. On suppose, uniquement dans cette question, que le vecteur e_1 n'est pas dans $\text{Im}(\Gamma(f))$.
   (a) Démontrer que l'on a l'inclusion $\text{Im}(\Gamma(f)) \oplus vect(e_1) \subset F^\circ$.
   (b) En déduire l'inégalité : $\text{rang}\left(\Gamma(f)^2\right) \leqslant n - (s + 1)$.
26. On suppose, uniquement dans cette question, qu'il existe un vecteur z de E tel que $e_1 = \Gamma(f)(z)$.
   (a) Démontrer que la famille $(e_1, ..., e_s, z)$ est libre dans E.
   (b) En déduire l'inégalité : $\text{rang}\left(\Gamma(f)^2\right) \leqslant n - (s + 1)$.
27. Démontrer qu'il existe des vecteurs $e_{s+1}, ..., e_n$ de E tels que $\mathcal{B} = (e_1, ..., e_s, e_{s+1}, ..., e_n)$ soit une base de E de telle sorte que $Mat_{\mathcal{B}}(f) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ et $A = Mat_{\mathcal{B}_1}(g)$. On précisera la taille des matrices B et C.
28. Démontrer l'inégalité $\text{rang}(\Gamma(f)^2) \geqslant \text{rang}(\Gamma(C)^2)$.
29. (a) On suppose que les polynômes Γ et χ_C sont premiers entre eux. Dans ce cas, démontrer que la matrice $\Gamma(C)$ est inversible.
   (b) À l'aide des questions précédentes, mettre en évidence une contradiction dès lors que Γ et χ_C sont des polynômes qui sont premiers entre eux.
   (c) Démontrer que χ_f a un moins un facteur multiple dans sa décomposition en facteurs irréductibles.
30. On suppose que $\chi_f = (X - \lambda)^2 S$, avec S un polynôme sans facteurs multiples dans sa décomposition en facteurs irréductibles.
Démontrer que $(X - \lambda) | \Gamma$ et $(X - \lambda) | \chi_C$, puis qu'il existe $u \in F$ non nul tel que $f(u) = \lambda u$.

Tournez la page S.V.P.

Partie IV. Arithmétique des polynômes dans $\mathbb{F}_p[X]$

Soit un entier naturel $n \in \mathbb{N}^*$. Dans cette partie, p désignera un nombre premier. Fixons un polynôme $R = \sum_{k=0}^{n} r_k X^k \in \mathbb{F}_p[X]$ de degré n unitaire.

31. Soit $k \in [\![1, p-1]\!]$, démontrer que l'on a $p | \binom{p}{k}$.

32. Démontrer que l'application $F : \left\{ \begin{array}{ccc} \mathbb{F}_p[X] & \to & \mathbb{F}_p[X] \\ S & \mapsto & S^p \end{array} \right.$ est un morphisme d'anneaux.

33. Soit $a \in \mathbb{F}_p \backslash \{\overline{0}\}$, démontrer que $a^{p-1} = \overline{1}$. En déduire que l'on a

$$\forall x \in \mathbb{F}_p,\ x^p = x.$$

34. On suppose que R', le polynôme dérivé de R, vérifie la relation $R' = \overline{0}$.
    (a) Démontrer que $R = \sum_{l=0}^{\lfloor n/p \rfloor} r_{lp} X^{lp}$, où $\lfloor n/p \rfloor$ désigne la partie entière de n/p.
    (b) En déduire qu'il existe $W \in \mathbb{F}_p[X]$ tel que $R = W^p$.

35. On suppose que $R = (X-\lambda)^2 \prod_{i=1}^{r} T_i$, avec $\lambda \in \mathbb{F}_p$ et $T_1, ..., T_r \in \mathbb{F}_p[X]$ des polynômes deux à deux distincts et irréductibles dans $\mathbb{F}_p[X]$ qui vérifient $\forall i \in [\![1, r]\!],\ T_i(\lambda) \neq \overline{0}$.
    (a) Soit $j \in [\![1, r]\!]$ tel que $T_j | R'$. Démontrer que $T_j' = \overline{0}$.
    (b) En déduire que $R \wedge R' = X - \lambda$.

Partie V. Forme normale de Smith

*Dans cette partie, on pourra s'aider des résultats obtenus dans la **partie I**.*
Soit un entier naturel $n \in \mathbb{N}^*$. Soit une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ non nulle, on note

$$\mu(M) = \min\{|m_{i,j}|,\ i, j \in [\![1, n]\!] \text{ et } m_{i,j} \neq 0\}.$$

Nous allons démontrer qu'il existe des matrices U et V dans $GL_n(\mathbb{Z})$ et une matrice diagonale

$$\Omega = \begin{pmatrix} d_1 & 0 & 0 & & \cdots & & 0 \\ 0 & d_2 & 0 & & \cdots & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ \vdots & & & d_r & & & \vdots \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & & 0 \end{pmatrix}$$

dans $\mathcal{M}_n(\mathbb{Z})$ telles que $M = U\Omega V$, avec $d_1, ..., d_r$ non nuls qui vérifient $\forall i \in [\![1, r-1]\!],\ d_i | d_{i+1}$.

36. Soient des entiers naturels $i, j \in [\![1, n]\!]$, avec $i \neq j$. *On reprend la notation $P_{i,j}$ des matrices définies la **partie I**.*
    Démontrer que $\mu(P_{i,j} M) = \mu(M P_{i,j})$.

37. Démontrer qu'il existe des matrices $P_0, Q_0 \in GL_n(\mathbb{Z})$ telles que

$$\forall P, Q \in GL_n(\mathbb{Z}),\ \mu(P_0 M Q_0) \leqslant \mu(PMQ).$$

38. On pose la matrice $A = P_0MQ_0 = [a_{i,j}]_{1\leqslant i,j\leqslant n}$. Quitte à modifier P_0 et Q_0, démontrer que, l'on peut supposer que : $|a_{1,1}| = \mu(A)$, puis que : $a_{1,1} = \mu(A)$.

Dans la suite, on se place donc dans le cas où l'on a $a_{1,1} = \mu(A)$

39. Soit un entier $j \in [\![2, n]\!]$. Notons q_j le quotient et r_j le de reste la division euclidienne de $a_{1,j}$ par $a_{1,1}$ ce qui conduit à la relation $a_{1,j} = a_{1,1}q_j + r_j$.
Soit $\widetilde{A}$ la matrice obtenue à partir de la matrice A après les opérations élémentaires $C_j \leftarrow C_j - q_jC_1$, pour tout j de $[\![2, n]\!]$.
   (a) S'il existe $j_0 \in [\![2, n]\!]$ tel que $r_{j_0} \neq 0$, démontrer l'inégalité $\mu(\widetilde{A}) < \mu(A)$.
   (b) En déduire que $\widetilde{A}$ est de la forme $\begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ u_{2,1} & u_{2,2} & \cdots & u_{2,n} \\ \vdots & \vdots & & \vdots \\ u_{n,1} & u_{n,2} & \cdots & u_{n,n} \end{pmatrix}$ et que $\forall j \in [\![2, n]\!],\ a_{1,1}|a_{1,j}$.

40. Démontrer qu'il existe des matrices $P_1, Q_1 \in GL_n(\mathbb{Z})$ telles que la matrice $B = P_1MQ_1$ soit de la forme $B = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n,2} & \cdots & b_{n,n} \end{pmatrix}$ avec $\mu(B) = \min\{\mu(PMQ),\ P, Q \in GL_n(\mathbb{Z})\}$.

41. Soit un entier naturel $i \in [\![2, n]\!]$. Soit $\widetilde{B}$ la matrice obtenue à partir de B en effectuant l'opération $L_1 \leftarrow L_1 + L_i$.
   (a) Démontrer l'égalité $\mu(\widetilde{B}) = \mu(B)$.
   (b) En utilisant le résultat de la question 39b et en s'aidant de la matrice $\widetilde{B}$, démontrer que l'on a

$$\forall i, j \in [\![2, n]\!],\ a_{1,1}|b_{i,j}.$$

On peut donc écrire $B = \begin{pmatrix} d_1 & 0 \\ 0 & d_1N \end{pmatrix}$, avec N une matrice dans $\mathcal{M}_{n-1}(\mathbb{Z})$.

42. Démontrer que pour toute matrice M de $\mathcal{M}_n(\mathbb{Z})$ non nulle, il existe des matrices U et V dans $GL_n(\mathbb{Z})$ et une matrice diagonale

$$\Omega = \begin{pmatrix} d_1 & 0 & 0 & & \cdots & & 0 \\ 0 & d_2 & 0 & & \cdots & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ \vdots & & & d_r & & & \vdots \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & & 0 \end{pmatrix}$$

dans $\mathcal{M}_n(\mathbb{Z})$ telles que $M = U\Omega V$, avec $d_1, ..., d_r$ des entiers non nuls qui vérifient $\forall i \in [\![1, r-1]\!],\ d_i|d_{i+1}$.
Cette décomposition s'appelle la forme normale de Smith.

43. Soient une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ non nulle décomposée comme dans la question 42 et soit p un nombre premier. On suppose qu'il existe une matrice colonne $Y \in \mathcal{M}_{n,1}(\mathbb{Z})$ telle que $Y \not\equiv 0[p]$ et $MY \equiv 0[p^2]$.
   (a) Si $r = n$, démontrer que $p^2|d_n$.

(b) Démontrer que $p^2 | \det(M)$.

Partie VI. Preuve du premier résultat

On reprend les notations des parties précédentes, et on rappelle que $\ell(Q)$ est le plus petit entier naturel non nul tel que $\ell(Q)Q$ soit dans $\mathcal{M}_n(\mathbb{Z})$.

On rappelle la notation suivante, étant donnée une matrice $M = [m_{i,j}]_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} \in \mathcal{M}_{n,p}(\mathbb{Z})$, on note $\overline{M} = [\overline{m_{i,j}}]_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ la matrice de $\mathcal{M}_{n,p}(\mathbb{F}_p)$, avec $\overline{m_{i,j}}$ la classe de $m_{i,j}$ dans $\mathbb{F}_p$. Étant données deux matrices $M \in \mathcal{M}_{r,s}(\mathbb{Z})$ et $N \in \mathcal{M}_{s,t}(\mathbb{Z})$, on pourra utiliser la relation $\overline{MN} = \overline{M}\,\overline{N}$ sans démonstration.

*Cette partie fait uniquement appel à des résultats des parties **I.**, **II.** et **III.**.*

Soit un entier naturel $n \in \mathbb{N}$ tel que $n \geqslant 2$ et soit une matrice $Q \in O_n(\mathbb{Q})$. On notera $\widehat{Q} = \ell(Q)Q$ et $C_1, ..., C_n$ les colonnes de $\widehat{Q}$.

Soit une matrice $A \in S_n(\mathbb{Z})$, on note[1] Δ_A l'entier relatif $\Delta_A = \Delta(\chi_A)$. L'objet de cette partie consiste à démontrer le résultat suivant :

Si la matrice $Q^T AQ$ est dans $S_n(\mathbb{Z})$, alors pour tout diviseur premier p de $\ell(Q)$, on a $p|\Delta_A$.

Dans cette partie, on suppose que la matrice $B = Q^T AQ$ est dans $S_n(\mathbb{Z})$.

44. Soit $\mathbb{K}$ un corps.

Soit l'application $\varphi : \begin{cases} (\mathcal{M}_{n,1}(\mathbb{K}))^2 & \to & \mathbb{K} \\ (Y,Z) & \mapsto & Y^T Z \end{cases}$. Démontrer que φ est une forme bilinéaire symétrique non dégénérée.

Pour toute la suite de cette partie, on prendra $\mathbb{K} = \mathbb{F}_p$, avec p un nombre premier qui divise $\ell(Q)$.

45. (a) Démontrer que l'on a
$$\forall i, j \in [\![1, n]\!],\ \varphi(\overline{C_i}, \overline{C_j}) = \overline{0}.$$

(b) Démontrer que l'on a
$$\forall (Y,Z) \in \mathrm{Im}\left(\overline{\widehat{Q}}\right)^2,\ \varphi(Y,Z) = \overline{0}.$$

46. Démontrer que $\mathrm{Im}\left(\overline{\widehat{Q}}\right)$ est stable par l'application $Y \mapsto \overline{A}.Y$ définie sur $\mathcal{M}_{n,1}(\mathbb{F}_p)$.

47. Démontrer l'inégalité $\dim\left(\mathrm{Im}\left(\overline{\widehat{Q}}\right)\right) < n$.

48. En utilisant la partie **III.**, démontrer que le polynôme $\chi_{\overline{A}}$ possède au moins un facteur multiple dans sa décomposition en facteurs irréductibles sur $\mathbb{F}_p[X]$.

49. En déduire que l'on a $p|\Delta_A$.

1. On se réfère à la notation de la **PartieII.**

Partie VII. Preuve du second résultat

On reprend les notations des parties précédentes.

Soit un entier naturel $n \in \mathbb{N}$ tel que $n \geqslant 2$ et soit une matrice $Q \in O_n(\mathbb{Q})$. On note $\widehat{Q} = \ell(Q)Q$. On note $C_1, ..., C_n$ les colonnes de $\widehat{Q}$. Soit une matrice $A \in S_n(\mathbb{Z})$. On note $\Delta_A = \Delta(\chi_A)$.

L'objet de cette partie consiste à démontrer le résultat suivant :

Si $Q^T AQ$ est dans $S_n(\mathbb{Z})$ et si Δ_A est un entier impair sans facteurs multiples dans sa décomposition en facteurs premiers, alors Q est dans $O_n(\mathbb{Z})$.

Dans la suite de cette partie, on suppose que $Q^T AQ$ est dans $S_n(\mathbb{Z})$ et que Δ_A est un entier impair sans facteurs multiples dans sa décomposition en facteurs premiers. De plus, p désignera un nombre premier impair qui divise $\ell(Q)$; d'après la partie précédente on sait que $p|\Delta_A$, par conséquent l'hypothèse faite sur Δ_A implique que p^2 ne divise pas Δ_A.

50. Soient un entier naturel $l \in \mathbb{N}^*$ et une matrice $M \in \mathcal{M}_l(\mathbb{Z})$ tels que le rang de $\overline{M}$ dans $\mathcal{M}_l(\mathbb{F}_p)$ vérifie $\text{rang}(\overline{M}) = l - k$, avec k dans $[\![0, l]\!]$.
    (a) Démontrer qu'il existe deux matrices $B \in \mathcal{M}_l(\mathbb{Z})$ et $C \in \mathcal{M}_{l-k,l}(\mathbb{Z})$ telles que l'on a les deux égalités $\overline{BM} = \begin{pmatrix} \overline{C} \\ \hline \overline{O} \end{pmatrix}$, où O désigne la matrice mulle, et $\det(\overline{B}) \neq \overline{0}$.
    (b) En déduire que $p^k | \det(B) \det(M)$.
    (c) Puis, en déduire que $p^k | \det(M)$.
51. En reprenant les notations de la partie **II.**, avec $\mathbb{K} = \mathbb{F}_p$, démontrer que $\text{Ker}(\psi_{\overline{\chi_A}})$ est de dimension 1.
52. Montrer qu'il existe un entier relatif $\lambda \in \mathbb{Z}$ et un polynôme $S \in \mathbb{Z}[X]$ unitaire de degré $n-2$ tels que l'on a $\overline{\chi_A} = (X - \overline{\lambda})^2 \overline{S}$, avec $\overline{S}$ sans facteurs multiples dans sa décomposition en facteurs irréductibles dans $\mathbb{F}_p[X]$ et $\overline{S(\lambda)} \neq \overline{0}$.
    *On pourra s'aider des résultats de la partie **II**.*
53. En utilisant la question 30, la partie **II.** et la partie **IV.**, démontrer qu'il existe une matrice colonne $Y \in \mathcal{M}_{n,1}(\mathbb{Z})$ telle qu'il existe des entiers relatifs $\beta_1, ..., \beta_n \in \mathbb{Z}$ vérifiant
$$\overline{Y} = \sum_{i=1}^{n} \overline{\beta_i}.\overline{C_i}$$
    avec $\overline{Y} \neq \overline{0}$ et $\overline{A}.\overline{Y} = \overline{\lambda}.\overline{Y}$.
54. On suppose dans cette question que le rang de la matrice $\overline{\lambda}.\overline{I_n} - \overline{A}$ de $\mathcal{M}_n(\mathbf{F}_p)$ vaut $n-1$. Soit la matrice colonne $Z = \dfrac{1}{p}(AY - \lambda Y)$, avec Y la matrice trouvée dans la question précédente.
    (a) Démontrer que $\overline{Y}^T \overline{Z} = \overline{0}$. On pourra utiliser la question 5.
    (b) En utilisant la question 21, démontrer qu'il existe une matrice colonne $Y_1 \in \mathcal{M}_{n,1}(\mathbb{Z})$ telle que
$$\overline{Z} = (\overline{A} - \overline{\lambda}.\overline{I_n})\overline{Y_1}.$$
    (c) En déduire qu'il existe une matrice colonne $Y_2 \in \mathcal{M}_{n,1}(\mathbb{Z})$ telle que
$$\overline{Y_2} \neq \overline{0} \text{ et } (A - \lambda I_n)Y_2 \equiv 0[p^2]$$
    puis que $p^2 | \chi_A(\lambda)$.
    On pourra utiliser la question 43b pour cette dernière relation.

Tournez la page S.V.P.

55. (a) Démontrer qu'il existe deux polynômes R_1 et R_2 dans $\mathbb{Z}[X]$, avec $d^\circ(R_1) < n-1$ tels que
$$\chi_A = (X-\lambda)^2 S + p(X-\lambda)R_1 + p^2 R_2.$$

(b) Comment peut-on choisir μ dans $\mathbb{Z}$ de telle sorte que $\overline{\left(\frac{R_1+2\mu S}{X-\lambda}\right)}$ définisse un polynôme de $\mathbb{F}_p[X]$ de degré au plus $n-3$?

On note $H \in \mathbb{Z}[X]$ de degré au plus $n-3$ tel que $\overline{\left(\frac{R_1+2\mu S}{X-\lambda}\right)} = \overline{H}$, pour ce μ.

(c) On pose les polynômes $T = 2S+(X-\lambda)S'+pR_1'+pH+\mu pS'$ et $W = (X-\lambda)S+pR_1+\mu pS$, avec μ choisi comme dans la question précédente.
Démontrer que $\overline{W}$ est non nul dans $\mathbb{F}_p[X]$ et que $d^\circ(T) < n-1$ et $d^\circ(W) < n$.

(d) Démontrer que l'on a $T\chi_A \equiv W\chi_A'[p^2]$.

56. En s'aidant des questions 14 et 43b, mettre en évidence une contradiction

57. Démontrer que si la matrice $Q^T AQ$ est dans $S_n(\mathbb{Z})$ et si l'entier Δ_A est impair sans facteurs multiples dans sa décomposition en facteurs premiers, alors Q est dans $O_n(\mathbb{Z})$.

FIN DU SUJET