4

Agrégation interne 1996, épreuve 1

Dans tout le problème $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ désignent les ensembles de nombres habituels.

Pour $\mathbb{E} \in \{\mathbb{Z}, \mathbb{R}, \mathbb{C}\}$ on note $\mathcal{M}_n(\mathbb{E})$ l'algèbre des matrices (n, n) $(n \in \mathbb{N}^*)$ à coefficients dans $\mathbb{E}$. La matrice unité est notée I_n ; $\mathrm{tr}(A)$ désigne la trace de l'élément A de $\mathcal{M}_n(\mathbb{E})$ et $\det(A)$ son déterminant.

Pour $\mathbb{E} \in \{\mathbb{Z}, \mathbb{R}, \mathbb{C}\}$, $\mathbb{E}[X]$ désigne l'anneau des polynômes à coefficients dans $\mathbb{E}$. Un polynôme non nul est dit unitaire si, et seulement si, le coefficient de son terme dominant est 1.

Dans le cadre de ce problème une matrice A de $\mathcal{M}_n(\mathbb{E})$ est appelée matrice cyclique si, et seulement si, il existe un entier naturel non nul p tel que $A^p = I_n$; le plus petit entier naturel non nul p réalisant cette égalité est appelé ordre de la matrice cyclique A ; c'est l'ordre du groupe cyclique engendré par A ; il sera noté $h(A)$.

L'ensemble des matrices cycliques de $\mathcal{M}_n(\mathbb{E})$ est noté $\mathcal{C}_n(\mathbb{E})$. Nous appellerons groupe de $\mathcal{C}_n(\mathbb{E})$ toute partie de $\mathcal{C}_n(\mathbb{E})$ muni d'une structure de groupe pour le produit matriciel.

L'objet du problème est l'étude de propriétés des éléments et des groupes de $\mathcal{C}_n(\mathbb{Z})$, ainsi que la mise en évidence de représentations géométriques de certains groupes de $\mathcal{C}_n(\mathbb{Z})$ pour $n = 2, 3$ ou 4.

Partie I

Cette partie a pour but de déterminer $h(A)$ pour $A \in \mathcal{C}_2(\mathbb{Z})$ et de montrer que, pour $n \geq 2$, $\mathcal{C}_n(\mathbb{Z})$ n'est pas un groupe pour le produit matriciel.

Soit A une matrice cyclique de $\mathcal{C}_n(\mathbb{Z})$, d'ordre $h(A) = p$.

Pour $n = 2$, on notera $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

1.
   (a) En considérant A comme un élément de $\mathcal{C}_n(\mathbb{C})$, montrer que A est diagonalisable sur $\mathbb{C}$, et que ses valeurs propres $\lambda_1, \lambda_2, \cdots, \lambda_n$ sont des racines p-èmes de l'unité.

   (b) Soit $q_i = \min\{q \in \mathbb{N}^* \mid \lambda_i^q = 1\}$ pour $i = 1, \cdots, n$. Prouver que $h(A) = \underset{1 \leq i \leq n}{\mathrm{ppcm}}(q_i)$.

   (c) Prouver que $\mathrm{tr}(A) \in \{-n, -(n-1), \cdots, -1, 0, 1, \cdots, n-1, n\}$ et que $\det(A) = \pm 1$.

2. Démontrer que, pour tout entier naturel $n \geq 2$ et toute suite $(z_1, \cdots, z_n)$ de nombres complexes non nuls, l'égalité :

$$\left|\sum_{k=1}^{n} z_k\right| = \sum_{k=1}^{n} |z_k|$$

est réalisée si, et seulement si, il existe suite $(\alpha_2, \cdots, \alpha_n)$ de nombres réels strictement positifs telle que :

$$\forall k \in \{2, \cdots, n\}, \ z_k = \alpha_k z_1.$$

3. On pose $\varepsilon = \pm 1$. On suppose que $\mathrm{tr}\,(A) = n\varepsilon$. Prouver que toutes les valeurs propres de A sont égales à ε, que $A = \varepsilon I_n$ et que $h\,(A) = \dfrac{1}{2}\,(3-\varepsilon)$.

4. On pose $\varepsilon = \pm 1$ et on suppose que $n = 2$.

   (a) On suppose que A a deux valeurs propres réelles distinctes λ_1 et λ_2.
   Prouver que $\lambda_1 = \varepsilon$, $\lambda_2 = -\varepsilon$ et que $h\,(A) = 2$.
   Prouver qu'il existe une infinité de matrices A satisfaisant à cette condition.

   (b) On suppose que A a deux valeurs propres non réelles λ_1 et λ_2.
   Déterminer ces valeurs propres λ_1 et λ_2, puis $h\,(A)$ dans les trois cas suivants :

   $$\mathrm{tr}\,(A) = -1, \ \mathrm{tr}\,(A) = 0, \ \mathrm{tr}\,(A) = 1.$$

   Dans chacun des cas, prouver qu'il existe une infinité de matrices A satisfaisant aux conditions imposées.

5. On suppose que $n = 2$.

   (a) Montrer qu'il existe un entier naturel non nul N_2 tel que pour toute matrice A de $\mathcal{C}_2\,(\mathbb{Z})$ on ait :

   $$A^{N_2} = I_2.$$

   (b) Cette propriété est-elle encore vraie pour les matrices de $\mathcal{C}_2\,(\mathbb{R})$?

6.

   (a) Prouver que A^{-1} appartient également à $\mathcal{C}_n\,(\mathbb{Z})$. Déterminer $h\,(A^{-1})$.

   (b) Prouver que $\mathcal{C}_2\,(\mathbb{Z})$ n'est pas un groupe pour la multiplication matricielle.

   (c) En déduire que, pour tout $n \geq 2$, $\mathcal{C}_n\,(\mathbb{Z})$ n'est pas un groupe pour la multiplication matricielle.

Partie II

Cette partie a pour but de mettre en évidence une famille de groupes de $\mathcal{C}_2\,(\mathbb{Z})$ et d'en donner une interprétation géométrique.

Soit $j = e^{\frac{2i\pi}{3}}$ et $\alpha = e^{\frac{i\pi}{3}}$. On désigne par $\mathbb{Z}\,[j]$ [resp. $\mathbb{Z}\,[\alpha]$] l'ensemble des complexes de la forme $m + qj$ [resp. $m + q\alpha$] où (m, q) parcourt $\mathbb{Z}^2$.

1.

   (a) Prouver que $\mathbb{Z}\,[j]$ est un sous-anneau de $\mathbb{C}$ et que $\mathbb{Z}\,[\alpha] = \mathbb{Z}\,[j]$.

   (b) Déterminer l'ensemble (m, q) d'entiers relatifs tels que $0 < |m + qj| \leq 1$; en déduire le groupe U_6 des unités de $\mathbb{Z}\,[j]$ (c'est-à-dire des éléments de $\mathbb{Z}\,[j]$ inversibles dans $\mathbb{Z}\,[j]$).

2. U_6 est l'ensemble des affixes des sommets d'un hexagone P.
   Montrer que le groupe $I\,(P)$ des isométries conservant P est engendré par deux éléments r et s vérifiant les relations $r^6 = I_d = s^2$ et $r \circ s \circ r \circ s = I_d$ où I_d désigne l'application identique.

3. Les nombres 1 et j constituent une base $\mathcal{B}$ de $\mathbb{C}$ considéré comme un espace vectoriel réel.
   (a) Écrire les matrices de r et s dans la base $\mathcal{B}$.
   (b) Établir un isomorphisme entre $I(P)$ et un groupe G de $\mathcal{C}_2(\mathbb{Z})$. On précisera un groupe de générateurs de G vérifiant les relations analogues à **II.2**. pour le produit matriciel.

4.
   (a) Soit $z_1 = m_1 + q_1 j$ et $z_2 = m_2 + q_2 j$ deux éléments de $\mathbb{Z}[j]$ tels que $m_1 q_2 - m_2 q_1 = -1$. Prouver que tout élément de $\mathbb{Z}[j]$ s'écrit d'une et d'une seule façon comme combinaison linéaire à coefficients entiers de z_1 et z_2.
   (b) Soit B une matrice de $\mathcal{C}_2(\mathbb{Z})$ telle que $h(B) = 2$.
   Prouver que l'ensemble des matrices de la forme BAB où A décrit le groupe G défini au **II.3.b.** est un groupe de $\mathcal{C}_2(\mathbb{Z})$ isomorphe à G.
   (c) Déterminer explicitement une infinité de groupes de $\mathcal{C}_2(\mathbb{Z})$ isomorphes à G et préciser pour chacun d'eux un isomorphisme sur $I(P)$.

Partie III

Dans cette partie, n est un entier supérieur ou égal à 2.

On établit que les groupes de $\mathcal{C}_n(\mathbb{Z})$ sont finis, ainsi que l'existence d'un entier naturel non nul N_n tel que $A^{N_n} = I_n$ pour toute matrice A de $\mathcal{C}_n(\mathbb{Z})$.

1. Soit G un groupe de $\mathcal{C}_n(\mathbb{Z})$. Nous désignons par $\langle G \rangle$ le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ engendré par les éléments de G.
   (a) Montrer que $\langle G \rangle$ est de dimension finie ; on posera alors $\dim(\langle G \rangle) = k$.
   (b) Soit $(X_i)_{1 \le i \le k}$ une base de $\langle G \rangle$ formée d'éléments de G ; nous posons :
   $$T : \begin{array}{ccc} G & \to & \mathbb{C}^k \\ A & \mapsto & T(A) = (\mathrm{tr}(AX_i))_{1 \le i \le k} \end{array}$$
   Soit A et B deux éléments de G vérifiant $T(A) = T(B)$; prouver que pour tout X de G on a :
   $$\mathrm{tr}\left(\left(AB^{-1} - I_n\right) X\right) = 0.$$
   (c) Montrer que l'application T est injective et en déduire que G est un groupe fini.

2.
   (a) Démontrer que l'ensemble des polynômes unitaires de degré n à coefficients entiers dont les racines complexes sont de module 1 est fini.
   (b) En déduire qu'il existe un entier naturel non nul N_n tel que :
   $$\forall A \in \mathcal{C}_n(\mathbb{Z}),\ A^{N_n} = I_n.$$

Partie IV

L'objet de cette partie est de donner la liste des valeurs possibles de $h(A)$ pour A élément de $\mathcal{C}_i(\mathbb{Z})$ où $i = 2, 3, 4$.

Pour $d \in \mathbb{N}^*$ on note U_d le groupe des racines d-èmes de l'unité de $\mathbb{C}$.

E_d désigne l'ensemble des éléments d'ordre d de ce groupe, dits racines primitives d-èmes de l'unité. Rappelons que ce sont les complexes α^r où α est une racine primitive d-ème de l'unité et r décrit l'ensemble des entiers naturels inférieurs à d et premiers avec d.

Soit A une matrice cyclique de $\mathcal{C}_n(\mathbb{Z})$, d'ordre $h(A)$ et $\mathrm{Sp}(A)$ l'ensemble de toutes les valeurs propres complexes de A.

L'indicateur d'Euler $\varphi(d)$ $(d \in \mathbb{N}^*)$ dénombre les entiers naturels inférieurs ou égaux à d et premiers avec d.

1.
   (a) Montrer que :
   $$\text{si } (d_1 > 1 \text{ et } d_2 > 1 \text{ et } d_1 \text{ premier avc } d_2) \text{ alors } \varphi(d_1 d_2) = \varphi(d_1)\varphi(d_2).$$
   (b) Soit p un nombre premier et $k \in \mathbb{N}^*$; prouver que $\varphi\left(p^k\right) = p^k - p^{k-1}$.
2. Soit $d \in \mathbb{N}^*$. Montrer que si $E_d \cap \mathrm{Sp}(A) \neq \emptyset$, alors $E_d \subset \mathrm{Sp}(A)$.
3. Soit $d_1, d_2, \cdots, d_m$ les différents ordres des valeurs propres de A comme racines de l'unité dans $\mathbb{C}$.
   (a) Prouver que :
   $$n \geq \sum_{i=1}^{m} \varphi(d_i).$$
   (b) Soit $\prod_{j=1}^{q} p_j^{k_j}$ la décomposition en facteurs premiers de $h(A)$; prouver que :
   $$n \geq \max_{1 \leq j \leq q} \left(p_j^{k_j} - p_j^{k_j - 1}\right).$$
4. Déduire des deux majorations qui viennent d'être obtenues la liste des valeurs possibles de $h(A)$ et indiquer une valeur de N_n dans les cas $n = 2$, $n = 3$, $n = 4$.

Partie V

Cette partie propose deux applications géométriques de l'étude précédente dans les cas $n = 3$ et $n = 4$.

Partie V.A

Dans l'espace affine euclidien orienté de dimension 3, muni d'un repère orthonormé direct $\mathbf{R} = \left(O, \overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}\right)$ on considère l'octaèdre régulier V_3 de centre O ayant pour sommets les points A, B, C de coordonnées $A = (1, 0, 0)$, $B = (0, 1, 0)$, $C = (0, 0, 1)$, ainsi que leurs symétriques A', B', C' par rapport à l'origine O.

On se propose d'étudier le groupe $I(V_3)$ des isométries qui conservent V_3 et son sous-groupe $I^+(V_3)$ des isométries positives.

1. Préciser l'ordre du groupe $I(V_3)$ et celui de $I^+(V_3)$.

2. Prouver que $I^+(V_3)$ est engendré par trois rotations r_1, r_2, r_3 d'angles respectifs $\frac{\pi}{3}, \frac{2\pi}{3}, \pi$ dont on précisera les axes orientés.
3. Soit $G(V_3)$ le groupe des matrices représentant dans la base $\left(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}\right)$ les parties linéaires des éléments de $I(V_3)$.
   (a) Prouver que $G(V_3)$ est un groupe de $\mathcal{C}_3(\mathbb{Z})$.
   (b) Donner une famille de générateurs de $G(V_3)$.
   (c) Donner explicitement un élément A de $G(V_3)$ tel que $h(A) = 6$.
   (d) Quelles sont toutes les valeurs $h(A)$ effectives quand A décrit $G(V_3)$.

Partie V.B

On considère un espace affine euclidien orienté de dimension 4, muni d'un repère orthonormé direct $\mathbf{R} = (O, e_1, e_2, e_3, e_4)$; $O(4)$ désigne le groupe orthogonal en dimension 4.

On considère le polytope V_4 de centre O, ayant pour sommets les points A, B, C, D de coordonnées $A = (1,0,0,0)$, $B = (0,1,0,0)$, $C = (0,0,1,0)$, $D = (0,0,0,1)$ ainsi que leurs symétriques A', B', C', D' par rapport à l'origine O.

On se propose d'étudier le groupe $I(V_4)$ des isométries qui conservent V_4 et son sous-groupe $I^+(V_4)$ des isométries positives.

1.
   (a) Déterminer un morphisme injectif de $I(V_4)$ dans le groupe des permutations de l'ensemble des sommets du polytope V_4.
   (b) Préciser l'ordre du groupe $I(V_4)$.
2. Donner explicitement un élément $I^+(V_4)$ d'ordre 8.
3. En déduire un exemple de matrice A appartenant à $\mathcal{C}_4(\mathbb{Z}) \cap O(4)$, telle que $h(A) = 8$.