Agrégation interne 1996, épreuve 1
Le 02 Décembre 2006, de 09 h. à 14 h.
Institut Fourier. Salle 18

1 Énoncé

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 ; $\operatorname{tr}(A)$ 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 $h(A) = \underset{1 \leq i \leq n}{\operatorname{ppcm}}(q_i)$.

   (c) Prouver que $\operatorname{tr}(A) \in \{-n, -(n-1), \cdots, -1, 0, 1, \cdots, n-1, n\}$ 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 $\operatorname{tr}(A) = n\varepsilon$. 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 :

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

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 $h\left(A^{-1}\right)$.

   (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 $(X_i)_{1\leq i\leq k}$ une base de $\langle G \rangle$ formée d'éléments de G ; nous posons :

$$T: \begin{array}{ccc} G & \to & \mathbb{C}^k \\ A & \mapsto & T(A) = (\mathrm{tr}(AX_i))_{1\leq i\leq k} \end{array}$$

   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 $h(A) = 8$.

2 Corrigé

Partie I

On identifie, dans ce qui suit, une matrice complexe d'ordre n à l'endomorphisme qu'elle définit dans la base canonique de $\mathbb{C}^n$.

D'autre part, si A et B sont deux matrices complexes semblables, alors A est cyclique d'ordre p si, et seulement si, B l'est, c'est-à-dire que $h(A) = h(B)$. En effet avec $B = P^{-1}AP$ où P est une matrice inversible d'ordre n, on a $B^k = P^{-1}A^kP$ pour tout entier $k \geq 1$ et $B^k = I_n$ si, et seulement si, $A^k = I_n$.

Enfin on rappelle qu'une matrice réelle ou complexe d'ordre n ayant une seule valeur propre d'ordre n est diagonalisable si, et seulement si, c'est une homothétie.

1.

(a) Une matrice cyclique d'ordre p dans $\mathcal{C}_n(\mathbb{C})$ est diagonalisable puisque annulée par le polynôme $X^p - 1$ qui est scindé à racines simples dans $\mathbb{C}$.
Si $A \in \mathcal{C}_n(\mathbb{C})$ est cyclique d'ordre p, de $A^p = I_n$, on déduit que pour toute valeur propre λ de A et tout vecteur propre associé $X \in \mathbb{C}^n \setminus \{0\}$, on a $X = A^pX = \lambda^pX$ et $\lambda^p = 1$. Donc λ est une racine p-ième de l'unité.

(b) La matrice A est semblable à une matrice diagonale :

$$D = \operatorname{diag}(\lambda_1, \cdots, \lambda_n)$$

où les λ_k sont des racines p-èmes de l'unité et $h(A) = h(D)$.En désignant, pour tout k compris entre 1 et n par q_k l'ordre de λ_k dans $\mathbb{C}^*$ et par μ le ppcm de ces ordres, on a $\lambda_k^\mu = 1$ pour tout k compris entre 1 et n et $D^\mu = I_n$, donc $h(D)$ divise μ. D'autre part de $D^{h(D)} = I_n$, on déduit que $\lambda_k^{h(D)} = 1$ pour tout k compris entre 1 et n et $h(D)$ est multiple de tous les q_k donc de μ. On a donc $h(A) = h(D) = \mu$.

(c) De $A^p = I_n$, on déduit que $(\det(A))^p = \det(A^p) = 1$ avec $\det A \in \mathbb{Z}$ et nécessairement $\det A = \pm 1$. On peut remarquer que pour p impair, on a nécessairement $\det(A) = 1$.
En notant $\lambda_1, \cdots, \lambda_n$ les valeurs propres complexes de A, on a :

$$|\operatorname{tr}(A)| = \left|\sum_{k=1}^n \lambda_k\right| \leq \sum_{k=1}^n |\lambda_k| = n$$

puisque $|\lambda_k| = 1$ pour tout k. Tenant compte de $\operatorname{tr}(A) \in \mathbb{Z}$, on déduit que :

$$\operatorname{tr}(A) \in \{-n, -(n-1), \cdots, -1, 0, 1, \cdots, n-1, n\}.$$

2. Chaque nombre complexe non nul z_k $(1 \leq k \leq n)$ peut s'écrire $z_k = \rho_k e^{i\theta_k}$ avec $\rho_k = |z_k| > 0$ et $\theta_k \in]-\pi, \pi]$. On a alors :

$$\begin{cases} \left|\sum\limits_{k=1}^n z_k\right|^2 = \sum\limits_{k=1}^n |z_k|^2 + 2 \sum\limits_{1\leq j<k\leq n} \rho_j\rho_k \cos(\theta_j - \theta_k), \\ \left(\sum\limits_{k=1}^n |z_k|\right)^2 = \sum\limits_{k=1}^n |z_k|^2 + 2 \sum\limits_{1\leq j<k\leq n} \rho_j\rho_k \end{cases}$$

et l'égalité $\left|\sum\limits_{k=1}^n z_k\right| = \sum\limits_{k=1}^n |z_k|$ est équivalente à :

$$\sum_{1\leq j<k\leq n} \rho_j\rho_k (1 - \cos(\theta_j - \theta_k)) = 0.$$

Tous les termes de cette somme étant positifs ou nuls avec $\rho_j\rho_k > 0$, on en déduit que $\cos(\theta_j - \theta_k) = 1$ avec $\theta_j - \theta_k \in]-2\pi, 2\pi[$ pour $1 \leq j < k \leq r$ (on a $-\pi < \theta_j \leq \pi$ et $-\pi < \theta_k \leq \pi$ donc $-\pi \leq -\theta_k < \pi$ et

$-2\pi < \theta_j - \theta_k < 2\pi$), ce qui donne $\theta_j = \theta_k$ et en notant θ cette valeur commune on a $z_k = \rho_k e^{i\theta} = |z_k| e^{i\theta}$ pour tout entier k compris entre 1 et n ou encore :

$$z_k = \frac{|z_k|}{|z_1|} |z_1| e^{i\theta} = \alpha_k z_1 \ \ (1 \leq k \leq n)$$

où on a posé $\alpha_k = \dfrac{|z_k|}{|z_1|}$ pour tout k compris entre 1 et n.

Réciproquement si $z_k = \alpha_k z_1$ avec $\alpha_k > 0$ pour tout k compris entre 2 et n et $\alpha_1 = 1$, on a :

$$\left| \sum_{k=1}^{n} z_k \right| = |z_1| \sum_{k=1}^{n} \alpha_k = \sum_{k=1}^{n} \alpha_k |z_1| = \sum_{k=1}^{n} |z_k| .$$

On peut aussi démontrer ce résultat par récurrence sur $n \geq 1$, le cas $n = 2$ correspondant au cas d'égalité dans l'inégalité triangulaire sur $\mathbb{C}$.

3. Si $\operatorname{tr}(A) = n\varepsilon$, on a alors :

$$n = |\operatorname{tr}(A)| = \left| \sum_{k=1}^{n} \lambda_k \right| = \sum_{k=1}^{n} |\lambda_k|$$

et $\lambda_k = \alpha_k \lambda_1$ avec $\alpha_k = \dfrac{|\lambda_k|}{|\lambda_1|} = 1$, c'est-à-dire que A n'a qu'une valeur propre λ_1 d'ordre n. Comme A est diagonalisable, c'est l'homothétie de rapport λ_1, soit $A = \lambda_1 I_n$. De $\operatorname{tr}(A) = n\lambda_1 = n\varepsilon$, on déduit que $\lambda_1 = \varepsilon$, soit $A = \varepsilon I_n = \pm I_n$ avec $h(A) = 1$ pour $A = I_n$ et $h(A) = 2$ pour $A = -I_n$, ce qui peut s'écrire $h(A) = \dfrac{1}{2}(3 - \varepsilon)$.

4.

(a) Si les deux valeurs propres de A sont réelles et distinctes, comme elles sont de module égal à 1, elles valent nécessairement -1 et 1. On a donc $\lambda_1 = \varepsilon$, $\lambda_2 = -\varepsilon$ et A est semblable à $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, ce qui donne $h(A) = h(J) = 2$. Pour toute matrice $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$ (i. e. $P \in \mathcal{M}_2(\mathbb{Z})$ et $\det(P) = ps - qr = \pm 1$) la matrice :

$$\begin{aligned} A = PJP^{-1} &= \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} \\ &= \begin{pmatrix} ps + qr & -2pq \\ 2rs & -(ps + qr) \end{pmatrix} = \begin{pmatrix} 2qr \pm 1 & -2pq \\ 2rs & -(2qr \pm 1) \end{pmatrix} \end{aligned}$$

est une matrice de ce type, il y en donc bien une infinité.

On peut par exemple prendre p et r premier entre eux, le théorème de Bézout nous dit alors qu'il existe deux entiers s_0 et q_0 tels que $ps_0 - q_0 r = 1$ (ou -1) et les couples d'entiers $(s, q) = (s_0 + kq, r_0 + kp)$ où k décrit Z nous fournissent une infinité de matrices P et donc de matrices A.

Plus simplement, on peut aussi remarquer que pour tout entier relatif n, la matrice $A_n = \begin{pmatrix} \varepsilon & 0 \\ n & -\varepsilon \end{pmatrix}$ convient, ce qui en donne bien une infinité.

(b) Si les deux valeurs propres de A ne sont pas réelles, elles s'écrivent $\lambda_1 = e^{i\theta}$ et $\lambda_2 = \overline{\lambda_1} = e^{-i\theta}$ avec $\theta \in \left]-\pi, \pi\right[\setminus \{0\}$. On a alors $\det(A) = \lambda_1 \lambda_2 = 1$ et $\operatorname{tr}(A) = 2\cos(\theta) \in \{-1, 0, 1\}$ d'après **I.1.a** et **I.4.a.** Il reste donc trois cas à étudier.

– Si $\operatorname{tr} A = -1$, on a alors $\cos(\theta) = -\dfrac{1}{2}$ et $\theta = \pm\dfrac{2\pi}{3}$, soit $\lambda_1 = e^{\frac{2i\pi}{3}} = j$, $\lambda_2 = e^{-\frac{2i\pi}{3}} = \overline{j}$ et A est semblable à $J_{-1} = \begin{pmatrix} j & 0 \\ 0 & \overline{j} \end{pmatrix}$, ce qui donne $h(A) = h(J_{-1}) = 3$. Pour déterminer de telles matrices $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$, on écrit que nécessairement :

$$\begin{cases} \operatorname{tr}(A) = a + d = -1 \\ \det(A) = ad - bc = 1 \end{cases}$$

ce qui donne $d = -a-1$ et $bc = -a^2-a-1$, c'est-à-dire que b est un diviseur de $m = -a^2-a-1$ et $c = \frac{m}{b}$. Faisant varier a dans $\mathbb{Z}$, on a une infinité de telles matrices. Réciproquement toutes ces matrices conviennent, du fait qu'elles ont toutes le même polynôme caractéristique :

$$P_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = \lambda^2 + \lambda + 1$$

de racines j et $\overline{j}$.
Par exemple, en prenant, pour tout entier relatif n, $a = n$, $b = m$, $c = 1$, $d = -n-1$, la matrice :

$$A_n = \begin{pmatrix} n & -n^2-n-1 \\ 1 & -n-1 \end{pmatrix}$$

convient et on en a bien une infinité.

- Si $\mathrm{tr}\, A = 0$, on a alors $\cos(\theta) = 0$ et $\theta = \pm\frac{\pi}{2}$, soit $\lambda_1 = i$, $\lambda_2 = -i$ et A est semblable à $J_0 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, ce qui donne $h(A) = h(J_0) = 4$. Pour déterminer de telles matrices $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$, on écrit que nécessairement :

$$\begin{cases} \mathrm{tr}(A) = a + d = 0 \\ \det(A) = ad - bc = 1 \end{cases}$$

ce qui donne $d = -a$ et $bc = -a^2 - 1$, c'est-à-dire que b est un diviseur de $m = -a^2 - 1$ et $c = \frac{m}{b}$. Faisant varier a dans $\mathbb{Z}$, on a une infinité de telles matrices. Réciproquement toutes ces matrices conviennent, du fait qu'elles ont toutes le même polynôme caractéristique :

$$P_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = \lambda^2 + 1$$

de racines i et $-i$.
Par exemple, en prenant, pour tout entier relatif n, $a = n$, $b = m$, $c = 1$, $d = -n$, la matrice :

$$A_n = \begin{pmatrix} n & -n^2-1 \\ 1 & -n \end{pmatrix}$$

convient et on en a bien une infinité.

- Si $\mathrm{tr}\, A = 1$, on a alors $\cos(\theta) = \frac{1}{2}$ et $\theta = \pm\frac{\pi}{3}$, soit $\lambda_1 = e^{\frac{i\pi}{3}}$, $\lambda_2 = e^{-\frac{i\pi}{3}}$ et A est semblable à $J_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, ce qui donne $h(A) = h(J_1) = 6$. Pour déterminer de telles matrices $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$, on écrit que nécessairement :

$$\begin{cases} \mathrm{tr}(A) = a + d = 1 \\ \det(A) = ad - bc = 1 \end{cases}$$

ce qui donne $d = 1-a$ et $bc = -a^2+a-1$, c'est-à-dire que b est un diviseur de $m = -a^2+a-1$ et $c = \frac{m}{b}$. Faisant varier a dans $\mathbb{Z}$, on a une infinité de telles matrices. Réciproquement toutes ces matrices conviennent, du fait qu'elles ont toutes le même polynôme caractéristique :

$$P_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A) = \lambda^2 - \lambda + 1$$

de racines $\lambda_1$et $\overline{\lambda_1}$.
Par exemple, en prenant, pour tout entier relatif n, $a = n$, $b = m$, $c = 1$, $d = 1-n$, la matrice :

$$A_n = \begin{pmatrix} n & -n^2+n-1 \\ 1 & 1-n \end{pmatrix}$$

convient et on en a bien une infinité.

5.

(a) Les questions précédentes nous disent qu'une matrice $A \in \mathcal{C}_2(\mathbb{Z})$ a pour ordre $h(A) = 1, 2, 3, 4$ ou 6. Il en résulte que pour $N_2 = \text{ppcm}(1, 2, 3, 4, 6) = 12$, on a $A^{N_2} = I_2$ pour tout $A \in \mathcal{C}_2(\mathbb{Z})$.

(b) En remarquant qu'une matrice de rotation d'angle $\frac{2\pi}{n}$, où n est un entier naturel non nul, est d'ordre n, on voit que la propriété précédente n'est pas vrai dans $\mathcal{C}_2(\mathbb{R})$.

6.

(a) On a vu que pour toute matrice $A \in \mathcal{C}_n(\mathbb{Z})$, on a $\det A = \pm 1$, ce qui signifie qu'elle est inversible dans $\mathcal{M}_2(\mathbb{Z})$. En fait, pour A d'ordre $p \geq 1$, de $A^p = I_n$ on déduit que $A^{-1} = A^{p-1} \in \mathcal{M}_2(\mathbb{Z})$. L'égalité $A^k = I_n$ étant équivalente à $\left(A^{-1}\right)^k = I_n$ pour tout entier $k \geq 1$ (on a $\left(A^{-1}\right)^k = \left(A^k\right)^{-1}$), on déduit qu'une matrice $A \in GL_n(\mathbb{Z})$ est dans $\mathcal{C}_n(\mathbb{Z})$ si, et seulement si $A^{-1} \in \mathcal{C}_n(\mathbb{Z})$ et ces deux matrices ont même ordre.

(b) Si A, B sont dans $\mathcal{C}_2(\mathbb{Z})$ leur trace est comprise entre -2 et 2. Pour montrer que $\mathcal{C}_2(\mathbb{Z})$ n'est pas un groupe pour la multiplication matricielle, il suffit donc de trouver deux telles matrices telles que $|\text{tr}(A)| \geq 3$. Par exemple, pour $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, on a :

$$AB = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} a & -c \\ b & -d \end{pmatrix}$$

et $\text{tr}(AB) = a - d$. Prenant $d = -a$, $bc = -a^2 - 1$ (équivalent à $\text{tr}(A) = 0$ et $\det(A) = 1$, ce qui donne $h(A) = h(J_0) = 4$), on a $\text{tr}(AB) = 2a = 4$ pour $a = 2$ et $AB \notin \mathcal{C}_2(\mathbb{Z})$. Par exemple, on a :

$$A = \begin{pmatrix} 2 & -1 \\ 5 & -2 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; AB = \begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix}$$

avec $A^4 = I_2$, $B^2 = I_2$ et $(AB)^p \neq I_n$ pour tout entier $p \geq 1$ (la matrice AB étant à coefficients tous strictement positifs, il en est de même des A^p).

On peut aussi s'inspirer des exemples donnés en **I.4.b.** pour prendre $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$ qui donnent $AB = \begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix} \notin \mathcal{C}_2(\mathbb{Z})$ puisque cette matrice est de trace égale à -3.

Ou plus généralement, pour tout $n \in \mathbb{Z}$, $A_n = \begin{pmatrix} n & -n^2 - n - 1 \\ 1 & -n - 1 \end{pmatrix}$ et $B_n = \begin{pmatrix} n & -n^2 + n - 1 \\ 1 & 1 - n \end{pmatrix}$ dans $\mathcal{C}_2(\mathbb{Z})$ donnent $A_n B_n = \begin{pmatrix} -n - 1 & n^2 - n - 1 \\ -1 & n - 2 \end{pmatrix} \notin \mathcal{C}_2(\mathbb{Z})$ puisque cette matrice est de trace égale à -3.

(c) En gardant les notations de la question précédente, pour tout $n \geq 3$, les matrices $A' = \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix}$ et $B' = \begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$ sont dans $\mathcal{C}_n(\mathbb{Z})$ alors que $A'B'$ n'y est pas. Donc $\mathcal{C}_n(\mathbb{Z})$ n'est pas un groupe pour la multiplication matricielle.

Partie II

1.

(a) Pour tout nombre complexe z, l'application $\varphi : \mathbb{Z}[X] \to \mathbb{C}$ définie par $\varphi(Q) = Q(z)$ est un morphisme d'anneau, donc son image $\mathbb{Z}[z]$ est un sous-anneau de $\mathbb{C}$.
Le nombre complexe $z \in \{\alpha, j\}$ étant racine d'un polynôme de degré deux à coefficients entiers $P(X) = X^2 + \varepsilon X + 1$ avec $\varepsilon = -1$ pour α et $\varepsilon = 1$ pour j, il vérifie $z^2 = -\varepsilon z - 1$ et par récurrence $z^n = m_n + q_n z$ pour tout entier naturel n, où m_n et q_n sont des entiers relatifs. Il en résulte que $\mathbb{Z}[z] = \left\{m + qz \mid (m, q) \in \mathbb{Z}^2\right\}$.
Enfin avec $\alpha^2 = j$ et $1 + j = -j^2 = \alpha$, on déduit que $\mathbb{Z}[j] = \mathbb{Z}[\alpha]$.

(b) Pour tout $(m, q) \in \mathbb{Z}^2$, on a :

$$\begin{aligned}|m + qj|^2 &= \left|m - \frac{q}{2} + q\frac{\sqrt{3}}{2}i\right|^2 = \left(m - \frac{q}{2}\right)^2 + \frac{3}{4}q^2 \\ &= m^2 + q^2 - mq \in \mathbb{N}\end{aligned}$$

et l'encadrement $0 < |m + qj| \leq 1$ équivaut à $|m + qj|^2 = 1$, soit à :

$$Q(m, q) = \left(m - \frac{q}{2}\right)^2 + \frac{3}{4}q^2 - 1 = 0.$$

Pour $|q| \geq 2$, on a $\frac{3}{4}q^2 - 1 \geq 2 > 0$ et $Q(m, q) > 0$.
Pour $q = 0$, on a $m^2 = 1$ et $m = \pm 1$.
Pour $|q| = 1$, cette équation s'écrit $Q(m, q) = m^2 - qm = 0$ et $m = 0$ ou $m = q$.
En définitive, l'ensemble des solutions entières de l'équation $Q(m, q) = 1$ est :

$$S = \{(0, -1), (0, 1), (-1, 0), (-1, -1), (1, 0), (1, 1)\}.$$

On peut remarquer que $|m + qj| = 0$ si, et seulement si, $q = 0$ et $m = 0$.
On a donc montré que l'intersection de $\mathbb{Z}[j]$ avec le disque unité fermée D de $\mathbb{C}$ est :

$$\begin{aligned}P = \mathbb{Z}[j] \cap D &= \{-j, j, -1, -1 - j, 1, 1 + j\} \\ &= \left\{e^{ik\frac{\pi}{3}} \mid k = 0, \cdots, 5\right\} = \left\{\alpha^k \mid k = 0, \cdots, 5\right\} = \langle \alpha \rangle.\end{aligned}$$

C'est le groupe cyclique des racines 6-èmes de l'unité engendré par α ou encore l'ensemble des affixes des sommets de l'hexagone régulier P.
Un élément z de $\mathbb{Z}[j]$ est inversible si, et seulement si, il existe $z' \in \mathbb{Z}[j]$ tel que $zz' = 1$, ce qui entraîne $z \neq 0$ et $|z|^2 |z'|^2 = 1$ avec $|z|^2 \in \mathbb{N}^*$. On a donc $|z|^2 = 1$ et $z \in P$. Comme tous les éléments de P sont inversibles, on a $U_6 = P$.

2. On désigne par $r : z \mapsto \alpha z$ la rotation d'angle $\frac{\pi}{3}$, par s la réflexion $s : z \mapsto \overline{z}$ et par $G = \langle r, s \rangle$ le groupe des isométries engendré par r et s. La rotation r est d'ordre 6, la réflexion s d'ordre 2 et pour tout $z \in \mathbb{C}$, on a :

$$(r \circ s)^2(z) = \alpha\overline{\alpha\overline{z}} = |\alpha|^2 z = z$$

avec $r \circ s \neq I_d$, c'est-à-dire que $r \circ s$ est d'ordre 2.
On vérifie de manière analogue que $s \circ r$ est d'ordre 2.
L'hexagone P étant globalement invariant par la rotation r, le groupe cyclique $\langle r \rangle$ est contenu dans groupe $I^+(P)$ des rotations laissant P globalement invariant.
D'autre part toute rotation $\rho \in I^+(P)$ étant une application affine, elle doit conserver le barycentre 0 des sommets de P, donc $\rho(0) = 0$ et $\rho : z \mapsto e^{i\theta}z$. Comme $\rho(\alpha) \in P$, on a $\rho(\alpha) = \alpha^k$ avec k compris entre 1 et 6, soit $e^{i\theta}\alpha = \alpha^k$ et $e^{i\theta} = \alpha^{k-1}$, ce qui signifie que $\rho = r^k \in \langle r \rangle$. On a donc $I^+(P) = \langle r \rangle$.
En notant $I^-(P) = I(P) \setminus I^+(P)$ et en remarquant que l'application :

$$\begin{array}{rccc}\varphi : & I^+(P) & \to & I^-(P) \\ & \rho & \mapsto & s \circ \rho\end{array}$$

est bijective, on déduit que

$$I(P) = I^+(P) \cup I^-(P) = I^+(P) \cup s\left(I^+(P)\right) \subset \langle r, s \rangle$$

et comme la réflexion s conserve aussi P, on a $\langle r, s \rangle \subset I(P)$ et :

$$I(P) = \langle r, s \rangle = \left\{r^k \mid 0 \leq k \leq 5\right\} \cup \left\{s \circ r^k \mid 0 \leq k \leq 5\right\}$$

est le groupe d'ordre 12 engendré par r et s.
On peut aussi utiliser le morphisme de groupes multiplicatifs :

$$\begin{array}{cccc} \delta : & I(P) & \to & \{-1,1\} \\ & \rho & \mapsto & \det(\rho) \end{array}$$

Le noyau de ce morphisme est $\ker(\delta) = I^+(P) = \langle r \rangle$ de cardinal 6. Comme δ est surjectif ($\delta(r) = 1$ et $\delta(s) = -1$), il induit une bijection de l'ensemble quotient $\dfrac{I(P)}{\ker(\delta)}$ sur $\{-1,1\}$ et il en résulte de $I(P)$ est de cardinal 12. Comme $\left\{ s \circ r^k \mid 0 \leq k \leq 5 \right\}$ est contenu dans $I(P) \setminus I^+(P)$ avec 6 éléments, on en déduit que :

$$I(P) = \left\{ r^k \mid 0 \leq k \leq 5 \right\} \cup \left\{ s \circ r^k \mid 0 \leq k \leq 5 \right\}.$$

3.

(a) De :

$$\left\{ \begin{array}{l} r(1) = \alpha = -j^2 = 1 + j \\ r(j) = \alpha j = -1 \end{array} \right. \text{ et } \left\{ \begin{array}{l} s(1) = 1 \\ s(j) = \overline{j} = j^2 = -1 - j \end{array} \right.$$

on déduit que les matrices de r et s dans la base $\mathcal{B}$ sont respectivement :

$$R = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } S = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

(b) On désigne respectivement par $GL(\mathbb{C})$ le groupe des automorphismes du $\mathbb{R}$-espace vectoriel $\mathbb{C}$ et par $GL_2(\mathbb{R})$ le groupe multiplicatif des matrices inversibles d'ordre 2. On sait alors que l'application φ qui associe à tout automorphisme $u \in GL(\mathbb{C})$ sa matrice $A \in GL_2(\mathbb{R})$ dans la base $\mathcal{B}$ réalise un isomorphisme de groupes de $GL(\mathbb{C})$ sur $GL_2(\mathbb{R})$. La restriction de φ au groupe $I(P) = \langle r, s \rangle$ définit alors un isomorphisme de groupes de $I(P)$ sur $G = \varphi(\langle r, s \rangle) = \langle R, S \rangle$. Comme G est fini à 12 éléments et formé de matrices à coefficients entiers, on a bien $G \subset \mathcal{C}_n(\mathbb{Z})$. Avec $R^k = \varphi(r^k)$ et $S^k = \varphi(s^k)$, on déduit que R est d'ordre 6 et S, SR et RS d'ordre 2.
On a donc :

$$G = \left\{ R^k \mid 0 \leq k \leq 5 \right\} \cup \left\{ S \cdot R^k \mid 0 \leq k \leq 5 \right\} = G^+ \cup G^-$$

avec :

$$G^+ = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\}$$

et :

$$G^- = \left\{ \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \right\}$$

4.

(a) Si $\det_{\mathcal{B}}(z_1, z_2) = m_1 q_2 - m_2 q_1 = -1 \neq 0$ alors (z_1, z_2) est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$ et tout nombre complexe $z = m + qj \in \mathbb{Z}[j]$, s'écrit de façon unique sous la forme :

$$m + qj = az_1 + bz_2$$

où a, b sont a priori réels. En utilisant la formule de changement de bases :

$$\begin{pmatrix} m \\ q \end{pmatrix} = \begin{pmatrix} m_1 & m_2 \\ q_1 & q_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

on obtient :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m_1 & m_2 \\ q_1 & q_2 \end{pmatrix}^{-1} \begin{pmatrix} m \\ q \end{pmatrix} = - \begin{pmatrix} q_2 & -m_2 \\ -q_1 & m_1 \end{pmatrix} \begin{pmatrix} m \\ q \end{pmatrix}$$

et on en déduit que a et b sont des entiers relatifs.
On obtient un résultat analogue si $\det_{\mathcal{B}}(z_1, z_2) = 1$.
On a en fait montré qu'un couple (z_1, z_2) est une $\mathbb{Z}$-base de $\mathbb{Z}[j]$ si, et seulement si, sa matrice dans la base $\mathcal{B}$ est dans $GL_2(\mathbb{Z}) = \{P \in \mathcal{M}_2(\mathbb{Z}) \mid \det(P) = \pm 1\}$.

(b) L'hypothèse $B \in \mathcal{C}_2(\mathbb{Z})$ avec $h(B) = 2$ équivaut à $B \in GL_2(\mathbb{Z})$ et $B^{-1} = B$. Il en résulte que l'application :

$$\begin{array}{cccc} \varphi_B : & GL_2(\mathbb{Z}) & \to & GL_2(\mathbb{Z}) \\ & A & \mapsto & BAB = BAB^{-1} \end{array}$$

est un automorphisme intérieur de $GL_2(\mathbb{Z})$ et $\varphi(G)$ est un sous-groupe de $GL_2(\mathbb{Z})$ isomorphe à G. Comme G est fini à 12 éléments, il en est de même $\varphi_B(G)$ et $\varphi_B(G) \subset \mathcal{C}_2(\mathbb{Z})$.

En fait, on a :

$$\begin{aligned} \varphi_B(G) &= \varphi_B(\langle R, S\rangle) = \varphi_B\left(\left\{R^k \mid 0 \leq k \leq 5\right\} \cup \left\{SR^k \mid 0 \leq k \leq 5\right\}\right) \\ &= \left\{BR^kB \mid 0 \leq k \leq 5\right\} \cup \left\{BSR^kB \mid 0 \leq k \leq 5\right\} \end{aligned}$$

avec :

$$BR^kB = (BRB)^k = (\varphi_B(R))^k$$

et :

$$BSR^kB = (BSB)\left(BR^kB\right) = \varphi_B(S)(\varphi_B(RS))^k$$

puisque $B^2 = I_2$. Donc :

$$\begin{aligned} \varphi_B(G) &= \left\{(\varphi_B(R))^k \mid 0 \leq k \leq 5\right\} \cup \left\{\varphi_B(S)(\varphi_B(RS))^k \mid 0 \leq k \leq 5\right\} \\ &= \langle \varphi_B(R), \varphi_B(S)\rangle \end{aligned}$$

avec $\varphi_B(S) \in \mathcal{C}_2(\mathbb{Z})$ d'ordre 2 et $\varphi_B(R) \in \mathcal{C}_2(\mathbb{Z})$ d'ordre 6.

On peut remarquer, d'après l'étude faite en **I** que si $B \in \mathcal{C}_2(\mathbb{Z})$ est telle que $h(B) = 2$, on a soit $B = -I_2$ et $\operatorname{tr}(B) = -2$, $\det(B) = 1$, soit $B \neq -I_2$ et B a deux valeurs propres réelles qui sont -1 et 1 et $\det(B) = -1$.

Pour $B = -I_2$, on a $\varphi_B(G) = G$.

(c) On a vu en **I.4.a.** qu'on dispose d'une infinité de matrices $B_n \in \mathcal{C}_2(\mathbb{Z})$ d'ordre 2, de la forme $B_n = \begin{pmatrix} 1 & 0 \\ n & -1 \end{pmatrix}$ où $n \in \mathbb{Z}$. À un telle matrice B_n, on associe l'isomorphisme φ_{B_n} de G sur le groupe $\varphi_{B_n}(G)$ qui est contenu dans $\mathcal{C}_2(\mathbb{Z})$ et de même cardinal que G, soit 12.

Pour tout $n \in \mathbb{Z}$ on a $B_n^{-1} = B_n$ puisque $B_n^2 = I_n$ et :

$$\begin{aligned} \varphi_{B_n}(R) &= \begin{pmatrix} 1 & 0 \\ n & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ n & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1-n & 1 \\ -n^2+n-1 & n \end{pmatrix} \end{aligned}$$

ce qui donne une infinité de matrices. Il y a donc une infinité de groupes $\varphi_{B_n}(G)$ puisque tous ces groupes sont de cardinal 12. En utilisant l'isomorphisme φ de $I(P)$ sur G défini en **II.3.b.** on dispose d'un isomorphisme de groupes de $I(P)$ sur chacun de ces groupes $\varphi_{B_n}(G)$. Cet isomorphisme est tout simplement défini en associant à toute isométrie $\rho \in I(P)$ de matrice $A \in G$ dans la base $\mathcal{B} = (1, j)$, la matrice $B_nAB_n = B_n^{-1}AB_n$ qui est la matrice de ρ dans la base $\mathcal{B}_n = (1 + nj, -j)$.

Partie III

1.

(a) Comme $\mathcal{M}_n(\mathbb{C})$ est un $\mathbb{C}$-espace vectoriel de dimension n^2, le sous-espace vectoriel $\langle G\rangle$ engendré par G est de dimension finie $k \leq n^2$.

(b) Comme G est un système de générateurs de $\langle G\rangle$, on peut en extraire une base $(X_i)_{1\leq i\leq k}$.
Dire que $T(A)=T(B)$ équivaut à dire que, pour i compris entre 1 et k, on a $\operatorname{tr}(AX_i)=\operatorname{tr}(BX_i)$ encore équivalent à $\operatorname{tr}(AX)=\operatorname{tr}(BX)$ pour tout $X\in\langle G\rangle$ du fait que $(X_i)_{1\leq i\leq k}$ une base de $\langle G\rangle$ et que l'application trace est une forme linéaire sur $\langle G\rangle$. On a alors en particulier :

$$\forall X\in G,\ \operatorname{tr}(AX-BX)=\operatorname{tr}\left(\left(AB^{-1}-I_n\right)BX\right)=0$$

encore équivalent à :

$$\forall Y\in G,\ \operatorname{tr}\left(\left(AB^{-1}-I_n\right)Y\right)=0$$

du fait que l'application $X\mapsto BX$ réalise une bijection de G sur lui même.

(c) Si A,B dans G sont tels que $T(A)=T(B)$, on a alors $\operatorname{tr}\left(\left(AB^{-1}-I_n\right)X\right)=0$ pour tout X dans G et pour $X=I_n$, on obtient $\operatorname{tr}\left(AB^{-1}-I_n\right)=0$, soit $\operatorname{tr}\left(AB^{-1}\right)=\operatorname{tr}(I_n)=n$ avec $AB^{-1}\in G\subset\mathcal{C}_n(\mathbb{Z})$, ce qui équivaut à $AB^{-1}=I_n$ d'après **I.3.** soit à $A=B$. L'application T est donc injective et réalise une bijection de G sur $\operatorname{Im}(T)\subset\mathbb{C}^k$.
D'autre part, pour tout $A\in G$ et i compris entre 1 et k, on a $AX_i\in G\subset\mathcal{C}_n(\mathbb{Z})$, de sorte que $|\operatorname{tr}AX_i|\leq n$, soit $\operatorname{Im}(T)\subset\{-n,\cdots,0,\cdots,n\}^k$ et :

$$\operatorname{card}(G)=\operatorname{card}(\operatorname{Im}(T))\leq(2n+1)^k.$$

2.

(a) Soit $P(X)=\sum\limits_{k=0}^{n}a_kX^k$ dans $\mathbb{Z}[X]$ tel que $a_n=1$ et ayant toutes ses racines complexes de module égal à 1. En notant $\lambda_1,\cdots,\lambda_n$ ces racines, on sait que les fonctions symétriques des racines s'écrivent :

$$\sigma_k=\sum_{1\leq i_1<\cdots<i_k\leq n}\lambda_{i_1}\cdots\lambda_{i_k}=(-1)^k a_{n-k}$$

pour tous k compris entre 1 et n, ce qui donne

$$|a_{n-k}|\leq\sum_{1\leq i_1<\cdots<i_k\leq n}|\lambda_{i_1}\cdots\lambda_{i_k}|\leq\sum_{1\leq i_1<\cdots<i_k\leq n}1=C_n^k=C_n^{n-k}.$$

Le $(n-1)$-uplet $(a_0,a_1,\cdots,a_{n-1})$ qui défini le polynôme P est donc dans l'ensemble fini :

$$\prod_{k=0}^{n-1}\left\{-C_n^k,\cdots,0,\cdots,C_n^k\right\}.$$

Il en résulte que l'ensemble de ces polynômes P est fini.

(b) On vu que toute matrice $A\in\mathcal{C}_n(\mathbb{Z})$ est diagonalisable de valeurs propres racines de l'unité. De plus, toute matrice $A\in\mathcal{C}_n(\mathbb{Z})$ a son polynôme caractéristique P_A dans $\mathbb{Z}[X]$, le polynôme $(-1)^n P_A$ étant unitaire de degré n. L'ensemble $\mathcal{P}_n$ de tous ces polynômes est donc fini ainsi que l'ensemble Λ_n de toutes les racines de ces polynômes (les valeurs propres des matrices $A\in\mathcal{C}_n(\mathbb{Z})$), cet ensemble étant contenu dans un groupe U_{N_n} de racines N_n-èmes de l'unité (il suffit de prendre pour N_n le ppcm des ordres de toutes les valeurs propres $\lambda\in\Lambda_n$). On a donc :

$$\forall\lambda\in\Lambda_n,\ \lambda^{N_n}=1.$$

et en diagonalisant chaque matrice $A\in\mathcal{C}_n(\mathbb{Z})$, on déduit que :

$$\forall A\in\mathcal{C}_n(\mathbb{Z}),\ A^{N_n}=I_n.$$

Partie IV

1. On note, pour tout entier $n\geq1$, $\mathbb{Z}_n=\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

(a) Le théorème chinois nous dit que si d_1 et d_2 sont deux entiers premiers entre eux alors les anneaux $\mathbb{Z}_{d_1 d_2}$ et $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ sont isomorphes, un isomorphisme étant réalisé par :

$$\forall \overline{k} \in \mathbb{Z}_{d_1 d_2},\ f\left(\overline{k}\right) = \left(\dot{k}, \ddot{k}\right),$$

où on a noté $\overline{k}$ la classe de k modulo $d_1 d_2$, $\dot{k}$ la classe de k modulo d_1 et $\ddot{k}$ la classe de k modulo d_2. La restriction de f à $\mathbb{Z}_{d_1 d_2}^{\times}$ réalise un isomorphisme de groupes multiplicatifs de $\mathbb{Z}_{d_1 d_2}^{\times}$ sur $\mathbb{Z}_{d_1}^{\times} \times \mathbb{Z}_{d_2}^{\times}$, ce qui entraîne :

$$\varphi(d_1 d_2) = \operatorname{card}\left(\mathbb{Z}_{d_1 d_2}^{\times}\right) = \operatorname{card}\left(\mathbb{Z}_{d_1}^{\times}\right) \operatorname{card}\left(\mathbb{Z}_{d_2}^{\times}\right) = \varphi(d_1)\varphi(d_2).$$

(b) Si p est premier, alors un entier r compris entre 1 et p^k n'est pas premier avec p^k si, et seulement si, il est divisible par p, ce qui équivaut à $r = mp$ avec $1 \leq m \leq p^{k-1}$, il y a donc p^{k-1} possibilités. On en déduit alors que :

$$\varphi\left(p^k\right) = p^k - p^{k-1} = (p-1)\,p^{k-1}.$$

2. Soit λ une valeur propre de A dans E_d. Comme λ est une racine d-ème de l'unité, c'est un nombre complexe algébrique sur $\mathbb{Q}$ (λ est annulé par $X^d - 1 \in \mathbb{Q}[X]$) et on sait que son polynôme minimal est le polynôme cyclotomique Φ_d. En désignant par π_A le polynôme minimal de A, on a $\pi_A(\lambda) = 0$ et π_A est un multiple de Φ_d. L'ensemble E_d des racines de Φ_d est donc contenu dans l'ensemble $\mathrm{Sp}(A)$ des racines de π_A (on peut aussi raisonner avec le polynôme caractéristique P_A de A).

3.

(a) Soit $A \in \mathcal{C}_n(\mathbb{Z})$ d'ordre p.
Le polynôme minimal π_A de A divise le polynôme $X^p - 1 = \prod_{d/p} \Phi_d(X)$ où les $\Phi_d(X) = \prod_{z \in E_d} (X - z)$ sont les polynômes cyclotomiques. On rappelle que chaque polynôme Φ_d est irréductible dans $\mathbb{Q}[X]$, donc π_A est un produit de polynômes cyclotomiques Φ_d où d est un diviseur de p. On sait de plus que les valeurs propres de A sont les racines de π_A. On a donc $\pi_A(X) = \prod_{i=1}^{m} \Phi_{d_i}(X)$, où $d_1, d_2, \cdots, d_m$ sont les différents ordres des valeurs propres de A. Comme π_A divise le polynôme caractéristique P_A, on a :

$$n = \deg(P_A) \geq \deg(\pi_A) = \sum_{i=1}^{m} \deg(\Phi_{d_i})$$

avec $\deg(\Phi_{d_i}) = \operatorname{card}(E_{d_i}) = \varphi(d_i)$.
Plus simplement, on peut aussi dire que $\bigcup_{i=1}^{m} E_{d_i}$ est contenue dans $\mathrm{Sp}(A)$, cette réunion étant disjointe, ce qui entraîne :

$$\begin{aligned}\operatorname{card}\left(\bigcup_{i=1}^{m} E_{d_i}\right) &= \sum_{i=1}^{m} \operatorname{card}(E_{d_i}) = \sum_{i=1}^{m} \varphi(d_i) \\ &\leq \operatorname{card}(\mathrm{Sp}(A)) \leq n.\end{aligned}$$

(b) On a :

$$h(A) = \operatorname{ppcm}(d_1, \cdots, d_m) = \prod_{j=1}^{q} p_j^{k_j},$$

chaque d_r, pour r compris entre 1 et m, admettant la décomposition en facteurs premiers $d_r = \prod_{j=1}^{q} p_j^{k_{r,j}}$ et, pour tout j compris entre 1 et q, $k_j = \max_{1 \leq r \leq m} k_{r,j}$.

Pour j compris entre 1 et q, il existe un entier r compris entre 1 et m tel que $k_j = k_{r,j}$, ce qui signifie que d_r est divisible par $p_j^{k_j}$ et :

$$n \geq \sum_{i=1}^{m} \varphi(d_i) \geq \varphi(d_r) \geq \varphi\left(p_j^{k_j}\right) = p_j^{k_j} - p_j^{k_j-1}.$$

On a donc bien :

$$n \geq \max_{1\leq j\leq q} \left(p_j^{k_j} - p_j^{k_j-1}\right).$$

4.

(a) Soit $n = 2$. Les facteurs premiers p de $h(A)$ doivent être tels que $p^{k-1}(p-1) \leq 2$ avec $k \geq 1$, ce qui impose $p = 2$ et $k = 1$ ou 2, ou $p = 3$ et $k = 1$, soit :

$$h(A) \in \{1, 2, 3, 4, 6, 12\}.$$

Et en partie **I** on a vu que les seules valeurs possibles et atteintes pour $h(A)$ sont $1, 2, 3, 4, 6$, c'est-à-dire que la valeur 12 est exclue. On a vu également que $N_2 = 12$.

(b) Soit $n = 3$. Les facteurs premiers p de $h(A)$ doivent être tels que $p^{k-1}(p-1) \leq 3$ avec $k \geq 1$, ce qui impose $p = 2$ et $k = 1$ ou 2, ou $p = 3$ et $k = 1$, soit :

$$h(A) \in \{1, 2, 3, 4, 6, 12\}.$$

En utilisant les matrices du cas $n = 2$, on voit que les valeurs $1, 2, 3, 4, 6$ sont atteintes (prendre les matrices $\begin{pmatrix} A & 0 \\ 1 & 1 \end{pmatrix}$ où A est une matrice 2×2 d'ordre $1, 2, 3, 4$ ou 6).
Supposons qu'il existe une matrice A telle que $h(A) = \text{ppcm}(d_1, \cdots, d_m) = 12 = 2^2 3$. Si $m = 1$, alors $d_1 = 12$ ce qui est incompatible avec $n = 3 \geq \varphi(12) = 4$. Si $m = 2$, alors (d_1, d_2) peut prendre les valeurs $(1, 12)$ ou $(3, 4)$ incompatibles avec $n = 3 \geq \varphi(d_1) + \varphi(d_2)$. La valeur 12 est donc exclue et $h(A) \in \{1, 2, 3, 4, 6\}$. Là encore $N_3 = 12$.

(c) Soit $n = 4$. Les facteurs premiers p de $h(A)$ doivent être tels que $p^{k-1}(p-1) \leq 4$ avec $k \geq 1$, ce qui impose $p = 2$ et $k = 1, 2$ ou 3, ou $p = 3$ et $k = 1$, ou $p = 5$ et $k = 1$, soit :

$$h(A) \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}.$$

Avec $4 \geq \sum_{i=1}^{m} \varphi(d_i)$, on voit que $d_i \leq 12$ pour tout i compris entre 1 et m puisque $\varphi(12) = 4$ et $\varphi(d) \geq 8$ pour $d \geq 15$ ($h(A)$ étant le ppcm des d_i, chaque d_i divise $h(A)$ qui divise 120). Les d_i, pour i compris entre 1 et m, sont donc dans $\{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Comme $\varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$, on a $m = 1$ si l'un des d_i vaut $5, 8, 10$ ou 12 et $h(A) = 12$ dans ce cas. Si tous les d_i sont dans $\{1, 2, 3, 4, 6\}$, on a $h(A) \leq 12$ puisque c'est le ppcm des d_i. On a donc :

$$h(A) \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$$

et $N_4 = \text{ppcm}(1, 2, 3, 4, 5, 6, 8, 10, 12) = 120$ est un multiple de tous les $h(A)$.
En utilisant les matrices du cas $n = 3$, on voit que les valeurs $1, 2, 3, 4, 6$ sont atteintes
En utilisant les matrices $R^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ d'ordre 3 et $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ d'ordre 4, on construit les matrices :

$$\begin{pmatrix} R^2 & 0 \\ 0 & T \end{pmatrix} \text{ et } \begin{pmatrix} 0 & I_2 \\ T & 0 \end{pmatrix}$$

qui son respectivement d'ordre 12 et 8.
On vérifie que les matrices :

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

sont respectivement d'ordre 5 et 10. Toutes les valeurs prévues pour $h(A)$ sont donc permises et $N_4 = 120$ est la plus petite valeur possible.

(d) Plus généralement, pour $n \geq 2$, on peut montrer (mais c'est difficile) que :

$$\{h(A) \mid A \in \mathcal{C}_n(\mathbb{Z})\} = \left\{ \operatorname{ppcm}(d_1, \cdots, d_m) \text{ où } \left\{ \begin{array}{l} 1 \leq m \leq n, \\ 1 \leq d_m \leq \cdots \leq d_1, \\ n = \sum\limits_{i=1}^{m} \varphi(d_i) \end{array} \right. \right\}$$

Partie V

Partie V.A

1. Une isométrie $\rho \in I(V_3)$ étant une application affine qui permute les sommets de V_3, elle laisse invariant l'isobarycentre O de ces sommets et on peut l'identifier à sa partie linéaire.
Le morphisme de groupes multiplicatifs :

$$\begin{array}{rccc} \delta : & I(V_3) & \rightarrow & \{-1, 1\} \\ & \rho & \mapsto & \det(\rho) \end{array}$$

a pour noyau $\ker(\delta) = I^+(V_3)$ et est surjectif (si σ est la symétrie par rapport à O, alors $\delta(\sigma) = -1$), il induit donc une bijection de l'ensemble quotient $\dfrac{I(V_3)}{\ker(\delta)}$ sur $\{-1, 1\}$ et :

$$\operatorname{card}(I(V_3)) = 2 \operatorname{card}\left(I^+(V_3)\right).$$

À toute isométrie $\rho \in I(V_3)$ on peut associer la permutation :

$$\sigma = \begin{pmatrix} A & B & C & A' & B' & C' \\ \rho(A) & \rho(B) & \rho(C) & \rho(A') & \rho(B') & \rho(C') \end{pmatrix}$$

L'application $\psi : \rho \mapsto \sigma$ réalise alors un morphisme de groupes de $I(V_3)$ dans le groupe S_6 des permutations de l'ensemble $S = \{A, B, C, A', B', C'\}$ des sommets de V_3.
Si $\sigma = \psi(\rho) = I_d$, alors ρ laisse fixe les points O, A, B, C qui forment un repère affine de $\mathbb{R}^3$ et $\rho = I_d$.
Le morphisme ψ est donc injectif et ψ réalise un isomorphisme de groupes de $I(V_3)$ sur $\operatorname{Im}(\psi)$. Il nous suffit donc de compter les éléments de $\operatorname{Im}(\psi)$.
Pour $\rho \in I(V_3)$, on a 6 possibilités pour $\rho(A)$ et comme le milieu O du segment $[AA']$ a pour image le milieu $\rho(O) = O$ de $[\rho(A)\rho(A')]$, l'image $\rho(A')$ est uniquement déterminée par $\rho(A)$. Le couple $(\rho(A), \rho(A'))$ étant choisi, il reste 4 possibilités pour $\rho(B)$, l'image $\rho(B')$ étant déterminée par $\rho(B)$ puisque O est le milieu de $[BB']$. Enfin, ayant choisi $\rho(A)$ et $\rho(B)$, il reste 2 possibilités pour $\rho(C)$, l'image $\rho(C')$ étant déterminée par celle de C. On a donc $\operatorname{card}(\operatorname{Im}(\psi)) \leq 6 \cdot 4 \cdot 2 = 48$. Réciproquement la donnée d'une de ces 48 permutations définit un élément de $I(V_3)$. On a donc :

$$\operatorname{card}(I(V_3)) = \operatorname{card}(\operatorname{Im}(\psi)) = 48$$

et :

$$\operatorname{card}\left(I^+(V_3)\right) = 24.$$

2. On désigne par r_1 la rotation d'axe orienté d'axe $\mathbb{R}\overrightarrow{k}$ et d'angle $\dfrac{\pi}{2}$, r_2 la rotation d'axe orienté d'axe $\mathbb{R}\left(\overrightarrow{\imath} + \overrightarrow{\jmath} + \overrightarrow{k}\right)$ et d'angle $\dfrac{2\pi}{3}$ et r_3 la rotation d'axe orienté d'axe $\mathbb{R}\overrightarrow{\jmath}$ et d'angle π. Ces rotations sont dans $I^+(V_3)$, r_1 étant d'ordre 4, r_2 d'ordre 3 et r_3 d'ordre 2.
Le groupe $H = \langle r_1, r_2, r_3 \rangle$ engendré par r_1, r_2, r_3 contient le groupe :

$$H' = \langle r_1, r_2 \rangle = \left\{ r_1^{k_1} r_2^{k_2} \mid 0 \leq k_1 \leq 3,\ 0 \leq k_2 \leq 2 \right\}$$

qui a 12 éléments et r_3, donc $\operatorname{card}(H) \geq 13$ et $\operatorname{card}(H)$ divise $\operatorname{card}(I^+(V_3)) = 24$ (théorème de Lagrange), ce qui donne $\operatorname{card}(H) = 24$ et $H = I^+(V_3)$.

3.

(a) En désignant par $I\left(\mathbb{R}^3\right)$ le groupe des isométries de $\mathbb{R}^3$ qui laissent fixe l'origine O, l'application $\mathcal{A}$ qui associe à toute isométrie $f \in I\left(\mathbb{R}^3\right)$ la matrice $A \in GL_3(\mathbb{R})$ dans la base $(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k})$ de sa partie linéaire u, réalise un morphisme de groupes injectif de $I\left(\mathbb{R}^3\right)$ dans $GL_3(\mathbb{R})$ et $G(V_3) = \mathcal{A}(I(V_3))$ est un sous-groupe d'ordre 48 de $GL_3(\mathbb{R})$, il en résulte que $G(V_3)$ est un groupe de $\mathcal{C}_3(\mathbb{R})$.
Pour toute isométrie $f \in I(V_3)$, l'application linéaire associée u transformant la base $\left(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}\right)$ en $\left(\pm\overrightarrow{\imath}, \pm\overrightarrow{\jmath}, \pm\overrightarrow{k}\right)$, on en déduit que la matrice A de u dans cette base est à coefficients entier, donc $G(V_3) \subset \mathcal{C}_3(\mathbb{Z})$.

(b) Les matrices dans la base $\left(\overrightarrow{\imath}, \overrightarrow{\jmath}, \overrightarrow{k}\right)$ des trois rotations qui engendrent $I^+(V_3)$ sont respectivement :

$$R_1 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ R_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ R_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

et celle de la symétrie s par rapport à O est $-I_3$. Comme r_1, r_2, r_3, s engendrent $I(V_3)$, on déduit que les matrices R_1, R_2, R_3, S engendrent $G(V_3)$.

(c) Comme R_2 est d'ordre 3, la matrice

$$A = -R_2 = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

est d'ordre 6 dans $G(V_3)$, c'est la matrice d'un antidéplacement qui laisse O fixe.

(d) On a $G(V_3) \subset \mathcal{C}_3(\mathbb{Z})$ et on a vu en partie **IV** que les valeurs prises par h sur $\mathcal{C}_3(\mathbb{Z})$ sont $1, 2, 3, 4, 6$. On vient de voir qu'il existe dans $G(V_3)$ des éléments d'ordre $2, 3, 4, 6$ et tenant compte de I_3 qui est d'ordre 1, on a toutes les valeurs possibles de h sur $G(V_3)$.

Partie V.B

1.

(a) Comme dans le cas $n = 3$, on voit que si S_8 est le groupe des permutations des sommets $\{A, B, \cdots, D'\}$ de V_4, alors l'application :

$$\begin{array}{cccc} \Psi : & I(V_3) & \to & S_4 \\ & \rho & \mapsto & \begin{pmatrix} A & B & \cdots & D' \\ \rho(A) & \rho(B) & \cdots & \rho(D') \end{pmatrix} \end{array}$$

réalise un morphisme de groupes injectif de $I(V_3)$ dans S_8 ((O, A, B, C, D) est un repère affine).

(b) Là encore, le même raisonnement que dans le cas $n = 3$, nous donne :

$$\mathrm{card}(I(V_4)) = 2\,\mathrm{card}\left(I^+(V_4)\right) = 384.$$

De manière plus générale, en désignant, pour $n \geq 3$, par O une origine de l'espace affine euclidien $\mathbb{R}^n$, par $(e_k)_{1 \leq k \leq n}$ la base canonique de $\mathbb{R}^n$, par $(A_k)_{1 \leq k \leq n}$ et $(A'_k)_{1 \leq k \leq n}$ les suites de points définies par $\overrightarrow{OA'_k} = -\overrightarrow{OA_k} = -e_k$ et par V_n le polytope de centre O et de sommets $A_1, \cdots, A_n, A'_1, \cdots, A'_n$, on a :

$$\mathrm{card}(I(V_n)) = 2\,\mathrm{card}\left(I^+(V_n)\right) = 2^n n!$$

La démonstration se faisant comme dans le cas $n = 3$.

2. La permutation :
$$\begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_2 & e_3 & e_4 & -e_1 \end{pmatrix}$$
définit un élément $\rho \in I^+ (V_4)$ d'ordre 8.
3. La matrice de ρ :
$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
est d'ordre 8 dans $\mathcal{C}_4 (\mathbb{Z}) \cap O (4)$.
Plus généralement la matrice d'ordre $n \geq 3$:
$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$
a pour polynôme caractéristique $P_A (X) = X^n + 1$. Ces valeurs propres sont donc les n racines n-ème de -1, donc A est diagonalisables et sur la forme diagonale, on voit que $A^k \neq I_n$ pour $1 \leq k \leq 2n - 1$ et $A^{2n} = I_n$. On a donc une matrice d'ordre $2n$ dans $\mathcal{C}_n (\mathbb{Z}) \cap O (n)$.