

Agrégation interne 1996 de Mathématiques première composition

solution proposée par Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159,
dany-jack.mercier@univ-ag.fr

NB : Le sujet de l'épreuve n'est pas joint à ce document. Il pourra être téléchargé au format pdf sur le site <http://perso.wanadoo.fr/megamaths>.

⁰[ag40] v1.04

© 2007 D.-J. Mercier. Vous pouvez faire une copie de ces notes pour votre usage personnel.

Solution de la première composition de l'agrégation interne 1996

***** **Partie I** *****

I.1.a Si λ est valeur propre de A , il existe un vecteur non nul X dans \mathbb{C}^n tel que $AX = \lambda X$. Une récurrence montre que $A^k X = \lambda^k X$ pour tout entier naturel k . En particulier, si $A^p = I$, on trouve $X = A^p X = \lambda^p X$ soit $\lambda^p = 1$, et λ est bien une racine p -ième de l'unité.

I.1.b Soient λ_1 et λ_2 les valeurs propres de A . Le polynôme caractéristique de A s'écrit

$$\chi_A(X) = X^2 - (\text{tr } A)X + \det A = (X - \lambda_1)(X - \lambda_2) = X^2 - (\lambda_1 + \lambda_2)X + \lambda_1\lambda_2$$

λ_1 et λ_2 sont de module 1 puisque racines p -ièmes de l'unité, et donc

$$|\text{tr } A| = |\lambda_1 + \lambda_2| \leq |\lambda_1| + |\lambda_2| = 2$$

Par suite $\text{tr } A \in \{-2, -1, 0, 1, 2\}$. D'autre part $A^p = I$ entraîne $(\det A)^p = 1$, et donc $\det A = \pm 1$ puisque $\det A$ est un entier relatif.

I.2.a Si $\text{tr } A = 2\varepsilon$, $\chi_A(X) = X^2 - 2\varepsilon X + \det A$. Le discriminant est $\Delta = 4(1 - \det A)$. Si $\det A = -1$, les racines λ_1 et λ_2 de χ_A sont $\frac{2\varepsilon \pm 2\sqrt{2}}{2} = \varepsilon \pm \sqrt{2}$, ce qui est absurde car ce ne sont pas des racines de l'unité. Par conséquent $\det A = 1$ et $\Delta = 0$. Cela prouve que $\lambda_1 = \lambda_2 = \varepsilon$. La matrice A sera semblable à εI (A est toujours diagonalisable dans \mathbb{C} , puisque, étant cyclique, elle annule un polynôme du type $X^p - 1$ scindé sur \mathbb{C} et dont toutes les racines sont simples), et par conséquent il existe P inversible telle que $A = P^{-1}(\varepsilon I)P = \varepsilon I$.

On a alors clairement $h(I) = 1$ et $h(-I) = 2$, ce que l'on peut traduire par $h(A) = \frac{1}{2}(3 - \varepsilon)$.

I.2.b Les valeurs propres de A sont réelles et distinctes, et ne peuvent valoir que ± 1 , donc $\lambda_1 = \varepsilon$ et $\lambda_2 = -\varepsilon$. A possède deux valeurs propres distinctes donc sera diagonalisable et semblable à la matrice diagonale $\text{diag}(\varepsilon, -\varepsilon)$. On aura donc $h(A) = 2$. Il existe une infinité de matrice A de ce type. Il suffit de choisir une matrice $P = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ avec $\det P = \alpha\delta - \beta\gamma = \pm 1$ pour que P soit inversible avec $P^{-1} \in \mathcal{M}_2(\mathbb{Z})$, et que

$$A = P^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} P = \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

convienne. Bezout nous offre d'ailleurs une infinité de solutions entières à $\alpha\delta - \beta\gamma = 1$. Prenons par exemple $\delta = 3$ et $\gamma = 5$. On sait résoudre $3\alpha - 5\beta = 1$ en nombres entiers. On trouve $(\alpha, \beta) = (5u + 2, 3u + 1)$ où $u \in \mathbb{Z}$ avec

$$A = \begin{pmatrix} 3 & -5 \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha & 5 \\ \beta & 3 \end{pmatrix} = \begin{pmatrix} 3\alpha + 5\beta & 30 \\ -2\alpha\beta & -(3\alpha + 5\beta) \end{pmatrix}$$

$$A = \begin{pmatrix} 30u + 11 & 30 \\ -30u^2 - 22u - 4 & -(30u + 11) \end{pmatrix} \quad \text{où } u \in \mathbb{Z}$$

Deuxième solution : Si $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$ vérifie $\lambda_1 = 1, \lambda_2 = -1$ et $h(A) = 2$, alors

$$\begin{cases} \operatorname{tr} A = a + d = 0 \\ \det A = ad - bc = -1 \end{cases} \quad \text{i.e.} \quad \begin{cases} d = -a \\ a^2 + bc = 1 \end{cases}$$

et donc $A = \begin{pmatrix} a & c \\ b & -a \end{pmatrix}$ avec $a, b, c \in \mathbb{Z}$ et $a^2 + bc = 1$ (*).

Réciproquement, si A vérifie (*), ses valeurs propres vérifieront $\lambda_1 + \lambda_2 = 0$ et $\lambda_1 \lambda_2 = -1$, d'où $(\lambda_1, \lambda_2) = (1, -1)$. A sera semblable à $\operatorname{diag}(1, -1)$ donc d'ordre $h(A) = 2$. On remarque pour finir qu'il existe bien une infinité de matrices du type (*) (prendre $b = 1$ et $c = 1 - a^2$ par exemple).

I.2.c On suppose que λ_1 et λ_2 ne sont pas réelles. Alors $\operatorname{tr} A \neq \pm 2$ d'après I.2.a et l'on va envisager les trois cas restants. On rappelle que

$$\chi_A(X) = X^2 - (\operatorname{tr} A)X + \det A = X^2 - (\lambda_1 + \lambda_2)X + \lambda_1 \lambda_2$$

- Si $\operatorname{tr} A = -1$, $\chi_A(X) = X^2 + X + \det A$. Le discriminant $\Delta = 1 - 4 \det A$ doit être strictement négatif pour que λ_1, λ_2 soient complexes non réelles, donc $\det A = 1$ et $\Delta = -3$. Par suite $\{\lambda_1, \lambda_2\} = \left\{ \frac{-1 \pm i\sqrt{3}}{2} \right\} = \{j, j^2\}$. A est semblable à $\begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$ et donc $A^k = I$ si, et seulement si, k est multiple de 3. Dans ce cas $h(A) = 3$.

- Si $\operatorname{tr} A = 0$, $\chi_A(X) = X^2 + \det A$ admet des racines complexes non réelles si, et seulement si, $\det A = 1$, et alors $\{\lambda_1, \lambda_2\} = \{\pm i\}$. Dans ce cas A est semblable à $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ et $h(A) = 4$.

- Si $\operatorname{tr} A = 1$, $\chi_A(X) = X^2 - X + \det A$ et $\Delta = 1 - 4 \det A$ sera strictement négatif pour $\det A = 1$. Par suite $\Delta = -3$ et $\{\lambda_1, \lambda_2\} = \left\{ \frac{1 \pm i\sqrt{3}}{2} \right\} = \{\alpha, -j\}$ où $\alpha = e^{i\frac{\pi}{3}}$. A est semblable à $\begin{pmatrix} \alpha & 0 \\ 0 & -j \end{pmatrix}$ donc $A^k = I$ si, et seulement si, k est multiple de 6. Ici $h(A) = 6$.

- Montrons qu'il existe une infinité de matrice $A \in \mathcal{M}_2(\mathbb{Z})$ telles que $\operatorname{tr} A = -1$, les autre cas se traitant de la même façon. Si

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

est solution, alors

$$\begin{cases} \operatorname{tr} A = a + d = -1 \\ \det A = ad - bc = 1 \end{cases} \Rightarrow \begin{cases} bc = -a^2 - a - 1 \\ d = -a - 1 \end{cases}$$

et

$$A = \begin{pmatrix} a & -\frac{a^2+a+1}{b} \\ b & -a-1 \end{pmatrix}$$

Réciproquement, cette matrice est à coefficients entiers dès que $b \mid (a^2 + a + 1)$ et vérifie $\operatorname{tr} A = -1$. Un calcul montre que $A^3 = I$, de sorte que A soit cyclique.

I.3.a On vient de voir que $h(A) \in \{1, 2, 3, 4, 6\}$ pour tout $A \in \mathcal{C}_2(\mathbb{Z})$ donc $A^{12} = I$ pour tout $A \in \mathcal{C}_2(\mathbb{Z})$.

I.3.b Cette propriété est évidemment fausse dans $\mathcal{C}_2(\mathbb{R})$. Pour le voir, il suffit de considérer la matrice d'une rotation d'angle $\frac{2\pi}{n}$. C'est une matrice cyclique d'ordre n , et ceci quelque soit l'entier n .

I.4.a Si $A \in \mathcal{C}_2(\mathbb{Z})$ est d'ordre p , alors $A^p = I$ donc $AA^{p-1} = A^{p-1}A = I$ et A est inversible d'inverse $A^{-1} = A^{p-1} \in \mathcal{M}_2(\mathbb{Z})$. De plus $(A^{-1})^p = I$ donc $A^{-1} \in \mathcal{C}_2(\mathbb{Z})$. Enfin $h(A^{-1}) = h(A)$ car

$$A^k = I \Leftrightarrow (A^{-1})^k = I$$

I.4.b A la fin de la question I.2.c, on a exhibé une matrice de $\mathcal{C}_2(\mathbb{Z})$ non triviale en fonction de a et b . Prenons $(a, b) = (1, 3)$. On obtient

$$A = \begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix} \in \mathcal{C}_2(\mathbb{Z})$$

La matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ est aussi cyclique et

$$DA = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -3 & 2 \end{pmatrix}$$

est une matrice de trace 3, donc non cyclique d'après I.1.b.

***** **Partie II** *****

II.1.a $(\mathbb{Z}[j], +)$ est un sous-groupe de $(\mathbb{C}, +)$ puisque c'est une partie non vide de \mathbb{C} ($0 \in \mathbb{Z}[j]$) et puisque si $m + qj$ et $m' + q'j$ sont deux éléments de $\mathbb{Z}[j]$, alors

$$(m + qj) - (m' + q'j) = (m - m') + (q - q')j \in \mathbb{Z}[j].$$

La loi \times est interne dans $\mathbb{Z}[j]$ car $j^2 + j + 1 = 0$ entraîne

$$(m + qj)(m' + q'j) = mm' - qq' + (mq' + qm' - qq')j \in \mathbb{Z}[j].$$

Finalement $\mathbb{Z}[j]$ est un sous-anneau de \mathbb{C} .

$\alpha^3 = -1$ entraîne $\alpha^3 + 1 = 0$, et comme $\alpha \neq -1$, $\alpha^2 - \alpha + 1 = 0$. Par suite

$$j = \alpha^2 = -1 + \alpha \in \mathbb{Z}[\alpha] \quad \text{et} \quad \alpha = -j^2 = 1 + j \in \mathbb{Z}[j]$$

prouve que $\mathbb{Z}[j] = \mathbb{Z}[\alpha]$.

II.1.b • On a

$$|m + qj|^2 = \left| m - \frac{q}{2} + q\frac{\sqrt{3}}{2}i \right|^2 = \left(m - \frac{q}{2} \right)^2 + \frac{3}{4}q^2 = m^2 + q^2 - mq$$

de sorte que

$$(*) \quad 0 < |m + qj| \leq 1 \Leftrightarrow 0 < m^2 + q^2 - mq \leq 1 \\ \Leftrightarrow m^2 + q^2 - mq = 1 \quad \text{puisque } m, q \in \mathbb{Z}$$

L'équation $m^2 - qm + q^2 - 1 = 0$ en m est de discriminant $\Delta = 4 - 3q^2$, et admettra des racines réelles si, et seulement si, $\Delta \geq 0$, i.e. $q \in \{-1, 0, 1\}$. Pour chacune de ces valeurs de q , on obtient les valeurs correspondantes de m . On trouve

$$(m, q) \in \{(0, -1), (-1, -1), (1, 0), (-1, 0), (1, 1), (0, 1)\}$$

et l'ensemble des solutions de (*) est

$$A = \{1, j, j^2, -1, -j, -j^2\}.$$

C'est l'ensemble des affixes des sommets d'un hexagone régulier.

Autre solution : (*) entraîne $(m - \frac{q}{2})^2 + \frac{3}{4}q^2 \leq 1$ puis $|m - \frac{q}{2}| \leq 1$ et $|\frac{\sqrt{3}}{2}q| \leq 1$. On doit donc avoir

$$-1 - \frac{1}{\sqrt{3}} \leq m \leq 1 + \frac{1}{\sqrt{3}} \quad \text{et} \quad -\frac{2}{\sqrt{3}} \leq q \leq \frac{2}{\sqrt{3}}.$$

Comme $(m, q) \in \mathbb{Z}^2$, on déduit $m, q \in \{-1, 0, 1\}$. Réciproquement, on constate que $(0, 0)$, $(-1, 1)$, $(1, -1)$ sont à rejeter mais que tous les autres couples vérifient (*).

• Dire que $m + qj \in U_6$, équivaut à dire l'existence de $m', q' \in \mathbb{Z}$ tels que $(m + qj)(m' + q'j) = 1$, ce qui entraîne $|m + qj|^2 |m' + q'j|^2 = 1$. L'entier $|m + qj|^2$ est donc un diviseur de 1, et l'on peut écrire $|m + qj|^2 = 1$. D'après ce qui précède, cela équivaut à $(m, q) \in A$ et l'on aura $U_6 \subset A$. La réciproque est triviale, donc $U_6 = A$.

II.2 $P = \{e^{ik\frac{\pi}{3}} / k = 0, \dots, 5\}$. P est clairement invariant par la rotation r et la réflexion s définie par

$$r(z) = e^{i\frac{\pi}{3}}z \quad \text{et} \quad s(z) = \bar{z}.$$

On constate facilement que $r^6 = Id = s^2$, et $r^5 \neq Id$. r est donc d'ordre 6.

Si ρ est une rotation conservant P , ρ est affine donc transforme l'isobarycentre O de P en l'isobarycentre de $\rho(P) = P$, i.e. O . Cela montre que $\rho(O) = O$ et donc que O est le centre de la rotation ρ . Comme $\rho(e^{i\frac{\pi}{3}}) \in P$, il existe $k \in \{0, \dots, 5\}$ tel que $\rho(e^{i\frac{\pi}{3}}) = e^{ik\frac{\pi}{3}}$. ρ s'exprime par $\rho(z) = \zeta z$ où $\zeta \in \mathbb{C}^*$, de sorte qu'ici $\zeta = e^{i(k-1)\frac{\pi}{3}}$. Cela entraîne $\rho = r^{k-1}$ et prouve que si $I^+(P)$ désigne le sous-groupe des déplacements laissant P globalement invariant,

$$I^+(P) \subset\subset \langle r \rangle = \{Id, r, r^2, \dots, r^5\}$$

L'inclusion inverse ayant été déjà signalée, on déduit

$$I^+(P) = \{Id, r, r^2, \dots, r^5\}$$

Soit $I^-(P) = I(P) \setminus I^+(P)$. On vérifie sans peine que l'application

$$\begin{aligned} \Psi : I^+(P) &\rightarrow I^-(P) \\ \rho &\mapsto s \circ \rho \end{aligned}$$

est bijective, donc $I(P) = I^+(P) \cup (s \circ I^+(P))$ est bien engendré par r et s .

II.3.a

$$\begin{cases} r(1) = e^{i\frac{\pi}{3}} = -j^2 = 1 + j \\ r(j) = e^{i\frac{\pi}{3}} e^{i\frac{2\pi}{3}} = -1 \end{cases} \quad \text{et} \quad \begin{cases} s(1) = 1 \\ s(j) = \bar{j} = j^2 = -1 - j \end{cases}$$

donc les matrices de r et s dans la base $(1, j)$ sont respectivement

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

II.3.b L'application qui à un automorphisme du \mathbb{R} -espace vectoriel \mathbb{C} associe sa matrice (inversible) dans la base $(1, j)$ est un isomorphisme de groupe, et par restriction on obtient le monomorphisme

$$\begin{aligned} \Phi : I(P) &\rightarrow \mathcal{M}_2(\mathbb{R}) \\ f &\mapsto \text{Mat}(f; (1, j)) \end{aligned}$$

L'image de Φ est un sous-groupe G de $GL_2(\mathbb{R})$ formé d'éléments de $\mathcal{C}_2(\mathbb{Z})$, et

$$\begin{aligned} \Phi : I(P) &\rightarrow G \\ f &\mapsto \text{Mat}(f; (1, j)) \end{aligned}$$

sera un isomorphisme. On aura encore $R^6 = I = S^2$, $R^5 \neq I$ et $RS = SR^{-1}$.

II.4.a $\begin{vmatrix} m_1 & m_2 \\ q_1 & q_2 \end{vmatrix} = -1 \neq 0$ donc (z_1, z_2) est une base du \mathbb{R} -espace vectoriel \mathbb{C} . Tout complexe, et en particulier tout nombre $m + qj \in \mathbb{Z}[j]$, s'écrit de façon unique dans cette base :

$$m + qj = m'z_1 + q'z_2.$$

Les formules de changement de base sont

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

qui s'inversent dans \mathbb{Z} en

$$\begin{pmatrix} m' \\ q' \end{pmatrix} = - \begin{pmatrix} q_2 & -m_2 \\ -q_1 & m_1 \end{pmatrix} \begin{pmatrix} m \\ q \end{pmatrix}$$

et l'on constate que $m', q' \in \mathbb{Z}$.

II.4.b L'application

$$\begin{aligned} \Psi : (G, \times) &\rightarrow (GL_2(\mathbb{R}), \times) \\ A &\mapsto BAB \end{aligned}$$

est un monomorphisme de groupes car $B^2 = I$. En effet $BAB = I$ entraîne $A = I$ et :

$$\Psi(AA') = BAA'B = BABBA'B = \Psi(A)\Psi(A')$$

Par suite, l'image $\mathcal{G} = \{BAB / A \in G\}$ de Ψ sera un sous-groupe de $GL_2(\mathbb{R})$ isomorphe à G . On a $\mathcal{G} \subset \mathcal{C}_2(\mathbb{Z})$.

II.4.c L'application

$$\begin{aligned} \Lambda : (G, \times) &\rightarrow (GL_2(\mathbb{R}), \times) \\ A &\mapsto Q^{-1}AQ \end{aligned}$$

où $Q = \begin{pmatrix} m_1 & m_2 \\ q_1 & q_2 \end{pmatrix}$ représente la matrice de passage de la base $(1, j)$ à la base (z_1, z_2) de la question II.4.a, est bien définie puisque Q et Q^{-1} sont à coefficients dans \mathbb{Z} . Λ est un monomorphisme de groupes car

$$\Lambda(AA') = Q^{-1}AA'Q = (Q^{-1}AQ)(Q^{-1}A'Q) = \Lambda(A)\Lambda(A')$$

et $Q^{-1}AQ = I$ entraîne $A = I$. On pose $\mathcal{G}_Q = \text{Im } \Lambda = \{Q^{-1}AQ / A \in G\}$. \mathcal{G}_Q est un groupe de $\mathcal{C}_2(\mathbb{Z})$ isomorphe à G par Λ et aussi à $I(P)$ via l'isomorphisme

$$I(P) \xrightarrow{\Phi} G \xrightarrow{\Lambda} \mathcal{G}_Q.$$

Pour montrer que l'on obtient ainsi une infinité de groupes \mathcal{G}_Q , on utilisera le lemme :

Lemme : $Q \neq \pm Q' \Rightarrow \mathcal{G}_Q \neq \mathcal{G}_{Q'}$

Preuve : Si $\mathcal{G}_Q = \mathcal{G}_{Q'}$ alors pour tout $A \in G$ il existe $A' \in G$ telle que $Q^{-1}AQ = Q'^{-1}A'Q'$, soit $A = (Q'Q^{-1})^{-1}A'(Q'Q^{-1})$ et A est semblable à A' . Cela entraîne que A et A' représentent la même application linéaire de $I(P)$ dans la base $(1, j)$, i.e. $A = A'$. En posant $W = Q'Q^{-1}$, on aura donc

$$\forall A \in G \quad WA = AW.$$

Comme R et S engendrent G , cette dernière condition équivaut à

$$WR = RW \text{ et } WS = SW$$

soit en notant $W = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$,

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

soit encore

$$\begin{pmatrix} a+c & -a \\ b+d & -b \end{pmatrix} = \begin{pmatrix} a-b & c-d \\ a & c \end{pmatrix} \text{ et } \begin{pmatrix} a & -a-c \\ b & -b-d \end{pmatrix} = \begin{pmatrix} a-b & c-d \\ -b & -d \end{pmatrix}$$

cela équivaut à $a = d$ et $b = c = 0$. Compte tenu de

$$ad - bc = \det W = \det(Q'Q^{-1}) = (-1)^2 = 1$$

on trouve $a^2 = 1$ donc $a = \pm 1$. Ainsi $W = \pm I$ et $Q = \pm Q'$. ■

Ce lemme prouve qu'il y a une infinité de groupes \mathcal{G}_Q quand Q décrit l'ensemble des matrices $\begin{pmatrix} m_1 & m_2 \\ q_1 & q_2 \end{pmatrix}$ à coefficients entiers telles que $m_1q_2 - m_2q_1 = -1$. Pour le voir, il suffit de fixer deux entiers q_1 et q_2 premiers entre eux puis de résoudre l'égalité de Bezout $m_1q_2 - m_2q_1 = -1$. On trouve $(m_1, m_2) = (\tilde{m}_1 + uq_1, \tilde{m}_2 + uq_2)$ où u décrit \mathbb{Z} , d'où une infinité de matrices Q avec $m_1 > 0$ (et donc ne pouvant pas être opposées ou égales les unes des autres).

***** Partie III *****

III.1.a A annule le polynôme $X^p - 1$ dont toutes les racines sont simples (en effet, $(X^p - 1)' = pX^{p-1}$ ne s'annule que pour $X = 0$ qui n'est pas racine de $X^p - 1$), donc est diagonalisable. Il existe une matrice inversible P telle que $D = P^{-1}AP = \text{Diag}(\lambda_1, \dots, \lambda_n)$. De $D^p = I$, on tire $\lambda_i^p = 1$ et λ_i sera une racine p -ième de l'unité.

III.1.b Avec les notations précédentes, $h(A) = h(D)$ puisque $D^k = I$ équivaut à $P^{-1}A^kP = I$, i.e. $A^k = I$. q_i est l'ordre de λ_i dans \mathbb{C}^* et l'on sait que

$$\lambda_i^k = 1 \Leftrightarrow q_i \mid k$$

En effet, si $k = q_i u$, $\lambda_i^k = (\lambda_i^{q_i})^u = 1$. Réciproquement, si $\lambda_i^k = 1$, la division euclidienne de k par q_i permet d'écrire $k = a q_i + r$ où $0 \leq r < q_i$, et $\lambda_i^{a q_i} \lambda_i^r = 1$ entraîne $\lambda_i^r = 1$, soit $r = 0$ par définition de q_i .

On a

$$\begin{aligned} D^k = \text{Diag}(\lambda_1^k, \dots, \lambda_n^k) = I &\Leftrightarrow \forall i \quad \lambda_i^k = 1 \\ &\Leftrightarrow \forall i \quad q_i \mid k \\ &\Leftrightarrow k \text{ est multiple de } \text{ppcm}(\lambda_1, \dots, \lambda_n) \end{aligned}$$

ce qui prouve que $h(A) = h(D) = \text{ppcm}(\lambda_1, \dots, \lambda_n)$.

III.1.c On a

$$|\text{tr} A| = |\lambda_1 + \dots + \lambda_n| \leq |\lambda_1| + \dots + |\lambda_n| = n \quad (*)$$

Lemme : Soient $\lambda_1, \dots, \lambda_n$ des complexes tels que

$$|\lambda_1 + \dots + \lambda_n| = |\lambda_1| + \dots + |\lambda_n|$$

On suppose $\lambda_1 \neq 0$. Il existe alors un réel θ tel que $\lambda_i = |\lambda_i| e^{i\theta}$ pour tout i .

Preuve : Si $n = 2$, il s'agit du cas d'égalité dans l'inégalité de Minkowski. On peut le montrer directement en élevant au carré :

$$\begin{aligned} |\lambda_1 + \lambda_2| = |\lambda_1| + |\lambda_2| &\Leftrightarrow 2 \text{Re} \lambda_1 \bar{\lambda}_2 = 2 |\lambda_1| |\lambda_2| \\ &\Leftrightarrow \text{Re} \lambda_1 \bar{\lambda}_2 = |\lambda_1 \bar{\lambda}_2| \\ &\Leftrightarrow \lambda_1 \bar{\lambda}_2 \in \mathbb{R}_+ \\ &\Leftrightarrow \bar{\lambda}_1 \lambda_2 = r \in \mathbb{R}_+ \\ &\Leftrightarrow \lambda_2 = \frac{r}{|\lambda_1|^2} \lambda_1 \Leftrightarrow \exists \mu \in \mathbb{R}_+ \quad \lambda_2 = \mu \lambda_1 \end{aligned}$$

Au rang n ,

$$|\lambda_1 + \dots + \lambda_n| \leq |\lambda_1 + \lambda_i| + \left| \widehat{\lambda_1} \right| + \dots + \left| \widehat{\lambda_i} \right| + \dots + |\lambda_n| \leq |\lambda_1| + \dots + |\lambda_n|$$

entraîne, si les extrémités de ces inégalités sont identiques

$$|\lambda_1 + \lambda_i| = |\lambda_1| + |\lambda_i|$$

et d'après ce que l'on vient de voir, $\lambda_i = \mu_i \lambda_1$ avec $\mu_i \in \mathbb{R}_+$. Cela implique $\lambda_i = |\lambda_i| e^{i\theta}$ où $\theta = \arg \lambda_1$, et pout tout i . ■

Revenons à notre problème. Si $|\text{tr} A| = |\lambda_1 + \dots + \lambda_n| = n$, (*) entraîne

$$|\lambda_1 + \dots + \lambda_n| = |\lambda_1| + \dots + |\lambda_n|$$

et le lemme prouve que $\lambda_i = |\lambda_i| e^{i\theta} = e^{i\theta}$ pour tout i . Donc $D = \text{Diag}(\lambda_1, \dots, \lambda_n) = e^{i\theta} I$, et $A = e^{i\theta} I$ est la matrice d'une homothétie. Elle est réelle, donc $A = \pm I$. Si $\text{tr} A = n$, on aura nécessairement $A = I$.

III.2.a $\mathcal{M}_n(\mathbb{C})$ est un \mathbb{C} -espace vectoriel de dimension finie n^2 , donc tous ses sous-espaces vectoriels seront de dimension finie.

III.2.b $T(A) = T(B)$ équivaut à $\text{tr} AX_i = \text{tr} BX_i$ pour tout i , soit $\text{tr}((A - B)X_i) = 0$ puisque l'application trace est linéaire. Tout élément X de $\langle G \rangle$ s'exprime $X = \sum_{i=1}^k \lambda_i X_i$ où $\lambda_i \in \mathbb{C}$, et la linéarité de tr permet d'écrire

$$\forall X \in \langle G \rangle \quad \text{tr}((A - B)X) = \sum_{i=1}^k \lambda_i (\text{tr}(A - B)X_i) = 0$$

L'application $X \mapsto B^{-1}X$ est une bijection de G dans G , donc

$$\forall X \in \langle G \rangle \quad \text{tr}((A - B)B^{-1}X) = 0$$

ce qui s'écrit $\text{tr}((AB^{-1} - I)X) = 0$ comme demandé.

III.2.c $T(A) = T(B)$ entraîne $\text{tr}((AB^{-1} - I)X) = 0$ en particulier pour $X = I$, d'où $\text{tr} AB^{-1} = \text{tr} I = n$, et III.1.c implique $AB^{-1} = I$, soit $A = B$. L'injectivité de T est démontrée. On a vu en III.1.c que $|\text{tr} AX_i| \leq n$ pour tout $A \in G$, de sorte que $\text{Im } T \subset [-n, n]^k$ soit un ensemble fini. Comme T est injective, G sera aussi un ensemble fini de cardinal $\leq (2n + 1)^k$.

III.3.a Soit $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ un polynôme de $\mathbb{Z}[X]$ n'admettant que des racines de module 1. Si $\lambda_1, \dots, \lambda_n$ désignent ces racines, les relations entre coefficients d'un polynôme et racines permettent d'écrire

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

pour tous $k \in \mathbb{N}_n$. D'où $|a_{n-k}| \leq C_n^k$. Les coefficients de P étant entiers et dans des intervalles bornés, seront en nombre fini, et les polynômes P seront aussi.

III.3.b Les racines des polynômes caractéristiques χ_A des matrices $A \in \mathcal{C}_n(\mathbb{Z})$ sont, on l'a vu, des racines de l'unité. Ces polynômes sont à coefficients entiers et la question précédente montre qu'il y en a un nombre fini. Soit \mathcal{P} l'ensemble de tous ces polynômes et \mathcal{L} celui de toutes les racines de ces polynômes. Le ppcm N_n des ordres de toutes ces racines vérifie

$$\forall \lambda \in \mathcal{L} \quad \lambda^q = 1$$

Si $A \in \mathcal{C}_n(\mathbb{Z})$, A est semblable à une matrice

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \text{où } \lambda_i \in \mathcal{L}$$

et donc $D^{N_n} = I$. On déduit

$$\forall A \in \mathcal{C}_n(\mathbb{Z}) \quad A^{N_n} = I$$

***** **Partie IV** *****

IV.1.a Un entier m est premier avec p^k si, et seulement si, p ne divise pas m . Les entiers m , compris entre 1 et p^k , et qui ne sont pas premiers avec p^k sont donc les multiples de p . Il vérifie

$$1 \leq m = up \leq p^k \quad \text{et donc} \quad 1 \leq u \leq p^{k-1}$$

Il y en a p^{k-1} . Par suite, il y aura exactement $p^k - p^{k-1}$ entiers m inférieurs ou égaux à p^k et premiers avec p^k . Soit $\varphi(p^k) = p^k - p^{k-1}$.

IV.1.b Les ensembles E_d sont disjoints deux à deux puisqu'aucun complexe ne peut avoir deux ordres multiplicatifs différents. L'énoncé a rappelé le résultat : si $\lambda \in E_d$ est valeur propre de A , toutes les racines primitives d -ièmes de l'unité sont valeurs propres de A , donc racines du polynôme caractéristique de A , qui est de degré n . On en déduit, en notant $\text{Sp } A$ l'ensemble des valeurs propres de A (le spectre de A) :

$$\bigcup_{1 \leq i \leq m} E_{d_i} \subset \text{Sp } A \quad (\text{réunion disjointe})$$

d'où $n \geq \sum_{i=1}^m \varphi(d_i)$ puisque $\varphi(d_i) = \#E_{d_i}$.

IV.1.c

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

Si $j \in \mathbb{N}_q$, il existe $s \in \mathbb{N}_m$ tel que d_s admette $p_j^{k_j}$ comme diviseur. On déduit

$$n \geq \sum_{i=1}^m \varphi(d_i) \geq \varphi(d_s) \geq \varphi(p_j^{k_j}) = p_j^{k_j} - p_j^{k_j-1}$$

IV.2 • Si $n = 2$, on cherche p premier et k tels que $p^k - p^{k-1} \leq 2$.

$$\begin{aligned} \text{Si } p = 2, \quad 2^k - 2^{k-1} &= \begin{cases} 1 & \text{si } k = 1 \\ 2 & \text{si } k = 2 \end{cases} \\ \text{Si } p = 3, \quad 3^k - 3^{k-1} &= \begin{cases} 1 & \text{impossible car multiple de 2} \\ 2 & \text{si } k = 1 \end{cases} \\ \text{Si } p > 3, \quad p^k - p^{k-1} &\text{ est } p - 1 \text{ ou multiple de } p \end{aligned}$$

Conclusion : $h(A) = 2^\alpha 3^\beta$ où $\alpha \in \{0, 1, 2\}$ et $\beta \in \{0, 1\}$, de sorte que

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

Il s'agit de la liste des valeurs possibles de $h(A)$. On a vu, en I, que 12 n'était jamais atteinte. Ici $N_2 = 12$ convient.

• Si $n = 3$, on résout $p^k - p^{k-1} \leq 3$.

$$\begin{aligned} \text{Si } p = 2, \quad 2^k - 2^{k-1} &= \begin{cases} 1 & \text{si } k = 1 \\ 2 & \text{si } k = 2 \\ 3 & \text{impossible car multiple de 2} \end{cases} \\ \text{Si } p = 3, \quad 3^k - 3^{k-1} &= \begin{cases} 1 & \text{impossible car multiple de 2} \\ 2 & \text{si } k = 1 \\ 3 & \text{impossible car multiple de 2} \end{cases} \\ \text{Si } p > 3, \quad p^k - p^{k-1} &\text{ est } p - 1 \text{ ou multiple de } p \end{aligned}$$

Conclusion : On trouve la même liste que dans le cas $n = 2$, soit

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

et bien sûr $N_3 = N_2 = 12$.

• Si $n = 4$, on résout $p^k - p^{k-1} \leq 4$.

$$\begin{aligned} \text{Si } p = 2, \quad 2^k - 2^{k-1} &= \begin{cases} 1 & \text{si } k = 1 \\ 2 & \text{si } k = 2 \\ 3 & \text{impossible car multiple de 2} \\ 4 & \text{si } k = 3 \end{cases} \\ \text{Si } p = 3, \quad 3^k - 3^{k-1} &= \begin{cases} 1 & \text{impossible} \\ 2 & \text{si } k = 1 \\ 3 & \text{impossible car multiple de 2} \\ 4 & \text{impossible car multiple de 3} \end{cases} \\ \text{Si } p = 5, \quad 5^k - 5^{k-1} &= \begin{cases} 1 & \text{impossible car multiple de 4} \\ 2 & \text{impossible car multiple de 4} \\ 3 & \text{impossible car multiple de 4} \\ 4 & \text{si } k = 1 \end{cases} \\ \text{Si } p \geq 7, \quad p^k - p^{k-1} &\text{ est } p - 1 \text{ ou multiple de } p \end{aligned}$$

Conclusion : $h(A) = 2^\alpha 3^\beta 5^\gamma$ où $\alpha \in \{0, 1, 2, 3\}$, $\beta \in \{0, 1\}$, $\gamma \in \{0, 1\}$. On trouve les diviseurs de 120

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

et $N_4 = 120$.

***** **Partie V** *****

V.A.1 Toute isométrie f de $I(V_3)$ conserve l'ensemble des sommets de V_3 , donc laisse invariant l'isobarycentre O de ces sommets (En effet, une application affine conserve les barycentres, donc f transformera l'isobarycentre O des sommets en $f(O)$ isobarycentre de ces mêmes sommets, soit $f(O) = O$). Le groupe $I^+(V_3)$ est donc formé de rotations d'axes passant par O , et $I^-(V_3)$ est formé de réflexions par rapport à des plans contenant O . La réflexion s par rapport au plan (OAB) laisse V_3 invariant, donc $I^-(V_3) \neq \emptyset$ et l'on peut affirmer que $I^-(V_3) = sI^+(V_3)$. On vérifie en effet que l'application

$$\begin{aligned} \Psi : I^+(V_3) &\rightarrow I^-(V_3) \\ r &\mapsto s \circ r \end{aligned}$$

est une bijection. Ainsi

$$\#I^-(V_3) = \#I^+(V_3) = \frac{\#I(V_3)}{2}.$$

Toute isométrie f de $I(V_3)$ transforme la face ABC en l'une des 8 faces $SS'S''$ de l'octaèdre. L'application

$$\begin{aligned} \Phi : I(V_3) &\rightarrow \mathcal{F} = \text{ensemble des faces de } V_3 \\ f &\mapsto \text{face } f(A)f(B)f(C) \end{aligned}$$

est surjective et

$$\forall SS'S'' \in \mathcal{F} \quad \#\Phi^{-1}(SS'S'') = 3! = 6.$$

En effet, $\Phi(f) = SS'S''$ équivaut à $\{f(A), f(B), f(C)\} = \{S, S', S''\}$, et cette égalité se réalise de $3! = 6$ façons possibles correspondant aux listes $(f(A), f(B), f(C))$ dont les éléments sont distincts et dans $\{S, S', S''\}$. Pour chaque liste (S, S', S'') fixée, il existe une et une seule isométrie f telle que

$$(f(O), f(A), f(B), f(C)) = (O, S, S', S'')$$

(car (O, A, B, C) est un repère affine de l'espace, voir [1], Théorème 206).

De plus cette isométrie f conserve V_3 car les sommets de V_3 sont toujours placés aux mêmes distances des sommets de l'une quelconque de ses faces ou de O (symétrie de l'octaèdre) et car un point M de l'espace est parfaitement déterminé par ses distances à chacun des points d'un repère affine (ici, il s'agira de (O, A, B, C) et de (O, S, S', S'') ; pour bien comprendre ce passage, on pourra lire la Remarque Ξ).

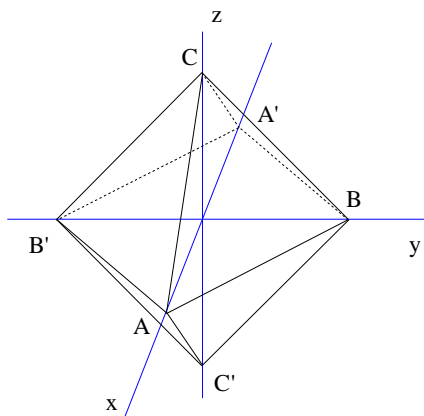
En conclusion, le principe du berger donne

$$\#I(V_3) = 6 \times \#\mathcal{F} = 6 \times 8 = 48.$$

Deuxième solution : Comme les isométries f de $I(V_3)$ laissent toutes O invariant, il existe un isomorphisme de groupe entre $I(V_3)$ et les matrices carrées orthogonales de taille 3 transformant les vecteurs de bases $\vec{i}, \vec{j}, \vec{k}$ en des vecteurs de l'ensemble $\{\pm \vec{i}, \pm \vec{j}, \pm \vec{k}\}$. Ces matrices sont faciles à dénombrer : elles sont de la forme

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & 0 & \pm 1 \\ 0 & \pm 1 & 0 \end{pmatrix}$$

où les coefficients sont tous des 0 ou des ± 1 , où l'on ne trouve jamais deux ± 1 sur une même ligne ou une même colonne, et où aucune ligne ou colonne n'est nulle. Il y a $3!$ façons de choisir les places des ± 1 , puis une fois ces places choisies, 2^3 façons de placer les signes $+1$ ou -1 . En tout, il y aura donc $3! \times 2^3 = 48$ matrices possibles, et $\#I(V_3) = 48$.



Remarque Ξ : Revenons ici sur le passage délicat rencontré à la fin de la première solution. Il s'agissait de comprendre qu'une isométrie f telle que

$$(f(O), f(A), f(B), f(C)) = (O, S, S', S'')$$

conserve nécessairement les sommets de V_3 . Si X désigne un sommet quelconque de l'octaèdre, on sait (en utilisant les symétries de l'octaèdre, et en remarquant que toutes les faces de l'octaèdre jouent le même rôle) qu'il existe un sommet Y tel que

$$OX = OY, \quad AX = SY, \quad BX = S'Y, \quad CX = S''Y.$$

Puisque f conserve les distances,

$$OX = Of(X), \quad AX = Sf(X), \quad BX = S'f(X), \quad CX = S''f(X),$$

et l'on déduit

$$OY = Of(X), \quad SY = Sf(X), \quad S'Y = S'f(X), \quad S''Y = S''f(X).$$

Puisqu'un point de l'espace est parfaitement repéré par les distances entre lui et chacun des quatre points du repère affine (O, S, S', S'') ([1], Théorème 212), on obtient $f(X) = Y$, et l'on a prouvé que l'image $f(X)$ du sommet X était encore égale à un sommet.

V.A.2 On constate que les rotations suivantes laissent V_3 globalement invariant :

- La rotation r_1 d'axe $(CC') = \mathbb{R}\vec{k}$ et d'angle $\pi/2$,
- La rotation r_2 d'axe $\mathbb{R}(1, 1, 1)$ et d'angle $2\pi/3$,
- La rotation r_3 d'axe $(BB') = \mathbb{R}\vec{j}$ et d'angle π .

où les axes sont orientés par les vecteurs directeurs exhibés. Clairement r_1 est d'ordre 4, r_2 est d'ordre 3 et r_3 est d'ordre 2. On vérifie ensuite que l'ensemble

$$H = \left\{ r_1^\alpha r_2^\beta / \alpha \in \{0, 1, 2, 3\} \text{ et } \beta \in \{0, 1, 2\} \right\}$$

est de cardinal $4 \times 3 = 12$. En effet, si $r_1^\alpha r_2^\beta = r_1^{\alpha'} r_2^{\beta'}$ pour certains exposants $\alpha, \alpha' \in \{0, 1, 2, 3\}$ et $\beta, \beta' \in \{0, 1, 2\}$, alors $r_1^{\alpha-\alpha'} = r_2^{\beta'-\beta}$ avec $|\alpha - \alpha'| \leq 3$ et $|\beta' - \beta| \leq 2$. Comme les axes des rotations $r_1^{\alpha-\alpha'}$ et $r_2^{\beta'-\beta}$ sont différents (dès que ces rotations sont distinctes de l'identité), on aura nécessairement $\alpha - \alpha' = 0$ et $\beta' - \beta = 0$ (voici autre façon de le voir : d'après le Théorème de Lagrange, l'ordre de $r_1^{\alpha-\alpha'} = r_2^{\beta'-\beta}$ est un diviseur des ordres 4 et 3 respectifs des sous-groupes engendrés par r_1 et r_2 , c'est donc 1 et $r_1^{\alpha-\alpha'} = r_2^{\beta'-\beta} = Id \dots$).

On constate enfin que $r_3 \notin H$ en cherchant toutes les images possibles du triangle ABC . En effet, si l'on avait $r_3 = r_1^\alpha r_2^\beta$, on aurait

$$C' = r_3(C) = r_1^\alpha r_2^\beta(C) \in r_1^\alpha(\{A, B, C\}) \subset \{A, A', B, B', C\},$$

ce qui est absurde. Pour conclure, on note que le sous-groupe T engendré par r_1, r_2, r_3 contient l'ensemble $H' = H \cup \{r_3\}$ de cardinal 13. Comme l'ordre de T est un diviseur de 24, et comme les diviseurs de 24 sont 1, 2, 3, 4, 6, 8, 12, 24, l'ordre de T sera 24 et $T = I^+(V_3)$.

Remarques : 1) Pour vérifier que r_2 conserve V_3 , le plus simple est d'écrire l'expression analytique de r_2 . Cette expression s'obtient facilement puisque $A \xrightarrow{r_2} B \xrightarrow{r_2} C \xrightarrow{r_2} A$. On obtient :

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

et il est alors très simple de vérifier que r_2 transforme un sommet en un sommet en utilisant les coordonnées.

2) On constate que $r_1 r_3 \neq r_3 r_1$ en calculant

$$\begin{aligned} ABC &\xrightarrow{r_3} A'BC' \xrightarrow{r_1} B'A'C' \\ ABC &\xrightarrow{r_1} BA'C \xrightarrow{r_3} BAC', \end{aligned}$$

et cela prouve que le groupe $I^+(V_3)$ n'est pas commutatif.

V.A.3.a Notons $GL(3, \mathbb{R})$ le groupe des matrices carrées inversibles d'ordre 3 à coefficients réels. Notons $I_O(\mathbb{R}^3)$ le groupe des isométries de \mathbb{R}^3 qui laissent le point O fixe. L'application

$$L : I_O(\mathbb{R}^3) \rightarrow GL(3, \mathbb{R})$$

qui à une isométrie f de $I_O(\mathbb{R}^3)$ associe la matrice de la partie linéaire de f dans la base $(\vec{i}, \vec{j}, \vec{k})$, est clairement un monomorphisme de groupes, et $G(V_3) = L(I(V_3))$ est un sous-groupe d'ordre 48 de $GL(3, \mathbb{R})$ comme l'image du groupe $I(V_3)$ par un morphisme de groupes injectif. Les matrices de $G(V_3)$ sont toutes cycliques (puisque d'ordre fini, un diviseur de 48). Les matrices de $G(V_3)$ sont exhibées dans la deuxième solution de la question A.1, et l'on constate qu'elles sont toutes à coefficients entiers.

V.A.3.b Notons M_i la matrice de r_i dans la base canonique. On trouve

$$M_1 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \quad M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \quad M_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

La matrice de la réflexion de base le plan Oxy est

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

Puisque $G(V_3) = L(I(V_3))$ et puisque r_1, r_2, r_3 et s engendrent $I(V_3)$, on déduit que les matrices M_1, M_2, M_3 et S engendrent $G(V_3)$.

Remarque : Puisque les matrices M_i et S sont à coefficients entiers et engendrent $G(V_3)$, toutes les matrices de $G(V_3)$ seront à coefficients entiers, et l'on redémontre ce résultat sans passer, comme dans la questions précédente, par l'énumération effective des 48 matrices de $G(V_3)$.

V.A.3.c M_2 est d'ordre 3, donc son opposée $-M_2$ sera d'ordre 6. On notera que $-M_2$ est la matrice d'un antidéplacement qui possède O comme point invariant mais qui n'est pas une réflexion (elle n'est pas d'ordre 2). Il s'agit donc de la composée de trois réflexions par rapport à des plans qui contiennent O .

V.A.3.d • A priori, l'ordre d'un élément est un diviseur de l'ordre $48 = 2^4 \times 3$ du groupe. Il n'y a pas d'élément d'ordre 48 car le groupe n'est pas commutatif. Les ordres possibles sont donc :

$$\underline{1}; \underline{2}; \underline{2^2}; 2^3; 2^4; \underline{3}; \underline{2.3}; 2^2.3; 2^3.3.$$

On a déjà trouvé des éléments d'ordre 1, 2, 3, 4, 6 (soulignés ci-dessus).

- S'il existait une rotation r de $I(V_3)$ d'ordre 8, 12, 16 ou 24, cette rotation serait d'axe une droite D et il existerait 8, 12, 16 ou 24 sommets distincts de l'octaèdre situés dans un même plan perpendiculaire à D . C'est impossible.

Le raisonnement précédent montre en fait qu'il n'existe pas de rotation de $I(V_3)$ d'ordre > 4 , et l'on va utiliser cette information pour déterminer les ordres possibles des antidéplacements de $I(V_3)$.

- Un antidéplacement f de $I(V_3)$ qui n'est pas d'ordre 2 est la composée $r_D \circ s_\Pi$ d'une rotation r_D d'axe D et d'une réflexion par rapport à un plan Π de direction $\vec{\Pi} = \vec{D}^\perp$. Le cours montre que cette écriture canonique de f est commutative ([1], Théorème 111 et 222), de sorte que $f^2 = (r_D \circ s_\Pi)^2 = r_D^2$ soit une rotation de $I(V_3)$. On vient de voir que l'ordre de r_D^2 est nécessairement ≤ 4 , et l'on peut donc affirmer que l'ordre de f est ≤ 8 (en effet, si ω désigne l'ordre de r_D^2 , alors $\omega \leq 4$ et $f^{2\omega} = (r_D^2)^\omega = Id$ nous assure que l'ordre de f est ≤ 8).

- Nous allons montrer maintenant qu'il n'existe aucun antidéplacement f de $I(V_3)$ d'ordre 8. Supposons, par l'absurde, que $f = r_D \circ s_\Pi$ soit un antidéplacement de $I(V_3)$ d'ordre 8. Dans ce cas

$$Id = f^8 = (r_D \circ s_\Pi)^8 = r_D^8 \circ s_\Pi^8 = r_D^8,$$

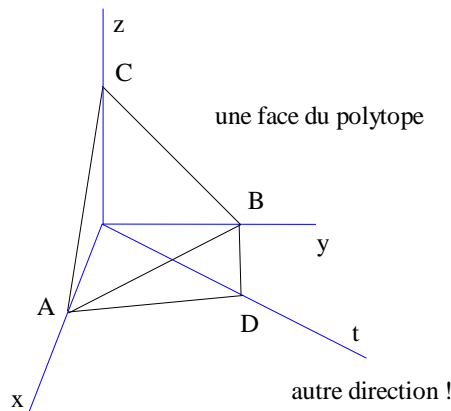
et r_D^2 est une rotation d'ordre 4 de $I(V_3)$. Il existe donc quatre sommets de l'octaèdre situés dans un même plan perpendiculaire à D . Ce plan ne peut être que l'un des trois plans de coordonnées xOy , yOz ou zOx . Par suite (et puisque D et Π contiennent O), l'axe D de r_D ne peut être que l'un des trois axes de coordonnées Ox , Oy ou Oz . Supposons par exemple que $D = Oz = (CC')$ et $\Pi = xOy$. La rotation r_D est alors la rotation d'axe $D = (CC')$ et d'angle $2\pi/8 = \pi/4$. On constate alors que l'image de A par $f = r_D \circ s_\Pi$ n'est pas un sommet du tétraèdre, ce qui est absurde.

En conclusion les seuls ordres possibles sont 1 ; 2 ; 3 ; 4 ; 6.

V.B.1.a

$$\begin{aligned} \Psi : I(V_3) &\rightarrow S(\{A, B, \dots, D'\}) \\ f &\mapsto \begin{pmatrix} A & B & D' \\ f(A) & f(B) & f(D') \end{pmatrix} \end{aligned}$$

est un monomorphisme de groupes de $I(V_3)$ sur le groupe des permutations de $\{A, B, \dots, D'\}$. C'est clairement un morphisme, et il est injectif car il existe une seule isométrie de \mathbb{R}^3 dont les images des points O, A, B, C, D formant un repère affine, sont les points donnés $O, f(A), f(B), f(C), f(D)$.



V.B.1.b Les faces du polytope V_4 sont $ABCD$ (de dimension 3) et les itérés des symétriques de $ABCD$ par rapport à des hyperplans de coordonnées de \mathbb{R}^4 . On trouve (puisque les plans de coordonnées s'écrivent $OB'CD = OB'CD \dots$) :

$ABCD$
 $A'BCD ; AB'CD ; ABC'D ; ABCD'$
 $A'B'CD ; A'BC'D ; A'BCD' ; AB'C'D ; AB'CD' ; ABC'D'$
 $AB'C'D' ; A'BC'D' ; A'B'CD' ; A'B'C'D$
 $A'B'C'D'$.

Il y a donc 16 faces.

Toute isométrie f de $I(V_4)$ transforme la face $ABCD$ en l'une des 16 faces $SS'S''S'''$ du polytope. L'application

$$\begin{aligned} \Phi : I(V_3) &\rightarrow \mathcal{F} = \text{ensemble des faces de } V_4 \\ f &\mapsto \text{face } f(A)f(B)f(C)f(D) \end{aligned}$$

est surjective et

$$\forall SS'S''S''' \in \mathcal{F} \quad \#\Phi^{-1}(SS'S''S''') = 4!.$$

En effet, $\Phi(f) = SS'S''S'''$ équivaut à

$$\{f(A), f(B), f(C), f(D)\} = \{S, S', S'', S'''\}$$

et se réalise de $4! = 24$ façons possibles correspondant aux listes

$$(f(A), f(B), f(C), f(D))$$

dont les éléments sont distincts et dans $\{S, S', S'', S'''\}$. Pour chaque liste (S, S', S'', S''') fixée, il existe une et une seule isométrie f telle que

$$(f(O), f(A), f(B), f(C), f(D)) = (O, S, S', S'', S''')$$

(toujours parce que (O, A, B, C, D) est un repère affine de l'espace).

De plus cette isométrie f conserve V_4 car les sommets de V_4 sont toujours placés aux mêmes distances des sommets de l'une quelconque de ses faces ou de O (symétrie de l'octaèdre) et car un point M de l'espace est parfaitement déterminé par ses distances à chacun des points d'un repère affine (ici, il s'agira de (O, A, B, C, D) et de (O, S, S', S'', S''')). Le principe du berger donne encore

$$\#I(V_4) = 16 \times \#\mathcal{F} = 16 \times 24 = 384.$$

Deuxième solution : Comme les isométries f de $I(V_4)$ laissent toutes O invariant, il y aura isomorphisme de groupe entre $I(V_3)$ et les matrices carrées orthogonales de taille 4 transformant les vecteurs de base $\vec{e}_1, \vec{e}_2, \vec{e}_3, \vec{e}_4$ en des vecteurs de l'ensemble $\{\pm\vec{e}_1, \pm\vec{e}_2, \pm\vec{e}_3, \pm\vec{e}_4\}$. Elles sont de la forme

$$\begin{pmatrix} \pm 1 & 0 & 0 & 0 \\ 0 & \pm 1 & 0 & 0 \\ 0 & 0 & 0 & \pm 1 \\ 0 & 0 & \pm 1 & 0 \end{pmatrix}$$

où les coefficients sont des 0 ou des ± 1 , où l'on ne trouve jamais deux ± 1 sur une même ligne ou une même colonne, et où aucune ligne ou colonne n'est nulle. Il y a $4!$ façons de choisir les places des

± 1 , puis une fois ces places choisies, 2^4 façons de placer les signes $+1$ ou -1 . On dénombre donc $4! \times 2^4 = 384$ matrices possibles, soit $\#I(V_3) = 384$.

V.B.2 et 3 Il suffit de définir f sur les vecteurs de base. La permutation

$$\begin{aligned} \vec{i} &\mapsto \vec{j} \\ \vec{j} &\mapsto \vec{k} \\ \vec{k} &\mapsto \vec{l} \\ \vec{l} &\mapsto \vec{i} \end{aligned}$$

définit une application linéaire d'ordre 4. Pour passer à une application d'ordre 8, l'idée est de perturber ce cycle en remplaçant la première ligne $\vec{i} \mapsto \vec{j}$ par $\vec{i} \mapsto -\vec{j}$ pour obtenir

$$\begin{aligned} \vec{i} &\mapsto -\vec{j} \\ \vec{j} &\mapsto \vec{k} \\ \vec{k} &\mapsto \vec{l} \\ \vec{l} &\mapsto \vec{i} \end{aligned}$$

et la matrice correspondante

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

d'ordre 8.

References

- [1] D.-J. Mercier, Cours de géométrie, préparation au CAPES et à l'agrégation, Publibook, 2004.

THAT'S ALL FOLKS !