Correction Agrèg interne ep1 2022

Rappel : théorème spectral :
Si A est une matrice $n \times n$ symétrique réelle alors il existe une matrice D diagonale et une matrice P orthogonale (i.e. $P^{-1} = P^T$) telles que $A = PDP^{-1} = PDP^T$.

Vrai ou faux

1.

(a) Faux car $\forall M, N \in \mathcal{M}_n(\mathbf{C}), tr(MN) = tr(NM)$
En effet si on note $M = (m_{i,j})$ et $N = (n_{i,j})$

$$tr(MN) = \sum_{i=1}^{n}\sum_{k=1}^{n} m_{i,k}n_{k,i} = \sum_{k=1}^{n}\sum_{i=1}^{n} m_{i,k}n_{k,i} = \sum_{k=1}^{n}\sum_{i=1}^{n} n_{k,i}m_{i,k} = tr(NM)$$

Si $M = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{pmatrix}$ et $N = \begin{pmatrix} & C_1 & C_2 & \cdots & C_n & \end{pmatrix}$ Alors $MN = \begin{pmatrix} \langle L_1, C_1\rangle & & \\ & & \\ & & \langle L_i, C_j\rangle \\ & & \end{pmatrix}$

$\langle L_i, C_j\rangle = m_{i,1}n_{1,j} + m_{i,2}n_{2,j} + ... = \sum_{k=1}^{n} m_{i,k}n_{k,j}$

(b) Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbf{C})$ alors

$$\begin{aligned} \chi_A(X) &= \det\begin{pmatrix} X-a & -b \\ -c & X-d \end{pmatrix} = X^2 - (a+d)X + ad - bc \\ \chi_A(X) &= X^2 - tr(A)X + \det A \end{aligned}$$

Donc VRAI.

(c) Si $A = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$ alors $trA = 0$ et $\det A = 0$ donc $\chi_A(X) = X^2$ donc la seule valeur propre est 0, donc si A est diagonalisable alors A la matrice diagonale associée est la matrice nulle donc il existe $P \in GL_2(\mathbf{C}), A = P0_nP^{-1} = 0_n$ donc c'est FAUX car $A \neq 0_n$.

(d) Si $\varphi : \mathbb{Z} \to \mathbb{R}, n \to n.$ donc FAUX.

Exercice préliminaire

2. Montrons par récurrence sur $d \geq 2$ que $\chi_{C_P}(X) = P(X)$
Si $d = 1, C_P = (-a_0)$ donc $\chi_{C_P}(X) = X + a_0 = P(X)$.
Si $d = 2, C_P = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}$ donc

$$\chi_{C_P}(X) = \begin{vmatrix} X & a_0 \\ -1 & X + a_1 \end{vmatrix} = X^2 + a_1X + a_0 = P(X)$$

Supposons le résultat vrai pour un entier d fixé.

Soit $P = X^{d+1} + \sum_{i=0}^{d} a_i X^i$ alors

$$\begin{aligned}
\chi_{C_P}(X) &= \begin{vmatrix} X & \cdots & \cdots & 0 & a_0 \\ -1 & X & & \vdots & a_1 \\ 0 & -1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & X & a_{d-1} \\ 0 & \cdots & 0 & -1 & X + a_d \end{vmatrix} \\
&= X \begin{vmatrix} X & 0 & 0 & a_1 \\ -1 & \ddots & 0 & \vdots \\ 0 & \ddots & X & a_{d-1} \\ 0 & 0 & -1 & X + a_d \end{vmatrix} + (-1)^{d+2} a_0 \begin{vmatrix} -1 & X & 0 & 0 \\ 0 & -1 & \ddots & 0 \\ \vdots & \ddots & \ddots & X \\ 0 & \cdots & 0 & -1 \end{vmatrix} \\
&= X\left(X^d + a_d X^{d-1} + ... + a_2 X + a_1\right) + (-1)^{d+2} a_0 (-1)^d \\
&= X^{d+1} + a_d X^d + ... + a_2 X^2 + a_1 X + a_0 = P(X)
\end{aligned}$$

Donc le résultat est vrai par récurrence.

3.

(a)

i. Soit $u \in L(\mathbf{C}^p)$, l'application linéaire dont la mtrice par rapport à la base canonique est M.
La famille $\left\{x, Mx, ..., M^{\mu-1}x\right\}$ est libre par définition de μ. On complète cette famille pour obtenir une base $\mathcal{B}$ de $\mathbf{C}^p$.
La famille $\{x, Mx, ..., M^{\mu}x\}$ est liée donc il existe des coefficients $(\alpha_i)_{i\in[[0,\mu-1]]}$ tels que $M^{\mu}x + \alpha_{\mu-1}M^{\mu-1}x + ... + \alpha_1 Mx + \alpha_0 x = 0_{\mathbf{C}^p}$
Dans la base $\mathcal{B}$ la matrice de u s'écrit

$$M' = \begin{array}{c} \begin{matrix} Mx & M^2x & \cdots & \cdots & M^{\mu}x & * \end{matrix} \\ \begin{pmatrix} 0 & 0 & & & -\alpha_0 & * \\ 1 & 0 & & & -\alpha_1 & * \\ 0 & 1 & & & \vdots & \\ \vdots & 0 & \ddots & & \vdots & \\ \vdots & \vdots & \ddots & 1 & -\alpha_{\mu-1} & * \\ \mathcal{O} & \mathcal{O} & \cdots & \mathcal{O} & \mathcal{O} & N \end{pmatrix} \end{array} \begin{matrix} x \\ Mx \\ \vdots \\ \\ M^{\mu-1}x \\ * \end{matrix}$$

ii. Notons $P = X^{\mu} + \alpha_{\mu-1}X^{\mu-1} + ... + \alpha_1 X + \alpha_0$
La matrice précédente est

$$M' = \begin{pmatrix} C_P & * \\ 0_{p-\mu} & N \end{pmatrix}$$

donc $\chi_{M'}(X) = \det \begin{pmatrix} XI_{\mu} - C_P & * \\ 0_{p-\mu} & XI_{p-\mu} - N \end{pmatrix} = \chi_{C_P}(X) \times \chi_N(X) = P(X) \times \chi_N(X)$

Donc $\chi_{M'}(M) = P(M) \times \chi_N(M) = \chi_N(M) \times P(M)$
Par définition de P on a $P(M)x = M^{\mu}x + \alpha_{\mu-1}M^{\mu-1}x + ... + \alpha_1 Mx + \alpha_0 x = 0_{\mathbf{C}^p}$
Donc $\chi_{M'}(M)x = 0_{\mathbf{C}^p}$ mais comme M' est semblable à M, $\chi_M = \chi_{M'}$ donc $\chi_M(M)x = 0_{\mathbf{C}^p}$.

(b) $\forall x \in \mathbf{C}^p, \chi_M(M)x = 0_{\mathbf{C}^p}$ donc $\chi_M(M) = 0_{L(\mathbf{C}^p)}$ donc χ_M est annulateur de M (théorème de Cayley-Hamilton).

Problème

I. Exemple dans $S_p^+(\mathbf{R})$

4. Il faut prendre comme produit scalaire sur $\mathbf{R}^p$ celui défini par $\forall X, Y \in \mathbf{R}^p, \langle X, Y\rangle = {}^tXY$

On a $\forall X, Y \in \mathbf{R}^p, \langle a(X), Y\rangle = {}^t(AX)Y = {}^tX{}^tAY = {}^tXAY$ car A est symétrique et donc $\forall X, Y \in \mathbf{R}^p, \langle a(X), Y\rangle = \langle X, a(Y)\rangle$ donc a est symétrique.

5. Si $\forall Y \in \mathbf{C}^p,\ {}^tYSY \geq 0$ alors $\forall \lambda$: valeur propre de S si on choisit X un vecteur propre associé on a

$$ {}^tXSX = {}^tX(\lambda X) = \lambda\left({}^tXX\right) \geq 0$$

Or, ${}^tXX = \|X\|^2 > 0$ car X est non-nul donc $\lambda \geq 0$. Donc toutes les valeurs propres sont positives et donc $S \in \mathcal{S}_p^+(\mathbf{R})$.

Réciproquement si on suppose que $S \in \mathcal{S}_p^+(\mathbf{R})$ alors S est diagonalisable dans une base orthonormée (théorème spectral), c'est-à-dire qu'il existe P inversible telle que $S = P^{-1}DP$ avec $P^{-1} = {}^tP$.

Donc $\forall Y \in \mathbf{R}^p,\ {}^tYSY = {}^tY{}^tPDPY = {}^t(PY)D(PY)$ Notons $\delta_1, ..., \delta_n$ les valeurs propres (positives) de S et notons $PY = (p_1, ..., p_n)$ alors

$$ {}^tYSY = \delta_1 p_1^2 + \delta_2 p_2^2 + ... + \delta_n p_n^2 \geq 0$$

car $\begin{pmatrix} \delta_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \delta_n \end{pmatrix}\begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} \delta_1 p_1 \\ \vdots \\ \delta_n p_n \end{pmatrix}$

6. $\forall Y \in \mathbf{R}^p,\ {}^tYSY \geq 0$ et ${}^tYTY \geq 0$ donc ${}^tYSY + {}^tYTY \geq 0$ donc ${}^tY(S+T)Y \geq 0$

Comme $S+T$ est symétrique, d'après la question précédente $S+T \in \mathcal{S}_p^+(\mathbf{R})$.

7. On peut écrire $S = P^{-1}DP$ avec $D = \begin{pmatrix} \delta_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \delta_n \end{pmatrix}$ avec $\forall i \in [[1,n]], \delta_i \geq 0$.

Soit $\alpha_i = \sqrt[n]{\delta_i}$ alors si on note $A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \alpha_n \end{pmatrix}$ on a $A^n = D$.

Donc $\left(P^{-1}AP\right)^n = P^{-1}A^nP = P^{-1}DP = S$ donc on peut choisir $R = P^{-1}AP$.

8.

(a) **Rappel** : si f et $g \in L(E)$ commutent alors $\ker f$ est stable par g
(du coup $f - \alpha id$ et g commutent également et donc les sous-espaces propres de f sont stables par g).
Preuve : Soit $x \in \ker f$, alors $f(g(x)) = g(f(x)) = g(0_E) = 0_E$ donc $g(x) \in \ker f$.
Ici on a $U \times S = U \times U^n = U^{n+1} = U^n \times U = S \times U$. Donc s et u commutent donc tout sous-espace propre de s : $E_{\lambda_i}(s) = \ker(s - \lambda_i id)$ est stable par u.
D'autre par $\forall x, y \in \mathbf{R}^p, \langle u(x), y\rangle = \langle x, u(y)\rangle$ donc en particulier $\forall x, y \in E_{\lambda_i}(s), \langle u(x), y\rangle = \langle x, u(y)\rangle$ donc la restriction de u à $E_{\lambda_i}(s)$ induit $u_i : E_{\lambda_i}(s) \to E_{\lambda_i}(s), x \to u(x)$.

(b) Soit α une valeur propre de u_i donc il existe $x \in E_{\lambda_i}(s)$ non nul tel que $u_i(x) = \alpha x$ mais alors $u_i^n(x) = u^n(x) = \alpha^n x = s(x)$
Or, $s(x) = \lambda_i x$ car $x \in E_{\lambda_i}(s) = \ker(s - \lambda_i id)$. Finalement, $\alpha^n x = \lambda_i x$ donc $\alpha^n = \lambda_i$. Or $U, S \in \mathcal{S}_p^+(\mathbf{R})$ donc $\alpha \geq 0$ et $\lambda_i \geq 0$ donc $\alpha = \sqrt[n]{\lambda_i}$.

(c) La matrice de u_i est réelle est symétrique donc u_i est diagonalisable et sa seule valeur propre c'est $\sqrt[n]{\lambda_i}$ donc $u_i = \sqrt[n]{\lambda_i} id$
Comme s est diagonalisable on a $\mathbf{R}^p = E_{\lambda_1}(s) \oplus E_{\lambda_2}(s) \oplus ... \oplus E_{\lambda_q}(s)$
Donc $\forall x \in \mathbf{R}^p$, il existe des $x_i \in E_{\lambda_i}(s)$ uniques tels que $x = \sum_{i=1}^q x_i$
Et $u(x) = \sum_{i=1}^q u(x_i) = \sum_{i=1}^q u_i(x_i) = \sum_{i=1}^q \sqrt[n]{\lambda_i} x_i$
Donc u est déterminé de façon unique.

9. Relire les deux questions précédentes...

10. $\forall U, V \in \mathcal{S}_p^+(\mathbf{R}), \left(\sqrt[n]{U}\right)^n + \left(\sqrt[n]{V}\right)^n = U + V = \left(\sqrt[n]{U+V}\right)^n$

Donc ψ est bien définie.

Si $\psi(U,V) = \psi(U',V')$ alors $\sqrt[n]{U} = \sqrt[n]{U'}$ donc $\left(\sqrt[n]{U}\right)^n = U = \left(\sqrt[n]{U'}\right)^n = U'$ donc $U = U'$ et de même $V = V'$ donc ψ est injective.

Soit $(X,Y,Z) \in \left(\mathcal{S}_p^+(\mathbf{R})\right)^3$ tels que $X^n+Y^n=Z^n$ alors Soit $U=X^n$ et $V=Y^n$ on a bien $\psi(U,V)=\left(X,Y,\sqrt[n]{X^n+Y^n}\right)$ car la racine n^e de X^n est X et on a $\sqrt[n]{X^n+Y^n}=\sqrt[n]{Z^n}=Z$ par unicité de la racine n^e. Donc ψ est surjective.

Finalement, ψ est une bijection.

PARTIE II

11. $\forall M \in \mathcal{M}_2(\mathbf{Z}), M^2=(trM)\times M-(\det M)\,I_2$ d'après Cayley-Hamilton.

Donc $\forall M \in SL_2(\mathbf{Z}), M^2=(trM)\times M-I_2$

Et donc

$$tr\left(M^2\right)=(trM)^2-2.$$

$\forall M \in SL_2(\mathbf{Z}), M^2 \in SL_2(\mathbf{Z})$ donc en appliquant la formule précédente à M^2 on obtient

$$\begin{aligned} tr\left(M^4\right) &= \left(tr\left(M^2\right)\right)^2-2 \\ &= \left((trM)^2-2\right)^2-2 \\ &= (trM)^4+4-4(trM)^2-2 \\ tr\left(M^4\right) &= (trM)^4-4(trM)^2+2 \end{aligned}$$

12. $0^2\equiv 0\,[8]\,;1^2\equiv 1\,[8]\,;2^2\equiv 4\,[8]\,;3^2\equiv 1\,[8]\,;4^2\equiv 0\,[8]\,;5^2\equiv 1\,[8]\,;6^2\equiv 4\,[8]\,;7^2\equiv 1\,[8]$

Si $(trM)^2\equiv 0\,[8]$ alors $(trM)^4\equiv 0\,[8]$ et $tr\left(M^4\right)\equiv 2\,[8]$

Si $(trM)^2\equiv 1\,[8]$ alors $(trM)^4\equiv 1\,[8]$ et $tr\left(M^4\right)\equiv 1-4+2\,[8]\equiv -1\,[8]$

Si $(trM)^2\equiv 4\,[8]$ alors $(trM)^4\equiv 0\,[8]$ et $tr\left(M^4\right)\equiv -4\times 4+2\,[8]\equiv 2\,[8]$

Dans tous les cas, on a bien $tr\left(M^4\right)\equiv 2\,[8]$ ou $tr\left(M^4\right)\equiv -1\,[8]$

13. Si $X^4+Y^4=Z^4$ alors $tr\left(X^4\right)+tr\left(Y^4\right)=tr\left(Z^4\right)$

Mais $tr\left(X^4\right)+tr\left(Y^4\right)\equiv \left\{\begin{array}{c} 4\,[8] \\ 1\,[8] \\ -2\,[8] \end{array}\right.$ et $tr\left(Z^4\right)\equiv \left\{\begin{array}{c} 2\,[8] \\ -1\,[8] \end{array}\right.$ donc $tr\left(Z^4\right)\neq tr\left(X^4\right)+tr\left(Y^4\right)$ et donc il n'y a pas de solutions à $X^4+Y^4=Z^4$ dans $SL_2(\mathbf{Z})$.

14. Si 4 divise n alors $n=4p$ avec $p\in\mathbb{Z}$ donc l'équation est $X^{4p}+Y^{4p}=Z^{4p}$ qui peut s'écrire $(X^p)^4+(Y^p)^4=(Z^p)^4$: impossible d'après la question précédente car $X^p,Y^p,Z^p\in SL_2(\mathbf{Z})$.

PARTIE III

RAPPELS : $\mathbf{K}=\mathbf{Q}(\delta)=\{a+b\delta | a,b\in\mathbf{Q}\}$ avec $\delta^2\in\mathbf{Q}$ et $\varphi(a+b\delta)=\overline{a+b\delta}=a-b\delta$.

15. $\mathbf{K}\subset\mathbf{C}$: $\mathbf{Q}-$ espace vectoriel.

Méthode 1 (classique) :

Si $x=a+b\delta\in\mathbf{K}$ et $y=a'+b'\delta\in\mathbf{K}$ alors

$$\forall\alpha\in\mathbf{Q}, x+\alpha y=(a+\alpha a')+(b+\alpha b')\,\delta\in\mathbf{K}$$

Méthode 2 (sioux) :

$\mathbf{K}=vect(1,\delta)$ donc c'est un sous $\mathbf{Q}-$espace vectoriel de $\mathbf{C}$.

Comme $\delta\notin\mathbf{Q}$, la famille $(1,\delta)$ est libre sur $\mathbf{Q}$ donc $\mathbf{K}$ est de dimension 2.

16. $(\mathbf{K},+)$ est un groupe commutatif d'après la question précédente.

Comme $\mathbf{K}\subset\mathbf{C}$ la multiplication est associative et distributive par rapport à l'addition. $1=1+0\times\delta\in\mathbf{K}$ est un élément neutre pour la multiplication. De plus $\forall x=a+b\delta\in\mathbf{K}$ et $y=a'+b'\delta\in\mathbf{K}$ on a

$$\begin{aligned} xy &= aa'+(ab'+a'b)\,\delta+bb'\delta^2 \\ &= \left(aa'+bb'\delta^2\right)+(ab'+a'b)\,\delta\in\mathbf{K} \end{aligned}$$

car $\delta^2 \in \mathbf{Q}$.

Donc $\mathbf{K}$ est un sous-anneau de $\mathbf{C}$.

Soit $x = a + b\delta \in \mathbf{K}$, si $x \neq 0$, comme $a - b\delta \neq 0$ car $\delta \notin \mathbf{Q}$, on a

$$\begin{aligned} \frac{1}{x} &= \frac{1}{a+b\delta} = \frac{a-b\delta}{(a+b\delta)(a-b\delta)} = \frac{a-b\delta}{a^2-b^2\delta^2} \\ &= \frac{a}{a^2-b^2\delta^2} - \frac{b}{a^2-b^2\delta^2}\delta \in \mathbf{K} \end{aligned}$$

Donc l'inverse de x est dans $\mathbf{K}$ et donc $\mathbf{K}$ est un corps.

17. Un morphisme de corps c'est juste un morphisme d'anneaux où les anneaux de départ et d'arrivée sont des corps.
Donc, il faut montrer que

$$\begin{aligned} \forall x, x' &\in \mathbf{K}, \varphi(x+x') = \varphi(x) + \varphi(x') \\ \forall x, x' &\in \mathbf{K}, \varphi(xx') = \varphi(x)\varphi(x') \\ \varphi(1_{\mathbf{K}}) &= 1_{\mathbf{K}} \end{aligned}$$

$\forall x = a + b\delta \in \mathbf{K}$ et $x' = a' + b'\delta \in \mathbf{K}$,

$$\begin{aligned} \varphi(x+x') &= \varphi(a+a'+(b+b')\delta) = a + a' - (b+b')\delta \\ &= a - b\delta + a' - b'\delta = \varphi(x) + \varphi(x') \\ \varphi(xx') &= \varphi\left(aa' + bb'\delta^2 + (ab'+a'b)\delta\right) = aa' + bb'\delta^2 - (ab'+a'b)\delta \\ &= (a-b\delta)(a'-b'\delta) = \varphi(x)\varphi(x') \end{aligned}$$

De plus, $\varphi(1) = 1$.

Donc φ est un morphisme de corps.

On a $\forall x \in \mathbf{K}, \varphi(\varphi(x)) = x$ donc φ est bijective.

18.

(a) Si $\psi(x) = \psi(y)$ alors

$$\frac{x+\delta}{x-\delta} = \frac{y+\delta}{y-\delta}$$

donc

$$xy + \delta(y-x) - \delta^2 = xy + \delta(x-y) - \delta^2$$

donc

$$\delta(y-x) = \delta(x-y)$$

donc $y - x = x - y$ (car $\delta \neq 0$) donc $x = y$. Donc ψ est injective.

(b) $\forall a, b \in \mathbf{Z}$ avec $b \neq 0$, on a

$$\psi\left(\frac{a}{b}\right) = \frac{\frac{a}{b} + \delta}{\frac{a}{b} - \delta} = \frac{a+b\delta}{a-b\delta} = \frac{\theta}{\overline{\theta}}$$

avec $\theta = a + b\delta \in \mathbf{K}\backslash\{0\}$

Donc $\psi(\mathbf{Q}) \subset \left\{\frac{\theta}{\overline{\theta}}, \theta \in \mathbf{K}\backslash\{0\}\right\}$

Comme ψ est injective $card(\psi(\mathbf{Q})) = card(\mathbf{Q}) = +\infty$

Donc $\left\{\frac{\theta}{\overline{\theta}}, \theta \in \mathbf{K}\backslash\{0\}\right\}$ est infini.

PARTIE IV

19. $\forall i, j \in \{1, ..., n\}$,

$$\overline{\sum_{k=1}^{n} a_{i,k}b_{k,j}} = \sum_{k=1}^{n} \overline{a_{i,k}b_{k,j}} = \sum_{k=1}^{n} \overline{a_{i,k}}\,\overline{b_{k,j}}$$

car φ est un morphisme de corps. Donc $\overline{AB} = \overline{A}\,\overline{B}$.

20. Si $F \in GL_p(\mathbf{K})$ alors $\exists G \in GL_p(\mathbf{K})$ tel que $FG = I_p$

Mais alors $\overline{FG} = \overline{I_p} = I_p = \overline{FG}$ donc $\overline{F} \in GL_p(\mathbf{K})$ et $\left(\overline{F}\right)^{-1} = \overline{G} = \overline{F^{-1}}$.

Si $\overline{F} \in GL_p(\mathbf{K})$ alors $\overline{\left(\overline{F}\right)} = F \in GL_p(\mathbf{K})$.

Finalement $F \in GL_p(\mathbf{K})$ ssi $\overline{F} \in GL_p(\mathbf{K})$ et $\left(\overline{F}\right)^{-1} = \overline{F^{-1}}$.

21.

(a) Si $X = F\left(\overline{F}\right)^{-1}$ alors

$$X\overline{X} = F\left(\overline{F}\right)^{-1} \times \overline{F}(F)^{-1} = I_p$$

(b)

i. Si $\bar{\theta} \neq 0$ et si $F(\theta)$ n'est pas inversible alors $X + \dfrac{\theta}{\overline{\theta}} I_p$ n'est pas inversible donc $-\dfrac{\theta}{\overline{\theta}}$ est une racine du polynôme caractéristique de X. Ce polynôme complexe est de degré p donc il admet au plus p racines. Or l'ensemble $\left\{ \dfrac{\theta}{\overline{\theta}}, \theta \in \mathbf{K} \backslash \{0\} \right\}$ est infini donc il existe θ_0 tel que $\dfrac{\theta_0}{\overline{\theta_0}}$ n'est pas racine de ce polynôme donc tel que $\overline{\theta_0} X + \theta_0 I_p$ est inversible.
Attention : Si $\mathbb{A}$ est un anneau commutatif et si $P \in \mathbb{A}[X]$ est de degré p alors P peut avoir plus de p racines !!!!!
Exemple : $X^3 - X$ dans $\mathbb{Z}/6\mathbb{Z}$, tous les éléments de A sont des racines !!!
Si $P, Q \in \mathbb{A}[X]$ et si Q est unitaire alors $\exists D$ et $R \in \mathbb{A}[X]$ tels que $P = DQ + R$ avec $\deg R < \deg Q$.

ii. $X \times \overline{F(\theta_0)} = X \times \left(\overline{\theta_0} I_p + \theta_0 \overline{X}\right) = \overline{\theta_0} X + \theta_0 X\overline{X} = \overline{\theta_0} X + \theta_0 I_p = F(\theta_0)$ donc comme $\overline{F(\theta_0)}$ est inversible on a

$$X = F(\theta_0) \times \left(\overline{F(\theta_0)}\right)^{-1}$$

(c) Supposons qu'il existe $F \in GL_p(\mathbf{K})$ telle que $F^{-1}AF$ et $F^{-1}BF$ appartiennent à $\mathcal{M}_p(\mathbf{Q})$.
Donc $\overline{F^{-1}AF} = F^{-1}AF = \overline{F^{-1}}\overline{AF} = \left(\overline{F}\right)^{-1}\overline{AF}$ et

$$\overline{F}F^{-1}AF\left(\overline{F}\right)^{-1} = \overline{A}$$

donc si on pose $X = F\left(\overline{F}\right)^{-1}$ on a bien $X^{-1} = \overline{F}F^{-1}$ et donc

$$X^{-1}AX = \overline{A}$$

De même, $X^{-1}BX = \overline{B}$.
Et d'après la question **21.a.** $X\overline{X} = I_p$
Réciproquement, supposons $\exists X \in GL_p(\mathbf{K}), \begin{cases} X^{-1}AX = \overline{A} \\ X^{-1}BX = \overline{B} \\ X\overline{X} = I_p \end{cases}$
D'après la question **21.b.ii.** $\exists F \in GL_p(\mathbf{K}), X = F\left(\overline{F}\right)^{-1}$
Et donc

$$\begin{aligned} X^{-1}AX &= \overline{A} \Leftrightarrow \overline{F}F^{-1}AF\left(\overline{F}\right)^{-1} = \overline{A} \\ &\Leftrightarrow F^{-1}AF = \left(\overline{F}\right)^{-1}\overline{AF} = \overline{F^{-1}AF} \end{aligned}$$

donc $F^{-1}AF \in \mathcal{M}_p(\mathbf{Q})$ et de même pour B.

22.

(a) Notons $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$

$$\begin{aligned} X\overline{A} &= AX \Leftrightarrow \begin{pmatrix} x & y \\ z & t \end{pmatrix}\begin{pmatrix} \overline{\lambda} & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} x\overline{\lambda} & y\lambda \\ z\overline{\lambda} & t\lambda \end{pmatrix} = \begin{pmatrix} x\lambda & y\lambda \\ z\overline{\lambda} & t\overline{\lambda} \end{pmatrix} \\ &\Leftrightarrow x = 0 \text{ et } t = 0 \end{aligned}$$

Donc $X = \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}$ et $X\overline{X} = \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}\begin{pmatrix} 0 & \overline{y} \\ \overline{z} & 0 \end{pmatrix} = \begin{pmatrix} y\overline{z} & 0 \\ 0 & \overline{y}z \end{pmatrix} = I_2$

Donc $y \neq 0$ et $z = \dfrac{1}{\overline{y}}$ et finalement $X = \begin{pmatrix} 0 & y \\ \dfrac{1}{\overline{y}} & 0 \end{pmatrix}$

Réciproquement, si il existe $u \in \mathbf{K}\backslash\{0\}$ tel que $X = \begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix}$

Alors $X\overline{X} = I_2$ et

$$\begin{aligned} AX &= \begin{pmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{pmatrix}\begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \lambda u \\ \dfrac{\overline{\lambda}}{\overline{u}} & 0 \end{pmatrix} \\ X\overline{A} &= \begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix}\begin{pmatrix} \overline{\lambda} & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 0 & \lambda u \\ \dfrac{\overline{\lambda}}{\overline{u}} & 0 \end{pmatrix} \end{aligned}$$

donc $X^{-1}AX = \overline{A}$.

(b) $\det A = \det\left(F^{-1}AF\right) = 1 = \det B$.

D'après la question **21.c.** $\exists X \in GL_2(\mathbf{K})$ telle que $\begin{cases} X^{-1}AX = \overline{A} \\ X^{-1}BX = \overline{B} \\ X\overline{X} = I_2 \end{cases}$

Et donc d'après **22.a.** On a $X = \begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix}$

Et $BX = X\overline{B}$ donne

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & u \\ \dfrac{1}{\overline{u}} & 0 \end{pmatrix}\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

ce qui implique $\dfrac{d}{\overline{u}} = \dfrac{\overline{a}}{\overline{u}}$ donc $d = \overline{a}$, et $\dfrac{b}{\overline{u}} = u\overline{c}$

$\det B = \begin{vmatrix} a & b \\ c & \overline{a} \end{vmatrix} = a\overline{a} - bc = 1$ et $bc = u\overline{c}\overline{u}c = x\overline{x}$ avec $x = u\overline{c}$.

On a donc bien $a\overline{a} - 1 = x\overline{x}$ donc $N(a) - 1 = N(x)$.

PARTIE V

23. $\det B_1 = ad - bc = 1$

$\det(A_1 + B_1) = (\alpha + \delta + a)(\alpha - \delta + d) - bc = 1$

Donc $(\alpha + \delta)d + (\alpha - \delta)a + \alpha^2 - \delta^2 = 0$ donc $\alpha(d + a) + \delta(d - a) + 1 = 0$

Et finalement, $\delta(a - d) = 2\alpha m_1 + 1$ et

$$a - d = \frac{2\alpha m_1 + 1}{\delta}$$

24.

(a) On a $\chi_A(X) = X^2 - TrAX + \det A = X^2 - 2\alpha X + 1$

$\Delta = 4\alpha^2 - 4 = 4\delta^2$ donc les racines de χ_A sont $\alpha + \delta \in \mathbf{K}$ et $\alpha - \delta \in \mathbf{K}$.

Comme $\delta \notin \mathbf{Q}$ on a $\delta \neq 0$ et donc la matrice $A \in \mathcal{M}_2(\mathbf{K})$ possède deux valeurs propres distinctes dans $\mathbf{K}$ et donc elle est diagonalisable dans $\mathcal{M}_2(\mathbf{K})$. C'est–à-dire, il existe une matrice $P \in GL_2(\mathbf{K})$ telle que $P^{-1}AP = \begin{pmatrix} \alpha + \delta & 0 \\ 0 & \alpha - \delta \end{pmatrix} = A_1$.

(b) Soit $B_1 = P^{-1}BP = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alors $\det(A + B) = \det\left(P^{-1}(A + B)P\right) = \det(A_1 + B_1) = 1$

D'après la question **23** on a $a - d = \dfrac{2\alpha m + 1}{\delta}$

Comme $PB_1P^{-1} = B$ et $PA_1P^{-1} = A$ sont dans $SL_2(\mathbf{Q})$, la question **22.b)** nous donne $d = \overline{a}$ et $\exists x \in \mathbf{K}$ tel que $a\overline{a} - 1 = x\overline{x}$.

On a $a - \dfrac{2\alpha m+1}{\delta} = \overline{a}$ et $m = \dfrac{a+d}{2} = \dfrac{a+\overline{a}}{2} = a + \dfrac{\alpha m + \dfrac{1}{2}}{\delta}$

Finalement, $a = \dfrac{m\delta - \alpha m - \dfrac{1}{2}}{\delta}$

$$\begin{aligned} a\overline{a} - 1 &= \frac{m\delta - \alpha m - \frac{1}{2}}{\delta} \frac{-m\delta - \alpha m - \frac{1}{2}}{-\delta} - 1 \\ &= \frac{\left(\alpha m + \frac{1}{2}\right)^2 - m^2\delta^2 + \delta^2}{-\delta^2} \\ &= \frac{\left(\alpha m + \frac{1}{2}\right)^2 - \left(\alpha^2 - 1\right)\left(m^2 - 1\right)}{1 - \alpha^2} \end{aligned}$$

(c) Sens direct :

On a $\left(\alpha m + \dfrac{1}{2}\right)^2 - \left(\alpha^2 - 1\right)\left(m^2 - 1\right) = -\delta^2 x\overline{x} = (\delta x)\left(\overline{\delta x}\right)$ donc on prend $y = \delta x$ et zoup.

Réciproque : Si $\left(\alpha m + \dfrac{1}{2}\right)^2 - \left(\alpha^2 - 1\right)\left(m^2 - 1\right) = y\overline{y}$

Alors on pose $x = \dfrac{y}{\delta} \in \mathbf{K}$ car $\delta \neq 0$ et on obtient le résultat précédent.

PARTIE VI

25.

(a) $\forall x \in \mathbf{Z}/9\mathbf{Z}, x^3 - 3x \in \left\{\dot{0}, \dot{2}, \dot{7}\right\}$
Donc pour $x = 0, x^3 - 3x \equiv 0\,[9]$, pour $x = 2, x^3 - 3x \equiv 2\,[9]$ et pour $x = 4, x^3 - 3x \equiv 7\,[9]$.

(b) On a $M^2 = (TrM) \times M - \det M \times I_2$ d'après Cayley-Hamilton.
Donc $M^3 = (TrM) \times M^2 - M$ car $M \in SL_2(\mathbf{Z})$.
On obtient en prenant la trace de chaque côté :

$$\begin{aligned} Tr\left(M^3\right) &= (TrM) \times \left(TrM^2\right) - Tr(M) \\ &= (TrM) \times \left((TrM)^2 - 2\right) - Tr(M) \\ &= (TrM)^3 - 3Tr(M) \end{aligned}$$

(c)

i. On a $Tr\left(A^3\right) + Tr\left(B^3\right) = Tr\left(C^3\right)$ et $\forall M \in SL_2(\mathbf{Z}), Tr\left(M^3\right) \equiv \begin{cases} 0\,[9] \\ 2\,[9] \\ 7\,[9] \end{cases}$

Notons que $\forall M \in SL_2(\mathbf{Z}), \det(-M) = (-1)^2 \det M = 1$ et $Tr(-M) = -Tr(M)$.

- Si $Tr\left(A^3\right) \equiv 2\,[9]$ alors
soit $Tr\left(B^3\right) \equiv 0\,[9]$ et $Tr\left(C^3\right) \equiv 2\,[9]$ et alors on prend $A_1 = B, B_1 = A$ et $C_1 = C$
soit $Tr\left(B^3\right) \equiv 7\,[9]$ et $Tr\left(C^3\right) \equiv 0\,[9]$
alors on prend $A_1 = C, B_1 = -B$ et $C_1 = A$
- Si $Tr\left(A^3\right) \equiv 7\,[9]$ alors on a $(-A)^3 + (-B)^3 = (-C)^3$ avec $Tr\left((-A)^3\right) \equiv 2\,[9]$ donc on est ramené au cas précédent avec $-A, -B$ et $-C$ à la place de A, B et C.
- Si $Tr\left(A^3\right) \equiv 0\,[9]$ alors
soit $Tr\left(B^3\right) \equiv 2\,[9]$ et $Tr\left(C^3\right) \equiv 2\,[9]$ et alors on prend $A_1 = A, B_1 = B$ et $C_1 = C$.
soit $Tr\left(B^3\right) \equiv 7\,[9]$ et $Tr\left(C^3\right) \equiv 7\,[9]$
On prend $A_1 = -A, B_1 = -B$ et $C_1 = -C$.

ii. On a $\det\left(\dot{B_1}\right) = (\det \dot{B_1}) = \dot{1}$ et de même $\det\left(\dot{C_1}\right) = \dot{1}$.
On a $Tr\left(B_1^3\right) \equiv Tr\left(B_1\right)^3 [3]$ d'après la question **25.b.**
Et d'après le petit théorème de Fermat $Tr\left(B_1\right)^3 \equiv Tr\left(B_1\right) [3]$
Or $Tr\left(B_1\right)^3 \equiv 2 [9]$ donc $Tr\left(B_1\right)^3 \equiv 2 [3]$ et finalement $Tr\left(\dot{B_1}\right) = \dot{2}$ et donc

$$\chi_{\dot{B_1}}(X) = X^2 - \dot{2}X + \dot{1} = \left(X - \dot{1}\right)^2$$

et de même pour C_1 ...

iii. Comme le polynôme caractéristique de $\dot{B_1}$ est scindé, elle est trigonalisable sur le corps $\mathbf{Z}/3\mathbf{Z}$.
Donc comme sa seule valeur propre est $\dot{1}$ elle est semblable à une matrice qui s'écrit $\begin{pmatrix} \dot{1} & k \\ \dot{0} & \dot{1} \end{pmatrix}$ avec $k \in \mathbf{Z}/3\mathbf{Z}$. Et même raisonnement pour C_1.

iv. $\forall k \in \mathbf{Z}/3\mathbf{Z}, \begin{pmatrix} \dot{1} & k \\ \dot{0} & \dot{1} \end{pmatrix}^3 = \begin{pmatrix} \dot{1} & \dot{0} \\ \dot{0} & \dot{1} \end{pmatrix} = I_2$
Donc $\dot{B_1}^3$ est semblable à I_2 et donc $\dot{B_1}^3 = I_2$ et de même $\dot{C_1}^3 = I_2$. Or, $A_1^3 = C_1^3 - B_1^3$ donc

$$\dot{A_1^3} = \dot{C_1^3} - \dot{B_1^3} = 0_2$$

Or $\det \dot{A_1} = \dot{1}$ ce qui donne une contradiction !

26.

(a) Notons

$$(4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right) \equiv 2^2 - 16 [9]$$

car $2\alpha \equiv 0 [9]$ et $2m \equiv 0 [9]$ et donc

$$(4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right) \equiv 6 [9]$$

De plus

$$\begin{aligned} (4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2 &\equiv (4xd)^2 + 4(2yd)^2 [9] \\ &\equiv (4xd)^2 + (2yd)^2 [3] \end{aligned}$$

Par ailleurs, on a

$$(4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2 \equiv 6d^2 [9]$$

d'après le calcul précédent, et donc finalement

$$(4xd)^2 + (2yd)^2 \equiv 6d^2 [3] \equiv 0 [3]$$

(b) Les carrés dans $\mathbf{Z}/3\mathbf{Z}$ sont $\dot{0}$ et $\dot{1}$ donc $\forall t \in \mathbf{Z}, t^2 \equiv \begin{cases} 0 [3] \\ 1 [3] \end{cases}$
Donc une somme de deux carrés n'est congrue à 0 modulo 3 que si chaque carré est congru à 0 modulo 3 et donc

$$(4xd)^2 + (2yd)^2 \equiv 0 [3] \Rightarrow (4xd)^2 \equiv 0 [3] \text{ et } (2yd)^2 \equiv 0 [3]$$

Par suite, $4xd \equiv 0 [3]$ et $2yd \equiv 0 [3]$.

(c) D'après ce qui précède en élevant au carré, on a $(4xd)^2 \equiv 0 [9]$ et $(2yd)^2 \equiv 0 [9]$ donc

$$(4xd)^2 - \left((2\alpha)^2 - 4\right)(2yd)^2 \equiv 0 [9]$$

donc en utilisant $(**)$

$$d^2\left((4\alpha m + 2)^2 - \left((2\alpha)^2 - 4\right)\left((2m)^2 - 4\right)\right) \equiv 6d^2 [9] \equiv 0 [9]$$

Donc $2d^2 \equiv 0 [3]$ donc $d^2 \equiv 0 [3]$ donc $d \equiv 0 [3]$ et 3 divise d.

(d) On a $4xd = 4r \equiv 0\,[3]$ donc r est multiple de 3 et d également donc $x = \dfrac{\left(\frac{r}{3}\right)}{\left(\frac{d}{3}\right)}$ de même on a $2yd = 2s \equiv 0\,[3]$ donc s est multiple de 3 et on a $y = \dfrac{\left(\frac{s}{3}\right)}{\left(\frac{d}{3}\right)}$ donc $\dfrac{d}{3}$ est un dénominateur commun de x et y ce qui est contradictoire avec la définition de d qui est la plus petit dénominateur commun.

27. D'après la conclusion de la partie V si de telles matrices U et V existaient alors on aurait une relation de la forme
$$\left(\alpha m + \frac{1}{2}\right)^2 - \left(\alpha^2 - 1\right)\left(m^2 - 1\right) = u^2 - \left(\alpha^2 - 1\right)v^2$$
avec $u, v \in \mathbf{Q}$ et ça c'est impossible d'après la question **26** si $2\alpha \equiv 0\,[9]$ et $2m \equiv 0\,[9]$.

28. Si $A^3 + B^3 = C^3$ avec $A, B, C \in SL_2(\mathbf{Z})$ alors $Tr\left(A^3\right) \equiv 0\,[9]$ et $Tr\left(B^3\right) \equiv 0\,[9]$. Donc si on pose $U = A^3$ et $V = B^3$ on a bien $U, V \in SL_2(\mathbf{Z})$
$Tr(U) \equiv 0\,[9]$ et $Tr(V) \equiv 0\,[9]$ et $\det(U+V) = \det\left(C^3\right) = 1$
D'après la question **27 ces matrices** U et V ne peuvent exister donc il n'existe pas de solution dans $SL_2(\mathbf{Z})$ de l'équation $X^3 + Y^3 = Z^3$.
De plus, si n est multiple de 3, on note $n = 3k$ et l'équation $X^n + Y^n = Z^n$ s'écrit
$$\left(X^{\frac{n}{3}}\right)^3 + \left(Y^{\frac{n}{3}}\right)^3 = \left(Z^{\frac{n}{3}}\right)^3$$
avec $X^{\frac{n}{3}}, Y^{\frac{n}{3}}, Z^{\frac{n}{3}} \in SL_2(\mathbf{Z})$ qui n'a pas de solutions.

PARTIE VII

29. Si $M \in \mathcal{M}_p(\mathbf{C})$ est k périodique alors le polynôme $X^k - 1$ est un polynôme annulateur de M. Or, $X^k - 1 = \prod_{r=0}^{k-1}\left(X - e^{\frac{2ir\pi}{k}}\right)$ est scindé à racines simples. Donc M est diagonalisable.

30.

(a) Notons $X = \begin{pmatrix} a & b \\ c & -1-a \end{pmatrix}$ on a $-a(1+a) - bc = 1$ donc $a^2 + bc = -a - 1$
et $X^2 = \begin{pmatrix} a^2+bc & -b \\ -c & bc + (1+a)^2 \end{pmatrix} = A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$
Donc on a $b = 1$ et $c = -1$ donc $a^2 - 1 = 0$ et $-1 + (1+a)^2 = -1$
donc $(1+a)^2 = 0$ donc $a = -1$. Donc $X = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = B$
$A^2 = -A - I_2$ donc $A^3 = -A^2 - A = I_2$
Donc $X^6 = I_2$ et donc X est $6-$ périodique donc $12-$ périodique...

(b) $A^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} = B$ et $Y = A$ est $3-$ périodique

(c) Soit $Z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on a $Z^2 = -I_2 = C$ et donc Z est $4-$ périodique donc 12 périodique
et comme $A + B = C$ on peut écrire $X^2 + Y^2 = Z^2$ avec X, Y et Z toutes $12-$ périodiques.

31. On a $n = 2 + 12k$ avec $k \in \mathbb{Z}$ et donc Pour toute matrice M : $12-$ périodiques on a
$$M^n = M^{2+12k} = M^2\left(M^{12}\right)^k = M^2\left(I_2\right)^k = M^2$$
Donc comme les matrices de la question précédente sont $12-$ périodiques et vérifient $X^2 + Y^2 = Z^2$ elles vérifient également $X^n + Y^n = Z^n$.

32. Les matrices X, Y et Z sont inversible et leur inverse est dans $SL_2(\mathbb{Z})$, de plus elles vérifient $X^2 + Y^2 = Z^2$ donc le triplet de matrice X^{-1}, Y^{-1}, Z^{-1} est solution de $X^{-2} + Y^{-2} = Z^{-2}$
Si $n \equiv -2\,[12]$ pour toute matrice M : $12-$ périodique on a $M^{-2} = M^n$
Finalement, on a bien $\left(X^{-1}\right)^n + \left(Y^{-1}\right)^n = \left(Z^{-1}\right)^n$.

33. A et B sont $3-$ périodique et C est $2-$ périodique donc elle sont toutes $6-$ périodiques et donc

$$\forall k \in \mathbb{Z}, A^{1+6k} + B^{1+6k} = A + B = C = C^{1+6k}$$

De plus $A^{-1} + B^{-1} = B + A = C = C^{-1}$ et donc

$$\forall k \in \mathbb{Z}, A^{-1+6k} + B^{-1+6k} = C^{-1+6k}$$

Finalement, si $n \equiv \pm 1\,[6]$ le triplet (A, B, C) est solution de $X^n + Y^n = Z^n$.

34. Si $n \equiv 0\,[6]$ ou $n \equiv 3\,[6]$ alors n est multiple de 3 et l'équation $X^n + Y^n = Z^n$ n'admet pas de solution d'après la partie VI.

Si $n \equiv 1\,[6]$ ou $n \equiv 5\,[6]$ alors il y a des solutions (question précédentes)

Si $n \equiv 2\,[6]$ on a $n = 2 + 6k$ alors soit k est pair et $n \equiv 2\,[12]$ et il y a des solutions, soit k est impair et $n = 2 + 6\,(2p + 1) = 8 + 12p = 4\,(2 + 3p)$ donc n est multiple de 4 et on a pas de solutions.

Si $n \equiv 4\,[6]$ on a $n = 4 + 6k$ alors soit k est pair et n est multiple de 4 donc pas de solutions, soit k est impair et $n = 4 + 6\,(2q + 1) = 10 + 12q$ donc $n \equiv -2\,[12]$ et il y a des solutions.

PARTIE VIII : Réseaux de $\mathbf{Q}^n$.

35. $\mathcal{R} = \langle v_1, ..., v_m \rangle$ donc c'est un sous-groupe de $(\mathbf{Q}^n, +)$.

36. Si $n = 1, \mathcal{R} = \mathbf{Z}v_1 + ... + \mathbf{Z}v_m$ avec $v_1, ..., v_m \in \mathbf{Q}$ soit d le ppcm des dénominateurs de $v_1, v_2, ..., v_m$ alors il existe des entiers $a_1, ..., a_m$ tels que $\forall i, v_i = \dfrac{a_i}{d}$.

Les éléments de $\mathcal{R}$ sont de la forme

$$\sum_{i=1}^{m} \frac{k_i a_i}{d} = \frac{\sum_{i=1}^{m} k_i a_i}{d}$$

avec $k_i \in \mathbf{Z}$.

$\{\sum_{i=1}^{m} k_i a_i\}$ est le sous-groupe de $(\mathbf{Z}, +)$ engendré par les entiers a_i et donc c'est $p\mathbf{Z}$ avec $p = \mathsf{p}\gcd(a_1, a_2, ..., a_m)$.

Finalement, $\mathcal{R} = r\mathbf{Z}$ avec $r = \dfrac{p}{d}$.

r n'est pas unique car $-r$ marche aussi.

37. Comme π est un morphisme de groupe de $(\mathbf{Q}^n, +)$ dans $(\mathbf{Q}, +)$ on a

$$\forall x \in \pi(\mathcal{R}), x = \pi\left(\sum_{i=1}^{m} k_i v_i\right) = \sum_{i=1}^{m} k_i \pi(v_i)$$

donc on est ramené à la situation de la question précédente. Donc il existe $s \in \mathbf{Q}$ tel que $\pi(\mathcal{R}) = s\mathbf{Z}$.

Du coup $s \in \pi(\mathcal{R})$ donc $\exists \omega \in \mathcal{R}, \pi(\omega) = s$ et on a bien $\pi(\mathcal{R}) = \pi(\omega)\,\mathbf{Z}$.

38.

(a) $\pi(x) \in \pi(\omega)\,\mathbf{Z}$ donc $\exists q \in \mathbf{Z}, \pi(x) = q\pi(\omega) = \pi(q\omega)$ et donc si on pose $\tilde{x} = x - q\omega$ alors $\tilde{x} \in \mathcal{R}$ et on a $\pi(\tilde{x}) = \pi(x) - \pi(q\omega) = 0$. Donc $\tilde{x} \in \mathbf{Q}^{n-1} \times \{0\}$. Finalement, on a bien $x = q\omega + \tilde{x}$ avec $q \in \mathbf{Z}$ et $\tilde{x} \in \mathbf{Q}^{n-1} \times \{0\} \cap \mathcal{R}$.

(b) Si $x = q\omega + \tilde{x} = p\omega + \tilde{y}$ avec $p \in \mathbf{Z}$ et $\tilde{y} \in \mathbf{Q}^{n-1} \times \{0\} \cap \mathcal{R}$. Alors $\tilde{x} - \tilde{y} = (p - q)\,\omega$ et $\pi(\tilde{x}) = \pi(\tilde{y})$ donc $\pi(\tilde{x} - \tilde{y}) = 0$ et donc $(p - q)\,\pi(\omega) = 0$ donc soit $p = q$ et alors $\tilde{x} = \tilde{y}$ soit $\pi(w) = 0$ et donc $\pi(\mathcal{R}) = \pi(\omega)\,\mathbf{Z} = \{0\}$ et donc $\omega = (0, 0, ..., 0)$ et donc $\tilde{x} = \tilde{y}$.
Donc $\tilde{x}$ est unique. Par contre si on remplace ω par $-\omega$ alors $-q$ est un entier qui donne la relation donc l'entier q n'est pas unique.

39. En utilisant la question 38 appliqué à $v_1..., v_m$ on peut écrire

$$\forall x \in \mathcal{R}, x = \sum_{i=1}^{m} k_i v_i = \sum_{i=1}^{m} k_i \widetilde{v_i} + \sum_{i=1}^{m} k_i q_i \omega$$

et comme $\sum_{i=1}^{m} k_i \widetilde{v_i} \in \mathbf{Q}^{n-1} \times \{0\} \cap \mathcal{R}$ l'unicité vu ci-dessus nous dit que $\tilde{x} = \sum_{i=1}^{m} k_i \widetilde{v_i}$
Si $x \in \mathbf{Q}^{n-1} \times \{0\} \cap \mathcal{R}$ alors $x = x + 0\omega$ donc $x = \tilde{x} = \sum_{i=1}^{m} k_i \widetilde{v_i}$ et donc on a bien

$$\mathbf{Q}^{n-1} \times \{0\} \cap \mathcal{R} = \left\{ \sum_{i=1}^{m} k_i \widetilde{v_i} | k_1, ..., k_m \in \mathbf{Z} \right\}$$

40. Si $n=1$ alors on a vu qu'il existe $r \in \mathbf{Q}$ tel $\mathcal{R}=r\mathbf{Z}$ donc $u_1=r$ convient.

Supposons le théorème vrai pour la dimension $n-1$, et soit $\mathcal{R} \subset \mathbf{Q}^n$ on a que $\mathbf{Q}^{n-1}\times\{0\}\cap\mathcal{R}=\{\sum_{i=1}^{m} k_i\widetilde{v_i}|k_1,...,k_m \in \mathbf{Z}\}$ est de dimension $n-1$ donc il existe $u_1,...,u_p \in \mathbf{Q}^{n-1}\times\{0\}\cap\mathcal{R}$ tels que $\mathbf{Q}^{n-1}\times\{0\}\cap\mathcal{R}=\mathbf{Z}u_1\oplus...\oplus\mathbf{Z}u_p$

Et donc $\mathcal{R}=\mathbf{Z}u_1\oplus...\oplus\mathbf{Z}u_p\oplus\mathbf{Z}\omega$ ce qui conclut la récurrence.

41. Si $(u_1,...,u_p)$ est une $\mathbf{Z}$ base de $\mathcal{R}$ alors $\forall i, v_i \in vect\,(u_1,...,u_p)$ donc la famille $u_1,...,u_p$ est une famille génératrice de $\mathbf{Q}^n$ (car la famille $(v_1,...,v_m)$ est génératrice). Donc $p \geq n$.

Supposons qu'il existe $q_1,...,q_p \in \mathbf{Q}$ tels que $\sum_{i=1}^{p} q_iu_i=0_{\mathbf{Q}^n}$ En multipliant par le dénominateur commun des fraction q_i on obtient $\sum_{i=1}^{p} k_iu_i=0_{\mathbf{Q}^n}$ avec $k_i \in \mathbf{Z}$ mais alors $\forall i, k_i=0$ car $(u_1,...,u_p)$ est une $\mathbf{Z}$ base et donc $\forall i, q_i=0$ et donc la famille $(u_1,...,u_p)$ est libre.

Finalement, la famille $(u_1,...,u_p)$ est une base de $\mathbf{Q}^n$ et donc $n=p$.

PARTIE I

42.

(a) $I_p \in G$ car c'est l'élément neutre de $SL_p(\mathbf{Q})$ et donc $\forall i, e_i \in \mathcal{M} \subset H$.

(b) $\forall y \in \mathcal{M}$ on a $y=Ne_i$ ou $y=-Ne_i$ avec $N \in G$ donc $\forall M \in G, My=(MN)\,e_i$ ou $My=-(MN)\,e_i$ donc $My \in \mathcal{M}$. Donc si $h=\sum_{i=1}^{q} y_i$ on a $Mh=\sum_{i=1}^{q} My_i \in H$.

(c) On a $Me_j=\sum_{i=1}^{p}\alpha_ie_i$ avec $\alpha_i=\dfrac{a_i}{b_i} \in \mathbf{Q}$ et tels que $\forall i, \alpha_id=k_i \in \mathbf{Z}$ et donc $\dfrac{a_i}{b_i}=\dfrac{a_i}{b_i}\times d\times\dfrac{1}{d}=\dfrac{k_i}{d}$

Si on fait la division euclidienne de k_i par d, on obtient $k_i=q_id+r_i$ avec $0 \leq r_i < d$ et donc

$$Me_j=\sum_{i=1}^{p}\frac{k_i}{d}e_i=\sum_{i=1}^{p}\left(q_i+\frac{r_i}{d}\right)e_i=\sum_{i=1}^{p}q_ie_i+\frac{1}{d}\sum_{i=1}^{p}r_ie_i$$

(d) La famille $\left(e_1,...,e_p,\dfrac{e_1}{d},...,\dfrac{e_p}{d}\right)$ est $\mathbf{Z}$ génératrice de Me_j pour tout M dans G et pour tout j et donc une somme et différence d'éléments de ce type est toujours dans le sous-groupe engendré par $\left(e_1,...,e_p,\dfrac{e_1}{d},...,\dfrac{e_p}{d}\right)$ et cette famille est génératrice car $(e_1,...,e_p)$ est une base de $\mathbf{Q}^p$.

(e) D'après la question 40 il existe $(u_1,...,u_p)$ une $\mathbf{Z}$ base de H et comme d'après le b) $Mu_i \in H$ il existe des entiers k_i tels que $Mu_i=\sum_{i=1}^{p}k_iu_i$.

(f) Soit F la matrice de passage de la base $(e_1,...e_p)$ à la base $(u_1,...,u_p)$ alors $\forall M \in G$, les coefficients de Mu_i dans la base $(u_1,...,u_p)$ sont des entiers donc $F^{-1}MF \in SL_p(\mathbf{Z})$.

43.

(a) On $A^2-tr\,(A)\,A+I_2=0_2$ (Cayley-Hamilton) donc $A\,(A-tr\,(A)\,I_2)=-I_2$ donc $A^{-1}=tr\,(A)\,I_2-A \in K$ car $tr\,(A) \in \mathbf{Z}$. De même pour B^{-1}.

(b) $(ABAB)=(AB)^2=tr\,(AB)\,AB-I_2 \in K$

$A^2=tr\,(A)\,A-I_2 \in K$ de même pour B^2 et BA (car $tr\,(AB)=tr\,(BA)$)et on montre facilement par récurrence que $\forall n \in \mathbf{N}$,$A^n \in K, B^n \in K$, $(AB)^n \in K$ et $(BA)^n \in K$.

Donc si on prend $m \in K$ alors $MA \in K$ et $MB \in K$ et du coup tout produit de matrice A, B, A^{-1}, B^{-1} est dans $\mathbf{K}$.

Donc $G \subset K$.