Agrégation inerne de mathématiques

Mathématiques générales 2022

12 octobre 2022

(1) (a) Faux. Écrivons $M = (m_{i,j})_{1 \leq i,j \leq n}$ et $N = (n_{i,j})_{1 \leq i,j \leq n}$. On a

$$\mathrm{Tr}(MN) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{n} m_{i,j} n_{j,i} \Big) = \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} n_{j,i} m_{i,j} \Big) = \mathrm{Tr}(NM).$$

(b) Vrai. Si $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$. On a

$$\begin{aligned} \chi_M(X) &= \det(X\,\mathrm{I}_2 - M) = \det \left(\begin{smallmatrix} X-a & -b \\ -c & X-d \end{smallmatrix} \right) = (X-a)(X-d) - bc \\ &= X^2 - (a+d)X + ad - bc = X^2 - \mathrm{Tr}(M)X + \det(M) \end{aligned}$$

ce qui prouve que $\chi_M(X)$ ne dépend que de $\mathrm{Tr}(M)$ et $\det(M)$.
(c) Faux. La matrice $S = \left(\begin{smallmatrix} 1 & i \\ i & -1 \end{smallmatrix} \right) \in \mathsf{M}_2(\mathbf{C})$ est symétrique, et $\chi_S(X) = X^2$: si S était diagonalisable, on aurait $S = 0$, ce qui n'est pas.
(d) Faux. La surjection canonique $\varphi\colon\ \mathbf{Z}\,/ \to \mathbf{Z}\,/2\,\mathbf{Z}$ est un morphisme d'anneaux, et $\varphi(3) = \overline{1}$ est inversible dans $\mathbf{Z}\,/2\,\mathbf{Z}$, alors que $3 \notin \mathbf{Z}^{\times}\{\pm 1\}$.

Remarque. On peut aussi considérer l'inclusion $\mathbf{Z} \subset \mathbf{Q}$.

(2) On procède par récurrence sur $d \in \mathbf{N}_{>0}$, le cas $d = 1$ étant trivial. Supposons $d > 1$. On a

$$\chi_{C_P}(X) = \begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{d-1} \\ 0 & \cdots & 0 & -1 & X+a_{d-1} \end{vmatrix} = X \underbrace{\begin{vmatrix} X & 0 & \cdots & 0 & a_1 \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{d-1} \\ 0 & \cdots & 0 & -1 & X+a_{d-1} \end{vmatrix}}_{=\chi_{C_Q}(X)} + (-1)^{d+1} a_0 \underbrace{\begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & X \\ 0 & \cdots & \cdots & 0 & -1 \end{vmatrix}}_{=(-1)^{d-1}} = X\chi_{C_Q}(X) + a_0$$

où $Q(X) = X^{d-1} + a_{d-1}X^{d-2} + \cdots + a_1$. Par hypothèse de récurrence, on a $\chi_{C_Q}(X) = Q(X)$, de sorte que $\chi_{C_P}(X) = XQ(X) + a_0 = P(X)$.

Remarque. Autre approche : soient $L_1, \ldots, L_d$ les lignes de $X\,\mathrm{I}_d - C_P$, on a $\chi_{C_P}(X) = \begin{vmatrix} X & 0 & \cdots & 0 & P(X) \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & a_{d-1} \\ 0 & \cdots & 0 & -1 & X+a_{d-1} \end{vmatrix} = (-1)^{d+1} P(X) \begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & X \\ 0 & \cdots & \cdots & \cdots & -1 \end{vmatrix} = P(X)$ en faisant l'opération $L_1 \leftarrow L_1 + XL_2 + X^2L_3 + \cdots + X^{d-1}L_d$.

(3) (a) (i) Par minimalité de μ, la famille $(x, Mx, \ldots, M^{\mu-1}x)$ est libre dans $\mathbf{C}^p$: complétons-la en une base $\mathfrak{B} = (e_1, \ldots, e_p)$ de $\mathbf{C}^p$. On a $e_k = M^{k-1}x$ si $1 \leq k \leq \mu$, d'où $Me_k = M(M^{k-1}x) = M^k x = e_{k+1}$ pour $1 \leq k < \mu$. Par définition de μ, la famille $(x, Mx, \ldots, M^{\mu-1}x, M^{\mu}x)$ est liée : comme $(x, Mx, \ldots, M^{\mu-1}x)$ est libre, on a donc

$$Me_\mu = M(M^{\mu-1}x) = M^{\mu}(x) \in \mathrm{Vect}(x, Mx, \ldots, M^{\mu-1}x) = \mathrm{Vect}(e_1, \ldots, e_\mu).$$

il existe donc $\alpha_0, \ldots, \alpha_{\mu-1} \in \mathbf{C}$ tels que $Me_\mu = -\alpha_0 e_1 - \cdots - \alpha_{\mu-1}e_\mu = -\sum\limits_{k=0}^{\mu-1} \alpha_k M^k x$. Cela montre que la matrice dans la base $\mathfrak{B}$ de l'endomorphisme de $\mathbf{C}^p$ associé à M est de la forme $M' = \left(\begin{smallmatrix} C_P & * \\ 0 & N \end{smallmatrix} \right)$ (par blocs), où $P(X) = X^{\mu} + \alpha_{\mu-1}X^{\mu-1} + \cdots + \alpha_0$ et $N \in \mathsf{M}_{p-\mu}(\mathbf{C})$.

(ii) On a $\chi_M(X) = \chi_{M'}(X) = \chi_{C_P}(X)\chi_N(X) = \chi_N(X)P(X)$ en vertu de la question précédente. Cela implique que $\chi_M(M)x = \chi_N(M)P(M)x$. D'après la question précédente, on a $M^\mu x = -\sum_{k=0}^{\mu-1} \alpha_k M^k x$, soit encore $P(M)x = 0$, de sorte que $\chi_M(M)x = 0$.
(b) Dans la question précédente, on a montré que si $x \in \mathbf{C}^p \setminus \{0\}$, alors $\chi_M(M)x = 0$. Appliqué aux vecteurs de la base canonique, cela montre que les colonnes de la matrice $\chi_M(M)$ sont toutes nulles : on a $\chi_M(M) = 0$.

(4) Soient $x, y \in \mathbf{R}^p$ deux vecteurs. On a $\langle a(x)|y\rangle = {}^t(Ax)y = {}^tx{}^tAy = {}^txAy = \langle x|a(y)\rangle$, parce que ${}^tA = A$, ce qui montre que a est un endomorphisme symétrique.

(5) Supposons $S \in \mathcal{S}_p^+(\mathbf{R})$. La matrice S est diagonalisable en base orthonormée : il existe $\Omega \in \mathsf{O}_n(\mathbf{R})$ telle que ${}^t\Omega S\Omega = \operatorname{diag}(\lambda_1, \ldots, \lambda_p)$ où $\lambda_1, \ldots, \lambda_p$ sont les valeurs propres de S. Si $Y \in \mathsf{M}_{p,1}(\mathbf{R})$ et $X = (x_i)_{1\leq i\leq p} = \Omega Y \in \mathsf{M}_{p,1}(\mathbf{R})$, on a

$$ {}^tYSY = {}^tX \operatorname{diag}(\lambda_1, \ldots, \lambda_p)X = \sum_{k=1}^{p} \lambda_k x_k^2 \geq 0 $$

parce que $\lambda_1, \ldots, \lambda_p \geq 0$.
Réciproquement, supposons que ${}^tYSY \geq 0$ pour tout $Y \in \mathsf{M}_{p,1}(\mathbf{R})$. Si $\lambda \in \operatorname{Sp}(S)$ et $Y \in \mathsf{M}_{p,1}(\mathbf{R}) \setminus \{0\}$ un vecteur propre associé, on a $\lambda \|Y\|^2 = {}^tYSY \geq 0$, et donc $\lambda \geq 0$ vu que $\|Y\| > 0$ (parce que $Y \neq 0$).

(6) Si $S, T \in \mathcal{S}_p^+(\mathbf{R})$, la matrice $S + T$ est symétrique. Par ailleurs, si $Y \in \mathsf{M}_{p,1}(\mathbf{R})$, on a ${}^tY(S+T)Y = {}^tYSY + {}^tYTY \geq 0$ vu que ${}^tYSY \geq 0$ et ${}^tYTY \geq 0$ en vertu de la question précédente. Comme c'est vrai pour tout $Y \in \mathsf{M}_{p,1}(\mathbf{R})$, cette dernière implique que $S + T \in \mathcal{S}_p^+(\mathbf{R})$.

(7) La matrice S est diagonalisable en base orthonormée : soit $\Omega \in \mathsf{O}_p(\mathbf{R})$ telle que $S = {}^t\Omega \operatorname{diag}(\lambda_1, \ldots, \lambda_p)\Omega$ où $\lambda_1, \ldots, \lambda_p \in \mathbf{R}_{\geq 0}$ sont les valeurs propres de S. On a $S = R^n$ avec $R = {}^t\Omega \operatorname{diag}\big(\sqrt[n]{\lambda_1}, \ldots, \sqrt[n]{\lambda_p}\big)\Omega \in \mathcal{S}_p^+(\mathbf{R})$.

(8) (a) Observons que $us = uu^n = u^{n+1} = u^n u = su$: les endomorphismes u et s commutent. Cela implique que les sous-espaces propres de s sont stables par u (si $x \in E_{\lambda_i}(s)$, on a $s(u(x)) = u(s(x)) = u(\lambda_i x) = \lambda_i u(x)$ donc $u(x) \in E_{\lambda_i}(s)$). Cela implique que u induit un endomorphisme u_i de $E_{\lambda_i}(s)$. Si $x, y \in E_{\lambda_i}(s)$, on a $\langle u_i(x)|y\rangle = \langle u(x)|y\rangle = \langle x|u(y)\rangle = \langle x|u_i(y)\rangle$ vu que u est symétrique en vertu de la question (4) (parce que $U \in \mathcal{S}_p^+(\mathbf{R})$).
(b) Soit λ une valeur propre de u_i. C'est une valeur propre de u donc de U : on a $\lambda \in \mathbf{R}_{\geq 0}$. Soit $x \in E_{\lambda_i}(s)$ un vecteur propre non nul associé. On a $u_i(x) = \lambda x$, donc $u(x) = \lambda x$, d'où $s(x) = u^n(x) = \lambda^n x$. Comme $x \in E_{\lambda_i}(s)$, on a aussi $s(x) = \lambda_i x$, de sorte que $\lambda^n = \lambda_i$ vu que $x \neq 0$, et donc $\lambda = \sqrt[n]{\lambda_i}$ (parce que $t \mapsto t^n$ est une bijection de $\mathbf{R}_{\geq 0}$ sur lui-même, de bijection réciproque $t \mapsto \sqrt[n]{t}$). Il en résulte que $\sqrt[n]{\lambda_i}$ est la seule valeur propre possible de u_i.
(c) Comme u_i est symétrique, il est diagonalisable (en base orthonormée) : sa seule valeur propre étant $\sqrt[n]{\lambda_i}$, c'est nécessairement $\sqrt[n]{\lambda_i}\,\mathsf{Id}_{E_{\lambda_i}(s)}$. Cela implique que $u = \sum_{i=1}^{q} \sqrt[n]{\lambda_i}\pi_i$ où π_i est le projecteur sur $E_{\lambda_i}(s)$ parallèlement à $\bigoplus_{\substack{1\leq j\leq q\\ j\neq i}} E_{\lambda_j}(s)$. Cela prouve l'unicité de u.

(9) L'existence a été prouvé dans la question (7), l'unicité résulte de la question (8).

(10) Si $U, V \in \mathcal{S}_p^+(\mathbf{R})$, on a $U + V \in \mathcal{S}_p^+(\mathbf{R})$ en vertu de la question (6). Par ailleurs, on a $(\sqrt[n]{U})^n = U$, $(\sqrt[n]{V})^n = V$ et $(\sqrt[n]{U+V})^n = U + V$ par définition. On a donc $(\sqrt[n]{U})^n + (\sqrt[n]{V})^n = (\sqrt[n]{U+V})^n$, ce qui montre que l'application ψ est bien définie. Elle est injective parce que si $\psi(U, V) = (X, Y, Z)$, on a $U = X^n$ et $V = Y^n$. Si maintenant $(X, Y, Z) \in \big(\mathcal{S}_p^+(\mathbf{R})\big)^3$ est tel que $X^n + Y^n = Z^n$, posons $U = X^n$ et $Y = V^n$: on a $U, V \in \mathcal{S}_p^+(\mathbf{R})$, $X = \sqrt[n]{U}$ et $Y = \sqrt[n]{V}$. En outre, on a $Z^n = X^n + Y^n = U + V$, donc $Z = \sqrt[n]{U+V}$, ce qui montre que $(X, Y, Z) = \psi(U, V)$. On a montré que l'application ψ est bijective (et que $\psi^{-1}(X, Y, Z) = (X^n, Y^n)$).

(11) D'après le théorème de Cayley-Hamilton prouvé dans la question (3), $\chi_M(X) = X^2 - \operatorname{Tr}(M)X + \det(M)$ est un polynôme annulateur de M : on a $M^2 = \operatorname{Tr}(M)M - \mathrm{I}_2$ (parce que $\det(M) = 1$ par hypothèse). en prenant la trace, on a déjà $\operatorname{Tr}(M^2) = \operatorname{Tr}(M)^2 - 2$. Par ailleurs, on a $M^4 = (\operatorname{Tr}(M)M - \mathrm{I}_2)^2 = \operatorname{Tr}(M)^2M^2 - 2\operatorname{Tr}(M)M + \mathrm{I}_2$: en prenant la trace, il vient

$$\operatorname{Tr}(M^4) = \operatorname{Tr}(M)^2\operatorname{Tr}(M^2) - 2\operatorname{Tr}(M)^2 + 2 = \operatorname{Tr}(M)^2(\operatorname{Tr}(M)^2 - 2) - 2\operatorname{Tr}(M)^2 + 2 = \operatorname{Tr}(M)^4 - 4\operatorname{Tr}(M)^2 + 2.$$

Remarque. On peut aussi utiliser les valeurs propres de M : si ce sont λ et μ, on a $\lambda\mu = 1$ puisque $\det(M) = 1$, et $\mathrm{Tr}(M)^4 - 4\,\mathrm{Tr}(M)^2 + 2 = (\lambda+\mu)^4 - 4(\lambda+\mu)^2 + 2 = \lambda^4 + \mu^4 = \mathrm{Tr}(M^4)$ en développant.

(12) Si $\mathrm{Tr}(M) = 2k$ est paire, on a $\mathrm{Tr}(M^4) = (2k)^4 - 4(2k)^2 + 2 = 2 + 16(k^4 + k^2) \equiv 2 \mod 8$. Si $\mathrm{Tr}(M) = 2k+1$ est impaire, on a $(2k+1)^2 = 1 + 4k + 4k^2 = 1 + 8\binom{k}{2} \equiv 1 \mod 8$, de sorte que $\mathrm{Tr}(M^4) = (2k+1)^4 - 4(2k+1)^2 + 2 \equiv 1 - 4 + 2 \mod 8$, *i.e.* $\mathrm{Tr}(M^4) \equiv -1 \mod 8$.

(13) Soient $X, Y \in \mathsf{SL}_2^+(\mathbf{R})$. D'après les deux questions qui précèdent, l'image de $\mathrm{Tr}(X^4) + \mathrm{Tr}(Y^4)$ dans $\mathbf{Z}/8\,\mathbf{Z}$ appartient à $\{\overline{2}+\overline{2}, \overline{2}-\overline{1}, -\overline{1}-\overline{1}\} = \{\overline{4}, \overline{1}, -\overline{2}\}$. Comme cet ensemble no contient ni $\overline{2}$ ni $-\overline{1}$, cela montre qu'il n'existe pas $Z \in \mathsf{SL}_2(\mathbf{Z})$ tel que $\mathrm{Tr}(X^4) + \mathrm{Tr}(Y^4) = \mathrm{Tr}(Z^4)$. Il en résulte *a fortiori* qu'il n'existe pas $Z \in \mathsf{SL}_2(\mathbf{Z})$ tel que $X^4 + Y^4 = Z^4$.

(14) Supposons $n \equiv 0 \mod 4$: écrivons $n = 4m$ avec $m \in \mathbf{N}_{>0}$. Si on avait $X^n + Y^n = Z^n$ avec $X, Y, Z \in \mathsf{SL}_2(\mathbf{Z})$, on aurait $(X^m)^4 + (Y^m)^4 = (Z^m)^4$ et le triplet (X^m, Y^m, Z^m) contredirait la question précédente.

(15) K est le sous-$\mathbf{Q}$-espace vectoriel de $\mathbf{C}$ engendré par $\{1, \delta\}$. Comme on a supposé que $\delta \notin \mathbf{Q}$, la famille $\{1, \delta\}$ est libre sur $\mathbf{Q}$: cela implique que $\dim_{\mathbf{Q}}(K) = 2$.

(16) Si $x_1 = a_1 + b_1\delta$ et $x_2 = a_2 + b_2\delta$ avec $a_1, a_2, b_1, b_2 \in \mathbf{Q}$, on a

$$x_1 x_2 = (a_1 + b_1\delta)(a_2 + b_2\delta) = \underbrace{a_1 a_1 + b_1 b_2 \delta^2}_{\in\mathbf{Q}} + (\underbrace{a_1 b_2 + a_2 b_1}_{\in\mathbf{Q}})\delta \in K$$

(parce que $\delta^2 \in \mathbf{Q}$), ce qui montre que K est un sous-anneau de $\mathbf{C}$. Si $x = a + b\delta \in K \setminus \{0\}$, on a $N(x) = x\overline{x} = (a + b\delta)(a - b\delta) = a^2 - b^2\delta^2 \in \mathbf{Q}^\times$ (parce que $x, \overline{x} \neq 0$), ce qui montre que $x^{-1} = \frac{\overline{x}}{N(x)} \in K$. Cela prouve que K est un sous-corps de $\mathbf{C}$ (ce n'est autre que la sous-extension de $\mathbf{C}/\mathbf{Q}$ engendrée par δ).

(17) Cela résulte des égalités

$$\begin{aligned}
\varphi(x_1 + x_2) &= \varphi(a_1 + a_2 + (b_1 + b_2)\delta) = a_1 + a_2 - (b_1 + b_2)\delta \\
&= a_1 - b_1\delta + a_2 - b_2\delta = \varphi(x_1) + \varphi(x_2) \\
\varphi(x_1 x_2) &= \varphi(a_1 a_2 + b_1 b_2 \delta^2 + (a_1 b_2 + a_2 b_1)\delta) = a_1 a_2 + b_1 b_2 \delta^2 - (a_1 b_2 + a_2 b_1)\delta \\
&= (a_1 - b_1\delta)(a_2 - b_2\delta) = \varphi(x_1)\varphi(x_2)
\end{aligned}$$

pour tous $x_1 = a_1 + b_1\delta, x_2 = a_2 + b_2\delta \in K$ avec $a_1, a_2, b_1, b_2 \in \mathbf{Q}$. Comme $\varphi^2 = \mathsf{Id}_K$, le morphisme de corps $\varphi\colon K \to K$ est un isomorphisme.

Remarque. Si K est un corps et A un anneau (unitaire), tout morphisme d'anneaux $K \to A$ est injectif : dans le cas présent, cela implique automatiquemnt que φ est injectif. Comme c'est un endomorphisme du $\mathbf{Q}$-espace vectoriel de dimension finie K, c'est donc un automorphisme.

(18) (a) Si $x_1, x_2 \in \mathbf{Q}$ sont tels que $\psi(x_1) = \psi(x_2)$, on a $(x_1 + \delta)(x_2 - \delta) = (x_2\delta)(x_1 - \delta)$, ce qui implique $\delta(x_2 - x_1) = \delta(x_1 - x_2)$ d'où $x_1 = x_2$, et prouve l'injectivité de ψ.

Remarque. (1) Comme ψ n'est pas un morphisme (de groupes disons), cela n'a pas de sens de considérer son noyau.
(2) Autre preuve. Soient $x \in \mathbf{Q}$ et $y = \psi(x)$. Notons que $y \neq 1$ parce que $\delta \neq 0$. On a $x + \delta = y(x - \delta)$, d'où $(1 + y)\delta = (y - 1)x$, et donc $x = \frac{y+1}{y-1}\delta$, ce qui prouve l'injectivité de ψ.

(b) On a $\psi(\mathbf{Q}) \subset \big\{\frac{\theta}{\overline{\theta}}\big\}_{\theta \in K\setminus\{0\}}$: comme ψ est injectif et $\mathbf{Q}$ infini, cela montre que $\big\{\frac{\theta}{\overline{\theta}}\big\}_{\theta \in K\setminus\{0\}}$ est infini.

(19) L'application $\mathsf{M}_p(K) \to \mathsf{M}_p(K); A \mapsto \overline{A}$ est induite par l'automorphisme de corps φ : c'est un automorphisme de l'anneau $\mathsf{M}_p(K)$. En particulier, on a $\overline{AB} = \overline{A}\,\overline{B}$ pour tous $A, B \in \mathsf{M}_p(K)$.

(20) Si $F \in \mathsf{GL}_p(K)$, on a $FF^{-1} = \mathrm{I}_p$, donc $\overline{F}\,\overline{F^{-1}} = \overline{\mathrm{I}_p} = \mathrm{I}_p$, ce qui montre que $\overline{F} \in \mathsf{GL}_p(K)$ et $\overline{F}^{-1} = \overline{F^{-1}}$. De même, si $\overline{F} \in \mathsf{GL}_p(K)$, on a $F = \overline{\overline{F}} \in \mathsf{GL}_p(K)$.

(21) (a) On a $X\overline{X} = (F\overline{F}^{-1})(\overline{F\overline{F}^{-1}}) = F\overline{F}^{-1}\overline{F}\,\overline{\overline{F}^{-1}} = F\overline{\overline{F^{-1}}} = FF^{-1} = \mathrm{I}_p$ en vertu de la question précédente.
(b) (i) Supposons $\theta \in K^\times$. On a $F(\theta) = \overline{\theta}\big(\frac{\theta}{\overline{\theta}}\,\mathrm{I}_p + X\big)$, donc $\det(F(\theta)) = (-\overline{\theta})^p \chi_X\big(-\frac{\theta}{\overline{\theta}}\big)$. Si $\det(F(\theta)) = 0$ pour tout $\theta \in K^\times$, cela implique que tous les éléments de $\big\{-\frac{\theta}{\overline{\theta}}\big\}_{\theta \in K^\times}$ sont racines de χ_X. D'après la question (18)(b), cela implique que le polynôme χ_X a une infinité de racines : il est nul, ce qui est absurde. Il existe donc $\theta_0 \in K^\times$ tel que $\det(F(\theta_0)) \neq 0$, *i.e.* $\theta\,\mathrm{I}_p + \overline{\theta}X \in \mathsf{GL}_p(K)$.

(ii) On a
$$X\overline{F(\theta_0)} = X\big(\overline{\theta_0}\,\mathrm{I}_p + \theta\overline{X}\big) = \overline{\theta_0}X + \theta_0 X\overline{X} = \theta_0\,\mathrm{I}_p + \overline{\theta_0}X = F(\theta_0)$$
vu que $X\overline{X} = \mathrm{I}_p$.
(c) Supposons (i). Comme $F^{-1}AF \in \mathsf{M}_p(\mathbf{Q})$, on a $\overline{F^{-1}AF} = F^{-1}AF$, d'où $\overline{F}^{-1}\overline{A}\overline{F} = F^{-1}AF$, *i.e.* $\overline{A} = \overline{F}F^{-1}AF\overline{F}^{-1}$, soit encore $\overline{A} = X^{-1}AX$ avec $X = F\overline{F}^{-1} \in \mathsf{GL}_p(K)$. On a de même $\overline{B} = X^{-1}BX$. En outre, comme $X = F\overline{F}^{-1}$ avec $F \in \mathsf{GL}_p(K)$, on a $X\overline{X} = \mathrm{I}_p$ d'après la question (21)(a).
Supposons (ii). D'après la question (21)(b), il existe $F \in \mathsf{GL}_p(K)$ telle que $X = F\overline{F}^{-1}$. L'égalité $\overline{A} = X^{-1}AX$ s'écrit alors $\overline{A} = \overline{F}F^{-1}AF\overline{F}^{-1}$, *i.e.* $\overline{F}^{-1}\overline{A}\overline{F} = F^{-1}AF$, *i.e.* $\overline{F^{-1}AF} = F^{-1}AF$, soit encore $F^{-1}AF \in \mathsf{M}_p(\mathbf{Q})$. On a de même $F^{-1}BF \in \mathsf{M}_p(\mathbf{Q})$.

(22) (a) Supposons que $X^{-1}AX = \overline{A}$ et $X\overline{X} = \mathrm{I}_2$. Cela implique que $AX = X\overline{A}$. Écrivons $X = \left(\begin{smallmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2}\end{smallmatrix}\right)$: légalité qui précède s'écrit $\begin{pmatrix} \lambda x_{1,1} & \lambda x_{1,2} \\ \overline{\lambda} x_{2,1} & \overline{\lambda} x_{2,2}\end{pmatrix} = \begin{pmatrix} x_{1,1}\overline{\lambda} & \lambda x_{1,2} \\ \overline{\lambda} x_{2,1} & \lambda x_{2,2}\end{pmatrix}$, ce qui implique que $\lambda x_{1,1} = \overline{\lambda}x_{1,1}$ et $\overline{\lambda}x_{2,2} = \lambda x_{2,2}$. Comme $\lambda \notin \mathbf{Q}$ par hypothèse, on a $\overline{\lambda} \neq \lambda$: cela montre que $x_{1,1} = x2, 2 = 0$. On a alors $X = \begin{pmatrix} 0 & x_{1,2} \\ x_{2,1} & 0\end{pmatrix}$, ce qui implique que $X\overline{X} = \mathrm{diag}(x_{1,2}\overline{x_{2,1}}, \overline{x_{1,2}}x_{2,1})$: si $u = x_{1,2}$, on a $u \in K^\times$ et $u\overline{x_{2,1}} = 1$, *i.e.* $x_{2,1} = \frac{1}{\overline{u}}$.
Réciproquement, suppsons qu'il existe $u \in K^\times$ tel que $X = \left(\begin{smallmatrix} 0 & u \\ 1/\overline{u} & 0\end{smallmatrix}\right)$. Un calcul direct montre que $AX = \overline{A}X$ et $X\overline{X} = \mathrm{I}_2$.
(b) • On a $\det(A) = \det(F^{-1}AF) = 1$ et de même $\det(B) = 1$.
• D'après la question (21)(c), il existe $X \in \mathsf{GL}_2(K)$ telle que $X^{-1}AX = \overline{A}$, $X^{-1}BX = \overline{B}$ et $X\overline{X} = \mathrm{I}_2$. D'après la question précédente, il existe $u \in K^\times$ tel que $X = \left(\begin{smallmatrix} 0 & u \\ 1/\overline{u} & 0\end{smallmatrix}\right)$.
L'égalité $BX = X\overline{B}$ s'écrit alors $\begin{pmatrix} b/\overline{u} & au \\ d/\overline{u} & cu\end{pmatrix} = \begin{pmatrix} \overline{c}u & \overline{d}u \\ \overline{a}/\overline{u} & \overline{b}/\overline{u}\end{pmatrix}$, ce qui implique en particulier que $\frac{d}{\overline{u}} = \frac{\overline{a}}{\overline{u}}$ et donc $d = \overline{a}$. On a de même $\frac{b}{\overline{u}} = \overline{c}u$, *i.e.* $c = \frac{\overline{b}}{u\overline{u}}$. On a donc $1 = \det(B) = ad - bc = a\overline{a} - \frac{b\overline{b}}{u\overline{u}} = N(a) - N(x)$ *i.e.* $N(a) - 1 = N(x)$ avec $x = \frac{b}{u} \in K$.

(23) Ne pas confondre a et α qui se rensemblent hélas beaucoup dans l'énoncé... L'égalité $\det(B_1) = \det(A_1 + B_1)$ s'écrit $ad - bc = (a+\alpha+\delta)(d+\alpha-\delta) - bc$, soit encore $ad = ad + a(\alpha-\delta) + d(\alpha+\delta) + \alpha^2 - \delta^2$. Comme $\alpha^2 - \delta^2 = 1$, cela implique $0 = (a+d)\alpha + (d-a)\delta + 1$, soit $(a-d)\delta = \alpha\,\mathrm{Tr}(B_1) + 1 = 2am_1 + 1$, et donc $a - d = \frac{2\alpha m_1 + 1}{\delta}$.

(24) (a) Comme $\mathrm{Tr}(A) = 2\alpha$ et $\det(A) = 1$, on a
$$\chi_A(X) = X^2 - 2\alpha X + 1 = X^2 - 2\alpha X + \alpha^2 - \delta^2 = (X-\alpha)^2 - \delta^2 = (X - \alpha - \delta)(X - \alpha + \delta).$$
Comme $\delta \neq 0$, les deux valeurs propres sont distinctes : la matrice A est diagonalisable dans $\mathsf{M}_2(K)$.
(b) Posons $\lambda = \alpha + \delta$: on a $\lambda \in K \setminus \mathbf{Q}$. D'après la question précédente, il existe $F \in \mathsf{GL}_2(K)$ telle que $FAF^{-1} = A_1 = \mathrm{diag}(\lambda, \overline{\lambda})$. On a donc $A = F^{-1}A_1F \in \mathsf{SL}_2(\mathbf{Q})$. Posons de même $B_1 = FBF^{-1}$ et écrivons $B_1 = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. On a $B = F^{-1}B_1F \in \mathsf{SL}_2(\mathbf{Q})$. D'après la question (22)(b), on a $d = \overline{a}$ et il existe $x \in K$ tel que $N(a) - 1 = N(x)$.
Par hypothèse, on a aussi $\det(A_1 + B_1) = \det(A + B) = 1$: comme $\det(B_1) = \det(B) = 1$, la question (23) s'applique, et on a $a - d = \frac{2\alpha m + 1}{\delta}$ où $m = \frac{\mathrm{Tr}(B)}{2} = \frac{\mathrm{Tr}(B_1)}{2}$. On a donc $\left(\frac{a-d}{2}\right)^2 = \frac{(\alpha m + 1/2)^2}{\delta^2} = \frac{(\alpha m+1/2)^2}{\alpha^2 - 1}$, ce qui implique que
$$\tfrac{(\alpha m+1/2)^2 - (\alpha^2-1)(m^2-1)}{1-\alpha^2} = m^2 - 1 - \left(\tfrac{a-d}{2}\right)^2 = \left(\tfrac{a+d}{2}\right)^2 - \left(\tfrac{a-d}{2}\right)^2 - 1 = ad - 1 = N(a) - 1 = N(x)$$
vu que $d = \overline{a}$.
(c) L'égalité $\frac{(\alpha m+1/2)^2 - (\alpha^2-1)(m^2-1)}{1-\alpha^2} = N(x)$ équivaut à
$$\left(\alpha m + \tfrac{1}{2}\right)^2 - (\alpha^2 - 1)(m^2 - 1) = (1 - \alpha^2)N(x) = -\delta^2 N(x) = \delta\overline{\delta}x\overline{x} = (x\delta)\overline{(x\delta)} = N(y)$$
où $y = x\delta \in K$. Comme $\delta \in K^\times$, l'existence de $x \in K$ tel que $\frac{(\alpha m+1/2)^2 - (\alpha^2-1)(m^2-1)}{1-\alpha^2} = N(x)$ équivaut à celle de $y \in K$ tel que $\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2 - 1)(m^2 - 1) = N(y)$.

(25) (a) Observons que si $x = a + 3k$ avec $a, k \in \mathbf{Z}$, on a $x^3 - 3x = a^3 + 9a^2k + 27ak^2 + 27k^3 - 3a - 9k \equiv a^3 - 3a \mod 9$, de sorte que la classe de $x^3 - 3x$ modulo 9 ne dépend que de celle de x modulo 3. Les classes de congruence de $x^3 - 3x$ modulo 9 sont donc résumée dans le tableau suivant :

classe de x mdulo 3	0	1	2
classe de x^3-3x modulo 9	0	-2	2

(b) D'après le théorème de Cayley-Hamilton (*cf* question (3)(b)), on a $0 = \chi_M(M) = M^2 - \mathrm{Tr}(M)M + \mathrm{I}_2$ (parce que $\det(M) = 1$), d'où $M^2 = \mathrm{Tr}(M)M - \mathrm{I}_2$. En prenant la trace il vient $\mathrm{Tr}(M^2) = \mathrm{Tr}(M)^2 - 2$. En multipliant par M on a $M^3 = \mathrm{Tr}(M)M^2 - M$, et donc

$$\mathrm{Tr}(M^3) = \mathrm{Tr}(M)\,\mathrm{Tr}(M^2) - \mathrm{Tr}(M) = \mathrm{Tr}(M)\big(\mathrm{Tr}(M)^2 - 2\big) - \mathrm{Tr}(M) = \mathrm{Tr}(M)^3 - 3\,\mathrm{Tr}(M).$$

(c) (i) D'après les deux questions précédentes, si $M \in \mathsf{SL}_2(\mathbf{Z})$, la classe de congruence de $\mathrm{Tr}(M^3)$ modulo 9 appartient à $\{\overline{0}, \pm\overline{2}\}$. Les classes de congruence de $\mathrm{Tr}(A^3) + \mathrm{Tr}(B^3)$ sont donc $\{\overline{0}, \pm\overline{2}, \pm\overline{4}\}$. Comme la classe de congruence de $\mathrm{Tr}(C^3)$ n'est pas égale à $\pm\overline{4}$, cela implique que les classes de congruences de $\mathrm{Tr}(A^3)$ et $\mathrm{Tr}(B^3)$ sont distinctes (et non nulles, sinon les trois traces seraient divisibles par 9). Si elles sont opposées, on a $\mathrm{Tr}(C^3) \equiv 0 \mod 9$ et on pose $A_1 = C$, et $(B_1, C_1) = (-A, B)$ (resp. $(B_1, C_1) = (-B, A)$) si $\mathrm{Tr}(A^3) \equiv -2 \mod 9$ (resp. si $\mathrm{Tr}(A^3) \equiv 2 \mod 9$). Si elles ne sont pas opposées, c'est que l'une parmi $\mathrm{Tr}(A^3)$ et $\mathrm{Tr}(B^3)$ est divisible par 9 : quitte à échanger A et B, on peut supposer que c'est A : on pose alors $A_1 = A$. Les classes de congruence de $\mathrm{Tr}(B^3)$ et $\mathrm{Tr}(C^3)$ modulo 9 sont égales : on pose $(B_1, C_1) = (B, C)$ si celle classe est $\overline{2}$, et $(B_1, C_1) = (-C, -B)$ sinon.

(ii) On a $x^3 = x$ pour tout $x \in \mathbf{Z}/3\mathbf{Z}$: pour tout $M \in \mathsf{M}_2(\mathbf{Z})$, on a donc $\dot{M}^3 = \dot{M}$ (parce que la surjection canonique $\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}; a \mapsto \dot{a}$ est un morphisme d'anneaux). Si $M \in \mathsf{SL}_2(\mathbf{Z})$ est tel que $\mathrm{Tr}(M^3) \equiv 2 \mod 9$, on a $\mathrm{Tr}\left(\dot{M}\right) = \mathrm{Tr}\left(\dot{M}^3\right) = 2$ dans $\mathbf{Z}/3\mathbf{Z}$. Comme on a en outre $\det(M) = 1$ donc $\det\left(\dot{M}\right) = 1$ dans $\mathbf{Z}/3\mathbf{Z}$, ce qui implique que

$$\chi_{\dot{M}}(X) = X^2 - \mathrm{Tr}\left(\dot{M}\right)X + \det\left(\dot{M}\right) = X^2 - 2X + 1 = (X-1)^2$$

dans $(\mathbf{Z}/3\mathbf{Z})[X]$.
(iii) Soit $M \in \mathsf{SL}_2(\mathbf{Z})$ tel que $\mathrm{Tr}(M^3) \equiv 2 \mod 9$, d'après la question précédente, on a $\chi_{\dot{M}}(X) = (X-1)^2$ dans $(\mathbf{Z}/3\mathbf{Z})[X]$. On a $\mathrm{Sp}\left(\dot{M}\right) = \{1\} \subset \mathbf{Z}/3\mathbf{Z}$: la matrice $\dot{M}$ est trigonalisable dans $\mathsf{M}_2(\mathbf{Z}/3\mathbf{Z})$, elle est donc semblable à une matrice de la forme $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ avec $k \in \mathbf{Z}/3\mathbf{Z}$.

(iv) Si $k \in \mathbf{Z}/3\mathbf{Z}$, on a $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)^3 = \mathrm{I}_2$: si M est comme dans la question précédente, on a donc $\dot{M}^3 = \mathrm{I}_2$ dans $\mathsf{M}_2(\mathbf{Z}/3\mathbf{Z})$. Cela s'applique aux matrices B_1 et C_1 : on a donc $\dot{B_1}^3 = \dot{C_1}^3 = \mathrm{I}_3$. Comme $\dot{A_1}^3 + \dot{B_1}^3 = \dot{C_1}^3$, cela implique que $\dot{A_1}^3 = 0$ dans $\mathsf{M}_2(\mathbf{Z}/3\mathbf{Z})$. En particulier, on a $\det\left(\dot{A_1}\right) = \det\left(\dot{A_1}\right)^3 = 0$, contredisant le fait que $\det(A_1) = 1$.

(26) (a) Comme $2\alpha \equiv 0 \mod 9$ et $2m \equiv 0 \mod 9$, on a

$$\begin{aligned}\big((4\alpha m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4)\big) &\equiv 2^2 - (-4)^2 \mod 9 \\ &\equiv 6 \mod 9\end{aligned}$$

et donc $(4\alpha m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4) \equiv 0 \mod 3$. La congruence $(**)$ implique donc que $(4xd)^2 - ((2\alpha)^2 - 4)(2yd)^2 \equiv 0 \mod 3$. Comme $2\alpha \equiv 0 \mod 9$, on a en outre $(2\alpha)^2 - 4 \equiv -1 \mod 3$, ce qui implique que $(4xd)^2 + (2yd)^2 \equiv 0 \mod 3$.
(b) Les carrés de $\mathbf{Z}/3\mathbf{Z}$ sont 0 et 1. Si une somme de deux carrés est nulle, c'est que les deux carrés sont nuls : on a donc $4xd \equiv 0 \mod 3$ et $2yd \equiv 0 \mod 3$.
(c) D'après la question précédente, on a $9 \mid (4xd)^2 - ((2\alpha)^2 - 4)(2y)^2$: l'égalité $(**)$ implique donc que $9 \mid d^2\big((4\alpha m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4)\big)$. Comme $(4\alpha m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4) \equiv 6 \mod 9$ d'après la question (a), cela implique que $3 \mid d^2$, et donc $3 \mid d$.
(d) D'après la question (b), on a $3 \mid 4xd = 4r$, ce qui implique $3 \mid r$. On a de même $3 \mid s$. On peut donc écrire $d = 3d'$, $r = 3r'$ et $s = 3s'$ avec $d', r', s' \in \mathbf{Z}$ (et $d' > 0$). On a alors $x = \frac{r'}{d'}$ et $y = \frac{s'}{d'}$, contredisant la minimalité de d.

(27) Soient $U, V \in \mathsf{SL}_2(\mathbf{Z})$ telles que $\mathrm{Tr}(U) = 2\alpha$, $\mathrm{Tr}(B) = 2m$ et $\det(U+V) = 1$. D'après la question (24), il existe $u, v \in \mathbf{Q}$ tels que $\left(\alpha m + \frac{1}{2}\right)^2 - (\alpha^2 - 1)(m^2 - 1) = u^2 - (\alpha^2 - a)v^2$. C'est impossible en vertu de la question (26) : contradiction.

(28) Soit $(A,B,C) \in \mathsf{SL}_2(\mathbf{Z})^3$ une solution à l'équation $X^3+Y^3=Z^3$. D'après la question (25), on sait déjà que $\mathrm{Tr}(A^3) \equiv 0 \mod 9$, $\mathrm{Tr}(B^3) \equiv 0 \mod 9$ et $\mathrm{Tr}(C^3) \equiv 0 \mod 9$. Posons $U = A^3$ et $V = B^3$, et $\alpha = \frac{\mathrm{Tr}(U)}{2}$ et $m = \frac{\mathrm{Tr}(V)}{2}$, de sorte que $2\alpha = \mathrm{Tr}(U) \in \mathbf{Z}$ et $2\alpha \equiv 0 \mod 9$, et de même $2m = \mathrm{Tr}(V) \in \mathbf{Z}$ et $2m \equiv 0 \mod 9$. Comme $U+V = Z^3 \in \mathsf{SL}_2(\mathbf{Z})$, on a $\det(U+V) = 1$. D'après la question précédente, de telles matrices U et V n'existent pas : contradiction. Cela montre que l'équation $X^3+Y^3=Z^3$ n'a pas de solution dans $\mathsf{SL}_2(\mathbf{Z})^3$. Comme dans la question (14), cela implique que l'équation $X^n+Y^n=Z^n$ n'a pas de solution dans $\mathsf{SL}_2(\mathbf{Z})^3$ dès que $3 \mid n$.

(29) Par définition, une matrice $M \in \mathsf{M}_p(\mathbf{R})$ est k-périodique si X^k-1 est un polynôme annulateur. Comme $X^k - 1 = \prod_{a=0}^{k-1} \left(X - e^{\frac{2ia\pi}{k}}\right)$ est à racines simples dans $\mathbf{C}[X]$, cela implique que M est diagonalisable dans $\mathsf{M}_p(\mathbf{C})$.

(30) (a) • D'après le théorème de Cayley-Hamilton, on a $X^2 - \mathrm{Tr}(X)X + \det(X)\,\mathrm{I}_2 = 0$. Comme $X^2 = A$ et $\mathrm{Tr}(X) = -1$, on a $A + X + \det(X)\,\mathrm{I}_2 = 0$. Cela implique que $\mathrm{Tr}(A) + \mathrm{Tr}(X) + 2\det(X) = 0$, *i.e.* $\det(X) = 1$ (du coup l'hypothèse $\det(X) = 1$ de l'énoncé n'est pas nécessaire). On a donc nécessairement $X = -A - \mathrm{I}_2 = -A + C = B$.
• On a $B^3 = \mathrm{I}_2$, donc $X = B$ est 3-périodique, donc *a fortiori* 12-périodique.
(b) On a $B^3 = \mathrm{I}_2$, donc $B^4 = B$: la matrice $Y = B^2 = A$ répond à la question. Comme A est 3-périodique, la matrice $Y = A$ est 3-périodique, donc 12-périodique.
(c) En partant de la relation $A + B = C$, les deux questions précédentes donnent la relation $B^2 + A^2 = C$. Les matrices $X = B$ et $Y = A$ étant 3-périodiques donc 12-périodiques, il suffit de trouver une matrice 12-périodique Z telle que $Z^2 = C$. Géométriquement, la matrice C est la matrice de la rotation d'angle π : il suffit de poser $Z = R := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (la matrice de la rotation d'angle $\frac{\pi}{2}$) : elle est d'ordre 4 donc *a fortiori* d'ordre 12, et le triplet (B,A,R) répond à la question.

(31) Si $n \equiv 2 \mod 12$, on a $B^n = B^2$ (parce que $B^3 = \mathrm{I}_2$), et de même $A^n = A^2$ et $R^n = R^2$ (parce que $R^4 = \mathrm{I}_2$). Cela implique que $B^n + A^n = B^2 + A^2 = R^2 = R^n$ et le triplet (B,A,R) est solution de l'équation $X^n + Y^n = Z^n$.

(32) D'après ce qu'on a vu, on a $B^{-1} = B^2 = A \in \mathsf{SL}_2(\mathbf{Z})$ et de même $A^{-1} = B \in \mathsf{SL}_2(\mathbf{Z})$. Par ailleurs, on a $R^{-1} = R^3 \in \mathsf{SL}_2(\mathbf{Z})$. Si $n \equiv -2 \mod 12$, on a $A^n = (B^{-1})^n = B^2 = A$ et de même $B^n = B$ et $R^n = R^{-2} = R^2 = C$, de sorte que $A^n + B^n = A + B = C = R^2 = R^n$, ce qui montre que le triplet (A,B,R) est solution de l'équation $X^n+Y^n=Z^n$.

(33) Si $n \equiv \pm 1 \mod 6$, on a $2n \equiv \pm 2 \mod 12$, et on a vu plus haut que $A^{2n} + B^{2n} = R^{2n}$ où $R = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Cela implique que le triplet $(B^2, A^2, R^2) = (A,B,C)$ est solution de l'équation $X^n+Y^n=Z^n$.

(34) On discute suivant la classe de n modulo 12. On a vu que si $n \equiv 1 \mod 6$ ou $n \equiv 5 \mod 6$, c'est-à-dire si n est congru à 1, 5, 7 ou 11 modulo 12, alors l'équation $X^n+Y^n=Z^n$ admet au moins une solution dans $\mathsf{SL}_2(\mathbf{Z})^3$. C'est aussi le cas si $n \equiv 2 \mod 12$ ou $n \equiv 10 \mod 12$ en vertu des question (31) et (32). D'après la question (14), il n'y a pas de solution si $4 \mid n$, c'est-à-dire lorsque n est congru à 0, 4 ou 8 modulo 12. De même, la question (28) montre qu'il n'y a pas de solution si $3 \mid n$, c'est-à-dire lorsque n est congru à 0, 3, 6 ou 9 modulo 12. En résumé, l'équation $X^n+Y^n=Z^n$ a une solution dans $\mathsf{SL}_2(\mathbf{Z})^3$ si et seulement si n est congru à 1, 2, 5, 7, 10 ou 11 modulo 12.

(35) Si $k_1, \ldots, k_m$ et $\ell_1, \ldots, \ell_m$ sont des entiers relatifs, on a $\sum_{i=1}^m k_i v_i - \sum_{i=1}^m \ell_i v_i = \sum_{i=1}^m (k_i - \ell_i) v_i \in \mathcal{R}$, ce qui montre que $\mathcal{R}$ est un sous-groupe du groupe additif $\mathbf{Q}^n$.

(36) Soit $d \in \mathbf{N}_{>0}$ tel que $dv_i \in \mathbf{Z}$ pour tout $i \in \{1, \ldots, m\}$. On a alors $d\mathcal{R} = \sum_{i=1}^m \mathbf{Z}\, dv_i \subset \mathbf{Z}$, et c'est un sous-groupe additif de $\mathbf{Z}$. Il est donc de ma forme $a\,\mathbf{Z}$ avec $a \in \mathbf{N}$. On a alors $\mathcal{R} = r\,\mathbf{Z}$ avec $r = \frac{a}{d}$. Sauf s'il est nul, le rationnel r n'est pas unique puisque $-r\,\mathbf{Z} = r\,\mathbf{Z}$.

(37) On a $\pi(\mathcal{R}) = \sum_{i=1}^m \mathbf{Z}\,\pi(v_i) \subset \mathbf{Q}$: d'après la question précédente, il existe $r \in \mathbf{Q}$ tel que $\pi(\mathcal{R} = r\,\mathbf{Z}$. On prend alors $w \in \mathcal{R})$ tel que $\pi(w) = r$.

(38) (a) On a $\pi(x) \in \pi(\mathcal{R}) = \pi(w)\,\mathbf{Z}$: il existe $q \in \mathbf{Z}$ tel que $\pi(x) = q\pi(w)$, *i.e.* $\widetilde{x} := x - qw \in \mathrm{Ker}(\pi) = \mathbf{Q}^{n-1} \times \{0\}$. Comme $x, w \in \mathcal{R}$, on a en outre $\widetilde{x} \in \mathcal{R}$, de sorte que $\widetilde{x} \in \mathcal{R} \cap (\mathbf{Q}^{n-1} \times \{0\})$.

(b) Si $\pi(w)=0$, on a $\mathcal{R}\subset\mathrm{Ker}(\pi)$, et donc $\widetilde{x}=x$. Si $\pi(w)\neq 0$, on a $\pi(x)=q\pi(w)+\pi\big(\widetilde{x}\big)=q\pi(w)$, ce qui montre que $q=\frac{\pi(x)}{\pi(w)}$, et donc $\widetilde{x}=x-\frac{\pi(x)}{\pi(w)}$. Dans tous les cas, $\widetilde{x}$ est unique. *A contrario*, l'entier q n'est unique que lorsque $\pi(w)\neq 0$ (*cf* formule ci-dessus) : lorsque $\pi(w)=0$, il peut être choisi arbitrairement.

(39) Pour tout $i\in\{1,\dots,m\}$, on a $\widetilde{v_i}\in\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$: par $\mathbf{Z}$-linéarité, on a $\sum\limits_{i=1}^{m}\mathbf{Z}\,\widetilde{v_i}\subset\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$. Réciproquement, soit $x\in\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$. Il existe $q\in\mathbf{Z}$ tel que $x=qw+\widetilde{x}$: on a $qw=x-\widetilde{x}\in\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$, d'où $q\pi(w)=\pi(qw)=0$. Si $\pi(w)\neq 0$, on a donc $x=\widetilde{x}$; si $\pi(w)=0$, on a $w=0$ par hypothèse, donc $x=\widetilde{x}$ aussi. Par ailleurs, il existe $k_1,\dots,k_m\in\mathbf{Z}$ tels que $x=\sum\limits_{i=1}^{m}k_iv_i$. Pour tout $i\in\{1,\dots,m\}$, il existe $q_i\in\mathbf{Z}$ tel que $v_i=q_iw+\widetilde{v_i}$, de sorte que

$$x=\Big(\sum_{i=1}^{m}k_iq_i\Big)w+\sum_{i=1}^{m}k_i\widetilde{v_i}.$$

Comme $\sum\limits_{i=1}^{m}k_iq_i\in\mathbf{Z}$ et $\sum\limits_{i=1}^{m}k_i\widetilde{v_i}\in\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$, on a $\widetilde{x}=\sum\limits_{i=1}^{m}k_i\widetilde{v_i}$ par unicité de $\widetilde{x}$ (*cf* question précédente). On a donc $x=\sum\limits_{i=1}^{m}k_i\widetilde{v_i}\in\sum\limits_{i=1}^{m}\mathbf{Z}\,\widetilde{v_i}$, ce qui montre l'inclusion réciproque.

(40) L'hypothèse de récurrence est : « un sous-groupe $\mathcal{R}\subset\mathbf{Q}^n$ engendré par un nombre fini d'éléments est libre de rang fini ». Le cas $n=1$ n'est autre que la question (36). Supposons $n>1$. Choisissons $w\in\mathcal{R}$ comme dans la question (37). D'après la question précédente, $\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$ est un groupe abélien de type fini : par hypothèse de récurrence, il existe $r\in\mathbf{N}$ et $\overline{u}_1,\dots,\overline{u}_r\in\mathbf{Q}^{n-1}$ tels que $\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})=\bigoplus\limits_{i=1}^{r}\mathbf{Z}\,\overline{u}_i$. Averc les notations des questions qui précèdent, pour tout $i\in\{1,\dots,r\}$, il existe $u_i\in\mathcal{R}$ tel que $\overline{u}_i=\widetilde{u}_i$.
<u>Premier cas</u> : $\mathcal{R}\subset\mathbf{Q}^{n-1}\times\{0\}$. On a alors $\mathcal{R}=\bigoplus\limits_{i=1}^{r}\mathbf{Z}\,\overline{u}_i$, et on a fini (avec $p=r$ et $u_i=\overline{u_i}$ pour tout $i\in\{1,\dots,r\}$).
<u>Second cas</u> : $\mathcal{R}\not\subset\mathbf{Q}^{n-1}\times\{0\}$. Si $x\in\mathcal{R}$, il existe $q\in\mathbf{Z}$ tel que $x=qw+\widetilde{x}$. Par ailleurs, on a $\widetilde{x}\in\mathcal{R}\cap(\mathbf{Q}^{n-1}\times\{0\})$: il existe $q_1,\dots,q_r\in\mathbf{Z}$ uniques tels que $\widetilde{x}=\sum\limits_{i=1}^{r}q_i\widetilde{u}_i$, ce qui montre que $x=qw+\sum\limits_{i=1}^{r}q_iu_i$. Par ailleurs, si $x=0$, on a $\widetilde{x}=0$ (par unicité, *cf* question (38)(b)), ce qui implique que $q_1=\cdots=q_r=0$, et donc $0=\pi(x)=q\pi(w)$ d'où $q=0$ puisque $\pi(w)\neq 0$ (parce que $\mathcal{R}\not\subset\mathbf{Q}^{n-1}\times\{0\}$). Cela montre que la famille $(u_1,\dots,u_r,w)$ est libre dans le $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^n$. On a donc $\mathcal{R}\subset\bigoplus\limits_{i=1}^{p}\mathbf{Z}\,u_i$ en posant $p=r+1$ et $u_p=w$. L'inclusion réciproque est triviale : on a $\mathcal{R}=\bigoplus\limits_{i=1}^{p}\mathbf{Z}\,u_i$, ce qui achève la récurrence.

(41) Par hypothèse, on a $\mathrm{Vect}_{\mathbf{Q}}(u_1,\dots,u_p)=\mathrm{Vect}_{\mathbf{Q}}(\mathcal{R})=\mathbf{Q}^n$, ce qui montre que la famille $(u_1,\dots,u_p)$ est génératrice de $\mathbf{Q}^n$: pour conclure, il suffit de montrer qu'elle est libre. Soit $\lambda_1,\dots,\lambda_p\in\mathbf{Q}$ tels que $\sum\limits_{i=1}^{p}\lambda_iu_i=0$. Il existe $d\in\mathbf{N}_{>0}$ tel que $d\lambda_i\in\mathbf{Z}$ pour tout $i\in\{1,\dots,p\}$ (on prend pour d un dénominateur commun de $\lambda_1,\dots,\lambda_p$). On a alors $\sum\limits_{i=1}^{p}(d\lambda_i)u_i=0$. Comme la somme $\mathcal{R}=\bigoplus\limits_{i=1}^{p}\mathbf{Z}\,u_i$ est directe, cela implique que $d\lambda_i=0$ et donc que $\lambda_i=0$ pour tout $i\in\{1,\dots,p\}$, ce qui achève la preuve. Comme $\mathbf{Q}^n$ est de dimension n sur $\mathbf{Q}$, on a donc $p=n$.

(42) (a) On a $\mathrm{I}_p\in G$, donc $e_i=\mathrm{I}_p\,e_i\in\mathcal{M}\subset H$ pour tout $i\in\{1,\dots,p\}$.
(b) Si $y\in\mathcal{M}\setminus\{0\}$, il existe $M\in G$ et $i\in\{1,\dots,p\}$ tel que $y=\pm Me_i$: si $A\in G$, on a $Ay=\pm AMe_i\in\mathcal{M}$ parce que $AM\in G$ vu que G est un sous-groupe de $\mathsf{SL}_p(\mathbf{Q})$. Cela prouve de $\mathcal{M}$ est stable par G. Si $h\in H$, il existe $q\in\mathbf{N}$ et $y_1,\dots,y_q\in\mathcal{M}$ tels que $h=y_1+\cdots+y_q$. Si $A\in G$, on a alors $Ah=Ay_1+\cdots+Ay_q\in H$ parce que $Ay_1,\dots,Ay_q\in\mathcal{M}$ d'après ce qui précède.
(c) Par hypothèse, on a $dM\in\mathsf{M}_p(\mathbf{Z})$. Comme $e_j\in\mathbf{Z}^p$, on a $dMe_j\in\mathbf{Z}^p$: il existe $\lambda_1,\dots,\lambda_p\in\mathbf{Z}$ uniques tels que $dMe_j=(\lambda_1,\dots,\lambda_p)=\sum\limits_{i=1}^{p}\lambda_ie_i$. Pour tout $i\in\{1,\dots,p\}$, soit $\lambda_i=q_id+r_i$ (avec $q_i\in\mathbf{Z}$ et $r_i\in\{0,\dots,d-1\}$ la divison euclidienne de λ_i par d. On a $Me_j=\frac{1}{d}dMe_j=\sum\limits_{i=1}^{p}q_ie_i+\frac{1}{d}\sum\limits_{i=1}^{p}r_ie_i$.

(d) Observons que $\mathbf{Z}^p \subset H$. D'après la question précédente, on a en outre $\mathcal{M} \subset \frac{1}{d}\,\mathbf{Z}^p$, et donc $H \subset \frac{1}{d}\,\mathbf{Z}^d$ (par additivité). On a donc les inclusions $\mathbf{Z}^p \subset H \subset \frac{1}{d}\,\mathbf{Z}^p$. On dispose de la surjection canonique $\kappa\colon \frac{1}{d}\,\mathbf{Z}^p \to \frac{1}{d}\,\mathbf{Z}^p \,/\, \mathbf{Z}^p$. L'image $\kappa(H)$ est un sous-groupe du groupe fini $\frac{1}{d}\,\mathbf{Z}^p \,/\, \mathbf{Z}^p \simeq (\mathbf{Z}\,/d\,\mathbf{Z})^p$: elle est finie : il existe donc $v_1, \ldots, v_r \in H$ tels que $\kappa(H) = \{\kappa(v_1), \ldots, \kappa(v_r)\}$. On a donc $H = \sum_{i=1}^{m} \mathbf{Z}\, v_i$ en posant $m = r + p$ et $v_{r+j} = e_j$ pour tout $j \in \{1, \ldots, p\}$. La famille $\{v_1, \ldots, v_m\}$ est génératrice du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^p$ car elle contient la base $e_1, \ldots, e_p$.
(e) D'après la question précédente et des question (40) & (41), il existe une $\mathbf{Q}$-base $(u_1, \ldots, u_p)$ de $\mathbf{Q}^p$ telle que $H = \bigoplus_{i=1}^{p} \mathbf{Z}\, u_i$. Par définition, pour tout $i \in \{1, \ldots, p\}$ et tout $M \in G$, on a $Mu_i \in H = \bigoplus_{j=1}^{p} \mathbf{Z}\, u_j$.
(f) Soit $F \in \mathsf{GL}_p(\mathbf{Q})$ la matrice de changement de base de la base canonique vers la base $\mathfrak{B} := (u_1, \ldots, u_p)$ de la question précédente. Pour tout $M \in G$, la matrice $F^{-1}MF$ est la matrice dans la base $\mathfrak{B}$ de l'endomorphisme associé à M dans la base canonique. D'après la question précédente, cette matrice est à coefficients entiers, *i.e.* $F^{-1}MF \in \mathsf{M}_p(\mathbf{Z})$. Par ailleurs, on a $\det(F^{-1}MF) = \det(M) = 1$, donc $F^{-1}MF \in \mathsf{SL}_p(\mathbf{Z})$.

(43) (a) On a $p = 2$: d'après le théorème de Cayley-Hamilton, on a $A^2 - \mathrm{Tr}(A)A + \det(A)\,\mathrm{I}_2 = 0$. Comme $\det(A) = 1$, on a $A^{-1} = \mathrm{Tr}(A)\,\mathrm{I}_2 - A \in K$ vu que $\mathrm{Tr}(A) \in \mathbf{Z}$ par hypothèse. On a bien sûr de même $B^{-1} \in K$.
(b) La définition de G et la question précédente impliquent qu'il suffit de prouver que K est stable par produit dans $\mathsf{M}_2(\mathbf{Q})$. Il est suffisant de montrer qu'il est stable par la multiplication par A et par la multiplication par B. Là encore, cela repose sur le théorème de Cayley-Hamilton : on a $A^2 = \mathrm{Tr}(A)A - \mathrm{I}_2$, $B^2 = \mathrm{Tr}(B)B - \mathrm{I}_2$, $(AB)^2 = \mathrm{Tr}(AB)AB - \mathrm{I}_2$ et $(BA)^2 = \mathrm{Tr}(BA)BA - \mathrm{I}_2 = \mathrm{Tr}(AB)BA - \mathrm{I}_2$. les calculs sont résumés dans le tableau suivant :

M	A	B	AB	BA	ABA	BAB
AM	$\mathrm{Tr}(A)A - \mathrm{I}_2$	AB	$\mathrm{Tr}(A)AB - B$	ABA	$\mathrm{Tr}(A)ABA - BA$	$\mathrm{Tr}(AB)AB - \mathrm{I}_2$
BM	BA	$\mathrm{Tr}(B)B - \mathrm{I}_2$	BAB	$\mathrm{Tr}(B)BA - A$	$\mathrm{Tr}(AB)BA - \mathrm{I}_2$	$\mathrm{Tr}(B)BAB - AB$

(c) Il existe $d \in \mathbf{N}_{>0}$ tel que $\{\mathrm{I}_2, A, B, AB, BA, ABA, BAB\} \subset \frac{1}{d}\,\mathsf{M}_2(\mathbf{Z})$, de sorte que $dK \subset \mathsf{M}_2(\mathbf{Z})$ par $\mathbf{Z}$-linéarité. On a *a fortiori* $dG \subset \mathsf{M}_2(\mathbf{Z})$ en vertu de la question précédente.

(44) (a) Supposons (i) : on a $\mathrm{Tr}(A) = \mathrm{Tr}(F^{-1}AF) \in \mathbf{Z}$, $\mathrm{Tr}(B) = \mathrm{Tr}(F^{-1}BF) \in \mathbf{Z}$ vu que $F^{-1}AF$ et $F^{-1}BF$ sont à coefficients entiers. Par ailleurs, on a $\det(A+B) = \det(F^{-1}(A+B)F) = \det(F^{-1}AF + F^{-1}BF) \in \mathbf{Z}$. Réciproquement, supposons (ii). D'après le théorème de Cayley-Hamilton (toujours lui...), on a

$$\begin{aligned} A^2 - \mathrm{Tr}(A)A + \mathrm{I}_2 &= 0 \\ B^2 - \mathrm{Tr}(B)B + \mathrm{I}_2 0 & \\ (A+B)^2 - \mathrm{Tr}(A+B)(A+B) + \det(A+B)\,\mathrm{I}_2 &= 0 \end{aligned}$$

Comme $(A+B)^2 = A^2 + AB + BA + B^2$, cela implique que

$$\mathrm{Tr}(A)A - \mathrm{I}_2 + AB + BA + \mathrm{Tr}(B)B - \mathrm{I}_2 - (\mathrm{Tr}(A) + \mathrm{Tr}(B))(A+B) + \det(A+B)\,\mathrm{I}_2 = 0.$$

En prenant la trace, on a $\mathrm{Tr}(A)^2 + 2\,\mathrm{Tr}(AB) + \mathrm{Tr}(B)^2 - 4 - (\mathrm{Tr}(A) + \mathrm{Tr}(B))^2 + 2\det(A+B) = 0$, soit encore

$$\mathrm{Tr}(AB) = 2 + \mathrm{Tr}(A)\,\mathrm{Tr}(B) - \det(A+B) \in \mathbf{Z}\,.$$

D'après la question (43), cela implique l'existence de $d \in \mathbf{N}_{>0}$ tel que $dG \subset \mathsf{M}_2(\mathbf{Z})$. La question (42) s'applique donc : il existe $F \in \mathsf{GL}_2(\mathbf{Q})$ telle que $(\forall M \in G)\; F^{-1}MF \in \mathsf{SL}_2(\mathbf{Z})$, en particulier on a (i).
(b) Montrons par récurrence forte sur $n \in \mathbf{N}$ que $\mathrm{Tr}(X^n) \in \mathbf{Z}$. C'est trivial si $n = 0$ et c'est l'hypohèse si $n = 1$: supposons $n > 1$. D'après le théorème de Cayley-Hamilton (décidément...), on a $X^2 - \mathrm{Tr}(X)X + \mathrm{I}_2$: on a donc $X^n - \mathrm{Tr}(X)X^{n-1} + X^{n-2} = 0$, et donc $\mathrm{Tr}(X^n) = \mathrm{Tr}(X)\,\mathrm{Tr}(X^{n-1}) - \mathrm{Tr}(X^{n-2}) \in \mathbf{Z}$ (vu que $\mathrm{Tr}(X) \in \mathbf{Z}$ et $\mathrm{Tr}(X^{n-2}) \in \mathbf{Z}$ et $\mathrm{Tr}(X^{n-1}) \in \mathbf{Z}$ par hypothèse de récurrence). Cela montre que si $A = X^n$, alors $\mathrm{Tr}(A) \in \mathbf{Z}$. De même, si $B = Y^n$, on a bien entendu $\mathrm{Tr}(B) \in \mathbf{Z}$. Par ailleurs, on a $\det(A+B) = \det(Z^n) = \det(Z)^n = 1 \in \mathbf{Z}$. D'après la question précédente, il existe $F \in \mathsf{GL}_2(\mathbf{Q})$ telle que $F^{-1}AF \in \mathsf{SL}_2(\mathbf{Z})$ et $F^{-1}BF \in \mathsf{SL}_2(\mathbf{Z})$. Si $X_1 = F^{-1}XF$, $Y_1 = F^{-1}YF$ et $Z_1 = F^{-1}ZF$, l'égalité $X^n + Y^n = Z^n$ conjuguée par F donne $X_1^n + Y_1^n = Z_1^n$. Par ailleurs, on a $X_1^n = F^{-1}AF \in \mathsf{SL}_2(\mathbf{Z})$ et $Y_1^n = F^{-1}BF \in \mathsf{SL}_2(\mathbf{Z})$, ce qui implique que $Z_1^n = X_1^n + Y_1^n \in \mathsf{M}_2(\mathbf{Z})$. Comme $\det(Z_1^n) = \det(Z_1)^n = \det(Z)^n = 1$, on a en fait $Z_1^n \in \mathsf{SL}_2(\mathbf{Z})$, ce qui conclut.