Agrégation externe de mathématiques

Mathématiques générales 2024

I. Préliminaires

I.A. Commutation et trigonalisation simultanée

(1) (a) Soit $x \in \mathrm{Ker}(P(u))$. Comme $u \circ v = v \circ u$, on a $P(u) \circ v = v \circ P(u)$, donc $P(u)(v(x)) = v(P(u)(x)) = 0$, ce qui montre que $v(x) \in \mathrm{Ker}(P(u))$, et donc que $\mathrm{Ker}(P(u))$ est stable par v.

(1) (b) Soit $u \in \mathcal{L}$ qui n'est pas une homothétie. Comme u est trigonalisable, il a une valeur propre $\lambda \in K$: posons $F = \mathrm{Ker}(u - \lambda\,\mathsf{id}_E)$. On a bien sûr $F \neq \{0\}$, et comme $u \neq \lambda\,\mathsf{id}_E$ (puisque u n'est pas une homothétie), on a $F \neq E$. Enfin, F est stable par tous les éléments de $\mathcal{L}$ en vertu de la question précédente.

(2) (a) • Comme F est stable par u, on dispose de $u_{|F} \in \mathcal{L}(F)$: notons $A_u \in \mathcal{M}_m(K)$ la matrice de ce dernier dans la base $(e_1, \dots, e_m)$ de F. Posons $F' = \mathrm{Vect}(e_{m+1}, \dots, e_n)$ et notons $i \colon F' \to E$ (resp. $\pi \colon E \to F'$) l'inclusion (resp. le projecteur sur F parallèlement à F'. On dispose de $\pi \circ u \circ i \in \mathcal{L}(F')$ et $(\mathsf{id}_E - \pi) \circ u \circ i \in \mathcal{L}(F', F)$: notons $C_u \in \mathcal{M}_{n-m}(K)$ et $B_u \in \mathcal{M}_{m,n-m}(K)$ leurs matrices respectives dans les bases $(e_{m+1}, \dots, e_n)$ et $(e_1, \dots, e_m)$ de F' et F respectivement. La matrice de u dans la base $\mathbf{e} = (e_1, \dots, e_n)$ est alors $M_u = \left(\begin{smallmatrix} A_u & B_u \\ 0 & C_u \end{smallmatrix}\right)$ (écriture par blocs).
• Soient $u, v \in \mathcal{L}$. Comme $u \circ v = v \circ u$, on a $M_u M_v = M_v M_u$. Le produit matriciel par blocs implique que $A_u A_v = A_v A_u$ et $C_u C_v = C_v C_u$.

(2) (b) Avec les notations de la question précédente, on a

$$\begin{aligned}\chi_u &= \det(X\,\mathsf{id}_E - u) = \det(X\,\mathrm{I}_n - M_u) = \det\begin{pmatrix} X\,\mathrm{I}_m - A_u & -B_u \\ 0 & X I_{n-m} - C_u \end{pmatrix} \\ &= \det(X\,\mathrm{I}_m - A_u)\det(X\,\mathrm{I}_{n-m} - C_u) = \chi_{A_u}\chi_{C_u}\end{aligned}$$

puisque $X\,\mathrm{I}_n - M_u$ est triangulaire supérieure par blocs. Comme u est trigonalisable, son polynôme caractéristique χ_u est scindé dans $K[X]$: il en est de même des polynômes χ_{A_u} et χ_{C_u}. Cela implique que les matrices A_u et C_u sont trigonalisables.

(3) (a) On procède par récurrence forte. Notons $\mathscr{P}(n)$ la propriété : « Pour tout K-espace vectoriel E de dimension n et toute partie commutative $\mathcal{L} \subset \mathcal{L}(E)$ dont tous les éléments sont des trigonalisables, il existe une base $\mathbf{e}$ de E telle que, pour tout $u \in \mathcal{L}$, la matrice de u dans $\mathbf{e}$ appartienne à $\mathcal{T}_n(K)$ ». C'est trivial lorsque $n = 1$. Soit $n > 1$ tel que $\mathscr{P}(m)$ est vraie pour tout $m \in \{1, \dots, n-1\}$: montrons que $\mathscr{P}(n)$ est vérifiée. Soient donc E un K-espace vectoriel de dimension n et $\mathcal{L} \subset \mathcal{L}(E)$ une partie commutative dont tous les éléments sont trigonalisables : montrons qu'elle est co-trigonalisable. C'est trivial si $\mathcal{L}$ n'est constituée que d'homothéties (toute base de E est une base de co-trigonalisation) : supposons désormais que $\mathcal{L}$ contient un élément qui n'est pas une homothétie. D'après la question (1) (b), il existe un sous-espace F de E stable par tous les éléments de $\mathcal{L}$. Fixons alors une base $\mathbf{e} = (e_1, \dots, e_n)$ de E telle que $(e_1, \dots, e_m)$ soit une base de F. D'après la question (2) (a), pour tout $u \in \mathcal{L}$, la matrice de u dans $\mathbf{e}$ s'écrit $M_u = \left(\begin{smallmatrix} A_u & B_u \\ 0 & C_u \end{smallmatrix}\right)$ avec $A_u \in \mathcal{M}_m(K)$ et $C_u \in \mathcal{M}_{n-m}(K)$. Posons alors $\mathcal{L}' = \{A_u\}_{u \in \mathcal{L}} \subset \mathcal{M}_m(K)$ et $\mathcal{L}'' = \{C_u\}_{u \in \mathcal{L}} \subset \mathcal{M}_{n-m}(K)$. D'après la question (2) (a), les parties $\mathcal{L}' \subset \mathcal{M}_m(K)$ et $\mathcal{L}'' \subset\subset \mathcal{M}_{n-m}(K)$ sont commutatives. Par ailleurs, elles sont constituées de matrices trigonalisables en vertu de la question (2) (b). Comme $1 \leq m < n$ et $1 \leq n - m < n$ (parce que $\{0\} \subsetneq F \subsetneq E$), on peut appliquer l'hypothèse de récurrence à $\mathcal{L}' \subset \mathcal{M}_m(K) \simeq \mathcal{L}(K^m)$ et $\mathcal{L}'' \subset \mathcal{M}_{n-m}(K) \simeq \mathcal{L}(K^{n-m})$: il existe des bases $(\varepsilon_1, \dots, \varepsilon_m)$ et $(\varepsilon_{m+1}, \dots, \varepsilon_n)$ de F et $F' = \mathrm{Vect}(e_{m+1}, \dots, e_n)$ respectivement telles que pour tout $u \in \mathcal{L}$, la matrice de $u_{|F}$ (resp. $\pi \circ u \circ i$, avec les notations de la question (2) (a)) sans $(\varepsilon_1, \dots, \varepsilon_m)$ (resp. $(\varepsilon_{m+1}, \dots, \varepsilon_n)$) soit triangulaire supérieure. La base $\mathbf{e}' = (\varepsilon_1, \dots, \varepsilon_n)$ de E vérifie alors la condition demandée.

(3) (b) Posons $A_0 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ et $B_0 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Posons $A = \left(\begin{smallmatrix} A_0 & 0 \\ 0 & \mathrm{I}_{n-2} \end{smallmatrix}\right) \in \mathcal{T}_n(K)$ et $B = \left(\begin{smallmatrix} B_0 & 0 \\ 0 & \mathrm{I}_{n-2} \end{smallmatrix}\right) \in \mathcal{T}_n(K)$. On a $A_0 B_0 = \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right)$ et $B_0 A_0 = 0$, donc $A_0 B_0 \neq B_0 A_0$: on a *a fortiori* $AB \neq BA$. Cela montre que la réciproque

à la propriété démontrée dans la question précédente est fausse : la famille $\mathcal{L} = \{A, B\}$ est cotrigonalisable, mais pas commutative.

(3) (c) Montrons par récurrence sur n que $u_n \circ \cdots \circ u_1 = 0$. C'est trivial lorque $n = 1$: supposons $n > 1$. Posons $\mathcal{L} = \{u_1, \ldots, u_n\}$. Comme $u_1, \ldots, u_n$ sont nilpotents, ils sont trigonalisables. Comme ils commutent deux à deux, $\mathcal{L}$ est commutative. D'après la question (3) (a), elle est co-trigonalisable : soit $\mathbf{e} = (e_1, \ldots, e_n)$ une base de cotrigonalisation. Le sous-espace $Ke_1 \subset E$ étant stable par tous les éléments de $\mathcal{L}$, la matrice de u_k dans la base $\mathbf{e}$ s'écrit $M_{u_k} = \left(\begin{smallmatrix} 0 & L_{u_k} \\ 0 & C_{u_k} \end{smallmatrix}\right)$ (avec $L_{U-k} \in \mathcal{M}_{1,n-1}(K)$ et $C_{u_k} \in \mathcal{M}_{n-1}(K)$, *cf* question (2) (a) ; on a $A_{u_k} = 0$ parce que $u_k(e_1) = 0$) pour tout $k \in \{1, \ldots, n\}$. Si $k, \ell \in \{1, \ldots, n\}$, les matrices C_{u_k} et C_{u_ℓ} commutent (*cf* question (2) (a) encore) et sont nilpotentes : l'hypothèse de récurrence appliquée à $C_{u_1}, \ldots, C_{u_{n-1}}$ (vues comme endomorphismes de K^{n-1}) implique que $C_{u_{n-1}} \cdots C_{u_1} = 0$: la matrice du composé $u_{n-1} \circ \cdots \circ u_1$ est donc de la forme $\left(\begin{smallmatrix} 0 & L \\ 0 & 0 \end{smallmatrix}\right)$ avec $L \in \mathcal{M}_{1,n-1}(K)$ (produit matriciel par blocs). La matrice du composé $u_n \circ \cdots \circ u_1$ est alors le produit $\left(\begin{smallmatrix} 0 & B_{u_n} \\ 0 & C_{u_n} \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & L \\ 0 & 0 \end{smallmatrix}\right) = 0$ (produit matriciel par blocs encore). Cela montre que $u_n \circ \cdots \circ u_1 = 0$ et achève la récurrence.

Remarque. Autre rédaction. Soit $\mathbf{e} = (e_1, \ldots, e_n)$ une base de cotrigonalisation de $u_1, \ldots, u_n$. Pour $i \in \{0, 1, \ldots, n\}$, posons $E_i = \mathrm{Vect}(e_1, \ldots, e_i)$ (en particulier on a $E_0 = \{0\}$ et $E_n = E$). Pour tout $k \in \{1, \ldots, n\}$, la matrice $\mathcal{M}_{\mathbf{e}}(u_k)$ est triangulaire supérieure à coefficients diagonaux nuls : cela implique que $u_k(E_i) \subset E_{i-1}$ pour tout $i \in \{1, \ldots, n\}$. Il en résulte que $(u_k \circ \cdots \circ u_1)(E) \subset E_{n-k}$ pour tout $k \in \{1, \ldots, n\}$, en particulier que $(u_n \circ \cdots \circ u_1)(E) = E_0\{0\}$, *i.e.* que $u_n \circ \cdots \circ u_1 = 0$.

(4) Choisissons une base $\mathbf{e}$ de E . Cette dernière fournit des isomorphismes $f_0 \colon E \xrightarrow{\sim} \mathbf{R}^n$ et $f \colon \mathcal{L}(E) \xrightarrow{\sim} \mathcal{M}_n(\mathbf{R})$ (où $n = \dim_{\mathbf{R}}(E)$). On dispose alors de la partie commutative $f(\mathcal{L}) \subset \mathcal{M}_n(\mathbf{R}) \subset \mathcal{M}_n(\mathbf{C})$. Comme $\mathbf{C}$ est algébriquement clos, tous les éléments de $\mathcal{M}_n(\mathbf{C})$ sont trigonalisables. D'après la question (3) (a), la partie $f(\mathcal{L})$ est co-trigonalisable dans $\mathcal{M}_n(\mathbf{C})$. Le premier vecteur $e \in \mathbf{C}^n$ d'une base de co-trigonalisation est alors un vecteur propre commun à tous les éléments de $f(\mathcal{L})$. Écrivons $e = x + iy$ avec $x, y \in \mathbf{R}^n$. Comme $e \neq 0$, on a $x \neq 0$ ou $y \neq 0$. Par ailleurs, si $u \in \mathcal{L}$, il existe $\lambda \in \mathbf{C}$ tel que $f(u)(e) = \lambda e$. Écrivons $\lambda = a + ib$ avec $a, b \in \mathbf{R}$. On a donc $f(u)(x + iy) = (a + ib)(x + iy)$, soit $f(u)(x) + if(u)(y) = ax - by + i(bx + ay)$: comme $f(u) \in \mathcal{M}_n(\mathbf{R})$, on a donc

$$\begin{cases} f(u)(x) = ax - by \\ f(u)(y) = bx + ay \end{cases}$$

en séparant partie réelle et partie imaginaire. Cela montre que $\mathrm{Vect}(x, y) \subset \mathbf{R}^n$ est stable par $f(u)$ pour tout $u \in \mathcal{L}$. Comme x et y ne sont pas tous les deux nuls, on a $\dim_{\mathbf{R}}(\mathrm{Vect}(x, y)) \in \{1, 2\}$. Dans tous les cas, $f_0^{-1}(\mathrm{Vect}(x, y))$ est une droite ou un plan stable par tous les éléments de $\mathcal{L}$.

I.B. Sous-groupes abéliens de $\mathcal{O}_2(\mathbf{R})$

(5) (a) Soit $G \subset \mathbb{U}$ un sous-groupe d'ordre n. D'après le théorème de Lagrange, on a $z^n = 1$ pour tout $z \in G$, ce qui montre que $G \subset \mathbb{U}_n$. Comme $\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}}\right\}_{0 \leq k < n}$ est d'ordre n, cela montre que $G = \mathbb{U}_n$, et que $\mathbb{U}_n$ est le seul sous-groupe d'ordre n de $\mathbb{U}$.

(5) (b) Les morphismes de groupes $R \colon \mathbf{R} \to \mathsf{SO}_2(\mathbf{R})$; $t \mapsto \left(\begin{smallmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{smallmatrix}\right)$ et $\varepsilon \colon \mathbf{R} \to \mathbf{U}$; $t \mapsto e^{it}$ sont surjectifs et $\mathrm{Ker}(f) = \mathrm{Ker}(g) = 2\pi\,\mathbf{Z}$: ils induisent des isomorphismes $\widetilde{R} \colon \mathbf{R}/2\pi\,\mathbf{Z} \xrightarrow{\sim} \mathsf{SO}_2(\mathbf{R})$ et $\widetilde{\varepsilon} \colon \mathbf{R}/2\pi\,\mathbf{Z} \xrightarrow{\sim} \mathbb{U}$. On en déduit l'isomorphisme $\widetilde{R} \circ \widetilde{\varepsilon}^{-1} \colon \mathbb{U} \xrightarrow{\sim} \mathsf{SO}_2(\mathbf{R})$. Il envoie $e^{it} = a + ib \in \mathbb{U}$ sur $R(t) = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. La question précédente implique donc que $\mathsf{SO}_2(\mathbf{R})$ contient un unique sous-groupe d'ordre n, et c'est $\mathcal{R} = \widetilde{R} \circ \widetilde{\varepsilon}^{-1}(\mathbb{U}_n)$. Ses éléments sont les matrices de la forme $R\left(\frac{2k\pi}{n}\right) = \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix}$ pour $k \in \{0, \ldots, n-1\}$.

(6) (a) • Observons que si $t \in \mathbf{R}$, on a $SR(t)S = R(-t)$, et donc $R(t)S = SR(-t)$. On a $OS \in \mathsf{SO}_2(\mathbf{R})$: il existe $t \in \mathbf{R}$ tel que $OS = R(t)$, *i.e.* $O = R(t)S = R(t/2)^2 S = R(t/2)SR(-t/2) = R(t/2)SR(t/2)^{-1}$, ce qui montre que O est conjugué à S dans $\mathsf{O}_2(\mathbf{R})$.

Remarque. Ce qui précède résulte immédiatement de la réduction des matrices orthogonales. L'approche adoptée ici ne nécessite aucun prérequis.

• Si $M \in \mathcal{O}_2(\mathbf{R})$ commute à S, les sous-espace propres de S sont stables par M : la matrice M est diagonale. Étant orthogonale, ses coefficients diagonaux appartiennent à $\{\pm 1\}$. Cela signifie que $M \in \{\pm \mathrm{I}_2, \pm S\}$: le centralisateur de S dans $\mathcal{O}_2(\mathbf{R})$ est $\{\pm \mathrm{I}_2, \pm S\}$.

(6) (b) Comme $\mathsf{SO}_2(\mathbf{R}) \simeq \mathbb{U}$ est commutatif, il en est de même de ses sous-groupes. Il s'agit de d'étudier les sous-groupes commutatifs $G \leq \mathcal{O}_2(\mathbf{R})$ qui ne sont pas inclus dans $\mathsf{SO}_2(\mathbf{R})$. Un tel sous-groupe contient un

élément $O \in \mathcal{O}_2(\mathbf{R}) \setminus \mathsf{SO}_2(\mathbf{R})$. D'après la question précédente, il existe $P \in \mathsf{O}_2(\mathbf{R})$ (et même $P \in \mathsf{SO}_2(\mathbf{R})$) telle que $S \in P^{-1}GP$. Comme G est commutatif, il en est de même de $P^{-1}GP$: ce dernier est donc un sous-groupe du centralisateur de S dans $\mathcal{O}_2(\mathbf{R})$. D'après la question précédente, ce dernier est $\{\pm \mathrm{I}_2, \pm S\}$: comme $P^{-1}GP \not\subset \{\pm \mathrm{I}_2\}$ (parce que $G \not\subset \mathsf{SO}_2(\mathbf{R})$), c'est $\{\mathrm{I}_2, S\}$, $\{\mathrm{I}_2, -S\}$ ou $\{\pm \mathrm{I}_2, \pm S\}$. Comme $-S$ est conjugué à S dans $\mathcal{O}_2(\mathbf{R})$ (*cf* question (5) (b)), cela montre que G est conjugué, dans $\mathcal{O}_2(\mathbf{R})$, à $\{\mathrm{I}_2, S\}$ ou à $\{\pm \mathrm{I}_2, \pm S\}$.

(7) (a) On a $R\left(\frac{\pi}{3}\right) = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$, donc $R\left(\frac{\pi}{3}\right)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$. On a $P = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} \in \mathsf{GL}_2(\mathbf{R})$, et $P^{-1}R\left(\frac{\pi}{3}\right)P$ est de la forme $\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$: c'est la matrice compagnon associée au polynôme $X^2 - aX - b = \chi_{R\left(\frac{\pi}{3}\right)} = X^2 - X + 1$. On a donc $a = 1$ et $b = -1$, de sorte que $P^{-1}R\left(\frac{\pi}{3}\right)P = A$.

(7) (b) On a $\mathcal{R}_6 = \left\langle R\left(\frac{\pi}{3}\right)\right\rangle$: d'après la question précédente, il est conjugué, dans $\mathsf{GL}_2(\mathbf{R})$, au groupe $\langle A \rangle \leq \mathsf{GL}_2(\mathbf{Q})$.

II. Sous-algèbres commutatives de dimension maximale de $\mathcal{M}_n(K)$

II.A. Les sous-algèbres $\mathcal{A}_n(K)$ et $\mathcal{A}_n^i(K)$

(8) (a) • Supposons n pair : on écrit $n = 2m$. L'application $\mathcal{M}_m(K) \to \mathcal{V}_n(K)$; $A \mapsto \begin{pmatrix} 0 & A \\ 0 & a \end{pmatrix}$ est un isomorphisme. Cela implique que

$$\dim_K(\mathcal{V}_n(K)) = \dim_K(\mathcal{M}_m(K)) = m^2 = \left(\tfrac{n}{2}\right)^2 = \tfrac{n^2}{4} = b(n).$$

• Supposons n impair et $n \geq 3$: écrivons $n = 2m + 1$. On a $\frac{n^2}{4} = m^2 + m + \frac{1}{4}$, donc $b(n) = m^2 + m$. Par ailleurs, l'application $\mathcal{M}_{m,m+1}(K) \to \mathcal{V}_n^1(K)$; $A \mapsto \begin{pmatrix} 0 & A \\ 0 & a \end{pmatrix}$ est un isomorphisme. Cela implique que

$$\dim_K(\mathcal{V}_n^1(K)) = \dim_K(\mathcal{M}_{m,m+1}(K)) = m(m+1) = b(n).$$

Le raisonnement est le même pour $\mathcal{V}_n^2(K)$.

(8) (b) Le produit des matrices par blocs montre que si $M, M' \in \mathcal{V}_n(K)$, alors $MM' = 0$. C'est encore le cas dans $\mathcal{V}_n^i(K)$ lorsque n est impair et $i \in \{1, \ldots, 2\}$.

(9) (a) • On a déjà $\mathcal{A} = \mathrm{Vect}(\mathrm{I}_n, \mathcal{V})$, ce qui montre que $\mathcal{A}$ est un sous-K-espace vectoriel de $\mathcal{M}_n(K)$. Par ailleurs, si $X, X' \in \mathcal{A}$, on peut écrire $X = \lambda \mathrm{I}_n + M$ et $X' = \lambda' \mathrm{I}_n + M'$ avec $\lambda, \lambda' \in K$ et $M, M' \in \mathcal{V}$. On a alors

$$XX' = (\lambda \mathrm{I}_n + M)(\lambda \mathrm{I}_n + M') = \lambda\lambda' \mathrm{I}_n + (\lambda M' + \lambda' M) + MM' = \lambda\lambda' \mathrm{I}_n + (\lambda M' + \lambda' M) \in \mathcal{A}$$

vu que $MM' = 0$ par hypothèse. Cela montre que $\mathcal{A}$ est une sous-K-algèbre de $\mathcal{M}_n(K)$. En outre, le calcul qui précède montre que $XX' = X'X$, et donc que$\mathcal{A}$ est commutative.
• On a $\mathcal{A} = K\mathrm{I}_n + \mathcal{V}$. Comme $MM' = 0$ pour tous $M, M' \in \mathcal{V}$, on a $\mathrm{I}_n \notin \mathcal{V}$. Cela montre que $\mathcal{A} = K\mathrm{I}_n \oplus \mathcal{V}$. En particulier, on a $\dim_K(\mathcal{A}) = d + 1$.

(9) (b) Soit $X \in \mathcal{A}^\times$. Écrivons $X = \lambda \mathrm{I}_n + M$ avec $\lambda \in K$ et $M \in \mathcal{V}$. On dispose de $X^{-1} \in \mathcal{A}$: écrivons de même $X^{-1} = \lambda' \mathrm{I}_n + M'$ avec $\lambda' \in K$ et $M' \in \mathcal{V}$. Le calcul de la question précédente montre alors que $I_n = XX^{-1} = \lambda\lambda' \mathrm{I}_n + (\lambda M' + \lambda' M)$. Comme $\mathcal{A} = K\mathrm{I}_n \oplus \mathcal{V}$, cela implique que $\lambda\lambda' = 1$ et $\lambda M' + \lambda' M = 0$. En particulier, on a $\lambda \in K^\times$, $\lambda' = \lambda^{-1}$ et $M' = -\lambda^{-2}M$. Réciproquement, si $X = \lambda \mathrm{I}_n + M$ avec $\lambda \in K^\times$ et $M \in \mathcal{V}$, alors $XX' = \mathrm{I}_n$ avec $X' = \lambda^{-1}\mathrm{I}_n - \lambda^{-2}M \in \mathcal{A}$, *i.e.* $X \in \mathcal{A}^\times$. On a bien $\mathcal{A}^\times = \{\lambda \mathrm{I}_n + M\}_{\substack{\lambda \in K^\times \\ M \in \mathcal{V}}}$.

(9) (c) • On a $\mathcal{A} = K\mathrm{I}_n \oplus \mathcal{V}$: si $X \in \mathcal{A}$, il existe $f(X) \in K$ et $M \in \mathcal{V}$ uniques tels que $X = f(X)\mathrm{I}_n + M$. Les lois d'anneaux sur $\mathcal{A}$ décrites dans la question (9) (a) impliquent que $f\colon \mathcal{A} \to K$ est un morphisme surjectif d'anneaux. On a $\mathrm{Ker}(f) = \mathcal{V}$: c'est un idéal de $\mathcal{A}$. Il est maximal parce que f induit un isomorphisme $\mathcal{A}/\mathcal{V} \xrightarrow{\sim} K$.
• Soit maintenant $I \subset \mathcal{A}$ un idéal strict (*i.e.* différent de $\mathcal{A}$). Comme les éléments de $\mathcal{A}^\times$ engendrent l'idéal unité $\mathcal{A}$, on a $I \cap \mathcal{A}^\times = \varnothing$, *i.e.* $I \subset \mathcal{A} \setminus \mathcal{A}^\times$. D'après la question précédente, on a $\mathcal{A} \setminus \mathcal{A}^\times = \mathcal{V}$, donc $I \subset \mathcal{V}$. Cela montre que $\mathcal{V}$ est le seul idéal maximal de $\mathcal{A}$.

Remarque. L'énoncé comporte une petite erreur (de formulation ?) : à moins qu'il soit nul, $\mathcal{V}$ n'est pas le seul idéal strict de $\mathcal{A}$ (chacun de ses sous-espaces vectoriels fournit un idéal).

(10) (a) Choisissons un base $M_1, \dots, M_d$ de $\mathcal{V}$ sur K. Posons alors

$$\psi\colon K^\times \times K^d \to \mathcal{A}^\times$$
$$(\lambda, (x_1, \dots, x_d)) \mapsto \lambda\Big(\mathrm{I}_n + \sum_{i=1}^{d} x_i M_i\Big).$$

La question (9) (b) montre que cette application est bien définie, et que c'est une bijection. Soient $\lambda, \lambda' \in K^\times$ et $\mathbf{x} = (x_1, \dots, x_d), \mathbf{x}' = (x'_1, \dots, x'_d) \in K^d$. On a

$$\begin{aligned}
\psi\big((\lambda, \mathbf{x}) \cdot (\lambda', \mathbf{x}')\big) &= \psi(\lambda\lambda', \mathbf{x} + \mathbf{x}') \\
&= \lambda\lambda'\Big(\mathrm{I}_n + \sum_{i=1}^{d} (x_i + x'_i) M_i\Big) \\
&= \lambda\Big(\mathrm{I}_n + \sum_{i=1}^{d} x_i M_i\Big)\lambda'\Big(\mathrm{I}_n + \sum_{i=1}^{d} x'_i M_i\Big) \\
&= \psi(\lambda, \mathbf{x})\psi(\lambda', \mathbf{x}')
\end{aligned}$$

parce que $M_i M_j = 0$ pour tous $i, j \in \{1, \dots, d\}$. Cela montre que ψ est un morphisme de groupes : c'est un isomorphisme de $(K^\times, .) \times (K^d, +) \to (\mathcal{A}^\times, .)$ en vertu de ce qui précède.

(10) (b) Comme le groupe $(K^\times, .)$ est cyclique d'ordre $q-1$, on a $(K^\times, .) \simeq (\mathbf{Z}/(q-1)\mathbf{Z}, +)$. Par ailleurs, K est de caractéristique p : c'est un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel, de dimension r par cardinalité. Il existe donc un isomorphisme de groupes $((\mathbf{Z}/p\mathbf{Z})^r, +) \xrightarrow{\sim} (K, +)$, qui induit un isomorphisme de groupes $((\mathbf{Z}/p\mathbf{Z})^{rd}, +) \xrightarrow{\sim} (K^d, +)$. Via l'isomorphisme de la question précédente, on en déduit un isomorphisme $\big((\mathbf{Z}/(q-1)\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})^{rd}, +\big) \xrightarrow{\sim} (\mathcal{A}^\times, .)$

II.B. Sous-espaces vectoriels commutatifs de matrices nilpotentes

(11) (a) Notons que Ψ est bien défini vu que pour tout $u \in \mathcal{V}$, on a $\mathrm{Im}(u) \subset F$. Soit $u \in \mathrm{Ker}(\Psi)$. Montrons l'assertion $\mathscr{P}(k)$: « pour tous $u_1, \dots, u_k \in \mathcal{V}$, on a $u \circ u_1 \circ \cdots \circ u_k = 0$ » par récurrence descendante sur $k \in \{1, \dots, n-1\}$. Observons que $\mathscr{P}(n-1)$ résulte de la question (3) (c) (qu'on peut invoquer puisque $\mathcal{V}$ est commutatif). Soit $k \in \{2, \dots, n-1\}$ tel que $\mathscr{P}(k)$ soit vérifié. Soient $u_1, \dots, u_{k-1} \in \mathcal{V}$: par hypothèse, on a $u \circ u_1 \circ \cdots \circ u_k = 0$ pour tout $u_k \in \mathcal{V}$. Cela implique que $u \circ u_1 \circ \cdots \circ u_{k-1}$ est nul sur F. Par ailleurs, on a $u \circ u_1 \circ \cdots \circ u_{k-1} = u_1 \circ \cdots \circ u_{k-1} \circ u$ est nul sur S (parce que $u \in \mathrm{Ker}(\Psi)$). Il en résulte que $u \circ u_1 \circ \cdots \circ u_{k-1}$ est nul sur $F \oplus S = E$, *i.e.* que $u \circ u_1 \circ \cdots \circ u_{k-1} = 0$, ce qui montre que $\mathscr{P}(k-1)$ est vérifiée. Finalement, $\mathscr{P}(1)$ est vérifiée, ce qui montre que u est nul sur F : comme il est nul sur S par hypothèse, on a $u = 0$. On a prouvé que $\mathrm{Ker}(\Psi) = \{0\}$, *i.e.* que Ψ est injectif.

(11) (b) On a $\dim_K(\mathcal{L}(S, F)) = \dim_K(F)\dim_K(S) = \dim_K(F)(n - \dim_K(F))$: la première inégalité résulte de l'injectivité de Ψ. La deuxième résulte du fait que le maximum de l'application $t \mapsto t(n-t)$ est atteint en $\frac{n}{2}$, et vaut $\frac{n^2}{4}$, ce qui implique que $\dim_K(F)(n - \dim_K(F)) \leq \frac{n^2}{4}$, donc en fait que $\dim_K(F)(n - \dim_K(F)) \leq b(n)$ parce que $\dim_K(F)(n - \dim_K(F))$ est un entier.

(12) (a) Comme $\dim_K(\mathcal{V}) = b(n)$, les inégalités de la question précédente sont des égalités. On a en particulier $\dim_K(\mathcal{V}) = \dim_K(F)(n - \dim_K(F)) = \dim_K(\mathcal{L}(S, F))$: le morphisme injectif Ψ est un isomorphisme pour des raisons de dimension (par le théorème du rang).

(12) (b) On a $\dim_K(F) = n - d$: l'égalité $\dim_K(F)(n - \dim_K(F)) = b(n)$ (*cf* question précédente) s'écrit $b(n) = (n-d)d = \frac{n^2}{4} - \big(d - \frac{n}{2}\big)^2$, soit encore $\big(d - \frac{n}{2}\big)^2 = \frac{n^2}{4} - b(n)$. Si $n = 2m$, on a donc $(d-m)^2 = 0$, *i.e.* $d = m$. Si $n = 2m+1$, on a $\frac{n^2}{4} - b(n) = \frac{1}{4}$, d'où $\big(d - m - \frac{1}{2}\big)^2 = \frac{1}{4}$, soit $d - m - \frac{1}{2} \in \big\{\pm\frac{1}{2}\big\}$, *i.e.* $d \in \{m, m+1\}$.

(13) (a) Comme $\mathcal{V}$ est commutatif, il en est de même de $\mathcal{V} + K(u' \circ u)$. D'après la question (11) (b), on a donc $\dim_K(\mathcal{V} + K(u' \circ u)) \leq b(n)$. Comme $\dim_K(\mathcal{V}) = b(n)$ par hypothèse, cela montre que l'inclusion $\mathcal{V} \subset \mathcal{V} + K(u' \circ u)$ est une égalité, *i.e.* que $u' \circ u \in \mathcal{V}$. Comme $u' \circ u \neq 0$, on a $\Psi(u' \circ u) \neq 0$ en vertu de la question (11) (a). Il existe donc $x_1 \in S$ tel que $(u' \circ u)(x_1) \neq 0$.

(13) (b) On a $u'(x_2) \in F$: notons w l'unique élément de $\mathcal{L}(S, F)$ tel que $w(x_1) = u'(x_1)$ et $w(x_k) = 0$ pour tout $k \in \{2, \dots, d\}$. D'après la question (12) (a), l'application $\Psi\colon \mathcal{V} \to \mathcal{L}(S, F)$ est un isomorphisme : posons $v = \Psi^{-1}(w) \in \mathcal{V}$. On a alors $v(x_1) = u'(x_2)$ et $v(x_2) = 0$. De même, soit $w' \in \mathcal{L}(S, F)$ l'unique élément tel

que $w'(x_2) = u(x_1)$ et $w'(x_k) = 0$ pour $k \in \{1, 3, \dots, d\}$. L'élément $v' = \Psi^{-1}(w') \in \mathcal{V}$ vérifie $v'(x_1) = 0$ et $v'(x_2) = u(x_1)$.

(13) (c) On a $(v \circ v')(x_1) = v(0) = 0$, et $(v' \circ v)(x_1) = v'(u'(x_2)) = u'(v'(x_2)) = u'(u(x_1)) \neq 0$ (on a $v' \circ u' = u' \circ v'$ parce que $u', v' \in \mathcal{V}$ et $\mathcal{V}$ est commutatif). Cela montre que $v \circ v' \neq v' \circ v$. Comme $v, v' \in \mathcal{V}$, cela contredit l'hypothèse que $\mathcal{V}$ est commutatif.

(14) Plus généralement, montrons que si E est un K-espace vectoriel de dimension n et $\mathcal{V} \subset \mathcal{L}(E)$ un sous-espace vectoriel commutatif de dimension $b(n)$, alors il existe une base de E dans laquelle le sous-espace vectoriel des matrices des éléments de $\mathcal{V}$ est $\mathcal{V}_n(K)$ (resp, $\mathcal{V}_n^1(K)$ ou $\mathcal{V}_n^2(K)$) si n est pair (resp. impair). Reprenons les notations des questions (11), (12) et (13).
On a $\dim_K(F) = n - d$ et $F \oplus S = K^n$: soit $\mathfrak{B} = (e_1, \dots, e_n)$ une base de E telle que $F = \mathrm{Vect}(e_1, \dots, e_{n-d})$ et $S = \mathrm{Vect}(e_{n-d+1}, \dots, e_n)$. La question précédente montre que $(\forall u, u' \in \mathcal{V})\, u' \circ u = 0$. Cela implique que $F \subset \mathrm{Ker}(u)$ pour tout $u \in \mathcal{V}$. Par ailleurs, on a $\mathrm{Im}(u) \subset F$ pour tout $u \in \mathcal{V}$ par définition de F. Cela implique que

$$\mathcal{V} \simeq \{\mathcal{M}_{\mathfrak{B}}(u)\}_{u \in \mathcal{V}} \subset \left\{ \left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right) \right\}_{A \in \mathcal{M}_{n-d,d}(K)}.$$

Comme $d = m$ (resp. $d \in \{m, m+1\}$) si $n = 2m$ (resp. $n = 2m+1$), le membre de droite n'est autre que $\mathcal{V}_n(K)$ (resp. $\mathcal{V}_n^1(K)$ ou $\mathcal{V}_n^2(K)$) si n est pair (resp. impair). Comme $\dim_K(\mathcal{V}) = b(n) = \dim_K(\mathcal{V}_n^*(K))$ (pour $* \in \{\varnothing, 1, 2\}$) par hypothèse et en vertu de la question (8) (a), l'inclusion qui précède est une égalité, ce qui est précisément ce qu'il fallait démontrer.

II.C. Sous-algèbres commutatives de $\mathcal{M}_n(K)$

(15) On a vu dans la question (8) (a) que $b(n) = \frac{n^2}{4}$ si n est pair et $b(n) = \frac{n^2-1}{4}$ si n est impair. Dans tous les cas, on a $\frac{n^2-1}{4} \leq b(n) \leq \frac{n^2}{4}$.
• Supposons $n_1 > 1$: on a $n_1, n_2 \geq 2$. Cela montre que

$$b(n_1+n_2)+1 \geq \tfrac{(n_1+n_2)^2-1}{4} + 1 = \tfrac{n_1^2+n_2^2+2n_1n_2-1}{4} + 1 \geq \tfrac{n_1^2+n_2^2+8-1}{4} + 1 > \tfrac{n_1^2+n_2^2}{4} + 2 \geq b(n_1)+1+b(n_2)+1.$$

• Supposons $n_1 = 0$ et $n_2 \geq 2$. On a $b(n_1) = 0$, d'où

$$b(n_1+n_2)+1 = b(n_2+1)+1 \geq \tfrac{(n_2+1)^2-1}{4} + 1 = \tfrac{n_2^2+2n_2}{4} + 1 \geq \tfrac{n_2^2}{4} + 2 \geq b(n_2)+2 = b(n_1)+1+b(n_2)+1.$$

L'inégalité est aussi vérifiée (et c'est même une égalité) lorsque $n_1 = n_2 = 1$.

(16) (a) Il s'agit d'un résultat de décomposition de Dunford simultanée. On procède par récurrence forte sur n, de façon analogue à la partie I.A. Comme K est supposé algébriquement clos, le spectre de tout élément de $\mathcal{A}$ est non vide. Lorsque ce spectre est réduit à un élément pour tout les éléments de $\mathcal{A}$, on prend $r = 1$ et $E_1 = E$. Supposons maintenant que $\mathcal{A}$ contient un élément u_0 dont le spectre $\mathrm{Sp}(u_0)$ contient au moins deux éléments. Soit $\lambda \in \mathrm{Sp}(u_0)$. Notons $F = \mathrm{Ker}(u_0 - \lambda\,\mathsf{id}_E)^n)$ le sous-espace caractéristique de u_0 associé à la valeur propre λ : on a $\{0\} \subsetneq F \subsetneq E$. Si $u \in \mathcal{A}$ et $x \in F$, on a $(u_0 - \lambda\,\mathsf{id}_E)^n(u(x)) = u((u_0 - \lambda\,\mathsf{id}_E)^n(x)) = 0$ parce que u et u_0 commutent (vu que $\mathcal{A}$ est supposée commutative), et donc $u(F) \subset F$. Notons alors G la somme des sous-espaces caractéristiques de u_0 associés aux valeurs propres de u_0 distinctes de λ. On a $E = F \oplus G$, et G est lui aussi stable par tous les éléments de $\mathcal{A}$.
Posons $\mathcal{A}_F = \{u_{|F}\}_{u \in \mathcal{A}}$ et $\mathcal{A}_G = \{u_{|G}\}_{u \in \mathcal{A}}$. Ce sont des sous-algèbres commutatives de $\mathcal{L}(F)$ et $\mathcal{L}(G)$ respectivement. Comme $\dim_K(F) < n$ et $\dim_K(G) < n$, l'hypothèse de récurrence s'applique à $\mathcal{A}_F$ et $\mathcal{A}_G$. Il existe des décompositions $F = \bigoplus_{i=1}^{r_1} F_i$ et $G = \bigoplus_{i=1}^{r_2} G_i$ où $F_1, \dots, F_{r_1}, G_1, \dots, G_{r_2}$ sont stables par tous les éléments de $\mathcal{A}$ et pour tout $i \in \{1, \dots, r_1\}$ (resp. $i \in \{1, \dots, r_2\}$), $u_{|F_i}$ (resp. $u_{|G_i}$) est la somme d'une homothétie et d'un endomorphisme nilpotent. Il suffit alors de poser $r = r_1 + r_2$ et $E_i = \begin{cases} F_i & \text{si } 1 \leq i \leq r_1 \\ G_{i-r_1} & \text{si } r_1 + 1 \leq i \leq r \end{cases}$.

(16) (b) Soient E un K-espace vectoriel de dimension n et $\mathcal{A}$ une sous-algèbre commutative de $\mathcal{L}(E)$. D'après la question précédente, il existe une décomposition $E = \bigoplus_{i=1}^{r} E_i$ en sous-espaces stables par tous les éléments de $\mathcal{A}$ et telle que pour tout $i \in \{1, \dots, r\}$, on ait $\mathcal{A}_i := \{u_{|E_i}\}_{u \in \mathcal{A}} = K\,\mathsf{id}_{E_i} + \mathcal{V}_i$ ou $\mathcal{A}_i = \mathcal{V}_i$, où $\mathcal{V}_i$ est un

sous-espace de $\mathcal{L}(E_i)$ constitué d'endomorphismes nilpotents. Comme $\mathcal{A}$ est commutative, il en est de même des $\mathcal{A}_i$, et donc des $\mathcal{V}_i$.
• D'après la question (11), on a $\dim_K(\mathcal{V}_i) \leq b(n_i)$, de sorte que $\dim_K(\mathcal{A}_i) \leq b(n_1)+1$, où $n_i = \dim_K(E_i)$. Comme le morphisme $\mathcal{A} \to \prod_{i=1}^{r} \mathcal{A}_i$ donné par $u \mapsto (u_{|E_i})_{1\leq i\leq r}$ est injectif, cela montre que

$$\dim_K(\mathcal{A}) \leq \sum_{i=1}^{r} \dim_K(\mathcal{A}_i) \leq \sum_{i=1}^{r} (b(n_i)+1) \leq b\Big(\sum_{i=1}^{r} n_i\Big) + 1 = b(n)+1$$

en vertu de la majoration énoncée après la question (15) (et qui résulte d'une application répétée d'icelle). Cela prouve l'item (i) du théorème 2.
• Supposons désormais que $n \geq 4$ et $\dim_K(\mathcal{A}) = b(n)+1$. Cela requiert que toutes les inégalités qui précèdent soient des égalités. En particulier, on a $\sum_{i=1}^{r}(b(n_i)+1) \leq b\Big(\sum_{i=1}^{r} n_i\Big)+1$. D'après les cas d'égalité décrits dans l'énoncé, on a $r \leq 2$. Par ailleurs, si $r=2$, alors $n_1 = 1$ et $n_2 \leq 2$, de sorte que $n = n_1+n_2 \leq 3$, contredisant l'hypothèse $n \geq 4$: on a nécessairement $r=1$. D'après ce qui précède, il existe un sous-espace commutatif $\mathcal{V} \subset \mathcal{L}(E)$ constitué d'endomorphismes nilpotents tel que $\mathcal{A} = K\,\mathsf{id}_E + \mathcal{V}$ ou bien $\mathcal{A} = \mathcal{V}$. Comme $\dim_K(\mathcal{V}) \leq b(n)$ (*cf* question (11) (b)) et $\dim_K(\mathcal{A}) = b(n)+1$, on a nécessairement $\mathcal{A} = K\,\mathsf{id}_E + \mathcal{V}$ et $\dim_K(\mathcal{V}) = b(n)$. L'item (ii) du théorème 2 résulte alors de l'item (ii) du théorème 1 (démontré question (14).

(17) (a) Soit $(\omega_\lambda)_{\lambda\in\Lambda}$ une base de Ω sur K. Soient $x_1,\dots,x_m \in \Omega$ tels que $\sum_{i=1}^{m} x_i U_i = 0$. Pour tout $i \in \{1,\dots,m\}$, il existe $(x_{i,\lambda})_{\lambda\in\Lambda} \in K^{(\Lambda)}$ tel que $x_i = \sum_{\lambda\in\Lambda} x_{i,\lambda}\omega_\lambda$. On a alors $\sum_{\lambda\in\Lambda} \omega_\lambda\Big(\sum_{i=1}^{m} x_{i,\lambda}U_i\Big) = \sum_{i=1}^{m} x_i U_i = 0$ (toutes les sommes ne font intervenir qu'un nombre fini de termes non nuls). Cela implique que pour tout $\lambda\in\Lambda$, on a $\sum_{i=1}^{m} x_{i,\lambda}U_i = 0$, et donc $x_{1,\lambda} = \cdots = x_{m,\lambda} = 0$ puisque $(U_1,\dots,U_m)$ est libre sur K. Cela montre que $x_i = \sum_{\lambda\in\Lambda} x_{i,\lambda}\omega_\lambda = 0$ pour tout $i \in \{1,\dots,m\}$, et donc que la famille $(U_1,\dots,U_m)$ est libre sur Ω.

Remarque. On peut ne pas avoir envie d'invoquer l'existence de bases en dimension infinie : voici une approche alternative. Soient $X_1,\dots,X_m$ des indéterminées. En considérant les coefficients des matrices $U_1,\dots,U_m$, résoudre l'équation $X_1U_1+\cdots+X_mU_m = 0$ revient à résoudre un système linéaire à m inconnues et n^2 équations, *i.e.* de la forme MX avec $M \in \mathcal{M}_{n^2,m}(K)$ et X un vecteur colonne à m composantes. Le fait que la famille $(U_1,\dots,U_m)$ soit libre sur K (c'est une K-base de $\mathcal{A}$) implique que l'ensemble des solutions dans K^m est réduit à $\{0\}$, ce qui signifie que la matrice M est de rang m : on peut en extraire une matrice carrée de taille m inversible. Cela implique alors que l'ensemble des solutions dans Ω^m est lui aussi réduit à $\{0\}$, et donc que la famille $(U_1,\dots,U_m)$ est libre sur Ω.

On a prouvé que $\dim_\Omega(\mathcal{A}_\Omega) = m$, plus précisément que $\mathcal{A}_\Omega = \bigoplus_{i=1}^{m} \Omega U_i$. Comme $U_iU_j \in \mathcal{A} \subset \mathcal{A}_\Omega$ pour tout $i,j \in \{1,\dots,m\}$, le sous-Ω-espace vectoriel $\mathcal{A}_\Omega$ de $\mathcal{M}_n(\Omega)$ est une sous-algèbre, et qu'elle est commutative.
(17) (b) Soit $\mathcal{W} \subset \mathcal{M}_n(K)$ le sous-espace vectoriel constitué des matrices dont la première colonne est nulle : c'est le noyau de l'application linéaire $M \mapsto Me_1$ où $e_1 \in K^n$ est le premier vecteur de la base canonique. Cette application étant surjective, on a $\dim_K(\mathcal{W}) = n^2-n$. Comme $b(n) \geq \frac{n^2-1}{4}$, on a

$$\dim_K(\mathcal{W}) + \dim_K(\mathcal{A}) \geq n^2 - n + \tfrac{n^2-1}{4} + 1 = \tfrac{5n^2-4n+3}{4} = n^2 + \tfrac{(n-3)(n-1)}{4}.$$

Comme $n \geq 4$, on a donc $\dim_K(\mathcal{W}) + \dim_K(\mathcal{A}) > n^2 = \dim_K(\mathcal{M}_n(K))$. Il en résulte que

$$\dim_K(\mathcal{W}\cap\mathcal{A}) = \dim_K(\mathcal{W}) + \dim_K(\mathcal{A}) - \dim_K(\mathcal{W}+\mathcal{A}) > 0$$

i.e. que $\mathcal{W}\cap\mathcal{A} \neq \{0\}$. Il existe donc des éléments de $\mathcal{A}$ non nuls qui appartiennent à $\mathcal{W}$, et qui sont donc non inversibles.
(17) (c) D'après l'item (ii) du théorème 2 appliqué à $\mathcal{A}_\Omega$, il existe $P \in \mathsf{GL}_n(\Omega)$ telle que $P^{-1}\mathcal{A}_\Omega P = \mathcal{A}_n^*(\Omega)$ (avec $* \in \{\varnothing,1,2\}$). Cela signifie que $P^{-1}NP \in \mathcal{V}_n^*(\Omega)$. Ce même, comme $P^{-1}CP \in \mathcal{A}_n^*(\Omega) = \Omega\,\mathrm{I}_n + \mathcal{V}_n^*(\Omega)$ n'est pas inversible : elle est nilpotente, d'où $C \in \mathcal{V}_n^*(\Omega)$. D'après la question (8) (b), on a donc $NC = 0$, *i.e.* $(M-\lambda\,\mathrm{I}_n)C = 0$. Cela implique que $\lambda C = MC \in \mathcal{A} \subset \mathcal{M}_n(K)$. Comme $C \in \mathcal{M}_n(K) \subset \{0\}$, cela implique que $\lambda \in K$.
(17) (d) D'après la question précédente, on a $\mathcal{A} \subset K\,\mathrm{I}_n + \mathcal{V}$, où $\mathcal{V} \subset \mathcal{M}_n(K)$ est un sous-espace vectoriel constitué de matrices nilpotentes. D'après le théorème 1 (i), on a $\dim_K(\mathcal{V}) \leq b(n)$. Par hypothèse, on a $\dim_K(\mathcal{A}) = b(n)+1$, d'où nécessairement $\dim_K(\mathcal{V}) = b(n)$ et $\mathcal{A} = K\,\mathrm{I}_n + \mathcal{V}$. Comme $n \geq 4$, le théorème 1 (ii) implique que $\mathcal{V}$ est conjugué, dans $\mathcal{M}_n(K)$, à $\mathcal{V}_n^*(K)$ (avec $* \in \{\varnothing,1,2\}$), ce qui montre que $\mathcal{A}$ est conjugué, dans $\mathcal{M}_n(K)$, à $\mathcal{A}_n^*(K)$ (avec $* \in \{\varnothing,1,2\}$), *i.e.* l'item (ii) du théorème 2.

II.D. Cardinal maximal d'un sous-groupe abélien de $\mathsf{GL}_n(\mathbf{F}_q)$

(18) (a) Soient $x, y \in V_G$. Il existe $g_1, \dots, g_r, \gamma_1, \dots, \gamma_s \in G$ et $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_s \in K$ tels que $x = \sum_{i=1}^{r} \lambda_i g_i$ et $y = \sum_{j=1}^{s} \mu_j \gamma_j$. On a alors $xy = \sum_{\substack{1\leq i\leq r\\ 1\leq j\leq s}} \lambda_i\mu_j g_i\gamma_j = \sum_{\substack{1\leq i\leq r\\ 1\leq j\leq s}} \lambda_i\mu_j\gamma_j g_i = yx$ puisque $g_i\gamma_j = \gamma_j g_i$ pour tout $i \in \{1, \dots, r\}$ et tout $j \in \{1, \dots, s\}$ (parce que G est abélien). Cela montre que $xy \in V_G$, et donc que V_G Est une sous-K-algèbre de $\mathcal{M}_n(K)$, et qu'elle est commutative. On a bien entendu $G \subset V_G^\times \subset V_g \setminus \{0\}$, ce qui montre que $|G| \leq |V_G \setminus \{0\}| = |V_G| - 1 = q^{d_G} - 1$.

(18) (b) • D'après le théorème 2 (i), on a $d_G \leq b(n) + 1$. Par maximalité, on a aussi $\beta_q(n) \leq |G|$: d'après la question précédente, on a donc $\beta_q(n) \leq q^{d_G} - 1$, *i.e.* $(q-1)q^{b(n)} < q^{d_G}$, et donc $q^{b(n)} < q^{d_G}$: cela implique que $b(n) < d_G$. Joint à la majoration $d_G \leq b(n) + 1$ ci-dessus, cela montre que $d_G = b(n) + 1$.
• Comme $n \geq 4$, le théorème 2 (ii) implique que V_G est conjugué à $\mathcal{A}_n^*(\mathbf{F}_q)$ (avec $* \in \{\varnothing, 1, 2\}$). Cela montre que $V_G^\times \simeq \mathcal{A}_n^*(\mathbf{F}_q)^\times$, et donc $\left|V_G^\times\right| \mid |\mathcal{A}_n^*(\mathbf{F}_q)^\times| = (q-1)q^{b(n)} = \beta_q(n)$ en vertu de la question (10). Comme $G \subset V_G^\times$, on a en outre $|G| \mid \left|V_G^\times\right|$, d'où $|G| \mid \beta_q(n)$. Comme on a en outre $\beta_q(n) \leq |G|$ (par maximalité de $|G|$), on a en fait $|G| = \beta_q(n)$. Cela prouve aussi que l'inclusion $G \subset V_g^\times$ est une égalité, et donc que G est conjugué à $\mathcal{A}_n^*(\mathbf{F}_q)^\times$ (avec $* \in \{\varnothing, 1, 2\}$).

III. Sous-groupes abéliens finis de $\mathsf{GL}_n(\mathbf{Q})$ de cardinal maximal

III.A. Irréductibilité des polynômes cyclotomiques

(19) (a) Le morphisme de groupes $\mathbf{Z} \to \mathbf{C}^\times$; $k \mapsto e^{\frac{2ik\pi}{n}}$ induit un isomorphisme $\eta\colon \mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \mathbb{U}_n$. Les générateurs du groupe $\mathbf{Z}/n\mathbf{Z}$ sont les éléments de $(\mathbf{Z}/n\mathbf{Z})^\times$: ceux de $\mathbb{U}_n$ sont donc les éléments de $\eta((\mathbf{Z}/n\mathbf{Z})^\times) = \mu_n$. Ces derniers sont donc d'ordre n dans $\mathbb{U}$. Réciproquement, un élément $u \in \mathbb{U}$ d'ordre n engendre le groupe $\mathbb{U}_n$ (l'unique sous-groupe d'ordre n de $\mathbb{U}$ en vertu de la question (5) (a)). Il appartient donc à μ_n.

(19) (b) On partitionne $\mathbb{U}_n$ suivant l'ordre des éléments : on a $\mathbb{U}_n = \bigsqcup_{d\in D_n} \mu_d$, d'où

$$X^n - 1 = \prod_{\zeta\in\mathbb{U}_n} (X - \zeta) = \prod_{d\in D_n} \prod_{\zeta\in\mu_d} (X - \zeta) = \prod_{d\in D_n} \Phi_d.$$

(19) (c) On procède par récurrence forte sur n. On a $\Phi_1 = X - 1 \in \mathbf{Z}[X]$. Supposons $n > 1$. Par hypothèse de récurrence, on a $D = \prod_{\substack{d\in D_n\\ d<n}} \Phi_d \in \mathbf{Z}[X]$. L'égalité $X^n - 1 = D\Phi_n$ (*cf* question précédente) montre que Φ_n est la division euclidienne de $X^n - 1$ par le polynôme *unitaire* D : on a $\Phi_n \in \mathbf{Z}[X]$.

(20) (a) • Soit $x \in \overline{\mathbf{Z}} \cap \mathbf{Q}$. Écrivons $x = \frac{u}{v}$ avec $u \in \mathbf{Z}$ et $v \in \mathbf{N}_{>0}$ tels que $\mathsf{pgcd}(u, v) = 1$. Comme $x \in \overline{\mathbf{Z}}$, il existe $P = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbf{Z}[X]$ tel que $P(x) = 0$. On a alors $u^d + a_1u^{d-1}v + \cdots + a_dv^d = 0$, ce qui implique que $v \mid u^d$ dans $\mathbf{Z}$. Comme $\mathsf{pgcd}(u, v) = 1$, on a nécessairement $v = 1$, d'où $x = u \in \mathbf{Z}$. Cela montre que $\overline{\mathbf{Z}} \cap \mathbf{Q} \subset \mathbf{Z}$. L'inclusion réciproque est triviale.
• On a $\frac{b}{a} \in \overline{Z} \cap \mathbf{Q}$, donc $\frac{b}{a} \in \mathbf{Z}$, soit encore a divise b dans $\mathbf{Z}$.

(20) (b) Soit $P \in \mathbf{Z}[X]$ unitaire tel que $P(z) = 0$: on a $\Pi_z \mid P$ dans $\mathbf{Q}[X]$ (par définition du polynôme minimal). Les racines de P sont toutes des éléments de $\overline{\mathbf{Z}}$: il en est de même de celles de Π_z. Comme Π_z est unitaire, ses coefficients sont, au signe près, les polynômes symétriques en ses racines : comme $\overline{\mathbf{Z}}$ est un anneau, ces coefficients appartiennent à $\overline{\mathbf{Z}}$. Comme ce sont des rationnels, la question précédente montre que ce sont des entiers, et donc que $\Pi_z \in \mathbf{Z}[X]$.

(21) (a) On a $P' = \sum_{k=1}^{d} \prod_{\substack{1\leq\ell\leq d\\ \ell\neq k}} (X - z_\ell)$, donc $P'(z_k) = \prod_{\substack{1\leq\ell\leq d\\ \ell\neq k}} (z_k - z_\ell)$. On a donc $\prod_{k=1}^{d} P'(z_k) = \prod_{\substack{1\leq k,\ell\leq d\\ k\neq\ell}} (z_k - z_\ell)$.

En rassemblant les facteurs $z_k - z_\ell$ et $z_\ell - z_k$ pour $k < \ell$ dans ce produit (il y en a $\sum_{\ell=1}^{d} (\ell - 1) = \frac{d(d-1)}{2}$), on en déduit que $\prod_{k=1}^{d} P'(z_k) = (-1)^{\frac{d(d-1)}{2}} \Delta(P)$, *i.e.* le résultat voulu.

(21) (b) On applique ce qui précède à $P = X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta)$. Si $\zeta \in \mathbb{U}_n$, on a $P'(\zeta) = n\zeta^{n-1} = \frac{n}{\zeta}$: d'après la question précédente, on a $\Delta(X^n - 1) = (-1)^{\frac{n(n-1)}{2}} \prod_{\zeta \in \mathbb{U}_n} \frac{n}{\zeta}$. Observons que $-1 = P(0) = \prod_{\zeta \in \mathbb{U}_n} (-\zeta)$, de sorte que $\prod_{\zeta \in \mathbb{U}_n} \zeta = (-1)^{n-1}$. Cela montre que $\Delta(X^n - 1) = \varepsilon_n n^n$ avec $\varepsilon_n = (-1)^{\frac{n(n-1)}{2} + n - 1} = (-1)^{\frac{n(n+1)}{2} + 1} \in \{\pm 1\}$.

(22) (a) Par définition de la signature, on a $U(X_{\sigma(1)}, \dots, X_{\sigma(d)}) = \varepsilon(\sigma) U(X_1, \dots, X_d)$.

(22) (b) Le polynôme $V := U^2 = \prod_{1 \leq k < \ell \leq d} (X_\ell - X_k)^2$ vérifie $V(\sigma(1), \dots, X_{\sigma(d)}) = V(X_1, \dots, X_d)$ (*cf* question précédente). D'après le théorème des polynômes symétriques rappelé dans l'énoncé, il existe un polynôme $W \in \mathbf{Z}[X_1, \dots, X_d]$ (unique) tel que $V = W(\Sigma_1, \dots, \Sigma_d)$. Écrivons $P = X^d + a_1 X^{d-1} + \cdots + a_d$. D'après les relations coefficients-racines, on a $\Sigma_k(z_1, \dots, z_d) = (-1)^k a_k \in \mathbb{A}$ pour tout $k \in \{1, \dots, d\}$. Comme $\mathbb{A}$ est un sous-anneau de $\mathbf{C}$, cela implique que $\Delta(P) = V(z_1, \dots, z_d) = W(-a_1, a_2, \dots, (-1)^d a_d) \in \mathbb{A}$.

(23) (a) • Écrivons $P = a_0 X^d + a_1 X^{d-1} \cdots + a_d \in \mathbf{Z}[X]$. Si $a \in \mathbf{Z}$, notons $\overline{a}$ son image dans $\mathbf{Z}/p\mathbf{Z}$. L'élévation à la puissance p (le morphisme de Frobenius) est en endomorphisme d'anneaux en caractéristique p (pour les anneaux commutatifs). Par ailleurs, on a $\overline{a}^p = \overline{a}$ pour tout $a \in \mathbf{Z}$ (petit théorème de Fermat). Posons $\overline{P} = \sum_{k=0}^{d} \overline{a}_k X^{d-k} \in (\mathbf{Z}/p\mathbf{Z})[X] \simeq \mathbf{Z}[X]/p\mathbf{Z}[X]$. On a $\overline{P}^p = \Big(\sum_{k=0}^{d} \overline{a}_k X^{d-k} \Big)^p = \sum_{k=0}^{d} \overline{a}_k X^{p(d-k)} = \overline{P}(X^p)$. Cela signifie précisément que $P(X)^p - P(X^p) \in p\mathbf{Z}[X]$.

• D'après la question (20) (b), on a $\Pi_z \in \mathbf{Z}[X]$: il existe $Q \in \mathbf{Z}[X]$ tel que $\Pi_z(X^p) = \Pi_z(X)^p + pQ(X)$ (*cf* question précédente). En évaluant en z, on a donc $\Pi_z(z^p) = pQ(z)$. Comme $z \in \overline{\mathbf{Z}}$ et $\overline{\mathbf{Z}}$ est un sous-anneau de $\mathbf{C}$, on a $Q(z) \in \overline{\mathbf{Z}}$, et donc $\Pi_z(z^p) \in p\overline{\mathbf{Z}}$.

(23) (b) Comme z est racine de $X^n - 1$, le polynôme Π_z divise $P = X^n - 1$ dans $\mathbf{Q}[X]$. Étant unitaire, il le divise en fait dans $\mathbf{Z}[X]$: écrivons $P = \Pi_z D$ avec $D \in \mathbf{Z}[X]$. On a $z^p \in \mathbb{U}_n$, donc $P(z^p) = 0$. Comme $\Pi_z(z^p) \neq 0$, on a nécessairement $D(z^p) = 0$. Cela implique que $P'(z^p) = \Pi_z(z^p) D'(z^p)$. D'après la question (21) (a) & (b), on a donc

$$\varepsilon_n n^n = \Delta(P) = \Pi_z(z^p) a$$

avec $a = (-1)^{\frac{n(n-1)}{2}} D'(z^p) \prod_{\zeta \in \mathbb{U}_s \setminus \{z^p\}} P'(\zeta)$. Comme $D', P' \in \mathbf{Z}[X]$ et $\mathbb{U}_n \subset \overline{\mathbf{Z}}$, on a $a \in \overline{\mathbf{Z}}$. Comme en outre $\Pi_z(z^p) \in p\overline{\mathbf{Z}}$ d'après la question précédente, cela montre que p divise n^n dans $\overline{\mathbf{Z}}$. La question (2) (a) implique alors que p divise n^n dans $\mathbf{Z}$, de sorte que p divise n dans $\mathbf{Z}$.

(24) (a) Soit $z \in \mu_n$. Comme $\Phi_n(z) = 0$, on a $\Pi_z \mid \Phi_n$ dans $\mathbf{Q}[X]$. Soit $\zeta \in \mu_n$. Comme $z \in \mu_n$, il existe $m \in \mathbf{N}$, tel que $\mathsf{pgcd}(n, m) = 1$ et $\zeta = z^m$. Écrivons $m = p_1 \cdots p_r$ avec $p_1, \dots, p_r$ premier ne divisant pas n. Montrons par récurrence (finie) sur $k \in \{0, \dots, r\}$ que $\Pi_z(z^{p_1 \cdots p_k}) = 0$. C'est trivial pour $k = 0$. Soit $k \in \{0, \dots, r-1\}$ tel que $\Pi_z(z') = 0$ avec $z' = z^{p_1 \cdots p_{k-1}} \in \mu_n$. Comme Π_z est irréductible dans $\mathbf{Q}[X]$, on a aussi $\Pi_z = \Pi_{z'}$. Par ailleurs, comme $p_k \nmid n$, on a $\Pi_{z'}(z'^{p_k}) = 0$ (contraposée de la question précédente), *i.e.* $\Pi_z(z^{p_1 \cdots p_k}) = 0$. Finalement, on a montré que $\Pi_z(\zeta) = 0$. Comme c'est vrai pour tout $\zeta \in \mu_n$, on a donc $\Phi_n \mid \Pi_z$ dans $\mathbf{Q}[X]$, et donc $\Phi_n = \Pi_z$ (les deux sont unitaires), ce qui prouve que Φ_n est irréductible sur $\mathbf{Q}$.

(24) (b) Soit ζ une racine de P distincte de 1. Par hypothèse, c'est une racine de l'unité : soit n son ordre. Comme $P \in \mathbf{Q}[X]$ et Φ_n est le polynôme minimal de ζ sur $\mathbf{Q}$ (*cf* question précédente), on a $\Phi_n \mid P$ dans $\mathbf{Q}[X]$. Il suffit donc de traiter le cas où $P = \Phi_n$ avec $n \geq 2$. Écrivons $n = 2^r m$ avec $r \in \mathbf{N}$ et m impair. On procède par récurrence sur r.

• Si $r = 0$ *i.e.* n est impair, $\frac{n-1}{2}$ est entier et premier à n : si $\theta = \frac{n-1}{2}\frac{2\pi}{n} = \frac{n-1}{n}\pi$, on a $\theta \in \left[\frac{2\pi}{3}, \pi\right]$ $e^{i\theta} \in \mu_n$ et $\frac{2\pi}{3} \leq \theta < \pi$ (parce que $n \geq 3$).

• Si $r = 1$, on prend $\theta = \pi$ si $n = 2$ (*i.e.* $m = 1$). Si $m \geq 3$, posons $\theta = \left(1 - \frac{2}{m}\right)\pi \in \left[\frac{\pi}{3}, \pi\right]$. On a $e^{i\theta} = e^{i\pi - \frac{2i\pi}{m}} = -e^{-\frac{2i\pi}{m}}$: comme -1 est d'ordre 2 et $e^{-\frac{2i\pi}{m}}$ d'ordre m impair, $e^{i\theta}$ est d'ordre $n = 2m$.

• Supposons $r \geq 2$. Par hypothèse de récurrence, il existe $\theta' \in \left[\frac{\pi}{3}, \pi\right]$ tel que $e^{i\theta'} \in \mu_{2^{r-1}m}$. Si $\theta' \in \left[\frac{2\pi}{3}, \pi\right]$, alors $\theta = \frac{\theta}{2} \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right] \subset \left[\frac{\pi}{3}, \pi\right]$ et $e^{i\theta} \in \mu_n$. Reste à traiter le cas où $\frac{\pi}{3} \leq \theta' < \frac{2\pi}{3}$. On a alors $\frac{\pi}{6} \leq \frac{\theta'}{2} \leq \frac{\pi}{3}$: posons $\theta = \pi - \frac{\theta'}{2}$. On a $\theta \in \left[\frac{2\pi}{3}, \frac{5\pi}{6}\right] \subset \left[\frac{\pi}{3}, \pi\right]$, et $e^{i\theta} = -e^{-i\frac{\theta'}{2}}$, donc $e^{2i\theta} = e^{-i\theta'}$ est d'ordre $2^{r-1}m$, ce qui implique que $e^{i\theta}$ est d'ordre $\frac{n}{2}$ ou n. S'il était d'ordre $\frac{n}{2}$, on aurait $1 = (-1)^{2^{r-1}} = e^{i2^{r-2}m\theta'}$, et $e^{i\theta'}$ serait d'ordre divisant $2^{r-2}m$, ce qui n'est pas.

III.B. Sous-groupes abéliens finis de $\mathcal{O}_n(\mathbf{R})$

(25) Quitte à choisir une base orthonormale de E, on peut supposer que $E = \mathbf{R}^2$ (muni de sa structure euclidienne canonique) et $r_\theta = R(\theta)$. Soit alors $x = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \in \mathbf{R}^2$ tel que $\|x\|_2 = 1$, *i.e.* $x_1^2 + x_2^2 = 1$. On a

$$\begin{aligned}\|(R(\theta) - \mathrm{I}_2)x\|^2 &= \|R(\theta)x\|^2 + \|x\|^2 - 2\langle R(\theta)x | x\rangle = 2 - x_1(\cos(\theta)x_1 - \sin(\theta)x_2) + x_2(\sin(\theta)x_1 + \cos(\theta)x_2) \\ &= 2 - 2\cos(\theta)(x_1^2 + x_2^2) = 2 - 2\cos(\theta) = 4\sin^2\left(\tfrac{\theta}{2}\right)\end{aligned}$$

ce qui montre que $\|r_\theta - \mathsf{id}_E\|_{\mathrm{op}} = 2\left|\sin\left(\frac{\theta}{2}\right)\right|$.

(26) On procède par récurrence forte sur $n = \dim_{\mathbf{R}}(E)$. C'est trivial lorque $n = 1$. Supposons $n = 2$. D'après la question (6) (b), le groupe G est isomorphe à un sous-groupe de de $\{\pm \mathrm{I}_2, \pm S\}$ ou à un sous-groupe de $\mathsf{SO}(E)$. Dans le premier cas, on a $E = D \oplus D'$ où D et D' sont deux droites stables par tous les éléments de G, ce qui conclut dans ce cas.
Supposons désormais que $n > 3$. D'après la question (4), il existe un sous-espace vectoriel $F \subset E$ de dimension 1 ou 2 et stable par tous les éléments de G. Soient $x \in F^\perp$ et $g \in G$. Si $y \in F$, on a $\langle g(x)|y\rangle = \langle x|g(y)\rangle = 0$ parce que $g \in \mathcal{O}(E)$ et $g(y) \in F$. Comme c'est vrai pour tout $y \in F$, cela implique que $g(x) \in F^\perp$, et donc que $F^\perp$ est stable par tous les éléments de G. L'hypothèse de récurrence appliquée à $\{g_{|F}\}_{g\in G} \leq \mathcal{O}(F)$ et $\{g_{|F^\perp}\}_{g\in G} \leq \mathcal{O}(F^\perp)$ fournit des décompositions de F et de $F^\perp$ en somme directe de droites et de plan stables par tous les éléments de G et telles que les restrictions des éléments de G aux plans soient toutes de déterminant 1 : on en déduit une décomposition de E comme souhaité.

(27) (a) On a $\mathcal{O}(D_i) \simeq \{\pm 1\}$ pour tout $i \in \{1, \dots, k\}$: comme $G \subset \prod_{i=1}^{k} \mathcal{O}(D_i) \times G_0$, on a donc $|G| \mid 2^k\,|G_0|$.

(27) (b) Si $f \in \mathcal{L}(E)$ et $\omega \in \mathcal{O}(E)$, on a $\|(\|\,\omega \circ f)(x) = \|f(x)\|$ pour tout $x \in E$: cela implique que $\|\omega \circ f\|_{\mathrm{op}} = \max_{\|x\|=1} \|(\|\,\omega \circ f)(x) = \max_{\|x\|=1} \|f(x)\| = \|f\|_{\mathrm{op}}$. En particulier, si $g, g' \in G$, on a

$$\|g - g'\|_{\mathrm{op}} = \left\|g \circ (\mathsf{id}_E - g'g^{-1})\right\|_{\mathrm{op}} = \left\|\mathsf{id}_E - g'g^{-1}\right\|_{\mathrm{op}} \geq \varepsilon$$

(vu que $g'g^{-1} \in G$).

(27) (c) • Si $g \in G \setminus \{\mathsf{id}_E\}$, on a $g - \mathsf{id}_E \neq 0$, donc $0 < \|g - \mathsf{id}_E\|_{\mathrm{op}} \leq \|g\|_{\mathrm{op}} + \|\mathsf{id}_E\|_{\mathrm{op}} = 2$, *i.e.* $\varepsilon \in]0, 2]$.
• Si $j \in \{1, \dots, \ell\}$, le groupe $G_j := \{g_{|P_j}\}_{g\in G}$ est un sous-groupe commutatif de $\mathsf{SO}(P_j)$. Étant fini, il est cyclique (*cf* question (5)) : soit $d_j \in \mathbf{N}_{>0}$ son ordre. On a $r_{2\pi/d_j} \in G_j$. On a $2\sin\left(\frac{\pi}{d_j}\right) = \left\|r_{2\pi/d_j} - \mathsf{id}_{P_j}\right\|_{\mathrm{op}} \geq \varepsilon$ par hypothèse, d'où $\frac{\pi}{d_j} \geq \arcsin\left(\frac{\varepsilon}{2}\right)$, soit encore $d_j \leq \frac{\pi}{\arcsin\left(\frac{\varepsilon}{2}\right)}$.

(28) Soit $g \in G_0$. Il existe $\theta_1, \dots, \theta_\ell \in]-\pi, \pi]$ tels que $g_{|P_j} = r_{\theta_j}$ pour tout $j \in \{1, \dots, \ell\}$. On a alors $\chi_g = \prod_{j=1}^{\ell} (X - e^{i\theta_j})(X - e^{-i\theta_j})$: les racines de χ_g sont des racines de l'unité. Si $g \neq \mathsf{id}_E$, elles ne sont pas toutes égales à 1. Comme on a supposé que $\chi_g \in \mathbf{Q}[X]$, la question (24) (b) implique qu'une de ces racines est de la forme $e^{i\theta}$ avec $\frac{\pi}{3} \leq \theta \leq \pi$: il existe $j_0 \in \{1, \dots, \ell\}$ tel que $\frac{\pi}{3} \leq |\theta_{j_0}| \leq \pi$. On a donc

$$\|g - \mathsf{id}_E\|_{\mathrm{op}} = \max_{1\leq j\leq \ell} \left\|r_{\theta_j} - \mathsf{id}_{P_j}\right\|_{\mathrm{op}} = \max_{1\leq j\leq \ell} 2\left|\sin\left(\tfrac{\theta_j}{2}\right)\right| \geq 2\sin\left(\tfrac{\pi}{6}\right).$$

On peut donc poser $\varepsilon = 2\sin\left(\frac{\pi}{6}\right)$ et appliquer la question (25), qui fournit donc la majoration $|G_0| \leq 6^\ell$.

III.B. Sous-groupes abéliens finis de $\mathsf{GL}_n(\mathbf{Q})$

(29) L'application B est une forme bilinéaire symétrique définie positive : c'est un produit scalaire. En outre, les éléments de G sont tous des endomorphismes orthogonaux pour B, *i.e.* $G \subset \mathcal{O}(B)$. Soient $\mathfrak{B}$ la base canonique de $\mathbf{R}^n$ et $\mathfrak{B}'$ une base de $\mathbf{R}^n$ orthonormée pour B. Notons $P \in \mathsf{GL}_n(\mathbf{R})$ la matrice de changement de base de $\mathfrak{B}$ vers $\mathfrak{B}'$. Rappelons que si $X \in \mathbf{R}^n$, ses coordonnées X' dans la base $\mathfrak{B}'$ vérifient $X = PX'$. Soit $g \in G$: si $X, Y \in \mathbf{R}^n$, on a $B(gX, Y) = B(X, gY)$, soit $\left\langle P^{-1}gX | P^{-1}Y\right\rangle = \left\langle P^{-1}X | P^{-1}gY\right\rangle$ (parce que la matrice de B dans la base $\mathfrak{B}'$ est I_n), soit ${}^tX\,{}^tg\,{}^tP^{-1}P^{-1}Y = {}^tX\,{}^tP^{-1}P^{-1}gY$. Comme c'est vrai pour tous $X, Y \in \mathbf{R}^n$, on a ${}^tg\,{}^tP^{-1}P^{-1} = {}^tP^{-1}P^{-1}g$, *i.e.* ${}^tP\,{}^tg\,{}^tP^{-1} = P^{-1}gP$, ce qui signifie que $P^{-1}gP \in \mathsf{O}_n(\mathbf{R})$, *i.e.* $g \in P\mathsf{O}_n(\mathbf{R})P^{-1}$: comme c'est vrai pour tout $g \in G$, on a $G \subset P\mathsf{O}_n(\mathbf{R})P^{-1}$ et G est conjugué à un sous-groupe de $\mathsf{O}_n(\mathbf{R})$.

(30) (a) • Soit $G \subset \mathsf{GL}_n(\mathbf{Q})$ un sous-groupe commutatif. Pour tout $g \in G$, on a $\chi_g \in \mathbf{Q}[X]$. D'après la question (29), le groupe G est conjugué à un sous-groupe fini G' de $\mathcal{O}_n(\mathbf{R})$. Le groupe G' est commutatif. D'après les questions (27) (a) et (28) (qui s'applique parce que $\chi_g \in \mathbf{Q}[X]$ pour tout $g \in G'$), il existe des entiers k et ℓ tels que $k + 2\ell = n$ et $|G| = |G'| \leq 2^k 6^\ell = 2^k 6^{\frac{n-k}{2}} = 6^{\frac{n}{2}} \left(\frac{2}{\sqrt{6}}\right)^k$. Lorsque n est pair, on a donc $|G| \leq 6^{\frac{n}{2}}$. Lorsque n est impair, on a nécessairement $k > 0$, et donc $|G| \leq 6^{\frac{n-1}{2}} 2$. Dans tous les cas on a $|G| \leq c(n)$.

• Notons que dans chaque cas, le cardinal $c(n)$ est atteint : d'après la question (7) (b), il existe un sous-groupe G_6 de $\mathsf{GL}_2(\mathbf{Q})$ d'ordre 6. Lorsque $n = 2m$ est pair, on a $G_6^m \subset \mathsf{GL}_2(\mathbf{Q})^m \hookrightarrow \mathsf{GL}_n(\mathbf{Q})$ (par le morphisme $(A_1, \ldots, A_m) \mapsto \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_m \end{pmatrix}$) et $|G_6^m| = 6^m = c(n)$. Lorsque $n = 2m + 1$ est impair, on a de façon analogue $\{\pm 1\} \times G_6^m \subset \mathsf{GL}_1(\mathbf{Q}) \times \mathsf{GL}_2(\mathbf{Q})^m \hookrightarrow \mathsf{GL}_n(\mathbf{Q})$, et $|\{\pm 1\} \times G_6^m| = 2.6^m = c(n)$.

(30) (b) • Soit G un tel sous-groupe. D'après la question (28), il existe une matrice $P \in \mathsf{GL}_n(\mathbf{R})$ telle que $G' = P^{-1}GP \subset \mathcal{O}_n(\mathbf{R})$. D'après la question (26), il existe une décomposition en somme directe orthogonale $\mathbf{R}^n = \bigoplus_{i=1}^{k} D_i \oplus \bigoplus_{j=1}^{\ell} P_j$ par des sous-espaces stables par G' et tels que $g_{|P_j} \in \mathsf{SO}(P_j)$ pour tout $j \in \{1, \ldots, \ell\}$. Quitte à multiplier P par une matrice orthogonale, on peut donc supposer que

$$G' = P^{-1}GP \subset \prod_{i=1}^{k} \mathcal{O}(D_i) \times \prod_{j=1}^{\ell} \mathsf{SO}(P_j).$$

On a $\mathcal{O}(D_i) \simeq \{\pm 1\}$. Par ailleurs, on a vu dans la question (28) que pour tout $j \in \{1, \ldots, \ell\}$, on a $\left|G'_j\right| \leq 6$, où $G'_j = \{g_{P_j}\}_{g \in G'}$. Comme $|G| = |G'| = c(n)$, on a $k \leq 1$ et $\left|G'_j\right| = 6$ pour tout $j \in \{1, \ldots, \ell\}$, *i.e.* $G'_j = \mathcal{R}_6(P_j)$ (l'unique sous-groupe d'ordre 6 dans $\mathsf{SO}(P_j)$, *cf* question (5) (b)). L'égalité $|G| = c(n)$ implique alors que $G' = \prod_{i=1}^{k} \mathcal{O}(D_i) \times \prod_{j=1}^{\ell} \mathcal{R}_6(P_j)$. Cela montre que si n est pair (resp. impair), G est conjugué dans $\mathsf{GL}_n(\mathbf{R})$ au groupe $\begin{pmatrix} \mathcal{R}_6 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mathcal{R}_6 \end{pmatrix}$ (resp. $\begin{pmatrix} \{\pm 1\} & 0 & \cdots & 0 \\ 0 & \mathcal{R}_6 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \mathcal{R}_6 \end{pmatrix}$).

• On l'a vu dans la question (7) (b), le groupe $\mathcal{R}_6$ est conjugué, dans $\mathsf{GL}_2(\mathbf{R})$, à un sous-groupe de $\mathsf{GL}_2(\mathbf{Q})$. Cela montre que dans tous les cas, il existe effectivement un sous-groupe commutatif de $\mathsf{GL}_n(\mathbf{Q})$ d'ordre $c(n)$.