Mathématiques Générales : corrigé
Agrégation Externe de Mathématiques 2024

J. Le Borgne

I. Préliminaires

I.A. Commutation et trigonalisation simultanée.

1. a) Comme $u - \lambda \mathrm{id}_E$ est de la forme $P(u)$ (avec $P(X) = X - \lambda$), il suffit de démontrer le résultat général.
Soit $P \in K[X]$ et soit $F = \ker P(u)$. Soit $x \in F$. Alors $P(u)(v(x)) = v(P(u)(x)) = v(0) = 0$ car v et $P(u)$ commutent (comme v commute avec u, il commute avec les puissances de u par récurrence, donc avec les polynômes en u par linéarité). Donc $v(x) \in F$, ce qui démontre que F est stable par v.

b) Soit $u \in \mathcal{L}$ qui n'est pas une homothétie. Comme u est trigonalisable, u possède une valeur propre que l'on note λ. Soit $F = \ker(u - \lambda \mathrm{id}_E)$. Comme λ est valeur propre de u, $F \neq \{0\}$, et comme u n'est pas une homothétie, $F \neq E$. En outre, d'après la question précédente, F est stable par tous les éléments de $\mathcal{L}$ car ils commutent avec u.

2. a) Soit $u \in \mathcal{L}$. Comme $F = \mathrm{Vect}(e_1, \dots, e_m)$ est stable par u, chaque $u(e_i)$ pour $1 \leq i \leq m$ s'exprime comme combinaison linéaire des e_i pour $1 \leq i \leq m$. Les m premières colonnes de M_u ont donc leurs $n-m$ derniers coefficients nuls. Ainsi, la sous-matrice constituée des m premières colonnes de M_u est bien de la forme $\begin{pmatrix} A_u \\ 0 \end{pmatrix}$. Cela donne la forme attendue pour M_u.
De plus, pour $u, v \in \mathcal{L}$ on a $\begin{pmatrix} A_u & B_u \\ 0 & C_u \end{pmatrix} \begin{pmatrix} A_v & B_v \\ 0 & C_v \end{pmatrix} = \begin{pmatrix} A_u A v & A_u B_v + B_u C_v \\ 0 & C_u C_v \end{pmatrix}$.
Comme $M_u M_v = M_v M_u$, on en déduit que $A_u A_v = A_v A_u$, et $C_u C_v = C_v C_u$.

b) La formule du déterminant pour les matrices par blocs donne $\chi_u = \chi_{A_u} \chi_{C_u}$. En particulier, comme χ_u est scindé, χ_{A_u} et χ_{C_u} le sont aussi, donc A_u et C_u sont trigonalisables.

3. b) Pour $n \in \mathbf{N}^*$, l'hypothèse de récurrence est la suivante : « Soit E un K-espace vectoriel de dimension d avec $1 \leq d \leq n$ et soit $\mathcal{L}$ une famille d'éléments de $\mathcal{L}$(E) qui commutent entre eux et sont trigonalisables. Alors il existe une base de E dans laquelle tous les éléments de $\mathcal{L}$ ont une matrice triangulaire supérieure. »
Initialisation. Pour $d = 1$, la matrice de tout endomorphisme de E est triangulaire supérieure dans toute base, le résultat est donc acquis.
Hérédité. Supposons le résultat acquis pour $1 \leq d \leq n$, et supposons $\dim E = n+1$. Si tous les éléments de $\mathcal{L}$ sont des homothéties, alors leur matrice dans toute base est diagonale et en particulier triangulaire supérieure, donc le résultat est acquis (sans faire usage de l'hypothèse de récurrence). On peut donc supposer que $\mathcal{L}$ contient un endomorphisme qui n'est pas une homothétie. D'après la question 1, on dispose d'un sous-espace vectoriel $F \subset E$ tel que $1 \leq m = \dim F \leq n$. Soit $(e_1, \dots, e_n)$ une base de E comme à la question 2. Alors dans cette base, la matrice de $u \in \mathcal{L}$ est la

forme $\begin{pmatrix} A_u & B_u \\ 0 & C_u \end{pmatrix}$ avec A_u, C_u trigonalisables et pour tous $u, v \in \mathcal{L}$, $A_uA_v = A_vA_u$ et $C_uC_v = C_vC_u$. En appliquant l'hypothèse de récurrence à l'espace vectoriel K^m muni de la famille $(A_u)_{u\in\mathcal{L}}$ (dont on vient d'assurer qu'elle vérifie les hypothèses requises), on dispose d'une matrice $P_A \in GL_m(K)$ telle que pour tout $u \in \mathcal{L}$, $P_AA_uP_A^{-1}$ soit triangulaire supérieure. De même, en appliquant l'hypothèse de récurrence à K^{n+1-m} (ce qui est licite car $1 \leq n+1-m \leq n$) muni de la famille $(C_u)_{u\in\mathcal{L}}$, on dispose de $P_C \in GL_{n-m}(K)$ telle que $P_CC_uP_C^{-1}$ soit triangulaire supérieure. Un calcul immédiat montre alors que, si on pose $P = \begin{pmatrix} P_A & 0 \\ 0 & P_C \end{pmatrix}$, on a $P \in GL_{n+1-m}$ et PM_uP^{-1} est triangulaire supérieure. Ceci conclut le raisonnement par principe de récurrence.

b) Commençons par le cas $n = 2$. On note $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $B_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. On a $A_2B_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B_2A_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, donc $A_2B_2 \neq B_2A_2$. Pour $n \geq 2$ quelconque, on considère les matrices par blocs : $A = \begin{pmatrix} A_2 & 0 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} B_2 & 0 \\ 0 & 0 \end{pmatrix}$. On a alors immédiatement $AB \neq BA$ en effectuant le produit par blocs. En particulier, la réciproque de la propriété démontrée en a) n'est pas exacte (sauf en dimension 1 où elle est toujours vérifiée).

c) Soit $u_1, \ldots, u_n$ une telle famille. Comme ces endomorphismes sont nilpotents, ils sont trigonalisables et leur seule valeur propre est 0. Ainsi, il existe une base de E dans laquelle les matrices $M_1, \ldots, M_n$ respectives de $u_1, \ldots, u_n$ sont triangulaires supérieures strictes. Si on note $(e_1, \ldots, e_n)$ une telle base, on a pour tout $1 \leq i \leq n$ et pour tout $u \in \{u_1, \ldots, u_n\}$, $u(e_i) \in \mathrm{Vect}(\{e_j,\ j < i\})$. Une récurrence immédiate montre alors que pour tout $i \geq 1$, $\mathrm{Im}(u_i \circ \cdots \circ u_1) \in \mathrm{Vect}(\{e_j,\ j \neq n-i\})$. En particulier, $u_n \cdots u_1 = 0$.

4. Suivant l'indication de l'énoncé, fixons une base de E pour se ramener au cas où $E = \mathbf{R}^n$ et $\mathcal{L} \subset \mathcal{M}_n(\mathbf{R})$. Comme $\mathbf{C}$ est algébriquement clos, la question 3.a) montre qu'il existe $P \in GL_n(\mathbf{C})$ telle que pour tout $M \in \mathcal{L}$, $P^{-1}MP \in \mathcal{T}_n(\mathbf{C})$. Soit X la première colonne de P, alors on a $X \neq 0$ et $MX \in \mathbf{C}X$ pour tout $M \in \mathcal{L}$. Notons $X = x + iy$ avec $x, y \in \mathbf{R}^n$ et montrons que pour tout $M \in \mathcal{L}$, $F = \mathrm{Vect}(x, y)$ est stable par M. Soit $M \in \mathcal{L}$, soit $\lambda = \alpha + i\beta \in \mathbf{C}$ tel que $MX = \lambda X$ (avec $\alpha, \beta \in \mathbf{R}$). Alors, en identifiant les parties réelles et imaginaires (M est à coefficients réels) on a $Mx = \alpha x - \beta y$ et $My = \beta x + \alpha y$. Le sous-espace F est donc stable par M. Comme $X \neq 0$, $F \neq \{0\}$, donc F est de dimension 1 ou 2. C'est donc bien 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 un sous-groupe d'ordre n de $\mathbf{U}$. Soit $z \in G$, alors d'après le théorème de Lagrange, $z^n = 1$, donc $z \in \mathbf{U}_n$. En particulier, $G \subset \mathbf{U}_n$. Par égalité des cardinaux, $G = \mathbf{U}_n$.

b) Considérons l'application $\varphi : \mathbf{U} \to SO_2(\mathbf{R})$ définie par $z = e^{i\theta} \mapsto \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$: c'est un isomorphisme de groupes ($\varphi(\theta)$ est la matrice de la multiplication par z lorsque l'on identifie $\mathbf{C}$ à $\mathbf{R}^2$ en le munissant de sa base canonique $(1, i)$, ce qui justifie que φ est bien un morphisme de groupes ; l'injectivité comme la surjectivité découlent de l'écriture $e^{i\theta} = \cos\theta + i\sin\theta$). Comme $\mathbf{U}$ a pour unique sous-groupe d'ordre n le groupe $\mathbf{U}_n$, $SO_2(\mathbf{R})$ a pour unique sous groupe d'ordre n le groupe $\varphi(\mathbf{U}_n) = \left\{ \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & \sin\left(\frac{2k\pi}{n}\right) \\ -\sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix},\ 0 \leq k < n \right\}$.

6. a) Le fait que O soit orthogonalement semblable à $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ découle du théorème de réduction des endomorphismes normaux. On peut aussi le démontrer directement : soit $O \in O_2(\mathbf{R}) \setminus SO_2(\mathbf{R})$, alors $OS \in O_2(\mathbf{R})$. En particulier, $O = R(\theta)S$ pour un certain $\theta \in \mathbf{R}$. Notons alors que $R(\theta)S = SR(-\theta)$ pour tout $\theta \in \mathbf{R}$, de sorte que $O = R(\theta/2)R(\theta/2)S = R(\theta/2)SR(-\theta/2) = R(\theta/2)SR(\theta/2)^{-1}$, donc O est conjuguée à S dans $O_2(\mathbf{R})$.

Enfin, le centralisateur de S est l'ensemble des matrices $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in O_2(\mathbf{R})$ telles que $\begin{pmatrix}a & b\\ -c & -d\end{pmatrix} = \begin{pmatrix}a & -b\\ c & -d\end{pmatrix}$, c'est-à-dire les matrices diagonales de $O_2(\mathbf{R})$. C'est donc précisément le sous-groupe $\{I_2, S, -I_2, -S\}$.

b) Soit $G \subset O_2(\mathbf{R})$ un sous-groupe commutatif. Si G n'est pas inclus dans $SO_2(\mathbf{R})$, alors il existe $O \in G$ et $P \in O_2(\mathbf{R})$ tel que $O = P^{-1}SP$. Soit $g \in G$, alors $\gamma = PgP^{-1}$ vérifie $\gamma S = S\gamma$, et $\gamma \in O_2(\mathbf{R})$, donc $\gamma \in \{I_2, S, -I_2, -S\}$. Cela démontre que PGP^{-1} est un sous-groupe de $\{I_2, S, -I_2, -S\}$, et comme on a supposé que G n'est pas un sous-groupe de $SO_2(\mathbf{R})$, $G \neq \{I_2\}$ et $G \neq \{\pm I_2\}$. Ainsi, $G = P^{-1}\Gamma P$ avec $\Gamma = \{I_2, S\}$ ou bien $\Gamma = \{I_2, S, -I_2, -S\}$.
Réciproquement, les sous-groupes de $SO_2(\mathbf{R})$ et les sous-groupes conjugués à $\{I_2, S\}$ ou à $\{I_2, S, -I_2, -S\}$ sont bien abéliens, ce qui achève la classification de ces sous-groupes.

7. a) Le polynôme caractéristique de $R(\pi/3)$ est $X^2 - 2\cos(\pi/3)X + 1 = X^2 - X + 1$. C'est aussi le polynôme minimal de $R(\pi/3)$ car ce dernier est un diviseur de $X^2 - X + 1$ d'après le théorème de Cayley-Hamilton, et il ne peut pas être de degré 1 sinon $R(\pi/3)$ serait une homothétie. Ainsi, $R(\pi/3)$ est cyclique de polynôme caractéristique $X^2 - X + 1$ donc semblable à la matrice compagnon de ce polynôme, qui n'est autre que A. Donc il existe $P \in GL_2(\mathbf{R})$ telle que $R(\pi/3) = PAP^{-1}$.

b) Le groupe $\mathcal{R}_6$ est le sous-groupe de $SO_2(\mathbf{R})$ engendré par $R(2\pi/6) = R(\pi/3)$. Pour tout $k \in \mathbf{N}$, $P^{-1}R(\pi/3)^k P = A^k \in GL_2(\mathbf{Q})$, donc $R^{-1}\mathcal{R}_6 P$ est un sous-groupe de $GL_2(\mathbf{Q})$ (et même de $GL_2(\mathbf{Z})$).

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

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

8. a) Supposons que $n = 2m$ est pair, alors il est clair que l'application $A \mapsto \begin{pmatrix}0 & A\\ 0 & 0\end{pmatrix}$ est un isomorphisme (de $\mathbf{K}$-espaces vectoriels) de $\mathcal{M}_m(K)$ vers $\mathcal{V}_n(K)$. En particulier, $\dim \mathcal{V}_n(K) = m^2 = \frac{n^2}{4} = \lfloor \frac{n^2}{4} \rfloor = b(n)$.
Supposons maintenant $n = 2m+1$ impair avec $n \geq 3$, alors $\mathcal{V}_n^1(\mathbf{K})$ et $\mathcal{V}_n^2(\mathbf{K})$ sont tous deux isomorphes (en tant qu'espaces vectoriels) à $\mathcal{M}_{m,m+1}(\mathbf{K})$ et donc partagent sa dimension. On a $\dim \mathcal{V}_n^1(\mathbf{K}) = \dim \mathcal{V}_n^2(\mathbf{K}) = m(m+1) = \frac{n^2-1}{4} = b(n)$ car $\frac{n^2-1}{4} \leq \frac{n^2}{4} < \frac{n^2}{4} + 1$.

b) Notons $(e_1, \ldots, e_n)$ la base canonique de K^n. Si $n = 2m$, et $M \in \mathcal{V}_n(\mathbf{K})$, alors $\mathrm{Im}(M) \subset \mathrm{Vect}(e_1, \ldots, e_m)$ et $\mathrm{Vect}(e_1, \ldots, e_m) \subset \ker M$. Ainsi, si $M, M' \in \mathcal{V}_n(\mathbf{K})$, on a $M'M = 0$.
Le cas $n = 2m + 1$ est analogue : si $M \in \mathcal{V}_n^1(\mathbf{K})$ alors $\mathrm{Im}(M) \subset \mathrm{Vect}(e_1, \ldots, e_m)$ et $\mathrm{Vect}(e_1, \ldots, e_m) \subset \ker M$, on a donc encore $M'M = 0$ pour $M, M' \in \mathcal{V}_n^1(\mathbf{K})$. Enfin,

si $M \in \mathcal{V}_n^2(\mathbf{K})$ alors $\mathrm{Im}(M) \subset \mathrm{Vect}(e_1, \ldots, e_{m+1})$ et $\mathrm{Vect}(e_1, \ldots, e_{m+1}) \subset \ker M$, donc la même conclusion suit : pour $M, M' \in \mathcal{V}_n^2(\mathbf{K}), M'M = 0$.

9. a) On sait que $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{T}_n(\mathbf{K})$ et que $I_n = 1 \cdot I_n + 0 \in \mathcal{A}$. Il suffit donc de vérifier que $\mathcal{A}$ est stable par produit. Soient $A = \lambda I_n + M$ et $A' = \lambda' I_n + M'$ des éléments de $\mathcal{A}$. On a $A'A = \lambda\lambda' I_n + \lambda' M + \lambda M'$ car $M'M = 0$. Ainsi $A'A \in \mathcal{A}$, qui est donc bien une sous-algèbre de $\mathcal{M}_n(\mathbf{K})$. En outre, le calcul précédent montre que $A'A = AA'$, cette sous-algèbre est donc commutative. Enfin, par définition $\mathcal{A} = \mathbf{K}I_n \oplus \mathcal{V}$ (il est clair que ces deux sous-espaces sont en somme directe car $I_n \notin \mathcal{V}$, sans quoi on aurait $I_n^2 = 0$). Il en résulte que $\dim \mathcal{A} = d + 1$.

b) Soit $A = \lambda I_n + M \in \mathcal{A}^\times$, alors $\det A = \lambda^n$ (A est triangulaire) donc nécessairement $\lambda \in K^\times$. Réciproquement, soit $\lambda \in K^\times$ et $M \in \mathcal{V}$, alors $-\lambda^{-2}M \in \mathcal{V}$ et on a $(\lambda I_n + M)(\lambda^{-1} I_n - \lambda^{-2} M) = I_n + \lambda^{-1}M - \lambda^{-1}M = I_n$, donc $\lambda I_n + M$ est inversible dans $\mathcal{A}$ d'inverse $\lambda^{-1} I_n - \lambda^{-2} M$.

c) Soit $I \subset \mathcal{A}$ un idéal strict, alors I ne contient pas d'élément inversible donc $I \subset \mathcal{V} = \{0 \cdot I_n + M,\ M \in \mathcal{V}\}$. De plus, si $M \in \mathcal{V}$ et $A = \lambda I_n + M' \in \mathcal{A}$, alors $A = \lambda M \in \mathcal{V}$, donc $\mathcal{V}$ est un idéal de $\mathcal{A}$ (bilatère car $\mathcal{A}$ est commutative). Nous avons donc démontré que $\mathcal{V}$ est un idéal de $\mathcal{A}$, que tout idéal de $\mathcal{A}$ est contenu dans $\mathcal{V}$ (*i.e.* $\mathcal{V}$ est maximal pour l'inclusion et $\mathcal{V}$ est le seul idéal propre maximal pour l'inclusion dans $\mathcal{A}$) ; en général, $\mathcal{V}$ n'est pas le seul idéal de $\mathcal{A}$ car tout sous-espace vectoriel de $\mathcal{V}$ est aussi un idéal par les mêmes arguments.

10 a) D'après 9.b), on dispose d'une bijection $a : \mathbf{K}^\times \times \mathcal{V} \to A^\times$ définie par $a(\lambda, M) = \lambda(I + M)$ (tout élément de $A^\times$ est bien de cette forme, et l'injectivité est immédiate). De plus $a(\lambda, M)a(\lambda', M') = \lambda\lambda'(I_n + M' + M) = a(\lambda\lambda', M + M')$, donc a est un isomorphisme de groupes. Par ailleurs, le choix d'une base de $\mathcal{V}$ fournit un isomorphisme d'espaces vectoriels avec K^d. Un tel isomorphisme est aussi un isomorphisme de groupes, donc par composition $\mathcal{A}^\times \simeq \mathbf{K}^\times \times \mathbf{K}^d$.

b) Supposons $\mathbf{K} = \mathbf{F}_q$ avec $q = p^r$. Alors $\mathbf{K}^\times$ est cyclique d'ordre $q - 1$ donc isomorphe à $\mathbf{Z}/(q-1)\mathbf{Z}$, et $\mathbf{K}$ est un $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel de dimension r donc isomorphe à $(\mathbf{Z}/p\mathbf{Z})^r$, de sorte que K^d est isomorphe (en tant que $\mathbf{Z}/p\mathbf{Z}$-espace vectoriel et donc en tant que groupe) à $(\mathbf{Z}/p\mathbf{Z})^{rd}$. En combinant ces deux isomorphismes avec la question a), on obtient bien $A^\times \simeq \mathbf{Z}/(q-1)\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^{rd}$.

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

11. a) Démontrons d'abord par récurrence sur $k \geq 0$ que F est engendré par les éléments de la forme $u_j \circ \cdots \circ u_1(s)$ avec $1 \leq j \leq k$ et les éléments de la forme $u_{k+1} \circ \cdots \circ u_1(x)$, avec $u_i \in \mathcal{V}$, $s \in S$, $x \in E$. Le cas $k = 0$ est la définition de F. Démontrons l'hérédité. Par hypothèse de récurrence, F est engendré par les éléments de la forme $u_j \circ \cdots \circ u_1(s)$ (avec $1 \leq j \leq k$) et les éléments de la forme $u_{k+1} \circ \cdots \circ u_1(x)$. En écrivant $x = s' + \sum_{j=1}^r v_j(x_j)$ pour un certain $s' \in S$ et des $x_j \in E$, on voit qu'un élément de la forme $u_{k+1} \circ \cdots \circ u_1(x)$ s'écrit aussi comme somme de $u_{k+1} \circ \cdots \circ u_1(s')$ et d'éléments de la forme $u'_{k+2} \circ \cdots \circ u'_1(x')$ pour certains $x' \in E$, ce qui montre l'hérédité et achève la récurrence.

Le cas $k = n$ et la question 3.c) montrent alors que tout élément de F s'écrit comme somme d'éléments de la forme $u_j \circ \cdots \circ u_1(s)$ avec $1 \leq j \leq n - 1$. En particulier, si $u \in \ker \Psi$, alors pour tout $s \in S$ on a $u(s) = 0$. De plus, pour tout $x \in F$, $u(x) = 0$ car u s'annule sur tous les éléments de la forme $u_j \circ \cdots \circ u_1(s)$ (car $\mathcal{V}$ est commutatif). On a donc $u = 0$, ce qui démontre l'injectivité de Ψ.

b) Par injectivité de Ψ, $\dim \mathcal{V} \leq \dim \mathcal{L}(S, F) = \dim F \dim S = (n - \dim F) \dim F$, d'où la première inégalité. La seconde inégalité résulte d'une part du fait que pour tout

$0 \leq a \leq n$, $a(n-a) \leq n^2/4$ (ce que l'on obtient directement en étudiant la fonction $x \mapsto x(n-x)$ sur $[0,n]$, qui atteint son maximum en $x = n/2$), et d'autre part du fait que $(n - \dim F)\dim F$ est un entier, et doit donc être $\leq b(n)$.

12. a) On a démontré l'injectivité de l'application $\mathbf{K}$-linéaire Ψ. Or $\dim \mathcal{V} \leq \dim \mathcal{L}(S,F) \leq b(n)$, et comme on a supposé $\dim \mathcal{V} = b(n)$, on a $\dim \mathcal{V} = \dim \mathcal{L}(S,F)$. Le théorème du rang appliqué à Ψ montre alors que c'est un isomorphisme.

b) On a l'égalité $d(n-d) = b(n)$. Ainsi, le couple des racines du polynôme $X^2 - nX + b(n)$ est $(d, n-d)$. Mais ces racines sont aussi (m,m) si $n = 2m$, et $(m, m+1)$ si $n = 2m+1$ d'après la question 8.a). Ainsi, $d = m$ si $n = 2m$, et $d = m$ ou $d = m+1$ si $n = 2m+1$.

13. a) Par injectivité de Ψ, on a $Psi(u' \circ u) \neq 0$, donc il existe $x_1 \in S$ tel que $u' \circ u(x_1) \neq 0$.

b) Il existe $f, f' \in \mathcal{L}(S,F)$ telles que $f(x_1) = u'(x_2)$, $f(x_2) = 0$, et $f'(x_1) = 0$, $f'(x_2) = u(x_1)$ (pour toute famille libre d'un espace vectoriel, il existe une application linéaire envoyant cette famille libre sur une famille prescrite). Comme Ψ est un isomorphisme, on peut définir $v = \Psi^{-1}(f)$, $v' = \Psi^{-1}(f')$, et alors $v, v' \in \mathcal{V}$ vérifient les relation voulues.

c) On a $u'v'(x_2) = u'u(x_1) \neq 0$ et $v'u'(x_2) = v'v(x_1)$. Comme $\mathcal{V}$ est supposé commutatif, $u'v' = v'u'$, et on a donc $v'v(x_1) \neq 0$. D'autre part, $vv'(x_1) = 0$ car $v'(x_1) = 0$. En particulier, $vv' \neq v'v$, ce qui contredit la commutativité de $\mathcal{V}$. Le raisonnement par l'absurde conclut donc que $u' \circ u = 0$ pour tous $u, u' \in \mathcal{V}$.

14. Soit $\mathcal{V}$ un sous-espace vectoriel commutatif nilpotent de $\mathcal{M}_n(\mathbf{K})$ de dimension $b(n)$. D'après la question 12., on dispose d'un isomorphisme $\Psi : \mathcal{V} \simeq \mathcal{L}(S,F)$ où $E = F \oplus S$, $\dim S = m$ si $n = 2m$ et $\dim S \in \{m, m+1\}$ si $n = 2m+1$.
On fixe une base adaptée à la décomposition $K^n = F \oplus S$, on dispose alors d'un automorphisme φ envoyant cette base sur la base canonique de K^n. D'après la question 13., pour tout $u \in \mathcal{V}$, on a $u(F) = \{0\}$, et par hypothèse $u(S) \subset F$. Donc $\varphi \circ u \circ \varphi^{-1} \in \mathcal{V}_n(\mathbf{K})$ si n est pair, et si n est impair $\varphi \circ u \circ \varphi^{-1} \in \mathcal{V}_n^i(\mathbf{K})$ pour un certain $i \in \{1,2\}$ indépendant de u, selon que $\dim S = m$ ou $\dim S = m+1$. Par égalité des dimensions (la conjugaison par φ est injective) on a donc $\varphi \mathcal{V} \varphi^{-1} = \mathcal{V}_n(\mathbf{K})$ (si n pair) ou $\varphi \mathcal{V} \varphi^{-1} = \mathcal{V}_n^1(\mathbf{K})$ (si $n = 2m+1$ et $\dim S = m+1$) ou $\varphi \mathcal{V} \varphi^{-1} = \mathcal{V}_n^2(\mathbf{K})$ (si $n = 2m+1$ et $\dim S = m$). Ceci conclut la preuve du point (ii) du théorème 1.

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

15. On distingue 4 cas selon la parité de n_1 et n_2.

Cas 1. $n_1 = 2m_1$, $n_2 = 2m_2$. Alors $b(n_1) = m_1^2$, $b(n_2) = m_2^2$ et $b(n_1+n_2) = (m_1+m_2)^2 = b(n_1) + b(n_2) + 2m_1m_2 \geq b(n_1) + b(n_2) + 1$.

Cas 2. $n_1 = 2m_1$, $n_2 = 2m_2 + 1$. Alors $b(n_1) = m_1^2$, $b(n_1) = m_2(m_2+1)$ et $b(n_1+n_2) = (m_1+m_2)(m_1+m_2+1) = m_1^2 + m_2(m_2+1) + m_1(2m_2+1) \geq b(n_1) + b(n_2) + 1$.

Cas 3. $n_1 = 2m_1 + 1$, $n_2 = 2m_2$. Identique au cas 2 par symétrie.

Cas 4. $n_1 = 2m_1 + 1$, $n_2 = 2m_2 + 1$. Alors $b(n_1) = m_1(m_1+1)$, $b(n_2) = m_2(m_2+1)$ et $b(n_1+n_2) = (m_1+m_2+1)^2 = m_1(m_1+1) + (m_2+1)m_2 + 2m_1m_2 \geq b(n_1) + b(n_2) + 1$.

16. a) Il s'agit d'une version « en famille » de la décomposition de Jordan-Chevalley. Raisonnons pas récurrence sur $n = \dim E$. Le cas $n = 1$ est clair. Démontrons l'hérédité, supposons-donc le résultat valable en dimension $< n$ et démontrons-le en dimension n (avec $n \geq 2$). Soit E un $\mathbf{K}$-espace vectoriel de dimension n et $\mathcal{A}$ une sous-algèbre commutative de $\mathcal{L}(E)$. Comme $\mathbf{K}$ est algébriquement clos, tous les éléments de $\mathcal{A}$ ont leur polynôme caractéristique scindé. Si chaque élément de $\mathcal{A}$ possède une seule valeur propre, alors le résultat est acquis avec $r = 1$, $E_1 = E$, $\lambda_1(u)$ l'unique valeur propre de u et $\nu_1(u) = u - \lambda_1(u)\mathrm{Id}_E$, qui est bien nilpotent d'après le théorème de Cayley-Hamilton. On peut donc supposer qu'il existe $u \in \mathcal{A}$ ayant au moins deux

valeurs propres distinctes. Soit $u \in \mathcal{A}$, avec $\chi_u = \prod_{j=1}^{k}(X-\lambda_j)^{m_j}$ le polynôme caractéristique de u (et $k \geq 2$) alors en vertu du lemme des noyaux on peut écrire $E = F_1 \oplus \cdots \oplus F_k$ avec $F_j = \ker(u - \lambda_j \mathrm{Id}_E)^{m_j}$. D'après la question 1.a), chaque F_j est stable par tous les éléments de $\mathcal{A}$, et ils sont tous de dimension $< n$. On peut donc appliquer l'hypothèse de récurrence à F_j muni des endomorphismes induits par les éléments de $\mathcal{A}$. On obtient une décomposition pour chaque F_j, qui donne par concaténation une décomposition de E en somme directe $E = E_1 \oplus \cdots \oplus E_r$ de sous-espaces stables par tous les éléments de $\mathcal{A}$ ayant la propriété voulue.

b) Montrons le premier point par récurrence sur n. Si $n = 1$, alors $\dim \mathcal{M}_n(\mathbf{K}) = 1 = b(1)+1$ donc le résultat est vrai. Supposons le résultat acquis pour les sous-algèbres de $\mathcal{M}_d(\mathbf{K})$ avec $1 \leq d < n$, et démontrons-le pour $\mathcal{M}_n(\mathbf{K})$. Soit $\mathcal{A}$ une sous-algèbre commutative de $\mathcal{M}_n(\mathbf{K})$, on dispose alors d'une décomposition $E = E_1 \oplus \cdots \oplus E_r$ comme de 16.a). Supposons d'abord $r \geq 2$. Si on note $\mathcal{A}_i = \{u_i = u_{|E_i}^{|E_i},\ u \in \mathcal{A}\}$, on a $\mathcal{A} \simeq \bigoplus_{i=1}^{r} \mathcal{A}_i$ (l'isomorphisme étant donné par $u \mapsto (u_1, \ldots, u_r)$) et pour tout $1 \leq i \leq r$ $\mathcal{A}_i$ est une sous-algèbre commutative de $\mathcal{M}_n(E_i)$. Par hypothèse de récurrence, $\dim \mathcal{A}_i \leq b(\dim E_i)$ donc par le résultat admis suite à la question 15., on a $\dim \mathcal{A} = \sum_{1\leq i\leq r} \dim \mathcal{A}_i \leq b(n)+1$. Notons au passage que le cas d'égalité montre que cette inégalité est stricte si $n \geq 4$. Il reste à traiter le cas $r = 1$. Dans ce cas, tout élément de $\mathcal{A}$ possède une unique valeur propre ; notons $\lambda : \mathcal{A} \to \mathbf{K}$ l'application qui à $u \in \mathcal{A}$ associe son unique valeur propre. C'est un morphisme d'algèbres. L'application $\nu : \mathcal{A} \to \mathcal{M}_n(\mathbf{K})$ définie par $\nu(u) = u \mapsto u - \lambda(u)\mathrm{id}_E$ est linéaire, et à valeurs dans un sous-espace formé de matrices nilpotentes qui commutent. En particulier, d'après le Théorème 1, $\mathrm{rg}(\nu) \leq b(n)$. Par ailleurs, $\ker \nu = \{u \in \mathcal{A} \text{ t.q. } u = \lambda(u)\mathrm{id}_E\} \subset \mathbf{K}\mathrm{id}_E$ est de dimension ≤ 1. D'après le théorème du rang, $\dim \mathcal{A} \leq b(n)+1$.
Il reste à traiter point (ii). Supposons $n \geq 4$ et $\dim \mathcal{A} = b(n)+1$. Dans ce cas, comme remarqué précédemment, on a nécessairement $r = 1$. Cela implique alors que l'application ν est bien définie, et l'égalité des dimensions donne $\mathrm{rg}(\nu) = b(n)$. Ainsi, le Théorème 1 s'applique et montre que $\nu(\mathcal{A})$ est conjugué à $\mathcal{V}_n(\mathbf{K})$ si n pair, et conjugué à l'un des $\mathcal{V}_n^i(\mathbf{K})$ si n impair. En outre, on doit aussi avoir $\dim \ker \nu = 1$, de sorte que $\mathcal{A} = \mathbf{K}\mathrm{id} \oplus \nu(\mathcal{A})$ est bien conjugué à $\mathcal{A}_n(\mathbf{K})$ si n est pair, et à l'un des deux $\mathcal{A}_n^i(\mathbf{K})$ si n est impair. Ceci démontre le Théorème 2 sous l'hypothèse « $\mathbf{K}$ algébriquement clos ».

17. a) La famille $(U_i)_{1\leq i\leq m}$ est libre sur $\mathbf{K}$ donc sur Ω (le rang d'une famille de vecteurs est invariant par extension de corps, parce qu'on peut le calculer à l'aide de l'algorithme de Gauss). Donc $\mathcal{A}_\Omega$ est un sous-espace vectoriel de $\mathcal{M}_n(\Omega)$ de dimension m. En outre, par Ω-bilinéarité du produit défini sur $\mathcal{A}_\Omega^2$, $\mathcal{A}_\Omega$ est une Ω-sous-algèbre commutative de $\mathcal{M}_n(\Omega)$.

b) Soit $V_1 \subset \mathcal{M}_n(\mathbf{K})$ le sous-espace vectoriel des matrices dont la première colonne est nulle. Lorsque $n > 4$, $b(n)+1 \geq n^2/4 > n$, et $b(4)+1 = 5 > 4$. On a donc généralement $m > n$. Cela montre que la famille formée de la première colonne de chacun des $(U_i)_{1\leq i\leq m}$ est une famille liée. On dispose donc d'une combinaison linéaire nulle (mais à coefficients non nuls) de ces vecteurs. Cela montre qu'il existe $U \in \mathcal{A} \cap V_1$ non nul (car la famille $(U_i)_{1\leq i\leq m}$ est libre). Un tel U est un élément de $\mathcal{A}$ non nul et non inversible.

c) La matrice C s'écrit aussi (dans $\mathcal{M}_n(\Omega)$ sous la forme $\lambda' I_n + N'$ avec N' nilpotente. Mais C est non inversible, donc $\lambda' = 0$, ce qui montre que $C = N'$ est nilpotente. D'après le Théorème 2 dans le cas algébriquement clos, et la question 13, on a $NN' = 0$, c'est-à-dire $(M - \lambda I_n)C = 0$. Cela montre que $MC = \lambda C \in \mathcal{M}_n(\mathbf{K})$, et comme $C \neq 0$ et est à coefficients dans $\mathbf{K}$, $\lambda \in \mathbf{K}$. Par suite, $N = M - \lambda I_n \in \mathcal{M}_n(\mathbf{K})$.

d) D'après la question précédente, tout élément $M \in \mathcal{A}$ a une unique valeur propre $\lambda(M)$ et $M - \lambda(M)I_n$ est nilpotente. On peut donc développer le même argument qu'en 16.b) : l'application $\mathcal{A} \to \mathcal{M}_n(\mathbf{K})$ définie par $M \mapsto M - \lambda(M)I_n$ est linéaire et à valeurs dans un sous-espace vectoriel nilpotent de dimension $\geq b(n)$, et le théorème 1 et le théorème du rang montrent que $\mathcal{A} = \mathcal{A}_n(\mathbf{K})$ si $n \geq 4$ est pair, et $\mathcal{A} = \mathcal{A}_n(\mathbf{K})^1$ ou $\mathcal{A}_n^2(\mathbf{K})$ si n est impair.

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

18.

a) Soient $u, v \in V_G$, alors on peut écrire $u = \sum_{g\in G} \lambda_g g$, $v = \sum_{h\in G} \mu_h h$ (où les sommes sont à support fini), et donc $uv = \sum_{g,h} \lambda_g\mu_h gh \in V_G$, et $vu = uv$ par commutativité de G. De plus, $G \subset V_G \setminus \{0\}$ et $|V_G| = q^{d_G}$ donc $|G| \leq q^{d_G} - 1$.

b) Comme V_G est une sous-algèbre commutative de $\mathcal{M}_n(\mathbf{F}_q)$, on a $d_G \leq b(n)+1$. D'autre part, comme $GL_n(\mathbf{F}_q)$ contient un sous-groupe abélien d'ordre $\beta_n(q)$, on a $|G| \geq \beta_n(q)$, donc $(q-1)q^{b(n)} \leq q^{d_G} - 1$. Cela montre que $q^{d_G-b(n)-1} > 1 - 1/q \geq 1/q$ (car $q \geq 2$) donc $q^{d_G-b(n)-1} \geq 1$: on a aussi l'inégalité $d_G \geq b(n) + 1$. Il en résulte que $d_G = b(n) + 1$.
On a $G \subset V_G \cap GL_n(\mathbf{F}_q)$. Comme $\dim V_G = b(n) + 1$ et $n \geq 4$, V_G est conjuguée à $\mathcal{A}_n(\mathbf{F}_q)$ si n est pair, et à $\mathcal{A}_n^1(\mathbf{F}_q)$ ou $\mathcal{A}_n^2(\mathbf{F}_q)$ si n est impair. En particulier, d'après 9.b), $V_G^\times = V_G \cap GL_n(\mathbf{F}_q)$ et $G \subset V_G^\times$ est de cardinal $\leq \beta_q(n)$. Par maximalité, $|G| = \beta_n(q)$ et $G = V_G^\times$ est conjugué à $\mathcal{A}_n(\mathbf{F}_q)^\times$ si n est pair, et à $\mathcal{A}_n^1(\mathbf{F}_q)^\times$ ou $\mathcal{A}_n^2(\mathbf{F}_q)^\times$ si n est impair.

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

III.A. Irréductibilité des polynômes cyclotomiques.

19. a) Soit $z \in \mu_n$, alors $z^n = 1$ donc l'ordre de z divise n. Si $d|n$ avec $d \neq n$, on a $z^d = \exp(2i\pi k/n)^d = \exp(2i\pi kd/n)$ pour un certain k premier avec n, et comme exp est $2i\pi$-périodique et kd n'est pas divisible par n, $z^d \neq 1$. Ainsi, z est d'ordre exactement n. Réciproquement, si $z \in \mathbf{U}$ est d'ordre n alors $z = \exp(i\theta)$ avec $\theta \in \mathbf{R}$ tel que $n\theta \in 2\pi\mathbf{Z}$ et $d\theta \notin 2\pi\mathbf{Z}$ si d divise strictement n. Cela montre que $z = \exp(2i\pi k/n)$ avec k premier avec n, et par division euclidienne on peut supposer $1 \leq k < n$. Donc μ_n est exactement l'ensemble des éléments d'ordre n dans $\mathbf{U}$.

b) Dans $\mathbf{C}[X]$, $X^n - 1$ est scindé à racines simples. Les n racines de ce polynôme constituent un sous-groupe d'ordre $\mathbf{U}_n$ d'ordre n de $\mathbf{U}$. D'après le théorème de Lagrange, si $z \in \mathbf{U}_n$, l'ordre de z est dans D_n, et l'ensemble des éléments d'ordre d de $\mathbf{U}_n$ est l'ensemble des éléments d'ordre d de $\mathbf{U}$. Ainsi, $\mathbf{U}_n = \sqcup_{d\in D_n} \mu_d$. Cela montre que $\prod_{z\in\mathbf{U}_n}(X - z) = \prod_{d\in D_n} \prod_{z\in\mu_d}(X - z)$, d'où la relation voulue.

c) On procède par récurrence sur n. Si $n = 1$, $\Phi_n = X - 1 \in \mathbf{Z}[X]$. Supposons que pour tout $d < n$, $\Phi_d \in \mathbf{Z}[X]$. Comme $Q_n = \prod_{d|n,d<n} \Phi_d$ est unitaire, on peut effectuer la division euclidienne de X^n-1 par Q_n dans $\mathbf{Z}[X]$, et par unicité le résultat est le même que pour la division euclidienne dans $\mathbf{C}[X]$. Comme $X^n - 1 = \Phi_n Q_n$, $\Phi_n \in \mathbf{Z}[X]$.

20. a) Soit $z \in \bar{\mathbf{Z}} \cap \mathbf{Q}$. On peut écrire $z = p/q$ avec $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$ et $p \wedge q = 1$. Comme z est entier algébrique, il existe $a_0, \ldots, a_{d-1} \in \mathbf{Z}$ tels que $z^d = a_0 + a_1 z + \cdots + a_{d-1}z^{d-1}$. En multipliant par q^d, il vient $p^d = a_0 q^d + \cdots + a_{d-1}p^{d-1}q$. Ainsi, q divise p^d, donc q divise $q \wedge p^d = 1$ (car $q \wedge p = 1$). Ainsi, $q = 1$ et $z \in \mathbf{Z}$.

Si $a, b \in \mathbf{Z}$ sont non nuls et $a|b$ dans $\bar{\mathbf{Z}}$, alors $a/b \in \bar{\mathbf{Z}}$ par hypothèse, et $a/b \in \mathbf{Q}$, donc $a/b \in \mathbf{Z}$, c'est-à-dire que a divise b dans $\mathbf{Z}$.

b) Soit $z \in \bar{Z}$ et soit $\Pi_z \in \mathbf{Q}[X]$ son polynôme minimal. Il existe $P \in \mathbf{Z}[X]$ unitaire tel que $P(z) = 0$. On sait que Π_Z divise P dans $\mathbf{Q}[X]$, donc toutes les racines de Π_z dans $\mathbf{C}$ sont des entiers algébriques. En vertu des relations coefficients-racines, Π_z est à coefficients dans $\bar{\mathbf{Z}}$. Comme Π_z est à coefficients rationnels, $\Pi_z \in \mathbf{Z}[X]$.

21. a) On a défini $P(X) = \prod_{i=1}^{d}(X - z_k)$, on a donc $P'(X) = \sum_{i=1}^{d} \prod_{j\neq i}(X - z_j)$. Cela montre que

$$P'(z_i) = \prod_{j\neq i}(z_i - z_j) = \prod_{1\leq j<i}(z_i - z_j) \prod_{i<j\leq d}(z_i - z_j) = (-1)^{d-i} \prod_{1\leq j<i}(z_i - z_j) \prod_{i<j\leq d}(z_j - z_i).$$

On en déduit que

$$\prod_{1\leq i\leq d} P'(z_i) = (-1)^{\frac{d(d-1)}{2}} \prod_{1\leq j<i\leq d}(z_i - z_j) \prod_{1\leq i<j\leq d}(z_j - z_i) = (-1)^{\frac{d(d-1)}{2}} \Delta(P).$$

b) Soit $P = X^n - 1$. Alors, pour toute racine z de P, on a $P'(z) = nz^{n-1} = \frac{n}{z}$. Ainsi, $\Delta(P) = (-1)^{\frac{n(n-1)}{2}} n^n / \prod_{z^n=1} z = (-1)^{n-1+\frac{n(n-1)}{2}} n^n$ car le produit des racines de P est $(-1)^n P(0) = (-1)^{n-1}$. En posant $\varepsilon_n = (-1)^{\frac{(n-1)(n+2)}{2}}$, on a bien le résultat attendu.

22. a) Supposons que $\sigma \in \mathfrak{S}_d$ soit la transposition (i, j), avec $i < j$. Alors $U_\sigma(X_1, \ldots, X_d) = U(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = U(X_1, \ldots, X_j, \ldots, X_i, \ldots, X_d)$. On peut écrire $U =$

$$(X_j - X_i) \prod_{1\leq k<i}(X_i - X_k)(X_j - X_k) \prod_{i<k<j}(X_k - X_i)(X_j - X_k) \prod_{j<k\leq d}(X_k - X_i)(X_k - X_j) V$$

où V ne dépend pas des indéterminées X_i, X_j. ON remarque que chacun des facteurs $\prod_{1\leq k<i}(X_i - X_k)(X_j - X_k)$, $\prod_{i<k<j}(X_k - X_i)(X_j - X_k)$ et $\prod_{j<k\leq d}(X_k - X_i)(X_k - X_j)$ est invariant par la transposition (i, j), on a donc $U_\sigma = -U$. Par ailleurs, l'application $\mathfrak{S}_d \times \mathbf{Z}[X_1, \ldots, X_d] \to \mathbf{Z}[X_1, \ldots, X_d]$ définie par $P \mapsto P_\sigma$ est une action de groupes, et les transpositions engendrent $\mathfrak{S}_d$, ce qui montre que pour tout $\sigma \in \mathfrak{S}_d$, $U_\sigma = \varepsilon(\sigma)U$. Alternativement, on peut remarquer en reconnaissant la formule classique que U est le déterminant de Vandermonde associé à $X_1, \ldots, X_n$, c'est donc une quantité antisymétrique en les X_i, et donc $U(X_{\sigma(1)}, \ldots, X_{\sigma(d)}) = \varepsilon(\sigma)U$.

b) Soit $P \in \mathbf{A}[X]$ de degré d. Alors $\Delta(P) = U(z_1, \ldots, z_d)^2$, où $z_1, \ldots, z_d$ sont les racines de P dans $\mathbf{C}$. D'après la question précédente U^2 est symétrique donc on peut écrire U^2 comme un polynôme à coefficients entiers en les polynômes symétriques élémentaires $\Sigma_1, \ldots, \Sigma_d$. En particulier, $\Delta(P) = V(\Sigma_1(z_1, \ldots, z_d), \cdots, \Sigma_d(z_1, \ldots, z_d))$ pour un certain $V \in \mathbf{Z}[X_1, \ldots, X_d]$. Comme les $\Sigma_i(z_1, \ldots, z_d)$ sont au signe près les coefficients de $P \in \mathbf{A}[X]$ (relations coefficients-racines), et comme $\mathbf{A}$ est un sous-anneau de $\mathbf{C}$, on a bien $\Delta(P) \in \mathbf{A}$.

23. a) L'anneau $\mathbf{Z}[X]/p\mathbf{Z}[X]$ est de caractéristique p, donc l'élévation à la puissance p est un endomorphisme. En particulier, si $P = \sum_{i=0}^{d} a_i X^i$ alors $P(X)^p = \sum_{i=0}^{d} a_i^p X^{ip}$ mod $p\mathbf{Z}[X]$. En outre, $a_i^p - a_i \in p\mathbf{Z}$ d'après le petit théorème de Fermat, donc $P(X)^p = \sum_{i=0}^{d} a_i X^{ip} = P(X^p) \mod p\mathbf{Z}[X]$.
En particulier, $\Pi_z(X^p) - \Pi_Z(X) \in p\mathbf{Z}[X]$ et donc $\Pi_z(z^p) - 0 \in p\mathbf{Z}[z] \subset p\bar{\mathbf{Z}}$ car $\bar{\mathbf{Z}}$ est un sous-anneau et $z \in \bar{\mathbf{Z}}$.

b) Supposons $\Pi_z(z^p) \neq 0$. Comme Π_z divise $X^n - 1$, Π_Z est un produit de facteurs de la forme $X - a$ où $a \in \mu_n$, et par hypothèse z^p n'est pas racine de Π_z. Or, $\Delta(X^n - 1)$

est un produit de facteurs qui sont tous dans $\bar{\mathbf{Z}}$, et tous les $z^p - a$ (où a parcours l'ensemble des racines de Π_z) sont facteurs de $\Delta(X^n - 1)$. Cela montre que $\Pi_z(z^p)$ divise $\Delta(X^n - 1)$ dans $\bar{\mathbf{Z}}$. Donc n^n est divisible par p dans $\bar{Z}$ et comme ce sont deux entiers, cette relation de divisibilité a lieu dans $\mathbf{Z}$ donc p divise n dans $\mathbf{Z}$ car p est premier (en particulier p divise aussi n dans $\bar{\mathbf{Z}}$).

24. a) Soit $n \in \mathbf{N}^*$. Soit $z \in \mu_n$ et soit P_z son polynôme minimal. Soit $k \in \mathbf{N}$ tel que $k \wedge n = 1$. Montrons par récurrence sur le nombre r de facteurs dans la décomposition en produit de facteurs premiers de k que z^k est racine de Π_Z. Si $r = 0$, alors $k = 1$ et le résultat est clair. Supposons le résultat acquis pour r, et montrons-le pour $r + 1$. On peut écrire $k = pm$ avec p premier ne divisant pas n, et m premier avec n et produit de r facteurs premiers. Alors $z^m \in \mu_n$ et z^m est racine de Π_z par hypothèse de récurrence. On a donc $\Pi_z = \Pi_{z^m}$ par irréductibilité de Π_z (ces deux polynômes sont unitaires). Mais alors, $(z^m)^p$ est racine de Π_{z^m} d'après la question précédente donc $\Pi_z(z^k) = 0$. Ceci conclut la récurrence et montre que tous les éléments de μ_n sont racines de Π_z, donc Φ_n divise Π_z. Par irréductibilité de Π_z et comme ces deux polynômes sont unitaires, on a $\Phi_n = \Pi_z$ et Φ_n est irréductible.

b) Comme toutes les racines de P dans $\mathbf{C}$ sont des racines de l'unité, ses facteurs irréductibles sont des polynômes cyclotomiques. Comme P est non constant et a une racine différente de 1, P a un facteur de la forme Φ_n avec $n \geq 2$. Il suffit donc de montrer que tous les polynômes Φ_n ont une racine sur l'arc de cercle prescrit. Si $n = 2$, alors $-1 = \exp(i\theta)$ avec $\theta = \pi$ est racine. Si n est impair, alors en posant $k = \frac{n-1}{2}$, k est un entier premier avec n (car diviseur de $n - 1$) et $\frac{2k\pi}{n} = \pi - \frac{\pi}{n}$ est bien dans l'intervalle $[\pi/3, \pi]$. Enfin, si $n \geq 4$ est pair, montrons qu'on a l'alternative suivante : ou bien $n = 2d$ avec d impair, ou bien pour tout $z \in \mu_n$, $-z \in \mu_n$. En effet, alors soit $z \in \mu_n$. On a $(-z)^n = 1$ par parité de n, et si $d|n$ avec $d \neq n$, alors $1 = (-z)^d = (-1)^d z^d$ si et seulement si d est impair et $z^d = -1$, c'est-à-dire $n = 2d$ avec d impair. Dans ce cas, les entiers consécutifs $\frac{d+1}{2}$ et $\frac{d-1}{2}$ sont premiers avec d et l'un deux est impair. Celui-ci est donc premier avec n. Notons k cet entier, alors $\frac{2k\pi}{n} = \frac{d\pm1)\pi}{2d} \in [\pi/3, \pi]$ car $d \geq 3$. Enfin, dans le deuxième cas de l'alternative, on a pour tout $z \in \mu_n$, $-z \in \mu_n$. Par ailleurs, on a toujours $\bar{z} \in \mu_n$ lorsque $z \in \mu_n$. Ainsi, pour tout $z \in \mu_n$, $-\bar{z} \in \mu_n$. En particulier, si $z = \exp(2i\pi/n)$, on a $\exp(i\theta) \in \mu_n$ avec $\theta = \pi - \frac{2\pi}{n} \in [\pi/3, \pi]$.
Remarquons que les bornes sont atteintes : $\theta = \pi$ pour $n = 2$, et $\theta = \frac{\pi}{3}$ pour $n = 6$ (qui correspond au premier cas de l'alternative, avec $d = 3$).

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

25. Dans une base orthonormée convenable, la matrice de r_θ est $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. On en déduit que, pour $v \in E$ de norme 1, on a $\|r_\theta(v) - v\|_{op}^2 = 2(\cos\theta - 1)^2 + \sin^2\theta = 2 - 2\cos\theta = 4\sin^2\left(\frac{\theta}{2}\right)$, d'où $\|r_\theta(v) - v\|_{op} = 2\left|\sin\left(\frac{\theta}{2}\right)\right|$.

26. On raisonne par récurrence sur $\dim E$. Si $\dim E = 1$, le résultat est clair. Supposons $\dim E \geq 2$. D'après la question 4., il existe une droite ou un plan F stable par tous les éléments de G. Si $\dim E = 2$ et F est un plan, le résultat est acquis d'après la question 6b). Sinon, $E = F \oplus F^\perp$ et $F^\perp$ est stable par $\mathcal{O}(E)$ donc par tous les éléments de G. En outre, chaque élément $g \in G$ induit un endomorphisme g_F de F et un endomorphisme $g_{F^\perp}$ de $F^\perp$ qui sont respectivement dans $\mathcal{O}(F)$ et $\mathcal{O}(F^\perp)$. De plus, l'application $g \mapsto g_{F^\perp}$ est clairement un morphisme de groupes, et son image $G_{F^\perp}$ est un sous-groupe abélien de $\mathcal{O}(F^\perp)$. En appliquant l'hypothèse de récurrence à $F^\perp$ et au groupe $G_{F^\perp}$, on obtient la décomposition voulue.

27. a) L'application $\mathcal{L}(E) \to \mathcal{L}(V)$ définie par $u \mapsto u_V = u|_V^V$ est linéaire et sa restriction à G induit un morphisme de groupes $\rho : G \to GL(V)$ qui est en fait à valeurs dans $\mathcal{O}(V)$ car pour tout $u \in \mathcal{L}(E)$, $(u_V)^T = (u^T)_V$. Ceci justifie au passage que $G_0 = \ker \rho$ est un sous-groupe de G.

Soit $g \in G$. Par définition de V, chacune des droites D_i est stable par g, et pour tout $x \in D_i$, $\|g(x)\| = \|x\|$. Cela montre que, dans une base adaptée à la décomposition $V = \bigoplus_{i=1}^k D_i$, la matrice de g_V est de la forme $\begin{pmatrix} \pm 1 & 0 & \cdots & 0 \\ 0 & \pm 1 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & \cdots & 0 & \pm 1 \end{pmatrix}$. En particulier, l'image de G par ρ est contnue dans le sous-groupe de $\mathcal{O}(V)$ formé des matrices diagonales (à coefficients diagonaux ± 1), qui est d'ordre 2^k. Le premier théorème d'isomorphisme montre que $|G| = |G_0||\rho(G)| = 2^p|G_0|$ où $p \leq k$, qui divise $2^k|G_0|$.

b) Soit $g \in \mathcal{O}(E)$ et $x \in E$, alors $\|g(x) - x\| \leq \|g(x)\| + \|x\| = 2\|x\|$, donc $0 \leq \|g - \mathrm{id}_E\|_{op} \leq 2$. En outre, si $g \neq \mathrm{id}_E$ alors $\|g - \mathrm{id}_E\|_{op} > 0$. Comme G est fini et $G_0 \neq \{\mathrm{id}_E\}$, ε est bien défini et vérifie donc $0 < \varepsilon \leq 2$.

Soient $g, g' \in G$ et soit $x \in E$. On a $\|g(x) - g'(x)\| = \|g'((g')^{-1}g(x) - x)\| = \|(g')^{-1}g(x) - x\|$. Ainsi, $\|g - g'\|_{op} = \|(g')^{-1}g - \mathrm{id}_E\|_{op}$, et $(g')^{-1}g \in G$ car G est un groupe. Il suffit donc de montrer que pour tout $g \in G$, $\|g - \mathrm{id}_E\| \geq \varepsilon$. Supposons que $g \notin G_0$, alors il existe $1 \leq i \leq k$ tel que $g_{|D_i} \neq \mathrm{id}_{D_i}$. Soit e_i un vecteur directeur de D_i, on a alors $g(e_i) = -e_i$ (D_i est stable par g et $g \in \mathcal{O}_n(\mathbf{R})$) donc $\|g - id_E\|_{op} \geq \|g(e_i) - e_i\| = 2 \geq \varepsilon$. Comme cette inégalité est valable aussi pour $g \in G_0$ par définition, on a bien démontré le résultat.

c) L'application $G_0 \to \mathcal{O}(W)$ définie par $g \mapsto g_{|W}$ est un morphisme de groupes, et a pour noyau $\{g \in G_0 \text{ t.q. } g_{|W} = \mathrm{id}_W\} = \{\mathrm{id}_E\}$ car $E = V \oplus W$. Pour $1 \leq j \leq \ell$, notons $g_j = g_{|P_j}$. Alors l'application $\varphi : G_0 \to \mathcal{O}(P_1) \times \cdots \times \mathcal{O}(P_\ell)$ définie par $g \mapsto (g_1, \ldots, g_\ell)$ est un morphisme de groupes, injectif d'après ce qui précède. D'après les questions 5.b) et 6.b), pour tout $1 \leq j \leq \ell$, il existe un entier $n_j \geq 1$ tel que $\Gamma_j = \{g_j, g \in G_0\} = \langle r_{\theta_j} \rangle$ avec $\theta_j = \frac{2\pi}{n_j}$ (et r_{θ_j} désigne la rotation d'angle θ_j dans P_j). D'après la question 25, pour tout $1 \leq j \leq r$, $\|r_{\theta_j} - \mathrm{id}_{P_j}\|_{op} = 2\left|\sin\left(\frac{\theta_j}{2}\right)\right|$. Par définition de ε, pour tout $1 \leq j \leq \ell$, $2\left|\sin\left(\frac{\theta_j}{2}\right)\right| \geq \varepsilon$. On a donc pour tout $1 \leq j \leq \ell$, $\frac{\pi}{n_j} \geq \mathrm{Arcsin}(\varepsilon/2)$ (le second membre est bien défini et strictement positif car $\varepsilon \in]0, 2]$, et l'inégalité découle de la croissance de Arcsin), et en particulier, $n_j \leq \frac{\pi}{\mathrm{Arcsin}(\varepsilon/2)}$. Ainsi, $\varphi(G_0) = \Gamma_1 \times \Gamma_\ell$ avec pour tout $1 \leq j \leq \ell$, $|\Gamma_j| \leq \frac{\pi}{\mathrm{Arcsin}(\varepsilon/2)}$. Il en résulte $|G_0| \leq \left\lceil \frac{\pi}{\mathrm{Arcsin}(\varepsilon/2)} \right\rceil^\ell$.

28. On suppose que pour tout $g \in G$, $\chi_g \in \mathbf{Q}[X]$. On peut supposer que $G_0 \neq \{\mathrm{id}_E\}$. Soit $g \in G_0 \setminus \{\mathrm{id}_E\}$. Comme g est d'ordre fini, les racines de χ_g sont des racines de l'unité et g est diagonalisable sur $\mathbf{C}$. Comme $g \neq \{\mathrm{id}_E\}$, χ_g a au moins une racine différente de 1. D'après la question 24, χ_g a au moins une racine de la forme $\exp(i\theta)$ avec $\theta \in [\pi/3, \pi]$. Soit $\theta \in [0, \pi]$ maximal tel que $\exp(i\theta)$ soit valeur propre de g, alors le rayon spectral de $(g - \mathrm{id}_E)(g - \mathrm{id}_E)^T$ est $\|g - \mathrm{id}_E\|_{op}^2 = |e^{i\theta} - 1|^2$. On a donc $\|g - \mathrm{id}_E\|_{op}^2 = 2\sin(\theta/2) \geq 2\sin(\pi/6) = 1$. On peut donc appliquer le résultat précédent avec $\varepsilon \geq 1$, ce qui donne directement $|G_0| \leq 6^\ell$.

III.C. Sous-groupes abéliens finis de $GL_n(\mathbf{Q})$

29. Fixons un produit scalaire quelconque sur $E = \mathbf{R}^n$ et considérons l'application B définie par l'énoncé. Il est clair que B est un produit scalaire, donc (E, B) est un espace euclidien. On

vérifie en outre que pour tous $x, y \in E$ et $g \in G$, $B(g(x), g(y)) = B(x, y)$. En particulier, pour tout $g \in G$, $g \in \mathcal{O}(E)$. Cela montre que G est un sous-groupe de $\mathcal{O}(E) \simeq \mathcal{O}_n(\mathbf{R})$, car (E, B) est isomorphe à l'espace euclidien $\mathbf{R}^n$ muni de son produit scalaire canonique (car les formes quadratiques associées ont la même signature $(n, 0)$).

30. Soit $G \subset GL_n(\mathbf{Q})$ un sous-groupe fini.

a) D'après la question 29, G est conjugué à un sous-groupe Γ de $\mathcal{O}_n(\mathbf{R})$. Le polynôme caractéristique étant invariant par conjugaison, tous les éléments de Γ ont un polynôme caractéristique à coefficients dans $\mathbf{Q}$. D'après la partie III.B, il existe des entiers k, ℓ tels que $|G| = |\Gamma| \leq 2^k 6^\ell$, avec $k + 2\ell = n$. Comme $2 \leq 6$, cette quantité est majorée par $c(n)$. Cela montre que $|G| \leq c(n)$.

b) Commençons par vérifier que le groupe $GL_n(\mathbf{Q})$ possède bien un sous-groupe d'ordre $c(n)$. Si n est pair, on note Γ_n le sous-groupe des matrices diagonales par blocs de taille 2, dont les blocs diagonaux sont dans $\mathcal{R}_6 \subset GL_2(\mathbf{Q})$. Si n est impair, on note Γ_n le sous-groupe des matrices diagonales par blocs avec 1 bloc de taille 1 et $\frac{n-1}{2}$ blocs de taille 2, dont l'élément diagonal est ± 1 et dont les blocs diagonaux de taille 2 sont dans $\mathcal{R}_6 \subset GL_2(\mathbf{Q})$. On voit que par définition, $\Gamma_n \simeq \mathcal{R}_6^{n/2}$ si n est pair, et $\Gamma_n \simeq \{\pm 1\} \times \mathcal{R}_6^{(n-1)/2}$ si n est impair. On a donc bien $|\Gamma_n| = c(n)$ dans les deux cas.

Il reste à démontrer que tout sous-groupe abélien d'ordre n de $GL_n(\mathbf{Q})$ est conjugué à Γ_n. Soit donc $G \subset GL_n(\mathbf{Q})$ un sous-groupe abélien d'ordre $c(n)$. D'après la remarque admise par l'énoncé, il suffit de démontrer que G est conjugué dans $GL_n(\mathbf{R})$ à Γ_n. Enfin, d'après la question 29, G est conjugué à un sous-groupe abélien de $\mathcal{O}_n(\mathbf{R})$ dont tous les éléments ont un polynôme caractéristique à coefficients rationnels. Il suffit donc de démontrer le résultat suivant :

« Soit $G \subset \mathcal{O}_n(\mathbf{R})$ un sous-groupe abélien d'ordre $c(n)$ dont tous les éléments ont un polynôme caractéristique à coefficients rationnels. Alors G est conjugué à Γ_n dans $GL_n(\mathbf{R})$. »

On suppose désormais donné un tel sous-groupe G. Pour obtenir l'égalité $|G| = c(n)$, le cas d'égalité doit être atteint dans toutes les inégalités des questions 28 et 30.a). En particulier, dans la décomposition de la question 26, $\ell = \lfloor \frac{n}{2} \rfloor$ et $k = n - 2\ell$, et pour tout $1 \leq j \leq \ell$, si comme en 28.c), G_j désigne l'image de G par le morphisme $g \mapsto g_{P_j}$, on a $|G_j| = 6$ et G_j est un sous-groupe abélien de $SO(P_j)$, donc G_j est conjugué à $\mathcal{R}_6$, donc G_W est conjugué à $\mathcal{R}_6^{k/2} \subset GL_n(\mathbf{R})$. Enfin, dans le cas où n est impair, on doit aussi avoir $|G_V| = 2$ (où G_V désigne l'image de G par le morphisme canonique $G \to \mathcal{O}(V)$), ce qui montre que $G_V = \{\pm 1\}$. En conclusion le groupe G est bien conjugué dans $GL_n(\mathbf{R})$ au groupe Γ_n, ce qui conclut la démonstration.