Agrégation interne de mathématiques

Mathématiques générales 2003

24 septembre 2024

Première partie - Généralités

(I-1) (a) Soit $x \in V$. On a

$$x \in T_\lambda \Leftrightarrow vuv^{-1}(x) = \lambda x \Leftrightarrow u(v^{-1}(x)) = \lambda(v^{-1}(x)) \Leftrightarrow v^{-1}(x) \in U_\lambda \Leftrightarrow x \in v(U_\lambda)$$

ce qui montre que $T_\lambda = v(U_\lambda)$.

(I-1) (b) Comme u et v commutent, on a $t = u$, d'où $T_\lambda = U_\lambda$: la question précédente montre que $v(U_\lambda) = U_\lambda$.

(I-1) (c) D'après la question précédente, v induit un endomorphisme $v_{|U_\lambda}$ de U_λ. Comme v est diagonalisable, il existe un polynôme $P \in \mathbf{C}[X]$ à racines simples tel que $P(v) = 0$: par restriction, $P(V_{|U_\lambda}) = 0$, ce qui montre que $v_{|U_\lambda}$ est diagonalisable.

(I-2) Soit $u \in \mathsf{GL}(V)$ d'ordre fini : notons $d \in \mathbf{N}_{>0}$ son ordre. Cela signifie que $X^d - 1 \in \mathbf{C}[C]$ est un polynôme annulateur de u. Comme $X^d - 1$ est à racines simples (ses racines sont les d racines primitives d-èmes de l'unité), cela implique que u est diagonalisable.

(I-3) On procède par récurrence sur n, le cas $n = 1$ étant trivial : supposons $n > 1$. On peut bien entendu supposer X non vide (sinon il n'y a rien à faire). Si X est uniquement constitué d'homothéties, alors toute base de V est une base de codiagonalisation : supposons désormais qu'il existe $u \in X$ qui n'est pas une homothétie. Soit $\lambda \in \mathrm{Sp}(u)$: notons $U_\lambda = \mathrm{Ker}(u - \lambda \,\mathsf{Id}_V)$ le sous-espace propre associé, et W la somme des autres sous-espaces propres de u : on a $\dim_{\mathbf{C}}(U_\lambda) < n$ et $\dim_{\mathbf{C}}(W) < n$. Comme u est diagonalisable, on a $V = U_\lambda \oplus W$. Si $v \in X$, la question 1.c montre que v induit un endomorphisme diagonalisable de U_λ et un endormorphisme diagonalisable de W. Notons X_λ (resp. X_W) l'ensemble des endomorphismes de de U_λ (resp. W) induits par les éléments de X. Ce qui précède montre que l'hypothèse de récurrence s'applique à X_λ et X_W : il existe des bases $\mathfrak{B}_1$ et $\mathfrak{B}_2$ de U_λ et W respectivement, dans lesquelles les matrices des éléments de X_λ et X_W sont diagonales. La base $\mathfrak{B}_1 \cup \mathfrak{B}_2$ est alors une base de codiagonalisation des éléments de X.

(I-4) Si $z \in \mathbf{C}$, posons $M_z = \left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right) \in \mathsf{GL}_2(\mathbf{C})$. L'application

$$\begin{aligned} \varphi\colon\ \mathbf{C} &\to \mathsf{GL}_2(\mathbf{C}) \\ z &\mapsto M_z \end{aligned}$$

est un morphisme de groupes injectif : son image est un sous-groupe abélien G de $\mathsf{GL}_2(\mathbf{C})$. Comme M_1 n'est pas diagonalisable (sinon, sa seule valeur propre étant 1, il serait semblable, donc égal, à I_2, ce qui n'est pas). Cela montre que G n'est pas diagonalisable.

(I-5) Pour $x, y \in V$, posons

$$\Phi(x,y) = \tfrac{1}{|G|} \sum_{\gamma \in G} \Psi(\gamma(x), \gamma(y)).$$

C'est une forme sesquilinéaire sur V. Si $x \in V \setminus \{0\}$, on a $\Psi(\gamma(x), \gamma(x)) > 0$ pour tout $\gamma \in G$ (parce que Ψ est définie positive), ce qui montre que $\Phi(x,x) > 0$, et donc que Φ est définie positive. Enfin, si $g \in G$, l'application $\gamma \mapsto \gamma g$ est une permutation de G, ce qui montre que

$$\Phi(g(x), g(y)) = \tfrac{1}{|G|} \sum_{\gamma \in G} \Psi(\gamma g(x), \gamma g(y)) = \Phi(x,y)$$

et donc que g est unitaire pour Φ.

(I-6) Notons Ψ le produit scalaire hermitien canonique sur $V = \mathbf{C}^n$. Soit $G \leq \mathsf{GL}_n(\mathbf{C})$ un sous-groupe fini : la question précédente fournit un produit scalaire hermitien Φ pour lequel les éléments de G sont unitaires. Notons $\mathfrak{B}_0$ la base canonique de $\mathbf{C}^n$, $\mathfrak{B}$ une base orthonormée pour Φ et $P \in \mathsf{GL}_n(\mathbf{C})$ la matrice de changement de base de $\mathfrak{B}_0$ à $\mathfrak{B}$. Soient $x, y \in V$: les vecteurs colonne des coordonnées de x et y dans la base $\mathfrak{B}$ sont $P^{-1}x$ et $P^{-1}y$ respectivement. On a donc $\Phi(x,y) = (P^{-1}x)^*(P^{-1}y) = x^*P^{-1*}P^{-1}y$. Si $g \in G$, on a $\Phi(gx, gy) = \Phi(x,y)$, donc $x^*g^*P^{-1*}P^{-1}gy = x^*P^{-1*}P^{-1}y$ pour tout $x, y \in \mathbf{C}^n$. Cela équivaut à $g^*P^{-1*}P^{-1}g = P^{-1*}P^{-1}$, soit $(P^{-1}gP)^*(P^{-1}gP) = \mathrm{I}_n$, *i.e.* $P^{-1}gP \in \mathsf{U}_n$. Comme c'est vrai pour tout $g \in G$, on a $P^{-1}GP \leq \mathsf{U}_n$, et G est conjugué à un sous-groupe de U_n.

Deuxième partie - Le cas où n vaut 2

(II-A-1) (a) Soit $\mathfrak{B}$ une base *orthogonale* de V : on a un isomorphisme $f\colon \operatorname{End}(V) \xrightarrow{\sim} \mathsf{M}_2(\mathbf{C});\ g \mapsto \mathsf{Mat}_{\mathfrak{B}}(g)$. Soit $g \in \operatorname{End}(V)$ et $M = \mathsf{Mat}_{\mathfrak{B}}(g)$. Comme $\mathfrak{B}$ est orthogonale, on a $\mathsf{Mat}_{\mathfrak{B}}(g^*) = M^*$. Cela implique que $g \in E$ si et seulement si $M = M^*$ et $\operatorname{Tr}(M) = 0$. Écrivons $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$: les conditions qui précèdent équivalent à $a, d \in \mathbf{R}$, $c = \overline{b}$ et $a + d = 0$, soit encore $M = \left(\begin{smallmatrix} a & b \\ \overline{b} & -a \end{smallmatrix}\right)$ avec $a \in \mathbf{R}$ et $b \in \mathbf{C}$. Cela montre que $\dim_{\mathbf{R}}(E) = 3$

(II-A-1) (b) Conservons les notations de la question précédente. Si $g \in E$, on a $\mathsf{Mat}_{\mathfrak{B}}(g) = \left(\begin{smallmatrix} a & b \\ \overline{b} & -a \end{smallmatrix}\right)$, ce qui implique que $q(g) = -\det(g) = -\det(M) = a^2 + |b|^2$, et montre que q est une forme quadratique définie positive sur E.

Remarque. Point de vue plus conceptuel : soit $g \in \operatorname{End}(V)$. D'après le théorème de Cayley-Hamilton, on a $g^2 - Tr(g)g + \det(g)\,\mathsf{Id}_V = 0$. En prenant la trace, on a $\operatorname{Tr}(g^2) - \operatorname{Tr}(g)^2 + 2\det(g) = 0$, *i.e.* $-\det(g) = \frac{1}{2}\big(\operatorname{Tr}(g^2) - \operatorname{Tr}(g)^2\big)$. Cela montre que l'application $g \mapsto -\det(g)$ est une forme quadratique sur $\operatorname{End}(V)$ (la forme polaire associée est $(g_1, g_2) \mapsto \frac{1}{2}\big(\operatorname{Tr}(g_1g_2) - \operatorname{Tr}(g_1)\operatorname{Tr}(g_2)\big)$. La forme quadratique q n'est autre que la restriction de la précédente à $E \subset \operatorname{End}(V)$, et sa forme polaire est $(g_1, g_2) \mapsto \frac{1}{2}\operatorname{Tr}(g_1g_2)$ d'après ce qui précède.

(II-A-1) (c) Avec les notations de la question (II-A-1) (a), l'isomorphisme $f\colon \operatorname{End}(V) \xrightarrow{\sim} \mathsf{M}_2(\mathbf{C})$ induit un isomorphisme

$$E \xrightarrow{\sim} \{M \in \mathsf{M}_2(\mathbf{C})\,;\ M = M^*,\ \operatorname{Tr}(M) = 0\} = \operatorname{Vect}\{M_1, M_2, M_3\}$$

où $M_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $M_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $M_3 = \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right)$. On a $q(xM_1 + yM_2 + zM_3) = x^2 + y^2 + z^2$ (*cf* question précédente) : en polarisant, il vient

$$B(xM_1 + yM_2 + zM_3, x'M_1 + y'M_2 + z'M_3) = xx' + yy' + zz'.$$

Remarque. Comme on l'a vu dans la remarque précédente, on a $B(g_1, g_2) = \frac{1}{2}\operatorname{Tr}(g_1g_2)$.

(II-A-2) Comme $a \in \mathsf{U}(V)$, on a $a^* = a^{-1}$. Si $x \in E$, on a $x^* = x$, et donc

$$(axa^{-1})^* = (axa^*)^* = a^{**}x^*a^* = axa^{-1}$$

ce qui montre que $axa^{-1} \in \operatorname{End}(V)$ est hermitien. En outre, on a $\operatorname{Tr}(axa^{-1}) = \operatorname{Tr}(x) = 0$ vu que $x \in E$: cela montre que $axa^{-1} \in E$.

(II-A-3) Si $x \in E$, on a $q(\varphi(a)(x)) = q(axa^{-1}) = -\det(axa^{-1}) = -\det(x) = q(x)$, ce qui montre que $\varphi(a) \in \mathsf{O}(q)$.

(II-A-4) (a) Soit $a \in \operatorname{Ker}(\varphi)$: on a $\varphi(a) = \mathsf{Id}_E$. Pour tout $x \in E$, on a donc $\varphi(a)(x) = x$, *i.e.* $ax = xa$. Raisonnons matriciellement : soient $\mathfrak{B}$ une base orthonormée V et $U = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathsf{M}_2(\mathbf{C})$ la matrice de a dans $\mathfrak{B}$. Avec les notations de la question (II-A-1) (c), la matrice U commute aux matrices M_1, M_2 et M_3. L'égalité $UM_1 = M_1U$ implique que $\beta = \gamma = 0$. L'égalité $UM_2 = M_2U$ implique que $\alpha = \delta$, ce qui montre que $U = \alpha\,\mathrm{I}_2$. Comme $U \in \mathsf{U}_2$, on a en outre $|\alpha| = 1$: on en déduit que $a = \alpha\,\mathsf{Id}_V$. Réciproquement, si $\alpha \in \mathbf{C}$ est de module 1 et $a = \alpha\,\mathsf{Id}_V$, on a $\varphi(a) = \mathsf{Id}_E$. On a donc $\operatorname{Ker}(\varphi) = \{\alpha\,\mathsf{Id}_V\}_{\alpha \in U}$, où $U = \{\alpha \in \mathbf{C}^\times\,;\ |\alpha| = 1\}$.

(II-A-4) (b) Comme $a \in \mathsf{U}(V)$, l'endomorphisme a est diagonalisable en base orthonornée, est ses valeurs propres appartiennent au groupe U des nombres complexes de module 1 : il existe une base orthonormée $\mathfrak{B} = (e_1, e_2)$ de V et $\alpha_1, \alpha_2 \in U$ tels que $a(e_k) = \alpha_k e_k$ pour tout $k \in \{1, 2\}$. Il existe $\theta \in \mathbf{R}$ tel que $\alpha_1\alpha_2^{-1} = e^{i\theta}$ (comme a n'est pas une homothétie vu que $a \notin \operatorname{Ker}(\varphi)$, on a $\alpha_1 \neq \alpha_2$, et donc $\theta \notin 2\pi\mathbf{Z}$). Notons $g_1, g_2, g_3 \in \operatorname{End}(V)$ les éléments dont les matrices dans la base $\mathfrak{B}$ sont M_1, M_2 et M_3 respectivement. D'après le question (II-A-1) (c), la famille $\mathscr{B} := (g_1, g_2, g_3)$ est une base orthonormée de E (pour q) : cette dernière fournit une orientation de E. Comme $\mathsf{Mat}_{\mathfrak{B}}(a) = A := \operatorname{diag}(\alpha_1, \alpha_2)$, et $AM_1A^{-1} = M_1$,

$AM_2A^{-1} = \left(\begin{smallmatrix} 0 & e^{i\theta} \\ e^{-i\theta} & 0 \end{smallmatrix}\right) = \cos(\theta)M_2 + \sin(\theta)M_3$ et $AM_3A^{-1} = \left(\begin{smallmatrix} 0 & ie^{i\theta} \\ -ie^{i\theta} & 0 \end{smallmatrix}\right) = -\sin(\theta)M_2 + \cos(\theta)M_3$, la matrice de $\varphi(a)$ dans la base orthonormée $\mathscr{B}$ est $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{smallmatrix}\right)$. Cela montre que $\varphi(a)$ est la rotation d'axe $\mathrm{Vect}(g_1)$ et d'angle θ.

(II-A-4) (c) D'après la question précédente, on a $\varphi(\mathsf{U}(V)) \subset \mathsf{SO}(q) \simeq \mathsf{SO}_3(\mathbf{R})$. Montrons que c'est une égalité : soit $\rho \in \mathsf{SO}(q)$. C'est une rotation : soit $\gamma \in E$ un vecteur directeur unitaire de son axe. On a $\gamma \in E$ et $q(\gamma) = 1$, *i.e.* $\mathrm{Tr}(\gamma) = 0$ et $\det(\gamma) = -1$: le théorème de Cayley-Hamilton implique que $\gamma^2 - \mathsf{Id}_V = 0$, soit encore que γ est une symétrie, orthogonale vu que $\gamma \in E$ est hermitien. Il existe donc une base orthonormale (e_1, e_2) de V dans laquelle la matrice de γ est $\mathrm{diag}(1, -1) = M_1$ (rappelons que $\mathrm{Tr}(\gamma) = 0$). Soit θ l'angle de ρ (avec l'orientation de son axe donnée par θ). Notons $a \in \mathsf{U}(V)$ l'endomorphisme unitaire de V dont la matrice dans la base (e_1, e_2) est $\mathrm{diag}(e^{i\theta}, 1)$. La question précédente montre que $\varphi(a) = \rho$, ce qui conclut.

(II-A-5) D'après la question (II-A-4), le morphisme φ induit un isomorphisme $\mathsf{U}(V)/U\,\mathsf{Id}_V \xrightarrow{\sim} \mathsf{SO}(q)$. Soit $a \in \mathsf{U}(V)$: il existe une base orthonormée de V dans laquelle la matrice de a est $\mathrm{diag}(\alpha_1, \alpha_2)$, où $\alpha_1, \alpha_2 \in U$. Comme $\mathbf{C}$ est algébriquement clos, il existe $\alpha \in \mathbf{C}$ tel que $\alpha^2 = \alpha_1\alpha_2$. On a bien sûr $\alpha \in U$ et $\alpha^{-1}a \in \mathsf{SU}(V)$. Cela montre que l'application $\mathsf{SU}(V) \to \mathsf{U}(V)/U\,\mathsf{Id}_V$ induite par l'inclusion $\mathsf{SU}(V) \subset \mathsf{U}(V)$ est surjective. Son noyau est $\mathsf{SU}(V) \cap U\,\mathsf{Id}_V = \{\alpha\,\mathsf{Id}_V\,;\, \alpha \in \mathbf{C},\, \alpha^2 = 1\} = \{\pm\,\mathsf{Id}_V\}$. On en déduit un morphisme surjectif $\pi\colon \mathsf{SU}(V) \to \mathsf{SO}(q)$ de noyau $\{\pm\,\mathsf{Id}_V\}$.
Munissons $\mathbf{R}^3$ de sa structure canonique d'espace affine sur $\mathbf{R}$. On dispose d'un iscosaèdre régulier Ξ, qu'on peut supposer centré en 0 (quitte à faire une translation). On sait (admet ?) que le groupe Γ des isométries positives de Ξ est isomorphe au groupe alterné $\mathfrak{A}_5$. Posons $G = \pi^{-1}(\Gamma)$: d'après ce qui précède, on a $G/\{\pm\,\mathsf{Id}_V\} \xrightarrow{\sim} \Gamma \simeq \mathfrak{A}_5$. Le sous-groupe $G \subset \mathsf{SU}(V)$ est donc fini d'ordre 120, et si $A \subset G$ est un groupe abélien, alors $\pi(A)$ est un sous-groupe abélien de $\Gamma \simeq \mathfrak{A}_5$. Ce dernier est simple non abélien : on a $\pi(A) = \{e\}$, ce qui montre que $A \subset \{\pm\,\mathsf{Id}_V\}$, et donc que A est d'indice ≥ 60.

(II-B-1) (a) Il existe $a \in G \setminus Z$ tel que $a(D) = D$: on a $(gag^{-1})(g(D)) = g(D)$, ce qui montre que $g(D)$ est une droite propre de $gag^{-1} \in G \setminus Z$, et donc que $g(D) \in \mathcal{D}$.

(II-B-1) (b) Si $g_1, g_2 \in G$, on a $(g_1g_2)(D) = g_1(g_2(D))$ et bien sûr $\mathsf{Id}_V(D) = D$. Cela fournit une action de G sur $\mathcal{D}$, soit encore un morphisme de groupes $\sigma\colon G \to \mathfrak{S}_{\mathcal{D}}$. Si $g \in Z$ et $D \in \mathcal{D}$, on a bien sûr $g(D) = D$, ce qui montre que$\sigma(g) = \mathsf{Id}_{\mathcal{D}}$, et donc que $Z \subset \mathrm{Ker}(\sigma)$. Le morphisme σ se factorise donc en un morphisme de groupes $H = G/Z \to \mathfrak{S}_{\mathcal{D}}$, ce qui signifie précisément que l'action qui précède induit une action de H sur $\mathcal{D}$.

(II-B-2) (a) Soit $D \in \mathcal{D}$. Par hypothèse, il existe $a \in G \setminus Z$ tel que $a(D) = D$, *i.e.* $\overline{a} \cdot D = D$, où $\overline{a}$ désigne l'image de a dans le quotient $H = G/Z$. Comme $a \notin Z$, l'image $\overline{a}$ fournit un élément non trivial du stabilisateur de D : ce dernier n'est donc pas réduit à l'élément neutre. Il est donc d'ordre $e_D > 1$.

(II-B-2) (b) Posons $\mathscr{E} = \{(h, D) \in (H \setminus e) \times \mathcal{D}\,;\, h \cdot D = D\}$ (où e désigne l'élément neutre de H). On dénombre $\mathscr{E}$ de deux façons différentes. Comme tout élément de $G \setminus Z$ a exactement deux droites propres, pour tout $h \in H \setminus \{e\}$, on a $\#\{D \in \mathscr{D}\,;\, h \cdot D = D\} = 2$, ce qui montre que $\#\mathscr{E} = 2(m-1)$. Par aiileurs, on a

$$\#\mathscr{E} = \sum_{D \in \mathscr{D}} \#\{h \in H \setminus \{e\}\,;\, h \cdot D = D\} = \sum_{D \in \mathscr{D}} (e_D - 1)$$

par définition de e_D.

(II-B-3) Écrivons $D' = g(D)$ avec $g \in G$. Si $a \in G$, on a

$$a(D') = D' \Leftrightarrow ag(D) = g(D) \Leftrightarrow g^{-1}ag(D) = D$$

ce qui prouve de l'application $h \mapsto \overline{g}h\overline{g}^{-1}$ fournit une bijection du stabilisateur de D dans H sur celui de D'. Ces deus stabilisateurs ont donc même ordre, *i.e.* $e_{D'} = e_D$.

(II-B-4) (a) Si $i \in \{1, \dots, r\}$ et $D \in \Omega_i$, l'application

$$\begin{aligned} H &\to \Omega_i \\ h &\mapsto h \cdot D \end{aligned}$$

est surjective, et si $h_1, h_2 \in H$ alors $h_1 \cdot D = h_2 \cdot D$ si et seulement si $h_1^{-1}h_2$ appartient au stabilisateur de D : cela montre que chaque élément de Ω_i a exactement e_i antécedants par l'application précédente. Il en résulte que $m = \#H = e_i\#\Omega_i$. Par ailleurs, la formule de la question précédente implique que

$$2(m-1) = \sum_{i=1}^{r} \sum_{D \in \Omega_i} (e_i - 1) = \sum_{i=1}^{r} \#\Omega_i(e_i - 1) = \sum_{i=1}^{r} m\big(1 - \tfrac{1}{e_i}\big).$$

Cela montre que $\sum\limits_{i=1}^{r}\left(1-\frac{1}{e_i}\right)=2\left(1-\frac{1}{m}\right)$ en divisant par m.

(II-B-4) (b) D'après la question (II-B-2) (a), on a $e_i \geq 2$ *i.e.* $1 > 1-\frac{1}{e_i} \geq \frac{1}{2}$ pour tout $i\in\{1,\ldots,r\}$, donc $r > 2\left(1-\frac{1}{m}\right)=\sum\limits_{i=1}^{r}\left(1-\frac{1}{e_i}\right)\geq \frac{r}{2}$ (en vertu de la question précédente), *i.e.* $1 \leq 2\left(1-\frac{1}{m}\right) < r \leq 4\left(1-\frac{1}{m}\right) < 4$ (rappelons qu'on a supposé $m\geq 2$). Cela montre que $r\in\{2,3\}$.

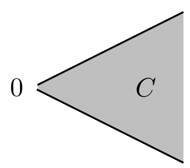
(II-B-5) On a $1-\frac{1}{e_1}+1-\frac{1}{e_2}=2\left(1-\frac{1}{m}\right)$, *i.e.* $\frac{1}{e_1}+\frac{1}{e_2}=\frac{2}{m}$. Comme $e_1\leq m$ et $e_2\leq m$ (en fait ce sont des diviseurs de m, étant des ordres de sous-groupes de H), cela implique que $e_1=e_2=m$. Cela signifie que le stabilisateur de tout élément de $\mathcal{D}$ est égal à H en entier, soit encore que l'action de H sur $\mathcal{D}$ est triviale : les orbites sont ponctuelles. Cela montre que $\#\mathcal{D}=2$. Les deux droites composant $\mathcal{D}$ sont donc propres pour tous les éléments de G : le choix de vecteurs directeurs de ces dernières fournit une base de co-diagonalisation de G, ce qui montre que G est abélien (isomorphe à un sous-groupe de U^2, où $U=\{z\in\mathbf{C},\ ,|z|=1\}$).

(II-B-6) Comme $\sum\limits_{i=1}^{3}\left(1-\frac{1}{e_i}\right)=2\left(1-\frac{1}{m}\right)$ et $e_1=e_2=2$, on a $e_3=\frac{m}{2}$. Soit alors $D\in\Omega_3$. Notons G_D le stabilisateur de D dans G : le stabilisateur de D dans H est G_D/Z. Par hypothèse, ce dernier est d'ordre $\frac{m}{2}$, donc d'indice 2 dans H. Cela implique que G_D est d'indice 2 dans G. Reste à voir que G_D est abélien. Soient $v\in D$ (resp. $w\in D^{\perp}$) un vecteur unitaire : (v,w) est une base orthonormale du plan hermitien V. Comme $G\subset \mathsf{U}(V)$, si $g(D)=D$, alors $g(D^{\perp})=D^{\perp}$: cela implique que la matrice de g dans la base (v,w) est diagonale, à coeffiicients diagonaux dans U. L'ensemble de ces éléments forme donc un sous-groupe de $\mathsf{U}(V)$ isomorphe à U^2 : il est abélien. Son sous-groupe G_D est donc abélien lui aussi.

(II-B-7) Supposons désormais que $r=3$ et $(e_1,e_2)\neq(2,2)$. On a $3-\frac{1}{e_1}-\frac{1}{e_2}-\frac{1}{e_3}=2\left(1-\frac{1}{m}\right)$, *i.e.* $1+\frac{2}{m}=\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}$. Comme $e_1\leq e_2\leq e_3$, on a donc $\frac{3}{e_1}\geq 1+\frac{2}{m}$, *i.e.* $e_1=\frac{3m}{m+2}<3$: comme $e_1\geq 2$ d'après la question (II-B-2) (a), on a nécessairement $e_1=2$: vu l'hypothèse, on a donc $e_2\geq 3$. L'égalité précedente implique alors que $\frac{1}{2}+\frac{2}{m}=\frac{1}{e_2}+\frac{1}{e_3}\leq\frac{2}{e_2}$ (vu que $e_2\leq e_3$), soit encore $e_2\leq\frac{4m}{m+4}<4$: comme $e_2\geq 3$, on a donc $e_2=3$, ce qui montre que $\frac{1}{e_3}=\frac{1}{2}+\frac{2}{m}-\frac{1}{3}=\frac{1}{6}+\frac{2}{m}>\frac{1}{6}$. Il en résulte que $e_3<6$: comme $e_3\geq e_2=3$, on a donc $e_3\in\{3,4,5\}$. Si $e_3=3$ (resp. $e_3=4$, resp. $e_3=5$), on a $m=12$ (resp. $m=24$, resp. $m=60$). Cela montre que $(G:Z)=\#H\leq 60$ et donc que le groupe abélien Z est d'indice au plus 60 dans G. Finalement, on a montré que tout sous-groupe fini de $\mathsf{U}(V)$ contient un sous-groupe abélien distingué d'indice ≤ 60.
Soit maintenant G un sous-groupe fini de $\mathsf{GL}_2(\mathbf{C})$. On muni $V:=\mathbf{C}^2$ de sa structure hermitienne canonique. D'après la question (I-6), il existe $P\in\mathsf{GL}_2(\mathbf{C})$ telle que $PGP^{-1}\subset\mathsf{U}_2=\mathsf{U}(V)$. D'après ce qui précède, le groupe fini PGP^{-1} contient un sous-groupe abélien distingué d'indice ≤ 60 : en conjuguant, il en est de même de G.

Troisième partie - La méthode de Frobenius

(III-A-1) Étant unitaire, v est diagonalisable en base orthonormée : soit $\mathfrak{B}=(e_1,\ldots,e_n)$ une base de diagonalisation. Par hypothèse, pour tout $k\in\{1,\ldots,n\}$ il existe $\theta_k\in[-\tau,\tau]$ tel que $v(e_k)=e^{i\theta_k}e_k$. Écrivons $x=\sum\limits_{k=1}^{n}x_ke_k$ avec $x_1,\ldots,x_n\in\mathbf{C}$: on a $\Phi(v(x),x)=\sum\limits_{k=1}^{n}|x_k|^2e^{i\theta_k}$. Si $z\in\mathbf{C}\setminus\mathbf{R}_{\leq 0}$, notons $\arg(z)\in]-\pi,\pi[$ son argument principal (de sorte que $z=|z|\,e^{i\arg(z)}$). Posons $C=\{z\in\mathbf{C}\setminus\mathbf{R}_{\leq 0}\,;\,|\arg(z)|\leq\tau\}$.



C'est un cône épointé dans $\mathbf{C}$. Comme $0\leq\tau<\frac{\pi}{2}$, il est convexe. Ses éléments sont les nombres complexes de la forme $re^{i\alpha}$ avec $r\in\mathbf{R}_{>0}$ et $\alpha\in[-\tau,\tau]$. Comme $e^{i\theta_k}\in C$ pour tout $k\in\{1,\ldots,n\}$, et comme les x_k sont non tous nuls (parce que $x\neq 0$) l'égalité qui précède montre que $\Phi(v(x),x)\in C$ par convexité, ce qui conclut.

(III-A-2) (a) Soit $x\in T_\lambda\cap U_\lambda^{\perp}$: on a $vuv^{-1}(x)=\lambda x$, *i.e.* $uv^{-1}(x)=\lambda v^{-1}(x)$, *i.e.* $v^{-1}(x)\in U_\lambda$. Comme $x\in U_\lambda^{\perp}$, on a donc $\Phi(x,v^{-1}(x))=0$. Comme v est unitaire, v^{-1} est l'adjoint de v : l'égalité précédente se réécrit $\Phi(v(x),x)=0$. La question précédente implique donc que $x=0$.

(III-A-2) (b) • Comme u et t commutent, les sous-espaces propres de u sont stables par t : on a $t(U_\lambda) \subset U_\lambda$. Comme t est unitaire, on a aussi $t(U_\lambda^\perp) \subset U_\lambda^\perp$. Soit maintenant $x \in T_\lambda$: écrivons $x = y + z$ avec $y \in U_\lambda$ et $z \in U_\lambda^\perp$. En appliquant t, il vient $\lambda y + \lambda z = \lambda x = t(x) = t(y) + t(z)$: comme $t(y) \in U_\lambda$ et $t(z) \in U_\lambda^\perp$ d'après ce qui précède, on a $t(y) = \lambda y$ et $t(z) = \lambda z$ par unicité, *i.e.* $y, z \in T_\lambda$. Il en résulte que $z \in T_\lambda \cap U_\lambda^\perp$, et donc $z = 0$ en vertu de la question précédente. On en déduit que $T_\lambda \subset U_\lambda$. Par ailleurs, le calcul effectué au début de la question précédente montre que $T_\lambda = v(U_\lambda)$, et donc que $\dim_{\mathbf{C}}(T_\lambda) = \dim_{\mathbf{C}}(U_\lambda)$: l'inclusion précédente est une égalité.
• Ce qu'on vient de démontrer montre que $\mathrm{Sp}(t) = \mathrm{Sp}(u)$, et que pour toute valeur propre λ de u, les sous-espaces propres correspondants de u et de t sont égaux. Comme u et t sont diagonalisables (parce qu'unitaires), ils sont donc égaux. L'égalité $u = t$ signifie précisément que u et v commutent.

(III-A-3) Soit $y \in V \setminus \{0\}$ un vecteur propre de vs^{-1} pour la valeur propre μ. Posons $x = s^{-1}(y) \in V$: on a $x \neq 0$, et $v(x) = \mu s(x)$. Cela implique que $\Phi(v(x), x) = \overline{\mu}\Phi(s(x), x)$. D'après la question (III-A-1) appliquée à v et à s, il existe $r, r' \in \mathbf{R}_{>0}$ et $\alpha, \alpha' \in [-\tau, \tau]$ tels que $\Phi(v(x), x) = re^{i\alpha}$ et $\Phi(s(x), x) = r'e^{i\alpha'}$, de sorte que $\mu = \frac{r}{r'}e^{i(\alpha'-\alpha)}$. Comme $|\mu| = 1$ (parce que $v, s \in \mathsf{U}(V)$, donc $vs^{-1} \in \mathsf{U}(V)$), on a $\mu = e^{i\beta}$ avec $\beta = \alpha' - \alpha \in [-2\tau, 2\tau]$ (parce que $\alpha, \alpha' \in [-\tau, \tau]$).

(III-A-4) Observons que si $g \in \mathrm{End}(V)$ et $u \in \mathsf{U}(V)$, on a $N(gu) = \mathrm{Tr}(u^*g^*gu) = \mathrm{Tr}(g^*g) = N(g)$ car $uu^* = \mathsf{Id}_V$. De même, on a $N(ug) = N(g)$. Dans la situation qui nous occupe, cela implique que

$$N(vuv^{-1}u^{-1} - \mathsf{Id}_V) = N\big((vuv^{-1}u^{-1} - \mathsf{Id}_V)uv\big) = N(vu - uv) = N(vg - gv)$$

où $g = u - \mathsf{Id}_V$. On a $v \in \mathsf{U}(V)$: l'endomorphisme v est diagonalisable en base orthonormée : soit $\mathfrak{B}$ une base orthogonale de diagonalisation de v. Écrivons $\mathsf{Mat}_{\mathfrak{B}}(v) = \mathrm{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)$ et $\mathsf{Mat}_{\mathfrak{B}}(g) = (a_{k,\ell})_{1\leq k,\ell\leq n}$. Si $k, \ell \in \{1, \ldots, n\}$, on a $e^{i\theta_k} - e^{i\theta_\ell} = e^{i\frac{\theta_k+\theta_\ell}{2}}\left(e^{i\frac{\theta_k-\theta_\ell}{2}} - e^{-i\frac{\theta_k-\theta_\ell}{2}}\right) = 2i\sin\left(\frac{\theta_k-\theta_\ell}{2}\right)e^{i\frac{\theta_k+\theta_\ell}{2}}$, ce qui implique que $\left|e^{i\theta_k} - e^{i\theta_\ell}\right| = 2\left|\sin\left(\frac{\theta_k-\theta_\ell}{2}\right)\right|$. Par hypothèse, on a $\theta_k, \theta_\ell \in [-\tau, \tau]$, cela montre que $\left|e^{i\theta_k} - e^{i\theta_\ell}\right|^2 \leq 4\sin^2(\theta)$. La matrice de $vg - gv$ dans la base orthonormée $\mathfrak{B}$ est $\left(\left(e^{i\theta_k} - e^{i\theta_\ell}\right)a_{k,\ell}\right)_{1\leq k,\ell\leq n}$: on a

$$N(vg - gv) = \sum_{1\leq k,\ell\leq n} \left|\left(e^{i\theta_k} - e^{i\theta_\ell}\right)a_{k,\ell}\right|^2 \leq 4\sin^2(\tau) \sum_{1\leq k,\ell\leq n} |a_{k,\ell}|^2 = 4\sin^2(\tau)N(g),$$

ce qui conclut.

(III-B-1) (a) Comme G est fini, on dispose de $\delta := \min\limits_{g\in G\setminus\{\mathsf{Id}_V\}} N(g - \mathsf{Id}_V) \in \mathbf{R}_{>0}$. Par hypothèse, on a $\mathrm{Sp}(v) = \{e^{i\alpha_k}\}_{1\leq k\leq n}$ avec $\alpha_k \in \left]-\frac{\pi}{6}, \frac{\pi}{6}\right[$. Posons $\tau_v := \max\limits_{1\leq k\leq n} |\alpha_k|$: on a $\tau_v < \frac{\pi}{6}$, et donc $c_v := 4\sin^2(\tau_v) < 1$. Si $k \in \mathbf{N}$, la question précédente appliquée avec $\tau = \tau_v$ et $u = u_k$ implique que $N(u_{k+1} - \mathsf{Id}_V) \leq c_v N(u_k - \mathsf{Id}_V)$. Une récurrence immédiate montre alors que $N(u_k - \mathsf{Id}_V) \leq c_v^k N(u - \mathsf{Id}_V)$. Comme $\lim\limits_{k\to\infty} c_v^k = 0$, il existe $k_0 \in \mathbf{N}$ tel que $k \geq k_0 \Rightarrow c_v^k N(u - \mathsf{Id}_V) < \delta$, d'où $k \geq k_0 \Rightarrow N(u_k - \mathsf{Id}_V) < \delta$. Par définition de δ, cela implique que $u_k = \mathsf{Id}_V$ dès que $k \geq k_0$.

(III-B-1) (b) • Soit $k \in \mathbf{N}$. Les valeurs propres de v (et donc de $s = u_k v u_k^{-1}$) sont toutes de la forme $e^{i\alpha}$ avec $\alpha \in \left[-\frac{\pi}{6}, \frac{\pi}{6}\right]$: d'après la question (III-A-3), les valeurs propres de $u_{k+1} = vs^{-1}$ sont de la forme $e^{i\beta}$ avec $\beta \in \left[-\frac{\pi}{3}, \frac{\pi}{3}\right]$. Vu l'hypothèse faite sur u, cela montre qu'il existe $\tau \in \left[0, \frac{\pi}{2}\right[$ tel que pour tout $k \in \mathbf{N}$, les valeurs propres de u_k sont de la forme $e^{i\theta}$ avec $\theta \in [-\tau, \tau]$.
• Soit maintenant $k \in \mathbf{N}_{>0}$ tel que $u_{k+1} = \mathsf{Id}_V$. Cela implique que v et $u_k = vu_{k-1}v^{-1}u_{k-1}^{-1}$ commutent, et donc que v et $t := u_{k-1}v^{-1}u_{k-1}^{-1}$ commutent. D'après ce qui précède, la question (III-A-2) (b) s'applique : les endomorphismes v et u_{k-1} commutent, *i.e.* $u_k = \mathsf{Id}_V$. On a donc $(\forall k \in \mathbf{N}_{>0})\, u_{k+1} = \mathsf{Id}_V \Rightarrow u_k = \mathsf{Id}_V$: comme $u_k = \mathsf{Id}_V$ si k assez grand (*cf* question précédente), on en déduit que $u_1 = 0$, *i.e.* que u et v commutent.

(III-B-2) Si $g, h \in G \subset \mathsf{U}(V)$, on a $N(g - h) = N(gh^{-1} - \mathsf{Id}_V)$ comme on l'a vu plus haut : il suffit de trouver $\eta \in \mathbf{R}_{>0}$ tel que $(\forall g \in G)\, N(G - \mathsf{Id}_V) < \eta \Rightarrow g \in S$. Soit donc $g \in G \subset \mathsf{U}(V)$: écrivons $\mathrm{Sp}(g) = \{e^{i\theta_k}\}_{1\leq k\leq n}$ avec $\theta_k \in]-\pi, \pi]$ pour tout $k \in \{1, \ldots, n\}$, et soit $\mathfrak{B}$ une base orthonormée de V telle qu'on ait $\mathsf{Mat}_{\mathfrak{B}}(g) = \mathrm{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)$. Cela implique que $\mathsf{Mat}_{\mathfrak{B}}(g - \mathsf{Id}_V) = \mathrm{diag}\left(e^{i\theta_1} - 1, \ldots, e^{i\theta_n} - 1\right)$, et donc $N(g - \mathsf{Id}_V) = \sum\limits_{k=1}^{n} \left|e^{i\theta_k} - 1\right|^2 = 4\sum\limits_{k=1}^{n} \sin^2\left(\frac{\theta_k}{2}\right)$. Si $\eta \in \mathbf{R}_{>0}$ est tel que $N(g - \mathsf{Id}_V) < \eta$, on a $4\sin^2\left(\frac{\theta_k}{2}\right) < \eta$, *i.e.* $\left|\sin\left(\frac{\theta_k}{2}\right)\right| < \frac{\sqrt{\eta}}{2}$, soit encore $\frac{|\theta_k|}{2} < \mathrm{Asin}\left(\frac{\sqrt{\eta}}{2}\right)$ pour tout $k \in \{1, \ldots, n\}$. Il suffit donc de choisir $\eta \in \mathbf{R}_{>0}$ tel que $2\mathrm{Asin}\left(\frac{\sqrt{\eta}}{2}\right) \leq \frac{\pi}{6}$, *i.e.* $\eta \leq 4\sin^2\left(\frac{\pi}{12}\right) = 2 - \sqrt{3}$ (c'est indépendant de n).

(III-B-3) On a $\dim_{\mathbf{R}}(E) = \dim_{\mathbf{R}}(\mathrm{End}(V)) = 2\dim_{\mathbf{C}}(\mathrm{End}(V)) = 2n^2$. Notons m la mesure de la boule unité de E. Pour tout $g \in \mathsf{U}(V)$, on a $N(g) = n$: les éléments de G se situent sur la boule de centre 0 et de rayon $\sqrt{n}$. Soit $g_1, \ldots, g_d$ un système de représentants de G/A : d'après la question précédente, on a $k \neq \ell \Rightarrow N(g_k - g_\ell) \geq \eta$. Cela implique que les boules (fermées) de rayon $r := \frac{\sqrt{\eta}}{2}$ centrées en $g_1, \ldots, g_d$ sont deux à deux disjointes. Par homogénéité, elles sont de mesure $r^{2n^2}m$: leur réunion étant disjointe, elle est de mesure $r^{2n^2}md$. Par ailleurs, elles se trouvent dans la boule fermée de centre 0 et de rayon $\sqrt{n}+r$ (de mesure $(\sqrt{n}+r)^{2n^2}m$), mais ne rencontrent pas la boule ouverte de centre 0 et de rayon $\sqrt{n}-r$ (de mesure $(\sqrt{n}-r)^{2n^2}m$) : elles sont incluses dans la couronne fermée comprise entre les sphères de centre 0 de rayon $\sqrt{n}-r$ et $\sqrt{n}+r$, qui est donc de mesure $\big((\sqrt{n}+r)^{2n^2} - (\sqrt{n}-r)^{2n^2}\big)m$. Cela montre que la mesure de la réunion des boules est inférieure à la mesure de la couronne, *i.e.* que $r^{2n^2}md \leq \big((\sqrt{n}+r)^{2n^2} - (\sqrt{n}-r)^{2n^2}\big)m$. En divisant par $r^{2n^2}m$, il vient $[G:A] = d \leq \big(\frac{\sqrt{n}}{r}+1\big)^{2n^2} - \big(\frac{\sqrt{n}}{r}+1\big)^{2n^2}$: on conclut en observant que $\frac{\sqrt{n}}{r} = 2\sqrt{\frac{n}{\eta}}$.

(III-B-4) Pour conclure, il s'agit de justifier que le sous-groupe A de G est abélien et distingué. D'après la question (III-B-1), les éléments de S commutent deux à deux : le sous-groupe de G qu'ils engendrent est abélien. Enfin, la partie S de G est stable par conjugaison (le spectre est un invariant de similitude) : cela implique que A est distingué dans G.