CORRIGÉ DE L'ÉPREUVE DE MATHÉMATIQUES GÉNÉRALES

PREMIÈRE PARTIE

I 1. Soit $x \in V$ on a $x \in T_\lambda$ exactement quand $vux^{-1}(x) = \lambda x$, c'est-à-dire $u(v^{-1}(x)) = \lambda v^{-1}(x)$; donc $x \in T_\lambda$ équivaut à $v^{-1}(x) \in U_\lambda$ et par suite $T_\lambda = v\,(U_\lambda)$. Si u et v commutent, on a $t = u$ d'où $T_\lambda = U_\lambda$ et $v(U_\lambda) = U_\lambda$ pour tout λ. Si en outre v est diagonalisable, son polynôme minimal est scindé à racines simples ; l'endomorphisme v_λ de U_λ induit par v annule aussi ce polynôme, donc v_λ est diagonalisable.

I 2. Si $g \in GL(V)$ est d'ordre fini n, il annule le polynôme $X^n - 1$ qui est scindé à racines simples (dans $\mathbb{C}[X]$), donc g est diagonalisable.

I 3. On prouve le résultat par récurrence sur dim $V \geq 1$. C'est évident si tous les éléments de X sont des homothéties, et en particulier si dim $V = 1$. Sinon, il existe un élément u de X qui n'est pas une homothétie. Alors V est somme directe de sous-espaces propres U_λ de u, et par I 1, les éléments x de X induisent des endomorphismes diagonalisables x_λ de U_λ commutant deux à deux. Comme les U_λ sont de dimension strictement inférieure à dim V, la partie $X_\lambda = \{x_\lambda \mid x \in X\}$ de End (U_λ) est diagonalisable. On peut donc choisir une base $\mathcal{B}_\lambda$ de U_λ telle que chaque x_λ, $x \in X$ ait une matrice diagonale dans cette base $\mathcal{B}_\lambda$. Par réunion on obtient une base de V telle que chaque élément x de X ait dans cette base une matrice diagonale.

I 4. Le sous-groupe G de $\mathrm{GL}_2(\mathbb{C})$ engendré par la matrice inversible $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est abélien car monogène. La matrice A n'a que 1 comme valeur propre et n'est pas l'identité donc elle n'est pas diagonalisable, et G ne l'est pas non plus. Comme A n'est pas diagonalisable, elle n'est pas d'ordre fini et G non plus.

I 5. Choisissons une forme hermitienne définie positive $\Psi : V \times V \to \mathbb{C}$. Pour (x, y) dans $V \times V$, posons $\Phi(x,y) = \sum_{g \in G} \Psi(gx, gy)$; comme G est formé d'endomorphismes de V, il est clair que $(x,y) \mapsto \Psi(gx, gy)$ est une forme hermitienne pour tout $g \in G$ et que Φ est une forme hermitienne. Pour $x = y$, on a $\Phi(x,x) = \sum \Psi(gx, gx)$, qui est > 0 si $x \neq 0$, par suite Φ est définie positive. Enfin, pour $h \in G$ on a $\Phi(hx, hy) = \sum_{g \in G} \Psi(ghx, ghy) = \sum_{g \in G} \Psi(gx, gy) = \Phi(x,y)$ puisque l'application $g \mapsto gh$ est une permutation de G. Mais cela signifie que h est unitaire pour Φ.

I 6. Identifions $\mathrm{GL}_n(\mathbb{C})$ à $\mathrm{GL}(\mathbb{C}^n)$ de la manière habituelle (déjà utilisée supra I 4). Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{C})$. Par I 5 il existe une forme hermitienne définie positive Φ sur $\mathbb{C}^n$ telle que G soit un sous- groupe du groupe unitaire pour Φ. Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$ et $(f_1, \ldots, f_n)$ une base orthonormée pour Φ. Soit v l'automorphisme de $\mathbb{C}^n$ qui envoie e_i sur f_i pour $i = 1, \ldots, n$. Par construction, on a $\Phi(v(x), v(y)) = \Phi_0(x,y)$ pour $x, y \in \mathbb{C}^n$, où Φ_0 est la forme hermitienne standard sur $\mathbb{C}^n$: en effet c'est vrai pour x, y dans la base canonique.

Soit $g \in G$, la relation $\Phi(x,y) = \Phi(gx,gy)$ pour $x,y \in \mathbb{C}^n$ qui traduit que g est unitaire pour Φ s'exprime aussi par $\Phi_0(x,y) = \Phi_0(v^{-1}gv(x), v^{-1}gv(y))$ pour $x,y \in \mathbb{C}^n$, c'est à dire $v^{-1}gv \in U_n$. On a donc $v^{-1}Gv \subset U_n$.

On peut aussi raisonner en termes de matrices. La matrice m de Φ dans la base canonique est hermitienne définie positive et les éléments g de G vérifient ${}^t\overline{g}mg = m$. On sait que m est le carré d'une matrice hermitienne $m = h^2$; pour $g \in G$ on a donc $(h^{-1}\,{}^t\overline{g}h)(hgh^{-1}) = 1_n$ de sorte que hgh^{-1} appartient à U_n, d'où $hGh^{-1} \subset U_n$.

DEUXIÈME PARTIE

II A 1. a) Fixons une base orthonormée (e_1, e_2) de V et identifions les $\mathbb{C}$-espaces vectoriels $\mathrm{End}(V)$ et $M_2(\mathbb{C}$ au moyen de cette base. Alors E est formée des matrices $\begin{pmatrix} a & b \\ \overline{b} & -a \end{pmatrix}$ où a est réel et b complexe ; une telle matrice x est la combinaison linéaire $x = a\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \mathcal{R}(b)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \Im(b)\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$,à coefficients réels ; cette écriture est unique, et il s'ensuit que E est un sous-espace vectoriel réel de $\mathrm{End}(V)$ dont les trois matrices exhibées forment une base ; il est donc de dimension 3.

b) Pour $x = \begin{pmatrix} a & b \\ \overline{b} & -a \end{pmatrix}$, comme précédemment, on a $q(x) = a^2 + b\overline{b} = a^2 + \mathcal{R}(b)^2 + \Im(b)^2$, et q est bien une forme quadratique définie positive ; la base donnée de E est d'ailleurs orthonormée pour le produit scalaire attaché à q.

c) Par polarisation on obtient, pour $x' = \begin{pmatrix} a' & b' \\ \overline{b'} & -a' \end{pmatrix}$, dans E,

$$B(x,x') = aa' + \frac{1}{2}(b\overline{b'} + b'\overline{b}) = aa' + \mathcal{R}(b)\mathcal{R}(b') + \mathcal{I}(b)\mathcal{I}(b')$$

Remarquons qu'on a aussi $B(x,x') = \frac{1}{2}\mathrm{tr}(xx'), q(x) = \frac{1}{2}\mathrm{tr}(x^2)$.

II A 2. Soit $a \in U(V)$ et $x \in E$; on a $a^{-1} = a^\star$ et $x^\star = x$ d'où $(axa^{-1})^\star = (axa^\star)^\star = ax^\star a^\star = axa^{-1}$ et axa^{-1} est hermitien. D'autre part on sait que la trace est invariante par conjugaison, d'où $\mathrm{tr}(axa^{-1}) = \mathrm{tr}(x) = 0$. Donc axa^{-1} appartient à E.

II A 3. Soit $a \in U(V)$. Pour $x \in E$ on a $q(axa^{-1}) = -\det(axa^{-1}) = -\det(x) = q(x)$ donc $\varphi(a) \in O(q)$.

II A 4. a) Soit $a \in U(V)$; fixons une base orthonormée de V formée de vecteurs propres de a. Dans cette base l'élément a de $U(V)$ a une matrice $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ où λ et μ sont des nombres complexes de module 1 ; si x appartient à E, il a dans cette base une matrice $\begin{pmatrix} \alpha & \beta \\ \overline{\beta} & -\alpha \end{pmatrix}$, et celle de axa^{-1} est alors $\begin{pmatrix} \alpha & \lambda\mu^{-1}\beta \\ \mu\lambda^{-1}\overline{\beta} & -\alpha \end{pmatrix}$. Si $\mu = \lambda$, on a $\varphi(a) = Id_E$. Si $\mu \neq \lambda$, $axa^{-1} = x$ équivaut à $\beta = 0$ et donc $\varphi(a) \neq Id_E$. Par conséquent le noyau de φ est formé des homothéties λId_V, λ nombre complexe de module 1.

b) Munissons E de l'orientation pour laquelle la base orthonormée exhibée en II A 1 —formée des éléments de matrices $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$— est directe. La matrice de $\varphi(a)$ dans cette base est $\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{pmatrix}$ si on a écrit $\lambda\mu^{-1} = e^{i\theta}$. Donc $\varphi(a)$ est bien une rotation de E, d'axe orienté par le premier vecteur de cette base, et d'angle θ.

c) En variant λ et μ, on obtient toutes les rotations de cet axe dans E. Soit x un élément non nul de E ; comme x est un automorphisme de V, hermitien et de trace nulle, on peut trouver une base orthonormée de V où x ait pour matrice $\begin{pmatrix}\alpha & 0\\ 0 & -\alpha\end{pmatrix}$, $\alpha \in \mathbb{R}^*$. Ce qui précède montre que toutes les rotations de E d'axe orienté par x sont dans l'image de φ. Par suite $\varphi(U(V)) = SO(q)$.

II A 5. L'espace euclidien E, de dimension 3, contient un icosaèdre régulier I, qu'on peut centrer en O. Les isométries positives de I forment alors un sous-groupe $\overline{G}$ de $SO(q)$, simple non abélien de cardinal 60. L'image réciproque G de $\overline{G}$ dans $SU(V)$ est d'ordre 120, car le noyau de la restriction de φ à $SU(V)$ est formé de $\pm Id_V$. Un sous-groupe abélien distingué H de G a pour image dans $\overline{G}$ un sous-groupe abélien distingué, qui ne peut être que le sous-groupe trivial. Par suite H est d'indice au moins 60 dans G.

II B 1. a) Soit $h \in G \setminus Z$, et soit D une droite propre pour h : $h(D) = D$. Soit $g \in G$. On a alors $ghg^{-1}(g(D)) = g(D)$ donc $g(D)$, qui est bien une droite de V, est propre pour $ghg^{-1} \in G$; on a $ghg^{-1} \notin Z$ car h n'est pas dans Z. Par suite $g(D) \in \mathcal{D}$.

b) On vient de voir qu'on a une application $(g, D) \mapsto g(D)$ de $G \times \mathcal{D}$ dans $\mathcal{D}$. Il est immédiat que c'est une action de G sur $\mathcal{D}$, ce qui donne un morphisme de groupes de G dans $S(\mathcal{D})$. Pour $g \in Z$ on a $g(D) = D$ pour tout $D \in \mathcal{D}$ et cet homomorphisme de groupes se factorise donc en un homomorphisme de groupes de $H = G/Z$ dans $S(\mathcal{D})$. Si on note l'action correspondante $(h, D) \to h.D$, elle est donnée par $h.D = g(D)$ où $g \in G$ a pour image h dans H ; cette action de H sur $\mathcal{D}$ est ainsi déduite de celle de G.

II B 2. a) Soit $D \in \mathcal{D}$. Il existe un élément g de $G \setminus Z$ tel que $g(D) = D$. Comme g n'est pas dans Z, son image h dans H est d'ordre au moins 2. Mais alors, le stabilisateur de D dans H contient le sous-groupe de H engendré par h et on a bien $e_D \geq 2$.

b) Considérons l'ensemble X des couples $(h, D) \in H \times \mathcal{D}$ tels que $h.D = D$. Une droite $D \in \mathcal{D}$ fait partie de e_D tels couples, donc on a $|X| = \sum_{D\in\mathcal{D}} e_D$; mais d'autre part un élément g de $G \setminus Z$ stabilise exactement deux droites de $\mathcal{D}$, qui d'ailleurs ne dépendent que de l'image de h de g dans H ; en revanche l'élément neutre de H stabilise toutes les droites de $\mathcal{D}$. On a donc $|X| = |\mathcal{D}| + 2(m - 1)$. Comparant les deux formules pour $|X|$, on obtient $2(m - 1) = \sum_{D\in\mathcal{D}}(e_D - 1)$.

II B 3. Si $D \in \mathcal{D}$, $h \in H$ et $D' = hD$, le stabilisateur dans H de D' est hSh^{-1} où S est celui de D ; or S et hSh^{-1} sont deux groupes finis isomorphes donc de même cardinal, d'où $e_D = e_{D'}$. [On peut aussi utiliser que le cardinal de l'orbite de D est quotient de celui de H par celui du stabilisateur de D.]

II B 4. a) Regroupons selon les orbites dans la formule $2(m-1)=\sum_{D\in\mathcal{D}}(e_D-1)$. Notant d_i le cardinal de l'orbite Ω_i, on obtient

$$2(m-1)=\sum_{i=1}^{r} d_i(e_i-1)$$

Tenant compte de la formule $d_ie_i=m$ pour $m=1,\ldots,r$, on a

$$2\left(1-\frac{1}{m}\right)=\sum_{i=1}^{r}\left(1-\frac{1}{e_i}\right).$$

b) Comme $e_i\geq 2$ on a $1-\frac{1}{e_i}\geq\frac{1}{2}$ pour $i=1,\ldots,r$ et comme $m\geq 2$ on a $2(1-\frac{1}{m})<2$ ce qui montre que r vaut au plus 3. Mais on ne peut pas avoir $r=1$ car $2(1-\frac{1}{m})>1-\frac{1}{m}\geq 1-\frac{1}{e_1}$. Donc r vaut 2 ou 3.

II B 5. Supposons $r=2$; on a $2(1-\frac{1}{m})=1-\frac{1}{e_1}+1-\frac{1}{e_2}$ et $e_1\leq e_2\leq m$; cela implique $e_1=e_2=m$. Donc il existe deux droites D dans $\mathcal{D}$ que H stabilise. Dans une base formée de vecteurs directeurs de ces deux droites, les éléments de G ont une matrice diagonale, donc G est abélien.

II B 6. Supposons $r=3$ et $e_1=e_2=2$; on a alors $e_3=\frac{m}{2}$. Le stabilisateur d'un élément D de Ω_3 est d'ordre $\frac{m}{2}$ donc d'indice 2 dans H. Son image réciproque A dans G est d'indice 2, donc distinguée dans G. Les éléments de A stabilisent D et donc la droite orthogonale à D. Par suite A est abélien.

II B 7. Dans les cas restants, on a $r=3$, $1+\frac{2}{m}=\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}$, $e_1\leq e_2\leq e_3$. On ne peut avoir $e_1\geq 3$ car si $e_1\geq 3$, on a $\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}\leq 1<1+\frac{2}{m}$. On a donc $e_1=2$ d'où $\frac{1}{2}+\frac{2}{m}=\frac{1}{e_2}+\frac{1}{e_3}$, et $e_2\geq 3$ puisque l'on n'est pas dans le cas 6. Mais $e_2\geq 4$ est impossible car alors $\frac{1}{e_2}+\frac{1}{e_3}\leq\frac{1}{2}<\frac{1}{2}+\frac{2}{m}$; donc e_2 vaut 3 et on a $\frac{1}{6}+\frac{2}{m}=\frac{1}{e_3}$, ce qui donne $e_3=3,4$ ou 5 avec $m=12,24,60$ respectivement. Ainsi H est d'ordre 12, 24 ou 60 et G a un sous-groupe abélien distingué d'indice 12, 24 ou 60 respectivement, à savoir Z.

TROISIÈME PARTIE

III A 1. Prenons une base orthonormée $(x_1,\ldots,x_n)$ de V formée de vecteurs propres de v ; soit $e^{i\theta_j}$ la valeur propre correspondant à x_j. Pour $x=\sum\lambda_jx_j$ dans V, on a $\Phi(v(x),x)=\sum|\lambda_j|^2e^{-i\theta_j}$. Ainsi pour $x\neq 0$, $\Phi(v(x),x)$ est une combinaison linéaire, à coefficients strictements positifs de certains (au moins un) des $e^{-i\theta_j}$. L'assertion vient alors du fait, évident sur un dessin, que le cône

$$\{re^{i\theta}\mid r>0,\theta\in[-\tau,\tau]\}$$

est convexe parce que $0\leq\tau<\frac{\pi}{2}$. Ce cône est en fait l'intersection des demi-plans d'équations $x>0$, $y\leq x\tan\tau$, $y\geq -x\tan\tau$: en effet si $r>0$ et $\theta\in[-\tau,\tau]$, $0\leq\tau<\frac{\pi}{2}$, alors on a $\cos\theta>0$ donc $x=r\cos\theta>0$ et $\frac{y}{x}=\tan\tau\in[-\tan\tau,\tan\tau]$ puisque la fonction tangente croît de $-\frac{\pi}{2}$ à $\frac{\pi}{2}$; inversement si $x>0$ et $\frac{y}{x}\in[-\tan\tau,\tan\tau]$ alors l'argument θ vérife bien $\theta\in[-\tau,\tau]$.

III A 2. a) On a vu en I 1 qu'on a $T_\lambda = v(U_\lambda)$; si $x \in U_\lambda$ n'est pas nul, on a $\Phi(v(x), x) \neq 0$ par III A 1 donc $v(x)$ n'appartient pas à $U_\lambda^\perp$, et par suite $T_\lambda \cap U_\lambda^\perp = \{0\}$.

b) Remarquons que $T_\lambda = v(U_\lambda)$ a même dimension que U_λ. Si u et t commutent alors T_λ est stable par u (I 1). Or u étant diagonalisable, tout sous-espace stable T est somme directe des $T \cap U_\lambda$, λ parcourant les valeurs propres de u (par le théorème des noyaux appliqué à l'endomorphisme u_T de T induit par u et au polynôme minimal de u). Comme $U_\lambda^\perp$ est la somme directe des U_μ pour $\mu \neq \lambda$, on voit que T_λ est somme directe de $T_\lambda \cap U_\lambda$ et $T_\lambda \cap U_\lambda^\perp$.
Comme par a) $T_\lambda \cap U_\lambda^\perp = \{0\}$, on a $T_\lambda = T_\lambda \cap U_\lambda$ i.e. $T_\lambda \subset U_\lambda$; Cela donne $T_\lambda = U_\lambda$ puisque T_λ et U_λ ont même dimension. Ceci étant vrai pour tout $\lambda \in \mathbb{C}$, on a $t = u$ et u et v commutent.

III A 3. Soit μ une valeur propre de vs^{-1}, y un vecteur propre correspondant, $y \neq 0$ et $x = s^{-1}(y)$. On a $(v - \mu s)(x) = 0$ d'où $\Phi(v(x), x) = \overline{\mu}\Phi(s(x), x)$. Comme x n'est pas nul et que v et s vérifient l'hypothèse de III A 1, on voit que $\Phi(v(x), x)$ et $\Phi(s(x), x)$ sont de la forme $re^{i\alpha}$ avec $r > 0$ et $\alpha \in [-\tau, \tau]$. Par suite μ est de la forme $r'e^{i\alpha'}$ avec $r' > 0$ et $\alpha' \in [-2\tau, 2\tau]$. Mais μ est de module 1 car $vs^{-1} \in U(V)$, d'où le résultat.

III A 4. Pour $u \in U(V)$ et $g \in$End(V), on a $N(gu) = \mathrm{tr}(u^\star g^\star gu) = \mathrm{tr}(u^{-1} g^\star gu)$ $= N(g)$. On a donc pour $u \in U(V)$, $N(vuv^{-1}u^{-1} - Id_V) = N(vu - uv) =$
$N(v(u - Id_V) - (u - Id_V)v)$. Calculons dans une base orthonormée de V formée de vecteurs propres de v. La matrice de v est diagonale de termes $\lambda_j = e^{i\theta_j}$ et si la matrice de $u - Id_V$ est $(a_{j,k})$ on obtient

$$N(vuv^{-1}u^{-1} - Id_V) = \sum_{j,k} \mid \lambda_j - \lambda_k|^2 |a_{j,k}|^2.$$

On montre ci-après $|\lambda_j - \lambda_k|^2 = 4\sin^2\left(\frac{\theta_j - \theta_k}{2}\right)$ d'où $|\lambda_j - \lambda_k|^2 \leq 4\sin^2\tau$ et $N(vuv^{-1}u^{-1} - Id_V) \leq 4\sin^2(\tau)\sum_{j,k}|a_{j,k}|^2$ ce qui donne le résultat.
<u>Calcul</u> : $|\lambda_j - \lambda_k|^2 = |1 - e^{i(\theta_j - \theta_k}|^2 = (1 - \cos(\theta_j - \theta_k))^2 + \sin^2(\theta_j - \theta_k) =$
$2 - 2\cos(\theta_j - \theta_k) = 4\sin^2\frac{\theta_j - \theta_k}{2}$.
On peut aussi faire un dessin :

III B 1. a) Comme v appartient à S, on peut choisir, dans III A, $\tau \in [0, \frac{\pi}{6}[$. On alors $2\sin\tau < 1$ et donc $N(vuv^{-1}u^{-1} - Id_V) < N(u - Id_V)$ pour $u \in U(V)$, $u \neq Id_V$. Si $u_k = Id_V$ pour un entier k, on a $u_l = Id_V$ pour l entier $l \geq k$. Si u_k n'est jamais égal à Id_V, alors la suite $N(u_k - Id_V)$ est strictement décroissante mais, comme les u_k sont dans G, elle ne peut prendre qu'un nombre fini de valeurs, ce qui est contradictoire.

b) Pour $k \geq 1$, dire qu'on a $u_{k+1} = Id_V$ signifie que v commute à $u_k = vu_{k-1}v^{-1}u_{k-1}^{-1}$; comme v commute à lui-même cela signifie que v commute à $u_k^{-1}v = u_{k-1}vu_{k-1}^{-1}$.

Montrons que l'on peut appliquer III A 2 avec v et u_{k-1} à la place de u et v. Il s'agit de voir que les valeurs propres de u_{k-1} sont de la forme $e^{i\theta}$ avec $\theta \in]-\frac{\pi}{2}, \frac{\pi}{2}[$. C'est vrai par hypothèse pour $k = 1$ car $u_0 = u$. Pour $k \geq 2$, u_{k-1} est le produit de v par $s = u_{k-2}v^{-1}u_{k-2}^{-1}$; mais v et s vérifient les hypothèses de III A 3 avec $\tau \in [0, \frac{\pi}{6}[$ donc les valeurs propres de u_{k-1} sont de la forme $e^{i\theta}$, $|\theta| \in [0, \frac{\pi}{3}[$. Appliquant III A 2 on voit que v et u_{k-1} commutent.

Pour $k \geq 1$ on a donc prouvé que $u_{k+1} = Id_V$ implique $u_k = Id_V$. Comme $u_k = Id_V$ pour k assez grand, on a $u_1 = Id_V$ et u et v commutent.

III B 2. On a $N(g-h) = N(h^{-1}g - Id_V)$ car $h^\star h = Id_V$. Calculons à l'aide de matrices dans une base orthonormée de V formée de vecteurs propres de $h^{-1}g$. On obtient $N(g-h) = \sum |\lambda_j - 1|^2 = \sum 4\sin^2\left(\frac{\theta_j}{2}\right)$ si $\lambda_j = e^{i\theta_j}$. Comme $\theta \mapsto \sin^2\left(\frac{\theta}{2}\right)$ est paire, croissante de 0 à π, on voit qu'en posant $\eta = 4\sin^2\left(\frac{\pi}{12}\right)$, l'inégalité $|\lambda - 1|^2 < \eta$ (où $\lambda = e^{i\theta}$) implique qu'on peut prendre $\theta \in]-\frac{\pi}{6}, \frac{\pi}{6}[$. Alors $N(g-h) < \eta$ implique $h^{-1}g \in S$.

III B 3. Choisissons un système de représentants B de G/A dans G. Pour b et b' distincts dans B, on a $N(b-b') \geq \eta$ car $N(b-b') < \eta$ implique $b'^{-1}b \in S \subset A$ i.e. $bA = b'A$ et $b = b'$. Par suite les boules ouvertes de E de centres les éléments de B et de rayon $\frac{\sqrt{\eta}}{2}$ sont disjointes. D'autre part les éléments de $U(V)$ sont de norme $\sqrt{n}$ dans E, donc ces boules sont comprises entre la sphère de centre O et de rayon $\sqrt{n} - \frac{\sqrt{\eta}}{2}$ et celle de centre O et de rayon $\sqrt{n} + \frac{\sqrt{\eta}}{2}$. Notant m le volume de la boule unité de E, on obtient alors :

$$|G/A| \left(\frac{\sqrt{\eta}}{2}\right)^{2n^2} m \leq \left(\sqrt{n} + \frac{\sqrt{\eta}}{2}\right)^{2n^2} m - \left(\sqrt{n} - \frac{\sqrt{\eta}}{2}\right)^{2n^2} m$$

d'où

$$|G/A| \leq \left(\frac{2\sqrt{n}}{\sqrt{\eta}} + 1\right)^{2n^2} - \left(\frac{2\sqrt{n}}{\sqrt{\eta}} - 1\right)^{2n^2} .$$

III B 4. Par III B 1 les éléments de S commutent 2 à 2 donc A est abélien. D'autre part un conjugué dans G d'un élément de S est encore dans S donc A est distingué dans G. Enfin l'indice de A dans G est majoré par la quantité $a(n)$ de III B 3, qui ne dépend que de n. On a donc montré qu'un sous-groupe fini de $U(V)$ a un sous-groupe abélien distingué d'indice au plus $a(n)$. La question I 6 donne alors le théorème de Jordan.