0. Notations.

Dans tout le problème, n désigne un entier ≥ 1 et E un $\mathbf{C}$-espace vectoriel de dimension n. On note $\mathbf{U}$ le groupe multiplicatif des nombres complexes de module 1. Si $A = (a_{ij})$ est une matrice carrée $n \times n$ à coefficients dans $\mathbf{C}$ on note $\overline{A}$ sa conjuguée (i.e. la matrice $(\overline{a_{ij}})$) et A^* son adjointe (i.e. la matrice ${}^t\overline{A}$). On note I la matrice identité $n \times n$. On rappelle qu'une homothétie est une application $h : E \to E$ telle qu'il existe $\lambda \in \mathbf{C}$ tel que $h(x) = \lambda x$ pour tout $x \in E$.

Si G est un groupe on rappelle que deux éléments u et v de G sont dits conjugués dans G s'il existe $g \in G$ vérifiant $v = gug^{-1}$.

Dans tout le problème on fixe une forme hermitienne f sur E. On rappelle que f est une application qui à $(x, y) \in E \times E$ associe $f(x, y) \in \mathbf{C}$, qui est $\mathbf{C}$-linéaire par rapport à la variable x, et telle que $f(y, x)$ est le complexe conjugué de $f(x, y)$. On en déduit que $f(x, \lambda y) = \overline{\lambda} f(x, y)$ pour $x, y \in E$ et $\lambda \in \mathbf{C}$.
On suppose de plus que f est définie positive, c'est-à-dire que, pour tout $x \in E$, $f(x, x)$ est un réel ≥ 0 et que $f(x, x)$ n'est nul que si x l'est. On pose $q(x) = f(x, x)$. On notera que la restriction de f à tout sous-espace vectoriel V de E est encore une forme hermitienne définie positive.
On rappelle que si $\mathcal{B} = (e_1, \cdots, e_n)$ est une base de E, la matrice M de f dans cette base est la matrice de terme général $m_{i,j} = f(e_i, e_j)$.

Si V est un sous-espace vectoriel de E on note $V^\perp$ son orthogonal relativement à f. On a donc : $V^\perp = \{x \in E \mid \forall y \in V,\ f(x, y) = 0\}$. On rappelle qu'on a alors $V \oplus V^\perp = E$ et $(V^\perp)^\perp = V$.

On note $U(q)$ le groupe unitaire relatif à q (ou à f), c'est-à-dire l'ensemble des endomorphismes u de E qui vérifient, pour tous $x, y \in E$, $f(u(x), u(y)) = f(x, y)$, ou, ce qui revient au même, $q(u(x)) = q(x)$ pour tout $x \in E$.
Si A (resp. M) est la matrice de l'endomorphisme u (resp. de la forme f) dans la base $\mathcal{B}$, on rappelle que u est unitaire pour f si et seulement si on a $A^* M A = M$.

I. Préliminaires.

1) Montrer qu'il existe une base $\mathcal{B} = (e_1, e_2, \cdots, e_n)$ de E qui est orthonormée pour f, c'est-à-dire telle que l'on ait $f(e_i, e_j) = \delta_{i,j}$ où $\delta_{i,j}$ est le symbole de Kronecker (on pourra raisonner par récurrence sur n en utilisant l'orthogonal). Si $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{i=1}^n y_i e_i$ sont écrits dans une base orthonormée, calculer $f(x, y)$ et $q(x)$. Quelle est la matrice de f dans une telle base ?

2) Soit u un endomorphisme de E et $\mathcal{B}$ une base orthonormée pour f. Montrer que u est unitaire si et seulement si l'image de $\mathcal{B}$ par u est une base orthonormée.

3) Soit $u \in U(q)$. Montrer que la matrice A de u dans une base orthonormée $\mathcal{B}$ vérifie $A^* A = I$. En déduire que $\det u$ est un nombre complexe de module 1.

4) Soit $u \in U(q)$ et soit λ une valeur propre de u. Montrer qu'on a $\lambda \in \mathbf{U}$.

5) Déterminer les homothéties qui sont dans $U(q)$.

6) On considère l'application dét $: U(q) \to \mathbf{U}$ qui à un endomorphisme unitaire u associe son déterminant. Quelle est son image ? On note $SU(q)$ l'ensemble des

éléments de $U(q)$ qui vérifient $\text{dét}\, u = 1$. Montrer que $SU(q)$ est un sous-groupe distingué de $U(q)$. Déterminer les homothéties qui sont dans $SU(q)$.

II. Conjugaison.

1) Soit $u \in U(q)$, λ une valeur propre de u, e un vecteur propre non nul associé à λ et D la droite engendrée par e. Montrer que l'hyperplan orthogonal $D^\perp$ est stable par u.

2) Soit $u \in U(q)$. Montrer qu'il existe une base orthonormée de E dans laquelle u est diagonalisable. (On pourra raisonner par récurrence sur n).

3) Déduire de ce qui précède que deux éléments u et u' sont conjugués dans $U(q)$ si et seulement si u et u' ont même spectre (i.e. mêmes valeurs propres, avec les mêmes multiplicités). Montrer qu'on peut supposer qu'on a $u' = gug^{-1}$ avec $g \in SU(q)$.

4) Soit $u \in U(q)$. Montrer qu'il existe $v \in U(q)$ tel que $u = v^2$. Même question avec $u, v \in SU(q)$.

5) On suppose $n = 2$. Montrer que deux éléments de $U(q)$ sont conjugués si et seulement si ils ont même trace et même déterminant. Montrer que deux éléments de $SU(q)$ sont conjugués si et seulement si ils ont même trace.

6) On suppose $n = 2$. Soit $u \in SU(q)$.
   a) Montrer que u est conjugué de u^{-1} dans $SU(q)$.
   b) Montrer qu'il existe $g, h \in SU(q)$ tels que $u = ghg^{-1}h^{-1}$. (On utilisera II.4 et a)).

III. Quasi-réflexions, quasi-renversements.

Soit a un vecteur non nul de E, D la droite engendrée et soit H l'hyperplan orthogonal $D^\perp$. Soit $\alpha \in \mathbf{U}$. On appelle quasi-réflexion de vecteur a et de rapport α l'endomorphisme $\tau_{a,\alpha}$ de E défini par $\tau_{a,\alpha}|_H = \text{Id}_H$ et $\tau_{a,\alpha}(a) = \alpha a$.

1) Montrer que $\tau_{a,\alpha}$ est dans $U(q)$. Préciser sa matrice dans une base obtenue en adjoignant a à une base de H. À quelle condition a-t'on $\tau_{a,\alpha} = \tau_{b,\beta}$? Calculer $\text{dét}\, \tau_{a,\alpha}$.

2) Soit $u \in U(q)$. Calculer le conjugué $u\tau_{a,\alpha}u^{-1}$. À quelle condition u et $\tau_{a,\alpha}$ commutent-ils ?

3) a) Soit u un endomorphisme de E. On suppose que $u(a)$ est colinéaire à a pour tout vecteur a non nul de E. Montrer que u est une homothétie.

b) Montrer que le centre de $U(q)$ (i.e. l'ensemble des $u \in U(q)$ tels que $uv = vu$ pour tout $v \in U(q)$) est formé des homothéties de $U(q)$.

c) Montrer que le centre de $SU(q)$ est formé des homothéties de $SU(q)$. (On pourra montrer que pour tout vecteur non nul $e \in E$ et tout $\lambda \in \mathbf{U}$, $\lambda \neq \pm 1$, il existe $u \in SU(q)$ tel que la droite $\mathbf{C}e$ soit l'unique droite propre relative à λ.)

4) Montrer que tout élément u de $U(q)$ s'écrit comme un produit fini de quasi-réflexions. (Utiliser II.2).

5) On suppose $n \geq 2$. Soit $P \subset E$ un plan vectoriel. Un élément u de $SU(q)$ est appelé un quasi-renversement de plan P si on a $u|_{P^\perp} = \text{Id}_{P^\perp}$.

a) On fixe le plan P. Montrer que tout quasi-renversement est conjugué dans $SU(q)$ d'un quasi-renversement de plan P.

b) Montrer que tout élément de $SU(q)$ est un produit fini de quasi-renversements.

IV. La simplicité de $PSU(q)$, cas $n = 2$.

Dans cette partie, on se propose de montrer que le groupe quotient $PSU(q) = SU(q)/\{\mathrm{Id}_E, -\mathrm{Id}_E\}$ est simple pour $n = 2$. Cela signifie que, si N est un sous-groupe distingué de $SU(q)$, contenant $\{\mathrm{Id}_E, -\mathrm{Id}_E\}$ et non réduit à $\{\mathrm{Id}_E, -\mathrm{Id}_E\}$, on a $N = SU(q)$. Soit $s \in N$, $s \neq \mathrm{Id}_E, -\mathrm{Id}_E$. On rappelle que si N contient un élément $u \in SU(q)$ il contient aussi ses conjugués gug^{-1} pour $g \in SU(q)$.

1) Montrer que la matrice de s dans une base orthonormée $\mathcal{B}$ convenable est de la forme $\begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$ avec $\alpha \in \mathbf{U}$, $\alpha \neq \pm 1$. On pose $\alpha = e^{i\theta}$. Montrer que, quitte à changer l'élément s, on peut supposer $0 < \theta < \pi/2$.

2) Soit g un élément quelconque de $SU(q)$.

a) Montrer que la matrice de g dans $\mathcal{B}$ est de la forme $\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ avec $a\overline{a} + b\overline{b} = 1$.

b) Montrer que $\gamma_g = gsg^{-1}s^{-1}$ est dans N et calculer sa matrice dans la base $\mathcal{B}$. Soit β un réel vérifiant $\cos 2\theta \leq \beta \leq 1$. Montrer qu'il existe $g \in SU(q)$ tel que la trace de γ_g soit égale à 2β.

3) Soit $\lambda \in [0, 1]$. Montrer qu'il existe $v \in N$ tel que $\mathrm{Tr}\,(v) = 2\lambda$ (on pourra itérer la méthode de 2.b) pour trouver des éléments de trace comprise entre $2\cos 4\theta$ et $2\cos 2\theta$, etc.). Montrer qu'il existe $v' \in N$ tel que $\mathrm{Tr}\,(v') = -2\lambda$.

4) Montrer que N est égal à $SU(q)$.

5) Montrer que les seuls sous-groupes distingués de $SU(q)$ sont $\{\mathrm{Id}_E\}$, $\{\mathrm{Id}_E, -\mathrm{Id}_E\}$ et $SU(q)$. (On utilisera 4) et le fait qu'il existe $u \in SU(q)$ tel que $u^2 = -\mathrm{Id}_E$.)

V. La simplicité de $PSU(q)$, cas général.

Le groupe $PSU(q)$ est le quotient de $SU(q)$ par son centre Z (formé des homothéties de $SU(q)$). Le but de cette partie est de montrer que $PSU(q)$ est simple. Soit N un sous-groupe distingué de $SU(q)$ contenant le centre Z de $SU(q)$ et distinct de Z. Il s'agit de montrer que N est égal à $SU(q)$. Soit $u \in N$, $u \notin Z$. On choisit une base orthonormée $e_1, \cdots, e_n$ de E dans laquelle u est diagonale avec des valeurs propres $\alpha_1, \cdots, \alpha_n$ et on suppose, par exemple, $\alpha_1 \neq \alpha_2$. Soit V le sous-espace orthogonal au plan P engendré par e_1 et e_2.

1) Montrer qu'il existe $g \in SU(q)$ tel que $g|_V = \mathrm{Id}_V$ et tel que, si $\gamma = gug^{-1}u^{-1}$, $\gamma|_P$ soit $\neq \pm\mathrm{Id}_P$. Montrer que $\gamma \in N$.

2) a) Montrer que N contient le groupe G de tous les éléments de $SU(q)$ qui induisent l'identité sur V (on appliquera les résultats de IV à la restriction à P du groupe $N \cap G$).

b) Montrer que N contient tous les quasi-renversements et en déduire que $N = SU(q)$ (utiliser III 5).

4) Déterminer tous les sous-groupes distingués de $SU(q)$.