ÉCOLE NORMALE SUPÉRIEURE
CASA BLANCA
CENTRE DE PRÉPARATION D'AGRÉGATION
EN MATHÉMATIQUES

MÉMOIRE

Présenté pendand

PÉRIODE DE FORMATION

2005-2008

Spécialité : Mathématiques

LE GROUPE LINÉAIRE D'UN ESPACE VECTORIEL $\mathbb{E}$, DE DIMENSION FINIE SOUS-GROUPES DE GL($\mathbb{E}$) ET APPLICATIONS

Par l'agrégé

Khalid EL BAKKIOUI

INTRODUCTION

On avait toujours regardé avec profit le groupe linéaire comme une source de bons thèmes applicatifs qu'ils soient en algèbre et géométrie ou en analyse.

Dans le but de dévoiler quelques unes de ces applications, nous avons essayer, par ce modeste travail, d'élaborer un panorama sur le groupe linéaire ; ainsi, ce mémoire est-il subdivisé en quatre chapitres : le premier est une allusion aux sous-groupes remarquables du groupe linéaire, le second traite l'étude des générateurs et centres dans ce groupe, un troisième consacré au groupe orthogonal et le quatrième est réservé aux quelques applications.

En fin, une annexe qui met en oeuvre le théorème de Hahn-Banach sous son aspect géometrique.

Finalement, pour terminer je tiens à remercier chaleureusement mr C.Durant qui nous a accompagner pendant cette période de prépartion à l'agrégation, qui était disponible tout le temps, qu'il en soit, une fois plus, bien remercié. Et tous ceux qui m'apporté de l'aide pour réaliser ce travail.

Chapitre I

SOUS-GROUPES REMARQUABLES DU GROUPE LINÉAIRE

$\mathbb{K}$ etant un corps commutatif. $\mathbb{E}$ désigne un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$.

I-Généralités :

Définition 1 : Le groupe linéaire $GL(\mathbb{E})$ de $\mathbb{E}$ est le groupe des endomorphismes inversibles de $\mathcal{L}(\mathbb{E})$.

Remarque 1 :Soit $GL_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K})/det(A) \neq 0\}$. Grace à l'isomorphisme canonique entre $\mathcal{L}(\mathbb{E})$ et $\mathcal{M}_n(\mathbb{K})$ on a l'identification : $GL(\mathbb{E}) \simeq GL_n(\mathbb{K})$.

définition 2 : on appelle groupe spécial linéaire de $\mathbb{E}$, et que l'on note $SL(\mathbb{E})$, le noyau de det : $GL(\mathbb{E}) \longrightarrow \mathbb{K}^*$; $SL(\mathbb{E}) = \{\mathbb{A} \in GL(\mathbb{E})/det(A) = 1\}$.

Remarque 2 : soit $SL_n(\mathbb{K}) = \{\mathbb{A} \in \mathcal{M}_n(\mathbb{K})/det(A) = 1\}$.
On a l'identification : $SL(\mathbb{E}) \simeq SL_n(\mathbb{E})$.

Proposition 1 : si $\mathbb{K} = \mathbb{R}$ OU $\mathbb{C}$ alors :
i) $GL_n(\mathbb{K})$ est un ouvert dense de $\mathcal{M}_n(\mathbb{K})$.
ii) les applications $A \longmapsto A^{-1}$ et $(A,B) \longmapsto AB$ sont continues.

Preuve :
i). l'application $\mathcal{M}_n(\mathbb{K}) \longrightarrow \mathbb{K}$, $M \longmapsto det(M)$ est continue car det(M) s'exprime comme fonction polynomiale des coefficients de M. et comme $\mathbb{K}^* = \mathbb{K} - \{0\}$ est un ouvert de $\mathbb{K}$, alors $GL_n(\mathbb{K}) = det^{-1}(\mathbb{K}^*)$ est un ouvert de $\mathcal{M}_n(\mathbb{K})$.
* `Densité :` * soit $M \in \leq \mathcal{M}_n(K)$. le polynôme caractéristique P_M de M n'a qu'un nombre fini de racines, donc : $\exists r > 0$ tq : $\forall \lambda \in \mathbb{K}$, $0 < \| \lambda \| < r : P_M(\lambda) \neq 0$.
en d'autres termes, pour tout $\lambda \in \mathbb{K}$; $0 < \| \lambda \| < r$ on a : $M - \lambda I_n \in GL_n(\mathbb{K})$ or $M = lim_{\lambda \longrightarrow 0, \lambda \neq 0}(M - \lambda I_N)$. donc M est limite d'éléments de $GL_n(\mathbb{K})$ ainsi $\overline{GL_n(\mathbb{K})} = \mathcal{M}_n(\mathbb{K})$.

ii).L'application bilinéaire $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \longrightarrow \mathcal{M}_n(\mathbb{K}), (A,B) \longmapsto AB$ définie sur $\mathcal{M}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K})$ qui est de dimension finie, est continue.

* L'application $A \in GL_n(\mathbb{K}) \longrightarrow A^{-1} \in GL_n(\mathbb{K})$ est continue car : $A^{-1} = (detA)^{-1}(^\top \widetilde{A})$ où : $\tilde{A}$ designe la comatrice de A. Et vu la contnuité des applications : $X \longmapsto \tilde{X}$, $X \longmapsto^T X$, $X \longmapsto detX$ on a le résultat.

Application 1 :
Si $A, B \in \mathcal{M}_n(\mathbb{R})$ alors $\chi_{AB} = \chi_{BA}$ où χ_M désigne le polynôme caractéristique de M.

Preuve :
1^{er} cas : Si A *ou* $B \in GL_n(\mathbb{R})$.
On suppose par exemple $A \in GL_n(\mathbb{R})$, on a :

$$\begin{aligned} \chi_{AB} &= det(AB - XI_n) \\ &= det(ABAA^{-1} - XAA^{-1}) \\ &= detAdet(BA - XI)det(A^{-1}) \\ &= det(BA - XI) \\ &= \chi_{BA} \end{aligned}$$

2^e cas : ni A, ni B $\in GL_n(\mathbb{R})$.
On sait que $GL_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(K)$, donc : $\exists (A_p)_{p\in\mathbb{N}} \subset GL_n(K)$ tq $A = lim_{p\longrightarrow+\infty} A_p$.
D'aprés ce qui précède on a : $\forall p \in \mathbb{N}, \chi_{ApB} = \chi_{BAp}$ ainsi, par continuité des applications : $A \longmapsto detA$ et $(A,B) \longmapsto AB$, et en faisant tendre p vers $+\infty$ on recupère $\chi_{AB} = \chi_{BA}$.

Proposition 2 : $GL_n(\mathbb{C})$ est connexe, mais $GL_n(\mathbb{R})$ ne l'est pas.

Preuve :
. $GL_n(\mathbb{C})$ est connexe par arcs, en effet :
Soient A et B deux matrices de $GL_n(\mathbb{C})$.
On pose : $P(X) = det(XA+(1-X).B)$, $\mathcal{Z}(p) = \{\alpha \in \mathbb{C}/P(\alpha) = 0\}$, $\varphi : z \longmapsto zA+(1-z)B$, continue.
On a $\mathcal{Z}(P)$ est fini donc $\mathbb{C} \setminus \mathcal{Z}(P)$ est connexe. Et comme $\varphi(\mathbb{C} \setminus \mathcal{Z}(p))$ est un connexe de $GL_n(\mathbb{C})$ qui contient A et B ; ($A = \varphi(1)$ et $B = \varphi(0)$).
Donc $GL_n(\mathbb{C})$ est connexe par arcs, ainsi $GL_n(\mathbb{C})$ est connexe. (on peut mentionner que $GL_n(\mathbb{C})$ est ouvert de l'e.v.n $\mathcal{M}_n(\mathbb{C})$ qui est de dimension finie.
.. L'espace topologique $\mathbb{R}^*$ est non connexe et l'application det : $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ est continue et surjective, par conséquent, $GL_n(\mathbb{R})$ est non connexe.

Proposition 3 : La suite $1 \longrightarrow SL_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^* \longrightarrow 1$ est exacte et on a : $GL_n(\mathbb{K}) \simeq SL_n(\mathbb{K}) \times \mathbb{K}^*$.

Preuve :
Soit H le sous groupe de $GL_n(\mathbb{K})$ formé des matrices de la forme :

$$A(\lambda) = \begin{pmatrix} \lambda & 0 & . & . & . & 0 \\ 0 & 1 & 0 & & & . \\ . & . & . & . & & . \\ . & & . & . & . & . \\ . & & & . & . & 0 \\ 0 & . & . & . & 0 & 1 \end{pmatrix}, \quad \lambda \in \mathbb{K}^*$$

Alors la restriction $det_{/H}$ induit un isomorphisme de H sur $\mathbb{K}^*$. Ce qui prouve la surjectivité du determinant et le produit semi-direct.

II- Sous-groupes remarquables de $GL_n(\mathbb{K})$:

Définition 1 : On appelle respectivement groupes orthogonal, spécial orthogonal, unitaire et spécial unitaire, les groupes :

$$O(n) = \{A \in GL_n(\mathbb{R}) \; ; \; {}^\top A = A^{-1}\}.$$

$$\mathcal{S}O(n) = \{A \in O(n) \; ; \; detA = 1\}.$$

$$\mathcal{U}(n) = \{A \in GL_n(\mathbb{C}) \; ; \; A^* = A^{-1}\}.$$

$$\mathcal{S}\mathcal{U}(n) = \{A \in \mathcal{U}(n) \; ; \; detA = 1\}.$$

Proposition 1 : $O(n)$ et $\mathcal{U}(n)$ sont compactes, mais $\{A \in \mathcal{M}_n(\mathbb{C}), {}^tA = A^{-1}\}$ ne l'est pas.

Preuve :
.L'application $\varphi : \mathcal{M}_n(\mathbb{R}) \longrightarrow \mathcal{M}_n(\mathbb{R})$, $M \longmapsto {}^t M.M$ est continue et $O((n) = \varphi^{-1}(\{I_n\})$
Ainsi O_n est un fermé de $\mathcal{M}_n(\mathbb{R})$.
D'autre part : si l'on pose : $\| M \| = (tr({}^tM.M))^{1/2}$.
On aura : $\| A \| = \sqrt{n}$ pour tout élement A de $O(n)$ ainsi $O(n)$ est borné.
Le groupe $O(n)$ est donc un compact de $\mathcal{M}_n(\mathbb{R})$.
..Il en est de même pour $\mathcal{U}(n)$ en considérant l'application continue $M \longmapsto M^*M$ et la norme : $\| M \| = (tr(M^*M))^{1/2}$.
...On considère $O(n,\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \; ; \; {}^tA = A^{-1}\}$, le groupe des matrices orthogonales à coefficients dans $\mathbb{C}$. Celui-ci n'est pas compact. En effet, pour n=2 on peut exhiber dans $O(2,\mathbb{C})$ des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ pour les quelles a est arbitrairement grand.

Proposition 2 : Soit E un espace euclidien et soit $u \in \mathcal{L}(\text{ E })$ une isométrie alors il existe une base isometrie alors il existe une base orthonormale $\mathcal{B}$ de E dans laquelle la matrice de u est de forme :

$$mat_{\mathcal{B}}(u) = \begin{pmatrix} \varepsilon_1 & 0 & . & . & . & . & . & . & . & 0 \\ 0 & . & 0 & & & & & & & . \\ . & . & . & . & & & & & & . \\ . & & . & . & . & & & & & . \\ . & & & . & \varepsilon_r & . & & & & . \\ . & & & & . & R_{\theta_1} & . & & & . \\ . & & & & & . & . & . & & . \\ . & & & & & & . & . & . & . \\ . & & & & & & & . & . & 0 \\ 0 & . & . & . & . & . & . & . & 0 & R_{\theta_s} \end{pmatrix} (*).$$

où pour tout $i \in \{1,...,r\}$, $\varepsilon_i \in \{-1,1\}$ et pour tout $j \in \{1,...,s\}$, $R_{\theta_j} = \begin{pmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$; $\theta_j \in \mathbb{R}$, $\theta_j \neq 0(mod\pi)$.

Preuve :
On procède par reccurence sur n = dim E.
Pour n =1, c'est évident .
H.R : "supposons que le résultat est vrai jusqu'au rang n-1". Montrons le à l'ordre n. nous traitons deux cas :
1^{er}cas :
L'isométrie u a au moins une valeur propre rèelle ε. Soit x un vecteur propre associé à ε. On a : $\| u(x) \| = \| \varepsilon x \| = | \varepsilon | \| x \|$et comme $\| u(x) \| = \| x \|$ on a $| \varepsilon | = 1$, de plus $\varepsilon \in \mathbb{R}$ donc $\varepsilon \in \{-1,1\}$. Maintenant, comme $F = vert(x)$ est stable par u, il en est de même pour $F^{\perp}$ car u est une isométrie. En appliquant H.R à $u/F^{\perp}$ on récupère une base orthonormale $\mathcal{B}_0$ de $F^{\perp}$ dans laquelle la matrice de $u/F^{\perp}$ est de la forme(*). En completant $\mathcal{B}_0$ par x, on obtient une base orthogonale $\mathcal{B}$ de E dans laquelle la matrice de u est de la forme souhaitée.
2^ecas :
L'isométrie u n'a aucune valeur propre rèelle.
On considère l'endomorphisme $v = u + u^*(u^* = {}^t u$ dans le cas rèel). Comme v est symétrique. v admet une valeur propre rèelle λ associée à un vecteur propre x.
On a : $(u+u^*)(x) = \lambda x$ donc $u(u+u^*)(x) = u^2(x) + x = \lambda u(x)$ d'où : $u^2(x) = \lambda u(x) - x \quad (1)$
Par ailleurs, la famille $(x, u(x))$ est libre puisque u n'admet pas de valeurs propre rèelles.
En posant $F = vert(x, u(x))$, on voit que $dimF = 2$ et que F est stable par u. (d'après (1)).
Soit $N = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ la matrice de u/F dans une base orthonormée $\mathcal{B}_1$ de F.

Comme u/F est une isométrie on a : $N^*N = I_n = NN^*$, parmi les équations issues de ces égalités, on trouve : $a^2+b^2 = a^2+c^2 = 1$ et $ab+cd = 0$. (2)
La première assertion de (2) entraine $c = \pm b$
Si $c = b$, N sera symétrique, ce qui est impossible car u n'admet pas de valeur propre rèelle. donc $c = -b \neq 0$.
La deusième assertion de (2) fournit alors $d = a$.
Et comme $a^2+b^2 = 1$, il existe $\theta \in \mathbb{R}$ tq : $a = \cos\theta$ et $b = \sin\theta$.
On a $b \neq 0$ exige que $\theta \neq k\pi$ ainsi $\theta \neq 0(mod\pi)$.
Finalement, on recupère la matrice N sous la forme : $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.
En fin, u étant une isométrie, le s.e.v $F^\perp$ est stable par u. Et $u/F^\perp$ est une isomètrie donc d'après H.R, il existe une base orthonormale $\mathcal{B}_0$ dans la quelle la matrice de $u/F^\perp$ est de la forme (*). La base $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1$ est alors orthonormale de E dans la quelle la matrice de u est de la forme souhaitée.

Application 1 : $O(n)$ a deux composantes connexes, notées $O^+(n)$ et $O^-(n)$ avec : $O^+(n) = \{A \in O(n), detA = 1\}, (= \mathcal{S}O(n))$, $O^-(n) = \{A \in O(n), detA = -1\}$, de plus $O^+(n)$ et $O^-(n)$ sont connexes par arcs.

preuve :
Connexité de $O^+(n) = \mathcal{S}O(n))$:
Soit O un élément de $\mathcal{S}O(n)$, il existe alors une matrice orthogonale $\mathcal{P}$ telle que :

$$\mathcal{P}^{(-1)}O\mathcal{P} = O' = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & -1 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & -1 & & & & & \\ & & & & & & R_{\theta_1} & & & & \\ & & & & & & & \ddots & & & \\ & & & & & & & & R_{\theta_k} & & \end{pmatrix}, \quad avec \quad R_{\theta_j} = \begin{pmatrix} cos(\theta_j) & sin(\theta_j) \\ -sin(\theta_j) & cos(\theta_j) \end{pmatrix}.$$

puisque $O \in \mathcal{S}O(n)$, les -1 sont en nombre pair, on peut donc les regrouper deux à deux pour donner les rotations de matrices :

$$\begin{pmatrix} cos(\theta) & sin(\theta) \\ -sin(\theta) & cos(\theta) \end{pmatrix}, \qquad avec \qquad \theta = \pi.$$

Alors l'application, $\varphi : [0,1] \to \mathcal{S}O(n), t \mapsto \varphi(t) = O'(t)$ (où $O'(t)$ est obtenue en remplaçant chaque θ_j par $t.\theta_j$ et θ par $t.\theta$), qui verifie $\varphi(0) = I_n$ et $\varphi(1) = O'$, est un chemin continu liant O' à I_n. Et puisque $\mathcal{P}$ est orthoganale, l'application $t \mapsto \mathcal{P}O'\mathcal{P}^{-1}$ définit un chemin continu dans $\mathcal{S}O(n)$ est connexe par arcs, et donc connexe.
..La connexité de $O^-(n)$ resulte clairement de celle de $O^+(n)$ grâce à l'application :

$$O \mapsto \begin{pmatrix} -1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & 1 & 0 \\ 0 & . & . & . & 0 & 1 \end{pmatrix} O$$

qui réalise un homeomorphisme entre $\mathcal{S}O(n)$ et $O^-(n)$.
...L'espace topologique $\{-1,1\}$ est non connexe et $det : O(n) \to \{-1,1\}$ est une application continue et surjective, par suite $O(n) = \mathcal{S}O(n) \cup O^-(n)$ alors $O(n)$ a bien deux composantes connexes.

Proposition 3 : Soit E un espace hermitien et $u \in \mathcal{L}(\text{ E })$ un endomorphisme unitaire. Alors il existe une base orthonormele qui diagonalise u, et toutes les valeurs propres de u sont de module égal à 1.

preuve :
Il est d'abord clair que toute valeur propre λ de u verifie $\mid \lambda \mid = 1$ car : si $u(x) = \lambda x$ on a : $\| x \| = \| u(x) \| = \| \lambda x \| = \mid \lambda \mid \| x \|$.
On procède ensuite par recurrence sur $n = dimE$.
Le cas de $n = 1$ est trivial, et le passage du rang $n-1$ au rang n se fait comme suit :
Le corps de base $\mathbb{C}$ étant algébriquement clos, u admet au moins une valeur propre complexe λ. Soit x un vecteur propre associé, $\| x \| = 1$. La droite $F = vect(x)$ est stable par u et comme u est unitaire l'hyperplan $F^\perp$ est également stable par u. L'endomorphisme $u_{/F^\perp}$ est unitaire et d'après l'hypothèse de récurrence, il existe une base orthonormale $\mathcal{B}_0$ de $F^\perp$ si on completé par x, on obtient une base $\mathcal{B}$ orthonormale de E qui diagonalise u, ainsi la proposition est prouvée.

Corollaire 1 : Soit $U \in \mathcal{M}_n(\mathbb{C})$ une matrice unitaire. Alors, il existe une matrice unitaire P telle que

$$P^{-1}UP = P^\star UP = \begin{pmatrix} \exp(i\theta_1) & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \exp(i\theta_n) \end{pmatrix},$$

où les θ_i, $\quad 1 \leq i \leq n$, sont des nombres réels.

preuve :
...C'est immediate d'après (la proposition 3. $\oint .II$).

Application 2 : $U(n)$ et $SU(n)$ sont connexes par arcs.

preuve :
...La même méthode comme dans l'application 2 montre que les groupes $U(n)$ et $SU(n)$ sont connexes par arcs.

Définition 2 : Un groupe de torsion est un groupe G dont tous les éléments sont d'ordre fini. Si de plus, ces ordres sont tous majorés par un même entier, on dit que le groupe G est d'exposant fini ; l'exposant de G étant alors le ppcm de ces ordres.

Définition 3 : Un groupe est dit de type fini s'il est engendré par l'une de ses parties finies.

Lemme 1 : $u \in \mathcal{L}(\mathbb{C}^n)$ est nilpotent si et seulement si : $tr(u^p) = 0$ pour tout p tel que $1 \leq p \leq n$.

preuve :
.Si u est nilpotent alors toutes ses valeurs propres sont nulles, donc il en est de même pour celles de u^p, $1 \leq p \leq n$

ainsi $tr(u^p)=0$ pour tout $1\leq p\leq n$.
..Réciproquement : Notons $\chi_u=(-1)^n X^\alpha(X-\lambda_1)^{\alpha_1}...(X-\lambda_r)^{\alpha_r}$, où les λ_i, $1\leq i\leq r$, sont non nuls et deux à deux distincts, le polynôme caractéristique de u. On a alors : pour tout $1\leq p\leq n$; $\alpha_1\lambda_1^p+\alpha_2\lambda_2^p+...+\alpha_r\lambda_r^p=tr(u^p)=0$. ie : $(\alpha_1,...,\alpha_r)$ est zéro non trivial du système :

$$\begin{cases} \lambda_1X_1 & + & . & . & . & + & \lambda_rX_r=0 \\ . & & . & . & . & . & . \\ . & & . & . & . & . & . \\ . & & . & . & . & . & . \\ \lambda_1^rX_1 & + & . & . & . & + & \lambda_r^rX_r=0 \end{cases}$$

donc le déterminant de ce système nul, ie :

$$\lambda_1\lambda_2...\lambda_r\begin{vmatrix} 1 & 1 & . & . & . & . & 1 \\ \lambda_1 & \lambda_2 & . & . & . & . & \lambda_r \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ \lambda_1^{r-1} & \lambda_2^{r-1} & . & . & . & . & \lambda_r^{r-1} \end{vmatrix}=0.$$

d'où en explicitant ce déterminat de Vandermonde :

$$\lambda_1\lambda_2...\lambda_r\Pi_{1\leq i<j\leq r}(\lambda_j-\lambda_i)=0.$$

Ce qui est impossible puisque les λ_i sont non nuls et deux à deux distincts.

Théorème 1 : (de W. Burnside) Un sous groupe G de $GL_n(\mathbb{C})$ est fini si et seulement s'il est d'exposant fini.

preuve :
..Condition nécessaire : si G est fini alors G est d'exposant fini d'après le théorème de Lagrange.
..condition suffisante : supposans qu'il existe un entier $e\geq 1$ tel que : $A^e=I_n$ pour tout $A\in G$. Considérons une famille génératrice $c_1,c_2,...,c_r$ de la sous-algèbre $\mathcal{J}$ de $\mathcal{M}_n(\mathbb{C})$ engendrée par G. On définit alors une application,

$$\begin{array}{rccl} \tau & : & G & \to & \mathbb{C}^r \\ & & A & \mapsto & \tau(A)= (tr(Ac_1),tr(Ac_2),...,tr(Ac_r)) \end{array}$$

Montrons que τ est injective :
si A et B vérifient $\tau(A)=\tau(B)$ alors on a : $tr(AM)=tr(BM)$ pour tout $M\in G$, car les c_i engendrent $\mathcal{J}$ qui contient G.
Notons : $N=AB^{-1}-I_n$. N est diagonalisable ; En effet : Comme $AB^{-1}\in G$, alors AB^{-1} annule le polynôme X^e-1 qui est sindé à racines simples dans $\mathbb{C}$, donc AB^{-1} est diagonalisable, ainsi, il existe P inversible tel que : $PAB^{-1}P^{-1}=\Delta$ soit diagonale, mais dans ce cas $PAB^{-1}P^{-1}-I_n=\Delta-I_n$ est aussi diagonale d'où $P(AB^{-1}-I_n)P^{-1}$ est diagonale, ce qui signifie que N est diagonalisable. D'autre part on a :

$$\begin{array}{rcl} tr((AB^{-1})^p) & = & tr(A(B^{-1}(AB^{-1})^{p-1})) \\ & = & tr(B(B^{-1}(AB^{-1})^{p-1})) \\ & = & tr((AB^{-1})^{p-1}). \end{array}$$

d'où, de proche en proche, on a pour tout $p\in\mathbb{N}$:
$tr((AB^{-1})^p)=tr(I_n)=n$.
Et comme les matrices AB^{-1} et I_n commutent, on a :

$$N^k=(AB^{-1}-I_n)^k=\Sigma_{p=0}^k\binom{k}{p}(-1)^{k-p}(AB^{-1})^p$$

d'où :

$$\begin{array}{rcl} tr(N^k) & = & \Sigma_{p=0}^k\binom{k}{p}(-1)^{k-p}tr((AB^{-1})^p) \\ & = & \Sigma_{p=0}^k\binom{k}{p}(-1)^{k-p}n \\ & = & n\Sigma_{p=0}^k\binom{k}{p}(-1)^{k-p}=n(1-1)^k=0. \end{array}$$

ainsi $tr(N^k)=0$ pour tout k, et il découle alors du lemme que N est diagonalisable et nilpotente, on a $N=0$ ainsi $AB^{-1}=I_n$ d'où $A=B$, ce qui montre que τ est injective.
Les éléments de G annulent le polynôme X^e-1 qui est sindé à racines simples dans $\mathbb{C}$. Donc tous les éléments de G sont diagonalisables à valeurs propres dans l'ensemble des racines e^{ime} de l'unité ; Il s'en suit que les traces des éléments de G ne peuvent prendre qu'un nombre fini de valeurs ; $\tau(G)$ est donc fini, mais τ est injective, donc G est aussi fini.

Lemme 2 : Soit $\mathbb{K}$ une extention de $\mathbb{Q}$ de degré δ, et soit $P\in\mathbb{K}[T_1,...,T_m]$. Il existe $\overline{P}\in\mathbb{Q}[T_1,...,T_m]$ tel que $deg(\overline{P})=\delta.deg(P)$ et $\forall(z_1,...,z_m)\in\mathbb{C}^m$, $P(z_1,...,z_m)=0\Longrightarrow\overline{P}(z_1,...,z_m)=0$.

preuve :
Le théorème de l'élément primitif donne : $\mathbb{K}=\mathbb{Q}(\theta)$; on note P_θ le polynôme minimal de θ. Les conjugués : $\theta_2,...,\theta_\delta$ de θ sont les autres racines complexes de P_θ et sont simples puisque P_θ est irreductible sur $\mathbb{Q}$. On note σ_k le morphisme canonique $\mathbb{Q}(\theta)\to\mathbb{Q}(\theta_k)$ et $\sigma_1=id_{\mathbb{K}}$. On écrit :

$$P=\Sigma_l c_l(\theta)T^l,\qquad avec\qquad c_l\in\mathbb{Q}[X]\qquad et\qquad deg(c_l)<\delta$$

d'où l'unicité de c_l. On pose :

$$P^{\sigma_k}=\Sigma_l c_l(\theta_k)T^l\in\mathbb{Q}(\theta_k)[T_1,...,T_m]\qquad et\qquad \overline{P}=PP^{\sigma_2}...P^{\sigma_\delta}$$

Le coefficient en X^l de P est :

$$\overline{c}_l(\theta_1,...,\theta_\delta)=\Sigma_{l_1+...+l_\delta=l}c_{l_1}(\theta_1)...c_{l_\delta}(\theta_\delta).$$

ie : est une expression polynômiale à coefficients rationnels en des polynômes symétriques élémentaires $\Sigma_k(\theta_1,...,\theta_\delta)$ or ces derniers sont les coefficients, à un signe prés, de P_θ donc $\overline{P}\in\mathbb{Q}[T_1,...,T_m]$. De plus on a clairement $deg(\overline{P})=\delta.deg(P)$ et le fait que $P=P^{\sigma_1}$ divise $\overline{P}$ assure la derniére assertion.

Lemme 3 : Soit E une extension de degré d de $T=\mathbb{Q}(a_1,...,a_t)$ où les $a_i, 1\le i\le t$ sont algébriquement indépendants sur $\mathbb{Q}$, alors $E\cap\overline{\mathbb{Q}}$ est une extension de $\mathbb{Q}$ de degré au plus d. ($\overline{\mathbb{Q}}$ étant une clôture algébrique de $\mathbb{Q}$).

preuve :
Notons $F=E\cap\overline{\mathbb{Q}}$ et considérons $(z_1,...,z_{d+1})\in F^{d+1}$. Comme E est de degré d sur T, $(z_1,...,z_{d+1})$ est liée sur T. c-à-d : il existe $P_1,P_2,...,P_{d+1}\in\mathbb{Q}[T_1,...,T_t]$ tels que : $P_1(a_1,...,a_t)z_1+...+P_{d+1}(a_1,...,a_t)z_{d+1}=0$. On pose alors : $P=\Sigma_{k=1}^{d+1}P_k(T_1,...,T_t)z_k$. D'après le lemme précédent, il existe $\overline{P}\in\mathbb{Q}[T_1,...,T_t]$ tel que $\overline{P}(a_1,...,a_t)=0$ ie : $\overline{P}=0$ par l'hypothèse sur les a_i. Avec les notations du lemme précédent on a $P^{\sigma_{k_0}}=0$ pour un certain k_0, donc $c_l(\theta_{k_0})=0$ ie : c_l est divisible dans $\mathbb{Q}[X]$ par le polynôme minimal de θ_{k_0} ie : par P_θ, d'où $x_l(\theta)=0$ et $P=0$. Considérons enfin $(x_1,...,x_t)\in\mathbb{Q}^t$ tel que $P_k(x_1,...,x_t)\in\mathbb{Q}$ pour tout k ; alors la relation :

$$P_1(x_1,...,x_t)z_1+...+P_{d+1}(x_1,...,x_t)z_{d+1}=0$$

. signifie que les z_i sont liés sur $\mathbb{Q}$.

Théorème 2 : (de I. Schur) Un sous groupe G de $GL_n(\mathbb{C})$ est d'exposant fini si et seulement s'il est de torsion et de type fini.

preuve :
.Condition nécessaire : Si G est d'exposant fini, alors G est de torsion d'après (définition 2, $\oint$ II). et vu (le théorème de Burnside, $\oint$ II) G est fini, donc de type fini.
..Condition suffisante : Soit E le sous corps de $\mathbb{C}$ engendré par une partie génératrice de G. On peut supposer que E est une extension finie de degré d de $T=\mathbb{Q}(a_1,...,a_t)$ où les a_i sont algébriquement indépendants.
de A ; Comme G est de torsion, donc A annule un polynôme de la forme X^N-1, d'où ξ est une racine primitive $N^{ième}$ de l'unité. De plus ξ est une racine de χ_A donc ξ est algébrique sur E de degré $r\le n$. Le polynôme

minimal R de ξ divise X^N-1 dans $E[X]$ donc dans $\mathbb{C}[X]$, d'où R s'écrit : $R=\Pi_{\alpha\in\mathcal{A}}(X-\alpha)$ où $\mathcal{A}$ désigne une partie du groupe des racines $N^{ième}$ de l'unité. Donc les coefficients de R sont dans le corps cyclotomique $\mathbb{Q}(\xi)$ donc dans $\overline{\mathbb{Q}}$ et en conséquence dans $(E\cap\overline{\mathbb{Q}})[X]$.
D'après le second lemme, $E\cap\overline{\mathbb{Q}}$ est une extension finie de $\mathbb{Q}$ de degré au plus d. D'après le premier lemme, il existe $\overline{R}\in\mathbb{Q}[X]$ tel que $\overline{R}(\xi)=0$, $deg(\overline{R})=[E\cap\overline{\mathbb{Q}}:\mathbb{Q}].deg(R)$ et $deg(\overline{R})\leq dr$. Le polynôme minimal ϕ_N de ξ sur $\mathbb{Q}$ divise $\overline{R}$ dans $\mathbb{Q}[X]$ donc $deg(\phi_N)\leq deg(\overline{R})$, d'où $\varphi(N)\leq dr\leq dn$. Ainsi $\varphi(N)$ est borné indépendament de A. Comme $\varphi(N)$ tend vers $+\infty$ quand $N\to+\infty$, N est majoré par une constante e ne dépendant que de G et, quitte à prendre $e!$, on peut supposer que e est un multiple de N. donc $\xi^e=1$ ie : les valeurs propres de A^e valent toutes 1. Mais $A^e\in G$ est diagonalisable donc $A^e=I_n$ ie : G est d'exposant fini.

Exemple 1 : Si G est un sous groupe de $GL_n(\mathbb{C})$ d'exposant 2 alors il existe $k\leq n$ tel que : $G\simeq(\mathbb{Z}/2\mathbb{Z})^k$.

Application 3 : soient m et n deux entièrs ≥ 1. Pour que $GL_n(\mathbb{C})$ et $GL_m(\mathbb{C})$ soient isomorphes (en tant que groupes), il faut et il suffit que $n=m$.

preuve :
Cherchons à caractériser n à l'aide de l'ensemble des sous-groupes abéliens de $GL_n(\mathbb{C})$. On note r l'ordre maximal des sous-groupes abéliens finis G de $GL_n(\mathbb{C})$ vérifiant :

$$\forall M\in G : M^2=I \qquad (*)$$

Soit H un sous-groupe abélien de $GL_n(\mathbb{C})$ vérifiant $(*)$ et d'ordre r. Comme H est abélien et que tous les éléme nts de H sont diagonalisables (ils annulent un polynôme scindé à racines simples), ils sont codiagonalisables. Ainsi, à conjugaison près, H e st exactement l'ensemble des matrices de la forme (n'oublions pas que H est d'ordre maximal) :

$$\begin{pmatrix} \pm1 & & & & \\ & \pm1 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & \pm1 \end{pmatrix}$$

et donc $r=2^n$. Mais alors, si $GL_n(\mathbb{C})$ et $GL_m(\mathbb{C})$ sont isomorphes, ils ont le même r et $m=n$. On trouvra un résultat plus général dans [Che].

Chapitre II

GÉNÉRTEURS ET CENTRE

I-Dilatation et transvection :

Définition 1 : Soit $f \in GL(E)$ avec $f \neq id_E$ et soit H un hyperplan de E stable par f avec $f/H = id_E$. On dit que f est une dilatation d'hyperplan H et de rapport $\lambda \neq 1$ s'il existe une base dans laquelle la matrice de f soit $diag(1,...,1,\lambda)$.

Proposition 1 : Deux dilations sont conjuguées dans $GL(E)$ si et seulement si elles ont le même rapport.

preuve :
C'est clair, car elles ont même matrice dans des bases convenables.

Définition 2 : Soient $f \in GL(E)$ avec $f \neq id_E$ et $H = ker(\psi)$ un hyperplan de E stable par f avec $f/H = id_H$. On dit que f est une transvection d'hyperplan H et de droite $< a >$ s'il existe une base dans laquelle la matrice de f soit :

$$\begin{pmatrix} 1 & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & 0 & 0 \\ . & . & . & 1 & 1 \\ 0 & . & . & 0 & 1 \end{pmatrix}.$$

ie : si $f(x) = x + \psi(x).a$ pour tout $x \in E$.

Exemple : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est une matrice de transvection.

Proposition 2 : Deux transvections sont conjuguées dans $GL(E)$ et, si $n \geq 3$ alors elles sont conjuguées dans $SL(E)$.

preuve :
Dans $GL(E)$, c'est clair, elles ont même forme reduite de Jordan.
Supposons $n \geq 3$ et soient u, v deux transvections et $w \in GL(E)$, telles que : $v = wuw^{-1}$. Si $\lambda = det(w)$, il suffit de trouver $s \in GL(E)$, avec $det(s) = \lambda^{-1}$ et $svs^{-1} = v$. En effet, on aura alors : $(sw)u(sw)^{-1} = v$ et $sw \in SL(E)$; pour ceci, on se place dans une base dans laquelle v a pour matrice :

$$\begin{pmatrix} 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & 1 & 1 \\ 0 & . & . & . & . & . & 0 & 1 \end{pmatrix}, \quad et \quad on \quad prend, \quad s = \begin{pmatrix} 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & \lambda & . & . \\ . & . & . & . & . & . & 1/\lambda & 0 \\ 0 & . & . & . & . & . & 0 & 1/\lambda \end{pmatrix}.$$

Ce qui est possible puisqu'on a $n \geq 3$. IL est alors clair que s convient.

Remarque : Les tranvections $s = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $SL_2(\mathbb{K})$ si et seulement si $\lambda\mu^{-1}$ est un carre de $\mathbb{K}$.

En effet : supposons qu'il existe $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\alpha\delta - \beta\gamma = 1$ verifiant : $gsg^{-1} = t$ on a alors $gs = tg$; c-à-d :

$$gs = \begin{pmatrix} \alpha & \alpha\lambda+\beta \\ \gamma & \gamma\lambda+\delta \end{pmatrix} = tg = \begin{pmatrix} \alpha+\mu\gamma & \beta+\mu\delta \\ \gamma & \delta \end{pmatrix}$$

Ce qui implique : $\gamma = 0$ et $\alpha\lambda = \mu\delta$, en plus, $det(g) = 1$ éxige : $\delta = 1/\alpha$ ainsi, $\lambda/\mu = \delta^2$; $\lambda\mu^{-1}$ est un carré de $\mathbb{K}$.
...Réciproquement : si $\lambda/\mu = \delta^2$ avec $\delta \in \mathbb{K}^*$, on prend alors $\alpha = 1/\delta$, $\gamma = 0$ et β quelconque, et g convient pour passer de s à t.

Proposition 3 : Soit τ une transvection de droite D et d'hyperplan H, et soit $u \in GL(E)$. Alors, $u\tau^{-1}u$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$. Précisément si on a : $\tau = \tau(f,a)$ alors : $u\tau u^{-1} = \tau(f \circ u^{-1}, u(a))$.

preuve :
On a, pour $x \in E$: $\tau u^{-1}(x) = u^{-1}(x) + f(u^{-1}(x)).a$, d'où : $u\tau u^{-1}(x) = x + f(u^{-1}(x)).u(a)$; d'où le resultat. On notera que si $H = ker(f)$, alors : $u(H) = ker(f \circ u^{-1})$.

II-Centre de $GL(E)$, Centre de $SL(E)$:

Lemme : Soit $u \in GL(E)$ si u laisse invariantes toutes les droites vectorielles de E, alors u est une homothetie.

preuve :
En formules, ceci s'écrit comme une interversion de quantificateurs :

$$(\forall x \in E), (\exists \lambda \in \mathbb{K}^*); (u(x) = \lambda x) \Rightarrow (\exists \lambda \in \mathbb{K}^*), (\forall x \in E), (u(x) = \lambda x).$$

Pour $n = 1$ c'est clair, sinon : soient $x, y \in E$:
-Si x, y sont non colinéaires on a : $u(x) = \lambda x$, $u(y) = \mu y$ mais aussi : $u(x+y) = \nu(x+y) = \lambda x + \mu y$ ainsi $(\nu - \lambda)x + (\nu - \mu)y = 0$ d'où $\lambda = \mu = \nu$, ainsi : $\forall x \in E$, $u(x) = \lambda x$.
-Si x et y sont colinéaires le resultat est evident.

Application 1 : i- Le centre de $GL(E)$ est formé des homotheties de rapport $\lambda \in \mathbb{K}^*$; $\mathcal{Z}(GL(E)) = \mathbb{K}^* id_E \simeq \mathbb{K}^*$.
ii- Le centre de $SL(E)$ est l'ensemble des homotheties dont le rapport est une racine $n^{ième}$ de l'unité dans $\mathbb{K}$; $\mathcal{Z}(SL(E)) = \mathbb{K}^* id_E \cap SL(E) \simeq \mathbb{U}_n(\mathbb{K}) = \{\lambda \in \mathbb{K}, \lambda^n = 1\}$.

preuve :
i-Soit $u \in \mathcal{Z}(GL(E))$. Pour toute transvection τ d'hyperplan H et de droite D on a : $u\tau u^{-1} = \tau$ est une transvection de droite $u(D) = D$ ainsi $\forall x \in E$ $(x, u(x))$ est liée.
On en déduit que u est une homothetie, ainsi $u = \lambda.id_E$ avec $\lambda \in \mathbb{K}^*$.
..Réciproquement ; $\forall \lambda \in \mathbb{K}^*$, $\lambda id_E \in \mathcal{Z}(GL(E))$ ainsi $\mathcal{Z}(GL(E)) = \mathbb{K}^* id_E \simeq \mathbb{K}^*$.
ii- On a : $\mathcal{Z}(SL(E)) = \mathcal{Z}(GL(E)) \cap SL(E) = \mathbb{K}^* id_E \cap SL(E)$. donc si $u \in \mathcal{Z}(SL(E))$ on a : $u = \lambda id_E$ et $det(u) = 1$ d'où $\lambda^n = 1$ donc $\lambda \in \mathbb{U}_n(\mathbb{K})$. Inversement si $\lambda \in \mathbb{U}_n(K)$, on a évidement : $u = \lambda.id_E \in \mathcal{Z}(GL(E)) \cap SL(E) = \mathcal{Z}(SL(E))$ ainsi $\mathcal{Z}(SL(E)) \simeq \mathbb{U}_n(\mathbb{K})$.

Définition 1 : Le quotient de $GL(E)$ par son centre est applé le groupe projectif linéaire. Noté $PGL(E) = GL(E)/\mathcal{Z}(GL(E))$. De façon analogue on définit : $PSL(E) = SL(E)/\mathcal{Z}(SL(E))$, dit le groupe projectif spécial linéaire.

Remarque : Si $\mathbb{K}$ est algébriquement clos alors : $PGL(E) \simeq PSL(E)$; En effet : Soit h_λ l'homothétie $x \mapsto \lambda x$ on a $det(h_\lambda) = \lambda^n$, de sorte qu'on a une suite exacte :

$$1 \quad \to \quad PSL(E) \quad \to \quad PGL(E) \quad \xrightarrow{\overline{det}} \quad \mathbb{K}^*/(\mathbb{K}^*)^n \quad \to \quad 1$$

où on a posé $(\mathbb{K}^*)^n = \{\lambda \in \mathbb{K}^* / \exists \mu \in \mathbb{K}^*, \lambda = \mu^n\}$ En particulier, si $\mathbb{K}$ est algébriquement clos, on a $\mathbb{K}^* = (\mathbb{K}^*)^n$, donc on a un isomorphisme entre $PSL(E)$ et $PGL(E)$; $PSL(E) \simeq PGL(E)$.

III-Générateurs :

Proposition 1 :Soit $u \in GL(E)$, $u \neq id_E$.Les propriétés suivantes sont équivalentes :
i-u est une transvection de droite D.
ii-On a $u/D = id$ et l'homomorphisme $\overline{u} : E/D \to E/D$ est l'identité.

preuve :
i)⇒ ii) : est claire.
ii)⇒ i) : La condition sur le quotient $\overline{u}(\overline{x}) = \overline{x}$, s'écrit encore : $\forall x \in E, u(x) - x \in D$. On a donc $Im(u - id_E) \subseteq$ et comme $u \neq id_E$, cela impose $Im(u - id_E) = D$; Il en résulte que $ker(u - id_E)$ est un hyperplan, contenant D. Et puisque $u/D = id$, u est bien une transvection de droite D.

Lemme : Soient $x, y \in E \setminus \{0\}$. Il existe une translation u ou un produit de deux translations uv tels que $u(x) = y$ ou $uv(x) = y$.

preuve :
-Supposons x et y non colinéaires. On cherche u sous la forme $u(x) = x + f(x)a$. On prend $a = y - x$ et pour H un hyperplan contenant a mais pas x. On choisit alors l'equation f de H de sorte que l'on ait $f(x) = 1$; ainsi $u = \tau(f, a)$ convient.
-Si x et y sont colinéaires ; on prend z non colinéaire à x, y et on trouve, d'après ce qui précede, deux transvections u et v telles que : $v(x) = z$ et $u(z) = y$, ainsi $uv(x) = y$.

Théorème : Les transvections engendrent $SL(E)$.

preuve :
Par récurrence sur n. Pour n=1, c'est clair. Soit $u \in SL(E)$ et soit $x \in E$, $x \neq 0$ quitte à remplacer u par vu où v est un produit de deux transvections, on peut supposer que l'on a : $u(x) = x$ (lemme précédent).
Soit D la droite engendrée par x et soient $\pi : E \to E/D$ la projection canonique, et $\overline{u} : E/D \to E/D$ l'automorphisme induit par u.
..Montrons tout d'abord qu'on a : $\overline{u} \in SL(E/D)$, pour ce faire, on prend une base, $e_1 = x, e_2, ..., e_n$ de E, de sorte que $\pi(e_2), ..., \pi(e_n)$ soit une base de E/D. Si on écrit les matrices de u et $\overline{u}$ dans ces bases, en tenant compte de $u(e_1) = e_1$, le développement de $det(u)$ par rapport à la première colonne montre qu'on a aussi $det(\overline{u}) = 1$.
-On applique alors à $\overline{u}$, l'hypothèse de recurrence, on a : $\overline{u} = \overline{\tau}_1 \overline{\tau}_2 ... \overline{\tau}_r$, où $\overline{\tau}_i = (\overline{f}_i, \overline{a}_i)$ est une transvection de E/D. Soit alors $a_i \in E$ tel que $\overline{u}(a_i) = a_i$ et $f_i \in E^*$ définie par $f_i = \overline{f}_i \circ \pi$. Posons $\tau_i = \tau(f_i, a_i)$, il est clair que τ_i induit $\overline{\tau}_i$ sur E/D. De plus, comme $f_i(x) = \overline{f}_i \circ \pi(x) = 0$, on a $\tau_i(x) = x$. posons alors $v = \tau_1 \tau_2 ... \tau_r$ on a : $v(x) = u(x)$ et $\overline{v} = \overline{u}$, donc en vertu de la proposition1 ($\oint III$, chapitre II), $v^{-1}u$ est une transvection de sorte que u est produit de transvections.

corollaire : Les transvections et les dilatations engendrent $GL(E)$.

preuve :
Soit $u \in GL(E)$ avec $\lambda = det(u)$, et soit v une dilatation de rapport λ^{-1}. On a alors $vu \in SL(E)$, et donc, u est produit de v^{-1} et de transvections.

Rappels : On note E_{ij} les matrices élémentaires de $M_n(\mathbb{K})$: 1 en place (i, j) et 0 ailleurs.
.Les matrices $D_i(\lambda) = I + (\lambda - 1)E_{ij} = Diag(1, ..., 1, \lambda, 1, ..., 1)$, où $\lambda \in \mathbb{R}^*$ en place (i, i), sont dites matrices de dilatations.
.On appelle matrice de transvection toute matrice de la forme $T_{ij}(\mu) = I + \mu E_{ij}$, avec μ réel et $i \neq j$.

Application 1 : $GL_n(\mathbb{R})$ a deux composantes connexes homéomorphe ; $GL_n^+(\mathbb{R}) = \{A \in M_n(\mathbb{R}); \quad det(A) > 0\}$, $GL_n^-(\mathbb{R}) = \{A \in M_n(\mathbb{R}); \quad det(A) < 0\}$. $GL_n^+(\mathbb{R})$ et $GL_n^-(\mathbb{R})$ sont connexes par arcs.

preuve :
Chaque matrice A de $GL_n(\mathbb{R})$ s'écrit de façon unique sous la forme : $A = D_n(a).S$ (resp.$S'.D_n(a)$), où a est dans $\mathbb{R}^*$.
S et S' sont des produits de matrices de transvections, et pour $D_n(a)$ ($c.f$ rappel ci-dessus). On a alors $a = det(A)$.
.Soit $A \in GL_n^+(\mathbb{R})$. Ecrivons : $A = D_n(a)T_{i_1 j_1}(\mu_1)T_{i_2 j_2}(\mu_2)...T_{i_r j_r}(\mu_r)$; Avec : $a = det(A) > 0$ et les $\mu_k, 1 \leq k \leq r$, dans $\mathbb{R}$. On pose : $A(t) = D_n((1-t)a+t)T_{i_1 j_1}((1-t)\mu_1)....T_{i_r j_r}((1-t)\mu_r)$. pour $t \in [0,1]$, l'application continue $t \to A(t)$ est un chemin, dans $GL_n^+(\mathbb{R})$, qui permet de connecter $A(0) = A$ à $A(1) = I$. Le point I est donc un point pivot de $GL_n^+(\mathbb{R})$ et la connexité par arcs en resulte.
.On procéde de la même façon pour mettre en évidence la connexité (par arcs) de $GL_n^-(\mathbb{R})$, et aussi avec $SL_n(\mathbb{R})$; $(a = 1)$.
.On a $GL_n(\mathbb{R}) = GL_n^+(\mathbb{R}) \cup GL_n^-(\mathbb{R})$, avec $GL_n(\mathbb{R})$ étant non connexe (prop.2. $\oint I$, chapitre I). Ce qui achève la démonstration.

IV-Groupe derivé :

Proposition 1 :
$D(GL(E)) = SL(E)$ sauf si $E = \mathbb{F}_2^2$.
$D(SL(E)) = SL(E)$ sauf si $E = \mathbb{F}_2^2$ (resp.$\mathbb{F}_3^2$).

preuve :
On note toujours que E est un-$\mathbb{K}$ .e.v de dimention n.
.i) Si g et h sont dans $GL(E)$ on a : $det(ghg^{-1}h^{-1}) = 1$ et donc on a toujours : $D(GL(E)) \subseteq SL(E)$ et $D(SL(E)) \subseteq SL(E)$.
.ii) Pour établir les autres inclusions, il suffit de prouver qu'une transvection u est un commutateur ; En effet :
Si on a : $u = aba^{-1}b^{-1}$ avec $ab \in SL(E)$, (resp $a.b \in GL(E)$), et si v est une autre transvection, u et v sont alors conjuguées dans $GL(E)$, (prop2 $\oint I$, chapitre II), ainsi il existe $g \in GL(E)$ tel que $v = gug^{-1} = i_g(u)$ où i_g désigne l'automorphisme intérieur de $GL(E)$ défini par g, on a alors :
$v = i_g(u) = i_g(a)i_g(b)i_g(a)^{-1}i_g(b)^{-1}$, et comme $SL(E)$ est distingué dans $GL(E)$, on a : $i_g(a), i_g(b) \in SL(E)$ (resp.$GL(E)$). On voit ainsi que toutes les transvections sont des commutateurs, mais comme elles engendrent $SL(E)$ on a $SL(E) \subseteq D(SL(E))$, resp $SL(E) \subseteq D(GL(E))$.
a-Un cas particulier bien agréable est le suivant : $n \geq 3$ et $car(\mathbb{K}) \neq 2$, En effet : Si u est une transvection, u^2 en est aussi une car $u^2 \neq id_E$ puisque $car(\mathbb{K}) \neq 2$; (C'est visible matriciellement). $n \geq 3$, donc u et u^2 sont conjuguées dans $SL(E)$, d'où $u^2 = sus^{-1}$ avec $s \in SL(E)$, ainsi $u = sus^{-1}u^{-1} = [s,u]$ et donc $u \in D(SL(E))$ on montré ainsi que : $D(SL(E)) = SL(E)$ et, à fortiori, $D(GL(E)) = SL(E)$.
b-Supposons que $n = 2$ et $|\ \mathbb{K}\ | > 3$ (ie : $\mathbb{K} \neq \mathbb{F}_2, \mathbb{F}_3$).
Si on pose : $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $s = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $\lambda \neq 0$ on aura : $\tau = sts^{-1}t^{-1} = \begin{pmatrix} 1 & \lambda^2 - 1 \\ 0 & 1 \end{pmatrix}$ et si on choisit $\lambda \neq 1$, ce qui est possible car $|\ \mathbb{K}\ | > 3$, alors τ est une transvection et on a : $D(SL_2(\mathbb{K})) = D(GL_2(\mathbb{K})) = SL(\mathbb{K})$.
b-Supposons que $n = 2$ et $|\ \mathbb{K}\ | > 3$ (ie : $\mathbb{K} \neq \mathbb{F}_2, \mathbb{F}_3$). Si on pose : $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $s = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $\lambda \neq 0$ on aura : $\tau = sts^{-1}t^{-1} = \begin{pmatrix} 1 & \lambda^2 - 1 \\ 0 & 1 \end{pmatrix}$ et si on choisit $\lambda \neq 1$, ce qui est possible car $|\ \mathbb{K}\ | > 3$, alors τ est une transvection et on a : $D(SL_2(\mathbb{K})) = D(GL_2(\mathbb{K})) = SL_2(\mathbb{K})$.
-pour $n > 2$, la méthode fonctionne en choisissant un plan P, un supplémentaire S de P et en prolongeant les matrices ci-dessus par id_S.
c-Si $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$ mais $n \geq 3$. On considère les matrices : $u = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$, $t = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et $s =$

$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ de sorte que : u soit une transvection et on ait : $u = tst^{-1}s^{-1}$ avec $s,t \in SL(E)$. Et on conclut comme en b.

d-Il reste à montrer que : $D(GL_2(\mathbb{F}_3)) = SL_2(\mathbb{F}_3)$ on regarde les matrices : $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; on a : $sts^{-1}t^{-1} = t$ donc $t \in D(GL(E))$. On prendra garde que s n'appartient pas à $SL(E)$ et qu'on ne peut conclure pour $D(SL(E))$.

e-Enfin, pour les cas exceptionnels, on a : $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ donc $D(SL_2(\mathbb{F}_2)) = D(GL_2(\mathbb{F}_2)) \simeq \mathfrak{A}_3$ et comme $| SL_2(\mathbb{F}_3) | = 24$, $D(SL_2(\mathbb{F}_3)) \simeq \mathbb{H}_8$. Pour plus de details (c.f. D.PERRIN, cours d'algèbre).

Théorème : Le groupe $PSL(E)$ est simple si $E \neq \mathbb{F}_2^2$ et $\mathbb{F}_3^2$.

preuve :

E étant un-$\mathbb{K}$.e.v de dimension n. Soit $\overline{N}$ un sous groupe distingué de $PSL(E)$, non réduit à l'élément neutre. Par image réciproque, il lui correspond un sous groupe distingué N de $SL(E)$ contenant le centre $\mathcal{Z}$ de $SL(E)$ et distinct de $\mathcal{Z}$. Il faut montrer que l'on a : $N = SL(E)$.

.1^{er} cas : si $n \geq 3$: comme les transvections engendrent $SL(E)$ et sont toutes conjuguées, il suffit de montrer que l'une d'elles est dans N.

Soit $\sigma \in N$, $\sigma \notin \mathcal{Z}$. Comme σ n'est pas une homothétie ; il existe $a \in E$ tel que $b = \sigma(a)$ ne soit pas colinéaire à a. Soit τ une transvection de droite $< a >$ et posons $\rho = \sigma\tau\sigma^{-1}\tau^{-1}$. Soit H un hyperplan contenant le plan $< a, b >$ (il en existe, puisqu'on a $n \geq 3$) ; on a alors les trois propriétés suivantes :

i) $\rho \in N$ et $\rho \neq id_E$.

ii) $\forall x \in E$, $\rho(x) - x \in H$.

iii) $\rho(H) = H$.

En effet :

.Il est clair que ρ est dans N. Si on avait $\rho = id_E$, on aurait, $\tau = \sigma\tau\sigma^{-1}$, mais ces transvections ont respectivement pour droites $< a >$ et $< b >$ ce qui entraine $< a >=< b >$. (impossible).

.Pour ii), on remarque qu'on a $\rho(x) - x \in < a, b > \subseteq H$.

iii) resulte aussitôt de ii).

Deux eventualités possibles sont alors à envisager.

a-Il existe une transvection u, d'hyperplan H, qui ne commute pas avec ρ. Alors, si on pose : $v = \rho u \rho^{-1} u^{-1}$, on a : $v \in N$, $v \neq id_E$ et v est produit des transvections u^{-1} d'hyperplan H et $\rho u \rho^{-1}$ d'hyperplan $\rho(H) = H$, donc v est une transvection non triviale de N.

b-Sinon, ρ commute avec toutes les transvections d'hyperplan H. Soit $f \in E^*$ une équation de H et u une transvection de vecteur $c \in H$ qui s'écrit : $u(x) = x + f(x)c$ on a : $\rho u = u\rho$, donc, pour tout $x \in E$: $\rho(x) + f(x)\rho(c) = \rho(x) + f(\rho(x))c$. Soit $x \notin H$, comme $\rho(x) - x \in H$, on a : $f(\rho(x)) = f(x) \neq 0$, d'où $\rho(c) = c$; mais ceci vaut pour tout $c \in H$, donc $\rho/H = id_H$ et, comme $det(\rho) = 1$, ρ est déjà une transvection ; donc $N = SL(E)$. Ce qui achève la démonstration du cas $n \geq 3$.

..$2^{ième}$ cas : si $n = 2$.

Deux points essentiels ne subsistent plus :

i) Les transvections ne forment plus une seule classe de conjugaison (sauf si on a : $\mathbb{K}^* = (\mathbb{K}^*)^2$).

ii)L'hypohtèse $n \geq 3$.

Notons que pour $n = 2$, l'existence d'un hyperplan stable par un $g \in SL(E)$ revient à celle d'un vecteur propre non nul, donc d'une valeur propre de g dans $\mathbb{K}$, en particulier, si $\mathbb{K}$ est algébriquement clos, la méthode précédente s'applique sans modification.

Dans la suite de cette démonstration, on suppose que : $| \mathbb{K} | \geq 7$. $(*)$

. On énonce d'abord quelques lemmes utiles.

Lemme 1 : On suppose $| \mathbb{K} | \geq 7$. Soit $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{K})$, avec $c \neq 0$. Alors : Il existe $g \in SL_2(\mathbb{K})$ telle que $g^{-1}s^{-1}gs$ admette une valeur propre $\lambda \in SL_2(\mathbb{K})$, $\lambda \neq 0, 1, -1$.

preuve :
On cherche g sous la forme $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Soit $e_1 = (1,0)$ le premier vecteur de la base. Il suffit de résoudre l'équation :

$$g^{-1}s^{-1}gs(e_1) = \lambda e_1 \qquad ie: \quad gs(e_1) = \lambda sg(e_1)$$

C'est à dire encore :

$$\begin{array}{lccccccc} (1) & \alpha a & + & \beta c & = & \lambda & (\alpha a & + & \gamma b) \\ (2) & \gamma a & + & \delta c & = & \lambda & (\alpha c & + & \gamma d) \end{array}$$

Soit $\lambda \in (\mathbb{K}^*)^2$, $\lambda \neq \pm 1$ (un tel λ existe car $|\mathbb{K}| \geq 7$, donc $|(\mathbb{K}^*)^2| \geq 3$). On prend alors :
$\gamma = 0$, $\delta = \sqrt{\lambda}$, $\alpha = 1/\sqrt{\lambda}$ et (2) est satisfaite. Puis comme $c \neq 0$, on prend : $\beta = \frac{(\lambda-1)a}{c.\sqrt{\lambda}}$, ainsi (1) est verifiée.

Lemme 2 : Si $s \in SL_2(\mathbb{K})$ a une valeur propre $\lambda \in \mathbb{K}^*$ avec $\lambda \neq \pm 1$, alors s est conjuguée dans $SL_2(\mathbb{K})$ de $t = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$.

preuve :
On note d'abord que s et t sont conjuguées dans $SL_2(\mathbb{K})$; En effet : Comme on a $det(s) = 1$, les valeurs propres de s sont λ et $1/\lambda$, donc elles sont distinctes, et s est diagonalisable ; $s = utu^{-1}$ avec $u \in GL_2(\mathbb{K})$. En suite, si on pose $d = det(u)$, $d \in \mathbb{K}^*$ et $v = \begin{pmatrix} 1/d & 0 \\ 0 & 1 \end{pmatrix}$ on voit que v commute avec t et donc $t = v^{-1}tv = v^{-1}u^{-1}suv$ avec $det(uv) = 1$.

Lemme 3 : Soit $\lambda \in \mathbb{K}^*$, $\lambda \neq \pm 1$ et posons : $s = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$. Soit $\mu \in \mathbb{K}$, $\mu \neq 0$ et posons : $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$; Alors, il existe $g \in SL_2(\mathbb{K})$ tel que l'on ait : $g^{-1}s^{-1}gs = t$.

preuve :
On cherche g sous la forme $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ avec $\alpha\delta - \beta\gamma = 1$, verifiant : $gs = sgt$. Or on a : $gs = \begin{pmatrix} \alpha\lambda & \beta/\lambda \\ \gamma\lambda & \delta/\lambda \end{pmatrix}$ et $sgt = \begin{pmatrix} \alpha\lambda & \alpha\lambda\mu + \beta\lambda \\ \gamma/\lambda & \gamma\mu/\lambda + \delta/\lambda \end{pmatrix}$. La relation $\gamma\lambda = \gamma/\lambda$ implique $\gamma = 0$ car $\lambda^2 \neq 1$. Il reste $\beta/\lambda = \alpha\lambda\mu + \beta\lambda$ et $\alpha\delta = 1$. On prend alors : $\alpha = 1/\lambda - \lambda$ (de sorte que α soit non nul) et $\beta = \lambda\mu$.
Retour à la preuve du théorème :
Maitenant, on est capable de prouver le théorème pour $n = 2$. Soit $s \in N$, $s \neq \pm id_E$.
i) Si s a une valeur propre $\lambda \in \mathbb{K}^*$, $\lambda \neq \pm 1$, s est conjuguée dans $SL_2(E)$ de $s' = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}$, (lemme2). On en déduit que s' est dans N ; Alors pour tout $\mu \in \mathbb{K}^*$, il existe $g \in SL_2(E)$ tel que : $t = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = g^{-1}s'^{-1}gs$. (lemme3). On a, donc, $t \in N$ et donc $N = SL_2(\mathbb{K})$, car dans $SL_2(\mathbb{K})$, toute transvection est conjuguée d'une matrice $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, avec $\lambda \in \mathbb{K}^*$.
ii) Si $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, avec $c \neq 0$, comme on a supposer $|\mathbb{K}| \geq 7$, il existe $g \in SL_2(E)$ telle que : $g^{-1}s^{-1}gs$ ait une valeur propre $\lambda \neq \pm 1$ (lemme1). Comme $g^{-1}s^{-1}gs$ est dans N, on est ramené au cas précédent.
iii) Avec les notations de ii) si on a $c = 0$ et si on n'est pas dans le cas i) on a : $s = \begin{pmatrix} \varepsilon & \mu \\ 0 & \varepsilon \end{pmatrix}$ avec $\varepsilon = \pm 1$ et $\mu \neq 0$ (car s n'est pas diagonalisable, donc a une valeur propre ε double).
Soit alors $t = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, on a $t \in SL_2(E)$ et $tst^{-1} = \begin{pmatrix} \varepsilon & 0 \\ -\mu & \varepsilon \end{pmatrix}$, mais alors, comme tst^{-1} est dans N, on est ramené au cas ii). Ce qui achève de prouver le théorème.

Remarque sur (∗) : D.PERRIN dans le (cours d'algèbre) assure que les cas où $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$ sont exceptionnels et que : $PSL_2(\mathbb{F}_4)$ et $PSL_2(\mathbb{F}_5)$ sont tous les deux isomorphes à $\mathfrak{A}_5$, donc ils sont simples, ce qui justifie enfin l'hypothèse $|\mathbb{K}| \geq 7$.

Chapitre III

LE GROUPE ORTHOGONAL

I-Décomposition polaire :

Théorème : Les applications suivantes :

$$\begin{array}{ccccccc} \mathcal{U}(n)\times\mathcal{H}^{++}(n) & \to & GL_n(\mathbb{C}) & ; & (U,H) & \mapsto & UH \\ \mathcal{U}(n)\times\mathcal{H}^{++}(n) & \to & GL_n(\mathbb{C}) & ; & (U,H) & \mapsto & HU \\ O(n)\times\mathcal{S}^{++}(n) & \to & GL_n(\mathbb{C}) & ; & (O,S) & \mapsto & OS \\ O(n)\times\mathcal{S}^{++}(n) & \to & GL_n(\mathbb{C}) & ; & (O,S) & \mapsto & SO \end{array}$$

sont des homéomorphismes.
Avec $\mathcal{H}^{++}(n)$ (resp $\mathcal{S}^{++}(n)$) désigne l'ensemble des matrices hermitiennes (resp. symétriques) définies positives.

preuve :
-Pour le cas complexe.
Soit $M \in GL_n(\mathbb{C})$, on a : $(M^*M)^* = M^*M$. Donc la matrice M^*M est hermitienne, d'autre part pour tout X non nul de $\mathbb{C}^n$: $X^*(M^*M)X = (MX)^*MX = \| MX \|^2 > 0$ ie : la matrice M^*M est hermitienne définie positive.
Donc il existe $U \in \mathcal{U}(n)$ telle que la matrice $U(M^*M)U$ soit diagonale à coefficients diagonaux rèels strictement positifs, $\lambda_1, ..., \lambda_n$ on pose alors :

$$H = U \begin{pmatrix} \sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \sqrt{\lambda_n} \end{pmatrix} U^*$$

on a : $H = H^*$, ie : H est hermitienne. De plus pour tout X non nul de $\mathbb{C}^n$, on a :

$$X^*MX = X^*U \begin{pmatrix} \sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \sqrt{\lambda_n} \end{pmatrix} U^*X = (U^*X)^* \begin{pmatrix} \sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \sqrt{\lambda_n} \end{pmatrix} U^*X > 0$$

ie : H est hermitienne définie positive. On pose $V = MH^{-1}$, alors :

$$V^*V = (MH^{-1})^*(MH^{-1}) = (H^{-1})M^*MH^{-1} = (H^*)^{-1}U \begin{pmatrix} \lambda_1 & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \lambda_n \end{pmatrix} U^*H^{-1}$$

d'où :

$$V^*V = (U^*)^{-1} \begin{pmatrix} 1/\sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & 1/\sqrt{\lambda_n} \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \lambda_n \end{pmatrix} \begin{pmatrix} 1/\sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & 1/\sqrt{\lambda_n} \end{pmatrix} U^{-1}$$

Or $U \in \mathcal{U}(n)$ donc $V^*V = (U^*)^{-1}U^{-1} = I_n$. ie : $V \in \mathcal{U}(n)$. Ainsi on a bien l'existence de la décomposition polaire.
On considère une décomposition polaire quelconque $M = VH$, alors $M^*M = (VH)^*VH = H^*V^*VH$. Or V est unitaire et H est hermitienne donc : $MM^* = H^2$. On note m et h les deux endomorphismes de $\mathbb{C}^n$ dont les matrices dans la base canonique de $\mathbb{C}^n$ sont respectivement M^*M et H.
Si $\mu_1, ..., \mu_k$ sont les valeurs propres de m (qui sont rèelles positives) et $E_{\mu_1}, ..., E_{\mu_k}$ sont les sous espaces associés, alors les E_{μ_i} sont stables par h (puisque m et h commutent). On peut donc considérer $h_i = h/E_{\mu_i}$ pour tout $1 \leq i \leq k$. Comme h_i est hermitien, h_i est diagonalisable et toute valeur propre λ de h_i est réelle positive et verifie $\lambda^2 = \mu_i$ donc $h_i = \sqrt{\mu_i} id_{E_{\mu_i}}$. Ainsi, h est complètement déterminée par m ie : H par M ce qui assure l'unicité de la décomposition.
L'application : $\mathcal{U}(n) \times \mathcal{H}^{++}(n) \to GL_n(\mathbb{C}); (U,H) \mapsto UH$ est continue et est bijictive (d'après ce qui précéde). Étudions la continuité de la réciproque ; Considérons une suite $(M_p)_p$ de $GL_n(\mathbb{C})$ qui converge vers une matrice $M \in GL_n(\mathbb{C})$ on pose : $M = UH$ et $M_p = U_pH_p$ pour tout p. Puisque le groupe $\mathcal{U}(n)$ est compact, (prop1 $\oint II$ chapitreI), la suite $(U_p)_p$ admet une sous suite convergente $(H_{\varphi(p)})_p$ dont on note U_0 la limite, alors la suite $(H_{\varphi(p)})_p$ converge vers une matrice hermitienne positive H_0 et, comme $H_0 = MU_0^{-1}$ est inversible, H_0 est définie positive. L'unicité de la décomposition polaire donne alors $U = U_0$ et $H = H_0$ ce la signifie que la suite $(U_p)_p$ n'admet que U pour valeur d'adhérence et comme $\mathcal{U}(n)$ est compact, $(U_p)_p$ converge vers U ; Il en résulte que $(H_p)_p$ converge vers H. L'application réciproque est donc bien continue.
-Pour le cas réel, le même raisonnement se calque.

Application 1 : $\mathcal{U}(n)$ est un sous groupe compact maximal de $GL_n(\mathbb{C})$.

preuve :
Soit G un sous groupe compact de $GL_n(\mathbb{C})$ tel que $\mathcal{U}(n) \subseteq G$, soit $A \in G$. La décomposition polaire permet d'écrire : $A = UH$ avec U unitaire et H hermitienne définie positive. Puisque $A \in G$ et $U \in \mathcal{U}(n)$ avec $\mathcal{U}(n) \subseteq G$, la matrice $H = AU^*$ est dans G, donc $(H^k)_{k\in\mathbb{Z}}$ est une suite d'éléments de G, et puisque G est compact, cette suite est bornée. Soit λ une valeur propre de H, puisque H est hermitienne, elle est diagonalisable. Le fait que la suite $(H^k)_{k\in\mathbb{Z}}$ soit bornée implique donc $|\lambda| = 1$. Or H est hermitienne définie positive, donc ses valeurs propres sont réelles strictement positives, on obtient $H = I_n$ ie : $A = U \in \mathcal{U}(n)$ donc $G = \mathcal{U}(n)$.

Remarque : Soit $M \in \mathcal{M}_n(\mathbb{C})$. Par densité de $GL_n(\mathbb{C})$ dans $\mathcal{M}(\mathbb{C})$, il existe une suite $(M_p)_p$ dans $GL_n(\mathbb{C})$ qui converge vers M. Pour tout P on écrit $M_p = U_pH_p$ avec U_p unitaire et H_p hermitienne définie positive. Puisque $\mathcal{U}(n)$ est compact, la suite $(U_p)_p$ admet une sous-suite convergente $(U_{\varphi(p)})_p$, dont on note U la limite. Alors la suite $(U^*_{\varphi(p)}M_p)_p$ converge vers la matrice U^*M ie : U^*M est la limite de la suite $(H_{\varphi(p)})_p$ donc $H = U^*M$ est hermitienne positive. On obtient donc bien $M = UH$ avec U unitaire et H hermitienne positive.

Application 2 : Deux matrices unitairement semblables de $\mathcal{M}_n(\mathbb{R})$ sont orthogonalement semblables.

Lemme : Deux matrices réelles A et B semblables sur $\mathbb{C}$ sont semblables sur $\mathbb{R}$.

preuve :
Si $A = PBP^{-1}$, avec $P \in GL_n(C)$; $P = P_1 + iP_2$ alors : $AP_1 = P_1B$, $AP_2 = P_2B$. On en déduit que $A(P_1 + \lambda P_2) = (P_1 + \lambda P_2)B$ pour tout réel λ. Le polynôme à coefficient réels $Q(\lambda) = det(P_1 + \lambda P_2)$ n'est pas nul car $Q(i) \neq 0$ ainsi, pour tout les λ réels (sauf un nombre fini d'entre eux), la matrice $P_1 + \lambda P_2$ est inversible ; un seul aurait suffi.

preuve de l'application2 : On a : $A = UBU^{-1}$ et ${}^{\top}A = U\,{}^{\top}BU^{-1}$. Il en résulte (en adaptant la démonstration du lemme), l'existence d'un élément P de $GL_n(R)$ tel que $A = PBP^{-1}$ et ${}^{\top}A = P\,{}^{\top}BP^{-1}$. Or $P = OS$ d'où $A = OSBS^{-1}O^{-1}$.
Le resultat sera prouvé quand on s'est assuré que B et S commutent, mais $PBP^{-1} = A = {}^{\top}({}^{\top}A) = {}^{\top}P^{-1}B\,{}^{\top}P$. La matrice B commute avec ${}^{\top}PP$, donc si

$$ {}^{\top}PP = O' \begin{pmatrix} \lambda_1 & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \lambda_n \end{pmatrix} O'^{-1} $$

d'après la démonstration du théorème de décomposition polaire

$$ S = O' \begin{pmatrix} \sqrt{\lambda_1} & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & \sqrt{\lambda_n} \end{pmatrix} O'^{-1} $$

soit Q un polynôme tel que $Q(\lambda_i) = \sqrt{\lambda_i}$ (on peut penser aux polynôme de Lagrange). Alors $Q({}^{\top}PP) = S$, donc aussi B commute avec S qui est un polynôme en ${}^{\top}PP$.

II-Quelques aspects géometriques dans $O(n)$:

Lemme : Les formes linéaires sur $\mathcal{M}_n(\mathbb{K})$ sont les applications $\mathcal{M}_n \to \mathbb{K}$, $M \mapsto Tr(AM)$ où $A \in \mathcal{M}_n(\mathbb{K})$.

preuve :
On considère le morphisme $f : \mathcal{M}_n(\mathbb{K}) \to (\mathcal{M}_n(\mathbb{K}))'$, $A \mapsto f_A$ où $f_A(M) = Tr(AM)$.
Il s'agit de montrer que f est un isomorphisme ie : (puisque $dim(\mathcal{M}_n(\mathbb{K})) = dim((\mathcal{M}_n(\mathbb{K}))')$ il suffit de montrer que f est injective. Si $A = (a_{ij})_{1 \leq i,j \leq n}$ est telle que $f_A = 0$ alors, pour tout : $1 \leq i, j \leq n$ on a : $0 = f_A(E_{ij}) = Tr(AE_{ij})$ mais $AE_{ij} = \Sigma_{1 \leq k,l \leq n} a_{kl} E_{kl} E_{ij} = \Sigma_{1 \leq k,l \leq n} a_{kl} \delta_{li} E_{kj} = \Sigma_{k=1}^{n} a_{ki} E_{kj}$.
d'où :

$$ \begin{aligned} 0 &= Tr(AE_{ij}) \\ &= Tr(\Sigma_{k=1}^{n} a_{ki} E_{kj}) \\ &= \Sigma_{k=1}^{n} a_{ki} Tr(E_{kj}) \\ &= \Sigma_{k=1}^{n} a_{ki} \delta_{kj} \\ &= a_{ji} \end{aligned} $$

ie : $A = 0$.

Théorème 1 : L'enveloppe convexe de $O(n)$ dans $\mathcal{M}_n(\mathbb{R})$ est la boule unité.

preuve :
Il est clair que $\mathbb{B}_{\mathcal{M}_n(\mathbb{R})}$ contient l'enveloppe convexe de $O(n)$, on considère donc une matrice $M \in \mathcal{M}_n(\mathbb{R})$ telle que $|||\, M \,|||_2 < 1$.
D'après un corolaire du théorème de Hahn-Banach, pour montrer que M est dans l'enveloppe convexe de $O(n)$, il suffit de montrer que $\varphi(M) \leq sup_{O \in O(n)}(\varphi(O))$, pour toute forme linéaire φ sur $\mathcal{M}_n(\mathbb{R})$. D'après le lemme, cela revient à montrer que $Tr(AM) \leq sup_{O \in O(n)} Tr(AO)$, $\forall A \in \mathcal{M}_n(\mathbb{R})$. On considère une décomposition polaire $A = \Omega S$ de A (ie : Ω est orthogonale et S est symétrique positive) et une base orthogonale $(e_1, ..., e_n)$ de $\mathbb{R}^n$ formée de vecteurs propres de S alors :

$$ sup_{O \in O(n)} Tr(AO) \geq Tr(A\Omega^{-1}) = Tr(\Omega^{-1}A) = Tr(S) = \Sigma_{i=1}^{n} \parallel Se_i \parallel_2 . $$

D'autre part on a :

$$ Tr(AM) = Tr(MA) = \Sigma_{i=1}^{n} \langle MAe_i, e_i \rangle = \Sigma_{i=1}^{n} \langle Ae_i, M^* e_i \rangle $$

d'où d'après l'inégalité de cauchy-schwarz :

$$ Tr(AM) \leq \Sigma_{i=1}^{n} \parallel Ae_i \parallel_2 \parallel M^* e_i \parallel_2 \leq \Sigma_{i=1}^{n} \parallel Ae_i \parallel_2 \parallel M^* \parallel_2 \parallel e_i \parallel_2 $$

mais $|||\ M\ |||_2 \leq 1$ implique $|||\ M^*\ |||_2 \leq 1$ et la base : $(e_1,...,e_n)$ est orthogonale donc

$$Tr(AM) = \leq \Sigma_{i=1}^n \parallel Ae_i \parallel_2 \leq \Sigma_{i=1}^n \parallel \Omega S e_i \parallel_2 = \Sigma_{i=1}^n \parallel Se_i \parallel_2$$

et donc finalement bien $Tr(AM) \leq sup_{O\in O(n)} Tr(AO)$.

Définition : Un élément U de $\mathbb{B}_{\mathcal{M}_n(\mathbb{R})}$ (la boule unité de $\mathbb{B}_{\mathcal{M}_n(\mathbb{R})}$) est dit extrémal si toute écriture du type $U = (V+W)/2$ avec $V,W \in \mathbb{B}_{\mathcal{M}_n(\mathbb{R})}$ implique $U = V = W$.

Théorème 2 : $O(n)$ est l'ensemble des points extrémaux de la boule unité.

preuve :
.Notons tout d'abord que si $|||\ u\ ||| < 1$ alors u n'est pas extrémal, en effet : si $u = 0$ alors $u = \frac{1}{2}(I + (-I))$ et si $u \neq 0$ alors : $u = \frac{1}{|||u|||}u + (2 - \frac{1}{|||u|||})u)$. D'autre part, tout élément, $u \in O(n)$ est extrémal. En effet, écrivons : $u = \frac{1}{2}(v+w)$ alors pour tout $x \in \mathbb{R}^n$, on a : $2u(x) = v(x) + w(x)$ d'où : $4 \parallel x \parallel^2 = \parallel 2u(x) \parallel^2 = \parallel v(x) \parallel^2 + \parallel w(x) \parallel^2 + 2\langle v(x), w(x)\rangle \leq ||| v |||^2 \parallel x \parallel^2 + ||| w |||^2 \parallel x \parallel^2 + ||| v ||| . ||| w ||| \parallel x \parallel^2 \leq 4 \parallel x \parallel^2$. ce qui implique que les inégalités ci-dessus sont en fait des égalités ie : on a $\parallel v(x) \parallel = \parallel x \parallel$, $\parallel w(x) \parallel = \parallel x \parallel$ et $\langle v(x), w(x)\rangle = \parallel v(x) \parallel . \parallel w(x) \parallel$; la dernière égalité implique que $v(x)$ et $w(x)$ sont positivement liés et les deux premières montrent qu'on a en fait $v(x) = w(x)$, d'où $u = v = w$.
-Soit A un élément extrémal de la boule unité, on considère une décomposition polaire $A = SO$, ce qui peut aussi s'écrire : $A = {}^\top \Omega D \Omega O$ où

$$D = \begin{pmatrix} d_1 & 0 & . & . & 0 \\ 0 & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & d_n \end{pmatrix}$$

et $\Omega, O \in O(n)$ et $d_1,...,d_n \geq 0$. d'autre part on a : $|||\ A\ ||| = ||| D ||| = sup_{1\leq i\leq n} d_i$, donc : $0 \leq d_i \leq 1$ pour tout i supposons que l'un des d_i soit non nul, par exemple $d_1 \neq 1$, et posons :

$$D_1 = \begin{pmatrix} 1 & 0 & . & . & 0 \\ 0 & d_2 & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & d_n \end{pmatrix}, \quad et \quad D_2 = \begin{pmatrix} 2d_1 - 1 & 0 & . & . & 0 \\ 0 & d_2 & . & . & . \\ . & . & . & . & . \\ . & . & . & . & 0 \\ 0 & . & . & 0 & d_n \end{pmatrix}$$

puis : $v = {}^\top \Omega D_1 \Omega O$ et $w = {}^\top \Omega D_2 \Omega O$ alors $v \neq w$ $|||\ v\ ||| = ||| D_1 ||| \leq 1$, $|||\ w\ ||| = ||| D_2 ||| \leq 1$ et $A = \frac{1}{2}(v+w)$ ce qui contredit le caractère extrémal de A par conséquent, tous les d_i sont nuls, ie : $A = {}^\top \Omega\Omega O = O \in O(n)$.

Proposition 1 : (une caractérisation géometrique de $SO(n)$ dans $SL_n(\mathbb{R})$)
On a : $d_2(O, SL_n(\mathbb{R})) = inf_{M\in SL_n(\mathbb{R})} |||\ M\ |||_2 = \sqrt{n}$. Et le lieu de $SL_n(\mathbb{R})$ où cette distance est atteinte est exactement $SO(n)$.

preuve :
On considère les applications f et q de $\mathcal{M}_n(\mathbb{R})$ dans $\mathbb{R}$ definies pour $M = (m_{ij})_{ij}$ respectivement par : $f(M) = det(M) - 1$ et $q(M) = \parallel M \parallel_2^2 = \Sigma_{1\leq i,j\leq n} m_{ij}^2 = Tr({}^\top MM)$. Il s'agit de deux fonctions de classe $\mathcal{C}^\infty$ puisque ce sont des fonctions polynômiales en les n^2 variables réelles m_{ij}. De plus, on a : $\frac{\partial q}{\partial m_{ij}}(M) = 2m_{ij}$ pour tout i, j. ie : $\nabla q(M) = 2M$. si M_{ij} désigne le cofacteur de m_{ij} alors $det(M) = \Sigma_{j=1}^n m_{ij} M_{ij}$ mais M_{ij} ne dépend pas de la variable m_{ij} d'où $\frac{\partial f}{\partial m_{ij}}(M) = M_{ij}$ donc $\nabla f(M)$ est la comatrice de M. ie : $\nabla f(M) = com(M)$. On southaite minimiser l'expression $q(M)$ sous la contrainte de $f(M) = 0$. (ce minimum existe bien puisque $SL_n(\mathbb{R})$ est un fermé de $\mathcal{M}_n(\mathbb{R})$). On se rappelle du théorème des extrema-liés : - (si U est un ouvert de $\mathbb{R}^N$ et $u, v : U \to \mathbb{R}^N$ de classe $\mathcal{C}^1$ telles que $V = \{x \in U; \quad v(x) = 0\} \neq \emptyset$ et u/V a un extremum local en $a \in V$ et $\nabla v(a) \neq 0$, alors : il existe $\lambda \in \mathbb{R}$ tel que $\nabla u(a) = \lambda \nabla v(a)$) ainsi, si $inf_{M\in SL_n(\mathbb{R})} \parallel M \parallel_2$ est atteint en $A \in SL_n(\mathbb{R})$ alors il existe

un réel μ tel que $A = \mu com(A)$ or $det(A) = det(com(A)) = 1$ d'où $\mu = 1$ or $A^{-1} = {}^{\top} com(A)$ donc ${}^{\top}AA = I_n$ ie : $A \in O(n)$ d'où $A \in SO(n)$.
Réciproquement, si $A \in SO(n)$, alors on a $q(a) = n$.

Proposition 2 : (distance au groupe orthogonal)
Pour tout $M \in \mathcal{M}_n(\mathbb{R})$ on a : $d(M, O(n)) = \| \sqrt{{}^{\top}MM} - I_n \|_2$.

preuve :
Notons tout d'abord que si S et T sont symétriques positives et si $\langle .,. \rangle$ désigne le produit scalaire euclidien sur $\mathcal{M}_n(\mathbb{R})$ alors $\langle S,T \rangle \geq 0$. Par densité, il suffit de vérifier cela pour T symétrique définie positive, on note $\sqrt{T}$ l'unique racine carrée de T. Alors : $R = \sqrt{T}S\sqrt{T}$ est symétrique positive et on a : $\langle S,T \rangle = Tr(ST) = Tr(\sqrt{T}ST\sqrt{T}^{-1}) = Tr(R) \geq 0$ on considère l'action de $O(n) \times O(n)$ sur $\mathcal{M}_n(\mathbb{R})$ donnée par : $(\Omega_1, \Omega_2) \star M = \Omega_1 M \Omega_2$, on a alors $\| (\Omega_1, \Omega_2) \star M \|_2 = \| M \|_2$ donc tous les points d'une même orbite sont à la même distance de $O(n)$. Soit $M = SO$ une décomposition polaire de M, alors il existe $\Omega \in O(n)$ telle que $S = {}^{\top} \Omega D \Omega$ avec D diagonale à coefficients positifs. Il s'ensuit que D est dans l'orbite de M, or on a : $\| D - I_n \|_2 = \| {}^{\top} \Omega (D - I_n) \Omega \|_2 = \| {}^{\top} \Omega D \Omega - I_n \|_2 = \| S - I_n \|_2 = \| \sqrt{{}^{\top}MM} - I_n \|_2$ donc, il reste à montrer que $\| D - I_n \|_2^2$ est la distance de D à $O(n)$. Soit $U \in O(n)$ et $\delta = \| D - U \|_2^2 - \| D - I_n \|_2^2$; Montrons que : $\delta \geq 0$. En développant, on obtient : $\delta = 2\langle I_n - U, D \rangle = 2\langle I_n - E, D \rangle$ où $E = \frac{1}{2}(U + {}^{\top} U)$. Si $|||\ .\ |||_2$ est la norme sur $\mathcal{M}_n(\mathbb{R})$ induite par la norme $\| \ . \ \|_2$ de $\mathbb{R}^n$, alors $||| U |||_2 = 1$ donc $||| E |||_2$ et il s'en suit que la matrice symétrique $I_n - E$ est positive puisque $\langle (I_n - E)X, X \rangle = \| X \|_2^2 - \langle EX, X \rangle \geq (1 - ||| E |||_2) \| X \|_2^2 \geq 0$ D'après la remarque préliminaire, on a donc : $\delta = 2\langle I_n - E, D \rangle \geq 0$.

III-Centre et générateurs :

Proposition 1 : Soit $F \subseteq E$ un sous espace non isotrope et τ_F la symétrie orthogonale par rapport à F (c-à-d verifiant $E^+(\tau_F) = F$). Soit $u \in O(n)$. Alors $u\tau_F u^{-1}$ est la symétrie par rapport à $u(F)$, ie : $\tau_{u(F)}$. De plus, on a : $E^-(\tau_{u(F)}) = u(E^-(\tau_F))$.

preuve :
τ_F est une involution, il en est de même de $u\tau_F u^{-1}$. On vérifie aussi tôt la formule $E^+(u\tau_F u^{-1}) = u(E^+(\tau_F))$ et de même pour E^-. D'où le résultat.

Théorème 1 : 1) Le centre de $O(n)$ est $\mathcal{Z} = \{I_n, -I_n\}$. En particulier pour $n \geq 2$, $O(n)$ n'est pas commutatif.
2) Pour $n \geq 3$, le centre de $SO(n)$ est $\mathcal{Z} \cap SO(n)$ c-à-d $\{I_n\}$ si n est pair et $\{I_n, -I_n\}$ si n est impair.

preuve :
1) Il est clair que l'on a :$\{I_n, -I_n\} \subseteq \mathcal{Z}$.
Réciproquement, soit $u \in \mathcal{Z}$ et τ_D une réflexion de droite D, on a : $u\tau_D u^{-1} = \tau_D$ puisque u est central, mais aussi $u\tau_D u^{-1} = \tau_{u(D)}$, de sorte qu'on a : $u(D) = D$ autrement dit ; u laisse invariantes toutes les droites de E, donc est une homothétie donc $u = \pm I_n$ car u doit être une isométrie.
Pour $n \geq 2$ on a : $O(n) \neq \{I_n, -I_n\}$; (Il y a par exemple les réflexions orthogonales) donc $O(n)$ n'est pas commutatif.
.Pour $n = 1$, O(n) est réduit à $\{I_n, -I_n\}$.
2) Remarquons que $-I_n \in SO(n)$ si et seulement si n est pair si u est dans le centre $SO(n)$ et si τ_P est un renversement de plan P on a : $u\tau_P u^{-1} = \tau_P = \tau_{u(P)}$ donc $u(P) = P$, pour tout plan P. Mais comme on a supposé $n \geq 3$, toute droite est intersection de deux plans, donc u laisse aussi invariantes toutes les droites de E et u est une homothétie.

Théorème 2 : Le groupe $O(n)$ est engendré par les réflexions orthogonales. Plus précisément, si u est dans $O(n)$, u est produit d'au plus n réflexions.

preuve :

Soit $u \in O(n)$ et $F_u = \{x \in E / u(x) = x\}$, l'espace des points fixes de u, posons $P_u = n - dim(F_u)$.
Nous allons prouver que u est produit d'au plus P_u réflexions, (on convient que I_n est produit de zéro réflexion).
On raisonne par récurrence sur P_u, le cas $P_u = 0$ correspond à $u = I_n$.
Supposons $P_u > 0$ soit $x \in F_u^\top$, $x \neq 0$ et soit $y = u(x)$ on a $y \neq x$ (car x n'est pas dans F_u) et $y \in F_u^\top$, car F_u est stable par u donc $F_u^\top$ l'est aussi. De plus, comme on a : $\| x \| = \| y \|$, on en déduit $\langle x-y / x+y \rangle = 0$, de sorte que $x-y$ soit orthogonal à $x+y$. Soit alors τ la réflexion définie par le vecteur $x-y$ on a $\tau(x-y) = y-x$ et $\tau(x+y) = x+y$, donc $\tau(y) = x$. De plus, comme $x-y$ est dans $F_u^\top$, on a $\tau / F_u = id$ on a donc l'inclusion $F_{\tau u} \supseteq F_u$ et, comme x est dans $F_{\tau u}$ et pas dans F_u, on a : $P_{\tau u} < P_u$.
Par hypothèse de recurrence, on peut écrire : $\tau u = \tau_1 ... \tau_r$ où les τ_i sont des réflexions et $r \leq P_{\tau u}$. Mais alors on a aussi : $u = \tau\tau_1 ... \tau_r$ et $r+1 \leq P_u$, CQFD.

Théorème 3 : Pour $n \geq 3$, $SO(n)$ est engendré par les renversement, précisement, tout élément u de $O(n)$ est produit d'au plus n renversements.

preuve :
1) Supposons $n = 3$; on a $u \neq I_n$, $u = \tau_1\tau_2$ où τ_1, τ_2 sont des réflexions (car : si τ est une réflexion, alors : $det(\tau) = -1$ et donc si $u \in SO(n)$, u est produit d'un nombre pair de réflexions). Mais, comme on a $n = 3$; $-\tau_i = \sigma_i$ est un renversement (comme on le voit aussi tôt sur les matrices) et on a $u = \sigma_1\sigma_2$.
2) Pour $n \geq 3$ quelconque, soit $u \in O(n)$, on a : $u = \tau_1 ... \tau_{2p}$ avec $2p \leq n$, les τ_i étant des réflexions. Il suffit donc de prouver l'existence des renversement σ_1, σ_2 tels que : $\tau_1\tau_2 = \sigma_1\sigma_2$. Posons $u = \tau_1\tau_2$, soient H_1, H_2 les hyperplans de τ_1, τ_2 et soit V un sous-espace de dimension $n-3$ de $H_1 \cap H_2$ (n étant ≥ 3). on a $u/V = id$ et donc $u(V^\top) \subseteq V^\top$. D'après le cas 1) on a : $u/V^\top = \sigma_1\sigma_2$ où σ_1 est un renversement de $V^\top$ et on obtient le résultat en prolongeant les σ_i par l'identité sur V.

IV-Simplicité de SO(3) :

a-Forme matricielle des éléments de O(n) :
.Dans le cas où $n = 2$, un calcul aisé fournit deux types d'éléments, matriciellement, on a :
$u = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ et $v = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ avec : $a, b \in \mathbb{R}$ et $a^2 + b^2 = 1$
.Les matrices du type u forment un groupe, noté $O^+(2)$, il est dit groupe des isométries directes et est isomorphe au groupe $\mathbb{U}$ des nombres complexes de module 1. On retrouve, en particulier, le fait que $O^+(2)$ est commutatif.

b-Angle d'une rotation :
Supposons avoir choisi une orientation de E, (dim$E$=2), c'est -à-dire, une base orthonormée particulière (e_1, e_2) est fixée. Si $(\varepsilon_1, \varepsilon_2)$ est une autre base orthonormée de E, elle sera dite directe, ou positive (resp indirecte ou négative) si l'unique élément $u \in O(n)$ défini par $u(e_i) = \varepsilon_i$ est dans $SO(n)$ (resp, dans $O^-(n)$).

Proposition : L'application $\varphi : (\mathbb{R}, +) \to (\mathbb{U}, \times)$, $t \mapsto e^{it}$ est un homomorhpisme surjectif de groupe, son noyau est $ker(\varphi) = 2\pi\mathbb{Z}$, elle induit un isomorphisme de groupes topologiques entre $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathbb{U}$.

Preuve : (facile)
.En reprenant, la notation du a). Chaque élément de $O^+(2)$ s'écrit sous la forme :

$$R(t) = \begin{pmatrix} cos(t) & -sin(t) \\ sin(t) & cos(t) \end{pmatrix} \qquad avec \qquad t \in \mathbb{R} \qquad et\, on\, a :$$

Définition : l'élément $\bar{t}$, image de t dans $\mathbb{R}/2\pi\mathbb{Z}$, s'appelle l'angle de $R(t)$. Le groupe $\mathbb{R}/2\pi\mathbb{Z}$ est dite le groupe des angles.

c-Structure des éléments de $O(n)$
Chaque élément u de $O(n)$, s'écrit matriciellement dans une base orthonormée adéquate sous la forme : (on

rappelle ici la proposition 2, $\oint II$, chapitre I)

$$\begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & -1 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & -1 & & & & & \\ & & & & & & R_{\theta_1} & & & & \\ & & & & & & & \ddots & & & \\ & & & & & & & & R_{\theta_k} & & \end{pmatrix}, \quad avec \quad R_{\theta_j} = \begin{pmatrix} cos(\theta_j) & sin(\theta_j) \\ -sin(\theta_j) & cos(\theta_j) \end{pmatrix}.$$

d) La simplicité de $SO(3)$:
Théorème : Le groupe $SO(3)$ est simple.

preuve :
Soit N un sous groupe distingé de $SO(3)$ avec $N \neq \{I_3\}$ il s'agit de prouver que N est égal à $SO(3)$.
1) Comme les renversement engendrent $SO(3)$ et sont conjugués, il suffit de prouver que N contienne un renversement.
2) Soit $u \in N$, $u \neq Id$, comme 3 impair, u admet $+1$ pour valeur propre. On est alors dans l'un des cas suivants :
$i)$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (identité), $ii)$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ (renversement), $iii)$ $\begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\theta) & -sin(\theta) \\ 0 & sin(\theta) & cos(\theta) \end{pmatrix}$ avec $\theta \in \mathbb{R}$ et $\theta \notin \pi\mathbb{Z}$.(rotation d'axe $\mathbb{R}e_1$ et d'angle $\overline{\theta}$).
Le cas i) ne peut avoir lieu, car $u \neq Id$, si ii) a lieu c'est fini. Donc u est une rotation d'axe $\mathbb{R}a$, avec $\| a \| = 1$ et d'angle θ, ayant pour matrice dans une base orthonormée convenable :

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\theta) & -sin(\theta) \\ 0 & sin(\theta) & cos(\theta) \end{pmatrix}$$

si $\theta = \pi$, u est un renversement, sinon, comme on a aussi $u^{-1} \in N$, on peut supposer $0 < \theta < \pi$.
Soit P le plan orthogonale à $\mathbb{R}a$ et notons S_2 la sphère unité de E ; $S_2 = \{x \in E / \| x \| = 1\}$ soit x un point de l'équateur de S_2 (ie : sur $P \cap S_2$) et soit $y = u(x)$. On a la figure ci-dessus :

posons $\alpha = \| x - y \|$ un calcul immédiat fournit : $d^2 = 2(1 - cos(\theta))$.

3) On a la proprieté suivante :
$\forall m, 0 \leq m \leq d, \exists x_1, x_2 \in S_2, u(x_1) = x_2$ et $\| x_1 - x_2 \| = m$. Géométriquement, c'est clair. En effet : u transforme S_2 en elle-même et conserve a. Le méridien de x se transforme donc en celui de y, et lorsque x_1 varie sur ce méridien entre x et a, $\| x_1 - u(x_1) \|$ varie entre d et 0. De façon précise on considère les vecteurs : $x + \lambda a$, $\lambda \in \mathbb{R}$. On a : $\| x + \lambda a \| = 1 + \lambda^2$ donc : $x_1 = \frac{x+\lambda a}{\sqrt{1+\lambda^2}} \in S_2$ et $\| u(x_1) - x_1 \| = \frac{d}{\sqrt{1+\lambda^2}}$ il suffit alors de prendre si $m \neq 0$, $\lambda = \frac{1}{m}\sqrt{\lambda^2 - m^2}$.
4) Soit alors m tel que $0 \leq m \leq d$ si y_1, y_2 sont dans S_2 avec $\| y_1 - y_2 \| = m$, il existe $u' \in N$, tel que $u'(y_1) = y_2$, en effet : il existe $S \in SO(n)$ tel que $S(y_1) = x_1$, $S(y_2) = x_2$ (c'est le $3^{ième}$ cas d'égalité des triangles) on pose alors $u' = S^{-1}uS$, on a $u' \in N$, puisque N est distingué et $u'(y_1) = y_2$.
5) On va maintenant prouver que N contient un renversement en obtenant celui-ci comme composé de (petites) rotations au sens de 4). Soit $n \in \mathbb{N}^*$ et ρ_n la rotation d'axe a et d'angle π/n on a $\| x - \rho_n(x) \| = 2(1 - cos(\pi/n))$. Comme $\mathbb{R}$ est archimédien, le rapport π/n tend vers 0 quand n tend vers $+\infty$, et donc pour n assez grand on a : $\| x - \rho_n(x) \| \leq d$. On pose $x_0 = x$, $x_1 = \rho_n(x), ..., x_{i+1} = \rho_n(x_i), ...$ et on a : $x_n = -x$. Comme $\| x_{i+1} - x_i \| = \| x_1 - x_0 \| = \| x - \rho_n(x) \| \leq d$, il existe $u_i \in N$ tel que $u_i(x_i) = x_{i+1}$. (d'après 4). Mais alors, si on pose $v = u_n ... u_1$, on a $v \in N$ et $v(x) = -x$.
Il en resulte que v est un renversement, et le théorème est démontré.

V-Autour des sous-groupes compacts de $GL(E)$:

Proposition : Soit E un espace euclidien de dimension n et H un sous-groupe compact de $GL(E)$. Si K est un convexe compact de E tel que $u(K) \subseteq K$ pour tout $u \in H$, alors, il existe $a \in K$ tel que $u(a) = a$ pour tout $u \in H$.

preuve :
Il s'agit de montrer que $\cap_{u \in H} \{x \in K, u(x) = x\} \neq \emptyset$ donc, puisque K est compact et puisque $\{x \in K, u(x) = x\}$ est fermé pour tout $u \in H$, il s'agit de montrer que si $u_1, ..., u_p \in H$ alors $\cap_{i=1}^{p} \{x \in K, u_i(x) = x\} \neq \emptyset$ on pose $v = \frac{1}{p}(u_1 + ... + u_p)$ alors on a $v(K) \subseteq K$ par convexité et puisque $u_i(K) \subseteq K$ pour tout $1 \leq i \leq p$. Si $x_0 \in K$ est fixé, on note :
$x_k = \frac{1}{k}(x_0 + v(x_0) + ... + v^{k-1}(x_0))$, alors : $v(x_k) = \frac{1}{k}(v(x_0) + v^2(x_0) + ... + v^k(x_0)) = x_k - \frac{1}{k}x_0 + \frac{1}{k}v^k(x_0)$ puisque la suite $(x_k)_k$ est à valeurs dans le compact K, on peut en extraire une sous suite $(x_{\varphi(k)})_k$ qui converge vers un élément $a \in K$. On a alors :

$$\| v(x_{\varphi(k)}) - x_{\varphi(k)} \| = \frac{1}{k} \| x_0 - v^k(x_0) \| \leq \frac{1}{k} diam(K) \to 0, k \mapsto +\infty$$

or $x_{\varphi(k)} \underset{k \mapsto +\infty}{\longrightarrow} a$ et v est continue d'où $v(a) = a$ si $x \in K$ est fixé, alors l'application : $u \in H \to \| u(x) \|$ est continue sur le compact H, donc on peut poser : $\| x \|' = sup_{u \in H} \| u(x) \|$. Les relations $\| \lambda x \|' = | \lambda | \| x \|'$ et $\| x + y \|' \leq \| x \|' + \| y \|'$ sont claires et si $\| x \|' = 0$ alors $u(x) = 0$ (ie : $x \in ker(u)$) pour tout $u \in H$, mais $H \subseteq GL(\mathbb{R}^n)$ donc $x = 0$, ainsi $\| . \|'$ est une norme sur $\mathbb{R}^n$. En plus pour tout $f \in H$ on a :
$\| x \|' = sup_{u \in H} \| u(x) \| = sup_{(u \circ f) \in H} \| u \circ f(x) \| = sup_{u \in H} \| u(f(x)) \| = \| f(x) \|'$. D'autre part, on peut supposer que la norme $\| . \|$ est la norme euclidienne. Si $\| x + y \|' = \| x \|' + \| y \|'$, alors, il existe $u_0 \in H$ tel que $\| x + y \|' = \| u_0(x + y) \| = \| u_0(x) + u_0(y) \|$, (En effet : le sup est atteint en un certain $u_0 \in H$) or : $\| x + y \|'^2 = \| u_0(x) + u_0(y) \|^2 = \| u_0(x) \|^2 + \| u_0(y) \|^2 + 2 \| u_0(x) \| \| u_0(y) \| \leq \| x \|'^2 + \| y \|'^2 + 2 \| u_0(x) \| \| u_0(y) \|$ d'où : $\| u_0(x) \|^2 + \| u_0(y) \|^2 + 2\langle u_0(x), u_0(y) \rangle = \| u_0(x) \|^2 + \| u_0(y) \|^2 + 2 \| u_0(x) \| \| u_0(y) \|$ ie : $\langle u_0(x), u_0(y) \rangle = \| u_0(x) \| \| u_0(y) \|$ donc il existe $\lambda \geq 0$ tel que : $u_0(x) = \lambda u_0(y)$ ou $u_0(y) = \lambda u_0(x)$. En composant par u_0^{-1}, on a : $x = \lambda y$ ou $y = \lambda x$. Puisque $v(a) = a$ on a :

$$\begin{aligned} \| a \|' = \| v(a) \|' &= \frac{1}{p} \| \Sigma_{k=1}^{p-1} u_k(a) + u_p(a) \|' \\ &\leq \frac{1}{p} \| \Sigma_{k=1}^{p-1} u_k(a) \|' + \frac{1}{p} \| u_p(a) \|' \\ &\leq \frac{1}{p} \Sigma_{k=1}^{p} \| u_k(a) \|' = \frac{1}{p} \Sigma_{k=1}^{p} \| a \|' = \| a \|' \end{aligned}$$

d'où $\frac{1}{p} \| \Sigma_{k=1}^{p-1} u_k(a) + u_p(a) \|' = \frac{1}{p} \| \Sigma_{k=1}^{p-1} u_k(a) \|' + \frac{1}{p} \| u_p(a) \|'$ d'après le point précédent, il existe $\lambda_p \geq 0$ tel que $\frac{1}{p}\Sigma_{k=1}^{p-1} u_k(a) = \lambda_p \frac{1}{p} u_p(a)$ ou $\lambda_p \frac{1}{p}\Sigma_{k=1}^{p-1} u_k(a) = \frac{1}{p} u_p(a)$. Le cas où $\lambda_p = 0$, correspond à $a = 0$, donc a est

alors clairement un point fixe commun aux u_i puisque ce sont des isomorphismes.
On peut donc supposer qu'il existe $\lambda_p > 0$ tel que $\frac{1}{p}\Sigma_{k=1}^{p-1} u_k(a) = \lambda_p \frac{1}{p} u_p(a)$ puis (en substituant ci-dessus) : $\frac{\lambda_p+1}{p} \parallel u_p(a) \parallel' = \frac{1}{p} \parallel \lambda_p u_p(a) \parallel' + \frac{1}{p} \parallel u_p(a) \parallel' = \parallel a \parallel'$ or $\parallel u_p(a) \parallel' = \parallel a \parallel'$ donc $\lambda_p = p-1$, d'où $v(a) = \frac{1}{p}\Sigma_{k=1}^{p-1} u_k(a) + \frac{1}{p} u_p(a) = \frac{1}{p}\lambda_p u_p(a) + \frac{1}{p} u_p(a) = u_p(a)$ ce qui a été montré pour l'indice p peut, en effet, être fait pour n'importe quel indice $1 \leq i \leq p$, donc on a : $u_i(a) = v(a) = a$ pour tout $1 \leq i \leq p$. En particulier on a bien : $\cap_{i=1}^{p} \{x \in K, u_i(x) = x\} \neq \emptyset$.

Proposition : Si G est un sous-groupe compact de $GL_n(\mathbb{R})$, alors il existe $P \in GL_n(\mathbb{R})$ avec $PGP^{-1} \subseteq O(n)$.

preuve :
On considère l'application $\rho : G \to GL(Sym_n)$, $A \mapsto \rho_A$ où $\rho_A(S) = {}^{\top}ASA$. (Sym_n étant l'ensemble des matrices symétriques d'ordre n). Cette application est bien définie puisque ${}^{\top}ASA \in Sym_n$ lorsque $S \in Sym_n$ De plus ρ_A est inversible (d'inverse $\rho_{A^{-1}}$). L'application ρ est la composée de l'application $A \mapsto (A,A)$ et de l'application $(A,B) \mapsto (S \mapsto {}^{\top}ASB)$ donc ρ est continue.
.Puisque ρ est continue sur le compact G, le groupe $H = \rho(G)$ est compact. D'autre part ; L'ensemble $\xi = \{{}^{\top}MM; M \in G\}$ est compact donc d'après le théorème de Carathéodory, son enveloppe convexe K est compacte. Les éléments de ξ sont des matrices symétriques définies positives (ceci, puisque ${}^{\top}MM \in Sym_n$; et pour tout $X \in \mathbb{R}^n$ non nul, on a MX non nul et ${}^{\top}X({}^{\top}MM)X = {}^{\top}(MX)MX = \parallel MX \parallel^2 > 0$) or Sym_n^{++} est convexe donc $K \subseteq Sym_n^{++}$. En fin : Si $B \in K$, alors il existe $\alpha \in [0,1]$, ${}^{\top}MM \in \xi$ et ${}^{\top}NN \in \xi$ tels que $B = \alpha {}^{\top}MM + (1-\alpha){}^{\top}NN$. Considérons un élément $u \in H$, on a $u = \rho_A$ pour un certain $A \in G$ d'où :

$$\begin{aligned} u(B) &= \alpha u({}^{\top}MM) + (1-\alpha)u({}^{\top}NN) \\ &= \alpha\rho_A({}^{\top}MM) + (1-\alpha)\rho_A({}^{\top}NN) \\ &= \alpha {}^{\top}A({}^{\top}MM)A + (1-\alpha){}^{\top}A({}^{\top}NN)A \\ &= \alpha {}^{\top}(MA)MA + (1-\alpha){}^{\top}(NA)NA \end{aligned}$$

or $A \in G$ donc $MA, NA \in G$ donc $u(B) \in K$. On a donc montré que H est un sous-groupe compact de $GL(\mathbb{R}^N)$ (où $N = dim(Sym_n^{++})$) et K est un compact convexe de $Sym_n^{++} \simeq \mathbb{R}^N$ qui est stable par tous les éléments de H. D'après la proposition 1, il existe $S \in K$ tel que $u(S) = S$ pour tout $u \in H$ ie : $\rho_A(S) = S$ pour tout $A \in G$.
.En fin, la matrice $S \in K$ est symetrique définie positive,donc il en est de même pour S^{-1}, il s'ensuit que S^{-1} admet une carrée symétrique définie positive ie : il existe une matrice R symétrique définie positive telle que $S = R^2 = {}^{\top}RR$. Pour tout $A \in G$, la relation : ${}^{\top}ASA = S$ s'écrit donc : ${}^{\top}A{}^{\top}RRA = {}^{\top}RR$ ie : ${}^{\top}R^{-1}.{}^{\top}A{}^{\top}RRAR^{-1} = I_n$ d'où ${}^{\top}(RAR^{-1}) = I_n$ ainsi : $RAR^{-1} \in O(n)$.

Chapitre IV

QUELQUES APPLICATIONS

I-Groupes d'isométries :

Proposition 1 : Si G est un sous-groupe fini de $SO(3)$ alors G est isomorphe à l'un des groupes : $\mathbb{Z}/n\mathbb{Z}$, D_n, $\mathfrak{A}_4$, S_4 ou $\mathfrak{A}_5$.

preuve :
-Si g est une rotation non triviale, alors il existe deux points P et $-P$, applés pôles de g, sur la sphère unité qui sont stable par g. On note $\mathcal{P}$ l'ensemble des pôles des éléments de $G \setminus \{I_3\}$.
Puisqu'une rotation est une isométrie, G agit sur la sphère. D'autre part, si $h \in G$ et si P est un pôle de $g \in G$, alors $hgh^{-1}h(P) = hg(P) = h(P)$ ie : $h(P)$ est un pôle de hgh^{-1}. Donc G agit sur l'ensemble $\mathcal{P}$ des pôles. Le nombre k d'orbites de cette action verifie :

$$k = \frac{1}{\mid G \mid}\Sigma_{g\in G} \mid Fix(g) \mid = \frac{1}{n}(\mid \mathcal{P} \mid +2(n-1)).$$

d'où, puisque $2 \leq \mid \mathcal{P} \mid \leq 2(n-1)$ on a : $2 \leq k \leq \frac{4(n-1)}{n} = 4(1-\frac{1}{n}) < 4$ ie : $k = 2$ ou $k = 3$.
Dans le cas où $k = 3$, on note $\mathcal{P}_1, \mathcal{P}_2$ et $\mathcal{P}_3$ les orbites avec $\mid \mathcal{P}_1 \mid \geq \mid \mathcal{P}_2 \mid \geq \mid \mathcal{P}_3 \mid$. Pour $i = 1,2,3$, on note m_i l'ordre du stabilisateur d'un point de $\mathcal{P}_i$ (ce qui ne dépent pas du point choisi) alors : $m_i \mid \mathcal{P}_i \mid = n$ d'où $m_1 \leq m_2 \leq m_3$.
Si P est un point de $\mathcal{P}_1$ alors P est stabilisé par l'identité et par un élément g dont P est un pôle d'où $m_1 \geq 2$.
On a : $3n = \mid \mathcal{P} \mid +2(n-1)$ ie : $\mid \mathcal{P} \mid = n+2$ D'après l'équation aux classes :
$n+2 = \mid \mathcal{P}_1 \mid + \mid \mathcal{P}_2 \mid + \mid \mathcal{P}_3 \mid = \frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3}$, d'où : $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n}$, on en tire que : $1 < \frac{3}{m_1}$ et donc $m_1 = 2$, par suite, $\frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n}$, on a donc : $\frac{1}{2} < \frac{2}{m_2}$, ce qui fournit : $m_2 = 2$ ou $m_2 = 3$, lorsque $m_2 = 3$, on obtient : $\frac{1}{m_3} = \frac{1}{6} + \frac{2}{n}$ ie : $m_3 = 3,4$ ou 5 ; Ainsi on est dans l'un des cas suivants :
. $k = 2$
. $k = 3$ et $m_2 = 2$
. $k = 3$, $m_2 = 3$ et $m_3 = 3$, alors $n = 12$, $\mid \mathcal{P}_1 \mid = 6$, $\mid \mathcal{P}_2 \mid = 4$ et $\mid \mathcal{P}_3 \mid = 4$.
. $k = 3$, $m_2 = 3$ et $m_3 = 4$, alors $n = 24$, $\mid \mathcal{P}_1 \mid = 12$, $\mid \mathcal{P}_2 \mid = 8$ et $\mid \mathcal{P}_3 \mid = 6$.
. $k = 3$, $m_2 = 3$ et $m_3 = 5$, alors $n = 60$, $\mid \mathcal{P}_1 \mid = 30$, $\mid \mathcal{P}_2 \mid = 20$ et $\mid \mathcal{P}_3 \mid = 12$.
1- On considère le cas où il y a $k = 2$ orbites. Alors $\mid \mathcal{P} \mid = 2$ et tous les éléments $g \in G$ distincts de l'identité admettent les deux points P et P' pour pôles ie : ont tous le même axe de rotation donc stabilise tout le plan orthogonal à cet axe.
A toute rotation g de G on associe donc canoniquement une rotation $f(g)$ de ce plan ie : on a un isomorphisme $f : G \to f(G)$. Ainsi $f(G)$ est un sous-groupe d'ordre n du groupe des rotations de $\mathbb{R}^2$, il est donc un groupe cyclique d'ordre n. On a donc : $G \simeq \mathbb{Z}/n\mathbb{Z}$.
2- On considère le cas où il y a $k = 3$ orbites et où $m_1 = m_2 = m_3$. On a alors $\mid \mathcal{P} \mid = n+2$ et $\mid \mathcal{P}_3 \mid = \mid \mathcal{P} \mid - \mid \mathcal{P}_1 \mid - \mid \mathcal{P}_2 \mid = n+2-\frac{n}{2}-\frac{n}{2} = 2$ on note P et $-P$ les deux pôles de $\mathcal{P}_3$. Le stabilisateur G_P de P est d'ordre $\frac{n}{2}$ et (en raisonnant comme dans le premier cas) est cyclique ie : $G_P \simeq \mathbb{Z}/\frac{n}{2}\mathbb{Z} \simeq \mathbb{U}_{\frac{n}{2}}$. Si $g \in G$ ne stabilise pas P alors $gP = -P$ et $g(-P) = P$ donc g est un demi-tour ; En particulier tout $g \in G$ qui ne stabilise pas P est d'ordre 2. On en déduit que $G \simeq \langle a, b / a^n, (ab)^2 \rangle \simeq D_{\frac{n}{2}}$.
3- On considère le cas où il y a $k = 3$ orbites et où $m_2 = 3$ et $m_3 = 3$, alors $n = 12$, $\mid \mathcal{P}_1 \mid = 6$, $\mid \mathcal{P}_2 \mid = 4$ et $\mid \mathcal{P}_3 \mid = 4$. Toute rotation g de G laisse $\mathcal{P}_2$ stable donc induit une permutation $\mathcal{S}_g$ de $\mathcal{P}_2$ ie : on a un morphisme :

$$\begin{array}{rccc} \mathcal{S} : & G & \to & \mathcal{S}_4 \\ & g & \mapsto & \mathcal{S}_g \end{array}$$

Soit $g \in ker(\mathcal{S})$ alors $\mathcal{S}_g$ est l'identité i.e : g stabilise les quatre points de $\mathcal{S}$ ce qui n'est possible que si g est l'identité.Il en résulte que $\mathcal{S}(G)$ est un sous-groupe de $\mathcal{S}_4$ isomorphe à G ie : G est isomorphe à un sous-groupe d'ordre 12 de $\mathcal{S}_4$. Donc $G \simeq \mathfrak{A}_4$.

4- On considère le cas où il y a $k=3$ orbites et où $m_2=3$ et $m_3=4$. Alors : $n=24$, $|\mathcal{P}_1|=12$, $|\mathcal{P}_2|=8$ et $|\mathcal{P}_3|=6$. Les pôles de $\mathcal{P}_1$ et $\mathcal{P}_3$ ne sont pas d'ordre 3 et si un pôle P est d'ordre 3, alors il en est de même pour $(-P)$, on peut donc écrire $\mathcal{P}_2=\{\pm P_1,...,\pm P_4\}$. Toute rotation $g\in G$ non triviale admet, soit l'un des couples $\pm P_i$ pour pôles, soit n'admet pas de pôles dans $\mathcal{P}_2$. Donc G agit par permutation sur les couples $(P_i,-P_i)$ ie : on a un morphisme :

$$\begin{array}{rccc} \mathcal{S}: & G & \to & \mathcal{S}_4 \\ & g & \mapsto & \mathcal{S}_g \end{array}$$

soit $g\in ker(\mathcal{S})$ alors g stabilise chaque couple $\{-P_i,P_i\}$, si on a $gP_i=-P_i$ alors g n'a que deux pôles, donc il existe $k\neq l$ distincts de i tels que $gP_k=-P_k$ et $gP_l=-P_l$ or (O,P_i,P_k,P_l) est un repère cartésien ; En effet si h stabilise P_1, alors il s'agit d'une rotation d'angle $\pm\frac{2\pi}{3}$ qui permute $P_1,...,P_4$. Donc les points P_j pour $j\neq 1$ forment un triangle équilateral, ainsi g échange l'orientation du repère (O,P_i,P_k,P_l). Par conséquent, g n'inverse pas les points de $\mathcal{P}_2$ ie : admet chaque point de $\mathcal{P}_2$ pour point fixe et c'est donc l'identité. Ainsi $\mathcal{S}$ réalise une injection de G dans $\mathcal{S}_4$ ie : $\mathcal{S}(G)$ est un groupe (isomorphe à G) d'ordre 24 qui est un sous-groupe de $\mathcal{S}_4$ donc $G\simeq\mathfrak{A}_4$.
5- Dans le dernier cas, la méthode est analogue (et ce cas est admis).

Remarque :
$\mathfrak{A}_4$ est le groupe du tétraèdre.
$\mathcal{S}_4$ est le groupe du cube et de l'octaèdre.
$\mathfrak{A}_5$ est le groupe de l'icosaèdre et du dodécaèdre.

II-Représentations linéaires :

Définitions 1 : Soit G un groupe et E un $\mathbb{C}$.e.v.
i) Une représentation linéaire de G est un morphisme $\rho: G\to GL(E)$, si $dim(E)=n$, alors n est appelé degré de la représentation.
ii) Un sous-espace F de E est G-invariant si F est stable par tout $\rho(g)$; Si on pose $\rho/F=\rho(g)/F$; alors $\rho/F: G\to GL(F)$ est une sous-représentation.
iii) ρ est irreductible si E et $\{0\}$ sont les seuls sous-espaces G-invariants.
iv) ρ est totalement décompsable si $E=\bigoplus_{i\in I}E_i$ avec, chaque E_i G-invariant et ρ/E_i irreductible.

Théorème : $\rho: G\to GL(V)$ une représentation linéaire de G sur V et soit W un sous-espace vectoriel de V stable par G. Il existe alors un supplémentaire W° de W dans V qui est stable par G.

preuve :
Soit W' un supplémentaire quelconque de W dans V, et soit P le projecteur de V sur W correspondant. Formons la moyenne P° des transformés de P par les éléments de G. $P^\circ=\frac{1}{g}\Sigma_{t\in G}\rho_t P\rho_t^{-1}$, ($g$ étant l'ordre de G) puisque P applique V dans W, d'autre, si $x\in W$, on a $\rho_t^{-1}x\in W$, d'où $P\rho_t^{-1}x=\rho_t^{-1}x$, $\rho_t P\rho_t^{-1}x=x$ et donc $P^\circ x=x$. Ainsi, P° est un projecteur de V sur W, correspondant à un certain supplémentaire W° de W on a en outre : $\rho_s P^\circ=P^\circ\rho_s$ pour tout $s\in G$. En effet, si l'on calcule $\rho_s P^\circ\rho_s$, on trouve :

$$\rho_s P^\circ\rho_s^{-1}=\frac{1}{g}\Sigma_{t\in G}\rho_s\rho_t P\rho_t^{-1}\rho_s^{-1}=\frac{1}{g}\Sigma_{t\in G}\rho_{st}P\rho_{st}^{-1}=P^\circ$$

. Si maintenant $x\in W^\circ$ et $s\in G$, on a $P^\circ(x)=0$, d'où $P^\circ\rho_s(x)=\rho_s P^\circ(x)=0$, c'est-à-dire : $\rho_s x\in W^\circ$, ce qui montre que W° est stable par G, et achève la démonstration.

Lemme de Schur : Si (ρ,E) est irreductible, ses endomorphismes sont exactement les homothéties λid_E, $\lambda\in\mathbb{C}$.

preuve :
. Soit σ un endomorphisme de la représentation ρ, σ commute avec les divers $\rho(g)$, $g\in G$. Si λ est une valeur propre complexe de σ, alors $(\sigma-\lambda id_E)$ est un endomorphisme non injectif de la représentation ρ et par irreductibilité, $\sigma-\lambda id_E=0$.

.. La réciproque est immédiate.

Proposition : Une représentation continue d'un groupe topologique compact est totalement décomposable.

Remarque : Pour établir qu'une représentation finie (ρ, E) est complétement décomposable, il suffit de vérifier que chaque sous-espace invariant admet un supplémentaire invariant.

Exemple : Les représentations de degré 1 d'un groupe fini G sont les morphismes $G \to \mathbb{U}$.

Définition 2 : Soit (ρ, E) une représentation linéaire, si F est un sous-espace vectoriel de E tel que : $\forall g \in G$, $\rho(g)(F) \subseteq F$ on a (changer g en g^{-1}) : $\forall g \in G, \rho(g)(F) = F$. Lorsque la donnée de la représentation est sans ambiguité, on dit qu'un tel F est un sous-espace invariant. Si de plus $F \neq \{0\}$ et $F \neq E$, il est intéressant de considérer la sous représentation (ρ_F, F), et la représentation quotient $(\rho^F, E/F)$ définies par : $\rho_F(g)(x) = \rho(g)(x)$; $\rho^F(g)(x+F) = \rho(g)(x) + F$.

Exemple : Si G est fini et $(e_h)_{h \in G}$ est une base de $E = \mathbb{C}^G$ on pose $\rho(g)(e_h) = e_{gh}$. Alors ρ est appelée représentation régulière de G.

Corollaire : Supposons G abélien, la représentation ρ est irreductible si et seulement si elle est de degré 1.

preuve :
Pour g et h dans G, $\rho(g) \circ \rho(h) = \rho(gh) = \rho(hg) = \rho(h) \circ \rho(g)$. Donc $\rho(g)$ est un endomorphisme de représentation irreductible (ρ, E), c'est une homothétie (lemme de Schur). Comme g est arbitraire, chaque sous-espace de E est invariant et $dim(E) = 1$ par irréductibilité.

III-Utilisation des matrices transvections au changement de base :

On note E_{ij} la matrice de $\mathcal{M}_n(\mathbb{R})$ dont tous les coefficient sont nuls sauf celui à la place (i,j) qui vaut 1 ; Alors, multiplier $A \in \mathcal{M}_n(\mathbb{R})$ par $I + \alpha E_{ij}$.
- à droite permet de remplacer la colonne c_j par $c_j + \alpha c_i$.
- à gauche permet de remplacer la ligne l_i par $l_i + \alpha l_j$
Pour échanger deux lignes k et l, On multiplie à gauche par $(\delta_{i,\tau(j)})_{i,j}$ où τ est la transposition (k, l).

Application 1 : (Théorème des bases adaptées)
Si Λ est un sous-réseau de rang m d'un réseau Γ de $\mathbb{R}^n$, alors il existe $e_1, ..., e_n$ et $d_1, ..., d_n \in \mathbb{N}^*$, avec d_j divise d_{j+1}, pour tout $1 \leq j \leq n-1$ tels que $\Gamma = \mathbb{Z}e_1 \oplus ... \oplus \mathbb{Z}e_n$ et $\Lambda = \mathbb{Z}d_1e_1 \oplus ... \oplus \mathbb{Z}d_me_m$.

preuve :
(cf : [GO],p :33).

Application 2 : (Méthode de Gauss) :
Si $A = (a_{ij})_{1 \leq i,j \leq n}$ telle que $(a_{ij})_{1 \leq i,j \leq k} \in GL_k(\mathbb{R})$ pour tout $1 \leq k \leq n$, alors : $A = LU$, avec : L triangulaire inférieure à coefficients diagonaux égaux à 1 et U triangulaire supérieure.

preuve 1 :
(cf : [DU] : polycopié d'analyse numérique).

preuve 2 :
Dans le but de rendre plus fertile ce thème, nous présentons ici une autre démonstration.
. Si $A = LU$ comme dans l'énoncé, alors U et (comme A) inversible. Donc les coefficients diagonaux de U sont tous non nuls. De plus on contate que :

$\forall k \in \{1,...,n\}$; $(a_{ij})_{1\leq i,j\leq k} = (l_{ij})_{1\leq i,j\leq k} \times (u_{ij})_{1\leq i,j\leq k}$

$$det((a_{ij})_{1\leq i,j\leq k}) = \prod_{j=1}^{k} u_{jj} \neq 0$$

. On raisonne par récurrence. Pour $n = 1$, c'est trivialement vrai.
Soit $n \geq 2$ et supposons le résultat vrai pour $n-1$. Soit $A \in GL_n(\mathbb{R})$ dont tous les mineurs principaux sont non nuls. En appliquant l'hypothèse de recurrence à la matrice $(a_{ij})_{1\leq i,j\leq n-1} = A'$, on peut écrire : $A' = L'U'$ avec L' et U' comme dans l'énoncé ; $L' = (l_{ij})_{1\leq i,j\leq n-1}$, $U' = (u_{ij})_{1\leq i,j\leq n-1}$. On va (compléter) L' et U' pour obtenir les matrices L et U demandées.

$$\begin{pmatrix} a_{1,1} & . & . & . & a_{1,n-1} & a_{1,n} \\ . & & & & . & . \\ . & & & & . & . \\ . & & & & . & . \\ a_{n-1,1} & . & . & . & a_{n-1,n-1} & . \\ a_{n,1} & . & . & . & a_{n,n-1} & a_{n,n} \end{pmatrix} = \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ . & 1 & . & & & . \\ . & & . & . & & . \\ . & & & . & . & . \\ l_{n-1,1} & . & . & . & 1 & 0 \\ \times & \times & \times & \times & \times & 1 \end{pmatrix} \begin{pmatrix} u_{1,1} & . & . & . & . & u_{1,n} \\ 0 & . & & & & . \\ . & . & . & & & . \\ . & & . & . & & . \\ . & & & . & . & . \\ 0 & . & . & . & 0 & u_{n,n} \end{pmatrix}$$

on doit avoir :
$a_{n,1} = l_{n,1}u_{1,1}$ ce qui détermine $l_{n,1}$
$a_{n,2} = l_{n,1}u_{1,2} + l_{n,2}u_{2,2}$ d'où $l_{n,2}$
.
.
.
$a_{n,k} = l_{n,1}u_{1,k} + ... + l_{n,k}u_{k,k}$; $(k \leq n-1)$
ainsi, de proche, en proche, on détermine les $l_{n,k}$ car les $u_{k,k}$ sont $\neq 0$.
On a donc déterminé la dernière ligne de L. Maintenant déterminons U, on doit avoir :
$a_{1,n} = u_{1,n}$
$a_{2,n} = l_{2,1}u_{1,n} + u_{2,n}$
.
.
.
$a_{n,n} = l_{n,1}u_{1,n} + l_{n,2}u_{2,n} + ... + l_{n,n}u_{n,n}$;
De proche en proche on détermine les $u_{j,n}$. Il est alors évident que $A = LU$.
. Prouvons l'unicité :
Si $A = L_1U_1 = L_2U_2$ alors : $L_2^{-1}L_1 = U_2U_1^{-1}$. $L_2^{-1}L_1$ est triangulaire inférieure, tandis que $U_2U_1^{-1}$ est triangulaire supérieure, donc $L_2^{-1}L_1$ est diagonale et comme ses coefficients diagonaux valent 1 on a : $L_2^{-1}L_1 = I_n$ d'où $L_1 = L_2$ et donc $U_1 = U_2$ ce qui prouve l'unicité.

IV-Action du groupe modulaire :

On considère le groupe modulaire $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$, on note $\mathcal{P}$ le demi-plan de Poincaré :

$$\mathcal{P} = \{z \in \mathbb{C} : Imz > 0\}$$

et on pose

$$D = \{z \in \mathbb{C} :| z | \geq 1 et | Rez | \leq \frac{1}{2}\}.$$

1) Définition de l'action :
. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}$ et $z \in \mathcal{P}$, on note :

$$A \star z = \frac{az+b}{cz+d}$$

on a : $Im(A\star z) = Im(\frac{az+b}{cz+d}) = Im(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}) = \frac{ad-bc}{|cz+d|^2}Im(z)$
or $ad-bc=1$ et $Im(z)>0$ donc $Im(A\star z) = \frac{Im(z)}{|cz+d|^2} > 0$
. De plus si $B \in SL_2(\mathbb{Z})$ on a facilement :
$B\star(A\star z) = (BA)\star z$, pour tout $z \in \mathcal{P}$, et comme $I_2 \star z = z$ pour tout $z \in \mathcal{P}$. Donc on vient de bien définir une action de $SL_2(\mathbb{Z})$ sur $\mathcal{P}$.
De plus $\forall z \in \mathcal{P} : A\star z = z \Leftrightarrow cz^2+(d-a)z+b=0$ donc $c=b=0$ et $a=d$ or $det(A) = ad = 1$ donc $A = \pm I_2$.
Il s'ensuit que l'action de $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$ sur $\mathcal{P}$ est fidèle.

2) Transversale d'une action :

On note G le sous-groupe de $SL_2(\mathbb{Z})$ engendré par les matrices : $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et on fait agir G sur $\mathcal{P}$ comme ci-dessus.
Si $z \in \mathcal{P}$ alors $\mid c \mid Im(z) = \mid Im(cz+d) \mid \leq \mid cz+d \mid \leq 1$ donc l'ensemble des couples $(c,d) \in \mathbb{Z}^2$ tels que $\mid cz+d \mid \leq 1$ est fini. Notons O_z l'orbite de z et $I_z = \{Im(u) : u \in O_z\} = \{Im(A\star z) : A \in G\}$.
Mais $Im(A\star z) = \frac{Im(z)}{|cz+d|^2}$ si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donc il n'y a qu'un nombre fini d'éléments $Im(u)$ de I_z vérifiant $Im(u) \geq Im(z)$.
En particulier, il existe $A_1 \in G$ telle que $Im(A_1\star z)$ soit maximal dans I_z.
On note $z_1 = A_1 \star z$ et $n = E(Re(z_1)+\frac{1}{2})$, (partie entière) puisque $T\star u = u+1$ on a :

$$\frac{-1}{2} \leq Re(z_1) - n = Re(z_1 - n) = Re(T^{-n}\star z_1) \leq \frac{1}{2}$$

et

$$Im(T^{-n}\star z_1) = Im(z_1)$$

i.e : $z_2 = T^{-n}\star z_1$ est dans la bande $\mid Re(u) \mid \leq \frac{1}{2}$ et tel que $Im(z_2)$ soit maximal dans I_z. Il s'ensuit que $Im(z_2) \geq Im(S\star z_2) = \frac{Im(z_2)}{|z_2|^2}$ d'où $\mid z_2 \mid \geq 1$.
On a donc montré que toute orbite pour cette action rencontre D.

3) Optimalité du domaine :

Soit $z \in D$ et $A \in SL_2(\mathbb{Z})$ tel que $A\star z \in D$. On commence par considerer le cas où $Im(A\star z) \geq Im(z)$. Alors : si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a $\mid cz+d \mid^2 \leq 1$.
On a : $\mid c \mid Im(z) \leq 1$ donc $\mid c \mid \leq \frac{2}{\sqrt{3}}$ i.e : $c = -1, 0$ ou 1.
i) Si $c=0$, alors $d = det(A) = 1$, d'où (quitte à changer A en $-A$) $a = d = 1$ et $A\star z = z+b$, on a alors trois sous-cas à traiter :
-Si $\mid Rez \mid < \frac{1}{2}$ alors $b=0$ ie : $A = \pm I_2$.
-Si $Rez = -\frac{1}{2}$ alors $b = 0$ ou 1 ie : $A = \pm I_2$ ou T.
-Si $Rez = \frac{1}{2}$ alors $b = 0$ ou -1 ie : $A = \pm I_2$ ou T^{-1}.
ii) Si $c=1$ alors $\mid z+d \mid \leq 1$ donc $d=0$ et $z=j$ ou $d=-1$ et $z = -\frac{1}{j}$. On distingue encore 3 cas :
1) Si $d=0$ alors $b = -detA = -1$ ie : $A\star z = a - \frac{1}{z}$, de plus on a : $\mid z \mid \leq 1$ donc $\mid z \mid = 1$ et $\frac{-1}{z}$ est le symétrique de z par rapport à l'axe des imaginaires purs ; $A\star z$ n'est donc dans D que si $a=0$, ou $z=j$ et $a=-1$, ou $z = \frac{-1}{j}$ et $a=1$.
donc $A = S$ ou $(ST)^2$ ou TS.
2) Si $d=1$ et $z=j$, alors $a-b = detA = 1$ donc $A\star j = \frac{a_j+(a-1)}{j+1} = a+j$ qui n'est dans D que si $a=0$ ou 1, ie : si $A = ST$ ou TST.
3) Si $c=-1$, alors on se ramène au cas précédent en changeant A en $-A$ ce qui ne modifie pas $A\star z$ si $Im(A\star z) < Im(z) = Im(A^{-1}(A\star z))$, alors, puisque z et $A\star z$ sont dans $\mathcal{P}$, on applique le même raisonnement que ci-dessus à A^{-1}.
Il résulte de l'analyse ci-dessus que z et z' de D sont dans la même orbite si et seulement si on est dans l'une des situations suivantes :
. $Re(z) = \frac{-1}{2}$ et $z' = z+1 = T\star z$,

. $Re(z) = \frac{1}{2}$ et $z' = z - 1 = T^{-1} \star z$,
. $|\, z \,| = 1$ et $z' = \frac{-1}{z} = S \star z$.
Donc une transversale pour l'action de G sur $\mathcal{P}$ est le domaine $D_\circ$ défini par les relations suivantes :
$\frac{-1}{2} \leq Re(z) \leq \frac{1}{2}$ et $|\, z \,| > 1$ ou $\frac{-1}{2} \leq Re(z) \leq 0$ et $|\, z \,| = 1$.

4) Conséquences :
On en déduit que les matrices S et T engendrent $SL_2(\mathbb{Z})$. En effet : Soit $A \in SL_2(\mathbb{Z})$ et $z \in$ intérieur à D alors $A \star z$ est sur l'orbite de z donc il existe $B \in G$ tel que $B \star (A \star a) \in D$ ie on a : $BA \star z \in D$. D'après ce qui précède, cela impose que $BA = \pm I_n$ i.e : $A = \pm B^{-1} \in G$.

V-Classification des réseaux :

1) Préliminaire :
On note $L = \{(u_1, u_2) \in \mathbb{C}^{*2}, Im(\frac{u_2}{u_1}) > 0\}$. Un réseau est une partie $\Gamma(u_1, u_2) = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2$ de $\mathbb{C}$ où (u_1, u_2) est une base de $\mathbb{C}$. On note $\mathcal{R}$ l'ensemble des réseaux. On considère l'action de $SL_2(\mathbb{Z})$ sur L par :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .(u_1, u_2) = (au_1 + bu_2, cu_1 + du_2).$$

Le fait qu'il s'agisse bien d'une action vient du fait que

$$A.(u_1, u_2) = (u_1', u_2') \Leftrightarrow A \star \frac{u_1}{u_2} = \frac{u_1'}{u_2'}.$$

Si $\Gamma = \Gamma(u_1, u_2)$ est un réseau alors $\frac{u_1}{u_2} \notin \mathbb{R}$ donc, quitte à changer u_1 en $-u_1$, on peut supposer que $(u_1, u_2) \in L$. Cela signifie que l'application $\varphi : L \to \mathcal{R}$, $(u_1, u_2) \mapsto \Gamma(u_1, u_2)$ est surjective. Par ailleurs, l'application $\psi : L \to \mathcal{P}$, $(u_1, u_2) \mapsto \frac{u_1}{u_2}$ est aussi surjective.

2) Les identifications :
L'ensemble $\mathcal{R}$ des réseaux s'identifie à $L/SL_2(\mathbb{Z})$ i.e. on a :

$$\Gamma(u_1, u_2) = \Gamma(u_1', u_2') \Leftrightarrow \exists A \in SL_2(\mathbb{Z}) / A.(u_1, u_2) = (u_1', u_2').$$

En effet, l'égalité $\Gamma(u_1, u_2) = \Gamma(u_1', u_2')$ signifie que l'on a $u_1' = au_1 + bu_2$ et $u_2' = cu_1 + du_2$ i.e. il existe $A \in \mathcal{M}_2(\mathbb{Z})$ tel que $A.(u_1, u_2) = (u_1', u_2')$. Cette matrice A est en fait la matrice de passage de la $\mathbb{R}$-base (u_1, u_2) à la $\mathbb{R}$-base (u_1', u_2') donc il existe $B \in \mathcal{M}_2(\mathbb{Z})$ telle que $AB = BA = I_n$ ce qui implique $detA = \pm 1$. Enfin, la relation $Im(A \star z) = \frac{detA}{|cz+d|}^2 Imz$ conjuguée au fait que (u_1, u_2) et (u_1', u_2') soient dans L assure que $detA = 1$. La réciproque est claire.
Le groupe $\mathbb{C}^*$ opère naturalement sur L par homothéties et la congruence modulo cette opération est précisément la congruence modulo ψ puisque

$$\frac{u_1}{u_2} = \frac{u_1'}{u_2'} \Leftrightarrow \exists \lambda \in \mathbb{C}^* / (u_1', u_2') = \lambda(u_1, u_2)$$

La surjectivité de ψ permet donc d'identifier $\mathcal{R}$ avec $L/\mathbb{C}^*$.
Le groupe $\mathbb{C}^*$ opère naturellement sur $\mathcal{R}$ par homothéties donc on peut considérer l'application $f : \mathcal{R}/\mathbb{C}^* \to \mathcal{P}/PSL_2(\mathbb{Z})$ qui a $\Gamma(u_1, u_2)$ associe la classe de $\frac{u_1}{u_2}$ modulo $PSL_2(\mathbb{Z})$. Si $\Gamma(u_1, u_2) = \Gamma(u_1', u_2')$ alors il existe $A \in SL_2(\mathbb{Z})$ telle que $A.(u_1, u_2) = (u_1', u_2')$ i.e. $A \star \frac{u_1}{u_2} = \frac{u_1'}{u_2'}$ donc $\frac{u_1}{u_2}$ et $\frac{u_1'}{u_2'}$ sont dans la classe modulo $PSL_2(\mathbb{Z})$. De plus, $\lambda.\Gamma(u_1, u_2) = \Gamma(\lambda u_1, \lambda u_2)$ et $\frac{\lambda u_1}{\lambda u_2} = \frac{u_1}{u_2}$. Donc l'image de la classe d'un réseau par f ne dépend ni du choix du représentant du réseau, ni de la base choisie i.e. f est bien définie. La surjectivité de f est assuré par celle de ψ. Si $\frac{u_1}{u_2}$ et $\frac{u_1'}{u_2'}$ sont dans la même classe modulo $PSL_2(\mathbb{Z})$ alors il existe $A \in SL_2(\mathbb{Z})$ telle que $\pm A.(u_1, u_2) = (u_1', u_2')$ i.e. $\pm A \star \frac{u_1}{u_2} = \frac{u_1'}{u_2'}$ donc $\Gamma(u_1, u_2) = \Gamma(u_1', u_2')$ i.e. f est injective. On a donc $\mathcal{R}/\mathbb{C}^* \sim \mathcal{P}/PSL_2(\mathbb{Z})$.

On a vu que $\mathcal{P}/PSL_2(\mathbb{Z})$ s'identifiait à $\mathcal{D}_\circ$ donc on a aussi $\mathcal{R}/\mathbb{C}^* \sim \mathcal{D}_\circ$.

Annexe

THÉORÈME DE HAHN-BANACH

Théorème : Soit E un espace vectoriel, normé. M un sous-espace de E et A un ouvert convexe non vide de E tel que $M \cap A = .$ Alors il existe un hyper-plan linéaire fermé H de E tel que $M \subseteq H$ et $H \cap A = \emptyset$.

preuve :
Notons $\mathcal{F}$ l'ensemble des sous-espaces N de E qui contiennent M et qui ne rencontrent pas A.
On ordonne $\mathcal{F}$ par inclusion de sorte que se soit un ensemble inductif, alors le lemme de Zorn donne un élément maximal H. On pose alors :
$\Omega = H + \cup_{\lambda>0} \lambda A = \cup_{h\in H}(h + \cup_{\lambda>0}\lambda A)$ qui est un ouvert de E.
• On a $\Omega \cap (-\Omega) = \emptyset$; $((-\Omega) = H + \cup_{\lambda<0}\lambda A)$. En effet : sinon, il existe $x = h_1 + \lambda_1 a_1 = h_2 - \lambda_2 a_2$ avec $h_1, h_2 \in H$ et $\lambda_1, \lambda_2 > 0$, et $a_1, a_2 \in A$ on peut alors écrire :

$$\frac{\lambda_1}{\lambda_1+\lambda_2}a_1 + \frac{\lambda_2}{\lambda_1+\lambda_2}a_2 = \frac{1}{\lambda_1+\lambda_2}(h_1 - h_2) \in H.$$

alors que cet élément appartient à A par convexité ce qui est impossible car $H \cap A = \emptyset$.
• On a : $E = H \cup \Omega \cup (-\Omega)$, en effet : sinon on considère $x \in E \setminus (H \cup \Omega \cup (-\Omega))$, puis on pose $\widetilde{H} = H \oplus \mathbb{R}x$ alors $H \subset \widetilde{H}$ et $\widetilde{H} \neq H$, donc, par maximalité de H, on doit avoir $\widetilde{H} \cap A \neq \emptyset$ ie : il existe $h \in H$ et $\lambda \neq 0$ tels que : $y = h + \lambda x \in \widetilde{H} \cap A$. Mais comme $y \in A$, on a : $x = \frac{-1}{\lambda}h + \frac{1}{\lambda}y \in \Omega \cup (-\Omega)$. Ce qui contredit le choix de x.
• On a : $H \cap (\Omega \cup (-\Omega)) = \emptyset$. En effet : puisque H coupe Ω si et seulement si H coupe $(-\Omega)$, il suffit de montrer que $H \cap \Omega = \emptyset$. On suppose donc qu'il existe $x = h + \lambda a$ dans H, où $h \in H$, $\lambda > 0$ et $a \in A$, alors $a = \frac{1}{\lambda}(x - h) \in A \cap H$ ce qui est impossible.
• Puisque Ω est ouvert et $H = E \setminus (\Omega \cup (-\Omega))$, H est fermé dans E.
• Enfin, H est un hyperplan linéaire. En effet : considérons un élément x non nul dans $\Omega \setminus H$ et posons $\widetilde{H} = H \oplus \mathbb{R}x$. si $\widetilde{H} \neq E$ alors il existe $y \in (-\Omega)$ tel que $y \notin \widetilde{H}$ (on peut prendre y dans Ω puisque $(-\Omega) \subset \widetilde{H}$ implique $\Omega \subset \widetilde{H}$) et on considère alors l'application :

$$f : [0,1] \to E \quad , \quad t \mapsto tx + (1-t)y$$

on a $0 \in f^{-1}(-\Omega)$ et $1 \in f^{-1}(\Omega)$ or $f^{-1}(-\Omega)$ et $f^{-1}(\Omega)$ sont deux ouverts non vides du connexe $[0,1]$ qui sont disjoints puisque $\Omega \cap (-\Omega) = \emptyset$. Il s'ensuit que $f^{-1}(-\Omega) \cup f^{-1}(\Omega)$ inclus strictement dans $[0,1]$. Ainsi, il existe $t \in]0,1[$ tel que $f(t) \in H$ ie :

$$y = \frac{1}{1-t}[f(t) - (-x)] \in H \oplus \mathbb{R}x = \widetilde{H}.$$

Ce qui est impossible par choix de y. On a donc $H \oplus \mathbb{R}x = \widetilde{H} = E$ i.e. H est un hyperplan.

Corollaire 1 : Soit E un $\mathbb{R}$-espace vectoriel normé, F un convexe fermé de E et C un convexe compact de E tel que $F \cap C = \emptyset$. Alors, il existe une forme lineaire continue φ telle que : $sup_{x\in C}\varphi(x) < inf_{y\in F}\varphi(y)$.

preuve :
On pose $G = F - C$, alors G est fermé et ne contient pas 0. En effet, $0 \notin G$ puisque $F \cap C = \emptyset$ et considérons deux suites $(x_n)_n$ et $(y_n)_n$ respectivement dans F et C telles que la suite $(z_n)_n$, où $z_n = x_n - y_n$, converge vers $z \in E$. Puisque C est compact, il existe $\psi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que la suite $(y_{\psi(n)})_n$ converge vers $y \in C$. Notons $x = y + z$ alors :

$$\lim_{n\to+\infty} x_{\psi(n)} = \lim_{n\to+\infty}(y_{\psi(n)} + z_{\psi(n)}) = y + z = x$$

or F est fermé donc $x \in F$ ie : $z = x - y \in F - C = G$ En particulier, il existe $r > 0$ tel que $B(0,r) \cap G = \emptyset$ on pose $A = G + B(0,r) = G - B(0,r)$, alors $0 \notin A$ et il existe une forme linéaire continue $\varphi : E \to \mathbb{R}$ telle que $\varphi(z) > 0$

pour tout $z \in A$. En effet, on a $0 \notin A$ et puisque A est un ouvert convexe, on pose $M = \{0\}$ et on applique le théorème de Hahn-Banach géometrique, donc il existe un hyperplan fermé H tel que $H \cap A = \emptyset$.
En écrivant : $H = ker\varphi$ avec $\varphi : E \to \mathbb{R}$ linéaire, on voit que φ est continue. Comme $ker\varphi \cap A = \emptyset$, on a $0 \notin \varphi(A)$ avec $\varphi(A)$ convexe dans $\mathbb{R}$ donc $\varphi(A)$ est un intervalle et on a donc : Soit $\varphi(A) \subseteq]0, +\infty[$, soit $\varphi(A) \subseteq]-\infty, 0[$; quitte à prendre $-\varphi$ au lieu φ, on a bien $\varphi(z) > 0$ pour tout $z \in A$.
On a alors $m = inf_{x \in G}\varphi(x) > 0$. En effet, supposons que $m = 0$, alors il existe une suite $(x_n)_n$ dans G telle que la suite $(\varphi(x_n))_n$ tende vers 0. Puisque φ est non nulle, il existe $u \in B(0,r)$ tel que $\varphi(u) \neq 0$. On pose $v = -\frac{|\varphi(u)|}{\varphi(u)}.u$, alors on a $\| v \| = \| u \|$ donc $v \in B(0,r)$. Comme $x_n + v \in G + B(0,r) = A$, on a $0 < \varphi(x_n + v) = \varphi(x_n) + \varphi(v) = \varphi(x_n) - | \varphi(u) |$ d'où

$$0 < | \varphi(u) | < \varphi(x_n) \quad \to \quad 0$$
$$n \to 0$$

Ce qui est impossible, on a donc bien $m > 0$.
Considérons maintenant $x \in G$ et $y \in F$, alors $y - x \in G$ d'où $\varphi(y) - \varphi(x) \geq m$ donc $\forall y \in F$, $sup_{x \in C}\varphi(x) < sup_{x \in C}(m + \varphi(x)) \leq m + \varphi(y)$ d'où

$$sup_{x \in C}\varphi(x) \leq m + inf_{y \in F}\varphi(y) < inf_{y \in F}\varphi(y).$$

Corollaire 2 : Soit E un espace vectoriel normé et A une partie compacte de E. Alors, $x \in E$ est adhérent à l'enveloppe convexe de A si et seulement si pour toute $\varphi \in E'$ on a :

$$\varphi(x) \leq sup_{y \in A}\varphi(y).$$

preuve :
On pose $F = \{x\}$ et on note C l'adhérence de l'enveloppe convexe de A, alors F est un convexe fermé et C est un convexe compact (d'après le théorème de Caratheodory). Si $x \notin F$ alors $C \cap F = \emptyset$ avec C convexe compact et F convexe fermé donc le corollaire précédent donne une forme linéaire φ telle que : $sup_{y \in C}\varphi(y) < inf_{y \in F}\varphi(y)$ i.e. $sup_{y \in C}\varphi(y) < \varphi(x)$.
Réciproquement, si $x \in C$ alors il existe $(x_n)_n$ dans l'enveloppe convexe de A tendant vers x, on a donc $\varphi(x_n) \leq sup_{y \in C}\varphi(y)$ pour tout $\varphi \in E'$ et tout n, d'où $\varphi(x) \leq sup_{y \in C}\varphi(y)$ par continuité de φ.

TABLE DES MATIÈRES

RÉFÉRENCES

Livres :

[AL] : M.Alessandri, Thèmes de géometrie. Groupes en situation géometrique. Dunod, 1999 .

[COM] : F.Combes, Algèbre et géometrie. Bréal, 1998 .

[GO] : R.Goblot, Algèbre commutative. Masson,1996 .

[MT] : R.Mneimné et F.Testard, Groupes de lie classiques, Hermann, 1986 .

[PER] : D.Perrin, Cours d'algèbre. Ellipses. 1996 .

[Ro] : J-E.Rombaldi, Thèmes pour l'agrégation de mathématiques. EDP sciences, 1999 .

[SE] : J-P.Serre, Représentations linéaires des groupes finis, Hermann,1998.

[LS_1] : Leichtnam et Schauer. Exercices corrigés de mathématiques, option M'.P'-Tome1-Ellipses .

[Che] : Jacques Chevallet-243 exircices d'algèbre et de géométrie-Vuibert.

Autres :

[DU] :Cours de M^r C.Durand, enseigné en 2^e année de préparation à l'agrégation (2006/2007) .