Quelques propriétés des sous-groupes de GL(n,k)

Mathilde Kammerer et Clément Rau
Sous la direction d'Yves Lazslo

16 juin 1999

Introduction

On appelle groupe linéaire un sous-groupe de $GL(n,k)$ où k désigne un corps commutatif de caractéristique nulle. Le but de cet exposé est de montrer le résultat suivant :

Alternative de Tits : tout groupe linéaire contient soit un sous-groupe résoluble d'indice fini, soit un groupe libre à deux générateurs.

Un outil fondamental pour l'étude des groupes linéaires est la topologie de Zariski : les fermés d'un espace vectoriel de dimension finie n sont les ensembles formés des vecteurs dont les coordonnées dans une base fixée annulent un idéal de $k[X_1,...,X_n]$. On cherchera un mode de construction pratique des groupes libres (lemme du tennis de table), que l'on illustrera par la dynamique de Schottky. On appliquera les résultats trouvés au problème des groupes linéaires : pour cela, il est nécessaire de trouver des éléments ayant au moins une valeur propre de module strictement plus grand que 1. Mais si on a pris par exemple un sous-groupe de $SO(n,\mathbb{R})$, c'est impossible à ce stade. L'astuce consistera à changer de corps de base, et à injecter notre groupe dans un groupe à coefficients p-adiques, de telle sorte que la valeur absolue d'au moins une valeur propre d'un élément de ce groupe soit strictement plus grande que 1...

Dans tout ce qui suit, les corps seront toujours supposés commutatifs et de caractéristique nulle.

1 Topologie de Zariski

Définitions - Notations

Soit k un corps et V un k-espace vectoriel de dimension finie m. Soit W une partie de V.
On note $k[W] = k[X_1,X_2,...,X_m]/I_W$ où les $(X_i)_{i=1..m}$ sont les coordonnées dans une base fixée et I_W est l'idéal des polynômes de $K[X_1,X_2,...X_m]$ s'annulant sur W, de sorte que $k[V]$ s'identifie a $k[X_1,X_2,...,X_m]$.

Pour toute partie E de V on note $I(E)$ l'idéal des polynômes s'annulant sur E,
ie : $I(E) = \{P \in k[V]/\ \forall v \in E\ \ P(v) = 0\}$.

On note aussi $Z(I)$ l'ensemble des zéros communs aux polynômes de I,
ie : $Z(I) = \{v \in V/\ \forall P \in I\ \ P(v) = 0\}$.

Une partie F de V est dite *Zariski fermée* s'il existe un idéal I de $k[V]$ tel que $F = Z(I)$.
Une partie est dite *Zariski ouverte* si son complémentaire dans V est Zariski fermé .

On vérifie que la donnée de cette famille de fermés définit bien une topologie sur V que l'on appelle *topologie de Zariski*

[en effet, une intersection de fermés est un fermé puisque $\bigcap_s Z(I_s) = Z(<\bigcup_s I_s>)$;
et une union finie de fermés est un fermé car $Z(I) \cup Z(J) = Z(I \cap J)$:

- $Z(I) \cup Z(J) \subset Z(I \cap J)$ est clair
-soit $x \in Z(I \cap J)$; si l'on suppose que $\exists (P,Q) \in I \times J$ tel que $P(x) \neq 0$ *et* $Q(x) \neq 0$ alors le polynôme $PQ \in I \cap J$ *et* $(PQ)(x) \neq 0$. Absurde, donc $x \in Z(I \cup J)$] .

L'ensemble $\overline{E}$ défini par $Z(I(E))$ est *l'adhérence de Zariski* de E, c'est le plus petit fermé de Zariski contenant E.
Pour toute partie E de V, on appelle *topologie de Zariski sur* E la topologie induite sur E par la topologie de Zariski de V.
Une partie E est dite *Zariski dense* dans E' si $\overline{E'} = E$.
Une partie E de V est *Zariski connexe* si elle n'est pas réunion disjointe de deux parties Zariski fermées disjointes non vides. On appelle *composantes Zariski connexes* de E les parties Zariski connexes maximales de E.
Toutes ces précisions ne sont ne fait que les définitions usuelles d'adhérence et de connexité, appliquées à la famille d'ouverts que l'on s'est donnée.
Enfin une partie E de V est *irréductible* si elle n'est pas réunion de deux parties Zariski fermées non vides distinctes de E. En particulier une partie irréductible de V est Zariski connexe.
On appelle *composantes irréductibles* de E les parties irréductibles maximales de E (pour l'inclusion).

Exemples :
-le groupe linéaire $GL(V)$ est un ouvert de Zariski dans $End(V)$.
-la réunion de deux droites distinctes de V est une partie Zariski connexe de V, mais elle n'est pas irréductible.

Proposition 1.1 :
(i) une partie E de V n'a qu'un nombre fini de composantes irréductibles ; elles sont fermées, et E est la réunion de ses composantes irréductibles ;
(ii) pour un groupe linéaire, Zariski connexe est équivalent à irréductible.
(iii) soit Γ un sous-groupe de $GL(V)$, et Γ_e la composante irréductible de Γ contenant l'élément neutre ; alors Γ_e est un sous-groupe distingué d'indice fini de Γ .

Démonstration :
-pour (i) on utilise le lemme suivant :

Lemme : V un k-espace vectoriel de dimension finie, E une partie de V.
On munit E de la topologie de Zariski.
Alors tout fermé de E est réunion finie de fermés irréductibles.

Démonstration du lemme :
soit $G = \{F$, *F fermé de E, F n'étant pas réunion finie de fermés de E* $\}$.
- G est inductif, en effet toute chaîne (descendante) admet un plus petit élément :
si $(F_i)_{i \in I}$ est une chaîne descendante, $F_{i_1} \supset F_{i_2}$ si $i_2 > i_1$.
on a les inclusions suivantes entre idéaux de $k[V]$: $I(F_{i_1}) \subset I(F_{i_2})$.
Or k étant un corps, k est noethérien, donc par le théorème de transfert de Hilbert $k[X_1, ..., X_n]$ est noethérien. Donc $k[V]$ est noethérien.
Il existe alors N tel que pour $n > N$ $(I(F_{i_n}))_n$ est stationnaire, et pour $n > N$ $F_{i_n} = Z(I(F_{i_n}))$ est stationnaire : on a donc un plus petit élément.
- d'après le lemme de Zorn, G admet donc un élément minimal, notons-le Y.
- Y n'est pas irréductible par construction, donc on peut écrire $Y = Y_1 \cup Y_2$ avec Y_1 et Y_2 Zariski fermés, non vides, différents de Y. Par minimalité de Y, Y_1 et Y_2 sont réunion finie de fermés irréductibles, mais alors Y aussi, contradiction.
Cela achève la démonstration du lemme.

□

Démonstration de la proposition 1.1 (i) :
E muni de la topologie de Zariski est fermé, donc en particulier E est réunion finie de fermés irréductibles : $E = F_1 \cup ... \cup F_s$.

Soit D une composante irréductible de E.
On a $D = D \cap E = (D \cap F_1) \cup ... \cup (D \cap F_s)$.
Or pour tout i $(D \cap F_i)$ est fermé pour la topologie de Zariski sur D, et donc par irréductibilité de D, il existe i tel que $D \cap F_i = D$. Donc $D \subset F_i$ et par maximalité de la composante irréductible D, on obtient : $D = F_i$.
Donc les composantes irréductibles sont parmi les F_i, qui sont en nombre fini.
Pour tout $x \in E$, il existe une composante irréductible qui contient x, donc E est bien réunion de ses composantes irréductibles.

Montrons maintenant (ii).
On a déjà vu que «irréductible» entraine «Zariski connexe».
Réciproquement : soit Γ un groupe Zariski connexe. Alors Γ est réunion de ses composantes irréductibles $(F_i)_i$, qui sont en nombre fini (cf (i)) : $\Gamma = F_1 \cup ... \cup F_s$ (on suppose dans cette écriture que tous les F_i sont distincts, elle est donc unique à l'ordre des facteurs près) .
Alors $\forall \gamma \in \Gamma \ \ \gamma\Gamma = \Gamma = \gamma F_1 \cup ... \cup \gamma F_s$.
Cela donne une application de Γ dans le groupe symétrique $\mathfrak{S}_s$:

$$\begin{aligned} \phi : \Gamma &\longrightarrow \mathfrak{S}_s \\ \gamma &\mapsto \tilde{\gamma} \end{aligned}$$

où $\tilde{\gamma}$ est défini par : $\gamma F_i = F_{\tilde{\gamma}(i)}$.
Γ étant connexe et ϕ continue (pour la topologie discrète sur $\mathfrak{S}_s$), on déduit que ϕ est constante, et $\phi(\Gamma)$ est l'élément neutre de $\mathfrak{S}_s$.
Soit i fixé. Du fait que $\forall \gamma \in \Gamma \ \gamma F_i = F_i$, on a $F_i = \Gamma$. Or les F_i sont supposés distincts. D'où nécessairement $s = 1$. Donc Γ est irréductible.

Montrons (iii).
Soit $\Gamma_e^{'}$ la composante Zariski connexe contenant l'élément neutre e de Γ.
$\Gamma_e^{'}$ est un sous groupe distingué de Γ, puisque qu'on a :
- $Id \in \Gamma_e^{'}$;
- si $g \in \Gamma_e^{'}$, $g^{-1}\Gamma_e^{'}$ est une composante connexe qui contient Id et donc c'est $\Gamma_e^{'}$, d'où $g^{-1} \in \Gamma_e^{'}$;
- de même, $\Gamma_e^{'}$ est stable par produit de deux éléments, et est distingué dans Γ.
Par (ii) $\Gamma_e^{'}$ est irréductible, soit alors $\Gamma_e^{''}$ une composante irréductible contenant e. $\Gamma_e^{''}$ est donc Zariski connexe, donc $\Gamma_e^{''} = \Gamma_e^{'}$, et «la» composante irréductible Γ_e a bien un sens.
Comme $\Gamma_e^{'} = \Gamma_e$, Γ_e est un sous groupe distingué de Γ.
- Γ_e est d'indice fini dans Γ puisque $\Gamma/\Gamma_e = \{$ *composantes irréductibles de* $\Gamma\}$ qui est fini par (i) .

□

Proposition 1.2 : soit G un groupe Zariski connexe.
(i)Si G est virtuellement nilpotent, alors G est nilpotent.
(ii) $D(G) = [G, G]$ est Zariski connexe.

Démonstration :
-(i) :
Lemme : soit G un groupe connexe.
Alors un sous-groupe non trivial fermé de G ne peut pas être d'indice fini.
Démonstration du lemme :
on suppose qu'il existe un sous-groupe G_1 de G fermé et d'indice fini; alors la projection canonique $\pi : G \longrightarrow G/G_1$ est continue pour la topologie discrète sur G/G_1 . Alors par connexité de G, π est constante, ie : $G = G_1$, ce qui est absurde.
Démonstration de la proposition (i) :
supposons G non nilpotent, et supposons qu'il existe un sous-groupe G_1 de G nilpotent d'indice fini.
G_1 n'est pas fermé (d'après le lemme) ; considérons son adhérence de Zariski $\overline{G_1}$: $G_1 \subset \overline{G_1} \subset G$.
$\overline{G_1}$ est d'indice fini dans G, nilpotent (car G_1 est dense dans $\overline{G_1}$), et fermé dans G , donc d'après le lemme : $\overline{G_1} = G$. Or on a supposé G non nilpotent. Contradiction.

-(ii) :
soit $\gamma = [\gamma_1, \gamma_2]...[\gamma_{2n+1}, \gamma_{2n+2}] \in D(G)$, montrons que e et γ sont dans la même composante Zariski connexe.

Soit $\phi : G^{2n+2} \longrightarrow D(G)$
$(\gamma_1, \gamma_2, ..., \gamma_{2n+1}, \gamma_{2n+2}) \mapsto [\gamma_1, \gamma_2]...[\gamma_{2n+1}, \gamma_{2n+2}]$
e et γ appartiennent à $Im(\phi)$ qui est l'image d'un ensemble Zariski connexe par une application continue (car polynomiale) donc Zariski connexe.
D'où le résultat.

□

2 Torsion dans les groupes linéaires

rappels : Un groupe est dit *sans torsion* si l'élément neutre est le seul élément d'ordre fini.
Un groupe est dit *de torsion* si tous ses éléments sont d'ordre fini.
Soit $K \subset L$ deux corps et soit $(l_1, ..., l_p) \in L^p$. On dit que $(l_1, ..., l_p)$ est algébriquement indépendante sur K si $\forall Q \in K[X_1, ..., X_p]$, $Q(l_1, ..., l_p) = 0 \implies Q = 0$.
On appelle *degré de transcendance* de L sur K le cardinal d'une famille algébriquement indépendante maximale.

Définitions :
un groupe est dit *avoir virtuellement une propriété* s'il existe un sous-groupe d'indice fini qui vérifie cette propriété.
Un élément g de $GL(m, k)$ est dit *unipotent* si 1 est sa seule valeur propre dans une clôture algébrique de k ; on dit qu'il est *virtuellement unipotent* s'il existe $n \geq 1$ tel que g^n est unipotent.

Proposition 2.1 : soit k un corps de caractéristique nulle et m un entier, alors tout sous-groupe Γ de $GL(m, k)$ de type fini contient un sous-groupe d'indice fini Γ' tel que :
$\forall g \in \Gamma'$ (*g virtuellement unipotent* $\Rightarrow$ *g unipotent*) .

Démonstration : on va procéder par étapes en «compliquant» davantage le corps k à chaque fois.

1^{er}*cas* : $k = \mathbb{Q}$

Soit E une partie finie formée des générateurs de Γ et de leurs inverses. Soit s le ppcm de tous les dénominateurs des coefficients qui apparaissent dans les éléments de E.
Soit A l'anneau $A = \mathbb{Z}[1/s]$.
Le groupe Γ est donc inclus dans $\Gamma_0 = GL(m, A)$. Il suffit donc de montrer le résultat pour Γ_0
[en effet, si l'on a trouvé Γ_0' vérifiant la propriété pour Γ_0 alors,
de $\Gamma \hookrightarrow \Gamma_0$
et $\Gamma \cap \Gamma_0' \hookrightarrow \Gamma_0'$
on déduit une application de $\Gamma/\Gamma \cap \Gamma_0' \hookrightarrow \Gamma_0/\Gamma_0'$
$g(\Gamma \cap \Gamma_0') \longmapsto g\Gamma_0'$
et donc $card(\Gamma/\Gamma \cap \Gamma_0') \leq card(\Gamma_0/\Gamma_0') < \infty$ et $\Gamma \cap \Gamma_0'$ vérifie que les seuls éléments virtuellement unipotents sont les éléments unipotents].
Soit p un nombre premier supérieur à $2m$ et à s .
On a une surjection naturelle ϕ de A dans $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Elle induit donc un morphisme de groupe $\tilde{\phi}$ de Γ_0 dans le groupe fini $GL(m, \mathbb{Z}/p\mathbb{Z})$:
$$\tilde{\phi} : \Gamma_0 \longrightarrow GL(m, \mathbb{Z}/p\mathbb{Z})$$
Par conséquent le noyau $\Gamma_0' = Ker(\tilde{\phi})$ de ce morphisme est d'indice fini.

Montrons que les seuls éléments de Γ_0' virtuellement unipotent sont les éléments unipotents.

Soit $g \in \Gamma_0'$ virtuellement unipotent (ie : $\exists n \in \mathbb{N}$ tel que g^n n'a que 1 comme valeur propre).
Alors les valeurs propres de g sont des racines n-ièmes de l'unité.
$\phi \circ Tr = Tr \circ \tilde{\phi}$, donc $Tr(g) \in \phi^{-1}(\overline{m})$.
D'où $Tr(g) \in m + p\mathbb{Z}$.
Par ailleurs $Tr(g)$ est une somme de m racines de l'unité donc $|Tr(g)| \leq m$.
Or $p \geq 2m$, donc $Tr(g) = m$.

Finalement toutes les valeurs propres de g valent 1 et donc g est bien unipotent.

$\underline{2^{eme}cas}$: $k = \mathbb{Q}(X_1, X_2, ..., X_r)$.

C'est la même méthode que dans le premier cas. Il existe $f \in \mathbb{Z}[X] - \{0\}$ tel que $\Gamma \subset \Gamma_0 = GL(m, A)$ où $A = \mathbb{Z}[X_1, ...X_r, 1/f]$.
Soit p un nombre premier assez grand pour que $p \geq 2m$ et $f \neq 0 \ \ mod(p)$.
On peut alors trouver $(a_1, ..., a_r) \in (\overline{\mathbb{F}_p})^r$ tels que $f(a_1, ..., a_r) \neq 0$. On a alors une surjection de A sur le corps fini $A_p = \mathbb{F}_p[a_1, ..., a_r]$ qui envoie X_i sur a_i ; elle induit un morphisme de groupe de Γ_0 dans le groupe fini $GL(m, A_p)$. On prouve comme ci-dessus que le noyau Γ_0' de ce morphisme, d'indice fini dans Γ_0, est sans torsion.

$\underline{3^{eme}cas}$: cas général .

Soit $y_1, ..., y_s$ les coefficients qui interviennent lorsqu'on prend une famille (finie) de générateurs de Γ et de leurs inverses. On a donc $\Gamma \subset GL(m, \mathbb{Q}(y_1, ..., y_s))$. Il suffit donc de prouver le résultat lorsque k est une extension de type fini de $\mathbb{Q}$.
Soit $x_1, ..., x_r$ une famille maximale algébriquement indépendante de k. Le corps $F = \mathbb{Q}(x_1, ..., x_r)$ est un corps de fractions rationnelle et k est une extension finie de degré d de F.
Un espace vectoriel de dimension m sur k est un espace vectoriel de dimension md sur F. On a donc les inclusions suivantes : $\Gamma \subset GL(m, k) \subset GL(md, F)$. Le deuxième cas prouve alors que Γ contient un sous groupe d'indice fini Γ' sans torsion.

□

Théorème 2.2 (Selberg) : soit k un corps de caractéristique nulle et soit $m \in \mathbb{N}$, alors tout sous groupe de type fini de $GL(m, k)$ est *virtuellement sans torsion.*

Démonstration : c'est une conséquence facile de la proposition précédente.
Gardons les mêmes notations. Soit Γ' le sous-groupe d'indice fini obtenu par la proposition 2.1 .
Soit $g \in \Gamma'$. Si l'on suppose que $\exists n \in \mathbb{N}\ g^n = Id$ alors g est *virtuellement unipotent*, donc il est *unipotent* et la seule possibilité est $g = Id$
[en effet par la propriété que vérifie g, on en déduit que g est diagonalisable :
$P(X) = X^n - 1$ *est bien scindé à racines simples car caractéristique(k)= 0*].
Cela prouve que le sous-groupe Γ' donné par la proposition précédente est sans torsion.

□

Corollaire 2.3 : en caractéristique zéro, tout groupe linéaire de type fini et de torsion est fini.

Démonstration : soit G un groupe linéaire, toujours avec les mêmes notations, le sous-groupe de G d'indice fini et sans torsion que nous donne le théorème de *Selberg* est, par les hypothèses, nécessairement réduit à $\{Id\}$. D'où le résultat.

□

Autrement dit, on a :

$$\left.\begin{array}{l} \text{k corps de caracteristique 0} \\ G \text{ sous-groupe de } GL(m,k) \text{ engendré par un nombre fini d'éléments} \\ \text{tout élément de G est d'ordre fini} \end{array}\right\} \Longrightarrow G \text{ est fini.}$$

Définition : on dit qu'un groupe linéaire est *unipotent* si tous ses éléments sont unipotents.

Grâce à la proposition 2.1 et à cette définition on a alors le corollaire suivant :

Corollaire 2.4 : soit k un corps de caractéristique nulle et m un entier. Soit Γ un sous-groupe de type fini de $GL(m, k)$ dont tous les éléments sont virtuellement unipotents.
Alors Γ est virtuellement unipotent.

Théorème 2.5 (Schur) : en caractéristique nulle, tout sous-groupe linéaire Γ de torsion contient un sous-groupe abélien d'indice fini.

La démonstration de ce théorème utilise des méthodes différentes de celles vues jusqu'à présent, basées sur les algèbres de Lie, et ne fait pas partie de notre exposé.
Grâce à ce théorème on démontre le corollaire suivant (que nous avons admis) :

Corollaire 2.6 : soit k un corps et m un entier. Soit Γ un groupe linéaire. Alors :
(i)si tous les sous-groupes de type fini de Γ sont virtuellement résolubles, Γ est virtuellement résoluble ;
(ii)si tous les sous-groupes de type fini de Γ sont résolubles, Γ est résoluble.

3 Sous-groupes libres des groupes linéaires

On commence d'abord par un critère très utile pour caractériser les groupes libres.

Définition : un groupe G est produit *libre* des $(G_j)_{j=1..r}$ si tout élément de G s'écrit de manière unique comme produit d'éléments de $G_j - \{e\}$. On note $G = G_1 * G_2 * ... * G_r$.

Caractérisation : G est libre si et seulement si tout mot de G de la forme $g_1 g_2 ... g_n$ avec les $g_k \in G_{j_k} - \{e\}$ et $j_k \neq j_{k+1}$ on a $g_1 g_2 ... g_n \neq e$.

Lemme 3.1 (Tennis de table) : soit G un groupe qui agit sur un ensemble X, soit $(G_j)_{j\in J}$ des sous-groupes de G qui engendrent G, soit $(X_j)_{j\in J}$ des parties de X et soit $x \in X - \cup_{i\in J} X_i$.
On suppose que $\begin{cases} \forall j \in J \ \forall g \in G_j - \{e\},\ g.x \in X_j \\ \forall j \in J \ \forall g \in G_j - \{e\} \text{ et } \forall j' \in J - \{j\}\ ,\ g.(X_{j'}) \subset X_j \end{cases}$
alors G est produit libre des G_j .

Preuve : supposons $\exists (g_1, g_2, ..., g_n) \in G_{j_1} - \{e\} \times G_{j_2} - \{e\} \times ... \times G_{j_n} - \{e\}$, $g_1 g_2 ... g_n = e$ et $j_k \neq j_{k+1}$. Alors $(g_1 g_2 ... g_n).x = x$. Or $g_n.x \in X_{j_n}$, donc $g_{n-1}.(g_n.x) \in X_{j_{n-1}}$ d'où $g_1.(g_2 g_3 ... g_n.x) \in X_{j_1}$ donc $x \in X_{j_1}$, ce qui contredit le choix de x.

□

Remarque : réciproquement, si G est le produit libre des G_j, on peut trouver un tel ensemble X ainsi qu'une famille X_j et un tel $x \in X$. Il suffit de prendre $X = G$ et de faire agir G sur lui-même par multiplication à gauche, avec $x = e$ et X_j les mots qui commencent par un element de $G_j - \{e\}$.

Grâce à ce lemme, on peut construire des sous-groupes libres du groupe $PSL(2, \mathbb{C})$, que l'on appelle *groupes de Schottky* .

Groupes de Schottky dans $PSL(2, \mathbb{C})$

On considère l'action naturelle de $G = PSL(2, \mathbb{C})$ sur la droite projective $X = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \bigcup \{\infty\}$ (ceci revient donc à faire agir G sur les droites de $\mathbb{C}^2$). L'action est donc donnée par :

$$\begin{array}{ccccc} G & \times & X & \longrightarrow & X \\ \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) & \times & x & \longmapsto & \frac{ax+b}{cx+d} \end{array}$$

On notera $g.x$ l'action de $g \in G$ sur $x \in X$.

Définitions : un point fixe x_γ^+ de γ dans X est dit *attracteur* s'il existe un voisinage U de x_γ^+ tel que pour tout autre voisinage U' de x_γ^+ on ait $\gamma^n(U) \subset U'$ pour n entier assez grand.

L'ensemble $B^+ = \{x \in X \ / \ \lim_{n\to\infty} \gamma^n.x = x_\gamma^+ \}$ est un ouvert de X appelé *bassin d'attraction* de x_γ^+.
Un point fixe x_γ^- de γ dans X est dit *répulseur* s'il est attracteur pour γ^{-1} .
Et on appelle *bassin de répulsion* le bassin d'attraction pour γ^{-1}.
On peut trigonaliser un élément g de $SL(2,\mathbb{C})$, soit λ et $1/\lambda$ ses deux valeurs propres :
-soit elles sont égales, auquel cas $\lambda = \pm 1$;
-soit elles sont différentes alors g est diagonalisable et on peut encore distinguer 2 sous-cas suivant que $|\lambda| = 1$ ou $|\lambda| \neq 1$.
Finalement, il y a trois types d'éléments dans $G - \{e\}$:

-les éléments elliptiques : ils sont de la forme $\{ \pm P\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}P^{-1} , \ P \in SL(2,\mathbb{C}) , \ \theta \in \mathbb{R} \}$.
Un tel élément a deux points fixes dans X.

-les éléments paraboliques : ils sont de la forme $\{ \pm P\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}P^{-1} , \ P \in SL(2,\mathbb{C}) , n \in \mathbb{C}^* \}$.
Un tel élément a un point fixe dans X (sous la forme canonique, c'est ∞).

-les éléments loxodromiques : ils sont de la forme$\{ \pm P\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}P^{-1} , \ P \in SL(2,\mathbb{C}) , \ |\lambda| \neq 1 \}$.
Un tel élément a deux points fixes dans X .
Si par exemple $|\lambda| > 1$, alors le point de $\mathbb{C}$ associé à la droite propre (associé à la valeur propre λ) est attracteur alors que le point de $\mathbb{C}$ associé à la droite propre (associé à la valeur propre λ^{-1}) est répulseur.
Si g est un tel élément, on peut trouver deux disques ouverts D^+ et D^- disjoints tels que $g.(X - \overline{D^-}) = D^+$.

Définition : un *groupe de Schottky* Γ est un sous-groupe de G engendré par t éléments $\gamma_1, ..., \gamma_t$ pour lesquels il existe $2t$ disques ouverts $D_1^+, ..., D_t^+, D_1^-, ..., D_t^-$ disjoints tels que :
pour tout j $\gamma_j.(X - \overline{D_j^-}) = D_j^+$ et $\gamma_j^{-1}.(X - \overline{D_j^+}) = D_j^-$.

Lemme 3.2 : un groupe de Schottky est libre et discret.

Démonstration : posons $X_j = D_j^- \cup D_j^+$ et soit x dans le complémentaire de tous les $\overline{D_j^\pm}$. Le lemme du tennis de table assure alors qu'un groupe de Schottky est produit libre des sous-groupes engendrés par les γ_i.
Pour la discrétude, on considère une suite $(g_n)_n$ d'éléments de $G - \{e\}$ alors la suite $(g_n.x)_n$ prend ses valeurs dans les disques $D_j^\pm$ donc ne peut converger vers x. Donc g_n ne peut converger vers e, ie G est dicret.

□

Lemme 3.3 : soit Γ un groupe qui agit sur un espace métrique compact X. Soit $\gamma_1, ..., \gamma_t$ des éléments de Γ tels que, en notant $E = \{\gamma_1, ..., \gamma_t, \gamma_1^{-1}, ..., \gamma_t^{-1}\}$ on ait :
- tout élément g de E a un point fixe attracteur x_g^+ dans X de bassin d'attraction B_g^+ ;
- les points x_g^+ sont tous distincts ;
- pour tous g , h dans E tels que $g \neq h^{-1}$, x_h^+ est dans B_g^+ ;
Alors il existe $p > 0$ tel que le groupe engendré par $\gamma_1^p, ...\gamma_t^p$ est libre.

Démonstration : on choisit des voisinages compacts disjoints K_g^+ des attracteurs x_g^+, de sorte que pour $g \neq h^{-1}$ on ait $K_h^+ \subset B_g^+$. Soit alors $L_g^+ = \bigcup_{h \neq g^{-1}} K_h^+$.
On peut choisir p tel que, pour tout $g \in E$, $g^p.(L_g^+) \subset K_g^+$.
On applique alors le lemme du tennis de table avec $X_j = K_{\gamma_j} \cup K_{\gamma_j^{-1}}$.

□

4 Éléments proximaux dans $\mathbb{P}(V)$

Soit k un corps (local) [on peut supposer dans un premier temps que k est simplement un corps, voir le paragraphe5 pour la définition exacte] muni d'une valeur absolue notée $|\ |$. Soit V un $k-$espace vectoriel de dimension finie m et $X = \mathbb{P}(V)$ l'espace projectif de V (ie : l'ensemble des droites de V).
On munit V d'une norme $||\ ||$ et on définit une distance d sur X par :

$d(x_1,x_2) = inf\{||v_1 - v_2||\ ,\ \forall i \in \{1,2\}\ v_i \in x_i\ et\ ||v_i|| = 1\}$
X est alors un espace métrique compact.
Soit $g \in End(V)$.
Pour $\lambda > 0$ on note $V_\lambda(g)$ le plus grand sous-espace vectoriel $g-$invariant de V dans lequel toutes les valeurs propres α de g ont pour module λ.
Autrement dit, on a $V_\lambda(g) = \bigoplus_{|\alpha|=\lambda} E_\alpha(g)$ ($E_\alpha(g)$ désigne l'espace caratéristique associé à α) .
Les valeurs propres de g sont dans une extension finie k' de k, on munit alors implicitement cette extension de l'unique valeur absolue qui prolonge celle de k (on admet l'existence et l'unicité de cette valeur absolue ; à titre indicatif, avec les notations du paragraphe 5 on a :
$\forall x' \in k'\ |x'|_{k'} = |det_{k'/k}(m_{x'})|_k^{\frac{1}{d}}$ où d désigne le degré de l'extension k' sur k).
Rangeons alors par ordre décroissant les valeurs absolues de ces valeurs propres, comptées avec leur ordre de multiplicité : $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_m$.
L'espace vectoriel V se décompose alors en une somme directe de sous-espaces $g-$invariant V_λ .
On pose $V_g^+ = V_{\lambda_1}$, $m_g = dim(V_g^+)$, et $V_g^< = \bigoplus_{\lambda \neq \lambda_1} V_\lambda$.

Définition : on dit que g est ***proximal dans*** $\mathbb{P}(V)$ si $m_g = 1$.

Remarque : un projecteur est proximal si et seulement si il est de rang 1.

Lemme 4.1 : soit k un corps (local), et V un $k-$espace vectoriel de dimension m.
Alors un élément g de $GL(V)$ est proximal dans $\mathbb{P}(V)$ si et seulement si son action sur $\mathbb{P}(V)$ a un seul point fixe attracteur x_g^+.
Ce point fixe x_g^+ est la droite V_g^+ et son bassin d'attraction B_g^+ est le complémentaire de l'hyperplan $X_g^< = \mathbb{P}(V_g^<)$.

Démonstration : c'est presque clair...
Si l'on suppose g proximal, alors, en notant x_g^+ la droite de $\mathbb{P}(V)$ associé à V_g^+, x_g^+ est attracteur puisque $\lambda_2^n = o(\lambda_1^n)$ si $\lambda_1 > \lambda_2$.
Réciproquement, si l'action de g sur $\mathbb{P}(V)$ possède un seul point fixe attracteur, alors $dim(V_g^+) = 1$ (sinon on aurait au moins 2 points fixes attracteurs).

□

Lemme 4.2 : soit k un corps local, V un k-espace vectoriel de dimension m, g un élément de $End(V)$ et $p \geq 1$.
L'ensemble $E_p := \{g \in End(V)\ ,\ \ m_g \leq p\}$ est un ouvert de $End(V)$.
En particulier, l'ensemble des éléments proximaux dans $\mathbb{P}(V)$ est ouvert.

Démonstration : le polynôme caractéristique de g dépend continûment de g, les réels $\lambda_i(g)$ aussi, donc l'ensemble $\{g,\ \lambda_1(g) > \lambda_{p+1}(g)\}$, qui est égal à E_p, est ouvert.

□

Lemme 4.3 : soit k un corps, V un k-espace vectoriel de dimension m , et g un élément de $End(V)$ et $p \geq 1$. Alors
(i) si $p = m_g$, $\bigwedge^p g$ est proximal dans $\mathbb{P}(\bigwedge^p V)$;
(ii) si $\bigwedge^p g$ est proximal dans $\mathbb{P}(\bigwedge^p V)$, alors on a $p \geq m_g$.

Démonstration : les modules des valeurs propres de $\bigwedge^p g$ sont les réels :
$\mu_A = \prod_{i \in A} \lambda_i$ où A est une partie à p éléments de $\{1,...,m\}$.
Le réel μ_A est maximal lorsque $A = \{1,...,p\}$. Aucune autre partie A' n'atteint cette valeur si et seulement si $\lambda_p > \lambda_{p+1}$. C'est le cas pour $p = m_g$, mais jamais pour $p < m_g$.

□

Lemme 4.4 : soit k un corps local et V un k-espace vectoriel de dimension m . Soit g un élément de $End(V)$. Alors

$$g \text{ est proximal dans } \mathbb{P}(V) \iff \begin{cases} \text{il existe des constantes } c_n \in k \text{ telles que la suite} \\ (c_n g^n)_n \text{ converge vers un projecteur } \pi \text{ de rang 1.} \end{cases}$$

Démonstration : si g est proximal dans $\mathbb{P}(V)$, la suite $c_n = \lambda_1^{-n}$ convient .

Réciproquement, par le lemme 5.2 et du fait qu'un projecteur de rang 1 est proximal, on déduit qu'à partir d'un certain rang $c_n g^n$ est proximal. Et donc g est proximal.

□

Lemme 4.5 : soit k un corps local, V un k-espace vectoriel de dimension $m \geq 2$, Γ un sous-groupe Zariski connexe de $GL(V)$ qui contient un élément proximal dans $\mathbb{P}(V)$.
On suppose que V est irréductible (au sens des représentations de groupe). Alors
(a)il existe un élément γ de Γ tel que γ et γ^{-1} sont proximaux dans $\mathbb{P}(V)$;
(b) Γ contient un sous-groupe libre à deux générateurs.

Démonstration :
(a) soit g un élément de Γ qui est proximal dans $\mathbb{P}(V)$.
Par le lemme 4.4 , il existe une suite $(c_n)_{n\in\mathbf{N}} \in k^{\mathbf{N}}$ telle que la suite $(c_n g^n)_n$ converge vers un projecteur π de rang 1 .
On peut multiplier chaque élément de la suite $(g^{-n})_n$ par une constante d_n de sorte que cette suite soit bornée. Puis par compacité de $\mathbb{P}(V)$ on en extrait une suite convergente de limite non nulle, ie : il existe une suite d'entiers S, une suite $(d_n)_{n\in\mathbf{N}} \in k^{\mathbf{N}}$ et un élément σ de $\mathbb{P}(V)$ (donc non nul) tels que $lim_{n\in S} d_n g^{-n} = \sigma$.
Remarquons que l'on a $\sigma\pi = 0$ (c'est un élément proportionnel à l'identité et de rang plus petit que 1 dans un espace de dimension supérieure à 2).
Par irréductibilité de V et Zariski connexité de Γ, on peut trouver un élément $h \in \Gamma$ tel que $\begin{cases} h(Im(\pi)) \not\subset Ker(\sigma) \\ \text{et} \\ h(Im(\sigma)) \not\subset Ker(\pi) \end{cases}$

[en effet, soit $F_1 = \{h \in \Gamma \ , \ \sigma h\pi = 0\}$ et $F_2 = \{h \in \Gamma \ , \ \pi h\sigma = 0\}$.
Raisonnons par l'absurde : supposons $\Gamma = F_1 \cup F_2$.
(i) F_1 et F_2 sont non vides car $\sigma\pi = 0$ donc $Id \in F_1 \cap F_2$.
(ii)F_1 et F_2 sont Zariski fermés.
(iii) F_1 et F_2 sont distincts de Γ
(si par exemple $\Gamma = F_1$, on a $\forall h \in \Gamma \ h(Im(\pi)) \subset Ker(\sigma)$;
soit alors V_1 l'espace vectoriel engendré par les $h(Im(\pi))$ lorsque $h \in \Gamma$. V_1 est Γ stable :

$$V_1 = Vect\{h(Im(\pi)) \ , \ h \in \Gamma\}.$$

-$V_1 \neq \{0\}$ car $Id \in \Gamma$ et π non nul.
-$V_1 \subset Ker(\sigma) \neq V$ car σ non nul .
Donc V_1 est non trivial et distinct de V, dans V irréductible sous Γ. Contradiction.)

Or Γ est Zariski connexe donc irréductible (proposition 1.1) et donc (i),(ii)et(iii) ne sont pas possibles, d'où $\Gamma \neq F_1 \cup F_2$.
Donc il existe h ayant les propriétés souhaitées.]
Soit alors $g_n = g^n h g^{-n} h^{-1} \in \Gamma$ et soit $u = lim_{n\in S} c_n d_n g_n = \pi h\sigma h^{-1}$, u est de rang exactement 1 et verifie (avec les conditions supplémentaires ci dessous) $Im(u) \not\subset Ker(u)$, donc n'est pas nilpotent et est donc proximal.
Donc en appliquant le lemme 5.2, à partir d'un certain rang g_n est proximal dans $\mathbb{P}(V)$. Donc pour n assez grand $\gamma = g_n$ est proximal dans $\mathbb{P}(V)$.
Le même raisonnement s'applique a γ^{-1} si on a choisi h vérifiant les deux conditions supplémentaires
$\begin{cases} h^{-1}(Im(\pi)) \not\subset Ker(\sigma) \\ h^{-1}(Im(\sigma)) \not\subset Ker(\pi) \end{cases}$

(b) Soit γ proximal dans $\mathbb{P}(V)$ ainsi que son inverse (cf (a)). Par le même type d'arguments on peut trouver $h \in \Gamma$ vérifiant les quatre conditions $\forall \delta \ , \delta' \in \{\gamma \ , \ \gamma^{-1}\} \ \ h(V_\delta^+) \not\subset V_{\delta'}^<$. On peut alors appliquer le lemme 3.3 à $\gamma_1 = \gamma$ et $\gamma_2 = h\gamma h^{-1}$.

□

5 Alternative de Tits

Comme on l'a déjà dit, on va changer de corps de base de façon à ce que l'une au moins des valeurs absolues des valeurs propres soit strictement supérieure à 1 .

On rappelle qu'une ***valeur absolue*** $|.|$ sur un corps K est une application de K dans $\mathbb{R}_+$ qui vérifie :
(i)$\forall (a,b) \in K^2,\ |ab| = |a||b|$
(ii)$\forall (a,b) \in K^2,\ |a+b| \leq |a| + |b|$
(iii)$\forall a \in K\ |a| = 0 \ \Leftrightarrow\ a = 0$.

Lorsque (ii) est remplacé par $\forall (a,b) \in K^2, |a+b| \leq\ max(|a|,|b|)$ on parle de valeur absolue ***ultra-métrique.***

Soit p un nombre premier . Soit $|.|_p$ la valeur absolue donnée par :
$|p^n \frac{a}{b}|_p = p^{-n}$ avec a, b premiers à p .
On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour $|.|_p$, et $\mathbb{Q}_\infty = \mathbb{R}$ le complété de $\mathbb{Q}$ pour la valeur absolue habituelle $|.|_\infty$.

Définition : en caractéristique 0, un ***corps local*** est une extension finie de $\mathbb{Q}_p$ (p premier) ou de $\mathbb{Q}_\infty$.
On notera K_v un tel corps .
Un corps local est donc un espace vectoriel de dimension finie sur $\mathbb{Q}_p$ ou sur $\mathbb{Q}_\infty$.

Définition : soit K un corps de nombre (ie : une extension finie de $\mathbb{Q}$). On appelle ***place de*** K une injection de K à image dense dans un corps local K_v (à isomorphisme près).
On a $\quad \mathbb{Q} \hookrightarrow K \hookrightarrow K_v$.
Une place est donc la donnée sur K d'une valeur absolue qui prolonge l'une des valeurs absolues $|.|_p$ (p premier) ou $|.|_\infty$.
La place est dite ***finie*** ou ***infinie*** selon que K_v contient $\mathbb{Q}_p$ ou $\mathbb{Q}_\infty$.

Décrivons les places d'un corps de nombre.

a-Places finies : soit $n = K : \mathbb{Q}$ le degré de K sur $\mathbb{Q}$.
Soit A' l'anneau des entiers de K (ie : $A' = \{x \in K,\ \exists P \in \mathbb{Z}[X]\ unitaire,\ P(x) = 0\ \}$).
On peut montrer que A' est un anneau de Dedekind (voir [Sam]), c'est-à-dire qu'il est noethérien, intégralement clos et que tout idéal premier non nul est maximal.
Soit I le groupe des ***idéaux fractionnaires*** : ce sont des A'-sous modules de K de type fini sur K. On peut définir un produit de deux idéaux fractionnaires α *et* β par : $\alpha\beta = \{\sum a_i b_i,\ a_i \in \alpha\ et\ b_i \in \beta\}$.
On a alors le théorème suivant :
Théoreme 5.1 : A' anneau de Dedekind, Γ l'ensemble des idéaux premiers non nuls de A'.
Tout idéal fractionnnaire non nul β, s'ecrit de manière unique comme $\beta = \prod_{P \in \Gamma} P^{n_P(\beta)}$
où $(n_P(\beta))_\beta$ est une famille presque nulle d'entiers relatifs.

On obtient alors la flèche suivante de l'ensemble Γ des idéaux premiers non nuls de A' dans l'ensemble des places finies de K :

$$\Gamma \longrightarrow \{places\ finies\ de\ K\}$$
$$P \longmapsto \begin{cases} |y|_P = q^{-n_P(A'y)} \\ K \hookrightarrow K_v = \overline{K}^{|.|_P} \end{cases}$$

où q est un réel positif : si $p = min\{k\ premier,\ |k|_P < 1\}$ alors $q = p^{\frac{1}{n_P(A'p)}}$.
En fait, c'est une bijection.

b-Places infinies : K est une extension finie de $\mathbb{Q}$ donc, par le théoreme de l'élément primitif, il existe $x \in K$ tel que $K = \mathbb{Q}[x]$.
x est algébrique sur $\mathbb{Q}$, soit alors Π son polynôme minimal unitaire et n son degré .
Soit $x_1, ..., x_{r_1}$ les racines réelles de Π
et $x_{r_1+1}, ..., x_{r_1+r_2}, x_{r_1+r_2+1}, ..., x_{r_1+2r_2}$ ses racines non réelles de telle sorte que $\begin{cases} x_{r_2+j} = \overline{x_j} & r_1 < j \leq r_1 + r_2 \\ et\ \ n = r_1 + 2r_2 \end{cases}$

Soit alors $\sigma_i : K \hookrightarrow \mathbb{R}$ *pour* $1 \leq i \leq r_1$.
$Q(x) \longmapsto Q(x_i)$
On verifie que ceci définit bien une application.
Soit
$\sigma_i : K \hookrightarrow \mathbb{C}$ *pour* $r_1 + 1 \leq i \leq r_1 + 2r_2$

$Q(x) \longmapsto Q(x_i)$

On a $\sigma_i = \overline{\sigma_{r_1+i}}$ *pour* $r_1 \leq i \leq r_1 + r_2$.
Soit $\sigma = (\sigma_1, ..., \sigma_{r_1}, \sigma_{r_1+1}, ..., \sigma_{r_1+r_2})$
$\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$
$Q(x) \longmapsto (Q(x_1), ..., Q(x_{r_1+r_2}))$

C'est une injection car si $\sigma(Q(x)) = 0$ alors Q appartient à l'idéal engendré par Π donc $Q(x) = 0$.

Proposition 5.2 : A' est un $\mathbb{Z}$-module libre de rang n.

Avant de donner la démonstration, commençons par deux remarques générales sur les modules.
Remarque 1 :
soit B un anneau et A un sous anneau de B tel que B soit un A-module libre de rang fini n.
Pour $x \in B$, on note m_x l'endomorphisme du A-module B représentant la multiplication par x :
$m_x : B \longrightarrow B$
$y \longmapsto xy$

Définition : on appelle *trace de x relativement à B et A* et on note $Tr_{A/B}(x)$ la trace de l'endomorphisme m_x : $Tr_{A/B}(x) = Tr(m_x) \in A$.

On a évidemment $\begin{cases} Tr_{A/B}(x + x') = Tr_{A/B}(x) + Tr_{A/B}(x') \\ \forall a \in A \;\; Tr_{A/B}(ax) = aTr_{A/B}(x) \end{cases}$

Lemme 5.a : soit K un corps de caractéristique nulle, et L une extension algébrique de K de degré n.
Soit $x \in L$, et $x_1, ..., x_n$ les racines du polynôme minimal de x sur K (chacune répétées $[L : K[x]]$ fois).
Alors $Tr_{L/K}(x) = x_1 + ... + x_n$.

Démonstration :
1^{er} *cas* : x est un élément primitif de L sur K (ie : $L = K[x]$) .

Soit Π le polynôme minimal de x sur K. Son degré est n, et on a
$\frac{K[x]}{(\Pi)} \simeq L$ (isomophisme d'espace vectoriel) ; $(1, x, ..., x^{n-1})$ est une base de L sur K.
Posons $\Pi(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$.
La matrice de m_x dans cette base de L sur K est :

$$\begin{pmatrix} 0 & 0 & & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & . & & & . \\ . & & . & & . \\ . & & & . & . \\ 0 & & & 1 & -a_{n-1} \end{pmatrix}$$

d'où $Tr_{L/K}(x) = -a_{n-1} = x_1 + x_2 + ... + x_n$.

2^{eme} *cas* : cas général.

Soit $r = [L : K[x]]$, $(y_1, ..., y_q)$ une base de $K[x]$ sur K,
$(z_1, ..., z_r)$ une base de L sur$K[x]$.
Alors $(y_i z_j)_{(i,j)}$ est une base de L sur K, et $n = qr$.
Soit M la matrice de la multiplication par x dans $K[x]$ exprimée dans la base $(y_i)_i$. Si on ordonne lexicographiquement la base $(y_i z_j)_{(i,j)}$ de L sur K, on voit que la matrice M' de la multiplication par x dans cette base est de la forme :

$$\begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix}$$

(r fois la matrices M) .
D'où $Tr_{L/K}(x) = [\ L : K[x]\ ](x_1 + ... + x_q) = x_1 + ... + x_n$.

□

Lemme 5.b : soit A un anneau intègre, K son corps des fractions ($car(K) = 0$), et L une extension de degré fini de K.
Soit x un élément de L entier sur A.
Alors $Tr_{L/K}(x)$ est entier sur A, en particulier $Tr_{L/K}(x) \in A$.

Démonstration : on garde les notations précédentes.
$Tr_{L/K}(x)$ est somme des x_i, donc il suffit de prouver que les x_i sont entiers sur A.
Soit σ_i : $K[x] \longrightarrow K[x_i]$
$Q(x) \longmapsto Q(x_i)$
S'il existe $Q \in A[X]$ tel que $Q(x) = 0$ alors $\sigma_i(Q(x)) = 0$.
Donc $Q(x_i) = 0$ et x_i est entier sur A.
Alors $Tr_{L/K}(x)$ est entier sur A et appartient à K, donc $Tr_{L/K}(x) \in A$.

□

Remarque 2 :
étant donnée une base $(x_1, ..., x_n)$ de L sur K, on cherche une base $(y_1, ..., y_n)$ telle que $Tr_{L/K}(x_i y_j) = \delta_{i,j}$.

Lemme de Dedekind 5.c : soit G un groupe, et $\sigma_1, ..., \sigma_n$ n homomorphismes distincts de G dans $\mathbb{C}^*$. Alors les σ_i sont linéairement indépendants sur $\mathbb{C}$.

Démonstration : supposons les σ_i linéairement dépendants .
On considère alors une relation $\sum_{i=1..q} \lambda_i \sigma_i = 0$ où tous les λ_i qui apparaissent sont non nuls et où on a choisi un entier q minimal.
On a donc $\forall g \in G \ \ \lambda_1\sigma_1(g) + ... + \lambda_q\sigma_q(g) = 0$
$q \geq 2$ car les σ_i sont non nuls.
$$\forall (g,h) \in G^2 \begin{cases} \lambda_1\sigma_1(gh) + ... + \lambda_q\sigma_q(gh) = 0 \\ \lambda_1\sigma_1(g) \ + ... + \lambda_q\sigma_q(g) = 0 \end{cases}$$
$$\forall (g,h) \in G^2 \begin{cases} \lambda_1\sigma_1(g)\sigma_1(h) + ... + \lambda_q\sigma_q(g)\sigma_q(h) = 0 \\ \lambda_1\sigma_1(g)\sigma_1(h) + ... + \lambda_q\sigma_q(g)\sigma_1(h) = 0 \end{cases}$$
Puis en soustrayant la deuxième ligne à la première, on obtient :
$\lambda_2\sigma_2(g)(\sigma_2(h) - \sigma_1(h)) + ... + \lambda_q\sigma_q(g)(\sigma_q(h) - \sigma_1(h) = 0$
Comme q a été choisi minimal, on a $\forall i \in [|2, q|]\ \forall h \in G \ \ \lambda_i(\sigma_i(h) - \sigma_1(h)) = 0$.
Donc $\forall h \in G \ \ \sigma_i(h) = \sigma_1(h)$ car $\lambda_i \neq 0$,
ce qui est absurde puisque les σ_i sont distincts.

□

Définition : soit B un anneau, A un sous anneau de B tel que B soit un A-module libre de rang n.
Pour $(x_1, ..., x_n) \in B^n$, on appelle ***discriminant du système*** $(x_1, ..., x_n)$ l'élément de A défini par :
$D(x_1, ..., x_n) = det(Tr_{B/A}(x_i x_j))$.

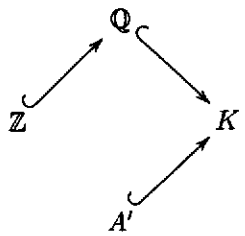
Proposition 5.3 : soit K un corps de caractéristique nulle, et L une extension de K de degré fini n .
Soit $\sigma_1, ..., \sigma_n$ les n injections distinctes de L dans un corps algébriquement clos C contenant K.
Alors si $(x_1, ..., x_n)$ est une base de L sur K, on a : $D(x_1, ..., x_n) = det(\sigma_i(x_j))^2 \neq 0$.

Démonstration : supposons $det(\sigma_i(x_j)) = 0$.
Alors $\exists(\lambda_1, ..., \lambda_n) \in C^n,\ \forall j \in [|1,n|]\ \ \sum_{i=1..n} \lambda_i \sigma_i(x_j) = 0$.
Par linéarité on a : $\sum_{i=1..n} \lambda_i \sigma_i = 0$,
ce qui constitue une contradiction d'après le Lemme de Dedekind.

□

Revenons au problème initial (cf : énoncé de la deuxième remarque).
La relation $D(x_1, ..., x_n) \neq 0$ exprime que la forme bilinéaire $(x, y) \longmapsto Tr_{L/K}(xy)$ est non dégénérée (ie $\{x \in L,\ \forall y \in L\ \ Tr_{L/K}(xy) = 0\} = \{0\}$).
Alors on a une injection $S_x : L \longrightarrow L^* = Hom_K(L, K)$ (en tant que K-espace vectoriel).
$x \longmapsto (y \longmapsto Tr_{L/K}(xy))$
Comme L et $Hom_K(L, K)$ ont même dimension, il en résulte que S_x est une bijection. Ainsi pour toute base $(x_1, ..., x_n)$ de L sur K, il existe (en utilisant la notion de base duale sur un espace vectoriel) une autre base $(y_1, ..., y_n)$ telle que $Tr_{L/K}(x_i y_j) = \delta_{i,j}$.

On est maintenant en mesure de démontrer la proposition 5.2.
Démonstration du Théorème 5.2 :
On a



Soit $(k_1, ..., k_n)$ une base de K sur $\mathbb{Q}$ où k_i est algébrique sur $\mathbb{Q}$ pour tout i, ie :
$\forall i\ \exists(a_0, ..., a_n) \in \mathbb{Z}^n,\ a_n k_i^n + ... + a_1 k_i + a_0 = 0\ (a_n \neq 0)$.
En multipliant par a_n^{n-1} , on a :
$(a_n k_i)^n + a_{n-1}(a_n k_i)^{n-1} ... + a_1 a_n^{n-1}(a_n k_i) + a_0 a_{n-1} = 0$.
Donc $a_n k_i$ est entier sur $\mathbb{Z}$.
Posons alors $k_i' = a_n k_i$, alors $(k_1', ..., k_n')$ est une base de K sur $\mathbb{Q}$ contenue dans A' .
D'après la remarque 2, il existe une base $(y_1, ..., y_n)$ de K sur $\mathbb{Q}$ telle que $Tr_{K/Q}(k_i' y_j) = \delta_{i,j}$.
Soit $z \in A'$; comme $(y_1, ..., y_n)$ est une base de K sur $\mathbb{Q}$, on peut écrire $z = \sum_{j=1..n} b_j y_j$ avec $b_j \in \mathbb{Q}$.
Comme $z \in A'$ et $\forall i\ k_i \in A'$, on a $k_i z \in A'$,
et donc par le lemme 5.b, il vient : $Tr_{K/\mathbb{Q}}(k_i' z) \in \mathbb{Z}$.
Or $Tr_{K/\mathbb{Q}}(k_i' z) = Tr_{K/\mathbb{Q}}(\sum_j b_j k_i' y_j) = \sum_j b_j Tr_{K/\mathbb{Q}}(k_i' y_j) = \sum_j b_j \delta_{i,j} = b_i$.
D'où $b_i \in \mathbb{Z}$ et donc $A' \subset \underbrace{\sum \mathbb{Z} y_i}$
module libre de rang n .
Or $\mathbb{Z}$ est principal, donc A' est libre.
Comme les $(k_i')_{i=1..n}$ forment une base et sont dans A', on en déduit que A' est un module libre de rang n.

□

Remarque : la même démonstration est valable en remplaçant $\mathbb{Z}$ par A , $\mathbb{Q}$ par $Frac(A)$, et K par une extension de type fini de K.

Définition : un sous-groupe additif H de $\mathbb{R}^n$ est *discret* si et seulement si quel que soit K compact de $\mathbb{R}^n$, $H \cap K$ est fini.
Lorsque H est engendré (comme $\mathbb{Z}$-module) par n vecteurs indépendants, on dit que H est un *réseau* de $\mathbb{R}^n$.

Revenons à l'application σ définie plus haut.
Théorème 5.4 : $\sigma(A')$ est un sous-groupe discret de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Démonstration : on a vu que A' est un $\mathbb{Z}$-module libre de rang n.
Soit $(a_1, ..., a_n)$ une base de A' .
Calculons le déterminant suivant :

$$|D| = |det \begin{pmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \dots & \sigma_1(a_n) \\ \sigma_2(a_1) & \cdot & & \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \sigma_{r_1}(a_1) & \sigma_{r_1}(a_2) & & \cdot \\ Re(\sigma_{r_1+1}(a_1)) & \cdot & & \cdot \\ Im(\sigma_{r_1+1}(a_1)) & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ Re(\sigma_{r_1+r_2}(a_1)) & \cdot & & Re(\sigma_{r_1+r_2}(a_n)) \\ Im(\sigma_{r_1+r_2}(a_1)) & \cdot & \dots & Im(\sigma_{r_1+r_2}(a_n)) \end{pmatrix} | = | \left(\frac{1}{2i}\right)^{r_2} det(\sigma_j(a_i)) |$$

Si $D = 0$ par le même raisonement que précédemment, on arrive à une contradiction en utilisant le lemme de Dedekind.
Donc $D \neq 0$ et les vecteurs $(\sigma(a_i))_i$ sont linéairement indépendants dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$, et le $\mathbb{Z}$-module qu'ils engendrent, $\sigma(A')$, est discret.

□

On peut alors maintenant énoncer le théorème d'existence d'une valeur absolue dilatante.
Théorème 5.5 : soit K une extension de type fini de $\mathbb{Q}$. Soit $\lambda \in K^*$, λ n'étant pas une racine de l'unité.
Alors il existe une injection de K dans un corps local K_v muni d'une valeur absolue $|.|_v$ telle que $|\lambda|_v > 1$.

Démonstration :
1er étape K est un corps de nombre :

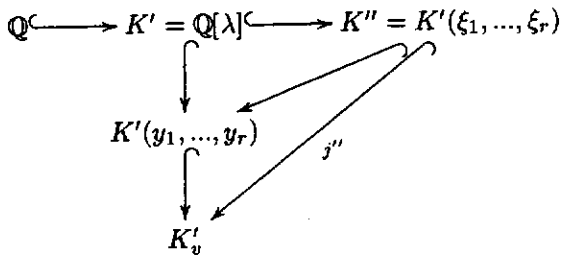
raisonnons par l'absurde, supposons que pour toute place on ait $|\lambda|_v \leq 1$.
Alors, par l'étude des places finies, on sait que pour tout idéal premier non nul P de A', $n_P(A'\lambda) \geq 0$.
Or par le Théorème 5.1 on a $A'\lambda = \prod_{P \in \Gamma} P^{n_P(A'\lambda)}$.
Donc $\lambda \in A'$.
La suite $\sigma(\lambda^n)$ reste bornée et l'étude des places infinies montre qu'elle prend ses valeurs dans un ensemble discret. De l'injectivité de σ, on déduit alors que l'on peut extraire de la suite $(\lambda^n)_n$ une suite constante, donc convergente et nécessairement vers 0 ou 1.
0 est exclu car $\lambda \in K^*$, finalement λ est une racine de l'unité. Absurde.

2eme étape cas général.

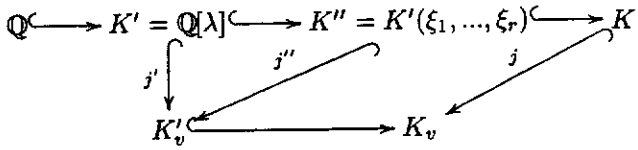
Cas 1 : λ est algébrique sur $\mathbb{Q}$.

Soit $K' = \mathbb{Q}[\lambda]$ (un corps de nombre). D'après la première étape, il existe une valeur absolue $|.|_v$ sur K' telle que $|\lambda|_v > 1$. Soit K'_v le complété de K' pour cette valeur absolue, et $j' : K' \longrightarrow K'_v$.
K'_v est non dénombrable
[sinon, en tant que K'-espace vectoriel, K'_v admettrait une base au plus dénombrable, et comme il est complet on aurait une contradiction en appliquant le théorème de Baire].
K'_v est de transcendance infinie sur K'
[en effet, s'il était de transcendance finie, de degré t sur K', il existerait $(x_1, ..., x_t) \in K'^t_v$ famille maximale algébriquement indépendante sur K'.
Soit alors $x \in K'_v$, la maximalité entraînerait l'existence d'un polynôme $Q \in K'[X_1, ..., X_t, X_{t+1}] - \{0\}$ tel que $Q(x_1, ..., x_t, x) = 0$, auquel cas K'_vest inclus dans la clôture algébrique de $K'(x_1, ..., x_t)$.
Or $K'(x_1, ..., x_t)$ est dénombrable, puisque K' l'est, et donc l'ensemble des racines des polynômes sur $K'(x_1, ..., x_t)$ est dénombrable (union dénombrable d'ensembles dénombrables) , ce qui contredit le fait que K'_v n'est pas dénombrable].

Soit $(\xi_1, ..., \xi_r)$ une famille maximale de K algébriquement indépendante sur K' et $K'' = K'(\xi_1, ..., \xi_r)$. L'injection j' se prolonge sur K'' en j'', car comme K'_v est de degré de transcendance infinie sur K', on peut trouver $(y_1, ..., y_r)$ dans K'_v algébriquement indépendants sur K' et on alors une injection naturelle de K'' dans $K'(y_1, ..., y_r) \subset K'_v$:



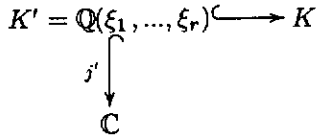
K est une extension finie de K'' [en effet la maximalité de $\xi_1, ..., \xi_r$ entraîne que tout élément $x \in K$ est algébrique sur K''. Donc $K[x]$ est de dimension finie sur K'', or $K \subset K[x]$ donc K est de dimension finie sur K''] .
On peut donc prolonger l'injection j'' en j de K sur un corps local K_v
[en effet, on peut écrire $\exists x \in K,\ K = K''[x]$. Soit alors P_m le polynôme minimal de x, on a $K = \frac{K''[X]}{(P_m)}$; on pose alors $K_v = \frac{K'_v[X]}{(P_m)}$ que l'on munit de l'unique valeur absolue qui prolonge celle de K'_v].
On obtient alors :



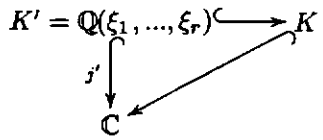
La valeur absolue sur K_v convient alors.

Cas 2 : λ est transcendant sur $\mathbb{Q}$.

On choisit $K_v = \mathbb{C}$ et $\xi_1 = \lambda$. On complète ξ_1 en $(\xi_1, \xi_2, ..., \xi_r)$ une famille maximale de K algébriquement indépendante sur $\mathbb{Q}$ (c'est possible car ξ_1 est algébrique). Il existe alors une injection j' du corps $K' = \mathbb{Q}(\xi_1, ..., \xi_r)$ dans $\mathbb{C}$ telle que $|j'(\lambda)| > 1$: en effet, il suffit d'envoyer la famille $(\xi_1, ..., \xi_r)$ sur $(z_1, ..., z_r)$ où les (z_i) sont des nombres complexes algébriquement indépendants sur $\mathbb{Q}$. Pour se convaincre que c'est possible, il faut voir qu'on peut trouver des familles de complexes algébriquement indépendantes sur $\mathbb{Q}$ de cardinal aussi grand que l'on souhaite (sinon, il existerait un $n \in \mathbb{N}$ tel que toutes les familles de complexes algébriquement indépendantes sur $\mathbb{Q}$ soient de cardinal $\leq n$. Soit alors $(w_1, ..., w_u)$ algébriquement indépendante sur $\mathbb{Q}$ et maximale $(u \leq n)$.
Pour tout $w \in \mathbb{C}$, il existe donc un $P \in \mathbb{Q}[X_1, ..., X_u, X_{u+1}]$ non nul, tel que $P(w_1, ..., w_u, w) = 0$ et donc $\mathbb{C} \subset$ ***clôture algébrique de*** $Q(w_1, ..., w_u)$ ce qui est comme précédemment contradictoire par un argument de dénombrabilité).
Pour ensuite avoir $|j'(\lambda)| > 1$, il suffit de remplacer z_1 par az_1 avec a assez grand dans $\mathbb{Q}$. Il est clair que la famille $(az_1, z_1..., z_r)$ reste algébriquement indépendante sur $\mathbb{Q}$:



Comme précédemment, la maximalité de $(\xi_1, ..., \xi_r)$ implique que K est de dimension finie sur K'.
Donc cette injection se prolonge en une injection j de K dans $\mathbb{C}$ [en effet, on peut encore écrire $K = K'[x]$ avec $x \in K$, noter P_m le polynôme minimal de X , x_i une racine dans $\mathbb{C}$ de P_m, et envoyer bijectivement K' dans $\mathbb{C}$, en associant à x la valeur x_i].
La valeur absolue qu'on obtient sur $\mathbb{C}$ est alors solution.



□

Théorème (Tits) 5.6 : en caractéristique nulle, un groupe linéaire Γ contient
-soit un sous-groupe résoluble d'indice fini,
-soit un groupe libre à deux générateurs.

Démonstration : supposons Γ non virtuellement résoluble.
Montrons que dans ce cas Γ contient un sous-groupe libre à deux générateurs.
- Γ étant non virtuellement résoluble, il n'est pas résoluble, et donc par le corollaire (2.6 (i)) il existe un sous-groupe de type fini de Γ non virtuellement résoluble. Par conséquent il suffit de démontrer le résultat pour ce sous-groupe. Ceci revient à supposer Γ de type fini.
On peut ainsi supposer que le corps k est le corps engendré par les coefficients des générateurs de Γ, donc k est de type fini.
- Quitte à remplacer Γ par Γ_e (la composante irréductible de l'identité, sous-groupe d'indice fini irréductible, donc Zariski connexe), on peut supposer Γ Zariski connexe.
- Le groupe dérivé $D(\Gamma) = [\Gamma, \Gamma]$ est Zariski connexe (par la proposition 1.2 (ii)).
Si $[\Gamma, \Gamma]$ est nilpotent, alors $[\Gamma, \Gamma]$ est résoluble donc Γ aussi, et donc virtuellement résoluble. Contradiction. Donc $[\Gamma, \Gamma]$ n'est pas nilpotent.
- $[\Gamma, \Gamma]$ n'est pas virtuellement nilpotent (*)
[en effet $[\Gamma, \Gamma]$ est Zariski connexe et n'est pas nilpotent et on applique la contraposée du lemmme 1.2].
-Si toutes les valeurs propres de tous les éléments de $[\Gamma, \Gamma]$ étaient racines de l'unité, $[\Gamma, \Gamma]$ serait viruellement unipotent (d'après le corollaire 2.4), et donc virtuellement unipotent d'après le théorème d'Engels, ce qui est contradictoire avec (*). Donc il existe un élément γ de $[\Gamma, \Gamma]$ dont une valeur propre α n'est pas une racine de l'unité.
- Grâce au théorème 5.5, on peut remplacer k par un corps localement compact K muni d'une valeur absolue pour laquelle $|\alpha| > 1$.
Soit $\lambda_1(\gamma)$ la plus grande valeur absolue des valeurs propres de γ ; $\lambda_1(\gamma) > 1$.
Soit V_γ^+ le sous-espace γ-invariant correspondant, $p = m_\gamma$ sa dimension, et soit $W = \wedge^p V$.
Γ agit sur W et $\wedge^p\gamma$ est proximal dans $\mathbb{P}(W)$.
On construit une suite de Jordan-Hölder de la façon suivante : soit $W_0 = W$.
On considère $\{A \subset W_0$, A *sous − espace vectoriel de* W , $A\ \Gamma - invariant\}$, et on prend dans cet ensemble un élément de dimension maximale, W_1.
W_0/W_1 est irréductible (au sens des représentations de groupe)
(sinon, on peut trouver un sous-espace vectoriel non trivial A de W_0/W_1 stable sous l'action de Γ ; on prend alors son image réciproque par la projection canonique de W_0 sur W_0/W_1, ce qui donne un sous-espace vectoriel de W_0 Γ stable, distinct de W_0 , et contenant strictement W_1, ce qui contredit la définition de W_1).
Puis on réitère ce processus, qui s'arrête au bout d'un temps fini car la suite des dimensions est strictement décroissante.

$$\begin{cases} \{0\} = W_l \subset W_{l-1} \subset \ldots \subset W_1 \subset W_0 = W \\ \forall i \in [|0, l|] \quad W_i \text{ est } \Gamma\text{-invariant.} \\ \forall i \in [|1, l|] \quad W_{i-1}/W_i \text{ irréductible (au sens des representations de groupe).} \end{cases}$$

Soit V' l'unique sous-quotient dans lequel $\wedge^p\gamma$ a une valeur propre de module égal à $\lambda_1(\gamma)^p$.
On définit alors : $\rho : \Gamma \longrightarrow GL(V')$ l'action induite, et $\Gamma' = \rho(\Gamma)$.
Γ' est l'image d'un sous-groupe Zariski connexe Γ par ρ qui est un morphisme, donc Γ' est un sous-groupe

Zariski connexe de $GL(V')$.
Soit $\gamma' = \rho(\gamma)$.
-γ' est proximal dans $\mathbb{P}(V')$.
-V' est irréductible sous Γ.
- $dim(V') \geq 2$ (car $\gamma' \in SL(V') \Rightarrow det(\gamma') = 1$, et γ' a une valeur propre de module $\lambda_1(\gamma)^p > 1$).
Donc d'après le lemme 4.5, Γ' contient un sous-groupe libre à deux générateurs, et Γ contient aussi un sous-groupe libre à deux générateurs.

□

En Guise de Conclusion : la démonstration de l'alternative de Tits est un bel exemple d'application de la théorie des corps à l'étude des groupes linéaires.

Réferences :

[1]Y.Amice - Les nombres p-adiques
[2]Y.Benoist - Sous-groupes discrets des groupes de Lie.
[3]R.Hartshorne - Algebraic geometry.
[4]S.Lang - Algebra.
[5]P.Samuel - Théorie algébrique des nombres, Hermann Paris (1971).
[6]JP.Serre - Cours d'arithmétique.