NOTES DU COURS PECCOT 2006 : PROPRIÉTÉS QUALITATIVES DES GROUPES DISCRETS

EMMANUEL BREUILLARD

Résumé. In these notes, we discuss some aspects of finitely generated groups of matrices dealing with the existence of free subgroups in them. We first study dense subgroups of Lie groups and show in particular that a dense subgroup of a semisimple Lie group always contain a dense free subgroup. We then discuss some generalizations of this result and give an application to the geometry of foliations. In the second part of the course, we discuss the notions of uniform Tits alternative and of spectral gap for finitely generated groups and at the end we give a complete proof of the uniform exponential growth of linear groups.

Table des matières

Le cours traite de quelques aspects des sous-groupes de matrices ayant égard à la présence de sous-groupes libres dans ceux-ci. Dans un premier temps, on esquisse une brève étude des sous-groupes denses des groupes de Lie ; on démontre notamment que dans un groupe de Lie semisimple, un sous-groupe dense contient toujours un sous-groupe libre et encore dense. On indique ensuite des généralisations possibles de ces résultats et nous donnons une application à la géométrie des feuilletages. Dans un deuxième temps, les notions d'alternative de Tits uniforme et de trou spectral pour les groupes de type fini seront discutées, et finalement nous donnerons une preuve de la croissance exponentielle uniforme pour les groupes linéaires.

1. Préliminaires sur les sous-groupes denses

Soit G un groupe de Lie connexe. On note $\mathfrak{g}$ son algèbre de Lie et $\mathcal{A}$ la sous $\mathbb{R}$-algèbre de $End(\mathfrak{g})$ engendrée par les $Ad(g)$, $g \in G$. On dit que G est *topologiquement parfait* si le groupe dérivé $[G,G]$ est dense dans G. Il revient au même de dire que G n'a pas de quotient résoluble non trivial, ou bien qu'il ne se surjecte pas sur le cercle. Bien sûr tout groupe de Lie semisimple est ainsi. L'objet de ce paragraphe est de démontrer l'assertion suivante :

Proposition 1.1. *Soit G un groupe de Lie connexe et topologiquement parfait. Alors il existe un voisinage U de l'identité dans G tel que pour toute partie finie de U, soit $g_1,...,g_k$, on a la propriété suivante : les $Ad(g_i)$ engendrent $\mathcal{A}$ si et seulement si les g_i engendrent un sous-groupe dense de G.*

Ainsi, au voisinage de l'identité, une partie est topologiquement génératrice si et seulement si elle engendre $\mathcal{A}$ algébriquement, en tant qu'algèbre.

Pour la preuve, nous aurons besoin du lemme suivant :

Lemme 1.1. *(Zassenhaus) Soit G un groupe de Lie connexe. Il existe un voisinage U de l'identité tel que pour tout épimorphisme $\pi : G \to H$ et toute famille $\{g_i\}$ de points de U, si les $\{\pi(g_i)\}$ engendrent un sous-groupe discret de H, alors ce sous-groupe est nilpotent.*

Démonstration. Voir le Raghunathan, [36] chapitre VIII. □

Preuve de la Proposition. Seul un sens mérite explication. On suppose donc que les $Ad(g_i)$ engendrent $\mathcal{A}$. Soit H le groupe engendré par les g_i. La composante connexe de l'identité H° est distinguée dans H et son algèbre de Lie $\mathfrak{h}$ est invariante par les $Ad(g_i)$ donc par $\mathcal{A}$ toute entière ; c'est donc un idéal de $\mathfrak{g}$. Ainsi H° est distingué dans G. De plus, par hypothèse, les $\{\pi(g_i)\}$ engendrent un sous-groupe discret de G/H°, donc par le lemme de Zassenhaus, un sous-groupe nilpotent. Il s'ensuit que les $\{Ad(\pi(g_i))\}$ aussi engendrent un sous-groupe nilpotent de $GL(\mathfrak{g}/\mathfrak{h})$, donc triangularisable dans une base de $\mathfrak{g}/\mathfrak{h}$. La sous-algèbre

$\pi(\mathcal{A})$, engendrée par les $\{Ad(\pi(g_i))\}$, est donc aussi triangularisable, donc résoluble. Ainsi $Ad(\pi(G))$ et donc aussi $\pi(G) = G/H^\circ$ est résoluble. Puisque G est topologiquement parfait, c'est que $G = H^\circ = H$, ce qu'il fallait démontrer. □

Remarque 1.1. *Dans la Proposition 1.1, on peut remplacer la condition que les $Ad(g_i)$ engendrent $\mathcal{A}$ par celle que les $\log(g_i)$ engendrent $\mathfrak{g}$, si les g_i sont dans un voisinage suffisamment petit de l'identité pour que l'exponentielle soit un difféomorphisme.*

Corollaire 1.1. *Si G est topologiquement parfait, la condition sur $(g_1, ..., g_k) \in G^k$ pour qu'ils engendrent un groupe dense est une condition ouverte dans G^k.*

En effet, engendrer la sous-algèbre $\mathcal{A}$ est une condition algébrique de type non annulation d'un déterminant, donc une condition ouverte ; plus précisément :

Corollaire 1.2. *Si G est topologiquement parfait et U comme ci-dessus, alors pour tout $k \in \mathbb{N}$, les k-uplets de points $g_1, ..., g_k$ de U qui n'engendrent pas un sous-groupe dense de G sont tous contenus dans sous-variété analytique fermée propre de G^k constituée des k-uplets tels que les $Ad(\pi(g_i))$ n'engendrent pas la sous-algèbre $\mathcal{A}$.*

En particulier, on peut trouver des ouverts $U_1, ..., U_k$ de G tels que tout choix d'un k-uplet $(g_1, ..., g_k)$ avec $g_i \in U_i$ engendre un sous-groupe dense.

Corollaire 1.3. *Soit $d(G)$ le nombre minimal de g_i qui engendrent G topologiquement. Si G est topologiquement parfait, alors tout sous-groupe dense Γ de G contient un sous-groupe dense engendré par $d(G)$ éléments.*

En effet, il suffit de choisir des $\gamma_i \in \Gamma$ qui tombent dans chacun des U_i.

Remarque 1.2. *Si G est semisimple, alors $d(G) = 2$. De même $\mathcal{A}$ et $\mathfrak{g}$ sont 2-engendrées. Par exemple si $G = SL_n(\mathbb{R})$, $\mathfrak{g} = sl_n(\mathbb{R})$ et si $a = \sum_{i \neq j} E_{ij}$ et b est diagonale, alors a et b engendrent $\mathfrak{g}$ dès que les $b_{ii} - b_{jj}$ sont tous distincts.*

Pour un groupe de Lie connexe G quelconque, on peut montrer que $d(G) \leq 2\dim(G)$.

Remarque 1.3. *La proposition 1.1 devient fausse si les g_i ne sont pas choisis proches de l'identité. Par exemple si $a = Id + \alpha E_{12}$ et $b = Id + \alpha E_{21}$ dans $SL_2(\mathbb{R})$, alors le sous-groupe $\langle a, b \rangle$ est dense si α est assez petit et non nul, mais discret si $|\alpha| \geq 2$. Pourtant $Ad(a)$ et $Ad(b)$ engendrent $\mathcal{A}$ pour tout α non nul.*

Corollaire 1.4. *Si G est semisimple et Γ est dense et engendré par n éléments alors pour tout voisinage de l'identité V, il existe une partie génératrice de Γ à $n+2$ éléments de V.*

En effet peut trouver U_1 et U_2 deux ouverts de V tels que tout choix de $a \in U_1$ et $b \in U_2$ engendre un sous-groupe dense. On peut choisir a et b dans Γ aussi. Si $\gamma_1, ..., \gamma_n$ engendrent Γ, alors on peut trouver des mots $w_1, ..., w_n$ en a et b tels que chaque $w_i\gamma_i \in V$. Clairement les $w_i\gamma_i$ avec a et b engendre Γ tout entier.

Conséquence du dernier corollaire pour la propriété (T) : Si Γ est un groupe de type fini dense d'un groupe de Lie semisimple G et Γ a la propriété T de Kazhdan, alors il n'a pas la propriété (T) uniforme, i.e. la constante de Kazhdan ne peut être choisie de façon indépendante de la partie génératrice finie.

Rappelons que Γ a la propriété (T) de Kazhdan si pour tout (pour une) partie génératrice finie Σ de Γ, il existe une constante $\varepsilon(\Sigma) > 0$ telle que pour toute représentation unitaire continue de Γ sans vecteur invariant non nul, on a $\max_{\gamma\in\Sigma} \|\pi(\gamma)v - v\| \geq \varepsilon(\Sigma)$ pour tout vecteur v de norme 1.

Ici on peut clairement rendre $\varepsilon(\Sigma)$ aussi petit que l'on veut en changeant Σ en une partie génératrice proche de l'identité. Ceci s'applique par exemple si Γ est un réseau co-compact d'un groupe de Lie simple de rang supérieur, comme $\Gamma = SO(Q) \cap SL_5(\mathbb{Z}[\sqrt{2}])$ où $Q = x_1^2 + x_2^2 + x_3^2 - \sqrt{2}(x_4^2 + x_5^2)$ qui peut se voir à la fois comme un sous-groupe discret co-compact dans $SO(3,2)$ et un sous-groupe dense de $SO(5) = SO(Q^\sigma)$ ou σ est l'automorphisme de Galois envoyant $\sqrt{2}$ sur $-\sqrt{2}$.

2. Déformations de sous-groupes denses

On démontre ici que tout sous-groupe dense est la déformation arbitraitrement petite de tout autre sous-groupe dense, plus précisément :

Proposition 2.1. *Soit G un groupe de Lie semisimple. Il existe un voisinage ouvert U de l'identité avec la propriété suivante. Soit $\gamma_1, ..., \gamma_n$ dans U tel que $\Gamma = \langle \gamma_i,\ i = 1, ..., n\rangle$ est dense. Soit $s_1, ..., s_{n+1}$ dans U quelconques. Alors, pour tout voisinage ouvert V de l'identité, il existe des éléments $t_1, ..., t_{n+1}$ proches des s_i (i.e. $t_i \in s_iV$) et tels que $\Gamma = \langle t_i,\ i = 1, ..., n+1\rangle$.*

Démonstration. Soit U comme au paragraphe précédent. Quitte à perturber un peu s_1 et s_2 on peut supposer que le sous-groupe $\langle s_1, s_2\rangle$ qu'ils engendrent est dense dans G. Comme Γ est dense, les $Ad(\gamma_i)$ engendrent $\mathcal{A}$, la sous-algèbre engendrée par les $Ad(g)$, $g \in G$. Ainsi pour tout $i = 1, ..., n$ la condition que $Ad(g)$, $Ad(\gamma_1)$, ..., $\widehat{Ad(\gamma_i)}$, ..., $Ad(\gamma_n)$ engendrent $\mathcal{A}$ est une condition ouverte et non vide. Donc d'après la proposition 1.1, $\{g \in U$ tel que $\langle g, \gamma_1, ..., \widehat{\gamma_i}, ..., \gamma_n\rangle$ est dense pour chaque $i\}$ est un ouvert dense de U. Soit $\gamma_{n+1} \in \Gamma$ dans cet ouvert.

On peut trouver un mot w_1 en $\gamma_2, ..., \gamma_{n+1}$ tel que $w_1\gamma_1$ est très proche de s_1 et tel que $\langle w_1\gamma_1, \gamma_3, ..., \gamma_{n+1}\rangle$ est dense. Ensuite on trouve un mot w_2 en $w_1\gamma_1, \gamma_3, ..., \gamma_{n+1}$ tel que $w_2\gamma_2$ est très proche de s_2. Ainsi $\langle w_1\gamma_1, w_2\gamma_2\rangle$ est dense.

Finalement, on trouve des mots $w_3, ..., w_{n+1}$ en $w_1\gamma_1$ et $w_2\gamma_2$ tels que chaque $w_i\gamma_i$ est très proche de s_i pour $i = 3, ..., n+1$. Clairement les $w_i\gamma_i$, $i = 1, ..., n+1$ engendrent Γ tout entier. □

Remarque 2.1. *On a dû ajouter artificiellement un générateur. Sans cette liberté, la situation semble plus rigide : par exemple peut-on déformer tout groupe dense à deux générateurs en un autre ? Cependant, si $\langle \gamma_2, \gamma_3, ..., \gamma_n\rangle$ est déjà dense, alors le même argument s'applique sans $n+1$-ème générateur. On verra plus bas que si Γ est un groupe libre, on n'a pas cet inconvénient.*

Exemple 2.1. *Prenons $G = SU(2)$, alors il est facile de vérifier que toute paire a, b de points de G peut se déformer en une paire a', b' telle que a', b' et $a'b'$ sont* *d'ordre fini. Alors le sous-groupe $\langle a', b'\rangle$ a la propriété (FA) de Serre, i.e. toute action de ce groupe sur un arbre fixe un point. Il s'ensuit (Stallings) que $\langle a', b'\rangle$ n'est pas virtuellement libre. Comme on le verra plus bas, on peut aussi perturber a et b de sorte que a' et b' engendre un groupe libre. On peut donc aller dans les deux sens. Cette remarque s'applique à tout groupe de Lie compact semisimple, mais c'est un peu plus délicat à vérifier en général (cf.* [16]*).*

3. Existence de certains sous-groupes denses

Dans ce paragraphe, on décrit deux constructions qui permettent d'obtenir aisément des plongements denses de groupes libres, d'une part, et de π_1 de surfaces d'autre part, dans un groupe de Lie. Elles reposent toutes deux sur le théorème de Baire.

On note F_k le groupe libre (non abélien) de rang $k \geq 2$.

3.1. **Sous-groupes libres.**

Proposition 3.1. *Soit G un groupe de Lie semisimple. Alors $\{(a,b) \in G^2$ tel que $\langle a, b\rangle$ est libre$\}$ est un G_δ-dense de G^2.*

Corollaire 3.1. *G possède un sous-groupe libre F_2 dense.*

Preuve de la Proposition. Soit $w \in F_2 \backslash \{1\}$ et $\mathcal{A}_w = \{(a,b) \in G^2,\ w(a,b) = 1\}$ est une sous-variété analytique de G^2. Par suite, si $\mathcal{A}_w$ est d'intérieur non-vide, alors $\mathcal{A}_w = G^2$ et $w(a,b) = 1$ pour tout a et b dans G, donc aussi pour tout a et b dans le complexifié $H = G(\mathbb{C})$ de G. Mais ceci contredit le

Lemme 3.1. *Si H est un groupe de Lie semisimple complexe, alors il existe a et b dans H qui engendrent un groupe libre F_2.*

Démonstration. D'après la structure des algèbres de Lie semisimples complexes, on sait qu'elle contiennent $sl(2,\mathbb{C})$ comme sous-algèbre. H contient donc une copie de $SL(2,\mathbb{C})$ ou de $PSL(2,\mathbb{C})$. Mais ces groupes contiennent le sous-groupe engendré par $a = Id + 3E_{12}$ et $b = a = Id + 3E_{21}$ qui est libre par un argument de ping pong classique (voir plus bas Remarque 5.2). □

Il en résulte que $\mathcal{A}_w$ est un fermé d'intérieur vide de G^2 et donc par le théorème de Baire $\cup_{w \in F_2 \backslash \{1\}} \mathcal{A}_w$ est un F_σ et son complémentaire, le G_δ des paires (a,b) qui engendrent un sous-groupe libre. □

3.2. **Groupes de surface.**

Par groupe de surface, on entend le groupe fondamental Γ_g d'une surface fermée orientable de genre $g \geq 2$. Nous allons démontrer la proposition suivante :

Proposition 3.2. *Soit G un groupe topologique compact. Si G possède un groupe libre dense alors il possède un sous-groupe dense isomorphe à un groupe de surface, et réciproquement.*

Remarque 3.1. *En fait on démontre que si G a un F_{2r} $(r \in \mathbb{N})$ dense alors il a un Γ_{2r} dense, et s'il a un Γ_r dense alors il a un F_{2r} dense.*

Remarque 3.2. *Ici on ne suppose pas G de Lie. Des considérations semblables s'appliquent si G est un groupe de Lie non discret quelconque. On démontre : G possède un groupe libre dense ssi il possède un groupe de surface dense et ssi la composante connexe G° est non-résoluble et G/G° est de type fini.*

Remarque 3.3. *Tout groupe de surface Γ_{2r} a une présentation de la forme*

$$\Gamma_{2r} = \{a_i, a_i', b_i, b_i', 1 \leq i \leq r | [a_1, a_1']...[a_r, a_r'][b_r', b_r]...[b_1', b_1] = 1\}$$

qui provient de la décomposition classique de la surface en méridiens et longitudes.

L'idée de la preuve de la proposition consiste à déformer le sous-groupe libre pour en faire un groupe de surface, en utilisant le fait que le groupe de surface a de nombreux épimorphismes sur le groupe libre. On utilisera le

Lemme 3.2. *On considère le groupe de surface Γ_{2r} avec la présentation ci-dessus. On note F_{2r} un groupe libre de générateurs x_i, x_i' $i = 1, ..., r$. On note $\sigma : \Gamma_{2r} \to \Gamma_{2r}$ l'automorphisme défini par $\sigma(a_i) = a_i$, $\sigma(a_i') = a_i'$, $\sigma(b_i) = \gamma b_i \gamma^{-1}$ et $\sigma(b_i') = \gamma b_i' \gamma^{-1}$ où $\gamma = [a_1, a_1']...[a_r, a_r']$. Enfin on note $f : \Gamma_{2r} \to F_{2r}$ le morphisme qui envoie a_i et b_i sur x_i et a_i' et b_i' sur x_i'. Alors la suite $(f \circ \sigma^n)_{n \geq 1}$ est fidèle à la limite, c'est-à-dire que pour tout $w \in \Gamma_{2r} \backslash \{1\}$ il existe n_0 tel que pour tout $n \geq n_0$, $f \circ \sigma^n(w) \neq 1$.*

Interprétation géométrique : la surface Σ_{2r} a $2r$ trous et γ correspond au lacet simple qui sépare la surface en deux surfaces identiques de bord γ et à r trous. L'automorphisme σ correspond à un twist de Dehn le long de γ et le morphisme f provient de la réflexion par rapport à γ qui envoie la surface Σ_{2r} sur la surface à r trous de bord γ.

Preuve de la Proposition 3.2. Soit $F_{2r} = \langle x_i, x_i' \rangle$ le sous-groupe libre et dense de G. Soit $\gamma = [x_1, x_1']...[x_r, x_r'] \in F_{2r}$. Soit K le sous-groupe fermé engendré par γ, i.e. $K = \overline{\langle \gamma \rangle}$. Pour tout α dans K, on note $\sigma_\alpha : \Gamma_{2r} \to G$ le morphisme défini par $\sigma(a_i) = x_i$, $\sigma(a_i') = x_i'$, $\sigma(b_i) = \alpha x_i \alpha^{-1}$ et $\sigma(b_i') = \alpha x_i' \alpha^{-1}$. On vérifie que c'est bien un morphisme, puisque la relation qui définit Γ_{2r} est bien envoyée sur l'identité, car α commute avec γ. Par le lemme 3.2, $\{\sigma_{\gamma^n}\}_{n \geq 1}$ est fidèle à la limite. Donc si $w \in \Gamma_{2r} \backslash \{1\}$, alors $\mathcal{O}_w = \{\alpha \in K, \sigma_\alpha(w) \neq 1\}$ est un ouvert non-vide de K. Comme K est compact, $\{\gamma^n, n \geq n_0\}$ est dense dans K pour tout n_0. Ainsi $\mathcal{O}_w$ est un ouvert dense de K. Par le théorème de Baire, $\cap_{w \neq 1} \mathcal{O}_w$ est dense et donc non-vide. On peut donc choisir $\alpha \in \cap_{w \neq 1} \mathcal{O}_w$, ce qui montre que σ_α est fidèle. L'image de σ_α est dense car elle contient déjà F_{2r} qui est dense dans G. La preuve de la réciproque passe par un argument semblable. □

Reste à démontrer le lemme 3.2. Sa preuve repose sur le

Lemme 3.3. *(Baumslag) Soit F un groupe libre et $u, a_1, ..., a_k$ des éléments de F tels que u ne commute à aucun des a_i. Alors il existe un entier n_0 tel que pour tous $n_1, ..., n_k \in \mathbb{Z}$, si $|n_i| \geq n_0$ pour chaque $i = 1, ..., k$ alors*

$$a_1 u^{n_1} a_2 u^{n_2} ... a_k u^{n_k} \neq 1$$

Démonstration. C'est un exercice. □

Preuve du lemme 3.2. Soit $w \in \Gamma_{2r}$. On peut écrire $w = w_1 w_2 ... w_{2p}$ où chaque w_{2i+1} est un mot en les a_i et a_i' tandis que chaque w_{2i} est un mot en les b_i et b_i'. Si w n'est pas une puissance de Γ alors on peut réécrire w de sorte de aucun des w_i de soit une puissance de γ (en effet si l'un d'entre eux est une puissance de γ, on peut convertir les a_i,a_i' en b_i,b_i' et réciproquement grâce à la relation qui définit Γ_{2r}). Mais le centralisateur de γ dans Γ_{2r} est égal au sous-groupe cyclique $\langle\gamma\rangle$, donc on peut supposer que les w_i ne commutent pas avec γ. Le lemme de Baumslag permet de conclure. □

4. Alternative de Tits topologique

Dans ce paragraphe et le suivant, nous allons démontrer ceci :

Proposition 4.1. *Soit G un groupe de Lie semisimple et Γ un sous-groupe dense. Alors Γ contient un sous-groupe libre F_2 dense dans G.*

Ce résultat est un cas particulier (pour $k = \mathbb{R}$ et $\overline{\Gamma}$ semisimple) du

Théorème 4.1. *(Alternative de Tits topologique) Soit k un corps local et Γ un sous-groupe de type fini de $GL_n(k)$. Alors*
- *Soit l'adhérence $\overline{\Gamma}$ contient un sous-groupe ouvert résoluble de $GL_n(k)$.*
- *Soit Γ contient un sous-groupe libre F de rang fini ($\leq d(\Gamma)$) tel que $\overline{F} = \overline{\Gamma}$.*

C'est une généralisation de la célèbre alternative de Tits :
Alternative de Tits : Soit K un corps quelconque et Γ un sous-groupe de $GL_n(K)$ de type fini. Alors
- Soit Γ contient un sous-groupe résoluble d'indice fini.
- Soit Γ contient un sous-groupe libre F_2.

Une conséquence de l'alternative de Tits est que tout sous-groupe dense d'un groupe de Lie G semisimple possède un sous-groupe libre. Cependant, la méthode utilisée dans la preuve de l'alternative ne permet pas de garantir a priori que l'on peut choisir ce sous-groupe libre de sorte qu'il soit encore dense, et c'est bien l'objet de cette alternative topologique. En fait, dans de nombreux cas, le sous-groupe libre construit par Tits sera discret dans G. Démontrons maintenant que l'alternative topologique est bien une généralisation de l'alternative classique.

Preuve que le théorème 4.1 entraîne l'alternative de Tits. Soit Γ un sous-groupe de type fini de $GL_n(K)$. Puisque Γ est de type fini, on a que $\Gamma \leq GL_n(R)$ où R est un sous-anneau de K de type fini (R est le sous-anneau engendré par les coefficients de matrice des générateurs de Γ). Par le théorème de normalisation de Noether, on peut plonger R dans l'anneau $\mathcal{O}_k$ des entiers d'un corps local non archimédien k bien choisi. Ainsi Γ apparaît comme un sous-groupe du groupe $GL_n(\mathcal{O}_k)$ qui est un groupe compact et totalement discontinu (i.e. profini) et ouvert dans $GL_n(k)$. D'après l'alternative topologique, on a deux cas. Dans le premier $\overline{\Gamma}$ contient un sous-groupe résoluble ouvert dans $GL_n(\mathcal{O}_k)$. Mais un sous-groupe ouvert d'un groupe profini est d'indice fini. Ainsi Γ est virtuellement résoluble. Dans le deuxième cas Γ contient un sous-groupe libre F. On obtient donc l'énoncé initial de l'alternative classique. □

Remarque 4.1. *En fait ce raisonnement montre plus : à savoir que dans le deuxième cas on obtient un sous-groupe libre F qui est aussi Zariski dense dans Γ. En effet la topologie de Zariski a moins de fermés que la topologie usuelle issue du corps local.*

Pour démontrer la proposition 4.1 nous allons en fait établir le résultat plus général suivant :

Théorème 4.2. *Soit K un corps de type fini avec car$(K) = 0$, $\mathbb{G}$ un groupe algébrique semisimple, Zariski connexe et défini sur K, et R un sous-anneau de K de type fini et Ω une partie Zariski dense de $\mathbb{G}(R)$. Alors pour tous $a_1, ..., a_n$ dans $\mathbb{G}(K)$, il existe $x_1, ..., x_n$ tels que pour chaque $i = 1, ..., n$ $x_i \in \Omega^4 a_i \Omega$ et les x_i sont les générateurs d'un sous-groupe libre F_n.*

Preuve que le théorème 4.2 entraîne la proposition 4.1. Quitte à factoriser par un sous-groupe central discret de G, on peut supposer que $G = \mathbb{G}(\mathbb{R})^\circ$ où $\mathbb{G}$ est un groupe algébrique semisimple Zariski connexe et défini sur $\mathbb{Q}$. Comme Γ est de type fini, $\Gamma \leq GL_n(R)$ où R est un sous-anneau de type fini de $\mathbb{R}$ dont on note K le corps des fractions. On se donne $a_1, ..., a_n$ des générateurs de Γ et on applique le théorème à cette situation avec $\Omega = \Gamma \cap U$ où U est le voisinage de l'identité dans G obtenu à la proposition 1.1. Le sous-groupe de Γ engendré par les x_i sera encore dense grâce à la proposition 1.1. Il faut seulement vérifier que Ω est bien Zariski dense. Si $\mathbb{X}$ est l'adhérence de Zariski de Ω, alors $U \subseteq \mathbb{X}(\mathbb{R})^\circ$ car Γ est dense, et donc $\mathbb{X}(\mathbb{R})^\circ = G$ car $\mathbb{X}(\mathbb{R})$ est une sous-variété analytique de $\mathbb{G}(\mathbb{R})$, ce qui force $\mathbb{X} = \mathbb{G}$. □

Remarque 4.2. *Le théorème 4.2 est valable sans l'hypothèse de Zariski connexité et aussi en caractéristique quelconque. Cependant la preuve est plus délicate sans ces hypothèses. C'est ce cas général dont on a besoin pour le théorème 4.1.*

Remarque 4.3. *D'après les paragraphes* 2 *et* 3*, toute partie génératrice finie de Γ peut être déformée dans G pour engendrer un sous-groupe libre et dense. L'argument qu'on vient de donner montre que l'on peut effectuer la déformation en restant dans Γ. On obtient donc en fait un peu mieux que ce qui est énoncé dans la proposition 1.1.*

5. Proximalité et ping pong

Dans ce paragraphe, nous démontrons le théorème 4.2. Nous allons d'abord introduire quelques notations et définitions.

5.1. **Transformations projectives.** Soit k un corps local. On note $\|\cdot\|$ la norme euclidienne (resp. hermitienne, du max) sur k^n si k est $\mathbb{R}$ (resp. $\mathbb{C}$, non-archimédien). Cette norme s'étend naturellement à l'algèbre extérieure $\Lambda^* k^n$. Elle induit une métrique sur l'espace projectif $\mathbb{P}(k^n)$ définie ainsi pour u, v vecteurs $\neq 0$

$$d([u],[v]) = \frac{\|u \wedge v\|}{\|u\| \, \|v\|}$$

Décomposition KAK. Notons $K = SO(n)$ si $k = \mathbb{R}$, $K = SU(n)$ si $k = \mathbb{C}$, $K = SL_n(\mathcal{O}_k)$ si k est non-archimédien, où $\mathcal{O}_k$ est l'anneau des entiers de k. Si k est $\mathbb{R}$ ou $\mathbb{C}$, on note A l'ensemble des matrices diagonales de déterminant $diag(a_1, ..., a_n)$ dont les coefficients sont réels positifs et rangés par ordre décroissant $a_1 \geq ... \geq a_n$. Si k est non-archimédien, on note A les matrices diagonales $diag(\pi^{k_1}, ..., \pi^{k_n})$ où les entiers k_i vérifient $\Sigma k_i = 0$ et $k_1 \leq ... \leq k_n$ et où π est un uniformisant de $\mathcal{O}_k$. On a alors la décomposition

$$SL_n(k) = KAK$$

avec de plus unicité de la composante en A que l'on note $a_g = diag(a_1(g), ..., a_n(g))$.

Remarquons que K agit par isométries sur $\mathbb{P}(k^n)$ pour la métrique d, et que tout $g \in PGL_n(k)$ est bi-Lipschitz. De plus si $g \in SL_n(k)$ on a $\|g\| = |a_1(g)|$ et $\left\|\Lambda^2 g\right\| = |a_1(g)a_2(g)|$ où la norme est la norme d'opérateur.

Définition 5.1. *Soit $r > 2\varepsilon > 0$. On dit que $g \in PGL_n(k)$ est ε-**contractant** s'il existe un point $v_g \in \mathbb{P}(k^n)$ et un hyperplan projectif H_g tel que g envoie presque tout l'espace projectif dans un voisinage de v_g, c'est-à-dire $\forall x\ d(x, H_g) \geq \varepsilon \Rightarrow d(gx, v_g) \leq \varepsilon$. On dit que g est (r, ε)-**proximal** s'il est ε-contractant et de plus $d(v_g, H_g) \geq r$. On dit que g est ε-très contractant (resp. (r, ε)-très proximal) si g et g^{-1} sont ε-contractant (resp. (r, ε)-proximal).*

Le lemme suivant montre qu'être ε-contractant se lit aisément sur la décomposition KAK.

Lemme 5.1. *Si g est ε-contractant alors $|\frac{a_2(g)}{a_1(g)}| \leq C_1\varepsilon$ et réciproquement si $|\frac{a_2(g)}{a_1(g)}| \leq \varepsilon$ alors g est $C_2\varepsilon$-contractant, où C_i $i = 1, 2$ sont des constantes positives dépendant de $\mathbb{P}(k^n)$ seulement.*

Démonstration. Comme K agit par isométries, il suffit de considérer le cas $g = a_g$, qui est clair. □

Remarque 5.1. *Si g est (r, ε)-proximal, alors on peut montrer que g est proximal au sens usuel, c'est-à-dire que g possède une unique valeur propre de module maximal. De plus la direction fixe de g correspondante sera ε-proche de v_g et la somme des sous-espaces caractéristiques des autres valeurs propres sera un hyperplan ε-proche de H_g.*

5.2. **Ping-pong.** On dit que le m-uplet $g_1, ..., g_m$ de $PGL_n(k)$ **joue au ping pong** sur $\mathbb{P}(k^n)$ s'il existe $r > 2\varepsilon > 0$ tels que les g_i sont (r, ε)-proximaux relativement aux points $v_{g_i^{\pm}}$ et aux hyperplans $H_{g_i^{\pm}}$ et si de plus on est dans la configuration géométrique suivante pour tous $i \neq j$

$$d(v_{g_i^{\pm}}, H_{g_j^{\pm}}) \geq r \tag{1}$$

Lemme 5.2. *(Lemme du ping pong) Si le m-uplet $g_1, ..., g_m$ joue au ping pong, alors les g_i sont les générateurs d'un sous-groupe libre F_m de $PGL_n(k)$.*

Démonstration. C'est clair : la condition géométrique sur les g_i est faite pour que tout mot réduit non trivial en les g_i agisse non trivialement sur $\mathbb{P}(k^n)$. □

Remarque 5.2. *Il y a d'autres façons de jouer au ping pong, i.e. on peut y jouer sur d'autres espaces, avec d'autres type d'éléments. Il est possible de formuler ainsi un lemme de ping pong un peu général qui s'applique à de nombreuses situations, à la notre en particulier. Soit X un ensemble et H et K deux sous-groupes de bijections de X tels qu'il existe une partie non-vide V de X ayant la propriété suivante : pour tous $h \in H\backslash\{1\}$ et $k \in K\backslash\{1\}$ on a $hkV \subsetneq V$. Alors, comme on le vérifie aisément, le sous-groupe de bijections de X engendré par H et K est isomorphe au produit libre $H * K$. Cette formulation s'applique au lemme 5.2 avec $m = 2$, mais aussi à l'exemple du lemme 3.1 du sous-groupe libre engendré par deux matrices unipotentes.*

5.3. **Partie géométrique de la preuve.** On montre ici que pour construire un m-uplet qui joue au ping pong, il suffit de deux ingrédients géométriques :

– des éléments ε-contractants avec ε aussi petit que l'on veut.
– une partie séparante finie.

Définition 5.2. *Une partie F de $PGL_n(k)$ est dite (m, r)**-séparante** si pour tout choix de m points $v_1, ..., v_m$ sur $\mathbb{P}(k^n)$ et de m hyperplans $H_1, ..., H_m$ il existe $f \in F$ tel que pour tout $s = \pm 1$ et pour tous i et j*

$$d(f^s v_i, H_j) \geq r$$

Proposition 5.1. *Soit $a_1, ..., a_m$ dans $PGL_n(k)$, F une partie $(2m, r)$-séparante finie, et γ une transformation ε-très contractante (avec $\varepsilon < \frac{r}{2C^4}$ où C est le max des constantes bi-Lipschitz des $f \in F$ et des a_i). Alors pour tout $i = 1, ..., m$ il existe h_i et g_i dans F tels que le m-uplet*

$$\gamma a_1 h_1, g_2 \gamma a_2 h_2, ..., g_m \gamma a_m h_m$$

joue au ping pong.

Démonstration. Remarquons que :

1) Si γ est ε-très contractant et si *bi-Lip*$(a) \leq C$ alors γa est $C\varepsilon$-très contractant et qu'on peut prendre $v_{\gamma a} = v_\gamma$ et $H_{\gamma a} = a^{-1} H_\gamma$.

2) Si γ est ε-très contractant alors $\exists f \in F$ tel que γf est $C\varepsilon$-très proximal.

3) On peut donc choisir $h_1 \in F$ tel que $\gamma a_1 h_1$ est $C^2\varepsilon$-très proximal. Maintenant supposons construits les $i_0 - 1$ premiers $g_i \gamma a_i h_i$ et indiquons comment choisir $h = h_{i_0}$ et $g = g_{i_0}$. Soit $v^\pm$ et $H^\pm$ les points et hyperplans de γa_{i_0} et $v_i^\pm$ et $H_i^\pm$ ceux des $g_i \gamma a_i h_i$ pour $i < i_0$. On aura $v_{i_0}^+ = gv^+$, $H_{i_0}^+ = h^{-1}H^+$, $v_{i_0}^- = h^{-1}v^-$ et $H_{i_0}^- = gH^-$. Pour être dans la configuration du ping pong (1) il faut vérifier les conditions suivantes : $d(gv^+, h^{-1}H^+) \geq r$, $d(h^{-1}v^+, gH^-) \geq r$, $d(gv^+, H_i^\pm) \geq r$, $d(v_i^\pm, gH^-) \geq r$, $d(v_i^\pm, h^{-1}H^+) \geq r$, et $d(h^{-1}v^-, H_i^\pm) \geq r$. On voit que l'on peut choisir $h \in F$ tel que les deux dernières conditions soient remplies. On peut ensuite choisir $g \in F$ qui verifie les conditions restantes. □

Notons que l'on a utilisé ici un élément très contractant γ. En fait, comme nous allons l'expliquer maintenant, on peut toujours en construire un à partir d'un élément contractant et d'une partie séparante.

Proposition 5.2. *Soit F une partie finie $(1,r)$-séparante et g un élément ε-contractant. Alors il existe $f \in F$ tel que gfg^{-1} est $C\varepsilon$-très contractant, où C est une constante dépendant de F et de $\mathbb{P}(k^n)$ seulement.*

Démonstration. On utilise la remarque suivante :

Lemme 5.3. *Soit $g \in SL_n(k)$. S'il existe un ouvert O de $\mathbb{P}(k^n)$ sur lequel g est ε-Lipschitz, alors g est $C\varepsilon$-contractant, où C est une constante ne dépendant que de $\mathbb{P}(k^n)$.*

Démonstration. Bien sûr il suffit de le démontrer pour $g = a_g$. On voit que cela doit entraîner $|\frac{a_2(g)}{a_1(g)}| \leq c\varepsilon$ pour une constante $c > 0$ et donc que g est $C\varepsilon$-contractant d'après le lemme 5.1. □

Remarquons aussi que pour tout $h \in SL_n(k)$ il existe toujours un ouvert O de $\mathbb{P}(k^n)$ sur lequel h est 2-Lipschitz : se ramener à $h = a_h$ et prendre par exemple un petit voisinage autour du premier vecteur de la base canonique. On applique cette remarque à g^{-1} et on obtient un point $v \in \mathbb{P}(k^n)$ et un petit ouvert O autour de v où g^{-1} est 2-Lipschitz. Il suffit alors de choisir $f \in F$ tel que $d(fv, H_g) \geq r$ et $d(f^{-1}v, H_g) \geq r$, car alors gfg^{-1} et son inverse $gf^{-1}g^{-1}$ sont $C\varepsilon$-Lipschitz sur O pour une constante C dépendant de f et de $\mathbb{P}(k^n)$ seulement. □

Remarque 5.3. *Notons que le sous-groupe libre obtenu à la proposition 5.1 est discret dans $PGL(k^n)$. On voit donc que pour obtenir un groupe libre et dense, il nous faut changer de corps et considérer des plongements dans d'autres corps locaux que le corps $\mathbb{R}$ d'origine.*

5.4. **Partie algébrique de la preuve.** Le but maintenant est de construire une représentation de Γ dans un $PGL_n(k)$ pour un corps local k à déterminer, pour laquelle on peut trouver dans Ω les deux ingrédients qu'il nous faut, à savoir des éléments ε-contractants et une partie finie séparante. On reprend les notations du théorème 4.2.

Proposition 5.3. *Soit $I \subseteq \mathbb{G}(R)$ une partie infinie, $\Omega \subseteq \mathbb{G}(K)$ une partie Zariski dense, alors il existe un corps local k, un plongement $K \hookrightarrow k$, et une représentation irréductible de $\mathbb{G}$ définie sur K, soit $\rho : \mathbb{G} \to GL(V)$ telle que*
- *Pour tout $\varepsilon > 0$ il existe $g \in I$ tel que $\rho(g)$ est ε-contractant.*
- *Pour tout $m \in \mathbb{N}$ il existe $r > 0$ et $F \subseteq \Omega$ une partie finie (m,r)-séparante.*

Démonstration. On peut supposer que $\mathbb{G} \subseteq \mathbb{GL}_n$ est défini sur $\mathbb{Q}$, donc sur K. Le corps local adéquat sera déterminé grâce au lemme suivant :

Lemme 5.4. *Soit R un anneau intègre de type fini et $I \subseteq R$ une partie infinie. Alors il existe un corps local k et un morphisme injectif $\sigma : R \hookrightarrow k$ tel que $\sigma(I)$ est non borné dans k.*

Nous retardons la preuve de ce lemme pour terminer d'abord celle de la proposition. Grâce au lemme, la partie I devient non bornée dans $GL_n(k)$, et donc $\{|a_1(g)|, g \in I\}$ est non borné dans k. Comme $\det g = 1$, il existe un indice i_0 tel que $\{|a_{i_0}(g)/a_{i_0+1}(g)|, g \in I\}$ est non borné. Quitte alors à remplacer k^n par

$\Lambda^{i_0} k^n$ et prendre la représentation de $\mathbb{G}$ correspondante, on peut supposer que $\{|a_1(g)/a_2(g)|, g \in I\}$ est non borné. Comme $car(k) = 0$, on peut décomposer $\Lambda^{i_0} k^n$ en somme directe de représentations irréductibles de $\mathbb{G}(k)$. Il y en a forcément une, disons ρ, pour laquelle $\{|a_1(\rho(g))/a_2(\rho(g))|, g \in I\}$ est non borné. On obtient donc la représentation qu'il nous faut et aussi une infinité d'éléments $g \in I$ tels que $\rho(g)$ est ε-contractant pour ε aussi petit que l'on veut. Reste à montrer l'existence de la partie séparante dans Ω.

Lemme 5.5. *Soit $\mathbb{G}$ un groupe algébrique Zariski connexe défini sur k et soit $\rho : \mathbb{G} \to GL(k^n)$ une représentation définie sur k et irréductible. Soit $\Omega \subseteq \mathbb{G}(k)$ une partie Zariski dense. Alors pour tout $m \in \mathbb{N}$ il existe $r > 0$ et $F \subseteq \Omega$ une partie finie (m, r)-séparante.*

Démonstration. Pour chaque $\gamma \in \Omega$, on note $M_\gamma = \{(v_i, H_i)_{i=1,...,m} \in (\mathbb{P}(k^n) \times \mathbb{P}(k^{n\vee}))^m$ tq $\exists i, j$ tq $\gamma v_i \in H_j$ ou bien $\gamma^{-1} v_i \in H_j\}$. Alors M_γ est un compact de $(\mathbb{P}(k^n) \times \mathbb{P}(k^{n\vee}))^m$. De plus je prétends que $\cap_{\gamma\in\Omega} M_\gamma$ est vide. En effet ce n'était pas vide, cela contredirait l'irréductibilité de ρ ou la Zariski connexité de $\mathbb{G}$ de la façon suivante. Si $(v_i, H_i)_{i=1,...,m} \in \cap_{\gamma\in\Omega} M_\gamma$ alors $\Omega \subseteq \cup_{i,j} F_{i,j}$ où $F_{i,j} = \{g \in \mathbb{G}(k), \rho(g^\pm) v_i \in H_j\}$. Mais chaque $F_{i,j}$ est un fermé algébrique de $\mathbb{G}$, et Ω est Zariski dense, donc $\mathbb{G}(k) \subseteq \cup_{i,j} F_{i,j}$. Chaque $F_{i,j}$ doit être un fermé propre sinon l'orbite $\rho(\mathbb{G}(k)) v_i$ est incluse dans un hyperplan, ce qui contredit l'irréductibilité. Enfin comme $\mathbb{G}$ est Zariski connexe, il n'est pas réunion finie de fermés algébriques propres. On a démontré que $\cap_{\gamma\in\Omega} M_\gamma$ est vide. Par compacité, il existe une partie finie $F \subseteq \Omega$ telle que $\cap_{\gamma\in F} M_\gamma$ est vide. Alors $\max_{f\in F} \min_{s=\pm,i,j} d(f^s v_i, H_j)$ est une fonction strictement positive et continue sur $(\mathbb{P}(k^n) \times \mathbb{P}(k^{n\vee}))^m$. Si $r > 0$ est son minimum, on voit que F est (m, r)-séparante. □

□

5.5. **Un lemme de Polya.** Pour compléter la preuve de l'alternative topologique, i.e. la proposition 4.1 via le théorème 4.2, il nous reste à indiquer comment démontrer le lemme 5.4. Grâce au théorème de normalisation de Noether, on peut voir que le lemme se ramène au cas où R est de la forme $\mathbb{Z}[\frac{1}{p_1}, ..., \frac{1}{p_k}, X_1, ..., X_m]$ où les p_i sont premiers. On peut alors procéder par récurrence sur le degré de transcendance et se ramener à deux cas essentiels : lorsque $R = \mathbb{Z}[\frac{1}{p_1}, ..., \frac{1}{p_k}]$ d'une part, et lorsque $R = \mathbb{Z}[X]$ d'autre part. Dans le premier cas R se plonge de façon discrète dans le produit $\mathbb{R} \prod_{i=1,...,k} \mathbb{Q}_{p_i}$ donc le lemme est clair. Nous traitons ci-dessous le cas $\mathbb{Z}[X]$ en détail. La preuve est analytique.

La preuve pour $\mathbb{Z}[X]$ repose sur le

Lemme 5.6. *Soit A une partie mesurable de $\mathbb{C}$ de mesure de Lebesgue $\lambda(A) \geq \pi e^2$. Alors pour tout polynôme unitaire $P \in \mathbb{C}[X]$ on a*

$$\int_A \log |P(z)| d\lambda(z) \geq d^\circ P$$

Remarque 5.4. *Ceci implique en particulier que $\lambda(\{z, |P(z)\} \leq 1\}) \leq \pi e^2$ pour tout P unitaire. Ce qui est important ici c'est que la borne est indépendante de*

P et en particulier du degré de P. En fait $\lambda(\{z, |P(z)\} \leq 1\}) \leq \pi$ pour tout P unitaire, c'est un fameux lemme de Polya.

Preuve que le lemme 5.6 entraîne le lemme 5.4 pour $R = \mathbb{Z}[X]$. On se donne une famille infinie $\{P_n(X)\}_{n\in I}$ dans $\mathbb{Z}[X]$. Il s'agit de trouver un nombre transcendant $\xi \in \mathbb{C}$ tel que la famille $\{P_n(\xi)\}_{n\in I}$ est non bornée.

Supposons d'abord que le degré des P_n est borné par disons d. Prenons $\xi_1, ..., \xi_{d+1}$ des nombres transcendants distincts. L'isomorphisme entre $\mathbb{C}_d[X]$ et $\mathbb{C}^{d+1}$ donné par $P \mapsto (P(\xi_1), ..., P(\xi_{d+1}))$ plonge $\mathbb{Z}_d[X]$ de façon discrète, donc pour au moins un i la famille $\{P_n(\xi_i)\}_{n\in I}$ est non bornée.

Supposons maintenant que les degrés sont non bornés. Quitte à diviser P_n par son coefficient dominant $a_n \in \mathbb{Z}$ on peut supposer que les $P_n \in \mathbb{C}[X]$ sont unitaires et forment une famille infinie. Soit pour chaque $C \geq 1$ le compact $K_C = \{z \in \mathbb{C}, |P_n(z)| \leq C$ pour tout $n\}$. Je prétends que $\lambda(\cup_{C\geq 1} K_C) \leq \pi e^2$. En effet si ce n'est pas le cas, alors $\lambda(K_C) > \pi e^2$ pour un certain C, ce qui entraîne par le lemme 5.6

$$\lambda(K_C) \log C \geq d^\circ P_n$$

pour tout n, ce qui contredit notre hypothèse que $d^\circ P_n$ est non borné. On peut donc choisir ξ transcendant en dehors de $\cup_{C\geq 1} K_C$, ce qu'il fallait démontrer. □

Preuve du lemme 5.6. La fonction $\log|z|$ est localement intégrable sur $\mathbb{C}$ et croissante en $|z|$. Il en résulte que $\int_A \log|z| d\lambda(z)$ est minimum quand A est un disque de rayon t centré en 0 tel que $\lambda(A) = \lambda(D(0,t)) = \pi t^2$. Si $\lambda(A) \geq \pi e^2$alors $t = e$ et ce minimum vaut $\pi e^2/2 \geq 1$ comme on le calcule aisément. Ainsi

$$\begin{aligned}
\int_A \log|P(z)| d\lambda(z) &= \sum_i \int_A \log|z - z_i| d\lambda(z) \\
&= \sum_i \int_{A+z_i} \log|z| d\lambda(z) \\
&\geq d^\circ P
\end{aligned}$$

□

6. Equidistribution des sous-groupes denses, problèmes ouverts

6.1. **Comptage.** Le problème de la répartition asymptotique d'un groupe dense dans un groupe de Lie reste un problème largement ouvert. Considérons la question suivante. On se donne G un groupe de Lie connexe et Γ un sous-groupe dense engendré par une partie finie Σ symétrique ($\Sigma = \Sigma^{-1}$) et contenant e. Sur Γ on peut considérer la fonction de longueur des mots $\ell(\gamma)$ qui donne le nombre minimal d'éléments de Σ nécessaires pour écrire γ comme produit de ces éléments. Pour tout ouvert borné U de G, disons tel que la frontière ∂U est de mesure négligeable, on peut se poser la question de déterminer l'asymptotique de

$$a_n(U) = \#\{\gamma \in \Gamma | \ell(\gamma) \leq n, \gamma \in U\}$$

quand $n \to +\infty$. Notamment, est-ce que $\frac{a_n(U)}{a_n(V)}$ a une limite positive lorsque U et V sont deux ouverts bornés ? La fonction $a_n(U)$ est appelée *fonction de croissance locale* du groupe dense Γ dans G.

Si G est nilpotent, on peut montrer, grâce à la théorie ergodique (l'équidistribution des flots sur les nilvariétés) que $a_n(U)$ est asymptotique à $n^\alpha vol(U)$ où α est un entier dépendant de G et de Γ seulement, et vol est une mesure de Haar sur G dont la constante multiplicative dépend de Γ et de Σ.

Si G est un groupe compact et Γ est libre, on peut aussi, grâce à la décomposition spectrale, montrer que l'on a équidistribution, au sens où $\frac{a_n(U)}{a_n(G)} \to vol(U)$ où vol est la mesure de Haar normalisée.

Cependant, si G est semisimple et non-compact, où même si G est le groupe des déplacements de $\mathbb{R}^3$, alors cela reste un problème ouvert. L'alternative de Tits topologique permet de montrer (voir plus bas, proposition 8.1) que

$$\liminf \frac{1}{n} \log a_n(U) > 0$$

dès que G n'est pas nilpotent, mais ne donne rien de plus précis.

6.2. **Vitesse d'équidistribution et trou spectral.** Soit G un groupe de Lie semisimple compact. Considérons les propriétés suivantes pour un couple $(a, b) \in G^2$:

i) Trou spectral, i.e. $\left\|\pi(\mu_{a,b})\right\| < 1$ où $\mu_{a,b} = \frac{1}{4}(\delta_a + \delta_{a^{-1}} + \delta_b + \delta_{b^{-1}})$ et π la représentation unitaire $\mathbb{L}^2_0(G)$. Autrement dit il n'existe pas de fonctions $\mathbb{L}^2$ sur G d'intégrale nulle qui soit presque invariante pour a et b à la fois.

ii) Vitesse exponentielle d'équidistribution, i.e. $\left\|\int_G f d\mu_{a,b}^{*n} - \int_G f\right\|_2 \leq \beta^n \|f\|_2$ pour tout $n \geq 0$ et $f \in \mathbb{L}^2(G)$ et pour un certain $\beta < 1$.

iii) Densité exponentielle : les mots en a et b deviennent ε-denses dans G en $O(|\log \varepsilon|)$ étapes, i.e. $\exists \delta < 1$ tel que $\{w(a, b), \ell(w) \leq n\}$ est δ^n-dense pour tout n assez grand, où ℓ est la longueur des mots.

iv) Condition diophantienne faible : peu de mots s'approchent exponentiellement vite de 1, i.e. $\exists \delta < 1$ et $\eta < 1$ tels que, en notant $B_{a,b}(n) = \{w(a, b), \ell(w) \leq n\}$, $\#B_{a,b}(n) \cap \{g \in G, d(g, 1) \leq \delta^n\} \leq \#B_{a,b}(n)^\eta$.

Il est facile de voir que $i) \Leftrightarrow ii)$ et que $ii) \Rightarrow iii) \Rightarrow iv)$. Aussi on remarque que la condition *iv*) est remplie dès que a et b ont des coefficients dans $\overline{\mathbb{Q}}$ dans une représentation matricielle fidèle de G, car dans ce cas tout $B_{a,b}(n) \setminus \{e\}$ reste δ^n-éloignée de 1 pour un $\delta < 1$. Cependant il est très difficile de trouver des couples (a, b) qui vérifient *i*). Les premiers exemples ont été constuits par Drinfeld dans $SU(2)$ et apparaissent comme des quaternions entiers. Dans ce cas le trou spectral peut se déduire de la conjecture de Ramanujan prouvée par Deligne. Récemment (2005) Bourgain et Gamburd ont montré de façon remarquable que pour $G = SU(2)$ on a l'équivalence entre ces quatre propriétés *i*) à *iv*). En particulier on obtient que tous les couples (a, b) à coordonnées algébriques ont un trou spectral. L'extension aux autres groupes compacts soulève des difficultés techniques supplémentaires.

C'est une question ouverte (due à Sarnak) de montrer *iv*) pour tout, ou même pour presque tout couple (a, b).

Remarque 6.1. *Avec peu d'effort, on peut obtenir une propriété plus faible que iii) à savoir la densité sous-exponentielle : on peut montrer, en considérant des* *commutateurs successifs, que $B(n)$ devient δ^{n^α}-dense pour un certain $\alpha < 1$. Mais ce n'est pas assez pour entraîner un trou spectral.*

7. Croissance des groupes

Soit Γ un groupe de type fini et $\Sigma = \{s_1, ..., s_n\}$ une partie génératrice finie et symétrique. Rappelons quelques définitions classiques. La donnée de Σ définit une distance invariante à gauche sur Γ, dite métrique des mots : $d(\gamma_1, \gamma_2) = \ell_\Sigma(\gamma_1^{-1}\gamma_2)$ où ℓ_Σ est la longueur minimale d'un mot en les s_i qui représente γ. On note $B_\Sigma(1, n)$ la boule de rayon n centrée en l'identité pour cette métrique : $B_\Sigma(1, n) = \{\gamma \in \Gamma, \ell(\gamma) \leq n\}$.

Soit $\gamma_\Sigma(n) = \#B_\Sigma(1, n)$ la *fonction de croissance* de (Γ, Σ). On dit que Γ est *à croissance exponentielle* si $S(\Sigma) := \lim \frac{1}{n} \log(\gamma_\Sigma(n))$ est strictement positif, et on dit que Γ est *à croissance polynomiale* si au contraire il existe des constantes positives C_1 et C_2 telles que $\gamma_\Sigma(n) \leq C_1 n^{C_2}$ pour tout n.

Remarque 7.1. *Ces notions sont bien définies pour le groupe Γ et indépendantes du choix de la partie génératrice Σ. Elles sont aussi stables par passage à un sous-groupe d'indice fini ou à un quotient par un groupe fini.*

La suite $\gamma_\Sigma(n)$ est sous-additive, donc la limite $S(\Sigma)$ est bien définie et est finie, quelque soit Γ.

Une des premières études de la fonction $\gamma_\Sigma(n)$ a été réalisée par Milnor et Wolf dans un article où ils démontrent notamment la dichotomie suivante :

Théorème 7.1. *(Milnor-Wolf) Soit Γ un groupe résoluble de type fini. Alors,*
a) Si Γ est virtuellement nilpotent, Γ est à croissance polynomiale.
b) Si Γ n'est pas virtuellement nilpotent, Γ est à croissance exponentielle.

Ci-dessous, nous donnons un argument pour montrer *a*) et au paragraphe 9 nous montrerons *b*) et en fait beaucoup plus.

Les groupes à croissance polynomiale sont relativement bien compris grâce aux théorèmes suivants :

Théorème 7.2. *(Gromov) Tout groupe de type fini à croissance polynomiale est virtuellement nilpotent.*

Théorème 7.3. *(Guivarc'h, Pansu) Pour tout groupe Γ virtuellement nilpotent, il existe un entier d tel que si Σ est une partie génératrice finie*

$$\lim_{n \to +\infty} \frac{\gamma_\Sigma(n)}{n^d} = C(\Sigma)$$

où $C(\Sigma)$ est une constante positive.

Le théorème de Milnor-Wolf suggère que cette dichotomie pourrait s'étendre à tous les groupes de type fini sans l'hypothèse résoluble. C'est une suggestion trop optimiste, et Grigorchuk a le premier construit un exemple de groupe de type fini à *croissance intermédiaire*. Ce groupe est de torsion et vérifie $n^{\frac{1}{2}} \preceq \log(\gamma_\Sigma(n)) \preceq n^{\frac{\log 31}{\log 32}}$. Cependant, aucun contre-exemple à présentation finie n'a été construit au jour d'aujourd'hui. Pour les groupes linéaires, en revanche, la dichotomie a bien lieu, comme on le déduit aisément de l'alternative de Tits et du théorème de Milnor-Wolf :

Corollaire de l'alternative de Tits : Si $\Gamma \leq GL_n(K)$ est de type fini, et K un corps quelconque, alors
– soit Γ est virtuellement nilpotent, donc à croissance polynomiale.
– soit Γ est à croissance exponentielle.

Preuve du a) du théorème 7.1. Soit Γ un groupe de type fini virtuellement nilpotent. Montrons qu'il est à croissance polynomiale. Quitte à passer à un sous-groupe d'indice fini, on peut supposer Γ nilpotent. Soit donc Γ un groupe nilpotent de classe r et à k générateurs. Alors Γ est un quotient du groupe nilpotent libre $H(r,k)$ de classe r à k générateurs. Il suffit donc de montrer que $H(r,k)$ est à croissance polynomiale. Ce groupe $H(r,k)$ est lui-même un réseau co-compact dans le groupe de Lie simplement connexe $\mathbb{H}(r,k)$ dont l'algèbre de Lie est l'algèbre de Lie nilpotente libre à k générateurs $e_1, ..., e_k$ et de classe r. Si d est une distance invariante à gauche sur $\mathbb{H}(r,k)$ alors il est clair que $B_\Sigma(1,n)$ est contenue dans la boule $B_d(1,Cn)$ de $\mathbb{H}(r,k)$ pour la distance d, où $C = \max_{s\in\Sigma} d(1,s)$. Soit U est un petit voisinage de l'identité dans $\mathbb{H}(r,k)$ tel que $U \subseteq B_d(1,C)$ et $\gamma U \cap U$ est vide pour tout $\gamma \in H(r,k) \backslash \{1\}$. Alors $\#B_\Sigma(1,n) \leq \frac{vol B_d(1,Cn+C)}{vol(U)}$. Donc il suffit de montrer que le volume de $B_d(1,n)$ croît au plus polynomialement. On n'a fait aucune hypothèse sur la distance invariante à gauche pour l'instant. On va prendre pour d une métrique de Carnot-Carathéodory d_{cc} sur $\mathbb{H}(r,k)$. Cette métrique est la métrique sous-riemannienne invariante à gauche induite par un produit scalaire sur la première strate V_1, i.e. le sous-espace vectoriel de l'algèbre de Lie de $\mathbb{H}(r,k)$ engendré par les générateurs e_i. Cette métrique est homogène par rapport aux dilatations δ_t qui sont les automorphismes de $\mathbb{H}(r,k)$ définis par $\delta_t(e_i) = te_i$ pour chaque i, c'est-à-dire que

$$d_{cc}(\delta_t(x), \delta_t(y)) = td_{cc}(x,y).$$

Ainsi $B_{d_{cc}}(1,n) = \delta_n(B_{d_{cc}}(1,1))$ et le volume de $B_{d_{cc}}(1,n)$ égale $Jac(\delta_n)\cdot vol(B_{d_{cc}}(1,1))$. Mais, clairement, le jacobien $Jac(\delta_n)$ égale n^d où $d = \sum i \dim V_i$ où V_i est la i-ème strate, i.e. le sous-espace vectoriel engendré par les commutateurs d'ordre i. Donc $vol(B_{d_{cc}}(1,n))$ est à croissance polynomiale. $\square$

8. Feuilletages et croissance locale

Dans ce paragraphe, on décrit une application de l'alternative topologique à la théorie des feuilletages riemanniens. Tout comme l'alternative de Tits permet de montrer la dichotomie polynomial/exponentiel pour la croissance des groupes linéaires, l'alternative topologique admet un corollaire du même ordre pour la croissance des feuilles dans les feuilletages riemanniens.

8.1. **Feuilletages riemanniens.** Soit M une variété compacte connexe et $\mathcal{F}$ un feuilletage sur M. Formellement $\mathcal{F}$ est défini à partir de la donnée d'un recouvrement ouvert $(U_i)_i$ de M et de submersions locales $f_i : U_i \to f_i(U_i)$ où $f_i(U_i)$ est un ouvert d'une variété fixée T, dite *variété transverse*. Les fibres de f_i dans chaque U_i s'appellent *les plaques* de $\mathcal{F}$ dans U_i et *les feuilles* de $\mathcal{F}$ sont les sous-variétés immergées connexes de M qui coincident localement avec les plaques. Les changements de cartes $h_{ij} : f_j(U_i \cap U_j) \to f_i(U_i \cap U_j)$ sont des difféomorphismes.

On se donne maintenant une métrique riemannienne sur M. Etant donnée une feuille $\mathcal{F}_x$ qui passe par $x \in M$, on peut parler de *la croissance de* $\mathcal{F}_x$ en considérant la fonction de croissance $\gamma_x(t) = vol_d(B_{\mathcal{F}_x}(x,t))$ où vol_d est le volume riemannien pour la métrique riemannienne induite sur la feuille $\mathcal{F}_x$. On dit que la feuille $\mathcal{F}_x$ est à croissance exponentielle (resp. polynomiale) si $\gamma_x(t)$ croît exponentiellement vite avec t (resp. polynomialement).

Remarque 8.1. *On vérifie aisément que $\gamma_x(t) \leq C\rho^t$ pour un certain $\rho > 1$ et $C > 0$, i.e. comme pour les groupes, la croissance est au plus exponentielle. De plus on vérifie aussi que le type de croissance (par exemple exponentiel ou polynomial) ne dépend pas du choix de la métrique riemannienne d sur la variété compacte M, ni du choix du point x sur la feuille $\mathcal{F}_x$, mais ne dépend que de la feuille.*

On va s'intéresser à une classe de feuilletages dits feuilletages riemanniens :

Définition 8.1. *On dit que le feuilletage $\mathcal{F}$ est* ***riemannien****, si T est une variété riemannienne et les changements de cartes h_{ij} sont des isométries locales de T. On dit que $\mathcal{F}$ est un* ***feuilletage de Lie,*** *si $T = G$ est un groupe de Lie simplement connexe et les changements de cartes h_{ij} sont localement des translations à gauche par un élément fixe de G.*

De manière équivalente, $\mathcal{F}$ est riemannien si on peut trouver une métrique riemannienne sur M pour laquelle les feuilles de $\mathcal{F}$ restent localement équidistantes. Clairement, tout feuilletage de Lie est aussi riemannien, car on peut trouver une métrique invariante à gauche sur G.

Le théorème suivant est l'analogue feuilleté de la dichotomie de croissance pour les groupes linéaires de type fini. Sa preuve repose sur l'alternative topologique comme nous l'expliquons plus bas.

Théorème 8.1. *Soit M une variété compacte connexe et $\mathcal{F}$ un feuilletage sur M.*
- *Supposons que $\mathcal{F}$ est un G-feuilletage de Lie. Si G n'est pas nilpotent, les feuilles de $\mathcal{F}$ sont à croissance exponentielle ; si G est nilpotent elles sont à croissance polynomiale.*
- *Supposons que $\mathcal{F}$ est riemannien. Si l'algèbre de Lie structurale $\mathfrak{g}$ de $\mathcal{F}$ n'est pas nilpotente, les feuilles de $\mathcal{F}$ sans holonomie (elles forment un G_δ-dense dans M) sont à croissance exponentielle ; si $\mathfrak{g}$ est nilpotente, toutes les feuilles sont à croissance polynomiale.*

Remarque 8.2. *Si on connaissait un groupe de présentation finie à croissance intermédiaire qui se plonge dans $Diff(T)$ où T est une variété compacte connexe, alors on pourrait aisément construire, par suspension, un feuilletage (non riemannien !) sur une variété compacte dont les feuilles sont à croissance intermédiaire.*

Exemple 8.1. *Voici quelques exemples de feuilletages de Lie.*

- *On prend le tore* $M = \mathbb{R}^2/\mathbb{Z}^2$ *et le feuilletage par des droites parallèles de pente* $\alpha \notin \mathbb{Q}$. *Le groupe de Lie ici est* $\mathbb{R}$.
- *Soit* G *un groupe de Lie semisimple compact. On prend* $M = (\mathbb{H}^2 \times G)/\Gamma$ *où* $\Gamma \simeq \pi_1(\Sigma_g)$ *le groupe fondamental d'une surface orientable compacte de genre* g. *On fait agir* Γ *sur le plan hyperbolique* $\mathbb{H}^2$ *de façon discrète et co-compacte et on fait agir* Γ *sur* G *par translations à gauche grâce à un homomorphisme* $\rho : \Gamma \to G$ *d'image dense (d'après le paragraphe 3.2, on peut choisir* ρ *fidèle ; on peut aussi par exemple envoyer* Γ *sur un groupe libre dense de* G*). Les feuilles sont les images des* $\mathbb{H}^2 \times \{g\}$ *dans* M. *C'est un* G*-feuilletage de Lie dont les feuilles sont denses et isométriques à la surface de volume infini* $\mathbb{H}^2/Ker(\rho)$.
- *Soit* H *et* G *des groupes de Lie semisimples sans facteurs compacts tels qu'il existe un réseau* Γ *de* $H \times G$ *irréductible et co-compact. Alors on prend* $M = (H \times G)/\Gamma$ *et le feuilletage dont les feuilles sont les images des* $H \times \{g\}$ *dans* M. *C'est un* G*-feuilletage de Lie à feuilles denses. Par exemple, on peut prendre* $H = SO(q_{\alpha_1}, \mathbb{R})$, $G = SO(q_{\alpha_2}, \mathbb{R})$ *et* $\Gamma = SO(q_\alpha, \mathcal{O}_{\mathbb{Q}(\alpha)})$ *où* $q_\alpha = x^2 + y^2 + \alpha z^2$ *où* α *est de degré* 3 *sur* $\mathbb{Q}$ *avec deux conjugués réels négatifs* α_1 *et* α_2 *et un autre positif.*

Exemple 8.2. *Voici un exemple de feuilletage riemannien qui n'est pas de Lie. On considère* $M = (\mathbb{H}^2 \times S^3)/\Gamma$ *où* S^3 *est la sphère de dimension* 3 *et* $\Gamma \simeq \pi_1(\Sigma_g)$ *agit par rotation sur les grands cercles de* S^3, *i.e. on a* $\rho : \Gamma \to SO(3)$ *(que l'on prend fidèle) et on voit* $SO(3)$ *agissant sur* $S^3 = SO(4)/SO(3)$. *Clairement cette action préserve la métrique sur* S^3 *donc le feuilletage obtenu (dont les feuilles sont les images des* $\mathbb{H}^2 \times \{x\}$ *dans* M*) est riemannien. Il y a trois types de feuilles : la feuille générique est isométique à* $\mathbb{H}^2$, *les feuilles passant par les points de* S^3 *fixés par un élément* γ *de* Γ *sont isométriques à* $\mathbb{H}^2/\langle\gamma\rangle$, *et il y a aussi deux feuilles compactes isométriques à* Σ_g *aux deux poles de* S^3.

Dans le théorème ci-dessus, le b) se déduit du a) grâce au théorème de structure des feuilletages riemanniens :

Théorème 8.2. *(Molino) Soit* $\mathcal{F}$ *un feuilletage riemannien sur une variété compacte connexe* M. *Soit* O_M *le fibré des repères transverses orthonormaux et* $\mathcal{F}_0$ *le feuilletage relevé à* O_M *(les feuilles de* $\mathcal{F}$ *et* $\mathcal{F}_0$ *ont la même dimension). Alors*

- *Les feuilles sans holonomie de* $\mathcal{F}$ *(donc presque toute feuille) sont isométriques à leur relevé dans* $\mathcal{F}_0$.
- *Le feuilletage* $\mathcal{F}_0$ *sur* O_M *est transversalement parallélisable. L'adhérence d'une feuille est une sous-variété.*
- *Il exite un unique groupe de Lie simplement connexe* G *tel que la restriction de* $\mathcal{F}_0$ *à l'adhérence d'une feuille quelconque est un* G*-feuilletage de Lie à feuilles denses.*

L'algèbre de Lie $\mathfrak{g}$ de G s'appelle a*lgèbre de Lie structurale* du feuilletage riemannien. Elle est déterminée de façon unique en termes du feuilletage. Plus précisément, en se restreignant à l'adhérence d'une feuille, $\mathfrak{g}$ coincide avec le quotient

$N(\mathfrak{p})/\mathfrak{p}$ où $\mathfrak{p}$ est la sous-algèbre des champs de vecteurs parallèles aux feuilles et $N(\mathfrak{p})$ son normalisateur dans l'algèbre de Lie de tous les champs de vecteurs ($N(\mathfrak{p})$ correspond aux champs de vecteurs dont la partie transverse est localement constante le long d'une feuille).

8.2. **Croissance dans les feuilletages de Lie.** Nous allons maintenant démontrer le théorème 8.1 pour les feuilletages de Lie. Faisons d'abord quelques observations sur la structure de ceux-ci.

Soit $\mathcal{F}$ un G-feuilletage de Lie sur une variété compacte connexe M, où G est un groupe de Lie simplement connexe. Soit $\widetilde{M}$ le revêtement universel. Alors les objets suivants sont bien définis :

- L'application développante $D : \widetilde{M} \to G$
- La représentation d'holonomie $\rho : \pi_1(M) \to G$ et le groupe d'holonomie $\Gamma = \operatorname{Im} \rho$.

On fixe un point base x_0 dans $\widetilde{M}$. La développante s'obtient en suivant la projection sur la transversale tout le long d'un chemin partant de x_0. Elle est bien définie car les changements de cartes sont localement des translations à gauche par un élément fixé de G. On définit alors $\rho(\gamma) = D(\gamma \cdot x_0)$ et on vérifie qu'il s'agit d'un morphisme de groupe et que D est ρ-équivariante.

On vérifie maintenant les points suivants :

(1) Les fibres de D coincident avec les feuilles du relevé $\widetilde{\mathcal{F}}$ du feuilletage $\mathcal{F}$ au revêtement universel $\widetilde{M}$. Dans un sens c'est évident, dans l'autre il s'agit d'homotoper dans G vers le lacet trivial l'image d'un chemin dans $\widetilde{M}$ en gardant les extrémités dans la même feuille.

(2) $\mathcal{F}$ est transversalement parallélisable, c'est-à-dire qu'il existe $q = \dim G$ champs de vecteurs $Z_1, ..., Z_q$ sur M tels que leurs projections transverses $\overline{Z_1}, ..., \overline{Z_q}$ forment, en chaque point, une base de l'espace tangent transverse. En effet, il suffit de considérer une base de l'algèbre de Lie de G, c'est-à-dire des champs de vecteurs invariants à gauche sur G, puis de la tirer en arrière dans M. En particulier, le groupe $Aut(\mathcal{F})$ des difféomorphismes de M qui preservent le feuilletage (globalement) agit transitivement sur M, et les feuilles sont toutes difféomorphes.

(3) Si $x \in M$ et x est dans U_i, un ouvert de carte, alors pour tout $y \in U_i$, les feuilles $\mathcal{F}_x$ et $\mathcal{F}_y$ coincident si et seulement si $f_i(x) = \gamma \cdot f_i(y)$ pour un certain $\gamma \in \Gamma$. En particulier une (toute) feuille de $\mathcal{F}$ est dense ssi Γ est dense dans G.

(4) Soit N le revêtement galoisien de M de groupe d'automorphismes Γ. Alors D passe au quotient et induit $\overline{D} : N \to G$, de plus on peut trouver une métrique riemannienne Γ-invariante sur N telle que $\overline{D}$ devienne une submersion riemannienne (on munit G d'une métrique invariante à gauche). Le feuilletage $\mathcal{F}$ se relève à N et chaque feuille est une fibre de $\overline{D}$ qui est isométrique à la feuille de M qu'elle relève.

(5) Les feuilles dans N sont totalement géodésiques et sur une même feuille, la métrique riemannienne induite et la restriction à la feuille de la distance dans N coincident.

Supposons maintenant que $\mathcal{F}$ est à feuilles denses. Alors Γ est dense dans G. Il y a une condition nécessaire importante que Γ vérifie :

Définition 8.2. *Soit Γ un sous-groupe dense d'un groupe de Lie G engendré par une partie finie Σ. On dit que Γ est **compactement engendré** s'il existe un voisinage compact U de l'identité et un compact K de G tel que tout $\gamma \in \Gamma \cap U$ s'écrit $\gamma = s_1 \cdot ... \cdot s_n$ avec les $s_i \in \Sigma$ et $s_1 \cdot ... \cdot s_i \in K$ pour chaque $i \leq n$.*

Remarquons que si Γ est compactement engendré alors la propriété reste vraie pour tout autre voisinage compact U' de l'identité et pour tout autre partie génératrice Σ'.

Lemme 8.1. *Soit $(M, \mathcal{F})$ un G-feuilletage de Lie à feuilles denses et Γ son groupe d'holonomie. Alors Γ est compactement engendré.*

Démonstration. On prend pour U une boule centrée en l'identité. Si $\gamma \in \Gamma \cap U$, on choisit un chemin dans U qui relie γ à l'identité et on le relève dans $\widetilde{M}$ par D en partant de x_0. Ce relevé reste à distance bornée (au plus $diam(U)$) de la feuille $\mathcal{F}_{x_0}$. Comme le π_1 de M agit co-compactement sur $\widetilde{M}$ on peut trouver des générateurs $s_1, ..., s_n$ de $\pi_1(M)$ tels que $\rho(s_1 \cdot ... \cdot s_n) = \gamma$ et $s_1 \cdot ... \cdot s_i \cdot x_0$ reste à distance bornée (au plus $diam(F)$ où F est un domaine fondamental) du chemin relevé pour chaque i, ce qui implique que $\rho(s_1 \cdot ... \cdot s_i)$ reste à distance bornée dans G. □

Remarque 8.3. *Ainsi tout sous-groupe dense ne peut pas nécessairement se réaliser comme groupe d'holonomie. Par exemple, on vérifie aisément qu'un groupe libre et dense n'est pas compactement engendré.*

La croissance des feuilles est comparable à la croissance locale de Γ dans G (voir le paragraphe 6.1), c'est le contenu du lemme suivant. On fixe un système de générateurs de Γ, ce qui permet de définir la longueur des mots $\ell(\gamma)$.

Lemme 8.2. *Il existe des constantes c_1 et c_2 strictement positives telles que pour tout entier n, et $x \in M$,*

$$c_1 a_{c_1 n}(c_1) \leq vol(B_{\mathcal{F}_x}(n)) \leq c_2 a_{c_2 n}(c_2) \tag{2}$$

où $B_{\mathcal{F}_x}(n)$ est la boule de rayon n centrée en x dans la feuille $\mathcal{F}_x$ et $a_n(t) = \#\{\gamma \in \Gamma \cap B_G(t), \ell(\gamma) \leq n\}$ où $B_G(t)$ est la boule de rayon t centrée en l'identité dans G.

Démonstration. D'après le point (5) ci-dessus, $B_{\mathcal{F}_x}(n)$ est isométrique à $B_N(\overline{x}, n) \cap \overline{\mathcal{F}}_{\overline{x}}$ où $\overline{\mathcal{F}}$ est le feuilletage relevé au revêtement N et $\overline{x}$ est au-dessus de x dans N. Comme Γ agit co-compactement sur N, $B_N(\overline{x}, n) \cap \overline{\mathcal{F}}_{\overline{x}}$ est recouverte par la réunion des $B_N(\gamma\overline{x}, r)$ tels que $d_N(\gamma\overline{x}, \overline{\mathcal{F}}_{\overline{x}}) \leq r$ et $d_N(\gamma\overline{x}, \overline{x}) \leq n + r$, où r est le diamètre d'un domaine fondamental. Mais $d_N(\gamma\overline{x}, \overline{\mathcal{F}}_{\overline{x}}) \leq r$ équivaut à $\gamma \in B_G(r)$ et $d_N(\gamma\overline{x}, \overline{x}) \leq n + r$ entraîne $\ell(\gamma) \leq c_2 n$ pour une constante c_2 ne dépendant que de r et de la partie génératrice de Γ. Quitte changer c_2 on peut supposer que $c_2 > r$ et c_2 est plus grand que le volume d'une feuille quelconque restreinte au domaine fondamental. D'où la borne supérieure dans (2). La borne inférieure se traite de façon similaire. □

Corollaire 8.1. *Le type de croissance d'une feuille de M est le même que celui de $\{a_n(t)\}_n$ (i.e. croissance locale de Γ dans G).*

Dans l'énoncé suivant, on détermine le type de croissance locale en ayant recours à l'alternative topologique (Théorème 4.1, cas $k = \mathbb{R}$).

Proposition 8.1. *Soit Γ un sous-groupe dense de type fini du groupe de Lie connexe G.*

Si G n'est pas nilpotent alors la croissance locale de Γ est exponentielle (i.e. $a_n(t)$ croît exponentiellement pour chaque $t > 0$).

Si G est nilpotent elle est polynomiale (i.e. $a_n(t) \leq C_t n^d$ pour un certain d).

Démonstration. On fixe $t > 0$. Il est facile de trouver un nombre fini de points $a_1, ..., a_k$ de $B_G(t)$ ayant la propriété suivante : pour tout $x \in B_G(t)$ il existe au moins deux indices $i \neq j$ tels que xa_i et xa_j soient dans $B_G(t)$. Supposons G non-résoluble. D'après l'alternative topologique (et la remarque 4.3), on peut perturber, de façon aussi faible que l'on veut, les a_i en des éléments γ_i de Γ tels qu'ils engendrent un sous-groupe libre. En prenant une perturbation suffisamment faible, on peut supposer que les γ_i vérifient aussi la propriété des a_i. Ainsi on peut trouver au moins 2^n mots distincts de longueur n en les γ_i qui sont dans $B_G(t)$; on multiplie à chaque étape par deux γ_i différents tout en restant dans $B_G(t)$. Ainsi $a_n(t)$ croît exponentiellement vite avec n. Si G est résoluble et non nilpotent, on peut montrer une propriété analogue à l'alternative topologique, i.e. on peut perturber de sorte que l'on obtienne dans Γ des générateurs d'un semi-groupe libre. Si G est nilpotent, Γ aussi, et la croissance $\{\gamma \in \Gamma, \ell(\gamma) \leq n\}$ est bornée par un polynôme. □

Cela conclut la preuve du théorème 8.1 pour les feuilletages de Lie.

9. Croissance uniforme

La suite de ces notes est consacrée à la croissance exponentielle uniforme et à l'alternative de Tits uniforme. Nous donnons une preuve complète de la croissance exponentielle uniforme pour les groupes linéaires et du trou entropique pour les groupes discrets. Dans ce paragraphe, après avoir énoncé les résultats, nous traiterons le cas des groupes résolubles de type fini.

Soit Γ un groupe de type fini. On introduit les notations suivantes. Etant donné une partie génératrice finie et symétrique Σ de Γ, on note $d^+(\Sigma)$ le plus petit entier n tel que Σ^n contienne deux éléments a et b qui engendrent un semigroupe libre (i.e. tous les mots distincts en a et b donnent lieu à des éléments distincts de Γ). De même, on note $d(\Sigma)$ le plus petit entier n tel que Σ^n contienne a et b qui engendrent un sous-groupe libre (i.e. tout mot réduit en a, b et leurs inverses est non trivial dans Γ).

De plus, on note $d_\Gamma^+ = \sup d^+(\Sigma)$ et $d_\Gamma = \sup d(\Sigma)$ où le sup est pris sur toutes les parties génératrices de Γ. Les quantités d_Γ^+ et d_Γ sont appelées respectivement diamètre de semi-liberté et **diamètre de liberté** du groupe Γ. D'autre part, on pose $S(\Sigma) = \lim \frac{1}{n} \log \#\Sigma^n$ et $S_\Gamma = \inf S(\Sigma)$. Le nombre S_Γ est appelé **entropie algébrique** du groupe Γ. On dit que Γ est *à croissance exponentielle uniforme* si $S_\Gamma > 0$.

Si $d^+(\Sigma)$ est fini, alors $\Sigma^{d^+(\Sigma)n}$ contient au moins 2^n éléments (les mots distincts de longueur n en a et b). Par suite, on a

$$\begin{aligned} S(\Sigma) &\geq \frac{\log 2}{d^+(\Sigma)} \\ S_\Gamma &\geq \frac{\log 2}{d_\Gamma^+} \end{aligned}$$

En particulier, si d_Γ^+ est fini alors Γ est à croissance exponentielle uniforme. Nous allons voir que pour les groupes résolubles et pour les groupes linéaires la réciproque est aussi vraie. Cependant elle est fausse en général : par exemple les grands groupes de Burnside ont un d^+ infini (ils sont de torsion) mais sont à croissance exponentielle uniforme (Osin [32]).

Théorème 9.1. *(Croissance uniforme pour les groupes linéaires) Si $\Gamma \leq GL_n(K)$ est de type fini, où K est un corps quelconque. Alors soit Γ est virtuellement nilpotent, soit d_Γ^+ est fini.*

Remarque 9.1. *Un contre-exemple célèbre de Wilson (voir* [43]*) montre qu'il existe des groupes de type fini à croissance exponentielle tels que $S_\Gamma = 0$.*

Théorème 9.2. *(Trou entropique) Pour tout entier $d \geq 1$, il existe une constante $c(d) > 0$ telle que $d_\Gamma^+ \leq c(d)$ pour tout sous-groupe discret Γ de $GL_n(\mathbb{C})$ qui n'est pas virtuellement nilpotent.*

Théorème 9.3. *(Croissance uniforme pour les groupes résolubles) Si Γ est un groupe résoluble de type fini, alors soit Γ est virtuellement nilpotent, soit d_Γ^+ est fini. Plus précisément si d_Γ^+ est fini, alors il existe un sous-groupe d'indice fini Γ_0 de Γ tel que $d_{\Gamma_1}^+ \leq 3$ pour tout sous-groupe d'indice fini Γ_1 de Γ_0.*

Ce dernier résultat pour les groupes résolubles est une amélioration du théorème de Milnor-Wolf cité ci-dessus (théorème 7.1). En voici une preuve par un argument direct de ping pong.

Preuve du théorème 9.3. Le point clé de la preuve est le fait suivant, propre aux groupes résolubles (nous renvoyons à [4] pour une preuve). Pour un corps K, on note

$$\mathbb{A}(K) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in K^\times, b \in K \right\}$$

Proposition 9.1. *(J. Groves, P. Hall) Si Γ est résoluble et non virtuellement nilpotent, alors un existe un corps K et un homomorphisme $\rho : \Gamma \to \mathbb{A}(K)$ tel que $\rho(\Gamma)$ n'est pas virtuellement nilpotent.*

On peut donc supposer que Γ est lui-même un sous-groupe de type fini non virtuellement nilpotent de $\mathbb{A}(K)$. Les éléments de $\mathbb{A}(K)$ sont les transformations affines de la droite, c'est-à-dire soit des homothéties centrées en un point, soit des translations. Pour construire des éléments qui engendrent un semigroupe libre, nous allons jouer au ping pong sur la droite affine. Plus précisément, on a :

Lemme 9.1. *(Lemme du ping) Soit k un corps local et A et B deux homothéties de k de centres $p \neq q$ et de rapport α et β.*

Si $k = \mathbb{R}$ ou $\mathbb{C}$ et si $|\alpha| \leq \frac{1}{3}$ et $|\beta| \leq \frac{1}{3}$ alors A et B engendrent un semigroupe libre.

Si k est non archimédien et si $|\alpha| < 1$ et $|\beta| < 1$ alors A et B engendrent un semigroupe libre.

Démonstration. Si U et V sont les boules ouvertes de rayon $|p-q|/2$ (resp. $|p-q|$ dans le cas non archimédien) centrées en p et en q respectivement, alors U et V sont disjointes, mais $U \cup V$ est envoyé dans U par A et dans V par B. Il en résulte que deux mots distincts en A et B agissent différemment sur la droite. $\square$

Pour exhiber ces joueurs A et B, il nous faut plonger K de façon adéquate dans un corps local, grâce au lemme suivant, qui est standard. Un élément $\alpha \in K$ est un entier algébrique s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$ (ou dans $\mathbb{F}_p$ en caractéristique positive).

Lemme 9.2. *Soit K un corps de type fini.*

a) Soit $\alpha \in K$. Si α^{-1} n'est pas un entier algébrique, alors il existe un corps local non archimédien k et un plongement $\sigma : K \hookrightarrow k$ tel que $|\sigma(\alpha)| < 1$.

b) Il existe $\varepsilon_0 = \varepsilon_0(K) > 0$ tel que si $\alpha \in K$ et α^{-1} sont des entiers algébriques tels que $|\log|\sigma(\alpha)|| < \varepsilon_0$ pour tout plongement $\sigma : K \hookrightarrow k$ dans un corps local archimédien k, alors α est une racine de l'unité.

Finissons la preuve du théorème. Considérons le sous-groupe Q de $K^\times$ engendré par les parties multiplicatives $a(\gamma)$ de $\gamma \in \Gamma$.

Si Q n'est pas contenu dans le groupe des unités algébriques de K, alors il existe $s \in \Sigma$ tel que $a(s)$ ou $a(s)^{-1}$ n'est pas un entier algébrique. Par le lemme, on peut plonger K dans un corps local non archimédien de sorte que $|a(s)| \neq 1$. Ainsi s est une homothétie de k. Le stabilisateur d'un point de k est abélien. Il existe donc un autre élément x de la partie génératrice Σ tel que xsx^{-1} et s engendrent un semigroupe libre (d'après le lemme du ping ci-dessus).

Si Q est constitué d'unités algébriques, il existe $s \in \Sigma$ qui n'est pas une racine de l'unité (sinon Q serait fini et Γ virtuellement abélien). Par le lemme ci-dessus, on peut donc plonger K dans un corps local archimédien k tel que $|\log|a(s)|| > \varepsilon_0$. On choisit n_0 tel que $n_0\varepsilon_0 > \log 3$. D'après le lemme du ping (et quitte à changer s en s^{-1}) s^{n_0} et $xs^{n_0}x^{-1}$ jouent au ping et engendrent un semi-groupe libre. Donc $d^+(\Sigma) \leq 3n_0$.

Pour contruire le groupe Γ_0 il suffit de prendre l'image réciproque du sous-groupe d'indice fini Q^{n_0} de Q. $\square$

Remarque 9.2. *Remarquons que si l'on peut faire le plongement dans un corps non archimédien, alors on obtient une borne universelle* $d^+ \leq 3$. *C'est ce qui se passe pour les groupes métabéliens non polycycliques. En revanche, il n'y a pas de borne supérieure universelle pour tous les groupes résolubles, même pour les sous-groupes de* $\mathbb{A}(\mathbb{C})$.

9.1. **Alternative uniforme, croissance des sphères.** Au paragraphe précédent nous ne nous sommes intéressés qu'aux semigroupes libres. Le théorème suivant construit un sous-groupe libre et améliore ainsi l'énoncé original de l'alternative de Tits.

Théorème 9.4. *(Alternative de Tits uniforme) Si* $\Gamma \leq GL_n(K)$ *est de type fini, où* K *est un corps quelconque, alors soit* Γ *est virtuellement résoluble, soit* d_Γ *est fini.*

Nous ne démontrerons pas ce théorème dans ces notes, mais nous donnerons une démonstration du théorème 9.1 dont la preuve est une première étape vers celle de l'alternative uniforme. Nous renvoyons le lecteur à [10].

Concernant la croissance, l'alternative uniforme admet le corollaire suivant, qui montre que les sphères (et non plus seulement les boules) ont une croissance exponentielle uniforme.

Corollaire 9.1. *Soit* $\Gamma \leq GL_n(K)$ *de type fini non virtuellement résoluble. Alors il existe une constante* $c = c(\Gamma) > 0$ *telle que pour toute partie génératrice* Σ *finie symétrique et pour tout* n,

$$\#(\Sigma^{n+1} \backslash \Sigma^n) \geq c(1+c)^n \# \Sigma$$

Ce corollaire est un cas particulier du suivant (pour les fonctions indicatrices des boules), qui montre que les groupes linéaires non virtuellement résolubles sont *uniformément non moyennables* (voir [2] et [39]).

Corollaire 9.2. *Soit* $\Gamma \leq GL_n(K)$ *de type fini non virtuellement résoluble. Alors il existe* $\varepsilon_0 = \varepsilon_0(\Gamma) > 0$ *tel que pour tout* $f \in \ell^2(\Gamma)$, *et pour toute partie génératrice finie* Σ *de* Γ, *on a*

$$\max_{s \in \Sigma} \|s \cdot f - f\|_2 \geq \varepsilon_0 \|f\|_2$$

$\ell^2(\Gamma)$ *est la représentation régulière gauche de* Γ.

Démonstration. Soit a et b dans Σ^{d_Γ} qui engendrent un sous-groupe libre H. La restriction de $\ell^2(\Gamma)$ à H se décompose, le long des classes à droite de H, en sous-représentations de H isomorphes à la régulière gauche de H, $\ell^2(H)$:

$$\ell^2(\Gamma) = \bigoplus_{H \backslash \Gamma} V_{H\gamma}$$

où $V_{H\gamma}$ est l'espace des fonctions ℓ^2 à support dans $H\gamma$. Comme H est un groupe libre F_2, il est non moyennable et il existe donc $\varepsilon_{F_2} > 0$ tel que pour tout $f \in \ell^2(H)$, soit $\|a \cdot f - f\|_2 \geq \varepsilon_{F_2} \|f\|_2$ soit $\|b \cdot f - f\|_2 \geq \varepsilon_{F_2} \|f\|_2$. En décomposant $f = \sum f 1_{H\gamma}$ on obtient

$$\|a \cdot f - f\|_2^2 + \|b \cdot f - f\|_2^2 \geq \varepsilon_{F_2}^2 \|f\|_2^2$$

Mais a et b sont dans Σ^{d_Γ}, d'où

$$\max_{s\in\Sigma} \|s\cdot f - f\|_2^2 \geq \frac{\varepsilon_{F_2}^2}{2d_\Gamma}\|f\|_2^2$$

$\square$

10. Déplacement minimal sur les espaces symétriques

Dans ce paragraphe, nous développons quelques préliminaires à la preuve des théorèmes 9.1 et 9.2. La stratégie de la preuve consiste à nouveau à exhiber des éléments qui jouent au ping pong sur l'espace projectif. Cependant, ici nous n'avons qu'un nombre fini d'éléments, à la différence de la situation étudiée dans l'alternative topologique. Pour trouver un élément proximal dans Σ^n, il nous faudra porter une attention particulière au choix de la métrique sur l'espace projectif. Le point essentiel est de trouver une métrique telle que Σ^n possède au moins un élément proximal dont la plus grande valeur propre domine les normes de tous les éléments de Σ^n. C'est précisément ce que nous permet de faire le lemme principal de ce paragraphe, qui établit une équivalence entre la plus grande valeur propre de Σ et la plus grande taille d'un conjugué de Σ.

Soit k un corps local et $\|\cdot\|$ la norme canonique sur k^d (comme au paragraphe 5.1). Pour un compact Q de $M_d(k)$, on note

- $\Lambda(Q) = \max\{|\lambda|, \lambda$ valeur propre d'un élément $g\in Q\}$.
- $\|Q\| = \max\{\|g\|, g\in Q\}$ où $\|g\|$ est la norme d'opérateur associée à $\|\cdot\|$.
- $E(Q) = \inf\{\|xQx^{-1}\|, x\in GL_d(k)\}$.

La quantité $\Lambda(Q)$ est le *spectre maximal* de Q alors que $E(Q)$ est la *norme minimale* de Q. Ces quantités sont reliées par les propriétés immédiates suivantes :

1. $\Lambda(Q)\leq E(Q)$.
2. $\Lambda(Q)^n \leq \Lambda(Q^n)\leq E(Q^n)\leq E(Q)^n$ pour tout $n\in\mathbb{N}$.

Nous établissons une sorte de réciproque :

Lemme 10.1. *(Lemme de comparaison Norme-Spectre) Pour tout entier $d\geq 1$, il existe une constante $C = C(d)$ telle que pour tout compact Q de $M_d(k)$ il existe un entier $i_0 \leq d^2$ tel que*

$$\Lambda(Q^{i_0}) \leq E(Q)^{i_0} \leq C(d)\cdot\Lambda(Q^{i_0})$$

Autrement dit, quitte à élargir Q en considérant tous les mots de longueur au plus d^2 en les éléments de Q, on obtient un ensemble dont la norme minimale et le spectre minimal sont comparables.

Ce lemme admet l'interprétation géométrique suivante. Considérons un espace symétrique $X = G/K$ où G est un groupe semisimple connexe sans facteur compact et K un compact maximal. Pour un élément $g\in Isom(X)^\circ$ on note $d_g(x) = d(g\cdot x, x)$ son déplacement au point $x\in X$ et $d_g = \inf_{x\in X} d_g(x)$ son déplacement minimal. De même pour une partie compacte Q de G on note $d_Q(x) = \max_{g\in Q} d(g\cdot x, x)$ et $d_Q = \inf_{x\in X} d_Q(x)$, le déplacement minimal de Q. Le lemme précédent se traduit géométriquement en l'énoncé suivant qui lui est équivalent :

Lemme 10.2. *(Version géométrique) Il existe une constante $C = C(X) > 0$ telle que pour toute partie compacte Q de $G = Isom(X)^\circ$ il existe $i_0 \leq d^2$ ($d = \dim G$) et $g \in Q^{i_0}$ tel que*

$$\frac{1}{\sqrt{d}} d_Q - C \leq d_g \leq d^2 \cdot d_Q$$

Pour passer de la version matricielle à la version géométrique, il suffit de noter que, comme le montre la décomposition de Cartan (cf. [30]), $\log \left\| hgh^{-1} \right\| \leq d_g(x) \leq \sqrt{d} \log \left\| hgh^{-1} \right\|$ si $x = h \cdot x_0$ et $K = Stab(x_0)$.

La preuve du lemme repose sur l'algèbre linéaire et d'abord sur la version limite suivante :

Proposition 10.1. *Pour une partie bornée Q de $M_d(k)$, les propriétés suivantes sont équivalentes :*

(i) $\Lambda(Q^i) = 0$ *pour tout* $i \leq d^2$.

(ii) $E(Q) = 0$.

(iii) La sous-algèbre $\mathcal{A}$ de $M_d(k)$ engendrée par Q est nilpotente, i.e. $\mathcal{A}^N = 0$ pour un $N \geq 1$.

Démonstration. $(iii) \Rightarrow (ii)$: peut trouver une base de k^d pour laquelle $\mathcal{A}$ est contenue dans les matrices triangulaires supérieures nilpotentes. On peut alors conjuguer par une matrice diagonale de la forme $diag(t^d, ..., t)$ et réduire la norme des éléments de $\mathcal{A}$ par un facteur $\frac{1}{t}$ au moins. D'où $E(Q) = 0$. $(ii) \Rightarrow (i)$ est clair par l'inégalité (2). Pour montrer $(i) \Rightarrow (iii)$, il suffit d'invoquer le théorème de Wedderburn sur la structure des sous-algèbres de $M_d(k)$. Celui-ci implique en particulier que si $\mathcal{A}$ n'est pas nilpotente alors il existe $e \in \mathcal{A}$ tel que $e^2 = e$ et $trace(e) = 1$. Mais $\mathcal{A}$ possède une base de vecteurs appartenant à $\cup_{i \leq d^2} Q^i$, car $\dim_k \mathcal{A} \leq d^2$. Donc (iii) entraîne $trace(x) = 0$ pour tout $x \in \mathcal{A}$. Contradiction. $\square$

Preuve du lemme 10.1. Raisonnons par l'absurde. On peut alors trouver une suite Q_n de compacts de $M_d(k)$ tels que pour tout $i \leq d^2$, $\Lambda(Q_n^i) \leq \frac{1}{n} E(Q_n)^i$. Quitte à renormaliser et à conjuguer Q_n on peut supposer que $E(Q_n) = 1$ et $\|Q_n\| \to 1$ alors que $\Lambda(Q_n^i) \to 0$. On peut donc prendre un compact limite Q. Il vérifie $E(Q) = 1$, $\Lambda(Q^i) = 0$ pour $i \leq d^2$, ce qui contredit la proposition précédente. $\square$

Remarque 10.1. *L'argument ci-dessus n'est pas effectif. Cependant il est possible de le rendre effectif. Lorsque k est non archimédien il suffit d'appliquer Wedderburn dans le corps résiduel, $C = |\pi|^{-d}$ convient, où π est un uniformisant. Si k est $\mathbb{R}$ ou $\mathbb{C}$, il faut démontrer une version effective du théorème de Wedderburn, et $C \simeq \exp(d^{d^2})$ convient.*

11. Bornes inférieures sur l'entropie algébrique

Dans ce dernier paragraphe, nous démontrons les théorèmes 9.1 et 9.2. Tous deux résultent du théorème suivant qui donne une borne uniforme sur le diamètre de semi-liberté en fonction de la norme minimale. Soit k un corps local et $d \in \mathbb{N}$.

Théorème 11.1. *Pour tout $\delta > 0$ il existe un entier m avec la propriété suivante. Pour toute partie compacte $Q \ni e$ de $SL_d(k)$ telle que l'adhérence de Zariski du groupe engendré par Q est semisimple et telle que $E(Q) \geq 1+\delta$, on a $d^+(Q) \leq m$.*

Voyons maintenant comment déduire les théorèmes 9.1 et 9.2 du précédent.

Preuve du théorème 9.2. Si le groupe Γ est virtuellement résoluble, on peut montrer que Γ est engendré par un nombre borné (en termes de d seulement) de générateurs. On peut alors appliquer un argument semblable à celui donné dans le paragraphe 9. Nous renvoyons le lecteur à [9] pour les détails. Si Γ n'est pas virtuellement résoluble et $\mathbb{G}$ est son adhérence de Zariski, alors sa projection dans $\mathbb{S} = \mathbb{G}/\mathbb{R}ad$ où $\mathbb{R}ad$ est le radical résoluble de $\mathbb{G}$ est encore discrète d'après un théorème d'Auslander (voir [36] Theorem 8.24.). On peut donc se ramener à la situation du théorème 11.1. La borne inférieure uniforme sur $E(Q)$ est donnée par le lemme de Margulis :

Lemme 11.1. *(Lemme de Margulis) Il existe un $\delta = \delta(d) > 0$ tel que si une partie Q de $SL_d(\mathbb{C})$ engendre un sous-groupe discret non virtuellement nilpotent, alors $E(Q) \geq 1+\delta$.*

□

Preuve du théorème 9.1. On se place dans le cas où Γ n'est pas virtuellement résoluble, car sinon on a déjà démontré la finitude du diamètre de semi-liberté au théorème 9.3. Quitte à prendre le quotient par le radical résoluble de l'adhérence de Zariski de Γ, on peut supposer que Γ est Zariski dense dans $\mathbb{G}(K)$ où $\mathbb{G}$ est semisimple et défini sur K. On peut supposer K de type fini. Il y a donc une borne supérieure sur l'ordre des racines de l'unité de K, et par conséquent les éléments de torsion de Γ appartiennent à la sous-variété algébrique propre $\{g \in \mathbb{G}(K), g^m = 1\}$ pour un certain entier m. D'après le lemme 11.5 ci-dessous, il existe $N = N(\Gamma)$ tel que pour toute partie génératrice de Γ, Σ^N contient au moins un élément g_0 semisimple d'ordre infini. Cet élément g_0 a une valeur propre qui n'est pas une racine de l'unité. D'après le lemme 9.2, on peut trouver un corps local k et un plongement de K dans k tel que cette valeur propre (ou son inverse) soit de module au moins $1+\varepsilon_0$, où $\varepsilon_0 = \varepsilon_0(K)$. Ainsi $\Lambda(\Sigma^N) \geq 1+\varepsilon_0$ et $E(\Sigma) \geq E(\Sigma^N)^{\frac{1}{N}} \geq 1+\delta$ où δ ne dépend que de K et N, donc que de Γ. On peut alors appliquer le théorème 11.1. □

Pour démontrer le théorème 11.1, nous allons à nouveau jouer au ping pong sur l'espace projectif. Cependant, dans notre situation, nous cherchons à construire un semi-groupe libre et non pas un groupe libre tout entier. C'est donc plus facile et la version du lemme du ping pong (ou du *ping* ici car il s'agit de semi-groupes seulement) qu'il nous faut est semblable à celle du lemme 9.1 ci-dessus dans le cas affine.

Lemme 11.2. *(Lemme du ping) Soit A et B dans $SL_n(k)$ tel que A est (r, ε^3)-proximal sur $\mathbb{P}(k^n)$ ($r > 2\varepsilon > 0$ voir définition 5.1) avec point attractif v et hyperplan répulsif H. Supposons que $Bv \neq v$ et que $d(Bv, H) \geq \varepsilon$ et $\max\{\|B\|, \|B^{-1}\|\} \leq \frac{1}{\varepsilon}$. Alors A et BA engendrent un semi-groupe libre.*

Démonstration. L'argument est semblable à celui du lemme 9.1 et nous laissons au lecteur le soin de le retrouver. Notons que nous ne faisons pas d'hypothèse sur la distance entre les deux points attractifs v et Bv, juste qu'ils sont distincts. C'est une différence essentielle avec le lemme de ping pong classique où on cherche à engendrer un sous-groupe libre. □

Pour être en mesure d'appliquer ce lemme du ping, il nous faut construire dans Q^n (n borné) un élément proximal A dont la plus grande valeur propre (qui contrôle le ε du lemme) domine les normes de tous les autres éléments de Q^n. L'irréductibilité de la représentation nous permettra ensuite de trouver un B dans Q^n qui vérifie les conditions du lemme du ping. Dans une première étape nous montrerons que quitte à prendre des mots de longueur bornée en les éléments de Q, on peut augmenter la norme minimale autant que l'on veut :

Lemme 11.3. *Pour tout $\delta > 0$ et pour tout $t > 0$ il existe $N = N(\delta, t)$ tel que pour toute partie Q de $SL_d(k)$, $E(Q) \geq 1 + \delta$ entraîne $E(Q^N) \geq t$.*

Démonstration. Par l'absurde, on a un t et une suite Q_n telle que $E(Q_n^n) \leq t$. Quitte à prendre une sous-suite convergente, on obtient à la limite un compact Q tel que $\|Q^n\| \leq t$ pour tout $n \geq 0$ et $E(Q) \geq 1 + \delta$. L'adhérence du semi-groupe engendré par Q est compacte, c'est donc un sous-groupe compact. Mais tout sous-groupe compact est conjugué dans $GL_d(k)$ à un sous-groupe du compact maximal canonique de $SL_d(k)$. Donc $E(Q) = 1$. Contradiction. □

D'après le lemme de comparaison Norme-Spectre 10.1, on peut trouver A dans une puissance bornée de Q tel que la plus grande valeur propre de A soit au moins égal à $E(Q)$. Cet élément sera notre candidat pour être le premier joueur de ping. Notons que si un élément g est (r, ε)-proximal, alors la plus grande valeur propre de g est comparable à la norme de g. Le lemme qui vient établit une sorte de réciproque, qui nous permettra de montrer que ce choix de A conduit bien à un élément proximal.

Lemme 11.4. *Soit $A \in SL_d(k)$ de valeurs propres $(\lambda_i)_i$ avec $|\lambda_1| \geq |\lambda_2| \geq ... \geq |\lambda_d|$. Supposons $|\lambda_1| \geq 2|\lambda_2|$. Alors il existe une constante $c = c(d)$, une matrice $P \in SL_d(\overline{k})$ telle que $\|P\|, \left\|P^{-1}\right\| \leq c\,\|A\|^{2d}$ et telle que si $A' = PAP^{-1}$, alors $A'e_1 = \lambda_1 e_1$ et $\left\|A'_{|H}\right\| \leq \frac{3}{2}|\lambda_2|$ où $H = \langle e_2, ..., e_d\rangle$ et $(e_i)_i$ est la base canonique de k^d. En particulier A' est $(1, \varepsilon)$-proximal dès que $|\lambda_2|/|\lambda_1| \leq \varepsilon^2$.*

Démonstration. La preuve est sans surprise. On montre successivement :

(1) Si $A \in SL_d(k)$ alors il existe $P \in SL_d(\overline{k})$ tel que $\|P\|, \left\|P^{-1}\right\| \leq c\,\|A\|^d$ et $\left\|PAP^{-1}\right\| \leq \frac{3}{2}|\lambda_1|$ (triangulariser A dans une base orthonormale).

(2) Si $A \in SL_d(k)$ vérifie $|\lambda_1| \geq 2|\lambda_2|$, alors il existe $v \in k^d$ tel que $Av = \lambda_1 v$ et un hyperplan H fixé par A tel que $d(v, H) \geq 1/\|A\|$.

Pour démontrer le lemme, on obtient v et H par le point (2), puis on applique le point (1) à la restriction de A à H, et enfin on conjugue à nouveau pour "redresser" v en e_1. □

Avant de finir la preuve du théorème 11.1, nous discutons un lemme très utile qui montre que l'on peut sortir des variétés algébriques propres en temps borné :

Lemme 11.5. *Soit $\mathbb{G}$ un groupe algébrique Zariski connexe défini sur un corps K et X un fermé de Zariski de $\mathbb{G}$ tel que $X \subsetneq \mathbb{G}$. Alors il existe un entier N tel que pour toute partie Q de $\mathbb{G}(K)$ telle que Q engendre un sous-groupe Zariski dense de $\mathbb{G}$, on a que Q^N n'est pas inclus dans $X(K)$. De plus N ne dépend que du degré des composantes irréductibles de X, de leurs dimensions et de leur nombre.*

Démonstration. Rappelons le théorème de Bezout en géométrie : si X et Y sont des variétés irréductibles et $X \cap Y = \cup Z_i$ la décomposition en irréductibles de leur intersection, alors

$$\sum \deg Z_i \leq \deg X \deg Y$$

Remarquons qu'il existe $s \in Q$ tel que $s^{-1}X \cap X \neq X$ sinon Q et donc $\mathbb{G}(K)$ stabiliserait $X(K)$ et on aurait $X = \mathbb{G}$. En prenant l'intersection $s^{-1}X \cap X$, soit le nombre de composantes irréductibles de dimension maximale diminue, soit la dimension de la variété diminue (par rapport à celle de X). De plus quand la dimension diminue, le nombre de composantes irréductibles et leur degré reste borné en termes du nombre de composantes de X et de leur degré, d'après le théorème de Bezout. On peut donc répéter ce procédé en trouvant $s_i \in Q$ tel que $X_{i+1} = s_i^{-1}X_i \cap X_i$ et $X_{i+1} \neq X_i$. Cela s'arrête au bout d'un nombre d'étapes N qui ne dépend que du degré des composantes de X et de leur nombre. On obtient $\cap g_i^{-1}X = \emptyset$, où les $g_i \in Q^N$. Si Q^N était inclus dans $X(K)$ alors l'identité e serait dans $\cap g_i^{-1}X(K)$, contradiction. □

Preuve du théorème 11.1. Par constante nous entendons une quantité qui ne dépend que des données de l'énoncé, i.e. d, k, δ. Fixons dès à présent les constantes $\varepsilon = \frac{1}{10}$ et t_0 tel que $(c_d t_0)^{\frac{1}{d}} = \varepsilon^{-2}$, où c_d est la constante du lemme de comparaison Norme-Spectre 10.1. On choisit une constante N de sorte que $t = E(Q^N) \geq t_0$ par le lemme 11.3. D'après le lemme de comparaison Norme-Spectre, lemme 10.1, $\Lambda(Q^{i_0 N}) \geq c_d t$ pour un $i_0 \leq d^2$. Pour alléger la notation, on remplace $Q^{i_0 N}$ par Q. On choisit A dans Q tel que $\Lambda(Q) = \Lambda(A)$. Quitte à prendre une puissance extérieure et un facteur irréductible, de dimension $D \leq 2^d$, on peut supposer que $|\lambda_1/\lambda_2|(A) \geq (c_d t)^{\frac{1}{d}}$ et $\|Q\| \leq t^d$ (noter que $\|\rho(g)\| \leq \|g\|^d$ si $\rho = \Lambda^i k^d$). D'après le lemme 11.4, quitte à conjuguer Q, on peut supposer que $Ae_1 = \lambda_1 e_1$, $\left\|A'_{|H}\right\| \leq \frac{3}{2}|\lambda_2|$ où $H = \langle e_2, ..., e_D \rangle$ et la norme de Q est peu affectée : $\|Q\| \leq t^{5D} C_d$ pour une autre constante C_d. Ainsi A est $(1, \varepsilon)$-proximal car $(c_d t)^{\frac{1}{d}} \geq \varepsilon^{-2}$. Et pour tout entier k, A^k est $(1, \varepsilon^{k/2})$-proximal pour les mêmes $v = e_1$ et H.

On choisit maintenant B, le second joueur. Tout B dans Q est de norme au plus $t^{5D} C_d$ et aussi, comme $B \in SL_D(k)$, $\left\|B^{-1}\right\| \leq \|B\|^{D-1} \leq (t^{5D} C_d)^{D-1}$. La condition sur la norme dans le lemme du ping est donc automatiquement remplie, à t fixé, si k est assez grand. Cependant, il faut que $Bv \neq v$ et que $d(Bv, H) \geq \varepsilon^{k/6}$. L'ensemble $\{g \in \mathbb{G}(K),\ g^i v = v \text{ pour un } 0 < i \leq D\}$ est un fermé algébrique propre de $\mathbb{G}$ dont le nombre de composantes irréductibles et leurs degrés sont indépendants du vecteur v. D'après dernier lemme ci-dessus, il y a un entier $N_1 = N_1(\mathbb{G})$ tel que l'on peut trouver B dans Q^{N_1} avec $g^i v \neq v$ pour tout $0 < i \leq D$. D'après Cayley-Hamilton, $B \in SL_D$ satisfait une équation $B^D + a_{D-1}B^{D-1} + ... + 1 = 0$ où $|a_i| \leq 2^D \|B\|^D \leq 2^D(t^{5D}C_d)^{N_1 D^2}$. Si f est la forme linéaire duale $f = e_1^*$, alors $f(x) = d(x, H)$ si $\|x\| = 1$. Puisque $f(v) = 1$, il s'ensuit que $f(B^i v) \geq (2^D(t^{5D}C_d)^{D^2})^{-1}$ pour au moins un i, $0 < i \leq D$. Il suffit de choisir k tel que $\varepsilon^{k/6}$ soit inférieur à cette constante et les conditions du lemme du ping seront remplies pour A^k et BA^k. □

12. Notes

(1) Paragraphe 1. Le contenu ici est tiré de [7]. Pour la propriété (T) non uniforme, voir [17].

(2) Paragraphe 2. Voir [16]. Pour la propriété (FA) de Serre, voir [38].

(3) Paragraphe 3. La proposition 3.1 et le corollaire 3.1 sont dus à Kuranishi [26]. Pour la proposition 3.2 voir l'article original [11]. Le lemme de Baumslag se trouve dans [3].

(4) Paragraphe 4. La proposition 4.1 et sa preuve son tirées et [7]. L'alternative topologique dans le cas général (théorème 4.1) est démontrée dans [8]. Pour l'alternative de Tits, voir l'article original de Tits [41].

(5) Paragraphe 5. Voir [7]. L'utilisation de la décomposition KAK est inspirée de [20] et de [1]. Le lemme de ping pong énoncé dans la remarque 5.2 se trouve dans [40]. Pour le lemme de Polya (i.e. remarque 5.4), voir l'article original [34], aussi [35]. Les lemmes 5.6 et 5.4 sont démontrés dans [8].

(6) Paragraphe 6. Pour l'équidistribution des groupes nilpotents denses, voir [5]. Pour le problème du trou spectral, voir le livre de Sarnak [37] et l'article récent de Bourgain et Gamburd [12]. La remarque est démontrée dans l'appendice du livre [25].

(7) Paragraphe 7. Le théorème 7.1 est dû à Milnor et Wolf [28]. Le théorème de Gromov apparaît dans [22]. Dans [19], Guivarc'h démontre que $\gamma_\Sigma(n)$ est entre deux constantes fois n^d, l'existence de la limite est démontrée par Pansu dans [33]. Pour la construction du groupe de Grigorchuk, voir [21] et [24]. Pour la géométrie des groupes nilpotents, les métriques de Carnot, on peut voir aussi [6] et ses références.

(8) Paragraphe 8. Pour les feuilletages riemanniens et de Lie, on renvoie au livre de Molino [29]. La croissance des feuilles est étudiée dans [13] et le théorème 8.1 répond à une question posée dans [23] et est démontré dans [8].

(9) Paragraphe 9. La croissance exponentielle uniforme et la finitude de d_Γ^+ pour les groupes linéaires en caractéristique 0 est due à Eskin-Mozes-Oh [14]. L'argument donné ici pour le théorème 9.1 (voir aussi [9]) est différent et plus direct que celui de [14] ; il traite aussi la caractéristique positive. Cependant la stratégie des preuves de ce paragraphe est largement inspiree de l'article [14]. Le théorème 9.2 est tiré de [9]. Pour les groupes résolubles

le fait que $S_\Gamma > 0$ est due à Osin [31]. La finitude de d_Γ^+ est tirée de [4]. Pour la proposition 9.1, le lemme 9.2 et la remarque 9.2, voir [4]. L'alternative de Tits uniforme fait l'objet de l'article [10].

(10) Paragraphe 10. Le lemme de comparaison est démontré dans [9]. Pour la géométrie des espaces symétriques, on renvoie à [30]. Le théorème de Wedderburn est par exemple démontré dans Lang [27].

(11) Paragraphe 11. Pour ce paragraphe, on renvoie à [9]. Le lemme de Margulis est démontré dans [42], voir aussi [18]. Pour le théorème de Bezout, voir [15]. Le lemme 11.5 est dû à Eskin-Mozes-Oh [14].

Références

[1] H. Abels, G.A. Margulis, G.A. Soifer, *Semigroups containing proximal linear maps*, Israel J. Math. **91** (1995), no. 1-3, p. 1–30.

[2] G.N. Arzhantseva, J. Burillo, M. Lustig, L. Reeves, H. Short, E. Ventura, *Uniform non-amenability*, Advances in Math., (2005).

[3] G. Baumslag, *On generalized free products*, Math. Zeitschrift **78** (1962) 423–438.

[4] E. Breuillard, *On uniform exponential growth for solvable groups*, preprint (2006).

[5] E. Breuillard, *Equidistribution in nilpotent Lie groups*, in preparation.

[6] E. Breuillard, *Geometry of locally compact groups of polynomial growth and shape of large balls*, preprint (2006).

[7] E. Breuillard, T. Gelander, *On dense free subgroups of Lie groups*, J. Algebra, **261** , no. 2, pp. 448–467, (2003).

[8] E. Breuillard, T. Gelander, *A topological Tits alternative*, to appear in the Annals of Math.

[9] E. Breuillard, T. Gelander, *Lower bounds for the algebraic entropy of discrete subgroups*, in preparation.

[10] E. Breuillard, T. Gelander, *A uniform Tits alternative*, in preperation.

[11] E. Breuillard, T. Gelander, J. Souto, P. Storm, *Dense embeddings of surface groups*, to appear in Geometry and Topology.

[12] J. Bourgain, A. Gamburd, *On the spectral gap for finitely generated subgroups of* $SU(2)$, preprint (2006).

[13] Y. Carrière *Feuilletages riemanniens à croissance polynômiale*, Comment. Math. Helv. **63** (1988), no. 1, p. 1-20.

[14] A. Eskin, M. Mozes, H. Oh, *On uniform exponential growth for linear groups in characteristic zero*, Invent. Math. **160**, no. 1, pp. 1–30, (2005).

[15] W. Fulton, *Intersection theory*, Ergeb. der Math. und ihrer Grenzgebiete, Springer-Verlag, (1984) 470 pp.

[16] T. Gelander, appendix to a paper of G. Soifer in the Margulis Conference volume.

[17] T. Gelander, A. Zuk, *Dependence of Kazhdan constants on generating subsets*, Israel J. Math. 129 (2002), 93–98.

[18] T. Gelander, *Homotopy type and volume of locally symmetric manifolds*, Duke Math. J. 124 (2004), no. 3, 459–515

[19] Y. Guivarc'h, *Croissance polynômiale et périodes des fonctions harmoniques*, Bull. Sc. Math. France **101**, (1973), p. 353-379.

[20] Y. Guivarc'h, *Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire*, Ergodic Theory Dynam. Systems **10** (1990), no. 3, 483–512.

[21] R. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Izv. Akad. Nauk. SSSR Ser. Mat. **48** (1984), no 5, 939-985.

[22] M. Gromov, *Groups of polynomial growth and expanding maps*, Publications Mathématiques de l'IHES, no **53** (1981), 53-73.

[23] A. Haefliger, *Feuilletages Riemanniens*, Séminaire Bourbaki, Vol. 1988/89. Astérisque No. **177-178** (1989), Exp. No. 707, p. 183–197.

[24] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago University Press, (2001).

[25] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi., *Classical and quantum computation*, volume 47 of Graduate Studies in Mathematics. AMS, (2002).

[26] M. Kuranishi, *On everywhere dense embedding of free groups in Lie groups*, Nagoya Math. **J 2** (1951), 63-71.

[27] S. Lang, *Algebra,* Third Edition, Addison-Wesley (1994).

[28] J. Milnor, *Growth of finitely generated solvable groups*, J. Wolf, *Growth of finitely generated solvable groups and curvature of Riemanniann manifolds*, J. Differential Geometry, **2** (1968) p. 421–449.

[29] P. Molino, *Riemannian foliations*, Prog. in Math. **73**, Birkhäuser, (1988), 339 pp.

[30] D. Mostow, *Strong rigidity of locally symmetric spaces*, Annals of Mathematics Studies, No. **78**. Princeton University Press, (1973) 195 pp.

[31] D. Osin, *The entropy of solvable groups*, Erg. Theory. Dyn. Sys. **23**, no. 3, (2003) p. 907–918.

[32] D. Osin, *Uniform non-amenability of free Burnside groups*, preprint arXiv math.GR/0404073.

[33] P. Pansu, *Croissance des boules et des géodésiques fermées dans les nilvariétés*, Ergodic Theory Dynam. Systems **3** (1983), no. 3, 415–445.

[34] G. Pólya*, Beitrag zur Verallgemeinerung des Verzerrungssatzes auf mehrfach Zusammenhangende Gebiete*, S.B. Preuss. Akad. Wiss., Berlin, K.L. Math. Phys. Tech. (1928), p. 228-232 and p. 280-282.

[35] T. Ransford, *Potential theory in the complex plane*, London Mathematical Society Student Texts, **28**, CUP, Cambridge, (1995) 232 pp.

[36] M.S. Raghunathan, *Discrete Subgroups of Lie Groups,* Ergebnisse der Mathematik und Ihrer Grenzgebiete. Band **68** (1972).

[37] P. Sarnak, *Some applications of modular forms*, Cambridge Tracts in Mathematics, **99**, CUP, Cambridge, (1990) 111 pp.

[38] J-P. Serre, *Arbres, amalgames, SL2,* Astérisque **46**, SMF, (1977).

[39] Y. Shalom, *Explicit Kazhdan constants for representations of semisimple and arithmetic groups*, Annales de l'institut Fourier, **50** no. 3 (2000), p. 833-863.

[40] T. Poznansky, Yale University dissertation, (2006).

[41] J. Tits, *Free subgroups of Linear groups*, Journal of Algebra **20** (1972), 250-270.

[42] W. Thurston, *Three-dimensional geometry and topology*, Vol. 1. Edited by Silvio Levy, Princeton Mathematical Series, **35**, Princeton University Press, (1997) 311 pp.

[43] J. Wilson, *On exponential growth and uniformly exponential growth for groups*, Invent. Math. **155** (2004), no. 2, p. 287–303.