UNIVERSITÉ DE RENNES 1

Théorème de Gromov sur les groupes de type fini à croissance polynômiale

Séminaire de M2

Université de Rennes 1

Jad Abou Yassin

Encadré par Benoît Claudon

Janvier 2023

Table des matières

Introduction

Le théorème de Gromov sur les groupes de type fini est un théorème fondamental de la théorie géométrique des groupes. L'étude des groupes a été historiquement motivée par leurs actions sur des objets géométriques, mais ces groupes eux-mêmes peuvent posséder des structures géométriques intéressantes, en particulier en considérant la métrique des mots sur les groupes de type finis. Le théorème de Gromov établit alors un lien entre le volume des boules d'un groupe (propriété géométrique) et le caractère virtuellement nilpotent de celui-ci (propriété « théorie des groupes »).

I Théorème de Gromov

Commençons par énoncer le théorème de Gromov

Théorème 1 - Gromov (1981)

Un groupe de type fini est à croissance polynomiale si et seulement si il est virtuellement nilpotent.

Ce théorème fut originellement démontré par Mikhail Gromov en 1981 [Gro81], en utilisant des outils mathématiques très avancés. Une seconde preuve plus élémentaire a été proposée par Bruce Kleiner en 2007 [Kle07], qui se repose notamment sur l'alternative de Tits. Enfin, et il s'agit ici de la preuve que nous allons présenter dans ce rapport, une preuve n'utilisant que des outils « élémentaires » a été mise au point par Terrence Tao et Yehuda Shalom en 2010 [Tao10].

II Croissance d'un groupe de type fini

Nous allons maintenant définir quelques notions de base sur la croissance d'un groupe de type fini. Cette sous-partie est majoritairement inspirée de [DLH00].

II.1 Fonction de croissance

Dans toute la suite, on considère un groupe de type fini G engendré par une partie finie S. Sans perdre de généralité, on peut supposer S symétrique, c'est-à-dire stable par passage à l'inverse.

Définition 1 - Fonction longueur

Soit $g \in G$. On appelle longueur de g relativement à S, noté $l_S(g)$, le plus petit entier n tel que g s'écrive comme produit de n éléments de S :

$$l_S(g) = \min\{n \in \mathbb{N}^* \ ; \ \exists s_1, \dots, s_n \in S \ ; \ g = s_1 \dots s_n\}$$

Remarquons que le minimum est bien défini car il porte sur une partie non vide de $\mathbb{N}$. On remarque aussi qu'on a

$$l_S(g) = 1 \Leftrightarrow g \in S \quad \text{et} \quad l_S(g) = 0 \Leftrightarrow g = \mathrm{id}$$

Définition 2 - Fonction de croissance

On appelle la fonction de croissance de G relativement à S la fonction $\beta(G, S, \cdot)$ définie par :

$$\forall k \in \mathbb{N} \; ; \; \beta(G, S, k) = |\{g \in G \; ; \; l_S(g) \leq k\}|$$

Cette fonction est bien définie car il ne peut y avoir plus de $|S|^k$ éléments de longueur k, donc qu'un nombre fini d'éléments de longueur au plus k.

Exemple élémentaire Soit $G = (\mathbb{Z}, +)$. G est engendré par la partie (symétrique) $S = \{-1, 1\}$. Alors pour tout $k \in \mathbb{N}$, on a $\beta(G, S, k) = 2k + 1$.

II.2 Types de croissance

II.2.1 Comparaison de fonctions de croissance

Nous allons voir que le choix d'une partie génératrice d'un groupe n'influe pas sur la nature de sa fonction de croissance. Cela vient du fait que c'est le cas sur les fonctions longueurs relativement à une partie génératrices.

Proposition 1 - Comparaison de longueur, de croissance

Soit G un groupe de type fini, et S et Σ deux parties génératrices finies de G. Alors il existe une constante $C > 0$ telle que pour tout $g \in G$,

$$\frac{1}{C} l_S(g) \leq l_\Sigma(g) \leq C l_S(g)$$

En particulier, la fonction de croissance de G vérifie, pour toutes parties génératrices finies S et Σ :

$$\exists C > 0, \; \forall k > 0, \quad \beta\left(G, S, \frac{k}{C}\right) \leq \beta(G, \Sigma, k) \leq \beta(G, S, kC) \tag{II.2.1}$$

II.2.2 Types de croissance

Ce qui précède permet alors de définir sans ambiguïté les notions de types de croissance pour un groupe de type fini (indépendamment du choix d'une partie génératrice)

Définition 3 - Types de croissance

Soit G un groupe de type fini. On dit que G est

- à croissance polynômiale si pour une partie génératrice finie S de G, il existe une constante $A > 0$ et un entier $d \in \mathbb{N}$ tels que pour tout $k > 0$, $\beta(G, S, k) \leq Ak^d$
- à croissance exponentielle si pour une partie génératrice finie S de G, il existe une constante $a > 0$ telle que pour tout $k > 0$, $\beta(G, S, k) \geq k^a$
- à croissance intermédiaire sinon.

La partie précédente permet de remplacer « pour une » par « pour toute » dans la définition. On dit alors que « la » [1] fonction de croissance de G est à croissance polynômiale/exponentielle/intermédiaire.

Exemples

- On considère le groupe de Heisenberg :

$$H_3 = \langle x, y, z \mid [x, y] = z,\ [x, z] = 1,\ [y, z] = 1 \rangle \subset GL_3(\mathbb{C})$$

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  On remarque que tout élément de H_3 s'écrit de manière unique $x^k y^l z^m$, pour $(k, l, m) \in \mathbb{Z}^3$. En considérant le système de générateur $S = \{x, x^{-1}, y, y^{-1}\}$, on peut montrer en remarquant que $[x^k, y^k] = z^{k^2}$ que H_3 est à croissance polynômiale d'ordre 4.

- Un groupe libre de rang $r \geq 2$ est à croissance exponentielle. En effet, si $G = F_S$ où $S = \{s_1, \ldots, s_r\}$, alors tout mot sur l'alphabet $S \cup S^{-1}$ ne contenant pas de facteurs ss^{-1} est une écriture réduite. Ainsi, on a :

$$\forall k > 0, \quad \beta(G, S \cup S^{-1}, k) = 1 + \sum_{i=1}^{k} 2r(2r-1)^{i-1} = \frac{r(2r-1)^k - 1}{r-1} \geq (2r-1)^k$$

En particulier, si G est un groupe de type fini, sa croissance est au plus exponentielle, et la définition précédente recouvre donc tous les groupes de type fini. Il est naturel de se demander s'il existe des groupes à croissance intermédiaire. Le résultat est positif, mais est loin d'être immédiat [2].

III Preuve du théorème de Gromov

Nous allons démontrer seulement le sens direct. Le sens réciproque se ramène au cas des groupes nilpotents, car un groupe de type fini virtuellement à croissance polynômiale est à croissance

1. C'est un abus de langage, mais la relation (II.2.1) est en fait une relation d'équivalence et on considère les classes. Ceci est expliqué en détail dans [DLH00]
2. Voir le séminaire de Habiba Hmamed, qui devrait le présenter juste avant moi

polynômiale (les classes à gauche d'un sous-groupe d'indice fini forment une partition finie du groupe). Dans le cas des groupes nilpotents, on a la formule de Bass-Guivarc'h [Gui70] [Bas72] :

Proposition 2 - formule de Bass-Guivarc'h (1970, 1972)

Si $G = G_1 \supset G_2 \supset \dots$ est la suite centrale de G, alors G est à croissance polynômiale d'ordre

$$d(G) = \sum_{k \geq 1} k \text{ rang}(G_k/G_{k+1})$$

III.1 Résultats intermédiaires

La preuve de ce résultat est très largement inspirée de [Tao10]. Elle se repose sur les quatre lemmes suivants :

Lemme 1 - Existence d'une fonction harmonique Lipschitz non triviale

Soit G un groupe infini de type fini. Alors il existe une fonction $f : G \to \mathbb{R}$ harmonique, lipschitzienne et non constante.

Lemme 2 - Théorème de Kleiner

Soit G un groupe de type fini à croissance polynomiale. Alors l'espace vectoriel V des fonctions harmoniques Lipschitz est de dimension finie.

Lemme 3 - Théorème de Gromov dans le cas d'un groupe de Lie compact

Soit G un sous-groupe de type fini à croissance polynomiale d'un groupe de Lie compact $H \subset GL_n(\mathbb{C})$. Alors G est virtuellement abélien.

Lemme 4 - Théorème de Gromov dans le cas d'un quotient monogène infini

Soit G un groupe de type fini à croissance polynomiale d'ordre au plus d. On suppose que le théorème de Gromov est vrai pour les groupes de type fini à croissance polynomiale d'ordre au plus $d-1$. Si G contient un sous-groupe d'indice fini G' tel qu'il existe un morphisme de groupes surjectif $G' \twoheadrightarrow \mathbb{Z}$, alors G est virtuellement nilpotent.

Dans ce devoir, nous démontrerons intégralement le lemme 3 ainsi qu'une partie du lemme 1. Nous renvoyons à [Tao10] pour la preuve des autres lemmes, et plus précisément à [Kle07] pour la preuve du lemme 2.

III.2 Mise en commun

Précisons d'abord quelques notions apparaissant dans les énoncés des lemmes 1 et 2.

Définition 4 - Fonctions harmoniques, fonctions lipschitziennes

Soit G un groupe engendré par une partie finie symétrique S et $f : G \to \mathbb{R}$. On dit que f est harmonique si

$$\forall x \in G, \quad f(x) = \frac{1}{|S|} \sum_{s \in S} f(xs)$$

et qu'elle est lipschitzienne s'il existe une constante $C \geq 0$ telle que :

$$\forall x \in G, \forall s \in S, \quad |f(xs) - f(x)| \leq C$$

Soit G un groupe de type fini à croissance polynomiale d'ordre d. On montre par récurrence sur d le théorème de Gromov. Le cas $d = 0$ est trivial, il s'agit alors d'un groupe fini, qui est bien évidemment (virtuellement) nilpotent.

On suppose vrai le résultat aux rangs $\leq d-1$. Soit S une partie finie symétrique engendrant G. Si G est fini, alors le résultat est immédiat. On suppose donc que G est infini. Par le lemme 1, il existe une fonction harmonique lipschitzienne non constante. Ainsi, si V est l'espace de ces fonctions sur G, alors $W = V/\mathbb{C}$ est un espace vectoriel non-trivial.

G agit sur V par translation à gauche : $g \cdot f = f(g^{-1}\cdot)$. De plus, cette action fixe les constantes, donc elle induit une action sur W. Si $f \in V$, on note $||f||_{Lip}$ la constante de Lipschitz optimale de f. Il ne s'agit pas d'une norme sur V mais d'une semi-norme. Plus précisément, on a

$$||f||_{Lip} = 0 \quad \Leftrightarrow \quad f \text{ est constante}$$

Ainsi, comme $||f + \lambda||_{Lip} = ||f||_{Lip}$, alors on peut induire $|| \cdot ||_{Lip}$ sur W qui devient alors une norme sur W. De plus, l'action de G sur W préserve cette norme. Comme W est de dimension finie (car V est de dimension finie par le lemme 2), alors toutes les normes sur W sont équivalentes. Comme G agit par isométrie sur $(W, || \cdot ||_{Lip})$, son image est précompacte. Son adhérence est alors un sous-groupe compact de $GL(W)$, et donc un groupe de Lie (linéaire) compact. Par le lemme 3, l'image de l'action de G sur W est virtuellement abélienne. Deux cas se présentent :

- Si l'image de l'action de G sur W est infinie, alors on considère un sous-groupe d'indice fini abélien de l'image de l'action de G, qui nous donne en prenant l'image réciproque un sous-groupe d'indice fini de G dont l'image est abélien infini. En particulier, ce sous-groupe se surjecte dans $\mathbb{Z}$. Par le lemme 4, G est virtuellement nilpotent et on conclut.
- Sinon, le noyau de cette action est d'indice fini. On note G' ce sous-groupe de G. Il agit sur W de manière triviale, et donc sur V par $g \cdot f = f + \lambda_g(f)$ où $\lambda_g : f \mapsto g \cdot f - f$ est une forme linéaire sur V.

  On remarque que $\lambda : g \in G' \mapsto \lambda_g \in V^*$ est un morphisme de groupes (pour l'addition dans V^*). Si l'image de λ est infinie, on conclut comme précédemment par le lemme 4 que G' est virtuellement nilpotent, donc G est virtuellement nilpotent (car G' est d'indice fini dans G). Ainsi, on suppose que l'image de λ est finie. Le noyau de λ est donc un sous-groupe d'indice

fini de G', qu'on note G'', et on a :

$$\forall g \in G'', \forall f \in V,\ g \cdot f = f + \lambda_g(f) = f$$

Ainsi, toutes les fonctions harmoniques lipschitziennes sur G sont invariantes par l'action de G''. Comme G'' est d'indice fini dans G, alors tous les éléments de V ne prennent qu'un nombre fini de valeurs (les valeurs $f(g)$ pour g dans une transversale de G/G'', qui est finie). Par le principe du maximum, f est constante. C'est absurde car il existe des fonctions non constantes dans V par le lemme 1. Ce cas est donc impossible, et ceci conclut la preuve du théorème de Gromov. □

III.3 Preuve partielle du lemme 1 : existence d'une fonction harmonique et lipschitzienne non constante

On cherche à montrer qu'il existe des fonctions harmoniques lipschitziennes non constantes. Posons

$$\mu = \frac{1}{|S|} \sum_{s \in S} \delta_s$$

où δ_s est le Dirac en s. Alors une fonction $f : G \to \mathbb{R}$ est harmonique si et seulement si $\mu * f = f$, où le produit de convolution est défini par

$$\forall f, g : G \to \mathbb{R}, \quad f * g(x) = \sum_{y \in G} f(xy^{-1}) g(y)$$

L'idée pour construire une fonction harmonique non constante et de considérer la suite $(\mu^{(m)})_{m \in \mathbb{N}}$ des itérés de μ pour la convolution, et de la moyenniser : on considère la suite de fonction $(f_n)_{n \in \mathbb{N}}$ définie par

$$f_n = \frac{1}{n} \sum_{m=1}^{n} \mu^{(m)}$$

Si cette suite converge, alors la limite f vérifiera $\mu * f = f$. De plus, on a pour tout $m \in \mathbb{N}$, $||\mu^{(m)}||_{\ell^1(G)} = 1$, donc $||f_n||_{\ell^1(G)} = 1$. Enfin, on a :

$$f_n * \mu - f = \frac{1}{n} \sum_{m=1}^{n} \mu^{(m+1)} - \mu^{(m)} = \frac{1}{n} \left(\mu^{(n+1)} - \mu \right)$$

Ainsi, la suite $(f_n)_n$ est « asymptotiquement harmonique », car elle vérifie

$$||f_n - f_n * \mu||_{\ell^1(G)} \leq 2/n \xrightarrow[n \to +\infty]{} 0$$

Le reste de la preuve consiste à extraire une sous-suite convergente de $(f_n)_n$, et de montrer que la valeur d'adhérence obtenue sera bien une fonction harmonique et lipschitzienne non constante. On distingue deux cas :

Cas non-moyennable Dans ce cas, on a

$$\exists \varepsilon > 0,\ \exists s \in S, \quad \liminf_{n\in\mathbb{N}} ||f_n - f_n * \delta_s||_{\ell^1(G)} > \varepsilon$$

Comme $\ell^1(G)$ et $\ell^\infty(G)$ sont duaux[3], alors pour tout $n \in \mathbb{N}$, il existe $H_n \in \ell^\infty(G)$ telle que

$$||H_n||_{\ell^\infty(G)} = 1 \quad \text{et} \quad \langle H_n, \widetilde{f_n} - \widetilde{f_n * \delta_s}\rangle = ||f_n - f_n * \delta_s||_{\ell^1(G)}$$

donc en particulier,

$$\liminf_{n\in\mathbb{N}} |H_n * f_n(\mathrm{id}) - H_n * f_n(s)| > \varepsilon \tag{III.3.1}$$

Or, par l'inégalité de Young, on a

$$\begin{cases} ||H_n * f_n||_{\ell^\infty(G)} \leq ||H_n||_{\ell^\infty(G)}||f_n||_{\ell^1(G)} = 1 \\ ||H_n * f_n - H_n * f_n * \mu||_{\ell^\infty(G)} \leq ||H_n||_{\ell^\infty(G)}||f_n - f_n * \mu||_{\ell^1(G)} \leq 2/n \end{cases} \tag{III.3.2}$$

Par le théorème de Banach-Alaoglu, il existe une suite extraite de $(H_n * f_n)_{n\in\mathbb{N}}$ qui converge simplement vers une fonction bornée notée f. Cette fonction est harmonique car elle vérifie $f = f*\mu$ en passant à la limite dans (III.3.2), et elle est non triviale car elle vérifie $f(\mathrm{id}) \neq f(s)$ en passant à la limite dans (III.3.1). Comme elle est de plus bornée, elle est en particulier lipschitzienne, ce qui conclut l'existence d'une fonction harmonique lipschitzienne non triviale dans ce cas.

Cas moyennable Nous renvoyons à [Tao10] pour la preuve de ce cas. L'idée est similaire à ce qui précède, mais on utilise des outils d'analyse fonctionnelle plus avancés afin d'obtenir une suite de fonctions $(G_n)_n$ uniformément lipschitzienne et asymptotiquement harmonique. Le théorème d'Ascoli permet alors d'en extraire une sous-suite convergente, et la limite est une fonction harmonique lipschitzienne non triviale. □

III.4 Preuve du lemme 3 : cas d'un groupe de Lie compact

Tout d'abord, il est connu que les représentations de groupes de Lie linéaires compacts sont unitaires. Ainsi, on peut supposer dans la suite que $H = U(n)$, et considérer G un sous-groupe de type fini à croissance polyomiale de $U(n) \subset GL_n(\mathbb{C})$.

On démontre le lemme 3 par récurrence sur n. Le cas $n = 1$ est trivial, car $U(1)$ est abélien.

Supposons maintenant le résultat vrai aux rangs $1, \ldots, n-1$. Si G contient un élément g de $Z(H)$ différent d'une homothétie, alors G est inclus dans $Z(g)$. Or, $Z(g) \simeq U(n_1) \times \cdots \times U(n_k)$ où $k \geq 2$ et $n_1 + \cdots + n_k = n$ par le théorème spectral et stabilité des sous-espaces propres de g par les éléments commutant à g. Notons G_i l'image de G dans $U(n_i)$. Par l'hypothèse de récurrence, il existe H_i un sous-groupe de G_i abélien et d'indice fini. Or, $G \hookrightarrow G_1 \times \cdots \times G_k$. On

3. On remarque que le produit scalaire usuel peut s'exprimer par le produit de convolution : $\langle f, g\rangle = (f * \widetilde{g})(\mathrm{id})$ où $\widetilde{g}(x) = g(x^{-1})$

pose $H = G \cap (H_1 \times \cdots \times H_k)$. C'est un sous-groupe abélien de G, et on a alors :

$$[G : H] \leq [G_1 \times \cdots \times G_k : H] \leq [G_1 \times \cdots \times G_k : H_1 \times \cdots \times H_k] \leq [G_1 : H_1] \dots [G_k : H_k]$$

Donc H est abélien et d'indice fini dans G, d'où le lemme 3.

On suppose maintenant que tous les éléments centraux de G sont des homothéties. Soit $\varepsilon > 0$. On pose G' le sous-groupe de G engendré par $S \subset G$ composé des éléments $g \in G$ tels que $||g - \mathrm{id}||_{op} \leq \varepsilon$.

On a besoin de la définition d'un ε-net (terminologie anglaise qu'on pourrait traduire en ε-filet) :

Définition 5 - ε-net

Soit (X, d) un espace métrique et A une partie de X. On dit que A est un ε-net si les boules de rayon ε centrées en les éléments de A recouvrent X, et si les boules de rayon $\varepsilon/2$ centrées en les éléments de A sont deux à deux disjointes.

Remarquons que si $\varepsilon > 0$, alors un ε-net est un ensemble discret. Et si X est précompact, alors un ε-net existe toujours et c'est un ensemble fini [4].

En considérant un ε-net de G, nous allons montrer que G' est d'indice fini. Soit A un ε-net de G et R une transversale de G/G'. Montrons que $|R| \leq |A|$. Comme G est précompact, alors $|A| < +\infty$ ce qui conclura. Soit $g \in R$ un représentant de gG'. Comme A est un ε-net, alors il existe un $a \in A$ tel que $||g - a||_{op} \leq \varepsilon$. Comme g est une isométrie, alors

$$||g^{-1}a - \mathrm{id}||_{op} = ||g - a||_{op} \leq \varepsilon$$

Ainsi, $g^{-1}a \in G'$ car c'est un générateur de G'. Donc $gG' = aG'$. Finalement, on peut trouver une transversale de G/G' à valeurs dans A, donc $|R| \leq |A|$, donc G' est d'indice fini dans G (d'ailleurs, d'indice majoré par le cardinal d'un ε-net maximal).

De même que précédemment, si G' possède un élément central différent d'une homothétie, on conclut la preuve par le théorème spectral. On suppose donc que les seuls éléments centraux de G' sont des homothéties. Deux cas se présentent alors, soit G' n'est constitué que d'homothéties, et dans ce cas il est abélien et on n'a plus rien à faire, soit il existe un élément de G' différent d'une homothétie. On se place alors dans ce second cas.

L'idée fondamentale est que, si h est un générateur de G' et g un élément de G', alors le crochet $[g, h]$ est bien plus proche de l'identité que ne l'est g. En effet, on a :

$$||ghg^{-1}h^{-1} - 1||_{op} = ||gh - hg||_{op} = ||(g-1)(h-1) - (h-1)(g-1)||_{op}$$

car g et h sont des isométries. Ainsi, par inégalité triangulaire

$$||[g, h] - \mathrm{id}||_{op} \leq 2||g - \mathrm{id}||_{op}||h - \mathrm{id}||_{op} \leq 2\varepsilon||g - \mathrm{id}||_{op} \tag{III.4.1}$$

Prenons $h_1 \in S$ qui n'est pas une homothétie (h_1 existe bien car si tous les éléments de S

4. On peut construire un ε-net en ajoutant à chaque étape un nouvel élément qui n'est pas dans l'union des boules de rayon $\varepsilon/2$ des éléments précédents, la compacité assure que ceci termine en un nombre fini d'étapes.

sont des homothéties, alors tous les éléments de G' le sont aussi). On note $\delta_1 = ||h_1 - \mathrm{id}||_{op}$. Par l'inégalité (III.4.1), l'ensemble des commutateurs de h_1 par des éléments de S est constitué d'éléments tous à distance inférieure à $2\varepsilon\delta_1$ de l'identité. Si tous ces éléments sont des homothéties, alors pour tout $g \in S$, $[g, h_1] = \lambda \mathrm{id}$ où $\lambda^n = 1$ car $\det([g, h_1]) = 1$, et $|\lambda - 1| \leq 2\varepsilon^2\delta_1$. Si ε est assez petit par rapport à n, alors nécessairement $\lambda = 1$, donc h_1 commute avec tous les éléments de S, ce qui est absurde car ils s'agit alors d'un élément central de G' différent d'une homothétie.

Ainsi, il existe $h_2 = [g_1, h_1]$ pour un certain $g_1 \in S$ qui n'est pas une homothétie, et qui est à distance $\delta_2 = c_1\varepsilon\delta_1$ de l'identité où $c_1 \leq 2$. En procédant de même, on construit par récurrence une suite $(h_n)_n$ qui vérifie :

- $\forall i \in \mathbb{N}^*$, $h_i = [h_{i-1}, g_{i-1}] \in G'$ pour un certain $g_{i-1} \in S$ n'est pas une homothétie.
- $\delta_1 = ||h_1 - \mathrm{id}||_{op} \leq \varepsilon$
- $\forall i \in \mathbb{N}^*$, $\delta_{i+1} = ||h_{i+1} - \mathrm{id}||_{op} = c_i\varepsilon\delta_i$ où $c_i \leq 2$

Montrons qu'il existe une constance $c > \varepsilon$ tel que pour tout $m \in \mathbb{N}^*$ et pour tous entiers $0 \leq i_1, \ldots, i_m \leq c\varepsilon^{-1}$, les éléments $h_1^{i_1} \ldots h_m^{i_m}$ sont deux à deux distincts. En effet, si on a deux mots

$$h_1^{i_1} \ldots h_m^{i_m} \quad \text{et} \quad h_1^{j_1} \ldots h_m^{j_m}$$

où $(i_1, \ldots, i_m) \neq (j_1, \ldots, j_m)$, on note r le premier indice tel que $i_r \neq j_r$. Quitte à inverser i et j, on peut supposer que $i_r - j_r > 0$.

Or, si $0 \leq k_s, \ldots, k_m \leq c\varepsilon^{-1}$ (avec $1 \leq s \leq m$), on a les inégalités :

$$||h_s^{k_s} \ldots h_m^{k_m} - \mathrm{id}||_{op} \leq 2c\varepsilon^{-1}\delta_s \tag{III.4.2}$$

$$||h_s^{k_s} \ldots h_m^{k_m} - \mathrm{id}||_{op} \geq (1 - 4c)\delta_s \tag{III.4.3}$$

Démontrons-les. Pour l'inégalité (III.4.2), on utilise le fait que $||fg - \mathrm{id}||_{op} \leq ||f - \mathrm{id}||_{op}||g - \mathrm{id}||_{op}$. On obtient alors

$$\begin{aligned} ||h_s^{k_s} \ldots h_m^{k_m} - \mathrm{id}||_{op} &\leq \sum_{i=s}^{m} k_i||h_i - \mathrm{id}||_{op} \leq \sum_{i=s}^{m} c\varepsilon^{-1}\delta_i \leq c\varepsilon^{-1}\sum_{i=s}^{m}(2\varepsilon)^{i-s}\delta_s \\ &\leq c\varepsilon^{-1}\delta_s\frac{1}{1-2\varepsilon} \leq 2c\varepsilon^{-1}\delta_s \end{aligned}$$

si ε est assez petit ($\varepsilon < 1/4$ pour être précis).

Pour l'inégalité (III.4.3), on utilise le fait que si λ est un complexe de module 1 tel que $|1-\lambda| \leq \varepsilon$, alors pour tout entier $|k| \leq \pi\varepsilon^{-1}$, on a $|1-\lambda^k| \geq |1-\lambda|$ (intuitivement, les premières puissances de λ s'éloignent de 1 sur le cercle unité). Dans ce qui suit, on choisit $c \leq \pi$. Comme h_s est unitaire, il se diagonalise en base orthonormée par le théorème spectral et ses valeurs propres sont des racines de l'unité. Ainsi,

$$||h_s - \mathrm{id}||_{op} = \max\{|1 - \lambda| \ ; \ \lambda \in \sigma(h_s)\}$$

(la norme d'opérateur associée à la norme euclidienne est la plus grande valeur singulière). Par hypothèse, on a $||h_s - \mathrm{id}||_{op} \leq \varepsilon$, donc toutes ses valeurs propres vérifient l'inégalité $|1-\lambda| \leq \varepsilon$. Par

ce qui précède, pour tout entier $|k| \leq c\varepsilon^{-1}$, on a $|1-\lambda^k| \geq |1-\lambda|$, et donc $||h_s^k - \mathrm{id}||_{op} \geq ||h_s - \mathrm{id}||_{op}$. De ceci découle l'inégalité (III.4.3) :

$$\begin{aligned}||h_s^{k_s} \dots h_m^{k_m} - \mathrm{id}||_{op} &= ||h_s^{k_s} \dots h_m^{k_m} - h_s^{k_s} + h_s^{k_s} - \mathrm{id}||_{op} \geq \left| ||h_s^{k_s}(h_{s+1}^{k_{s+1}} \dots h_m^{k_m} - \mathrm{id})||_{op} - ||h_s^{k_s} - \mathrm{id}||_{op} \right| \\ &\geq ||h_s^{k_s} - \mathrm{id}||_{op} - ||h_{s+1}^{k_{s+1}} \dots h_m^{k_m} - \mathrm{id}||_{op} \geq ||h_s - \mathrm{id}||_{op} - 2c\varepsilon^{-1}\delta_{s+1} \\ &= \delta_s - 2c\varepsilon^{-1}2\varepsilon\delta_s = (1-4c)\delta_s\end{aligned}$$

Il reste à conclure : on a deux mots $h_1^{i_1} \dots h_m^{i_m}$ et $h_1^{j_1} \dots h_m^{j_m}$ tels que $(i_1, \dots, i_m) \neq (j_1, \dots, j_m)$, avec r le premier indice où $i_r \neq j_r$. Par les inégalités (III.4.2) et (III.4.3), on a :

$$\begin{aligned}||h_1^{i_1} \dots h_m^{i_m} - h_1^{j_1} \dots h_m^{j_m}||_{op} &= ||h_r^{i_r - j_r} \dots h_m^{i_m} - h_{r+1}^{j_{r+1}} \dots h_m^{j_m}||_{op} \\ &\geq ||h_r^{i_r - j_r} \dots h_m^{i_m} - \mathrm{id}||_{op} - ||h_{r+1}^{j_{r+1}} \dots h_m^{j_m} - \mathrm{id}||_{op} \\ &\geq (1-4c)\delta_r - 2c\varepsilon^{-1}\delta_{r+1} \geq (1-4c)\delta_r - 4c\delta_r = (1-8c)\delta_r\end{aligned}$$

En prenant alors $c < 1/8$, on obtient que les mots considérés désignent bien des éléments distincts. Il y en a au total $(c\varepsilon^{-1})^m$ (on choisit c de sorte que $c\varepsilon^{-1} \in \mathbb{N}^*$, quitte à réduire ε).

Or, pour tout i, h_{i+1} est un commutateur de h_i avec un générateur, on a alors

$$l_S(h_{i+1}) \leq 2 + 2l_S(h_i) \leq 4l_S(h_i)$$

Ainsi, si $0 \leq i_1, \dots, i_m \leq c\varepsilon^{-1}$, alors

$$l_S(h_1^{i_1} \dots h_m^{i_m}) \leq i_1 4^0 + \dots + i_m 4^{m-1} \leq c\varepsilon^{-1}\frac{4^m - 1}{3} \leq \frac{c\varepsilon^{-1}}{3}4^m$$

Donc la fonction de croissance de G' par rapport à S vérifie :

$$\beta\left(G', S, \frac{c\varepsilon^{-1}}{3}4^m\right) \geq (c\varepsilon^{-1})^m$$

Or, G' est à croissance polynômiale, disons d'ordre $d \in \mathbb{N}$. On a alors une constante $A > 0$ vérifiant

$$\beta\left(G', S, \frac{c\varepsilon^{-1}}{3}4^m\right) \leq A\left(\frac{c\varepsilon^{-1}}{3}4^m\right)^d$$

On choisit alors c de sorte que $c\varepsilon^{-1} > 4^d$ (en supposant ε assez petit pour que ce soit possible), et on obtient une contradiction en faisant tendre m vers $+\infty$ dans l'inégalité

$$(c\varepsilon^{-1})^m \leq A\left(\frac{c\varepsilon^{-1}}{3}4^m\right)^d$$

Ainsi, tous les éléments centraux de G' sont des homothéties, et on a déjà conclut la preuve du lemme 3 dans ce cas. □

Remarque *Ce théorème est très similaire au théorème de* Jordan-Schur *« Soit G un sous-groupe fini de $U(n)$. Alors il existe une constante $C_n \in \mathbb{N}$ ne dépendant que de n telle que G contient un sous-groupe abélien d'indice au plus C_n ». Seule la dernière partie de la preuve change, où on utilise la finitude du groupe au lieu de sa compacité.*

Références

[Bas72] Hyman Bass. The degree of polynomial growth of finitely generated nilpotent groups. *Proceedings of the London Mathematical Society*, s3-25, 1972.

[DLH00] Pierre De La Harpe. *Topics in geometric group theory*. Univ. of Chicago Press, 2000.

[Gro81] Michael Gromov. Groups of polynomial growth and expanding maps (with an appendix by Jacques Tits). *Publications Mathématiques de l'IHÉS*, 53 :53–78, 1981.

[Gui70] Yves Guivarc'h. Groupes de lie à croissance polynomiale. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 271, 1970.

[Kle07] Bruce Kleiner. A new proof of gromov's theorem on groups of polynomial growth, 2007.

[Tao10] Terrence Tao. A proof of gromov's theorem. https://terrytao.wordpress.com/2010/02/18/a-proof-of-gromovs-theorem/, Dec 2010.