Ultraproduits de groupes de type fini et application à un théorème de Gromov

Malo Jézéquel, Jean Kieffer

27 juin 2015

Ce document est consacré à la preuve, inspirée de [1], de l'énoncé suivant :

Un groupe de type fini est à croissance polynomiale si, et seulement si, il admet un sous-groupe nilpotent d'indice fini.

Après avoir introduit les notions et propriétés essentielles dans la première section, on présente les différents résultats de théorie des groupes qui mènent au sens réciproque de l'énoncé. La preuve de celui-ci fait l'objet de la troisième partie.

Le coeur de la preuve du sens direct, le théorème de Gromov, consiste en la construction d'un certain espace métrique Y sur lequel le groupe agit. La quatrième section introduit les outils de logique nécessaires à sa construction ; on présente ensuite les propriétés essentielles de cet espace, et celles-ci sont mises à profit dans la sixième partie, qui clôt la preuve.

Enfin, la dernière section présente une version finie du théorème de Gromov, établie grâce à des arguments de théorie des modèles.

Table des matières

1 Définitions et premières propriétés

Définition 1.1. Soit G un groupe de type fini, muni d'un système de générateurs $X = \{x_1, \dots, x_n\}$.

1. Pour $g \in G$, on appelle *longueur* de g (sur X), notée $|g|$, le plus petit entier k tel que g s'écrive sous la forme
$$g = x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}$$
avec $\varepsilon_i = \pm 1$.
En particulier, l'élément neutre du groupe est de longueur nulle. G est alors muni de la distance
$$x, y \longmapsto |x^{-1}y|$$
qui est invariante par multiplication à gauche par un élément de G.
2. Pour tout $m \in \mathbb{N}$, on note $C(m) = C_X(m)$ le nombre d'éléments de G de longueur inférieure à m (sur X). La fonction C est appelée *fonction de croissance* de G.
3. G est dit *à croissance polynomiale* s'il existe des constantes $k, d \geqslant 0$ telles que
$$\forall\, m \in \mathbb{N}^{>0},\ C(m) \leqslant k m^d.$$
On dit alors que la croissance est *de degré au plus d*. G est dit à croissance *quasi-polynomiale* si cette propriété est vraie pour une infinité de m.
4. G est dit *à croissance exponentielle* s'il existe des constantes $k, r > 1$ telles que
$$\forall\, m \in \mathbb{N},\ C(m) \geqslant k r^m.$$

Pour que cette définition ait un sens, il reste à vérifier que ces notions de croissance ne dépendent pas de la partie génératrice X choisie.

Proposition 1.2. *Soient X, Y deux systèmes de générateurs finis d'un groupe G. Alors C_X et C_Y sont équivalentes au sens suivant : il existe $A > 0$ tel que*
$$\forall\, m \in \mathbb{N},\ C_Y(m) \leqslant C_X(Am).$$

Démonstration. Si A est un majorant des longueurs dans le système X des éléments de Y, un mot de longueur m sur Y est un mot de longueur au plus Am sur X. Par conséquent $C_Y(m) \leqslant C_X(Am)$. □

Proposition 1.3. *Soit G un groupe de type fini, et K un sous-groupe d'indice fini de G. Alors K est de type fini. De plus, K est à croissance polynomiale de degré au plus d (resp. exponentielle) si et seulement si G l'est.*

Démonstration. $\star$ Montrons que K est de type fini. Soit $X = \{x_1, \dots, x_n\}$ un système de générateurs de G, que l'on suppose clos par $x \mapsto x^{-1}$, et $u_1, \dots, u_p$ des représentants dans G des éléments de $K\backslash G$; on prend $u_1 = e$. Pour tous $1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant p$, il existe $1 \leqslant l \leqslant p$ et un certain $k_{ij} \in K$ tels que $u_j x_i = k_{ij} u_l$. Soit $g \in K$. g s'écrit dans le système de générateurs X :

$$\begin{aligned} g = x_{i_1} \cdots x_{i_m} &= u_1 x_{i_1} \cdots x_{i_m} \\ &= k_{i_1,1} u_{l_1} x_{i_2} \cdots x_{i_m} \\ &= k_{i_1,1} \cdots k_{i_m,l_{m-1}} u_{l_m} \end{aligned}$$

et $l_m = 1$ puisque $g \in K$. K est donc engendré par les k_{ij}.
$\star$ Soit $Y = \{y_1, \dots, y_q\}$ un système de générateurs fini de K. Alors $Z = Y \cup \{u_1, \dots, u_p\}$ est clairement une partie génératrice de G.

Si $k \in K$ est de longueur n sur Y, alors $ku_1, \cdots, ku_p$ sont p mots distincts dans G, de longueur au plus $n+1$ sur Z. On a donc

$$C_Y(m) \leqslant \frac{1}{p} C_Z(m+1).$$

On se donne maintenant un élément x de longueur n sur Z. On cherche à écrire x sous la forme $k'u_i$, avec $k' \in K$, et à majorer la longueur de k' sur Y. Soient k_{ij}, k'_{ij} des éléments de K tels que l'on ait $u_j y_i = k_{ij} u_l,\ u_j u_i = k'_{ij} u_{l'}$ où l, l' dépendent de i, j. Soit M un majorant des longueurs des k_{ij}, k'_{ij} sur Y. En écrivant $x = u_1 x$ et en décalant le u vers la droite grâce à ces éléments, on voit que l'on peut écrire x sous la forme

$$x = k' u_i$$

où $1 \leqslant i \leqslant p$, et où $k' \in K$ est de longueur au plus nM sur Y. Il y a au plus $pC_Y(nM)$ tels éléments, donc

$$C_Z(n) \leqslant pC_Y(Mn).$$

On en déduit que G et K ont même croissance. □

La notion de croissance d'un groupe provient de la géométrie différentielle ; elle a été introduite par J. Milnor, afin d'étudier les liens entre la courbure d'une variété et la croissance de son groupe fondamental.

Définition 1.4. Soit G un groupe.

1. Sa *suite centrale descendante* est la suite de groupes $(G_k)_{k \geqslant 0}$ définie par
$$G_0 = G, \quad \forall\, k \in \mathbb{N}, G_{k+1} = [G, G_k].$$
où l'on prend la convention $[a, b] = aba^{-1}b^{-1}$, et où $[X, Y]$ désigne le sous-groupe engendré par les commutateurs de la forme $[x, y]$ avec $x \in X$, $y \in Y$.

2. G est dit *nilpotent* si sa suite centrale descendante stationne à $\{e\}$; sa *classe de nilpotence* est alors le plus petit entier k tel que $G_k = \{e\}$.
3. G est dit *virtuellement nilpotent* si G admet un sous-groupe nilpotent d'indice fini.

Les théorèmes principaux de ce document sont alors :

Théorème 1.5 (Gromov)**.** *Un groupe à croissance polynomiale est virtuellement nilpotent.*

Théorème 1.6 (Wolf, Tits)**.** *Un groupe de type fini virtuellement nilpotent est à croissance polynomiale.*

Avec les arguments qui suivent, on pourrait en fait démontrer le théorème de Gromov avec une hypothèse de croissance quasi-polynomiale. Par 1.6, il n'existe donc pas de groupe à croissance quasi-polynomiale qui ne soit pas à croissance polynomiale.

2 Outils de théorie des groupes

Cette section présente des résultats de théorie des groupes plus ou moins classiques nécessaires à la compréhension des preuves ultérieures. La plupart sont sous-entendus dans [1] et [2].

2.1 Au sujet des sous-groupes d'indice fini

Proposition 2.1. *Soit G un groupe, H un sous-groupe de G d'indice fini n. Alors $\bigcap_{g\in G} gHg^{-1}$ est un sous-groupe distingué de G d'indice fini au plus $n!$.*

Démonstration. On fait agir G sur l'ensemble des classes à gauche modulo H :

$$\rho(x) \ : \ gH \mapsto xgH.$$

ρ est un morphisme de G dans $\mathfrak{S}(G/H) \simeq S_n$. De plus, pour tous $g, x \in G$,

$$xgH = gH \iff xgHg^{-1} = gHg^{-1} \iff x \in gHg^{-1}.$$

Donc $\operatorname{Ker}\rho = \bigcap_{g\in G} g^{-1}Hg$, d'où le résultat. □

Proposition 2.2. *Soient G, H des groupes, f un morphisme surjectif de G sur H, et K un sous-groupe d'indice fini de H. Alors $f^{-1}(K)$ est un sous-groupe d'indice fini de G et $[G : f^{-1}(K)] = [H : K]$.*

Démonstration. Soit $\pi \ : \ H \longrightarrow H/K$ la projection canonique.
$\pi \circ f \ : \ G \longrightarrow H/K$ est surjective et est compatible avec l'égalité modulo $f^{-1}(K)$ dans G, donc se factorise via $G/f^{-1}(K)$ en une application surjective. Elle est de plus injective : si $x, y \in G$ vérifient $f(x)K = f(y)K$, alors $f(x)^{-1}f(y) \in K$ donc $x^{-1}y \in f^{-1}(K)$. □

Théorème 2.3. *Soit F_n le groupe libre de rang fini n. Alors pour tout entier $k \geqslant 1$, F_n admet un nombre fini de sous-groupes d'indice k.*

Démonstration. L'idée de la preuve est tirée de [3]. On dit qu'une partie S de F_n est un *système de Schreier* si elle vérifie la propriété suivante : pour tout $g \in S$, si $a_1 \cdots a_p$ est l'unique écriture réduite de g, alors $a_2 \cdots a_p \in S$. En particulier, un système de Schreier contient toujours l'élément neutre 1.

Si U est un sous-groupe d'indice fini k de F_n, alors il existe un système de Schreier contenant exactement un représentant de chaque classe à gauche modulo U. Ce système est en fait facile à exhiber : il suffit de choisir, dans

chaque classe à gauche, le plus petit élément dans l'ordre alphabétique (un ordre total étant mis sur les générateurs et leurs inverses). Ce système de Schreier a k éléments, donc ses éléments sont tous de longueur au plus k ; il n'existe qu'un nombre fini de tels systèmes de Schreier. Cependant, un système donné peut a priori correspondre à plusieurs sous-groupes.

Si S est un système de Schreier correspondant à U, on définit une action π de F sur S de la façon suivante : si $g \in S$ et $x \in F$, $\pi(x)(g)$ est l'élément de S qui est dans la classe à gauche de xg modulo U (il s'agit bien d'une permutation car $xg \in xg'U \implies g \in g'U$). On remarque alors que U est déterminé par S et π, puisque U est précisément le stabilisateur de 1 sous cette action. De plus, π est déterminée par l'image d'une base libre, c'est à dire n permutations d'un ensemble à k éléments. En conséquence, on peut faire correspondre à U un système de Schreier de taille k et n permutations d'un ensemble à k éléments de manière injective : il n'y a qu'un nombre fini de sous-groupes d'indice k dans F_n. □

Remarque. Cette démonstration donne aussi une borne pour le nombre de tels sous-groupes : il y en a au plus $\binom{n^k}{k}(k!)^n$. Cette borne est loin d'être optimale. On pourra se référer à [3] pour un résultat plus précis.

Théorème 2.4. *Soit G un groupe de type fini. Alors G admet un nombre fini de sous-groupes d'indice k et leur intersection est un sous-groupe caractéristique de G d'indice fini.*

Démonstration. Si G est de type fini, c'est l'image par un morphisme du groupe libre d'un certain rang n. G n'admet donc qu'un nombre fini de groupes d'indice k car leurs préimages sont des sous-groupes d'indice k de F_n, donc sont en nombre fini.

En regroupant ces sous-groupes grâce au premier théorème, on se ramène à montrer la chose suivante : si H_1 et H_2 sont deux sous-groupes distingués de G d'indice fini, alors $H_1 \cap H_2$ l'est aussi. Or le morphisme

$$\begin{aligned} \varphi \ : G &\longrightarrow G/H_1 \times G/H_2 \\ x &\longmapsto (xH_1, xH_2) \end{aligned}$$

a pour noyau $H_1 \cap H_2$, et son image est finie. Par factorisation, on en déduit le résultat. □

2.2 Au sujet des groupes nilpotents

Lemme 2.5. *Soit G un groupe nilpotent de classe $s+1$, dont la suite centrale descendante est notée*

$$G = G_0 \supset G_1 \cdots \supset G_{s+1} = \{e\}.$$

On note également $\pi_k : G \longrightarrow G/G_{k+1}$ *la projection canonique. On suppose* G/G_1 *de type fini ; soit* T_0 *une partie finie de* G *telle que* $\pi_0(T_0)$ *engendre* G/G_1*. On pose pour* $k \geqslant 1$ *:* $T_k = \{[x, y] \,|\, x \in T_0,\ y \in T_{k-1}\}$*.*
Alors G_k/G_{k+1} *est engendré par* $\pi_k(T_k)$*, et* T_0 *engendre* G*.*

En particulier, tous les facteurs de la suite centrale descendante sont des groupes abéliens de type fini.

Démonstration. $\pi_0(T_0)$ engendre G/G_1 ; supposons la propriété vraie pour $T_0, \ldots, T_{k-1}$. On pose $\Delta = G/G_{k+1}$, et l'on note

$$\Delta = \Delta_0 \supset \Delta_1 \supset \cdots$$

la suite centrale descendante de Δ.

Comme $\Delta_l = \pi_k(G_l)$, Δ est nilpotent de classe $k+1$. $\Delta_k = [\Delta, \Delta_{k-1}]$ est donc central dans Δ. On a donc, si $\alpha, \alpha_1, \alpha_2 \in \Delta,\ \beta, \beta_1, \beta_2 \in \Delta_{k-1}$,

$$[\alpha_1\alpha_2, \beta] = \alpha_1\alpha_2\beta\alpha_2^{-1}\alpha_1^{-1}\beta^{-1} = \alpha_1 \left(\alpha_2\beta\alpha_2^{-1}\beta^{-1}\right)\beta\alpha_1^{-1}\beta^{-1} = [\alpha_1, \beta][\alpha_2, \beta]$$

$$[\alpha, \beta_1\beta_2] = \alpha\beta_1\beta_2\alpha^{-1}\beta_2^{-1}\beta_1^{-1} = \alpha\beta_1\alpha^{-1}\left(\alpha\beta_2\alpha^{-1}\beta_2^{-1}\right)\beta_1^{-1} = [\alpha, \beta_1][\alpha, \beta_2]$$

Or, $\pi_{k-1}(T_{k-1})$ engendre $G_{k-1}/G_k = (G_{k-1}/G_{k+1})/(G_k/G_{k+1}) = \Delta_{k-1}/\Delta_k$ donc $\pi_k(T_{k-1})$ et Δ_k engendrent Δ_{k-1}. Par une récurrence ascendante, on voit que $\pi_k(T_0), \ldots, \pi_k(T_{k-1}), \Delta_k$ engendrent Δ, c'est à dire que $\pi_k(T_0)$ et Δ_k engendrent Δ.

Or, ajouter un élément de Δ_k, central, dans les commutateurs précédents n'en change pas la valeur. Avec les calculs ci-dessus, on en déduit que $\Delta_k = G_k/G_{k+1} = [\pi_k(T_0), \pi_k(T_{k-1})] = \langle \pi_k(T_k) \rangle$, ce qui termine la récurrence.

De plus, on a montré que $\pi_{s+1}(T_0)$ et G_{s+1} engendrent G/G_{s+1}, autrement dit que T_0 engendre G. □

Remarque. Le caractère nilpotent de G n'est pas nécessaire pour montrer que G_k/G_{k+1} est engendré par $\pi_k(T_k)$: il suffit d'appliquer le résultat précédent au groupe G/G_{k+1} qui est nilpotent de classe $k+1$.

On en déduit en particulier :

Théorème 2.6. *Soit* G *un groupe nilpotent de type fini. Alors tous les facteurs de la suite centrale descendante de* G *sont des groupes abéliens de type fini.*

Théorème 2.7. *Soit* G *un groupe,* H *un sous-groupe distingué de* G*. On suppose que* H *et* G/H *sont de présentation finie (donc en particulier de type fini). Alors* G *est de présentation finie.*

Démonstration. La preuve est tirée de [4]. On se donne une présentation de H et G/H :

$$H = \langle\, x_1, \ldots, x_m \,|\, r_1 = \cdots = r_k = 1 \,\rangle$$
$$G/H = \langle\, y_1 H, \ldots, y_n H \,|\, s_1 = \cdots = s_l = 1 \,\rangle\,.$$

Alors G est engendré par les x_i et y_j, qui vérifient des relations de la forme :

$$\begin{array}{cccc} r_i(x) = 1, & & s_j(y) = t_j(x) & (1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l) \\ y_j x_i y_j^{-1} = u_{ij}(x), & & y_j^{-1} x_i y_j = v_{ij}(x) & (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n) \end{array}$$

la deuxième ligne indiquant que H est distingué dans G.

Soit $\bar{G}$ le groupe engendré par $\bar{x_1}, \ldots, \bar{y_n}$ muni de ces relations. Il existe alors un morphisme surjectif $f : \bar{G} \longrightarrow G$ qui à $\bar{x_i}$ associe x_i et $\bar{y_j}$ associe y_j ; c'est simplement le quotient du même morphisme du groupe libre de rang $n+m$ vers G. On note $\bar{H}$ le sous-groupe de $\bar{G}$ engendré par les $\bar{x_i}$; vu les relations, c'est un sous-groupe distingué de G.

f induit alors un morphisme surjectif de $\bar{H}$ vers H, qui admet un morphisme surjectif réciproque (par la même propriété) ; c'est un isomorphisme. f induit donc également un morphisme de $\bar{G}/\bar{H}$ vers G/H, qui admet un morphisme réciproque ; c'est également un isomorphisme. f est donc un isomorphisme de $\bar{G}$ sur G. On en déduit que G est de présentation finie. □

Remarque. On peut également montrer par des arguments similaires que si un groupe admet une présentation finie, il admet une présentation finie sur toute partie génératrice finie.

Lemme 2.8. *Soit G un groupe de type fini ayant un sous-groupe nilpotent d'indice fini, alors G est de présentation finie.*

Démonstration. Soit H un tel sous-groupe de G. On pose $H' = \cap_{g \in G} g H g^{-1}$. Par 2.1, H' est d'indice fini dans G et donc de type fini. De plus, H' est nilpotent, donc H' est de présentation finie (on peut le voir par 2.7, car un groupe abélien de type fini est clairement de présentation finie). Mais H' est aussi distingué dans G et G/H' est fini et donc de présentation finie. Par le même lemme, G est de présentation finie. □

2.3 Au sujet des groupes de Lie

Un *groupe de Lie* est un groupe muni d'une structure de variété différentielle réelle qui rend les opérations de groupes régulières. $GL_n(\mathbb{C})$ en est un exemple.

On ne développera pas ici la théorie des groupes de Lie, même si certains résultats comme 2.9 sont accessibles en toute généralité.

Proposition 2.9. *Soit G un groupe de Lie d'élément neutre e. Alors pour tout $n > 0$, il existe un voisinage U de e dans G tel que $U\backslash\{e\}$ ne contient pas d'élément d'ordre inférieur à n.*

Démonstration. On prouve ce résultat dans le cas où $G = GL_n(\mathbb{C})$; la preuve dans le cas général est très similaire. L'espace tangent T_eG de G en l'identité est $\mathcal{M}_n(\mathbb{C})$ et l'application exponentielle exp : $T_eG \longrightarrow G$ est un difféomorphisme local en 0. exp est donc injective sur un voisinage V de 0. On se donne $n > 0$; soit W un voisinage de 0 dans T_eG tel que $nW \subset V$. On note $U = \exp(W)$, qui est donc un voisinage de l'identité dans G.

Soit g un élément de U d'ordre $k \leqslant n$. On peut écrire $g = \exp(w)$ avec $w \in W$. Mais alors kw et 0 ont même image par exp et sont dans V ; on en déduit $w = 0$ et $g = e$. □

Théorème 2.10 (Représentation adjointe)**.** *Soit L un groupe de Lie connexe, n sa dimension et C son centre. Alors L/C se plonge dans $GL_n(\mathbb{C})$.*

Les preuves des trois théorèmes qui suivent sont trop difficiles pour être discutées ici. On trouvera des références dans [1].

Théorème 2.11 (Corollaire du 5^e problème de Hilbert)**.** *Soit Y un espace métrique. On suppose Y homogène, complet, connexe, localement connexe, localement compact et de dimension de Hausdorff finie. Alors pour une certaine topologie, le groupe $Isom(Y)$ des isométries de Y est un groupe de Lie possédant un nombre fini de composantes connexes.*

Théorème 2.12 (Jordan)**.** *Pour tout entier $n \geqslant 1$, il existe un entier q tel que tout sous-groupe fini de $GL_n(\mathbb{C})$ admet un sous-groupe abélien d'indice au plus q.*

Théorème 2.13 (Tits)**.** *Tout sous-groupe de type fini de $GL_n(\mathbb{C})$ possède un sous-groupe résoluble d'indice fini ou un sous-groupe libre de rang 2.*

La topologie sur $Isom(Y)$ à laquelle fait référence le théorème 2.11 sera précisée par la suite.

3 Réciproque du théorème

Nous disposons maintenant des outils nécessaires à la démonstration de la réciproque du théorème de Gromov.

Théorème 3.1 (Wolf, Tits)**.** *Un groupe nilpotent de type fini est à croissance polynomiale.*

Vu la proposition 1.3, le résultat est également valable pour les groupes virtuellement nilpotents. On suit ici la preuve donnée par Tits [2].

Dans toute cette partie, on se donne un groupe G nilpotent de type fini, et $(G_i)_{i\geqslant 1}$ une *filtration* de G, c'est à dire une suite décroissante de sous-groupes telle que $G = G_1$, $[G_i, G_j] \subseteq G_{i+j}$ et $G_i = 1$ à partir d'un certain rang. Par exemple, la suite centrale descendante de G est une filtration. (Pour une preuve de ce fait, on pourra se référer à [4], paragraphe 5.1).

Définition 3.2. On appelle *système f-générateur* de G une partie finie E de G telle que pour tout i, $E \cap G_i$ engendre G_i. On note alors $E_i = E \cap G_i$ et $E'_i = E \backslash E_{i+1}$.

Étant donné un mot m sur $E \cup E^{-1}$, la *f-longueur* de m est la suite croissante stationnaire $(n_1, n_2, \dots)$ où n_i est la longueur de la contribution de $E'_i \cup E'^{-1}_i$ dans m. Un élément de G est dit *de f-longueur inférieure à* $(r_1, r_2, \dots)$ s'il peut être exprimé comme un mot de f-longueur $(n_1, n_2, \dots)$ avec $n_i \leqslant r_i$ pour tout i. On note $C_f(r_1, r_2, \dots)$ le nombre de tels éléments. On fera attention au fait que *la* f-longueur d'un élément de G, au contraire de sa longueur, n'est pas bien définie.

L'existence d'un système f-générateur est assurée par le lemme 2.5. Par ailleurs, de même que dans la première partie, les fonctions de croissance de deux systèmes générateurs distincts sont équivalentes. Cela justifie la définition suivante :

Définition 3.3. On dit que G est à *f-croissance polynomiale* de degré au plus d s'il existe une constante $M > 0$ telle que

$$\forall\, r \in \mathbb{R}_+,\ C_f(r, r^2, \dots, r^p, \dots) \leqslant M r^d + 1.$$

On remarque que si G est à f-croissance polynomiale de degré au plus d, alors G est à croissance polynomiale de degré au plus d. En effet, on a toujours $C(r) \leqslant C_f(r, r^2, \dots)$.

Il suffit donc de montrer la proposition suivante :

Proposition 3.4. *Soit d_i le rang du groupe abélien G_i/G_{i+1}. Alors G est à f-croissance polynomiale de degré au plus $\sum i d_i$.*

Démonstration. On note a le plus grand entier tel que $G_a = G$, et m la taille du plus petit système générateur de G_a/G_{a+1}. D'après le lemme 2.5, on peut choisir un f-système générateur E de telle sorte que E'_a soit de cardinal m. Quitte à ajouter des éléments, on peut également supposer que les commutateurs d'éléments de $E \cup E^{-1}$ sont dans E. On se donne $y \in E'_a$, et on note G' le sous-groupe de G engendré par $E\backslash\{y\}$.

Démontrons par récurrence sur q le résultat suivant :

Si w est un mot de f-longueur inférieure à $(n_1, \dots)$ sur $E \cup E^{-1}$, et si $(y_1, \dots, y_p)$ sont les occurrences de y et y^{-1} dans w, alors il existe un mot w_q représentant le même élément de G que w, qui a les mêmes occurrences de y et y^{-1}, qui commence par $y_1 \cdots y_q$ et dont la f-longueur $(n_1^{(q)}, n_2^{(q)}, \cdots)$ vérifie

$$n_i^{(q)} \leqslant n_i + qn_{i-a} + \binom{q}{2} n_{i-2a} + \cdots$$

C'est évident pour $q = 0$. Supposons le résultat vrai au rang $q-1$: on dispose donc d'un mot w_{q-1} qui vérifie les propriétés annoncées. On ramène alors y_q vers la gauche par commutations successives : le croisement de y_q et d'un élément de E_i introduit un élément de E_{i+a} (qui peut être l'identité). On obtient ainsi un nouveau mot w_q qui représente le même élément de G, qui a les mêmes occurrences de y et y^{-1}, et qui commence par $y_1 \cdots y_q$. De plus, on a

$$\begin{aligned} n_i^{(q)} &\leqslant n_i^{(q-1)} + n_{i-a}^{(q-1)} \\ &\leqslant \sum_{k \geqslant 0} \binom{q-1}{k} n_{i-ka} + \sum_{k \geqslant 1} \binom{q-1}{k-1} n_{i-ka} \\ &= \sum_{k \geqslant 0} \binom{q}{k} n_{i-ka} \end{aligned}$$

ce qui termine la récurrence.

On se donne maintenant $r \in \mathbb{R}_+$, et l'on suppose $n_i \leqslant r^i$ pour tout i. Soit e le plus petit entier tel que $G_e = \{1\}$. En appliquant le résultat précédent pour $q = p$ $(\leqslant r^a)$, et en majorant $\binom{q}{j}$ par q^j, on voit que tout $g \in G$ de f-longueur inférieure à $(r, r^2, \dots)$ peut s'écrire

$$g = y^s g'$$

avec $|s| \leqslant r^a$ et $g' \in G'$. De plus, on peut choisir g' de f-longueur $(n'_1, \dots)$ (le f-système générateur étant maintenant $E\backslash\{y\}$) telle que pour tout $i \leqslant e$,

$$\begin{aligned} n'_i + |s| &\leqslant \sum_{k \geqslant 0} q^k n_{i-ka} \\ &\leqslant \sum_{0 \leqslant k \leqslant e-1} r^{ak} r^{i-ak} \\ &\leqslant er^i. \end{aligned}$$

La f-longueur étant stationnaire à partir du rang e, cette inégalité reste valable pour $i > e$. On suppose que le résultat de la proposition est valable pour G' muni de la filtration $(G' \cap G_i)_{i \geqslant 1} = (G', \dots, G', G_{a+1}, \dots, 1, \dots)$: deux cas se présentent.

Premier cas : G/G' est infini. Alors les rangs d'_i des quotients dans la filtration de G' vérifient : $d'_i = d_i$ pour tout $i \neq a$, et $d'_a < d_a$. En effet, G'/G_{a+1} ne peut être de rang maximal dans G/G_{a+1}, puisqu'il n'intersecte pas le sous-groupe engendré par l'image de y (par l'hypothèse $|G/G'| = \infty$), et est donc de rang au plus $d_a - 1$. Il existe alors au plus $2r^a + 1$ choix possibles pour s et $M'r^{(\sum id_i)-a}$ choix pour g', ce qui donne le résultat.

Deuxième cas : G/G' est fini. Il existe donc un plus petit $t > 0$ tel que $y^t \in G'$. En effectuant la division euclidienne de s par t, on peut écrire

$$g = y^{s_1} g'_1$$

avec $|s_1| < t$ et $g'_1 \in G'$. De plus, il existe un certain M tel que y^t soit de f-longueur inférieure à $(M, M, \dots)$. g'_1 peut donc être choisi de f-longueur inférieure à $(M(er - |s|) + M|s|, \dots) = (Mer, Mer^2, \dots)$. Par l'hypothèse faite sur G', il existe au plus $M'r^{\sum id_i}$ choix pour g'_1 et un nombre fini de choix pour s_1, d'où le résultat.

On s'est donc ramené à montrer le résultat pour G'. Or, par rapport à G, $e - a$ a diminué et s'il est resté constant, alors m a strictement diminué. Il suffit donc de faire une récurrence double, qui s'initialise aisément. □

Remarque. On peut en fait montrer (cf. [2]) que le groupe G est à croissance polynomiale de degré *exactement* $d = \sum id_i$, au sens suivant : il existe des constantes $A, B > 0$ telles que pour tout entier $n > 0$ on ait

$$An^d \leqslant C(n) \leqslant Bn^d.$$

On peut donc déduire du théorème de Gromov et de cette propriété qu'un groupe à croissance polynomiale a toujours un degré entier.

4 Outils de logique

4.1 Ultrapuissances et théorème de Łos

On se donne un langage $\mathcal{L}$ et une $\mathcal{L}$-structure M, c'est à dire que M est un ensemble non vide muni d'interprétations des constantes, relations et fonctions de $\mathcal{L}$.

Définition 4.1. Soit I un ensemble infini. Un *filtre* sur I est une classe $\mathcal{F}$ de parties de I telle que

1. $\emptyset \notin \mathcal{F}$, $I \in \mathcal{F}$
2. Si $U, V \in \mathcal{F}$, alors $U \cap V \in \mathcal{F}$
3. Si $U \in \mathcal{F}$ et $U \subset V$, alors $V \in \mathcal{F}$.

Un *ultrafiltre* est un filtre maximal pour l'inclusion, ou encore un filtre $\mathcal{F}$ qui vérifie :

$$\forall\, J \in \mathcal{P}(I), \quad J \in \mathcal{F} \quad \text{ou} \quad I \backslash J \in \mathcal{F}.$$

Le *filtre de Fréchet* sur I est la classe des parties cofinies de I. Comme tous les filtres, il est inclus dans un filtre maximal (par le lemme de Zorn) ; un tel ultrafiltre est dit *non principal*, et ne contient pas de partie finie de I.

Définition 4.2. Soit $\mathcal{F}$ un ultrafiltre non principal sur I. On définit une relation d'équivalence sur M^I en posant :

$$(a_i) \equiv (b_i) \iff \{i \in I \,|\, a_i = b_i\} \in \mathcal{F}.$$

On dit alors que $a_i = b_i$ *pour presque tout* i, noté $a_i = b_i$ p.p.i.

On note M^* le quotient de M^I par cette relation, dans lequel on identifiera un élément avec n'importe lequel de ses représentants. On fait de M^* une $\mathcal{L}$-structure en posant :

1. Si c est une constante de $\mathcal{L}$,

$$c^{M^*} = (c^M)_{i \in I}$$

2. Si f est une fontion n-aire de $\mathcal{L}$,

$$f^{M^*}\left((m_i^1)_{i\in I}, \ldots, (m_i^n)_{i\in I}\right) = \left(f^M(m_i^1, \ldots, m_i^n)\right)_{i\in I}$$

3. Si $\mathcal{R}$ est un prédicat n-aire de $\mathcal{L}$,

$$\left((m_i^1)_{i\in I}, \ldots, (m_i^n)_{i\in I}\right) \in \mathcal{R}^{M^*} \iff \left(m_i^1, \ldots, m_i^n\right) \in \mathcal{R}^M \text{ p.p.i}$$

On vérifie que ces définitions sont indépendantes des choix de représentants. M^* est appelée *ultrapuissance* de M.

Remarque. On peut également considérer une structure *à plusieurs sortes* $(M_1, \dots, M_p)$, c'est à dire que les M_j sont différents univers et que les constantes, relations et fonctions viennent avec leur « typage ». Dans les formules logiques du premier ordre, on fait alors apparaître les variables avec leur sorte : $\forall\, x \in M_1 \exists\, y \in M_2 \dots$

Ce cas se ramène en fait au précédent, puisqu'il suffit de prendre pour M la réunion disjointe des M_k munie de p prédicats unaires indiquant la sorte d'un élément.

L'intérêt des ultrapuissances provient entre autres du théorème suivant :

Théorème 4.3 (de Łos)**.** *Soit $\varphi(x_1, \dots, x_n)$ une $\mathcal{L}$-formule. Alors, avec les notations précédentes :*

$$M^* \models \varphi\left((m_i^1)_{i\in I}, \dots, (m_i^n)_{i\in I}\right) \iff M \models \varphi(m_i^1, \dots, m_i^n) \text{ p.p.i.}$$

En particulier, si φ est un $\mathcal{L}$-énoncé vrai dans M, il est vrai dans M^*.

Ce théorème se montre par induction sur la complexité de la formule. La définition de l'ultrapuissance donne le résultat pour les termes ; la conjonction provient de la stabilité du filtre par intersection, et le quantificateur existentiel ne pose pas non plus de problème. La maximalité du filtre intervient uniquement pour la négation.

Remarque. Une conséquence immédiate de ce théorème est que le plongement diagonal $x \mapsto (x_i)_{i\in I}$ de M dans M^* est élémentaire. On identifie M à son image, dont les éléments sont dits *standard*. Un autre aspect de cette méthode est son caractère fonctoriel : si l'on a besoin d'un nouvel objet dans l'ultrapuissance, il suffit de l'ajouter à la structure de départ pour en disposer. Par exemple, on peut prendre l'ultrapuissance d'un groupe G, puis avoir besoin d'une fonction longueur dans le nouveau groupe G^* ; il suffit de rajouter la fonction dans le langage et les entiers dans la structure.

4.2 Conséquences

On se donne maintenant un groupe de type fini G, muni de générateurs $x_1, \dots, x_k$, et un ultrafiltre non principal sur un ensemble dénombrable I, que l'on prendra égal à $\mathbb{N}$.

Vu la remarque précédente, on pourra sans problème parler d'entiers, de réels, de cardinal, de longueur, de fonctions à valeurs réelles ou entières, de parties de G, $\mathbb{N}$ ou $\mathbb{R}$, de suites non standard. On fera attention à distinguer

ces parties, fonctions et suites qui apparaissent dans le passage à l'ultrapuissance (c'est à dire les éléments de $(\mathcal{P}(\mathbb{N}))^*$, etc.), appelées *internes*, des parties de G^* par exemple, qui sont plus nombreuses.

Du théorème de Łos découlent entre autres les propriétés suivantes.

Proposition 4.4. *1. $\mathbb{R}^*$ est un corps totalement ordonné.*

2. *Toute partie interne non vide de $\mathbb{N}^*$ a un plus petit élément.*
3. *G^* est un groupe engendré par $x_1, \dots, x_k$ au sens suivant : pour tout $g \in G^*$, il existe $n \in \mathbb{N}^*$ et des fonctions internes $f, h : [\![0, n]\!] \longrightarrow G^*$ telles que*
$$f(0) = e, \quad f(n) = g,$$
$$\forall\, i,\ h(i) \in \{x_1, \dots x_k\} \cup \{x_1, \dots x_k\}^{-1} \text{ et } f(i+1) = f(i)h(i+1).$$
On écrira $g = h(1) \cdots h(n)$ comme s'il s'agissait d'un produit fini.
4. *$|\cdot| : G^* \longrightarrow \mathbb{N}^*$, toujours appelée* longueur*, est le minimum des n pour lesquels les fonctions précédentes existent.*
5. *Les propriétés usuelles des cardinaux finis restent valables, à condition de parler de parties et applications internes.*

Remarque. Certaines parties non vides de $\mathbb{N}^*$ n'admettent pas de plus petit élément (par exemple $\mathbb{N}^* \backslash \mathbb{N}$) ; en particulier, il existe des parties de $\mathbb{N}^*$ qui ne sont pas internes.

La définition de l'ultrapuissance donne la caractérisation suivante des parties internes : une partie P de M^* est interne si, et seulement si, il existe des parties $(P_i)_{i \in I}$ de M appelées *composantes* de P telles que l'on ait

$$(x_i)_{i \in I} \in P \Longleftrightarrow x_i \in P_i \text{ p.p.i.}$$

On dispose également d'une caractérisation analogue des fonctions internes.

Lemme 4.5. *Les parties définissables (éventuellement avec paramètres) sont internes.*
Les fonctions définissables (éventuellement avec paramètres) sont internes.

Démonstration. Il s'agit d'une conséquence immédiate du théorème de Łos : il suffit de considérer la formule

$$\exists P \in \mathcal{P}(M)\ \forall\, x \in M\ \ (x \in P \Longleftrightarrow \varphi(x))$$

et une formule analogue faisant intervenir une fonction définissable. Le cas des parties et fonctions définissables avec paramètres est similaire. □

Lemme 4.6. *Soit $n \in \mathbb{N}^*$. On suppose qu'il existe $M \in \mathbb{N}$ tel que $n \leqslant M$. Alors $n \in \mathbb{N}$. Autrement dit, les entiers non-standard sont infinis.*

Démonstration. Soit $(n_i)_{i\in\mathbb{N}}$ un représentant de n. Alors $n_i \leqslant M$ pour presque tout i. Autrement dit, en notant pour $k \in [\![0, M]\!]$

$$A_k = \{i \in \mathbb{N} \,|\, n_i = k\},$$

on a

$$\bigcup_{k=0}^{n} A_k \in \mathcal{F}.$$

$\mathcal{F}$ étant un ultrafiltre, cela signifie que l'un des A_k est dans $\mathcal{F}$, autrement dit que $n = k$ pour un certain k. Donc $n \in \mathbb{N}$. □

Lemme 4.7. *Tout partie interne infinie de M^* contient un élément non-standard.*

Démonstration. Soit P une partie interne infinie de M^* incluse dans M, et $P_i,\ i \in \mathbb{N}$ des composantes de P. Il existe une suite injective $x_1, x_2, \ldots$ d'éléments de P. Pour tout entier i, on pose $y_i = x_j$ où j est maximal tel que $x_j \in P_i$, s'il existe, et sinon j minimal tel que $j \geqslant i$, $x_j \in P_i$. Alors $(y_i)_{i\in\mathbb{N}}$ est un élément de P, que l'on note y. Par hypothèse, $y \in M$ donc pour presque tout i, $y = y_i$. En particulier, il existe un entier k tel que $y = x_k$. Pour presque tout i, $k < i$; on est donc dans le premier cas et l'on a $x_{k+1} \notin P_i$. On a donc $x_{k+1} \notin P$, ce qui est absurde. □

Lemme 4.8. *Soient $a_n \in M^*$, $n \in \mathbb{N}$. Il existe alors une fonction interne $F : \mathbb{N}^* \longrightarrow M^*$ telle que $\forall\, n \in \mathbb{N},\ F(n) = a_n$.*

Démonstration. On choisit un représentant $(g_{n,i})_{i\in\mathbb{N}}$ pour chaque a_n. Pour $i \in \mathbb{N}$, on note $F_i : \mathbb{N} \longrightarrow M$ qui à n associe $g_{n,i}$. Alors la fonction interne F de composantes F_i convient. □

Remarque. Si les a_n sont dans M, le lemme découle simplement du plongement de $M^{\mathbb{N}}$ dans son ultrapuissance.

Proposition 4.9. *Soit $(\varphi_n(x))_{n\in\mathbb{N}}$ une famille de formules à une variable libre, éventuellement avec paramètres dans M^*. On suppose que cet ensemble de formules est finiment satisfaisable dans M^*, c'est à dire que pour toute partie finie J de $\mathbb{N}$, il existe $x \in M^*$ telles que les $\varphi_j(x)$, $j \in J$, soient vérifiées dans M^*.*

Alors il existe $x \in M^*$ tel que toutes les formules $\varphi_n(x)$ sont vérifiées dans M^*. On dit que la structure M^* est $\aleph_1$-saturée.

Démonstration. Pour tout entier m, on fixe $x_m \in M^*$ satisfaisant $\varphi_0, \ldots, \varphi_m$. On étend $(x_m)_{m\in\mathbb{N}}$ en une suite interne $(x_m)_{m\in\mathbb{N}^*}$. Pour tout m, on considère l'ensemble

$$\{t \in \mathbb{N}^* \,|\, \forall\, k \in \mathbb{N}^*, m \leqslant k \leqslant t \implies \varphi_m(x_k)\}.$$

Cet ensemble est définissable donc interne, et contient $\mathbb{N}$, donc un certain entier non standard $N(m)$. On étend $(N(m))_{m\in\mathbb{N}}$ en une suite interne $(N(m))_{m\in\mathbb{N}^*}$. On considère l'ensemble

$$\{t \in \mathbb{N}^* \,|\, \exists k \in \mathbb{N}^* \ \forall\, m \leqslant t,\ m \leqslant k \leqslant N(m)\}.$$

qui est interne et contient $\mathbb{N}$, donc contient un élément non standard T. On fixe le k correspondant. k est infini et inférieur à tous les $N(m)$ pour $m \in \mathbb{N}$, donc x_k convient. □

4.3 Hyperréels

Étudions à titre d'exemple la structure de $\mathbb{R}^*$, dont les éléments sont appelés *hyperréels*. Il découle du théorème de Łos que $\mathbb{R}^*$ est un corps totalement ordonné dans lequel $\mathbb{R}$ se plonge naturellement.

Définition 4.10. On appelle *hyperréels finis* les éléments de

$$\mathbb{R}_{fin} = \{x \in \mathbb{R}^* | \exists n \in \mathbb{N},\ -n < x < n\}$$

et *infinitésimaux* les éléments de

$$\mathbb{R}_0 = \left\{x \in \mathbb{R}^* | \forall\, n \in \mathbb{N}^{>0},\ -\frac{1}{n} < x < \frac{1}{n}\right\}.$$

Par $\aleph_1$-saturation, l'inclusion de $\mathbb{R}_{fin}$ dans $\mathbb{R}^*$ est stricte, en particulier $\mathbb{R}^*$ n'est pas archimédien. Notons par ailleurs que $\mathbb{R}_{fin}$ et $\mathbb{R}_0$ sont des parties bornées non vides de $\mathbb{R}^*$ qui n'admettent pas de borne supérieure. On en déduit que l'archimédianité et la propriété de la borne supérieure ne sont pas des énoncés du premier ordre.

On remarque que $\mathbb{R}_{fin}$ est un sous-anneau de $\mathbb{R}^*$. De plus, $\mathbb{R}_{fin}$ est un anneau local d'idéal maximal $\mathbb{R}_0$. On note π la projection de $\mathbb{R}^*$ sur le corps $\mathbb{R}_{fin}/\mathbb{R}_0$ et ρ la composée de l'inclusion de $\mathbb{R}$ dans $\mathbb{R}^*$ par π.

Proposition 4.11. *ρ est un isomorphisme de corps.*

Démonstration. ρ étant un morphisme de corps, il suffit de montrer que ρ est surjectif.

Soit x un hyperréel fini. Posons

$$y = \sup\{t \in \mathbb{R} \,|\, t < x\} = \inf\{t \in \mathbb{R} \,|\, x \leqslant t\}.$$

Pour tout entier standard non nul n, il existe un réel entre $x - \frac{1}{n}$ et x (par exemple $\sup \frac{1}{n}\mathbb{Z} \cap]-\infty, x]$) et donc

$$x - \frac{1}{n} \leqslant y \leqslant x + \frac{1}{n},$$

la majoration provenant d'un raisonnement analogue. On en déduit que $x-y$ est infinitésimal puis que $\rho(y) = \pi(x)$. ρ est donc surjectif. □

On peut donc définir l'application « partie standard » $st = \pi \circ \rho^{-1}$, qui à un hyperréel fini associe l'unique réel qui lui est infiniment proche.

Les hyperréels donnent un nouvel aperçu de la notion de limite grâce aux résultats suivants. Jusqu'à la fin de cette partie, f désigne une fonction de $\mathbb{R}$ dans lui-même, qui s'identifie à une fonction interne de $\mathbb{R}^*$ dans lui-même.

Proposition 4.12. *Soit x un réel. f est continue en x si, et seulement si, on a $st\,(f(x+\varepsilon)) = f(x)$ pour tout infinitésimal ε.*

Démonstration. ⋆ Supposons f continue en x. Soit ε un infinitésimal.

Pour tout $n \in \mathbb{N}^{>0}$, il existe un réel strictement positif η tel que

$$\forall\, h \in \mathbb{R} \ : \ |h| < \eta \implies |f(x+h) - f(x)| < \frac{1}{n}$$

et donc

$$\forall h \in \mathbb{R}^* \ : \ |h| < \eta \implies |f(x+h) - f(x)| < \frac{1}{n}$$

et ε étant infinitésimal on a $|\varepsilon| < \eta$.

Ainsi $f(x+\epsilon) - f(x)$ est infinitésimal et donc $st\,(f(x+\varepsilon)) = f(x)$.

⋆ Supposons maintenant que pour tout infinitésimal ε on ait $st\,(f(x+\varepsilon)) = f(x)$.

Soit $(x_n)_{n\in\mathbb{N}}$ une suite de réels convergeant vers x. Considérons la suite $(x_n)_{n\in\mathbb{N}^*}$ d'hyperréels associée. Comme précédemment, on voit que pour tout entier non standard n, x_n est infiniment proche de x et donc $st\,(f(x_n)) = f(x)$.

Pour tout réel strictement positif k l'ensemble

$$\{n \in \mathbb{N}^* \ : \ |f(x_n) - f(x)| > k\}$$

est donc inclus dans $\mathbb{N}$ et définissable, donc interne. Par le lemme 4.7, il est fini ; on en déduit que $(f(x_n))_{n\in\mathbb{N}}$ tend vers $f(x)$ puis que f est continue en x. □

On dispose d'un énoncé similaire en l'infini :

Proposition 4.13. *Soit l un réel.*

f tend vers l en $+\infty$ si et seulement si pour tout hyperréel R positif infini, $f(R)$ est fini et $st\,(f(R)) = l$.

Toujours de la même manière, on obtient un résultat pour les limites infinies :

Proposition 4.14. *f tend vers $+\infty$ en $+\infty$ si et seulement si pour tout hyperréel R positif infini $f(R)$ est positif infini.*

On peut également parler de dérivabilité.

Proposition 4.15. *Soit x un réel.*

f est dérivable en x de dérivée $f'(x)$ si et seulement si pour tout infinitésimal ε, il existe un infinitésimal ζ tel que $f(x+\epsilon) = f(x) + \epsilon f'(x) + \zeta\varepsilon$.

5 L'espace Y

L'idée de la preuve du théorème de Gromov consiste en une récurrence sur le degré de la croissance, que formalise le lemme de récurrence de la section suivante. Pour utiliser ce lemme, il faut construire un morphisme surjectif du groupe vers $\mathbb{Z}$. Dans ce but, on fait agir le groupe par isométries sur un certain espace métrique, que l'on notera Y. On construit ici cet espace grâce à un ultraproduit ; dans la preuve originale de Gromov, Y était obtenu comme une « limite » d'espaces métriques.

Dans toute cette section, G désigne un groupe de type fini, X une partie génératrice finie de ce groupe et C la fonction de croissance de G associée à X. G sera toujours muni de la distance définie en 1.1. Par ailleurs, dans tout espace métrique on notera $B_x(r)$ la boule fermée de centre x et de rayon r. On utilisera également cette notation dans G^* muni de sa distance non-standard à valeurs dans $\mathbb{R}^*$.

5.1 Construction

Soit R un hyperréel positif infini.

Définition 5.1. On notera dans toute cette section

$$G^{(R)} = \left\{ g \in G^* : \frac{|g|}{R} \in \mathbb{R}_{fin} \right\}$$

$$\mu^{(R)} = \left\{ g \in G^* : \frac{|g|}{R} \in \mathbb{R}_0 \right\}.$$

$G^{(R)}$ et $\mu^{(R)}$ sont clairement des sous-groupes de G et $\mu^{(R)} \subset G^{(R)}$. Posons $Y = G^{(R)}/\mu^{(R)}$ et :

$$\begin{array}{rccc} \delta & : & G^{(R)} \times G^{(R)} & \to & \mathbb{R} \\ & & (g,h) & \mapsto & st\left(\frac{|g^{-1}h|}{R}\right). \end{array}$$

Remarquons que si g et h sont des éléments de $G^{(R)}$ congrus respectivement à g' et h' modulo $\mu^{(R)}$ alors $\delta(g,h) = \delta(g',h')$. δ se factorise donc une application d de $Y \times Y$ sur $\mathbb{R}$. Une vérification élémentaire montre que d est une distance.

5.2 Propriétés élémentaires

Proposition 5.2. *L'espace métrique Y est homogène.*

Démonstration. L'action de $G^{(R)}$ sur Y par translation à gauche se fait par isométrie et est transitive. □

Proposition 5.3. *Y est complet.*

Démonstration. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans Y.

Pour tout entier standard n choisissons un représentant g_n de x_n dans $G^{(R)}$. Notons pour tous $k, n \in \mathbb{N}$:

$$\varphi_{k,n}(x) \ : \ |g_n^{-1}x| < 2^{-k}R.$$

Comme la suite est de Cauchy, il existe des entiers $n_0(k)$ tels que l'ensemble de formules

$$\{\varphi_{k,n} \,|\, n \geqslant n_0(k)\}$$

soit finiment satisfaisable (il suffit de choisir g_p pour p assez grand). Par $\aleph_1$-saturation, il existe un $h \in G^*$ satisfaisant toutes les $\varphi_{k,n}$ $(n \geqslant n_0(k))$, qui est clairement dans $G^{(R)}$. Si x désigne la classe d'équivalence de h dans Y, cela signifie que x_n converge vers x dans Y. On en déduit que ce dernier est complet. □

Proposition 5.4. *Pour tout couple (p, q) de points de Y, il existe une isométrie de $[0, d(p, q)]$ dans Y qui à 0 et $d(p, q)$ associe respectivement p et q. En particulier, Y est connexe et localement connexe.*

Démonstration. L'homogénéité de Y nous autorise à supposer que p est la classe d'équivalence de l'identité dans Y. Soit g un représentant de q dans $G^{(R)}$. g s'écrit comme un produit non-standard d'éléments de $X \cup X^{-1}$ (au sens défini précédemment) de longueur minimale $u = |g|$:

$$g = g_1 \cdots g_u.$$

On définit alors :

$$\begin{array}{rccl} f & : & [0, d(p,q)] & \longrightarrow & G^{(R)} \\ & & t & \longmapsto & g_1 \cdots g_{\lfloor tR \rfloor} \text{ si } \lfloor tR \rfloor \leqslant u, \ g \text{ sinon.} \end{array}$$

Si s et t sont des éléments de $[0, d(p, q)]$ tels que $s < t$, on a alors, dans le cas où $\lfloor tR \rfloor \leqslant u$:

$$\begin{aligned} |f(s)^{-1}f(t)| &= |g_{\lfloor sR \rfloor + 1} \cdots g_{\lfloor tR \rfloor}| \\ &= \lfloor tR \rfloor - \lfloor sR \rfloor \end{aligned}$$

sans quoi on contredirait la minimalité de $|g|$, et donc :

$$\begin{aligned} st\left(\frac{|f(s)^{-1}f(t)|}{R}\right) &= st\left(\frac{\lfloor tR \rfloor}{R}\right) - st\left(\frac{\lfloor sR \rfloor}{R}\right). \\ &= t - s \end{aligned}$$

En effet si a est un réel standard alors $\frac{\lfloor aR \rfloor}{R}$ est fini et $st\left(\frac{\lfloor aR \rfloor}{R}\right) = a$ car $\lim\limits_{x \to +\infty} \frac{\lfloor ax \rfloor}{x} = a$.

Si $\lfloor tR \rfloor > u$, on remarque qu'alors :

$$t = st\left(\frac{\lfloor tR \rfloor}{R}\right) \geqslant st\left(\frac{|g|}{R}\right) = d(p,q)$$

et donc $t = d(p,q)$ puis :

$$\begin{aligned} st\left(\frac{|f(s)^{-1}f(t)|}{R}\right) &= st\left(\frac{|g_{\lfloor sR \rfloor + 1} \cdots g_u|}{R}\right) \\ &= st\left(\frac{|g| - \lfloor sR \rfloor}{R}\right) \\ &= d(p,q) - s \\ &= t - s. \end{aligned}$$

L'isométrie recherchée est donc obtenue en composant f par la projection canonique de $G^{(R)}$ sur Y. □

5.3 Compacité locale, dimension de Hausdorff

On montre dans cette partie que si G est à croissance quasi-polynomiale, alors R peut-être choisi de telle manière que Y soit localement compact et de dimension de Hausdorff finie. On montre aussi que si G est à croissance exponentielle, alors il n'existe pas de tel R.

Lemme 5.5. *Soit R_0 un réel positif infini tel que $C(R_0) \leqslant kR_0{}^d$ où k est un réel standard strictement positif et d un entier naturel standard. Alors il existe un réel positif infini S tel que pour tout entier standard i supérieur ou égal à 4 on ait :*

$P(i,S)$: S'il existe t boules fermées disjointes de G^* de rayon $\frac{S}{i}$ dont le centre est dans $B_e\left(\frac{S}{4}\right)$ (où $t \in \mathbb{N}^*$), alors $t \leqslant i^{d+1}$.

Démonstration. Supposons ce résultat faux. On va montrer qu'alors $B_e(R_0)$ contient trop d'éléments. La fonction f, qui à S positif inférieur à R_0 associe le plus petit entier i supérieur à 4 tel que $P(i,S)$ soit fausse (s'il existe) et 4 sinon (S est alors nécessairement fini) est interne car définissable. Mais on a la propriété :

$$\forall a \in \mathbb{R}\, \forall \varphi \in \mathbb{N}^{\mathbb{R}}\, \exists v \in \mathbb{N}^{\mathbb{N}} \ : \ v(0) = 1 \wedge \left(\forall n \in \mathbb{N} v(n+1) = \varphi\left(\frac{a}{4v(0)\cdots v(n)}\right)\right)$$

et donc par Łos

$$\forall a \in \mathbb{R}^*\, \forall \varphi \in \left(\mathbb{N}^{\mathbb{R}}\right)^*\, \exists v \in \left(\mathbb{N}^{\mathbb{N}}\right)^* \ : \ v(0) = 1 \wedge \left(\forall n \in \mathbb{N}^* v(n+1) = \varphi\left(\frac{a}{4v(0)\cdots v(n)}\right)\right).$$

On note $(i_n)_{n\in\mathbb{N}^*}$ la suite obtenue en appliquant cette propriété à R_0 et f. Notons que pour tout entier n plus grand que 1 on a $4 \leqslant i_n$ et donc $\frac{R_0}{4i_0\cdots i_n} \leqslant \frac{R_0}{4^{n+1}}$. Par conséquent, $\lim_{n\to\infty} \frac{R_0}{4i_0\cdots i_n} = 0$. On note u le plus petit élément de l'ensemble définissable non vide $\left\{n \in \mathbb{N}^* : \frac{R_0}{4i_0\cdots i_n} < \ln(R_0)\right\}$.

Par un raisonnement similaire, on construit une fonction interne g de $\mathbb{N}^* \times \mathbb{N}^*$ dans G^* telle que pour tout entier l entre 1 et u, en posant $t_l = (i_l)^{d+1} + 1$, $g(l,1), \ldots, g(l,t_l)$ sont dans $B_e\left(\frac{R_0}{4i_1\cdots i_{l-1}}\right)$ et si j et j' sont des entiers distincts entre 1 et t_l alors $B_{g(l,j)}\left(\frac{R_0}{i_1\cdots i_l}\right)$ et $B_{g(l,j')}\left(\frac{R_0}{i_1\cdots i_l}\right)$ sont disjointes. L'existence de tels éléments suit de la définition de f.

Posons alors $T = \{(s_1, \ldots, s_u) \in (\mathbb{N}^*)^u : \forall l \in \{1, \ldots, u\}\, 1 \leqslant s_l \leqslant t_l\}$, où $(\mathbb{N}^*)^u$ désigne l'ensemble des fonctions internes de $[\![1, u]\!]$ dans $\mathbb{N}^*$. Posons également pour tout $s = (s_1, \ldots, s_l) \in T$: $g_s = g(1, s_1)g(2, s_2)\cdots g(u, s_u)$ et notons qu'alors :

$$|g_s| \leqslant \sum_{l=1}^{u} |g(l, s_l)| \leqslant \sum_{l=1}^{u} \frac{R_0}{4i_1\cdots i_{l-1}} \leqslant \sum_{l=1}^{u} \frac{R_0}{4^l} < R_0$$

et donc g_s est dans $B_e(R_0)$.

Soient $s = (s_1, \ldots, s_u)$ et $s' = (s'_1, \ldots, s'_u)$ deux éléments distincts de T. Supposons $g_s = g_{s'}$ et notons alors $v = \min\{k \in \{1, \ldots, u\} : s_k \neq s'_k\}$. Ainsi :

$$g(v, s_v)\cdots g(u, s_u) = g(v, s'_v)\cdots g(u, s'_u)$$

et donc

$$g(v, s'_v)^{-1}g(v, s_v) = g(v+1, s'_{v+1})\cdots g(u, s'_u)g(u, s_u)^{-1}\cdots g(v, s_{v+1})^{-1}$$

d'où puisque $B_{g(v,s_v)}\left(\frac{R_0}{i_1\cdots i_v}\right)$ et $B_{g(v,s'_v)}\left(\frac{R_0}{i_1\cdots i_v}\right)$ sont disjointes

$$\begin{aligned}
\frac{R_0}{i_1\cdots i_v} &\leqslant |g(v, s'_v)^{-1}g(v, s_v)| \\
&\leqslant \sum_{l=v+1}^{u} |g(l, s_l)| + |g(l, s'_l)| \\
&\leqslant 2\sum_{l=v+1}^{u} \frac{R_0}{4i_1\cdots i_{l-1}} \\
&\leqslant \frac{R_0}{2i_1\cdots i_v} \sum_{l=v+1}^{u} \frac{1}{i_{v+1}\cdots i_{l-1}} \\
&\leqslant \frac{R_0}{2i_1\cdots i_v} \sum_{l=v+1}^{u} \frac{1}{4^{l-v-1}} \\
&< \frac{R_0}{i_1\cdots i_v}
\end{aligned}.$$

Ce qui est absurde. $s \mapsto g_s$ est donc injective.

Notons par ailleurs que cette fonction est interne car définissable. On en déduit alors que :

$$\begin{aligned} C(R_0) &\geqslant \#T \\ &\geqslant \prod_{l=1}^{u} {i_l}^{d+1} \\ &\geqslant \left(\frac{R_0}{\ln R_0}\right)^{d+1} \\ &> k{R_0}^d \end{aligned}.$$

Le passage de l'avant-dernière ligne à la dernière provient du fait que R_0 est infini positif, et $\#$ désigne l'extension non-standard de la fonction cardinal.

Cette contradiction achève la preuve du lemme. □

Lemme 5.6. *Les propriétés suivantes sont équivalentes :*

1. *Y est localement compact ;*
2. *une boule fermée de Y est compacte ;*
3. *toute boule fermée de Y est compacte.*

Démonstration. Il est clair que le troisième point implique le premier qui implique le deuxième, Y étant non vide.

Supposons donc le deuxième point vérifié. Soient $x \in Y$ et r un réel strictement positif tels que $B_x(r)$ soit compacte. Il existe alors des éléments $x_1,\ldots,x_n$ de $B_x(r)$ tels que

$$B_x(r) \subset \bigcup_{i=1}^{n} B_{x_i}\left(\frac{r}{2}\right).$$

Soit y un élément de $B_x\left(\frac{3r}{2}\right)$. Par la proposition 5.4, il existe un point z de Y tel que $d(x,z) = r$ et $d(y,z) = d(x,y) - r \leqslant \frac{r}{2}$. Mais alors $z \in B_{x_i}\left(\frac{r}{2}\right)$ pour un certain i entre 1 et n et donc $y \in B_{x_i}(r)$. On a donc

$$B_x\left(\frac{3r}{2}\right) \subset \bigcup_{i=1}^{n} B_{x_i}(r).$$

Par homogénéité de Y, les $B_{x_i}(r)$ sont isométriques à $B_x(r)$ donc compactes, et par conséquent $B_x\left(\frac{3r}{2}\right)$ est compacte. Par une récurrence immédiate, il vient que toute les boules fermées centrées en x sont compactes puis par homogénéité de Y que toutes les boules fermées de Y sont compactes. □

Proposition 5.7. *Soit d un entier naturel standard. Si G est à croissance quasi-polynomiale de degré au plus d, alors il existe un choix de R pour lequel Y est localement compact et de dimension de Hausdorff inférieure à $d+1$.*

Démonstration. Soit k la constante qui apparaît dans la définition d'être à croissance polynomiale. L'ensemble $\left\{r \in \mathbb{N}^*, C(r) \leqslant kr^d\right\}$ est interne et infini, et il contient donc un entier non standard R_0. En particulier, R_0 est un hyperréel positif infini tel que $C(R_0) \leqslant k{R_0}^d$. On note S l'hyperréel positif infini dont l'existence est donné par le lemme 5.5 et on pose $R = \frac{S}{4}$. Montrons que ce choix de R rend Y localement compact et de dimension de Hausdorff inférieure à $d+1$.

Soit n un entier standard strictement positif. Notons que si t est un élément de $\mathbb{N}^*$ et s'il existe $g_1, \ldots, g_t$ des éléments de $B_e(R)$ tels que les boules $B_{g_1}\left(\frac{R}{n}\right), \ldots, B_{g_t}\left(\frac{R}{n}\right)$ soient disjointes, alors $t \leqslant (4n)^{d+1}$ par définition de R, et en particulier t est fini. Prenons donc t maximal parmi les entiers ayant cette propriété et notons $g_1, \ldots, g_t$ des éléments de $B_e(R)$ qui la réalisent. Alors $B_e(R) \subseteq \bigcup_{i=1}^{t} B_{g_i}\left(2\frac{R}{n}\right)$ sans quoi on contredirait la maximalité de t. On a donc recouvert la boule fermée de centre $e\mu^{(R)}$ et de rayon 1 de Y par au plus $(4n)^{d+1}$ boules fermées de rayon $\frac{2}{n}$.

On en déduit que la boule fermée de rayon 1 de Y est précompacte puis, Y étant complet, qu'elle est compacte. Le lemme 5.3 assure donc que Y est localement compact. On en déduit également que la boule fermée de centre $e\mu^{(R)}$ et de rayon 1 est de mesure de Hausdorff de dimension $d+1$ inférieure à 16^{d+1}. En particulier, la dimension de Hausdorff de celle-ci est inférieure à $d+1$. Y étant homogène, c'est le cas de toutes les boules fermées de rayon 1 de Y. Enfin, Y étant connexe et localement compact il est séparable et peut donc être recouvert par un ensemble dénombrable de boules fermées de rayon 1. Y est donc de dimension de Hausdorff inférieure à $d+1$. □

Lemme 5.8. *La suite $\left(C(n)^{\frac{1}{n}}\right)_{n\in\mathbb{N}}$ admet une limite r. De plus, G est à croissance exponentielle si et seulement si $r > 1$.*

Démonstration. Pour tout $n \in \mathbb{N}$, posons $a_n = \ln(C(n))$.

Pour des raisons de dénombrement élémentaires, pour tout $(m,n) \in \mathbb{N}^2$, on a $C(n+m) \leqslant C(n)C(m)$ et donc $a_{n+m} \leqslant a_n + a_m$. Posons $b = \inf_{n\in\mathbb{N}^{>0}} \frac{a_n}{n}$. b est un élément de $\mathbb{R} \cup \{-\infty\}$. La suite $\left(\frac{a_n}{n}\right)_{n\in\mathbb{N}^{>0}}$ tend vers b (c'est un résultat classique) et on a le premier point en passant à l'exponentielle.

Le deuxième point est aisé. □

Proposition 5.9. *Si G est à croissance exponentielle alors aucun choix de R ne rend Y localement compact.*

Démonstration. On suppose G à croissance exponentielle et on note

$$r = \lim_{n\to\infty} C(n)^{\frac{1}{n}} > 1.$$

On a alors $st\left(C(R)^{\frac{1}{R}}\right) = st\left(C(2R)^{\frac{1}{2R}}\right) = r$ et donc

$$st\left(\left(\frac{C(2R)}{C(R)}\right)^{\frac{1}{R}}\right) = r > 1.$$

On en déduit que $\frac{C(2R)}{C(R)}$ est infini. Mais alors on ne peut pas recouvrir $B_e(2R)$ par un nombre fini de $B_g(R)$ avec $g \in G^{(R)}$. En effet, on a pour tout $k \in \mathbb{N}$ la propriété :

$$\forall R \in \mathbb{R} : \left(\exists g_1, \ldots, g_k \in G, \forall x \in G : |x| \leqslant 2R \implies \bigvee_{i=1}^{k} |g_i^{-1}x| \leqslant R\right) \implies \frac{C(2R)}{C(R)} \leqslant k$$

et donc par le théorème de Łos

$$\forall R \in \mathbb{R}^* : \left(\exists g_1, \ldots, g_k \in G^*, \forall x \in G^* : |x| \leqslant 2R \implies \bigvee_{i=1}^{k} |g_i^{-1}x| \leqslant R\right) \implies \frac{C(2R)}{C(R)} \leqslant k.$$

On ne peut donc pas recouvrir la boule fermée de centre $e\mu^{(R)}$ et de rayon 2 de Y par un nombre fini de boules de rayon 1, celle-ci n'est donc pas compacte et par le lemme 5.3, Y n'est pas localement compact. □

5.4 Action de G sur Y

Notons φ le morphisme de G^* dans le groupe des isométries de Y défini par l'action à gauche de G^* sur Y.

Définition 5.10. On munit le groupe $Isom(Y)$ des isométries de Y d'une structure de groupe topologique en choisissant comme base de voisinages de l'identité les ensembles (fermés)

$$U_{k,\varepsilon} = \{\sigma \in Isom(Y) \,|\, d(\sigma y, y) \leqslant \varepsilon \text{ pour tout } y \in B_{e\mu^{(R)}}(k)\}.$$

Il s'agit de la topologie mentionnée dans le théorème 2.11.

Nous allons démontrer dans cette section :

Proposition 5.11. *Si $\varphi(G)$ est fini et si G n'a pas de sous-groupe abélien d'indice fini, alors pour tout voisinage U de l'identité de Y dans $Isom\,(Y)$, il existe un morphisme de* $\mathrm{Ker}\left(\varphi_{|G}\right)$ *dans $Isom\,(Y)$ dont l'image intersecte U en un point distinct de l'identité.*

Ce morphisme sera en fait obtenu en considérant l'action d'un conjugué de $\mathrm{Ker}\left(\varphi_{|G}\right)$ sur Y. Dans toute la suite on notera $G' = \mathrm{Ker}\left(\varphi_{|G}\right)$. On suppose jusqu'à la fin de cette section que $\varphi\,(G)$ est fini. G' est alors d'indice fini dans G et donc de type fini, on en note S une partie génératrice finie. Enfin, on suppose que G n'a pas de sous-groupe abélien d'indice fini.

Lemme 5.12. *Sous ces hypothèses, l'ensemble* $\{|g^{-1}sg| : g \in G', s \in S\}$ *n'est pas borné dans* $\mathbb{N}$.

Démonstration. Si M était une borne de cet ensemble, tout s dans S aurait au plus M conjugués par des éléments de G' et donc son centralisateur serait d'indice au plus M dans G'. Mais alors le centre de G' qui n'est autre que l'intersection des centralisateurs des éléments de S serait d'indice fini dans G' par 2.4, ce qui contredit l'absence de sous-groupe abélien d'indice fini dans G. □

Pour tout g dans G^* et tout r strictement positif dans $\mathbb{R}^*$ posons :

$$\delta(g,r) = \max\left\{|a^{-1}ga| : a \in B_e(r)\right\}.$$

Lemme 5.13. *Pour tous* h *et* g *dans* G^* *et tout* r *strictement positif dans* $\mathbb{R}^*$ *on a :*

$$\delta\left(h^{-1}gh, r\right) \leqslant \delta(g,r) + 2|h|.$$

Démonstration. Si a est dans $B_e(r)$ alors

$$|a^{-1}h^{-1}gha| = |(ha)^{-1}gha| \leqslant \delta(g, |h| + r).$$

Mais un élément de $B_e(|h| + r)$ s'écrit comme le produit d'un élément b de $B_e(r)$ et d'un élément c de $B_e(|h|)$ et :

$$|(bc)^{-1}gbc| = |c^{-1}b^{-1}gbc| \leqslant 2|c| + |b^{-1}gb| \leqslant 2|h| + \delta(g,r).$$

On a donc $\delta(g, |h| + r) \leqslant \delta(g,r) + 2|h|$ puis l'inégalité annoncée. □

Proposition 5.14. *Sous les mêmes hypothèses, pour tout voisinage* U *de l'identité de* Y *dans* $Isom(Y)$*, il existe* β *dans* $(G')^*$ *et* s *dans* S *tels que* $\beta^{-1}G'\beta \subset G^{(R)}$ *et* $\varphi\left(\beta^{-1}s\beta\right)$ *est un point de* U *distinct de l'identité.*

Remarquons que cette proposition donne immédiatement la proposition 5.11.

Démonstration. Soient k, ε des réels strictement positifs. Le lemme 5.12 et le théorème de Łos donnent alors l'existence de g dans $(G')^*$ et de s dans S tels que $|g^{-1}sg| > \varepsilon R$. Écrivons alors $g = s_1 \cdots s_t$ où les s_i sont des éléments de S et t un élément de $\mathbb{N}^*$. Pour i entre 0 et t, posons $g_i = s_1 \cdots s_i$ et $M_i = \max\left\{\delta\left(g_i^{-1}sg_i, kR\right) : s \in S\right\}$. Posons en outre $A = \max\{|s| : s \in S\}$ et notons que A est un entier standard.

Remarquons que pour tous s dans S et tout i entre 0 et $t-1$, on a par le lemme 5.13 :

$$\begin{aligned}\delta\left(g_{i+1}^{-1}sg_{i+1}, kR\right) &= \delta\left(s_{i+1}^{-1}g_i^{-1}sg_is_{i+1}, kR\right)\\ &\leqslant \delta\left(g_i^{-1}sg_i, kR\right) + 2|s_{i+1}|\\ &\leqslant M_i + 2A\end{aligned}$$

et de la même manière $\delta\left(g_i^{-1}sg_i, kR\right) \leqslant M_{i+1} + 2A$. On en déduit que pour tout i entre 0 et $t-1$, $|M_{i+1} - M_i| \leqslant 2A$. On remarque également que M_0 est infinitésimal, car les éléments de s sont dans le noyau de φ, et en particulier $M_0 < \varepsilon R$. De plus, g a été choisi de telle manière que $M_t > \varepsilon R$. La fonction qui à i associe M_i étant interne (elle est définissable à partir de celle qui à i associe g_i et celle-ci est interne par définition de « $g = s_1 \cdots s_t$ »), il existe i_0 entre 0 et t telle que $|M_{i_0} - \varepsilon R| \leqslant 2A$. Posons alors $\beta = g_{i_0}$. β est ainsi un élément de $(G')^*$ car celui-ci est engendré par S.

De plus, les éléments de $\beta^{-1}G'\beta$ sont des produits finis de conjugués par β d'éléments de S et sont donc de longueur plus petite qu'un multiple fini de $M_{i_0} \leqslant \varepsilon R + 2A$. On en déduit $\beta^{-1}G'\beta \subset G^{(R)}$.

Notons s un élément de S tel que $\delta\left(\beta^{-1}s\beta, kR\right) = M_{i_0}$. Ainsi $\sigma = \varphi\left(\beta^{-1}s\beta\right)$ n'est pas l'identité puisque $st\left(\frac{\delta\left(\beta^{-1}s\beta, kR\right)}{R}\right) \geqslant \varepsilon > 0$. D'autre part, comme $M_{i_0} \leqslant \varepsilon R + 2A$, si a est un élément de $B_e\left(kR\right)$ on a

$$d\left(\sigma\left(a\mu^{(R)}\right), a\mu^{(R)}\right) = st\left(\frac{|a^{-1}\beta^{-1}s\beta a|}{R}\right) \leqslant \varepsilon.$$

On a donc $\sigma \in U_{k,\varepsilon}$, d'où le résultat annoncé. □

6 Fin de la preuve

6.1 Construction d'un morphisme vers $\mathbb{Z}$

Dans cette section, nous allons montrer le théorème suivant.

Théorème 6.1. *Soit G un groupe de cardinal infini à croissance polynomiale. Alors il existe un morphisme surjectif d'un sous-groupe d'indice fini de G sur $\mathbb{Z}$.*

Pour cela nous rappelons le résultat de la section précédente :

Théorème 6.2. *Soit G un groupe à croissance polynomiale. Il existe un espace métrique Y et un morphisme φ de G dans $Isom(Y)$ tels que :*
- *Y est complet, connexe, localement connexe, localement compact et de dimension de Hausdorff finie ;*
- *si $\varphi(G)$ est fini et si G n'a pas de sous-groupe abélien d'indice fini, alors pour tout voisinage U de l'identité de Y dans $Isom(Y)$, il existe un morphisme f de $\operatorname{Ker}\varphi$ dans $Isom(Y)$ dont l'image rencontre $U \setminus \{1_Y\}$.*

Soit donc G un groupe infini à croissance polynomiale. On note Y et φ l'espace métrique et le morphisme donnés par le théorème 6.2. Si G a un sous-groupe abélien d'indice fini (et donc de cardinal infini), le résultat découle immédiatement du théorème de structure des groupes abéliens de type fini, on suppose donc que ce n'est pas le cas. Par 2.11, il vient que $Isom(Y)$ est un groupe de Lie qui a un nombre fini de composantes connexes. Notons L la composante connexe de l'identité de Y dans $Isom(Y)$. L est ainsi un groupe de Lie connexe d'indice fini dans $Isom(Y)$. Notons C le centre de L. Par 2.10, L/C se plonge dans $GL_m(\mathbb{C})$ où $m = dim(L)$. On note $\pi : L \longrightarrow L/C \hookrightarrow GL_m(\mathbb{C})$ la surjection canonique.

Lemme 6.3. *G admet un sous-groupe d'indice fini H tel que pour tout entier n il existe un morphisme f de H dans L d'image de cardinal plus grand que n.*

Démonstration. Si $\varphi(G)$ est de cardinal infini alors $\varphi^{-1}(L)$ convient. Sinon, on note K le noyau de φ qui est donc d'indice fini dans G. Par ailleurs, on sait par 2.9 que pour tout entier n, il existe un voisinage U_n de l'identité dans L ne contenant pas d'élément d'ordre inférieur à n autre que l'identité.

D'après 6.2, il existe pour tout entier n un morphisme g_n de K dans $Isom(Y)$ dont l'image rencontre U_n en un point distinct de l'identité. Le cardinal de $\operatorname{Im} g_n \cap L$ est donc plus grand que n. De plus, $\operatorname{Im} g_n \cap L$ est d'indice inférieur à $[Isom(Y) : L]$ dans $\operatorname{Im} g_n$ et donc par 2.2, $g_n^{-1}(L)$ est d'indice inférieur à $[Isom(Y) : L]$ dans K. L'ensemble de ces sous-groupes

de K est donc fini et par conséquent K admet un sous-groupe H qui est égal à $g_n^{-1}(L)$ pour une infinité d'entiers n et qui vérifie donc la propriété voulue. □

Pour tout entier n, notons f_n un morphisme de H sur L dont l'image est de cardinal plus grand que n.

Lemme 6.4. *Supposons qu'il existe un entier q tel que pour tout entier n on ait $|\mathrm{Im}\ (\pi \circ f_n)| \leqslant q$. Alors il existe un morphisme surjectif d'un sous-groupe d'indice fini de G sur $\mathbb{Z}$.*

Démonstration. Posons $N = \cap_{n\in\mathbb{N}}\mathrm{Ker}\ (\pi \circ f_n)$. N est une intersection de sous-groupes de H d'indice inférieur à q. Cette intersection est donc finie, et N est d'indice fini dans H. Notons k l'indice de N dans H. Pour tout $n \in \mathbb{N}$, on a

$$[\mathrm{Im}\ f_n : f_n(N)] \leqslant [H : N] = k$$

et par conséquent

$$|f_n(N)| \geqslant \frac{n}{k}.$$

N a donc des quotients abéliens de cardinal arbitrairement grand. L'abélianisé de N est donc de cardinal infini. Comme il est par ailleurs de type fini (N est d'indice fini dans G), le théorème de structure des groupes abéliens de type fini nous donne le morphisme annoncé. □

Lemme 6.5. *Supposons que pour tout entier n, $\mathrm{Im}\ (\pi \circ f_n)$ est de cardinal fini et que $(|\mathrm{Im}\ (\pi \circ f_n)|)_{n\in\mathbb{N}}$ n'est pas bornée. Alors il existe un morphisme surjectif d'un sous-groupe d'indice fini de G sur $\mathbb{Z}$.*

Démonstration. Par 2.12, il existe un entier q tel que tout sous-groupe fini de $GL_m(\mathbb{C})$ admet un sous-groupe abélien d'indice inférieur à q. En particulier, pour tout entier n, $\mathrm{Im}\ (\pi \circ f_n)$ admet un sous-groupe abélien H_n d'indice inférieur à q. Mais alors par 2.2, pour tout entier n, le sous-groupe $g_n^{-1}(H_n)$ est d'indice inférieur à q dans H. L'ensemble de ces sous-groupes est fini, donc H admet un sous-groupe N tel que $N = g_n^{-1}(H_n)$ pour une infinité d'entiers n. N est alors d'indice fini dans H (et donc dans G) et admet des quotients abéliens arbitrairement grands. L'abélianisé de N est donc de cardinal infini et on conlut de la même manière que pour le lemme précédent. □

Lemme 6.6. *Supposons qu'il existe un entier n tel que $\mathrm{Im}\ (\pi \circ f_n)$ est de cardinal infini. Alors il existe un morphisme surjectif d'un sous-groupe d'indice fini de G sur $\mathbb{Z}$.*

Démonstration. Sous ces hypothèses, il existe un morphisme f de H vers $GL_m(\mathbb{C})$ dont l'image M est infinie. Par 2.13, M admet un sous-groupe libre de rang 2 ou M admet un sous-groupe résoluble d'indice fini. Or, M étant l'image de H, M est de type fini et à croissance polynomiale (pour des parties génératrices bien choisies, la fonction de croissance de M est majorée par celle de H), M ne peut donc admettre un sous-groupe libre de rang 2. M a donc un sous-groupe d'indice fini résoluble M'. Quitte à remplacer M par M' et H par $f^{-1}(M')$, on peut supposer M résoluble.

Il existe alors une suite de sous-groupes :

$$M = M_0 \rhd M_1 \rhd M_2 \rhd \cdots \rhd M_k = 1$$

dont les facteurs sont abéliens. Mais on a alors :

$$[M_0 : M_1]\,[M_1 : M_2] \cdots [M_{k-1} : M_k] = [M : 1] = |M| = \infty$$

et il existe donc i tel que $[M_i : M_{i+1}]$ est infini. Si de plus i est minimal parmi les entiers ayant cette propriété, M_i est d'indice fini dans M. Comme ci-dessus, on peut donc supposer que $M = M_i$. Mais alors l'abélianisé de M est de cardinal infini d'où l'existence d'un morphisme surjectif de M vers $\mathbb{Z}$. □

6.2 Lemme de récurrence

Lemme 6.7. *Soit G un groupe de type fini à croissance non-exponentielle. Alors pour tout $g \in G$, pour tout $k \in G$, le sous-groupe K de G engendré par les $g^n k g^{-n}$, $n \in \mathbb{Z}$ est de type fini.*

Démonstration. Pour tout $n \in \mathbb{Z}$, on note $e_n = g^n k g^{-n}$. On considère les mots de G de la forme $e_0^{\varepsilon_0} \cdots e_m^{\varepsilon_m}$, avec $\varepsilon \in \{0,1\}^{m+1}$. On remarque que

$$e_0^{\varepsilon_0} \cdots e_m^{\varepsilon_m} = k^{\varepsilon_0} g k^{\varepsilon_1} g \cdots k^{\varepsilon_{m-1}} g k^{\varepsilon_m} g^{-m}$$

Ces mots sont donc de longueur au plus $3m+1$ dans un système générateur adapté, et il y en a 2^{m+1}. Selon l'hypothèse de croissance, pour un certain $m > 0$ deux de ces mots doivent être égaux ; quitte à simplifier, cette égalité s'écrit

$$e_0^{\varepsilon_0} \cdots e_m^{\varepsilon_m} = e_0^{\delta_0} \cdots e_m^{\delta_m}\ , \quad \varepsilon_m \neq \delta_m.$$

Ainsi $e_m \in \langle e_0, \ldots, e_{m-1} \rangle$. Par une récurrence immédiate, c'est également le cas des e_p pour $p \geqslant m$. En raisonnant de même pour les m négatifs, on montre que pour un certain M,

$$\{e_p \,|\, p \in \mathbb{Z}\} \subset \langle e_p\,,\ |p| \leqslant M \rangle$$

et donc que K est de type fini. □

Théorème 6.8 (Lemme de récurrence)**.** *Soit G un groupe de type fini à croissance non-exponentielle, et K un sous-groupe de G. On suppose qu'il existe un morphisme de groupes $h : G \longrightarrow \mathbb{Z}$ surjectif de noyau K. Alors :*

1. *K est de type fini ;*
2. *Si G est à croissance polynomiale de degré au plus $d+1$, K est à croissance polynomiale de degré au plus d ;*
3. *Si K est virtuellement nilpotent, alors G l'est aussi.*

Remarque. Ce lemme et une récurrence immédiate terminent la preuve du théorème de Gromov.

Démonstration. Nous pouvons déjà montrer les deux premiers points :

- ⋆ Montrons que K est de type fini. Soit $\gamma \in G$ tel que $h(\gamma) = 1$. On complète γ en une partie finie $(\gamma, e_1, \ldots, e_n)$ génératrice de G. Quitte à multiplier les e_i par une certaine puissance de γ, on peut supposer que les e_i sont dans $\operatorname{Ker} h = K$. Alors K est engendré par les $\gamma_{m,i} = \gamma^m e_i \gamma^{-m}$, pour $1 \leqslant i \leqslant n,\ m \in \mathbb{Z}$.
  En effet, si $k = \gamma^{m_1} e_{i_1} \cdots \gamma^{m_p} e_{i_p}$ est un élément de K, on peut écrire :
  $$k = \gamma_{m_1,i_1} \gamma_{m_1+m_2,i_2} \cdots \gamma_{m_1+\cdots+m_p,i_p} \gamma^{m_1+\cdots+m_p}$$
  et $m_1 + \cdots + m_p = 0$ puisque $k \in \operatorname{Ker} h$. K est donc de type fini par le lemme précédent.
- ⋆ Supposons G à croissance polynomiale de degré au plu $d+1$. On choisit une partie finie Y génératrice de K, et l'on pose $X = Y \cup \{\gamma\}$, qui est une partie génératrice de G. Par hypothèse, on peut trouver $k > 0$ tel que
  $$\forall\, n \in \mathbb{N}^{>0},\ C_X(n) \leqslant k n^{d+1}.$$
  Soit $n \in \mathbb{N}$ et soient $g_i,\ 1 \leqslant i \leqslant C_Y(n)$ les éléments de K de longueur sur Y inférieure à n. Alors les $g_i \gamma^j,\ 1 \leqslant i \leqslant C_Y(n),\ -n \leqslant j \leqslant n$ sont $(2n+1)C_Y(n)$ éléments distincts de G de longueur sur X au plus $2n$. On en déduit :
  $$(2n+1)C_Y(n) \leqslant k(2n)^{d+1}, \quad \text{donc} \quad C_Y(n) \leqslant (2^d k) n^d.$$

□

Pour la dernière propriété, nous aurons besoin d'une définition et de deux lemmes.

Définition 6.9. Un endomorphisme d'un espace vectoriel de dimension finie est dit *semi-simple* s'il est diagonalisable, modulo extension des scalaires à un corps algébriquement clos. Cette définition est cohérente car le polynôme minimal est invariant par les extensions des scalaires.

Il est équivalent de demander que tout sous-espace stable admet un supplémentaire stable.

Lemme 6.10. *On suppose K nilpotent et on se donne $z \in G$ tel que $h(z) = 1$. Alors il existe une suite centrale $(L_i)_{1 \leqslant i \leqslant N}$ de K telle que*

1. *$zL_iz^{-1} \subset L_i$ pour tout i ;*
2. *L_i/L_{i+1} est soit fini, soit un groupe abélien libre de type fini ;*
3. *Si L_i/L_{i+1} est abélien libre, alors l'automorphisme α_i de $(L_i/L_{i+1}) \otimes \mathbb{C}$ induit par $g \mapsto zgz^{-1}$ est semi-simple.*

Démonstration. On remarque tout d'abord que la suite centrale descendante est formée de sous-groupes caractéristiques, donc normalisés par z. Dans les facteurs de cette suite, qui sont des groupes abéliens de type fini selon le lemme 2.6, les sous-groupes de torsion sont également normalisés par z : quitte à raffiner la suite en mettant de côté les facteurs de torsion, on s'est donc ramené au cas où tous les L_i sont normalisés par z et où L_i/L_{i+1} est soit fini, soit un groupe abélien libre de type fini.

On effectue ensuite l'opération suivante : tant que l'un des α_i stabilise un sous-groupe de rang non nul et non maximal, on raffine la suite par ce sous-groupe. La suite obtenue est toujours normalisée par z et le processus termine : on peut donc supposer qu'un sous-groupe de L_i/L_{i+1} stable par un α_i est de rang nul ou maximal.

Montrons que les α_i ainsi obtenus sont semi-simples. Soit P_i le polynôme minimal de α_i, étendu à $(L_i/L_{i+1}) \otimes \mathbb{Q}$ qui est de dimension finie. Alors P_i est irréductible sur $\mathbb{Q}$: en effet, si ce n'était pas le cas, selon le lemme des noyaux il existerait un $\mathbb{Q}$-sous-espace vectoriel non trivial stable, donc un sous-groupe de L_i/L_{i+1} stable qui serait de rang non nul et non maximal, ce qui est exclu.

P_i est irréductible sur $\mathbb{Q}$ donc premier avec son polynôme dérivé. Par conséquent, P_i est scindé à racines simples sur $\mathbb{C}$: α_i est semi-simple. □

Lemme 6.11. *Soit L un groupe abélien libre de type fini et α un automorphisme de L, que l'on étend en un automorphisme de l'espace vectoriel complexe $L \otimes \mathbb{C}$.*

1. *Si α est semi-simple et si toutes ses valeurs propres sont de module 1, alors α est d'ordre fini.*
2. *Si α admet une valeur propre de module supérieur à 2, alors il existe $x \in L$ tel que les sommes finies $\sum \varepsilon_i \alpha^i(x)$, avec $\varepsilon_i \in \{0, 1\}$, sont deux à deux distincts.*

Démonstration. 1. $L \otimes \mathbb{C}$ est de dimension finie, donc ses parties bornées sont relativement compactes. Dans $L \otimes \mathbb{C}$, une orbite pour l'action des α^k, $k \in \mathbb{Z}$ est donc relativement compacte. Cela est donc également vrai dans L. Or les parties relativement compactes de L sont les parties finies : toutes les orbites via α dans L sont donc finies. C'est vrai en particulier pour un système générateur fini de L : α est donc de type fini.

2. Il n'y a pas de raison a priori pour que l'espace propre correspondant à cette valeur propre ρ contienne un élément non nul de L.

   α admet ρ comme valeur propre donc son adjoint également : autrement dit, il existe une forme linéaire non nulle β sur $L \otimes \mathbb{C}$ telle que $\beta \circ \alpha = \rho\beta$. Il existe $x \in L$ tel que $\beta(x) \neq 0$, puisque Vect(L)=$L \otimes \mathbb{C}$. Alors :

$$\beta\left(\sum \varepsilon_i \alpha^i(x)\right) = \left(\sum \varepsilon_i \rho^i\right)\beta(x)$$

   et les $\sum \varepsilon_i \rho^i$ sont deux à deux distinctes vu l'hypothèse.

□

Terminons maintenant la preuve du théorème 6.8.

Démonstration. Une première étape consiste à se ramener au cas où K est réellement nilpotent, quitte à considérer K' un sous-groupe nilpotent de K d'indice fini, distingué dans G, et à remplacer G par le sous-groupe de G' de G engendré par K' et z, où z est un élément fixé d'image 1. En effet :

1. K' existe, car si H est un sous-groupe nilpotent de K d'indice fini, $\bigcap_{g\in G} gHg^{-1}$ est un sous-groupe de K qui est toujours nilpotent et d'indice fini, mais qui est distingué dans G.
2. Comme K' est clairement le noyau de h restreint à G', il reste à remarquer que G' est d'indice fini dans G, en fait au plus $[K : K']$.

On se donne alors une suite de décomposition (L_i) de K comme dans le premier lemme. Alors de deux choses l'une :

1. Soit les α_i sont tous d'ordre fini, il existe p tel que α_i^p est l'identité pour tout i. Alors le sous-groupe de G engendré par K et z^p est nilpotent (la série $(\langle L_i, z^p\rangle)$ convient) et d'indice fini dans G.
2. Soit il existe j tel que α_j est d'ordre infini. Il existe alors $n \in \mathbb{Z}$ tel que α_j^n a une valeur propre de module au moins 2. Alors le second lemme donne $x \in L_j$ tel que les éléments de la forme

$$x^{\varepsilon_0} \cdot \left(z^n x z^{-n}\right)^{\varepsilon_1} \cdots \left(z^{kn} x z^{-kn}\right)^{\varepsilon_k}$$

   sont deux à deux distincts (modulo L_{j+1}). Cela contredit la croissance non-exponentielle de G.

On est donc dans le premier cas, ce qui termine la preuve du lemme et celle du théorème de Gromov. □

7 Version finie du théorème de Gromov

Dans cette section, si G est un groupe et X une partie finie de G, on note $C_{G,X}$ la fonction de croissance du sous-groupe de G engendré par X associée à la partie génératrice X.

Théorème 7.1 (Version finie)**.** *Soient d et k des entiers naturels. Il existe des entiers naturels m, i et N tels que pour tout groupe G engendré par une partie finie X on ait :*

Si $C_{G,X}(n) \leqslant kn^d$ pour tout entier n entre 1 et m, alors $C_{G,X}(n) \leqslant kn^d$ pour tout entier $n > 0$, et G a un sous-groupe nilpotent d'indice fini inférieur à i et de classe de nilpotence inférieure à N.

Lemme 7.2 (Théorème de compacité)**.** *Soient $\mathcal{L}$ un langage, T une $\mathcal{L}$-théorie, Φ et Ψ des ensembles de $\mathcal{L}$-énoncés tels que :*

$$T \models \bigwedge_{\varphi \in \Phi} \varphi \Rightarrow \bigvee_{\psi \in \Psi} \psi.$$

Alors il existe des parties finies Φ' et Ψ' respectivement de Φ et Ψ telles que :

$$T \models \bigwedge_{\varphi \in \Phi'} \varphi \Rightarrow \bigvee_{\psi \in \Psi'} \psi.$$

Démonstration. Notons T' la théorie $T \cup \Phi \cup \{\neg\psi | \psi \in \Psi\}$. Par hypothèse, T' est contradictoire et donc, par compacité, finiment contradictoire. Il existe donc des parties finies Φ' et Ψ' respectivement de Φ et Ψ telles que $T \cup \Phi' \cup \{\neg\psi | \psi \in \Psi'\}$ est contradictoire. Mais alors un modèle de T qui est aussi modèle de Φ' est modèle d'un énoncé de Ψ', d'où le résultat annoncé par complétude. □

Nous pouvons maintenant démontrer le théorème 7.1.

Démonstration. Soient d et k des entiers naturels. On note $\mathcal{L}$ le langage des groupes auquel on ajoute k constantes $x_1,\ldots,x_k$. On note T la théorie des groupes dans le langage $\mathcal{L}$. Pour tout entier m, on note φ_m un $\mathcal{L}$-énoncé tel que pour tout modèle G de T on ait :

$$G \models \varphi_m \iff \forall\, n \in [\![1, m]\!],\ C_{G,X}(n) \leqslant kn^d$$

où $X = \left\{x_1^G, \ldots, x_k^G\right\}$. La construction d'une telle formule est aisée.

On note F le groupe libre sur $\{x_1, \ldots, x_k\}$. Si i et N sont deux entiers naturels, on sait que F a un nombre fini de sous-groupes d'indice inférieur à i et que ceux-ci sont de type fini. On note $H_1,\ldots,H_r$ ces sous-groupes et,

pour tout j entre 1 et r, $y_{j,1},\ldots,y_{j,s_j}$ des mots sur X représentant un système de générateurs de H_j. On note alors $\psi_{i,N}$ l'énoncé :

$$\bigvee_{j=1}^{r}\left(\bigwedge_{1\leqslant l_1,\ldots,l_N\leqslant s_j}[y_{j,l_1},\ldots,y_{j,l_N}]=1\right)$$

et on remarque en utilisant le lemme 2.5 que si G est un modèle de T, alors $G\models\psi_{i,N}$ si et seulement si l'image d'un des H_j par le morphisme naturel de F sur G (celui qui envoie x_t sur x_t^G pour t entre 1 et k) est nilpotent de classe inférieure à N.

Or, si G est un modèle de T, tout sous-groupe d'indice fini u du sous-groupe de G engendré par $\left\{x_1^G,\ldots,x_k^G\right\}$ est l'image par le morphisme naturel de F sur G d'un sous-groupe d'indice u de F. Le théorème de Gromov assure donc que

$$T\models\bigwedge_{m\in\mathbb{N}}\varphi_m\Rightarrow\bigvee_{i,N\geqslant 1}\psi_{i,N}.$$

Remarquons alors que pour tous entiers m, i et N, $T\models\varphi_{m+1}\Rightarrow\varphi_m$, $T\models\psi_{i,N}\Rightarrow\psi_{i+1,N}$ et $T\models\psi_{i,N}\Rightarrow\psi_{i,N+1}$. Vu le lemme 7.2, il existe donc des entiers naturels m_0, i_0 et N_0 tels que :

$$T\models\varphi_{m_0}\Rightarrow\psi_{i_0,N_0}.$$

Si G est un modèle de T tel que G est engendré par $X=\{x_1^G,\ldots,x_k^G\}$ et $C_{G,X}(n)\leqslant kn^d$ pour tout entier $n>0$, alors par le théorème de Gromov et le lemme 2.8, G est de présentation finie. On note θ_G le $\mathcal{L}$-énoncé indiquant que $x_1,\ldots,x_k$ vérifient les relations qui définissent G. Ainsi si H est un modèle de T, H vérifie θ_G si et seulement s'il existe un morphisme de G sur H qui envoie x_t^G sur x_t^H pour t entre 1 et k. Dans ce cas, on a alors $C_{H,X'}(n)\leqslant C_{G,X}(n)\leqslant kn^d$ pour tout entier $n>0$, où $X'=\left\{x_1^H,\ldots,x_k^H\right\}$. On a donc :

$$T\models\theta_G\Rightarrow\bigwedge_{m\in\mathbb{N}}\varphi_m. \tag{1}$$

Notons alors Θ la classe des formules θ_G ainsi construites. Cette classe est incluse dans l'ensemble des $\mathcal{L}$-énoncés et c'est donc un ensemble. Par construction de Θ on a

$$T\models\bigwedge_{m\in\mathbb{N}}\varphi_m\Rightarrow\bigvee_{\theta\in\Theta}\theta$$

et donc par compacité, il existe un entier m_1, que l'on peut supposer non nul, et un nombre fini de modèles de T $G_1,\ldots,G_u$ vérifiant les hypothèses du début du paragraphe précédent tels que

$$T\models\varphi_{m_1}\Rightarrow\bigvee_{j=1}^{u}\theta_{G_j}$$

et donc par (1) on a

$$T \models \varphi_{m_1} \Rightarrow \bigwedge_{m \in \mathbb{N}} \varphi_m.$$

Soit maintenant G un groupe engendré par une partie finie X et tel que $C_{G,X}(n) \leqslant kn^d$ pour tout entier entre 1 et m_1. En particulier,

$$|X| \leqslant |X \cup X^{-1}| = C_{G,X}(1) \leqslant k.$$

On peut donc faire de G une $\mathcal{L}$-structure telle que $X = \left\{x_1^G, \ldots, x_k^G\right\}$. Mais alors G vérifie φ_{m_1} et donc $C_{G,X}(n) \leqslant kn^d$ pour tout entier $n > 0$. En particulier, G vérifie φ_{m_0} et donc ψ_{i_0,N_0}, c'est à dire que G a un sous-groupe d'indice fini inférieur à i_0 qui est nilpotent de classe inférieure à N_0. □

La version finie du théorème est donc établie. On pourrait montrer qu'il existe une fonction récursive qui à des entiers k et d associe des entiers i et N vérifiant la concluion du théorème. Le cas de m est plus délicat.

Références

[1] L. van den Dries and J. Wilkie, "Gromov's theorem on groups of polynomial growth and elementary logic," *Journal of Algebra*, no. 89, pp. 349–374, 1984.

[2] J. Tits, "Appendix to M.Gromov's "Groups of polynomial growth and expanding maps"," *Publications mathématiques de l'I.H.É.S*, no. 53, pp. 74–78, 1981.

[3] M. Hall, *The Theory of Groups*. The Macmillan Company, 1959.

[4] D. Robinson, *A Course in the Theory of Groups*. Springer, 1996.

[5] J. A. Wolf, "Growth of finitely generated solvable groups and curvature on riemannian manifolds," *J. Differential Geometry*, no. 2, pp. 421–446, 1968.

[6] J. Milnor, "Growth of finitely generated solvable groups," *J. Differential Geometry*, no. 2, pp. 447–449, 1968.

[7] J. Tits, "Groupes à croissance polynomiale," in *Séminaire Bourbaki*, no. 572, 33e année, 1980/81, pp. 176–188.