Mémoire

Auteur : Stas, Pierre
Promoteur(s) : Leroy, Julien
Faculté : Faculté des Sciences
Diplôme : Master en sciences mathématiques, à finalité approfondie
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/14709

Faculté des Sciences
Département de Mathématique

Croissance des groupes : Solution au problème 5603

Mémoire de fin d'études présenté en vue de l'obtention du titre de
Master en Sciences Mathématiques, à finalité approfondie

Année académique 2021-2022

Auteur :
Pierre Stas

Promoteur :
Julien Leroy

Mes premiers remerciements vont à mon promoteur, Julien Leroy,
qui m'a conseillé et aidé lors de la rédaction de ce mémoire
et plus généralement au cours de mes études.

Je souhaite également remercier professeurs et assistants du département
qui, par leur bienveillance, m'ont transmis leur passion.
Je souhaite mettre à l'honneur Georges Hansoul en particulier.
Il nous a si bien raconté les maths qu'il les a rendues vivantes.

Ensuite, il me semble naturel de remercier mes parents
pour leur soutien et leur patience lors de mes études
et leurs relectures attentives.

Mes derniers remerciements vont à mes amis,
Bruno Dular, Thomas Lamby et Lucas Michel.
Les conversations que nous avons eues ont été précieuses
dans la rédaction de ce mémoire.

Table des matières

Introduction

Le sujet de ce mémoire est la *croissance des groupes*. Il fait partie du domaine de la *théorie géométrique des groupes*. Le paradigme de ce domaine est de munir les groupes d'une structure métrique et de les considérer comme des objets géométriques. Il y a deux manières de faire cela :

- On a un groupe finiment engendré. On sait alors que l'on peut, à partir d'un ensemble fini de multiplications à droite, transformer un élément en n'importe quel autre élément du groupe. Pour un ensemble fini de générateurs fixés, on prend comme distance entre deux éléments le nombre minimal de générateurs et inverses de générateurs nécessaires pour transformer le premier élément en le deuxième. On appelle cette métrique la *métrique des mots*.
- Le groupe qu'on souhaite étudier agit sur un espace métrique X. Dans ce cas, le *pullback* de la métrique sur X donne une pseudo-métrique sur G.

Lorsqu'il s'agit de croissance des groupes, on est dans le premier cas. L'espace métrique associé à un groupe G est identique à celui donné par le *graphe de Cayley* de G. Ce graphe a pour sommets les éléments du groupe et pour arcs les (g, gs), où g est un élément du groupe et s un générateur. Ce générateur est aussi l'étiquette de l'arc. La métrique induite par la distance sur ce graphe si on attribue un poids 1 aux arcs est la métrique des mots.

Un problème saute aux yeux dans ces explications sommaires : la dépendance vis-à-vis du choix des générateurs. Cependant, le graphe de Cayley et donc la métrique des mots sont uniques à une certaine relation d'équivalence près. Cette relation est la *quasi-isométrie*. Intuitivement, demander une quasi-isométrie entre espaces revient à demander qu'entre les deux il y ait une application de l'un dans l'autre qui conserve presque les distances (on minore et majore la distance des images par des fonctions affines de la distance initiale) et qui soit presque surjective (pour tout point de l'espace d'arrivée, il y a un point proche qui admet une pré-image). D'une certaine manière, cela revient à regarder des groupes qui sont isométriques de loin, dans le sens où on ne voit plus précisément où est un point mais on en a une idée. Ce principe de regarder les espaces métriques et donc les groupes finiment engendrés de loin est central en théorie géométrique des groupes.

Le profane se demande sans doute ce que l'on peut obtenir en voyant les groupes comme des espaces métriques. L'une des questions qui motive la théorie géométrique des groupes est la suivante :

Quelles propriétés géométriques d'un groupe se traduisent en propriétés algébriques ?

Dans ce mémoire, on limite les propriétés géométriques à la croissance du groupe. Cette croissance est définie comme étant l'évolution asymptotique selon n le nombre d'éléments que l'on peut écrire comme produit de moins de n générateurs ou inverses de générateurs.

On distingue trois classes de taux de croissance. Les *groupes à croissance polynomiale* qui, pour des n assez grands, ont une croissance polynomiale ou sous-polynomiale. Les *groupes à croissance exponentielle* qui ont une croissance aussi rapide qu'une exponentielle pour des n suffisamment grands. Finalement, on définit les *groupes à croissance intermédiaire* qui ont un taux de croissance trop rapide pour être polynomial mais trop lent pour être exponentiel.

Une brève histoire

L'étude de la croissance des groupes apparaît dans les années 50. On cite comme pionniers de ce sujet les noms de Albert Solomonovich Schwarz avec l'article [Sch55] et de John Milnor avec [Mil68a] et [Mil68b]. Dans les deux cas, on constate que la motivation initiale concernant l'étude de la croissance des groupes est de nature géométrique. Schwarz lie le taux de croissance du volume du revêtement universel de variétés riemanniennes compactes à la croissance du groupe fondamental de ladite variété. Milnor, lui, explore la relation entre la courbure des variétés riemanniennes et la croissance du groupe fondamental.

Bien que l'apport de Schwarz soit indéniable, c'est bien en 1968 avec les articles de Milnor que commence l'étude systématique de la croissance des groupes. L'un des catalyseurs de cette effervescence est l'article *Problem 5603* de John Milnor ([Mil68b]) dans lequel il pose deux questions :

- Est-il vrai que la croissance d'un groupe est soit polynomiale soit exponentielle ?
- Quels sont les groupes à croissance polynomiale ?

La première question a été résolue en 1983 dans [Gri83]. Bien que la réponse soit négative, cette découverte de groupes à croissance intermédiaire a contribué à de nombreuses avancées en théorie des groupes. Cela a mené à l'invention de nouvelles classes de groupes. Par exemple, les groupes auto-similaires ou encore les “branch groups”. De surcroît, les groupes à croissance intermédiaire sont aujourd'hui utilisés dans de nombreux domaines : l'étude des groupes moyennables, en topologie, l'étude des marches aléatoires sur des groupes...

La réponse à la deuxième question a été donnée par Mikhael Gromov en 1980 dans [Gro81]. Gromov montre que les groupes à croissance polynomiale sont exactement les groupes virtuellement nilpotents, ce sont les groupes qui ont un sous-groupe d'indice fini qui est presque abélien. C'est la première utilisation de la solution au cinquième problème de Hilbert. De plus, le squelette de la preuve a été réutilisé et est à l'origine de l'étude des cônes asymptotiques des groupes.

Structure du mémoire

Le mémoire est articulé autour des solutions apportées à *Problem 5603* ([Mil68b]). L'objet du chapitre 1 est de poser les premières définitions et propriétés qui ont trait à la croissance des groupes. On commence par y définir en détail l'espace métrique associé aux groupes ainsi que la relation de quasi-isométrie. Cette dernière est la relation d'équivalence pour laquelle la croissance des groupes est une propriété invariante. Ensuite, on définit le taux de croissance des groupes à partir des fonctions de croissance. On finit par classifier les groupes selon leurs taux de croissance.

Dans le chapitre 2, on commence par définir les groupes nilpotents. Ensuite, on en donne quelques propriétés basiques qui permettent de mieux les comprendre. On s'intéressera également à la croissance de ces groupes. Pour finir, on définira les groupes virtuellement nilpotents et on en donnera le taux de croissance.

Le chapitre 3 aborde la preuve du théorème de Gromov donnée par Terrence Tao et Yehuda Shalom dans [ST10]. Avant de passer à la preuve, on dira un mot sur la preuve originale de Gromov. Elle contient des idées qui ont été capitales dans les développements ultérieurs en théorie géométrique des groupes.

On termine par le chapitre 4 qui explicite la construction du groupe de Grigorchuk et prouve que son taux de croissance est intermédiaire. Cet exemple fait rentrer en jeu des notions théoriques riches telles que les produits semi-directs de groupes ou les automorphismes d'arbres binaires. L'autre intérêt majeur de ce chapitre est d'expliciter un calcul non trivial de taux de croissance.

Au long de ce mémoire, un soin particulier a été porté aux interprétations des différents concepts théoriques. Une attention spéciale a été donnée aux exemples et cas concrets à chaque fois que cela semblait pertinent. En annexe, on retrouve une brève introduction aux groupes libres, un résultat concernant les normes sur les espaces vectoriels de dimension finie. On y trouve aussi une note sur le problème de Burnside et sa relation avec le groupe de Grigorchuk.

Notations

On donne ici les conventions de notation moins communes utilisées au cours de ce mémoire.

A_0	l'ensemble A privé de 0 avec $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$,
$\mathbb{R}^+$	l'ensemble des réels positifs
$\|E\|$	cardinal de E, si E est un ensemble
$[x]$	désigne la classe d'équivalence de x
$\hookrightarrow$	injection
$\sqcup$	union disjointe
$\cdot$	opération d'un groupe quelconque
1	élément neutre d'un groupe quelconque
$+$	opération d'un groupe abélien
0	élément neutre d'un groupe abélien
A^{-1}	l'ensemble des inverses des éléments de A
$H \leq G$	H sous-groupe de G, si G est un groupe
$N \lhd G$	N sous-groupe normal de G, si G est un groupe
$Z(G)$	centralisateur du groupe G
$[G : H]$	indice de H comme sous-groupe de G
$\cong$	isomorphe à
Aut	le groupe des automorphismes
$R^\times$	le groupe des unités de R
$\langle X \rangle$	le sous-groupe engendré par l'ensemble X
x^g	le conjugué de x par g
ε	le mot vide
A^*	les suites finies d'éléments de A
A^+	les suites finies non-vides d'éléments de A
$\|w\|_a$	nombre d'occurrences de a dans w
$w_{[a,b]}$	$w_a w_{a+1} \dots w_b$
$\mathcal{V}(G)$	sommets du graphe G
$\mathcal{E}(G)$	arêtes du graphe G

Chapitre 1

Premières définitions

Le but de ce chapitre est de donner toutes les définitions nécessaires pour comprendre ce qu'est la *croissance d'un groupe* et de donner des propriétés et des exemples en lien avec ces nouvelles notions. Pour rédiger ce chapitre, les sources principales sont [Gri14] et [DK18].

Pour ce faire, on commence par *géométriser* les groupes. D'abord, on définit la *métrique de mots* sur les groupes. On verra que cette métrique n'est pas toujours bien définie. Pour qu'elle soit définie correctement, il faut travailler avec des *groupes finiment engendrés*. Ensuite, on expliquera comment les *graphes de Cayley* sont construits et comment ils permettent de visualiser la métrique des mots. On s'attellera aussi à expliquer la notion de *quasi-isométrie* qui est la relation d'équivalence entre espaces métriques utilisée en théorie géométrique des groupes.

Ensuite, on arrivera à la définition stricto sensu de la croissance des groupes. On commencera par donner la définition des *fonctions de croissance* et on en calculera quelques unes sur des exemples. On explorera ensuite la notion plus robuste de *taux de croissance* et on s'occupera de démontrer quelques propriétés de fermeture. On s'intéressera finalement à classifier les groupes selon leur taux de croissance.

1.1 Géométrisation des groupes

Comme annoncé dans l'introduction, la première étape nécessaire à la définition de la croissance des groupes est d'associer un espace métrique aux groupes. C'est ce que nous faisons ici de deux manières équivalentes. D'abord de manière combinatoire avec la métrique des mots. Ensuite de manière plus visuelle avec les graphes de Cayley. On termine cette section en introduisant les quasi-isométries, qui sont centrales en théorie géométrique des groupes. En effet, on considère souvent ces derniers à quasi-isométrie près.

1.1.1 Métrique des mots

Avant de définir une métrique sur les groupes, introduisons une notion de longueur. C'est à partir de cette dernière que l'on définira ensuite la distance.

Définition 1.1.1. Soient G un groupe et $S \subset G$ un système de générateurs de G. La *longueur* de $g \in G$ par rapport à S est notée $|g|_S$ (ou $|g|$ lorsqu'il n'y a pas d'ambiguïté sur le système de générateurs considéré) et est donnée par

$$n = \min \left\{ k \in \mathbb{N} \,|\, \exists s_1, ..., s_k \in (S \cup S^{-1}) \text{ tq. } g = s_1 s_2 ... s_k \right\}.$$

Un décomposition de g en $|g|_S$ éléments de $S \cup S^{-1}$ est appelé une *décomposition réduite* de g. Remarquons qu'on n'a pas l'unicité de la décomposition réduite.

On prouve ici un lemme qui découle de la définition. Il sera utilisé plus tard pour montrer que la distance induite par la longueur que l'on a défini est symétrique.

Lemme 1.1.1. *Dans tout groupe G,*

$$|g|_S = |g^{-1}|_S$$

avec S une partie génératrice de G.

Démonstration. Soient $s_1, ..., s_{|g|_S} \in S \cup S^{-1}$ tels que $g = s_1 ... s_{|g|_A}$. On a, $g^{-1} = s_{|g|_A}^{-1} ... s_1^{-1}$ et donc,

$$|g^{-1}|_S \leq |g|_S.$$

Bien entendu, de la même manière, on peut exprimer g comme produit de $|g^{-1}|_S$ éléments de $S \cup S^{-1}$ et donc obtenir :

$$|g^{-1}|_S \geq |g|_S.$$

Au total,

$$|g^{-1}|_S = |g|_S.$$

□

Nous verrons plus tard pourquoi nous restreignons l'étude des taux de croissance aux groupes finiment engendrés. La définition suivante ainsi que la proposition seront utiles à ces fins.

Définition 1.1.2. Un groupe G est dit *finiment engendré* ou *de type fini* s'il existe $S \subset G$ tel que $|S| < \infty$ et $G = \langle S \rangle$. On appelle un tel ensemble S un *système fini de générateurs* de G.

Remarque 1.1.1. Pour un groupe G et S une partie finie de G, il est clair que le groupe engendré par S et le groupe engendré par $S \cup S^{-1}$ sont les mêmes. Ainsi, pour tout groupe de type fini, on peut trouver un ensemble fini symétrique de générateurs. Cette observation permettra de simplifier beaucoup de notations dans la suite du travail.

Proposition 1.1.1. *Soient G un groupe de type fini et S, T des parties génératrices finies de G. Il existe une constante $C \in \mathbb{N}$ telle que, pour tout $g \in G$,*

$$|g|_S \leq C|g|_T \text{ et } |g|_S \leq C|g|_T.$$

Démonstration. On définit les trois constantes,

$$\begin{aligned} C_S &= \max(\{|s|_T | s \in S\}) \\ C_T &= \max(\{|t|_S | t \in T\}) \\ C &= \max(C_S, C_T). \end{aligned}$$

Vu que S et T sont finis, ces maxima existent et ils sont mêmes atteints. Soient $g \in G$ et $s_1, ..., s_{|g|_T} \in S \cup S^{-1}$ tels que

$$g = s_1 ... s_{|g|_S}.$$

Si on exprime chaque facteur s comme produit de $|s|_T$ éléments de $T \cup T^{-1}$, alors g est un produit d'au plus $C_S|g|_S$ éléments de $T \cup T^{-1}$ par définition de C_S et vu le lemme 1.1.1. Ainsi,

$$|g|_T \leq C_S|g|_S.$$

Comme $|g|_S$ est un naturel, $C_S|g|_S \leq C|g|_S$ et donc :

$$|g|_T \leq C|g|_S.$$

On montre de la même manière que

$$|g|_S \leq C|g|_T.$$

□

Nous sommes maintenant prêts à définir la métrique des mots et à montrer que c'est bien une distance.

Définition 1.1.3. Soient G un groupe et S une partie génératrice de G. La *métrique des mots d_S* est définie par

$$d_S(g, h) = |g^{-1}h|,$$

pour tout $g, h \in G$. Il s'agit bien là d'une métrique car :

- d_S est à valeurs dans $\mathbb{R}^+$.
- Vu le lemme 1.1.1, pour tout $g, h \in G$, $d_S(g, h) = |g^{-1}h| = |(g^{-1}h)^{-1}| = |h^{-1}g| = d_S(h, g)$.
- Pour tout $g, h \in G$,

$$\begin{aligned} &d_S(g, h) = |g^{-1}h| = 0 \\ \Leftrightarrow &g^{-1}h = 1 \\ \Leftrightarrow &g = h. \end{aligned}$$

— Pour tout $g_1, g_2, g_3 \in G$, on a $d_S(g_1, g_3) = |g_1^{-1}g_3| = |g_1^{-1}g_2g_2^{-1}g_3|$. De plus,

$$|g_1^{-1}g_2g_2^{-1}g_3| \leq |g_1^{-1}g_2| + |g_2^{-1}g_3| = d_S(g_1, g_2) + d_A(g_2, g_3)$$

car les expressions en éléments de S les plus courtes de $g_1^{-1}g_2$ et $g_2^{-1}g_3$ fournissent, en les concaténant, une expression dans S de $g_1^{-1}g_2g_2^{-1}g_3$ de longueur $|g_1^{-1}g_2| + |g_2^{-1}g_3|$. Par définition, cette expression est de longueur plus grande ou égale à $|g_1^{-1}g_2g_2^{-1}g_3|$. Au total, on a bien l'inégalité triangulaire :

$$d_S(g_1, g_3) \leq d_S(g_1, g_2) + d_S(g_2, g_3)$$

pour tout $g_1, g_2, g_3 \in G$.

Cette définition couplée à la proposition 1.1.1 justifie partiellement que l'on s'intéresse en théorie géométrique des groupes aux groupes de type fini. En effet, les métriques des mots sur un même groupe sont équivalentes (i.e : induisent la même topologie) si on choisit un ensemble fini de générateurs. On a donc une forme d'unicité de l'espace métrique que l'on associe aux groupes.

Nous finirons cette section en montrant l'invariance pour la multiplication à gauche de cette distance.

Proposition 1.1.2. *Cette distance est invariante pour la multiplication à gauche.*

Démonstration. Soient G un groupe et S une partie génératrice de G. On a, pour tout $g, h, x \in G$,

$$\begin{aligned} d_S(xg, xh) &= |(xg)^{-1}xh| \\ &= |g^{-1}x^{-1}xh| \\ &= |g^{-1}h| \\ &= d_S(g, h). \end{aligned}$$

□

1.1.2 Graphes de Cayley

On peut donner une définition plus visuelle et intuitive de l'espace métrique que l'on associe aux groupes. On le fait avec les graphes de Cayley.

Définition 1.1.4. Soient G un groupe et S un système de générateurs de G. On définit le *graphe de Cayley* de G par rapport à S, $\Gamma(G, S)$, comme suit :

— $\Gamma(G, S)$ est un graphe orienté dont les sommets sont les éléments de G

— pour $g, g' \in G$ et $s \in S$, on a un arc de g vers g' de label s si $gs = g'$.

Lorsque le contexte est clair, on désignera par $\Gamma(G)$ ou Γ le graphe $\Gamma(G, S)$.

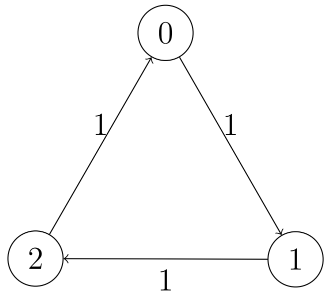


FIGURE 1.1 – Graphe de Cayley de $\dfrac{\mathbb{Z}}{3\,\mathbb{Z}}$.

Étudions quelques exemples plutôt simples afin de se faire une idée plus claire de ce que sont les graphes de Cayley.

Exemples 1.1.1. — Construisons $\Gamma\left(\dfrac{\mathbb{Z}}{3\mathbb{Z}}, \{1\}\right)$. On trouve facilement le graphe représenté à la figure 1.1.

— Prenons maintenant, $G = \mathcal{D}_3 = \langle a, b | a^3 = b^2 = 1 \text{ et } ab = ba^2 \rangle$ le groupe diédral d'ordre 6 et le système de générateurs $\{a, b\}$. On obtient facilement le graphe de Cayley de la Figure 1.2.

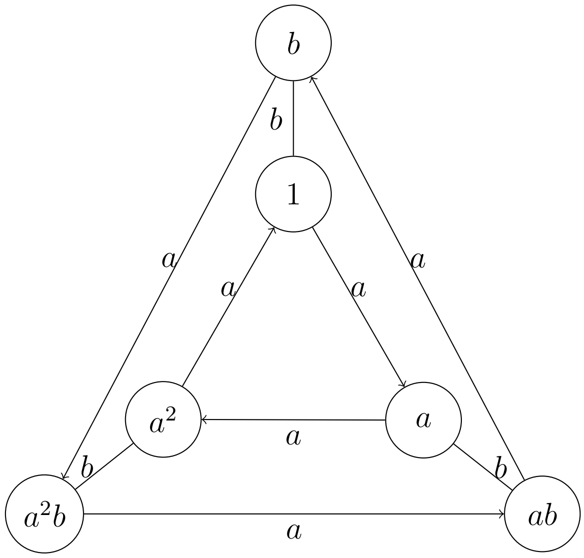


FIGURE 1.2 – Graphe de Cayley de $\mathcal{D}_3$.

— Voyons maintenant ce qui se passe pour le groupe infini $\mathbb{Z}$ avec l'ensemble de générateurs $\{1\}$, on obtient le graphe représenté à la figure 1.3.
À la figure 1.4, on voit ce que l'on obtient avec le système de générateurs $\{2, 3\}$.

On peut déduire plusieurs choses de ces quelques exemples. Premièrement, on constate que, dans le cas des groupes finis, le graphe de Cayley peut toujours être représenté dans

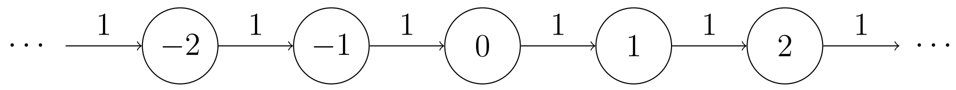


FIGURE 1.3 – Graphe de Cayley $\Gamma(\mathbb{Z}, \{1\})$.

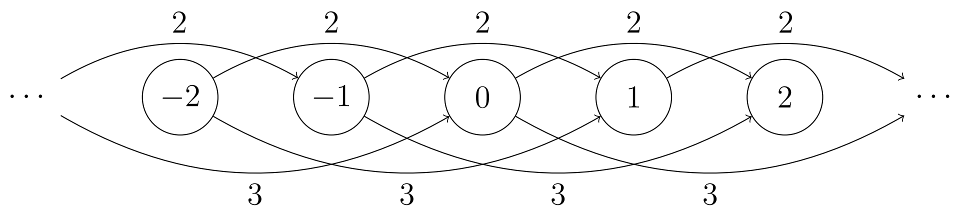


FIGURE 1.4 – Graphe de Cayley $\Gamma(\mathbb{Z}, \{2, 3\})$.

son entièreté. En effet, il suffit de déterminer tous les sommets atteignables par une multiplication à droite par un élément du système de générateurs à partir d'un sommet donné. Ensuite, on répète cette opération pour chaque sommet.

Ensuite, on se rend compte que certaines propriétés d'un élément sont visibles sur le graphe de Cayley du groupe. Par exemple, si, en un sommet g, il existe un cycle de label s^k, alors s est d'ordre fini. L'ordre de s est donné par la longueur du cycle non-nul le plus court de label s^k. Un peu plus de travail permet même à partir d'un bonne connaissance du graphe de Cayley d'un groupe de trouver l'ordre d'un élément quelconque de ce groupe.

Le dernier exemple nous montre que le diagramme de Cayley d'un groupe n'est pas unique puisqu'il dépend de l'ensemble de générateurs. On peut néanmoins avoir une certaine stabilité de ces graphes par rapport au choix de l'ensemble de générateurs. L'idée est d'associer un espace métrique à ces graphes de Cayley et de montrer que, pour tout ensemble de générateurs, ces espaces métriques sont équivalents.

L'idée est de considérer la "distance" usuelle sur les graphes orientés, non pas pour le graphe $\Gamma(G, S)$ mais pour $\Gamma(G, S \cup S^{-1})$. On a ainsi la symétrie et l'inégalité triangulaire, on récupère donc une "vraie" notion de distance, notée m_S. On remarque aisément que cette distance sur G est équivalente à la métrique des mots donnée à la définition 1.1.3. Ainsi, toutes les propriétés vraies pour la métrique des mots restent vraies pour (G, m_S). On a donc bien la stabilité par rapport au choix de l'ensemble de générateurs à équivalence près.

1.1.3 Quasi-isométries

Les graphes de Cayley ou de manière équivalente les espaces métriques induits par la métrique de mots ne sont pas uniques pour chaque groupe. La notion de quasi-isométrie permet de remédier à ce problème.

Définition 1.1.5. Soient (X, d) et (Y, d') deux espaces métriques. On dit qu'ils sont *quasi-isométriques* s'il existe une fonction, appelée quasi-isométrie, $\phi : X \to Y$ et des constantes $C \geq 1, D \geq 0$ et $L > 0$ telles que

— $\frac{1}{C}d(x,x') - D \leq d'(\phi(x),\phi(x')) \leq Cd(x,x') + D$, pour tout $x, x' \in X$.
— Pour tout $y \in Y$, il existe $x \in X$ tel que $d'(\phi(x), y) \leq L$.

La première partie de la définition est faite pour que les quasi-isométries ne laissent pas deux points éloignés se rapprocher de trop et que deux points rapprochés ne vont pas s'éloigner déraisonnablement. Les distances entre les points sont donc *presque* respectées par les quasi-isométries. La deuxième condition, elle, dit que l'espace d'arrivée ressemble assez à l'espace de départ pour que, aux alentours de n'importe quel point, on retrouve un point qui vient de l'espace de départ. Ces deux conditions donnent l'interprétation selon laquelle regarder des espaces métriques à quasi-isométrie près revient à les regarder de loin. En effet, si on ne regarde pas la structure précise des espaces mais qu'on se contente de les regarder grossièrement [1], alors des espaces quasi-isométriques se ressemblent.

Pour que cette notion puisse donner une forme d'unicité des espaces métriques que l'on a associé aux groupes, il faut qu'elle nous donne une relation d'équivalence.

Proposition 1.1.3. *"Être quasi-isométriques" est une relation d'équivalence sur la classe des espaces métriques.*

Démonstration. Il est clair que c'est une relation réflexive en prenant $\phi = \mathrm{id}, C = 1$ et $D = 0$ pour avoir le premier point de la définition et $x = y$ et $L = 1$ pour le second.

La transitivité est un peu plus longue mais pas plus compliquée à montrer. Soient $(X, d_1), (Y, d_2)$ et (Z, d_3) des espaces métriques et $\phi : X \to Y$ et $\psi : Y \to Z$ des quasi-isométries entre ces espaces. On sait qu'il existe $C_1, C_2 \geq 1, D_1, D_2 \geq 0$ et $L_1, L_2 > 0$ des constantes telles que :

— Pour tout $x, x' \in X, \frac{1}{C_1}d_1(x,x') - D_1 \leq d_2(\phi(x),\phi(x')) \leq C_1 d_1(x,x') + D_1$
— Pour tout $y \in Y$, il existe $x \in X$ tels que $d_2(\phi(x), y) \leq L_1$
— Pour tout $y, y' \in Y, \frac{1}{C_2}d_2(y,y') - D_2 \leq d_3(\psi(y),\psi(y')) \leq C_2 d_2(y,y') + D_2$
— Pour tout $z \in Z$, il existe $y \in Y$ tels que $d_3(\psi(y), z) \leq L_2$

Pour vérifier que c'est une relation symétrique, prenons $(X, d_1), (Y, d_2)$ des espaces métriques, $\phi : X \to Y$ une quasi-isométrie entre ces espaces, $C \geq 1$, $D \geq 0$ et $L > 0$ tels que, pour tout $y \in Y$,

— $\frac{1}{C}d_1(x,x') - D \leq d_2(\phi(x),\phi(x')) \leq Cd_1(x,x') + D$, pour tout $x, x' \in X$.
— Pour tout $y \in Y$, il existe $x \in X$ tel que $d_2(\phi(x), y) \leq L$.

Nous allons construire une fonction $\psi : Y \to X$ qui sera également une quasi-isométrie.

A chaque $y \in Y$, on va associer un $x_y \in \phi(X)$ tel que $d_2(y, x_y) \leq L$. On définit également une section $s : \phi(X) \to X$ qui à un x va associer un élément de $\phi^{-1}(x)$. On peut maintenant définir la fonction

$$\psi : Y \to X : y \mapsto s(x_y).$$

1. Traduction de *coarse*.

On a, pour tout $y, y' \in Y$,

$$\begin{aligned}\frac{1}{C}d_1(\psi(y),\psi(y')) - D \leq & d_2(\phi\circ\psi(y),\phi\circ\psi(y')) \\ \leq & d_2(x_y, x_{y'}) \\ \leq & d_2(x_y, y) + d_2(y,y') + d_2(y', x_{y'}) \\ \leq & 2L + d_2(y,y').\end{aligned}$$

Ce qui veut dire qu'on a

$$d_1(\psi(y),\psi(y')) \leq Cd_2(y,y') + CD + 2CL.$$

On a également, pour tout $y, y' \in Y$,

$$\begin{aligned}Cd_1(\psi(y),\psi(y')) + D \geq & d_2(\phi\circ\psi(y),\phi\circ\psi(y')) \\ \geq & d_2(x_y, x_{y'}) \\ \geq & d_2(y,y') - (d_2(x_y, y) + d_2(y', x_{y'})) \\ \geq & d_2(y,y') - 2L.\end{aligned}$$

On a donc l'inégalité :

$$d_1(\psi(y),\psi(y')) \geq \frac{1}{C}d_2(y,y') - \frac{2L+D}{C} \geq \frac{1}{C}d_2(y,y') - 2CL + DC.$$

On a donc bien le premier point de la définition de quasi-isométrie :

$$\frac{1}{C}d_2(y,y') - (CD + 2CL) \leq d_1(\psi(y),\psi(y')) \leq Cd_2(y,y') + CD + 2CL.$$

Montrons le deuxième point, on pose : $y = \phi(x)$,

$$\begin{aligned}d(x,\psi(y)) \leq & Cd'(\phi(x),\phi(\psi(y))) + CD \\ \leq & Cd'(\phi(x), x_{\phi(x)}) + CD \\ \leq & CL + CD.\end{aligned}$$

□

Avant d'aller plus loin, étudions quelques exemples d'espaces métriques quasi-isométriques.

Exemple 1.1.1. Soit $n \in \mathbb{N}_0$, on munit $\mathbb{Z}$ de la distance d avec $d(z,z') = |z - z'|$ et on munit $n\mathbb{Z}$ de la distance d_n avec $d_n(nz, nz') = |z - z'|$. Ces deux espaces métriques sont quasi-isométriques. La quasi-isométrie est donnée par l'inclusion de $n\mathbb{Z}$ dans $\mathbb{Z}$. En effet, on a

— $\frac{1}{n}d_n(nz,nz') \leq nd_n(nz,nz') = n|z-z'| = |nz - nz'| = d(nz,nz') \leq nd_n(nz,nz')$, pour tout $nz, nz' \in n\mathbb{Z}$

— Pour tout $z \in \mathbb{Z}$, il existe $a \in \mathbb{Z}$ et $b \in \{0, ..., n-1\}$ tels que $z = an + b$. On a $d(na, z) = b \leq n$.

Exemple 1.1.2. Les espaces métriques $\mathbb{R}$ muni de la distance euclidienne, d et $\mathbb{Z}$ muni de la restriction de la distance euclidienne à $\mathbb{Z}$ sont quasi-isométriques. On va montrer que la fonction plancher, $\lfloor\cdot\rfloor : \mathbb{R} \to \mathbb{Z} : x \mapsto \sup\{z \in \mathbb{Z} \,|\, z \leq x\}$, est une quasi-isométrie. Pour tout $x \in \mathbb{R}$, on pose $\{x\}$ la partie fractionnaire [2] de x. On observe que, pour $x, y \in \mathbb{R}$,

$$\begin{aligned} &|x-y| = |\lfloor x\rfloor + \{x\} - \lfloor y\rfloor - \{y\}| \leq |\lfloor x\rfloor - \lfloor y\rfloor| + |\{x\} - \{y\}| \\ \Rightarrow &|x-y| - |\{x\} - \{y\}| \leq |\lfloor x\rfloor - \lfloor y\rfloor| . \end{aligned}$$

Comme les parties fractionnaires sont dans $[0,1]$, on a $|\{x\} - \{y\}| \leq 1$ et donc $|x-y| - 1 \leq |\lfloor x\rfloor - \lfloor y\rfloor|$. De plus,

$$\begin{aligned} &|\lfloor x\rfloor - \lfloor y\rfloor| = |x - \{x\} - y + \{y\}| \leq |x-y| + |\{x\} - \{y\}| \\ \Rightarrow &|\lfloor x\rfloor - \lfloor y\rfloor| \leq |x-y| + 1. \end{aligned}$$

On a donc

— $|x-y| - 1 \leq |\lfloor x\rfloor - \lfloor y\rfloor| \leq |x-y| + 1$

— La fonction plancher est surjective. Ainsi, pour tout $z \in \mathbb{Z}$, $|\lfloor z\rfloor - z| \leq 0$.

On en conclut que le plancher est bien une quasi-isométrie.

Cet exemple permet de constater que des espaces topologiquement très différents peuvent tout de même être quasi-isométriques. Donc, avoir une propriété conservée par quasi-isométie est un résultat assez fort.

Nous pouvons maintenant passer aux deux propositions qui nous manquent pour pouvoir dire que l'on a correctement géométrisé les groupes. Nous devons d'abord montrer que les espaces métriques associés aux graphes de Cayley d'un groupe sont équivalents. De plus, pour que ce soit défini correctement dans la catégorie des groupes, il faut qu'à deux groupes isomorphes, on associe le même espace métrique. C'est l'objet de la proposition et du corollaire qui suivent.

Proposition 1.1.4. *Soient G un groupe et S et T deux systèmes finis de générateurs de G. Les espaces métriques (G, d_S) et (G, d_T) sont quasi-isométriques.*

Démonstration. On sait, par la proposition 1.1.1, qu'il existe $C \in \mathbb{N}$

$$\begin{aligned} d_S(g,h) = |g^{-1}h|_S &\leq C|g^{-1}h|_T = Cd_T(g,h) \\ \text{et } d_S(g,h) = |g^{-1}h|_S &\geq \frac{1}{C}|g^{-1}h|_T = \frac{1}{C}d_T(g,h). \end{aligned}$$

Il suffit maintenant de prendre $\phi = \mathrm{id}$ pour voir que l'on a bien une quasi-isométrie. □

2. C'est-à-dire le réel r tel que $x = \lfloor x\rfloor + r$.

Corollaire 1.1.1. *Soient G, H deux groupes finiment engendrés et $\varphi : G \to H$ un isomorphisme. Pour toute partie génératrice finie S de G et toute partie génératrice finie T de H, (G, d_S) et (H, d_T) sont quasi-isométriques.*

Démonstration. Il suffit de remarquer que $\varphi(S)$ est un générateur de H et que φ est une quasi-isométrie. On applique ensuite la proposition 1.1.4 à $(H, d_{\varphi(S)})$ et (H, d_T). On conclut par transitivité de la relation de quasi-isométrie. □

Cette proposition nous permet de définir les groupes quasi-isométriques.

Définition 1.1.6. Soient G et G' deux groupes de type fini. On dit que ce sont des *groupes quasi-isométriques* si, pour tout S système fini de générateurs de G et T un système fini de générateurs de G', on a (G, d_S) et (G', d_T) quasi-isométriques.

Vu ce qui précède et comme "être quasi-isométriques" est une relation d'équivalence, on sait que s'il existe un S et un T tels que (G, d_S) est quasi-isométrique à (G', d_T), alors G et G' sont quasi-isométriques. De la même manière, si pour deux systèmes de générateurs S et T, (G, d_S) et (G', d_T) ne sont pas quasi-isométriques, alors c'est le cas pour tous les systèmes finis de générateurs. C'est donc une notion indépendante du choix de générateurs.

1.2 Croissance des groupes

Nous avons muni tous les groupes d'un unique (à quasi-isométrie près) espace métrique. Le prisme par lequel on va étudier ces espaces métriques est leur taux de croissance. Cette section a pour vocation d'expliquer la manière dont on le fait.

1.2.1 Fonction de croissance

Les fonctions de croissance sont l'outil de base dont on se servira pour définir la croissance des groupes.

Définition 1.2.1. La *fonction de croissance* d'un groupe G de type fini par rapport à un système fini de générateurs S est la fonction

$$\gamma_G^S : \mathbb{N} \to \mathbb{N} : n \mapsto |\{g \in G | |g|_S \leq n\}|.$$

La valeur γ_G^S donne le nombre d'éléments dans la boule fermée de centre 1 et de rayon n du graphe $\Gamma(G, S \cup S^{-1})$. On note cet ensemble $B(1, n)$. C'est donc trivialement une fonction croissante. On interprète cette fonction comme étant le nombre d'éléments que l'on peut atteindre en n étapes à partir des générateurs et leurs inverses. Autrement dit, elle nous dit comment le groupe croit en s'autorisant une multiplication par un générateur supplémentaire à chaque étape.

La proposition 1.1.2 permet d'affirmer que si l'on avait choisi de centrer les boules en $x \in G \setminus \{1\}$, la fonction de croissance aurait été exactement la même.

Remarque 1.2.1. La notion de fonction de croissance n'est pas propre aux groupes et on aurait pu la définir dans le cadre plus général des espaces métriques discrets munis d'un point.

Cette première propriété des fonctions de croissance des groupes est fondamentale dans la démonstration de plusieurs résultats que nous verrons plus tard. Elle dit que tous les éléments de longueur plus petite que $n + m$ peuvent se décomposer en un élément de longueur plus petite que n et un élément de longueur plus petite que m.

Proposition 1.2.1. *Soient G un groupe finiment engendré et S un système de générateurs de G. Pour tout $m, n \in \mathbb{N}$, on a*

$$\gamma_G^S(m+n) \leq \gamma_G^S(m)\gamma_G^S(n).$$

Démonstration. C'est évident puisque si un élément $g \in G$ se décompose en $m + n$ générateurs, alors il se décompose forcément en un élément de $B(1, m)$ et un autre de $B(1, n)$. On n'a pas l'inégalité parce qu'un même élément peut avoir plusieurs décompositions dans $B(1, m)$ et $B(1, n)$. □

Maintenant que les définitions sont posées, on peut s'atteler à regarder la croissance de différents groupes finiment engendrés.

Exemple 1.2.1. Commençons par les groupes finis. Soit G un tel groupe, on peut prendre le système fini de générateurs G et on obtient bien entendu :

$$\gamma_G^G(n) = \begin{cases} |G| \text{ si } n \geq 1 \\ 1 \text{ si } n = 0. \end{cases}$$

Cet exemple nous montre pourquoi il est plus intéressant dans le cas de la croissance de regarder les groupes infinis finiment engendrés. Les groupes finis ont une croissance ultimement constante. Il a néanmoins son importance puisque c'est un premier exemple d'une propriété géométrique (avoir une fonction de croissance bornée) qui correspond à une propriété algébrique (être fini).

Exemple 1.2.2. Le cas de $G = \mathbb{Z}$ est lui aussi facile à résoudre. On prend le système de générateurs $\{1\}$. On peut alors facilement montrer par récurrence que, pour tout $n \in \mathbb{N}$,

$$\{g \in \mathbb{Z} | |g|_{\{1\}} \leq n\} = \{-n, -n+1, -n+2, ..., -1, 0, 1, ..., n-1, n\}.$$

On en tire que, pour tout naturel n,

$$\gamma_{\mathbb{Z}}^{\{1\}}(n) = 1 + 2n.$$

Passons maintenant à des groupes moins communs afin de voir comment ils se comportent.

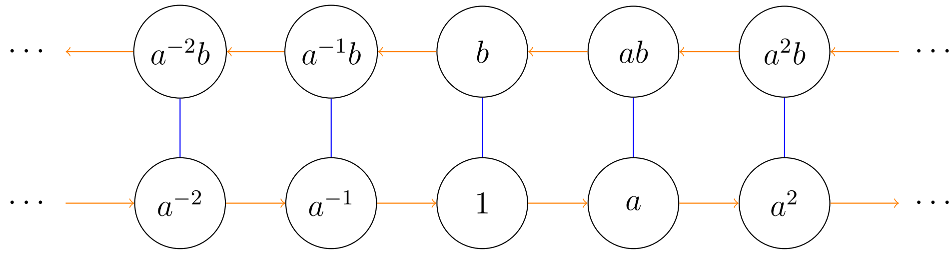


FIGURE 1.5 – Graphe de Cayley de $\mathcal{D}_\infty$.

Exemple 1.2.3. Le premier que nous allons étudier est

$$G = \mathcal{D}_\infty = \langle a, b | b^2 = 1 \text{ et } ab = ba^{-1} \rangle,$$

pour l'ensemble de générateurs $S = \{a, b\}$. Son graphe de Cayley est donné à la figure 1.5 avec pour convention que les arcs de label a sont oranges et ceux de label b sont bleus.

On calcule facilement les premières valeurs de γ_G^A :

$$\begin{aligned} \gamma_G^S(0) &= 1 \\ \gamma_G^S(1) &= 4 \\ \gamma_G^S(2) &= 8 \\ \gamma_G^S(3) &= 12 \\ \gamma_G^S(4) &= 16. \end{aligned}$$

On les trouve en appliquant l'algorithme décrit ci-dessous. C'est une version adaptée de l'algorithme tache d'huile de théorie des graphes. L'application de cet algorithme nous permet de conjecturer que la fonction de croissance de G par rapport à S est :

$$\gamma_G^S(n) = \begin{cases} 1 \text{ si } n = 0 \\ 4n \text{ si } n \geq 1. \end{cases}$$

Démonstration. On a, pour tout $n \geq 1$

$$B(1, n) = \{a^{-n}, ..., a^{-1}, 1, a, ..., a^n, a^{-n+1}b, ..., a^{-1}b, b, ab, ..., a^{n-1}b\}.$$

On le montre par récurrence. Clairement, pour $n = 1$, on a

$$B(1, n) = \{a^{-1}, 1, a, b\}.$$

Supposons que le résultat est vrai pour n et montrons qu'il est vrai pour $n+1$. Pour trouver $B(1, n+1)$ à partir de $B(1, n)$, on détermine les éléments à une distance 1 d'au moins un élément de $B(1, n)$. L'ensemble des tels éléments unis à $B(1, n)$ est $B(1, n+1)$. Or, par hypothèse de récurrence, on sait que

$$B(1, n) = \{a^{-n}, ..., a^{-1}, 1, a, ..., a^n, a^{-n+1}b, ..., a^{-1}b, b, ab, ..., a^{n-1}b\}.$$

De plus, pour tout $g \in \{a^{-n+1}, ..., a^{-1}, 1, a, ..., a^{n-1}, a^{-n+2}b, ..., a^{-1}b, b, ab, ..., a^{n-2}b\}$, ga^{-1}, ga et gb sont dans $B(1, n)$. Il reste donc à regarder les cas où $g = a^{-n}, a^n, a^{-n+1}b$ et $a^{n-1}b$.

— Si $g = a^{-n}$, alors $ga = a^{-n+1} \in B(1,n)$ et $ga^{-1} = a^{-n-1}, gb = a^{-n}b \notin B(1,n)$.

— Si $g = a^{n}$, alors $ga^{-1} = a^{n-1} \in B(1,n)$ et $ga = a^{n+1}, gb = a^{n}b \notin B(1,n)$.

— Si $g = a^{-n+1}b$, alors $ga^{-1} = a^{-n+1}ba^{-1} = a^{-n+2}b, gb = a^{-n+1} \in B(1,n)$ et $ga = a^{-n+1}ba = a^{-n}b \notin B(1,n)$.

— Si $g = a^{n-1}b$, alors $ga = a^{n-1}ba = a^{n-2}b, gb = a^{n-1} \in B(1,n)$ et $ga^{-1} = a^{n-1}ba = a^{n}b \notin B(1,n)$.

On en tire que

$$B(1,n+1) = \{a^{-(n+1)}, ..., a^{-1}, 1, a, ..., a^{n+1}, a^{-(n+1)+1}b, ..., a^{-1}b, b, ab, ..., a^{(n+1)-1}b\},$$

ce qui conclut le récurrence.

Un dernier comptage nous donne

$$|B(1,n)| = 4n,$$

pour tout $n \geq 1$.

On a donc bien, par définition,

$$\gamma_G^S(n) = \begin{cases} 1 \text{ si } n = 0 \\ 4n \text{ si } n \geq 1. \end{cases}$$

□

Exemple 1.2.4. Calculons la croissance du groupe libre $G = \langle a, b\rangle$ pour l'ensemble de générateurs $\{a,b\}$. Afin de ne pas ralentir la lecture, la définition de groupes libres est dans l'annexe A. Le graphe de Cayley $\Gamma(G,\{a,b\})$ est représenté à la figure 1.6 par où les arcs de label a sont représentés en bleu et vont de gauche à droite et les arcs de label b sont représentés en orange et vont de bas en haut ; les étiquettes des sommets ont été omises pour plus de lisibilité, le "centre" du graphe est en 1.

On compte facilement que le nombre de mots que l'on peut écrire en $n \geq 1$ lettres sur l'alphabet $S := \{a, a^{-1}, b, b^{-1}\}$ de manière à ce que deux inverses ne se suivent pas est :

$$4 \times 3^{n-1}.$$

On en tire que

$$\gamma_G^S(n) = 1 + \sum_{j=0}^{n-1} 4 \times 3^j = 2 \times 3^n - 1$$

Ce même raisonnement nous permet pour tout m d'avoir une fonction de croissance du groupe libre de rang m, F_m. Prenons un système de générateurs S à m éléments. On a

$$\gamma_{F_m}^S(n) = 1 + \sum_{j=0}^{n-1} 2m(2m-1)^j = \frac{m}{m-1}(2m-1)^n + 1 - \frac{m}{m-1}.$$

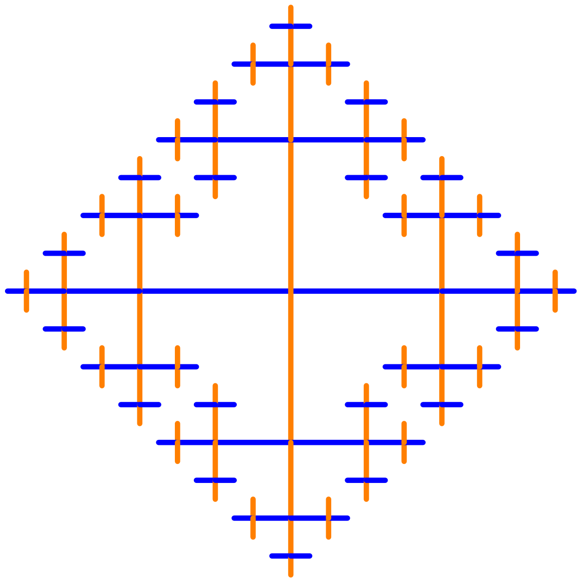


FIGURE 1.6 – Graphe de Cayley du groupe libre de rang 2.

1.2.2 Taux de croissance

Encore un fois, il y a un problème d'unicité par rapport au choix du système de générateurs. Cependant, on a pour deux systèmes finis de générateurs S et T l'existence d'un $C \in \mathbb{N}$ tel que

$$\gamma_G^S(n) \leq \gamma_G^T(Cn) \text{ et } \gamma_G^T(n) \leq \gamma_G^S(Cn)$$

pour tout $n \in \mathbb{N}$. En effet, on sait, par 1.1.1, qu'il existe un naturel C tel que

$$|g|_S \leq C|g|_T \text{ et } |g|_T \leq C|g|_S.$$

On en tire que

$$\{g \in G||g|_T \leq n\} \subset \{g \in G||g|_S \leq Cn\} \text{ et } \{g \in G||g|_S \leq n\} \subset \{g \in G||g|_T \leq Cn\},$$

pour tout $n \in \mathbb{N}$ et donc

$$\gamma_G^T(n) \leq \gamma_G^S(Cn) \text{ et } \gamma_G^S(n) \leq \gamma_G^T(Cn),$$

pour tout $n \in \mathbb{N}$. En fait, cette manière de voir les choses revient à considérer, les classes d'équivalences des fonctions de croissance pour la relation, $\approx$:

$$f \approx g \Leftrightarrow \exists C \in \mathbb{N} : \forall n \in \mathbb{N}_0, f(n) \leq g(Cn) \text{ et } g(n) \leq f(Cn),$$

pour $f, g \in \mathbb{N}^{\mathbb{N}}$. On définit également la relation d'ordre $\preceq$:

$$f \preceq g \Leftrightarrow \exists C \in \mathbb{N} : \forall n \in \mathbb{N}_0, f(n) \leq g(Cn).$$

En pratique on utilisera parfois la relation d'équivalence [3] formellement plus faible :

$$f \sim g \Leftrightarrow \exists C, A \in \mathbb{N} : \forall n \in \mathbb{N}_0, f(n) \leq Ag(Cn) \text{ et } g(n) \leq Af(Cn),$$

pour $f, g \in \mathbb{N}^{\mathbb{N}}$. Notons tout de même que ces relations d'équivalences sont équivalentes dans le cas des groupes infinis finiment engendrés (voir [Gri85]). Cette discussion permet de définir de manière unique le taux de croissance d'un groupe.

Définition 1.2.2. Pour G un groupe de type fini et S un système fini de générateurs, on appelle la classe d'équivalence $[\gamma_G^A]$ le *taux de croissance* de G ou plus simplement la *croissance* de G.

Ici, on a montré l'unicité du taux de croissance pour les groupes de type fini. C'est le seul cas raisonnable à traiter. En effet, sans cette restriction, on peut considérer des systèmes de générateurs infinis. Dans ce cas, $\gamma_G^G(n) = |G|$, pour tout $n \in \mathbb{N}_0$. Cela pose deux problèmes : les fonctions de croissance ne sont pas à valeurs naturelles et on n'a plus d'unicité. Il est donc naturel de se restreindre aux groupes de type fini. De plus, vu que le choix du système fini de générateurs n'importe pas, on peut toujours le prendre symétrique. Cela simplifie souvent les notations. Dans la suite, sauf mention de l'inverse, on considérera toujours les systèmes de générateurs comme étant finis et symétriques.

Stabilité du taux de croissance

Le taux de croissance est un invariant des groupes. Il l'est non seulement pour les groupes isomorphes mais aussi pour les groupes quasi-isométriques. C'est là la première propriété de stabilité du taux de croissance que l'on va montrer.

Proposition 1.2.2. *Deux groupes quasi-isométriques ont le même taux de croissance.*

Démonstration. Soient G, G' les deux groupes quasi-isométriques et $\phi : G \to G'$ une quasi-isométrie entre ces groupes. Montrons qu'il existe $M, C \in \mathbb{N}$ tels que

$$\gamma_G(n) \leq M\gamma_{G'}(Cn), \forall n \in \mathbb{N}\,.$$

On sait qu'il existe $C, D \in \mathbb{N}_0$ tels que

$$\frac{1}{C}|g^{-1}h|_S - D \leq |(\phi(g))^{-1}\phi(h)|_{S'} \leq C|g^{-1}h|_S + D,$$

pour tout $g, h \in G$, avec S, S' des systèmes de générateurs finis de G et G' respectivement. On en tire que

$$\phi\left(B(1_G, n)\right) \subset B(1_{G'}, Cn + D), \forall n \in \mathbb{N}\,.$$

En effet, prenons $g \in B(1_G, n)$, on a directement

$$|\phi(g)|_{S'} \leq C|g|_S + D \leq Cn + D.$$

3. Il est clair que ce sont des relations d'équivalence.

Dès lors,

$$|\phi\left(B(1_G, n)\right)| \leq |B(1_{G'}, (C + D)n)|\,, \forall n \in \mathbb{N},$$

à noter que le cas $n = 0$ se traite séparément.

On va maintenant montrer qu'il existe un M tel que

$$|B(1_G, n)| \leq M\,|\phi\left(B(1_{G'}, n)\right)|\,, \forall n \in \mathbb{N}\,.$$

On commence par observer que si $g_1, g_2 \in G$ sont tels que $\phi(g_1) = \phi(g_2)$, alors $|g_1^{-1}g_2|_S \leq CD$. Vu que $|B(1, CD)| = |B(x, CD)|$, pour tout x, on en déduit qu'un point de G' a au plus $|B(1, CD)|$ pré-images dans G par ϕ. On pose $M = |B(1, CD)|$ et on obtient

$$|B(1_G, n)| \leq M\,|\phi\left(B(1_{G'}, n)\right)|\,, \forall n \in \mathbb{N}\,.$$

Au total, on a

$$\gamma_G(n) = |B(1_G, n)| \leq M\,|B(1_{G'}, (C + D)n)| = M\gamma_{G'}((C + D)n), \forall n \in \mathbb{N}$$

et donc $\gamma_G \preceq \gamma_{G'}$. Vu la symétrie du problème, on peut conclure. □

Corollaire 1.2.1. *Deux groupes isomorphes ont le même taux de croissance.*

Démonstration. On a déjà établi, dans la preuve du corollaire 1.1.1, que les groupes isomorphes sont quasi-isométriques. On en tire qu'ils ont le même taux de croissance. □

On a établi que le taux de croissance des groupes était invariant aux isomorphismes. L'étape suivante est de voir comment se comporte cette propriété d'un groupe G par rapport aux groupes que l'on peut construire à partir de G. On pense aux sous-groupes, aux quotients et aux produits.

Proposition 1.2.3. *Soient G un groupe infini finiment engendré et H un sous-groupe de G finiment engendré. On a*

$$[\gamma_H] \preceq [\gamma_G].$$

Démonstration. Soient T un système fini de générateurs de H et S un système fini de générateurs de G. On peut supposer sans perte de généralité que $T \subset S$. Il devient alors clair que $\Gamma(H, T)$ est un sous-graphe de $\Gamma(G, S)$ et donc que

$$\gamma_H^T \leq \gamma_G^S.$$

La conclusion suit. □

Dans l'énoncé, il est bien précisé que l'on prend un sous-groupe finiment engendré d'un groupe finiment engendré. Cette précision peut au premier abord paraître superflue. Pourtant ce n'est pas le cas, tous les sous-groupes d'un groupe finiment engendrés ne sont pas nécessairement finiment engendrés. La notion de sous-groupe finiment engendré est centrale dans le reste du mémoire. On va donc prendre le temps de développer un contre-exemple bien que cela demande beaucoup de travail.

Définition 1.2.3. Soient G un groupe et $\mathrm{Aut}(G)$ le groupe des automorphismes de G. On définit l'*holomorphe* du groupe $G \rtimes \mathrm{Aut}(G)$ comme étant le groupe

$$(G \times \mathrm{Aut}(G), *),$$

où $(g, \varphi) * (h, \psi) = (g\varphi(h), \varphi \circ \psi)$, pour tout $g, h \in G$ et $\varphi, \psi \in \mathrm{Aut}(G)$. Classiquement, on omet le symbole $*$ lorsque le contexte est clair.

On vérifie facilement que c'est un groupe dont le neutre est $(1, \mathrm{id})$ et tel que $(g, \varphi)^{-1} = (\varphi^{-1}(g^{-1}), \varphi^{-1})$, pour tout $g \in G$ et $\varphi \in \mathrm{Aut}(G)$.

On remarque aussi que l'on a les plongements suivants :

$$\begin{aligned} G &\hookrightarrow G \rtimes \mathrm{Aut}(G) : g \mapsto (g, \mathrm{id}) \\ \mathrm{Aut}(G) &\hookrightarrow G \rtimes \mathrm{Aut}(G) : \varphi \mapsto (1, \varphi). \end{aligned}$$

On a même $G \lhd G \rtimes \mathrm{Aut}(G)$. En effet, pour tout $g, h \in G$ et $\varphi \in \mathrm{Aut}(G)$

$$\begin{aligned} (h, \varphi)(g, \mathrm{id})(h, \varphi)^{-1} &= (h\varphi(g), \varphi)(\varphi^{-1}(h^{-1}), \varphi^{-1}) \\ &= (h\varphi(g)h^{-1}, \mathrm{id}) \\ &\in G. \end{aligned}$$

Ce constat nous permet de donner un sens aux expressions de la forme $\varphi g \varphi^{-1}$, avec $g \in G$ et $\varphi \in \mathrm{Aut}(G)$. Dans $G \rtimes \mathrm{Aut}(G)$, on a

$$\varphi g \varphi^{-1} = \varphi(g),$$

pour tout $g \in G$ et $\varphi \in \mathrm{Aut}(G)$.

Définition 1.2.4. Soit $(G_i)_{i \in \mathcal{I}}$ une famille de groupes abéliens[4]. On définit la *somme directe* de ces groupes comme étant le groupe $\left(\bigoplus_{i \in \mathcal{I}}, * \right)$, où $\bigoplus_{i \in \mathcal{I}}$ est l'ensemble des éléments $(g_i)_{i \in \mathcal{I}}$ tels que $g_i \neq 0$ pour un nombre fini d'indices et où $*$ est la somme composante à composante.

On peut maintenant passer à la construction d'un groupe G de type fini qui admet un sous-groupe qui ne l'est pas. On prend $t \in \mathrm{Aut}\left(\bigoplus_{z \in \mathbb{Z}} \mathbb{Z} \right)$ le shift vers la droite (i.e : $t : (z_j)_{j \in \mathbb{Z}} \mapsto (z_{j-1})_{j \in \mathbb{Z}}$). On définit maintenant le groupe

$$G = \left\langle \bigoplus_{z \in \mathbb{Z}} \mathbb{Z}, t \right\rangle \leq \left(\bigoplus_{z \in \mathbb{Z}} \mathbb{Z} \right) \rtimes \left(\mathrm{Aut} \left(\bigoplus_{z \in \mathbb{Z}} \mathbb{Z} \right) \right). \tag{1.1}$$

On a $G = \langle s, t \rangle$, où $s \in \bigoplus_{z \in \mathbb{Z}} \mathbb{Z}$ est tel que $s_0 = 1$ et $s_j = 0, \forall j \in \mathbb{Z} \setminus \{0\}$. Cela découle du fait que $tst^{-1} = t(s)$. Cette astuce permet d'obtenir n'importe quel élément de $\bigoplus_{z \in \mathbb{Z}} \mathbb{Z}$. On en conclut, par définition de G que $\{s, t\}$ génère G.

4. On prend ici la notation additive pour l'opération de groupe.

Ainsi, G est finiment engendré. Cependant, ses sous-groupes ne le sont pas forcément. Le groupe

$$H = \bigoplus_{z \in \mathbb{Z}} \mathbb{Z}$$

peut être vu comme un sous-groupe de G par plongement. Ce H n'est pas finiment engendré. En effet, l'opération de groupe est l'addition composante à composante et le nombre de composantes est infini. Ainsi, en prenant n'importe quel ensemble fini, $F := \{g_1, ..., g_m\}$ de H, on sait par définition de la somme directe que, pour tout $i \in \{1, ..., m\}, (g_i)_j \neq 0$ seulement un nombre fini de fois. Ainsi, comme $\mathbb{Z}$ est infini, il existe un $j \in \mathbb{Z}$ tel que $(g_i)_j = 0$ pour tout $i \in \{1, ..., m\}$. Il n'est donc pas possible à partir d'un nombre fini d'opérations entre éléments de F d'obtenir l'élément $(\delta_{j,z})_{z\in\mathbb{Z}}$.

On se retrouve donc bien avec $H \leq G$ qui ne peut pas être généré par un ensemble fini alors qu'il est inclus dans un groupe de type fini. Ce qui conclut notre discussion sur les sous-groupes des groupes finiment engendrés.

Nous pouvons reprendre notre étude de la relation entre la croissance de G et la croissance des groupes créés à partir de G. La proposition qui suit concerne les sous-groupes d'indice fini de G et est d'une importance majeure.

Lemme 1.2.1. *Soient G un groupe de type fini et $H \leq G$. Si H est d'indice fini, alors H est de type fini.*

Démonstration. À chaque classe latérale droite, on associe un unique représentant de cette classe, en s'assurant que le représentant de H est 1. On définit alors $\varphi : G \to G$ qui à chaque élément g associe le représentant de sa classe latérale droite. Plus formellement, on définit $\psi : \left(\frac{G}{H}\right)_d \to G$ telle que $\psi(H) = 1$ et $\psi(Hg) \in Hg$. Ensuite, on pose $\varphi : G \to G : h \mapsto \psi(Hg)$.

On a immédiatement, pour tout $g, g' \in G$, les trois relations suivantes :

1. $\varphi(h) = 1, \forall h \in h$
2. $\varphi(\varphi(g)g') = \varphi(gg')$.

Prenons $S = \{\varphi(g) | g \in G\}$ et Y un ensemble fini symétrique de générateurs de G. On sait que S est fini, donc $\{sy(\varphi(sy))^{-1} | s \in S \text{ et } y \in Y\}$ l'est aussi. On va montrer que cet ensemble génère H. Fixons $h \in H$, il existe $y_1, ..., y_k \in Y$ tels que $h = y_1...y_k$. On a donc

$$\begin{aligned} h =& y_1(\varphi(y_1))^{-1} \cdot \varphi(y_1)y_2(\varphi(\varphi(y_1)y_2))^{-1} \cdot \varphi(\varphi(y_1)y_2)y_3(\varphi(\varphi(\varphi(y_1)y_2)y_3))^{-1} \cdot \\ & ... \cdot \varphi(...\varphi(y_1)...y_{k-1})y_k(\varphi(\varphi(...\varphi(y_1)...y_{k-1})y_k))^{-1} \end{aligned}$$

car $\varphi(\varphi(...\varphi(y_1)...y_{k-1})y_k) = \varphi(y_1...y_k) = e$ vu les relations 2 et 1. Chaque élément de H est donc bien de la forme souhaitée. $\square$

Proposition 1.2.4. *Soit G un groupe finiment engendré. Le taux de croissance de G est le même que le taux de croissance de ses sous-groupes d'indice fini.*

Démonstration. Soit $H \leq G$ d'indice fini n. On sait par le lemme 1.2.1 qu'il existe $T \subset H$ tel que T est fini et $\langle T \rangle = H$. On peut, par hypothèse, trouver S fini contenant T tel que $\langle S \rangle = G$. On pose également $\mathcal{C}$ tel que $[G : H] = |\mathcal{C}|$, les classes latérales droites de G sont $\{Hc | c \in \mathcal{C}\}$ et $1 \in \mathcal{C}$.

On va maintenant prouver que l'inclusion $H \hookrightarrow G$ est une quasi-isométrie, on pourra conclure par la proposition 1.2.2. Il est clair que, pour L bien choisi,

$$\forall g \in G, \exists h \in H : d_G(h, g) \leq L,$$

un tel L est donné par $\sup_{j=1}^{n}(c_j)$. En effet, pour tout g, il existe un c et un h tels que $g = hc_j$ et donc $d_G(x, h) = |c_j^{-1}|_G \leq L$. Prenons $h, h' \in H$, on voit facilement que

$$d_G(h, h') \leq d_H(h, h')$$

puisque $T \subset S$.

Il nous reste donc à montrer qu'il existe $C \geq 1$ et $D \geq 0$ indépendants de h, h' tels que

$$\frac{d_H(h, h')}{C} - D \leq d_G(h, h').$$

On peut prendre $C = \sup\left(\{|x|_H | x \in \mathcal{C}S\mathcal{C}^{-1} \cap H\}\right) + 1$ (cette borne supérieure existe car les ensembles $\mathcal{C}$ et S sont finis) et $D = 0$. Montrons-le : on sait que $h^{-1}h'$ peut s'écrire d'au moins une manière sous la forme $x_1 ... x_m$ où $m = |h^{-1}h'|_S$ et $x_j \in S$. Pour chacun des mots $x_1 ... x_k$, il existe un unique $c \in \mathcal{C}$ tel que $x_1 ... x_k c^{-1} \in H$, notons le c_k. On peut réécrire

$$h^{-1}h' = (x_1 c_1^{-1})(c_1 x_2 c_2^{-1}) ... (c_{n-2} x_{n-1} c_{n-1}^{-1})(c_{n-1} x_n^{-1}).$$

On remarque que chaque parenthèse est dans $\mathcal{C}S\mathcal{C}^{-1}$ car $1 \in \mathcal{C}$. Chaque parenthèse se trouve dans H par induction. On a $x_1 c_1^{-1} \in H$ par définition. Ensuite,

$$(x_1 c_1^{-1})(c_1 x_2 c_2^{-1}) ... (c_k x_k c_k^{-1}) = x_1 ... x_k c_k^{-1} \in H$$

et par hypothèse de récurrence, $(x_1 c_1^{-1}) ... (c_{k-1} x_{k-1} c_{k-1}^{-1}) \in H$, donc $(c_k x_k c_k^{-1}) \in H$. Ainsi, pour tout k, $(c_k x_k c_k^{-1}) \in \mathcal{C}S\mathcal{C}^{-1} \cap H$.

Dès lors, on peut écrire chacune de ces parenthèses en moins de C éléments de T et donc

$$d_H(h, h') \leq Cn = C d_G(h, h').$$

La conclusion suit. □

Cette proposition a une interprétation géométrique importante. Une fois de plus, on va regarder le groupe G de loin. Le groupe ressemble à son sous-groupe H d'indice fini. En effet, on a un ensemble fini d'éléments $\{c_1, ..., c_k\}$ tel que tout g s'écrit $c_j h$. En un sens, G est composé de k copies de H, qui sont proches car il existe une constante M telle que $|c_j| \leq M$ pour tout j. Ainsi, de loin, on ne pourrait pas distinguer ces différentes copies de H et G grandit alors exactement comme H.

Ce résultat nous sera utile dans plusieurs développements théoriques. Il peut également l'être en pratique. Il permet, si on connaît la croissance de H, de déterminer la croissance de tout G de type fini dont H est un sous-groupe d'indice fini.

Intéressons-nous aux taux de croissance des quotients et des produits de groupes.

Proposition 1.2.5. *Soient G un groupe infini finiment engendré et $N \lhd G$. On a*

$$\left[\gamma_{\frac{G}{N}}\right] \preceq [\gamma_G].$$

Démonstration. Soient S un système fini de générateurs de G et $\pi : G \to \dfrac{G}{N}$ la projection canonique. On a directement $|B_G(1,n)| \geq |\pi\left(B_G(1,n)\right)|$ pour tout n. Montrons maintenant que

$$\pi\left(B_G(1,n)\right) = B_{\frac{G}{N}}(1,n),$$

pour tout n, où $\dfrac{G}{N}$ est muni de la métrique induite par le système fini de générateurs $T = \{sN | s \in S\}$. L'inclusion de $\pi\left(B_G(1,n)\right)$ dans $B_{\frac{G}{N}}(1,n)$ est évidente. Pour l'autre sens, prenons $gN \in B_{\frac{G}{N}}(1,n)$, il existe alors $m \leq n$ et $s_1, ..., s_m \in S \cup S^{-1}$ tels que

$$gN = s_1 ... s_m N.$$

On a donc l'existence d'un $h \in N$ tel que

$$gh = s_1 ... s_m \in B_G(1,n) \text{ et } \pi(gh) = ghN = gN.$$

On a les deux inclusions et donc l'égalité souhaitée. On en tire l'inégalité souhaitée :

$$\gamma_{\frac{G}{N}}(n) = \left|B_{\frac{G}{N}}(1,n)\right| = |\pi\left(B_G(1,n)\right)| \leq |B_G(1,n)| = \gamma_G(n),$$

pour tout n. □

Proposition 1.2.6. *Soient $G_1, ..., G_k$ des groupes de type fini et $\gamma_1, ..., \gamma_k$ des fonctions de croissance de ces groupes. La fonction $n \mapsto \gamma_1(n) ... \gamma_k(n)$ est une fonction de croissance pour $G = G_1 \times ... \times G_k$.*

Démonstration. Soient $S_1, ..., S_k$ des systèmes finis de générateurs de $G_1, ..., G_k$ respectivement tels que, pour tout j, $\gamma_{G_j}^{S_j} = \gamma_j$. On pose

$$S = \{(s_1, ..., s_k) \in G | s_j \in S_j, \forall j\}.$$

Il est clair que cet ensemble est fini et comme le produit se fait composante à composante, il génère G. On a bien

$$\gamma_G^S(n) = \gamma_1(n) ... \gamma_k(n).$$

En effet, chaque k-uplet atteignable en n étapes a des composantes atteignables en n étapes pour le système de générateurs correspondant car on fait le produit composante à composante. De plus, pour chaque k-uplet g d'éléments qui s'écrivent en n générateurs et inverses de générateurs, on peut, en prenant le produit des k-uplets de générateurs, atteindre g en moins de n étapes. □

La définition des taux de croissance et, en particulier, l'équivalence par le biais de laquelle ils sont définis mènent à une discussion naturelle. Il s'agit de déterminer quelles fonctions sont équivalentes pour savoir quelles croissances peuvent l'être. On compile ici plusieurs relations entre des fonctions de croissance potentielles.

Proposition 1.2.7. *Pour tout $\alpha, \alpha' \geq 0$, si*

$$n \mapsto n^{\alpha} \sim n \mapsto n^{\alpha'},$$

alors $\alpha = \alpha'$. Plus généralement, si $\alpha \leq \alpha'$, on a

$$n \mapsto n^{\alpha} \preceq n \mapsto n^{\alpha'}.$$

Démonstration. Par l'absurde, s'il existe $p > 0$ et $C \in \mathbb{N}$ tel que $\alpha = \alpha' + p$ et pour tout $n \neq 0$,

$$n^{\alpha} \leq (Cn)^{\alpha'},$$

alors, pour tout $n \neq 0$,

$$\begin{aligned} & n^{\alpha} \leq (Cn)^{\alpha'} \\ \Leftrightarrow & n^{\alpha'} n^{p} \leq C^{\alpha'} n^{\alpha'} \\ \Leftrightarrow & n^{p} \leq C^{\alpha'}. \end{aligned}$$

C'est une absurdité pour n suffisamment grand. Le cas $\alpha' > \alpha$ se traite de la même manière, on peut donc conclure. □

Proposition 1.2.8. *Pour tout $d \in \mathbb{N}$, $c_0, ..., c_d \in \mathbb{R}$ avec $c_d > 0$,*

$$P : n \mapsto c_d n^d + c_{d-1} n^{d-1} + ... + c_1 n + c_0 \sim n \mapsto n^d,$$

si P est strictement croissante sur $\mathbb{N}_0$.

Démonstration. Commençons par chercher un K tel que $P(n) \leq (Kn)^d, \forall n \in \mathbb{N}$. Pour $C \in \mathbb{N}$ suffisamment, on sait que

$$\lim_{x \to +\infty} P(x) - (Cx)^d = \lim_{x \to +\infty} (c_d - C^d) x^d + c_{d-1} x^{d-1} + ... + c_0 = -\infty.$$

De plus, il existe un nombre fini de points d'intersection entre le graphe sur $\mathbb{R}$ de P et de $x \mapsto (Cx)^d$. On pose $M = 1 + \lceil \sup\{(x, y) | P(x) = (Cx)^d\} \rceil$. Par le théorème des valeurs intermédiaires et vu la limite calculée au-dessus, on en tire que, pour tout $x \geq M$, $P(x) \leq (Cx)^d$. Comme P est strictement croissante sur $\mathbb{N}_0$, on obtient au total :

$$P(n) \leq P(Mn) \leq (MCn)^d,$$

pour tout $n \in \mathbb{N}_0$, MC est le K annoncé. De la même manière, on peut trouver un C tel que

$$\lim_{x \to +\infty} -P(x) + (Cx)^d = \lim_{x \to +\infty} (1 - c_d C^d)x^d - C^{d-1} c_{d-1} x^{d-1} + ... + c_0 = -\infty.$$

La même astuce que celle utilisée dans le premier cas permet de conclure qu'il existe K' tel que $n^d \leq P(K'n)$ pour tout n non-nul. On conclut en prenant le maximum de K et K'. $\square$

Corollaire 1.2.2. *Pour P, P' des fonctions polynomiales strictement croissantes sur $\mathbb{N}_0$, si $P \sim P'$, alors $\deg(P) = \deg(P')$.*

Proposition 1.2.9. *Pour tout $\lambda \geq 1$,*

$$n \mapsto \lambda^n \sim n \mapsto 2^n.$$

Démonstration. Supposons que $\lambda \geq 2$, on a $2^n \leq \lambda^n$. De plus, on a $\lambda^n = 2^{\log_2(\lambda)n}$. On peut donc prendre $C = \log_2(\lambda)$ et on obtient les deux inégalités souhaitées puisque $n \mapsto 2^n$ est strictement croissante et $C > 1$. $\square$

Proposition 1.2.10. *Pour tout d, $n \mapsto n^d$ n'est pas dans la même classe d'équivalence que $n \mapsto 2^n$. De plus, $n \mapsto n^d \preceq n \mapsto 2^n$.*

Démonstration. Sinon, il existerait un C tel que $2^n \leq (Cn)^d$ pour tout $n \in \mathbb{N}_0$ or, on sait que c'est faux pour n suffisamment grand. Cependant, pour tout d, il existe un C tel que $n^d \leq 2^{Cn}$ pour tout n. En effet, on sait que, pour tout d, $\lim_{n \to +\infty} \frac{n^d}{2^n} = 0$. Par définition, cela implique qu'il existe un N tel que, pour tout $n \geq N$, $\frac{n^d}{2^n} < 1$. Si on prend $C = N$, on a

$$n^d \leq (Cn)^d < 2^{Cn}.$$

$\square$

Proposition 1.2.11. *Pour tout $\alpha, \alpha' \in \mathbb{R}^+$, si*

$$n \mapsto e^{n^\alpha} \sim n \mapsto e^{n^{\alpha'}},$$

alors $\alpha = \alpha'$. Plus généralement, si $\alpha \leq \alpha'$,

$$n \mapsto e^{n^\alpha} \preceq n \mapsto e^{n^{\alpha'}}.$$

Démonstration. C'est un corollaire de la proposition 1.2.7 puisque exp est strictement croissante sur $\mathbb{N}_0$. $\square$

1.2.3 Classification des groupes selon leur taux de croissance

Ces premières classes d'équivalences de fonctions de croissance nous permettent de classer les groupes selon leur taux de croissance.

Définition 1.2.5. Un groupe G est à *croissance polynomiale* si pour toute fonction de croissance γ,
$$\exists C, d > 0 : \forall n \in \mathbb{N}_0, \gamma(n) \leq Cn^d.$$
Autrement dit, il existe un d tel que $\gamma \preceq (n \mapsto n^d)$

Remarque 1.2.2. Vu la définition du taux de croissance, si une seule fonction de croissance est $\preceq$ à un polynôme, elles le sont toutes.

Ce sont les groupes qui sont "lents" dans le sens où il évoluent, asymptotiquement, moins vite qu'un polynôme. La proposition suivante illustre cette observation de manière analytique.

Proposition 1.2.12. *Soient G un groupe et γ une fonction de croissance de G,*
$$G \text{ est à croissance polynomiale } \Leftrightarrow \limsup_{n\to+\infty} \frac{\ln(\gamma(n))}{\ln(n)} \in \mathbb{R}\,.$$

Démonstration. Le sens $\Rightarrow$ est évident. L'autre sens se résout en posant $\alpha = \limsup_{n\to+\infty} \frac{\ln(\gamma(n))}{\ln(n)}$ et en appliquant la définition de la lim sup. Pour tout $\varepsilon > 0$, il existe un N tel que $n \geq N$ implique
$$\left| \sup_{j\geq n} \frac{\ln(\gamma(n))}{\ln(n)} - \alpha \right| < \varepsilon.$$
On en tire directement la suite d'implications :
$$\begin{aligned} &\forall n \geq N, \frac{\ln(\gamma(n))}{\ln(n)} < \varepsilon + \alpha \\ \Rightarrow &\forall n \geq N, \ln(\gamma(n)) < \ln(n)(\varepsilon + \alpha) \\ \Rightarrow &\forall n \geq N, \gamma(n) < n^{\lceil \varepsilon+\alpha \rceil}. \end{aligned}$$
Donc, pour $C = N$, on a
$$\gamma(n) \leq \gamma(Cn) \leq (Cn)^{\lceil \varepsilon+\alpha \rceil},$$
pour tout $n \in \mathbb{N}_0$. Ainsi, $\gamma \preceq (n \mapsto n^{\lceil \varepsilon+\alpha \rceil})$ et donc G est à croissance polynomiale. $\square$

On peut donner les exemples suivants de groupes à croissance polynomiale.

Exemple 1.2.5. Intéressons-nous aux groupes abéliens finiment engendrés. Soit $S = \{s_1, ..., s_m\}$ un ensemble de générateurs du groupe abélien A. On a
$$|B(1,n)| = \left\{ s_1^{\varepsilon_1} ... s_m^{\varepsilon_m} | \sum_{j=1}^{m} \varepsilon_j \leq n \text{ et } \forall j, \varepsilon_j \in \mathbb{N} \right\}.$$

pour tout $n \in \mathbb{N}$. On en tire que, pour tout $n \in \mathbb{N}_0$,

$$\begin{aligned} B(1,n) &\leq \left| \left\{ (\varepsilon_1, ..., \varepsilon_m) | \sum_{j=1}^{m} \varepsilon_j \leq n \text{ et } \forall j, \varepsilon_j \in \mathbb{N} \right\} \right| \\ &\leq |\{(\varepsilon_1, ..., \varepsilon_m) | \forall j, \varepsilon_j \in \{0, ..., n\}\}| \\ &\leq (n+1)^m \\ &\leq 2^m n^m. \end{aligned}$$

Le groupe A est donc à croissance polynomiale.

Exemple 1.2.6. Le groupe G présenté à la définition 1.1 est à croissance polynomiale. Reprenons le système de générateurs $S = \{s, t\}$. Voyons comment majorer le nombre d'éléments (x, y) que l'on peut obtenir en n produits de générateurs et leurs inverses. On constate que $x_j = 0$ pour tout $|j| \geq n+1$. De plus, pour tout $j, x_j \in \{-n, ..., n\}$. Pour finir, sur la deuxième composante, vu l'opération de G, on a $y \in \{t^{-n, ..., t^n}\}$. Au total,

$$B(1,n) \hookrightarrow \{-n, ..., n\}^{2n} \times \{t^{-n}, ..., t^n\},$$

où le plongement efface simplement les x_j pour des $j \notin \{-n, ..., n\}$. Ainsi, $\gamma_G^S(n) \leq 2n(2n+1)$ et donc G est bien à croissance polynomiale.

Après les groupes à croissance polynomiale et surtout leur caractérisation donnée à la proposition 1.2.12, il semble naturel de définir les groupes qui ne sont pas à croissance polynomiale. Ce sont les groupes qui grandissent plus vite que tous les polynômes. Attention cependant ce n'est pas une trivialité à montrer. La difficulté réside dans le fait qu'on n'a pas à priori de raison de penser que toutes les fonctions de croissance des groupes sont comparables (au sens de $\preceq$) aux polynômes.

Définition 1.2.6. On définit les groupes à *croissance superpolynomiale* comme étant les groupes G qui ne sont pas à croissance polynomiale.

Vu la proposition 1.2.12, c'est équivalent à demander qu'une fonction de croissance γ de G soit telle que

$$\limsup_{n \to +\infty} \frac{\ln(\gamma(n))}{\ln(n)} = +\infty.$$

Si γ a cette propriété, toutes les fonctions de croissance de G l'ont.

En pratique, beaucoup de groupes étudiés ont un taux de croissance que l'on peut comparer à $\exp(\cdot^\alpha)$. Il est donc utile de voir à quelle classe de croissance appartient un groupe dont une fonction de croissance γ est plus grande que $\exp(\cdot^\alpha)$.

Proposition 1.2.13. *Tout groupe à croissance* $\gamma \succeq \exp(\cdot^\alpha)$*, pour un* $\alpha > 0$ *est à croissance superpolynomiale.*

Démonstration. On sait qu'il existe C tel que

$$\exp(n^\alpha) \leq \gamma(Cn),$$

pour tout $n \in \mathbb{N}_0$. On a les inégalités :

$$\begin{aligned}\limsup_{n\to+\infty} \frac{\ln(\gamma(n))}{\ln(n)} &\geq \limsup_{n\to+\infty} \frac{\ln(\gamma(Cn))}{\ln(Cn)} \\ &\geq \limsup_{n\to+\infty} \frac{\ln(\exp(n^\alpha))}{\ln(Cn)} \\ &\geq \lim_{n\to+\infty} \frac{n^\alpha}{\ln(Cn)} = +\infty.\end{aligned}$$

C'est la caractérisation des groupes à croissance superpolynomiale. On peut conclure. □

Une classe importante de groupes est celle des groupes à croissance exponentielle. Son importance vient du fait qu'aucun groupe ne croit plus vite que les groupes à croissance exponentielle.

Définition 1.2.7. Un groupe G est à *croissance exponentielle* si ses fonctions de croissance sont équivalentes à exp.

Remarque 1.2.3. On note que le choix de la base de l'exponentielle dans la définition n'a pas d'importance. C'est une conséquence de la proposition 1.2.9.

Remarque 1.2.4. Comme pour les groupes à croissance polynomiale, par définition du taux de croissance, si une fonction de croissance est équivalente à l'exponentielle, alors elles le sont toutes.

Proposition 1.2.14. *La croissance exponentielle est la croissance la plus rapide pour un groupe. Autrement dit, pour tout groupe G de type fini*

$$\gamma_G^S \preceq \exp$$

pour tout système fini de générateurs S.

Démonstration. Dans l'exemple 1.2.4, on montre que le taux de croissance du groupe libre de rang m est

$$\left[n \mapsto \frac{m}{m-1}(2m-1)^n + 1 - \frac{m}{m-1}\right].$$

De plus, pour tout système de générateurs $S = \{s_1, ..., s_k\}$, l'identité $s_j s_j^{-1} = 1$ est vraie. Donc, le nombre d'éléments de G que l'on peut générer en n produits d'éléments de S est inférieur à γ_{F_k}. Par définition de $\preceq$, on peut conclure. □

On peut, à partir de la définition, établir une hiérarchie entre les groupes à croissance polynomiale, superpolynomiale et exponentielle.

Proposition 1.2.15. *La classe des groupes à croissance exponentielle et celle des groupes à croissance polynomiale sont disjointes.*

Démonstration. Vu la proposition 1.2.10, on sait que, pour tout d, $n \mapsto n^d \prec \exp$ et donc qu'un G à croissance polynomiale de fonction de croissance γ est tel que $\gamma \prec \exp$. Les groupes à croissance polynomiale ne sont donc pas à croissance exponentielle.

Prenons maintenant G un groupe à croissance exponentielle et γ une fonction de croissance de G. On sait que $\gamma \succeq \exp()$ et donc par la proposition 1.2.13, G n'est pas à croissance polynomiale. □

Corollaire 1.2.3. *Les groupes à croissance exponentielle sont à croissance superpolynomiale.*

Comme pour la croissance polynomiale, on peut donner un équivalent analytique à la croissance exponentielle. Dans ce cas-ci, elle demande un peu plus de travail. Commençons par deux résultats qui ne portent pas sur les groupes à croissance exponentielle.

Proposition 1.2.16. *Soient G un groupe finiment engendré et S un système fini de générateurs de G. La limite*

$$\lim_{n\to+\infty} \sqrt[n]{(\gamma_G^S(n))}$$

existe et est finie.

Démonstration. On sait que, pour tout q, si on prend $n \geq q$, il existe $k_n \in \mathbb{N}$ et $r_n \in \{0, ..., q-1\}$ tels que $n = k_n q + r_n$. On a donc,

$$\begin{aligned}
\sqrt[n]{(\gamma(n))} &\leq \sqrt[n]{\gamma((k_n-1)q + q + r_n))} \\
&\leq \sqrt[n]{\gamma(q)^{(k_n-1)\frac{q}{q}}}\sqrt[n]{\gamma(q+r_n)} && \text{vu la proposition 1.2.1} \\
&\leq \gamma(q)^{\frac{n-r_n}{nq}} \sqrt[n]{\gamma(q+r_n)}.
\end{aligned}$$

On peut prendre la lim sup des deux côtés de cette inégalité, dans le membre de droite, comme r_n est borné, on obtient $\sqrt[q]{\gamma(q)}$. Comme c'est vrai pour tout $q \geq 1$, on a

$$\limsup_{n\to+\infty} \sqrt[n]{(\gamma(n))} \leq \inf_{q\geq 1} \sqrt[q]{\gamma(q)}.$$

De plus, par définition de la lim inf, on a $\inf_{q\geq 1} \sqrt[q]{\gamma(q)} \leq \liminf_{n\to+\infty} \sqrt[n]{(\gamma(n))}$. Au total,

$$\limsup_{n\to+\infty} \sqrt[n]{(\gamma(n))} = \liminf_{n\to+\infty} \sqrt[n]{(\gamma(n))} = \lim_{n\to+\infty} \sqrt[n]{(\gamma(n))} = \inf_{q\geq 1} \sqrt[q]{\gamma(q)}.$$

□

Remarque 1.2.5. La proposition 1.2.16 est vraie pour toute suite $(u_n)_{n\in\mathbb{N}}$ telle que $u_{m+n} \leq u_m u_n$.

Corollaire 1.2.4. *Soit γ une fonction de croissance d'un groupe de type fini. La limite*

$$\lim_{n\to+\infty} \frac{\ln(\gamma(n))}{n}$$

existe et est finie.

Démonstration. Il suffit d'appliquer ln à la limite $\lim_{n\to+\infty} \sqrt[n]{(\gamma(n))}$. On conclut par les propriétés de ln, à savoir ln est continue et $\ln(x^r) = r\ln(x)$. $\square$

On peut maintenant passer à la caractérisation des groupes à croissance exponentielle.

Proposition 1.2.17. *Soient G un groupe finiment engendré et γ l'une de ses fonctions de croissance. On a l'équivalence suivante :*

$$G \textit{ est à croissance exponentielle } \Leftrightarrow \lim_{n\to+\infty} \sqrt[n]{(\gamma(n))} > 1.$$

Démonstration. Si G est à croissance exponentielle, on sait qu'il existe $C > 0$ tel que $\exp(n) \leq \gamma(Cn)$ pour tout $n \neq 0$. Dans ce cas,

$$\begin{aligned}
\lim_{n\to+\infty} \sqrt[n]{(\gamma(n))} &= \lim_{n\to+\infty} \sqrt[Cn]{(\gamma(Cn))} \qquad \lim_{n\to+\infty} \sqrt[n]{(\gamma(n))} \text{ vu la proposition 1.2.16} \\
&\geq \lim_{n\to+\infty} \sqrt[Cn]{(\exp(n))} \\
&\geq \exp\left(\frac{1}{C}\right) > 1.
\end{aligned}$$

Montrons l'autre sens de l'équivalence et supposons que $\lim_{n\to+\infty} \sqrt[n]{(\gamma(n))} > 1$. On a alors $\lim_{n\to+\infty} \frac{\ln(\gamma(n))}{n} > 0$, or

$$\begin{aligned}
\lim_{n\to+\infty} \frac{\ln(\gamma(n))}{n} > 0 &\Rightarrow \frac{\ln(\gamma(n))}{n} > 0, \text{ pour tout } n \text{ suffisamment grand} \\
&\Rightarrow \ln(\gamma(n)) > n, \text{ pour tout } n \text{ suffisamment grand} \\
&\Rightarrow \gamma(n) > \exp(n), \text{ pour tout } n \text{ suffisamment grand.}
\end{aligned}$$

On peut prendre C assez grand pour que $\gamma(Cn) \geq \exp(Cn) \geq \exp(n)$, pour tout $n \in \mathbb{N}_0$. On a donc bien $\gamma \succeq \exp$ et vu la proposition 1.2.14, on a également $\gamma \preceq \exp$. On peut donc conclure. $\square$

De cette caractérisation, on peut tirer une deuxième caractérisation en appliquant un ln.

Corollaire 1.2.5. *Soient G un groupe finiment engendré et γ l'une de ses fonctions de croissance. On a l'équivalence suivante :*

$$G \textit{ est à croissance exponentielle } \Leftrightarrow \lim_{n\to+\infty} \frac{\ln(\gamma(n))}{n} > 0.$$

Comme dans ce qui a été fait pour les groupes à croissance polynomiale, on peut définir les groupes qui ne sont pas à croissance exponentielle. Ce sont les groupes à croissance sous-exponentielle. Comme toutes les fonctions de croissance sont $\preceq$ à l'exponentielle, les groupes à croissance sous-exponentielle peuvent être vus comme les groupes à croissance plus lente que l'exponentielle.

Définition 1.2.8. On définit les groupes à *croissance sous-exponentielle* comme étant les groupes dont les fonctions de croissance γ sont telles que $\gamma \prec \exp$.

Vu la proposition 1.2.17 et la proposition 1.2.14, on peut de manière équivalente demander que les fonctions de croissance γ soient telles que

$$\lim_{n\to+\infty} \sqrt[n]{\gamma(n)} \leq 1.$$

On a même l'égalité car $\gamma(n) \geq 1$ pour tout n.

Remarque 1.2.6. Si une fonction de croissance est plus lente que l'exponentielle, elles le sont toutes.

Similairement à ce qui a été fait pour les groupes à croissance superpolynomiale, on peut déduire la croissance sous-exponentielle d'un groupe à partir d'un comparaison avec $\exp(\cdot^\nu)$.

Proposition 1.2.18. *Tout groupe G à croissance $\gamma \preceq \exp(\cdot^\nu)$, pour un $\nu < 1$ est à croissance sous-exponentielle.*

Démonstration. On sait qu'il existe C tel que, pour tout $n \in \mathbb{N}_0$, $\gamma(n) \leq \exp((Cn)^\nu)$. On a

$$\begin{aligned}\lim_{n\to+\infty} \frac{\ln(\gamma(n))}{n} &\leq \lim_{n\to+\infty} \frac{\ln(\exp((Cn)^\nu))}{n} \\ &\leq \lim_{n\to+\infty} \frac{(Cn)^\nu}{n} = 0\end{aligned}$$

car $\nu < 1$. On conclut par le corollaire 1.2.5 que le groupe G n'est pas à croissance exponentielle et donc, il est à croissance sous-exponentielle. □

On observe que, de manière analogue aux groupes à croissance exponentielle inclus dans les groupes à croissance superpolynomiale, les groupes à croissance polynomiale sont à croissance sous-exponentielle.

La dernière classe que nous définirons ici sont les groupes à croissance intermédiaire. Ils permettent de partitionner les groupes en fonction de leurs taux de croissance.

Définition 1.2.9. Les groupes à *croissance intermédiaire* sont les groupes à croissance superpolynomiale et sous-exponentielle. Autrement dit, ce sont les fonctions qui ne sont ni à croissance polynomiale, ni à croissance exponentielle.

Proposition 1.2.19. *Les groupes à croissance polynomiale, intermédiaire et exponentielle partitionnent la classe des groupes finiment engendrés.*

Chapitre 2

Groupes nilpotents

L'objectif de ce chapitre est de prouver que les *groupes nilpotents* sont à croissance polynomiale. Pour ce faire, nous commencerons par définir les groupes nilpotents de deux manières équivalentes et nous en donnerons quelques propriétés qui seront utilisées dans les sections suivantes. Ensuite, on montrera la croissance polynomiale de groupes nilpotents en tant que tel. On finira le chapitre par une définition des groupes *virtuellement nilpotents* et on en donnera le taux de croissance. Ces résultats sont importants puisque les groupes virtuellement nilpotents sont les seuls groupes à croissance polynomiale.

Les sources utilisées pour la rédaction de ce chapitre sont surtout [DK20] et [Man12] pour ce qui est des détails techniques et des exemples. La marche à suivre pour établir la croissance polynomiale des groupes nilpotents vient, elle, de [DlCM13].

2.1 Définitions

Les groupes nilpotents sont une généralisation de groupes abéliens. Cette section explique comment les définir et pourquoi ils sont "presque" abéliens.

Avant toute autre chose, un bref rappel sur ce que sont les centralisateurs semble à propos. Souvenons-nous également qu'ils permettent de caractériser les groupes abéliens.

Définition 2.1.1. Pour un groupe G, le *centralisateur* de G est le sous-groupe $\{x \in G | xg = gx, \forall x \in G\}$. On le note $Z(G)$.

Proposition 2.1.1. *Un groupe G est abélien si et seulement s'il est son propre centralisateur.*

Une autre notion cruciale dans l'étude des groupes abéliens est celle de commutateur. Elle est tout aussi importante lorsqu'il s'agit de groupes nilpotents.

Définition 2.1.2. Soient G un groupe et $a, b \in G$. On définit le *commutateur* de a et b comme étant $[a, b] = a^{-1}b^{-1}ab$. On a directement les propriétés suivantes :

— $[a, b]^{-1} = [b, a]$

— $[a, b] = 1 \Leftrightarrow ab = ba$.

Pour $H, K \leq G$, on définit également $[H, K]$ comme étant le groupe engendré par les éléments $[h, k]$, où $h \in H$ et $k \in K$. On notera que $[H, K] = [K, H]$ puisque, pour tout $h \in H, k \in K$, $[h, k]^{-1} = [k, h]$. On en tire que le groupe $[H, K]$ est donné par l'ensemble des produits finis d'éléments de la forme $[h, k]$ ou $[k, h]$, avec $h \in H$ et $k \in K$.

Cette définition permet de montrer les deux propositions suivantes.

Proposition 2.1.2. *Soit G un groupe, on a $Z(G) = \{x \in G | [x, g] = 1, \forall g \in G\}$.*

Proposition 2.1.3. *Soient G, G' un groupe, $a, b \in G$ et $\phi : G \to G'$ un morphisme. On a*

$$\phi([a, b]) = [\phi(a), \phi(b)].$$

De plus, pour $H, K \leq G$, $\phi([H, K]) = [\phi(H), \phi(K)]$.

Démonstration. On a directement :

$$\phi([a, b]) = \phi(a^{-1}b^{-1}ab) = (\phi(a))^{-1}(\phi(b))^{-1}\phi(a)\phi(b) = [\phi(a), \phi(b)].$$

La deuxième partie de la proposition est immédiate. □

Nous avons tous les outils pour définir les groupes nilpotents.

Définition 2.1.3. Soit G un groupe. G est *nilpotent* s'il existe un naturel s et une suite finie croissante de sous-groupes normaux de G,

$$1 = G_0 \leq G_1 \leq ... \leq G_{s-1} \leq G_s = G$$

telle que, pour tout $j \in \{0, ..., s\}$,

$$\frac{G_{j+1}}{G_j} \subset Z\left(\frac{G}{G_j}\right). \tag{2.1}$$

On appelle une telle suite de sous-groupes normaux une *suite centrale*.

Si la suite est de longueur s, on dit que G est nilpotent de classe inférieure à s. On dit que G est nilpotent de *classe* s si sa plus courte suite centrale est de longueur s.

Remarque 2.1.1. La condition (2.1) est équivalente à demander

$$\left[\frac{G_{j+1}}{G_j}, \frac{G}{G_j}\right] = 1$$

ou encore

$$[G_{j+1}, G] \leq G_j.$$

Remarque 2.1.2. On a directement l'inclusion des groupes nilpotents dans les groupes résolubles. Tout comme celle des abéliens dans les nilpotents.

Un exemple classique de groupe nilpotent est le groupe d'Heisenberg. L'exemple suivant met en évidence une classe plus grande de groupes nilpotents mais il demande à montrer la proposition suivante.

Proposition 2.1.4. *Soient R un anneau unitaire, $n \in \mathbb{N}$ et $I \subset R$ un sous-anneau de R tel que $I^n = 0$, où I^j est le sous-anneau engendré par $\{x_1...x_j | x_i \in I, \forall i\}$ (i.e : I^j = les sommes de produits d'éléments de la forme $x_1...x_j$ où $x_j \in I$). On a*

1. *Pour tout $j \in \mathbb{N}, G_j = 1 + I^j$ est un sous-groupe $R^\times$.*
2. *La suite*
$$1 = G_n \leq G_{n-1} \leq ... \leq G_2 \leq G_1$$
est une suite centrale de G_1 et G_1 est donc nilpotent de classe $\leq n-1$.

Démonstration. 1. Prenons S un sous-anneau quelconque de R et montrons que $1+S$ est un sous-groupe de $R^\times$. Soient $x, y \in R$, on a

$$\begin{aligned} &1 \in 1+S, \\ &(1+x)(1+y) \in 1+S \\ &\quad \text{car } (1+x)(1+y) = 1+x+y+xy \text{ et } \forall s_1, s_2 \in S, s_1+s_2, s_1s_2 \in S \\ \text{et } &(1+x)^{-1} = (1-x+x^2-x^3...+(-1)^{n-1}x^{n-1}) \in 1+S \\ &\quad \text{car } I^n = 0 \text{ et } (1+x)(1-x+x^2-x^3...+(-1)^{n-1}x^{n-1}) = 1+(-1)^{n-1}x^n. \end{aligned}$$

µ On a bien $1+S \leq R^\times$. En particulier, pour tout j, G_j est un groupe.

2. Commençons par montrer que ces inclusions sont légitimes. On a $I^{j+1} \subset I^j$ pour tout j car tout générateur $x_1...x_jx_{j+1}$ de I^{j+1} est un générateur de I^j, il suffit pour le voir de remarquer que $x_jx_{j+1} \in I$. On a donc bien $G_{j+1} \leq G_j$
Vu la remarque 2.1.1, il suffit de montrer que, pour tout $i \leq n-1$, $[G_1, G_i] \leq G_{i+1}$. Prenons $g \in G_1$ et $h \in G_i$, on a
$$[g,h] - 1 = g^{-1}h^{-1}(gh - hg).$$
Comme il existe $x, z \in I$ et $y \in I^i$ tels que $g = 1+x$, $h = 1+y$ et $g^{-1}h^{-1} \in I$,
$$[g,h] - 1 = (1+z)(xy - yx) = xy - yx - zxy + zyx,$$
or tous ces termes sont dans I^{i+1} vu les inclusions de I^j dans les I^i si $i \leq j$. Ainsi,
$$[g,h] = 1 + xy - yx - zxy + zyx \in 1 + I^{i+1} = G_{i+1}.$$

□

Exemple 2.1.1. Soient A un anneau avec unité, $n \geq 2$ un naturel et $B = (A^{n \times n}, +, \cdot)$. On va montrer que le groupe

$$G = (\{(a_{ij})_{1 \leq i,j \leq n} \in B | a_{ij} \in A, a_{ii} = 1 \text{ et } a_{ij} = 0, \forall i > j\}, \cdot)$$

est nilpotent de classe $n-1$.

On peut se servir de la proposition 2.1.4 pour montrer que G est nilpotent de classe $\leq n-1$. Il suffit de remarquer que, pour $I = \{(a_{ij})_{1\leq i,j\leq n} \in B | a_{ij} \in A \text{ et } a_{ij} = 0, \forall i \geq j\}$, I est un sous-anneau de $B^\times$, $G = 1 + I$ et $I^n = 0$.

En particulier, le groupe de Heisenberg

$$H = \left(\left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} | x, y, z \in \mathbb{Z} \right\}, \cdot \right)$$

est nilpotent de classe plus petite ou égale à 2.

On sait aussi que

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Donc H n'est pas abélien, autrement dit, pas nilpotent de classe 1. Il est donc nilpotent de classe 2.

Cette définition des groupes nilpotents basée sur l'existence de suites centrales n'est pas idéale pour déterminer facilement si un groupe est nilpotent. Le problème est qu'on ne sait pas quelle suite tester pour vérifier si elle est centrale. Les calculs sont simplifiés en sachant avec quelle suite travailler. On peut par exemple utiliser la suite centrale descendante.

Définition 2.1.4. Soit G un groupe, on définit la *suite centrale descendante* (ou LCS pour *Lower Central Series*) comme étant la suite $(\gamma_j(G))_{j\in N_0}$ telle que $\gamma_1(G) = G$ et $\gamma_{j+1}(G) = [\gamma_j(G), G]$. Un élément de $\gamma_j(G)$ est appelé un *commutateur de profondeur j*. Le groupe $[G, G]$ est appelé *groupe dérivé* de G ou encore le *commutateur* de G.

On montrera que si la suite centrale descendante d'un groupe est ultimement triviale, alors le groupe est nilpotent et réciproquement. Avant la démonstration du résultat qui nous intéresse, nous allons démontrer deux lemmes.

Lemme 2.1.1. *Soit G un groupe quelconque. Pour tout $j \in \mathbb{N}_0$, $\gamma_j(G) \lhd G$.*

Démonstration. On procède par induction. Le cas de $\gamma_1(G) = G$ est évident. Ensuite, par hypothèse de récurrence, $\gamma_{j-1}(G)$ est normal dans G. On en tire, vu la proposition 2.1.3 que, pour tout $g \in G$,

$$g\gamma_j(G)g^{-1} = g[\gamma_{j-1}(G), G]g^{-1} = [g\gamma_{j-1}(G)g^{-1}, gGg^{-1}].$$

Donc par normalité de $\gamma_{j-1}(G)$ et G,

$$g\gamma_j(G)g^{-1} = [\gamma_{j-1}(G), G] = \gamma_j(G).$$

□

Lemme 2.1.2. *Soit G un groupe nilpotent de suite centrale*

$$1 = G_0 \leq G_1 \leq ... \leq G_s = G.$$

Pour tout $j \in \{1, ..., s+1\}$, on a

$$\gamma_j(G) \leq G_{s+1-j}$$

Démonstration. On procède par récurrence sur j. Si $j = 1$, alors $\gamma_1(G) = G = G_s = G_{s+1-j}$. Supposons que le résultat est vrai pour $j - 1 < s - 1$. Pour tout $c_{j-1} \in \gamma_{i-1}(G)$ et $g \in G$, on a

$$c_{j-1}^{-1} g^{-1} c_{j-1} g \in [G_{s+1-(j-1)}, G]$$

car par hypothèse de récurrence, $\gamma_{j-1}(G) \subset G_{s+1-(j-1)}$. Or, par la remarque 2.1.1, $[G_{s+1-(j-1)}, G] \leq G_{s+1-j}$. On en tire que $\gamma_j(G) \leq G_{s+1-j}$ car tous ses générateurs sont inclus dans G_{s+1-j}. □

Théorème 2.1.1. *Soit G un groupe.*

$$G \text{ est nilpotent de classe } s \Leftrightarrow \gamma_{s+1}(G) = 1.$$

Démonstration. Commençons par le sens $\Rightarrow$. Soit $1 = G_0 \leq G_1 \leq ... \leq G_s = G$ une suite centrale de longueur minimale de s. Vu le lemme, $\gamma_{s+1}(G) \leq G_{s+1-(s+1)} = G_0 = 1$.

Montrons maintenant l'autre sens. On va commencer par montrer que la suite de $\gamma_{s+1}(G), ..., \gamma_2(G), \gamma_1(G)$ est ascendante. On sait par le lemme 2.1.1 que $\gamma_j(G) \lhd G$ pour tout j. On en tire la suite d'équivalences suivantes :

$$\begin{aligned}
&\gamma_j(G) \lhd G \\
\Leftrightarrow &\forall g \in G, \forall c_j \in \gamma_j(G), g^{-1} c_j g \in \gamma_j(G) \\
\Leftrightarrow &\forall g \in G, \forall c_j \in \gamma_j(G), [g, c_j] = c_j^{-1} g^{-1} c_j g \in \gamma_j(G) \\
\Leftrightarrow &\gamma_{j+1}(G) = [\gamma_j(G), G] \leq \gamma_j(G)
\end{aligned}$$

car $[\gamma_j(G), G]$ est le sous-groupe des produits finis d'éléments de la forme $[c_j, g]$. Ensuite, pour tout j

$$[\gamma_j(G), G] = \gamma_{j+1}(G) \leq \gamma_{j+1}(G),$$

$\gamma_1(G) = G$ et $\gamma_{s+1} = 1$. Ainsi, par la remarque 2.1.1, la LCS bien une suite centrale [1].

Il reste à montrer que cette suite centrale est de longueur minimale pour prouver que G est nilpotent de classe s. C'est évident vu le lemme car la LCS est incluse composante à composante dans toute suite centrale. □

Cette proposition met en lumière une autre manière de voir que les groupes nilpotents sont presque abéliens. On sait que, pour un groupe nilpotent G, si on imbrique assez de commutateurs, on obtient un élément qui commute avec tous les $g \in G$. En effet, si $h \in \gamma_s(G)$, alors $[h, g] \in \gamma_{s+1}(G) = 1$ et donc $gh = hg$.

Cette caractérisation des groupes nilpotents nous permet d'aborder de nouveaux exemples. En effet, le calcul de suites centrales descendantes peut s'avérer assez facile.

1. Observons qu'il faut ré-indicer la suite pour obtenir exactement une suite centrale.

Exemple 2.1.2. Le groupe diédral d'ordre 8, $\mathcal{D}_4$ est nilpotent. Posons

$$\mathcal{D}_4 = \{1, a, a^2, a^3, ab, a^2b, a^3b\},$$

on a

$$\gamma_1(\mathcal{D}_4) = \mathcal{D}_4.$$

Ensuite, on remarque que, pour tout $g, g' \in \mathcal{D}_4$, $[g, g']$ contient un nombre pair de b et donc est égal à $1, a, a^2$ ou a^3. De plus, puisque $a^{-1} = a^3$, le nombre de a dans $[g, g']$ est pair. Ainsi, $[\mathcal{D}_4, \mathcal{D}_4] \subset \{1, a^2\}$. Or, $[a, b] = a^2$ et donc

$$\gamma_2(\mathcal{D}_4) = [\mathcal{D}_4, \mathcal{D}_4] = \{1, a^2\}.$$

Comme $1, a^2 \in Z(\mathcal{D}_4)$, on a

$$\gamma_3(\mathcal{D}_4) = [\{1, a^2\}, \mathcal{D}_4] = 1$$

et donc $\mathcal{D}_4$ est nilpotent de classe 2.

Exemple 2.1.3. Le groupe diédral d'ordre 6, $\mathcal{D}_3 = \{1, a, a^2, b, ab, a^2b\}$ n'est pas nilpotent. On sait que $\gamma_1(\mathcal{D}_3) = \mathcal{D}_3$. Comme pour l'exemple 2.1.2, on sait que $[\mathcal{D}_3, \mathcal{D}_3] \subset \{1, a, a^2\}$. De plus, $[a, b] = a$ et $[b, a] = a^2$, donc

$$\gamma_2(\mathcal{D}_3) = [\mathcal{D}_3, \mathcal{D}_3] = \{1, a, a^2\}.$$

Ensuite, on sait que $\gamma_3(\mathcal{D}_3) \subset \gamma_2(\mathcal{D}_3) = \{1, a, a^2\}$ et que $[a, a] = 1, [a, b] = a$ et $[a^2, b] = a^2$. Donc, $\{1, a, a^2\} \subset [\gamma_2(\mathcal{D}_3), \mathcal{D}_3]$. Par récurrence, on a, pour tout $j \geq 3$

$$\gamma_j(\mathcal{D}_3) = [\gamma_{j-1}(\mathcal{D}_3), \mathcal{D}_3] = [\{1, a, a^2\}, \mathcal{D}_3] = \{1, a, a^2\}.$$

Le groupe $\mathcal{D}_3$ n'est donc pas nilpotent car la suite $(\gamma_j(\mathcal{D}_3))_{j \in \mathbb{N}_0}$ se stabilise avant 1.

2.2 Quelques propriétés

Après avoir défini les groupes nilpotents de deux manières, on s'attarde ici sur quelques propriétés de ces groupes. Elles concernent la stabilité du caractère nilpotent d'un groupe et le type fini des $\gamma_j(G)$ sous certaines conditions.

Commençons par vérifier que "être nilpotent des classe s" est bien une propriété préservée par les isomorphismes.

Proposition 2.2.1. *Soient G et G' deux groupes isomorphes et $s \in \mathbb{N}_0$. On a la bi-implication*

$$G \text{ nilpotent de classe } s \Leftrightarrow G' \text{ nilpotent de classe } s$$

Définition 2.2.1. Supposons que G est nilpotent de classe s et que $\varphi : G \to G'$ est un isomorphisme. Par la proposition 2.1.3, on sait que $\gamma_j(G') = \gamma_j(\varphi(G)) = \varphi(\gamma_j(G))$, pour tout j. Or, $\varphi(\gamma_s(G)) = \varphi(1) = 1$. Ainsi, G' est nilpotent de classe $\leq s$. Supposons que G' soit nilpotent de classe $t < s$. Dans ce cas, on aurait, grâce à l'isomorphisme φ^{-1}, G de nilpotent de classe $< s$. Cela contredit notre hypothèse. Ainsi, on a bien G' nilpotent de classe s.

L'autre sens de l'implication se prouve de la même manière.

La proposition suivant montre la stabilité de la nilpotence pour les sous-groupes et les quotients de groupes nilpotents.

Proposition 2.2.2. *Soit G un groupe nilpotent de classe plus petite que s. Pour tout $H \leq G$, H est nilpotent de classe inférieure à s et pour tout $N \lhd G$, $\dfrac{G}{N}$ est nilpotent de classe inférieure à s.*

Démonstration. Soit $1 = G_0 \leq G_1 \leq ... \leq G_i \leq G_{i+1} \leq ... \leq G_s = G$ une suite centrale de G. La suite $(H \cap G_i)_{i=0}^s$ est telle que $[H, H_{i+1}] \leq H_i$, $H \cap G_0 = 1$ et $H \cap G_s = H$. Vu la remarque 2.1.1, on a donc H nilpotent de classe $\leq s$. La suite $\left(\frac{G_i N}{N}\right)_{i=0}^s$ est telle que $\left[\frac{G}{N}, \frac{G_{i+1}N}{N}\right] \leq \frac{G_i N}{N}$, $\frac{G_0 N}{N} = 1$ et $\frac{G_s N}{N} = \frac{G}{N}$. Cette même remarque 2.1.1 nous permet de conclure. $\square$

Dans le chapitre 1, on a insisté sur l'importance de comprendre les sous-groupes finiment engendrés des groupes finiment engendrés. On comprendra pourquoi c'est important lorsqu'on calculera la croissance des groupes nilpotents finiment engendrés. Avant de le faire, nous avons besoin de montrer que le groupe dérivé d'un groupe nilpotent finiment engendré est finiment engendré. Démontrer ce résultat est l'objet de la fin de cette section.

Lemme 2.2.1. *Soient G un groupe, j un naturel, $a, b \in \gamma_j$ et $c, d \in G$. On a*

$$[ab, cd]\gamma_{j+2}(G) = [a, d][b, d][a, c][b, c]\gamma_{j+2}(G)$$

et

$$[a^{-1}, b]\gamma_{j+2}(G) = [a, b]^{-1}\gamma_{j+2}(G) = [a, b^{-1}]\gamma_{j+2}(G).$$

On dit abusivement que le commutateur est bilinéaire modulo $\gamma_j(G)$.

Démonstration. On commence par remarquer que, de manière générale, pour $x, y, z \in G$,

$$\begin{aligned}
[xy, z] &= y^{-1}x^{-1}z^{-1}xyz \\
&= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz \\
&= y^{-1}[x, z]y[y, z] \\
&= [x, z][x, z]^{-1}y^{-1}[x, z]y[y, z] \\
&= [x, z][[x, z], y][y, z]
\end{aligned}$$

et

$$\begin{aligned}[x,yz] &= x^{-1}z^{-1}y^{-1}xyz \\ &= x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz \\ &= [x,z]z^{-1}[x,y]z \\ &= [x,z][x,y][x,y]^{-1}z^{-1}[x,y]z \\ &= [x,z][x,y][[x,y],z].\end{aligned}$$

Si on applique ces résultats à a, b, c, d modulo $\gamma_{j+2}(G)$, on obtient la première identité de l'énoncé. En effet,

$$\begin{aligned}[ab,c]\gamma_{j+2}(G) \quad &= [a,c][[a,c],b][b,c]\gamma_{j+2}(G) = [a,c][b,c]\gamma_{j+2}(G) \text{ car } \gamma_{j+2}(G)\lhd \\ \text{et } [a,cd]\gamma_{j+2}(G) \quad &= [a,d][a,c][[a,c],d]\gamma_{j+2}(G) = [a,d][a,c]\gamma_{j+2}(G).\end{aligned}$$

Il nous reste à montrer la deuxième identité :

$$\begin{aligned}1\gamma_{j+2}(G) &= [aa^{-1},c]\gamma_{j+2}(G) = [a,c][a^{-1},c]\gamma_{j+2}(G) \\ \text{et } 1\gamma_{j+2}(G) &= [a,cc^{-1}]\gamma_{j+2}(G) = [a,c^{-1}][a,c]\gamma_{j+2}(G).\end{aligned}$$

Ce qui veut bien dire que $[a^{-1},c]$ et $[a,c^{-1}]$ sont l'inverse de $[a,c]$ modulo $\gamma_{j+2}(G)$. □

Proposition 2.2.3. *Soit G un groupe engendré par M, supposé symétrique. Le sous-groupe $\gamma_j(G)$ est engendré par $\gamma_{j+1}(G)$ et les éléments de la forme*

$$[...[[m_1,m_2],m_3]...,m_j],$$

où $m_1,...,m_j \in M$.

Démonstration. On procède par récurrence sur j. Si $j=1$, alors $\gamma_1(G) = G = \langle M\rangle$, avec $m \in M$ vu comme un commutateur de longueur 1. Passons à l'induction et supposons que le résultat est vérifié pour j et montrons qu'il est toujours vrai pour $j+1$. Par l'hypothèse de récurrence et la normalité de $\gamma_{j+1}(G)$, un élément $x \in \gamma_j(G)$ est de la forme

$$x_1^{\epsilon_1}x_2^{\epsilon_2}...x_r^{\epsilon_r}z,$$

où $x_k = [...[[m_1^{(k)},m_2^{(k)}],m_3^{(k)}]...,m_j^{(k)}]$ pour des $m_l^{(k)} \in M$ bien choisis, $\epsilon_j \in \{-1,1\}$ et $z \in \gamma_{j+1}(G)$. On sait aussi qu'un élément $y \in G$ peut s'écrire

$$a_1...a_s,$$

pour $a_1,...,a_s \in M$ bien choisis.

Par ailleurs, on sait que $\gamma_{j+1}(G) = [\gamma_j(G),G] = \langle\{[x,y] | x \in \gamma_j(G), y \in G\}\rangle$. Il est donc raisonnable d'étudier les éléments $[x,y]$ tels que $x \in \gamma_j(G), y \in G$. Fixons un tel couple (x, y). On peut, vu que $\gamma_{j+2}(G)$ est dans l'ensemble de générateurs que l'on souhaite attribuer à $\gamma_{j+1}(G)$, se contenter de regarder les $[x, y]$ modulo $\gamma_{j+2}(G)$:

$$\begin{aligned}
[x, y]\gamma_{j+2}(G) &= [x_1^{\varepsilon_1}...x_r^{\varepsilon_r} z, a_1...a_s]\gamma_{j+2}(G) \\
&= \prod_{l=1}^{r}\prod_{k=1}^{s}[x_l, a_{s+1-k}]^{\varepsilon_l}\prod_{k=1}^{s}[z, a_{s+1-k}]\gamma_{j+2}(G) \\
&= \prod_{l=1}^{r}\prod_{k=1}^{s}[x_l, a_{s+1-k}]^{\varepsilon_l}\gamma_{j+2}(G)
\end{aligned}$$

car modulo $\gamma_{j+2}(G)$, le commutateur est bilinéaire vu le lemme 2.2.1.

Donc, les générateurs de $\gamma_{j+1}(G)$ sont de la forme souhaitée. On en tire que

$$\gamma_{j+1}(G) \leq \langle\{[[...[[m_1, m_2], m_3]..., m_j], m_{j+1}]|m_k \in M, \forall k\} \cup \gamma_{j+2}(G)\rangle$$

□

Corollaire 2.2.1. *Les groupes nilpotents finiment engendrés ont un commutateur finiment engendré.*

Démonstration. Soient s la classe de nilpotence de G et M un système fini symétrique de générateurs de G. Vu la proposition, un système de générateurs de $[G, G]$ est donné par $S = \{[...[[m_1, m_2], m_3]..., m_k]|k \in \mathbb{N}_0, m_j \in M\}$. Or, comme G est nilpotent, si $k \geq c + 1$, alors $\gamma_k(G) = 1$. On a donc

$$S = \{[...[[m_1, m_2], m_3]..., m_k]|k \leq c, m_j \in M\},$$

ce S est bien fini. □

2.3 Croissance des groupes nilpotents

On prouve dans cette section que les groupes nilpotents sont à croissance polynomiale. Pour ce faire, on a un lemme technique et ensuite une démonstration élémentaire du résultat.

Lemme 2.3.1. *Soient G un groupe nilpotent finiment engendré et $H \leq G$ finiment engendré et à croissance polynomiale tel que $[G, G] \leq H$. On a $K = \langle H, t\rangle$ à croissance polynomiale pour tout $t \in G$.*

Démonstration. Commençons par montrer que tout élément $x \in K$ peut s'écrire $t^z h$ avec $z \in \mathbb{Z}$ et $h \in H$. On sait que $x = k_1...k_n$ avec $k_j \in \{t, t^{-1}\} \cup H$ et pour tout $h \in H, \varepsilon \in \{-1, 1\}$, $ht^\varepsilon = t^\varepsilon h[h, t^\varepsilon]$ et $[h, t^\varepsilon] \in [G, G] \leq H$. Donc, on peut ramener tous les $k_j \in \{t, t^{-1}\}$ à gauche quitte à ajouter des commutateurs dans la décomposition. Cette astuce est l'outil principal de cette démonstration.

Posons $T = \{h_1, ..., h_m\}$ un système fini symétrique de générateurs de H. Prenons un élément $x \in K = \langle H, t\rangle$, il peut se décomposer en un produit fini d'éléments de $T \cup t, t^{-1}$. Soient w une telle décomposition de x et n le nombre de facteurs de ce produit. Vu le paragraphe précédent, on sait qu'il existe $h \in H, z \in \mathbb{Z}$ tels que $x = t^z h$. On décrit ci-dessous une procédure qui permet de modifier w en une décomposition w' de cette forme.

1. On initialise w' à w.
2. On cherche la position p du premier t ou t^{-1} dans w' qui n'est ni en première position de la décomposition ni précédé d'un t ou d'un t^{-1}. S'il n'y en a pas, on passe à l'étape suivante, sinon on termine.
3. On met à jour w' en définissant w''

$$\begin{aligned}
&w''_j \leftarrow w'_j \text{ pour tout } j < k-1\\
&w''_{k-1} \leftarrow w'_k\\
&w''_k \leftarrow w'_{k-1}\\
&w''_{k+1} \leftarrow [w'_{k-1}, w_k]\\
&w''_j \leftarrow w'_{j-1} \text{ pour tout } j > k+1
\end{aligned}$$

   et en faisant après, $w' \leftarrow w''$.
4. On retourne à l'étape (2).

Il est clair que cet algorithme se finit puisqu'on ne crée jamais de nouveaux t ou t^{-1} et à chaque passage dans la boucle, on a rapproché un t ou t^{-1} de la gauche. En sortie, on se retrouve avec une décomposition w' dont les facteurs sont dans

$$\{[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_j}] | h_i \in T, j \in \mathbb{N} \text{ et } \varepsilon_q \in \{-1, 1\}\} \cup \{t, t^{-1}\}.$$

Intéressons-nous aux derniers termes de la décomposition w', à savoir le produit v de tous les facteurs de w' différents de t ou t^{-1}. Soit s la classe de nilpotence de G. On peut enlever de v tous les facteurs de la forme

$$[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_s + j}],$$

car ils seront égaux à 1.

Maintenant, nous allons majorer le nombre de facteurs de la forme $[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_j}]$, pour tout $j \leq s$. Si $j = 0$, on sait que la construction de w ne rajoute pas de facteurs qui sont dans T, elle les déplace juste. Donc on a moins de n facteurs de la forme h_i.

Supposons que v ait moins de n^j facteurs de la forme $[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_j}]$. On va montrer qu'alors il contient moins de n^{j+1} facteurs de la forme $[[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_j}], t^{\varepsilon_{j+1}}]$. On sait que pour créer un commutateur de profondeur $j+1$, il faut que, lors de la construction de w', un commutateur de profondeur j ait été créé à gauche d'un t^ε avec $\varepsilon \in \{-1, 1\}$. Comme w contient n facteurs et que dans la construction de w', on ne crée jamais de nouveaux facteurs t^ε, on sait qu'il y a au plus n facteurs t^ε qui peuvent être à gauche d'un commutateur de profondeur j donné. Comme on a au plus n^j commutateurs de profondeur

j, on peut déduire qu'on créera au plus $n \times n^j = n^{j+1}$ commutateurs de profondeur $j+1$. Ceci conclut l'induction.

Au total, w' est une décomposition de x de la forme $t^z h$ avec $z \in \mathbb{Z}$ et $h \in H$, où h se décompose en moins de $n + n^2 + ... + n^s$ éléments de $C = \{[...[[h_i, t^{\varepsilon_1}], t^{\varepsilon_2}], ..., t^{\varepsilon_j}] | h_i \in T, j \leq s \text{ et } \varepsilon_q \in \{-1, 1\}\}$. Comme T est fini, C l'est aussi. Comme $C \subset [G, G] \subset H$, on peut définir un nombre A tel que tout élément de C admet une décomposition réduite de longueur plus petite que A. Ainsi, h se décompose en $A(n + ... + n^s)$ éléments de T.

Pour conclure, il nous reste à remarquer qu'un élément de K qui peut se décomposer en moins de n éléments de $T \cup \{t\}$ doit pouvoir s'écrire comme $t^z h$ où $z \in \{-2n, ..., 2n\}$ et $h \in B(1, A(n + ... + n^s))$. Autrement dit,

$$\gamma_K(n) \leq (2n+1)\gamma_H(A(n+n^s)).$$

Or, on sait que H est à croissance polynomiale et donc qu'il existe un polynôme P tel que, pour tout n, $\gamma_H(n) \leq P(n)$. On en tire que, pour tout n,

$$\gamma_K(n) \leq (2n+1)P(A(n + ... + n^s)).$$

On peut conclure car on a $\gamma_K \preceq Q$ où $Q(n) = (2n+1)P(A(n + ... + n^s))$ est un polynôme car c'est le produit d'un polynôme par une composition de polynômes. $\square$

Théorème 2.3.1. *Soit G un groupe nilpotent finiment engendré, G est à croissance polynomiale.*

Démonstration. On sait par le corollaire 2.2.1 que $[G, G]$ est finiment engendré, posons $T = \{t_1, ..., t_m\}$ un tel ensemble de générateurs. On peut donc trouver un système de générateurs fini $S = \{t_1, ..., t_m, s_1, ..., s_n\}$ de G qui contient T.

On peut montrer par récurrence sur la classe de nilpotence s de G que G est à croissance polynomiale. Si $s = 1$, alors G est abélien et on a la croissance polynomiale par l'exemple 1.2.5.

Passons à l'induction et supposons que la propriété est vérifiée pour tous les groupes de classe de nilpotence $< s$. On sait que $[G, G]$ est de classe de nilpotence $< s$ car

$$\gamma_{s+1}(G) = 1 \geq ... \geq \gamma_3(G) \geq \gamma_2(G) = [G, G]$$

est une suite centrale. On en tire que $[G, G]$ est à croissance polynomiale par hypothèse de récurrence. Définissons la suite de groupes :

$$[G, G] = \langle T \rangle \leq \langle T, s_1 \rangle \leq \langle T, s_1, s_2 \rangle \leq ... \leq \langle T, s_1, ..., s_{n-1} \rangle \leq \langle T, s_1, ..., s_n \rangle = G.$$

Ensuite, il suffit d'itérer le lemme 2.3.1 pour voir que les groupes ci-dessus sont à croissance polynomiale, on peut conclure. $\square$

2.4 Groupes virtuellement nilpotents

Dans la dernière section de ce chapitre, nous définissons les groupes virtuellement nilpotents de type fini. Leur importance ne peut pas être exagérée. Ils caractérisent les groupes à croissance polynomiale. On montrera ici que les groupes virtuellement nilpotents finiment engendrés sont à croissance polynomiale. La réciproque est l'objet du chapitre 3.

Commençons par définir la notion de virtuellement nilpotent.

Définition 2.4.1. Soit $\mathcal{P}$ une propriété de groupes (i.e : stable par isomorphisme). On dit qu'un groupe G est *virtuellement* $\mathcal{P}$ s'il existe un sous-groupe H de G d'indice fini tel que H est $\mathcal{P}$. Ainsi, un groupe *virtuellement nilpotent* est un groupe qui contient un sous-groupe d'indice fini nilpotent.

Remarque 2.4.1. Les groupes finis sont virtuellement nilpotents car $1 \leq G$ est d'indice fini et abélien donc nilpotent pour tout G fini.

On a immédiatement la proposition suivante puisque les groupes sont quasi-isométriques à leurs sous-groupes d'indice fini.

Proposition 2.4.1. *Les groupes virtuellement nilpotents finiment engendrés sont à croissance polynomiale.*

Démonstration. Soit $H \leq G$ d'indice fini et nilpotent. On sait par le lemme 1.2.1 que H est finiment engendré et donc par le théorème 2.3.1 qu'il est à croissance polynomiale. On tire donc de la proposition 1.2.4 que G lui-même est à croissance polynomiale. $\square$

Chapitre 3

Théorème de Gromov

Le théorème de Gromov est l'un des points centraux de l'étude de la croissance des groupes. Il permet de caractériser les groupes à croissance polynomiale et donc, en un sens, de justifier la classification des groupes par leurs taux de croissance. Comme dit dans l'introduction, la question vient de John Milnor en 1968 dans [Mil68b]. Sa conjecture est que les groupes à croissance polynomiale sont exactement les groupes qui contiennent un sous-groupe nilpotent d'indice fini. Cette conjecture sera prouvée par Mikhael Gromov en 1981 dans *Groups of polynomial growth and expanding maps* [Gro81]. Elle sera ensuite connue sous le nom de *Théorème de Gromov.*

Ce résultat est fondamental en théorie géométrique des groupes. Il permet de caractériser algébriquement certains groupes à partir d'une propriété géométrique grossière, leur croissance. Cette équivalence permet de montrer plusieurs résultats non-triviaux en géométrie riemannienne (voir [Tao14]). Par exemple, il permet de montrer le théorème suivant :

Théorème 3.0.1. *Soit M une variété riemannienne compacte. Si la courbure de Ricci de M est positive, alors le groupe fondamental de M est virtuellement nilpotent.*

Comme mentionné dans l'introduction, la démonstration de Gromov et les outils qu'il développe dans sa preuve ont également eu une grande influence sur le domaine. Depuis, plusieurs preuves de ce résultat ont été écrites. Chacune présente des avantages et des inconvénients.

Dans ce chapitre, nous donnerons un bref aperçu de la preuve originale de Gromov basé sur ce qui en est dit dans [Man12] et [DK18]. Ensuite, nous détaillerons la preuve du théorème de Gromov proposée en 2010 sur le blog de Terrence Tao sous le nom *A proof of Gromov's theorem*, [Tao10]. Elle est inspirée de son article [ST10] co-écrit avec Yehuda Shalom. Cette démonstration présente l'avantage d'être accessible car elle évite deux résultats fondamentaux trop subtils pour être traités avec rigueur dans ce mémoire. Ces deux résultats sont la solution au cinquième problème de Hilbert et l'alternative de Tits.

3.1 L'approche de Gromov

La démonstration présentée dans [Gro81] est d'une importance capitale. Sa nature géométrique permet de montrer le résultat mais aussi, de le comprendre fondamentalement. De plus, elle est la première à utiliser la solution au cinquième problème de Hilbert trouvée dans les années 50 par Montgomery et Zippin.

Donnons un bref résumé de cette preuve afin de mieux comprendre pourquoi elle est si importante. L'idée de Gromov est de regarder le groupe "de loin". C'est une idée commune dans le domaine. Souvenons-nous de l'interpétation des quasi-isométries. Plus spécifiquement, ce que Gromov propose est de considérer le groupe comme une suite d'espaces métriques. Il en prend la limite et se sert ensuite des propriétés de cette limite pour appliquer le cinquième problème de Hilbert et se ramener à un groupe de Lie. L'utilisation de résultats tels que l'alternative de Tits et le théorème de Milnor-Wolf permet de conclure.

Ce court paragraphe ne rend pas justice à la preuve originale mais il rend compte des nombreuses connaissances théoriques qu'elle demande. C'est là son défaut et la raison qui fait qu'on préférera pour ce mémoire se consacrer à une preuve qui nécessite moins de pré-requis.

Un point de la preuve originale mérite malgré tout d'être encore un peu détaillé, c'est la limite d'espaces métriques qui est considérée. Commençons par remarquer que $\mathbb{Z}$ muni de la distance euclidienne est un espace métrique. De même pour $\mathbb{Z}$ muni de la distance euclidienne divisée par deux, par trois... Ces espaces successifs sont isométriques au plongement de $\mathbb{Z}$ dans $\mathbb{R}$ où l'on divise les entiers par le même facteur que les distances. Ce faisant, on a obtenu tous les points de $\mathbb{Q}$. On peut alors intuitivement voir la limite de ces espaces métriques comme $\mathbb{R}$ tout entier. On peut visualiser une suite de représentations de $\mathbb{Z} \times \mathbb{Z}$ devenant $\mathbb{R} \times \mathbb{R}$ de la même manière. On comprend à partir de cette construction pourquoi on dit regarder le groupe de loin. À chaque étape, comme on divise les distances par un naturel plus grand, on s'éloigne du groupe.

Gromov a formalisé cette notion et il l'a surtout rendue plus générale en l'appliquant aux graphes de Cayley. Il se sépare ainsi de la nécessité de plonger le groupe dans un espace $\mathbb{R}^n$. On doit à chaque étape changer la pondération des graphes. Ce procédé permet de ne plus avoir une structure topologique discrète quand on géométrise les groupes. Après cette première approche utilisée par Gromov, van den Dries, Wilkie et Gromov ont simplifié les arguments en utilisant la théorie des ultrafiltres. Cette manière de voir les choses a fait émerger les cônes asymptotiques d'espaces métriques et donc de groupes dans les années 1990. Ces cônes sont un invariant de groupes à quasi-isométrie près et présentent l'avantage d'être connexes par arcs, localement connexes et complets. Comme la croissance permet l'utilisation d'outils de combinatoire en théorie des groupes, les cônes asymptotiques permettent de faire appel à des outils topologiques et analytiques.

3.2 L'approche de Tao

Dans cette section, nous donnons la démonstration, que Tao propose sur son blog ([Tao10]), du théorème de Gromov. On commence par donner quelques pré-requis théoriques. Ensuite, on se servira de ces pré-requis pour prouver le théorème de Gromov. Les détails de la preuve sont tirés de [DlCM13].

3.2.1 Pré-requis théoriques

On présentera deux notions dans cette sous-section. Elles seront centrales dans la preuve du théorème principal de ce chapitre. Ces concepts sont ceux de fonctions harmoniques, de fonctions lipschitziennes sur un groupe et de norme opérateur. Le but est ici de les définir et d'en donner les propriétés qui seront déterminantes pour la suite.

Définition 3.2.1. Soient G un groupe de finiment engendré, S un système de générateurs de ce groupe et $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$. Les *fonctions harmoniques* (sur (G, S) à valeurs dans $\mathbb{F}$) sont les fonctions $f : G \to \mathbb{F}$ telles que, pour tout $x \in G$,

$$f(x) = \frac{1}{|S|} \sum_{s \in S} f(xs).$$

Remarque 3.2.1. Les fonctions harmoniques munies de l'addition et la multiplication par un scalaire usuelles forment un $\mathbb{F}$-vectoriel. En effet, pour f, g deux fonctions harmoniques sur (G, S) un groupe finiment engendré muni d'un système fini de générateurs et $\lambda \in \mathbb{F}$, on a

$$\begin{aligned}(f + \lambda g)(x) &= f(x) + \lambda g(x) \\ &= \frac{1}{|S|} \sum_{s \in S} f(xs) + \lambda \frac{1}{|S|} \sum_{s \in S} g(xs) \\ &= \frac{1}{|S|} \sum_{s \in S} (f + \lambda g)(xs).\end{aligned}$$

On définit également les deux opérateurs suivants. Ils vont nous permettre de comprendre la dénomination de fonction harmonique.

Définition 3.2.2. Soient G un groupe de finiment engendré, S un système de générateurs fini et $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$. L'*opérateur valeur moyenne* $\mathcal{M}_{G,S} : \mathbb{F}^G \to \mathbb{F}^G$ est défini par

$$\mathcal{M}_{G,S} f(x) = \frac{1}{|S|} \sum_{s \in S} f(xs),$$

pour tout $x \in G$. On définit également le *laplacien* $\Delta_{G,S} = \mathrm{id}_{\mathbb{F}^G} - \mathcal{M}_{G,S}$.

Remarque 3.2.2. Lorsque le contexte est clair, l'indice G, S sera omis dans les notations.

On remarque immédiatement que les fonctions harmoniques sont exactement les f tels que $\Delta_{G,S} f = 0$. Cela justifie que l'on appelle l'opérateur $\Delta_{G,S}$ laplacien. En effet, classiquement, on définit les fonctions harmoniques comme étant les fonctions de laplacien nulle et l'une de leurs propriétés est la propriété de la moyenne [1]. Ici, on définit le laplacien de telle sorte que les fonctions harmoniques sont les fonctions qui satisfont la propriété de la moyenne.

De cette propriété, on déduit le théorème de Liouville.

Théorème 3.2.1 (Théorème de Liouville)**.** *Soient G un groupe finiment engendré, S un système fini symétrique de générateurs et $f : G \to \mathbb{F}$, où $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$. Si f est bornée, alors f est constante.*

Démonstration. Notons M tel que $|f(x)| \leq M$ pour tout $x \in G$ et supposons que $1 \in S$. Pour tout $x \in G$, on a

$$\begin{aligned} |f(x) - f(1)| &= \frac{1}{|S|} \left| \sum_{s \in S} f(xs) - \sum_{s \in S} f(s) \right| \\ &= \dots \\ &= \frac{1}{|S|^n} \left| \sum_{s_1, \dots, s_n \in S} f(xs_1 \dots s_n) - \sum_{s_1, \dots, s_n \in S} f(s_1 \dots s_n) \right| \end{aligned} \tag{3.1}$$

On sait qu'il existe un N tel que $xs_1 \dots s_N = t_1 \dots t_N$ avec $s_j, t_j \in S$ pour tout j. On constate donc que $f(xs_1 \dots s_N s_{N+1} \dots s_n) = f(t_1 \dots t_N s_{N+1} \dots s_n)$ pour tout $s_{N+1}, \dots, s_n \in S$. Donc dans (3.1), ces termes s'annulent.

Au total, cela veut dire que cette somme contient moins de $2|S|^N(|S|-1)^{n-N}$ termes. Comme f est bornée par hypothèse, cela nous donne la majoration suivante :

$$|f(x) - f(1)| \leq 2M \frac{|S|^N}{(|S|-1)^N} \frac{(|S|-1)^n}{|S|^n}.$$

Le membre de droite tend vers 0. On en déduit que, pour tout x, $f(x) = f(1)$. La fonction f est constante comme annoncé. $\square$

Passons maintenant à la définition des fonctions lipschitziennes et des semi-normes lipschitziennes.

Définition 3.2.3. Soient G un groupe de finiment engendré, $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$ et S un système fini de générateurs. Une *fonction lipschitzienne* (sur (G, S) à valeurs dans $\mathbb{F}$) est une fonction $f : G \to \mathbb{F}$ telle qu'il existe une constante positive C donnant l'inégalité

$$|f(x) - f(xs)| \leq C,$$

pour tout $x \in G$ et $s \in S$. On note $\mathrm{Lip}(G, S, \mathbb{F})$ (ou Lip lorsque le contexte est clair) l'ensemble des fonctions lipschitzienne sur (G, S) à valeurs dans $\mathbb{F}$.

1. Une fonction f a la propriété de la moyenne si en tout point a, $f(a)$ vaut la moyenne des points autour de $f(a)$.

Avant de définir une semi-norme sur l'espace des fonctions lipschitziennes, il convient de montrer que c'est un espace vectoriel.

Proposition 3.2.1. *Soient G un groupe de finiment engendré, $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$ et S un système fini de générateurs. L'ensemble* $\mathrm{Lip}(G, S, \mathbb{F})$ *muni de l'addition et a multiplication par scalaire usuels forme un espace vectoriel.*

Démonstration. Soient f, g deux fonctions lipschitziennes et λ un scalaire. On sait qu'il existe $C, D \geq 0$ tels que

$$|f(x) - f(xs)| \leq C \text{ et } |g(x) - g(xs)| \leq D,$$

pour tout $s \in S$. On a alors

$$\begin{aligned} |(f+g)(x) - (f+g)(xs)| &= |f(x) - f(xs) + g(x) - g(xs)| \\ &\leq |f(x) - f(xs)| + |g(x) - g(xs)| \\ &\leq C + D, \end{aligned}$$

pour tout $s \in S$. On a aussi,

$$\begin{aligned} |(\lambda f)(x) - (\lambda f)(xs)| &= |\lambda(f(x) - f(xs))| \\ &\leq |\lambda||f(x) - f(xs)| \\ &\leq |\lambda| C, \end{aligned}$$

pour tout $s \in S$. On a donc bien $f + g, \lambda f \in \mathrm{Lip}$. $\square$

Définition 3.2.4. Si f est lipschitzienne, on définit la *semi-norme lipschitzienne* $\mathrm{LIP}(f)$ comme étant le minimum des constantes C telles que $|f(x) - f(xs)| \leq C$, pour tout $x \in G$ et $s \in S$. De manière équivalente,

$$\mathrm{LIP}(f) = \sup_{x \in G, s \in S} |f(x) - f(xs)|.$$

On vérifie facilement que l'application LIP est une semi-norme, c'est-à-dire que, pour $f, g \in \mathrm{Lip}$ et $c \in \mathbb{F}$,

— $\mathrm{LIP}(f + g) \leq \mathrm{LIP}(f) + \mathrm{LIP}(g)$ (sous-additivité)

— $\mathrm{LIP}(cf) = |c| \,\mathrm{LIP}(f)$ (absolue homogénéité).

Démonstration. Soient $f, g \in \mathrm{Lip}$ et $c \in \mathbb{F}$. L'application est sous-additive, en effet,

$$\begin{aligned} \mathrm{LIP}(f+g) &= \sup_{x \in G, s \in S} |(f+g)(x) - (f+g)(xs)| \\ &\leq \sup_{x \in G, s \in S} |f(x) - f(xs)| + |g(x) - g(xs)| \\ &\leq \sup_{x \in G, s \in S} |f(x) - f(xs)| + \sup_{x \in G, s \in S} |g(x) - g(xs)| \\ &\leq \mathrm{LIP}(f) + \mathrm{LIP}(g). \end{aligned}$$

On a aussi l'absolue homogénéité :

$$\begin{aligned}\mathrm{LIP}(cf) &= \sup_{x\in G, s\in S} |cf(x) - cf(xs)| \\ &= |c| \sup_{x\in G, s\in S} |f(x) - f(xs)| \\ &= |c|\,\mathrm{LIP}(f).\end{aligned}$$

□

De plus, si $\mathrm{LIP}(f) = 0$, alors pour tout $s \in S$, $f(x) = f(xs)$. Comme S est une partie génératrice de G, f est constante. LIP n'est donc pas une norme.

On finit cette section en remarquant que cette définition des fonctions lipschitziennes est consistante avec la définition usuelle. On munit G de la métrique des mots pour le système de générateurs S. Pour $f \in \mathrm{Lip}$, il existe C tel que $|f(x) - f(xs)| \leq C$ pour tout $x \in G, s \in S$. Soient $x, y \in G$ et $n = d(x, y)$. On a donc l'existence de $s_1, ..., s_n \in S$ tels que $xs_1...s_n = y$. On a donc

$$\begin{aligned}|f(x) - f(y)| =&|f(x) - f(xs_1...s_n)| \\ =&|f(x) - f(xs_1) + f(xs_1) - f(xs_1s_2) + f(xs_1s_2) - f(xs_1s_2s_3) \\ &+ ... + f(xs_1...s_{,-1}) - f(xs_1...s_n)| \\ \leq&|f(x) - f(xs_1)| + |f(xs_1) - f(xs_1s_2)| + |f(xs_1s_2) - f(xs_1s_2s_3)| \\ &+ ... + |f(xs_1...s_{,-1}) - f(xs_1...s_n)| \\ \leq&Cn = Cd(x, y).\end{aligned}$$

Réciproquement, s'il existe k tel que $|f(x) - f(y)| = kd(x, y)$ pour tout $x, y \in G$, alors $|f(x) - f(xs)| \leq k$ pour tout $x \in G, s \in S$.

Les fonctions harmoniques et lipschiziennes sont deux espaces vectoriels. On se servira de leur intersection pour prouver le théorème de Gromov.

Définition 3.2.5. Soient $\mathbb{F}$ un champ, G un groupe de type fini et S un système fini de générateurs de G. Les *fonctions lipschitziennes harmoniques* (sur (G, S) à valeurs dans $\mathbb{F}$) sont les fonctions qui sont à la fois lipschiziennes et harmoniques. On les note $\mathcal{H}^{\mathrm{Lip}}(G, S, \mathbb{F})$.

Il nous reste une dernière notion à définir avant de passer à la démonstration : la norme opérateur. Avant de définir celle-ci, rappelons ce qu'est une norme.

Définition 3.2.6. Soit $\mathbb{K}$ un champ. Une *valeur absolue* de $\mathbb{K}$ est une fonction $|\cdot| : \mathbb{K} \to \mathbb{R}^+$ telle que, pour tout $x, y \in \mathbb{K}$,

— $|x| = 0 \Leftrightarrow x = 0$

— $|x + y| \leq |x| + |y|$

— $|xy| = |x||y|$.

Définition 3.2.7. Soit V un $\mathbb{K}$-espace vectoriel, où $\mathbb{K}$ est un champ muni d'une valeur absolue $|\cdot|$. Un *norme* sur V est une fonction $\| \cdot \|\colon V \to \mathbb{R}^+$ telle que, pour tout $k \in \mathbb{K}, v, v' \in V$,

— $\| v \| = 0 \Leftrightarrow v = 0$ (séparation)

— $\| kv \| = |k| \, \| v \|$ (absolue homogénéité)

— $\| v + v' \| \leq \| v \| + \| v' \|$ (inégalité triangulaire).

Définition 3.2.8. Soient V et W des espaces vectoriels normés et $T : V \to W$ une application linéaire. La norme opérateur de T est l'infimum des c tels que, pour tout $v \in V$, $|T(v)| \leq c|v|$. On la note $|T|_{\mathrm{op}}$ et on l'appelle la norme opérateur induite par les normes de V et W.

On vérifie facilement qu'il s'agit bien d'une norme et on se permettra par isomorphisme de parler de la norme d'opérateur d'une matrice.

3.2.2 La preuve

Avant de passer à la preuve du théorème de Gromov à proprement dire, nous devons encore énoncer quatre théorèmes qui serviront à la résolution. Étant de nature assez technique, nous en passerons les démonstrations. [2]

Théorème 3.2.2 (Théorème A). *Soit G un groupe infini de finiment engendré. Il existe une fonction lipschitzienne harmonique non-constante de G dans $\mathbb{C}$.*

Théorème 3.2.3 (Théorème B). *Soient G un groupe infini de finiment engendré à croissance polynomiale et S un système de générateurs fini. L'ensemble de fonctions lipschitziennes harmoniques sur (G, S), $\mathcal{H}^{\mathrm{Lip}}(G, S, \mathbb{C})$ est un $\mathbb{C}$-vectoriel est de dimension finie.*

Théorème 3.2.4 (Théorème C). *Soient $H \leq \mathrm{GL}_n(\mathbb{C})$ et G un sous-groupe de H de finiment engendré à croissance polynomiale. G est virtuellement abélien.*

Théorème 3.2.5 (Théorème D). *Soit G un groupe de finiment engendré à croissance polynomiale de degré maximal d. Supposons que le théorème de Gromov soit vrai pour les groupes à croissance polynomiale de degré moins de $d-1$. Si G contient un sous-groupe G' d'index fini tel qu'il existe un morphisme surjectif de G' sur $\mathbb{Z}$, alors G est virtuellement nilpotent.*

Nous pouvons maintenant combiner ces quatre théorèmes afin d'obtenir une preuve du théorème de Gromov.

Théorème 3.2.6. *Soit G un groupe finiment engendré. On a l'équivalence suivante :*

$$G \text{ est nilpotent } \Leftrightarrow G \text{ est à croissance polynomiale.}$$

2. On peut les trouver dans [Tao10].

Démonstration. Bien entendu, on a déjà montré que les groupes virtuellement nilpotents finiment engendrés sont à croissance polynomiale. On va montrer l'autre sens de l'équivalence.

On procède par récurrence sur le degré d de la fonction de croissance. Le cas $d = 0$ se traite trivialement car, dans ce cas, le groupe est fini et donc virtuellement nilpotent vu la remarque 2.4.1. Supposons que le théorème est vrai pour les groupes de croissance polynomiale au plus $d-1$ et montrons qu'il est alors vrai pour les groupes dont le taux de croissance est majoré par $[n^d]$.

Étant donné que $d > 0$, on sait que G est un groupe infini et donc que $\mathcal{H}^{\mathrm{Lip}}(G, S, \mathbb{C})$ contient une fonction non-triviale (théorème 3.2.2) et qu'il est de dimension finie (théorème 3.2.3). Notons S un ensemble fini symétrique de générateurs de G et $\mathcal{V}$ l'ensemble des fonctions lipschitziennes harmoniques sur (G, S) à valeurs dans $\mathbb{C}$. On définit une action du groupe G sur $\mathcal{V}$, notée $\cdot$, par

$$\gamma \cdot f : G \to \mathbb{C} : x \mapsto f(\gamma^{-1}x),$$

pour tout $\gamma \in G$ et $f \in \mathcal{V}$. On voit immédiatement que cette action est triviale sur $\mathbb{C}$.

Par le théorème 3.2.2, on sait que $\mathbb{C}$ est un sous-espace propre de $\mathcal{V}$. On a donc une action induite sur $\mathcal{W} := \dfrac{\mathcal{V}}{\mathbb{C}}$, on la note Ψ, elle est donnée par :

$$\Psi : G \to \mathrm{GL}(\mathcal{W}) : \gamma \mapsto (f + \mathbb{C} \mapsto \gamma \cdot f + \mathbb{C}).$$

La semi-norme lipschitzienne, LIP sur $\mathcal{V}$ devient une norme sur $\mathcal{W}$, on la note $|\cdot|_{\mathrm{LIP}}$. En effet, puisqu'on quotiente par l'ensemble qui annule LIP, on obtient bien le critère de séparabilité qui permet de conclure. On remarque que l'action Ψ préserve cette norme. En effet, pour tout $\gamma \in G$ et $f \in \mathcal{V}$,

$$\begin{aligned}
|\Psi(\gamma)(f + \mathbb{C})|_{\mathrm{LIP}} &= |\gamma \cdot f + \mathbb{C}\,|_{\mathrm{LIP}} \\
&= \sup_{x \in G, s \in S} |f(\gamma^{-1}x) - f(\gamma^{-1}xs)| \\
&= \sup_{x \in G, s \in S} |f(x) - f(xs)| \qquad\qquad \text{car } x \mapsto \gamma^{-1}x \text{ est bijectif} \\
&= |f + \mathbb{C}\,|_{\mathrm{LIP}}.
\end{aligned}$$

On en tire que si on munit $\mathrm{GL}(\mathcal{W})$ de la norme opérateur induite par la norme lipschitzienne, $|\Psi(\gamma)|_{\mathrm{op}} = 1$ pour tout $\gamma \in G$. Donc, le groupe $G' := \Psi(G)$ est borné. La preuve se sépare à présent en deux cas :

Cas 1 : G' est infini.

On commence par montrer que G' est virtuellement abélien. On sait que l'adhérence de G' est compacte car on a la série d'implications suivante :

$\mathcal{V}$ est de dimension finie.
$\Rightarrow \mathcal{W}$ est de dimension finie.
$\Rightarrow$ GL($\mathcal{W}$) est de dimension finie.
$\Rightarrow$Toutes les normes de GL($\mathcal{W}$) sont équivalentes, voir l'annexe B.
En particulier, la norme opérateur est équivalente à la norme euclidienne.
$\Rightarrow$Les bornés de GL($\mathcal{W}$) ont une adhérence compacte.

On sait donc que G' est le sous-groupe d'un groupe de Lie compact et bien entendu, G' est finiment engendré et à croissance polynomiale. Ainsi, par le théorème 3.2.4, G' est virtuellement abélien.

Soit H' un sous-groupe abélien d'indice fini de G'. Par Lagrange, H' est infini et donc isomorphe à un groupe de la forme $\mathbb{Z}^k \times F$, avec $k \in \mathbb{N}_0$ et F un groupe abélien fini, notons cet isomorphisme φ. Soit H la pré-image de H' sous Ψ, H est d'index fini car $[G : H] \leq [G' : H'] < \infty$. En effet, posons $[G' : H'] = n$ et supposons qu'il existe $x_1, ..., x_{n+1} \in G$ tels que $x_j H \neq x_i H$ pour tout $i \neq j$. Vu le nombre de classes latérales de H', on sait qu'il existe i, j différents tels que $\Psi(x_j)H' = \Psi(x_i)H'$. De plus, on a les équivalences suivantes :

$$\begin{aligned}
&\exists i \neq j \in \{1, ..., n+1\} : \Psi(x_j)H' = \Psi(x_i)H' \\
\Leftrightarrow &\exists h' \in H' : \Psi(x_j) = \Psi(x_i)h' \\
\Leftrightarrow &\Psi(x_i^{-1}x_j) \in H' \\
\Leftrightarrow &x_i^{-1}x_j \in \Psi^{-1}(H') = H \\
\Leftrightarrow &\exists h \in H : x_j = x_i h \\
\Leftrightarrow &x_j H = x_i H.
\end{aligned}$$

C'est un contradiction. Supposer un nombre $\geq n+1$ de classes latérales était absurde.

On pose maintenant π une projection de $\mathbb{Z}^k \times F$ sur $\mathbb{Z}$. On constate alors que $\pi \circ \varphi \circ \Psi : H \to \mathbb{Z}$ est surjectif. On en tire par le théorème 3.2.5 que G est virtuellement nilpotent.

Cas 2 : G' est fini.

On sait, par Lagrange, que $\{\text{id}\}$ est un sous-groupe d'indice fini de G'. On pose $H = \Psi^{-1}(\text{id})$. On a encore $[G : H] \leq [G' : \{\text{id}\}] = |G'| < \infty$. Par définition de H, la restriction de Ψ à H est l'action triviale sur $\mathcal{W}$. Ainsi,

$$\gamma \cdot f + \mathbb{C} = \Psi(\gamma)(f + \mathbb{C}) = f + \mathbb{C},$$

pour tout $\gamma \in H, f \in \mathcal{W}$ et donc $\gamma \cdot f - f \in \mathbb{C}$ pour tout $\gamma \in H, f \in \mathcal{W}$. Pour tout $\gamma \in H$, on définit $L_\gamma \in \mathcal{V}^*$ par

$$L_\gamma(f) = (\gamma \cdot f - f)(1),$$

pour tout $f \in \mathcal{V}$. On peut dès lors définir l'homomorphisme de groupes $L : H \to (\mathcal{V}^*, +) : \gamma \mapsto L_\gamma$. C'est bien un homomorphisme car :

$$\begin{aligned}
L_{\gamma'\gamma}(f) =&(\gamma'\gamma \cdot f - f)(1)\\
=&f(\gamma'\gamma) - f(1)\\
=&f(\gamma'\gamma) - f(\gamma) + f(\gamma) - f(1)\\
=&(\gamma' \cdot f - f)(\gamma) + (\gamma \cdot f - f)(1)\\
=&(\gamma' \cdot f - f)(1) + (\gamma' \cdot f - f)(1) && \text{car } \gamma \cdot f - f \in \mathbb{C}\\
=&L_{\gamma'}(f) + L_\gamma(f),
\end{aligned}$$

pour tout $f \in \mathcal{V}^*$. Comme $(\mathcal{V}^*, +)$ est un groupe abélien, $L(H)$ est abélien. Si $L(H)$ est infini, on peut le projeter sur $\mathbb{Z}$ et conclure.

Il nous reste donc à traiter le cas où $L(H)$ est fini. Par Lagrange, on sait que $\{0\}$ est d'indice fini dans $L(H)$. Ainsi, $K := L^{-1}(0)$ est un sous-groupe d'indice fini de H et donc de G car $[G : K] = [G : H][H : K]$. De plus, pour tout $\gamma \in K, f \in \mathcal{V}$,

$$L_\gamma(f) = (\gamma \cdot f - f)(1) = 0.$$

Or, $\gamma \cdot f - f$ est constant car $\gamma \in K \subset H$, donc $\gamma \cdot f = f$ et K agit trivialement sur $\mathcal{V}$.

Montrons maintenant que tout $f \in \mathcal{V}$ prend un nombre fini de valeurs. Comme $m := [G : K] < \infty$, on peut trouver $\gamma_1, ..., \gamma_m$ tels que $G = \bigsqcup_{j=1}^{m} K\gamma_j$. Pour tout x, il existe un $k \in K$ et un $1 \leq j_0 \leq m$ tels que $x = k\gamma_{j_0}$. On en tire que, pour tout $f \in \mathcal{V}$,

$$f(x) = f(k\gamma_{j_0}) = (k^{-1} \cdot f)(\gamma_{j_0}) = f(\gamma_{j_0})$$

et donc que f prend au plus m valeurs. En particulier, les fonctions de $\mathcal{V}$ sont bornées. Or, le théorème de Liouville 3.2.1 est applicable et donc toutes les fonctions sur (G, S) harmoniques bornées sont constantes. C'est une contradiction vu le théorème 3.2.2. On est donc jamais dans le cas où $L(H)$ est infini. Tous les cas ont été traités, on peut conclure. □

Bien qu'évident, le corollaire suivant est important en cela qu'il montre que des groupes qui sont les mêmes de loin préservent certaines propriétés algébriques.

Corollaire 3.2.1. *Soient G et G' deux groupes finiment engendrés quasi-isométriques. Si G est virtuellement nilpotent, alors G' est virtuellement nilpotent.*

Démonstration. Par le théorème de Gromov, on sait que G est à croissance polynomiale. Comme G et G' sont quasi-isométriques, ils ont le même taux de croissance et donc G' est finiment engendré et à croissance polynomiale. On en tire par le théorème de Gromov que G' est virtuellement nilpotent. □

Chapitre 4

Groupe de Grigorchuk

Dans ce chapitre, on s'intéresse à répondre à la première question de Milnor posée dans [Mil68b], à savoir :

Existe-t-il des groupes à croissance intermédiaire ?

Au moment où Milnor pose cette question, tous les groupes dont on a pu déterminer le taux de croissance sont soit à croissance polynomiale soit à croissance exponentielle. Pendant plus de 15 ans, on n'arrivera ni à prouver que tous les groupes intermédiaires n'existent pas ni à mettre en évidence un tel groupe. C'est en 1980 que Rotislav Grigorchuk crée le groupe $\mathcal{G}$, appelé après groupe de Grigorchuk, comme exemple d'un groupe infini finiment engendré de torsion. Ces groupes ont été étudiés dans le cadre du *problème de Burnside général*[1]. Plus tard, en 1984 dans [Gri85], il prouve que ce groupe est à croissance intermédiaire.

Dans ce chapitre, nous nous occuperons de le construire et de démontrer qu'il est à croissance intermédiaire. Le document de référence à ce sujet est [GP08] co-écrit par Igor Pak et Rotislav Grigorchuk lui-même. On commence par une section de définitions et résultats généraux qui seront utilisés plus tard dans le chapitre. Ensuite, on définit le groupe de Grigorchuk et on finit par montrer qu'il est à croissance intermédiaire.

4.1 Outils

On développe ici des outils qui seront utilisés dans les sections suivantes. On commence par deux lemmes techniques qui permettront d'établir la croissance intermédiaire du groupe de Grigorchuk. On définit ensuite les groupes multilatéraux et on majore leur croissance. On poursuit par la définition des produits semi-directs et des produits en couronne. On termine par une discussion sur l'arbre binaire et ses automorphismes.

1. Une introduction au problème de Burnside ainsi qu'une preuve que le groupe de Grigorchuk en est un exemple sont proposés dans l'annexe C.

4.1.1 Deux lemmes d'analyse

Lemme 4.1.1 (Lower Bound Lemma). *Soit $f : \mathbb{N} \to \mathbb{R}^+ : n \mapsto f(n)$ une fonction strictement croissante qui tend vers l'infini lorsque n tend vers l'infini. S'il existe $m > 1$ tel que $f^m \preceq f$, alors il existe $\alpha > 0$ tel que* $\exp(\cdot^\alpha) \preceq f$.

Démonstration. Nous allons montrer que le résultat est vrai pour la fonction $\mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto f(\lceil x \rceil)$. Par un léger abus de notation, nous la noterons f également. On se fixe un $n \in \mathbb{N}_0$ et on pose $\pi(n) = \ln(f(n))$. Par hypothèse, on sait qu'il existe $C, \alpha > 0$ tels que $f(n) \geq C(f(\alpha n))^m$. On en tire que

$$\pi(n) \geq c + m\pi(\alpha n),$$

où $c = \ln(C)$. En itérant k fois, on obtient :

$$\pi(n) \geq m^k \pi(\alpha^k n) + c(1 + m + ... + m^{k-1}) \geq m^k(\pi(\alpha^k n) + c).$$

Comme $f(n)$ tend vers l'infini, $\pi(n)$ également et donc il existe N tel que, pour $n \geq N$, on a $\pi(\alpha^k n) + c \geq 1$. Pour un tel n, on a

$$\pi(n) \geq m^k.$$

Or, pour $k = \left\lceil \log_\alpha \left(\frac{e}{n}\right) \right\rceil$, on a

$$\begin{aligned} m^k &\geq m^{\log_\alpha\left(\frac{e}{n}\right)} \\ &= \left(m^{1-\ln(n)}\right)^{\frac{1}{\ln(\alpha)}} \\ &= \left(m m^{-\ln(n)}\right)^{\frac{1}{\ln(\alpha)}} \\ &= \left(m n^{-\ln(m)}\right)^{\frac{1}{\ln(\alpha)}} \\ &= m^{\frac{1}{\ln(\alpha)}} n^{\frac{-\ln(m)}{\ln(\alpha)}}. \end{aligned}$$

Remarquons que la constante $\nu = \dfrac{-\ln(m)}{\ln(\alpha)}$ est positive car $\alpha < 1$. En effet, on peut procéder par l'absurde et supposer que $\alpha \geq 1$. On a alors

$$\begin{aligned} m\pi(\alpha n) - \pi(n) &> m\pi(n) + \pi(n) \\ &= (m-1)\pi(n) \\ &\to +\infty && \text{quand } n \to +\infty. \end{aligned}$$

C'est absurde car $-c \geq m\pi(\alpha n) - \pi(n)$.

Pour $A > 0$ suffisamment proche de zéro (i.e : plus petit que $m^{\frac{1}{\ln(\alpha)}}$ et tel que, pour tout $0 < n < N$, $\pi(n) \geq An^{\frac{-\ln(m)}{\ln(\alpha)}}$). C'est ce qu'il fallait démontrer. $\square$

Définition 4.1.1. Soient $f : \mathbb{R}^+ \to \mathbb{R}^+$ une fonction strictement croissante et $k \in \mathbb{N}$. On pose, pour tout $n \in \mathbb{N}$,

$$f^{\star k}(n) = \sum_{(n_1,\ldots,n_k)\in D_n} f(n_1)\ldots f(n_k),$$

où $D_n = \{(n_1, \ldots, n_k) \in \mathbb{N}^k \,|n_1 + \ldots + n_k \leq n\}$

Lemme 4.1.2 (Upper Bound Lemma)**.** *Soit $f : \mathbb{R}^+ \to \mathbb{R}^+ : n \mapsto f(n)$ une fonction strictement croissante qui tend vers l'infini lorsque n tend vers l'infini. S'il existe $k \in \{2, 3, \ldots\}, C > 0$ et $\alpha \in]0, 1[$ tels que $f(n) \leq Cf^{\star k}(\alpha n)$ pour tout $n \in \mathbb{N}_0$, alors il existe un $\beta < 1$ tel que $f \preceq \exp(\cdot^{\beta})$.*

Démonstration. Commençons par définir $\nu < 1$ une constante telle que $k\dfrac{\alpha^\nu}{k^\nu} < 1$. Une telle constante existe car $\lim\limits_{\nu\to 1^-} c^\nu = c$ pour toute constante c. Donc,

$$\lim_{\nu\to 1} k\frac{\alpha^\nu}{k^\nu} = \alpha < 1.$$

Posons $\varepsilon > 0$ tel que $k\dfrac{\alpha^\nu}{k^\nu} = 1 - \varepsilon$. Remarquons que, pour un n suffisamment grand, on a par le théorème des valeurs comparées :

$$\ln C + k \ln n \leq \varepsilon n^\nu$$

et donc pour A suffisamment grand,

$$\ln C + k \ln n \leq \varepsilon A n^\nu, \tag{4.1}$$

pour tout $n \in \mathbb{N}_0$.

Cette inéquation nous sera utile dans l'induction qui nous permettra de montrer que, pour tout $n \in \mathbb{N}_0$, il existe $M > 0, N < 1$ tels que

$$\ln(f(n)) \leq Mn^N.$$

Lorsque $n = 1$, on peut prendre $M = \sup\{A, f(1)\}$ et $N = \nu$. Supposons maintenant que, pour tout $m < n$, on ait $\ln(f(n)) \leq Mm^N$.

On a

$$\begin{aligned} f(n) &\leq Cf^{\star k}(\alpha n) \\ &\leq C \sum_{(n_1,\ldots,n_k)\in D_n} f(n_1)\ldots f(n_k) \\ &\leq C|D_n| \sup_{(n_1,\ldots,n_k)\in D_n} (f(n_1)\ldots f(n_k))\,. \end{aligned}$$

Or,

$$\begin{aligned}
\ln(f(n_1)...f(n_k)) &\leq \pi(n_1) + ... + \pi(n_k) \\
&\leq M(n_1^N + ... + n_k^N) \\
&\leq M\frac{k}{k}(\alpha n)^N \\
&\leq Mk(\frac{\alpha n}{k})^N && \text{car } N < 1 \text{ et } k > 1 \\
&\leq Mn^N(1-\varepsilon)
\end{aligned}$$

et

$$|D_n| \leq (\lfloor \alpha n \rfloor)^k \leq (\alpha n)^k.$$

Au total, $f(n) \leq C(\alpha n)^k \exp(Mn^N(1-\varepsilon))$ et donc

$$\begin{aligned}
\pi(n) &\leq \ln\left(C(\alpha n)^k \exp(Mn^N(1-\varepsilon))\right) \\
&\leq \ln C + k \ln n - \varepsilon M n^N + M n^N + k \ln \alpha \\
&\leq M n^N && \text{car } \alpha < 1 \text{ et } (4.1)
\end{aligned}$$

Ceci conclut l'induction. Pour conclure, il nous suffit d'appliquer exp et on obtient

$$f(n) \leq \exp(Mn^N),$$

pour tout $n \in \mathbb{N}_0$. □

4.1.2 Groupes multilatéraux

Commençons par définir la relation de commensurabilité de groupes. Elle nous sera utile pour définir les groupes multilatéraux.

Définition 4.1.2. Soient G_1, G_2 deux groupes. Ils sont dits *commensurables* s'il existe $H_1 \leq G_1$ et $H_2 \leq G_2$ tels que

$$H_1 \cong H_2 \text{ et } [G_1, H_1], [G_2, H_2] < \infty.$$

On note $G_1 \simeq G_2$.

De la définition, on a immédiatement les deux propositions suivantes.

Proposition 4.1.1. *Soit G un groupe, on a*

- *$G \simeq G'$ pour tout G' isomorphe à G*
- *$G \simeq H$ pour tout H sous-groupe d'indice fini de G*

Proposition 4.1.2. *Deux groupes commensurables ont le même taux de croissance.*

Démonstration. Puisque ce sont des sous-groupes d'indice fini, les groupes G_1 et H_1 sont quasi-isométriques et les groupes H_2 et G_2 aussi. De plus, comme ils sont isomorphes, H_1 et H_2 sont quasi-isométriques. Au total, par transitivité de la quasi-isométrie, G_1 et G_2 sont quasi-isométriques or des groupes quasi-isométriques ont le même taux de croissance (voir la proposition 1.2.2). On peut conclure. □

On se sert de cette proposition pour majorer la croissance des groupes multilatéraux.

Définition 4.1.3. Un groupe G est dit *multilatéral* s'il est infini et s'il existe un $m \geq 2$ tel que $G \simeq G^m$.

Proposition 4.1.3. *Tous les groupes multilatéraux finiment engendrés ont une croissance superpolynomiale. De plus, pour un G multilatéral tel que $G \cong G^m$,*

$$\gamma_G \preceq \exp(\cdot^{\alpha}),$$

où $\alpha > 0$.

Démonstration. Par la proposition 4.1.2, pour γ_G une fonction de croissance de G, $\gamma_G \approx \gamma_{G^m}$. Ainsi, vu la proposition 1.2.6, on a

$$\gamma_{G^m} \approx \gamma_G^m \preceq \gamma_G.$$

Comme G est infini par définition, on peut appliquer le *Lower Bound Lemma* 4.1.1 à γ_G. On en tire que $\gamma_G \succeq \exp(\cdot^{\alpha})$, où $\alpha > 0$. □

4.1.3 Produit semi-direct et produit en couronne

On définit ici les produits semi-directs et une version restreinte des produits en couronne. Ces deux constructions sont importantes en théorie des groupes indépendamment de la croissance des groupes.

Définition 4.1.4. Soient K, L des groupes et $\phi : L \to \mathrm{Aut}(K)$ un morphisme (en d'autres termes, L agit sur K). On définit le *produit semi-direct* de K par L induit par ϕ comme étant le groupe $K \rtimes_\phi L := (K \times L, *)$, où

$$(k_1, l_1) * (k_2, l_2) = (k_1\phi(l_1)(k_2), l_1l_2),$$

pour tout $k_1, k_2 \in K$ et $l_1, l_2 \in L$. Lorsque le contexte est clair, on se contentera de noter $K \rtimes L$.

On vérifie facilement que le produit semi-direct $K \rtimes_\phi L$ défini ci-dessus est bien un groupe.

Démonstration. L'opération $*$ est interne. L'élément $(1_K, 1_L)$ est neutre pour $*$ car $\phi(1_L) = \mathrm{id}_K$. On a l'associativité : soient $k_1, k_2, k_3 \in K$ et $l_1, l_2, l_3 \in L$, on a

$$\begin{aligned}((k_1, l_1) * (k_2, l_2)) * (k_3, l_3) &= (k_1\phi(l_1)(k_2), l_1l_2) * (k_3, l_3) \\ &= (k_1\phi(l_1)(k_2)\phi(l_1l_2)(k_3), l_1l_2l_3) \\ &= (k_1\phi(l_1)(k_2)\phi(l_1)(\phi(l_2)(k_3)), l_1l_2l_3) \\ &= (k_1\phi(l_1)(k_2\phi(l_2)(k_3)), l_1l_2l_3) \\ &= (k_1, l_1) * (k_2\phi(l_2)(k_3), l_2l_3) \\ &= (k_1, l_1) * ((k_2, l_2) * (k_3, l_3)).\end{aligned}$$

Cherchons maintenant un inverse pour $(k, l) \in K \times L$. L'élément $(\phi(l^{-1})(k^{-1}), l^{-1})$ est le seul inverse à droite. C'est donc le seul candidat pour être l'inverse de (k, l). Il est aussi inverse à gauche car :

$$\begin{aligned}(\phi(l^{-1})(k^{-1}), l^{-1}) * (k, l) &= (\phi(l^{-1})(k^{-1})\phi(l^{-1})(k), l^{-1}l) \\ &= (\phi(l^{-1})(k^{-1}k), l^{-1}l) = (1_K, 1_L).\end{aligned}$$

□

On remarque aussi que l'on peut généraliser les plongements mentionnés à la définition 1.2.3. Les morphismes

$$\begin{aligned}K \hookrightarrow K \rtimes_\varphi L : k \mapsto (k, 1) \\ \text{et } L \hookrightarrow K \rtimes_\varphi L : l \mapsto (1, l)\end{aligned}$$

sont des plongements de K et L dans $K \rtimes_\varphi L$.

Remarque 4.1.1. Il est clair que, pour deux groupes G, G' tels que $\psi : G \to G'$ est un isomorphisme, si $G \rtimes_\varphi H$ existe, il est isomorphe à $G' \rtimes_\theta H$, où $\theta : H \to \mathrm{Aut}(G') : g' \mapsto \psi^{-1}(\varphi(\psi(g')))$.

Voyons sur un exemple de groupes usuels ce que fait ce produit semi-direct.

Exemple 4.1.1. Un exemple d'un tel groupe est donné par l'holomorphe d'un groupe rencontré à la définition 1.2.3. On peut aussi considérer un exemple plus concret en regardant $G := \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$, où

$$\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n) : \begin{cases} 0_2 \mapsto \mathrm{id}_{\mathbb{Z}_n} \\ 1_2 \mapsto \cdot^{-1}. \end{cases}$$

Ce groupe est engendré par $r := (1_n, 0_2)$ et $s := (0_n, 1_2)$. En effet, on voit facilement que $\mathbb{Z}_n \times 0 = \langle (1_n, 0_2) \rangle$ et que $0 \times \mathbb{Z}_2 = \langle (0_n, 1_2) \rangle$. On voit aussi que pour générer un $(a, 1_2)$

quelconque, il suffit de voir que $(a, 0_2) * (0_n, 1_2) = (a, 1_2)$. Que peut-on dire de plus sur G ? On remarque qu'on a les relations suivantes :

$$\begin{aligned}
r^n &= (0_n, 0_2),\\
s^2 &= (0_n, 0_2) \text{ et}\\
srs &= (0_n, 1_2) * (1_n, 0_2) * (0_n, 1_2)\\
&= (0_n\phi(1_2)(1_n), 1_2 + 0_2) * (0_n, 1_2) = (0_n - 1_n, 1_2) * (0_n, 1_2)\\
&= (-1_n + \phi(1_2)(0_n), 1_2 + 1_2) = (-1_n - 0_n, 0_2)\\
&= r^{-1}.
\end{aligned}$$

On en tire que $G = \langle r, s | r^n = 1 = s^2 \text{ et } srs = r^{-1}\rangle$ et donc que G est le groupe diédral d'ordre $2n$.

Le produit semi-direct nous sert, ici, d'une part, à construire l'exemple d'un groupe finiment engendré dont un sous-groupe n'est pas finiment engendré et, d'autre part, à définir le produit en couronne. Notons tout de même que le produit en couronne que nous présenterons ici en est une version restreinte. On peut les définir dans un contexte plus général.

Définition 4.1.5. Soit G un groupe, on définit le *produit en couronne* de G par $\mathbb{Z}_2$ est le produit semi-direct $(G \times G) \rtimes_\phi \mathbb{Z}_2$, où $\phi(0) = \mathrm{id}_{G\times G}$ et $\phi(1) = ((g, h) \mapsto (h, g))$. On note cette construction $G \wr \mathbb{Z}_2$.

4.1.4 Arbre binaire

Le groupe de Grigorchuk que l'on s'apprête à définir est un sous-groupe du groupes des automorphismes de l'arbre binaire. Il convient donc de poser des bases solides pour le comprendre.

Définition 4.1.6. On définit l'*arbre binaire infini complet* [2] $\mathbf{T}$ comme étant le graphe orienté qui a pour sommets $\mathcal{V}(\mathbf{T}) = \{0, 1\}^*$ et pour arêtes, $\mathcal{E}(\mathbf{T}) = \{(u, v) \in S^2 | v = ua, a \in \{0, 1\}\}$. Il est représenté à la Figure 4.1. Soit v un sommet de $\mathbf{T}$, on appelle $|v|$ l'*étage* de v. Le n^{e} étage de $\mathbf{T}$ est l'ensemble des sommets v de $\mathbf{T}$ tels que $|v| = n$.

Pour $v \in \{0, 1\}^*$, on pose $\mathbf{T}_v$ le sous-graphe orienté de $\mathbf{T}$ donné par les sommets $\mathcal{V}(\mathbf{T}_v) = v\{0, 1\}^*$ et les arêtes $\mathcal{E}(\mathbf{T}_v) = \mathcal{E}(\mathbf{T}) \cap (v\{0, 1\}^* \times v\{0, 1\}^*)$.

Remarque 4.1.2. L'arbre binaire $\mathbf{T}$ est égal à $\mathbf{T}_\varepsilon$.

Remarque 4.1.3. Pour tout $v, u \in \{0, 1\}^*$, on a $\mathbf{T}_v$ isomorphe à $\mathbf{T}_u$. l'isomorphisme est $\varphi : \mathcal{V}(\mathbf{T}_v) \to \mathcal{V}(\mathbf{T}_u) : vw \mapsto uw$.

On notera $\mathrm{Aut}(\mathbf{T})$ le *groupe des automorphismes de* $\mathbf{T}$. Pour rappel, ce sont les bijections τ de $\mathcal{V}(\mathbf{T})$ dans lui-même telles que si $(u, v) \in \mathcal{E}(\mathbf{T})$, alors $(\tau(u), \tau(v)) \in \mathcal{E}(\mathbf{T})$ munies de l'opération de composition usuelle.

Un type d'automorphismes nous sera particulièrement utile.

2. On s'autorisera dans ce mémoire le raccourci de l'appeler simplement l'arbre binaire.

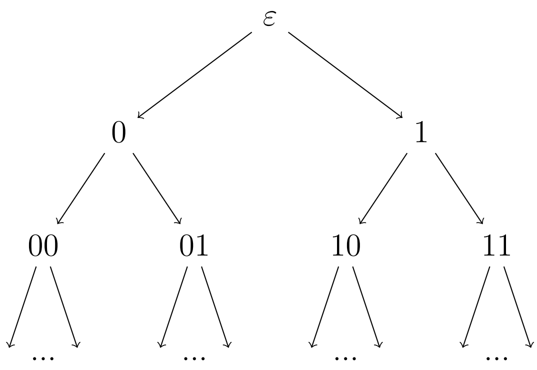


FIGURE 4.1 – Arbre binaire.

Définition 4.1.7. Pour tout $v \in \{0,1\}^*$, on définit $a_v \in \mathrm{Aut}(\mathbf{T})$ par

$$a_v : \mathcal{V}(\mathbf{T}) \to \mathcal{V}(\mathbf{T}) : w \mapsto \begin{cases} w & \text{si } v0, v1 \notin \mathrm{Pref}(w) \\ v1w' & \text{si } w = v0w' \\ v0w' & \text{si } w = v1w'. \end{cases}$$

L'image d'un tel automorphisme est représenté à la Figure 4.2.

Remarque 4.1.4. On remarque immédiatement que, pour tout $v \in \{0,1\}^*$, $a_v \circ a_v = \mathrm{id}$.

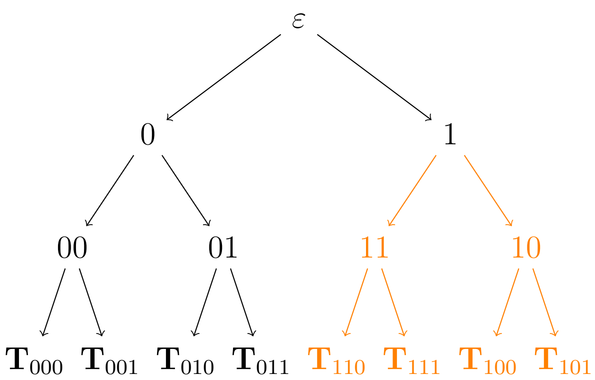


FIGURE 4.2 – Image de $\mathbf{T}$ par a_1.

La proposition suivante nous permet de mieux comprendre les automorphismes et la manière dont ils peuvent ou non transformer l'arbre binaire.

Proposition 4.1.4. *Soit $\tau \in \mathrm{Aut}(\mathbf{T})$. On a $\tau(\varepsilon) = \varepsilon$. Plus généralement, τ préserve les étages.*

Démonstration. Supposons qu'il existe v différent de ε tel que $\tau(v) = \varepsilon$. Dans ce cas, il existe $u \in \mathcal{V}(\mathbf{T})$ et $w \in \mathcal{V}(\mathbf{T}) \setminus \{\varepsilon\}$ tels que $\tau(u) = w$ et $v = u0$ ou $u1$. Par définition de τ, on a alors $(\tau(u), \varepsilon) \in \mathcal{E}(\mathbf{T})$. C'est absurde car ε est de degré entrant 0.

Pour la deuxième partie, soit $u = a_1...a_m$. On sait que

$$[(\tau(\varepsilon), \tau(a_1)), (\tau(a_1), \tau(a_1a_2)), ..., (\tau(a_1...a_{m-1}), \tau(a_1...a_m))]$$

est un chemin de ε à $\tau(u)$ et donc que $|\tau(u)| = m = |u|$. □

On définit également des sous-groupes privilégiés de $\mathrm{Aut}(\mathbf{T})$ qui n'en transforment qu'un sous-arbre.

Définition 4.1.8. On définit $\mathrm{Aut}(\mathbf{T}_v)$ le sous-groupe de $\mathrm{Aut}(\mathbf{T})$ dont les éléments sont les $a \in \mathrm{Aut}(\mathbf{T})$ tels que $a(w) = w$ pour tout $w \in \mathcal{V}(\mathbf{T})$ tel que $v \notin \mathrm{Pref}(w)$.

Ces automorphismes peuvent être vus comme des copies du groupe $\mathrm{Aut}(\mathbf{T})$.

Proposition 4.1.5. *Soit $v \in \mathcal{V}(\mathbf{T})$. Il existe un isomorphisme $\iota_v : \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}_v)$.*

Démonstration. Soit $a \in \mathrm{Aut}(\mathbf{T})$, on définit $\iota_v(a)$ par

$$\iota_v(a)(w) = \begin{cases} w & \text{si } v0, v1 \notin \mathrm{Pref}(w) \\ va(w') & \text{si } w = vw'. \end{cases}$$

Il est clair que c'est un isomorphisme de groupes, l'inverse étant donné par

$$\iota_v^{-1}(a)(w) = a(vw)_{[|v|+1, |a(vw)|]},$$

pour tout $a \in \mathrm{Aut}(\mathbf{T}_v)$. □

Une autre manière de voir les automorphismes est de les caractériser en chaque sommet par l'échange ou non des arêtes sortantes.

Définition 4.1.9. Pour chaque automorphisme τ de $\mathbf{T}$, on voit facilement que

$$\tau(v0), \tau(v1) \in \{\tau(v)0, \tau(v)1\}$$

et sont différents pour tout $v \in \mathcal{V}(\mathbf{T})$. Dès lors, on peut définir la *signature* de τ en v par

$$\epsilon_v(\tau) = \begin{cases} 0 & \text{si } \tau(v0) = \tau(v)0 \\ 1 & \text{si } \tau(v0) = \tau(v)1. \end{cases}$$

En des termes plus intuitifs, la signature en v de τ est nulle si l'enfant de gauche de v devient l'enfant de gauche de $\tau(v)$ et elle vaut 1 si l'enfant de gauche devient l'enfant de droite.

Proposition 4.1.6. *Il y a un bijection entre* $\mathrm{Aut}(\mathbf{T})$ *et l'ensemble des familles de la forme* $\{\epsilon_v\}_{v \in \mathcal{V}(\mathbf{T})}$*, où* $\epsilon_v \in \{0, 1\}$*.*

Démonstration. Cette bijection est donnée par l'application

$$\varphi : \tau \mapsto \{\epsilon_v(\tau)\}_{v \in S}.$$

L'inverse est donné par $\psi : \{\epsilon_v\}_{v \in S} \mapsto \tau$, où

$$\begin{aligned} \tau(\varepsilon) &= \varepsilon, \\ \tau(v0) &= \begin{cases} \tau(v)0 & \text{si } \epsilon_v = 0 \\ \tau(v)1 & \text{sinon} \end{cases} \quad \text{et} \\ \tau(v1) &= \begin{cases} \tau(v)1 & \text{si } \epsilon_v = 0 \\ \tau(v)0 & \text{sinon .} \end{cases} \end{aligned}$$

Il est clair que ψ est à valeurs dans $\mathrm{Aut}(\mathbf{T})$. Vu la définition de la signature, il est clair également que φ et ψ sont inverses l'un de l'autre. □

Cette bijection nous donne gratuitement la proposition suivante qui ne nous sera pas utile directement mais donne des propriétés fondamentales de $\mathrm{Aut}(\mathbf{T})$.

Corollaire 4.1.1. *Le groupe* $\mathrm{Aut}(\mathbf{T})$ *est indénombrable et ne peut être finiment engendré.*

Un outil essentiel pour étudier les automorphismes de l'arbre est de pouvoir appliquer un automorphisme différent au sous-arbre $\mathbf{T}_0$ et au sous-arbre $\mathbf{T}_1$.

Définition 4.1.10. On peut à partir de deux automorphismes τ_0, τ_1 de $\mathbf{T}$ définir un nouvel automorphisme τ grâce à l'application :

$$\varphi : \mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T}) \to \mathrm{Aut}(\mathbf{T}) : (\tau_0, \tau_1) \mapsto \iota_0(\tau_0) \circ \iota_1(\tau_1).$$

Cette définition est raisonnable puisque $\iota_0(\tau_0) \in \mathrm{Aut}(\mathbf{T}_0)$, $\iota_1(\tau_1) \in \mathrm{Aut}(\mathbf{T}_1)$ et $\mathbf{T}_0, \mathbf{T}_1$ sont disjoints, c'est-à-dire que le domaine de l'un est disjoint du domaine et de l'image de l'autre. Dans ce cas de figure, on s'autorisera à écrire la composition $\cdot$ ou à omettre de l'indiquer pour alléger les notations. Visuellement, cela revient à transformer le sous-arbre de gauche selon τ_0 et celui de droite selon τ_1. On a représenté un tel automorphisme à la Figure 4.3.

Cette dernière proposition nous permet de décomposer les automorphismes de $\mathbf{T}$ en un automorphisme sur $\mathbf{T}_0$ et un automorphisme sur $\mathbf{T}_1$, nous devons toutefois être précautionneux et garder en mémoire ce que l'automorphisme fait aux sommets 1 et 0. L'outil idéal pour faire cela est le produit en couronne. En effet, il garde en mémoire ce qu'il faut faire aux deux premiers sommets et tient compte du nombre de transformations encore à effectuer sur 0 et 1 leurs deux sous-arbres.

Proposition 4.1.7. *Les groupes* $\mathrm{Aut}(\mathbf{T})$ *et* $\mathrm{Aut}(\mathbf{T}) \wr \mathbb{Z}_2$ *sont isomorphes.*

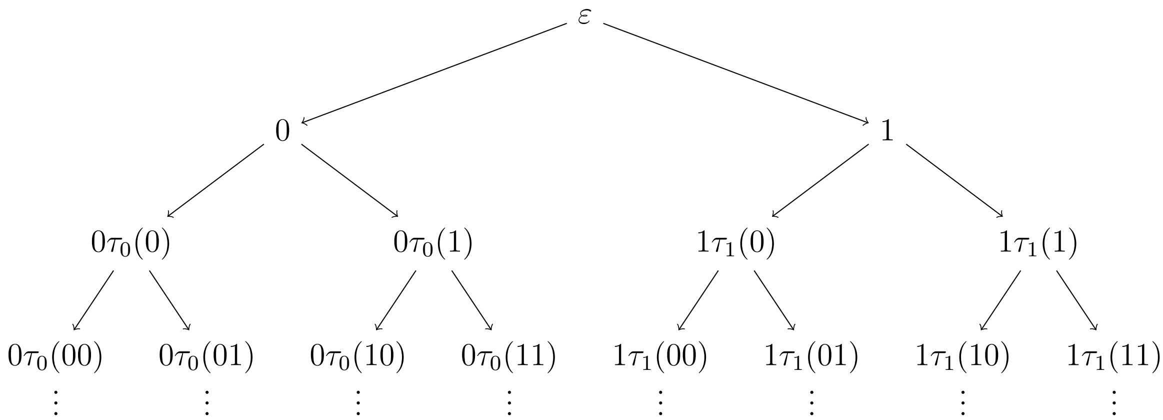


FIGURE 4.3 – Image de $\mathbf{T}$ par $\varphi(\tau_0, \tau_1)$.

Démonstration. L'isomorphisme que nous allons utiliser est une extension de φ défini ci-dessus. On pose

$$\varphi : \mathrm{Aut}(\mathbf{T}) \wr \mathbb{Z}_2 \to \mathrm{Aut}(\mathbf{T}) : (\tau_0, \tau_1, \sigma) \mapsto \begin{cases} \varphi(\tau_0, \tau_1) & \text{si } \sigma = 0 \\ \varphi(\tau_0, \tau_1) \circ a_\varepsilon & \text{si } \sigma = 1. \end{cases}$$

Montrons que c'est un isomorphisme de groupes.

Morphisme : Prenons $(\tau_0, \tau_1, \sigma), (\rho_0, \rho_1, \delta) \in \mathrm{Aut}(\mathbf{T}) \wr \mathbb{Z}_2$. On a

$$\begin{aligned}
\varphi((\tau_0, \tau_1, \sigma) * (\rho_0, \rho_1, \delta)) &= \varphi((\tau_0, \tau_1)\phi(\sigma)(\rho_0, \rho_1), \sigma + \delta) \\
&= \begin{cases} \varphi(\tau_0 \circ \rho_0, \tau_1 \circ \rho_1, \sigma + \delta) & \text{si } \sigma = 0 \\ \varphi(\tau_0 \circ \rho_1, \tau_1 \circ \rho_0, \sigma + \delta) & \text{si } \sigma = 1 \end{cases} \\
&= \begin{cases} \varphi(\tau_0 \circ \rho_0, \tau_1 \circ \rho_1) & \text{si } \sigma = 0 \text{ et } \delta = 0 \\ \varphi(\tau_0 \circ \rho_0, \tau_1 \circ \rho_1) \circ a_\varepsilon & \text{si } \sigma = 0 \text{ et } \delta = 1 \\ \varphi(\tau_0 \circ \rho_1, \tau_1 \circ \rho_0) \circ a_\varepsilon & \text{si } \sigma = 1 \text{ et } \delta = 0 \\ \varphi(\tau_0 \circ \rho_1, \tau_1 \circ \rho_0) & \text{si } \sigma = 1 \text{ et } \delta = 1 \end{cases} \\
&= \begin{cases} \varphi(\tau_0, \tau_1) \circ \varphi(\rho_0, \rho_1) & \text{si } \sigma = 0 \text{ et } \delta = 0 \\ \varphi(\tau_0, \tau_1) \circ (\varphi(\rho_0, \rho_1) \circ a_\varepsilon) & \text{si } \sigma = 0 \text{ et } \delta = 1 \\ (\varphi(\tau_0, \tau_1) \circ a_\varepsilon) \circ \varphi(\rho_0, \rho_1) & \text{si } \sigma = 1 \text{ et } \delta = 0 \\ (\varphi(\tau_0, \tau_1) \circ a_\varepsilon) \circ (\varphi(\rho_0, \rho_1) \circ a_\varepsilon) & \text{si } \sigma = 1 \text{ et } \delta = 1 \end{cases} \\
&= \varphi(\tau_0, \tau_1, \sigma) \circ \varphi(\rho_0, \rho_1, \delta).
\end{aligned}$$

Bijection : Commençons par montrer la surjectivité. Soit τ un élément quelconque de $\mathrm{Aut}(\mathbf{T})$. Vu que les automorphismes préservent les étages, il y a deux cas possibles :

<u>Cas 1 : $\tau(0) = 0$</u>

Dans ce cas, on a $\tau(1) = 1$ et on pose $\sigma = 0$. Étudions l'application

$$\tau_0 : \mathbf{T} \to \mathbf{T} : v \mapsto \begin{cases} v & \text{si } v \notin 0\{0,1\}^+ \\ \tau(v) & \text{si } v \in 0\{0,1\}^+. \end{cases}$$

Les sommets de $\mathbf{T}_0$ sont envoyés sur des sommets de $\mathbf{T}_0$. En effet, supposons qu'il existe $0u$ tel que $\tau_0(0u) \in \mathcal{V}(\mathbf{T}_1)$. On pourrait de proche en proche affirmer que tous les ancêtres de $0u$ sont à image dans $\mathbf{T}_1$. Or, 0 est un ancêtre de $0u$ et il n'est pas à image dans $\mathbf{T}_1$. On en tire que $\tau_0 \in \mathrm{Aut}(\mathbf{T}_0)$.

De la même manière,

$$\tau_1 : \mathbf{T} \to \mathbf{T} : v \mapsto \begin{cases} v & \text{si } v \notin 1\{0,1\}^+ \\ \tau(v) & \text{si } v \in 1\{0,1\}^+. \end{cases}$$

est un élément de $\mathrm{Aut}(\mathbf{T}_1)$.

Au total, en appliquant $\varphi(\tau_0, \tau_1, \sigma)$, on obtient τ.

<u>Cas 2 : $\tau(0) = 1$</u>

Dans ce cas, on a $\tau(1) = 0$ et on pose $\sigma = 1$. Étudions l'application

$$\tau_0 : \mathbf{T} \to \mathbf{T} : \begin{cases} \varepsilon \mapsto \varepsilon \\ 0v \mapsto \tau(1v) \\ 1v \mapsto 1v. \end{cases}$$

Par les mêmes arguments que précédemment, $\tau_0 \in \mathrm{Aut}(\mathbf{T}_0)$. De la même manière, on peut construire τ_1 qui va singer τ sur la partie gauche (i.e : $\mathbf{T}_1$ puisqu'on a échangé 0 et 1) de l'arbre binaire.

Au total, on a encore $\varphi(\tau_0, \tau_1, \sigma) = \tau$.

L'injectivité suit puisque nous remarquons que lorsqu'on fixe un τ, le choix de (τ_0, τ_1, σ) est fixé. $\square$

Notation 4.1.1. L'inverse de l'isomorphisme φ défini ci-dessus sera utilisé dans la suite de ce chapitre, il convient donc de lui attribuer une notation propre : ψ.

La définition suivante ainsi que les deux propositions qui suivent peuvent sembler arbitraires mais elles seront utilisées dans la suite. Conceptuellement, on définit les automorphismes qui ne font qu'échanger les premiers sommets de l'arbre mais ne touchent pas aux étages les plus bas. On formalise ce principe et on en donne deux propriétés.

Définition 4.1.11. Soit $m \in \mathbb{N}$, on note A_m le sous-groupe de $\mathrm{Aut}(\mathbf{T})$ dont les éléments τ sont tels que $\epsilon_v(\tau) = 0$ pour tout v de longueur $\geq m$.

Proposition 4.1.8. *Pour tout $m \in \mathbb{N}$, $|A_m| = 2^{2^m - 1}$.*

Démonstration. Il s'agit d'un problème de dénombrement. On sait que jusqu'à l'étage $m-1$, il y a $2^m - 1$ sommets. En effet, un étage n comporte 2^n sommets et

$$\sum_{j=0}^{m-1} 2^j = 2^m - 1.$$

Pour chaque $v \in V$ tel que $|v| < m$, on doit déterminer si $\epsilon_v = 0$ ou 1. Cela nous donne 2^{2^m-1} suites $(\epsilon_v)_{|v|<m}$ possibles or ces suites sont en bijection avec A_m vu le proposition 4.1.6. La conclusion suit. □

Proposition 4.1.9. *On a*

$$A_m \cong \mathbb{Z}_2 \wr \mathbb{Z}_2 \wr \ldots \wr \mathbb{Z}_2 \ \ (m \text{ fois}).$$

Démonstration. On procède par récurrence sur m. Commençons par remarquer que $A_0 = 1$ et que $A_1 = \{\mathrm{id}, a_\varepsilon\}$. Passons à l'induction et montrons que $A_{m-1} \wr \mathbb{Z}_2 \cong A_m$. On définit le morphisme

$$\varphi : (A_{m-1} \times A_{m-1}) \rtimes \mathbb{Z}_2 \to A_m : (\tau_0, \tau_1, \sigma) \mapsto \begin{cases} \varphi(\tau_0, \tau_1) & \text{si } \sigma = 0 \\ \varphi(\tau_0, \tau_1) \circ a_\varepsilon & \text{si } \sigma = 1. \end{cases}$$

C'est un isomorphisme. Les arguments pour le montrer sont identiques à ceux dans la preuve de la proposition 4.1.7. On peut conclure par la remarque 4.1.1 que

$$A_m \cong \mathbb{Z}_2 \wr \mathbb{Z}_2 \wr \ldots \wr \mathbb{Z}_2 \ \ (m \text{ fois}).$$

□

4.2 Définition et premières propriétés

Dans cette section, on définit le groupe de Grigorchuk. Son intérêt réside en partie dans le fait que c'est la solution de deux problèmes majeurs de théorie des groupes. D'abord, il résout le problème de Burnside. Ensuite, il donne un exemple de groupe à croissance intermédiaire.

Il est fascinant dans le sens où il répond à ces questions en revenant aux bases les plus fondamentales de la théorie des groupes : on étudie les symétries des objets.

On notera le groupe de Grigorchuk $\mathcal{G}$. C'est le sous-groupe de $\mathrm{Aut}(\mathbf{T})$ généré par a, b, c, d, où $a = a_\varepsilon$ et b, c, d vérifient :

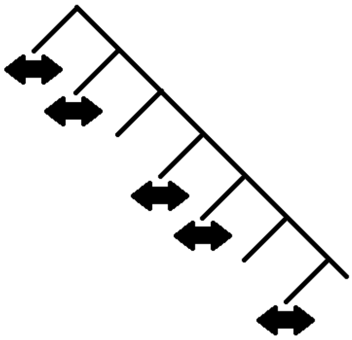
$$b = \varphi(a, c), \ c = \varphi(a, d) \text{ et } d = \varphi(\mathrm{id}, b). \tag{4.2}$$

Les automorphismes b, c et d sont bien définis. Vérifions-le explicitement : soit $v \in \mathcal{V}(\mathbf{T})$, on va procéder par récurrence sur $|v|$. Si $|v| = 0$, alors $b(v) = c(v) = d(v) = \varepsilon$ par définition de φ. Supposons maintenant que b, c, d soient définis pour tout u tel que $|u| < |v|$. Dans ce cas,

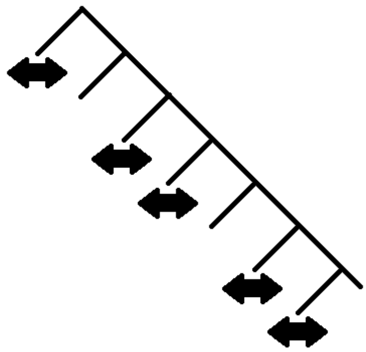
$$b(v) = \varphi(a, c)(v) = \begin{cases} 0a(u) & \text{si } v = 0u \\ 1c(u) & \text{si } v = 1u, \end{cases}$$

par hypothèse de récurrence, $c(u)$ est bien défini. Les calculs de $c(v)$ et $d(v)$ sont similaires. Les applications b, c et d sont donc bien définies. Elles sont également des morphismes. Pour le voir, il suffit de remarquer que de proche en proche, les arêtes ne peuvent qu'être respectées puisqu'on se ramène toujours à a ou id.

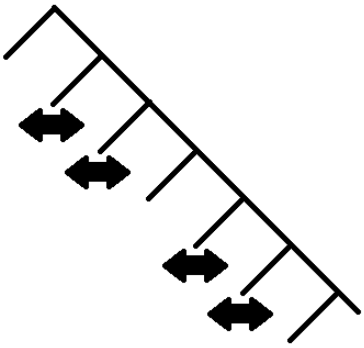
On peut visualiser les éléments b, c et d, c'est ce qui est fait à la Figure 4.4. Les doubles flèches représentent un sous-arbre auquel on a appliqué a.



(a) Image de b.



(b) Image de c.



(c) Image de d.

FIGURE 4.4 – Représentation de b, c et d.

On peut donner ces éléments sous une formule close :

$$\begin{aligned} b' &= (a_0 \cdot a_{1^3 0} \cdot a_{1^6 0} \cdot ...)(a_{10} \cdot a_{1^4 0} \cdot a_{1^7 0} \cdot ...) \\ c' &= (a_0 \cdot a_{1^3 0} \cdot a_{1^6 0} \cdot ...)(a_{1^2 0} \cdot a_{1^5 0} \cdot a_{1^8 0} \cdot ...) \\ d' &= (a_{10} \cdot a_{1^4 0} \cdot a_{1^7 0} \cdot ...)(a_{1^2 0} \cdot a_{1^5 0} \cdot a_{1^8 0} \cdot ...). \end{aligned}$$

Remarque 4.2.1. De telles compositions n'ont de sens que parce que les $a_{1^k 0}$ sont disjoints. Ils sont donc commutatifs, ce qui permet d'affirmer que b', c' et d' sont bien définis si on les donne de la sorte.

Vérifions que les éléments définis ainsi correspondent bien aux éléments b, c et d que l'on souhaitait obtenir.

$$\begin{aligned}
\varphi(a, c') &= \iota_0(a) \cdot \iota_1(c) \\
&= a_0 \cdot \iota_1((a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{1^20} \cdot a_{1^50} \cdot a_{1^80} \cdot \ldots)) \\
&= a_0 \cdot (a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots)(a_{1^30} \cdot a_{1^60} \cdot a_{1^90} \cdot \ldots) \\
&= (a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots) \\
&= b'.
\end{aligned}$$

Les calculs pour c' et d' sont similaires. On a donc $b = b'$, $c = c'$ et $d = d'$.

Définition 4.2.1. Le *groupe de Grigorchuk* $\mathcal{G}$ est le groupe

$$\langle a, b, c, d \rangle \leq \mathrm{Aut}(\mathbf{T}).$$

À présent, on utilisera la notation multiplicative pour ces groupes et on notera l'unité $\mathtt{I}$.

Après cette définition, vérifions quelques propriétés de base. Elles permettent de mieux appréhender $\mathcal{G}$ et seront utilisées dans les développements de propriétés plus fines.

Proposition 4.2.1. *Les éléments b, c et d sont des involutions (i.e : leur carré est leur inverse), ils commutent et $bcd = \mathtt{I}$.*

Démonstration. Il est facile de voir que b, c et d sont des involutions à partir de leurs formules closes. On a établi que a_{1^k0} et $a_{1^{k'}0}$ commutent lorsque $k \neq k'$, or si $k = k'$ c'est vrai aussi. Par conséquent, on peut réécrire

$$\begin{aligned}
b^2 &= (a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots)(a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots) \\
&= (a_0^2 \cdot a_{1^30}^2 \cdot a_{1^60}^2 \cdot \ldots)(a_{10}^2 \cdot a_{1^40}^2 \cdot a_{1^70}^2 \cdot \ldots) = \mathtt{I},
\end{aligned}$$

le même argument montre que $c^2 = d^2 = \mathtt{I}$.

Le fait que les a_{1^k0} commutent permet aussi d'obtenir la commutativité de b, c et d entre-eux. Pour finir, cet argument nous permet aussi d'obtenir la dernière identité :

$$\begin{aligned}
bcd =& (a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots) \\
& (a_0 \cdot a_{1^30} \cdot a_{1^60} \cdot \ldots)(a_{1^20} \cdot a_{1^50} \cdot a_{1^80} \cdot \ldots) \\
& (a_{10} \cdot a_{1^40} \cdot a_{1^70} \cdot \ldots)(a_{1^20} \cdot a_{1^50} \cdot a_{1^80} \cdot \ldots) \\
=& (a_0^2 \cdot a_{1^30}^2 \cdot a_{1^60}^2 \cdot \ldots)(a_{10}^2 \cdot a_{1^40}^2 \cdot a_{1^70}^2 \cdot \ldots)(a_{1^20}^2 \cdot a_{1^50}^2 \cdot a_{1^80}^2 \cdot \ldots) \\
=& \mathtt{I}\,.
\end{aligned}$$

□

Corollaire 4.2.1. *Le groupe $\langle b, c, d \rangle$ est isomorphe à $\mathbb{Z}_2^2$.*

Démonstration. Commençons par vérifier que $G := \langle b, c, d\rangle$ est d'ordre 4. On sait que $G = \{g_1 ... g_n | n \in \mathbb{N} \text{ et } g_j \in \{b, c, d\}\}$ vu que $b^2 = c^2 = d^2 = \mathtt{I}$. De plus, on sait que

$$bc = d, bd = c \text{ et } cd = b.$$

Ainsi, $|G| = 4$ car faire le produit de deux éléments ne crée aucun nouvel élément. On en déduit immédiatement que $G \cong \mathbb{Z}_2^2$ car $g \in G \Rightarrow g^2 = \mathtt{I}$. □

Corollaire 4.2.2. *Le groupe $\mathcal{G}$ peut être engendré par trois éléments.*

Démonstration. On sait que $bc = d$, dès lors, $\mathcal{G} = \langle a, b, c\rangle$. □

La propriété suivante est utile pour démontrer que $\mathcal{G}$ est un solution au problème de Burnside aussi bien que pour montrer qu'il est infini.

Proposition 4.2.2. *Dans $\mathcal{G}$,*

$$(ad)^4 = (ac)^8 = (ab)^{16} = \mathtt{I}\,.$$

Démonstration. Commençons par montrer que $(ad)^4 = \mathtt{I}$. On a les implications suivantes :

$$\begin{array}{rlcl} & d & = & \varphi(\mathtt{I}, b) \\ \Rightarrow & ad & = & \varphi(b, \mathtt{I})a \\ \Rightarrow & (ad)^2 & = & a\varphi(b, \mathtt{I})\varphi(b, \mathtt{I})a \\ & & = & a\varphi(b, b)a \\ & & = & \varphi(b, b) \\ \Rightarrow & (ad)^4 & = & \varphi(b, b)\varphi(b, b) \\ & & = & \varphi(b^2, b^2) = \mathtt{I}\,. \end{array}$$

L'équation $(ad)^2 = \varphi(b, b)$ est représentée visuellement à la Figure 4.5, où le point orange représente l'image de 1. Notons que

$$(ad)^4 = \mathtt{I} \Leftrightarrow \mathtt{I} = (da)^4.$$

On en tire les implications suivantes :

$$\begin{array}{rlcl} & c & = & \varphi(a, d) \\ \Rightarrow & ac & = & a\varphi(a, d) \\ & & = & \varphi(d, a)a \\ \Rightarrow & (ac)^2 & = & a\varphi(a, d)a\varphi(d, a)a \\ & & = & a\varphi(ad, da)a \\ \Rightarrow & (ac)^4 & = & a\varphi(ad, da)aa\varphi(ad, da)a \\ & & = & a\varphi((ad)^2, (da)^2)a \\ \Rightarrow & (ac)^8 & = & a\varphi((ad)^2, (da)^2)aa\varphi((ad)^2, (da)^2)a \\ & & = & a\varphi((ad)^4, (da)^4)a \\ & & = & a\varphi(\mathtt{I}, \mathtt{I})a = \mathtt{I}\,. \end{array}$$

Pour conclure, il nous reste à remarquer que

$$\begin{array}{rlcl} & b & = & \varphi(a,c) \\ \Rightarrow & ab & = & a\varphi(a,c) \\ & & = & \varphi(c,a)a \\ \Rightarrow & (ab)^2 & = & a\varphi(ac,ca)a \\ \Rightarrow & (ab)^{16} & = & ((ab)^2)^8 \\ & & = & a\varphi((ac)^8,(ca)^8)a = \mathtt{I}\,. \end{array}$$

□

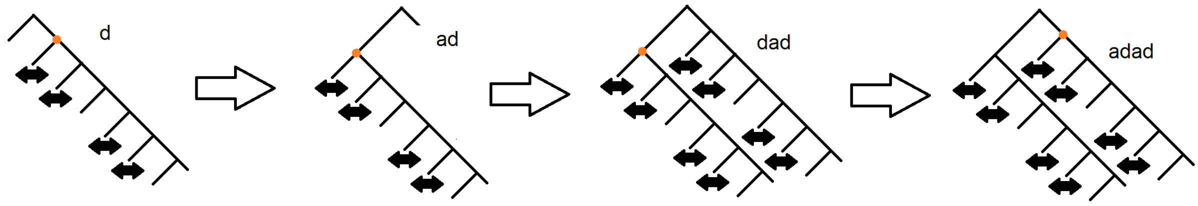


FIGURE 4.5 – L'automorphisme *adad*.

Corollaire 4.2.3. *Les groupes*

$$\langle a,b\rangle, \langle a,c\rangle, \langle a,d\rangle \leq \mathcal{G}$$

sont finis.

Démonstration. On sait que, pour $x \in \{b,c,d\}$, le groupe $\langle a,x\rangle = \{g_1...g_n | n \in \mathbb{N}$ et $g_j = a$ ou $x, \forall j\}$. On va montrer que si $n > 32$, alors $g_1...g_n$ n'est pas un nouvel élément [3], peu importe la suite $(g_j)_{j=1}^n$. S'il existe un j tel que $g_j = g_{j+1}$, alors l'élément peut se réécrire $g_1...g_{j-1}g_{j+2}...g_n$ car $a^2 = x^2 = \text{id}$ et donc $g_1...g_n$ n'est pas un nouvel élément. On en tire que $g_1...g_n$ est de la forme $a(xa)^{\frac{n-1}{2}}$, $x(ax)^{\frac{n-1}{2}}$, $(xa)^{\frac{n}{2}}$ ou $(ax)^{\frac{n}{2}}$. Dès lors, vu que $n > 32$ et que $(ax)^{16} = \text{id}$ pour tout x, $g_1...g_n$ peut se réécrire de manière plus courte.

On a $|\langle a,x\rangle| \leq |\{a,x\}^{32}| < \infty$. □

Pour que la croissance de $\mathcal{G}$ existe, il faut non seulement que le groupe soit finiment engendré mais aussi qu'il soit infini. C'est ce que nous allons vérifier. Avant de le faire, nous avons besoin de définir un dernier type d'automorphismes, les transformations qui n'agissent que sur les derniers étages de l'arbre.

Définition 4.2.2. Pour tout $v \in \mathbf{T}$, on définit $\text{St}_{\mathcal{G}}(v)$ le *stabilisateur* de v. C'est le sous-groupe de $\mathcal{G}$ dont les éléments envoient v sur lui-même. On définit le *nième stabilisateur* de $\mathcal{G}$ comme étant le sous-groupe de $\mathcal{G}$ qui stabilise l'étage n de $\mathbf{T}$. On le note $\text{St}_{\mathcal{G}}(n)$. Plus explicitement,

$$\text{St}_{\mathcal{G}}(n) = \{\tau \in \mathcal{G}\,|\,\tau(v) = v, \forall v \in \mathbf{T} \text{ tel que } |v| = n\}.$$

Le groupe $\text{St}_{\mathcal{G}}(1)$ est appelé *sous-groupe fondamental* de $\mathcal{G}$ et on le note $\mathcal{H}$.

3. Dans le sens où il existe $m < n$ tel que $g_1...g_n = h_1...h_m$

Par définition, on a

$$\mathrm{St}_{\mathcal{G}}(n) = \bigcap_{v:|v|=n} \mathrm{St}_{\mathcal{G}}(v).$$

On perçoit intuitivement que ces stabilisateurs sur les étages les plus élevés sont le "dual" des A_n. C'est sur cette intuition que se repose la proposition suivantes.

Proposition 4.2.3. *Pour tout $n \in \mathbb{N}$, $\mathcal{H}_n := \mathrm{St}_{\mathcal{G}}(n)$ est d'indice fini dans $\mathcal{G}$. Plus précisément,*

$$[\mathcal{G} : \mathcal{H}_n] \leq |A_n| = 2^{2^n-1}.$$

Démonstration. Soit $R = \{g_j \in \mathcal{G} \,|\, j \in \mathcal{J}\}$ tel que chaque classe latérale de $\mathcal{H}_n$ admet exactement un représentant dans R. On définit l'injection

$$p : R \to A_n : g_j \mapsto g'_j,$$

où $g'_j : v \mapsto \begin{cases} g_j(v) & \text{si } |v| \leq n \\ g_j(v')s & \text{si } v = v's, \text{ où } |v'| = n. \end{cases}$ C'est bien une injection car si on suppose qu'il existe $i \neq j$ tels que $p(g_i) = p(g_j)$, alors $g_i^{-1}g_j \in \mathcal{H}_n$. C'est absurde puisqu'on a supposé que $g_i\mathcal{H}_n \neq g_j\mathcal{H}_n$.

On peut conclure car

$$[\mathcal{G} : \mathcal{H}_n] = |R| \leq |A_n| = 2^{2^n-1},$$

la dernière égalité est donnée par la proposition 4.1.8. □

Passons aux trois lemmes qui seront utiles pour prouver que $\mathcal{G}$ est infini.

Lemme 4.2.1. *Soient G un groupe et $H \leq G$. Si H est d'indice 2, alors H est normal dans G.*

Démonstration. Comme il y a deux classes latérales, elles sont forcément égales à H et $G \setminus H$. Ainsi, si $h \in H$, on a évidemment $hH = Hh$. Si $x \in G \setminus H$, alors $xH = G \setminus H = Hx$. On en conclut que $H \lhd G$. □

Lemme 4.2.2. *Le groupe fondamental $\mathcal{H}$ est tel que*

$$\mathcal{H} = \langle b, c, d, b^a, c^a, d^a \rangle, \ \mathcal{H} \lhd \mathcal{G} \ \text{ et } [\mathcal{G}, \mathcal{H}] = 2.$$

Démonstration. Vu les relations que la proposition 4.2.1 nous donne, on sait que n'importe quelle décomposition de longueur minimale d'un élément de $\mathcal{G}$ en $\{a, b, c, d\}$ est de la forme

$$(a)g_1ag_2ag_3a...ag_n(a),$$

où les symboles entre parenthèses peuvent ne pas être pris et les $g_j \in \{b, c, d\}$.

Soient $g \in \mathcal{G}$ et $w \in \{a, b, c, d\}^*$ une représentation minimale de g. On remarque que $|w|_a = 0 \mod (1)$ si et seulement si $g \in \mathcal{H}$. Cette observation couplée avec la propriété 4.2.2 nous permettent d'affirmer que $\mathcal{H}$ et $a\mathcal{H}$ sont les seules classes latérales de $\mathcal{H}$. En effet, si $|w|_a$ est pair, g est dans $\mathcal{H}$. Sinon, on peut montrer qu'il peut s'écrire sous la forme ah, où $h \in \mathcal{H}$. Si w commence par a, on a fini. Sinon, on sait que $(g_1a)^{16} = \mathtt{I}$ et donc $g_1a = (ag_1)^{15}$. Ainsi,

$$g = a(g_1a)^{14}g_1ag_2ag_3a...ag_n(a),$$

c'est la forme souhaitée car $|(g_1a)^{14}g_1ag_2ag_3a...ag_n(a)|_a = 14 + (|w|_a - 1)$ est pair. On a donc bien $[\mathcal{G} : \mathcal{H}] = 2$.

Dès lors, $\mathcal{H}$ est normal dans $\mathcal{G}$ vu le lemme 4.2.1.

On finit par remarquer que si $g \in \mathcal{H}$, $g \in \langle b, c, d, b^a, c^a, d^a\rangle$ et réciproquement. En effet, comme $a = a^{-1}$, que $g_j^a = ag_ja$ pour tout $j \in \{1, ..., n\}$ et donc comme $|w|_a$ est pair, on peut conclure. De plus, le produit d'éléments de $\{b, c, d, b^a, c^a, d^a\}$ est dans $\mathcal{H}$. □

Lemme 4.2.3. *L'image $\psi(\mathcal{H})$ est un sous-groupe de $\mathcal{G} \times \mathcal{G}$ (à plongement de $\mathcal{G} \times \mathcal{G}$ dans $(\mathcal{G} \times \mathcal{G}) \rtimes \mathbb{Z}_2$ près) tel que la projection de $\psi(\mathcal{H})$ selon chaque composante est surjective. Pour rappel, la notation ψ est fixée en 4.1.1.*

Démonstration. Par définition, $\mathcal{H}$ fixe 0 et 1, donc $\psi(\mathcal{H}) \leq \mathrm{Aut}(\mathbf{T}) \times \mathrm{Aut}(\mathbf{T})$. De plus,

$$\psi : \begin{cases} b \mapsto (a, c) \\ c \mapsto (a, d) \\ d \mapsto (\mathtt{I}, b) \\ b^a \mapsto (c, a) \\ c^a \mapsto (d, a) \\ d^a \mapsto (b, \mathtt{I}). \end{cases}$$

D'un part, on a montré que $\mathcal{H} = \langle b, c, d, b^a, c^a, d^a\rangle$, donc $\psi(\mathcal{H}) \leq \mathcal{G} \times \mathcal{G}$. D'autre part, si on regarde les projections que $\psi(x)$, où $x \in \{b, c, d, b^a, c^a, d^a\}$, on constate que tous les générateurs de $\mathcal{G}$ sont présents. Les projections sont donc surjectives. □

Ces deux derniers lemmes forcent que $\mathcal{G}$ soit infini par l'absurde.

Théorème 4.2.1. *Le groupe $\mathcal{G}$ est infini.*

Démonstration. Par le lemme 4.2.2, on sait que $\mathcal{H}$ est un sous-groupe propre de $\mathcal{G}$. Par ailleurs, le lemme 4.2.3 nous permet d'affirmer qu'il y a une surjection de $\mathcal{H}$ sur $\mathcal{G}$. Donc, si $|\,\mathcal{G}\,| < \infty$, alors $|\mathcal{H}| < |\,\mathcal{G}\,|$ et $|\,\mathcal{G}\,| \leq |\mathcal{H}|$. C'est une absurdité, on peut conclure. □

On a donc avec $\mathcal{G}$ un groupe finiment engendré et infini, cela a donc du sens d'en étudier la croissance.

4.3 Croissance

Cette section s'occupe de déterminer que $\mathcal{G}$ se trouve dans la classe des groupes à croissance intermédiaire. On commence par montrer que $\mathcal{G}$ est à croissance superpolynomiale en montrant qu'il est multilatéral. Ensuite, on montrera que $\mathcal{G}$ est à croissance sous-exponentielle. Cette preuve demande plus de travail. On devra découper $\mathcal{G}$ en plusieurs copies de lui-même. Ce découpage nous permettra de majorer la croissance de $\mathcal{G}$ par la croissance étoilée de $\mathcal{G}$.

4.3.1 Croissance superpolynomiale

Dans cette sous-section, l'objectif est de montrer que $\mathcal{G}$ est multilatéral. Ensuite, on appliquera la proposition 4.1.3 pour conclure que $\mathcal{G}$ est à croissance superpolynomiale.

La démonstration de ce fait est technique et demande de définir la clôture normale de b.

Définition 4.3.1. Soient G un groupe et $A \subset G$, la *clôture normale* de A est le plus petit sous-groupe normal de G contenant A.

Ce groupe existe toujours car G est normal dans G et contient A, pour tout A. De plus, comme l'intersection de groupes normaux est normale, la clôture normale de A est l'intersection des sous-groupes normaux de G contenant A.

Le but des deux lemmes suivants est de montrer que $\psi(\mathcal{H})$ est d'indice fini dans $\mathcal{G} \times \mathcal{G}$. Pour le faire, l'idée est de définir un sous-groupe de $\psi(\mathcal{H})$ qui soit d'indice fini dans $\mathcal{G} \times \mathcal{G}$. Le sous-groupe en question est $\mathcal{B}^2$.

Lemme 4.3.1. *Soit $\mathcal{B} \leq \mathcal{G}$ la clôture normale de $b \in \mathcal{G}$. On a $[\mathcal{G}, \mathcal{B}] \leq 8$.*

Démonstration. Commençons par remarquer que

$$\mathcal{B} = \langle b^g | g \in \mathcal{G} \rangle.$$

Notons également que $\langle a, d \rangle$ est isomorphe à $\mathcal{D}_4$, le groupe diédral d'ordre 8. En effet, $\langle a, d \rangle = \langle a, ad \rangle = \{\mathtt{I}, a, d, ad, ada, adad, adada, adadad\}$ et $a^2 = (ad)^4 = a(ad)a^{-1}(ad) = \mathtt{I}$.

On sait grâce à la proposition 4.2.1 que $\mathcal{G} = \langle a, b, d \rangle$. Ainsi,

$$\frac{\mathcal{G}}{\mathcal{B}} \cong \frac{\langle a, d \rangle}{\mathcal{B} \cap \langle a, d \rangle}.$$

On a donc $[\mathcal{G} : \mathcal{B}] = \left| \frac{\mathcal{G}}{\mathcal{B}} \right| = \left| \frac{\langle a, d \rangle}{\mathcal{B} \cap \langle a, d \rangle} \right| \leq 8.$ □

Lemme 4.3.2. *On a l'inclusion*

$$(\mathcal{B} \times \mathcal{B}) \leq \psi(\mathcal{H}) \leq (\mathcal{G} \times \mathcal{G})$$

Démonstration. Par le lemme 4.2.2, on sait que $\langle (\mathtt{I}, b), (b, \mathtt{I}) \rangle = \langle \psi(d), \psi(d^a) \rangle \leq \psi(\mathcal{H})$. Soit $x \in \mathcal{H}$ et posons $\psi(x) = (x_0, x_1)$. On a

$$\begin{aligned} \psi(d^x) &= \psi(x^{-1})\psi(d)\psi(x) \\ &= (x_0^{-1}, x_1^{-1})(\mathtt{I}, b)(x_0, x_1) = (\mathtt{I}, b^{x_1}). \end{aligned}$$

Vu le lemme 4.2.3, on en tire que tout élément $(\mathtt{I}, b^g) \in \psi(\mathcal{H}))$. Ce sont les générateurs de $\mathtt{I} \times \mathcal{B}$ et donc $\mathtt{I} \times \mathcal{B} \leq \psi(\mathcal{H})$. De la même manière, $\psi((d^a)^x) = (b^{x_0}, \mathtt{I})$ et donc $\mathcal{B} \times \mathtt{I}$. Vu que le produit se fait composante à composante, on a $\mathcal{B} \times \mathcal{B} \leq \psi(\mathcal{H})$.

La deuxième inclusion vient du lemme 4.2.3. □

On a maintenant tous le résultats qui permettent de montrer que $\mathcal{G}$ est multilatéral et d'en déduire qu'il est à croissance superpolynomiale.

Proposition 4.3.1. *Les groupes $\mathcal{G}$ et $\mathcal{G} \times \mathcal{G}$ sont commensurables.*

Démonstration. On sait que ψ est un isomorphisme et donc que $\mathcal{H}$ est isomorphe à $\psi(\mathcal{H})$. Par le lemme 4.2.2, on sait aussi que $\mathcal{H}$ est d'indice fini dans $\mathcal{G}$. Si on montre que $\psi(\mathcal{H})$ est d'indice fini, alors on peut conclure. Vu le lemme 4.3.2, on sait que $\mathcal{B} \times \mathcal{B} \leq \psi(\mathcal{H})$. De plus, par le lemme 4.3.1, on a

$$[\mathcal{G} \times \mathcal{G} : \psi(H)] \leq [\mathcal{G} \times \mathcal{G} : \mathcal{B} \times \mathcal{B}] = [\mathcal{G} : \mathcal{B}]^2 \leq 8^2 < \infty.$$

□

Corollaire 4.3.1. *Le groupe $\mathcal{G}$ est à croissance superpolynomiale. Plus précisément,*

$$\gamma_{\mathcal{G}} \succeq \exp(\cdot^{\alpha}),$$

où $\alpha > 0$.

Démonstration. Le groupe de Grigorchuk $\mathcal{G}$ est multilatéral. Par la proposition 4.1.3. Par la proposition 1.2.13, on peut conclure. □

4.3.2 Croissance sous-exponentielle

Dans cette sous-section, on démontre que $\mathcal{G}$ est à croissance sous-exponentielle. Cette partie est plus technique et repose sur une étude systématique des décompositions réduites des automorphismes.

On a déjà vu que les décompositions réduites des éléments de $\mathcal{G}$ sont de la forme

- i $ag_1ag_2a...g_{n-1}ag_na$
- ii $ag_1ag_2a...g_{n-1}ag_n$
- iii $g_1ag_2a...g_{n-1}ag_na$
- iv $g_1ag_2a...g_{n-1}ag_n$

où les $g_j \in \{b, c, d\}$. On appellera ces différentes formes que peut prendre une décomposition réduite des types. Bien entendu, un élément g peut avoir plusieurs décompositions réduites et donc à priori plusieurs types. Cependant, il y a tout de même une certaine stabilité du type de décompositions réduites que peut admettre un élément.

Proposition 4.3.2. *Soit $g \in \mathcal{G}$. Toutes les décompositions réduites de g sont soit de type (i) ou elles sont toutes de type (iv) ou encore elles sont toutes de type (ii) ou (iii).*

Démonstration. Si la longueur [4] de g est paire, la décomposition réduite de g ne peut être que de type (ii) ou (iii). Si la longueur de g est impaire, alors les décompositions réduites de g sont de type (i) ou (iv). De plus, on sait que si $g \in \mathcal{H}$, alors le nombre de a de toutes les décompositions est pair. Toutes les décompositions réduites de g sont alors de type (iv). Pour finir, si $g \in \mathcal{G} \setminus \mathcal{H}$, alors il y a un nombre impair de a dans les décompositions réduites. Elles sont alors de type (i). □

La proposition ne peut pas être renforcée car on sait qu'il y a des éléments qui admettent une décomposition réduite de type (ii) et de type (iii). Un exemple est donné par $adad$ qui est également décomposé en $dada$. On note que ces décompositions sont forcément réduites car $adad$ ne peut pas être décomposé en trois éléments de $\{a, b, c, d\}$ ou moins. La définition suivante est donc légitime.

Définition 4.3.2. Soit $g \in \mathcal{G}$. On peut à partir de la proposition 4.3.2 définir le *type* de g. On dit que g est de type 1 si les décompositions réduites de g sont de type (i). Si elles sont de type (ii) ou (iii), on dit que g est de type 2/3. Finalement, si elles sont de type (iv), on dit que g est de type 4.

La proposition suivante nous permettra à l'avenir de décomposer un automorphisme en deux automorphismes plus courts. Elle sera utilisée dans des démonstrations par récurrence.

Proposition 4.3.3. *Soient $g, g_0, g_1 \in \mathcal{G}$ et $\sigma \in \mathbb{Z}_2$ tels que $\psi(g) = (g_0, g_1, \sigma)$. On a*

$$\begin{aligned} g \text{ de type 1 } &\Rightarrow |g_0|, |g_1| \leq \frac{|g|-1}{2}, \\ g \text{ de type 2/3 } &\Rightarrow |g_0|, |g_1| \leq \frac{|g|}{2} \\ \text{et } g \text{ de type 4 } &\Rightarrow |g_0|, |g_1| \leq \frac{|g|+1}{2} \end{aligned}$$

Démonstration. On définit $w = (a)g_1a...ag_n(a)$ une décomposition réduite de g et $\pi : \{1, ..., n\} \to \mathbb{N} : j \mapsto |(a)g_1a...ag_j|_a$. Considérons les deux règles des réécriture suivantes :

$$\Phi_0 : \begin{cases} a \mapsto \mathtt{I}\,,\ b \mapsto a,\ c \mapsto a,\ d \mapsto \mathtt{I} & \text{si } \pi(j) \in 2\,\mathbb{N} \\ a \mapsto \mathtt{I}\,,\ b \mapsto c,\ c \mapsto d,\ d \mapsto b & \text{si } \pi(j) \in 2\,\mathbb{N}+1 \end{cases}$$

$$\Phi_1 : \begin{cases} a \mapsto \mathtt{I}\,,\ b \mapsto a,\ c \mapsto a,\ d \mapsto \mathtt{I} & \text{si } \pi(j) \in 2\,\mathbb{N}+1 \\ a \mapsto \mathtt{I}\,,\ b \mapsto c,\ c \mapsto d,\ d \mapsto b & \text{si } \pi(j) \in 2\,\mathbb{N}\,. \end{cases}$$

Il est clair que $\Phi_0(g) = g_0$ et $\Phi_1(g) = g_1$. La conclusion suit car les règles de réécriture effacent chaque a et remplacent b, c et d par une lettre ou l'effacent. □

4. Notons que la longueur dans ce chapitre est toujours considérée avec l'ensemble de générateurs $\{a, b, c, d\}$.

Corollaire 4.3.2. *Soient $g, g_0, g_1 \in \mathcal{G}$ et $\sigma \in \mathbb{Z}_2$ tels que $\psi(g) = (g_0, g_1, \sigma)$. On a*

$$|g_0| + |g_1| \leq |g| + 1.$$

Le but est maintenant de décomposer les éléments de $\mathcal{G}$ en des éléments dont on contrôle la longueur. L'idée est de commencer par appliquer des automorphismes disjoints à chaque sous-arbre à un étage donné et ensuite d'appliquer un dernier morphisme qui donnera les déplacements sur les étages précédents. Pour que cette décomposition fonctionne, il faut qu'il y ait une correspondance 1 :1 entre les restrictions des éléments de $\mathcal{G}$ à un $\mathbf{T}_v$ et les éléments de $\mathcal{G}$. Ce principe est formalisé par les groupes auto-similaires et les propriétés qui suivent.

Définition 4.3.3. Soient $G \leq \mathrm{Aut}(\mathbf{T})$ et $v \in \mathcal{V}(\mathbf{T})$. On note $G_v = \mathrm{St}_G(v) \restriction_{\mathbf{T}_v} \leq \mathrm{Aut}(\mathbf{T}_v)$ le sous-groupe de $\mathrm{Aut}(\mathbf{T}_v)$ dont les éléments sont les restrictions à $\mathbf{T}_v$ des $g \in G$ qui fixent le sommet v. Autrement dit, $g \in G_v$ si $g(v) = v$ et il existe $g' \in G$ tel que

$$g(u) = \begin{cases} g'(u) & \text{si } v \in \mathrm{Pref}(u) \\ u & \text{sinon,} \end{cases}$$

pour tout $u \in \mathcal{V}(\mathbf{T})$, on note alors cet élément g, $g' \restriction_{\mathbf{T}_v}$.

Définition 4.3.4. On dit que G est *auto-similaire* si $G_v \cong G$ pour tout $v \in \mathcal{V}(\mathbf{T})$.

Lemme 4.3.3. *Le groupes de Grigorchuk $\mathcal{G}$ est auto-similaire.*

Démonstration. On procède par induction sur $|v|$. Si v est le mot vide, on a $\mathcal{G}_v = \mathcal{G}$. Passons à l'induction et supposons que la propriété est vérifiée pour v. Montrons que $\mathcal{G}_{v0} \cong \mathcal{G}_v$. L'isomorphisme que l'on va utiliser est

$$\phi : \mathcal{G}_v \to \mathcal{G}_{v0} : g \mapsto \phi(g),$$

où $\phi(g)(u) = \begin{cases} g(vw) & \text{si } u = v0w \\ u & \text{si } v0 \notin \mathrm{Pref}(u) \end{cases}.$

Pour montrer que c'est un isomorphisme, il faut d'abord montrer que les images de ϕ sont bien à valeurs dans $\mathcal{G}_{v0}$. En renforçant notre hypothèse de récurrence, on peut supposer que des équivalents de ϕ permettent de proche en proche d'aller de $\mathcal{G}$ à $\mathcal{G}_v$. Cela signifie que l'isomorphisme entre $\mathcal{G}$ et $\mathcal{G}_v$ est donné par $\iota_v \restriction_{\mathcal{G}}$. Par abus de langage, nous omettrons le ι_v et parlerons de $a, b, c, d \in \mathcal{G}_v$. Vu le lemme 4.2.3, on sait que ϕ est à valeurs dans $\mathcal{G}_{v0}$. En effet, $\mathcal{H}$ peut être envoyé surjectivement sur $\mathcal{G}$ par ψ composé avec la projection selon la première composante.

Définissons maintenant $\phi' = \iota_v \circ \iota_{v0}^{-1}$. Montrons que ϕ' est bien à valeurs dans $\mathcal{G}_v$. C'est évident puisque les automorphismes de $\mathcal{G}_{v0}$ sont les restrictions à gauche d'automorphismes de $\mathcal{G}_v$ qui eux-même sont, en omettant ι_v, les automorphismes de $\mathcal{G}$. Or les restrictions à gauche de $\mathcal{G}$ sont encore des éléments de $\mathcal{G}$. Ainsi, quand on applique ϕ^{-1}, on reste dans $\mathcal{G}$.

Dès lors, on peut conclure car il est clair que ϕ et ϕ' sont inverses et que ce sont des morphismes. On traite le cas de $\mathcal{G}_{v1}$ de la même manière. □

Corollaire 4.3.3. *Il existe un plongement* $\chi : \mathcal{H}_3 \to \mathcal{G}^8 : h \mapsto (g_{000}, g_{001}, ..., g_{110}, g_{111})$.

Démonstration. Naturellement, il y a un plongement $\psi_3 : \mathcal{H}_3 \to \mathcal{G}_{000} \times \mathcal{G}_{001} \times ... \times \mathcal{G}_{111} : h \mapsto (h \restriction_{\mathbf{T}_{000}}, ..., h \restriction_{\mathbf{T}_{111}})$. Par auto-similarité, on sait que $\mathcal{G}_v \cong \mathcal{G}$ pour les v de longueur 3 en particulier. Ces isomorphismes sont les restrictions des ι_v^{-1} au groupe de Grigorchuk. Le plongement que l'on recherche est $\chi = (\iota_{000}^{-1}, ..., \iota_{111}^{-1}) \circ \psi_3$. Pour tout $h \in \mathcal{H}_3$, on note $\chi(h) = (g_{000}, g_{001}, ..., g_{110}, g_{111})$ avec $g_v \in \mathcal{G}$ pour tout $v \in \{0,1\}^3$. □

Cette décomposition nous permettra de faire apparaître la fonction $\gamma_{\mathcal{G}}^{\star 8}$ pour majorer $\gamma_{\mathcal{G}}$. En effet, lorsqu'on voudra majorer le nombre d'éléments de longueur n, il nous suffira de compter le nombre de décompositions possibles. Cependant, pour appliquer le *upper bound lemma* (lemme 4.1.2), il nous faut majorer la longueur des décompositions d'un élément de longueur n par des décompositions dont la somme des longueurs est plus petite qu'un αn, avec $\alpha < 1$.

Lemme 4.3.4 (Cancellation Lemma). *Soit* $h \in \mathcal{H}_3$. *On a*

$$|g_{000}| + |g_{001}| + ... + |g_{110}| + |g_{111}| \leq \frac{5}{6}|h| + 8.$$

Démonstration. Fixons $w = (a)g_1a...g_n(a)$ une décomposition réduite de h. A partir de w, on peut construire de nouveaux mots en appliquant les règles de réécriture Φ_0 et Φ_1. On pose w_0 et w_1 comme étant les mots obtenus en appliquant Φ_0 et Φ_1 respectivement à w et en effaçant tous les $\mathtt{I}$. De la même manière, on construit w_{00}, w_{01}, w_{10} et w_{11} et ensuite $w_{000}, w_{001}, ..., w_{111}$. Si on considère les éléments du groupe donnés par ces mots, on obtient des décompositions de h en g_0g_1, $g_{00}g_{01}g_{10}g_{11}$ et $g_{000}g_{001}...g_{111}$, où g_v est l'élément du groupe qui correspond au mot w_v.

Notons que ces décompositions ne sont pas nécessairement réduites. On a donc les inégalités suivantes

$$|g_v| \leq |w_v|, \tag{4.3}$$

pour tout $v \in \{0,1\}^{\leq 3}$.

On a aussi, vu la corollaire 4.3.2,

$$\begin{aligned} |g_0| + |g_1| &\leq |h| + 1 \\ |g_{00}| + |g_{01}| + |g_{10}| + |g_{11}| &\leq |g_0| + |g_1| + 2 \\ |g_{00}| + |g_{001}| + ... + |g_{111}| &\leq |g_{00}| + |g_{01}| + |g_{10}| + |g_{11}| + 4. \end{aligned} \tag{4.4}$$

Posons $w' = w_0w_1, w'' = w_{00}w_{01}w_{10}w_{11}$ et $w''' = w_{000}w_{001}...w_{111}$. Vu les règles de réécriture, on sait que $|w'| = 2|w|_b + 2|w|_c + |w|_d$ puisque d est effacé soit par Φ_0 soit par Φ_1. Ainsi, $|w'| \leq 2(|w|_b + |w|_c + |w|_d) - |w|_d \leq |w|_b + |w|_c + |w|_d + |w|_a + 1 - |w|_d = |w| + 1 - |w|_d$.

Majorons maintenant $|w''|$ et $|w'''|$. On sait que

$$w'' = \Phi_0(\Phi_0(w))\Phi_1(\Phi_0(w))\Phi_0(\Phi_1(w))\Phi_1(\Phi_1(w)).$$

Chaque b donne un c et un a à la première étape et ensuite, le a s'efface et le c donne un d et un a. Chaque c donne d'abord un d et un a puis le a s'efface et le d donne un seul b. Chaque d quant à lui donne un seul b puis ce b donne un c et un a. Au total, $|w''| = 2|w|_b+|w|_c+2|w|_d \leq 2(|w|_b+|w|_c+|w|_d)-|w|_c \leq |w|_b+|w|_c+|w|_d+|w|_a+1-|w|_c = |w|+1-|w|_c$. De la même manière, on obtient $|w'''| \leq |w|+1-|w|_b$. En résumé, on a les inégalités suivantes :

$$\begin{aligned} |w'| &\leq |w|+1-|w|_d \\ |w''| &\leq |w|+1-|w|_c \\ |w'''| &\leq |w|+1-|w|_b \end{aligned} \tag{4.5}$$

Remarquons encore que comme $|w|_b+|w|_c+|w|_d \geq \dfrac{|w|-1}{2}$, on a forcément un $x \in \{b,c,d\}$ tel que $|w|_x > \dfrac{|w|}{6} - 1$. Sinon,

$$|w|_b+|w|_c+|w|_d \leq \frac{|w|}{2} - 3 \leq \frac{|w|-1}{2}. \tag{4.6}$$

Les inégalités obtenues nous permettent d'avoir la suite d'inégalités ci-dessous :

$$\begin{aligned} |g_{000}|+|g_{001}|+\ldots+|g_{111}| &\leq \max\{|w'''|,|w''|+4,|w'|+2+4\} && \text{par (4.3) et (4.4)} \\ &\leq \max\{|w'''|,|w''|,|w'|\}+6 \\ &\leq |w|+1-\max\{|w|_b,|w|_c,|w|_d\}+6 && \text{par (4.5)} \\ &\leq |w|+7-\left(\frac{|w|}{6}-1\right) && \text{par (4.6)} \\ &= \frac{5}{6}|w|+8 && \text{par définition de } w. \end{aligned}$$

□

Nous sommes maintenant prêts à prouver que $\mathcal{G}$ est à croissance sous-exponentielle. On en déduira qu'il est à croissance intermédiaire.

Proposition 4.3.4. *Le groupe de Grigorchuk $\mathcal{G}$ a une croissance sous-exponentielle. Plus précisément, il existe $\nu < 1$ tel que*

$$\gamma_{\mathcal{G}} \preceq \exp(\cdot^{\nu})$$

Démonstration. On sait par 4.2.3 que $[\mathcal{G},\mathcal{H}_3] \leq 2^{2^3-1} = 128$. Soit $R = \{u_i | i \in \mathcal{I}\}$ un ensemble tel que chaque classe latérale de $\mathcal{H}_3$ a exactement un représentant dans R. On sait que $|\mathcal{I}| = |R| \leq 128$ et on pose $t = \max\{|u_i| | i \in \mathcal{I}\} \in \mathbb{N}$.

Soit g un élément quelconque de $\mathcal{G}$. Il existe une unique décomposition de g en uh, où $u \in R$ et $h \in \mathcal{H}_3$. On sait que $|h| \leq t+|g|$ car $h = u^{-1}g$.

Écrivons g sous la forme $u\iota_{000}(g_{000})...\iota_{111}(g_{111})$, comme précédemment. Dans la suite, nous omettrons les ι_v. Par le lemme 4.3.4, on a

$$|g_{000}| + |g_{001}| + ... + |g_{110}| + |g_{111}| \leq \frac{5}{6}|h| + 8 \leq \frac{5}{6}|g| + \frac{5t+48}{6}.$$

Dès lors, on peut majorer $\gamma_{\mathcal{G}}(n)$ car tout élément g qui peut s'écrire en n générateurs ou moins doit pouvoir s'écrire sous la forme $ug_{000}...g_{111}$, où $u \in R$ et $|g_{000}| + |g_{001}| + ... + |g_{110}| + |g_{111}| \leq \frac{5}{6}|g| + \frac{5t+48}{6}$. Donc

$$\gamma_{\mathcal{G}}(n) \leq |R| \sum_{(n_1,...,n_8)\in D} \gamma_{\mathcal{G}}(n_1)...\gamma_{\mathcal{G}}(n_8) \leq 128\gamma_{\mathcal{G}}^{\star 8}\left(\frac{5}{6}n + \frac{5t+48}{6}\right), \tag{4.7}$$

où $D = \left\{(n_1, ..., n_8) \in \mathbb{N}^8 \,|n_1 + ... + n_8 \leq \frac{5}{6}n + \frac{5t+48}{6}\right\}$.

Prenons maintenant $k = t + 10$ et $m = n + k$. On a

$$\frac{5}{6}n + \frac{5t+48}{6} < \frac{5}{6}n + \frac{5t+50}{6} = \frac{5}{6}(n+k) = \frac{5}{6}m. \tag{4.8}$$

On en tire la suite d'inégalité :

$$\begin{aligned}
\gamma_{\mathcal{G}}(m) &= \gamma_{\mathcal{G}}(n+k) \\
&\leq \gamma_{\mathcal{G}}(n)\gamma_{\mathcal{G}}(k) && \text{par la proposition 1.2.1} \\
&\leq 4^k\gamma_{\mathcal{G}}(n) && \text{par la proposition 1.2.14} \\
&\leq 4^k 128\gamma_{\mathcal{G}}^{\star 8}\left(\frac{5}{6}n + \frac{5t+48}{6}\right) && \text{par (4.7)} \\
&\leq 2^{2k+7}\gamma_{\mathcal{G}}^{\star 8}\left(\frac{5}{6}m\right) && \text{car } \gamma_{\mathcal{G}}^{\star 8} \text{ est croissant et on a (4.8).}
\end{aligned}$$

On a donc pour tout $n \geq t + 10, \gamma_{\mathcal{G}}(n) \leq 2^{2k+7}\gamma_{\mathcal{G}}^{\star 8}\left(\frac{5}{6}m\right)$. Pour les n plus petits, comme $\gamma_{\mathcal{G}}(n) > 0$, on a $\gamma_{\mathcal{G}}(\alpha n) > 0$ pour tout $0 < \alpha < 1$. Donc pour une constante C suffisamment grande, on a

$$\gamma_{\mathcal{G}}(n) \leq C\gamma_{\mathcal{G}}^{\star 8}\left(\frac{5}{6}m\right),$$

pour tout $n \in \mathbb{N}$. On peut donc appliquer le lemme 4.1.2 et on obtient

$$\gamma_{\mathcal{G}} \preceq \exp(\cdot^{\nu}),$$

pour un $\nu < 1$. Ainsi, par la proposition 1.2.18, on a bien $\mathcal{G}$ à croissance sous-exponentielle. $\square$

On a donc bien le résultat annoncé.

Théorème 4.3.1. *Le groupe de Grigorchuk est à croissance intermédiaire.*

Démonstration. Le corollaire 4.3.1 nous donne la croissance superpolynomiale et la proposition 4.3.4 la croissance sous-exponentielle. On conclut par la définition des groupes à croissance intermédiaire. $\square$

Conclusion

Au cours de ce mémoire, nous avons étudié un invariant quasi-isométrique : le taux de croissance. Nous avons vu que cette notion géométrique était intimement liée aux propriétés algébriques des groupes. Le théorème de Gromov illustre parfaitement cette notion. Il caractérise les groupes virtuellement nilpotents à partir de leur taux de croissance. Une piste logique pour poursuivre l'exploration de la théorie géométrique des groupes serait de travailler la preuve originale du théorème de Gromov et les concepts qui en sont nés.

On a également montré que la croissance des groupes peut avoir un comportement plus compliqué qu'il n'y paraît. En effet, le groupe de Grigorchuk $\mathcal{G}$ est à croissance intermédiaire, c'est-à-dire qu'asymptotiquement, sa croissance ne se comporte ni comme une exponentielle, ni comme un polynôme.

Même si beaucoup de questions historiques ont été résolues,le domaine de la croissance des groupes reste fécond en recherche fondamentale. Certaines questions ouvertes peuvent sembler surprenantes. Par exemple, on ne sait pas s'il existe un $\alpha \in]0,1[$ tel que

$$\gamma_{\mathcal{G}} \approx \exp(\cdot^{\alpha}).$$

Un autre problème ouvert s'appelle la conjecture du gap, elle est due à Grigorchuk en 1991, dans [Gri91].

Conjecture. *Soit G un groupe de type fini. Si $\gamma_G \prec \exp(\sqrt{\cdot})$, alors G est à croissance polynomiale.*

En d'autres termes, il y aurait un "trou" entre les groupes à croissance polynomiale et les groupes à croissance $\exp(\sqrt{\cdot})$. Remarquons qu'on ne sait pas non plus s'il existe des groupes dont la croissance est équivalente à $\exp(\sqrt{\cdot})$. Dans [Gri14], Grigorchuk donne plusieurs classes de groupes pour lesquels la conjecture du gap est vraie. En réalité, il espère même montrer un résultat plus fort.

Conjecture. *Pour tout groupe G de type fini, si γ est une fonction de croissance, on a*

$$G \text{ à croissance superpolynomiale } \Leftrightarrow \exp(\sqrt{\cdot}) \preceq \gamma.$$

Autrement dit, $\exp(\sqrt{\cdot})$ est une borne inférieure des groupes à croissance superpolynomiale. La résolution de cette conjecture changera la compréhension que l'on a des groupes.

On peut donc conclure ce mémoire l'esprit tranquille. Bien que beaucoup de développements mathématiques autour de la croissance des groupes ont été faits, on n'a pas fini de l'explorer.

Annexe A

Groupes libres

Les groupes libres font partie des groupes les plus étudiés en théorie géométrique des groupes. Leur propriété universelle permet de comprendre pourquoi. Cette annexe a pour vocation de définir ces groupes et de démontrer leur propriété universelle.

Soit X un ensemble de lettres. Un mot w sur $A := X \cup X^{-1}$ est *réduit* s'il ne contient dans ces facteurs de deux lettres aucun mot de la forme xx^{-1} ou $x^{-1}x$. La *réduction* d'un mot est la suppression de tous ces facteurs. On remarque que si on itère la réduction sur un mot w, la suite de mots obtenue se stabilise car, à chaque itération, soit on diminue la longueur de w ou alors w reste inchangé. On appelle cette limite le *simplifié* de w et on la note $s(w)$. On définit également l'ensemble $F(X)$ des mots réduits de A^*.

Définition A.0.1. Soit X un ensemble de lettres. Le *groupe libre sur X* est l'ensemble $F(X)$ muni de l'opération $*$ qui à tout couple (w, w') associe le simplifié de la concaténation de w et w'. On appelle $|X|$ le *rang* de $F(X)$.

Il est clair que c'est un groupe. En effet, le mot vide ε est clairement neutre. Nous le noterons dorénavant 1. De plus, comme $s(ww') = s(s(w)s'(w'))$ pour tout $w, w' \in A^*$, on a pour tout $w_1, w_2, w_3 \in F(X)$,

$$w_1 * (w_2 * w_3) = w_1 * s(w_2w_3) = s(w_1w_2w_3) = s(w_1w_2) * w_3 = (w_1 * w_2) * w_3.$$

Pour finir, pour tout $w = w_1...w_n \in F(X)$, $w_n^{-1}...w_1^{-1} \in F(X)$ en prenant pour convention que $(x^{-1})^{-1} = x$ pour tout $x \in X$. Il est clair aussi que $(w_1...w_n) * (w_n^{-1}...w_1^{-1}) = s(w_1...w_nw_n^{-1}...w_1^{-1}) = 1$. Donc $F(X)$ est bien un groupe.

Cette manière de voir les groupes libres n'est pas nécessairement la plus optimale car elle ne permet pas de donner du sens à des expressions non réduites. Pour leur donner du sens, on introduit la relation d'équivalence suivante.

Définition A.0.2. On définit la relation d'équivalence $\sim$ sur A^* par $w \sim w'$ si le simplifié de w coïncide avec le simplifié de w'.

Proposition A.0.1. *Pour X un ensemble de lettres,*

$$\varphi : F(X) \to \frac{A^*}{\sim} : w \mapsto [w]$$

avec $A = X \cup X^{-1}$ est une bijection.

Démonstration. Construisons l'inverse de φ :

$$\psi : \frac{A^*}{\sim} \to F(X) : [w] \mapsto s(w).$$

Il est clair que $s(w)$ est dans $F(X)$ et que, pour tout $w' \sim w, s(w') = s(w)$ donc ψ est bien défini. On a aussi immédiatement $\psi \circ \varphi = \mathrm{id}_{F(X)}$. Comme $s(w) \sim w$, on a également $\varphi \circ \psi = \mathrm{id}_{\frac{A^*}{\sim}}$. □

Cette proposition justifie que l'on considère le groupe libre comme étant $\left(\frac{A^*}{\sim}, \cdot\right)$ avec $A = X \cup X^{-1}$ et $[w] \cdot [w'] = [s(w) * s(w')]$. On remarque que $[w] \cdot [w'] = [w \cdot w']$. En effet, on a $s(s(w) \cdot s(w')) = s(ww')$ donc $s(w) * s(w') = s(w) \cdot s(w') \sim s(ww') \sim ww'$.

Cela permet de donner un sens à des éléments du groupe qui ont des occurrences de facteurs de la forme xx^{-1} ou $x^{-1}x$, ce qui est utile en pratique.

On ne peut pas terminer une discussion introductive sur les groupes libres sans parler de leur propriété universelle et de son corollaire : les groupes de type fini sont des quotients du groupe libre.

Proposition A.0.2 (Propriété universelle des groupes libres)**.** *Soit X un ensemble de lettres, G un groupe et $\varphi : X \to G$ une application. Il existe un unique prolongement $\Phi : F(X) \to G$ de cette application qui soit un morphisme de groupes.*

Démonstration. Posons $A = X \cup X^{-1}$. On prolonge φ sur $F(X)$ en posant

1. $\Phi(1) = 1$
2. $\Phi(x^{-1}) = \Phi(x)^{-1}$ pour tout $x \in X$
3. $\Phi(w) = \Phi(w_1)...\Phi(w_n)$ pour tout $w = w_1...w_m \in F(X)$

Ce Φ est trivialement un prolongement morphique de φ. Il est unique car chacun des points de sa définition doivent être satisfaits pour que ce soit un morphisme ou pour que ce soit un prolongement de φ. □

Corollaire A.0.1. *Tout groupe est le quotient d'un groupe libre.*

Démonstration. Soient G un groupe et X un système de générateurs de G.[1] On pose $\varphi = \mathrm{id}_X$ et on sait qu'il existe $\Phi : F(X) \to G$ un morphisme tel que $\Phi(x) = x$ pour tout $x \in X$. On en tire que Φ est surjectif et donc par le premier théorème d'isomorphisme, on a

$$\frac{F(X)}{\ker \Phi} \cong G.$$

□

1. On peut toujours trouver un tel X car $X = G$ convient.

Annexe B

Normes d'espaces vectoriels de dimension finie

Cette annexe s'occupe de démontrer que, sur un espace vectoriel de dimension finie, toutes les normes sont équivalentes. Cette propriété nous a servi dans la démonstration du théorème de Gromov. Elle implique que les topologies induites par deux normes distinctes sont les mêmes. Cela permet d'avoir à disposition les résultats de topologie euclidienne.

Proposition B.0.1. *Soit V un $\mathbb{K}$-espace vectoriel, où $\mathbb{K}$ est un champ. Toutes les normes sur V sont équivalentes, c'est-à-dire, pour deux normes $|\cdot|$ et $\|\cdot\|$, il existe $c, C \in \mathbb{R}_0^+$ tels que, pour tout $v \in V$,*

$$c|v| \leq \| v \| \leq C|v|.$$

Démonstration. Il est suffisant de montrer que toute norme $\|\cdot\|$ est équivalente à la norme $||\cdot||_2$ donnée par :

$$\| v \|_2 = \sqrt{\sum_{j=1}^{n} v_j^2}$$

pour tout $v \in V$, avec $B = \{b_1, ..., b_n\}$ une base de V telle que $\| b_j \| = 1$ pour tout j et $(v_1, ..., v_n)$ la décomposition de v dans cette base. La première constante se trouve à partir de l'inégalité triangulaire :

$$\begin{aligned}
\| v \| &= \| \sum_{j=1}^{n} v_j b_j \| \\
&\leq \sum_{j=1}^{n} \| v_j b_j \| \\
&\leq \sum_{j=1}^{n} |v_j| \, \| b_j \| \\
&\leq \sqrt{\left(\sum_{j=1}^{n} |v_j|^2\right)} \sqrt{\left(\sum_{j=1}^{n} \| b_j \|^2\right)} \\
&\leq \sqrt{n} \sqrt{\sum_{j=1}^{n} v_j^2} \\
&\leq \sqrt{n} \, \| v \|_2
\end{aligned}$$

pour tout $v \in V$.

Montrons que $\| \cdot \|$ est continu[1] sur V. Fixons $v \in V$ et $\varepsilon > 0$, on a

$$\| v - w \|_2 < \frac{\varepsilon}{2\sqrt{n}} \Rightarrow | \, \| v \| - \| w \| \, | < \varepsilon.$$

En effet,

$$\begin{aligned}
| \, \| v \| - \| w \| \, | &\leq \| v - w \| \\
&\leq \sqrt{n} \, \| v - w \|_2 \\
&< \sqrt{n} \frac{\varepsilon}{2\sqrt{n}} = \varepsilon
\end{aligned}$$

On sait que $S = \{v \in V | \, \| v \|_2 = 1\}$ est compact. Ainsi, par continuité de $\| \cdot \|$, il existe un point u de S tel que $m := \| u \|$ est minimal. On sait donc que, pour tout $v \in S$,

$$m \leq \| v \| .$$

On en tire que, pour tout $v \in V$ non-nul,

$$\begin{aligned}
&m \leq \left\| \frac{v}{\| v \|_2} \right\| \\
\Leftrightarrow &m \, \| v \|_2 \leq \| v \| .
\end{aligned}$$

On peut donc conclure. □

1. Au sens de la distance d donnée par $d(v_1, v_2) = \| v_1 - v_2 \|_2$.

Annexe C

Problème de Burnside

Le contenu de cette section est tiré majoritairement de [Hud06] et, dans une moindre mesure, de [Gri14].

Définition C.0.1. Soit G un groupe. On dit que G est *périodique* si chacun de ses éléments est d'indice fini. Autrement dit, si pour tout $g \in G$, il existe un naturel n tel que $g^n = 1$.

Cette définition permet d'énoncer le problème de Burnside :

Est-ce que tous les groupes finiment engendrés périodiques sont finis ?

La question fut posée par William Burnside en 1902 dans [Bur02]. C'est en 1964 que Golod et Shafarevich trouvent un exemple d'un groupe infini finiment engendré périodique dans [Gol64]. Beaucoup de variantes de ce problème existent. Certaines sont restées sans réponse jusque dans les années 90. Certaines sont toujours ouvertes. Par exemple, on ne sait pas s'il existe un groupe G infini engendré par deux éléments tel que, pour tout $g \in G$, $g^5 = 1$.

Nous allons montrer que le groupe de Grigorchuk $\mathcal{G}$ est une solution au problème de Burnside. Nous avons déjà établi dans le chapitre 4 qu'il est finiment engendré et infini. Il reste donc à montrer que tous ses éléments sont d'ordre fini.

Lemme C.0.1. *Soient G un groupe, n un naturel et $g \in G$. On a*

$$g^n = 1 \Leftrightarrow \exists a \in G : g^a = 1.$$

Théorème C.0.1. *Pour tout élément $g \in \mathcal{G}$, il existe m tel que $g^{2^m} = \mathtt{I}$.*

Démonstration. On sait que le résultat est vrai pour les éléments de longueur 0 et 1, vu la proposition 4.2.1 et le fait que $a^2 = 1$. Cette même proposition nous donne $bcd = \mathtt{I}$. Cela nous permet d'affirmer que, si un élément est de longueur 2, alors il contient un a. On a déjà prouvé, à la proposition 4.2.2, que $(ad)^{2^2} = (ac)^{2^3} = (ab)^{2^4} = \mathtt{I}$. On en tire évidemment, $(da)^{2^2} = (ca)^{2^3} = (ba)^{2^4} = \mathtt{I}$. Donc on a le résultat pour tout élément de longueur plus petite que 2. Pour la suite, on procède par récurrence sur $k = |g|$. Fixons $(a)g_1ag_2a...ag_n(a)$ un représentation réduite de g.

Le cas où k est impair se traite facilement. En effet, dans ce cas, g est de type 1 ou 4. S'il est de type 1, $g = g'^a$ avec $|g'| < |g|$. Par le lemme C.0.1 et l'hypothèse d'induction, on a l'existence d'un naturel m tel que $g^{2^m} = 1$. Si g est de type 4, soit $g_1 = g_n$ donc g est conjugué à un élément plus court. Soit on a $g^{g_1} = ag_2...ag'_n$ avec $g'_n \in \{b, c, d\} \setminus \{g_1, g_n\}$. Encore une fois, dans ce cas, on a réussi à se ramener à une longueur plus courte.

Passons au cas où k est impair. On subdivise ce cas-ci en deux cas distincts :

1. Si n est pair ; Dans ce cas, on peut parenthèser la décomposition réduite comme suit : $(ag_1a)g_2...(ag_{n-1}a)g_n$. On voit aussi que $g \in \mathcal{H}$ car il y a un nombre pair de a. Ainsi, en appliquant ψ à g, on obtient un couple (α, β) tel que $|\alpha|, |\beta| \leq n < k$. En effet, $\psi(x^a)$ renvoie un couple d'éléments de longueur 1 pour tout $x \in \{b, c, d\}$, vu la preuve du lemme 4.2.3. Par induction, on peut donc trouver p et q tels que $\alpha^{2^p} = \beta^{2^q} = \mathtt{I}$. Or, pour tout j, $g^j = \varphi(\alpha^j, \beta^j)$. On a donc
$$g^{2^{p+q}} = \varphi\left(\left(\alpha^{2^p}\right)^{2^q}, \left(\beta^{2^q}\right)^{2^p}\right) = \varphi(\mathtt{I}, \mathtt{I}) = \mathtt{I}\,.$$

2. Si n est impair ; Dans ce cas-ci, g n'est pas dans le groupe fondamental $\mathcal{H}$. Cependant, g^2 y est. De plus, on peut parenthèser la décomposition (pas nécessairement réduite) de g^2 comme suit :
$$(ag_1a)g_2...(ag_na)g_1(ag_2)...g_n.$$
Comme pour le cas (1), on peut appliquer ψ à g^2 et on obtient (α, β) tels que $|\alpha|, |\beta| \leq 2n = k$. Il nous reste un dernière étude de cas à faire pour conclure :
   (a) Si $d \in \{g_1, ..., g_n\}$, alors d et d^a sont réécrits par ψ et donc ce d sera effacé une fois dans α et une fois dans β. Ainsi, $|\alpha|, |\beta| < k$ et on peut appliquer l'hypothèse de récurrence. De la même manière que dans le cas 1, on en tire qu'il existe m tel que
   $$\mathtt{I} = \left(g^2\right)^{2^m} = g^{2^{m+1}}.$$
   (b) Si $d \notin \{g_1, ..., g_n\}$ et $c \in \{g_1, ..., g_n\}$, alors comme c apparait une fois seul et une fois dans c^a, on sait que α et β contiennent un d. Ainsi, si $|\alpha|$ ou $|\beta|$ est égal à k, il contient du d. Or, le cas des décompositions réduites de longueur k contenant du d a été traité. On peut donc conclure qu'il existe p, q tels que $\alpha^{2^p} = \beta^{2^q} = \mathtt{I}$ et donc qu'il existe m tel que
   $$\mathtt{I} = \left(g^2\right)^{2^m} = g^{2^{m+1}}.$$
   (c) Si $c, d \notin \{g_1, ..., g_n\}$, alors $g = (ab)^m$. Par la proposition 4.2.2, on en tire que
   $$g^{2^4} = ((ab)^m)^{2^4} = \left((ab)^{2^4}\right)^m = \mathtt{I}^m = \mathtt{I}\,.$$

On a épuisé tous les cas. On peut donc conclure la démonstration. □

Le groupe de Grigorchuk est donc bien un groupe infini finiment engendré périodique. Le problème de Burnside est donc résolu.

Index

Bibliographie

[ABR01] Sheldon Axler, Paul Bourdon et Wade Ramey : *Harmonic Function Theory*, chapitre 2, pages 31–32. Springer New York, NY, 2001.

[Bur02] William Burnside : On an unsettled question in the theory of discontinuous groups. *Quart.J.Math.*, 33:230–238, 1902.

[DK18] Cornelia Drutu et Michael Kapovich : *Geometric Group Theory*, volume 63 de *American Mathematical Society colloquium publications*. American Mathematical Society, Providence, Rhode Island, 2018.

[DK20] Karel De Kimpe : *Group Theory.* KULeuven, 2020.

[DlCM13] Carlos A. De la Cruz Mengual : Geometric group theory seminar : On shalom–tao's non-quantitative proof of gromov's polynomial growth theorem. ETH Zürich, novembre 2013.

[Gol64] Evgenii Solomonovich Golod : On nil algebras and finitely residual groups. *Izv. Akad. Nauk SSSR. Ser. Mat.*, pages 273–276, 1964.

[GP08] Rotislav Grigorchuk et Igor Pak : Groups of intermediate growth : an introduction for beginners. *L´Enseignement Mathématique*, 2:251–272, 2008.

[Gri83] Rotislav Grigorchuk : On the milnor problem of group growth. *Dokl. Akad. Nauk SSSR*, 271:30–33, 1983.

[Gri85] Rotislav Grigorchuk : Degrees of growth of finitely generated groups, and the theory of invariant means. *Math. USSR*, 25:259–300, avril 1985.

[Gri91] Rostislav Grigorchuk : On growth in group theory. *In Proceedings of the International Congress of Mathematicians*, volume 1, pages 325–338, Kyoto, 1991. Math. Soc. Japan.

[Gri14] Rostislav Grigorchuk : *Milnor's problem on the growth of groups and its consequences*, pages 705–774. Princeton University Press, 2014.

[Gro81] Mikhael Gromov : Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.*, 53:53–73, 1981.

[Han16] Georges Hansoul : *Algèbre II.* Uliege, 2016.

[Hud06] Drew A. Hudec : On the burnside problem, 2006.

[Lan19] Juan Lanfranco : An introduction to quasi-isometry and hyperbollic groups. Mémoire de D.E.A., University of Pennsylvania, 2019.

[Man12] Avinoam Mann : *How Groups Grow.* Numéro 395 de London Mathematical Society Lecture Note Series. Cambridge University Press, 2012.

[Mil68a] John Milnor : A note on curvature and fundamental group. *J. Differential Geometry*, 2:1–7, 1968.

[Mil68b] John Milnor : Problem 5603. *Amer. Math. Monthly*, 75:685–686, 1968.

[Rig09] Michel Rigo : *Théorie des graphes.* Ulg, 2009.

[Sch55] Albert Schwarz : A volume invariant of covering. *Dokl. Akad. Nauj SSSR*, 105:32–34, 1955.

[ST10] Yehuda Shalom et Terrence Tao : A finitary version of gromov's polynomial growth theorem. *Geom. Funct. Anal.*, 20:1502–1547, 2010.

[Tao10] Terrence Tao : A proof of Gromov's theorem. `https://terrytao.wordpress.com/2010/02/18/a-proof-of-gromovs-theorem/`, février 2010. Blog ; consulté le 20/05/2022.

[Tao14] Terrence Tao : *Hilbert's Fifth Problem and Related Topics*, volume 153 de *Graduate Studies in Mathematics*, chapitre 1-Introduction, pages 1–20. American Mathematical Society, Providence, Rhode Island, 2014.