TER
Croissance dans les groupes

RANGUIS Célian
encadré par
DAHMANI François



Institut Fourier
M1 Mathématiques générales 2025-2026

Table des matières

1 Introduction **2**

2 Généralités sur la croissance **4**
2.1 Premières définitions 4
2.2 Généralités sur les fonctions de croissances dans les espaces métriques 6
2.2.1 Fonctions de croissances 6
2.2.2 Espaces métriques et quasi-isométries 7
2.2.3 Applications aux groupes 10
2.3 Types de croissances dans les groupes 13

3 Exemples pour différents types de croissance **17**
3.1 Croissance polynomiale : le groupe de Heisenberg discret $\mathcal{H}_3(\mathbb{Z})$ 17
3.2 Croissance exponentielle : le groupe libre 19
3.2.1 Construction partielle 20
3.2.2 Croissance 21

4 Croissance intermédiaire – Premier groupe de Grigorchuk **21**
4.1 Construction et premiers résultats 22
4.1.1 Graphes, arbres, sous-arbres 22
4.1.2 Automorphismes 24
4.1.3 Définition du groupe de Grigorchuk et premiers résultats 28
4.2 Croissance super-polynomiale 34
4.3 Croissance sous-exponentielle 36
4.3.1 Décompositions réduites 36
4.3.2 Sous groupe $\mathbb{H}_3$ et croissance 38

1 Introduction

Croissance

Étant donné un groupe de type fini G et une partie génératrice finie S, il est possible d'étudier l'application croissance :

$$\begin{aligned}\beta(G,S,\cdot) : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto |\{s_1 \cdots s_k \mid k \leq n, s_1, \dots s_k \in S \cup S^{-1}\}| \\ &= \text{nombre d'éléments de } G \text{ atteignables par des} \\ &\quad \text{mots de longueurs au plus } n \text{ sur } S \cup S^{-1}\end{aligned}$$

On s'intéresse en particulier à l'asymptotique de cette fonction. Trois cas sont possibles :

— β est asymptotiquement exponentielle

— β est asymptotiquement polynomiale

— β est asymptotiquement sous-exponentielle, mais non polynomiale. La croissance est alors dite intermédiaire.

Par exemple, le groupe additif $\mathbb{Z}$ muni de la partie génératrice $\{1\}$ a une fonction de croissance linéaire : $n \mapsto 2n+1$ (Exemple 2.1.5).
De la même manière, on peut montrer que $\mathbb{Z}^k$ muni de $\{0,1\}^k$ a une fonction de croissance polynomiale, précisément $n \mapsto (2n+1)^k$ (Proposition 2.2.16).

Nous verrons que le type de croissance (mais pas la fonction de croissance) est indépendant de la partie génératrice (Corollaire 2.2.12). En conséquence, on parlera souvent directement du type de croissance d'un groupe (de type fini) sans préciser de partie génératrice.

Histoire et motivations

Pour une version plus détaillée de ce paragraphe, voir Grigorchuk [5, 2013].

L'étude de cette notion trouve ses premières motivations dans un théorème de Milnor en 1968 :

Théorème 1.1: Milnor *[8, 1968]*

— Soit X une variété riemannienne complète dont la courbure de Ricci est partout positive. Alors tout sous groupe de type fini de son groupe fondamental est à croissance polynomiale.

— Soit X une variété riemannienne compacte dont toutes les courbures sectionnelles sont strictement négatives. Alors son groupe fondamental est à croissance exponentielle.

L'étude des variétés riemannienne, de leurs courbures et des groupes fondamentaux va au delà des objectifs de ce mémoire. Nous ne définirons pas les notions en jeux dans ce théorème et ne les réutiliserons pas, l'auteur ne les maitrisant pas.
On mentionne simplement que le groupe fondamental est un invariant par homéomorphisme permettant de distinguer certaines variétés non homéomorphes les unes des autres. Le théorème de Milnor indique, qu'en plus, il contient une information géométrique sur la courbure. Par exemple, une variété ne pourra se munire de deux structures différentes de variété riemannienne dont l'une est à *courbure de Ricci* partout positive, et l'autre à *courbures sectionnelles* toutes strictement négatives.

Cet article va déclencher une grande vague de recherche sur le sujet. La même année, Wolf [12, 1968] démontre que les groupes virtuellement nilpotents sont à croissance polynomiale.

Définition 1.2: *Groupes nilpotents et virtuellement nilpotents*

— Soit G un groupe, on définit sa suite centrale descendante par $C^0(G) = G$ et $\forall n \geq 0,\ C^{n+1}(G) = [G, C^n(G)]$. On dit qu'un groupe est nilpotent s'il existe un entier n tel que $C^n(G) = \{1_G\}$.

— Un groupe G est dit virtuellement nilpotent s'il admet un sous groupe d'indice fini qui soit nilpotent.

Théorème 1.3: Wolf *[12, 1968]*

Tout groupe virtuellement nilpotent de type fini est à croissance polynomiale.

La réciproque est conjecturée par Milnor et al. [10, 1968] et démontrée par Gromov [7, 1981].

Théorème 1.4: Gromov *[7, 1981]*
Un groupe est à croissance polynomiale si et seulement s'il contient un sous groupe nilpotent d'indice fini.

La preuve de ce théorème (qui n'est pas présentée dans ce document) a nécessité l'étude approfondie d'une autre classe de groupes : les groupes résolubles.

Définition 1.5: *Groupes résolubles*
- Soit G un groupe, on dit que G est résoluble s'il existe une suite descendante de sous groupes distingués $\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$ telle que pour tout i, G_{i+1}/G_i soit abélien.
- On dit qu'un groupe G est polycyclique s'il existe une telle suite vérifiant en plus que chaque quotient est cyclique. En particulier, un groupe polycyclique est résoluble.

Dans le même article que précédemment, Wolf démontre également :

Théorème 1.6: Wolf *[12, 1968]*
Soit G un groupe polycyclique de type fini, deux cas sont possibles :
- G est virtuellement nilpotent et est donc à croissance polynomiale.
- G n'est pas virtuellement nilpotent et est alors à croissance exponentielle.

Ce résultat, couplé au résultat de Milnor suivant, permet alors de complètement caractériser la croissance des groupes résolubles :

Théorème 1.7: Milnor *[9, 1968]*
Si G est un groupe résoluble non polycyclique de type fini, alors G est à croissance exponentielle.

Corollaire 1.8:
Soit G un groupe résoluble, deux cas sont possibles :
- G est virtuellement nilpotent et est donc à croissance polynomiale
- G n'est pas virtuellement nilpotent. Soit il est polycyclique et le résultat de Wolf donne sa croissance exponentielle, soit il ne l'est pas et le résultat de Milnor donne à nouveau sa croissance exponentielle.

En résumé, un groupe résoluble est à croissance polynomiale s'il est virtuellement nilpotent, et à croissance exponentielle sinon.

Question

Dans ce qui précède, il semble que les groupes ont tous une croissance polynomiale ou exponentielle, la croissance intermédiaire n'apparait jamais. En 1968 déjà, Milnor pose la question de l'existence d'un groupe à croissance intermédiaire (Milnor et al. [10, 1968]).

Cette question trouve une réponse positive lorsque Rotislav Grigorchuk publie sa construction d'un groupe à croissance intermédiaire (Grigorchuk [4, 1983]). Il est possible de construire ce groupe de plusieurs manières, celle que Grigorchuk emploie dans son article introductif "Groups of Intermediate Growth : an Introduction for Beginners"(Grigorchuk et Pak [6, 2006]), et qui semble la plus commune, est basée sur le groupe d'automorphisme de l'arbre binaire infini $\mathcal{T}^{(2)}$.

Le point clé est le caractère autosimilaire de ce groupe.
Considérons σ l'automorphisme qui échange les deux sous arbre de la racine. Il est clair que le groupe d'automorphisme de chacun de ces sous arbre est le même que celui de $\mathcal{T}^{(2)}$. Il est alors assez facile de montrer que $\mathrm{Aut}(\mathcal{T}^{(2)})$ est isomorphe a $\left(\mathrm{Aut}(\mathcal{T}^{(2)}) \times \mathrm{Aut}(\mathcal{T}^{(2)})\right) \rtimes \langle\sigma\rangle$.
De plus, la réciproque de ce morphisme envoie surjectivement chacune des deux copies de $\mathrm{Aut}(\mathcal{T}^{(2)})$ sur $\mathrm{Aut}(\mathcal{T}^{(2)})$.
Un sous groupe quelconque de $\mathrm{Aut}(\mathcal{T}^{(2)})$ n'aura en général pas ce caractère autosimilaire. Cependant, le sous-groupe que construit Grigorchuk le possède également et c'est celui-ci qui fait fonctionner beaucoup de calculs menant à la preuve de sa croissance intermédiaire.

La croissance exacte du groupe n'a été démontré qu'en 2020 par Anna Erschler et Tianyi Zheng.

En utilisant des techniques fines de marches aléatoires sur les groupes, elles ont montré que sa fonction de croissance vérifie $\beta(n) \underset{n\to\infty}{\sim} e^{n^\nu}$ où $\nu \approx 0.7674$ est $\frac{\log 2}{\log \alpha}$ avec α la racine positive de $X^3 - X^2 - 2X - 4$ (Erschler et Zheng [3, 2020]).

En plus de sa croissance intermédiaire, le groupe de Grigorchuk présente de nombreuses autres propriétés intéressantes. Par exemple, il répond par la négative à un problème de Burnside [1, 1902] : il est de type fini, tous ses éléments sont d'ordre fini mais il est infini. En fait, tous ses éléments ont pour ordre une puissance de 2.

Plan

Dans ce document, on commence par détailler les notions d'équivalence des fonctions de croissances, l'indépendance au regard de la partie génératrice ainsi que quelques propriétés utiles.
On présente ensuite des exemples pour chaque type de croissances, notamment le groupe de Heisenberg à croissance polynomiale de degré 4 et le groupe libre à croissance exponentielle.
Enfin, on détaille une construction du groupe de Grigorchuk, une preuve de sa croissance ainsi que la preuve du résultat sur l'ordre de ses éléments.

2 Généralités sur la croissance

Les preuves de cette section sont souvent inspirées de "Topics in Geometric Group Theory"(De la Harpe [2, 2000]). Certaines n'y apparaissent cependant pas et la plupart sont plus détaillées ici.

2.1 Premières définitions

Définition 2.1.1: *Longueur*

Soit G un groupe et S une partie finie de G telle que $G = \langle S \rangle$. La longueur selon S dans G est définie comme :

$$\begin{aligned} l_S : G &\to \mathbb{N} \\ g &\mapsto \inf \left\{ n \in \mathbb{N} \middle| \exists s_1, \dots, s_n \in S^{\pm} \text{ t.q. } g = s_1 \cdots s_n \right\} \end{aligned}$$

Ou $S^{\pm} = S \cup S^{-1}$.
Par convention, on pose $l_S(g) = 0 \iff g = 1_G$.

Cette quantité représente en quelque sort la "taille" d'un élément G, mesurée par le nombre de symboles de $S^{\pm}$ nécessaires à minima pour l'obtenir.

Propriétée 2.1.2:

Soit G un groupe engendré par la partie finie S, alors :

1. $\forall g, h \in G,\ l_S(gh) \leq l_S(g) + l_S(h)$
2. $\forall g \in G,\ l_S(g^{-1}) = l_S(g)$

Preuve :

1. Soit $g, h \in G$, notons $l_S(g) = n$ et $l_S(h) = m$. Soit $a_1, \dots a_n \in S^{\pm}, b_1, \dots b_m \in S^{\pm}$ tels que $g = a_1 \cdots a_n$ et $h = b_1 \cdots b_m$.
   Alors, $gh = a_1 \cdots a_n b_1 \cdots b_m$ et $l_S(gh) \leq n + m$.
2. Si $g = s_1 \cdots s_n$, $g^{-1} = s_n^{-1} \cdots s_1^{-1}$ donc $l_S(g^{-1}) \leq l_S(g)$. Appliquant cela à $g' = g^{-1}$ on obtient le résultat voulu.

□

Ces propriétés nous permettent de définir une distance sur G :

Définition 2.1.3: *Métrique du mot*

La métrique du mot selon S dans G est définie comme :

$$\begin{aligned} d_S : G \times G &\to \mathbb{N} \\ g, h &\mapsto l_S(g^{-1}h) \end{aligned}$$

On vérifie qu'il s'agit bien d'une distance, munissant G d'une structure d'espace métrique.

Preuve :

Soit $g, h, k \in G$

Séparation : $d_S(g,h) = 0 \iff l_S(g^{-1}h) = 0 \iff g^{-1}h = 1_G \iff g = h$

Symétrie : $d_S(h,g) = l_S(h^{-1}g) = l_S((g^{-1}h)^{-1}) = l_S(g^{-1}h) = d_S(g,h)$

Inégalité triangulaire $d_S(g,k) = l_S(g^{-1}k) = l_S((g^{-1}h)(h^{-1}k)) \leq l_S(g^{-1}h) + l_S(h^{-1}k) = d_S(g,h) + d_S(h,k)$

□

À partir de cette distance, on définit l'application croissance :

Définition 2.1.4: *Croissance*

La fonction de croissance de (G,S) est définie par :

$$\begin{aligned} \beta(G,S,\cdot) : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto |\overline{\mathcal{B}}_{d_S}(1_G, n)| \end{aligned}$$

Également, la fonction de croissance sphérique est définie par :

$$\begin{aligned} \sigma(G,S,\cdot) : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto |\mathcal{S}_{d_S}(1_G, n)| \end{aligned}$$

$\overline{\mathcal{B}}_{d_S}(1_G, n)$ désigne la boule fermée de centre 1_G et de rayon n pour la distance d_S, et $\mathcal{S}_{d_S}(1_G, n)$ la sphère de centre 1_G de rayon n pour cette même distance.

Pour illustrer ces notions, traitons un exemple simple :

Exemple 2.1.5: *Groupe monogène*

Considérons le cas $(G,S) = (\mathbb{Z}, \{1\})$, alors : $\forall k \geq 1,\ \sigma(k) = 2$, en particulier $\beta(k) = 1 + \sigma(1) + \cdots \sigma(k) = 2k + 1$. A fortiori, la fonction de croissance de $(\mathbb{Z}, \{1\})$ est affine.

On énonce quelques propriétés simples sur la fonction de croissance :

Propriétée 2.1.6:

1. $\beta(G, S, k + l) \leq \beta(G, S, k)\beta(G, S, l)$
2. $\sigma(G, S, k) \leq 2n(2n - 1)^{k-1}$ si $|S| = n$
3. Si G est infini, β est strictement croissante. Si G est fini, elle est stationnaire sur son cardinal.

Preuve :

1. Soit $g \in \overline{\mathcal{B}}(1_G, k + l)$, on choisit $s_1, \ldots, s_k \in S^{\pm}$ et $s'_1, \ldots, s'_l \in S^{\pm}$ tels que $g = \underbrace{s_1 \cdots s_k}_{g_1} \underbrace{s'_1 \cdots s'_l}_{g_2}$

   Alors, $g_1 \in \overline{\mathcal{B}}(1_G, k)$ et $g_2 \in \overline{\mathcal{B}}(1_G, l)$ et on obtient une surjection $\overline{\mathcal{B}}(1_G, k) \times \overline{\mathcal{B}}(1_G, l) \twoheadrightarrow \overline{\mathcal{B}}(1_G, k + l)$. Passant aux cardinaux, le résultat suit.
2. Il est clair que la croissance (sphérique) de (G,S) est plus faible que celle du groupe libre sur S. Dans la Section 3.2 on en fait une construction partielle et on prouve que sa croissance sphérique est $n \mapsto 2n(2n - 1)^{k-1}$ (Proposition 3.2.5).

3. Supposons que $\exists N \in \mathbb{N}$ t.q. $\beta(N) = \beta(N+1)$. Alors, β est stationnaire, en effet cela veut dire qu'on ne peut former de nouveaux mots en ajoutant un élément de $S^{\pm}$ à un mot de longueur au plus N. De plus,
$$G = \bigcup_{n\in\mathbb{N}} \overline{\mathcal{B}}(1_G, n) = \overline{\mathcal{B}}(1_G, N)$$
donc $|G| = \beta(N)$

□

Note : Dans De la Harpe [2, 2000], le point 2 est énoncé avec β plutôt que σ. Il semblerait qu'il s'agisse d'une erreur.

2.2 Généralités sur les fonctions de croissances dans les espaces métriques

Dans cette section, on introduit une théorie plus générale sur les fonctions de croissance. On commence par introduire les différentes notions d'équivalences, puis on démontre que les fonctions de croissance de (G, S) et (G, T) sont équivalentes.

2.2.1 Fonctions de croissances

Définition 2.2.1: *Fonction de croissance*

Une fonction de croissance est une fonction croissante $\alpha : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$.

Tout ce qui suit s'étend aux fonctions croissantes $\tilde{\alpha} : \mathbb{N} \to \mathbb{R}_+$ en posant $\alpha(t) = \tilde{\alpha}(\lceil t \rceil)$

Définition 2.2.2: *Dominations fortes et faibles*

Soit α_1, α_2 des fonctions de croissances.

— On dit que α_2 domine faiblement α_1 et on note $\alpha_1 \overset{w}{\prec} \alpha_2$ si :
$$\exists A \geq 1, \exists B \geq 0 \text{ t.q. } \forall t \in \mathbb{R}_+ \ \alpha_1(t) \leq A\alpha_2(At + B) + B$$
Si $\alpha_1 \overset{w}{\prec} \alpha_2$ et $\alpha_2 \overset{w}{\prec} \alpha_1$ on dit que α_1 et α_2 sont faiblement équivalentes et on note $\alpha_1 \overset{w}{\sim} \alpha_2$

— On dit que α_2 domine fortement α_1 et on note $\alpha_1 \overset{s}{\prec} \alpha_2$ si :
$$\exists A \geq 1 \text{ t.q. } \forall t \in \mathbb{R}_+ \ \alpha_1(t) \leq \alpha_2(At)$$
Si $\alpha_1 \overset{s}{\prec} \alpha_2$ et $\alpha_2 \overset{s}{\prec} \alpha_1$ on dit que α_1 et α_2 sont fortement équivalentes et on note $\alpha_1 \overset{s}{\sim} \alpha_2$

On vérifie facilement que les dominations sont des relations transitives et réflexives et que les équivalences sont des relations d'équivalences.

Proposition 2.2.3:

Pour deux fonctions de croissance, $\alpha_1 \overset{s}{\prec} \alpha_2 \implies \alpha_1 \overset{w}{\prec} \alpha_2$.
En effet, $\alpha_1(t) \leq \alpha_2(At) \leq A\alpha_2(At)$ donc $B = 0$ donne la domination faible.

Le lemme suivant sera utile plus loin :

Lemme 2.2.4:

Soit α_1, α_2 des fonctions de croissances telles que : $\forall t \geq t_1 \in \mathbb{R}_+, \alpha_2(t) \geq 1$. Soit alors t_0 tel que $\alpha_2(t_0) > 0$. Si $\alpha_1 \overset{w}{\prec} \alpha_2$, il existe $\rho \geq 1$ t.q. $\alpha_1(t) \leq \rho\alpha_2(\rho t)$ pour tous $t \geq t_0$

Preuve :

Soit $A \geq 1, B \geq 0$ tels que

$$\forall t \in \mathbb{R}_+,\ \alpha_1(t) \leq A\alpha_2(At+B)+B$$

Soit $\tilde{t}_1 \geq 1$ tel que

$$\forall t \geq \tilde{t}_1,\ \alpha_2(At+B) \geq 1$$

Alors, pour tous $t \geq \tilde{t}_1$:

$$\begin{aligned}\alpha_1(t) &\leq A\alpha_2(At+B)+B \\ &\leq (A+B)\alpha_2((A+B)t)\end{aligned}$$

Si $\tilde{t}_1 \leq t_0$ on a le résultat avec $\rho = A+B$
Sinon, posons $\rho = \max\left\{A+B, \dfrac{\alpha_1(\tilde{t}_1)}{\alpha_2(t_0)}\right\} \geq 1$
Alors, pour tous $t \in [t_0, \tilde{t}_1]$

$$\alpha_1(t) \leq \alpha_1(\tilde{t}_1) \leq \rho\alpha_2(t_0) \leq \rho\alpha_2(t) \leq \rho\alpha_2(\rho t)$$

Ce qui précède concluant pour $t \geq \tilde{t}_1$, ceci termine la preuve.
□

2.2.2 Espaces métriques et quasi-isométries

On va ici travailler avec des espaces métriques mais tout ce qui est fait se généralise tel quel aux espaces pseudo-métriques (c'est-à-dire sans l'hypothèse de séparation).

Définition 2.2.5:

Soit (X,d) un espace métrique tel que $\forall x \in X, \forall r \geq 0, |\overline{\mathcal{B}}(x,r)| < \infty$. La fonction de croissance de (X,d) au point de base $x_0 \in X$ est la fonction :

$$\begin{aligned}\beta(X,d,x_0,\cdot) : \mathbb{R}_+ &\to \mathbb{R}_+ \\ t &\mapsto |\overline{\mathcal{B}}(x_0,t)|\end{aligned}$$

Remarque 2.2.6:

1. $\beta(X,d,x_0,\cdot)$ est une fonction de croissance au sens de la Définition 2.2.1
2. Si $G = \langle S \rangle$ avec S une partie finie, alors $\beta(G,d_S,1_G,t) = \beta(G,S,\lfloor t \rfloor)$ au sens de la Définition 2.1.4.

Définition 2.2.7:

Un espace métrique (X,d) est dit uniformément localement quasi borné si :

$$\forall t \in \mathbb{R}_+, \sup_{x \in X} |\overline{\mathcal{B}}(x,t)| < \infty$$

À partir d'ici et en l'absence d'indications contraires, tous les espaces métriques considérés sont supposés uniformément localement quasi bornés.

Définition 2.2.8:

Soit $(X_1,d_1),(X_2,d_2)$ des espaces métriques et $f : X_1 \longrightarrow X_2$. On dit que f est une inclusion quasi isométrique si

$$\exists A \geq 1, \exists B \geq 0 \text{ t.q. } \forall x,y \in X_1,\ \frac{1}{A}d_1(x,y) - B \leq d_2(f(x),f(y)) \leq Ad_1(x,y)+B$$

Si de plus

$$\exists C \geq 0, \forall z \in X_2, \exists x \in X_1 \text{ t.q. } d_2(z,f(x)) \leq C$$

on dit que f est une quasi-isométrie.
On dit que (X_1,d_1) est quasi isométrique à (X_2,d_2) s'il existe une quasi-isométrie $X_1 \longrightarrow X_2$

Proposition 2.2.9:

La relation de quasi-isométrie est une relation d'équivalence.

Preuve :

Réflexivité : L'identité est clairement une quasi-isométrie.

Symétrie : On garde les notations de la proposition et on cherche une quasi-isométrie $X_2 \longrightarrow X_1$.

En utilisant l'axiome du choix, on choisit pour tout $z \in X_2$ un élément $g(z) \in X_1$ t.q. $d_2(z, f(g(z))) \leq C$. Ceci définit une application $g : X_2 \longrightarrow X_1$.

Montrons que g est une quasi-isométrie. Soit $z, z' \in X_2$

$$\begin{aligned} d_2(z,z') &\leq d_2(z, f\circ g(z)) + d_2(f\circ g(z), f\circ g(z')) + d_2(f\circ g(z'), z') \\ &\leq C + (Ad_1(g(z), g(z')) + B) + C \end{aligned}$$

D'où

$$d_1(g(z), g(z')) \geq \frac{1}{A} d_2(z,z') - \frac{B+2C}{A} \underbrace{\geq}_{A\geq 1} \frac{1}{A} d_2(z,z') - A(B+2C)$$

De plus,

$$\begin{aligned} \frac{1}{A} d_1(g(z), g(z')) - B &\leq d_2(f\circ g(z), f\circ g(z')) \\ &\leq d_2(f\circ g(z), z) + d_2(z,z') + d_2(f\circ g(z'), z') \\ &\leq d_2(z,z') + 2C \end{aligned}$$

Donc, combinant ces inégalités,

$$\frac{1}{A} d_2(z,z') - A(B+2C) \leq d_1(g(z), g(z')) \leq Ad_2(z,z') + A(B+2C)$$

et g est une inclusion quasi isométrique.

Enfin, pour tout $x \in X_1$ et en notant $z = f(x)$,

$$\begin{aligned} d_1(x, g(z)) &\leq A(d_2(f(x), f(g(z))) + B) \\ &= Ad_2(z, f(g(z))) + AB \\ &\leq A(B+C) \end{aligned}$$

et g est une quasi-isométrie.

Transitivité : Montrons que la composition de deux quasi-isométries en est une :

Soit $(X_i, d_i), i = 1,2,3$ des espaces métriques et $f_1 : X_1 \to X_2,\ f_2 : X_2 \to X_3$ des quasi-isométries. On note A_i, B_i, C_i les constantes correspondantes.

Soit $x, y \in X_1$, on a :

$$\begin{aligned} \frac{1}{A_2}\left(\frac{1}{A_1} d_1(x,y) - B_1\right) - B_2 &\leq \frac{1}{A_2} d_2(f(x), f(y)) - B_2 \\ &\leq d_3(g\circ f(x), g\circ f(y)) \\ &\leq A_2 d_2(f(x), f(y)) + B_2 \\ &\leq A_2\left(A_1 d_1(x,y) + B_1\right) + B_2 \end{aligned}$$

On a donc

$$\frac{1}{A_1 A_2} d_1(x,y) - \left(\frac{B_1}{A_2} - B_2\right) \leq d_3(g\circ f(x), g\circ f(y)) \leq A_1 A_2 d_1(x,y) + (B_1 A_2 + B_2)$$

Mais, puisque $A_2 \geq 1$,

$$\frac{1}{A_1A_2}d_1(x,y) - (A_2B_1 - B_2) \leq \frac{1}{A_1A_2}d_1(x,y) - \left(\frac{B_1}{A_2} - B_2\right)$$

Finalement, en notant $A = A_1A_2$ et $B = B_1A_2 + B_2$:

$$\frac{1}{A}d_1(x,y) - B \leq d_3(g \circ f(x), g \circ f(y)) \leq Ad_1(x,y) + B$$

c'est-a-dire $g \circ f$ est une inclusion quasi isométrique.

Soit $z \in X_3$, puisque g est une quasi-isométrie, $\exists y \in X_2$ t.q. $d_3(z, g(y)) \leq C_2$.
Puisque f est une quasi-isométrie, $\exists x \in X_1$ t.q. $d_2(y, f(x)) \leq C_1$. Alors :

$$\begin{aligned} d_3(z, g \circ f(x)) &\leq d_3(z, g(y)) + d_3(g(y), g \circ f(x)) \\ &\leq C_2 + A_2 d_2(y, f(x)) + B_2 \\ &\leq C_2 + A_2C_1 + B_2 \end{aligned}$$

Posant $C = C_2 + A_2C_1 + B_2$:

$$\forall z \in X_3,\ \exists x \in X_1 \text{ t.q. } d_3(z, g \circ f(x)) \leq C$$

Ainsi, $g \circ f$ est une quasi-isométrie.

□

Proposition 2.2.10:

Soit $(X_1, d_1), (X_2, d_2)$ des espaces métriques, $(x_1, x_2) \in X_1 \times X_2$. Notons $\beta_i = \beta(X_i, d_i, x_i, \cdot)$. S'il existe une inclusion quasi isométrique $f : X_1 \to X_2$, alors $\beta_1 \overset{w}{\prec} \beta_2$.

Preuve :

Soit $A \geq 1, B \geq 0$ tels que

$$\forall x, y \in X_1,\ \frac{1}{A}d_1(x,y) - B \leq d_2(f(x), f(y)) \leq Ad_1(x,y) + B$$

Soit $t > 0, x \in \overline{\mathcal{B}}_1(x_1, t)$, on a :

$$\begin{aligned} d_2(f(x), x_2) &\leq d_2(f(x), f(x_1)) + d_2(f(x_1), x_2) \\ &\leq A\underbrace{d_1(x, x_1)}_{t} + \underbrace{B + d_2(f(x_1), x_2)}_{=:C} \\ &\leq At + C \end{aligned}$$

Par conséquent, $f(\overline{\mathcal{B}}_1(x_1, t)) \subseteq \overline{\mathcal{B}}_2(x_2, At + C)$ puis, passant aux cardinaux, $\forall t \in \mathbb{R}_+, |f(\overline{\mathcal{B}}_1(x_1, t))| \leq \beta_2(At + C)$. Notons que A et C ne dépendent pas de t.

Soit $z \in X_2$, si $f^{-1}(z) = \emptyset, |f^{-1}(z)| = 0$.
Sinon, soit $y \in f^{-1}(z)$. Alors,

$$\forall x \in f^{-1}(z), \frac{1}{A}d_1(x,y) - B \leq d_2(f(x), f(y)) = d_2(z,z) = 0$$

puis

$$\forall x \in f^{-1}(z), d_1(x,y) \leq AB \implies f^{-1}(z) \subseteq \overline{\mathcal{B}}_1(y, AB) \implies |f^{-1}(z)| \leq |\overline{\mathcal{B}}_1(y, AB)|$$

Or, X_1 est supposé uniformément localement borné donc $D = \sup_{y' \in X_1} |\overline{\mathcal{B}}_1(y', AB)| < \infty$ et $\sup_{z \in X_2} |f^{-1}(z)| \leq D$. À nouveau, on remarque que D ne dépend pas de t.

Finalement, pour tout $t \in \mathbb{R}_+$:

$$\begin{aligned} \overline{\mathcal{B}}_1(x_1,t) &\subseteq \bigsqcup_{z\in f(\overline{\mathcal{B}}_1(x_1,t))} f^{-1}(z) \\ \Longrightarrow \beta_1(t) = |\overline{\mathcal{B}}_1(x_1,t)| &\leq \sum_{z\in f(\overline{\mathcal{B}}_1(x_1,t))} |f^{-1}(z)| \leq D|f(\overline{\mathcal{B}}_1(x_1,t))| \leq D\beta_2(At+C) \end{aligned}$$

Finalement, notant $\tilde{A} = \max\{A, D\}$, $\forall t \in \mathbb{R}_+, \beta_1(t) \leq \tilde{A}\beta_2(\tilde{A}t + C) + C$ i.e. $\beta_1 \overset{w}{\prec} \beta_2$.
□

Corollaire 2.2.11:

Si X_1 et X_2 sont quasi isométriques alors $\beta_1 \overset{w}{\sim} \beta_2$

Preuve :

On applique la proposition précédente et la symétrie de la relation de quasi-isométrie.
□

2.2.3 Applications aux groupes

Corollaire 2.2.12:

Soit $G = \langle S_1 \rangle = \langle S_2 \rangle$ avec S_1, S_2 des parties finies. Alors $\beta(G, S_1, \cdot) \overset{w}{\sim} \beta(G, S_2, \cdot)$

Preuve :

Notons $d_i = d_{S_i}$ et $f : (G, d_1) \to (G, d_2)$ l'application identité. Montrons que c'est une quasi-isométrie.
Notons :

$$\begin{aligned} A_1 &= \max\{l_{S_2}(s_1) | s_1 \in S_1\} \\ A_2 &= \max\{l_{S_1}(s_2) | s_2 \in S_2\} \\ A &= \max\{A_1, A_2\} \end{aligned}$$

Soit alors $x, y \in G$ et notons $n_i = d_i(x, y)$. Soit $s_1^1, \ldots, s_n^1 \in S_1^{\pm}, s_1^2, \ldots, s_m^2 \in S_2^{\pm}$ tels que $x^{-1}y = s_1^1 \cdots s_n^1 = s_1^2, \cdots, s_m^2$. Alors :

$$\begin{aligned} \frac{1}{A} d_1(x,y) &= \frac{1}{A} l_{S_1}(x^{-1}y) \\ &= \frac{1}{A} l_{S_1}(s_1^2 \cdots s_m^2) \\ &\leq \frac{1}{A}(l_{S_1}(s_1^2) + \cdots + l_{S_1}(s_m^2)) \\ &\leq \frac{mA_2}{A} \\ &\leq m = d_2(x,y) \end{aligned}$$

De plus,

$$\begin{aligned} d_2(x,y) &= l_{S_2}(x^{-1}y) \\ &= l_{S_2}(s_1^1 \cdots s_n^1) \\ &\leq nA_1 \\ &\leq An = Ad_1(x,y) \end{aligned}$$

Par conséquent, f est une inclusion quasi isométrique.
Remarquons que cela suffirait à obtenir l'équivalence des fonctions de croissance puisque l'argument est symétrique.

On va cependant maintenant montrer que f est en fait une quasi-isométrie i.e :
$\exists C$ t.q. $\forall g \in G, \exists h \in G$ t.q. $d_2(g, f(h)) = d_2(g, h) \leq C$
Or ceci est clair, par exemple avec $C = 1$ et $h = gs$ pour $s \in S$

□

Proposition 2.2.13:
Soit $G_1 = \langle S_1 \rangle$ et $G_2 = \langle S_2 \rangle$ des groupes infinis avec S_1, S_2 finies. Notons $\beta_i = \beta(G_i, S_i, \cdot)$. Alors,

$$\beta_1 \overset{w}{\prec} \beta_2 \iff \beta_1 \overset{s}{\prec} \beta 2$$

Pour prouver cela, on utilise le lemme suivant :

Lemme 2.2.14:
Soit $G = \langle S \rangle$ un groupe infini avec S finie. Notons $\beta = \beta(G, S, \cdot)$. Alors :

$$\forall \rho \geq 1, \exists K \in \mathbb{N} \text{ t.q. } \forall k \geq 1, \rho\beta(\rho k) \leq \rho(Kk)$$

Preuve :

Fixons $k \geq 1$, puisque G est infini, $\exists y \in G$ t.q. $l_S(y) = 6k$
On choisit $s_1, \dots s_{6k} \in S^{\pm}$ tels que $y = s_1 \cdots s_{6k}$
Notons :

$$a = s_1 \cdots s_k$$
$$b = s_1 \cdots s_{5k}$$
$$c = s_1 \cdots s_{3k}$$

Alors : $d(a, b) = 4k$, $d(a, c) = 2k$ et $d(b, c) = 2k$ (sinon aurait $l_S(y) < 6k$).
Par inégalité triangulaire :

$$\forall x \in \overline{\mathcal{B}}(a, k),\ d(x, c) \leq d(x, a) + d(a, c) \leq 3k \text{ (idem pour b)}$$
$$\forall x \in \overline{\mathcal{B}}(a, k),\ d(x, b) \geq d(a, b) - d(a, x) \geq 3k$$

Ce qui implique :

$$\overline{\mathcal{B}}(a, k), \overline{\mathcal{B}}(b, k) \subseteq \overline{\mathcal{B}}(c, 3k) \text{ et } \overline{\mathcal{B}}(a, k) \cap \overline{\mathcal{B}}(b, k) = \emptyset$$

Passant aux cardinaux :

$$|\overline{\mathcal{B}}(a, k)| + |\overline{\mathcal{B}}(b, k)| \leq \beta(3k)$$

Or,

$$\forall g \in G, \forall n \geq 0, |\overline{\mathcal{B}}(g, n)| = |\overline{\mathcal{B}}(1_G, n)$$

En effet, notons

$$f : \overline{\mathcal{B}}(1_G, n) \to \overline{\mathcal{B}}(g, n) \qquad g : \overline{\mathcal{B}}(g, n) \to \overline{\mathcal{B}}(1_G, n)$$
$$h \mapsto gh \qquad h \mapsto g^{-1}h$$

Puisque

$$\forall h \in \overline{\mathcal{B}}(1_G, n), d(g, f(h)) = l_S(g^{-1}gh) = l_S(h) = d(1_G, h) \leq n$$

et

$$\forall h \in \overline{\mathcal{B}}(g, n), d(1_G, g(h)) = l_S(g^{-1}h) = d(g, h) \leq n$$

f et g sont bien définies. De plus, elles sont bien inverses l'une de l'autre d'où l'égalité des cardinaux.

Par conséquent, $2\beta(k) \leq \beta(3k)$ puis par récurrence,

$$\forall k, n \in \mathbb{N}, 2^n\beta(k) \leq \beta(3^n k)$$

.
On choisit alors n tel que $2^n > \lceil \rho \rceil$ et on obtient :

$$\begin{aligned} \rho\beta(\rho k) &\leq \lceil \rho \rceil \beta(\lceil \rho \rceil k) \\ &\leq 2^m \beta(\lceil \rho \rceil k) \\ &\leq \beta(\underbrace{3^m \lceil \rho \rceil}_{K} k) \end{aligned}$$

□

Prouvons alors la Proposition 2.2.13.
Preuve :

Le sens fort implique faible étant toujours vrai, il reste à prouver l'autre.

Supposons que $\beta_1 \overset{w}{\prec} \beta_2$. Soit $A \geq 1, B \geq 0$ tels que

$$\forall t \in \mathbb{R}_+, \alpha_1(t) \leq A\alpha_2(At + B) + B$$

On va utiliser le Lemme 2.2.4. Pour cela, on l'applique à $\alpha_i(t) = \beta_i(\lceil t \rceil)$. Les hypothèses du lemme sont vérifiées pour $t_0 = 0$, donnant :

$$\exists \rho \text{ t.q. } \forall k \geq 0, \beta_1(k) \leq \rho\beta_2(\rho k)$$

Le Lemme 2.2.14 donne

$$\exists K \in \mathbb{N} \text{ t.q. } \forall k \geq 0, \ \beta_1(k) \leq \beta_2(Kk)$$

□

Corollaire 2.2.15:

Soit $G = \langle S_1 \rangle = \langle S_2 \rangle$ avec S_1, S_2 des parties finies. Alors $\beta(G, S_1, \cdot) \overset{s}{\sim} \beta(G, S_2, \cdot)$

Preuve :

On applique le Corollaire 2.2.12 et la Proposition 2.2.13
□

Dans la suite, on ne précise plus si on parle de dominations faibles ou fortes lorsqu'on parle de groupes puisque celle-ci sont équivalentes.

Proposition 2.2.16:

1. Soit G un groupe, H un sous groupe d'indice fini. Alors, G est de type fini si et seulement si H l'est.
2. Supposons G de type fini et notons β_G, β_H les fonctions de croissance de respectivement G et H pour des parties génératrices quelconques. Alors, $\beta_G \sim \beta_H$.
3. Soit S une partie génératrice de G contenant 1_G. Alors $\beta(G^m, S^m, \cdot) = \beta(G, S, \cdot)^m$. En particulier, $\beta_{G^m} \sim \beta_G^m$ pour des parties génératrices quelconques.

Preuve :

1. **Sens direct :** La preuve s'inspire de celle qu'on trouve dans "Topics in Group Theory"(Smith et Tabachnikova [11, 2000]) à la page 151.

   Soit S une partie génératrice finie de G et R un système de représentants de G/H tel que 1_G représente H.
   On remarque que :

$$\forall s \in S, \forall r \in R, \ \exists! r' \in R \text{ t.q. } sr \in r'H$$

Or, $sr \in r'H \iff srH = r'H \iff r'^{-1}srH = H \iff r'^{-1}sr \in H$.
On pose alors $\phi : S \times R \to H$ défini par $\forall (s,r) \in S \times R,\ \phi(s,r) = r'^{-1}sr$.

Montrons que $\phi(S,R)$ est une partie génératrice de H (elle est finie, car S et R le sont).
Soit $h \in H$ et $s_1, \dots, s_n \in S^{\pm}$ tels que $h = s_n \cdots s_1$.
Posons alors la suite finie $(r_i)_{i \in [\![1,n+1]\!]}$ définie par $r_1 = 1_G$ et $\forall i \in [\![1,n]\!],\ r_{i+1}$ est l'unique élément de R t.q. $s_i r_i \in r_{i+1}H$ ou de manière équivalente $s_i r_i H = r_{i+1}H$.

On remarque que $r_{n+1}H = s_n r_n H = s_n s_{n-1} r_{n-1} H = \dots = s_n \cdots s_1 r_1 H = hH = H$ donc, par hypothèse sur le système de représentants R, on a $r_{n+1} = r_1 = 1_G$.
Finalement,

$$h = s_n \cdots s_1 = r_{n+1} s_n (r_n r_n^{-1}) s_{n-1} \cdots (r_2 r_2^{-1}) s_1 r_1 = \underbrace{r_{n+1}^{-1} s_n r_n}_{\phi(s_n, r_n)} \cdots \underbrace{r_2^{-1} s_1 r_1}_{\phi(s_1, r_1)}$$

Et $H = \langle \phi(S,R) \rangle$: H est finiement généré.

Sens réciproque : soit S' une partie génératrice de H et R un système de représentant de G/H, on pose $S = S' \cup R$ et alors $\forall g \in G, \exists r \in R,\ \exists h \in H$ t.q. $g = gh$.
Mais alors $\exists s_1, \dots s_n \in (S')^{\pm}$ t.q. $h = s_1 \cdots s_n$, en particulier $g = r s_1 \cdots s_n$ et $G = \langle S \rangle$.

2. Soit S' une partie génératrice de H et $R = \{r_1, \dots, r_n\}$ un système de représentants de G/H. La preuve de l'item précédent montre que $S = S' \cup R$ est une partie génératrice de G.

   Mais alors, $\mathcal{B}_{S'}(1_H, k) = \mathcal{B}_{S'}(1_G, k) \subseteq \mathcal{B}_S(1_G, k)$ d'où $\beta(G,S,k) \geq \beta(H,S',k)$.

   De plus, $\mathcal{B}_S(1_G,k) \subseteq \bigcup_{i=1}^n r_i \mathcal{B}_{S'}(1_G,k)$. En effet, soit $g \in \mathcal{B}_S(1_G,k)$, il existe un unique couple $(r,h) \in R \times H$ tel que $g = rh$. Mais alors, nécessairement, $h \in \mathcal{B}_{S'}(1_G,k)$ ce qui donne l'inclusion.

   Passant aux cardinaux, on obtient $\beta(G,S,k) \leq n\beta(H,S',k)$

   Finalement, on a bien $\beta(G,S,\cdot) \sim \beta(H,S',\cdot)$. Au regard du Corollaire 2.2.15, ceci est vrai pour toute partie génératrices choisies pour G et H.

3. On vérifie que : $\overline{\mathcal{B}}_{G^m}((1,\dots,1),n) = \overline{\mathcal{B}}_G(1,n)^m$.
   En effet, soit $(g_1, \dots, g_m) \in \overline{\mathcal{B}}_{G^m}((1,\dots,1),n)$.
   Par définition, il existe pour tout $i = 1, \dots, n$ un élément $(g_1^{(i)}, \dots, g_m^{(i)}) \in (S^m)^{\pm} = (S^{\pm})^m$ tel que pour tout $j = 1, \cdots, m,\ g_j = g_j^{(1)} \cdots g_j^{(n)}$ et a fortiori $l_S(g_j) \leq n$ d'où $\overline{\mathcal{B}}_{G^m}((1,\dots,1),n) \subseteq \overline{\mathcal{B}}_G(1,n)^m$.
   Pour l'autre inclusion, on considère $(g_1, \dots, g_m) \in \mathcal{B}_G(1_G,n)^m$. Puisque $1_G \in S$ et quitte à "remplir" avec des 1_G, on peut écrire pour tout $j = 1, \dots, m$: $g_j = g_j^{(1)} \cdots g_j^{(n)}$ avec les $g_j^{(i)} \in S^{\pm}$. Finalement, notant $\tilde{g}_i = (g_1^{(i)}, \dots, g_m^{(i)})$, on obtient $(g_1, \dots, g_m) = \tilde{g}_1 \cdots \tilde{g}_n$ et donc l'inclusion réciproque.

   Passant aux cardinaux, $\beta(G^m, \cdot) = \beta(G,\cdot)^m$ puis le Corollaire 2.2.15 conclut pour l'équivalence pour toutes parties génératrices.

□

2.3 Types de croissances dans les groupes

Définition 2.3.1: *Taux de croissance exponentielle*

Soit $(a_k)_{k \in \mathbb{N}} \in \mathbb{R}_+^{\mathbb{N}}$ une suite croissante. Son taux de croissance exponentielle est :

$$\omega = \limsup_k (a_k)^{1/k} \in [0, \infty]$$

Définition 2.3.2:

Soit $G = \langle S \rangle$ avec S une partie finie. Le taux de croissance exponentielle de (G, S) est :

$$\omega(G, S) = \limsup_k \beta(G, S, k)^{1/k}$$

Puisque $\beta(G, S, \cdot) \geq 1$, $\omega(G, S) \geq 1$ également.
On dit que (G, S) est à croissance :

Exponentielle : si $\omega(G, S) > 1$.

Polynomiale : si $\beta(G, S, k) \prec k^d$ pour $d \in \mathbb{N}$ donné. On vérifiera qu'alors $\omega(G, S) = 1$.

Intermédiaire : si $\omega(G, S) = 1$ mais la croissance n'est pas polynomiale.

Remarque 2.3.3:

1. Si $\omega(G, S) = 1$, on parle de croissance sous exponentielle.
2. On montre plus loin que cette limsup est en fait une limite (Proposition 2.3.7).

Proposition 2.3.4:

Pour tout groupe de type fini $G = \langle S \rangle$, (G, S) est nécessairement d'un et un unique type de croissance parmi exponentielle, polynomiale et intermédiaire.

Preuve :

Si la croissance est polynomiale, $\omega(G, S) = 1$: soit $d \in \mathbb{N}, A \geq 1$ tels que

$$\forall k \geq 0,\ \beta(G, S, k) \leq (Ak)^d$$

Alors,

$$\begin{aligned} \omega(G, S) &= \limsup_k \beta(G, S, k)^{1/k} \\ &\leq \limsup_k (Ak)^{d/k} \\ &= \limsup_k \exp\left(\frac{d}{k} \ln(Ak)\right) = 1 \end{aligned}$$

Or, $\omega(G, S) \geq 1$ donc $\omega(G, S) = 1$
Il est alors clair que les trois cas sont mutuellement exclusifs et couvrent toutes les possibilités.
□

Proposition 2.3.5:

Si $(a_k)_{k\in\mathbb{N}}, (a'_k)_{k\in\mathbb{N}} \in \mathbb{R}_+^{\mathbb{N}}$ sont des suites croissantes et telles que $a_k \overset{w}{\prec} a'_k$. Alors, $\omega > 1 \implies \omega' > 1$.

Preuve :

Soit $A \geq 1, B \geq 0$ t.q. $\forall k \in \mathbb{N},\ \alpha_k \leq A\alpha'_{Ak+B} + B$

$$\alpha_k \leq A\alpha'_{Ak+B} + B$$

$(\alpha_k)_{k\in\mathbb{N}}$ est non bornée : sinon, pour une borne M, on aurait $\omega = \limsup_k(\alpha_k)^{1/k} \leq \limsup_k M^{1/k} = 1$.
Soit donc K tel que $\forall k \geq K, \alpha_k \geq 1$. Alors, pour tous $k \geq K$:

$$1 \leq \alpha'_k \leq A\alpha'_{Ak+B} + B \leq (A + B)\alpha'_{(A+B)k}$$

Notons $C = A + B$.

$$1 < \omega \leq \limsup_k C^{1/k}(\alpha'_{Ck})^{1/k} \leq \limsup_k C^{1/k} \limsup_k (\alpha'_{Ck})^{1/k} = \limsup_k (\alpha'_{Ck})^{1/k}$$

Or, pour tous $N \in \mathbb{N}$

$$\begin{aligned}\sup_{k\geq N}(\alpha'_{Ck})^{1/k} &= \sup_{k\geq N}(\alpha'_{Ck})^{C/Ck}\\ &\leq \sup_{k\geq CN}(\alpha'_k)^{C/k}\\ &\leq \left(\sup_{k\geq CN}(\alpha'_k)^{1/k}\right)^C \xrightarrow[N\to\infty]{} (\omega')^C\end{aligned}$$

Donc $(\omega')^C \geq \omega > 1 \implies \omega' > 1$
□

Proposition 2.3.6:

Le type de croissance d'un groupe de type fini G est indépendant du choix de la partie génératrice choisie.

Preuve :

Soit $G = \langle S\rangle = \langle S'\rangle$ avec S, S' des parties finies.
On rappelle qu'alors $\beta \sim \beta'$ d'après le Corollaire 2.2.15.

Cas 1, $\omega > 1$ **:** La Proposition 2.3.5 donne que (G, S) est à croissance exponentielle implique que (G, S') aussi.

Cas 2, $\omega = 1$ **:** Puisque $\beta' \prec \beta$, les mêmes calculs que dans la Proposition 2.3.5 donnent $1 \leq \omega' \leq \omega^C = 1$, puis $\omega' = 1$.
Or, si $\beta \prec k^d$, $\beta' \prec \beta \prec k^d$ donc si (G, S) est à croissance polynomiale alors (G, S') aussi.

Cas arguments étant symétriques :

$$\begin{aligned}(G,S) \text{ à croissance exponentielle} &\iff (G,S') \text{ à croissance exponentielle}\\ (G,S) \text{ à croissance polynomiale} &\iff (G,S') \text{ à croissance polynomiale}\end{aligned}$$

L'équivalence pour le cas intermédiaire suit du fait qu'un groupe est d'un et un unique type de croissance parmi exponentielle, intermédiaire et polynomiale (Proposition 2.3.4).
□

Proposition 2.3.7:

La limsup définissant ω est une limite :
$\omega(G,S) = \lim_{k\to\infty}(\beta(G,S,k))^{1/k} = \inf_{k\geq 1}\beta(G,S,k)^{1/k}$

Ceci est un corollaire du lemme suivant :

Lemme 2.3.8: *de Fekete*

Soit $\alpha : \mathbb{N} \longrightarrow \mathbb{R}$ telle que $\forall a, b \in \mathbb{N},\ \alpha(a+b) \leq \alpha(a) + \alpha(b)$.
Alors, $\left(\frac{\alpha(k)}{k}\right)_{k\in\mathbb{N}}$ diverge grossièrement vers $-\infty$ ou converge. Dans ce cas : $\lim_{k\to\infty}\frac{\alpha(k)}{k} = \inf_{k\geq 1}\frac{\alpha(k)}{k}$.

Preuve :

Fixons $k \geq 1$ et soit $n \geq k$. La division euclidienne de n par k donne :

$$n = q_n k + r_n \text{ avec } r_n \in \{0, \ldots, k-1\},\ q_n \geq 1$$

Alors,

$$\begin{aligned}\frac{\alpha_n}{n} &= \frac{\alpha(q_n k + r_n)}{n} = \frac{\alpha((q_n-1)k + (k+r_n))}{n} \\ &\leq \frac{q_n - 1}{n}\alpha(k) + \frac{\alpha(k+r_n)}{n}. \quad \text{Or } q_n - 1 = \frac{n-k-r_n}{k} \\ &= \frac{n-k-r_n}{n}\frac{\alpha(k)}{k} + \frac{\alpha(k+r_n)}{n} \\ &\leq \underbrace{\frac{n-k-r_n}{n}}_{\xrightarrow[n\to\infty]{}1}\frac{\alpha(k)}{k} + \underbrace{\frac{1}{n}\max_{i\in\{0,\dots,k-1\}}\alpha(k+i)}_{\xrightarrow[n\to\infty]{}0}\end{aligned}$$

On a donc $\limsup_n \frac{\alpha(n)}{n} \leq \frac{\alpha_k}{k}$ pour tous $k \geq 1$. A fortiori, $\limsup_n \frac{\alpha(n)}{n} \leq \inf_{k\geq 1}\frac{\alpha(k)}{k}$.
Mais $\inf_{k\geq 1}\frac{\alpha(k)}{k} \leq \liminf_n \frac{\alpha(n)}{n}$ donc :

$$\limsup_n \frac{\alpha(k)}{k} \leq \inf_{k\geq 1}\frac{\alpha(k)}{k} \leq \liminf_n \frac{\alpha(k)}{k}$$

Soit finalement :

$$\limsup_n \frac{\alpha(k)}{k} = \liminf_n \frac{\alpha(k)}{k} = \lim_{n\to\infty}\frac{\alpha(k)}{k} = \inf_{k\geq 1}\frac{\alpha(k)}{k}$$

□

Corollaire 2.3.9:

Si $\beta : \mathbb{N} \to \mathbb{R}$ est telle que $\forall a, b \in \mathbb{N},\ \beta(a+b) \leq \beta(a)\beta(b)$.
Alors, $(\beta(k)^{1/k})_{k\geq 1}$ converge et $\lim_{k\to\infty}\beta(k)^{1/k} = \inf_{k\geq 1}\beta(k)^{1/k}$.
En effet, on applique le Lemme 2.3.8 à $\alpha(k) = \log(\beta(k))$.

On en déduit la Proposition 2.3.7.

Lemme 2.3.10:

Soit $\beta : \mathbb{N} \to \mathbb{R}_+$ une fonction de croissance telle que $\forall a, b \in \mathbb{N},\ \beta(a+b) \leq \beta(a)\beta(b)$. Notons $\lambda = \lim_{k\to\infty}(\beta(k))^{1/k}$ son taux de croissance exponentielle.
Alors :

1. $\beta(k) \overset{s}{\prec} e^k$
2. $\beta(k) \overset{s}{\sim} e^k \iff \beta(k) \overset{w}{\sim} e^k \iff \lambda > 1$
3. Soit $v \in]1, +\infty]$, sont équivalentes :
   (a) $\exists c > 0$ t.q. $\forall k \geq 1,\ \beta(k) \geq cv^k$
   (b) $\forall k \geq 1\ \beta(k) \geq v^k$

Preuve :

1. On a par récurrence $\beta(k) \leq \beta(1)^k = \left(e \times \frac{\beta(1)}{e}\right)^k$.
   Notant $\mu = \ln\left(\max\left\{\frac{\beta(1)}{e}, 1\right\}\right) \geq 0$, on obtient :
   $$\beta(k) \leq (e \times e^\mu)^k = e^{(\mu+1)k}$$
   Finalement, $\beta(k) \overset{s}{\prec} e^k$.
2. $\beta(k) \overset{s}{\sim} e^k \implies \beta(k) \overset{w}{\sim} e^k$ est claire. La Proposition 2.3.5 donne $\beta(k) \overset{w}{\sim} e^k \implies \lambda > 1$.
   Il nous reste à montrer $\lambda > 1 \implies \beta(k) \overset{s}{\sim} e^k$. Puisqu'on a déjà vu $\beta(k) \overset{s}{\prec} e^k$, montrons $e^k \overset{s}{\prec} \beta(k)$.
   D'après Corollaire 2.3.9, $\lambda = \inf_{k\geq 1}(\beta(k))^{1/k}$ donc $\forall k \geq 1, \beta(k) \geq \lambda^k$.

De plus, en notant $\mu = \frac{1}{\ln(\lambda)} \ln\left(\max\left\{\frac{e}{\lambda}, 1\right\}\right) = \log_\lambda\left(\max\left\{\frac{e}{\lambda}, 1\right\}\right)$:

$$e^k = \left(\lambda \times \frac{e}{\lambda}\right)^k \leq \lambda^{(1+\mu)k}$$

Car $\lambda > 1$ implique que $k \mapsto \lambda^k$ est croissante.

En conséquence, $e^k \overset{s}{\prec} \lambda^k \overset{s}{\prec} \beta(k)$ ce qui conclut.

3. Soit $v \in]1, +\infty]$
   - $(b) \implies (a)$ est claire
   - Supposons (a) et fixons $k \in \mathbb{N}$, soit $l \in \mathbb{N}^*$. Puisque $\beta(k)^l \geq \beta(kl) \geq cv^{kl}$, on a $\beta(k) \geq c^{1/l} v^k$. Ceci étant vrai pour tout l, on a $\beta(k) \geq (\lim_{l\to\infty} c^{1/l}) v^k = v^k$ ce qui conclut.

□

Corollaire 2.3.11: *Reformulation de la Définition 2.3.2*

Soit $G = \langle S \rangle$ un groupe avec S une partie finie, notons β la fonction de croissance associée. Alors, la définition suivante du type de croissance est équivalente à celle de la Définition 2.3.2.
On dit que G est à croissance :

Exponentielle : si $\beta(k) \geq cv^k$ pour certains $c > 0$ et $v > 1$

Polynomiale : si $\beta(k) \leq ck^d$ pour certains $c > 0$ et $d \geq 1$

Intermédiaire : sinon

Preuve :

Le cas exponentiel est l'application du Lemme 2.3.10. Le cas polynomial est clair. Le cas intermédiaire suit alors immédiatement de la Proposition 2.3.4.
□

3 Exemples pour différents types de croissance

3.1 Croissance polynomiale : le groupe de Heisenberg discret $\mathcal{H}_3(\mathbb{Z})$

On a déjà vu le cas de $\mathbb{Z}$ dans l'Exemple 2.1.5, on exhibe ici un groupe dont la croissance polynomiale est moins claire.

Définition 3.1.1:

On appelle groupe de Heisenberg discret le sous groupe de $GL_3(\mathbb{Z})$ donné par :

$$\mathcal{H}_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & k & l \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; k, l, m \in \mathbb{Z} \right\}$$

Le but de cette partie va être de montrer que ce groupe a une croissance polynomiale de degré 4.

Proposition 3.1.2:

Notons $a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, c = aba^{-1}b^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Alors,

$$\forall k, l, m \in \mathbb{N}, \begin{pmatrix} 1 & k & l \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} = b^m a^k c^l$$

Preuve :

On calcule :

$$\begin{pmatrix}1&\beta&0\\0&1&0\\0&0&1\end{pmatrix}\underbrace{\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}}_{a}=\begin{pmatrix}1&1+\beta&0\\0&1&0\\0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0\\0&1&\alpha\\0&0&1\end{pmatrix}\underbrace{\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}}_{b}=\begin{pmatrix}1&0&0\\0&1&1+\alpha\\0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&\gamma\\0&1&0\\0&0&1\end{pmatrix}\underbrace{\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}}_{c}=\begin{pmatrix}1&0&1+\gamma\\0&1&0\\0&0&1\end{pmatrix}$$

Par récurrence, on obtient

$$a^k=\begin{pmatrix}1&k&0\\0&1&0\\0&0&1\end{pmatrix}$$
$$b^m=\begin{pmatrix}1&0&0\\0&1&m\\0&0&1\end{pmatrix}$$
$$c^l=\begin{pmatrix}1&0&l\\0&1&0\\0&0&1\end{pmatrix}$$

Un dernier calcul donne

$$b^m a^k c^l=\begin{pmatrix}1&k&l\\0&1&m\\0&0&1\end{pmatrix}$$

□

Proposition 3.1.3:

$\beta(\mathcal{H}_3(\mathbb{Z}),\{a,b\},n)\sim n^4$. A fortiori, ceci est vrai pour toute partie génératrice (Corollaire 2.2.15).

Preuve :

Un rapide calcul permet de vérifier que c commute avec a et b.
Soit

$$M=\underbrace{a^{n_1}b^{m_1}\cdots a^{n_r}b^{m_r}}_{\text{pour } l(M)=\sum|n_i|+|m_i|}\in\mathcal{H}_3(\mathbb{Z})$$

On remarque :

$$ab=cba$$
$$a^{-1}b^{-1}=cb^{-1}a^{-1}$$
$$a^{-1}b=c^{-1}ba^{-1}$$
$$ab^{-1}=c^{-1}b^{-1}a$$

On en déduit qu'on peut écrire $M = c^l b^m a^k$ avec

$$\begin{aligned} l &= n_1 m_1 + (n_1 + n_2)m_2 + \cdots + (n_1 + \cdots + n_r)m_r \\ m &= \sum m_i \\ k &= \sum n_i \end{aligned}$$

Si $M \in \mathcal{B}(I_3, n)$, on a par choix que $\sum |n_i| + |m_i| \leq n$ donc $|m|, |k| \leq n$ et $|l| \leq (\sum |n_i|)(\sum |m_i|) \leq n^2$. De plus, l'écriture de M sous la forme $c^l b^m a^k$ est unique donc on a une injection

$$\mathcal{B}(I_3, n) \hookrightarrow \underbrace{\left\{(k, l, m) \in \mathbb{Z}^3 \middle| |m|, |k| \leq n, |l| \leq n^2\right\}}_{\text{card}=(2n+1)^2(2n^2+1)\sim n^4}$$

Par conséquent, $\beta(n) \prec n^4$
Pour la domination réciproque, on va montrer que $l_S(c^l b^m a^k) \leq 24\sqrt{|l|} + |m| + |k|$
On vérifie que $a^i b^j a^{-i} b^{-j} = c^{ij}$ donc $l_S(c^{l^2}) \leq 4|l|$
Soit alors $i = \left\lfloor \sqrt{l} \right\rfloor, j = l - i^2$, on suppose $l \geq 0$ le cas négatif étant similaire. Alors,

$$\begin{aligned} & \sqrt{l} - 1 < i \leq \sqrt{l} \\ \implies & 1 - 2\sqrt{l} + l < i^2 \leq l \\ \implies & 2\sqrt{l} > 2\sqrt{l} - 1 > j \geq 0 \end{aligned}$$

Puis,

$$\begin{aligned} l_S(c^l) &= l_S(c^{i^2+j}) \\ &\leq l_S(c^{i^2}) + l_S(c^j) \\ &\leq 4 l_S(c^i) + j l_S(c) \\ &\leq (4i + j) l_S(c) \\ &\leq 24\sqrt{l} \end{aligned}$$

Et,

$$l_S(c^l b^m a^k) \leq l_S(c^l) + l_S(b^m) + l_S(a^k) \leq 24\sqrt{|l|} + |m| + |k|$$

On a alors que pour tous m, l, k tels que $|m|, |k| \leq \dfrac{n}{3}$ et $|l| \leq \left(\dfrac{n}{72}\right)^2$, on a $l_S(c^l b^m a^k) \leq n$
Or,

$$\begin{aligned} \left| \left\{ m, k, l \in \mathbb{Z} \middle| |m|, |k| \leq \frac{n}{3},\ |l| \leq \left(\frac{n}{72}\right)^2 \right\} \right| &= 8 \left\lfloor \frac{n}{3} \right\rfloor^2 \left\lfloor \left(\frac{n}{72}\right)^2 \right\rfloor \\ &\geq 8 \left(\frac{n}{3} - 1\right)^2 \left(\left(\frac{n}{72}\right)^2 - 1 \right) \\ &\succ n^4 \end{aligned}$$

On a donc $\beta(n) \succ n^4$ et avec ce qui précède $\beta(n) \sim n^4$.
□

3.2 Croissance exponentielle : le groupe libre

Considérons un groupe $G = \langle S \rangle$. Par définition, il est possible d'écrire tout élément de G comme (au moins) un mot sur $S^{\pm}$.
Inversement, pour trouver quel élément du groupe est représenté par un mot sur $S^{\pm}$, on a tout intérêt à le *réduire*, c'est-a-dire à simplifier tous les sous-mots qui représentent 1_G. Naturellement, on aura tous les mots du type ss^{-1} avec $s \in S$. Cependant, on aura souvent d'autres relations. Par exemple, si un élément $s \in S$ est d'ordre n, on peut

simplifier les occurrences de $\underbrace{s \cdots s}_{n \text{ fois}}$.
On peut alors se demander s'il existe un groupe ou les seules relations sont les $ss^{-1} = 1_G$. La réponse est oui : le groupe libre.
Clairement, la fonction de croissance d'un tel groupe sera la plus grande pour le nombre de générateurs considérés.

3.2.1 Construction partielle

Considérons un ensemble S ainsi qu'un autre ensemble S' disjoint de S et équipotent à S qui représentera les inverses.
On fixe une bijection $f : S \to \mathcal{S}'$ et pour tout $s \in S$ on note $s' = f(s)$.
On considère la réunion disjointe $S \cup S'$ et on note $(S \cup S')^*$ l'ensemble des mots sur $S \cup S'$.

Définition 3.2.1: *Mot réduit*

Un mot réduit sur $S \cup S'$ est un élément de $(S \cup S')^*$ qui n'admet pas de sous mot de la forme ss' ou $s's$ avec $s \in S$.

Soit $m \in (S \cup S')^*$ un mot. Pour chaque élément $s \in S$, on retire chaque occurrence de ss' ou de $s's$.
Faisant ceci pour chaque élément de S, on obtient un nouveau mot m'. Bien sûr, ce nouveau mot peut contenir de nouveaux sous-mots simplifiables, par exemple pour $S = \{a, b\}$:

$$abb'a' \xrightarrow{a} abb'a' \xrightarrow{b} aa'$$

ou on peut simplifier aa'.
Cependant, puisque le mot est de longueur finie et que cette longueur est décroissante avec le nombre de réductions, en faisant ceci un nombre fini de fois, on obtient finalement un mot réduit.
On admet que l'ordre des réductions n'a pas d'importance et donc l'unicité du mot réduit pour un mot de départ w fixé, qu'on note $\underline{w}$.

Cette opération de réduction induit une relation d'équivalence sur $(S \cup S')^*$:

Définition 3.2.2:

$m \sim m' \iff \underline{m} = \underline{m'}$ définit une relation d'équivalence sur $(S \cup S')^*$. On note $F(S)$ l'ensemble $(S \cup S')^* / \sim$.

On admet la proposition suivante :

Proposition 3.2.3:

Considérons deux mots $w, w' \in (S \cup S')^*$, alors $\underline{ww'} = \underline{\underline{w}\ \underline{w'}}$.
Par conséquent, la concaténation passe au quotient par $\sim$.

À partir de maintenant, on désigne par $\underline{m}$ la classe de m sous la relation $\sim$.

Les considérations précédentes montrent que $F(S)$ admet la concaténation (passée au quotient) comme loi interne.

Proposition 3.2.4:

$F(S)$ est, muni de la concaténation passée au quotient, un groupe appelé le groupe libre sur S. Son élément neutre est $\underline{\epsilon}$, la classe du mot vide.

Preuve :

> On vérifie facilement que le mot vide est un élément neutre.
>
> Soit $\underline{m} \in F(S)$, $m = s_1 \cdots s_n,\ s \in S \cup S'$. Avec la convention $s'' = s$, on vérifie aisément que $m' = s'_n \cdots s'_1$ est un inverse de m.
>
> L'associativité suit immédiatement de la Proposition 3.2.3
> □

3.2.2 Croissance

Proposition 3.2.5:

Soit, pour $n \geq 2$, $S = \{s_1, \ldots, s_n\}$ un ensemble fini, alors pour tout $k \geq 1$:

$$\sigma(F(S), \{a, b\}, k) = 2n(2n-1)^{k-1}$$
$$\beta(F(S), \{a, b\}, k) = 1 + \frac{n}{n-1}((2n-1)^k - 1)$$

A fortiori, $F(S)$ est à croissance exponentielle.

Preuve :

On commence par σ et on procède par récurrence sur n.

Le cas $k = 1$ est clair (nombre d'éléments de $S \cup S'$).

Supposons le résultat vrai pour un $k \in \mathbb{N}$. Alors, notant $\underline{\epsilon} = 1$:
$\mathcal{S}_{d_s}(1, k+1) = \mathcal{S}_{d_S}(1, k)S^{\pm} = \{ms \mid m \in \mathcal{S}_{d_S}(1, k),\ s \in S^{\pm}\}$.
A fortiori $\sigma(k+1) \leq 2n\sigma(k)$, mais on peut améliorer cette borne.

Soit $m = s_1 \cdots s_k$, puisque $\underline{ms'_k} = \underline{s_1 \cdots s_{k-1}} \in \mathcal{S}(1, k-1)$, on a $\sigma(k+1) \leq (2n-1)\sigma(k)$.

Hors, les seules relations dans le groupe sont les inverses donc, pour tout $s \in S^{\pm} \setminus \{s_k\}$, ms est un mot réduit. A fortiori, $\sigma(k+1) = (2n-1)\sigma(k)$.
Appliquant l'hypothèse de récurrence, on obtient $\sigma(k+1) = 2n(2n-1)^k$ ce qui termine la récurrence.

Ensuite,

$$\begin{aligned}\beta(k) &= \sum_{l=0}^{k} \sigma(l) = 1 + \sum_{l=1}^{k} 2n(2n-1)^{l-1} \\ &= 1 + 2n\sum_{l=0}^{k-1}(2n-1)^l = 1 + 2n\frac{(2n-1)^k - 1}{(2n-1) - 1} \\ &= 1 + n\frac{(2n-1)^k - 1}{n-1} \\ &\underset{k\to\infty}{\sim} (2n-1)^k\end{aligned}$$

Le taux de croissance exponentielle est alors $2n - 1 > 1$ d'où la croissance exponentielle.
□

Remarque 3.2.6:

Si S n'a qu'un seul élément, on trouve $\sigma(k) = 2$. C'est logique puisque dans ce cas $F(S) \simeq \mathbb{Z}$, voir l'Exemple 2.1.5.

4 Croissance intermédiaire – Premier groupe de Grigorchuk

Cette section s'inspire de "Groups of Intermediate Growth : an Introduction for Beginners"(Grigorchuk et Pak [6, 2006]). On détaille cependant des points laissés en vérifications dans celui-ci. Également, on introduit plus en détail les objets considérés (notamment les notions d'arbre et d'automorphismes d'arbres) et certaines preuves sont faites différemment.

4.1 Construction et premiers résultats

4.1.1 Graphes, arbres, sous-arbres

Définition 4.1.1: *Graphe*

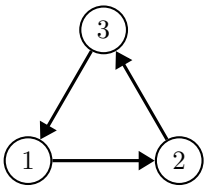
Un graphe (orienté) $\mathcal{G}$ est la donnée d'un couple $\mathcal{G} = (S, A)$ avec

— S un ensemble représentant les sommets du graphe.

— $A \subseteq S \times S$ représentant les arcs du graphe.

Exemple 4.1.2:

Notons $S = \{1, 2, 3\}$ et $A = \{(1, 2), (2, 3), (3, 1)\}$, alors $\mathcal{G} = (S, A)$ est le graphe suivant :



Définition 4.1.3: *Arbre*

Soit $\mathcal{G} = (S, A)$ un graphe, un circuit dans $\mathcal{G}$ est une suite finie $((a_n, b_n))_{n \leq N} \in A^N$ telle que :

$$a_0 = b_N \text{ et } \forall n \leq N - 1,\ b_n = a_{n+1}$$

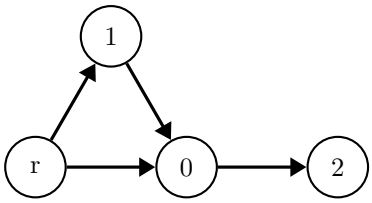
Si $\mathcal{G}$ ne possède pas de circuits, on dit qu'il est acyclique.
Un arbre (enraciné) $\mathcal{T} = (S, A)$ est un graphe acyclique tel que

$$\exists! r \in S \text{ t.q. } \{(a, b) \in A \mid b = r\} = \emptyset \text{ et } \forall s \in S \setminus \{r\}\ \#\{(a, b) \in A \mid b = s\} = 1$$

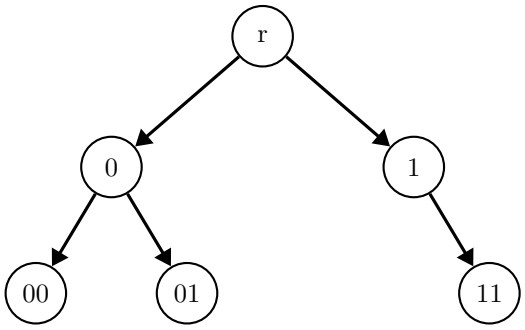
Autrement dit, $\mathcal{A}$ possède un unique sommet sans parents (appelé la racine) et tout autre sommet a exactement un parent.

Exemple 4.1.4:

Le graphe ci-dessous est acyclique mais n'est pas un arbre (0 a deux parents, les autres conditions sont vérifiées).



Le graphe ci-dessous est un arbre.



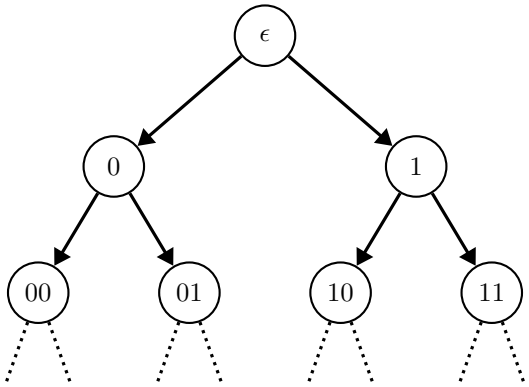


FIGURE 1 – Représentation de l'arbre binaire infini.

Définition 4.1.5: *Arbre binaire infini*

Notons $S = \{0,1\}^*$ l'ensemble des mots fini sur l'alphabet $\{0,1\}$. Notons A le sous ensemble de $S \times S$ défini par $(a,b) \in A \iff b = a0$ ou $b = a1$.
Alors, $\mathcal{T}^{(2)} = (S, A)$ est un arbre appelé arbre binaire infini dont la racine est le mot vide (noté ϵ).
On le représente sur la Figure 1.

Définition 4.1.6:

— Soit $\mathcal{G} = (S, A)$ un graphe, $u, v \in S$ des sommets. La distance entre u et v est :

$$d(u,v) = \begin{cases} \inf\{n \in \mathbb{N} \mid \exists w_1, \dots, w_{n-1} \in S \text{ t.q. } (u,w_1), \dots, (w_n, v) \in A\} & \text{si } u \neq v \\ 0 & \text{si } u = v \end{cases}$$

Remarque : Ce n'est pas une distance au sens usuel du terme si le graphe est orienté (pas de symétrie, potentielles valeurs infinies) ou non connexe (valeurs infinies).

— Soit (S, A) un arbre de racine r. Soit $v \in S$. Le niveau de v est $|v| := d(r, v)$, la distance de la racine r a v. On a bien pris garde d'écrire $d(r, v)$ et pas $d(v, r)$ au vu de la remarque ci-dessus.

Remarque 4.1.7:

Dans $\mathcal{T}^{(2)}$, le niveau d'un sommet est sa longueur comme mot de $\{0,1\}^*$.

Définition 4.1.8:

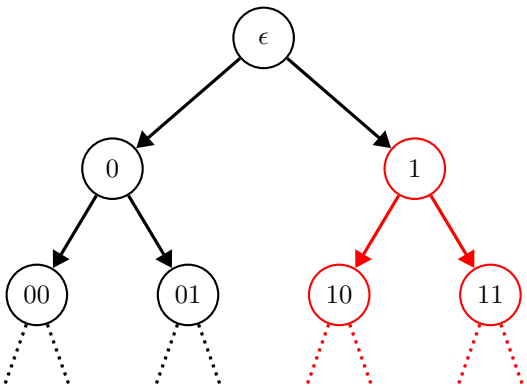
Soit $\mathcal{T} = (S, A)$ un arbre de racine r, soit $v \in S$. On définit le sous arbre de $\mathcal{T}$ enraciné en v par $\mathcal{T}_v = (S_v, A_v)$ avec :

— $S_v = \{u \in S \mid d(v,u) < \infty\}$

— $(u,w) \in A_v \iff u, w \in S_v$ et $(u,w) \in A$

Exemple 4.1.9:

Ci-dessous, on représente en rouge $\mathcal{T}_1^{(2)}$, le sous arbre de $\mathcal{T}^{(2)}$ enraciné en 1.



4.1.2 Automorphismes

Définition 4.1.10: *Morphisme de graphes*

Soit $\mathcal{G} = (S, A), \mathcal{G}' = (S', A')$ deux graphes. On dit que $f : S \to S'$ est un morphisme de graphe si

$$\forall (u, v) \in A,\ (f(u), f(v)) \in A'$$

Si de plus f est bijective et que sa réciproque est un morphisme, on dit que f est un isomorphisme et on note $\mathcal{G} \simeq \mathcal{G}'$. On note $\mathrm{Aut}(\mathcal{G})$ l'ensemble des isomorphismes de $\mathcal{G}$ vers $\mathcal{G}$.

Propriétée 4.1.11:

Soit $\mathcal{T} = (S, A)$ un arbre de racine r, $\tau \in \mathrm{Aut}(\mathcal{T})$. Alors :

- $\tau(r) = r$
- Pour tous $u, v \in S,\ d(u, v) = d(\tau(u), \tau(v))$. En particulier, pour tous $v \in S$, $|\tau(v)| = |v|$.

Preuve :

- Supposons par l'absurde que $\tau(r) = u \in S \setminus \{r\}$.
  Alors, par définition d'un arbre, u admet un parent v i.e. $\exists v \in S$ t.q. $(v, u) \in A$.
  Appliquant τ^{-1} on obtient $(\tau^{-1}(v), r) \in A$ en contradiction avec le fait que r soit la racine.
- Supposons d'abord que $d(u, v) = n < \infty$, soit $w_0, \dots, w_n \in S$ tels que $w_0 = u, w_n = v$ et $(w_i, w_{i+1}) \in A\ \forall i \in \{0, 1, \dots n-1\}$
  $\tau(w_0), \dots \tau(w_n)$ forme un chemin de longueur n reliant $\tau(u)$ à $\tau(v)$ donc $d(\tau(u), \tau(v)) \leq d(u, v)$.
  Appliquant cela à τ^{-1} on obtient l'égalité.
  Le cas ou $d(u, v) = \infty$ est alors clair puisque $\tau^{-1} \in \mathrm{Aut}(\mathcal{T})$. En effet, si $d(\tau(u), \tau(v)) = m < \infty$, ce qui précède donne $m = d(\tau^{-1} \circ \tau(u), \tau^{-1} \circ \tau(v)) = d(u, v) = \infty$ contradiction.

□

Proposition 4.1.12:

Soit $v \in \{0, 1\}^*$, alors $\mathcal{T}^{(2)} \simeq \mathcal{T}_v^{(2)}$.

Preuve :

Puisque $S_v = \{vu \mid u \in \{0, 1\}^*\}$, sont bien définies et inverse l'une de l'autre :

$$\begin{aligned} f_v : \{0,1\}^* &\to S_v & \qquad g_v : S_v &\to \{0,1\}^* \\ u &\mapsto vu & vu &\mapsto u \end{aligned}$$

Soit $(u, w) \in A$, ce qui équivaut à $w = u\alpha, \alpha \in \{0, 1\}$, on a :

$$(f_v(u), f_v(w)) = (vu, vu\alpha) \in A_v$$

En conséquence, f_v est un morphisme.
Soit $(u', w') \in A_v$, ce qui équivaut à $u' = vu, w' = vu\alpha, \alpha \in \{0, 1\}$, on a :

$$(g_v(u'), g_v(w')) = (u, u\alpha) \in A$$

En conséquence, g_v est un morphisme.

Finalement, il y a bien un isomorphisme entre $\mathcal{T}^{(2)}$ et $\mathcal{T}_v^{(2)}$.
□

Définition 4.1.13:

Dans la suite, l'isomorphisme f_v de la preuve ci-avant sera noté $\imath_v$.

Définition 4.1.14:

On définit $a \in \mathrm{Aut}(\mathcal{T}^{(2)})$ par $a(1u) = 0u$ et $a(1u) = 0u$ pour tous $u \in \{0, 1\}^*$.
On illustre son effet sur la Figure 2.

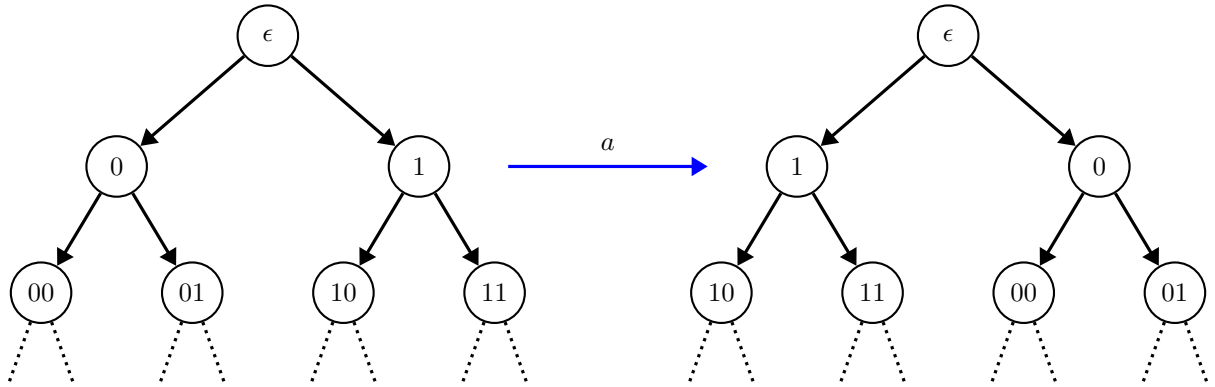


FIGURE 2 – Effet de a sur l'arbre : il échange les sous-arbres droits et gauches.

On vérifie que a est bien un automorphisme :
Preuve :

> Clairement, $a^2 = \mathrm{id}_{\mathcal{T}^{(2)}}$ donc $a^{-1} = a$. Il suffit donc de vérifier que a est bien un morphisme.
> Soit $\alpha, \gamma \in \{0,1\}, u \in \{0,1\}^*$ et β l'unique élément de $\{0,1\} \setminus \{\alpha\}$. On a :
>
> $$(a(\alpha u), a(\alpha u \gamma)) = (\beta u, \beta u \gamma) \in A$$
>
> □

Proposition 4.1.15:
Soit $\tau : \mathcal{G} \to \mathcal{G}'$ un morphisme de graphe, il induit un morphisme de groupe :

$$\tau_* : \mathrm{Aut}(\mathcal{G}) \to \mathrm{Aut}(\mathcal{G}')$$
$$\psi \mapsto \tau^{-1} \cdot \psi \cdot \tau = \tau \circ \psi \circ \tau^{-1}$$

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\psi} & \mathcal{G} \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ \mathcal{G}' & \xrightarrow[\tau_*(\psi)]{} & \mathcal{G}' \end{array}$$

De plus, si τ est un isomorphisme alors τ_* l'est aussi et $(\tau_*)^{-1} = (\tau^{-1})_*$.

On a désigné par $\cdot$ la composition à gauche, loi de groupe sur $\mathrm{Aut}(\mathcal{G})$.

Preuve :

> τ_* est clairement bien défini. De plus, c'est un morphisme : pour $\psi_1, \psi_2 \in \mathrm{Aut}(\mathcal{G})$, on a $\tau_*(\psi_1\psi_2) = \tau^{-1}\psi_1\psi_2\tau = \tau^{-1}\psi_1\tau\tau^{-1}\psi_2\tau = \tau_*(\psi_1)\tau_*(\psi_2)$
> Supposons que τ est un isomorphisme, un simple calcul donne que l'inverse de τ_* est $(\tau^{-1})_*$.
> □

Remarque 4.1.16:
Dans le cas de $\mathcal{T}^{(2)}$, considérant $v \in \{0,1\}^*$ un sommet, la proposition précédente permet de construire le morphisme $\tau_v \in \mathrm{Aut}(\mathcal{T}^{(2)})$ défini par $\tau_v(u) = (i_v)_*(\tau)(u)$. Celui-ci applique τ au sous arbre enraciné en v (isomorphe à $\mathcal{T}^{(2)}$) et laisse le reste de l'arbre invariant.

On va définir un outil utile pour savoir si un automorphisme de $\mathcal{T}^{(2)}$ inverse ou non les deux sous arbres partant d'un sommet donné :
Soit $\tau \in \mathrm{Aut}(\mathcal{T}^{(2)})$ et $v \in \{0,1\}^*$. Les arrêtes partant de v sont $(v, v0)$ et $(v, v1)$. A fortiori, celles partant de $\tau(v)$ sont $(\tau(v), \tau(v)0)$ et $(\tau(v), \tau(v)1)$. On a alors deux cas :

— Soit $\tau(v0) = \tau(v)0$ et a fortiori $\tau(v1) = \tau(v)1$
— Soit $\tau(v0) = \tau(v)1$ et a fortiori $\tau(v1) = \tau(v)0$

On définit alors :

Définition 4.1.17:
Soit $\tau \in \mathrm{Aut}(\mathcal{T}^{(2)})$ et $v \in \{0,1\}^*$, on note

$$\begin{aligned} \epsilon_v : \mathrm{Aut}(\mathcal{T}^{(2)}) &\to \{0,1\} \\ \tau &\mapsto \mathbb{1}_{[\tau(v0)=\tau(v)0]} \end{aligned}$$

Proposition 4.1.18:
On a une bijection

$$\begin{aligned} \mathcal{E} : \mathrm{Aut}(\mathcal{T}^{(2)}) &\to \{0,1\}^{\mathcal{T}^{(2)}} \\ \tau &\mapsto \begin{pmatrix} \mathcal{T}^{(2)} \to \{0,1\} \\ v \mapsto \epsilon_v(\tau) \end{pmatrix} \end{aligned}$$

Preuve :

Surjectivité : Soit $f : \mathcal{T}^{(2)} \to \{0,1\}$. On va construire inductivement $\tau \in \mathrm{Aut}(\mathcal{T}^{(2)})$ tel que $\mathcal{E}(\tau) = f$.
— Nécessairement, $\tau(\epsilon) = \epsilon$ car τ est un morphisme.
— Supposons que $\tau(v)$ est construit pour un certain $v \in \{0,1\}^*$. On pose alors :

$$\tau(v0) = \begin{cases} \tau(v)0 \text{ si } f(v0) = 1 \\ \tau(v)1 \text{ sinon} \end{cases}$$

de sorte que $\epsilon_{v0}(\tau) = f(v0)$.
Idem pour $v1$.

Finalement, on a bien par construction que τ est un élément de $\mathrm{Aut}(\mathcal{T}^{(2)})$ tel que $\mathcal{E}(\tau) = f$
On a donc bien la surjectivité de $\mathcal{E}$.

Injectivité : Soit $\tau, \tau' \in \mathrm{Aut}(\mathcal{T}^{(2)})$ tels que $\mathcal{E}(\tau) = \mathcal{E}(\tau') = f$. On procède par récurrence :
— $\tau(\epsilon) = \tau'(\epsilon) = \epsilon$ car un morphisme fixe la racine.
— Soit $n \in \mathbb{N}$ et supposons que τ et τ' coïncident tous les sommets de niveau $\leq n$. Soit v un sommet de niveau n,

$$\begin{aligned} \tau(v0) &= \begin{cases} \tau(v)0 \text{ si } f(v0) = 1 \\ \tau(v)1 \text{ sinon} \end{cases} \\ &= \tau'(v0) \end{aligned}$$

Idem pour $v1$, et on a bien τ et τ' coïncident sur les sommets de niveau $n+1$.
Ceci conclut la récurrence et la preuve.

□

Corollaire 4.1.19:
$\mathrm{Aut}(\mathcal{T}^{(2)})$ n'est pas dénombrable et a fortiori pas de type fini.

Théorème 4.1.20:

On a le produit semi-direct $\mathrm{Aut}(\mathcal{T}^{(2)}) \simeq \left(\mathrm{Aut}(\mathcal{T}^{(2)}) \times \mathrm{Aut}(\mathcal{T}^{(2)})\right) \rtimes_\rho \langle a \rangle$ pour le morphisme

$$\begin{aligned} \rho : \{\mathrm{id}, a\} &\to \mathrm{Aut}\left(\mathrm{Aut}(\mathcal{T}^{(2)}) \times \mathrm{Aut}(\mathcal{T}^{(2)})\right) \\ \mathrm{id} &\mapsto ((\psi_0, \psi_1) \mapsto (\psi_0, \psi_1)) \\ a &\mapsto ((\psi_0, \psi_1) \mapsto (\psi_1, \psi_0)) \end{aligned}$$

Preuve :

Notons

$$\begin{aligned} \phi : \left(\mathrm{Aut}(\mathcal{T}^{(2)}) \times \mathrm{Aut}(\mathcal{T}^{(2)})\right) \rtimes_\rho \langle a \rangle &\to \mathrm{Aut}(\mathcal{T}^{(2)}) \\ (\psi_0, \psi_1), a^k &\mapsto (i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1) \cdot a \end{aligned}$$

À nouveau, on désigne par $\cdot$ la composition à gauche $\psi \cdot \psi' = \psi' \circ \psi$. Alors, $\phi((\psi_0, \psi_1), a^k) = a^k \circ (i_1)_*(\psi_1) \circ (i_0)_*(\psi_0)$.
On remarque que pour tous automorphismes $\psi_0, \psi_1 \in \mathrm{Aut}(\mathcal{T}^{(2)})$ on a $(i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1) = (i_1)_*(\psi_1) \cdot (i_0)_*(\psi_0)$ et que donc l'ordre n'importe pas dans la définition de ϕ, on ne peut par contre pas déplacer a dans l'expression.

ϕ **est un morphisme :** Soit $\psi_0, \psi_1, \psi_0', \psi_1' \in \mathrm{Aut}(\mathcal{T}^{(2)})$

— Cas id, id :

$$\phi((\psi_0, \psi_1, \mathrm{id})(\psi_0', \psi_1', \mathrm{id})) = \phi(\psi_0\psi_0', \psi_1\psi_1', 1) = (i_0)_*(\psi_0\psi_0') \cdot (i_1)_*(\psi_1\psi_1')$$

$$\begin{aligned} \phi(\psi_0, \psi_1, \mathrm{id})\phi(\psi_0', \psi_1', \mathrm{id}) &= ((i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1)) \cdot ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1')) \\ &= ((i_0)_*(\psi_0) \cdot (i_0)_*(\psi_0')) \cdot ((i_1)_*(\psi_1) \cdot (i_1)_*(\psi_1')) \\ &= (i_0)_*(\psi_0\psi_0') \cdot (i_1)_*(\psi_1\psi_1') \end{aligned}$$

— Cas a, id :

$$\phi((\psi_0, \psi_1, a)(\psi_0', \psi_1', \mathrm{id})) = \phi(\psi_0\psi_1', \psi_1\psi_0', a) = (i_0)_*(\psi_0\psi_1') \cdot (i_1)_*(\psi_1\psi_0') \cdot a =: \gamma_1$$

$$\phi(\psi_0, \psi_1, a)\phi(\psi_0', \psi_1', \mathrm{id}) = ((i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1) \cdot a) \cdot ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1')) =: \gamma_2$$

Vérifions que $\gamma_1 = \gamma_2$, soit $u \in \{0,1\}^*$:

$$\begin{aligned} \gamma_1(0u) &= a(0\psi_0\psi_1'(u)) = 1\psi_0\psi_1'(u) \\ \gamma_2(0u) &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(a(0\psi_0(u))) \\ &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(1\psi_0(u)) = 1\psi_1'(\psi_0(u)) \\ &= 1\psi_0\psi_1'(u) \end{aligned}$$

$$\begin{aligned} \gamma_1(1u) &= a(1\psi_1\psi_0'(u)) = 0\psi_1\psi_0'(u) \\ \gamma_2(1u) &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(a(1\psi_1(u))) \\ &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(0\psi_1(u)) = 0\psi_0'(\psi_1(u)) \\ &= 0\psi_1\psi_0'(u) \end{aligned}$$

— Cas id, a :

$$\phi((\psi_0, \psi_1, \mathrm{id})(\psi_0', \psi_1', a)) = \phi(\psi_0\psi_0', \psi_1\psi_1', a) = (i_0)_*(\psi_0\psi_0') \cdot (i_1)_*(\psi_1\psi_1') \cdot a$$

$$\phi(\psi_0, \psi_1, \mathrm{id})\phi(\psi_0', \psi_1', a) = ((i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1)) \cdot ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1') \cdot a) = (i_0)_*(\psi_0\psi_0') \cdot (i_1)_*(\psi_1\psi_1') \cdot a$$

— Cas a, a :

$$\phi((\psi_0, \psi_1, a)(\psi_0', \psi_1', a)) = \phi(\psi_0\psi_1', \psi_1\psi_0', \mathrm{id}) = (i_0)_*(\psi_0\psi_1') \cdot (i_1)_*(\psi_1\psi_0') =: \gamma_1$$

$$\phi(\psi_0, \psi_1, a)\phi(\psi_0', \psi_1', a) = ((i_0)_*(\psi_0) \cdot (i_1)_*(\psi_1) \cdot a) \cdot ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1') \cdot a) =: \gamma_2$$

Vérifions que $\gamma_1 = \gamma_2$, soit $u \in \{0,1\}^*$:

$$\begin{aligned}
\gamma_1(0u) &= 0\psi_0\psi_1'(u) \\
\gamma_2(0u) &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1') \cdot a)\,(a(0\psi_0(u))) \\
&= a[((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(1\psi_0(u))] = a(1\psi_1'(\psi_0(u))) \\
&= 0\psi_0\psi_1'(u)
\end{aligned}$$

$$\begin{aligned}
\gamma_1(1u) &= 1\psi_1\psi_0'(u) \\
\gamma_2(1u) &= ((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1') \cdot a)\,(a(1\psi_1(u))) \\
&= a[((i_0)_*(\psi_0') \cdot (i_1)_*(\psi_1'))\,(0\psi_1(u))] = a(0\psi_0'(\psi_1(u))) \\
&= 1\psi_1\psi_0'(u)
\end{aligned}$$

En conséquence, ϕ est bien un morphisme de groupe.

ϕ est bijectif : On voit facilement que $\ker\phi$ est trivial. En effet, un élément de son noyau serait tel qu'il n'affecte ni le sous arbre droit, ni le gauche et qu'il ne les inverse pas non plus. Par conséquent, ϕ est injectif. Soit $\tau \in \mathrm{Aut}(\mathcal{T}^{(2)})$ un automorphisme de l'arbre binaire. On va construire (ψ_0, ψ_1, a^k) tels que $\phi(\psi_0, \psi_1, a^k) = \tau$. On a deux cas :

— Si $\tau(0) = 0$ (et donc $\tau(1) = 1$) : Puisque que τ est un morphisme d'arbre, les sommets de la forme $0u$ (sous arbre gauche) sont envoyés par τ sur des sommets de la forme $0\psi_0(u)$. L'application ψ ainsi définie est un isomorphisme d'arbre car τ l'est. On définit de même ψ_1 et alors $\tau = \phi(\psi_0, \psi_1, \mathrm{id})$.

— Si $\tau(0) = 1$ (et donc $\tau(1) = 0$) : De la même manière, $\tau(0u) = 1\psi_0(u)$ et $\tau(1u) = 0\psi_1(u)$ et $\tau = \phi(\psi_0, \psi_1, a)$

Finalement, ϕ est bijectif et a fortiori un isomorphisme.
□

On voit que le groupe $\mathrm{Aut}(\mathcal{T}^{(2)})$ se contient comme sous groupe strict, c'est cette même propriété qui fera fonctionner beaucoup de calculs pour le groupe de Grigorchuk.

4.1.3 Définition du groupe de Grigorchuk et premiers résultats

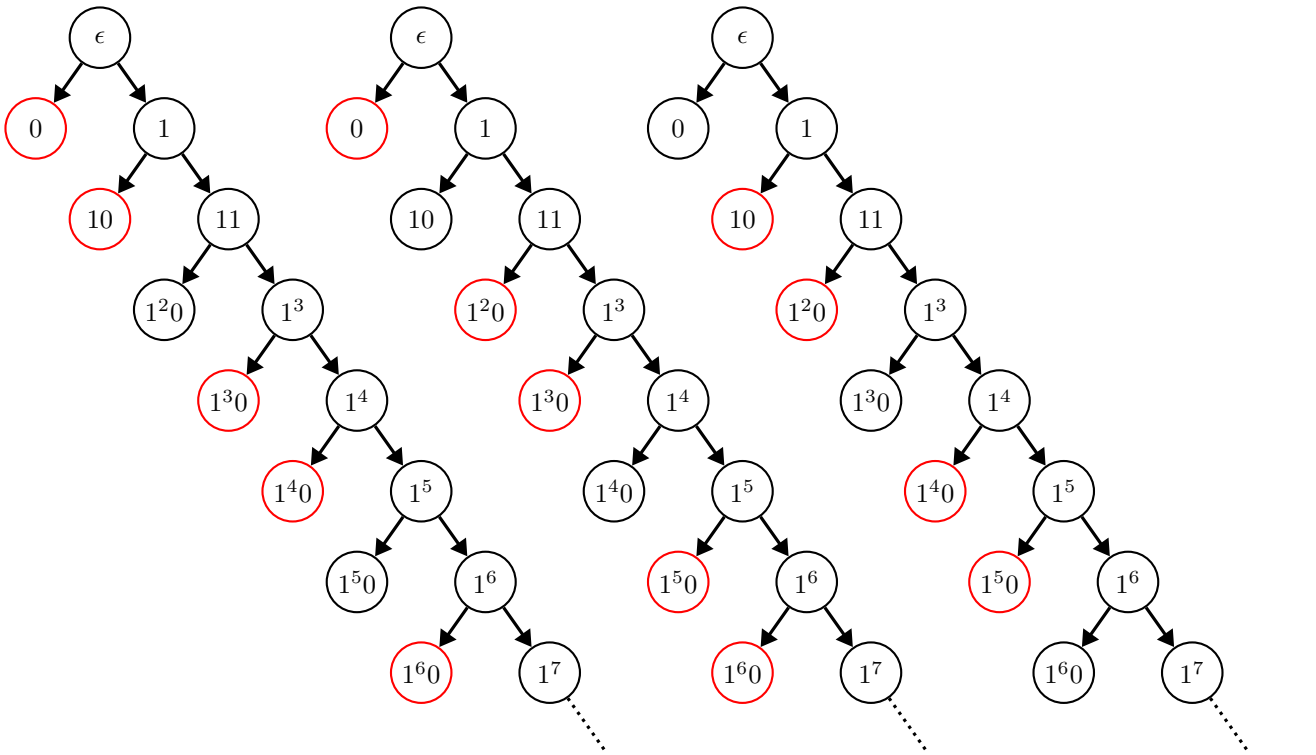
Définition 4.1.21:

On définit 3 automorphismes de $\mathcal{T}^{(2)}$: $a = \phi(\mathrm{id}, \mathrm{id}, a),\ b = \phi(a, c, \mathrm{id}),\ c = \phi(a, d, \mathrm{id}),\ \phi(\mathrm{id}, b, \mathrm{id})$

Ces définitions dépendent les une des autres, cependant, la dépendance se fait toujours "en dessous" de là où on applique l'un des morphismes donc on peut calculer leur effet récursivement. On le fait ci-dessous pour b :

Clairement, $b(1^k) = 1c(1^{k-1}) = \cdots = 1^k\gamma(\epsilon) = 1^k$ ou γ est l'un des trois automorphismes b, c, d selon la valeur de k. Soit $u = 1^k0v$:

$$\begin{aligned}
b(u) &= 1c(1^{k-1}0v) \\
&= 11d(1^{k-2}0v) \\
&= 111b(1^{k-3}0v)
\end{aligned}$$



Effet de b sur l'arbre Effet de c sur l'arbre Effet de d sur l'arbre

FIGURE 3 – Effet des automorphismes b, c, d sur $\mathcal{T}^{(2)}$, les sommets rouges sont ceux dont les sous-abres sont inversés.

On a donc $b(u) = \begin{cases} 1^k0a(v) & \text{si } k \equiv 0[3] \\ 1^k0a(v) & \text{si } k \equiv 1[3] \\ 1^k0v & \text{si } k \equiv 2[3] \end{cases}$

De manière analogue, on obtient :

Proposition 4.1.22:

Pour $u = 1^k0v$, on a :

$$b(u) = \begin{cases} 1^k0a(v) & \text{si } k \equiv 0[3] \\ 1^k0a(v) & \text{si } k \equiv 1[3] \\ 1^k0v & \text{si } k \equiv 2[3] \end{cases} \quad c(u) = \begin{cases} 1^k0a(v) & \text{si } k \equiv 0[3] \\ 1^k0v & \text{si } k \equiv 1[3] \\ 1^k0a(v) & \text{si } k \equiv 2[3] \end{cases} \quad d(u) = \begin{cases} 1^k0v & \text{si } k \equiv 0[3] \\ 1^k0a(v) & \text{si } k \equiv 1[3] \\ 1^k0a(v) & \text{si } k \equiv 2[3] \end{cases}$$

Les seuls sommets qui ne s'écrivent pas sous cette forme sont les sommets de la forme 1^k, ils sont fixés par b, c, d.

Concrètement, ces automorphismes "descendent" le long du bord droit de l'arbre et inversent les sous arbre de 2 fils gauches sur 3 des sommets qu'ils traversent. On visualise leurs effets sur la Figure 3.

À partir de ces automorphismes, on définit le groupe de Grigorchuk :

Définition 4.1.23: *Groupe de Grigorchuk*

On appelle premier groupe de Grigorchuk le groupe $\mathbb{G} = \langle a, b, c, d \rangle$

À partir de maintenant, on note $S = \{a, b, c, d\}$

Théorème 4.1.24:

$\mathbb{G}$ est un groupe à croissance intermédiaire. C'est-a-dire que sa fonction de croissance croit plus vite que tout polynôme, mais plus lentement que toute exponentielle.

La preuve de ce résultat occupera le reste de ce document.

Remarque 4.1.25:

On voit facilement que $a^2 = b^2 = c^2 = d^2 = bcd = \mathrm{id}$ et que a, b, c, d commutent deux à deux. De plus, $\langle b, c, d\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Preuve :

— Clairement $a^2 = \mathrm{id}$. Utilisant la Proposition 4.1.22 on obtient immédiatement que b, c, d sont d'ordre 2 (double inversion des mêmes sous-arbres). Cette proposition donne également que $bcd = \mathrm{id}$ car qu'importe la valeur de k, on appliquera deux fois a à v (avec les notations de Proposition 4.1.22).

— Commutativité : cela découle à nouveau facilement de la Proposition 4.1.22 (car a commute avec lui-même et l'identité).

— Isomorphisme :

$$bc = d^{-1} = d$$
$$cd = b^{-1} = b$$
$$bd = bcc^{-1}d = dc^{-1}d = d^2c^{-1} = c$$

On a donc que $\langle b, c, d\rangle$ est un groupe a 4 éléments, tous d'ordre au plus 2 : il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$

□

Proposition 4.1.26:

$(ad)^4 = (ac)^8 = (ab)^{16} = \mathrm{id}$

Preuve :

On va utiliser le produit semi-direct pour simplifier les calculs.
On note ψ la réciproque du morphisme de la preuve du Théorème 4.1.20.

Alors, $\psi(ad) = \psi(a)\psi(d) = (\mathrm{id}, \mathrm{id}, a)(\mathrm{id}, b, \mathrm{id}) = (b, \mathrm{id}, a)$. A fortiori, $\psi(ad)^2 = (b, b, \mathrm{id})$ puis $\psi(ad)^4 = (\mathrm{id}, \mathrm{id}, \mathrm{id})$.
Puisque ψ est un automorphisme, il suit que $(ad)^4 = \mathrm{id}$.

Ensuite $\psi(ac)^2 = (d, a, a)(d, a, a) = (da, ad, \mathrm{id}) = ((da)^{-1}, ad, \mathrm{id})$ est d'ordre divisant 4 par ce qui précède. Donc $(ac)^8 = \mathrm{id}$.

Enfin, $\psi(ab) = (c, a, a)(c, a, a) = (ca, ac, \mathrm{id}) = ((ac)^{-1}, ac, \mathrm{id})$ est d'ordre divisant 8 et comme avant $(ab)^{16} = \mathrm{id}$
□

Corollaire 4.1.27:

Les groupes $\langle a, b\rangle$, $\langle a, c\rangle$, $\langle a, d\rangle$ sont finis.

Preuve :

Soit $x \in \{b, c, d\}$, un élément de $\langle a, x\rangle$ peut se représenter comme un mot de $\{a, x\}^*$. En simplifiant toutes les occurrences de aa et xx (ordre 2), on se ramène a un mot de la forme $a^i x \underbrace{(ax \cdots ax)}_{k \text{ fois}} a^j$ avec $i, j \in \{0, 1\}$

Or, en simplifiant des occurrences de $(ax)^{16}$ on se ramène au cas $k \leq 16$.
Ainsi, il y a au plus 4×16 mots réduits possibles donc le groupe est fini.
□

Définition 4.1.28:

Le groupe $\mathbb{G}$ agit sur $\mathcal{T}^{(2)}$ par $u \cdot g = g(u)$.
On note $\mathbb{H}_n = \bigcap_{|u|=n} \mathrm{Stab}_{\mathbb{G}}(u)$ le sous groupe des éléments de $\mathbb{G}$ qui fixent tous les sommets de hauteur n.
On appelle sous-groupe fondamental le sous-groupe $\mathbb{H} = \mathbb{H}_1 = \mathrm{Stab}_{\mathbb{G}}(0) \cap \mathrm{Stab}_{\mathbb{G}}(1)$.

Remarque 4.1.29:

$\mathbb{H}_n = \bigcap_{|u|\leq n} \mathrm{Stab}_{\mathbb{G}}(u)$. En effet, puisque les éléments de $\mathbb{G}$ sont des morphismes, lorsque l'un d'entre eux déplace un sommet, il déplace le sous arbre enraciné en ce sommet avec et ne peut donc stabiliser aucun sommet de celui-ci. En particulier, pour $n \leq m$, $\mathbb{H}_m \subseteq \mathbb{H}_n$.

Lemme 4.1.30:

Le sous groupe fondamental vérifie $\mathbb{H} = \langle b, c, d, aba, aca, ada\rangle$ et $[\mathbb{G} : \mathbb{H}] = 2$. En particulier, $\mathbb{H} \triangleleft \mathbb{G}$.

Pour prouver ce lemme, on utilise le lemme suivant :

Lemme 4.1.31:

On appelle décomposition réduite de $g \in \mathbb{G}$ un mot $\alpha_1 \cdots \alpha_n,\ \alpha_i \in S^{\pm}$ tel que $g = \alpha_1 \cdots \alpha_n$ et $l_S(g) = n$.
Alors, une décomposition réduite de tout élément de $\mathbb{G}$ est nécessairement de la forme $(a) * a * \cdots * a * (a)$ ou les $*$ représentent des éléments de $\{b, c, d\}$.

Preuve :

> Puisque $bcd = \mathrm{id}$ et que b, c, d sont d'ordre 2, le produit de deux éléments distincts de $\{b, c, d\}$ donne le troisième.
>
> Partant d'un mot de $\{a, b, c, d\}$, on peut donc retirer tout couple aa, bb, cc, ou dd (ordre 2) et simplifier tout produit de deux éléments de $\{b, c, d\}$ en le troisième, donnant bien la forme voulue.
> □

Prouvons alors le Lemme 4.1.30
Preuve :

> **Caractérisation** $\mathbb{H} = \langle b, c, d, aba, aca, ada\rangle$ **:**
> Notons $H = \langle b, c, d, aba, aca, ada\rangle$
> — Clairement, $b, c, d \in \mathbb{H}$. De plus, $aba(0) = ba(1) = a(1) = 0$ et $aba(1) = ba(0) = a(0) = 1$ puis $aba \in \mathbb{H}$. Idem, on obtient $aca, ada \in \mathbb{H}$ et a fortiori, $H \subseteq \mathbb{H}$.
> — Soit $h \in \mathbb{H}$, considérons une décomposition réduite $h = a^i\alpha_1 a\alpha_2 a \cdots \alpha_n a^j$ avec $i, j \in \{0, 1\}$ et les $\alpha_k \in \{b, c, d\}$.
> La condition $h \in \mathbb{H}$ est équivalente au fait que le nombre de a dans cette décomposition est pair.
> On peut alors faire des groupes de la forme $a * a$ et consommer ainsi toutes les occurrences de a pour se retrouver avec un produit d'éléments de cette forme et d'éléments de $\{b, c, d\}$. A fortiori $h \in H$ et d'après ce qui précède $\mathbb{H} = H$.
>
> **Indice :** Soit $g \in \mathbb{G}$, si $g \notin \mathbb{H}$, alors $ag \in \mathbb{H}$ et inversement donc $\mathbb{G}/\mathbb{H} = \{\mathbb{H}, a\mathbb{H}\}$ d'où $[\mathbb{G} : \mathbb{H}] = 2$. Or, tous les sous groupes d'indices 2 sont distinguées et $\mathbb{H} \triangleleft \mathbb{G}$.
> □

Proposition 4.1.32:

Les sous groupes $\mathbb{H}_n$ vérifient $[\mathbb{G} : \mathbb{H}] \leq 2^{2^n-1}$

Pour la preuve, on a besoin d'un lemme :

Lemme 4.1.33:

Soit $A_n = \{\tau \in \mathrm{Aut}(\mathcal{T}^{(2)}) \mid \forall v \in \mathcal{T}^{(2)} \text{ t.q. } |v| \geq n, \epsilon_v(\tau) = 1\}$. Il s'agit de l'ensemble des automorphismes de $\mathcal{T}^{(2)}$ dont l'effet "en dessous"du niveau n se fait uniquement comme propagation des inversions de sous-arbres faites dans les premiers niveaux.
Alors, A_n est un sous groupe et $A_n \simeq (A_{n-1} \times A_{n-1}) \rtimes \langle a\rangle$. En particulier, $|A_n| = 2^{2^n-1}$.

Preuve :

Sous-groupe : Tous d'abord, montrons une identité utile : pour tous $g, h \in \mathrm{Aut}(\mathcal{T}^{(2)})$, pour tout $v \in \mathcal{T}^{(2)}$,

$$\begin{aligned}\epsilon_v(gh) &= \mathbb{1}_{[h\circ g(v0)=h\circ g(v)0]} \\ &= \mathbb{1}_{[g(v0)=g(v)0]}\mathbb{1}_{[h(g(v)0)=h(g(v))0]} + \mathbb{1}_{[g(v0)=g(v)1]}\mathbb{1}_{[h(g(v)1)=h(g(v))0]} \\ &= \epsilon_v(g)\epsilon_{g(v)}(h) + (1-\epsilon_v(g))(1-\epsilon_{g(v)}(h))\end{aligned}$$

Montrons alors que A_n est un sous groupe, soit $g, h \in A_n$
Alors, pour tout sommet v tel que $|v| \geq n$, l'identité précédente donne

$$\epsilon_v(gh) = \epsilon_v(g)\epsilon_{g(v)}(h) + (1-\epsilon_v(g))(1-\epsilon_{g(v)}(h)) = 1$$

C'est-a-dire $gh \in A_n$.
Reste à voir la stabilité par inverse. L'identité précédente donne

$$1 = \epsilon(gg^{-1}) = \epsilon_v(g)\epsilon_{g(v)}(g^{-1}) + (1-\epsilon_v(g))(1-\epsilon_{g(v)}(g^{-1})) = \epsilon_{g(v)}(g^{-1})$$

Puisque g est un automorphisme (et donc induit une bijection entre les sommets de niveau au moins n), on en déduis que $g^{-1} \in A_n$.

Finalement, A_n est bien un sous-groupe.
Isomorphisme : Notons ψ la réciproque du morphisme de la preuve du Théorème 4.1.20. Soit $g \in A_n$, notons $\psi(g) = (g_0, g_1, a^k)$.
Clairement, $g_0, g_1 \in A_{n-1}$ et alors $\psi(A_n) \subseteq (A_{n-1} \times A_{n-1}) \rtimes \langle a \rangle$. En effet, on remarque que g_0 (resp. g_1) représente l'effet de g sur le sous-arbre gauche (resp. droit).

Pour obtenir l'égalité (et donc l'isomorphisme) on considère $(g_0, g_1, a^k) \in (A_{n-1} \times A_{n-1}) \rtimes \langle a \rangle$. Alors, notant $g = \psi^{-1}(g_0, g_1, a^k)$, on obtient pour tout $v = 0u,\ |u| \geq n-1$:

$$\epsilon_v(g) = \mathbb{1}_{[g(0u0)=g(\alpha u)0]} = \mathbb{1}_{[g_j(u0)=g_j(u)0]} = 1$$

Ici, j désigne 0 si $a^k = \mathrm{id}$ et 1 sinon. On fait idem pour $v = 1u$.
En conséquence, $g \in A_n$ d'où l'isomorphisme.
Cardinal : On procède par récurrence, clairement $A_1 = \{\mathrm{id}, a\}$ et $2^{2^1-1} = 2$.

Soit $n \in \mathbb{N}$ tel que $|A_n| = 2^{2^n-1}$. Utilisant l'isomorphisme précédent, on obtient

$$|A_{n+1}| = 2 \times |A_n|^2 = 2 \times 2^{2^{n+1}-2} = 2^{2^{n+1}-1}$$

Ceci termine la récurrence et la preuve.

□

On peut alors prouver la Proposition 4.1.32 :
Preuve :

Notons $\mathcal{E}$ la bijection de la Proposition 4.1.18. On définit la fonction d'oubli en dessous du niveau n :

$$\begin{aligned} O_n : \{0,1\}^{\mathcal{T}^{(2)}} &\longrightarrow \{0,1\}^{\mathcal{T}^{(2)}} \\ f &\mapsto \left(v \mapsto \begin{cases} f(v) & \text{si } |v| < n \\ 1 & \text{si } |v| \geq n \end{cases} \right)\end{aligned}$$

Soit alors $\varphi_n = \mathcal{E}^{-1} \circ \mathcal{O}_n \circ \mathcal{E} : \mathrm{Aut}(\mathcal{T}^{(2)}) \to \mathrm{Aut}(\mathcal{T}^{(2)})$
Par construction, pour tout $\tau \in \mathrm{Aut}(\mathcal{T}^{(2)})$, $\varphi_n(\tau) \in A_n$.
À partir de maintenant, on désigne par φ_n la restriction $\mathcal{E}^{-1} \circ \mathcal{O}_n \circ \mathcal{E} : \mathbb{G} \to A_n$

Soit alors $g_1, g_2 \in \mathbb{G}$:

$$\varphi_n(g_1) = \varphi_n(g_2) \iff O_n(\mathcal{E}(g_1)) = O_n(\mathcal{E}(g_2)) \iff \forall v \in \mathcal{T}^{(2)},\ |v| < n,\ \epsilon_v(g_1) = \epsilon_v(g_2)$$

Or ceci équivaut à $g_2^{-1}g_1 \in \mathbb{H}_n$. En effet,

— **Sens direct :** Supposons $\epsilon_v(g_1) = \epsilon_v(g_2)$ pour tous sommets v de niveau $|v| < n$.
Rappelons que pour tous $g, h \in \mathrm{Aut}(\mathcal{T}^{(2)})$, $\epsilon_v(gh) = \epsilon_v(g)\epsilon_{g(v)}(h) + (1 - \epsilon_v(g))(1 - \epsilon_{g(v)}(h))$ (voir preuve de Lemme 4.1.33).
En conséquence, pour tout sommet v tel que $|v| < n$,

$$\begin{aligned}\epsilon_v(g_2^{-1}g_1) &= \epsilon_v(g_2^{-1})\epsilon_{g_2^{-1}(v)}(g_1) + (1 - \epsilon_v(g_2^{-1}))(1 - \epsilon_{g_2^{-1}(v)}(g_1)) \\ &= \epsilon_v(g_2^{-1})\epsilon_{g_2^{-1}(v)}(g_2) + (1 - \epsilon_v(g_2^{-1}))(1 - \epsilon_{g_2^{-1}(v)}(g_2)) \\ &= \epsilon_v(g_2^{-1}g_2) = \epsilon_v(\mathrm{id}) = 1\end{aligned}$$

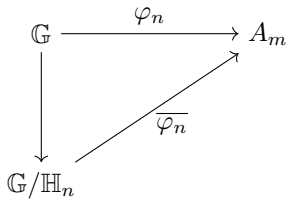
C'est-a-dire que pour tout sommet v de niveau $|v| < n$, $g_2^{-1}g_1$ n'échange pas ses deux sous arbres et a fortiori $g_2^{-1}g_1 \in \mathbb{H}_n$.

— **Sens indirect :** Supposons $g_2^{-1}g_1 \in \mathbb{H}$. Ceci équivaut à $\exists h \in \mathbb{H}$ t.q. $g_1 = g_2 h$, mais alors pour tout sommet v de niveau $|v| < n$,

$$\epsilon_v(g_1) = \epsilon_v(g_2h) = \epsilon_v(g_2)\epsilon_{g_2(v)}(h) + (1 - \epsilon_v(g_2))(1 - \epsilon_{g_2(v)}(h)) = \epsilon_v(g_2)$$

En effet, puisque $h \in \mathbb{H}_n$, il stabilise les sommets de niveau $\leq n$, donc n'échange pas les sous arbres des sommets de niveau $|v| < n$ et alors $\epsilon_v(h) = 1$ pour tous sommets v tels que $|v| < n$.

Finalement, $\varphi_n(g_1) = \varphi_n(g_2) \iff g_2^{-1}g_1 \in \mathbb{H}_n$ et donc, d'après le théorème de factorisation, il existe une unique application injective $\overline{\varphi}_n$ qui fasse commuter :



Le Lemme 4.1.33 conclut alors.

□

Lemme 4.1.34:

Notons $\psi = \phi^{-1} : \mathrm{Aut}(\mathcal{T}^{(2)}) \longrightarrow \mathrm{Aut}(\mathcal{T}^{(2)})^2 \rtimes \langle a \rangle$ l'inverse du morphisme de la preuve du Théorème 4.1.20. Décomposons ψ sur ses trois composantes : $\psi = (\psi_0, \psi_1, \psi_a)$. Alors, $\psi(\mathbb{H})$ est un sous-groupe de $\mathbb{G} \times \mathbb{G} \times \{\mathrm{id}\}$ et $\psi_0, \psi_1 : \mathbb{H} \to \mathbb{G}$ sont bien définies et surjectives.

Preuve :

Par définition de $\mathbb{H}$ (stabilise 0 et 1), $\psi(\mathbb{H}) \subseteq \mathrm{Aut}(\mathcal{T}^{(2)})^2 \times \{\mathrm{id}\}$. C'est un sous groupe car ψ est un morphisme.
Rappelons que $\mathbb{H} = \langle b, c, d, aba, aca, ada \rangle$. On a :

$$\left.\begin{aligned}\psi(b) &= (a, c, \mathrm{id}) \\ \psi(c) &= (a, d, \mathrm{id}) \\ \psi(d) &= (\mathrm{id}, b, \mathrm{id})\end{aligned}\right\} \in \mathbb{G} \times \mathbb{G} \times \{\mathrm{id}\}$$

De plus, $\psi(a) = (\mathrm{id}, \mathrm{id}, a)$ donc

$$\left.\begin{array}{l}\psi(aba) = (\mathrm{id}, \mathrm{id}, a)(a, c, \mathrm{id})(\mathrm{id}, \mathrm{id}, a) = (\mathrm{id}, \mathrm{id}, a)(a, c, a) = (c, a, \mathrm{id}) \\ \psi(aca) = (\mathrm{id}, \mathrm{id}, a)(a, d, \mathrm{id})(\mathrm{id}, \mathrm{id}, a) = (\mathrm{id}, \mathrm{id}, a)(a, d, a) = (d, a, \mathrm{id}) \\ \psi(ada) = (\mathrm{id}, \mathrm{id}, a)(\mathrm{id}, b, \mathrm{id})(\mathrm{id}, \mathrm{id}, a) = (\mathrm{id}, \mathrm{id}, a)(\mathrm{id}, b, a) = (b, \mathrm{id}, \mathrm{id})\end{array}\right\} \in \mathbb{G} \times \mathbb{G} \times \{\mathrm{id}\}$$

A fortiori, on a $\psi(\mathbb{H}) \subseteq \mathbb{G} \times \mathbb{G} \times \{\mathrm{id}\}$

On a de plus obtenu que, pour $i \in \{0, 1\}$, $\{a, b, c, d\} \subseteq \phi_i(\mathbb{H})$ et donc $\mathbb{G} \subseteq \operatorname{Im} \psi_i$ et d'après ce qui précède $\psi_i : \mathbb{H} \to \mathbb{G}$ est bien définie et surjective.

□

Corollaire 4.1.35:

Le groupe $\mathbb{G}$ est infini.

Preuve :

Supposons par l'absurde que $|\mathbb{G}| < \infty$. Alors, $|\mathbb{G}| = [\mathbb{G} : \mathbb{H}] \times |\mathbb{H}| = 2|\mathbb{H}|$.

De plus, $\psi_0 : \mathbb{H} \to \mathbb{G}$ est surjective ce qui implique $|\mathbb{G}| \leq |\mathbb{H}|$ puis $2|\mathbb{G}| \leq |\mathbb{G}|$: contradiction.

□

On obtient également le résultat clé :

Corollaire 4.1.36: *Auto-similarité de* $\mathbb{G}$

Le groupe de Grigorchuk vérifie $\mathbb{G} \simeq \psi(\mathbb{G}) \subseteq (\mathbb{G} \times \mathbb{G}) \rtimes \langle a \rangle$.

Preuve :

La preuve du Lemme 4.1.34 donne que $\psi(\{b, c, d\}) \subseteq (\mathbb{G} \times \mathbb{G}) \times \{\mathrm{id}\}$. De plus, $\psi(a) = (\mathrm{id}, \mathrm{id}, a)$ d'où $\psi(\mathbb{G}) \subseteq (\mathbb{G} \times \mathbb{G}) \rtimes \langle a \rangle$.

Le fait que $\mathbb{G} \simeq \psi(\mathbb{G})$ découle du fait que ψ est un isomorphisme.

□

4.2 Croissance super-polynomiale

Définition 4.2.1:

Deux groupes G_1 et G_2 sont dits commensurables s'il existe $H_1 < G_1$ et $H_2 < G_2$ des sous groupes tels que $H_1 \simeq H_2$ et $[G_1 : H_1], [G_2, H_2] < \infty$. On notera cela $G_1 \approx G_2$.

Le résultat ci-dessous nous permettra de conclure le caractère super-polynomial de la croissance de $\mathbb{G}$.

Proposition 4.2.2:

$\mathbb{G}$ est commensurable à $\mathbb{G} \times \mathbb{G}$: $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$

Preuve :

Avec les notations précédentes, notons $\tilde{\mathbb{H}} := (\psi_0, \psi_1)(\mathbb{H})$. Alors, $\tilde{\mathbb{H}}$ est un sous groupe de $\mathbb{G} \times \mathbb{G}$ (image par morphisme d'un sous-groupe).

De plus, $\tilde{\mathbb{H}} \simeq \mathbb{H}$. En effet, soit $h \in \mathbb{H}$, $h \in \ker((\psi_0, \psi_1)) \iff h$ stabilise les sous-arbres gauche et droit de la racine. Or, par définition de $\mathbb{H}$, h n'échange pas non plus ces deux sous-arbres donc $h = \mathrm{id}$ et le premier théorème d'isomorphisme donne $\mathbb{H} \simeq (\psi_0, \psi_1)(\mathbb{H}) = \tilde{\mathbb{H}}$

On démontre ci-après que $[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] < \infty$ ce qui conclut.

□

Démontrons $[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] < \infty$, pour cela, on introduit un autre sous-groupe.

Définition 4.2.3:

Soit $\mathbb{B} = \left\langle g^{-1}bg \;\middle|\; g \in \mathbb{G} \right\rangle$ le plus petit sous-groupe distingué contenant b

Lemme 4.2.4:

Le sous-groupe $\mathbb{B}$ vérifie : $[\mathbb{G} : \mathbb{B}] \leq 8$ et $\mathbb{B} \times \mathbb{B} \subseteq \tilde{\mathbb{H}}$

Preuve :

> **Indice :** Sachant que $a^2 = d^2 = (ad)^4 = \mathrm{id}$, $\langle a, d\rangle \simeq D_4$.
> De plus, $bcd = \mathrm{id}$ donc $c = b^{-1}d^{-1}$ et $\mathbb{G} = \langle a, b, d\rangle$.
> Finalement, $\mathbb{G}/\mathbb{B}$ est un quotient de $\langle a, d\rangle \simeq D_4$ puis $[\mathbb{G} : \mathbb{B}] \leq 8$.
>
> **Inclusion :** Soit $x = g^{-1}bg \in \mathbb{B}$.
> On a $(\psi_0, \psi_1)(d) = (\mathrm{id}, b)$ et $(\psi_0, \psi_1)((i_1)_*(g)) = (\mathrm{id}, g)$. Puisque $d, (i_1)_*(g) \in \mathbb{H}$, on a $(\mathrm{id}, x) \in \tilde{\mathbb{H}}$.
> De même, on montre que $(x, \mathrm{id}) \in \tilde{\mathbb{H}}$ et donc que $\mathbb{B} \times \mathbb{B} \subseteq \tilde{\mathbb{H}}$
> □

Corollaire 4.2.5:
$[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] < \infty$

Preuve :

> $$\underbrace{[\mathbb{G} \times \mathbb{G} : \mathbb{B} \times \mathbb{B}]}_{\leq 8^2} = [\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}][\tilde{\mathbb{H}} : \mathbb{B} \times \mathbb{B}]$$
> Donc $[\mathbb{G} \times \mathbb{G} : \tilde{\mathbb{H}}] \leq 64$.
> □

Ceci termine la preuve de $\mathbb{G} \approx \mathbb{G} \times \mathbb{G}$. On dit que $\mathbb{G}$ est multilatéral :

Définition 4.2.6:
On dit qu'un groupe G est multilatéral si $|G| = \infty$ et $\exists m \geq 2$ t.q. $G \approx G^m$.

Proposition 4.2.7:
Soit G un groupe multilatéral de type fini, alors G a croissance super-polynomiale.

La preuve de cette proposition se déduit du lemme suivant, il est purement analytique et ne dépend pas de la structure du groupe.

Lemme 4.2.8:
Soit $f : \mathbb{N} \to \mathbb{R}_+$ monotone croissante vérifiant $f(0) \geq 1$, et telle que $f(n) \xrightarrow[n\to\infty]{} \infty$. Supposons qu'il existe $m \geq 2$ tel que $f^m \overset{s}{\prec} f$. Alors, $\exists \sigma \in]0, 1[$ t.q. $e^{n^\sigma} \overset{s}{\prec} f$.

Généralisation de la preuve de "Topics in Geometric Group Theory"(De la Harpe [2, 2000]), page 223 :
Preuve :

> Notons $g(t) = f(\lceil t \rceil)$. Par hypothèse, il existe $A \geq 1$ tel que :
> $\forall t \geq 0,\ g(t)^m \leq g(At)$ ce qui équivaut à $\forall t \geq 0,\ g(t) \geq g(t/A)^m$.
>
> On remarque que, nécessairement, $A > 1$. En effet, si $A = 1$, pour tous $t \geq 0$, $g(t) \geq g(t)^m$. Or ceci n'est possible que si pour tous $t \geq 0$, on a $g(t) \leq 1$ ce qui contredit l'hypothèse $f(n) \to \infty$.
>
> Une récurrence immédiate donne que pour tous $t \geq 0$ et tous $k \in \mathbb{N}$, $g(t) \geq g(t/A^k)^{m^k}$.
> Or, en fixant un $t > 0$:
> — $f(n) \to \infty$ donc il existe l tel que $f(l) \geq e$. Notons $k_t = \lfloor \log_A(t/l) \rfloor$ (bien défini car $A > 1$). Alors :
>
> $$g(t) \geq g\left(\frac{t}{A^{k_t}}\right)^{m^{k_t}} \geq g\left(\frac{t}{A^{\log_A(t/l)}}\right)^{m^{k_t}} \geq e^{m^{k_t}}$$
>
> — En notant $\sigma = \dfrac{1}{\log_m(A)}$ (bien défini car $A > 1$) et $B = m^{1/\sigma} l \geq 1$ (qui ne dépendent pas de t) :
>
> $$m^{k_t} \geq m^{\log_A(t/l)-1} = \frac{1}{m} m^{\frac{\log_m(t/l)}{\log_m(A)}} = \frac{1}{m}(t/l)^\sigma = (t/B)^\sigma$$
>
> Combinant ces deux points, on obtient pour tout $t > 0$

$$g(t) \geq e^{m^{k_t}} \geq e^{(t/B)^\sigma}$$

soit

$$g(Bt) \geq e^{t^\sigma}$$

Le cas $t = 0$ est immédiat car $f(0) \geq 1$.

□

On peut alors prouver la Proposition 4.2.7 :
Preuve :

On a $[G : H], [G^m, \tilde{H}] < \infty$ et $H \simeq \tilde{H}$.
Or, utilisant la Proposition 2.2.16, on obtient $\beta(G, \cdot) \sim \beta(H, \cdot)$ et $\beta(G^m, \cdot) \sim \beta(\tilde{H}, \cdot)$.
Puisque H et $\tilde{H}$ sont isomorphes, ils ont croissances équivalentes et $\beta(G, \cdot) \sim \beta(G^m, \cdot)$, en particulier $\beta(G^m, \cdot) \overset{s}{\prec} \beta(G, \cdot)$.
Utilisant à nouveau la Proposition 2.2.16 : $\beta(G, \cdot)^m \overset{s}{\prec} \beta(G, \cdot)$.
Le Lemme 4.2.8 conclut.
□

Corollaire 4.2.9:
Le groupe $\mathbb{G}$ est à croissance super-polynomiale.

4.3 Croissance sous-exponentielle

4.3.1 Décompositions réduites

Afin de prouver la croissance sous-exponentielle, on commence par analyser plus en détail les décompositions réduites.

Définition 4.3.1:
Conformément au Lemme 4.1.31, on définit les quatre types de décompositions réduites possibles :

1. $a * a * \cdots a * a$
2. $a * a * \cdots a *$
3. $* a * \cdots a * a$
4. $* a * \cdots a *$

Proposition 4.3.2:
Pour chaque $g \in \mathbb{G}$, toutes les décompositions réduites de g sont toutes de type (1) ou toutes de types (4) ou toutes de type (2 ou 3).

Preuve :

Les types 2,3 et 1,4 n'ont pas la même parité donc g a forcément toutes ses décompositions réduites de type (1 et 4) ou (2 et 3).

De plus, $g \in \mathbb{H} \iff g$ a un nombre pair d'occurrence de a dans sa décomposition réduite. Or, à longueur égale, les types 1 et 4 n'ont pas la même parité de nombre de a impliquant que g ne peut pas avoir de décomposition des deux types à la fois.
□

Lemme 4.3.3:
Soit $g \in \mathbb{G}$ et notons $\psi(g) = (g_0, g_1, a^i)$. Alors, selon le type de décomposition de g, pour tout $i \in \{0, 1\}$:

Type 1 : $l_S(g_i) \leq \frac{1}{2}(l_S(g) - 1)$
Type 2/3 : $l_S(g_i) \leq \frac{1}{2} l_S(g)$
Type 4 : $l_S(g_i) \leq \frac{1}{2}(l_S(g) + 1)$

La preuve de ce lemme fait intervenir des objets qui nous resserviront plus tard :

Définition 4.3.4:

Soit w un mot sur S. On définit alors deux nouveaux mots $\Phi_0(w)$ et $\Phi_1(w)$ selon les règles de réécriture suivantes :

$$\Phi_0 : \begin{cases} a \to \text{id} \\ b \to a, c \to a, d \to \text{id} \text{ si nbr pair de } a \text{ avant} \\ b \to c, c \to d, d \to b \quad \text{si impair} \end{cases} \qquad \Phi_1 : \begin{cases} a \to \text{id} \\ b \to a, c \to a, d \to \text{id} \text{ si nbr impair de } a \text{ avant} \\ b \to c, c \to d, d \to b \quad \text{si pair} \end{cases}$$

Exemple 4.3.5:

Prenons $w = abacab$

Colorant en bleu lorsqu'on transforme dans le cas pair et en rouge dans le cas impair, on a :

	a	b	a	c	a	b
	↓	↓	↓	↓	↓	↓
Φ_0 :	id	c	id	a	id	c
Φ_1 :	id	a	id	d	id	a

On a donc que l'élément de $\mathbb{G}$ donné par $\Phi_0(w)$ est cac et celui donné par $\Phi_1(w)$ est ada.

Proposition 4.3.6:

Soit $g \in \mathbb{G}$ et w une décomposition de $\mathbb{G}$ (non nécessairement réduite). Alors, l'élément représenté par $\Phi_i(w)$ est g_i.

Preuve :

Par récurrence sur $n = l_S(g)$

Initialisation $n = 1$ **:**

- Pour a : $\Phi_0(a) = \Phi_1(a) = \text{id}$ or $a = (\text{id}, \text{id}, a)$
- Pour b : $\Phi_0(b) = a,\ \Phi_1(b) = c$ or $b = (a, c, \text{id})$
- Pour c, d : idem que pour b

Récurrence : Supposons que la proposition est vraie pour tout élément de longueur $\leq n$ et soit g de longueur $n+1$, soit $w = w_n\alpha$ une décomposition réduite de g. Notons $\psi(w_n) = (h_0, h_1, a^j)$, on a que j est le nombre de a dans w_n modulo 2, on disjoint alors deux cas :

- Cas $j = 0$:
  - $\alpha = a$, $\Phi_i(\alpha) = \text{id}$ donc $g_i = h_i$. De plus, $\psi(g) = (h_0, h_1, \text{id})(\text{id}, \text{id}, a) = (h_0, h_1, a)$ ce qui correspond.
  - $\alpha = b$, $\Phi_0(b) = a,\ \Phi_1(b) = c$ donc $g_0 = h_0a$ et $g_1 = h_1b$. De plus, $\psi(g) = (h_0, h_1, \text{id})(a, c, \text{id}) = (h_0a, h_1c, \text{id})$ ce qui correspond.
  - idem pour $\alpha = c, d$
- Cas $j = 1$:
  - $\alpha = a$, idem
  - $\alpha = b$, $\Phi_0(b) = c,\ \Phi_1(b) = a$ donc $g_0 = h_0c$ et $g_1 = h_1a$. De plus, $\psi(g) = (h_0, h_1, a)(a, c, \text{id}) = (h_0c, h_1a, a)$ ce qui correspond.
  - $\alpha = c, d$ idem

Remarque : L'hypothèse de récurrence sert à dire que h_0 et h_1 sont bien donnés par les Φ_i.

□

Exemple 4.3.7:

Toujours pour le mot $w = abacab$, on a :

$$\begin{aligned}\psi(abacab) &= (\mathrm{id}, \mathrm{id}, a)(a, c, \mathrm{id})\psi(acab)\\ &= (c, a, a)(\mathrm{id}, \mathrm{id}, a)\psi(cab)\\ &= (c, a, \mathrm{id})(a, d, \mathrm{id})\psi(ab)\\ &= (ca, ad, \mathrm{id})(\mathrm{id}, \mathrm{id}, a)\psi(b)\\ &= (ca, ad, a)(a, c, a)\\ &= (cac, ada, \mathrm{id})\end{aligned}$$

On retrouve bien cac et ada.

Remarquant que les éléments donnés par g_0 et g_1 ont les longueurs voulues pour le Lemme 4.3.3, on obtient immédiatement la preuve de celui-ci.

Corollaire 4.3.8:

Avec les notations du Lemme 4.3.3 : $l(g_0) + l(g_1) \leq l(g) + 1$

Ce lemme permet de démontrer une propriété remarquable du groupe de Grigorchuk, répondant à un problème de Burnside (Burnside [1, 1902]). La question posée étant de savoir si un groupe de type fini dont tous les éléments sont d'ordre fini est nécessairement fini.

Note : L'article cité ne semble pas être accessible, mais la littérature concorde pour le citer comme origine du problème.

Théorème 4.3.9:

Tous les éléments de $\mathbb{G}$ ont pour ordre une puissance de 2. En particulier, il répond par la négative au problème énoncé précédemment (puisqu'il est infini).

Preuve :

> Supposons que cela soit vrai pour tous les éléments de $\mathbb{H}$, alors cela est vrai pour tous les éléments. En effet, pour $g \in \mathbb{G}$, $\psi(g) = (g_0, g_1, a^i)$ et $\psi(g^2) = \psi(g)^2 = (g_0', g_1', \mathrm{id}) \in \mathbb{H}$. Le fait que ψ soit un isomorphisme conclut.
>
> Montrons alors que cela est vrai pour $\mathbb{H}$. On a déjà vu que c'est vrai pour les éléments de longueur 1. Supposons que cela est vrai pour tous les éléments de longueur $\leq n$ et soit $h \in \mathbb{H}$ de longueur $n+1$.
> On a $\psi(h) = (h_0, h_1, \mathrm{id})$, d'après le Lemme 4.3.3 : $l(h_0), l(h_1) \leq n$ et par hypothèse de récurrence ils sont d'ordre respectivement 2^{k_0} et 2^{k_1}. Soit alors $k = \max\{k_0, k_1\}$, on a $\psi(h^k) = (h_0^k, h_1^k, \mathrm{id}) = (\mathrm{id}, \mathrm{id}, \mathrm{id})$ donc $o(h) | 2^k$ ce qui conclut.
> □

4.3.2 Sous groupe $\mathbb{H}_3$ et croissance

Considérons les sous-groupes $\mathbb{H}_n$ qui stabilisent les sommets de hauteurs n.

Lemme 4.3.10:

Notons $\mathcal{U}_n$ l'ensemble des mots sur $\{0, 1\}$ de longueur exactement n.
L'isomorphisme $\psi : \mathbb{G} \to (\mathbb{G} \times \mathbb{G}) \rtimes \langle a \rangle$ induit un isomorphisme $\chi_n : \mathbb{H}_n \to \mathbb{G}^{\mathcal{U}_n}$.
De plus, pour $h \in \mathbb{H}_n$, si on note $\chi(h) = (h_u)_{u \in \mathcal{U}_n}$, alors on peut calculer h_u en utilisant les règles de réécriture Φ_0 et Φ_1 précédentes.
Pour cela, on choisit une décomposition réduite w de h et on applique l'algorithme suivant :

```
Tant que longeur(u)>0, faire:
    v ← premier caractère de u = vu'
    w ← Φ_v(w) ou on a retiré les id
    u ← u'
retourner w
```

Preuve :

On construit inductivement :
- $\psi(h) = (h_0, h_1, \mathrm{id})$, on a ainsi construit h_0 et h_1. Remarquons que $h_0, h_1 \in \mathbb{H}_{n-1}$.
- Supposons que h_u soit déjà construit pour tous les mots u de longueur $|u| \leq k < n$. Alors, pour tout $u \in \mathcal{U}_k$, $\psi(h_u) = (h_{u1}, h_{u2}, \mathrm{id})$, le troisième élément est bien id car $h_u \in \mathbb{H}_{n-k}$. On a ainsi construit $(h_u)_{u \in \mathcal{U}_{k+1}}$.

Le fait que ces éléments soient données par l'algorithme découle immédiatement de la manière dont ils sont construits et de la Proposition 4.3.6.

Ceci donne bien un morphisme car ψ en est un et qu'on ne traite qu'avec des id en troisième membre.
□

À partir de maintenant, on considère plus particulièrement le cas de $\mathbb{H}_3$.

Lemme 4.3.11:

Soit $h \in \mathbb{H}_3$, alors $\displaystyle\sum_{i,j,k=0,1} l(h_{ijk}) \leq \frac{5}{6} l_S(h) + 8$

Preuve :

Appliquant le Corollaire 4.3.8, on obtient :

$$\begin{aligned} &l(h_0) + l(h_1) \leq l(h) + 1 \\ &l(h_{i0}) + l(h_{i1}) \leq l(h_i) + 1 \implies l(h_{00}) + l(h_{01}) + l(h_{10}) + l(h_{11}) \leq l(h_0) + l(h_1) + 2 \\ &\sum_{i,j,k=0,1} l(h_{ijk}) \leq l(h_{00}) + l(h_{01}) + l(h_{10}) + l(h_{11}) + 4 \end{aligned}$$

Fixons w une décomposition réduite de h. Appliquant l'algorithme précédent, on construit w_0, w_1 puis $w_{00}, w_{01}, w_{10}, w_{11}$ et enfin les huit w_{ijk}.
Dans ce qui suit on note, pour tout $\alpha \in S$ et tout mot u sur S : $|u|_\alpha$ = le nombre d'occurrences de α dans u.
- Notons $w' = w_0 w_1$, en comptant uniquement les réductions des $a \to \mathrm{id}$, on a $|w'| \leq |w| + 1$, les seules autres réductions sont les $d \to \mathrm{id}$.
  Puisque w' est composé de w_0 et w_1, chaque d sera simplifié exactement une fois, soit par Φ_0 soit par Φ_1. On en déduit la majoration $|w'| \leq |w| + 1 - |w|_d$
- Notons $w'' = w_{00} w_{01} w_{10} w_{11}$, cette fois-ci, on a les simplifications en deux étapes de chaque c. En effet, lors de la construction de w_0 et w_1, chacun sera devenu soit un a soit un d, qui seront éliminés dans w'' comme avant. On en déduit : $|w''| \leq |w| + 3 - |w|_c$
- Notons $w''' = w_{000} \cdots w_{111}$, de la même manière, on a $|w'''| \leq |w| + 7 - |w|_b$

Également, $|w|_b + |w|_c + |w|_d \geq \dfrac{|w| - 1}{2}$ (au vu des types de décomposition réduite possibles) donc pour au moins un $\alpha \in \{b, c, d\}$, $|w|_\alpha \geq \dfrac{|w|}{6} - 1$

Combinant tous cela, on peut faire 3 majorations :

$$\begin{aligned} &\sum_{i,j,k=0,1} l(h_{ijk}) \leq |w'''| \leq |w| + 7 - |w|_b \\ &\sum_{i,j,k=0,1} l(h_{ijk}) \leq \sum_{i,j=0,1} l(h_{ij}) + 4 \leq |w''| + 4 \leq |w| + 7 - |w|_c \\ &\sum_{i,j,k=0,1} l(h_{ijk}) \leq \sum_{i,j=0,1} l(h_{ij}) + 4 \leq \sum_{i=0,1} l(h_i) + 2 + 4 \leq |w'| + 2 + 4 \leq |w| + 7 - |w|_d \end{aligned}$$

Finalement,

$$\begin{aligned}\sum_{i,j,k=0,1} l(h_{ijk}) &\leq \max\{|w|+7-|w|_b, |w|+7-|w|_c, |w|+7-|w|_d\} \\ &\leq |w|+7-\left(\frac{|w|}{6}-1\right) \\ &\leq \frac{5}{6}|w|+8\end{aligned}$$

□

Pour prouver la croissance sous-exponentielle, on va avoir besoin du lemme suivant. À nouveau, comme le Lemme 4.2.8, il est purement analytique et ne dépend pas de la structure du groupe.

Définition 4.3.12:

Soit $f : \mathbb{N} \to \mathbb{N}$, soit $k \geq 1$, on définit

$$\begin{aligned} f^{*k} : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\mapsto \sum_{\substack{(n_1,\dots,n_k):\\ \sum n_i \leq n}} f(n_1)\cdots f(n_k)\end{aligned}$$

Lemme 4.3.13:

Soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une fonction croissante, telle que :

— $f(n) \xrightarrow[n\to\infty]{} \infty$

— $\forall n \in \mathbb{N}\ f(n) \leq C f^{*k}(\alpha n)$ pour des $k \geq 2$, $\alpha \in]0,1[$

Alors, $f \overset{s}{\prec} \exp(n^\nu)$ pour un $\nu < 1$.

Preuve :

On va montrer par récurrence que, notant $\pi(n) = \log(f(n))$, on a $\pi(n) \leq An^\nu$ pour un $\nu \in]0,1[, A \geq 1$. On aura alors $f(n) \leq \exp(An^\nu)$ soit $f \overset{s}{\prec} \exp(n^\nu)$.

On commence par l'hérédité : soit $n \in \mathbb{N}$ et supposons qu'il existe $A \geq 1, \nu \in]0,1[$ tels que pour tout $m < n$, $\pi(m) \leq Am^\nu$. Alors,

$$\begin{aligned}\pi(n) &\leq \log\left(C \sum_{\substack{(n_1,\dots,n_k):\\ \sum n_i \leq \alpha n}} f(n_1)\cdots f(n_k)\right) \\ &\leq \log(C) + \log\left((\alpha n)^k \max_{\substack{(n_1,\dots,n_k):\\ \sum n_i \leq \alpha n}} f(n_1)\cdots f(n_k)\right) \\ &\leq \log(C) + k\log\alpha + k\log n + \max_{\substack{(n_1,\dots,n_k):\\ \sum n_i \leq \alpha n}} \log\left(f(n_1)\cdots f(n_k)\right)\end{aligned}$$

De plus, pour tout k-uplet $(n_1,\dots,n_k)$ tel que $\sum n_i \leq \alpha n$, on a

$$\begin{aligned}
\log(f(n_1)\cdots f(n_k)) &= \pi(n_1)+\cdots+\pi(n_k)\\
&\le A(n_1^\nu+\cdots+n_k^\nu) && \text{par hypothèse de reccurence}\\
&\le Ak\left(\frac{1}{k}\sum_{i=1}^{k} n_i\right)^\nu && \text{par concavité de } x\mapsto x^\nu\\
&\le Ak\left(\frac{\alpha n}{k}\right)^\nu = An^\nu \times \underbrace{\left[k\left(\frac{1}{k}\right)^\nu\right]}_{\xrightarrow[\nu\to 1]{}1}\\
&= An^\nu\times(1+o_\nu(1))
\end{aligned}$$

En conséquence,

$$\begin{aligned}
\pi(n) &\le (\log(C)+k\log(\alpha)+k\log(n)) + An^\nu\times(1+o_\nu(1))\\
&\le An^\nu \qquad \text{pour } A,\nu \text{ assez grand, uniformément en } n
\end{aligned}$$

On a donc bien hérédité. Pour l'initialisation, quitte à augmenter A, c'est clair.
□

Proposition 4.3.14:

$\mathbb{G}$ est à croissance sous-exponentielle. Plus précisément, $\beta(\mathbb{G},S,n)\prec\exp(n^\nu),\ \nu\in]0,1[$.

Preuve :

On considère les classes modulo $\mathbb{H}_3$, notons $N=[\mathbb{G}:\mathbb{H}_3]$. On a vu dans la Proposition 4.1.32 que $N\le 128$. On choisit un système de représentants $(u_i)_{i\in[\![0,N-1]\!]}$ tel que $l(u_i)\le 127$. On montre que cela est possible dans le lemme suivant (Lemme 4.3.15).
Soit $g\in\mathbb{G}$, g admet une unique écriture comme u_ih. Alors, $l(h)=l(u_i^{-1}g)\le 127+l(g)$
De plus, le Lemme 4.3.11 donne (avec ses notations) :

$$\sum_{i,j,k=0,1} l(h_{ijk}) \le \frac{5}{6}l(h)+8 \le \frac{5}{6}(127+l(g))+8 \le \frac{5}{6}l(g)+114$$

On peut alors majorer la fonction de croissance β de $\mathbb{G}$, pour cela on note $\mathcal{I}_n=\left\{(i_1,\dots,i_8)\in\mathbb{N}\ \middle|\ \sum_k i_k\le\frac{5}{6}n+114\right\}$. Alors,

$$\begin{aligned}
\beta(n) &\le \overbrace{128}^{\text{Nombre de classes}}\ \overbrace{\sum_{(i_1,\dots,i_8)\in\mathcal{I}_n}\beta(i_1)\dots\beta(i_8)}^{\text{Borne sur le nombre de h possibles}}\\
&\le 128\beta^{*8}\left(\frac{5}{6}n+114\right)
\end{aligned}$$

Notons alors, afin de se ramener au Lemme 4.3.13, $m=n+\lceil\frac{6}{5}114\rceil=n+137$, alors $\frac{5}{6}n+114\le\frac{5}{6}m$. De plus,

$$\beta(m)=\beta(n+137)\le\beta(n)\times|S|^{137}\le 4^{137}\beta(n)$$

Enfin,

$$\beta(m)\le 4^{137}\beta(n)\le 4^{137}\times 128\times\beta^{*8}\left(\frac{5}{6}n+114\right)\le 2^{281}\beta^{*8}\left(\frac{5}{6}m\right)$$

et le Lemme 4.3.13 conclut.
□

Lemme 4.3.15:

Soit G un groupe de type fini, soit $H < G$ un sous groupe tel que $[G : H] = N$. Fixons S une partie génératrice. Alors, il existe un système de représentants $(r_i)_{i\in[\![0,N-1]\!]}$ de G/H tel que pour tout $i \in [\![0, N-1]\!]$, on ait $l_S(r_i) \leq n-1$.

Preuve :

> On choisit 1_G pour représenter H.
>
> On considère alors les éléments de longueur 1. Parmi eux, on en choisit pour représenter autant de classes que possibles, on note leur nombre N_1.
>
> On fait idem pour toutes les longueurs k en notant le nombre de nouvelles classes représentés N_k.
>
> Supposons que pour un k donné, $N_k = 0$. Alors, pour tout $l \geq k$, $N_l = 0$. A fortiori, $N_k = 0$ si et seulement si on a déjà représenté toutes les classes.
>
> En particulier, pour tout k tel que $\sum_{i=0}^{k-1} N_i \leq N$ on a N_k non nul ce qui conclut.
>
> □

Ceci termine la preuve de la croissance intermédiaire du groupe de Grigorchuk et conclut ce document.

Je remercie mon encadrant François Dahmani pour son aide et ses conseils dans la rédaction de ce mémoire.

Références

[1] William Burnside. "On an unsettled question in the theory of discontinuous groups". In : *Quarterly Journal of Pure and Applied Mathematics* 33 (1902), p. 230-238.

[2] Pierre De la Harpe. *Topics in Geometric Group Theory*. en. Chicago Lectures in Mathematics. Chicago, IL : University of Chicago Press, 2000. ISBN : 978-0-226-31721-2. URL : https://press.uchicago.edu/ucp/books/book/chicago/T/bo3641370.html (visité le 10/02/2026).

[3] Anna Erschler et Tianyi Zheng. "Growth of periodic Grigorchuk groups". en. In : *Inventiones mathematicae* 219.3 (2020), p. 1069-1155. ISSN : 1432-1297. DOI : 10.1007/s00222-019-00922-0. URL : https://doi.org/10.1007/s00222-019-00922-0 (visité le 25/04/2026).

[4] R. I. Grigorchuk. "On Milnor's problem of group growth". English. In : *Soviet Mathematics. Doklady* 28 (1983), p. 23-26. ISSN : 0197-6788.

[5] Rostislav Grigorchuk. *Milnor's Problem on the Growth of Groups and its Consequences*. en. arXiv :1111.0512 [math]. 2013. DOI : 10.48550/arXiv.1111.0512. URL : http://arxiv.org/abs/1111.0512 (visité le 24/04/2026).

[6] Rostislav Grigorchuk et Igor Pak. *Groups of Intermediate Growth : an Introduction for Beginners*. arXiv :math/0607384 version : 1. 2006. DOI : 10.48550/arXiv.math/0607384. URL : http://arxiv.org/abs/math/0607384 (visité le 10/02/2026).

[7] Michael Gromov. "Groups of polynomial growth and expanding maps (with an appendix by Jacques Tits)". en. In : *Publications Mathématiques de l'IHÉS* 53 (1981), p. 53-78. ISSN : 0073-8301, 1618-1913. DOI : 10.1007/BF02698687. URL : https://pmihes.centre-mersenne.org/articles/10.1007/BF02698687/ (visité le 23/04/2026).

[8] J. Milnor. "A note on curvature and fundamental group". en. In : *Journal of Differential Geometry* 2.1 (1968). Publisher : Lehigh University, p. 1-7. ISSN : 0022-040X. DOI : 10.4310/jdg/1214501132. URL : https://projecteuclid.org/journals/journal-of-differential-geometry/volume-2/issue-1/A-note-on-curvature-and-fundamental-group/10.4310/jdg/1214501132.full (visité le 23/04/2026).

[9] John Milnor. "Growth of finitely generated solvable groups". en. In : *Journal of Differential Geometry* 2.4 (1968). ISSN : 0022-040X. DOI : 10.4310/jdg/1214428659. URL : https://projecteuclid.org/journals/journal-of-differential-geometry/volume-2/issue-4/Growth-of-finitely-generated-solvable-groups/10.4310/jdg/1214428659.full (visité le 24/04/2026).

[10] John Milnor et al. “Advanced Problems : 5600-5609”. In : *The American Mathematical Monthly* 75.6 (1968). Publisher : [Taylor & Francis, Ltd., Mathematical Association of America], p. 685-687. issn : 0002-9890. doi : 10.2307/2313822. url : https://www.jstor.org/stable/2313822 (visité le 24/04/2026).

[11] Geoff C. Smith et Olga M. Tabachnikova. *Topics in Group Theory*. Springer Undergraduate Mathematics Series. London : Springer, 2000. isbn : 978-1-85233-235-8 978-1-4471-0461-2. doi : 10.1007/978-1-4471-0461-2. url : http://link.springer.com/10.1007/978-1-4471-0461-2 (visité le 16/02/2026).

[12] Joseph Wolf. “Growth of finitely generated solvable groups and curvature of Riemannian manifolds”. In : *Journal of Differential Geometry - J DIFFEREN GEOM* 2 (1968). doi : 10.4310/jdg/1214428658.