Semi-groupes de matrices et applications

Paul Mercat

UNIVERSITÉ PARIS-SUD

ÉCOLE DOCTORALE 142
Mathématiques de la Région Paris-Sud
Laboratoire de Topologie et Dynamique UMR 8628

THÈSE DE DOCTORAT
de **mathématiques**

présentée par

Paul MERCAT

le 11/12/2012

Semi-groupes de matrices et applications

JURY :

Laurent BARTHOLDI	Professeur à l'Université Georg-August à Göttingen, Allemagne	Rapporteur
Yves BENOIST	Chercheur à l'Université Paris-Sud	Directeur de thèse
Gilles COURTOIS	Professeur à l'Université Paris 6	Examinateur
Vincent GUIRARDEL	Maître de conférences à l'Université de Rennes 1	Rapporteur
M. Frédéric PAULIN	Chercheur à l'Université Paris-Sud	Examinateur

À mes parents.

Remerciements

Jamais je n'arriverai à remercier suffisamment Yves Benoist. Son extrême gentillesse, sa grande disponibilité, ses connaissances étendues sur les mathématiques qu'il arrive toujours à présenter sous forme d'histoires passionnantes, sa bonne humeur communicative, en ont fait un directeur de thèse dont je ne pouvais rêver mieux. Il restera pour moi un modèle à suivre, tant sur le plan humain que sur celui des mathématiques.

Je remercie Laurent Bartholdi pour ses remarques qui ont entre autres permis d'obtenir un exemple de semi-groupe qui soit fortement automatique mais qui ne soit pas de présentation finie (voir proposition III.3.31), et permis de généraliser plusieurs résultats. Je remercie Yann Bugeaud pour ses remarques sans lesquelles je n'aurai probablement pas trouvé le théorème IV.7.13 et ses corollaires. Je remercie mes rapporteurs pour leur patience pour avoir lu ce long texte, et en particulier Vincent Guirardel pour ses nombreuses remarques pertinentes. J'aimerai également remercier Christian Mercat et Franck Gautier. Ils ont tous les deux participé à me faire aimer les mathématiques !

Et comme il n'y a pas que les maths dans la vie... Je remercie ma colocataire, pour avoir testé mes expériences culinaires et pour le cirque que l'on a fait ensemble. Je remercie les cirqueux : Denise, qui s'est beaucoup investie pour préparer les spectacles, Ismaël et son magnifique sourire, Séverine, toujours gentille et souriante, Chloé qui nous a invité de temps en temps à Nanterre, Rémi, Jérôme et Christophe pour m'avoir bien fait progressé en jonglage et accrobaties, Nathanaël avec qui j'ai appris à faire de la slack-line. Je remercie les choraleurs pour les soirées passées ensemble. Je remercie Sylvain pour les nombreuses soirées jeux et pour sa bonne cuisine. Je remercie Béatrice pour la valse, David pour le West Coast Swing et Fathi pour le rock. Je remercie notre entraîneur d'athlétisme Richard, ainsi que les membres du club athlé (qui font souvent de très bon gateaux !), Pierre-Alain, Elsa, Romain et Laure pour n'en citer que quelques-uns. Merci à Hervé, Xieyu et beaucoup d'autres que j'ai certainement oublié de citer.

Je remercie bien entendu aussi ma famille, et notamment Tiphaine et Clément qui m'ont invité de nombreuses fois chez eux, et chez qui je déguste à chaque fois des repas succulents ! Merci à mes soeurs Albane la philosophe, Sibylle la kiné, Titti la prof de maths, Armelle l'artiste, et à mon frère Jean le fashion. J'espère que l'on continuera à de se retrouver tous ensemble, à faire des voyages à vélo, et à chanter. Merci à ma mère pour les désormais traditionnels voyages à vélo dont je garde d'excellents souvenirs, et pour les nombreuses attentions qu'elle me porte. Merci à Asia et François pour leur bon accueil chaque fois que je viens à Clermont. Merci à tous ceux qui sont venu à ma soutenance, et je sais qu'il y en a qui viennent de loin.

Résumé

Nous étudions les semi-groupes de matrices avec des points de vue variés qui se recoupent. Le point de vue de la croissance s'avère relié à un point de vue géométrique : nous avons partiellement généralisé aux semi-groupes un théorème de Patterson-Sullivan-Paulin sur les groupes, qui donne l'égalité entre exposant critique et dimension de Hausdorff de l'ensemble limite. Nous obtenons cela dans le cadre général des semi-groupes d'isométries d'un espace Gromov-hyperbolique, et notre preuve nous a permis d'obtenir également d'autres résultats nouveaux. Le point de vue informatique s'avère également relié à la croissance, puisque la notion de semi-groupe fortement automatique, que nous avons introduit, permet de calculer les exposants critiques exacts de semi-groupes de développement en base β. Et ce point de vue donne également beaucoup d'autres informations sur ces semi-groupes. Cette notion de croissance s'avère aussi reliée à des conjectures sur les fractions continues telles que celle de Zaremba. Et c'est en étudiant certains semi-groupes de matrices que nous avons pu démontrer des résultats sur les fractions continues périodiques bornées qui permettent de petites avancées dans la résolution de conjectures de McMullen.

Abstract

We study matrix semigroups with different point of view that overlaps. The growth point of view seems to be related with the geometric point of view : we partially generalize to the semigroups a theorem on groups of Patterson-Sullivan-Paulin, that give the equality between the critical exponent and the Hausdorff dimension of the limit set. We obtain this in the general framework of isometries of a Gromov-hyperbolic space, and our proof give also others new results. The computer science point of view is also related to the growth, since we obtain a way to calculate exact values of critical exponents of somes β-adic development semigroups, from a notion of automatic semigroups that we introduce. Furthermore this point of view give a lot of information on these semigroups. This notion of growth shows to be also related to conjectures on continued fractions like Zaremba's one. And by studing some matrix semigroups we were able to prove some results on bounded periodic continued fractions, doing a little step in the resolution of McMullen's conjectures.

Table des matières

Chapitre I

Introduction

I.1 Motivations

Un des aspects magnifiques des mathématiques est le rapprochement de domaines qui n'avaient à priori rien à voir. Dans cette thèse, nous faisons des liens entre les fractions continues, les semi-groupes, la géométrie hyperbolique, la géométrie euclidienne, l'informatique, la théorie des nombres et la combinatoire. Précisons ces liens.

I.1.1 Arithmétique et fractions continues

L'équation de Pell-Fermat est un problème d'arithmétique bien connu. Il s'agit de trouver les solutions x et y entières de l'équation

$$x^2 - \delta y^2 = \pm 1,$$

où δ est un entier positif non carré. Il est bien connu que les solutions sont données par les développements en fractions continues tronquées du réel $\sqrt{\delta}$. Il n'est donc pas étonnant de rencontrer ces équations dans mes travaux sur les fractions continues.

I.1.2 Fractions continues et sous-semi-groupes de $SL(2,\mathbb{R})$

Dans cette thèse, je m'intéresse à des *fractions continues périodiques*, c'est-à-dire de la forme

$$[\overline{a_1, a_2, ..., a_k}] := a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k + \cfrac{1}{a_1 + \ddots}}}}}}}}.$$

Je m'intéresse en particulier aux suites de fractions continues bornées qui restent dans un même corps quadratique. Wilson a démontré (voir par exemple (Wil80), (McM09) ou le chapitre IV) que tout corps quadratique réel contient une infinité de fractions continues périodiques uniformément bornées. Par exemple les fractions continues périodiques

$$[\overline{1,1,2,1,1,2}]$$

$$[\overline{1,1,2,1,2,1,1,1,2,2,1,1}]$$

$$[\overline{1,1,2,1,2,1,1,2,1,1,1,2,2,1,1,2,1,1}]$$

$$[\overline{1,1,2,1,2,1,1,2,1,1,2,1,1,1,2,2,1,1,2,1,1,2,1,1}]$$

...

sont bornées par 2 et sont toutes dans le corps $\mathbb{Q}[\sqrt{10}]$. Pour étudier de telles fractions continues, j'utilise le lien suivant qu'il y a entre les fractions continues périodiques et certaines matrices de $SL(2,\mathbb{R})$.

$$\Updownarrow \begin{matrix} \begin{pmatrix}1\\x\end{pmatrix} \text{ est vecteur propre de } \begin{pmatrix}0&1\\1&a_1\end{pmatrix}\begin{pmatrix}0&1\\1&a_2\end{pmatrix}...\begin{pmatrix}0&1\\1&a_k\end{pmatrix}, \\ x = [\overline{a_1, a_2, ..., a_k}], \end{matrix}$$

pour $x > 1$, où $[\overline{a_1, a_2, ..., a_k}]$ est le *développement en fraction continue périodique* de x. Ainsi, l'étude des fractions continues périodiques bornées par une borne m se ramène à celle du semi-groupe engendré par les matrices $\begin{pmatrix}0&1\\1&i\end{pmatrix}$ pour $1 \leq i \leq m$, pour une borne m.

Il y a aussi un lien entre les développements en fractions continues de longueur finie

et les mêmes matrices :

$$\Updownarrow \begin{matrix} \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_2 \end{pmatrix} ... \begin{pmatrix} 0 & 1 \\ 1 & a_k \end{pmatrix} = \begin{pmatrix} * & p \\ * & q \end{pmatrix} \\ \frac{q}{p} = [a_1, a_2, ..., a_k], \end{matrix}$$

où $[a_1, a_2, ..., a_k] := a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_k}}}$ est le *développement en fraction continue* de $\frac{p}{q}$.

Le sous-semi-groupe de $SL(2, \mathbb{R})$ engendré par les matrices $\begin{pmatrix} 0 & 1 \\ 1 & i \end{pmatrix}$ pour $1 \leq i \leq m$, pour une borne m, apparaît naturellement quand on s'intéresse aux développements en fractions continues bornées de nombres rationnels. C'est en étudiant ce semi-groupe que Bourgain et Kontorovich sont parvenus dans (BK11) à faire une belle avancée dans la résolution de la conjecture de Zaremba dont l'énoncé est le suivant :

Conjecture I.1.1 (Zaremba)**.** *Il existe une constante m telle que pour tout entier $q \geq 1$, il existe un entier $0 < p < q$ premier à q tel que l'on ait*

$$\frac{p}{q} = [a_1, a_2, a_3, ...]$$

où les coefficients a_i sont des entiers entre 0 et m.

Et j'ai obtenu un autre lien entre fractions continues finies dont le dénominateur est fixé et fractions continues périodiques dans un corps fixé, qui permet de construire des fractions continues périodiques à partir de fractions continues finies.

I.1.3 Conjecture de Zaremba et combinatoire

Il y a un lien entre la conjecture de Zaremba et une donnée dynamique pour un sous-semi-groupe de $SL(2, \mathbb{R})$ que l'on appelle *exposant critique*. L'exposant critique δ_Γ d'un semi-groupe de matrices Γ s'obtient en comptant le nombre de matrices du semi-groupe qui sont de norme bornée ; c'est l'exposant de croissance de ce nombre de matrices quand la borne croît :

$$\delta_\Gamma := \limsup_{n \to \infty} \frac{\log(\#\{M \in \Gamma \; : \; \|M\| \leq n\})}{\log(n)}.$$

Il s'agit en réalité d'une vraie limite comme nous le verrons. On a alors un raffinement de la conjecture de Zaremba :

Conjecture I.1.2 (Hensley)**.** *Soit $A \subset \mathbb{N}$ un ensemble fini d'entiers, et soit δ_A l'exposant critique du sous-semi-groupe de $SL(2, \mathbb{R})$ engendré par les matrices $\begin{pmatrix} 0 & 1 \\ 1 & i \end{pmatrix}$, pour $i \in A$. Alors on a l'équivalence entre*

– $\delta_A > \frac{1}{2}$ *et*
– *pour tout entier* q *assez grand, il existe un entier* p *premier à* q *tel que l'on ait*

$$\frac{p}{q} = [a_1, a_2, a_3, ...]$$

où les coefficients a_i *sont dans l'ensemble* A.

I.1.4 Informatique, combinatoire et théorie des nombres

La conjecture de Hensley montre l'importance de savoir calculer des exposants critiques. En s'intéressant à certains semi-groupes d'un point de vue informatique, il est parfois possible de calculer la valeur exacte de l'exposant critique. Plus précisément, on s'intéresse aux semi-groupes *fortement automatiques*, c'est-à-dire les semi-groupes de type fini pour lesquels le problème de reconnaître si deux mots en les générateurs représentent le même élément du semi-groupe est décidable avec une quantité finie de mémoire et en lisant les deux mots en même temps et à la même vitesse. Cela permet de calculer des exposants critiques de semi-groupes de développements en base β, c'est-à-dire des semi-groupes de type fini engendrés par des applications $x \mapsto \beta x + t$. Il existe d'autres notions d'automaticité que j'ai relié à la mienne et que l'on trouvera par exemple dans (EC+92) et dans (Sak87).

Exemple de semi-groupe fortement automatique

Considérons le monoïde Γ, de développement en base 3, engendré par les trois transformations affines :

$$\begin{cases} 0 : & x & \mapsto & x/3, \\ 1 : & x & \mapsto & x/3 & + & 1, \\ 3 : & x & \mapsto & x/3 & + & 3. \end{cases} \tag{I.1}$$

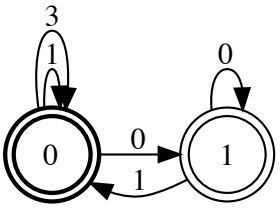
Par définition, c'est le plus petit semi-groupe contenant ces trois applications et l'identité, et l'on peut le voir comme le sous-monoïde de $SL(2, \mathbb{R})$ engendré par les matrices $\begin{pmatrix} 1/\sqrt{3} & k\sqrt{3} \\ 0 & \sqrt{3} \end{pmatrix}$, pour $k \in \{0, 1, 3\}$.
Voici quelques questions que l'on peut se poser :

– Quel est l'exposant critique de ce semi-groupe ?
– Quel est l'asymptotique du nombre d'éléments de longueur bornée en les générateurs ?
– Comment peut-on déterminer si deux mots en les générateurs représentent le même élément du semi-groupe ?
– Y a-t'il une façon de représenter les éléments du semi-groupes par des mots uniques particuliers (que l'on appelera mots réduits, ou encore forme normale) ?

La réponse à ces questions est donnée par la structure automatique du semi-groupe. Celle-ci est donnée par des automates tels que l'on peut en voir sur les figures suivantes (voir

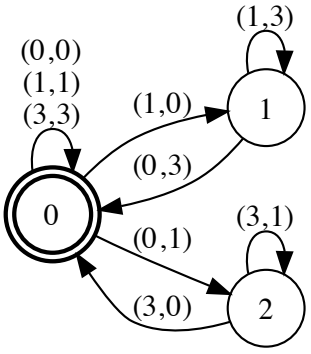
la partie III.1 pour des rappels sur les automates) :

FIGURE I.1 – Automate reconnaissant un ensemble de mots réduits du semi-groupe (I.1). Les mots réduits sont ici les mots minimaux pour l'ordre lexicographique inverse, avec $0 < 1 < 3$.



On appelle *mots réduits* un choix de représentants uniques pour les éléments du semi-groupe par des mots en les générateurs. On voit sur l'automate de la figure I.1 que les mots réduits sont ici exactement les mots ne contenant pas le mot 03.

FIGURE I.2 – Automate reconnaissant les relations du semi-groupe (I.1).



L'automate de la figure I.2 permet de voir que les relations du semi-groupe Γ s'obtiennent toutes à partir des relations $11^n0 = 03^n3$, par concaténation.

Exemple I.1.3. *Le mot* $(1,0)(1,3)(0,3)$ *est reconnu par l'automate de la figure I.2, et on a en effet la relation* $1 \circ 1 \circ 0 = 0 \circ 3 \circ 3$*, puisque l'on a l'égalité*

$$\frac{\frac{\frac{x}{3}+1}{3}+1}{3} = \frac{\frac{\frac{x}{3}+3}{3}+3}{3}.$$

Deux mots $u_1...u_n$ et $v_1...v_m$ en les générateurs $\{0,1,3\}$ représentent le même élément du semi-groupe si et seulement s'ils sont de même longueur et que le mot $(u_1,v_1)...(u_n,v_n)$ est reconnu par l'automate de la figure I.2.

L'automate de la figure I.1 fournit un moyen de connaître le nombre d'éléments du semi-groupe de longueur n donnée : celui-ci est en effet égal au nombre de chemins de longueur n de l'état initial 0 vers les états finaux 0 et 1. Ceci est donné par la somme des deux premiers coefficients des puissances de la matrice d'adjacence du graphe :

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

dont les valeurs propres sont $\frac{\sqrt{5}+3}{2}$ et $\frac{3-\sqrt{5}}{2}$. Ainsi, on voit que le nombre d'éléments du semi-groupe de longueur n est exactement f_{2n+2}, où $(f_n)_{n\in\mathbb{N}}$ est la suite de Fibonnacci :

$$\begin{aligned} f_0 &:= 0, \\ f_1 &:= 1, \\ f_{n+2} &:= f_{n+1} + f_n. \end{aligned}$$

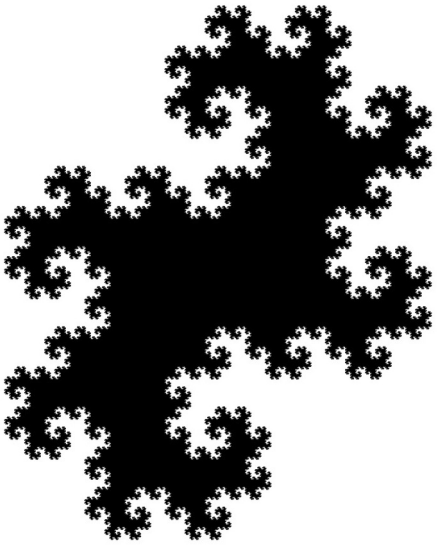
En particulier, le nombre d'éléments du semi-groupe de longueur n est asymptotiquement

$$c\left(\frac{\sqrt{5}+3}{2}\right)^n + O\left(\left(\frac{3-\sqrt{5}}{2}\right)^n\right)$$

pour une constante $c > 0$. Cela permet d'obtenir que l'exposant critique du semi-groupe vaut

$$\delta_\Gamma := \log(\frac{\sqrt{5}+3}{2}).$$

FIGURE I.3 – Ensemble limite du semi-groupe de développement en base le nombre de Pisot généralisé $\beta = 1 + i$, avec ensemble de chiffres $A = \{0, 1\}$.



La preuve du critère de forte automaticité que l'on obtient pour les semi-groupes de développement en base β utilise un peu de théorie des nombres, comme par exemple la discrétude de l'anneau des entiers du corps $\mathbb{Q}(\beta)$ dans un certain espace obtenu en considérant les conjugués réels, complexes et p-adiques de β, quand β est un nombre algébrique. L'informatique apparaît également sous une autre forme : j'ai démontré la non-forte automaticité d'un exemple explicite de semi-groupe à l'aide d'un programme informatique.

I.1.5 Théorie de Patterson-Sullivan : géométrie euclidienne et combinatoire

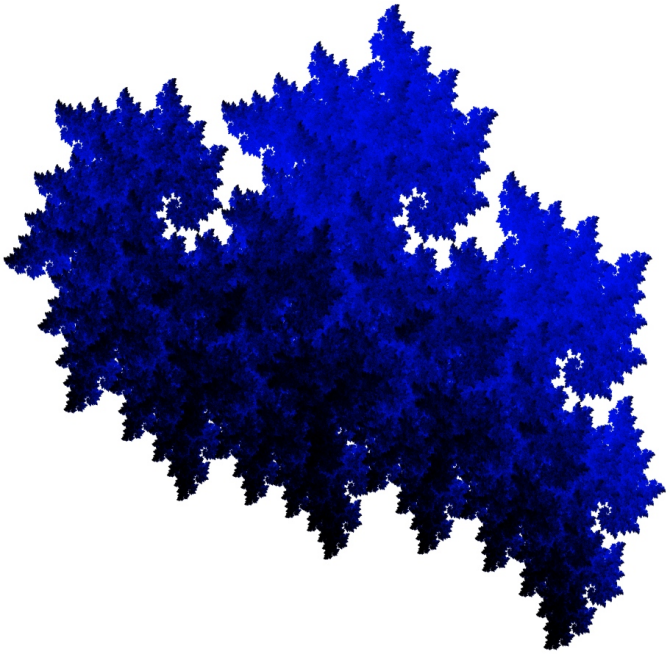
L'exposant critique δ_Γ d'un groupe Γ, qui est une donnée dynamique, peut être relié à une autre donnée qui n'avait à priori rien à voir, l'ensemble limite Λ_Γ.

L'ensemble limite Λ_Γ peut être défini, dans le cas d'un sous-groupe de $SL(2,\mathbb{R})$, comme le plus petit fermé invariant non vide pour l'action du groupe Γ sur $\hat{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$ par homographie. On s'intéressera à sa dimension de Hausdorff, que l'on notera $\dim_H(\Lambda_\Gamma)$. Il s'agit d'un nombre réel positif que l'on peut associer à toute partie de $\mathbb{R}$, ou plus généralement de $\mathbb{R}^n$ et qui mesure si un ensemble est « plus ou moins gros », et qui coïncide avec la notion de dimension pour un sous-espace vectoriel. Voici un lien entre exposant critique et ensemble limite.

Théorème I.1.4 (Patterson-Sullivan)**.** *Soit Γ un sous-groupe discret de $SL(2,\mathbb{R})$ non élémentaire et de type fini. Alors on a l'égalité*

$$\delta_\Gamma = \dim_H(\Lambda_\Gamma).$$

FIGURE I.4 – Ensemble limite d'un sous-semi-groupe de $SL(2,\mathbb{C})$ agissant par homographie sur la sphère de Riemann $\hat{\mathbb{C}}$.

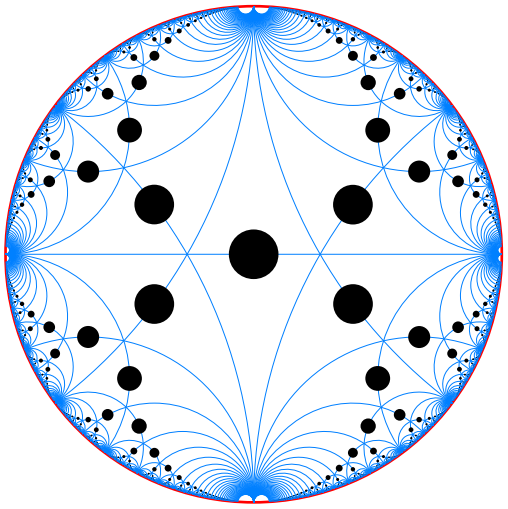


I.1.6 Géométrie hyperbolique

L'énoncé du théorème de Patterson-Sullivan ne fait pas intervenir de géométrie hyperbolique. Pourtant sa démonstration utilise de manière cruciale le fait que $SL(2,\mathbb{R})$ agisse de façon isométrique sur l'espace hyperbolique $\mathbb{H}^2_{\mathbb{R}}$. Le travail que j'ai fait pour généra-

liser ce théorème aux semi-groupes l'utilise également beaucoup et les espaces Gromov-hyperboliques forment d'ailleurs le cadre naturel de ce travail.

FIGURE I.5 – Action de $SL(2,\mathbb{Z})$ sur le disque de Poincaré



Par exemple, une des étapes clef de la preuve du théorème de Patterson-Sullivan I.1.4, est de s'intéresser à l'ensemble *limite radial* (ou conique) Λ_Γ^c qui est une partie de l'ensemble limite Λ_Γ que l'on défini grâce à l'action par isométrie sur l'espace hyperbolique du groupe (ou semi-groupe) Γ. Le lien entre géométrie euclidienne et géométrie hyperbolique est établi grâce au *produit de Gromov*. C'est un outil très utile en géométrie hyperbolique, qui permet de définir le bord d'un espace hyperbolique, qui correspondra au bord que l'on obtient par exemple avec le modèle du demi-plan $\mathbb{H}^2_{\mathbb{R}}$.

L'outil principal de la théorie de Patterson-Sullivan pour étudier l'ensemble limite d'un groupe discret d'isométries est la *mesure de Patterson-Sullivan*. C'est une mesure portée par l'ensemble limite du groupe, qui a de bonnes propriétés, et qui se définit en utilisant également l'action par isométrie sur l'espace hyperbolique.

I.2 Présentation de mes résultats

Mon travail soulève beaucoup de questions intéressantes et en résous quelques unes. Voyons quels sont les résultats obtenus et les questions qu'il reste à résoudre.

Construction de fractions continues périodiques uniformément bornées

Je me suis penché sur les conjectures de McMullen suivantes, voir (McM09) :

Conjecture I.2.1. *Tout corps quadratique réel $\mathbb{Q}[\sqrt{\delta}]$ contient une infinité de fractions continues périodiques ne comportant que les entiers* 1 *et* 2.

Voici une version moins forte mais néanmoins ouverte de cette conjecture :

Conjecture I.2.2. *Il existe un réel m tel que tout corps quadratique réel $\mathbb{Q}[\sqrt{\delta}]$ contient une infinité de fractions continues périodiques uniformément bornées par m.*

Nous démontrons les résultats :

Théorème I.2.3. *Il existe une infinité de corps quadratiques $\mathbb{Q}[\sqrt{\delta}]$ contenant chacun une infinité de fractions continues périodiques uniformément bornées par 2.*

Théorème I.2.4. *La conjecture I.1.1 de Zaremba implique la conjecture I.2.2 de McMullen.*

Le premier théorème découle d'un résultat que nous avons obtenu, permettant de construire des suites de fractions continues périodiques qui restent dans un corps quadratique donné à partir d'une fraction continue périodique d'une forme particulière :

Théorème I.2.5. *Si une fraction continue périodique de la forme*

$$[\overline{a_0, a_1, a_2, ..., a_2, a_1}]$$

est dans $\mathbb{Q}[\sqrt{\delta}]$, alors il existe deux uplets d'entiers strictement positifs $(b_1, b_2, ..., b_k)$ et $(c_1, c_2, ..., c_l)$ tels que $\mathbb{Q}[\sqrt{\delta}]$ contienne la suite injective de fractions continues périodiques

$$[\overline{b_1, b_2, ..., b_k, (a_0, a_1, a_2, ..., a_2, a_1)^n, c_1, c_2, ..., c_l, (a_1, a_2, ..., a_2, a_1, a_0)^n}]$$

En outre, si m est une borne sur les nombres a_i, alors on peut imposer que les nombres b_i et que les nombres c_i soient bornés par $2m + 1$.

Ici, $(a_0, a_1, a_2, ..., a_2, a_1)^n$ signifie que le motif $a_0, a_1, a_2, ..., a_2, a_1$ est répété n fois, et le motif $a_1, a_2, ..., a_2, a_1$ peut ou non contenir un terme médian.

Cela permet de retrouver le résultat suivant de Wilson (Wil80) :

Corollaire I.2.6. *Pour tout corps quadratique $\mathbb{Q}[\sqrt{\delta}]$, il existe un réel m_δ et une infinité de fractions continues périodiques $[\overline{a_0, a_1, ..., a_n}] \in \mathbb{Q}[\sqrt{\delta}]$ avec $1 \leq a_i \leq m_\delta$.*

Ici, m_δ dépend seulement de δ. Par exemple on peut prendre $m_{10} = 2$ d'après la suite annoncée au début. Nous démontrons que l'on peut même trouver, dans tout corps quadratique réel, une infinité de fractions continues périodiques ne comportants que trois nombres différents.

En appliquant le théorème aux réels $\sqrt{\delta} + \left\lfloor \sqrt{\delta} \right\rfloor$, on obtient que l'on peut prendre $m_\delta = 4\sqrt{\delta} + 1$, ce qui améliore le résultat de Wilson pour lequel $m_\delta = O_{\delta \to \infty}(\delta)$.

Le théorème I.2.4 découle du résultat suivant, qui permet de construire des fractions continues périodiques dans un corps donné à partir de fractions continues de certains rationnels :

Théorème I.2.7. *Soient a, b, c et δ des entiers positifs tels que*
- *(b, c) est solution de l'équation de Pell-Fermat : $c^2 - \delta b^2 = \pm 1$,*
- *a et c sont premiers entre eux et $a \leq c$.*

Alors on a l'une des égalités

$$\frac{c - a + \sqrt{\delta}}{c} = [\overline{1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n, 1, 1, a_n - 1, a_{n-1}, a_{n-2}, \ldots, a_2, a_1}]$$

ou

$$\frac{c - a + \sqrt{\delta}}{c} = [\overline{1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n - 1, 1, 1, a_n, a_{n-1}, a_{n-2}, \ldots, a_2, a_1}],$$

où $[0, a_1, a_2, \ldots, a_{n-1}, a_n]$ est le développement en fraction continue du rationnel $\frac{a}{c}$.

La conjecture de Zaremba I.1.1 est l'équivalent de la conjecture I.2.2 pour les fractions continues finies (et non plus périodiques).

Nous montrons le sens facile de la conjecture de Hensley, qui décrit quels sont les ensembles de chiffres pour lesquels la conjecture de Zaremba est vraie. Le résultat est facile et déjà connu depuis Hensley (voir (BK11)), mais nous avons jugé utile de présenter ici une preuve (courte), afin de voir le lien qu'il y a entre les fractions continues et les exposants critiques de certains sous-semi-groupes de $SL(2, \mathbb{R})$.

L'algorithme de factorisation d'entier que nous présentons n'est pas non plus un résultat important, mais il permet de voir un lien entre un problème informatique très important : la factorisation d'entiers, et un problème sur les fractions continues : le développement en fraction continue de $\sqrt{n}$ pour un entier n.

Il reste beaucoup de questions à résoudre sur les fractions continues périodiques bornées. Par exemple, la question suivante, qui est un cas particulier de la conjecture I.2.2, semble encore ouverte :

Conjecture I.2.8. *Il existe un réel m tel que tout corps quadratique réel contient une fraction continue périodique bornée par m.*

Et à nouveau la conjecture semble vraie pour $m = 2$. Nous l'avons vérifié à l'aide d'un ordinateur pour tous les corps quadratiques $\mathbb{Q}[\sqrt{\delta}]$ pour $\delta < 127$. Par exemple, le réel quadratique

$$\frac{28713227852610275789 + 5561940551265649512\sqrt{67}}{45526445508292066657}$$

a pour développement en fraction continue

$$[\overline{1, 1, 1, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 2, 1, 2, 2, 1, 2, 2, 1, 1, 2, 2, 1, 2, 1, 1, 1, 2, 2, 2, 1, 1, 1, 2, 1, 1, 2, 2, 1,}$$

$$\overline{1, 1, 1, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 1, 2, 2, 1, 1, 2, 1, 2, 2, 2, 1, 1, 1, 2, 2, 1, 2, 1, 1, 2, 2, 1,}$$

$$\overline{2, 1, 1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 1, 1, 1, 1, 2, 2, 1, 1, 2, 1, 1, 1, 2, 2, 2, 1, 1, 1, 2, 1, 2, 2, 1, 1, 2,}$$

$$\overline{2, 1, 2, 2, 1, 2, 1, 2, 2, 2, 2, 1, 2, 2, 2, 1, 2}].$$

Semi-groupes fortement automatiques

Dans ce chapitre, nous introduisons la notion de semi-groupe fortement automatique, qui consiste à avoir un ensemble de relations qui soit un langage rationnel, c'est-à-dire reconnaissable par un automate fini. Cela permet de calculer des valeurs exactes d'exposants critiques, grâce au fait que pour ces semi-groupes l'exposant critique pour la métrique des mots coïncident avec celui pour la métrique hyperbolique. Pour les semi-groupes correspondant aux développements en base β, nous démontrons le résultat suivant :

Théorème I.2.9. *Définissons un semi-groupe Γ engendré par les transformations :*

$$x \mapsto \beta x + t$$

pour $t \in A \subset \mathbb{C}$, où A est une partie finie de $\mathbb{C}$, et β un nombre complexe.

Si le nombre complexe β est transcendant, ou bien algébrique mais sans conjugué de Galois de module 1, alors pour toute partie $A \subset \mathbb{C}$ finie, le semi-groupe Γ est fortement automatique.

Réciproquement, si le nombre complexe β est algébrique et a au moins un conjugué de module 1, alors il existe une partie $A \subset \mathbb{C}$ finie telle que le semi-groupe Γ n'est pas fortement automatique.

Notre preuve étant effective, nous obtenons de plus un algorithme (dont celui de Kenyon est un cas particulier, voir (Ken97)) permettant de calculer exactement les exposants critiques des semi-groupes qui satisfont les hypothèses du théorème. Après implémentation, ceci nous a permis de donner explicitement, dans cette thèse, les exposants critiques pour de nombreux exemples de semi-groupes.

La réciproque du théorème ne permet pas de choisir la partie A. Nous parvenons à obtenir cette réciproque pour la partie $A = \{0, 1\}$ sur un exemple :

Proposition I.2.10. *Soit le nombre de Salem $\beta = \frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2} \simeq 1.8832035059$, qui est racine du polynôme $X^4 - 2X^3 + X^2 - 2X + 1$. Alors le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$

n'est pas fortement automatique.

Nous avons relié la notion de semi-groupes fortement automatiques à des notions existantes : celle de monoïde rationnel et celle de semi-groupe automatique.

Proposition I.2.11. *Un monoïde fortement automatique est rationnel. Réciproquement si un monoïde est rationnel et qu'il admet un ensemble de générateurs pour lequel il n'existe pas d'égalité entre des mots de longueurs différentes, alors il est fortement automatique.*

Proposition I.2.12. *Un semi-groupe fortement automatique est automatique.*

Pour un semi-groupe fortement automatique, nous obtenons un algorithme de recherche du mot réduit meilleur que celui existant pour les semi-groupes automatiques, car linéaire au lieu de quadratique :

Proposition I.2.13. *Si un semi-groupe est fortement automatique, alors il existe un algorithme linéaire prenant en entrée un mot et rendant le mot réduit correspondant.*

Étant donné un semi-groupe fortement automatique, la question se pose de savoir s'il est nécessairement de présentation finie. Nous montrons que la réponse est négative :

Proposition I.2.14. *Soit* $\beta \simeq 1.7924023578$ *la racine réelle du polynôme* $X^5 - X^4 - X^3 - X^2 + X - 1$. *Alors le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$

n'est pas de présentation finie.

Semi-groupes d'isométries d'un espace hyperbolique

Pour un sous-semi-groupe Γ du groupe d'isométries $\mathrm{Isom}(X)$ d'un espace Gromov-hyperbolique X propre, nous définissons une notion d'entropie (par analogie avec l'entropie volumique), qui généralise la notion d'exposant critique des groupes discrets. L'entropie est une façon de mesurer « l'espace occupé » par l'orbite d'un semi-groupe dans l'espace X, tandis que l'exposant critique mesure la quantité d'éléments. Cela permet de tenir compte des semi-groupes pour lesquels il y a un phénomène de chevauchements qui n'existe pas avec les groupes. L'énoncé suivant donne une caractérisation de l'entropie :

Théorème I.2.15. *Soit* X *un espace Gromov-hyperbolique propre à bord compacte, et soit* Γ *un semi-groupe d'isométries de* X *dont l'ensemble limite contient au moins deux points, alors on a*

$$\sup_{\substack{\Gamma' < \Gamma \\ \Gamma' \text{ semi-groupe de Schottky}}} \delta_{\Gamma'} = h_\Gamma.$$

Autrement dit, l'entropie h_Γ est la borne supérieure des exposants critiques des sous-semi-groupes de Schottky du semi-groupe Γ, c'est-à-dire des sous-semi-groupes ayant la dynamique la plus simple.

Nous supposons ici que l'espace est propre et de bord à l'infini compact, mais nous verrons que cette hypothèse n'est pas beaucoup plus forte que de demander seulement la propreté de l'espace X.

Remarque I.2.16. *Lorsque* Γ *est un groupe, si l'on remplace les semi-groupes de Schottky par des* groupes *de Schottky au sens classique, le résultat devient faux d'après un théorème de Doyle, voir (Doy88).*

Le théorème I.2.15 permet d'étudier la « dimension à l'infini » du semi-groupe, puisque l'on obtient en corollaire une généralisation d'un résultat de Paulin, voir (Pau97) :

Corollaire I.2.17. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un semi-groupe d'isométries de X dont l'ensemble limite contient au moins deux points. Alors la dimension visuelle de l'ensemble limite radial du semi-groupe Γ est égale à l'entropie du semi-groupe :*

$$\dim_{\text{vis}} \Lambda_\Gamma^c = h_\Gamma.$$

La dimension visuelle $\dim_{\text{vis}}$ est une généralisation naturelle de la dimension de Hausdorff au bord d'un espace hyperbolique. Et l'ensemble limite radial Λ_Γ^c (appelé aussi ensemble limite conique) du semi-groupe Γ est l'ensemble des points ξ du bord qui sont limite d'une quasi-géodésique de l'orbite Γo.

Ceci nous permet de calculer la dimension de Hausdorff de certains ensembles autosimilaires pour lesquels on ne savait pas encore faire à ma connaissance :

Corollaire I.2.18. *Si β est un nombre de Salem et si Γ est le sous-semi-groupe du groupe affine de $\mathbb{C}$ engendré par les applications*

$$x \mapsto \frac{x}{\beta} + t$$

où $t \in A$ pour A une partie finie de $\mathbb{Q}(\beta)$, alors on a l'égalité

$$\dim_H(\Lambda_\Gamma) = \delta_\Gamma.$$

Le résultat était connu pour un nombre de Pisot, mais semble nouveau pour un nombre de Salem. Une telle égalité est toujours à l'état de conjecture pour les semi-groupes de Kenyon.

Voici d'autres corollaires du théorème I.2.15 :

Corollaire I.2.19. *Soit X un espace Gromov-hyperbolique propre à bord compact et soit Γ un semi-groupe discret d'isométries de X dont l'ensemble limite contient au moins deux points. La limite supérieure dans la définition de l'exposant critique du semi-groupe Γ est une vraie limite :*

$$\delta_\Gamma = \lim_{n\to\infty} \frac{1}{n} \log(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}).$$

Roblin obtient des résultats plus forts pour les groupes. Voir (Rob03).

Corollaire I.2.20. *L'entropie est semi-continue inférieurement en les semi-groupes dont l'ensemble limite contient au moins deux points.*

Ce résultat généralise celui que donne F. Paulin à la fin de son article (Pau97), puisque l'on ne fait ni l'hypothèse que le semi-groupe soit un groupe, ni qu'il soit discret, ni qu'il soit de type fini, ni que l'espace soit géodésique ou quasi-géodésique, et cela fonctionne aussi bien pour la convergence algébrique que pour la convergence géométrique.

Nos résultats sur les semi-groupes permettent d'obtenir un résultat sur les groupes :

Corollaire I.2.21. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un groupe discret et sans torsion d'isométries de X ne fixant pas de point au bord, alors on a*

$$\sup_{\substack{\Gamma'<\Gamma \\ \Gamma' \text{ groupe de Schottky}}} \delta_{\Gamma'} \geq \frac{1}{2}\delta_\Gamma,$$

où la borne supérieure est prise sur l'ensemble des sous-groupes de Schottky du groupe Γ.

Dans ce dernier corollaire, déterminer si l'on peut remplacer la minoration $\geq \frac{1}{2}$ par une égalité $=$ (sans le facteur $\frac{1}{2}$) est une question ouverte.

I.3 Sommaire

Résumons les différents chapitre de cette thèse.

Chapitre II : Entropie des semi-groupes d'isométries d'espaces hyperboliques

Dans la section II.1, nous donnons les définitions et outils qui serviront dans la suite. La section II.2 est consacrée à définir et donner des propriétés sur les semi-groupes contractants. Nous y démontrons par exemple que l'ensemble limite d'un semi-groupe contractant de type fini est toujours radial. Nous construisons dans la section II.3 une grosse partie contractante d'un semi-groupe d'isométries. C'est l'étape principale pour démontrer le théorème I.2.15. Puis dans la section II.4, nous définissons ce qu'est un semi-groupe de Schottky, et l'on démontre l'existence de gros sous-semi-groupes de Schottky. Cela permettra d'avoir une preuve du théorème I.2.15. Ensuite, les sections II.5 à II.8 sont consacrées à des corollaires du théorème. Dans la première, nous obtenons une généralisation d'un résultat de F. Paulin (corollaire I.2.17, voir section II.5.1), que nous appliquons à l'étude des semi-groupes de développement en base β (voir section II.5.2). Dans la deuxième, nous voyons un résultat sur les sous-groupes de Schottky d'un groupe discret (corollaire I.2.21, voir section II.6). Nous montrons ensuite dans la section II.7 que l'exposant critique est une vraie limite. Et pour finir nous montrons la semi-continuité inférieure de l'entropie des semi-groupes (corollaire I.2.20, voir section II.8).

Chapitre III : Semi-groupes fortement automatiques

Nous commençons par faire des rappels sur les automates dans la section III.1. Dans la section III.2, nous définissons les semi-groupes fortement automatiques et voyons les liens avec les autres notions d'automaticités existantes. Nous définissons en III.2.1 ce qu'est un semi-groupe fortement automatique, et nous en donnerons quelques propriétés. Nous définissons en III.2.2 ce qu'est un monoïde rationnel et montrons la proposition I.2.11. Nous rappellons ensuite en III.2.3 ce qu'est un semi-groupe automatique, et nous montrerons en III.2.4 que les semi-groupes fortement automatiques sont automatiques (proposition I.2.12). Nous présentons notre algorithme pour le problème des mots réduits en III.2.5. Nous nous intéressons ensuite aux semi-groupes correspondants aux développements en base β dans la section III.3 où nous démontrons le théorème I.2.9 annoncé (voir théorème III.3.2 et proposition III.3.15). Enfin, la partie III.4 est consacrée à des exemples, et rappelle des travaux en lien avec les semi-groupes fortement automatiques.

Chapitre IV : Construction de fractions continues périodiques uniformément bornées

Nous commençons dans la section IV.1, par rappeler quelques propriétés des fractions continues et du semi-groupe des matrices positives. Dans la section IV.2 qui suit, nous

donnons une preuve rapide du théorème I.2.5. Puis le chapitre IV.3 explique pourquoi les suites de fractions continues périodiques de la forme $[\overline{b_1, b_2, ..., b_k, (a_1, a_2, ..., a_l)^n}]$, qui restent dans un corps quadratique donné, sont toujours triviales. Les chapitres IV.4 et IV.5 sont consacrés aux généralisations et réciproques des résultats qui nous ont permis d'obtenir le théorème I.2.5. Nous commençons dans la section IV.4 par étudier les fractions continues périodiques de la forme $BAC\,{}^tA$, puis nous continuons dans la section IV.5 en étudiant les suites de la forme $BA^nC\,{}^tA^n$. Enfin, dans le chapitre IV.6, nous explicitons les suites de fractions continues périodiques que permet d'obtenir la preuve du théorème I.2.5, et donnons des exemples. Nous finissons par la section IV.7, dans laquelle nous établissons des liens entre les fractions continues périodiques et d'autres notions. Dans la partie IV.7.1 nous montrons un lien avec l'exposant critique en démontrant le sens facile de la conjecture de Hensley, et dans la partie IV.7.2 nous démontrons le théorème IV.7.13 et montrons que la conjecture de Zaremba I.1.1 implique la conjecture de McMullen I.2.2.

Chapitre II

Entropie des semi-groupes d'isométries d'espaces hyperboliques

Nous définissons une notion d'entropie pour les semi-groupes d'isométries, qui généralise la notion d'exposant critique des groupes discrets, et qui correspond à mesurer la vitesse de croissance du point de vue de « l'espace occupé ». Le principal résultat de ce chapitre est le théorème suivant, qui permet de mesurer l'entropie d'un semi-groupe en ne regardant que ses sous-semi-groupes de Schottky (c'est-à-dire les sous-semi-groupes qui ont la dynamique la plus simple).

Théorème II.0.1. *Soit Γ un semi-groupe d'isométries d'un espace hyperbolique X propre à bord compact, dont l'ensemble limite contient au moins deux points. Alors on a l'égalité*

$$\sup\{\delta_S | S \text{ partie séparée de } \Gamma\} = \sup\{\delta_S | S \text{ semi-groupe de Schottky de } \Gamma\}.$$

Cela permet d'obtenir un certain nombre de corollaires tel que l'égalité entre entropie et dimension visuelle de l'ensemble limite (corollaire II.5.4). Nous appliquons ce corollaire aux semi-groupes de développement en base β, ce qui nous permet d'avoir l'égalité entre dimension de Hausdorff de l'ensemble limite et exposant critique d'un semi-groupe de développement en base β, pour un nombre β de Salem généralisé (proposition II.5.15). Comme autres corollaires du théorème ci-dessus, nous obtenons la semi-continuité inférieure de l'entropie (corollaire II.8.5), ou encore le fait que la limite supérieure dans la définition de l'exposant critiques des semi-groupes séparés soit une vraie limite (corollaire II.7.1). En outre, nous parvenons à reconstruire des groupes à partir de semi-groupes afin d'obtenir de « gros » sous-groupes de Schottky dans les groupes discrets (corollaire II.6.2).

II.1 Le cadre

Nous définissons ici les objets que nous manipulerons dans tout le chapitre, en commençant par les espaces Gromov-hyperboliques et leur bord. Nous verrons en particulier la définition et des propriétés de l'entropie.

On notera $d(x, y)$ la distance entre deux point $x, y \in X$ d'un espace métrique X.

II.1.1 Espaces hyperboliques

Étant donné un espace métrique, on peut définir le produit de Gromov, qui permet de mesurer le défaut d'égalité triangulaire de trois points x, y et o :

Définition II.1.1. *Soit X un espace métrique de point base o. On appelle produit de Gromov de deux points $x, y \in X$ le réel*

$$(x|y) := \frac{1}{2}\left(d(x,o) + d(y,o) - d(x,y)\right).$$

On peut alors définir la Gromov-hyperbolicité :

Définition II.1.2. *On dit qu'un espace X est δ-hyperbolique pour un réel $\delta \geq 0$, si c'est un espace métrique vérifiant l'inégalité*

$$(x|z) \geq \min\{(x|y), (y|z)\} - \delta$$

pour tous x, y et $z \in X$.

On dit qu'un espace X est Gromov-hyperbolique s'il existe un réel δ tel que l'espace X est δ-hyperbolique.

Un espace Gromov-hyperbolique est un espace qui ressemble, vu de loin, à un arbre. Les arbres sont d'ailleurs des espaces 0-hyperboliques. Dans un espace hyperbolique, un grand produit de Gromov caractérise des points qui sont « proches vus de o ».

Définissons l'exposant critique. Il s'agit de la vitesse exponentielle de croissance d'une partie de X.

Définition II.1.3. *On appelle exposant critique d'une partie $P \subset X$ d'un espace métrique X de point base o, le réel (éventuellement infini)*

$$\delta_P := \limsup_{n\to\infty} \frac{1}{n} \log(\#(B(o,n) \cap P)).$$

Par inégalité triangulaire, l'exposant critique ne dépend pas du point o choisi.

Remarque II.1.4. *On peut aussi considérer seulement les éléments d'un anneau. On a*

$$\delta_P = \limsup_{n\to\infty} \frac{1}{n} \log(\#((B(o,n+1)\backslash B(o,n)) \cap P))$$

si P est une partie non bornée.

On va maintenant définir l'entropie de n'importe quelle partie P de X. Cela correspond à la vitesse exponentielle de croissance du point de vue de l'espace occupé, et non plus du point de vu du comptage comme pour l'exposant critique.

Définition II.1.5. *Soit X un espace métrique. On dit qu'une partie $P \subseteq X$ est séparée s'il existe un réel $\epsilon > 0$ tel que la partie P soit ϵ-séparée, c'est-à-dire tel que*

$$d(x,y) > \epsilon$$

pour tous $x \neq y \in P$.
On dit qu'une partie $P \subseteq X$ est une partie couvrante de $Y \subseteq X$ s'il existe un réel $\epsilon > 0$ tel que la partie soit ϵ-couvrante de Y, c'est-à-dire telle que pour tout $y \in Y$, il existe $x \in P$ tel que

$$d(x, y) \leq \epsilon.$$

Définition II.1.6. *On appelle entropie d'une partie $P \subseteq X$ d'un espace métrique X, le réel (éventuellement infini)*

$$h_P := \sup_S \delta_{P \cap S},$$

où la borne supérieure est prise sur les parties S séparées de X.
On pose $h_\emptyset = 0$ par convention.

La remarque suivante justifie le nom d'« entropie » :

Remarque II.1.7. *Quand $X = \mathbb{H}^n_{\mathbb{R}}$, l'entropie d'une partie $P \subseteq X$ est égale à l'entropie volumique de l'ensemble $\{x \in X | d(x, P) \leq 1\}$.*

Démonstration. On peut trouver une partie S ϵ-séparée et r-couvrante de la partie P pour un réel $1 > \epsilon > 0$ assez petit et un réel r assez grand (voir II.1.30), et on peut montrer que son exposant critique est alors égale à l'entropie de P. Soit o un point de $X = \mathbb{H}^n_{\mathbb{R}}$. On a les inégalités

$$\mathrm{vol}(B(o, \epsilon)) \cdot \#B \cap S = \mathrm{vol}(\bigcup_{x \in S \cap B} B(x, \epsilon)) \leq \mathrm{vol}(B(o, n + \epsilon) \cap \{x \in X | d(x, P) \leq 1\}),$$

$$\begin{aligned} \mathrm{vol}(B(o, n) \cap \{x \in X | d(x, P) \leq 1\}) &\leq \mathrm{vol}(\bigcup_{x \in S \cap B(o, n+1+r)} B(x, r + 1)) \\ &\leq \mathrm{vol}(o, r + 1) \cdot \#B(o, n + 1 + r) \cap S. \end{aligned}$$

En passant à la limite après avoir pris le log et divisé par n, on obtient le résultat annoncé. □

Exemple II.1.8. *Dans l'espace $X = \mathbb{H}^2_{\mathbb{R}}$ muni de la métrique usuelle, l'entropie de $\mathbb{H}^2_{\mathbb{R}}$ vaut 1 et l'entropie d'une horoboule vaut $\frac{1}{2}$.*

Voici quelques propriétés de l'entropie.

Propriétés II.1.9. ***Propriétés de l'entropie***
Soit une partie $A \subseteq X$ d'un espace métrique X de point base o.

1. *L'entropie ne dépend pas du point base $o \in X$ choisi.*
2. *On a l'inégalité $h_A \leq \delta_A$.*
3. *Si la partie A est séparée, alors on a l'égalité $h_A = \delta_A$.*

4. *L'entropie est croissante : si $A \subseteq B \subseteq X$, alors on a*

$$h_A \leq h_B \leq h_X.$$

Démonstration. 1. Cela découle du fait que l'exposant critique ne dépende pas du point base o choisi, ce qui découle de l'inégalité triangulaire.

2. Pour toute partie séparée S, on a $\delta_{A\cap S} \leq \delta_A$. D'où le résultat en passant à la borne supérieure.
3. Si la partie A est séparée, on a $h_A = \sup_S \delta_{A\cap S} \geq \delta_{A\cap A} = \delta_A$.
4. Pour toute partie séparée S on a $A \cap S \subseteq B \cap S$, donc $\delta_{A\cap S} \leq \delta_{B\cap S}$. D'où le résultat en passant à la borne supérieure.

□

Définition II.1.10. *On dit qu'un espace métrique X est propre si ses boules fermées sont compactes.*

II.1.2 Bord d'un espace hyperbolique

Nous allons voir qu'à chaque espace hyperbolique on peut ajouter un bord sur lequel le produit de Gromov s'étend naturellement. L'espace hyperbolique muni de son bord est en quelque sorte une « compactification », puisque nous verrons que cette union est compacte si l'espace est propre et vérifie une propriété supplémentaire.

Soit X un espace Gromov-hyperbolique.

Définition II.1.11. *On dit qu'une suite $(x_i) \in X^{\mathbb{N}}$ est convergente si l'on a*

$$\lim_{i,j\to\infty} (x_i|x_j) = \infty.$$

On définit le bord $\partial_\infty A$ d'une partie A l'espace hyperbolique X comme quotient de l'ensemble des suites convergentes

$$\partial_\infty A := \{(x_i) \in A^{\mathbb{N}} | \lim_{i,j\to\infty} (x_i|x_j) = \infty\}/_\sim$$

par la relation d'équivalence $\sim$ définie par

$$(x_i)_{i\in\mathbb{N}} \sim (y_j)_{j\in\mathbb{N}} \quad si \quad \lim_{i,j\to\infty} (x_i|y_j) = \infty.$$

Remarque II.1.12. *Si l'on n'avait pas supposé l'espace X Gromov-hyperbolique, la relation $\sim$ définie ci-dessus ne serait pas nécessairement transitive. Par exemple elle ne l'est pas pour $X = \mathbb{R}^2$.*

Définition II.1.13. *On appelle adhérence de Gromov d'une partie $A \subseteq X \cup \partial_\infty X$ l'ensemble*

$$\overline{A} := \mathrm{Adh}\,(\mathrm{A}) \cup \partial_\infty A,$$

où $\mathrm{Adh}\,(\mathrm{A})$ *est l'adhérence de* A *dans* X*.*

Remarque II.1.14. *1. Le groupe* $\mathrm{Isom}(X)$ *agit naturellement sur le bord* $\partial_\infty X$*.*

2. Le produit de Gromov s'étend naturellement à l'adhérence de Gromov :

$$(\xi|\eta) := \sup_{\substack{x_i\to\xi\\ y_j\to\eta}} \liminf_{i,j\to\infty}(x_i|y_j),$$

pour $\xi,\eta\in\overline{X}$*.*

3. Un espace métrique X *est propre à bord compact si et seulement si l'adhérence* $\overline{X}$ *est compacte.*

Le premier point ci-dessus permet de généraliser la notion de suite convergentes à toute suite de $\overline{X}$. Cela définit la topologie que l'on considère sur l'espace $\overline{X}$. Voir aussi dans la partie « Compacité de l'adhérence » ci-dessous pour une caractérisation de la topologie de l'adhérence de Gromov de X.

Définition II.1.15. *Soit* X *un espace métrique. Étant donné un réel* $C>0$*, on dit que deux parties* A *et* B *de* X *sont* C*-disjointes si elles sont d'adhérence dans* X *disjointes et que l'on a*

$$\sup_{(a,b)\in A\times B}(a|b)<C.$$

On dit que les parties A *et* B *sont Gromov-disjointes s'il existe une constante* $C>0$ *telle que les parties* A *et* B *sont* C*-disjointes. Ces notions se généralisent de façon claire à des partie de l'espace* $\overline{X}$ *quand l'espace* X *est Gromov-hyperbolique.*

Remarque II.1.16. *Si l'espace* X *est propre et à bord compact, alors des parties* A *et* B *de* $\overline{X}$ *sont Gromov-disjointes si et seulement si leur adhérences de Gromov* $\overline{A}$ *et* $\overline{B}$ *sont disjointes, mais ceci est faux en général.*

Dire que deux partie A et B sont Gromov-disjointes revient à dire qu'elles sont disjointes en tant qu'ensembles, et « disjointes en l'infini vues du point base o ». Cette notion permettra de définir ce qu'est un semi-groupe contractant (voir II.2) et ce qu'est un semi-groupe de Schottky (voir II.4).

Compacité de l'adhérence

Nous aurons besoin de la compacité de l'adhérence $\overline{X}$ pour contrôler la façon dont l'entropie part à l'infini (voir la sous-section II.3.2).

On muni l'adhérence de Gromov $\overline{X}$ d'un espace Gromov-hyperbolique X, de la base de voisinages formée des boules ouvertes $B(x,r)$ de X et des boules

$$\beta(\xi,r) := \{x\in\overline{X}|(x|\xi)>-\log(r)\},$$

pour les points $\xi\in\partial_\infty X$. Cela définit bien la même topologie que celle donnée par les suites convergentes.

Voici une condition sur l'espace X qui sert à avoir la compacité de l'adhérence :

Définition II.1.17. *Soit X un espace métrique de point base o. On dit que l'espace X est C-strictement étoilé si pour tout point $x \in X$, il existe une C-géodésique stricte de o à x, c'est-à-dire une suite finie $(x_k)_{k=1}^n$ d'éléments de X telle que $x_0 = o$, $x_n = x$,*

$$d(x_k, x_{k+1}) \leq C,$$

$$d(x_i, x_j) \leq |d(o, x_i) - d(o, x_j)| + C,$$

pour tous $0 \leq k \leq n-1$ et $0 \leq i, j \leq n$.

Remarque II.1.18. *Un espace géodésique est C-strictement étoilé pour tout $C > 0$.*

Exemple II.1.19. *$\mathbb{Z}^n$ muni de la métrique euclidienne est $\sqrt{n}$-strictement étoilé.*

Dans cet exemple, il suffit de choisir les points x_i de $\mathbb{Z}^n$ qui sont à distance inférieure ou égale à $\sqrt{n}/2$ du segment $[o, x]$ dans $\mathbb{R}^n$.

Proposition II.1.20. *Soit X un espace Gromov-hyperbolique, propre, et C-strictement étoilé, alors son adhérence de Gromov $\overline{X}$ est compacte.*

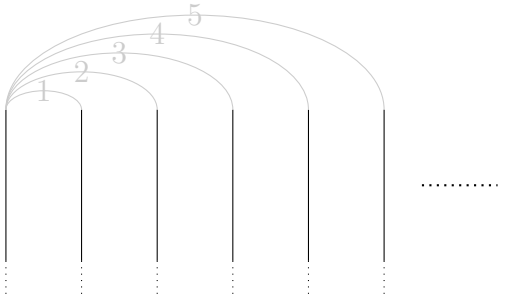
Démonstration. Il suffit de suivre la preuve du lemme 7.3 dans (HLV07). □

Exemple II.1.21. *L'ensemble $\mathbb{N} \times [0, \infty[$ muni de la métrique*

$$\begin{cases} d((i,x),(j,y)) &= i + j + x + y \quad \text{si } i \neq j \\ d((i,x),(i,y)) &= |x - y| \end{cases}$$

est Gromov-hyperbolique, propre, et d'adhérence non compacte (voir figure II.1).

FIGURE II.1 – Exemple d'espace Gromov-hyperbolique propre dont l'adhérence n'est pas compacte.

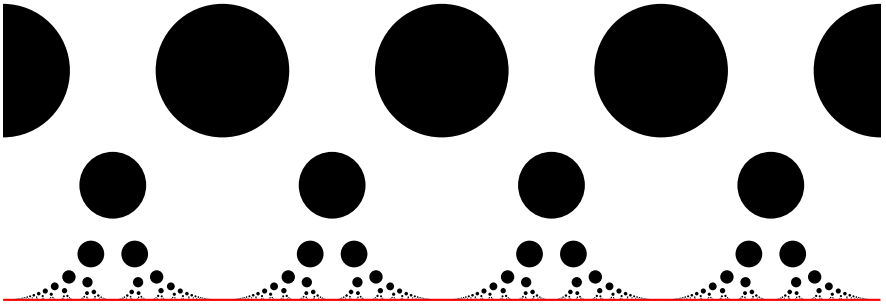


Sur la figure ci-dessus, les arêtes grises ne font pas parties de l'espace et indiquent des distances.

II.1.3 Action d'un semi-groupe d'isométries sur l'espace hyperbolique

Étant donné un ensemble d'isométries d'un espace métrique X, on définit son exposant critique, respectivement son entropie, qui correspondent aux vitesses auxquelles croît l'orbite d'un point sous l'action de l'ensemble d'isométries, d'un point de vue de comptage, respectivement d'un point de vue de l'espace occupé.

FIGURE II.2 – Action du groupe $SL(2,\mathbb{Z})$ sur le demi-plan de Poincaré $\mathbb{H}^2_{\mathbb{R}}$



Soit X un espace métrique de point base o.

Définition II.1.22. *On appelle exposant critique d'une partie $A \subset \mathrm{Isom}(X)$, l'exposant critique de l'orbite $Ao \subseteq X$:*

$$\delta_A := \delta_{Ao}.$$

Définition II.1.23. *On dit qu'une partie $A \subseteq \mathrm{Isom}(X)$ est séparée (respectivement ϵ-séparée) si l'orbite $Ao \subseteq X$ est séparée (respectivement ϵ-séparée), et si pour toutes les isométries $\gamma \neq \gamma' \in A$, on a $\gamma o \neq \gamma' o$.*

Remarque II.1.24. *En général, l'exposant critique dépend du point o choisi (par exemple pour un groupe elliptique dense), mais l'exposant critique d'une partie séparée de $\mathrm{Isom}(X)$ n'en dépend pas.*

Remarque II.1.25. *Si une partie $A \subseteq \mathrm{Isom}(X)$ est séparée et que l'orbite $A.o$ est infinie, alors l'exposant critique de la partie A est aussi l'exposant critique de la série de Poincaré P_s de A :*

$$P_s := \sum_{\gamma \in A} e^{-sd(o,\gamma o)}.$$

C'est-à-dire que la série diverge pour $s < \delta_A$ et converge pour $s > \delta_A$. Voir (Mer09) pour plus de détails.

Définition II.1.26. *On dit qu'une partie $A \subseteq \mathrm{Isom}(X)$ est une partie couvrante (respectivement ϵ-couvrante) de $B \subseteq \mathrm{Isom}(X)$ si l'orbite $Ao \subseteq X$ est une partie couvrante (respectivement ϵ-couvrante) de Bo.*

Définition II.1.27. *On appelle entropie d'une partie $A \subseteq \mathrm{Isom}(X)$ l'entropie de l'orbite $Ao \subseteq X$:*

$$h_A := h_{Ao}.$$

Remarque II.1.28. *Quand $X = \mathbb{H}^n_{\mathbb{R}}$, l'entropie d'une partie $A \subseteq \mathrm{Isom}(X)$ est égale à l'entropie volumique de l'orbite $AB(o,1)$ d'une boule $B(o,1)$.*

Voici quelques propriétés de l'entropie.

Propriétés II.1.29. ***Propriétés de l'entropie***
Soit X un espace métrique de point base o, et soit une partie $A \subseteq \mathrm{Isom}(X)$. On a les propriétés :

1. *L'entropie ne dépend pas du point base o choisi.*
2. *On a l'inégalité $h_A \leq \delta_A$.*
3. *Si la partie Ao est séparée, alors on a l'égalité $h_A = \delta_A$.*
   Ceci est en particulier le cas si A est un groupe discret.
4. *L'entropie est croissante : si $A \subseteq B \subseteq \mathrm{Isom}(X)$, alors on a*

$$h_A \leq h_B \leq h_{\mathrm{Isom}(X)}.$$

5. *Si l'espace X est propre, alors pour toute partie S couvrante de A, on a l'inégalité $h_S \geq h_A$.*
6. *Si A, B et C sont des parties de $\mathrm{Isom}(X)$ telles que l'on ait $A \subseteq B \cup C$, alors on a $h_A \leq \max\{h_B, h_C\}$.*
7. *Pour toute isométrie $\gamma \in \mathrm{Isom}(X)$, on a $h_{\gamma A} = h_A = h_{A\gamma}$.*
8. *Si l'espace X est propre, alors en posant $A_{>n} := \{\gamma \in A | d(o, \gamma o) > n\}$, on a*

$$h_{A_{>n}} = h_A.$$

Remarque II.1.30. *Pour toute partie $Y \subseteq X$ d'un espace métrique X, il existe une partie S ϵ-séparée et 2ϵ-couvrante de Y. Ainsi, quand l'espace X est propre, pour calculer l'entropie d'une partie A de $\mathrm{Isom}(X)$, on est ramené à calculer l'exposant critique d'une partie séparée de A.*

Démonstration. Les points 2, 3 et 4 sont évidents à partir des propriétés II.1.9. Le point 1 découle du fait que l'exposant critique d'une partie séparée ne dépende pas du point base o choisi.

Montrons le point 5. Soit S une partie couvrante de A et soit S' une partie séparée de A. Montrons que l'on a $\delta_{S'} \leq \delta_S$.

Cela va découler du lemme suivant.

Lemme II.1.31. *Soit X un espace métrique propre de point base o, et $Y \subseteq \mathrm{Isom}(X)$ une partie du groupe d'isométries. Alors, pour tous réels $r > 0$ et $r' > 0$, il existe une*

constante $C_{r,r'}$ telle que pour toute partie r-couvrante S de Y, pour toute partie r'-séparée S' de Y, et pour toute partie Z de Y, on ait l'inégalité

$$\#S'o \cap Z \leq C_{r,r'} \#So \cap Z^r,$$

où $Z^r := \{x \in X | \exists y \in Z : d(x,y) \leq r\}$ est le r-voisinage fermé de Z.

Démonstration. Soit S'' une partie r'-couvrante et séparée de la boule $B(o, r+r')$. Posons $C_{r,r'} := \#S''$ son cardinal, qui est fini par propreté.

Pour toute partie r'-séparée S' de X on a alors

$$\#B(o,r) \cap S' \leq \#S'' = C_{r,r'}.$$

Et comme pour toute isométrie $\gamma \in Y$, la partie $\gamma^{-1}S'$ est encore r'-séparée, on a aussi

$$\#B(\gamma o, r) \cap S' = \#B(o,r) \cap \gamma^{-1}S' \leq C_{r,r'}.$$

On a donc, pour toute partie S r-couvrante de Y, et S' partie r'-séparée de Y,

$$\#Z \cap S'o = \#Z \cap \bigcup_{\gamma \in S} B(\gamma o, r) \cap S'o \leq C_{r,r'} \#Z^r \cap So.$$

□

D'après le lemme ci-dessus, il existe une constante C telle que

$$\#(B(o,n) \cap S'o) \leq C \cdot \#(B(o, n+C) \cap So).$$

Ainsi, on a $\delta_{S'} \leq \delta_S$ en passant à la limite. On obtient alors l'inégalité souhaitée $h_A \leq \delta_S$ en passant à la borne supérieure sur les parties séparées S' de A.

Montrons maintenant le point 6. Si S est une partie séparée de A, alors on a

$$\sum_{\gamma \in A \cap S} e^{-sd(o,\gamma o)} \leq \sum_{\gamma \in B \cap S} e^{-sd(o,\gamma o)} + \sum_{\gamma \in C \cap S} e^{-sd(o,\gamma o)},$$

pour tout réel s. Donc

$$\max\{ \sum_{\gamma \in B \cap S} e^{-sd(o,\gamma o)}, \sum_{\gamma \in C \cap S} e^{-sd(o,\gamma o)} \} = \infty,$$

dès que $\sum_{\gamma \in A \cap S} e^{-sd(o,\gamma o)} = \infty$, et donc $\max\{h_B, h_C\} \geq h_A$.

Montrons le point 7. Soit $\gamma_0 \in \mathrm{Isom}(X)$, et soit S une partie r-séparée et couvrante de A, pour un réel $r > d(o, \gamma o)$. Pour tout $\gamma \in A$, l'inégalité triangulaire donne $d(o, \gamma\gamma_0 o) \leq d(o,\gamma o) + d(o, \gamma_0 o)$. Ainsi la partie $S\gamma_0$ est encore une partie séparée et couvrante de $A\gamma_0$, et on a

$$\#\{\gamma \in A \cap S | d(o,\gamma o) \leq n\} \leq \#\{\gamma' \in (A \cap S)\gamma_0 |\ d(o,\gamma' o) \leq n + d(o,\gamma_0 o)\},$$

d'où

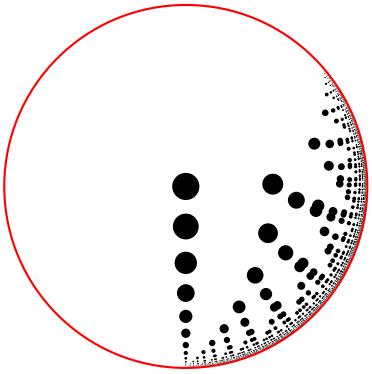
$$\begin{aligned}
h_A &= \delta_{A\cap S} \\
&= \limsup_{n\to\infty} \frac{1}{n} \log\left(\#\{\gamma \in A\cap S |\ d(o,\gamma o) \leq n\}\right) \\
&\leq \limsup_{n\to\infty} \frac{1}{n} \log\left(\#\{\gamma \in (A\cap S)\gamma_0 |\ d(o,\gamma o) \leq n + d(o,\gamma_0 o)\}\right) \\
&= \limsup_{n\to\infty} \frac{1}{n + d(o,\gamma_0 o)} \log\left(\#\{\gamma \in (A\cap S)\gamma_0 |\ d(o,\gamma o) \leq n + d(o,\gamma_0 o)\}\right) \\
&= \delta_{A\gamma_0\cap S\gamma_0} \\
&= h_{A\gamma_0}.
\end{aligned}$$

L'autre inégalité $h_{A\gamma_0} \leq h_A$ s'obtient par symétrie, en remplaçant l'élément γ_0 par γ_0^{-1} et la partie A par $A\gamma_0$. L'égalité $h_{\gamma A} = h_A$ s'obtient de la même façon.

Le point 8 s'obtient en remarquant que la partie $\Gamma\backslash\Gamma_{>n}o$ est bornée et que donc son intersection avec toute partie séparée est finie par propreté. □

Voici un exemple de semi-groupe d'exposant critique strictement supérieur à son entropie à cause d'un phénomène de chevauchements qui n'existe pas pour les groupes.

FIGURE II.3 – Orbite d'un point sous l'action du semi-groupe de l'exemple II.1.32 dans le disque de Poincaré.



Exemple II.1.32. *Le sous-semi-groupe de* $SL(2,\mathbb{R})$ *engendré par les matrices* $\begin{pmatrix} \sqrt{\frac{2}{\pi}} & 0 \\ 0 & \sqrt{\frac{\pi}{2}} \end{pmatrix}$ *et* $\begin{pmatrix} \sqrt{\frac{2}{\pi}} & 1 \\ 0 & \sqrt{\frac{\pi}{2}} \end{pmatrix}$ *et agissant sur le disque de Poincaré* $\mathbb{D}$*, a pour exposant critique* $\delta = \frac{\log(2)}{\log(\pi/2)} > 1$ *et a pour entropie* 1*. En particulier il n'est pas séparé.*

L'exposant critique du semi-groupe l'exemple ci-dessus s'obtient facilement puisque le semi-groupe est libre, et parce-que c'est un semi-groupe de développement β-adique, ce qui permet d'avoir que la norme d'un élément est comparable à sa longueur en les

générateurs :

$$\begin{aligned}\delta_\Gamma &= \limsup_{n\to\infty} \frac{1}{n}\log(\#\{\gamma\in\Gamma | d(o,\gamma o)\leq n\})\\ &= \limsup_{n\to\infty} \frac{1}{n\log(\pi/2)}\log(\#\{\gamma\in\Gamma \text{ de longueur } n\})\\ &= \frac{\log(2)}{\log(\pi/2)}.\end{aligned}$$

Le fait que l'entropie vaille 1 (le maximum pour un semi-groupe d'isométries de $\mathbb{D}$) découle du théorème I.2.17, parce-qu'il est facile de montrer que l'ensemble limite de ce semi-groupe est un segment de longueur non nulle (vu dans $\mathbb{R}$), et parce-que l'ensemble limite radial est égal à l'ensemble limite tout entier par la proposition II.2.9, puisque le semi-groupe est contractant et de type fini.

II.1.4 Action sur le bord

Les isométries d'un espace X Gromov-hyperbolique agissent naturellement sur le bord $\partial_\infty X$. Pour étudier cette action sur le bord, commençons par définir l'ensemble limite du semi-groupe.

Définition II.1.33. *Soit X un espace Gromov-hyperbolique de point base o, et soit Γ un semi-groupe d'isométries de X. On appelle ensemble limite du semi-groupe Γ, et on note Λ_Γ le bord de l'orbite Γo : $\Lambda_\Gamma := \partial_\infty(\Gamma o)$.*

Remarque II.1.34. *L'ensemble limite ne dépend pas du point base o choisi.*

On va maintenant définir une partie de l'ensemble limite appelée ensemble limite radial, dont on saura mieux contrôler la dimension visuelle.

Définition II.1.35. *On dit qu'une partie $A\subseteq X$ d'un espace métrique X est une sous-quasi-géodésique s'il existe une constante C telle que l'on ait*

$$d(x,y)+d(y,z)\leq d(x,z)+C$$

pour tous x, y et z dans A tels que $\max\{d(x,y),d(y,z)\}\leq d(x,z)$.

Remarque II.1.36. *Si l'espace X est géodésique, alors dire qu'une partie A est une sous-quasi-géodésique revient à dire qu'il existe une géodésique dont tout point de A est à distance bornée.*

Définition II.1.37. *Soit X un espace Gromov-hyperbolique de point base o et Γ un semi-groupe d'isométries de X. On appelle ensemble limite radial (ou ensemble limite conique) du semi-groupe Γ, et on note Λ_Γ^c l'ensemble :*

$$\Lambda_\Gamma^c := \{(x_i)\in(\Gamma o)^{\mathbb{N}} | \lim_{i,j\to\infty}(x_i|x_j)=\infty \text{ et } \{x_i\}_{i\in\mathbb{N}} \text{ est une sous-quasi-géodésique}\}/_\sim \subseteq \Lambda_\Gamma,$$

où $\sim$ est la relation d'équivalence vue dans la définition du bord d'un espace Gromov-hyperbolique.

Remarque II.1.38. *L'ensemble limite radial est une partie de l'ensemble limite qui ne dépend pas non plus du point base o choisi.*

Remarque II.1.39. *Si Γ est un semi-groupe de type fini d'isométries d'un espace Gromov-hyperbolique, alors son ensemble limite est auto-similaire :*

$$\Lambda_\Gamma = \bigcup_{g \text{ générateur}} g\Lambda_\Gamma.$$

Démonstration. On a clairement l'inclusion $\bigcup_{g \text{ générateur}} g\Lambda_\Gamma \subseteq \Lambda_\Gamma$. Montrons l'autre inclusion. Soit $\xi \in \Lambda_\Gamma$ et soit $(\gamma_n)_{n\in\mathbb{N}} \in \Gamma^{\mathbb{N}}$ une suite d'éléments de Γ telle que l'on ait

$$\lim_{n\to\infty} \gamma_n o = \xi.$$

(Ceci est une notation qui signifie $\lim_{n\to\infty}(\gamma_n o|\xi) = \infty$.)
Comme le semi-groupe Γ est de type fini, il existe un générateur g tel que l'on ait une sous-suite $(\gamma_{\phi(n)}) \in (g\Gamma)^{\mathbb{N}}$. On a alors $\xi = \lim_{n\to\infty} \gamma_{\phi(n)} o \in \Lambda_{g\Gamma} = g\Lambda_\Gamma$. □

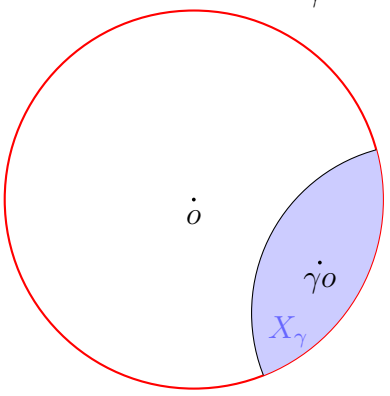
II.1.5 Les ensembles X_γ

On va associer à chaque isométrie γ d'un espace métrique X, une partie X_γ de l'espace X qui correspond à un domaine dans lequel l'élément γ contracte. Ceci nous servira dans toute la suite du chapitre.

Définition II.1.40. *Soit X un espace métrique. Pour $\gamma \in \mathrm{Isom}(X)$, on définit un domaine $X_\gamma \subseteq X$ par*

$$X_\gamma := \{x \in X | (x|\gamma o) \geq \frac{1}{2} d(o, \gamma o)\}.$$

FIGURE II.4 – X_γ



Remarque II.1.41. *L'inégalité* $(x|\gamma o) \geq \frac{1}{2}d(o,\gamma o)$ *est équivalente à*

$$d(x,\gamma o) \leq d(x,o).$$

Les éléments de X_γ *sont donc les points de* X *qui sont plus près de* γo *que de* o*.*

Le lemme suivant indique que l'ensemble X_γ est un domaine dans lequel γ contracte, et qu'il est de taille petite vue de o quand l'élément γ est de grande norme.

Lemme II.1.42. *Soit* X *un espace métrique. Pour tout* $\gamma \in \mathrm{Isom}(X)$*, on a*

1. $\gamma(X\backslash X_{\gamma^{-1}}) \subseteq X_\gamma$,
2. *Si l'espace* X *est* δ*-hyperbolique de point base* o*, alors pour tout* $(x,y) \in (\overline{X_\gamma})^2$*, on a*

$$(x|y) \geq \frac{1}{2}d(o,\gamma o) - \delta.$$

Démonstration. 1. On a

$$\begin{aligned} x \in X\backslash X_{\gamma^{-1}} &\Leftrightarrow d(x,\gamma^{-1}o) > d(x,o) \quad \text{par la remarque II.1.41,} \\ &\Leftrightarrow d(\gamma x,o) > d(\gamma x,\gamma o) \quad \text{parce-que } \gamma \text{ est une isométrie} \\ &\Rightarrow \gamma x \in X_\gamma. \end{aligned}$$

2. Soient x et y dans $\overline{X_\gamma}$. Par δ-hyperbolicité, on a

$$(x|y) \geq \min\{(x|\gamma o),(y|\gamma o)\} - \delta.$$

Or, par définition de X_γ on a pour tout x dans $\overline{X_\gamma}$

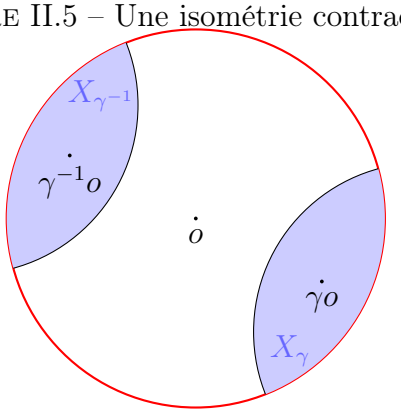
$$(x|\gamma o) \geq \frac{1}{2}d(o,\gamma o),$$

d'où le résultat.

□

Définition II.1.43. *On dit qu'une isométrie* $\gamma \in \mathrm{Isom}(X)$ *d'un espace métrique* X *est contractante si les domaines* X_γ *et* X_γ^{-1} *sont Gromov-disjoints.*

FIGURE II.5 – Une isométrie contractante.



Remarque II.1.44. *Si une isométrie γ est contractante, alors la partie $\gamma^{-1}X_\gamma \backslash X_\gamma$ est un domaine fondamental pour l'élément γ.*

Voici un critère de contraction.

Lemme II.1.45 (Critère de contraction)**.** *Soit X un espace δ-hyperbolique de point base o, et γ une isométrie de X. S'il existe deux points x et x' dans $\overline{X_\gamma} \cup \overline{X_{\gamma^{-1}}}$, tels que*

$$(x|x') < \frac{1}{2}d(o,\gamma o) - 3\delta,$$

alors l'isométrie γ est contractante.

Démonstration. Par contraposée, supposons que l'isométrie γ n'est pas contractante. Les ensembles X_γ et $X_{\gamma^{-1}}$ ne sont alors pas Gromov-disjoints. Soit alors $y \in X_{\gamma^{-1}}$ et $y' \in X_\gamma$ tels que $(y|y') \geq \frac{1}{2}d(o,\gamma o) - \delta$.

Soient aussi x et x' deux points de l'union $\overline{X_\gamma} \cup \overline{X_{\gamma^{-1}}}$. Si les points x et x' étaient tous les deux dans $\overline{X_\gamma}$ ou tous les deux dans $\overline{X_{\gamma^{-1}}}$, on aurait l'inégalité $(x|x') \geq \frac{1}{2}d(o,\gamma o) - \delta$ par le lemme II.1.42. On peut donc supposer que l'on a par exemple $x \in \overline{X_{\gamma^{-1}}}$ et $x' \in \overline{X_\gamma}$. Par δ-hyperbolicité et par le lemme II.1.42, on a alors

$$(x|x') \geq \min\{(x|y),(y|y'),(y'|x')\} - 2\delta \geq \frac{1}{2}d(o,\gamma o) - 3\delta.$$

□

Voici une propriété des isométries contractantes.

Lemme II.1.46. *Soit X un espace métrique propre, et soit $h \in \mathrm{Isom}(X)$ une isométrie contractante. Alors on a*

$$\lim_{n\to\infty} d(o,h^n o) = \infty.$$

De plus, si l'espace X est δ-hyperbolique, alors il existe un entier n_0 tel que pour tout $n \geq n_0$, les parties X_{h^n} et $X_{h^{-n}}$ soient $(M+2\delta)$-disjointes, où $M := sup_{(x,x')\in X_h \times X_{h^{-1}}}(x|x')$.

Démonstration. Montrons que l'on a $\lim_{n\to\infty} d(o, h^n o) = \infty$. Pour cela, choisissons un réel $\epsilon > 0$ tel que l'on ait

$$B(o, \epsilon) \subseteq X \backslash (X_h \cup X_{h^{-1}}).$$

Cela est possible puisque la partie $X\backslash(X_h \cup X_{h^{-1}})$ est ouverte et contient o.

Pour tous entiers $n \neq m \in \mathbb{Z}$, les boules $h^n B(o, \epsilon)$ et $h^m B(o, \epsilon)$ sont disjointes. En effet, quitte à tout composer à gauche par h^{-m}, on se ramène à $m = 0$. On a alors $B(h^n o, \epsilon) = h^n B(o, \epsilon) \subseteq X_h \cup X_{h^{-1}}$. Ainsi, l'orbite $(h^n o)_{n\in\mathbb{Z}}$ est une partie ϵ-séparée de X. Par propreté, on a donc bien $\lim_{n\to\infty} d(o, h^n o) = \infty$.

Montrons que les parties X_{h^n} et $X_{h^{-n}}$ sont $(M + 2\delta)$-disjointes. Par δ-hyperbolicité, pour $x \in X_{h^n}$ et $x' \in X_{h^{-n}}$, on a

$$(h^n o|h^{-n} o) \geq \min\{(h^n o|x), (x|x'), (x', h^{-n} o)\} - 2\delta.$$

Or, on a $h^n o \in X_h$ et $h^{-n} o \in X_{h^{-1}}$, donc on a $(h^n o|h^{-n} o) \leq M$. D'autre part, par définition de X_{h^n}, on a $(x|h^n o) \geq \frac{1}{2} d(o, h^n o)$ et de même $(x'|h^{-n} o) \geq \frac{1}{2} d(o, h^n o)$. Comme on a $\lim_{n\to\infty} d(o, h^n o) = \infty$, quitte à choisir n assez grand on a

$$d(o, h^n o) > 2M + 6\delta.$$

On obtient donc l'inégalité $(x|x') \leq M+2\delta$. Les ensembles X_{h^n} et $X_{h^{-n}}$ sont alors disjoints, puisque sinon on aurait pour $y \in X_{h^n} \cap X_{h^{-n}}$, par le lemme II.1.42, l'absurdité

$$M + 2\delta < \frac{1}{2} d(o, h^n o) - \delta \leq (y|y) \leq M + 2\delta.$$

□

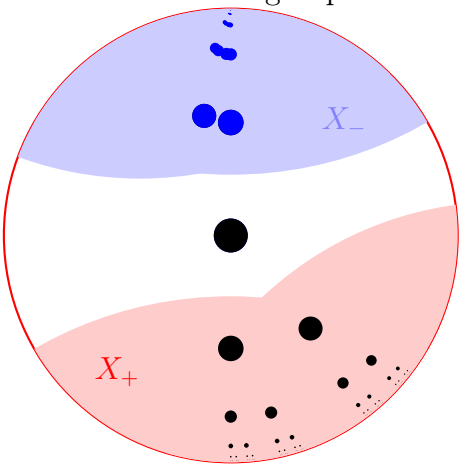
II.2 Parties contractantes de Isom(X)

Nous voyons ici la définition et des propriétés des parties contractantes. Il s'agit d'ensemble d'isométries qui contractent toutes dans la même direction, de façon contrôlée. Cette propriété est très pratique, puisqu'elle est stable par produit, et permet de contrôler la vitesse à laquelle les produits d'isométries tendent vers l'infini. Cela permet par exemple de garantir que l'ensemble limite d'un semi-groupe de type fini qui a cette propriété est radial (proposition II.2.9).

Définition II.2.1. *Soit X un espace métrique de point base o. On dit qu'une partie $A \subseteq \mathrm{Isom}(X)$ est contractante s'il existe deux domaines Gromov-disjoints X_- et X_+ de X tels que l'on ait $A(X\backslash X_-) \subseteq X_+$, et que l'on ait $o \in X \backslash \left(\overline{X_+} \cup \overline{X_-}\right)$.*

Cette définition dépend à priori du point base o choisi.

FIGURE II.6 – Un semi-groupe contractant.



Dans cette partie, nous donnons quelques résultats sur les parties contractantes qui nous seront utiles par la suite.

Voici quelques propriétés simples des parties contractantes.

Propriétés II.2.2. ***Propriétés des parties contractantes***
Soit X un espace métrique.

1. *Si γ est une isométrie contractante, alors le singleton $\{\gamma\}$ est contractant.*
2. *Si une partie $A \subseteq \mathrm{Isom}(X)$ est contractante, alors le semi-groupe engendré (c'est-à-dire l'ensemble des produits* non vides *d'éléments de A) l'est aussi.*
3. *Si une partie $A \subseteq \mathrm{Isom}(X)$ est contractante, alors l'inverse $A^{-1} := \{\gamma^{-1} | \gamma \in A\}$ l'est aussi.*

Démonstration. 1. Il suffit de prendre $X_- := X_{\gamma^{-1}}$ et $X_+ := X_\gamma$.

2. Si γ et γ' sont deux éléments d'une partie contractante A, alors on a

$$\gamma\gamma'(X \backslash X_-) \subseteq \gamma(X_+) \subseteq \gamma(X \backslash X_-) \subseteq X_+.$$

3. Si A est une partie contractante pour des domaines X_+ et X_-, alors la partie A^{-1} est contractante pour les domaines X_- et X_+ respectivement. En effet, on a pour tout $\gamma \in A$, l'inclusion $\gamma^{-1}(X \backslash X_+) \subseteq X_-$, qui se déduit de l'inclusion $\gamma(X \backslash X_-) \subseteq X_+$ par contraposée.

□

Remarque II.2.3. *La réciproque du point 1 est fausse : une isométrie γ telle que l'ensemble $\{\gamma\}$ est contractant n'est pas nécessairement contractante.*

Voici un critère de contraction.

Proposition II.2.4 (Critère de contraction)**.** *Soit X un espace δ-hyperbolique de point base o, et soit une partie $A \subseteq \mathrm{Isom}(X)$ telle que l'on ait*

$$\sup_{\gamma,\gamma' \in A} (\gamma^{-1}o | \gamma' o) < \frac{1}{2} \inf_{\gamma \in A} d(o, \gamma o) - 3\delta.$$

Alors la partie A est contractante.

Démonstration. Montrons que les domaines

$$X_+ := \bigcup_{\gamma\in A} X_\gamma \quad \text{et} \quad X_- := \bigcup_{\gamma\in A} X_{\gamma^{-1}}$$

conviennent.

On a déjà bien pour toute isométrie $\gamma \in A$, l'inclusion

$$\gamma(X\backslash X_-) \subseteq \gamma(X\backslash X_{\gamma^{-1}}) \subseteq X_\gamma \subseteq X_+.$$

Montrons maintenant que les domaines X_+ et X_- sont Gromov-disjoints. Soient $x \in X_-$ et $x' \in X_+$. Il existe alors deux isométries γ et γ' de X tels que l'on ait $x \in X_{\gamma^{-1}}$ et $x' \in X_{\gamma'}$. On a ensuite, par δ-hyperbolicité,

$$M \geq (\gamma^{-1}o|\gamma' o) \geq \min\{(\gamma^{-1}o|x), (x|x'), (x'|\gamma' o)\} - 2\delta,$$

où $M := \sup_{\gamma,\gamma'\in A}(\gamma^{-1}o|\gamma' o)$.

Or, on a $(\gamma^{-1}o|x) \geq \frac{1}{2}d(o,\gamma o)$ et $(\gamma' o|x') \geq \frac{1}{2}d(o,\gamma' o)$ par définition de $X_{\gamma^{-1}}$ et $X_{\gamma'}$. De plus, on a $M < \frac{1}{2}d(o,\gamma o) - 3\delta$ et $M < \frac{1}{2}d(o,\gamma' o) - 3\delta$ par hypothèse. On en déduit que l'on a

$$M \geq (x|x') - 2\delta.$$

Pour vérifier que les domaines X_+ et X_- sont bien Gromov-disjoints, il ne reste donc plus qu'à montrer qu'ils sont d'adhérences dans X disjointes. On a

$$\begin{aligned}
\inf_{(x,x')\in X_-\times X_+} d(x,x') &= \inf_{(x,x')\in X_-\times X_+} d(o,x) + d(o,x') - 2(x|x') \\
&\geq \left(\frac{1}{2}\inf_{\gamma\in A} d(o,\gamma o) - \delta\right) + \left(\frac{1}{2}\inf_{\gamma\in A} d(o,\gamma o) - \delta\right) - 2(M+2\delta) \\
&> (M+2\delta) + (M+2\delta) - 2(M+2\delta) \\
&= 0,
\end{aligned}$$

puisque l'on a $d(o,x) = (x|x) \geq \frac{1}{2}d(o,\gamma o) - \delta$ par le lemme II.1.42 pour $x \in X_{\gamma^{-1}}$, et de même $d(o,x') \geq \frac{1}{2}d(o,\gamma' o) - \delta$ pour $x' \in X_{\gamma'}$.

Les domaines X_- et X_+ sont donc bien Gromov-disjoints.

Pour finir, l'ensemble $X\backslash\left(\overline{X_+} \cup \overline{X_-}\right)$ contient bien le point base o, puisqu'il contient la boule ouverte $B(o, M+2\delta+\epsilon)$ pour un réel $\epsilon > 0$ assez petit. □

Voici un lemme qui permet de contrôler la taille de l'image du domaine X_+ par les éléments d'un semi-groupe contractant. Cela sera utilisé dans la preuve du théorème II.4.3.

Lemme II.2.5. *Soit X un espace métrique de point base o, soit une partie $X_+ \subseteq \overline{X}$ et soit une isométrie $\gamma \in \mathrm{Isom}(X)$ telles que l'on ait*

$$C := \sup_{x \in X_+} (\gamma^{-1}.o|x) < \infty.$$

Alors pour tous x et $x' \in X_+$, on a l'inégalité

$$(\gamma x|\gamma x') \geq d(o, \gamma o) - 2C.$$

Démonstration. Soient x et x' des éléments de X_+. On a

$$\begin{aligned}
(\gamma x|\gamma x') &= \frac{1}{2}\left[d(\gamma x, o) + d(o, \gamma x') - d(\gamma x, \gamma x')\right] \\
&= \frac{1}{2}[d(x, o) + d(\gamma^{-1}o, o) - 2(\gamma^{-1}o|x) \\
&\qquad + d(\gamma^{-1}o, o) + d(o, x') - 2(\gamma^{-1}o|x') - d(x, x')] \\
&= (x|x') - (\gamma^{-1}o|x) - (\gamma^{-1}o|x') + d(o, \gamma o) \\
&\geq (x|x') + d(o, \gamma o) - 2C \\
&\geq d(o, \gamma o) - 2C.
\end{aligned}$$

□

Le lemme qui suit dit que l'on a l'égalité triangulaire à une constante près dans un semi-groupe contractant.

Lemme II.2.6. *Soit X un espace métrique de point base o. Si A est une partie contractante de* $\mathrm{Isom}(X)$*, alors pour tous éléments γ et γ' de A on a*

$$d(o, \gamma\gamma' o) \geq d(o, \gamma o) + d(o, \gamma' o) - 2M,$$

où $M = \sup_{\gamma, \gamma' \in A}(\gamma^{-1}o|\gamma' o)$.

Démonstration. On a l'égalité $d(o, \gamma\gamma' o) = d(o, \gamma o) + d(o, \gamma' o) - 2(\gamma^{-1}o|\gamma' o)$. □

Voici une propriété intéressante des parties contractantes qui permettra de montrer que l'ensemble limite d'un semi-groupe contractant de type fini est radial.

Lemme II.2.7. *Si A est une partie contractante du groupe d'isométries* $\mathrm{Isom}(X)$ *d'un espace métrique X de point base o et si $(\gamma_n)_{n\in\mathbb{N}}$ est une suite de $A^{\mathbb{N}}$, alors l'ensemble $\{\gamma_0\gamma_1...\gamma_n o\}_{n\in\mathbb{N}}$ est une sous-quasi-géodésique.*

Preuve du lemme II.2.7. Montrons que pour $a \leq b \leq c \in \mathbb{N}$, on a

$$d(\gamma_0\gamma_1...\gamma_a o, \gamma_0\gamma_1...\gamma_b o) + d(\gamma_0\gamma_1...\gamma_b o, \gamma_0\gamma_1...\gamma_c o) \leq d(\gamma_0\gamma_1...\gamma_a o, \gamma_0\gamma_1...\gamma_c o) + M,$$

où $M = \sup_{\gamma, \gamma' \in A}(\gamma^{-1}o|\gamma' o)$. On se ramène à $a = 0$, et l'on conclut avec le lemme II.2.6 avec $\gamma = \gamma_0\gamma_1...\gamma_b$ et $\gamma' = \gamma_{b+1}\gamma_{b+2}...\gamma_c$. □

Le lemme qui suit dit que les isométries d'un semi-groupe contractant tendent vers l'infini avec leur longueur quand l'espace est propre.

Lemme II.2.8. *Si A est une partie contractante du groupe d'isométries* $\mathrm{Isom}(X)$ *d'un espace métrique propre X de point base o et si $(\gamma_n)_{n\in\mathbb{N}}$ est une suite de $A^{\mathbb{N}}$, alors on a*

$$\lim_{n\to\infty} d(o, \gamma_0\gamma_1...\gamma_n o) = \infty.$$

Démonstration. L'ensemble $\{\gamma_0...\gamma_n o\}_{n\in\mathbb{N}}$ est une partie séparée de X. En effet, il existe un réel $\epsilon > 0$ tel que la boule $B(o,\epsilon)$ soit incluse dans $X\backslash(X_+ \cup X_-)$, et ses images par les éléments $\gamma_0...\gamma_n$ sont disjointes, puisque pour toute isométrie γ de A, on a l'inclusion $\gamma B \subseteq X_+$. Le résultat découle alors de la propreté de l'espace X. □

Proposition II.2.9. *Soit X un espace métrique propre et Γ un semi-groupe d'isométries de X, contractant et de type fini. Alors l'ensemble limite de Γ est radial :*

$$\Lambda_\Gamma = \Lambda_\Gamma^c.$$

Démonstration. Soit ξ un point de l'ensemble limite Λ_Γ. D'après la remarque II.1.39, il existe un générateur g_0 du semi-groupe Γ tel que $\xi \in g_0\Lambda_\Gamma$. Par récurrence, il existe une suite $(g_i)_{i\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, on ait

$$\xi \in g_0...g_n\Lambda_\Gamma.$$

Puis par le lemme II.2.8, on a $\lim_{n\to\infty} d(o, g_0...g_n o) = \infty$. On a donc $\xi = \lim_{n\to\infty} g_0...g_n o$ par le lemme II.2.5 appliqué à l'isométrie $g_0...g_n$ et à l'ensemble $X_+ = \Lambda_\Gamma \cup \{o\}$. Or, le lemme II.2.7 affirme que l'ensemble $\{g_0...g_n o\}_{n\in\mathbb{N}}$ est une sous-quasi-géodésique, donc le point ξ est dans dans l'ensemble limite radial : $\xi \in \Lambda_\Gamma^c$. On a montré l'inclusion $\Lambda_\Gamma \subseteq \Lambda_\Gamma^c$. L'autre inclusion est claire. □

Le fait que le semi-groupe Γ soit de type fini est une hypothèse nécessaire, comme le montre le contre-exemple suivant :

Contre-exemple II.2.10. *Soit Γ le sous-semi-groupe de $SL(2,\mathbb{Z})$ engendré par les matrices* $\begin{pmatrix} 1 & n \\ n & n^2+1 \end{pmatrix}, n \geq 1$. *Alors le semi-groupe Γ est contractant, mais les ensembles limite et limite radial diffèrent : $\Lambda_\Gamma \neq \Lambda_\Gamma^c$.*

En effet, l'enveloppe convexe $X_+ \subset \mathbb{H}^2_{\mathbb{R}}$ de l'intervalle $[-\frac{1}{2}, 1]$ dans $\mathbb{H}^2_{\mathbb{R}}$ (en identifiant le bord de $\mathbb{H}^2_{\mathbb{R}}$ à $\mathbb{R}$ de façon usuelle) est envoyée dans celle de l'intervalle $[0, \frac{2}{3}]$, et donc le semi-groupe est contractant. Mais le point 0 est dans l'ensemble limite, et n'est pas radial.

II.3 Construction d'une grosse partie contractante

Le but de cette section est de démontrer le théorème :

Théorème II.3.1. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un semi-groupe d'isométries de X dont l'ensemble limite Λ_Γ contient au moins deux points. Alors il existe un sous-semi-groupe Γ' de Γ, contractant et de même entropie :*

$$h_{\Gamma'} = h_\Gamma.$$

Ce théorème est l'étape principale de la preuve du théorème I.2.15.

La preuve du théorème II.3.1 repose sur l'étude du support du semi-groupe Γ, qui est une partie fermée et $\Gamma \times \Gamma^{-1}$-invariante de $\partial_\infty X \times \partial_\infty X$ décrivant les directions dans lesquelles il y a beaucoup d'isométries qui contractent et dilatent. On montre que ce support, s'il n'est pas réduit à deux points, fournit un sous-semi-groupe contractant d'entropie h_Γ. Et pour cela, on commence par montrer qu'il existe une isométrie contractante dans le semi-groupe Γ, et on effectue un ping-pong entre cet élément et une « grosse » partie du semi-groupe Γ. Puis l'on montre que dans le cas où le support est réduit à deux points, le semi-groupe fixe un doublet de points au bord, ce qui permet de conclure rapidement si le semi-groupe ne fixe pas de point au bord. Enfin, on termine par le cas où le semi-groupe fixe un point au bord. Dans ce cas, on ne peut pas effectuer de ping-pong, mais l'existence d'une isométrie contractante nous permet de démontrer qu'il existe une proportion suffisante des éléments du semi-groupe qui contractent loin du point fixe. On fera cela en utilisant le lemme des tiroirs sur une partition en copies d'un domaine fondamental pour l'isométrie contractante.

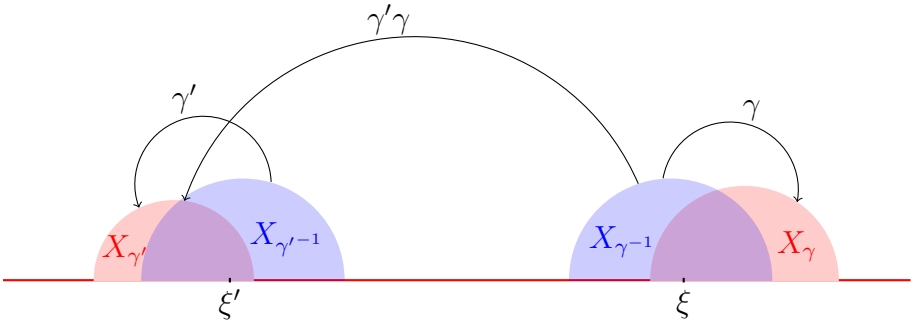
II.3.1 Construction d'une isométrie contractante

Nous allons montrer qu'un semi-groupe d'isométries d'un espace Gromov-hyperbolique dont l'ensemble limite contient au moins deux points possède toujours une isométrie contractante. On a la proposition :

Proposition II.3.2. *Soit X un espace Gromov-hyperbolique, et Γ un semi-groupe d'isométries de X dont l'ensemble limite n'est pas réduit à un point. Alors Γ contient une isométrie h contractante. De plus, si η est un point du bord de X, alors on peut choisir h tel que $\eta \notin X_h$.*

L'idée de la preuve est de considérer deux grands éléments de Γ qui contractent en deux endroits distincts (près de points distincts de l'ensemble limite). Le produit de ces deux élément est alors contractant parce-que ces deux éléments n'étant pas contractants (sinon il n'y a rien à démontrer) et ayant une grande norme, leur inverses contractent à nouveau près des mêmes points, et ainsi, le produit contracte depuis l'un des endroits vers l'autre. (voir figure II.7.)

FIGURE II.7 – Construction d'une isométrie contractante à partir de deux isométries γ et γ' non contractantes.



Démonstration. Supposons pour commencer que l'ensemble limite contienne au moins trois points. Soit $\eta \in \Lambda_\Gamma$, et soient $\xi \neq \xi'$ deux points distincts de l'ensemble limite Λ_Γ, et qui sont distincts du point η, et soient γ et γ' deux isométries de Γ telles que l'on ait

$$(\xi|\gamma o) > 2(\xi|\xi') + 10\delta + (\xi|\eta) \quad \text{et} \quad (\xi'|\gamma' o) > 2(\xi|\xi') + 10\delta + (\xi'|\eta).$$

On a alors également $d(o, \gamma o) \geq (\xi|\gamma o) > 2(\xi|\xi') + 10\delta + (\xi|\eta)$ et $d(o, \gamma' o) > 2(\xi|\xi') + 10\delta + (\xi'|\eta)$.

Si une des isométries γ ou γ' était contractante, alors elle conviendrait, et la preuve serait finie. En effet, on a $\eta \notin X_\gamma$ et $\eta \notin X_{\gamma'}$, puisque par δ-hyperbolicité on a

$$(\eta|\xi) \geq \min\{(\eta|\gamma o), (\gamma o|\xi)\} - \delta,$$

et donc $(\gamma o|\eta) \leq (\eta|\xi) + \delta < \frac{1}{2} d(o, \gamma o)$, et de même avec γ'. On peut donc supposer que les éléments γ et γ' ne sont pas contractants.

On a alors le lemme suivant.

Lemme II.3.3. *Les ensembles $X_{\gamma^{-1}}$ et $X_{\gamma'}$ sont $((\xi|\xi') + 2\delta)$-disjoints.*

Démonstration. Soient $x \in X_{\gamma^{-1}}$ et $x' \in X_{\gamma'}$. Par δ-hyperbolicité, on a

$$(\xi|\xi') \geq \min\{(\xi|x), (x|x'), (x'|\xi')\} - 2\delta.$$

Or, par le lemme II.1.45, on a $(\xi|x) \geq \frac{1}{2} d(o, \gamma o) - 3\delta > (\xi|\xi') + 2\delta$, et de même pour $(\xi'|x')$. On conclut donc que l'on a

$$(x|x') \leq (\xi|\xi') + 2\delta.$$

Pour finir la preuve du lemme, il reste à montrer que les parties $X_{\gamma^{-1}}$ et $X_{\gamma'}$ sont d'adhérences dans X disjointes. Par l'absurde, supposons qu'il existe $y \in \mathrm{Adh}\,(\mathrm{X}_{\gamma^{-1}}) \cap \mathrm{Adh}\,(\mathrm{X}_{\gamma'}) = X_{\gamma^{-1}} \cap X_{\gamma'}$. On a alors d'une part $(y|y) \geq \frac{1}{2} d(o, \gamma o) - \delta > (\xi|\xi') + 4\delta$ par le lemme II.1.42, et d'autre part $(y|y) \leq (\xi|\xi') + 2\delta$ par l'inégalité ci-dessus. Contradiction. □

Montrons alors que l'isométrie $\gamma'\gamma$ est contractante.

On a

$$\gamma'\gamma o \in \gamma'(X_\gamma) \subseteq \gamma'(X \backslash X_{\gamma'^{-1}}) \subseteq X_{\gamma'},$$

et de même $\gamma^{-1}\gamma'^{-1}o \in X_{\gamma^{-1}}$, donc par le lemme ci-dessus

$$(\gamma'\gamma o|(\gamma'\gamma)^{-1}o) \leq (\xi|\xi') + 2\delta < \frac{1}{2}d(o,\gamma o) - 3\delta.$$

Or, on a $d(o,\gamma o) \leq d(o,\gamma'\gamma o)$. En effet, on a

$$d(o,\gamma o) = d(o,\gamma'\gamma o) - d(o,\gamma' o) + 2(\gamma'^{-1}o|\gamma o).$$

Or, en utilisant le lemme ci-dessus avec γ et γ' permutés, on obtient $(\gamma'^{-1}o|\gamma o) \leq (\xi|\xi') + 2\delta$, et d'autre part, on a $d(o,\gamma' o) \geq 2(\xi|\xi') + 10\delta$. On obtient donc bien

$$d(o,\gamma o) \leq d(o,\gamma'\gamma o) - 2(\xi|\xi') - 10\delta + 2(\xi|\xi') + 4\delta \leq d(o,\gamma'\gamma o),$$

et donc

$$(\gamma'\gamma o|(\gamma'\gamma)^{-1}o) < \frac{1}{2}d(o,\gamma'\gamma o) - 3\delta.$$

Donc l'élément $\gamma\gamma'$ est contractant par le critère de contraction (lemme II.1.45). Pour finir, on a $\eta \notin X_{\gamma'} \supseteq X_{\gamma'\gamma}$ d'après ce que l'on a fait ci-avant.

Supposons maintenant que l'ensemble limite Λ_Γ soit réduit à deux points :

$$\Lambda_\Gamma = \{\xi, \eta\}.$$

Par Γ-invariance de l'ensemble limite, les isométries de Γ fixent le doublet $\{\xi, \eta\}$. Distinguons alors deux cas :

1. Si toutes les isométries de Γ fixent chacun des points ξ et η, considérons une isométrie γ telle que

   $$(\gamma o|\xi) > 2(\xi|\eta) + 6\delta.$$

   Celle-ci existe bien puisque l'on a $\xi \in \Lambda_\Gamma$. On a alors le lemme :

   Lemme II.3.4. *On a $\eta \notin X_\gamma$ et $\eta \in X_{\gamma^{-1}}$.*

   Démonstration. Commençons par montrer que l'on a $\eta \notin X_\gamma$. Par δ-hyperbolicité, on a

   $$(\xi|\eta) \geq \min\{(\xi|\gamma o), (\gamma o|\eta)\} - \delta,$$

   et donc $(\gamma o|\eta) \leq (\xi|\eta) + \delta < \frac{1}{2}d(o,\gamma o)$, ce qui prouve la première partie du lemme. On a ensuite $\eta = \gamma^{-1}\eta \in X_{\gamma^{-1}}$, puisque l'isométrie γ fixe le point η. □

   Pour terminer la preuve de la proposition dans le cas où toutes les isométries fixent chacun des points ξ et η, il ne reste plus qu'à démontrer le lemme :

   Lemme II.3.5. *L'isométrie γ est contractante.*

Démonstration. Le point fixe ξ est dans l'union $\overline{X_\gamma} \cup \overline{X_{\gamma^{-1}}}$, puisque si l'on avait $\xi \notin \overline{X_\gamma} \cup \overline{X_{\gamma^{-1}}}$, alors on aurait $\xi = \gamma\xi \in \overline{X_\gamma}$, ce qui est absurde.
Le fait que l'isométrie γ soit contractante découle alors du critère de contraction II.1.45, puisque l'on a

$$(\xi|\eta) < \frac{1}{2}d(o,\gamma o) - 3\delta.$$

□

2. S'il existe une isométrie $\gamma_0 \in \Gamma$ qui échange ξ et η, c'est-à-dire $\gamma_0\xi = \eta$ et $\gamma_0\eta = \xi$.
La première partie de la preuve permet d'obtenir une isométrie contractante $h \in \Gamma$, mais avec $\eta \in X_h$. En outre, on peut choisir l'isométrie h aussi grande que l'on veut, et donc demander à avoir l'inégalité

$$(ho|\eta) > 2(\xi|\eta) + 4d(o,\gamma_0 o) + 6\delta.$$

Montrons qu'alors l'isométrie $\gamma := \gamma_0 h \gamma_0$ convient. Pour cela, nous allons utiliser le critère de contraction II.1.45 avec les points ξ et η. On a le lemme suivant.

Lemme II.3.6. *On a $\eta \notin X_\gamma$ et $\xi \notin X_{\gamma^{-1}}$.*

Démonstration. Montrons que $\eta \notin X_\gamma$. On a

$$\begin{aligned}(\eta|\gamma o) &= (\gamma_0\xi|\gamma_0 h\gamma_0 o)\\ &= (\xi|h\gamma_0 o) - (\xi|\gamma_0^{-1}o) - (h\gamma_0 o|\gamma_0^{-1}o) + d(o,\gamma_0 o)\\ &\leq (\xi|h\gamma_0 o) + d(o,\gamma_0 o).\end{aligned}$$

Et par δ-hyperbolicité, on a

$$(\xi|\eta) \geq \min\{(\xi|h\gamma_0 o), (h\gamma_0 o|\eta)\} - \delta.$$

Or, le point $\gamma_0 o$ n'est pas dans l'ensemble $X_{h^{-1}}$ d'après le lemme II.1.42, puisque l'on a $(\gamma_0 o|\gamma_0 o) = d(o,\gamma_0 o) < \frac{1}{2}d(o,ho) - \delta$. On a donc $h\gamma_0 o \in X_h$. Comme on a aussi $\eta \in X_h$, le lemme II.1.42 donne

$$(\eta|h\gamma_0 o) \geq \frac{1}{2}d(o,ho) - \delta > (\xi|\eta) + \delta.$$

Ainsi, on obtient

$$\begin{aligned}(\eta|\gamma o) &\leq (\xi|h\gamma_0 o) + d(o,\gamma_0 o)\\ &\leq (\xi|\eta) + d(o,\gamma_0 o) + \delta\\ &< \frac{1}{2}d(o,ho) - d(o,\gamma_0 o)\\ &\leq \frac{1}{2}d(o,\gamma_0 h\gamma_0 o),\end{aligned}$$

ce qui prouve que η n'est pas dans X_γ.
On montre de manière semblable que ξ n'est pas dans $X_{\gamma^{-1}}$. □

Ainsi, on a $\xi = \gamma_0\eta = \gamma_0 h\eta = \gamma\xi \in X_\gamma$ et de même $\eta \in X_{\gamma^{-1}}$. Le critère de contraction II.1.45 s'applique donc, puisque l'on a bien l'inégalité

$$(\xi|\eta) < \frac{1}{2}d(o, ho) - d(o, \gamma_0 o) - 3\delta \leq \frac{1}{2}d(o, \gamma o) - 3\delta.$$

□

II.3.2 Support d'un semi-groupe

Définissons le support d'un ensemble d'isométries, qui correspond aux couples de points du bord pour lesquels il y a beaucoup d'isométries qui contractent dans un voisinage du premier point du couple et dilatent depuis un voisinage du deuxième point du couple. Le support d'un semi-groupe est à relier au support de la mesure de Patterson-Sullivan, mais il est plus simple à définir et à manipuler.

Définition II.3.7. *Soit X un espace Gromov-hyperbolique de point base o. On appelle support d'une partie $A \subseteq \mathrm{Isom}(X)$ l'ensemble*

$$\mathrm{supp}(A) := \{(\xi, \mu) \in \partial_\infty X \times \partial_\infty X |\ \textit{pour tout } \epsilon > 0,\ h_{A^{\beta(\xi,\epsilon)\times\beta(\mu,\epsilon)}} = h_A\},$$

où l'on a posé $\beta(\xi, \epsilon) := \{x \in \overline{X} |\ (\xi|x) > -\log(\epsilon)\}$ et

$$A^{\beta(\xi,\epsilon)\times\beta(\mu,\epsilon)} := \{\gamma \in A |\ \gamma o \in \beta(\xi, \epsilon)\ \textit{et}\ \gamma^{-1}o \in \beta(\mu, \epsilon)\}.$$

On peut montrer que le support ne dépend pas du point base o choisi.

Proposition II.3.8. *Soit X un espace Gromov-hyperbolique propre à bord compact. Alors le support de toute partie $\Gamma \subseteq \mathrm{Isom}(X)$ est non vide.*

Démonstration. Soit $\delta > 0$ tel que l'espace X soit δ-hyperbolique. Construisons par récurrence une suite $(\xi_n, \eta_n)_{n\in\mathbb{N}}$ de couples de points du bord telle que l'on ait l'égalité $h_{\Gamma^{\beta(\xi_n,e^{-2\delta n})\times\beta(\eta_n,e^{-2\delta n})}} = h_\Gamma$, et que l'on ait

$$\beta(\xi_n, e^{-2\delta n}) \times \beta(\eta_n, e^{-2\delta n}) \cap \beta(\xi_{n+1}, e^{-2\delta(n+1)}) \times \beta(\eta_{n+1}, e^{-2\delta(n+1)}) \neq \emptyset.$$

Pour $n = 0$, tous les points ξ_0 et $\eta_0 \in \partial_\infty X$ conviennent puisque l'on a $\beta(\xi_0, 1) = \overline{X} = \beta(\eta_0, 1)$.

Supposons ξ_n et η_n construits tels que $h_{\Gamma^{\beta(\xi_n,e^{-2\delta n})\times\beta(\eta_n,e^{-2\delta n})}} = h_\Gamma$. Le carré $\partial_\infty X \times \partial_\infty X$ du bord étant compact, il en va de même du pavé fermé $(\overline{\beta(\xi_n, e^{-2\delta n})} \cap \partial_\infty X) \times (\overline{\beta(\eta_n, e^{-2\delta n})} \cap \partial_\infty X)$, et l'on peut extraire un recouvrement fini du recouvrement par les pavés ouverts $\beta(\xi, e^{-2\delta(n+1)}) \times \beta(\eta, e^{-2\delta(n+1)})$ quand (ξ, η) décrit $\beta(\xi_n, e^{-2\delta n}) \times \beta(\eta_n, e^{-2\delta n})$.

Le complémentaire dans $\beta(\xi_n, e^{-2\delta n}) \times \beta(\eta_n, e^{-2\delta n})$ de ce recouvrement est alors borné. Or, l'entropie d'une partie bornée de X est nulle : on a

$$h_{\Gamma^{B(o,R)\times B(o,R)}} = 0,$$

pour tout $R > 0$, par propreté. Par le point 6 des propriétés II.1.29 de l'entropie, il existe alors un couple (ξ_{n+1}, η_{n+1}) de $\beta(\xi_n, e^{-2\delta n}) \times \beta(\eta_n, e^{-2\delta n})$ vérifiant

$$h_{\Gamma^{\beta(\xi_{n+1}, e^{-2\delta(n+1)})\times\beta(\eta_{n+1}, e^{-2\delta(n+1)})}} \geq h_{\Gamma^{\beta(\xi_n, e^{-2\delta n})\times\beta(\eta_n, e^{-2\delta n})}} = h_\Gamma.$$

La suite $\big(\beta(\xi_n, e^{-2\delta n+2\delta}) \times \beta(\eta_n, e^{-2\delta n+2\delta})\big)_{n\in\mathbb{N}}$ ainsi obtenue des pavés grossis de $e^{2\delta}$ est alors décroissante. En effet, soit $x \in \beta(\xi_{n+1}, e^{-2\delta(n+1)+2\delta})$ et soit $y \in \beta(\xi_{n+1}, e^{-2\delta(n+1)}) \cap \beta(\xi_n, e^{-2\delta n})$. Par δ-hyperbolicité on a alors

$$(x|\xi_n) \geq \min\{(x|\xi_{n+1}), (\xi_{n+1}|y), (y|\xi_n)\} - 2\delta > 2\delta n - 2\delta,$$

ce qui donne bien l'inclusion $\beta(\xi_{n+1}, e^{-2\delta(n+1)+2\delta}) \subseteq \beta(\xi_n, e^{-2\delta n+2\delta})$. En faisant de même avec η, on obtient bien la décroissance souhaitée.

La suite converge donc vers un point (ξ, η). Ce point est bien dans le support $\mathrm{supp}(\Gamma)$, puisque pour tout $\epsilon > 0$, on peut trouver par Gromov-hyperbolicité un entier n assez grand tel que l'on ait l'inclusion

$$\beta(\xi_n, e^{-2\delta n+2\delta}) \times \beta(\eta_n, e^{-2\delta n+2\delta}) \subseteq \beta(\xi, \epsilon) \times \beta(\eta, \epsilon),$$

et donc tel que l'on ait l'inégalité $h_\Gamma = h_{\Gamma^{\beta(\xi_n, e^{-2\delta n+2\delta})\times\beta(\eta_n, e^{-2\delta n+2\delta})}} \leq h_{\Gamma^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}}$.

□

Remarque II.3.9. *C'est un des seuls endroits de la preuve où l'on utilise la compacité de l'adhérence de l'espace X (l'autre endroit où l'on utilise cette compacité est pour définir la mesure de Patterson-Sullivan, voir II.5.1 a)). Cette hypothèse n'est pas beaucoup plus forte que de demander seulement la propreté de l'espace X (voir II.1.2).*

Voici une propriété de Γ-invariance du support :

Proposition II.3.10. *Soit X un espace Gromov-hyperbolique et soit Γ un semi-groupe d'isométries de X. Le support* $\mathrm{supp}(\Gamma)$ *est $\Gamma \times \Gamma^{-1}$-invariant pour l'action de* $\mathrm{Isom}(X) \times \mathrm{Isom}(X)$ *sur $\partial_\infty X \times \partial_\infty X$ donnée par*

$$(\gamma, \gamma'^{-1})(\xi, \eta) := (\gamma\xi, \gamma'^{-1}\eta),$$

pour toutes isométries γ et $\gamma' \in \mathrm{Isom}(X)$ et $(\xi, \eta) \in \partial_\infty X \times \partial_\infty X$.

C'est-à-dire que l'on a $(\gamma\xi, \gamma'^{-1}\eta) \in \mathrm{supp}(\Gamma)$ pour tout $(\xi, \eta) \in \mathrm{supp}(\Gamma)$ et tout $(\gamma, \gamma') \in \Gamma \times \Gamma$.

Démonstration. Soient $(\xi, \eta) \in \mathrm{supp}(\Gamma)$ et $(\gamma, \gamma') \in \Gamma\times\Gamma$. Montrons que l'on a $(\gamma\xi, \gamma'^{-1}\eta) \in$

supp(Γ). Soit $\epsilon > 0$. Par le point 7 des propriétés II.1.29, on a

$$h_\Gamma = h_{\Gamma^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}} = h_{\gamma\Gamma^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}\gamma'}.$$

Montrons que l'on a l'inclusion

$$\gamma\Gamma^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}\gamma' \subseteq \Gamma^{\beta(\gamma\xi,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})\times\beta(\gamma'^{-1}\eta,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})}.$$

Soit $\gamma'' \in \gamma\Gamma^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}\gamma'$. On a alors d'une part

$$(\gamma^{-1}\gamma'' o|\xi) \geq (\gamma^{-1}\gamma''\gamma'^{-1}o|\xi) - d(o,\gamma' o) > -\log(\epsilon) - d(o,\gamma' o).$$

et d'autre part

$$\begin{aligned}(\gamma'' o|\gamma\xi) &= (\gamma^{-1}\gamma'' o|\xi) + (\gamma o|\gamma'' o) + (\gamma o|\gamma\xi) - d(o,\gamma o)\\ &\geq (\gamma^{-1}\gamma'' o|\xi) - d(o,\gamma o)\\ &\geq -\log(\epsilon) - d(o,\gamma o) - d(o,\gamma' o).\end{aligned}$$

De la même façon on obtient les inégalités

$$(\gamma''^{-1}o|\gamma'^{-1}\eta) \geq (\gamma'\gamma''^{-1}o|\eta) - d(o,\gamma' o) \geq (\gamma'\gamma''^{-1}\gamma o|\eta) - d(o,\gamma o) - d(o,\gamma' o),$$

et donc $\gamma'' \in \Gamma^{\beta(\gamma\xi,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})\times\beta(\gamma'^{-1}\eta,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})}$.

On a donc $h_{\Gamma^{\beta(\gamma\xi,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})\times\beta(\gamma'^{-1}\eta,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})}} \geq h_\Gamma$, et on a l'autre inégalité

$$h_{\Gamma^{\beta(\gamma\xi,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})\times\beta(\gamma'^{-1}\eta,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})}} \leq h_\Gamma$$

par l'inclusion $\Gamma^{\beta(\gamma\xi,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})\times\beta(\gamma'^{-1}\eta,\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)})} \subseteq \Gamma$. Ceci prouve bien que le point $(\gamma,\gamma'^{-1})(\xi,\eta) = (\gamma\xi,\gamma'^{-1}\eta)$ est dans le support supp(Γ) puisque le réel $\epsilon e^{d(o,\gamma o)+d(o,\gamma' o)}$ parcours $\mathbb{R}_+^*$ quand ϵ parcours $\mathbb{R}_+^*$. □

Question . *On a l'inclusion* supp(Γ) $\subseteq \Lambda_\Gamma \times \Lambda_{\Gamma^{-1}}$, *mais a-t'on l'égalité ?*

II.3.3 Le cas générique

On va maintenant montrer que si le support supp(Γ) n'est pas réduit à certains sous-espaces de $\partial_\infty X \times \partial_\infty X$, alors on a la conclusion du théorème II.3.1, c'est-à-dire l'existence d'un sous-semi-groupe contractant de Γ qui est d'entropie totale h_Γ.

Proposition II.3.11. *Soit X un espace Gromov-hyperbolique, et soit Γ un semi-groupe d'isométries de X. Si le support de Γ n'est pas inclus dans la diagonale de $\partial_\infty X \times \partial_\infty X$, alors il existe un sous-semi-groupe contractant Γ' de Γ tel que $h_{\Gamma'} = h_\Gamma$.*

Démonstration. Soit $(\xi,\mu) \in$ supp(Γ) avec $\xi \neq \mu$. On peut alors trouver un réel $\epsilon > 0$ assez petit pour que le produit $\beta(\xi,\epsilon) \times \beta(\eta,\epsilon)$ soit Gromov-disjoint de la diagonale. D'après

le critère de contraction (proposition II.2.4), l'ensemble $\Gamma_{\geq n}^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}$ est alors contractant pour n assez grand, où l'on a posé

$$\Gamma_{\geq n}^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)} := \{\gamma \in \Gamma |\ \gamma o \in \beta(\xi,\epsilon), \gamma^{-1}o \in \beta(\eta,\epsilon) \text{ et } d(o,\gamma o) \geq n\}.$$

Or, par définition du support et par le point 8 des propriétés II.1.29 de l'entropie, on a

$$h_{\Gamma_{\geq n}^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}} = h_\Gamma.$$

Le semi-groupe engendré par $\Gamma_{\geq n}^{\beta(\xi,\epsilon)\times\beta(\eta,\epsilon)}$ convient donc.

□

Proposition II.3.12. *Soit X un espace Gromov-hyperbolique propre, et Γ un semi-groupe d'isométries de X. Si le semi-groupe Γ contient une isométrie contractante h, et que le support* $\mathrm{supp}(\Gamma)$ *contient au moins trois points, alors il existe un sous-semi-groupe contractant Γ' de Γ tel que $h_{\Gamma'} = h_\Gamma$.*

L'idée de la preuve est de montrer qu'il y a beaucoup d'éléments du semi-groupe avec lesquels l'élément h joue un ping-pong. Cela permet alors de faire contracter ces éléments d'un endroit précis vers un endroit précis en les composant à gauche et à droite avec h. On obtient alors un semi-groupe contractant en ne gardant que les éléments assez grands.

Démonstration. Pour une isométrie contractante h d'un espace δ-hyperbolique X, définissons une partie I_h de $X \cup \partial_\infty X$ par

$$I_h := \{\xi \in X \cup \partial_\infty X | (\xi|ho) \geq \frac{1}{2}d(o,ho) - \delta\}.$$

Montrons que si le support $\mathrm{supp}(\Gamma)$ n'est pas inclus dans $I_{h^{-1}} \times \partial_\infty X \cup \partial_\infty X \times I_h$, alors il existe un sous-semi-groupe contractant Γ' de Γ, avec $h_{\Gamma'} = h_\Gamma$.

Remarque II.3.13. *L'ensemble I_h contient X_h. Il est un peu plus gros que X_h afin de garantir que les éléments $\gamma \in \Gamma$ assez grands et tels que l'on ait $\gamma^{-1}o \notin I_h$ soient tels que les parties $X_{\gamma^{-1}}$ et X_h sont disjointes (et idem dans l'autre sens). Ceci permettra alors de faire le ping-pong.*

Lemme II.3.14. *Soit X un espace Gromov-hyperbolique, soit h une isométrie contractante de X et soient I_h et $I_{h^{-1}} \subseteq X$ les parties définies ci-dessus. Pour toute isométrie $\gamma \in \mathrm{Isom}(X)$ telle que $d(o,\gamma o) \geq d(o,ho)$ et $\gamma o \notin I_{h^{-1}}$, on a*

$$X_\gamma \cap X_{h^{-1}} = \emptyset,$$

et pour toute isométrie $\gamma \in \mathrm{Isom}(X)$ telle que $d(o,\gamma o) \geq d(o,ho)$ et $\gamma^{-1}o \notin I_h$, on a

$$X_{\gamma^{-1}} \cap X_h = \emptyset.$$

Démonstration. Soit $\gamma \in \mathrm{Isom}(X)$ tel que $d(o,\gamma o) \geq d(o,ho)$ et $\gamma o \notin I_{h^{-1}}$. Montrons l'inclusion $X_\gamma \subseteq X \backslash X_{h^{-1}}$.

Soit $x \in X_\gamma$. Par δ-hyperbolicité, on a

$$(\gamma o | h^{-1} o) \geq \min\{(x|\gamma o), (x|h^{-1}o)\} - \delta.$$

Or, par définition de $I_{h^{-1}}$ et de X_γ, on a les inégalités

$$\frac{1}{2} d(o,ho) - \delta > (\gamma o | h^{-1} o) \quad \text{et} \quad (x|\gamma o) \geq \frac{1}{2} d(o,\gamma o) \geq \frac{1}{2} d(o,ho).$$

D'où l'inégalité

$$\frac{1}{2} d(o,ho) - \delta > (x|h^{-1}o) - \delta$$

qui prouve que le point x n'est pas dans l'ensemble $X_{h^{-1}}$.

La deuxième partie du lemme découle de la première en remplaçant h par h^{-1} et γ par γ^{-1}. □

Posons H l'ensemble des isométries satisfaisant les conditions du lemme ci-dessus :

$$H := \{\gamma \in \mathrm{Isom}(X) | d(o,\gamma o) \geq d(o,ho), \gamma o \notin I_{h^{-1}} \text{ et } \gamma^{-1} o \notin I_h\}$$

Faisons alors un ping-pong entre les isométries de H et l'isométrie h pour obtenir une partie contractante.

Lemme II.3.15. *Soit X un espace Gromov-hyperbolique, soit h une isométrie contractante de X et soit H la partie de X définie ci-dessus. Alors l'ensemble*

$$hHh := \{h\gamma h | \gamma \in H\}$$

est une partie contractante de $\mathrm{Isom}(X)$.

Démonstration. Si γ est un élément de H, alors par le lemme II.3.14 on a

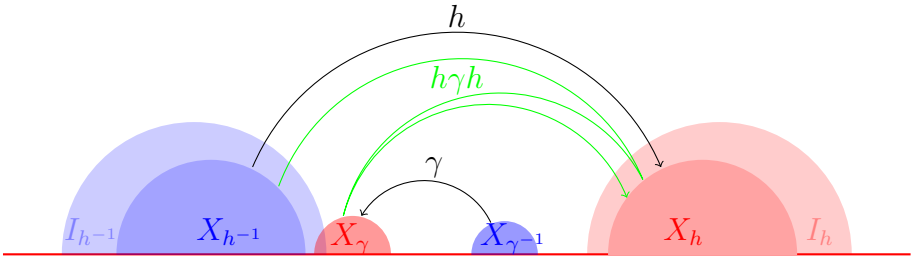
$$h\gamma h(X \backslash X_{h^{-1}}) \subseteq h\gamma(X_h) \subseteq h\gamma(X \backslash X_{\gamma^{-1}}) \subseteq h(X_\gamma) \subseteq h(X \backslash X_{h^{-1}}) \subseteq X_h,$$

et l'ensemble $X \backslash (\overline{X_h} \cup \overline{X_{h^{-1}}}) = X \backslash (X_h \cup X_{h^{-1}})$ contient bien le point base o.

La partie hHh est donc contractante pour les domaines $X_- := X_{h^{-1}}$ et $X_+ := X_h$.

□

FIGURE II.8 – Ping-pong avec l'isométrie contractante h.



Continuons la preuve de la proposition II.3.12. Soit $h \in \Gamma$ un élément contractant. Le semi-groupe engendré par $h(H \cap \Gamma)h$ est alors un sous-semi-groupe contractant de Γ d'après le lemme ci-dessus.

Si le support $\mathrm{supp}(\Gamma)$ n'est pas inclus dans $I_{h^{-1}} \times \partial_\infty X \cup \partial_\infty X \times I_h$, alors l'entropie de $H \cap \Gamma$ est égale à h_Γ par le point 8 des propriétés II.1.29. Or, par le point 7 des propriétés II.1.29, l'entropie de $h(H \cap \Gamma)h$ est égale à celle de $H \cap \Gamma$, et donc l'entropie du semi-groupe engendré est aussi égale à h_Γ.

On est donc ramené à ce que le support $\mathrm{supp}(\Gamma)$ soit inclus dans $I_{h^{-1}} \times \partial_\infty X \cup \partial_\infty X \times I_h$. Par les lemmes II.1.46 et II.1.45, comme l'espace X est propre, il existe un entier n_0 tel que pour tout $n \geq n_0$, l'isométrie h^n soit aussi une isométrie contractante du semi-groupe Γ. On est alors même ramené à ce que le support $\mathrm{supp}(\Gamma)$ soit inclus dans $I_{h^{-n}} \times \partial_\infty X \cup \partial_\infty X \times I_{h^n}$, pour tout $n \geq n_0$.

Or, le diamètre des ensembles I_{h^n} et $I_{h^{-n}}$ tend vers 0 : on a

$$\lim_{n\to\infty} \inf_{x,x' \in I_{h^n}} (x|x') = \infty.$$

On est donc ramené à ce que le support $\mathrm{supp}(\Gamma)$ soit inclus dans un ensemble

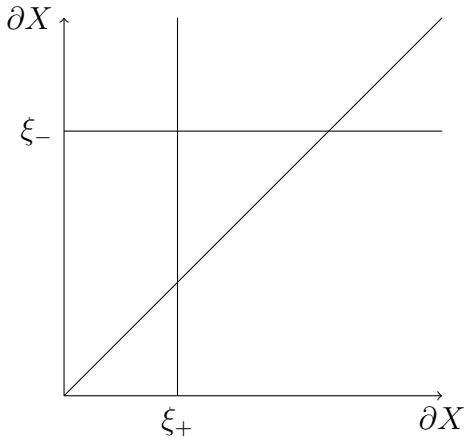
$$(\{\xi_-\} \times \partial_\infty X) \cup (\partial_\infty X \times \{\xi_+\}),$$

où ξ_- et ξ_+ sont des points du bord $\partial_\infty X$.

De plus, en utilisant la proposition II.3.11, on est ramené au cas où le support $\mathrm{supp}(\Gamma)$ est inclus dans la diagonale de $\partial_\infty X \times \partial_\infty X$, donc on est ramené à ce que le support soit inclus dans le doublet $\{(\xi_-, \xi_-), (\xi_+, \xi_+)\}$. Ainsi, on a bien démontré l'existence d'un sous-semi-groupe contractant d'entropie h_Γ dès que le support $\mathrm{supp}(\Gamma)$ contient au moins 3 points.

Ceci termine la preuve de la proposition II.3.12. □

FIGURE II.9 – supp(Γ)



II.3.4 Le cas où le support est un singleton

On a le lemme :

Lemme II.3.16. *Soit X un espace Gromov-hyperbolique et soit Γ un semi-groupe d'isométries de X. Si le support* supp(Γ) *est un singleton $\{(\xi, \xi)\}$, alors le semi-groupe Γ fixe le point ξ.*

Démonstration. Cela découle de la propriété de $\Gamma \times \Gamma^{-1}$-invariance du support (proposition II.3.10). □

Ainsi, on est ramené à ce que le semi-groupe fixe un point au bord (voir sous-section II.3.6).

II.3.5 Le cas où le support est un doublet de points

Supposons maintenant que le support supp(Γ) soit un doublet de points du bord $\{(\xi_+, \xi_+), (\xi_-, \xi_-)\}$. On a alors le lemme suivant.

Lemme II.3.17. *Soit X un espace Gromov-hyperbolique et soit Γ un semi-groupe d'isométries de X. Si le support* supp(Γ) *est un doublet de points $\{(\xi_+, \xi_+), (\xi_-, \xi_-)\}$, alors le semi-groupe Γ fixe le doublet $\{\xi_+, \xi_-\}$.*

Démonstration. Cela découle de la propriété de $\Gamma \times \Gamma^{-1}$-invariance du support (proposition II.3.10). □

Montrons maintenant que quitte à multiplier par un élément qui échange les deux points du doublet, si l'on se restreint aux éléments de norme assez grande et qui contractent dans un des deux sens (d'un des points du doublet vers l'autre), alors on obtient un ensemble contractant. Et l'un de ces deux sous-semi-groupes engendrés sera forcément d'entropie totale (c'est-à-dire d'entropie h_Γ).

Le lemme qui suit dit qu'un point fixe d'une isométrie est toujours dans son domaine de contraction ou dans son domaine de dilatation.

Lemme II.3.18. *Soit X un espace Gromov-hyperbolique et γ une isométrie de X. Si $\xi \in \overline{X}$ est un point fixe pour l'isométrie γ (i.e. $\gamma\xi = \xi$), alors on a*

$$\xi \in X_\gamma \cup X_{\gamma^{-1}}.$$

Démonstration. Supposons que l'on ait $\xi \notin X_\gamma$. Alors on a $\xi = \gamma^{-1}\xi \in X_{\gamma^{-1}}$. En faisant de même avec l'inverse γ^{-1}, on conclut. □

Le lemme suivant dit qu'une isométrie assez grande qui fixe deux points contracte de l'un des points vers l'autre ou bien échange les deux points.

Lemme II.3.19. *Si une isométrie γ d'un espace δ-hyperbolique X de point base o fixe un doublet de points du bord $\{\xi_+, \xi_-\} \subseteq X$ sans les échanger (i.e. $\gamma(\xi_-) \neq \xi_+$) et vérifie l'inégalité $d(o, \gamma o) > 2(\xi_+|\xi_-) + 2\delta$, alors on a*

$$(\xi_+ \in X_\gamma \text{ et } \xi_- \in X_{\gamma^{-1}}) \quad \text{ou} \quad (\xi_- \in X_\gamma \text{ et } \xi_+ \in X_{\gamma^{-1}}).$$

Démonstration. Comme l'élément γ fixe le doublet $\{\xi_-, \xi_+\}$, et n'échange pas ξ_- et ξ_+, les points ξ_- et ξ_+ sont fixes par γ. Le lemme II.3.18 nous donne donc l'inclusion

$$\{\xi_+, \xi_-\} \subseteq X_\gamma \cup X_{\gamma^{-1}}.$$

Or, on ne peut pas avoir $\{\xi_+, \xi_-\} \subseteq X_{\gamma^{-1}}$, puisque par le lemme II.1.42 on a

$$\inf_{x,x' \in X_{\gamma^{-1}}} (x|x') \geq \frac{1}{2} d(o, \gamma o) - \delta > (\xi_+|\xi_-).$$

En faisant de même avec X_γ, on obtient donc bien ce qui était annoncé. □

Démontrons donc le théorème II.3.1 dans le cas où le semi-groupe Γ fixe un doublet $\{\xi_+, \xi_-\} \subseteq \partial_\infty X$, mais ne fixe pas de point au bord. Considérons les parties suivantes du semi-groupe Γ :

$$\Gamma^+ := \{\gamma \in \Gamma | \xi_+ \in X_\gamma \text{ et } \xi_- \in X_{\gamma^{-1}}\}$$

$$\Gamma^- := \{\gamma \in \Gamma | \xi_- \in X_\gamma \text{ et } \xi_+ \in X_{\gamma^{-1}}\}$$

On a alors le lemme suivant.

Lemme II.3.20. *Les ensembles $\Gamma^+_{>n}$ et $\Gamma^-_{>n}$ sont contractants, pour tout entier $n > 2(\xi_+|\xi_-) + 10\delta$, où l'on a posé*

$$A_{>n} := \{\gamma \in A | d(o, \gamma o) > n\},$$

pour une partie $A \subseteq \Gamma$.

Démonstration. Montrons que $\Gamma^+_{>n}$ est contractant. Soient γ et γ' deux isométries de $\Gamma^+_{>n}$. Par δ-hyperbolicité, on a

$$(\xi_+|\xi_-) \geq \min\{(\xi_+|\gamma' o), (\gamma' o|\gamma^{-1} o), (\gamma^{-1} o|\xi_-)\} - 2\delta.$$

Or, par définition de $X_{\gamma'}$, on a $(\xi_+|\gamma' o) \geq \frac{1}{2} d(o, \gamma' o) > (\xi_+|\xi_-) + 2\delta$ et on a de même $(\xi_-|\gamma^{-1} o) > (\xi_+, \xi_-) + 2\delta$, puisque $\xi_+ \in X_{\gamma'}$ et $\xi_- \in X_{\gamma^{-1}}$. On en déduit l'inégalité

$$(\xi_+|\xi_-) \geq (\gamma' o|\gamma^{-1} o) - 2\delta.$$

Ainsi, on obtient

$$\sup_{\gamma, \gamma' \in \Gamma_+} (\gamma^{-1} o|\gamma' o) \leq (\xi_+|\xi_-) + 2\delta < \infty,$$

et on a bien pour tout $\gamma \in \Gamma_+$,

$$\frac{1}{2} d(o, \gamma o) - 3\delta > \frac{1}{2} n - 3\delta > (\xi_+|\xi_-) + 2\delta,$$

donc par le critère II.2.4, l'ensemble $\Gamma^+_{>n}$ est contractant. De la même façon, l'ensemble $\Gamma^-_{>n}$ est contractant. □

Pour terminer la preuve du théorème II.3.1 dans ce cas, il ne reste donc plus qu'à démontrer que l'entropie d'une de ces deux parties contractantes est h_Γ :

Lemme II.3.21. *On a* $\max(h_{\Gamma^+_{>n}}, h_{\Gamma^-_{>n}}) = h_\Gamma$, *pour* $n \geq 2(\xi_+|\xi_-) + 2\delta$.

Démonstration. Il y a deux cas :

1. Il n'existe pas d'élément qui échange ξ_- et $\xi+$. Dans ce cas, par le lemme II.3.19, on a
$$\Gamma_{>n} = (\Gamma_+)_{>n} \cup (\Gamma_-)_{>n}.$$
2. Il existe un élément $\gamma_0 \in \Gamma$ qui échange ξ_- et $\xi+$. Dans ce cas, on peut écrire
$$(\gamma_0 (\Gamma_{>n} \setminus (\Gamma_+ \cup \Gamma_-)))_{>n} \subseteq (\Gamma_+)_{>n} \cup (\Gamma_-)_{>n}.$$

Le résultat découle alors des point 6, 7 et 8 des propriétés II.1.29 de l'entropie. □

Les lemmes II.3.20 et II.3.21 donnent un semi-groupe contractant d'entropie h_Γ parmi l'un des deux semi-groupes suivants : l'un engendré par $\Gamma^+_{>n}$ et l'autre engendré par $\Gamma^-_{>n}$, pour n assez grand.

Ceci termine la preuve du théorème II.3.1 dans le cas où le semi-groupe Γ ne fixe pas de point au bord.

II.3.6 Le cas où le semi-groupe Γ fixe un point au bord

Supposons que le semi-groupe Γ fixe un point $\xi \in \partial_\infty X$ mais ait un ensemble limite Λ_Γ contenant au moins deux points.

Par la proposition II.3.2, il existe alors un élément contractant h tel que le point fixe ξ ne soit pas dans $\overline{X_h}$.

On a alors la proposition suivante.

Proposition II.3.22. *Soit X un espace métrique propre, soit Γ un semi-groupe d'isométries de X, et soit h une isométrie contractante. Si l'on pose*

$$\Gamma' := \{\gamma \in \Gamma | \gamma o \in X_h\},$$

alors on a l'égalité $h_{\Gamma'} = h_\Gamma$.

Ceci permettra de conclure grâce au lemme suivant.

Lemme II.3.23. *Soit X un espace Gromov-hyperbolique, soit Γ un semi-groupe d'isométries fixant un point $\xi \in \partial_\infty X$, et soit h une isométrie contractante telle que $\xi \notin \overline{X_h}$. Alors il existe un réel r tel que l'ensemble*

$$\Gamma'_{>r} := \{\gamma \in \Gamma | \gamma o \in X_h \text{ et } d(o, \gamma o) > r\}$$

soit contractant.

Le semi-groupe engendré sera alors encore contractant et aura encore pour entropie h_Γ par les points 4 et 8 des propriétés II.1.29 de l'entropie, donc on aura bien obtenu la conclusion du théorème II.3.1.

Preuve du lemme II.3.23. Soit

$$C := \sup_{x \in X_h} (x|\xi) < \infty.$$

Montrons que les réels $r > 2C + 8\delta$ conviennent.

Pour toute isométrie $\gamma \in \Gamma'_{>r}$, le point ξ est dans $X_{\gamma^{-1}}$. En effet, on a l'inégalité $(\xi|\gamma o) \leq C < \frac{1}{2} d(o, \gamma o)$ qui donne que ξ n'est pas dans X_γ, et donc on a

$$\xi = \gamma^{-1}\xi \in X_{\gamma^{-1}}.$$

Par δ-hyperbolicité, pour toutes isométries γ et $\gamma' \in \Gamma'_{>r}$ on a l'inégalité

$$C \geq (\xi|\gamma' o) \geq \min\{(\xi|\gamma^{-1} o), (\gamma^{-1} o|\gamma' o)\} - \delta.$$

Or, on a $(\xi|\gamma^{-1} o) \geq \frac{1}{2} d(o, \gamma o) > \frac{1}{2} r > C + \delta$, donc on obtient l'inégalité

$$(\gamma^{-1} o|\gamma' o) \leq C + \delta < \frac{1}{2} r - 3\delta.$$

Par le critère de contraction II.2.4, on obtient donc que la partie $\Gamma'_{>r}$ est contractante. □

Pour démontrer que l'ensemble Γ' est d'entropie h_Γ (i.e. la proposition II.3.22), nous allons découper les boules $B(o,R)$ en morceaux, selon les copies d'un domaine fondamental pour l'élément h, et montrer que quitte à appliquer à chaque morceau une puissance de l'élément h, on peut ramener chaque morceau dans une partie proche de X_h, tout en restant dans la boule. Le lemme suivant permettra de ramener chaque morceaux.

Lemme II.3.24. *Soit X un espace métrique, et soit h une isométrie contractante de X. Alors il existe une constante $C<\infty$ telle que pour tout entier $n\in\mathbb{N}$ et pour tout réel $R>0$ on ait l'inclusion*

$$h^n\left(h^{-n}X_{h^{-1}}\cap B(o,R)\right)\subseteq B(o,R+C).$$

Démonstration. Comme l'élément h est contractant, il existe une constante C telle que l'on ait

$$\sup_{(x,x')\in X_{h^{-1}}\times X_h}(x|x')\leq\frac{1}{2}C<\infty.$$

En particulier, pour tout entier $n\geq 1$ et tout point $x\in h^{-n}X_{h^{-1}}$, on a

$$\frac{1}{2}C\geq(h^nx|h^no)=\frac{1}{2}\left(d(o,h^nx)+d(o,h^no)-d(o,x)\right).$$

On a alors,

$$d(o,h^nx)\leq d(o,x)+C,$$

d'où l'inclusion souhaitée. □

Lemme II.3.25. *Soit X un espace métrique propre, soit Γ un semi-groupe d'isométries de X, soit h une isométrie contractante de Γ, et soit S est une partie ϵ-séparée et couvrante de Γ. Alors il existe une constante $C>0$, telle que pour tout rayon $R>0$ il existe une partie ϵ-séparée $S_R\subseteq\Gamma$ telle que l'on ait l'inégalité*

$$\#S_Ro\cap B(o,R+C)\cap X_h\geq\frac{1}{CR}\#So\cap B(o,R).$$

Ce lemme dit que l'on a une proportion non négligeable des éléments de la boule $B(o,R+C)$ qui sont dans le domaine X_h. Pour le démontrer, nous allons utiliser le lemme des tiroirs pour trouver un morceau de la boule qui contient beaucoup d'éléments, et ramener ce morceau par le lemme précédent dans le domaine X_h.

Démonstration. Posons

$$D_h:=h^{-2}\left(X_h\backslash hX_h\right).$$

Alors D_h est un domaine fondamental pour l'élément h qui est inclus dans $X_{h^{-1}}$.

Majorons le nombre de morceaux du découpage de la boule $B(o,R)$ par ce domaine fondamental.

Sous lemme II.3.26. *Il existe une constante $C_0>0$ telle que pour tout $R>1$ et tout*

$n \geq C_0 R$, on ait

$$B(o,R) \cap h^{-n} D_h = \emptyset.$$

Démonstration. Si $x \in h^{-n} D_h \subseteq h^{-n} X_{h^{-1}}$, par le lemme II.2.5 (pour $X_+ = X_{h^{-1}}$ et $\gamma = h^{-n}$), on a

$$d(o,x) = (x|x) \geq d(o,h^n o) - 2 \sup_{y \in X_{h^{-1}}} (ho|y).$$

Or, par les lemmes II.1.46 et II.2.6, il existe des constantes $C_1 > 0$ et $C_2 > 0$ telles que

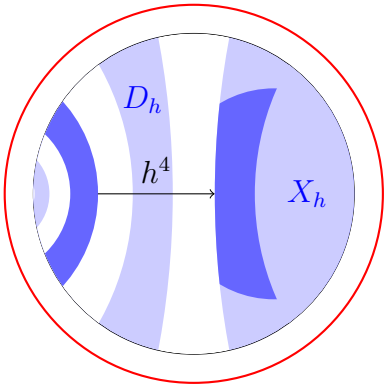
$$d(o,h^n o) \geq C_1 n - C_2.$$

Il existe donc une constante $C_0 > 0$ telle que pour tout $R \geq 1$ et $n \geq RC_0$ on ait

$$d(o,x) \geq C_1 n - C_2 - 2 \sup_{y \in X_{h^{-1}}} (ho|y) > n/C_0 \geq R.$$

D'où $x \notin B(o,R)$ pour $x \in h^{-n} D_h$ avec $n \geq RC_0$. □

FIGURE II.10 – Partition de la boule $B(o,R)$ à l'aide d'un domaine fondamental pour une isométrie contractante h.



D'après ce sous-lemme, on peut donc partitionner la boule $B(o,R)$ en $n = \lceil C_0 R \rceil + 2$ morceaux :

$$B(o,R) = (B(o,R) \cap X_h) \sqcup \bigsqcup_{k=-1}^{n-3} \left(B(o,R) \cap h^{-k} D_h \right).$$

Le lemme des tiroirs nous donne alors que l'un des morceaux du découpage que l'on obtient pour $B(o,R) \cap So$ est de cardinal au moins $\frac{1}{n} \# B(o,R) \cap So$. Si le morceau en question est $B(o,R) \cap X_h$ ou $B(o,R) \cap h^{-(-1)} D_h$, alors le résultat est clair : $S_R := hS$ convient. Sinon, le morceau est $B(o,R) \cap h^{-k} D_h$ pour un entier $k \geq 0$. Par le lemme précédent, on a alors

$$h^k \left(B(o,R) \cap So \cap h^{-k} D_h \right) \subseteq B(o, R + C') \cap D_h \cap h^k So,$$

pour une constante C' assez grande. Et par inégalité triangulaire, on a

$$h^2 \left(B(o,R+C') \cap D_h \cap h^k So \right) \subseteq B(o, R + C' + d(o,h^2 o)) \cap h^2 D_h \cap h^{k+2} So.$$

Comme on a l'inclusion $h^2 D_h \subseteq X_h$, les inégalités précédentes donne l'inégalité annoncée

$$\#S_R o \cap B(o, R+C) \cap X_h \geq \frac{1}{CR} \#So \cap B(o,R),$$

avec $S_R = h^{k+2} S$, pour tout $R \geq 1$, pour une constante C assez grande. □

Voici maintenant un lemme d'inversion des quantificateurs.

Lemme II.3.27. *Soit X un espace métrique propre, soit $\Gamma' \subseteq \mathrm{Isom}(X)$, et soient $h \geq 0$, $C > 0$ et $\epsilon > 0$ des réels. Si pour tout réel $R \geq 1$, il existe une partie ϵ-séparée $S_R \subseteq \Gamma'$ telle que l'on ait l'inégalité*

$$\#S_R \cap B(o,R) \geq Ce^{hR},$$

alors on a $h_{\Gamma'} \geq h$.

Démonstration. Soit $S \subseteq \Gamma'$ une partie séparée et $\frac{\epsilon}{2}$-couvrante. On a les inégalités

$$\begin{aligned} h_{\Gamma'} &= \limsup_{R\to\infty} \frac{1}{R} \log(\#So \cap B(o,R))) \\ &\geq \limsup_{R\to\infty} \frac{1}{R} \log(\#S_R o \cap B(o,R)))) \\ &\geq h. \end{aligned}$$

□

Preuve de la proposition II.3.22. Soit S une partie ϵ-séparée et couvrante du semi-groupe Γ. En utilisant le lemme II.3.25, on obtient l'inégalité

$$\#S_R o \cap B(o, R+C) \geq \frac{1}{CR} \#So \cap B(o,R),$$

pour une partie S_R ϵ-séparée de Γ', pour tout $R > 1$ et pour une constante C. Comme S est une partie couvrante de Γ, son exposant critique est minoré par h_Γ, ce qui donne

$$\frac{1}{CR} \#So \cap B(o,R) \geq e^{(h_\Gamma - \epsilon_R)R},$$

avec $\lim_{R\to\infty} \epsilon_R = 0$. Le lemme II.3.27 nous donne alors l'inégalité $h_{\Gamma'} \geq h_\Gamma - \epsilon_R$, puis on obtient l'inégalité $h_{\Gamma'} \geq h_\Gamma$ en faisant tendre R vers l'infini.

L'autre inégalité $h_{\Gamma'} \leq h_\Gamma$ se déduit de l'inclusion $\Gamma' \subseteq \Gamma$. □

Ceci termine la preuve du théorème II.3.1 : tous les cas ont été traités, puisque le support est non vide par la proposition II.3.8.

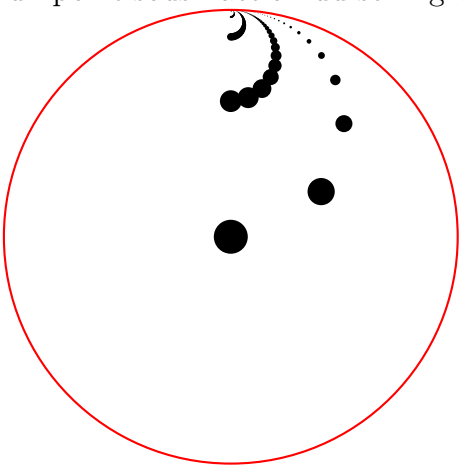
II.3.7 Contre-exemple quand l'ensemble limite du semi-groupe Γ est réduit à un point

Sans l'hypothèse $\#\Lambda_\Gamma \geq 2$, les théorèmes II.3.1 et I.2.15 sont faux en général.

Exemple II.3.28. *Pour $X = \mathbb{H}^2_{\mathbb{R}}$ muni de sa métrique usuelle, le sous-semi-groupe de $SL(2,\mathbb{R})$ engendré par les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ a pour entropie $\frac{1}{2}$, mais ne contient que des sous-semi-groupes contractants d'entropie nulle, donc en particulier ne contient que des sous-semi-groupes de Schottky d'exposant critique nul.*

Même chose avec le groupe parabolique engendré par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

FIGURE II.11 – Orbite d'un point sous l'action du semi-groupe de l'exemple II.3.28.

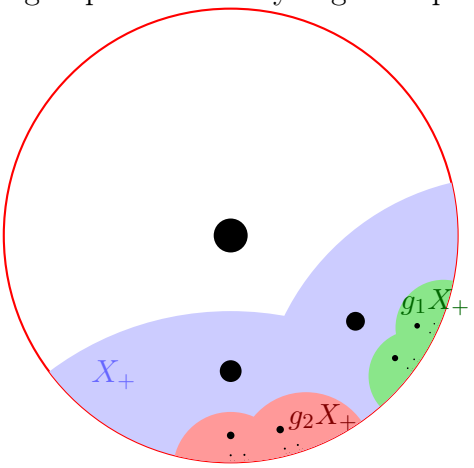


II.4 Semi-groupes de Schottky

Les semi-groupes de Schottky sont les semi-groupes ayant la dynamique la plus simple, puisque par définition leurs générateurs jouent au « ping-pong ». En particuliers ils sont libres et séparés. Le théorème principal de cette section, que nous démontrons ici (théorème II.4.3), affirme que l'entropie d'un semi-groupe est approchée aussi près que l'on veut par celle de ses sous-semi-groupes de Schottky.

Définition II.4.1. *Soient X un espace métrique, et Γ un semi-groupe d'isométries de X. On dit que le semi-groupe Γ est de Schottky pour une partie $X_+ \subseteq X$, s'il admet une partie génératrice finie $\{g_1, g_2, ..., g_n\}$, telle que les parties g_1X_+, g_2X_+, ..., g_nX_+ et $X \backslash X_+$ soient deux à deux Gromov-disjointes, et que l'ensemble $X_+ \backslash (g_1X_+ \cup ... \cup g_nX_+)$ soit d'intérieur non vide.*

FIGURE II.12 – Un semi-groupe de Schottky engendré par deux isométries g_1 et g_2



Propriétés II.4.2. *Soit X un espace métrique et soit Γ un semi-groupe de Schottky d'isométries de X. On a alors :*

1. *Le semi-groupe Γ est libre.*
2. *Le semi-groupe Γ est séparé (donc en particulier d'orbite discrète).*
3. *Le semi-groupe Γ est contractant.*
4. *Si l'espace X est propre, on a $\delta_\Gamma < \infty$.*

Démonstration. Soit B une boule incluse dans l'ensemble $X_+\backslash(g_1X_+ \cup ... \cup g_nX_+)$, alors ses images par les isométries de Γ sont toutes deux à deux disjointes. Donc le semi-groupe est libre et séparé. Le semi-groupe Γ est contractant pour les domaines $X\backslash X_+$ et $g_1X_+ \cup ... \cup g_nX_+$, en choisissant $o \in X_+\backslash(\overline{g_1X_+ \cup ... \cup g_nX_+})$. Pour obtenir la finitude de l'exposant critique, il suffit d'utiliser le lemme II.2.8 pour obtenir un entier k tel que pour tous générateurs γ_1, ..., γ_k, on ait

$$d(o, \gamma_1...\gamma_k o) \geq 2M + 1,$$

où M est la constante de Gromov-disjonction du semi-groupe contractant Γ. Puis on utilise le lemme II.2.6 pour obtenir la minoration

$$d(o, \gamma_1...\gamma_n o) \geq \left\lfloor \frac{n}{k} \right\rfloor,$$

pour tout n, et pour des générateurs γ_1, ..., γ_n. Et on obtient alors la majoration $\delta_\Gamma \leq k\log(N)$, où N est le nombre de générateurs du semi-groupe Γ. □

Théorème II.4.3. *Soit X un espace Gromov-hyperbolique propre, et soit Γ un semi-groupe d'isométries de X. Si le semi-groupe Γ est contractant, alors pour tout $\epsilon > 0$, il existe un sous-semi-groupe Schottky $\Gamma' \subseteq \Gamma$ tel que $\delta_{\Gamma'} \geq h_\Gamma - \epsilon$.*

Pour construire un « gros » sous-semi-groupe de Schottky, nous considèrerons une partie suffisamment séparée de ce semi-groupe contractant, et montrerons que les éléments de norme donnée assez grande, contractent à des endroits suffisamment écartés les

uns des autres pour jouer au « ping-pong » et donc engendrer un semi-groupe de Schottky.

Lemme II.4.4. *Soit X un espace Gromov-hyperbolique, et soient X_- et X_+ des parties de X. Alors il existe un réel r et un entier n_0 tels que pour tout semi-groupe contractant Γ d'isométries de X pour les parties X_+ et X_-, pour toute partie S r-séparée de Γ, et pour tout entier $n \geq n_0$, l'ensemble $S \cap A_n$ engendre un semi-groupe de Schottky pour le domaine X_+, où l'on a posé*

$$A_n := \{\gamma \in \mathrm{Isom}(X) | d(o, \gamma o) \in [n, n+1[\}.$$

Démonstration. Supposons qu'il existe un semi-groupe contractant pour les parties X_- et X_+ (sinon il n'y a rien à démontrer). Montrons que le réel $r := 4C + 4\delta + 2$ convient, où

$$C := \sup_{(x,x') \in X_+ \times X_-} (x|x'),$$

et δ est un réel tel que l'espace X soit δ-hyperbolique.

Soit Γ un semi-groupe contractant pour les parties X_- et X_+, et soient γ et γ' deux isométries de A_n qui vérifient l'inégalité

$$d(\gamma o, \gamma' o) \geq r.$$

Montrons qu'alors les domaines γX_+ et $\gamma' X_+$ sont Gromov-disjoints.

Soient $x \in \gamma X_+$ et $x' \in \gamma' X_+$. Par Gromov-hyperbolicité, on a alors

$$(\gamma o|\gamma' o) \geq \min\{(\gamma o|x), (x|x'), (x'|\gamma' o)\} - 2\delta.$$

Or, on a l'inégalité

$$\begin{aligned}(\gamma o|\gamma' o) &= \frac{1}{2}\left(d(\gamma o, o) + d(\gamma' o, o) - d(\gamma o, \gamma' o)\right) \\ &< (n+1) - \frac{r}{2} = n - 2C - 2\delta,\end{aligned}$$

et d'après le lemme II.2.5, on a les inégalités

$$(\gamma o|x) \geq d(o, \gamma o) - 2C \geq n - 2C$$

et de même $(x'|\gamma' o) \geq n - 2C$. On obtient donc l'inégalité

$$(x|x') < n - 2C.$$

Les ensembles γX_+ et $\gamma' X_+$ sont alors disjoints, puisque si l'on avait $y \in \gamma X_+ \cap \gamma' X_+$, on aurait l'absurdité

$$n - 2C - 2\delta > (\gamma o|\gamma' o) \geq \min\{(\gamma o|y), (y, \gamma' o)\} - \delta \geq n - 2C - \delta.$$

On a donc montré que les ensembles γX_+ et $\gamma' X_+$ sont $(n-2C)$-disjoints. Pour finir, l'intersection $B(o, n-1) \cap X_+$ est d'interieur non vide si l'entier n est assez grand, et elle est incluse dans $X_+ \setminus (\cup_{\gamma \in S \cap A_n} \gamma X_+)$.

□

Ainsi, pour n assez grand et pour le réel r donné par le lemme, si l'on considère une partie S r-séparée et couvrante de Γ, alors l'ensemble $A_n \cap S$ engendre un semi-groupe de Schottky. Et par les points 3 et 5 des propriétés II.1.29 et la remarque II.1.4 on a

$$h_\Gamma = \limsup_{n \to \infty} \frac{1}{n} \ln(\#(A_n \cap S)).$$

Pour tout $\epsilon > 0$, on peut donc trouver un entier n tel que

$$\ln(\#(A_n \cap S)) \geq n(h_\Gamma - \epsilon).$$

Montrons alors que le semi-groupe de Schottky Γ' engendré par $A_n \cap S$ a un exposant critique supérieur ou égal à $\frac{n}{n+1}(h_\Gamma - \epsilon)$. Pour cela, on va utiliser le lemme suivant.

Lemme II.4.5. *Soit X un espace métrique. Si une partie S du groupe d'isométries* $\mathrm{Isom}(X)$ *engendre un semi-groupe libre Γ, alors on a la minoration de l'exposant critique :*

$$\delta_\Gamma \geq \frac{\log(\#S)}{r},$$

où $r = \sup_{\gamma \in S} d(o, \gamma o)$.

Démonstration. Cela découle de l'inégalité triangulaire. Pour des générateurs $\gamma_1, ..., \gamma_n \in S$, on a

$$d(\gamma_1 ... \gamma_n o, o) \leq d(\gamma_1 o, o) + ... + d(\gamma_n o, o) \leq nr,$$

donc, par liberté du semi-groupe Γ pour la partie S, on obtient

$$\#\{\gamma \in \Gamma | d(o, \gamma o) \leq nr\} \geq (\#S)^n.$$

On a donc

$$\begin{aligned} \delta_\Gamma &= \limsup_{n \to \infty} \frac{1}{n} \ln(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}) \\ &\geq \limsup_{n \to \infty} \frac{1}{nr} \ln((\#S)^n) \\ &= \frac{\ln(\#S)}{r}. \end{aligned}$$

□

En appliquant le lemme II.4.5 à la partie $A_n \cap S$, qui engendre un semi-groupe qui est

de Schottky et qui est donc libre, on obtient l'inégalité

$$\delta_{\Gamma'} \geq \frac{\log(\#(A_n \cap S))}{n+1} \geq \frac{n}{n+1}(h_\Gamma - \epsilon).$$

Or, l'entier n pouvait être choisi arbitrairement grand, et le réel $\epsilon > 0$ est arbitraire. Ceci achève la preuve du théorème II.4.3.

On peut maintenant facilement démontrer le théorème I.2.15.

Preuve du théorème I.2.15. On déduit aisément des théorèmes II.3.1 et II.4.3 l'inégalité

$$\sup_{\substack{\Gamma' < \Gamma \\ \Gamma' \text{ sous-semi-groupe de Schottky}}} \delta_{\Gamma'} \geq h_\Gamma.$$

L'autre inégalité s'obtient en remarquant qu'un semi-groupe de Schottky est séparé. □

II.5 Dimension visuelle

Dans cette section, nous voyons une application du théorème I.2.15 à « l'étude au bord » d'un semi-groupe. Nous obtenons le corollaire II.5.4 ci-après qui est une généralisation d'un résultat de F. Paulin (voir (Pau97)) qui généralise lui-même un résultat de Coornaert (voir (Coo93)).

Soit X un espace Gromov-hyperbolique. Pour définir ce qu'est la dimension visuelle d'une partie Λ du bord $\partial_\infty X$, introduisons quelques notations.

On définit la *boule* $\beta(\xi, r)$ de centre ξ et de rayon r sur le bord $\partial_\infty X$ par

$$\beta(\xi, r) := \{\eta \in \partial_\infty X | (\xi|\eta) > -\log(r)\}.$$

Définition II.5.1. *On appelle mesure visuelle de dimension s d'une partie $\Lambda \subseteq \partial_\infty X$ du bord d'un espace X Gromov-hyperbolique, le réel*

$$H^s(\Lambda) := \lim_{\epsilon \to 0} H^s_\epsilon(\Lambda),$$

où $H^s_\epsilon(\Lambda)$ est la borne inférieure des sommes

$$\sum_{i \in \mathbb{N}} r_i^s$$

sur tous les recouvrements $(\beta(\xi_i, r_i))_{i \in \mathbb{N}}$ de l'ensemble Λ par des boules de rayons $r_i \leq \epsilon$.

On appelle dimension visuelle d'un ensemble $\Lambda \subseteq \partial_\infty X$ le réel

$$\dim_{\text{vis}}(\Lambda) := \inf\{s \in \mathbb{R}_+ | H^s(\Lambda) = 0\}.$$

Remarque II.5.2. *On a aussi*

$$\dim_{\text{vis}}(\Lambda) = \sup\{s \in \mathbb{R}_+ | H^s(\Lambda) = \infty\}.$$

Remarque II.5.3. *La mesure visuelle est une mesure.*

La notion de dimension visuelle généralise celle de dimension de Hausdorff.

II.5.1 Lien entre dimension visuelle et entropie

On a le résultat suivant.

Corollaire II.5.4. *Soit X un espace Gromov-hyperbolique propre à bord compact et soit Γ un semi-groupe d'isométries de X dont l'ensemble limite contient au moins deux points. Alors on a l'égalité*

$$\dim_{\text{vis}}(\Lambda_\Gamma^c) = h_\Gamma.$$

F. Paulin a énoncé ce résultat pour les groupes discret, et sa preuve semble s'adapter aux semi-groupes. Cependant, il fait des hypothèses supplémentaires par rapport à notre preuve, qui sont le fait que l'espace X soit géodésique, qu'il soit quasi-géodésique, que le semi-groupe soit séparé, et qu'il ne fixe pas de point au bord (voir (Pau97)).

Voici l'inégalité facile entre entropie et dimension visuelle de l'ensemble limite radial.

Proposition II.5.5. *Soit X un espace Gromov-hyperbolique propre, et soit Γ un semi-groupe d'isométries de X. On a l'inégalité*

$$\dim_{\text{vis}}(\Lambda_\Gamma^c) \leq h_\Gamma.$$

Démonstration. Soit S une partie séparée et couvrante de Γ. Montrons que l'on a l'inégalité $\dim(\Lambda_S^c) \leq \delta_S$. Comme on a les égalités $\Lambda_S^c = \Lambda_\Gamma^c$ et $\delta_S = h_\Gamma$, ceci donnera bien l'inégalité souhaitée.

Définissons l'*ombre* d'une boule $B(x,r)$ par

$$OB(x,r) := \{\xi \in \partial_\infty X | (o|\xi)_x \leq r\}.$$

On a alors l'inclusion

$$\Lambda_S^c \subseteq \bigcup_{r>0} \bigcap_{n\geq 0} \bigcup_{\gamma \in S_{\geq n}} OB(\gamma o, r),$$

où $S_{\geq n} := \{\gamma \in S | d(o, \gamma o) \geq n\}$. En effet, si un élément ξ est dans l'ensemble limite radial Λ_S^c, alors il existe un réel $r > 0$ et une partie A de So qui est une r-sous-quasi-géodésique telle que $\xi \in \partial_\infty A$. On a alors pour tout $x \in A$, $\xi \in OB(x,r)$, et pour tout $n \in \mathbb{N}$, $A_{\geq n} \neq \emptyset$.

Posons alors

$$\Lambda_r := \bigcap_{n\geq 0} \bigcup_{\gamma \in S_{\geq n}} OB(\gamma o, r),$$

pour un réel $r > 0$ et montrons que pour $s > \delta_S$, on a $H^s(\Lambda_r) < \infty$.

On peut recouvrir chaque ombre par une boule de rayon $e^{-d(o,x)+r+\delta}$. En effet, soient ξ et ξ' deux points de l'ombre $OB(x,r)$. On a alors

$$(\xi|\xi') \geq \min\{(\xi|x),(x|\xi')\} - \delta \geq d(o,x) - r - \delta,$$

par δ-hyperbolicité, et par l'inégalité

$$(\xi|x) = -(o|\xi)_x + d(o,x) \geq d(o,x) - r$$

et de même avec ξ'.

Ainsi, pour $\epsilon > 0$, en considérant un recouvrement de l'ensemble Λ_r par des boules de rayon $\leq \epsilon$ qui recouvrent les ombres $OB(\gamma o, r)$ pour $\gamma \in S$ assez grand, on obtient

$$H^s(\Lambda_r) = \lim_{\epsilon \to 0} H^s_\epsilon(\Lambda_r) \leq \sum_{\gamma \in S} e^{-s(d(o,\gamma o)-r-\delta)} = e^{s(r+\delta)} P_s,$$

où $P_s = \sum_{\gamma \in S} e^{-sd(o,\gamma o)}$ est la série de Poincaré de S. On a $P_s < \infty$ dès que $s > \delta_S$, d'où $H^s(\Lambda_r) < \infty$.

On a ensuite $H^s(\Lambda_r) = 0$ pour tout $s > \delta_S$, puis

$$H^s(\Lambda_S^c) = H^s(\bigcup_{r>0} \Lambda_r) = 0.$$

Ainsi, on a

$$\dim_{\text{vis}}(\Lambda_S^c) \leq s$$

pour tout $s > \delta_S$, d'où l'inégalité $\dim_{\text{vis}}(\Lambda_S^c) \leq \delta_S$.

□

Pour obtenir le corollaire II.5.4 à partir du théorème I.2.15, il suffit de démontrer le résultat dans le cas des semi-groupes de Schottky :

Proposition II.5.6. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un semi-groupe de Schottky d'isométries de X. Alors on a l'égalité*

$$\dim_{\text{vis}}(\Lambda_\Gamma) = \delta_\Gamma.$$

Démonstration. Par les propositions II.5.5 et II.2.9, on a déjà l'inégalité

$$\dim_{\text{vis}}(\Lambda_\Gamma) \leq h_\Gamma \leq \delta_\Gamma.$$

Montrons l'inégalité $\dim_{\text{vis}}(\Lambda_\Gamma) \geq \delta_\Gamma$. Pour cela, on va utiliser le lemme suivant, dû à Frostman, qui ramène le problème à construire une mesure convenable sur l'ensemble limite Λ_Γ du semi-groupe Γ.

Lemme II.5.7. *Soit X un espace Gromov-hyperbolique et soit μ une probabilité portée par une partie Λ du bord $\partial_\infty X$. S'il existe un réel s et une constante $C > 0$ tels que l'on ait*

$$\mu(\beta(\xi, r)) \leq Cr^s,$$

pour toute boule $\beta(\xi, r)$ du bord $\partial_\infty X$, alors on a l'inégalité

$$\dim_{\text{vis}} \Lambda \geq s.$$

Démonstration. Soit $\epsilon > 0$, et soit R un recouvrement de l'ensemble Λ par des boules de tailles inférieures à ϵ. On a alors les inégalités

$$\sum_{\beta(\xi,r)\in R} r^s \geq \sum_{\beta(\xi,r)\in R} \frac{1}{C}\mu(\beta(\xi, r)) \geq \frac{1}{C}\mu(\partial_\infty X) = \frac{1}{C}.$$

On en déduit, en passant à la borne inférieure sur tous ces recouvrements que l'on a l'inégalité $H^s_\epsilon(\Lambda) \geq \frac{1}{C}$, puis en passant à la limite quand ϵ tend vers 0, que l'on a $H^s(\Lambda) \geq \frac{1}{C}$. On obtient donc bien l'inégalité souhaitée.

□

La mesure à laquelle nous appliquerons ce lemme pour conclure est la mesure μ de Patterson-Sullivan, que nous allons définir maintenant.

a) Mesure de Patterson-Sullivan

Soit X un espace Gromov-hyperbolique propre à bord compact et soit Γ un semi-groupe discret d'isométries de X, avec $\delta_\Gamma < \infty$. Définissons des probabilités μ_s sur l'espace X, pour des réels $s > \delta_\Gamma$, par

$$\mu_s := \frac{1}{P_s} \sum_{\gamma\in\Gamma} e^{-sd(o,\gamma o)} D_{\gamma o},$$

où $P_s := \sum_{\gamma\in\Gamma} e^{-sd(o,\gamma o)}$ est la série de Poincaré de Γ, et D_x est le Dirac en x.

Remarque II.5.8. *La série de Poincaré P_s diverge pour $s < \delta_\Gamma$ et converge pour $s > \delta_\Gamma$.*

Pour définir la mesure μ, nous aurons besoin que la série de Poincaré soit divergente en δ_Γ (i.e. $P_{\delta_\Gamma} = \infty$). On la rend divergente grâce au lemme suivant.

Lemme II.5.9 (Astuce de Patterson)**.** *Soit s_0 un réel et $(a_n)_{n\in\mathbb{N}}$ une suite de réels positifs. Si la série de Dirichlet $\sum_{n\in\mathbb{N}} a_n^{-s}$ est divergente pour $s < s_0$ et convergente pour $s > s_0$, alors il existe une fonction croissante $k : [0, \infty[\to [0, \infty[$ telle que la série*

$$\sum_{n\in\mathbb{N}} k(a_n) a_n^{-s}$$

converge pour $s > s_0$ et diverge pour $s < s_0$ et pour $s = s_0$, et avec de plus la propriété : pour tout $\epsilon > 0$, il existe un réel y_0 tel que pour $y > y_0$ et $x > 1$, on ait

$$k(xy) \leq x^\epsilon k(y).$$

Voir (Pat76) pour une preuve.

Pour rendre la série de Poincaré divergente en $s = \delta_\Gamma$, il suffit de la remplacer par :

$$P_s := \sum_{\gamma \in \Gamma} k(e^{d(o,\gamma o)}) e^{-sd(o,\gamma o)},$$

où k est la fonction fournie par ce lemme, et l'on fait de même pour la définition des mesures μ_s.

Les mesures μ_s sont des mesures de probabilités. Or, par hypothèse, l'adhérence $\overline{X}$ est compacte. Et l'ensemble de probabilités $\mathcal{P}(\overline{X})$ sur le compact $\overline{X}$, muni de la convergence vague, est alors compact (voir par exemple (Rud21)). Il existe donc une suite de réels $(s_k)_{k\in\mathbb{N}}$, avec pour tout k, $s_k > \delta_\Gamma$, telle que la suite de mesures $(\mu_{s_k})_{k\in\mathbb{N}}$ converge vaguement vers une mesure de probabilité μ :

$$s_k \xrightarrow[k\to\infty]{} \delta_\Gamma \quad \text{et} \quad \mu_{s_k} \xrightarrow[k\to\infty]{} \mu.$$

La mesure μ est alors portée par le bord $\partial_\infty X$, puisque Γ est une partie discrète, que l'espace X propre et que l'on a $\lim_{s\to\delta_\Gamma} P_s = \infty$.

Avant de majorer la mesure μ sur toutes les boules, majorons là sur les ensembles γX_+.

Lemme II.5.10. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un semi-groupe d'isométries de X, de Schottky pour un domaine X_+. Alors il existe un point o tel que si μ est la mesure de Patterson-Sullivan définie ci-dessus (pour ce point o), alors il existe une constante $C > 0$ telle que pour toute isométrie $\gamma \in \Gamma$, on ait l'inégalité*

$$\mu(\partial_\infty(\gamma X_+)) \leq Ce^{-\delta_\Gamma d(o,\gamma o)}.$$

Démonstration. On a le lemme suivant.

Lemme II.5.11. *Soit X un espace métrique, et Γ un sous-semi-groupe de Schottky de $\mathrm{Isom}(X)$, pour une partie $X_+ \subset X$. Pour un point $o \in X_+ \setminus (\cup_{g \text{ générateur}} gX_+)$, on a les équivalences*

$$\gamma X_+ \cap \gamma' X_+ \neq \emptyset \iff (\gamma \in \gamma'\Gamma \text{ ou } \gamma' \in \gamma\Gamma),$$

$$\gamma' o \in \gamma X_+ \iff \gamma' \in \gamma\Gamma,$$

pour toutes isométries γ et $\gamma' \in \Gamma$.

Démonstration. Montrons la première équivalence. Soient γ et γ' deux isométries de Γ telles que l'on ait $\gamma X_+ \cap \gamma' X_+ \neq \emptyset$. Soient g et g' les générateurs tels que $\gamma \in g\Gamma$ et

$\gamma' \in g'\Gamma$. Étant donné que les ensembles gX_+ et $g'X_+$ sont Gromov-disjoints si $g \neq g'$ et que l'on a les inclusions $\gamma X_+ \subseteq gX_+$ et $\gamma' X_+ \subseteq g'X_+$, on a nécessairement $g = g'$. Par récurrence, on a bien obtenu que $\gamma \in \gamma'\Gamma$ ou $\gamma' \in \gamma\Gamma$. La réciproque est claire.

Montrons la deuxième équivalence. Soient γ et γ' deux isométries de Γ telles que l'on ait $\gamma' o \in \gamma X_+$. On a $\gamma' o \in \gamma' X_+ \cap \gamma X_+$ puisque $o \in X_+$. Par l'équivalence précédente, on a donc $\gamma' \in \gamma\Gamma$ ou $\gamma \in \gamma'\Gamma$. Supposons que l'on ait $\gamma' \notin \gamma\Gamma$. On peut alors trouver un générateur g tel que l'on ait $\gamma \in \gamma' g\Gamma$. On a ensuite l'inclusion $\gamma X_+ \subseteq \gamma' g X_+$, donc $\gamma' o \in \gamma' g X_+$, puis $o \in gX_+$, ce qui contredit l'hypothèse. Donc on a bien $\gamma' \in \gamma\Gamma$. La réciproque est claire. □

Choisissons un point $o \in X_+ \setminus (\cup_{g \text{ générateur}} gX_+)$ (i.e. comme dans le lemme II.5.11).

Supposons que le semi-groupe Γ soit divergent. Pour tout $s > \delta_\Gamma$ et pour toute isométrie $\gamma \in \Gamma$, on a alors

$$\mu_s(\gamma X_+) = \frac{1}{P_s} \sum_{\gamma' \in \gamma\Gamma} e^{-sd(o,\gamma' o)}.$$

Or, le lemme II.2.6 nous donne l'inégalité

$$d(o, \gamma'\gamma o) \geq d(o, \gamma' o) + d(o, \gamma o) - 2C',$$

où C' est la constante de contraction du semi-groupe Γ pour le point o :

$$C' := \sup_{\gamma, \gamma' \in \Gamma} (\gamma^{-1} o | \gamma' o) < \infty.$$

On obtient alors

$$\mu_s(\gamma X_+) \leq \frac{1}{P_s} e^{2sC'} e^{-sd(o,\gamma o)} \sum_{\gamma' \in \Gamma} e^{-sd(o,\gamma' o)} = e^{2sC'} e^{-sd(o,\gamma o)}.$$

D'où l'inégalité

$$\mu_s(\gamma X_+) \leq C_s e^{-sd(o,\gamma o)}.$$

avec $C_s = e^{2sC'}$. En passant à la limite, on obtient l'inégalité voulue

$$\mu(\partial_\infty(\gamma X_+)) \leq C e^{-\delta_\Gamma d(o,\gamma o)},$$

où $C = e^{2\delta_\Gamma C'}$, puisque l'ensemble $\partial_\infty(\gamma X_+) \cap \Lambda_\Gamma$ est isolé (c'est-à-dire ouvert et fermé) dans l'ensemble limite Λ_Γ.

Si le semi-groupe n'est pas divergent, on modifie le calcul précédent en conséquent en utilisant l'astuce de Patterson, et on conclut de la même façon. □

Montrons maintenant que la mesure μ est majorée pour toutes les boules.

Lemme II.5.12. *Soit X un espace Gromov-hyperbolique propre à bord compact, et soit Γ un semi-groupe d'isométries de X, de Schottky pour un domaine X_+. Soit o le point donné par le lemme II.5.11, et soit μ la mesure de Patterson-Sullivan correspondante.*

Alors il existe une constante $C > 0$ telle que pour toute boule $\beta(\xi, r)$ du bord $\partial_\infty X$, on ait l'inégalité

$$\mu(\beta(\xi, r)) \leq C r^{\delta_\Gamma}.$$

Démonstration. Soit C' la constante donnée par le lemme II.5.10. Soit $\beta(\xi, r)$ une boule. Si la boule n'intersecte pas l'ensemble limite Λ_Γ, on a $\mu(\beta(\xi, r)) = 0$, et il n'y a rien à démontrer. Supposons donc que la boule rencontre l'ensemble limite. On peut alors supposer que l'on a $\xi \in \Lambda_\Gamma$, quitte à recouvrir la boule $\beta(\xi, r)$ par une boule de rayon $2r$ centrée en un point de l'ensemble limite Λ_Γ, et à multiplier la constante C par 2^{δ_Γ}.

Notons

$$\Gamma_k := \{\gamma \in \Gamma | \gamma \text{ de longueur } k \text{ en les générateurs}\},$$

et $\Gamma_0 := \{id\}$. Soit n un entier tel que l'on ait

$$\#\{\gamma \in \Gamma_n | \partial_\infty(\gamma X_+) \cap \beta(\xi, r) \neq \emptyset\} = 1, \text{ et}$$

$$\#\{\gamma \in \Gamma_{n+1} | \partial_\infty(\gamma X_+) \cap \beta(\xi, r) \neq \emptyset\} \geq 2.$$

Cet entier existe bien, puisque pour $n = 0$ on a $\partial_\infty X_+ \cap \beta(\xi, r) \neq \emptyset$, et puisque l'on a

$$\lim_{n\to\infty} \#\{\gamma \in \Gamma_n | \partial_\infty(\gamma X_+) \cap \beta(\xi, r) \neq \emptyset\} = \infty.$$

En effet, si l'on a $\gamma_n o \xrightarrow[n\to\infty]{} \xi$ pour une suite $(\gamma_n)_{n\in\mathbb{N}}$ d'éléments de Γ, alors on a $\partial_\infty(\gamma_n X_+) \subseteq \beta(\xi, r)$ à partir d'un certain rang par le lemme II.2.5 et par Gromov-hyperbolicité.

Soit $\gamma \in \Gamma_n$ tel que $\partial_\infty(\gamma X_+) \cap \beta(\xi, r) \neq \emptyset$. Comme la mesure μ est portée l'ensemble limite Λ_Γ, on a

$$\mu(\beta(\xi, r)) \leq \mu(\partial_\infty(\gamma X_+)) \leq C' e^{-\delta d(o,\gamma o)}$$

par le lemme II.5.10 et par le choix de n. Il reste donc à majorer la quantité $e^{d(o,\gamma o)}$ en fonction de r.

Pour tout $\gamma' \in \Gamma_{n+1}$ tel que $\partial_\infty(\gamma' X_+) \cap \beta(\xi, r) \neq \emptyset$, on a $\gamma' \in \gamma\Gamma$. Soient alors $g \neq g'$ deux générateurs tels que l'on ait

$$\partial_\infty(\gamma g X_+) \cap \beta(\xi, r) \neq \emptyset \quad \text{et} \quad \partial_\infty(\gamma g' X_+) \cap \beta(\xi, r) \neq \emptyset.$$

Soit $C'' > 0$ une constante telle que les parties gX_+ pour g parcourant les générateurs, et X_+, soient deux à deux C''-Gromov disjointes. L'image $\gamma^{-1}\beta(\xi, r)$ de la boule $\beta(\xi, r)$ par l'isométrie γ^{-1} rencontre les ensembles $\partial_\infty(gX_+)$ et $\partial_\infty(g'X_+)$, donc il existe des points η et η' de $\gamma^{-1}\beta(\xi, r)$ tels que l'on ait l'inégalité

$$(\eta|\eta') \leq C''.$$

On a alors

$$\begin{aligned} C'' &\geq (\eta|\eta') \\ &= (\gamma\eta|\gamma\eta') + (\gamma^{-1}o|\eta) + (\gamma^{-1}o|\eta') - d(o,\gamma o) \\ &\geq -\log(r) - \delta + 0 + 0 - d(o,\gamma o) \end{aligned}$$

d'où l'inégalité

$$e^{-d(o,\gamma o)} \leq e^{C''+\delta} r.$$

On obtient donc l'inégalité escomptée avec $C = C' e^{C''+\delta}$. □

Les lemmes II.5.12 et II.5.7 donnent l'inégalité

$$\dim_{vis}(\Lambda_\Gamma) \geq \delta_\Gamma,$$

ce qui termine cette preuve de la proposition II.5.6. □

On peut maintenant facilement retrouver la généralisation du résultat de Paulin.

Preuve du corollaire II.5.4. Soit $\epsilon > 0$. Par le théorème I.2.15, il existe un sous-semi-groupe Γ' de Schottky de Γ tel que l'on ait $\delta_{\Gamma'} \geq h_\Gamma - \epsilon$. Par les propositions II.5.6 et II.2.9, on a donc les inégalités

$$\dim_{\text{vis}}(\Lambda_\Gamma^c) \geq \dim_{\text{vis}}(\Lambda_{\Gamma'}^c) = \dim_{\text{vis}}(\Lambda_{\Gamma'}) = \delta_{\Gamma'} \geq h_\Gamma - \epsilon.$$

Ceci étant vrai pour tout $\epsilon > 0$, on en déduit l'inégalité

$$\dim_{\text{vis}}(\Lambda_\Gamma^c) \geq h_\Gamma.$$

L'autre inégalité est donnée par la proposition II.5.5. □

II.5.2 Semi-groupes de développement β-adique

Dans cette sous-section, nous obtenons une application du corollaire II.5.4 aux semi-groupes de développement en base β.

Le *semi-groupe de développement en base $\beta \in \mathbb{C}$ avec ensemble de chiffres A* est le semi-groupe engendré par les applications affines :

$$x \mapsto x/\beta + t,$$

où $t \in A$, pour une partie finie A de $\mathbb{C}$.

On peut voir ce semi-groupe comme un sous-semi-groupe de $SL_2(\mathbb{C})$. En effet, à l'application $x \mapsto x/\beta + t$, on peut associer la matrice $\begin{pmatrix} \frac{1}{\sqrt{\beta}} & t\sqrt{\beta} \\ 0 & \sqrt{\beta} \end{pmatrix}$, où $\sqrt{\beta}$ est une racine carrée de β. On a donc une action par isométrie du semi-groupe sur l'espace $X = \mathbb{H}^3_{\mathbb{R}} := \{z + \tau j | z \in \mathbb{C}, \tau > 0\}$ (vu comme partie de l'ensemble des quaternions),

dont le bord $\partial_\infty X$ s'identifie à $\mathbb{C} \cup \{\infty\}$. L'action de l'application $x \mapsto x/\beta + t$ sur $\mathbb{H}^3_{\mathbb{R}}$ est donnée par

$$(x \mapsto x/\beta + t).(z + \tau j) = (z/\beta + t) + (\tau/|\beta|)j.$$

L'ensemble limite du semi-groupe est alors exactement l'ensemble des nombres complexes qui admettent un développement β-adique n'ayant qu'un seul chiffre avant la virgule et avec ensemble de chiffres A.

Tout ceci fonctionne également en remplaçant le corps $\mathbb{C}$ par $\mathbb{R}$.

Définition II.5.13. *On appelle nombre de Salem généralisé un entier algébrique $\beta \in \mathbb{C}$ de module strictement supérieur à 1, dont tous les conjugués sont de modules inférieurs ou égaux à 1, sauf éventuellement son conjugué complexe. On appelle* nombre de Pisot *généralisé un entier algébrique $\beta \in \mathbb{C}$ de module strictement supérieur à 1, dont tous les conjugués sont de modules* strictement *inférieurs à 1, sauf éventuellement son conjugué complexe.*

Remarque II.5.14. *Dans la définition classique de nombres de Pisot et de Salem, on demande à ce que le nombre soit un réel $\beta > 1$, mais tout ce que l'on verra est valable pour cette définition plus générale.*

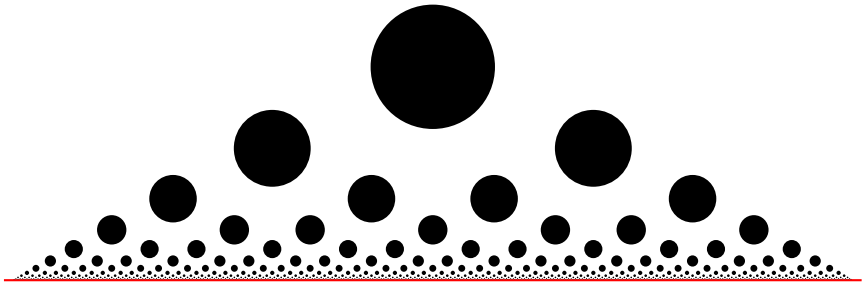
Proposition II.5.15. *Soit Γ le semi-groupe engendré par les applications*

$$x \mapsto x/\beta + t$$

où $t \in A$ pour une partie finie $A \subset \mathbb{Q}(\beta)$. Si β est un nombre de Salem généralisé, alors on a l'égalité

$$\dim_H(\Lambda_\Gamma) = \delta_\Gamma.$$

FIGURE II.13 – Développement en base $\beta = \varphi$ (le nombre d'or, qui est un nombre de Pisot), avec ensemble de chiffres $A = \{0, 1\}$.



Avant de démontrer la proposition, on a le lemme suivant.

Le lemme qui suit dit que si l'on regarde l'orbite d'une boule par le semi-groupe, alors le nombre de chevauchements en un point donné n'est pas trop grand par rapport à la distance au point base o.

Lemme II.5.16. *Sous les hypothèses de la proposition II.5.15, il existe un entier r tel que l'on ait*

$$\#\{\gamma \in \Gamma | d(\gamma j, x) \leq 1\} = \underset{d(j,x)\to\infty}{O}(d(j,x)^r),$$

pour $x \in \mathbb{H}^3_{\mathbb{R}}$.

Remarque II.5.17. *Si l'entier algébrique β est de Pisot, alors le semi-groupe Γ est même séparé (voir la condition de séparation de Lalley (Lal97)), et donc on peut prendre $r = 0$.*

Preuve du lemme II.5.16. Le resultat suivant permet de majorer le paramètre de translation des isométries du semi-groupe Γ.

Sous lemme II.5.18. *Si Γ est un sous-semi-groupe de $\mathrm{Aff}(\mathbb{C})$ engendré par des application $x \mapsto x/\beta + t$, pour $t \in A$, avec A partie finie de $\mathbb{C}$ et $\beta \in \mathbb{C}$ tel que $|\beta| > 1$, alors il existe une constante C telle que pour toute application $x \mapsto \alpha x + t \in \Gamma$, on ait $|t| \leq C$.*

Démonstration. Un élément du semi-groupe Γ s'écrit

$$x \mapsto x/\beta^n + \sum_{k=0}^{n-1} \frac{t_k}{\beta^k},$$

avec $t_k \in A$. On a alors la majoration

$$\left|\sum_{k=0}^{n-1} \frac{t_k}{\beta^k}\right| \leq \max_{t\in A} |t| \sum_{k=0}^{n-1} \frac{1}{|\beta|^k} \leq \frac{\max_{t\in A} |t|}{1 - \frac{1}{|\beta|}}.$$

□

Notons

$$\Gamma_x := \{\gamma \in \Gamma | d(\gamma j, x) \leq 1\}.$$

On a alors les resultats suivants.

Sous lemme II.5.19. *Il existe une constante C telle que pour tout $x \in \mathbb{H}^3_{\mathbb{R}}$, toute isométrie de Γ_x est de longueur au moins $\frac{d(j,x)-C}{\log(\beta)}$ et au plus $\frac{d(j,x)+C}{\log(\beta)}$ en les générateurs.*

Démonstration. En effet, on a l'inégalité triangulaire

$$d(j,x) - d(\gamma j, x) \leq d(j, \gamma j) \leq d(\gamma j, x) + d(j,x).$$

Par ailleurs, si l'on écrit $\gamma j = |\beta|^{-n} j + t$, on a

$$d(j, |\beta|^{-n} j) - d(j, j+t) \leq d(j, \gamma j) \leq d(j, |\beta|^{-n} j) + d(j, j+t)$$

où n est la longueur de γ. Ensuite, d'après le sous-lemme II.5.18, la quantité $d(j, j+t)$ est bornée par une constante C' indépendante de γ et de x. Et on vérifie que l'on a

$d(j, |\beta|^{-n} j) = n \log(\beta)$ pour la métrique usuelle de $\mathbb{H}^3_{\mathbb{R}}$. On obtient alors l'encadrement

$$d(j,x) - C' - 1 \leq n \log(\beta) \leq d(j,x) + C' + 1.$$

D'où l'encadrement sur la longueur n de γ avec $C = C' + 1$.

□

Posons

$$n_x := \left\lfloor \frac{d(j,x) + C}{\log(\beta)} \right\rfloor,$$

la plus grande longueur possible des éléments de Γ_x. On a alors le resultat suivant.

Sous lemme II.5.20. *Il existe une constante C telle que pour tout $x \in \mathbb{H}^3_{\mathbb{R}}$ on ait*

$$\operatorname{diam}(\beta^{n_x} \Gamma_x 0) \leq C,$$

où 0 est le point du bord $0 = 0 + 0j \in \partial_\infty \mathbb{H}^3_{\mathbb{R}}$.

Démonstration. L'application $y \mapsto \beta^{n_x} y$ étant une isométrie, on a

$$d(\beta^{n_x} \gamma j, \beta^{n_x} x) = d(\gamma j, x) \leq 1,$$

pour tout $\gamma \in \Gamma_x$. D'autre part, si l'on écrit $\gamma j = \gamma 0 + |\beta|^{-n} j$, alors on a

$$\beta^{n_x} \gamma j = \beta^{n_x} \gamma 0 + |\beta|^{n_x - n} j,$$

où n est la longueur de γ. Or, par le sous-lemme II.5.19, il existe une constante C telle que pour $\gamma \in \Gamma_x$, on ait $|n - n_x| \leq C$, où n est la longueur de γ. La distance

$$d(\beta^{n_x} \gamma 0, \beta^{n_x} x)$$

est donc bornée indépendamment de x et $\gamma \in \Gamma_x$, par inégalité triangulaire. □

Quitte à multiplier la partie A par les dénominateurs (ce qui ne change pas la conclusion du sous-lemme), on peut supposer que l'on a $A \subseteq \mathbb{Z}[\beta]$. La quantité

$$\beta^{n_x} \gamma 0 \in \mathbb{C}$$

est alors un polynôme en β à coefficients entiers, pour tout élément $\gamma \in \Gamma_x$.

Construisons alors un espace E (indépendant du point x), dans lequel l'anneau $\mathbb{Z}[\beta]$ sera discret.

Soit $\mathcal{P}$ l'ensemble des valeurs absolues archimédiennes du corps $k := \mathbb{Q}(\beta)$, à équivalence près. L'ensemble $\mathcal{P}$ est fini (de cardinal majoré par le degré de β), et l'on peut poser

$$E := \prod_{v \in \mathcal{P}} k_v,$$

où k_v est le complété du corps k pour la valeur absolue v.

On a alors $E = \mathbb{R}^r \times \mathbb{C}^s$, où r est le nombre conjugués réels de β, et $2s$ est son nombre de conjugués complexes.

On a maintenant le résultat suivant,

Proposition II.5.21. *L'anneau $\mathbb{Z}[\beta]$ est discret dans l'espace E.*

qui découle de la formule du produit, qui est un résultat classique de théorie des nombre (voir par exemple (Lan70)).

Remarque II.5.22. *On peut même montrer que $\mathbb{Z}[\beta]$ est un réseau co-compact de l'espace E, mais nous n'en aurons pas besoin.*

Proposition II.5.23 (Formule du produit)**.** *Soit k un corps de nombres. Pour tout $x \in k\backslash\{0\}$, on a*

$$\prod_{v\in\mathcal{P}_k} |x|_v = 1,$$

où $\mathcal{P}_k$ est l'ensemble des valeurs absolues de k à équivalence près, où l'on a choisis les valeurs absolues « standards » dans chaque classe d'équivalence.

Preuve de la proposition II.5.21. Il suffit de montrer que le point $0 \in \mathbb{Z}[\beta]$ est isolé. On aura alors bien la discrétude puisque l'ensemble $\mathbb{Z}[\beta]$ est un groupe additif. Soit B la boule de E de centre 0 et de rayon $1/2$. Si un point x est dans $B \cap \mathbb{Z}[\beta]$, alors on a

$$\prod_{v\in\mathcal{P}_k} |x|_v \leq \prod_{v\in\mathcal{P}} |x|_v \leq (\frac{1}{2})^{r+s} < 1,$$

puisque pour toute valeur absolue ultramétrique v, on a $|\beta|_v \leq 1$ et donc $|x|_v \leq 1$, étant donné que β est un entier algébrique. D'après la formule du produit, on a donc $x = 0$. D'où la discrétude de l'anneau $\mathbb{Z}[\beta]$ dans l'espace E. □

L'ensemble de valeurs absolues $\mathcal{P}$ peut s'écrire

$$\mathcal{P} := \mathcal{P}_- \cup \mathcal{P}_0 \cup \mathcal{P}_+,$$

où

- $\mathcal{P}_+$ est l'ensemble des valeurs absolues $v \in \mathcal{P}$ telles que $|\beta|_v > 1$,
- $\mathcal{P}_0$ est l'ensemble des valeurs absolues $v \in \mathcal{P}$ telles que $|\beta|_v = 1$,
- $\mathcal{P}_-$ est l'ensemble des valeurs absolues $v \in \mathcal{P}$ telles que $|\beta|_v < 1$.

On peut alors décomposer cet espace E dans lequel l'anneau $\mathbb{Z}[\beta]$ est discret en 3 morceaux :

$$E = E_+ \times E_0 \times E-,$$

où $E_- := \prod_{v\in\mathcal{P}_-} k_v$, $E_0 := \prod_{v\in\mathcal{P}_0} k_v$, et $E_+ := \prod_{v\in\mathcal{P}_+} k_v$.

Le nombre β étant de Salem généralisé, il existe une unique valeur absolue v telle que $|\beta|_v > 1$. On a donc $E_+ = \mathbb{R}$ ou $\mathbb{C}$ selon que le nombre β est réel ou complexe.

Montrons maintenant que la partie $\beta^n\Gamma_x 0$ est suffisamment bornée dans l'espace E.

Sous lemme II.5.24. *Il existe une constante $C > 0$ telle que pour tout point $x \in \mathbb{H}^3_{\mathbb{R}}$, il existe des compacts K_+, K_0 et K_- respectivement de E_+, E_0 et E_-, de diamètres majorés par C, tels que l'on ait l'inclusion*

$$\beta^{n_x}\Gamma_x 0 \subseteq \mathbb{Z}[\beta] \cap K_+ \times ((n_x+1)K_0) \times K_-.$$

Démonstration. Soit un point $x \in \mathbb{H}^3_{\mathbb{R}}$ et une isométrie $\gamma \in \Gamma_x$. L'expression $\beta^{n_x}\gamma 0$ est un polynôme en β à coefficients dans $\mathbb{Z}$, mais c'est aussi un polynôme en β, de degré au plus n_x, à coefficient dans A.

Pour obtenir le compact K_-, il suffit alors de remarquer que si γ est un nombre réel ou complexe avec $|\gamma| < 1$, alors pour toute suite $(a_k)_{k\in\mathbb{N}} \in A^{\mathbb{N}}$, on a

$$\left|\sum_{k=0}^{n_x} a_k\gamma^k\right| \leq \max_{a\in A}|a| \sum_{k=0}^{\infty}|\gamma|^k = \frac{\max_{a\in A}|a|}{1-|\gamma|}.$$

Si maintenant γ est un nombre de module 1, alors on a

$$\left|\sum_{k=0}^{n_x} a_k\gamma^k\right| \leq \max_{a\in A}|a| \sum_{k=0}^{n_x} 1 = (n_x+1)\max_{a\in A}|a|,$$

pour toute suite $(a_k)_{k\in\mathbb{N}} \in A^{\mathbb{N}}$, ce qui nous donne le compact K_0.

Pour finir, le lemme II.5.20 permet d'obtenir le compact K_+ dont le diamètre est indépendant de x, et les compacts K_0 et K_- ne dépendent pas du point $x \in \mathbb{H}^3_{\mathbb{R}}$. □

Finissons la preuve de la proposition II.5.16. Le groupe additif $\mathbb{Z}[\beta]$ étant discret dans l'espace E, il existe un réel $\epsilon > 0$ tel que les boules de E centrées aux points de $\mathbb{Z}[\beta]$ et de rayons ϵ sont disjointes. La quantité

$$\#\mathbb{Z}[\beta] \cap (K_+ \times ((n_x+1)K_0) \times K_-) \cdot \mathrm{vol}(B(j,\epsilon))$$

est donc majorée par le volume d'un ϵ-voisinage du compact $K_+ \times ((1+n)K_0) \times K_-$.

On obtient donc la majoration

$$\begin{aligned}\#\Gamma_x 0 &= \#\beta^{n_x}\Gamma_x 0 \\ &\leq \#\mathbb{Z}[\beta] \cap (K_+ \times ((n_x+1)K_0) \times K_-) \\ &\leq \frac{C(n_x+1)^{p_0}}{\mathrm{vol}(B(j,\epsilon))},\end{aligned}$$

pour une constante C, et pour p_0 le nombre de conjugués de β de module 1 (en comptant bien les conjugués complexes). D'autre part, on a $n_x = O(d(j,x))$. Par le sous-lemme II.5.19, on a alors, pour une constante C,

$$\#\Gamma_x \leq \sum_{n=n_x-C}^{n_x} \#\Gamma_x 0 = (C+1)\#\Gamma_x 0 = O(d(j,x)^{p_0}).$$

Ceci termine la preuve du lemme II.5.16. □

Preuve de la proposition II.5.15. Le cas où A est de cardinal inférieur ou égal à 1 est clair : on a facilement $\delta_\Gamma = 0 = \dim_H(\Lambda_\Gamma)$. Supposons donc que l'ensemble A est de cardinal au moins 2. L'ensemble limite contient alors au moins deux points. D'après la proposition II.2.9, l'ensemble limite du semi-groupe est radial : $\Lambda_\Gamma = \Lambda_\Gamma^c$. Or, d'après le corollaire II.5.4, l'ensemble limite radial a une dimension de Hausdorff égale à h_Γ (puisque la dimension de Hausdorf coïncide avec la dimension visuelle, voir (Ghy06) pour plus de détails). Il suffit donc de montrer l'égalité $h_\Gamma = \delta_\Gamma$ pour conclure.

Soit S une partie séparée et 1-couvrante de Γ. D'après le lemme II.5.16, il existe alors un entier r et une constante C tels que pour tout réel R assez grand on ait

$$\#\{\gamma \in \Gamma | d(\gamma j, j) \leq R\} \leq CR^r \#\{\gamma \in S | d(\gamma j, j) \leq R\},$$

On a alors

$$\begin{aligned}\delta_\Gamma &= \limsup_{n\to\infty} \frac{1}{n} \log(\#\{\gamma \in \Gamma | d(j, \gamma j) \leq n\} \\ &\leq \limsup_{n\to\infty} \frac{1}{n} \log(\#\{\gamma \in S | d(j, \gamma j) \leq n\} \\ &= \delta_S,\end{aligned}$$

puisque $\limsup_{n\to\infty} \frac{1}{n} \log(Cn^r) = 0$. D'autre part, on a $\delta_S = h_\Gamma$ puisque S est une partie séparée et couvrante de Γ. On a donc obtenu l'inégalité $h_\Gamma \geq \delta_\Gamma$, et l'autre inégalité $h_\Gamma \leq \delta_\Gamma$ est claire. Cela termine la preuve de la proposition II.5.15. □

Conjecture II.5.25 (Conjecture de Furstenberg modifiée et généralisée)**.** *Soit Γ un sous-semi-groupe de type fini de $SL(2, \mathbb{R})$ dont l'ensemble limite n'est pas réduit à un seul point. Alors on a l'égalité*

$$h_\Gamma = \min(\delta_\Gamma, 1).$$

La conjecture originale posait plutôt la question de l'égalité $\dim_H(\Lambda_\Gamma) = \min(\delta_\Gamma, 1)$. L'avantage de cette formulation, qui est équivalente grâce au corollaire II.5.4 quand le semi-groupe est contractant, est qu'elle ne fait plus intervenir le bord.

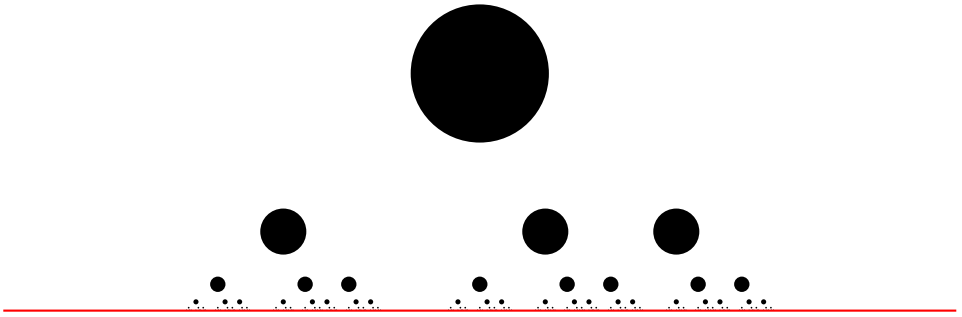
Kenyon attribue cette conjecture à Furstenberg, dans le cas particulier du semi-groupe engendré par les trois applications

$$\begin{cases} x & \mapsto x/3 \\ x & \mapsto x/3 + t \\ x & \mapsto x/3 + 1 \end{cases}$$

où t est un réel. Cette question, sur cet exemple particulier, est toujours ouverte à ma connaissance, bien que l'on sache dire pas mal de choses (voir (Ken97)). Sur cet exemple, la conjecture de Furstenberg se résume à déterminer si l'on a l'égalité $\dim_H(\Lambda_\Gamma) = 1$ quand t est irrationnel, puisque dans ce cas le semi-groupe est libre, ce qui donne $\delta = 1$. Le cas où

t est rationnel a été résolu par Kenyon (et est aussi conséquence de mes résultats puisque dans ce cas le semi-groupe est séparé). Avec mes travaux, la conjecture de Furstenberg se ramène à déterminer si l'on a l'égalité $h_\Gamma = 1$ pour tout t irrationnel.

FIGURE II.14 – Développement en base $\beta = 3$, avec ensemble de chiffres $A = \{0, \frac{2}{3}, 1\}$.



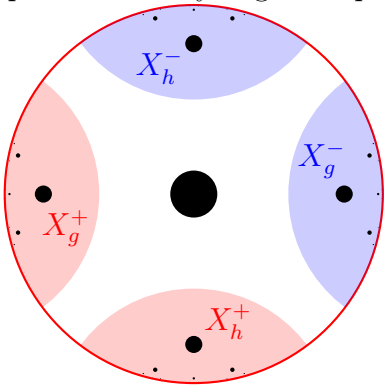
II.6 Sous-groupes de Schottky

Les résultats sur les semi-groupes permettent d'obtenir un résultat sur les groupes : voir corollaire II.6.2 ci-dessous. Plus précisément, nous parvenons à construire des sous-groupes de Schottky à partir de sous-semi-groupes de Schottky, et ceci nous donne des groupes de Schottky ayant un « gros » exposant critique.

Les groupes de Schottky sont définit de façon similaire aux semi-groupes de Schottky, il s'agit des groupes de type fini dont les générateurs jouent au « ping-pong » :

Définition II.6.1. *Soit X un espace métrique. On dit qu'un ensemble G d'isométries de X engendre un groupe de Schottky si c'est un ensemble fini et qu'il existe des parties X_γ^+ et X_γ^- pour tout $\gamma \in G$ qui sont toutes deux-à-deux Gromov-disjointes, et telles que pour tout $\gamma \in G$ on ait $\gamma(X \backslash X_\gamma^-) \subseteq X_\gamma^+$, et telles que l'ensemble $X \backslash (\bigcup_{\gamma \in G} X_\gamma^+ \cup X_\gamma^-)$ soit d'intérieur non vide.*

FIGURE II.15 – Un groupe de Schottky engendré par deux isométries g et h.



Corollaire II.6.2. *Soit X un espace Gromov-hyperbolique propre et soit Γ un groupe discret et sans torsion d'isométries de X ne fixant pas de point au bord, alors on a*

$$\sup_{\substack{\Gamma'<\Gamma \\ \Gamma' \text{ groupe de Schottky}}} \delta_{\Gamma'} \geq \frac{1}{2}\delta_\Gamma,$$

où la borne supérieure est prise sur l'ensemble des sous-groupes de Schottky du groupe Γ.

Ce résultat est à relier à une question dont parle M. Kapovich dans son article (Kap07) (voir Problem 10.27, The gap problem). Avec ses notations, mon résultat donne l'inégalité $d_n \geq n/2$. La question est de savoir si l'on peut atteindre $d_n = n$ ou non.

Preuve du corollaire II.6.2. Le théorème II.3.1 permet de trouver un sous-semi-groupe Γ^c du groupe Γ qui soit contractant pour des parties X_+ et $X_- \subset X$, et d'exposant critique $\delta_{\Gamma^c} = \delta_\Gamma$. On a alors le lemme suivant.

Lemme II.6.3. *Soit X un espace métrique de point base o, et soit Γ^c un sous-semi-groupe d'un groupe discret et sans torsion Γ d'isométries de X, qui soit contractant pour des parties X_+ et X_- de X. Pour tout $\epsilon > 0$, et pour un entier n arbitrairement grand, il existe une partie S_n de Γ^c telle que*

- *S_n engendre un semi-groupe de Schottky pour la partie X_+,*
- *S_n^{-1} engendre un semi-groupe de Schottky pour la partie X_-,*
- *$\#S_n \geq e^{n(\delta_{\Gamma^c}-\epsilon)}$,*
- *$S_n \subseteq A_n$, où*

$$A_n := \{\gamma \in \mathrm{Isom}(X) | d(o, \gamma o) \in [n, n+1[\}.$$

Démonstration. D'après le lemme II.4.4, il existe un réel r et un entier n_0, tels que pour toute partie r-séparée S de Γ^c et pour tout $n \geq n_0$, le semi-groupe engendré par $S \cap A_n$ soit de Schottky pour la partie X_+. En faisant de même pour le semi-groupe inverse $(\Gamma^c)^{-1}$, on obtient un réel r' et un entier n_0'.

Soit S une partie r-séparée et couvrante du semi-groupe contractant Γ^c. La partie $(S \cap A_n)^{-1}$ est séparée, puisque faisant partie du groupe discret et sans torsion Γ. Par le lemme des tiroirs, il existe donc une constante $C > 0$ (dépendant de la séparation du groupe Γ et du réel r'), et une partie r'-séparée S_n^{-1} de $(S \cap A_n)^{-1}$, telles que l'on ait

$$\#S_n \geq C\#(S \cap A_n).$$

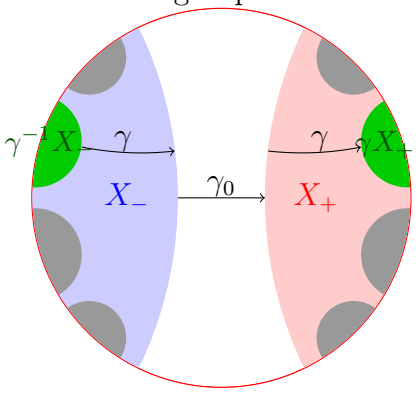
Pour $\epsilon > 0$ fixé, on peut alors trouver un entier n arbitrairement grand, pour lequel on a l'inégalité

$$\#S_n \geq e^{n(\delta_{\Gamma^c}-\epsilon)},$$

puisque l'on a $h_{\Gamma^c} = \delta_{\Gamma^c}$, par séparation du sous-semi-groupe Γ^c du groupe discret Γ. Et par le lemme II.4.4 les parties S_n et S_n^{-1} engendrent chacune un semi-groupe de Schottky respectivement pour les parties X_+ et X_-, puisqu'elles sont respectivement r-séparées et r'-séparée. □

Construisons alors un groupe de Schottky de la façon suivante :

FIGURE II.16 – Construction d'un groupe de Schottky à partir d'un semi-groupe de Schottky dont l'inverse est aussi un semi-groupe de Schottky.



Lemme II.6.4. *Soit X un espace métrique, et soit γ_0 une isométrie de X telle que l'ensemble $\{\gamma_0\}$ soit contractant pour des domaines X_- et X_+. Soit S les générateurs d'un semi-groupe de Schottky pour la partie X_+, tel que l'inverse S^{-1} engendre un semi-groupe de Schottky pour la partie X_-. Posons*

$$G := \{\gamma\gamma_0\gamma | \gamma \in S\}.$$

Alors G engendre un groupe de Schottky.

Démonstration. Pour toute isométrie $\gamma \in S$, on a l'inclusion

$$\gamma\gamma_0\gamma(X \backslash \gamma^{-1}X_-) = \gamma\gamma_0(X \backslash X_-) \subseteq \gamma(X_+) = \gamma X_+,$$

et les parties $\gamma^{-1}X_-$ pour γ décrivant S, et $\gamma' X_+$ pour γ' décrivant S, sont toutes deux à deux Gromov-disjointes. □

Ainsi, en appliquant le lemme II.6.4 avec la partie S_n donnée par le lemme II.6.3 et avec un élément $\gamma_0 \in \Gamma^c$ quelconque, on obtient une partie $G_n := \{\gamma\gamma_0\gamma | \gamma \in S_n\}$ qui engendre un groupe Γ_n de Schottky. Il reste maintenant à minorer l'exposant critique du groupe obtenu.

L'inégalité triangulaire donne $d(o, \gamma\gamma_0\gamma o) \leq 2d(o, \gamma o) + d(o, \gamma_0 o) \leq 2(n+1) + d(o, \gamma_0 o)$. Par le lemme II.4.5, on a donc la minoration

$$\delta_{\Gamma_n} \geq \frac{1}{2(n+1) + d(o, \gamma_0 o)} \log(\#\{G_n\}) \geq \frac{n(\delta_\Gamma - \epsilon)}{2(n+1) + d(o, \gamma_0 o)},$$

puisque l'ensemble G_n engendre un semi-groupe de Schottky (donc libre) qui est un sous-semi-groupe du groupe Γ_n.

L'entier n pouvait être choisi arbitrairement grand, et le réel $\epsilon > 0$ était arbitraire, donc on obtient bien l'inégalité annoncée, ce qui termine la preuve du corollaire II.6.2. □

Remarque II.6.5. *La minoration de la borne supérieure des exposants critiques des sous-groupes de Schottky par $\frac{1}{2}\delta_\Gamma$ n'est pas optimale. En pratique, les groupes de Schottky construits dans cette preuve ont des exposants critiques qui se rapprochent mieux que cela de l'exposant critique total δ_Γ.*

II.7 Caractérisation de l'entropie

Le corollaire suivant du théorème I.2.15 donne en particulier que l'exposant critique d'un semi-groupe séparé, qui était définit comme une limite supérieure d'une certaine quantité, est en fait une vraie limite. Ceci généralise un résultat que Roblin a établit pour un groupe discret d'isométries d'un espace CAT(-1) (mais avec une conclusion plus forte), voir (Rob03).

Corollaire II.7.1. *Soit X un espace Gromov-hyperbolique propre, et soit Γ un semi-groupe d'isométries de X dont l'ensemble limite contient au moins deux points. Alors on a*

$$h_\Gamma = \lim_{n\to\infty} \frac{1}{n} \log(\#\{\gamma \in S | d(o, \gamma o) \leq n\}),$$

pour toute partie S séparée et couvrante de Γ.

Démonstration. Soit $\epsilon > 0$. Par définition de la limite supérieure, il existe un entier n_0 tel que pour tout $n \geq n_0$, on ait

$$\frac{1}{n} \log(\#\{\gamma \in S | d(o, \gamma o) \leq n\}) \leq \delta_S + \epsilon = h_\Gamma + \epsilon.$$

Montrons l'autre sens. D'après le théorème II.3.1, il existe un sous-semi-groupe Γ^c de Γ qui est contractant et d'exposant critique $\delta_{\Gamma^c} = \delta_\Gamma$, puisque les semi-groupes Γ et Γ^c sont séparés.

Sous lemme II.7.2. *Soit X un espace métrique et $A \subseteq X$ une partie. Soit S une partie séparée et couvrante de A et $r > 0$ un réel. Alors il existe une partie $S' \subseteq S$ telle que S' est une partie r-séparée et couvrante de A.*

Démonstration. Par récurrence ordinale, on construit une suite (x_i) d'éléments de S indexée par les ordinaux, en choisissant un élément

$$x_i \in S \backslash \bigcup_{j<i} B(x_j, r)$$

tant que l'ensemble est non vide. Cela termine nécessairement puisque la suite ainsi construite ne peut pas avoir un cardinal strictement supérieur à celui de S. La partie S' constituée des éléments de la suite est alors r-séparée, et elle est $(C + r)$-couvrante de A, où C est telle que S est C-couvrante de A. En effet, si $x \in A$, il existe un élément $y \in S$ tel que $d(x, y) \leq C$. Et par construction, il existe un élément $z \in S'$ tel que $d(y, z) \leq r$. On a alors bien trouvé $z \in S'$ tel que $d(x, z) \leq C + r$. □

D'après le lemme II.4.4, quitte à remplacer la partie S par une sous-partie suffisamment séparée et encore couvrante de Γ^c, il existe un entier k_0 tel que pour tout $k \geq k_0$, l'ensemble $S \cap A_k$ engendre un semi-groupe de Schottky Γ_k, où

$$A_k := \{\gamma \in \mathrm{Isom}(X) | d(o, \gamma o) \in [k, k+1[\}.$$

Pour tout $n \geq k+1 \geq k_0+1$, en utilisant l'inégalité triangulaire et le fait que le semi-groupe Γ_k soit libre, on obtient l'inégalité

$$\#\{\gamma \in \Gamma_k | d(o, \gamma o) \leq n\} \geq \#\{\gamma \in \Gamma_k | \gamma \text{ de longueur } \left\lfloor \frac{n}{k+1} \right\rfloor\} = (\#(S \cap A_k))^{\left\lfloor \frac{n}{k+1} \right\rfloor}.$$

On a donc l'inégalité

$$\frac{1}{n} \log(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}) \geq \frac{1}{n} \left\lfloor \frac{n}{k+1} \right\rfloor \log(\#(S \cap A_k)),$$

pour tout $n \geq k$.

Or, il existe un entier k tel que

$$\frac{1}{k+1} \log(\#(S \cap A_k)) \geq \delta_S - \epsilon/2.$$

Et comme S est une partie couvrante de Γ^c, on a $\delta_S = h_{\Gamma^c} = h_\Gamma$.

De plus, on a $\frac{1}{n} \left\lfloor \frac{n}{k+1} \right\rfloor (k+1) \geq 1 - \frac{k+1}{n}$, ce qui nous donne l'inégalité

$$\frac{1}{n} \log(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}) \geq \left(1 - \frac{k+1}{n}\right) (h_\Gamma - \epsilon/2).$$

On peut alors trouver un entier $n_k \geq n_0$ tel que pour tout $n \geq n_k$ on ait

$$h_\Gamma + \epsilon \geq \frac{1}{n} \log(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}) \geq h_\Gamma - \epsilon.$$

Ainsi, on a bien montré que l'on a

$$\lim_{n \to \infty} \frac{1}{n} \log(\#\{\gamma \in \Gamma | d(o, \gamma o) \leq n\}) = h_\Gamma.$$

□

II.8 Semi-continuité inférieure de l'entropie

Nous allons voir que l'entropie est semi-continue inférieurement en un semi-groupe. Pour cela, commençons par donner une notion de convergence sur l'ensemble des semi-groupes d'isométries d'un espace métrique X.

Rappelons la définition de la topologie usuelle compacte-ouverte sur $\mathrm{Isom}(X)$.

Définition II.8.1. *Soit X un espace métrique. On dit qu'une suite d'isométries $(\gamma_n)_{n\in\mathbb{N}} \in (\mathrm{Isom}(X))^{\mathbb{N}}$ converge vers une isométrie $\gamma \in \mathrm{Isom}(X)$ si pour tout compact K de X, la suite $(\gamma_{n\,|K})_{n\in\mathbb{N}}$ des isométries restreintes à K converge uniformément vers $\gamma_{|K}$, et si de même la suite $({\gamma_n^{-1}}_{|K})_{n\in\mathbb{N}}$ converge uniformément vers ${\gamma^{-1}}_{|K}$.*

Remarque II.8.2. *Ici, la convergence uniforme des inverses $({\gamma_n^{-1}}_{|K})_{n\in\mathbb{N}}$ sur tout compact K est automatique à partir de la convergence uniforme de la suite $(\gamma_{n\,|K})_{n\in\mathbb{N}}$ pour tout compact K, puisque ce sont des isométries.*

Définition II.8.3. *Soit X un espace métrique. On dit qu'une suite $(\Gamma_n)_{n\in\mathbb{N}}$ de semi-groupes d'isométries de X converge géométriquement vers un semi-groupe Γ, si l'on a les deux propriétés :*

- *pour toute isométrie $\gamma \in \Gamma$, il existe une suite d'isométries $(\gamma_n)_{n\in\mathbb{N}}$, avec pour tout n, $\gamma_n \in \Gamma_n$ et telle que γ_n converge vers γ.*
- *pour toute partie infinie $P \subseteq \mathbb{N}$ et toute suite d'isométries $(\gamma_n)_{n\in P}$ qui converge vers une isométrie $\gamma \in \mathrm{Isom}(X)$, avec $\gamma_n \in \Gamma_n$ pour tout $n \in P$, on a $\gamma \in \Gamma$.*

Voir (Hae12) pour plus de détails sur la convergence géométrique.

Remarque II.8.4. *Dans notre résultat de semi-continuité, nous avons besoin seulement de la première de ces deux propriétés.*

Voici le résultat de semi-continuité :

Corollaire II.8.5. *Soit $(\Gamma_n)_{n\in\mathbb{N}}$ une suite de semi-groupes d'isométries d'un espace Gromov-hyperbolique propre à bord compact X qui converge vers un semi-groupe Γ dont l'ensemble limite contient au moins deux points. Alors on a l'inégalité*

$$h_\Gamma \leq \liminf_{n\to\infty} h_{\Gamma_n}.$$

Autrement dit, l'entropie est semi-continue inférieurement en les semi-groupes dont l'ensemble limite contient au moins deux points.

Remarque II.8.6. *On pourrait aussi montrer que l'entropie est continue en les semi-groupes de Schottky.*

L'idée de la preuve du corollaire II.8.5, est de montrer que si l'on a une suite de semi-groupes qui converge, alors on peut approcher un sous-semi-groupe de Schottky du semi-groupe limite par des sous-semi-groupes des semi-groupes de la suite, en trouvant des éléments qui s'approchent des générateurs. Ces semi-groupes seront alors des semi-groupes de Schottky dont les exposants critiques seront proches de celui du semi-groupe de Schottky de départ, et ainsi on obtiendra l'inégalité voulue.

Preuve du corollaire II.8.5. D'après le théorème II.3.1, il existe un sous-semi-groupe contractant Γ^c de Γ pour des parties X_- et $X_+ \subset X$, avec $h_{\Gamma^c} = h_\Gamma$. De plus, on peut supposer que les parties X_- et X_+ de X sont ouvertes, quitte à les remplacer chacune par un ϵ-voisinage ouvert, pour $\epsilon > 0$ assez petit.

D'après le critère de contraction (proposition II.2.4), il existe un réel n_0 tel que l'ensemble d'isométries

$$\mathrm{Isom}(X)^{X_-\times X_+}_{>n_0} := \{\gamma \in \mathrm{Isom}(X) | \gamma^{-1}o \in X_-, \gamma o \in X_+ \text{ et } d(o,\gamma o) > n_0\},$$

soit contractant, pour des domaines X'_- et X'_+.

D'après le lemme II.4.4, il existe alors un réel r et un entier n_1, tels que pour toute partie r-séparée S de $\mathrm{Isom}(X)^{X_-\times X_+}_{>n_0}$ et pour tout $n \geq n_1$, le semi-groupe engendré par $S \cap \overset{\circ}{A}_n$ soit de Schottky pour la partie X'_+, où

$$\overset{\circ}{A}_n := \{\gamma \in \mathrm{Isom}(X) | d(o,\gamma o) \in]n, n+1[\}.$$

Soit S une partie r-séparée et couvrante du semi-groupe contractant Γ^c.

L'ensemble $S \cap \overset{\circ}{A}_n$ étant fini, il existe une suite d'ensembles d'isométries $S_{k,n}$ de Γ_k, avec $\#S \cap \overset{\circ}{A}_n = \#S_{k,n}$, qui converge uniformément vers $S \cap \overset{\circ}{A}_n$.

Les ensembles $\overset{\circ}{A}_n \cap X_-$ et $\overset{\circ}{A}_n \cap X_+$ étant ouverts, il existe un entier k_0 tel que pour tout $k \geq k_0$, on ait $S_{k,n}o \subseteq \overset{\circ}{A}_n \cap X_+$ et $S^{-1}_{k,n}o \subseteq \overset{\circ}{A}_n \cap X_-$. Pour $n > n_0$ et $k \geq k_0$, on a donc l'inclusion $S_{k,n} \subseteq \mathrm{Isom}(X)^{X_-\times X_+}_{>n_0}$. La condition pour une partie S d'être r-séparée est également une condition ouverte, donc il existe un entier $k_1 \geq k_0$ tel que pour tout $k \geq k_1$ la partie $S_{k,n}$ soit r-séparée.

Ainsi, pour n assez grand et pour tout entier k assez grand en fonction de n, la partie $S_{k,n}$ est incluse dans le semi-groupe contractant $\mathrm{Isom}(X)^{X_-\times X_+}_{>n_0}$, et est r-séparée. Elle engendre donc un semi-groupe de Schottky.

Par le lemme II.4.5, on a donc l'inégalité

$$h_{\Gamma_k} \geq \frac{\log(\#S_{k,n})}{n+1} = \frac{\log(\#S \cap \overset{\circ}{A}_n)}{n+1},$$

pour tout n assez grand, et pour tout k assez grand en fonction de n.

On obtient donc ce que l'on voulait

$$\liminf_{k\to\infty} h_{\Gamma_k} \geq \limsup_{n\to\infty} \frac{\log(\#S \cap \overset{\circ}{A}_n)}{n+1} = h_\Gamma.$$

□

a) Exemple d'application : les semi-groupes de Kenyon

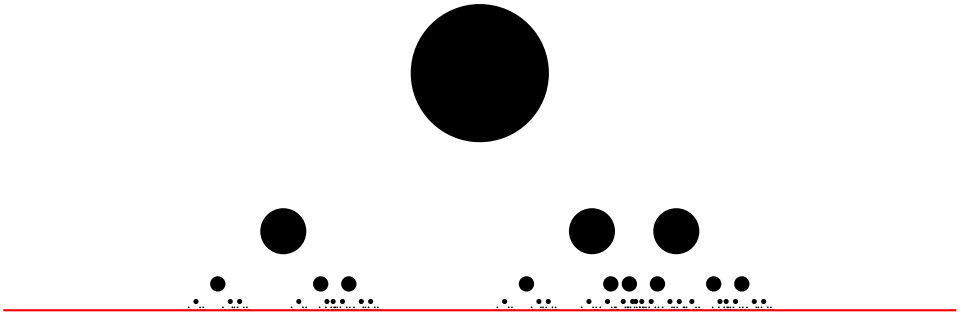
Les semi-groupes de Kenyon (voir (Ken97)) sont les semi-groupes Γ_t engendrés par les 3 transformations affines

$$\begin{cases} x & \mapsto x/3 \\ x & \mapsto x/3 + t \\ x & \mapsto x/3 + 1 \end{cases}$$

pour des réels t.

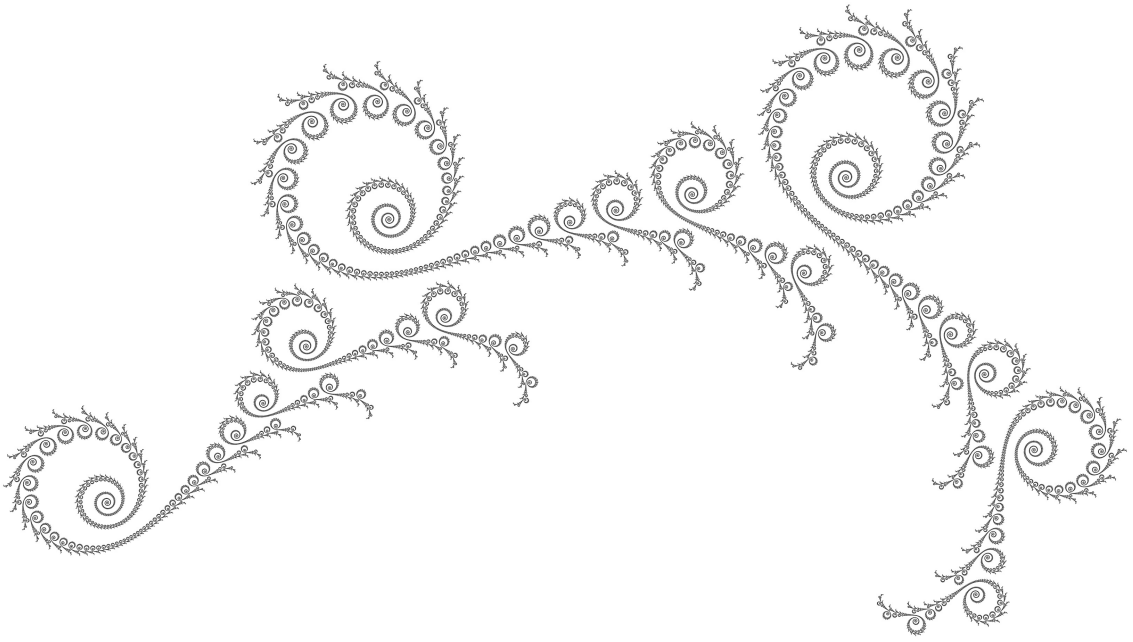
D'après le corollaire II.8.5, l'application $t \mapsto h_{\Gamma_t} = \dim(\Lambda_{\Gamma_t})$ est semi-continue inférieurement. En particulier, pour trouver un contre exemple à la conjecture de Furstenberg (i.e. un réel t pour lequel on a $\dim_H(\Lambda_{\Gamma_t}) < \delta_{\Gamma_t}$), il suffit de trouver une suite de rationnels $(t_n)_{n\in\mathbb{N}}$ qui converge vers un irrationnel et avec pour tout n, $\delta_{\Gamma_{t_n}} \leq C < 1$. Mais bien que l'on sache calculer l'exposant critique δ_{Γ_t} du semi-groupe Γ_t pour tout rationnel t, on ne sait pas s'il existe de telles suites. Voir (Ken97) et la section III.3 pour plus de détails.

FIGURE II.17 – Développement en base $\beta = 3$, avec ensemble de chiffres $A = \{0, \frac{\pi}{4}, 1\}$.



Remarque II.8.7. *L'application $t \mapsto h_{\Gamma_t} = \dim_H(\Lambda_{\Gamma_t})$ n'est pas continue. En effet, on sait que l'on a $\dim_H(\Lambda_{\Gamma_t}) = 1$ pour t dans une partie dense de $\mathbb{R}$, et on a par exemple $\dim_H(\Lambda_{\Gamma_{2/3}}) = \delta_{\Gamma_{2/3}} < 1$ (voir figure II.14).*

FIGURE II.18 – Ensemble limite d'un sous-semi-groupe de $SL(2, \mathbb{C})$



Chapitre III

Semi-groupes fortement automatiques

Dans ce chapitre, nous introduisons la notion de semi-groupe fortement automatique, qui consiste à avoir un ensemble de relations qui soit un langage rationnel, c'est-à-dire que l'on peut décider si deux mots en les générateurs représentent le même élémént du semi-groupe en lisant les deux mots à la même vitesse, et avec une mémoire finie. Cela permet de calculer des valeurs exactes d'exposants critiques. Voyons cela sur un exemple.

Exemple de semi-groupe fortement automatique

Considérons le monoïde Γ, de développement en base 3, engendré par les trois transformations affines :

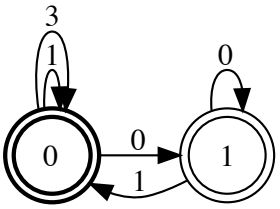
$$\begin{cases} 0: & x & \mapsto & x/3, \\ 1: & x & \mapsto & x/3 & + & 1, \\ 3: & x & \mapsto & x/3 & + & 3. \end{cases}$$

Par définition, c'est le plus petit semi-groupe contenant ces trois applications et l'identité, et l'on peut le voir comme le sous-monoïde de $SL(2,\mathbb{R})$ engendré par les matrices $\begin{pmatrix} 1/\sqrt{3} & k\sqrt{3} \\ 0 & \sqrt{3} \end{pmatrix}$, pour $k \in \{0,1,3\}$.
Voici quelques questions que l'on peut se poser :

- Quel est l'exposant critique de ce semi-groupe ?
- Quel est l'asymptotique du nombre d'éléments pour la longueur des mots ?
- Comment peut-on déterminer si deux mots en les générateurs représentent le même élément du semi-groupe ?
- Y a-t'il une façon de représenter les éléments du semi-groupes par des mots uniques particuliers (que l'on appelera mots réduits, ou encore forme normale) ?

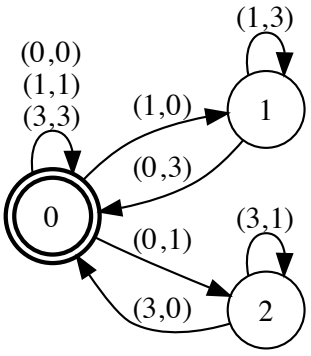
La réponse à ces questions est donnée par la structure automatique du semi-groupe. Celle-ci est donnée par des automates tels que l'on peut en voir sur les figures suivantes (voir la partie III.1 pour des rappels sur les automates) :

FIGURE III.1 – Automate reconnaissant un ensemble de mots réduits du semi-groupe. Les mots réduits sont ici les mots minimaux pour l'ordre lexicographique inverse, avec $0 < 1 < 3$.



On appelle *mots réduits* un choix de représentants uniques pour les éléments du semi-groupe par des mots en les générateurs. On voit sur l'automate de la figure I.1 que les mots réduits sont ici exactement les mots ne contenant pas le mot 03.

FIGURE III.2 – Automate reconnaissant les relations du semi-groupe.



On voit sur l'automate de la figure I.2 que les relations du semi-groupe Γ s'obtiennent toutes à partir des relations $11^n0 = 03^n3$, par concaténation.

Exemple III.0.8. *Le mot* $(1,0)(1,3)(0,3)$ *est reconnu par l'automate de la figure III.2, et on a en effet la relation* $1 \circ 1 \circ 0 = 0 \circ 3 \circ 3$*, puisque l'on a l'égalité*

$$\frac{\frac{\frac{x}{3}+1}{3}+1}{3} = \frac{\frac{\frac{x}{3}+3}{3}+3}{3}.$$

Deux mots $u_1...u_n$ et $v_1...v_n$ en les générateurs $\{0,1,3\}$ représentent le même élément du semi-groupe si et seulement si le mot $(u_1,v_1)...(u_n,v_n)$ est reconnu par l'automate de la figure III.2.

L'automate de la figure III.1 fournit un moyen de connaître le nombre d'éléments du semi-groupe de longueur n donnée : celui-ci est en effet égal au nombre de chemins de longueur n de l'état initial 0 vers les états finaux 0 et 1. Ceci est donné par la somme des deux premiers coefficients des puissances de la matrice d'adjacence du graphe :

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

dont les valeurs propres sont $\frac{\sqrt{5}+3}{2}$ et $\frac{3-\sqrt{5}}{2}$. Ainsi, on voit que le nombre d'éléments du semi-groupe de longueur n est exactement f_{2n+2}, où $(f_n)_{n\in\mathbb{N}}$ est la suite de Fibonnacci :

$$\begin{aligned} f_0 &:= 0, \\ f_1 &:= 1, \\ f_{n+2} &:= f_{n+1} + f_n. \end{aligned}$$

En particulier, le nombre d'éléments du semi-groupe de longueur n est asymptotiquement

$$c\left(\frac{\sqrt{5}+3}{2}\right)^n + O\left(\left(\frac{3-\sqrt{5}}{2}\right)^n\right)$$

pour une constante $c > 0$. Cela permet d'obtenir que l'exposant critique du semi-groupe vaut

$$\delta_\Gamma := \log(\frac{\sqrt{5}+3}{2}).$$

Résultats du chapitre

Le principal résultat du chapitre est le critère suivant, de forte automaticité pour les semi-groupes de développement en base β.

Théorème III.0.9. *Soit un semi-groupe Γ engendré par les transformations :*

$$x \mapsto \beta x + t$$

pout $t \in A \subset \mathbb{C}$, où A est une partie finie de $\mathbb{C}$, et β est un nombre complexe.

Si le nombre complexe β est transcendant, ou bien algébrique mais sans conjugué de module 1, alors pour toute partie $A \subset \mathbb{C}$ finie, le semi-groupe Γ est fortement automatique.

Réciproquement, si le nombre complexe β est algébrique et a au moins un conjugué de module 1, alors il existe une partie $A \subset \mathbb{C}$ finie telle que le semi-groupe Γ n'est pas fortement automatique.

Notre preuve étant effective, nous obtenons de plus un algorithme (dont celui de Kenyon est un cas particulier, voir (Ken97)) permettant de calculer exactement les exposants critiques des semi-groupes qui satisfont les hypothèses du théorème. Après implémentation, ceci nous a permis de donner explicitement, dans cette thèse, les exposants critiques pour de nombreux exemples de semi-groupes.

La réciproque du théorème ne permet pas de choisir la partie A. Nous parvenons à obtenir cette réciproque pour la partie $A = \{0, 1\}$ sur un exemple :

Proposition III.0.10. *Soit le nombre de Salem $\beta = \frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2} \simeq 1.8832035059$, qui est racine du polynôme $X^4 - 2X^3 + X^2 - 2X + 1$. Alors le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$

n'est pas fortement automatique.

Nous avons relié la notion de semi-groupes fortement automatiques à des notions existantes : celle de monoïde rationnel et celle de semi-groupe automatique.

Proposition III.0.11. *Un monoïde fortement automatique est rationnel. Réciproquement si un monoïde est rationnel et qu'il admet un ensemble de générateurs pour lequel il n'existe pas d'égalité entre des mots de longueurs différentes, alors il est fortement automatique.*

Proposition III.0.12. *Un semi-groupe fortement automatique est automatique.*

Pour un semi-groupe fortement automatique, nous obtenons un algorithme de recherche du mot réduit meilleur que celui existant pour les semi-groupes automatiques, car linéaire au lieu de quadratique :

Proposition III.0.13. *Si un semi-groupe est fortement automatique, alors il existe un algorithme linéaire prenant en entrée un mot et rendant le mot réduit correspondant.*

Étant donné un semi-groupe fortement automatique, la question se pose de savoir s'il est nécessairement de présentation finie. Nous montrons, que la réponse est négative :

Proposition III.0.14. *Soit* $\beta \simeq 1.7924023578$ *la racine réelle du polynôme* $X^5 - X^4 - X^3 - X^2 + X - 1$. *Alors le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x \mapsto \beta x \\ 1 : x \mapsto \beta x + 1 \end{cases}$$

n'est pas de présentation finie.

Organisation du chapitre

Nous commençons par faire des rappels sur les automates dans la section III.1. Dans la section III.2, nous définissons les semi-groupes fortement automatiques et voyons les liens avec les autres notions d'automaticités existantes. Nous définissons en III.2.1 ce qu'est un semi-groupe fortement automatique, et nous en donnerons quelques propriétés. Nous définissons en III.2.2 ce qu'est un monoïde rationnel et montrons la proposition III.0.11. Nous rappellons ensuite en III.2.3 ce qu'est un semi-groupe automatique, et nous montrerons en III.2.4 que les semi-groupes fortement automatiques sont automatiques (proposition III.0.12). Nous présentons notre algorithme pour le problème des mots réduits en III.2.5. Nous nous intéressons ensuite aux semi-groupes correspondants aux développements en base β dans la section III.3 où nous démontrons le théorème III.0.9 annoncé (voir théorème III.3.2 et proposition III.3.15). Enfin, la partie III.4 est consacrée à des exemples, et rappelle des travaux en lien avec les semi-groupes fortement automatiques.

III.1 Rappels sur les automates et les langages rationnels

Dans cette partie, je donne des rappels sur les automates qui seront utiles dans la suite. Les automates sont en quelques sortes des machines qui peuvent réaliser tous les calculs en temps linéaire ne nécessitant qu'une mémoire finie. Pour plus de détails, voir par exemple (Car08), sections 1.5.2, 1.6, et 1.7.

Définition III.1.1. *On appelle automate un quintuplet $\mathcal{A} := (\Sigma, Q, T, I, F)$, où*

1. *Σ est un ensemble fini appelé alphabet,*
2. *Q est un ensemble fini d'états,*
3. *$T \subseteq Q \times \Sigma \times Q$ est l'ensemble des transitions,*
4. *$I \subseteq Q$ est l'ensemble des états initiaux,*
5. *$F \subseteq Q$ est l'ensemble des états finaux.*

On dira que l'automate est déterministe si l'on a $\#I = 1$ et

$$[(p, a, q) \in T \text{ et } (p, a, r) \in T] \text{ implique } q = r.$$

Autrement dit, quand l'automate $\mathcal{A}$ est déterministe, T est le graphe d'une fonction partielle de transition $Q \times \Sigma \to Q$, et il n'y a qu'un seul état initial.

On considèrera parfois des automates infinis, c'est-à-dire des automates pour lesquels l'ensemble d'états Q est infini.

Notation . *On notera $p \xrightarrow{a} q$ si $(p, a, q) \in T$.*

Notation . *Étant donné un alphabet Σ, on notera $\Sigma^* := \Sigma^{(\mathbb{N})}$ l'ensemble des mots finis. Pour $u \in \Sigma^*$, on notera également $u^* := \cup_{n\in\mathbb{N}}\{u^n\} = \{u\}^*$.*

Représentation graphique

On représente les automates comme des graphes dont les arêtes sont étiquetées par des lettres de l'alphabet. Sur les dessins de ce chaitre, l'état initial est en gras, et les états finaux sont les ronds dessinés avec un trait double.

FIGURE III.3 – Automate ayant pour états {0, 1, 2, 3, 4}, pour alphabet {(0,0), (0,1), (1,0), (1,1)}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0}.

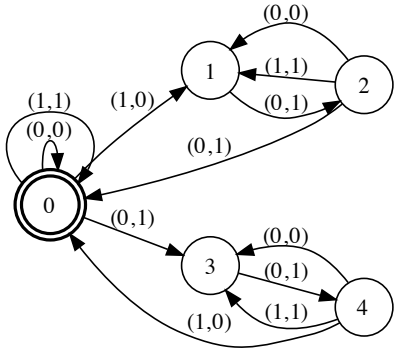


FIGURE III.4 – Automate ayant pour états {0, 1, 2, 3, 4}, pour alphabet {0, 1, *}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0}.

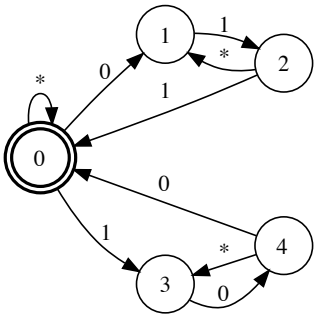
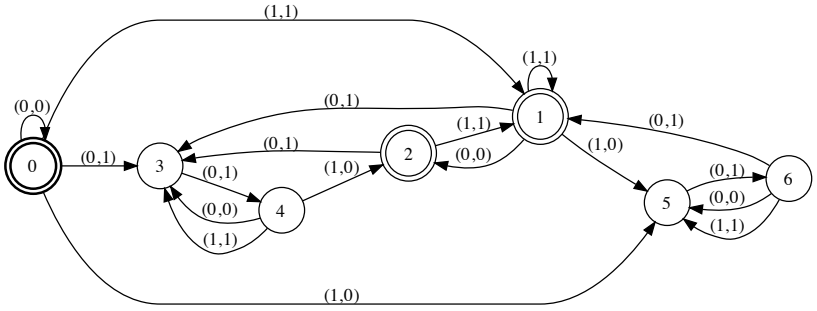


FIGURE III.5 – Automate ayant pour états {0, 1, 2, 3, 4, 5, 6}, pour alphabet {(0,0), (0,1), (1,0), (1,1)}, pour ensemble d'états initiaux {0} et pour ensemble d'états finaux {0, 1, 2}.



Définition III.1.2. *On appelle langage reconnu par un automate* $\mathcal{A} = (\Sigma, Q, T, I, F)$ *l'ensemble* $L_{\mathcal{A}}$ *des mots* $a_1 \dots a_n \in \Sigma^*$ *tels qu'il existe un chemin*

$$I \ni q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \dots\dots \xrightarrow{a_{n-1}} q_{n-1} \xrightarrow{a_n} q_n \in F$$

dans l'automate A, d'un état initial vers un état final.
On dit qu'un mot $u \in \Sigma^*$ *est reconnu par l'automate* $\mathcal{A}$ *si l'on a* $u \in L_{\mathcal{A}}$.

Un mot $a_1 \dots a_n$ est donc reconnu par l'automate $\mathcal{A}$ s'il existe un chemin dans le graphe, étiqueté par $a_1, a_2, \dots, a_n$, partant d'un état initial et aboutissant à un état final.

Remarque III.1.3. *Si l'automate est déterministe, un tel chemin est unique.*

Exemple III.1.4. *Voir figures III.5, III.7, III.8 et III.9.*

FIGURE III.6 – Automate reconnaissant l'ensemble des nombres écrits en binaires qui sont divisibles par 3.

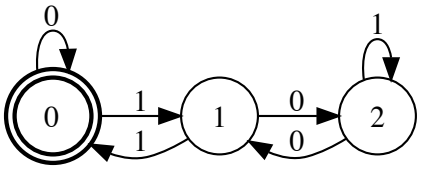


FIGURE III.7 – Automate reconnaissant l'ensemble des mots de la forme $a(baa)^n$.

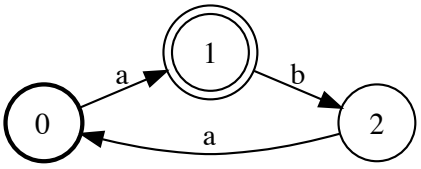


FIGURE III.8 – Automate non déterministe reconnaissant l'ensemble de mots {lapin, laitue}.

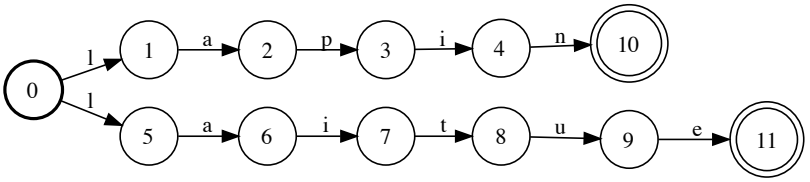
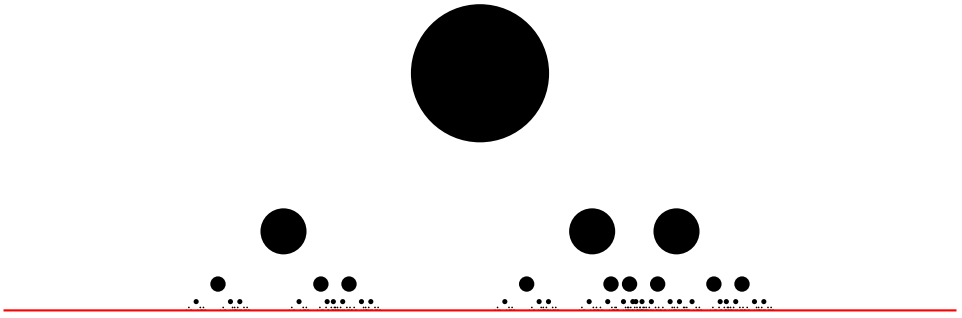


FIGURE III.9 – Automate reconnaissant les couples (u, v) de mots avec u strictement inférieur à v dans l'ordre lexicographique.



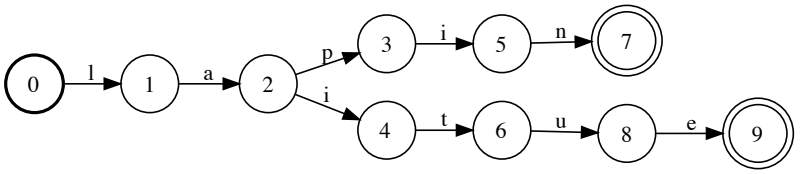
Dans la figure III.9, dire qu'un couple (u, v) de mots de Σ^* est reconnu signifie qu'un mot $(u_1, v_1) \dots (u_n, v_n) \in (\Sigma \times \Sigma)^*$ est reconnu, avec $u = u_1 \dots u_n$ et $v = v_1 \dots v_n$. On suppose que l'alphabet Σ est muni d'une relation d'ordre totale.

Définition III.1.5. *On dit que deux automates $\mathcal{A}$ et $\mathcal{A}'$ sont équivalents s'ils reconnaissent le même langage : $L_{\mathcal{A}} = L_{\mathcal{A}'}$.*

On a la proposition suivante :

Proposition III.1.6. *Tout automate est équivalent à un automate déterministe.*

FIGURE III.10 – Automate déterministe équivalent à celui de la figure III.8.



Définition III.1.7. *On appelle automate minimal d'un automate $\mathcal{A}$, un automate $\mathcal{A}'$ déterministe, équivalent à $\mathcal{A}$, et ayant un nombre minimal de sommets pour ces propriétés.*

Proposition III.1.8. *L'automate minimal d'un automate $\mathcal{A}$ est unique. De plus si l'automate $\mathcal{A}$ est déterministe et complet, alors l'automate minimal s'obtient comme le quotient de l'automate $\mathcal{A}$ par une relation d'équivalence consistant à identifier des sommets entre eux.*

Exemple III.1.9. *L'automate de la figure III.10 est minimal.*

Définition III.1.10. *On appelle transposée d'un automate $\mathcal{A} = (\Sigma, Q, T, I, F)$ l'automate*

$$\mathcal{A}^t := (\Sigma, Q, T^t, F, I)$$

où $T^t := \{(p, a, q) \in Q \times \Sigma \times Q | (q, a, p) \in T\}$.

Remarque III.1.11. *Le langage reconnu par l'automate transposé $\mathcal{A}^t$ est la transposée du langage reconnu par l'automate initial $\mathcal{A}$.*

Définition III.1.12. *On appelle émondé d'un automate, l'automate restreint aux sommets par lesquels il passe un chemin d'un état initial à un état final. On dit qu'un automate est émondé s'il est égal à son émondé.*

Autrement dit, un automate est émondé s'il n'existe pas de sommet qui ne sert à rien !

Proposition III.1.13. *Un automate (éventuellement infini) émondé déterministe, et de transposée déterministe est minimal. En particulier, s'il est infini, le langage qu'il reconnait n'est pas rationnel.*

Démonstration. Soit L un langage sur l'alphabet Σ. Pour tout mot $w \in \Sigma^*$, on définit un quotient à gauche

$$w^{-1}L := \{u \in \Sigma^* | wu \in L\}.$$

Il est alors bien connu que le langage L est rationnel si et seulement si l'ensemble de ses quotients à gauche est fini (voir prop. 1.82 dans (Car08)), et l'on peut construire un automate minimal pour le langage L dont les états sont les quotients à gauche (voir déf. 1.83 dans (Car08)).

Soit maintenant $\mathcal{A}$ un automate émondé déterministe, et de transposée déterministe, reconnaissant un langage L. On peut associer à chaque état q de l'automate $\mathcal{A}$ un quotient à gauche $w^{-1}L$ pour un mot w étiquetant un chemin de l'état initial jusqu'à l'état q. Cela est possible puisque l'automate est émondé, et ce quotient ne dépend alors pas du mot w choisi : on le notera L_q. On a alors le fait suivant.

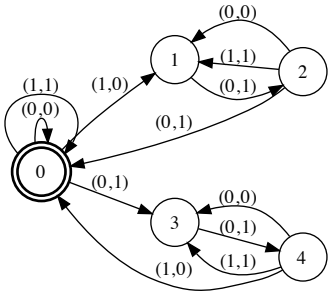
Fait . *Les quotients à gauches qui correspondent à deux états distincts de l'automate $\mathcal{A}$ sont distinctes.*

En effet, l'automate étant de transposée déterministe, si l'on considère un chemin d'un état q à un état final étiqueté par un mot w, alors il ne peut pas exister de chemin d'un état $q' \neq q$ vers un état final étiqueté par le même mot w. Cela se traduit par la disjonction $L_q \cap L_{q'} = \emptyset$. Or, chacun des deux langages est non vide, puisque l'automate est supposé émondé, d'où $L_q \neq L_{q'}$ si $q \neq q'$ sont deux états distincts de l'automate $\mathcal{A}$.

Les états de l'automate $\mathcal{A}$ correspondent donc à des quotients à gauche toutes distinctes, et la définition 1.83 dans (Car08) donne un automate minimal pour le langage L qui est exactement l'automate $\mathcal{A}$, d'où le résultat. □

Remarque III.1.14. *La réciproque est fausse : un automate minimal fini n'est pas nécessairement de transposée déterministe.*

FIGURE III.11 – Automate minimal car vérifiant les conditions de la proposition III.1.13.



Notation . *Dans tout le chapitre, ϵ dénote le mot vide, c'est-à-dire le mot ayant 0 lettres.*

Définition III.1.15. *On définit l'ensemble des langages rationnels comme étant la plus petite partie* Rat $\subset \mathcal{P}(\Sigma^*)$ *de l'ensemble des langages sur l'alphabet Σ vérifiant :*

1. $\emptyset \in$ Rat,
2. $\{\epsilon\} \in$ Rat *(où ϵ est le mot vide),*
3. $\{a\} \in$ Rat *pour tout $a \in \Sigma$,*
4. Rat *est stable par union :* $L, L' \in$ Rat *implique* $L \cup L' \in$ Rat.
5. Rat *est stable par concaténation :* $L, L' \in$ Rat *implique* $LL' \in$ Rat.
6. Rat *est stable par complémentaire :* $L \in$ Rat *implique* $\Sigma^* \backslash L \in$ Rat.
7. Rat *est stable par étoile :* $L \in$ Rat *implique* $L^* \in$ Rat.

On a le théorème suivant :

Théorème III.1.16 (Kleene)**.** *Un langage $L \subseteq \Sigma^*$ est rationnel si et seulement si c'est le langage d'un automate.*

Voir par exemple (Car08), théorème 1.59, page 36.

Définition III.1.17. *Étant donnés deux langages $L \subseteq \Sigma^*$ et $K \subseteq \Lambda^*$, respectivement sur les alphabets Σ et Λ, on appelle* produit *des deux langages, le langage noté $L \times K$ sur l'alphabet $\Sigma \times \Lambda$ définit par :*

$$L \times K := \{(a_1, b_1) \dots (a_n, b_n) \in (\Sigma \times \Lambda)^* | a_1 \dots a_n \in L \text{ et } b_1 \dots b_n \in K\}.$$

Proposition III.1.18. *Le produit de deux langages rationnels est un langage rationnel.*

Définition III.1.19. *Étant donné un langage $L \subset (\Sigma \times \Lambda)^*$, on définit les projetés $p_1(L) \subset \Sigma^*$ et $p_2(L) \subset \Lambda^*$ du langage L par*

$$p_1(L) := \{u \in \Sigma^* | \text{Il existe } v \in \Lambda^* \text{ tel que } (u, v) \in L\},$$

$$p_2(L) := \{v \in \Lambda^* | \text{Il existe } u \in \Sigma^* \text{ tel que } (u, v) \in L\}.$$

Proposition III.1.20. *Un projeté d'un langage rationnel est un langage rationnel.*

Voir (Car08), Proposition 1.95.

Lemme III.1.21 (de l'étoile)**.** *Si un langage L est rationnel, alors il existe une constante $N > 0$ telle que pour tout mot $u_1u_2u_3 \in \Sigma^*$ avec $|u_2| > N$, il existe trois mots v_1, v_2 et v_3 avec $|v_2| > 0$ tels que l'on ait $u_2 = v_1v_2v_3$ et*

$$\text{pour tout entier } n \in \mathbb{N}, \quad u_1v_1{v_2}^n v_3u_3 \in L.$$

(Ici, $|u|$ dénote la longueur du mot u)

III.2 Semi-groupe automatique et fortement automatique

Dans cette partie, nous allons définir ce que sont les structures automatique et fortement automatique, et nous allons voir comment déterminer la structure fortement automatique d'un sous-semi-groupe de type fini d'un groupe.

Dans toute la suite, Γ est un sous-semi-groupe d'un groupe G, et Σ est une partie génératrice finie de Γ. On notera e l'élément neutre du groupe G.

Remarque III.2.1 (Laurent Bartholdi)**.** *Tous les résultats qui suivent se généralisent aux monoïdes simplifiables. Mais on se place dans un cadre moins général par soucis de clarté.*

III.2.1 Semi-groupe fortement automatique

Définition III.2.2. *On dit que le semi-groupe Γ est fortement automatique pour la partie génératrice Σ si l'ensemble des relations*

$$L^{\text{rel}} := \{(u_1, v_1) \dots (u_n, v_n) \in (\Sigma \times (\Sigma \cup \{e\}))^* | u_1 \dots u_n = v_1 \dots v_n \text{ dans } \Gamma\}$$

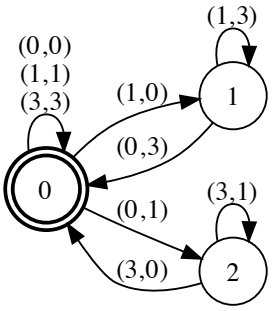
est un langage rationnel. On dira qu'un semi-groupe est fortement automatique s'il existe une partie génératrice pour laquelle il est fortement automatique.
On appelera automate des relations du semi-groupe Γ l'automate minimal reconnaissant le langage L^{rel}.

Exemple III.2.3. *Le monoïde engendré par les trois transformations*

$$\begin{cases} 0: & x & \mapsto & x/3, \\ 1: & x & \mapsto & x/3 & + & 1, \\ 3: & x & \mapsto & x/3 & + & 3. \end{cases}$$

est fortement automatique : voir figure III.12. Voir par exemple (Ken97) ou le théorème III.3.2 pour un preuve.

FIGURE III.12 – Automate des relations du monoïde de l'exemple III.2.3



Remarque III.2.4. *Cette définition est valable pour n'importe quel semi-groupe Γ de type fini, et pas seulement pour les semi-groupes qui se plongent dans un groupe.*

Obtention de la structure fortement automatique d'un monoïde

Dans ce paragraphe, nous allons voir comment obtenir la structure fortement automatique d'un sous-monoïde Γ d'un groupe.

Remarque III.2.5. *Un semi-groupe est fortement automatique si et seulement si le monoïde engendré (c'est-à-dire le semi-groupe auquel on ajoute l'élément neutre) l'est.*

Définition III.2.6. *On définit un automate $\mathcal{A} = (\Sigma_{\mathcal{A}}, Q, T, I, F)$ (éventuellement infini) de la façon suivante :*

1. $\Sigma_{\mathcal{A}} = \Sigma \times (\Sigma \cup \{e\})$,
2. $Q = \Gamma^{-1}\Gamma \subseteq G$,
3. $I = \{e\}$,
4. $F = \{e\}$,
5. *T est définit par : $(p, (g, h), q) \in T$ si et seulement si $q = g^{-1}ph$,*

où Γ est un sous-monoïde d'un groupe, d'élément neutre e, et engendré par une partie finie Σ (qui contient éventuellement l'élément e).

Proposition III.2.7. *L'émondé de l'automate $\mathcal{A}$ est l'automate minimal $\mathcal{A}^{\mathrm{rel}}$ des relations du monoïde Γ.*

On considèrera cet automate $\mathcal{A}^{\mathrm{rel}}$ dans la suite, même s'il est infini.

Remarque III.2.8. *On peut généraliser ce résultat aux monoïdes simplifiables.*

Démonstration. Montrons que l'automate $\mathcal{A}$ reconnait bien le langage L^{rel}.
Si $(a_1, b_1) \dots (a_n, b_n)$ est un mot reconnu par l'automate, alors par définition on a

$$a_n^{-1} \dots a_1^{-1} e b_1 \dots b_n = e$$

dans G. Donc on a bien $a_1 \dots a_n = b_1 \dots b_n$ dans Γ. Réciproquement, la relation $a_1 \dots a_n = b_1 \dots b_n$ dans Γ donne un chemin

$$e \xrightarrow{(a_1,b_1)} a_1^{-1} b_1 \to \dots \xrightarrow{(a_n,b_n)} a_n^{-1} \dots a_1^{-1} b_1 \dots b_n = e$$

dans l'automate $\mathcal{A}$.

Montrons maintenant que l'automate émondé est minimal. D'après la proposition III.1.13, il suffit de montrer qu'il est déterministe et de transposée déterministe. L'automate est clairement déterministe, et la transposée s'obtient en remplaçant l'ensemble des transitions par les $p \xrightarrow{(g,h)} q$ pour $q = gph^{-1}$, ce qui donne bien un automate déterministe. □

Propriétés III.2.9. *On a les propriétés :*

1. *Un groupe est fortement automatique si et seulement s'il est fini.*
2. *Un monoïde est libre (pour un système de générateurs donné) si et seulement si son automate des relations est trivial (c'est-à-dire réduit à un seul état).*
3. *Si un monoïde Γ est fortement automatique et simplifiable, et qu'il contient une relation entre deux éléments de longueurs distinctes, alors c'est un groupe fini.*
4. *Il y a unicité de la partie génératrice pour laquelle un semi-groupe ne contient pas de relation entre deux éléments de longueurs distinctes.*

De ces propriétés, on déduit qu'un semi-groupe possédant une partie génératrice pour laquelle il n'y a pas de relation entre deux éléments de longueurs distinctes est automatique si et seulement si il l'est pour cette partie génératrice.

Preuve des propriétés.

1. Si Γ est un groupe, alors l'automate $\mathcal{A}$ est déjà émondé et a pour ensemble de sommets Γ, d'où la propriété.
2. Si le semi-groupe Γ n'est pas libre pour la partie génératrice Σ, alors il existe une relation $a_1 \dots a_n = b_1 \dots b_n$ pour des éléments $a_i \in \Sigma$ et $b_i \in \Sigma \cup \{e\}$, avec $n \geq 1$ et $a_1 \neq b_1$. Le mot $(a_1, b_1) \dots (a_n, b_n)$ est reconnu par l'automate des relations, et donc il existe une arête de e à ${a_1}^{-1} b_1 \neq e$ dans l'automate des relations. Réciproquement,

si l'automate des relations n'est pas trivial, alors il existe un chemin de e vers un état $g \neq e$, et de g vers e puisque l'automate est émondé. Le chemin de e vers e obtenu en concaténant ces deux chemins fournit alors une relation non triviale dans le semi-groupe Γ (puisque les relations triviales de Γ correspondent à des chemins qui ne passent que par l'état e dans l'automate des relations).

3. Supposons qu'il existe une relation $u = v$ dans le semi-groupe fortement automatique Γ, pour deux mots u et $v \in \Sigma^*$, avec u de longueur strictement supérieure à v : $|u| > |v|$. Considérons alors le mot $w_n \in \Sigma \times (\Sigma \cup \{e\})$ correspondant au couple (u^n, v^n). Celui-ci termine par au moins n fois une lettre de la forme (a, e) pour des lettres $a \in \Sigma$. On a la relation $u^n = v^n$ dans le semi-groupe Σ, et donc le mot w_n est reconnu par l'automate $\mathcal{A}^{\text{rel}}$. En utilisant le lemme de l'étoile (voir III.1.21), avec u_2 de la forme $(a_1, e) \dots (a_k, e)$, on obtient, pour un entier k assez grand (et donc pour un entier n assez grand), une relation de la forme

$$u_1 u_2^k u_3 = v_1 e^{\alpha k + \beta} = v_1 \text{ dans } \Gamma, \text{ pour tout entier } k \in \mathbb{N},$$

avec $\alpha > 0$, et u_2 de longueur α. On a donc $u_1 u_2^k u_3 = u_1 u_2^{k+1} u_3$, d'où $u_2 = e$ dans le semi-groupe Γ, en simplifiant à droite et à gauche. De ceci, on déduit l'existence d'un générateur $a \in \Sigma$ qui est inversible à droite dans Γ (i.e. $a_d^{-1} \in \Gamma$). Posons $a' \in \Sigma^*$ tel que $a' = a_d^{-1}$ dans le semi-groupe Γ. En considérant maintenant la relation $a^n (a')^n b^n = b^n$ dans le semi-groupe Γ, pour un générateur $b \in \Sigma$ quelconque, le lemme de l'étoile nous donne, en prenant n assez grand, l'égalité $a^n (a')^n b^{n+kp} = b^n$ dans le semi-groupe Γ, pour un entier $p > 0$, et pour tout entier $k \in \mathbb{N}$. On obtient alors $b^{kp} = e$ en simplifiant, et donc le générateur b est inversible (à gauche et à droite). Tous les générateurs du semi-groupe étant ainsi inversibles, on en déduit que le semi-groupe Γ est un groupe. Par la première propriété, c'est un groupe fini.

4. Supposons que l'on ait deux partie génératrices Σ et Σ' du même semi-groupe Γ. Alors un générateur $a \in \Sigma$ s'écrit comme produit d'éléments de Σ' qui eux-même s'écrivent chacun comme produit d'éléments de Σ. Mais la longueur en la partie génératrice Σ du dernier produit obtenu doit être 1 puisque sinon on obtiendrait une relation entre des éléments de longueurs distinctes. On en déduit que l'on a $a \in \Sigma'$. Ainsi, on a l'inclusion $\Sigma \subseteq \Sigma'$, et par symétrie $\Sigma = \Sigma'$.

□

Exemple III.2.10. *Le sous-semi-groupe $\mathbb{Z}_{\geq 1}$ est fortement automatique, tandis que le sous-semi-groupe $\mathbb{Z}_{\geq 2}$ ne l'est pas.*

Exemple III.2.11. *Le sous-semi-groupe de $SL(2, \mathbb{Z})$ engendré par les trois matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$ est fortement automatique. Cela peut se démontrer en utilisant l'isomorphisme $PSL(2, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$, où $*$ dénote le produit libre des deux groupes cycliques. Les générateurs s'expriment sous la forme : abab, ababa et baba où $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 2 et $b = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 3 dans $PSL(2, \mathbb{Z})$.*

Voir la partie III.4 pour plus d'exemples.

Remarque III.2.12. *Déterminer si une partie finie d'un groupe engendre un semi-groupe libre (et donc déterminer si l'automate des relations correspondant est trivial) est décidable pour les sous-semi-groupes de type fini de $GL(2,\mathbb{Z})$ mais est indécidable pour les sous-semi-groupes de $SL(3,\mathbb{N})$ de type ≥ 13. C'est une question ouverte pour les sous-semi-groupes de type fini de $SL(2,\mathbb{Q})$. Voir (CN08) pour plus de détails. Ainsi, il ne peut pas exister d'algorithme pour déterminer la structure fortement automatique des sous-semi-groupes de type fini de $SL(3,\mathbb{N})$.*

Question . *Le problème de déterminer si un sous-semi-groupe de type fini de $PSL(2,\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ est fortement automatique est-il décidable ?*

(Ici, $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ est le produit libre des deux groupes $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$.)

III.2.2 Monoïde rationnel

Nous faisons ici le lien entre la notion de semi-groupe fortement automatique, et celle de monoïde rationnel. Dans son article (Sak87), Sakarovitch introduit la notion de monoïde rationnel, que l'on peut définir de la façon suivante (voir (Ber79) pour d'autres caractérisations) :

Définition III.2.13. *On dit qu'un monoïde M est rationnel s'il existe un ensemble fini Σ de générateurs, une partie $L^{\text{red}} \subseteq \Sigma^*$ et un langage rationnel $L^{\text{rat}} \subseteq (\Sigma \times \{0,1\})^*$ tels que*

- *L^{red} est un système de mots réduits. C'est-à-dire que pour tout élément γ de M, il existe un unique mot en les générateurs Σ qui est dans L^{red} et qui est égal à γ dans le monoïde M.*
- *Pour tout mot $u \in \Sigma^*$, il existe un mot $w \in L^{\text{rat}}$ tel que $p_0(w) = u$.*
- *Pour tout mot $w \in L^{\text{rat}}$, $p_1(w)$ est un mot réduit équivalent à $p_0(w)$ (c'est-à-dire que les deux mots sont égaux dans le monoïde M).*

où $p_0 : (\Sigma \times \{0,1\})^* \to \Sigma^*$ et $p_1 : (\Sigma \times \{0,1\})^* \to \Sigma^*$ sont les morphismes naturels tels que $p_i(\Sigma \times \{j\}) = \begin{cases} \{\epsilon\} & \text{si } i \neq j, \\ \Sigma \times \{j\} & \text{si } i = j. \end{cases}$

Reprenons l'exemple de l'introduction :

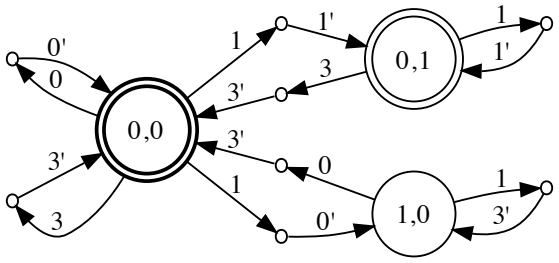
Exemple III.2.14. *Le monoïde engendré par les trois applications*

$$\begin{cases} 0 : & x & \mapsto & x/3, \\ 1 : & x & \mapsto & x/3 & + & 1, \\ 3 : & x & \mapsto & x/3 & + & 3. \end{cases}$$

est rationnel, pour l'alphabet $\Sigma = \{0,1,3\}$, l'ensemble de mots réduits

$$L^{\text{red}} = \{\text{mots de } \Sigma^* \text{ ne contenant pas le mot } 10 \text{ comme sous-mot }\} = (0|3|11^*3)^*,$$

et le langage $L^{\text{rat}} \subseteq (\Sigma \times \{0,1\})^*$ *reconnu par l'automate* $\mathcal{A}_{L^{\text{rat}}}$ *suivant :*



où l'on a remplacé l'alphabet $\Sigma \times \{0\}$ *par* $\{0,1,3\}$ *et l'alphabet* $\Sigma \times \{1\}$ *par* $\{0',1',3'\}$ *pour alléger les notations.*

La notion de monoïde rationnel est assez proche de celle de monoïde fortement automatique comme le montre les résultats suivants :

Proposition III.2.15. *Si un monoïde* M *est fortement automatique, alors il est rationnel.*

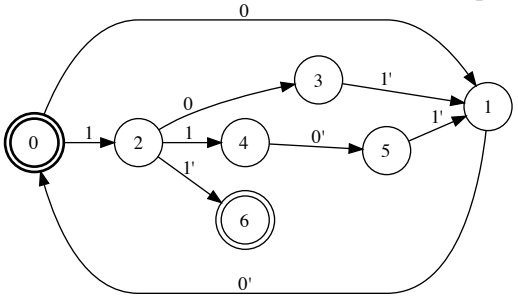
Voici une réciproque :

Proposition III.2.16. *Soit* M *un monoïde engendré par une partie finie* Σ *telle qu'il n'y ait pas d'égalité dans le monoïde entre deux mots en* Σ *de mêmes longueurs. Alors le monoïde* M *est rationnel si et seulement si il est fortement automatique.*

Et voici un exemple qui montre que les deux notions diffèrent :

Exemple III.2.17. *Le monoïde de présentation* $< 0,1|010 = 11 >$ *est rationnel (voir figure III.13) mais n'est pas fortement automatique (par III.2.9, puisqu'il est simplifiable et infini).*

FIGURE III.13 – Automate $\mathcal{A}_{L^{\text{rat}}}$ de l'exemple III.2.17



Preuve de la proposition III.2.15. Soit le langage rationnel

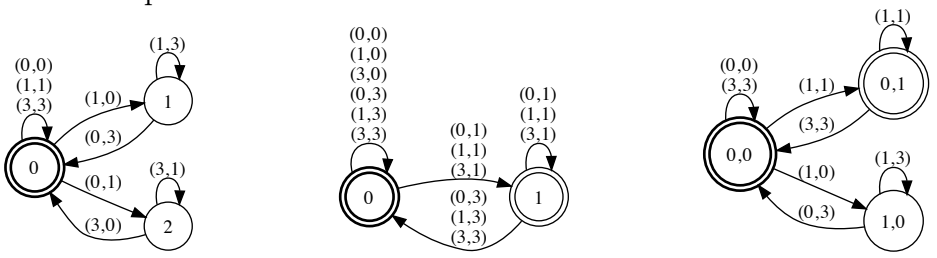
$$L := L^{\text{rel}} \cap \left(\Sigma^* \times L^{\text{red}} e^* \cup \Sigma^* e^* \times L^{\text{red}}\right),$$

où L^{red} est le langage rationnel des mots réduits correspondant aux mots minimaux dans l'ordre lexicographique. Soit $\mathcal{A}$ un automate déterministe et émondé reconnaissant le langage L. On modifie l'automate en remplaçant chaque transition

– $p \xrightarrow{(a,e)} q$ par $p \xrightarrow{(a,0)} q$,
– $p \xrightarrow{(e,a)} q$ par $p \xrightarrow{(a,1)} q$,
– $p \xrightarrow{(a,b)} q$ par $p \xrightarrow{(a,0)} p' \xrightarrow{(b,1)} q$, où p' est un nouvel état,

pour toutes lettres a et b dans Σ. On vérifie alors que le monoïde est rationnel avec l'ensemble de générateur Σ, les mots réduits L^{red} et le langage L^{rat} reconnu par l'automate que l'on vient de construire. □

FIGURE III.14 – Construction d'un automate reconnaissant le langage L de la preuve ci-dessus pour l'exemple III.2.14



Automate des relations | Automate reconnaissant le langage $\Sigma^* \times L^{\text{red}}$ | Automate reconnaissant l'intersection L

Preuve de la proposition III.2.16. Montrons qu'un monoïde rationnel qui satisfait l'hypothèse est fortement automatique. Soit L^{rat} le langage de la définition III.2.13, et soit $\mathcal{A}_{L^{\text{rat}}}$ un automate déterministe et émondé qui reconnait le langage L^{rat}.

Lemme III.2.18. *Les cycles de l'automate $\mathcal{A}_{L^{\text{rat}}}$ sont étiquetés par des mots contenant chacun autant de lettre de l'alphabet $\Sigma \times \{0\}$ que de l'alphabet $\Sigma \times \{1\}$.*

Démonstration. Supposons qu'il existe un cycle dans l'automate $\mathcal{A}_{L^{\text{rat}}}$ étiqueté par un mot $u \in (\Sigma \times \{0\} \sqcup \Sigma \times \{1\})^*$, avec par exemple $|p_0(u)| < |p_1(u)|$. L'automate $\mathcal{A}_{L^{\text{rat}}}$ étant émondé, il existe un mot $w \in L^{\text{rat}}$ qui parcours ce cycle. Plus précisément, on peut écrire $w = xuy$, tel qu'il existe des états p, q et r tels que $p \xrightarrow{x} q \xrightarrow{u} q \xrightarrow{y} r$ et avec $p \in I$ et $r \in F$. Le mot xy est alors aussi reconnu par l'automate, et on a

$$|p_0(xuy)| - |p_1(xuy)| = |p_0(xy)| - |p_1(xy)| + |p_0(u)| - |p_1(u)| < |p_0(xy)| - |p_1(xy)|\,.$$

Cela est impossible, puisque l'hypothèse que le monoïde ne contient que des relations entre des mots de même longueur entraîne que pour tout mot v reconnu par l'automate $\mathcal{A}_{L^{\text{rat}}}$, on a $|p_0(v)| - |p_1(v)| = 0$. On a donc bien montré le résultat par l'absurde. □

Il existe donc une borne M sur les différences $||p_0(u)| - |p_1(u)||$ sur tous les mots u qui sont préfixes d'un mot du langage L^{rat}.

Construisons alors un automate $\mathcal{A} = (\Sigma_{\mathcal{A}}, Q, T, I, F)$ en posant :
– $\Sigma_{\mathcal{A}} := (\Sigma \cup \{e\})^2$,
– $Q := Q_{\mathcal{A}_L} \quad \sqcup \quad Q_{\mathcal{A}_L} \times \bigcup_{i=1}^{M} \Sigma^i \times \{0\} \quad \sqcup \quad Q_{\mathcal{A}_L} \times \bigcup_{i=1}^{M} \Sigma^i \times \{1\}$,

- $I := I_{\mathcal{A}_L}$,
- $F := F_{\mathcal{A}_L}$,
- T est le plus petit ensemble tel que
  - Si $p \xrightarrow{(a,0)} q$ dans $\mathcal{A}_{L^{\mathrm{rat}}}$, alors pour tout $u \in \bigcup_{i=0}^{M-1} \Sigma^i$,
    - $(p, u, 0) \xrightarrow{\epsilon} (q, ua, 0)$ dans $\mathcal{A}$,
    - $(p, ub, 1) \xrightarrow{(a,b)} (q, u, 1)$ dans $\mathcal{A}$,

    avec la convention que $(p, \epsilon, 0) = p$ et $(q, \epsilon, 1) = q$.
  - Si $p \xrightarrow{(a,1)} q$ dans $\mathcal{A}_{L^{\mathrm{rat}}}$, alors pour tout $u \in \bigcup_{i=0}^{M-1} \Sigma^i$,
    - $(p, u, 1) \xrightarrow{\epsilon} (q, ua, 1)$ dans $\mathcal{A}$,
    - $(p, ub, 0) \xrightarrow{(b,a)} (q, u, 0)$ dans $\mathcal{A}$,

    avec la convention que $(p, \epsilon, 1) = p$ et $(q, \epsilon, 0) = q$.

Les "transitions" étiquetées par ϵ s'appellent des ϵ-transitions. On peut démontrer qu'un automate avec ϵ-transition est équivalent à un automate déterministe sans ϵ-transition (voir (Car08) pour plus de détails). Ainsi, le langage L de l'automate $\mathcal{A}$ est rationnel.

L'automate $\mathcal{A}$ ci-dessus consiste à "synchroniser" l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$, en stoquant en mémoire (grâce à de nouveaux états) le nombre fini de lettres qui font qu'un des deux mots, l'un sur l'alphabet $\Sigma \times \{0\}$ et l'autre sur l'alphabet $\Sigma \times \{1\}$, est plus long que l'autre. À un chemin dans $\mathcal{A}_{L^{\mathrm{rat}}}$, on fait donc correspondre un chemin dans l'automate $\mathcal{A}$ étiqueté par les mêmes lettres regroupées par couples (avec à gauche les lettres de l'alphabet $\Sigma \times \{0\}$ et à droite celles de $\Sigma \times \{1\}$), et avec les lettres qui restent qui sont "mémorisée" par l'état dans lequel on aboutit.

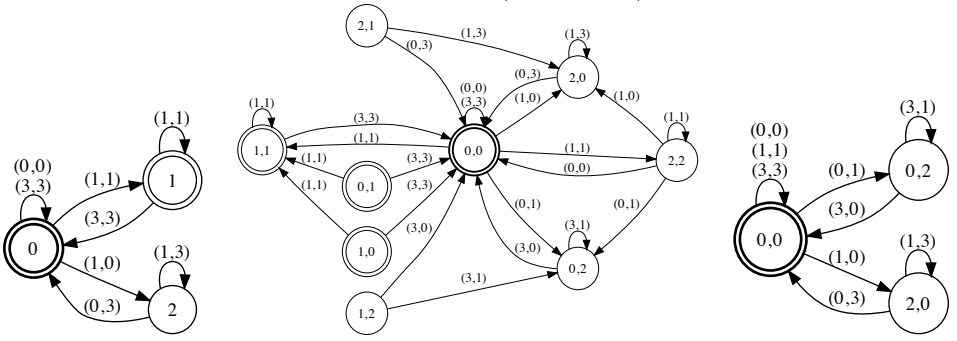
Lemme III.2.19. *On a $L = L^{\mathrm{rel}} \cap \left(\Sigma^* \times L^{\mathrm{red}}\right)$, où L est le langage de l'automate $\mathcal{A}$ défini ci-dessus.*

Démonstration. Il y a correspondance entre un chemin dans l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$ et dans l'automate $\mathcal{A}$, par la construction ci-dessus. On vérifie que l'on a un chemin $p \xrightarrow{u} q$ dans l'automate $\mathcal{A}_{L^{\mathrm{rat}}}$, si et seulement si le chemin correspondant $p \xrightarrow{(x,y)} (q, z, \alpha)$ dans l'automate $\mathcal{A}$ est tel que $p_0(u) = \begin{cases} xz & \text{si } \alpha = 0 \\ x & \text{si } \alpha = 1 \end{cases}$ et $p_1(u) = \begin{cases} y & \text{si } \alpha = 0 \\ yz & \text{si } \alpha = 1 \end{cases}$. Ainsi, un mot $(x, y) = (x_1, y_1) \dots (x_n, y_n)$ est reconnu par l'automate $\mathcal{A}$ si et seulement si il lui correspond un mot $u \in L^{\mathrm{rat}}$ tel que $x = p_0(u)$ et $y = p_1(u)$.

□

La preuve de la proposition III.2.16 est alors une conséquence du lemme suivant. □

FIGURE III.15 – Construction d'un automate reconnaissant le langage L^{rel} à partir d'un automate reconnaissant le langage $L = L^{\text{rel}} \cap \left(\Sigma^* \times L^{\text{red}}\right)$ pour l'exemple III.2.14



Automate $\mathcal{A}$ | Automate $\mathcal{A}^{\text{rel}}$ construit ci-dessus | Automate $\mathcal{A}^{\text{rel}}$ minimisé

Lemme III.2.20. *Si le langage $L = L^{\text{rel}} \cap \left(\Sigma^* \times L^{\text{red}}\right)$ est rationnel, alors le langage L^{rel} l'est aussi.*

Démonstration. Soit $\mathbb{L} := L \times L \subseteq (\Sigma^2 \times \Sigma^2)^*$ et $\mathbb{L}' := \mathbb{L} \cap \{(a,c,b,c) | a,b,c \in \Sigma\}$. Montrons que l'on a alors $L^{\text{rel}} = p_{13}(\mathbb{L}')$ où p_{13} est la projection sur les 1ère et 3e coordonnées.

Par définition, on a

$$(a,b) \in p_{13}(\mathbb{L}') \quad \Longleftrightarrow \quad \exists c \in L^{\text{red}}, (a,c) \in L^{\text{rel}} \text{ et } (b,c) \in L^{\text{rel}}.$$

On a l'implication $(a,c) \in L^{\text{rel}}$ et $(b,c) \in L^{\text{rel}} \Rightarrow (a,b) \in L^{\text{rel}}$ par définition de L^{rel}, et l'autre implication $(a,b) \in L^{\text{rel}} \Rightarrow \exists c \in L^{\text{red}}, (a,c) \in L^{\text{rel}}$ et $(b,c) \in L^{\text{rel}}$ découle de la définition de L^{red}.

□

III.2.3 Semi-groupe automatique

La structure fortement automatique est utile pour déterminer facilement si deux mots représentent le même élément du semi-groupe, et nous allons voir qu'elle permet également d'obtenir d'autres informations sur le semi-groupe puisqu'elle impliquera la structure automatique usuelle :

Définition III.2.21. *On dit que le semi-groupe Γ est automatique s'il existe une partie génératrice Σ, un automate $\mathcal{A}^{\text{red}}$ appelé automate des mots réduits et une famille d'automates $(\mathcal{A}^g)_{g \in \Sigma}$ appelés automates de multiplication vérifiants les propriétés :*

1. *$\mathcal{A}^{\text{red}}$ a pour alphabet Σ,*
2. *Le langage $L_{\mathcal{A}^{\text{red}}}$ est un ensemble de mots réduits. C'est-à-dire que l'on a :*

   pour tout $\gamma \in \Gamma$, il existe un unique $u \in L_{\mathcal{A}^{\text{red}}}$ tel que $\gamma = u$ dans Γ.

   Autrement dit, l'application de Σ^* dans Γ induit une bijection de $L_{\mathcal{A}^{\text{red}}}$ dans Γ : on peut identifier un mot réduit à un élément de Γ.

3. *Pour tout $g \in \Sigma$, $\mathcal{A}^g$ a pour alphabet $(\Sigma \cup \{e\}) \times (\Sigma \cup \{e\})$,*
4. *Pour tout $g \in \Sigma$, l'automate $\mathcal{A}^g$ reconnait si un mot réduit de Γ s'obtient à partir d'un autre par multiplication à droite par g. Plus précisément, le langage $L_{\mathcal{A}^g}$ est l'ensemble des mots $(u_1, v_1) \dots (u_n, v_n)$ vérifiant :*

$$(u_1, v_1) \dots (u_n, v_n) \in (L_{\mathcal{A}^{\text{red}}} g \times L_{\mathcal{A}^{\text{red}}} e^*) \cup (L_{\mathcal{A}^{\text{red}}} g e^* \times L_{\mathcal{A}^{\text{red}}}), \tag{III.1}$$

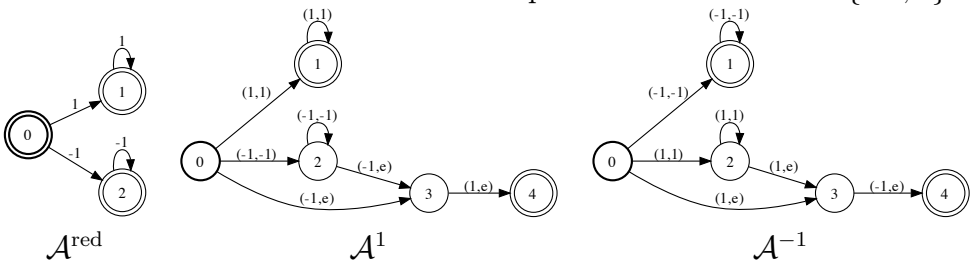
$$u_1 \dots u_n = v_1 \dots v_n \text{ dans } \Gamma. \tag{III.2}$$

Remarque III.2.22. *Il existe des variantes de la notion de structure automatique, qui autorise par exemple une notion de mots réduits un peu plus souple, ou encore qui reconnait si un mot réduit de Γ s'obtient à partir d'un autre par multiplication à droite par g d'une façon différente. Voir (Cai05) pour plus de détails.*

Exemple III.2.23. *Les semi-groupes suivants sont automatiques :*
- *$\mathbb{Z}$: voir figure III.16.*
- *Le semi-groupe donné en introduction : voir figures III.17, III.18, III.19 et III.20.*
- *Les groupes hyperboliques.*

Il y a de nombreux autres exemples de groupes automatiques. Voir par exemple (EC+92).

FIGURE III.16 – Structure automatique de $\Gamma = \mathbb{Z}$ avec $\Sigma = \{-1, 1\}$



La structure automatique d'un semi-groupe permet de manipuler celui-ci grâce à un système de mots réduits. Cela permet par exemple d'effectuer des calculs dans le semi-groupe sur ordinateur. Mais voici aussi un résultat donnant des informations sur le semi-groupe à partir de la structure automatique :

Proposition III.2.24. *Si Γ est automatique, alors le nombre c_n d'éléments de Γ de longueur n vérifie*

$$c_n = P(n)\alpha^n(1 + O_{n\to\infty}(e^{-\epsilon n}))$$

où P est un polynôme, $\epsilon > 0$ est un réel, et $1 \leq \alpha \leq \#\Sigma$ est un réel.

Plus précisément, c_n s'obtient comme la somme de coefficients de la puissance $n^{ième}$ de la matrice d'adjacence du graphe de l'automate $\mathcal{A}^{\text{red}}$.

Démonstration. Le nombre c_n cherché est le nombre de chemins de longueur n de l'automate $\mathcal{A}^{\text{red}}$, partant de l'état initial et aboutissant à un état final. Ceci est donné par les puissances de la matrice d'adjacence du graphe. Si l'automate est supposé émondé,

le théorème de Perron-Frobenius nous donne l'existence d'une plus grande valeur propre $\alpha > 0$, pour laquelle on a l'asymptotique annoncée. □

Exemple III.2.25. *Pour $\Gamma = \mathbb{Z}$ et $\Sigma = \{-1, 1\}$ (voir figure III.16), la matrice d'adjacence du graphe de l'automate $\mathcal{A}^{\mathrm{red}}$ est*

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

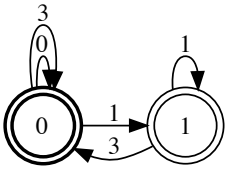
qui est idempotente. Le nombre c_n d'éléments de Γ de longueur n est donc $c_0 = 1$ pour $n = 0$ et $c_n = 2$ pour $n > 0$ (il s'agit en effet des éléments n et $-n$).

Les 4 figures qui suivent donnent une structure automatique complète de l'exemple de l'introduction :

FIGURE III.17 –
Automate $\mathcal{A}^{\mathrm{red}}$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : & x & \mapsto & x/3, \\ 1 : & x & \mapsto & x/3 & + & 1, \\ 3 : & x & \mapsto & x/3 & + & 3, \end{cases}$$

pour l'ordre lexicographique (avec $0 < 1 < 3$).



On voit que les mots réduits sont ici les mots ne contenant pas le sous-mot 10.

FIGURE III.18 –
Automate $\mathcal{A}^0$ du monoïde engendré par les trois applications

$$\begin{cases} 0 : & x & \mapsto & x/3, \\ 1 : & x & \mapsto & x/3 & + & 1, \\ 3 : & x & \mapsto & x/3 & + & 3. \end{cases}$$

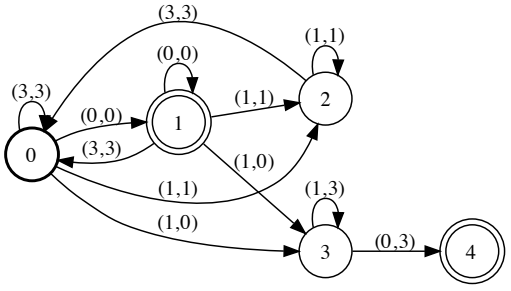


FIGURE III.19 –
Automate $\mathcal{A}^1$ du monoïde engendré par les trois applications

$$\begin{cases} 0: & x & \mapsto & x/3, \\ 1: & x & \mapsto & x/3 & + & 1, \\ 3: & x & \mapsto & x/3 & + & 3. \end{cases}$$

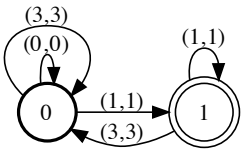
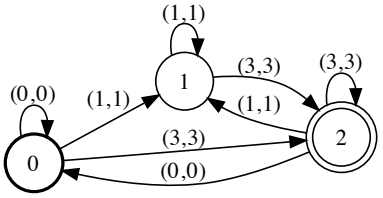


FIGURE III.20 –
Automate $\mathcal{A}^3$ du monoïde engendré par les trois applications

$$\begin{cases} 0: & x & \mapsto & x/3, \\ 1: & x & \mapsto & x/3 & + & 1, \\ 3: & x & \mapsto & x/3 & + & 3. \end{cases}$$



On voit sur la figure III.19 que le langage de $\mathcal{A}_1$ est formé des couples $(u1, u1)$ pour les mots u réduits. Sur la figure III.20, on voit de même que le langage de $\mathcal{A}_3$ est formé des couples $(u3, u3)$ pour les mots u réduits. L'automate de la figure III.18 est plus compliqué puisque le mot $u0$ n'est pas réduit quand le mot réduit u termine par un 1 : son langage est l'ensemble des couples $(u1^n0, u03^n)$ pour les mots réduits u et les entiers $n \in \mathbb{N}$.

III.2.4 Fortement automatique implique automatique

Voici un lien entre la structure fortement automatique et automatique :

Proposition III.2.26. *Si le monoïde* Γ *est fortement automatique, alors il est automatique.*

Démonstration. Supposons que le semi-groupe Γ soit fortement automatique : il existe donc un automate des relations $\mathcal{A}^{\text{rel}}$, qui reconnait un langage rationnel L^{rel}. Par le point 1 des propriétés III.2.9, le semi-groupe contient une relation entre des éléments de longueurs distinctes si et seulement si c'est un groupe fini. Mais il est facile de voir qu'un groupe fini est automatique. Ainsi, on supposera dans la suite de la preuve que les relations sont toujours entre des éléments de même longueur. On a donc l'inclusion de l'ensemble des relations L^{rel} dans $(\Sigma \times \Sigma)^*$.

i) Construction de l'automate des mots réduits

Considérons alors le langage rationnel

$$L := L^{\text{lex}} \cap L^{\text{rel}},$$

où L^{lex} est le langage de l'automate de la figure III.9, en ayant muni l'alphabet Σ d'un ordre total. Posons alors

$$L^{\text{nonred}} := p_2(L),$$

le projecté du langage L suivant la deuxième coordonnée. Par la proposition III.1.20, c'est un langage rationnel. Alors L^{nonred} est l'ensemble des mots de Σ^* qui sont non réduits pour l'ordre lexicographique. En effet, le langage L est l'ensemble des couples de mots équivalents (u, v) de Σ^* tels que u est strictement inférieur à v pour l'ordre lexicographique. Ainsi, un mot v est dans le langage L^{nonred} si et seulement s'il existe un mot u équivalent et strictement inférieur dans l'ordre lexicographique. En posant

$$L^{\text{red}} := \Sigma \backslash L^{\text{nonred}},$$

le langage L^{red} est donc un ensemble de mots réduits, et il est rationnel.

Ainsi, on a bien démontré l'existence de l'automate des mots réduits $\mathcal{A}^{\text{red}}$.

ii) Construction des automates de multiplication

Le paragraphe précédent a montré que le langage L^{red} des mots réduits est rationnel. Pour $g \in \Sigma$, considérons alors le langage rationnel

$$L^g := (L^{\text{red}} g \times L^{\text{red}}) \cap L^{\text{rel}}.$$

C'est bien un langage rationnel par la proposition III.1.18. Pour obtenir un automate de multiplication $\mathcal{A}^g$, il suffit de considérer un automate $\mathcal{A}^g$ reconnaissant le langage L^g.

Ceci termine la preuve de la proposition III.2.26. □

III.2.5 Recherche du mot réduit

Comment trouver le mot réduit correspondant à un mot donné ? La structure automatique permet de faire cela :

Proposition III.2.27. *Si le semi-groupe est automatique, alors il existe un algorithme quadratique qui prend en entrée un mot et rend le mot réduit correspondant.*

Démonstration. Voir (EC+92). □

Ceci permet en particulier de résoudre le problème des mots (i.e. déterminer si deux mots donnés sont équivalents) en temps quadratique :

Corollaire III.2.28. *Si le semi-groupe est automatique, il existe un algorithme prenant en entrée deux mots et répondant en temps quadratique si les deux mots sont équivalents ou non.*

Lorsque le semi-groupe est fortement automatique, le problème des mots se résoud en temps linéaire et avec une mémoire constante puisqu'il est résolu par un automate. Mais on peut aussi trouver le mot réduit correspondant à un mot donné rapidement :

Proposition III.2.29. *Si le semi-groupe est fortement automatique, alors il existe un algorithme linéaire prenant en entrée un mot et rendant le mot réduit correspondant.*

Démonstration. Définissons le langage

$$L := \{(a_1, b_1) \dots (a_n, b_n) \in L^{\text{rel}} | b_1 \dots b_n \in L^{\text{red}} e^*\} = (\Sigma^* \times L^{\text{red}} e^*) \cap L^{\text{rel}}.$$

Alors le langage L est rationnel.

Soit $\mathcal{A} = (\Sigma \times (\Sigma \cup \{e\}), Q, T, I, F)$ un automate déterministe reconnaissant le langage L. Définissons alors l'automate $\mathcal{A}' = (\Sigma, Q', T', I', F')$ par :

- $Q' := \mathcal{P}(Q)$ (l'ensemble des parties de Q),
- $I' := \{I\}$,
- $F' := \{P \in \mathcal{P}(Q) | P \cap F \neq \emptyset\}$,
- T' est défini par

$$(A, a, B) \in T' \text{ si et seulement si}$$

$$B = \{q \in Q | \text{Il existe } b \in (\Sigma \cup \{e\}) \text{ et } p \in A \text{ tels que } (p, (a, b), q) \in T\}.$$

L'automate $\mathcal{A}'$ est clairement déterministe, et il reconnait le langage Σ^*, puisque pour tout mot $u \in \Sigma^*$, il existe un mot réduit $v \in \Sigma^*$ tel que l'on ait la relation $u = v$ dans le semi-groupe Γ, ce qui donne un mot (u, ve^k) reconnu par l'automate $\mathcal{A}$ (en supposant que les mots réduits sont de longueur minimale).

Voici maintenant un algorithme permettant de trouver le mot réduit correspondant à un mot $u \in \Sigma^*$. Considérons le chemin

$$A_0 \xrightarrow{u_1} A_1 \to \dots \xrightarrow{u_n} A_n$$

dans l'automate $\mathcal{A}'$ étiqueté par le mot $u = u_1 \dots u_n$. Choisissons alors un état final $q_n \in A_n$ de l'automate $\mathcal{A}$. Par définition, il existe alors une lettre $v_n \in (\Sigma \cup \{e\})$ et un état $q_{n-1} \in A_{n-1}$ tels que l'on ait la transition $q_{n-1} \xrightarrow{(u_n, v_n)} q_n$ dans l'automate $\mathcal{A}$. Et on peut trouver la lettre v_n et l'état q_{n-1} en temps constant. On peut alors continuer : on trouve une lettre $v_{n-1} \in (\Sigma \cup \{e\})$ et un état $q_{n-2} \in A_{n-2}$ tels que l'on ait la transition $q_{n-2} \xrightarrow{(u_{n-1}, v_{n-1})} q_{n-1}$ dans l'automate $\mathcal{A}$, et ainsi de suite. On obtient finalement un chemin $q_0 \xrightarrow{(u_0, v_0)} q_1 \to \dots \xrightarrow{(u_n, v_n)} q_n$ dans l'automate $\mathcal{A}$. L'état q_0 est un état initial de l'automate $\mathcal{A}$ puisque l'on a $q_0 \in A_0 \in I' = \{I\}$. On obtient donc un mot $v_1 \dots v_n \in (\Sigma \cup \{e\})^*$ tel que le mot $(u_1, v_1) \dots (u_n, v_n)$ est dans le langage L. Le mot $v = v_1 \dots v_n$ est donc dans le langage $L_{\mathcal{A}}^{\text{red}} e^*$, et on a la relation $u_1 \dots u_n = v_1 \dots v_n$ dans le semi-groupe Γ. Ainsi, on

obtient le mot réduit correspondant au mot u en éliminant les lettres e à la fin du mot v. Et tout ce calcul s'effectue en temps linéaire. □

III.3 Semi-groupes correspondant aux développements β-adique

Soit k un corps. Dans cette partie, on s'intéresse au semi-groupe Γ engendré par les transformations affines

$$x \mapsto \beta x + t$$

pout $t \in A \subset k$, où A est une partie finie de k, et β est un élément de k.

Remarque III.3.1. *Si le corps k est de caractéristique 0, alors on peut supposer que l'on a $k = \mathbb{C}$.*

Ce semi-groupe correspond au développement en base β, en utilisant l'ensemble de chiffres A. Par exemple, l'exemple donné en introduction correspond au développement en base 3 en utilisant l'ensemble de chiffres $\{0, 1, 3\}$.

Nous donnons un critère de forte automaticité pour ces semi-groupes.

III.3.1 Forte automaticité

Cette sous-section est consacrée à la preuve du théorème suivant qui donne la forte automaticité de la plupart des semi-groupes de développement en base β.

Théorème III.3.2. *Le semi-groupe Γ est fortement automatique, sauf éventuellement dans le cas où le corps k est de caractéristique nulle, et que le nombre complexe β est algébrique, avec un conjugué de module 1.*

Preuve du théorème III.3.2. Commençons par le cas où β est une racine de l'unité. Par hypothèse, le corps k est alors de caractéristique finie. Dans ce cas, le semi-groupe Γ est un groupe fini (et est donc fortement automatique par le point 1 des propriétés III.2.9). En effet, tous les générateurs sont d'ordre fini donc c'est un groupe, et il est fini puisque toutes les applications de Γ sont de la forme $x \mapsto \beta^k x + t$ avec $1 \leq k \leq n$ où n est l'ordre de β et t dans le sous-$\mathbb{F}_p$-espace vectoriel de dimension finie de k engendré par $\cup_{k=1}^{n} \beta^k A$.

Supposons maintenant que β ne soit pas une racine de l'unité. Par les propriétés III.2.9, le semi-groupe est automatique si et seulement si il l'est pour la partie génératrice considérée ici, puisque les relations du semi-groupe Γ sont entre des éléments de même longueur. C'est-à-dire que si l'on a une égalité $a_1 \dots a_n = b_1 \dots b_n$ dans Γ pour deux mots $a_1 \dots a_n \in \Sigma^*$ et $b_1 \dots b_n \in (\Sigma \cup \{e\})^*$, alors on a $b_1 \dots b_n \in \Sigma^*$. Ainsi, on peut considérer l'automate des relations $\mathcal{A}^{\text{rel}}$ (à priori infini) sur l'alphabet $\Sigma \times \Sigma$ donné par la proposition III.2.7, et on va montrer qu'il est fini (i.e. qu'il a un nombre fini d'états). On peut aussi supposer que le semi-groupe Γ est un monoïde quitte à lui ajouter un élément neutre (ce qui ne change pas le fait qu'il soit fortement automatique).

Comme il n'y a pas d'égalité dans le semi-groupe entre deux mots de longueur différentes, on est ramené à ce que les états de l'automates soient tous de la forme $x \mapsto x + t$ pour $t \in k$. Ainsi, quitte à remplacer Γ par son inverse (ce qui ne change pas le fait qu'il soit fortement automatique), l'automate $\mathcal{A}^{\text{rel}}$ est donc l'émondé de l'automate $\mathcal{A} = (\Sigma_{\mathcal{A}}, Q_{\mathcal{A}}, T_{\mathcal{A}}, I_{\mathcal{A}}, F_{\mathcal{A}})$ définit par :

1. $\Sigma_{\mathcal{A}} = \Sigma \times \Sigma$,
2. $Q_{\mathcal{A}} = k$,
3. $I_{\mathcal{A}} = \{0\}$,
4. $F_{\mathcal{A}} = \{0\}$,
5. $T_{\mathcal{A}} \subseteq Q_{\mathcal{A}} \times \Sigma_{\mathcal{A}} \times Q_{\mathcal{A}}$ est définit par :

$$(p, (g, h), q) \in T_{\mathcal{A}} \text{ si et seulement si } q = \beta p + g - h.$$

Remarque III.3.3. *J'aurait pu considérer l'automate $\mathcal{A}$ qui correspond directement à celui du semi-groupe Γ et non pas à son inverse. Cela aurait donné les transitions $(p, (g, h), q) \in T_{\mathcal{A}} \Leftrightarrow q = (p - g + h)/\beta$. Mais la formule donnant les transitions de l'automate $\mathcal{A}$ pour le semi-groupe inverse me semblait plus agréable.*

Le lemme suivant fournit une critère algébrique d'appartenance à l'ensemble des sommets de l'automate des relations $\mathcal{A}^{\text{rel}}$:

Lemme III.3.4. *Un élément $x \in k$ est un état de l'automate des relations $\mathcal{A}^{\text{rel}}$ (c'est-à-dire de l'émondé de l'automate $\mathcal{A}$) si et seulement si il existe deux polynômes $P, Q \in (A - A)[X]$ à coefficients dans $A - A$ tels que l'on ait $x = P(\beta) = \beta^{-1}Q(\beta^{-1})$.*

Preuve du lemme. Un élément $x \in k$ est un état de l'automate des relations $\mathcal{A}^{\text{rel}}$ si et seulement si il existe un chemin

$$0 \xrightarrow{(a_1,b_1)} \dots \xrightarrow{(a_n,b_n)} x \xrightarrow{(a'_k,b'_k)} \dots \xrightarrow{(a'_0,b'_0)} 0$$

dans l'automate $\mathcal{A}$, avec a_i, b_i, a'_i et $b'_i \in A$. On a alors $x = \sum_{i=0}^{n-1}(a_{n-i} - b_{n-i})\beta^i$ et $\beta^k x + \sum_{i=0}^{k-1}(a'_i - b'_i)\beta^i = 0$, d'où $x = P(\beta) = \beta^{-1}Q(\beta^{-1})$, avec

$$P(X) = \sum_{i=0}^{n-1}(a_{n-i} - b_{n-i})X^i \quad \text{et} \quad X^{-1}Q(X^{-1}) = \sum_{i=0}^{k-1}(a'_i - b'_i)X^{i-k}.$$

Et réciproquement, deux tels polynômes nous donnent un chemin de 0 à 0 passant par x. □

Notons $\mathbb{F}_p := \text{Frac}(\mathbb{Z}/p\mathbb{Z})$ le corps de fractions de $\mathbb{Z}/p\mathbb{Z}$ où p est la caractéristique du corps k. On a ainsi $\mathbb{F}_0 = \mathbb{Q}$ si le corps k est de caractéristique nulle, et sinon $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est le corps fini à p éléments.

Considérons D le $\mathbb{F}_p(\beta)$-espace vectoriel engendré par la partie A, et soit C une base de cet espace vectoriel. Considérons la base duale $(c^*)_{c\in C}$ de C. Les formes linéaires $c^* : D \to \mathbb{F}_p(\beta)$ vérifient donc

$$\sum_{c\in C} c^* \cdot c = \mathrm{id}_D\,.$$

Pour chaque $c \in C$, considérons alors le semi-groupe Γ_c engendré par les transformations

$$x \mapsto \beta x + t, \text{ pour } t \in c^*(A).$$

On a alors le lemme :

Lemme III.3.5. *Le semi-groupe Γ est fortement automatique si et seulement si les semi-groupes Γ_c, $c \in C$, sont tous fortement automatiques.*

Démonstration. On peut voir le semi-groupe Γ comme le produit

$$\Gamma = \prod_{c\in C} \Gamma_c,$$

et chaque semi-groupe Γ_c est fortement automatique si et seulement s' il l'est pour la partie génératrice naturelle, de même que pour Γ, d'après les propriétés III.2.9. On conclut donc avec le lemme qui suit.

□

Lemme III.3.6. *Soit Σ une partie d'un produit de semi-groupes $\Gamma_1 \times \Gamma_2$, et soient Σ_1 et Σ_2 les projetés de Σ sur chacun des semi-groupes du produit. Alors la partie Σ enegendre un semi-groupe fortement automatique (relativement à la partie Σ) si et seulement si chacune des parties Σ_i engendre un semi-groupe fortement automatique (relativement à Σ_i), pour $i = 1$ et 2.*

Démonstration. On a $L^{\mathrm{rel}}_{<\Sigma>^+} = \prod_{i=1}^2 L^{\mathrm{rel}}_{<\Sigma_i>^+}$. □

Grâce au lemme III.3.5, on se ramène à ce que l'on ait $A \subseteq \mathbb{F}_p(\beta)$. Quitte à multiplier la partie A par un élément du corps k (ce qui ne change pas le semi-groupe), on peut supposer que l'on a même $A \subseteq (\mathbb{Z}/p\mathbb{Z})[\beta]$. Ainsi, on peut supposer que l'ensemble des états de l'automate $\mathcal{A}$ est $(\mathbb{Z}/p\mathbb{Z})[\beta]$.
Il y a maintenant deux cas à considérer :

- Si β est transcendant : Dans ce cas, on a $(\mathbb{Z}/p\mathbb{Z})[\beta] \simeq (\mathbb{Z}/p\mathbb{Z})[X]$, et on peut voir A comme une partie de $(\mathbb{Z}/p\mathbb{Z})[X]$. Montrons alors que le degré des états de l'automate $\mathcal{A}^{\mathrm{rel}}$ (vus comme des polynômes) est strictement majoré par

$$\max_{P\in A-A} \deg P.$$

Soit Q un état non nul de l'automate $\mathcal{A}$ de degré $\deg Q \geq \max_{P\in A-A} \deg P$. Pour toute transition $(Q,(U,V),R)$, on a alors

$$\deg R = \deg(XQ+U-V) = 1+\deg Q \geq \max_{P\in A-A} \deg P,$$

car $\deg(U-V) \leq \max_{P\in A-A} \deg P < \deg(XQ)$. Ainsi, par récurrence, il ne peut pas exister de chemin de l'état Q vers l'état final 0, donc l'état Q n'est pas dans l'automate émondé $\mathcal{A}^{\text{rel}}$.
Si le corps k est de caractéristique non nulle, cela prouve donc que l'ensemble des états de l'automate $\mathcal{A}^{\text{rel}}$ est fini.
Supposons maintenant que le corps k soit de caractéristique nulle. Montrons alors que les polynômes $P \in \mathbb{Z}[X]$ qui sont des états de l'automate $\mathcal{A}^{\text{rel}}$ ont leur $i^{\text{ème}}$ coefficient borné par

$$\sum_{j\geq i} \max_{\sum_s p_s X^s \in A-A} |p_j|\,.$$

Soit $Q = \sum_j q_j X^j$ un état de l'automate $\mathcal{A}$ ayant le $i^{\text{ème}}$ coefficient trop grand : $q_i > \sum_{j\geq i} \max_{\sum_j p_j X^j \in A-A} |p_j|$, et soit $(Q,(U,V),R)$ une transition de l'automate $\mathcal{A}$. Alors le $(i+1)^{\text{ème}}$ coefficient du polynôme $R = XQ+U-V$ est trop grand :

$$\begin{aligned} |q_i+u_{i+1}-v_{i+1}| &> (\sum_{j\geq i} \max_{\sum_s p_s X^s \in A-A} |p_j|) - |u_{i+1}-v_{i+1}| \\ &\geq (\sum_{j\geq i} \max_{\sum_s p_s X^s \in A-A} |p_j|) - \max_{\sum_s p_s X^s \in A-A} |p_{i+1}| \\ &= \sum_{j\geq i+1} \max_{\sum_s p_s X^s \in A-A} |p_j|\,. \end{aligned}$$

De la même façon que précédemment, il ne peut donc pas exister de chemin de l'état Q vers l'état final 0, donc l'état Q n'est pas dans l'automate émondé $\mathcal{A}^{\text{rel}}$.
On a montré que les polynômes P qui sont des états de l'automate $\mathcal{A}^{\text{rel}}$ ont tous leur coefficients bornés et ont leur degré borné. On conclut donc que l'automate $\mathcal{A}^{\text{rel}}$ est fini, et donc le semi-groupe Γ est fortement automatique.

– Si β est algébrique : Alors dans le cas où le corps k est de caractéristique non nulle, l'ensemble $(\mathbb{Z}/p\mathbb{Z})[\beta]$ des états de $\mathcal{A}$ est fini, et donc l'automate $\mathcal{A}^{\text{rel}}$ est aussi fini.
Supposons donc que le corps k est de caractéristique nulle. Sans perte de généralité, on supposera que l'on a $k = \mathbb{Q}(\beta)$.

Définition III.3.7. *Soit $\mathcal{P}$ l'ensemble (fini) des valeurs absolues v du corps $k = \mathbb{Q}(\beta)$ qui sont telles que $|\beta|_v \neq 1$. L'hypothèse sur le nombre β garantie que $\mathcal{P}$ contient toutes les valeurs absolues archimédiennes. On définit un anneau $\mathcal{R}$ stable par multiplication par β et par β^{-1}, par*

$$\mathcal{R} = \{x \in k |\ \textit{Pour toute valeur absolue } v \notin \mathcal{P}, |x|_v \leq 1\}.$$

Proposition III.3.8. *L'anneau $\mathcal{R}$ est un réseau dans l'espace*

$$E := \prod_{v \in \mathcal{P}} k_v,$$

dans lequel il est plongé diagonalement, où k_v est le complété du corps k pour la valeur absolue v.

Preuve de la proposition III.3.8. La discrétude de $\mathcal{R}$ dans E est une conséquence de la formule du produit :

Proposition III.3.9 (Formule du produit)**.**
Pour tout $x \in k \backslash \{0\}$, on a

$$\prod_{v \in \mathcal{P}_k} |x|_v = 1,$$

où $\mathcal{P}_k$ est l'ensemble des valeurs absolues du corps k (à équivalence près).

Remarque III.3.10. *Dans la proposition précédente, on a choisi les valeurs absolues "canoniques" dans chaque classe d'équivalence. Voir (Lan70), V.1. pour plus de détails.*

Étant donné un point $x_0 \in \mathcal{R}$, et un ensemble non vide de valeurs absolues $\mathcal{P}_0 \subseteq \mathcal{P}$ contenant les valeurs absolues archimédiennes, la formule du produit nous donne que le voisinage

$$V := \{x \in E | \text{ Pour toute valeur absolue } v \in \mathcal{P} \backslash \mathcal{P}_0, |x - x_0|_v \leq 1,$$
$$\text{et pour toute valeur absolue } v \in \mathcal{P}_0, |x - x_0|_v < 1\}$$

a pour intersection $\{x_0\}$ avec $\mathcal{R}$, ce qui donne bien la discrétude de $\mathcal{R}$ dans E.
Montrons maintenant la co-compacité de $\mathcal{R}$ dans E.
Pour cela, on utilise le théorème :

Théorème III.3.11.
Le corps k est discret et co-compact dans l'ensemble des adèles $\mathbb{A}_k$.

Voir (Lan70) pour la définition des adèles et une preuve du résultat.
L'espace $E' := E \times \prod_{v \in \mathcal{P}_k \backslash \mathcal{P}} \mathcal{O}_{k_v}$ est une partie ouverte de l'ensemble des adèles $\mathbb{A}_k$, donc son image dans le quotient $\mathbb{A}_k/k$ est aussi ouverte. On en déduit qu'elle est aussi fermée, puisque l'on peut écrire l'orbite de k sous l'action du groupe additif E' comme l'union des autres E'-orbites. Ainsi, l'image de E' dans le quotient $\mathbb{A}_k/k$ est compacte, d'où la co-compacité de $\mathcal{R} = k \cap E'$ dans E' et donc dans E. □

L'espace E est le produit d'un nombre fini de corps p-adiques, et de copies de $\mathbb{R}$ et $\mathbb{C}$.
Exemple III.3.12. *Pour $\beta = \frac{1+\sqrt{-14}}{5}$, l'espace E est*

$$E = \mathbb{C} \times \mathbb{Q}_3 \times \mathbb{Q}_5.$$

Pour $\beta = \frac{\sqrt{-14}}{5}$, l'espace E est

$$E = \mathbb{C} \times \mathbb{Q}_5 \times \mathbb{Q}_5 \times E_2 \times E_7,$$

où E_2 et E_7 sont respectivement des extensions de degré 2 de $\mathbb{Q}_2$ et de $\mathbb{Q}_7$.

On va montrer que l'ensemble des états de l'automate $\mathcal{A}^{\text{rel}}$ est inclu dans une partie compacte de E, ce qui prouvera sa finitude. Soit $v \in \mathcal{P}$ une des valeurs absolues. Montrons que les états x de l'automate $\mathcal{A}^{\text{rel}}$ vérifient

$$|x|_v < \frac{1}{|1 - |\beta|_v|} \max_{a \in A-A} |a|_v .$$

Par définition de $\mathcal{P}$, on a $|\beta|_v \neq 1$. On a alors deux cas :

1. $|\beta|_v < 1$
   D'après le lemme III.3.4, il existe un polynôme $P \in (A-A)[X]$ tel que l'on ait $x = P(\beta)$. On a alors
   $$|x|_v = |P(\beta)|_v < \max_{a \in A-A} |a|_v \sum_{i=0}^{\infty} |\beta|_v^i = \frac{1}{1 - |\beta|_v} \max_{a \in A-A} |a|_v .$$
2. $|\beta|_v > 1$
   D'après le lemme III.3.4, il existe un polynôme $Q \in (A-A)[X]$ tel que l'on ait $x = \beta^{-1} Q(\beta^{-1})$. On a alors
   $$|x|_v = \left|\beta^{-1} Q(\beta^{-1})\right|_v < \frac{1}{|\beta|_v - 1} \max_{a \in A-A} |a|_v .$$

Le domaine de l'espace E délimité par ces inégalités est relativement compact. Ainsi, la discrétude de l'anneau $\mathcal{R}$ dans l'espace E entraîne que l'automate $\mathcal{A}^{\text{rel}}$ n'a qu'un nombre fini d'états. Donc le semi-groupe Γ est fortement automatique.

Ceci termine la preuve du théorème III.3.2. □

Remarque III.3.13. *Dans les directions p-adiques, le fait que les valeurs absolues soient ultra-métriques permet d'obtenir les inégalités plus précises suivantes :*

$$|x|_p \leq \max_{a \in A-A} |a|_p \left|\beta^{-1}\right|_p \text{ si } |\beta|_p > 1,$$

$$|x|_p \leq \max_{a \in A-A} |a|_p \text{ si } |\beta|_p < 1,$$

pour tout état x non nul de l'automate $\mathcal{A}^{\text{rel}}$.

Remarque III.3.14. *La condition pour le nombre algébrique β d'être sans conjugué de module 1 est nécessaire : voir exemple III.3.23 et proposition III.3.15. Cependant, il existe tout de même des nombres algébriques ayant au moins un conjugué de module 1 et pour*

lequels le semi-groupe est automatique. Par exemple, le semi-groupe engendré par les deux applications

$$\begin{cases} x & \mapsto & \beta x \\ x & \mapsto & \beta x + 1 \end{cases}$$

est libre (et donc fortement automatique) dès que le nombre β a un conjugué de module strictement supérieur à 2. Ainsi, par exemple, il est libre pour le nombre de Salem qui est racine du polynôme $X^4 - 3X^3 - 3X^2 - 3X + 1$.

III.3.2 Réciproque

Voici une réciproque au théorème III.3.2, qui permet de voir que la condition sur le nombre β pour que le semi-groupe soit fortement automatique est optimale.

Proposition III.3.15. *En caractéristique nulle, si β est un nombre algébrique ayant un conjugué de module 1, alors il existe une partie finie $A \subset \mathcal{R}$ telle que le semi-groupe Γ n'est pas fortement automatique.*

Remarque III.3.16. *D'après le lemme III.3.4, la proposition III.3.15 revient à dire que si β a un conjugué de module 1, alors il existe une partie finie $A \subset \mathcal{R}$ telle que l'ensemble*

$$\{x \in \mathcal{R} | \textit{Il existe } P, Q \in (A - A)[X] \textit{ tels que } x = P(\beta) = \beta^{-1} Q(\beta^{-1})\}$$

est infini.

Remarque III.3.17. *Dans la proposition III.3.15, on peut même choisir $A \subset \mathbb{Z}[\beta]$.*

Remarque III.3.18. *Sous les hypothèses de la proposition, pour tout γ conjugué de β, l'inverse $1/\gamma$ est aussi un conjugué de β.*

En effet, si $\gamma \in \mathbb{C}$ est de module 1, alors $1/\gamma$ est son conjugué complexe.

L'idée de la preuve de la proposition III.3.15 est la suivante : grâce au lemme III.3.19 on se ramène à seulement montrer l'existence de chemins jusqu'à 0, plutôt que dans les deux sens. On choisit alors une partie finie A et un domaine infini $\mathbb{D}$ qui soient tels que l'on puisse trouver des transitions des points de $\mathbb{D}$ vers d'autres points de $\mathbb{D}$ plus proche de 0, jusqu'à tomber dans une partie compacte. Il suffira alors de rajouter à la partie A le bon ensemble fini de points pour obtenir des transitions de tous les points du compact vers 0.

Preuve de la proposition III.3.15. Soit $\beta \in \mathbb{C}$ un nombre algébrique ayant un conjugué de module 1. Pour toute partie A finie de $k = \mathbb{Q}(\beta)$, on considèrera l'automate $\mathcal{A}$ définit dans la preuve du théorème III.3.2. D'après la proposition III.3.8, on peut plonger l'anneau $\mathcal{R}$ dans un espace E qui est un produit de corps p-adiques et de copies des corps $\mathbb{R}$ et $\mathbb{C}$, de

façon à ce que l'anneau $\mathcal{R}$ soit un réseau dans l'espace E. On peut alors écrire l'espace E comme un produit de trois espaces :

$$E = E_- \times E_0 \times E_+,$$

où

- l'espace E_+ est le produit des complétés du corps k pour les valeurs absolues v telles que $|\beta|_v > 1$,
- l'espace E_0 est le produit des complétés du corps k pour les valeurs absolues archimédiennes v telles que $|\beta|_v = 1$,
- l'espace E_- est le produit des complétés du corps k pour les valeurs absolues v telles que $|\beta|_v < 1$.

On notera respectivement $\mathcal{P}_-$, $\mathcal{P}_0$ et $\mathcal{P}_+$ les ensembles de valeurs absolues des corps des espaces E_-, E_0 et E_+. On notera aussi $\|.\|_0$ la norme infinie sur E_0.

Notation . *Étant donné $x = P(\beta) \in \mathcal{R}$, on note $\overline{x} := P(\beta^{-1}) \in \mathcal{R}$.*

L'application $x \mapsto \overline{x}$ est un élément de $\mathrm{Gal}(\mathbb{Q}(\beta)/\mathbb{Q})$ d'après la remarque III.3.18.

Lemme III.3.19. *S'il existe un chemin de x à 0 dans l'automate $\mathcal{A}$, alors il existe aussi un chemin de 0 à $\overline{x}/\beta$.*

Preuve du lemme. De même que dans la preuve du lemme III.3.4, l'existence d'un chemin de x à 0 est équivalente à l'existence d'un polynôme $Q \in (A - A)[X]$ tel que $x = \beta^{-1}Q(\beta^{-1})$. On obtient alors un chemin de 0 à $\overline{x}/\beta = Q(\beta)$ dans l'automate $\mathcal{A}$. □

On va montrer qu'il existe une partie finie $A \subset \mathcal{R}$ et un domaine $\mathbb{D}$ de l'espace E, tels que pour tout point x de l'ensemble infini $\mathbb{D} \cap \mathcal{R}$, il existe un chemin de x à 0 dans l'automate $\mathcal{A}$.

Remarque III.3.20. *L'existence d'un tel chemin revient à démontrer que pour tout point $x \in \mathbb{D} \cap \mathcal{R}$, il existe un polynôme $Q \in (A - A)[X]$ tel que l'on ait $x = \beta^{-1}Q(\beta^{-1})$.*

iii) Construction de la partie A

Nous allons construire la partie A en deux morceaux : la partie A_R nous permettra de rapprocher de 0 les éléments de grande norme, tandis que la partie A' permettra d'obtenir une transition de tous les autres éléments vers 0.

Pour $R > 0$, on définit une partie $A_R \subseteq \mathcal{R}$ par $x \in A_R$ si et seulement si l'on a

$$|x|_v < R,$$

pour toute valeur absolue v. On va maintenant fixer un réel R assez grand de la façon suivante :

Soit r le diamètre d'une maille (c'est-à-dire d'un domaine fondamental) du réseau $\mathcal{R}$ dans E. Définissons une partie $K \subseteq E_0 \times E_+$ par $x \in K$ si et seulement si

$$\text{pour toute valeur absolue } v \in \mathcal{P}_0, \quad |x|_v < 3r,$$

$$\text{pour toute valeur absolue } v \in \mathcal{P}_+, \quad |x|_v < |\beta|_v \, r.$$

En choisissant le rayon $R = 3r \max_{v \in \mathcal{P}} |\beta|_v$, la partie A_R est r-couvrante dans l'ensemble K (c'est bien une partie de l'espace $E_0 \times E_+$, comme partie du corps k, qui se plonge diagonalement dans le produit de ses complétés). C'est-à-dire tel que l'on a :

$$K \subseteq \bigcup_{x \in A_R} B(x, r) \subseteq E_0 \times E_+.$$

On définit maintenant une partie $A' \subseteq \mathcal{R}$ par $x \in A'$ si et seulement si l'on a

$$\text{pour toute valeur absolue } v \in \mathcal{P}_+, \quad |x|_v < |\beta|_v \, r,$$

$$\text{pour toute valeur absolue } v \in \mathcal{P}_0, \quad |x|_v < 3r,$$

$$\text{pour toute valeur absolue } v \in \mathcal{P}_-, \quad |x|_v < \frac{\max_{x \in A_R} |x|_v}{1 - |\beta|_v},$$

La partie A finie de $\mathcal{R}$ que l'on considère est

$$A := A' \cup A_R.$$

iv) Construction du domaine $\mathbb{D}$

On considère le domaine $\mathbb{D} \subseteq E$ définit par $x \in \mathbb{D}$ si et seulement si

$$|x|_v < r, \quad \text{pour toute valeur absolue } v \in \mathcal{P}_+,$$

$$|x|_v < \frac{\max_{x \in A_R} |x|_v}{1 - |\beta|_v}, \quad \text{pour toute valeur absolue } v \in \mathcal{P}_-.$$

v) Preuve de la non finitude de $\mathcal{A}^{\text{rel}}$

Montrons pour commencer qu'il existe une transition de tout point assez grand du domaine $\mathbb{D}$, vers un point strictement plus proche de 0.

Lemme III.3.21. *Pour tout point $x \in \mathbb{D} \cap k$ tel que $\|x\|_0 \geq 3r$, il existe un point $y \in \mathbb{D} \cap k$ tel que*

- *Il existe une transition dans l'automate $\mathcal{A}$ de x à y,*
- *On a l'inégalité $\|y\|_0 < \|x\|_0$.*

Démonstration. Soit x un point de $\mathbb{D} \cap k$ tel que $\|x\|_0 \geq 3r$. Dans l'espace E_0, considérons une boule fermée B_0 de centre c sur le segment $[0, \beta x]$, de rayon r, ne contenant pas 0, et qui soit incluse dans la boule de centre 0 et de rayon $3r$. Le point de coordonnées c dans l'espace E_0 et βx dans l'espace E_+ est dans le compact K de l'espace $E_0 \times E_+$. La partie A_R étant r-couvrante, on peut alors trouver un point $t \in A_R$ qui est dans la boule B_0 dans l'espace E_0 et à distance au plus r de x dans l'espace E_+. Alors le point $y := \beta x - t$ convient car

1. Il y a bien une transition de x à y dans l'automate $\mathcal{A}$ puisque l'on a
$$-t \in -A \subseteq A - A.$$
2. Dans l'espace E_+, on a bien pour toute valeur absolue $v \in \mathcal{P}_+$, $|\beta x - t|_v < r$, puisque le point βx est dans la boule de centre t et de rayon r.
3. Dans l'espace E_0, par construction de la boule B_0, le fait que t soit dans B_0 nous donne l'inégalité stricte
$$\|\beta x - t\|_0 < \|\beta x\|_0 = \|x\|_0.$$
4. Dans l'espace E_-, on a bien pour toute valeur absolue $v \in \mathcal{P}_-$,
$$|\beta x - t|_v \leq |\beta|_v |x|_v + |t|_v < \frac{|\beta|_v \max_{a \in A_R} |a|_v}{1 - |\beta|_v} + \max_{a \in A_R} |a|_v \leq \frac{\max_{a \in A_R} |a|_v}{1 - |\beta|_v}.$$

□

Lemme III.3.22. *Pour tout point $x \in \mathbb{D} \cap \mathcal{R}$, il existe un chemin de x à 0 dans l'automate $\mathcal{A}$.*

Démonstration. Soit $x \in \mathbb{D} \cap \mathcal{R}$.

Supposons d'abord que l'on ait $\|x\|_0 < 3r$. Dans ce cas l'élément βx est dans l'ensemble A' (puisque l'on a $\|\beta x\|_0 = \|x\|_0 < 3r$). Il existe donc un élément $t \in -A' \subseteq -A \subseteq A - A$ tel que $\beta x + t = 0$, ce qui prouve l'existence d'une transition de x vers 0.

On est donc ramené à supposer que l'on ait $\|x\|_0 \geq 3r$. Le lemme III.3.21 permet alors d'obtenir une transition vers un état de norme $\|.\|_0$ strictement inférieure. Par récurrence, et par discrétude de $\mathcal{R}$ dans E, on est donc ramené au premier cas. □

Pour achever la preuve de la proposition III.3.15, il suffit de remarquer que les lemmes III.3.22 et III.3.19 entraînent que les éléments de l'ensemble infini

$$\mathbb{D} \cap \beta^{-1}\overline{\mathbb{D}} \cap \mathcal{R}$$

sont des états de l'automate émondé $\mathcal{A}^{\text{rel}}$. □

III.3.3 Un exemple non fortement automatique

La proposition III.3.15 nous donne des parties A finies pour lesquelles le semi-groupe n'est pas fortement automatique. Voici un exemple de semi-groupe non fortement automatique pour une partie $A = \{0, 1\}$ fixée.

Proposition III.3.23. *Soit le nombre de Salem $\beta = \frac{1+\sqrt{2}+\sqrt{2\sqrt{2}-1}}{2} \simeq 1.8832035059$ (qui est une racine du polynôme $X^4 - 2X^3 + X^2 - 2X + 1$). Alors, le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x & \mapsto & \beta x \\ 1 : x & \mapsto & \beta x + 1 \end{cases}$$

n'est pas fortement automatique.

Corollaire III.3.24. *Pour le nombre de Salem β de la proposition précédente, il n'existe aucune partie $A \subset \mathbb{C}$ finie et de cardinal au moins 2, telle que le monoïde Γ soit fortement automatique.*

Preuve du corollaire. Soit $A_0 \subseteq A$ une partie de A de cardinal 2, et soit Γ_0 le semi-groupe engendré par les deux applications

$$x \quad \mapsto \quad \beta x + t, \text{ pour } t \in A_0.$$

Alors les sommets de l'automate $\mathcal{A}^{\text{rel}}_{\Gamma_0}$ sont aussi des sommets de l'automate $\mathcal{A}^{\text{rel}}_{\Gamma}$. En effet, tout chemin de l'automate $\mathcal{A}^{\text{rel}}_{\Gamma_0}$ est aussi un chemin de l'automate $\mathcal{A}^{\text{rel}}_{\Gamma}$. Ainsi, la forte automaticité du semi-groupe Γ entraîne celle du semi-groupe Γ_0. Or, le semi-groupe Γ_0 est le même que le semi-groupe de la proposition III.3.23 modulo similitude (et donc le même d'un point de vue combinatoire). Ainsi, la proposition III.3.23 implique que le semi-groupe Γ n'est pas fortement automatique. □

L'idée de la preuve de la proposition est la suivante : De même que dans la preuve de la proposition III.3.15, on se ramène à montrer l'existence de chemins des points d'un domaine infini $\mathbb{D}$ vers 0. Et de la même façon, on commence par ramener tout point dans une partie compacte, puis on montre qu'il existe un chemin vers 0 pour chaque point de la partie compacte.

Ici il n'est pas possible de choisir la partie A pour pouvoir rapprocher les points de 0 en suivant une seule transition. Ce que l'on fera est de donner, suivant l'endroit où se trouve le point dans la partie contractante, des suites d'arêtes qui permettent de se rapprocher de 0 tout en restant bien dans le domaine $\mathbb{D}$.

Preuve de la proposition. Le réel β est strictement supérieur à 1, et possède un conjugué réel de module strictement inférieur à 1, ainsi que deux conjugués complexes conjugués de module 1. L'anneau des entiers $\mathbb{Z}[\beta] = \mathcal{R}$ de β se plonge donc dans $\mathbb{R}^2 \times \mathbb{C}$, et on a trois plongements σ_+, σ_0 et σ_- dans les complétés du corps k pour les valeurs absolues respectives $|.|_+$, $|.|_0$ et $|.|_-$ telles que $|\beta|_+ > 1$, $|\beta|_0 = 1$ et $|\beta|_- < 1$. La preuve du théorème

III.3.2 nous permet de voir que les sommets de l'automate $\mathcal{A}^{\text{rel}}$ sont dans un domaine de $\mathbb{R}^2 \times \mathbb{C}$ délimité par les inégalités

$$|x|_i < \frac{1}{||\beta|_i - 1|}, \text{ pour } i \in \{+, -\}.$$

Définissons alors le domaine $\mathbb{D} \subset \mathbb{R}^2 \times \mathbb{C}$ délimité par les inégalités

$$x \in \mathbb{D} \text{ si et seulement si } |x|_+ < \frac{c}{|\beta|_+ - 1} \text{ et } |x|_- < \frac{1}{1 - |\beta|_-},$$

où $0 < c < 1$ est une constante qui sera fixée ultérieurement.

De même que dans la preuve de la proposition III.3.15, on souhaite démontrer le lemme :

Lemme III.3.25. *Pour tout point x de $\mathbb{D} \cap \mathbb{Z}[\beta]$, il existe un chemin dans l'automate restreint au domaine $\mathbb{D}$ qui part de x et aboutit en 0.*

Remarque III.3.26. *Ceci revient à démontrer le résultat suivant :*

$$\textit{Pour tout } x \in \mathbb{D} \cap \mathbb{Z}[\beta], \textit{ il existe } Q \in \{-1, 0, 1\}[X] \textit{ tel que } x = \beta^{-1} Q(\beta^{-1}).$$

Pour cela, nous allons donner une stratégie qui permet, partant d'un point $x \in \mathbb{D}$, d'aboutir à un sommet $y \in \mathbb{D}$ tel que $|y|_0 < |x|_0$, en suivant des transitions de l'automate $\mathcal{A}$ données par une suite d'étiquettes dans $\{-1, 0, 1\}$. Nous allons donner cette stratégie de la façon suivante : étant donné un intervalle dans lequel se situe le point $(\beta - 1)x$ dans la direction dilatante $E_+ = \mathbb{R}$, nous donnerons trois suites d'éléments de $\{-1, 0, 1\}$ qui donnent des chemins vers trois états dont l'un au moins sera de module strictement inférieur à x dans la direction correspondant aux complexes conjugués.

Pour obtenir cela, nous avons découpé l'intervalle de la direction dilatante correspondant au domaine $\mathbb{D}$ en intervalles vérifiant le lemme :

Lemme III.3.27. *Soit I un intervalle de $E_+ = \mathbb{R}$. S'il existe trois suites $(a_i^1)_{1 \le i \le n_1}$, $(a_i^2)_{1 \le i \le n_2}$ et $(a_i^3)_{1 \le i \le n_3}$ de $\{-1, 0, 1\}^{(\mathbb{N})}$ vérifiant :*

1. *Dans l'espace $E_0 = \mathbb{C}$, les trois nombres complexes*

$$c_j := \sum_{i=1}^{n_j} a_i^j \beta^{-i} \quad \textit{pour } j \in \{1, 2, 3\},$$

   forment un triangle contenant 0 dans son intérieur.

2. *Pour tout $j \in \{1, 2, 3\}$, on a l'inclusion*

$$\beta^{n_j} I + \sum_{i=1}^{n_j} a_i^j \beta^{n_j - i} \subseteq \mathbb{D},$$

alors pour tout point $x \in \mathbb{D}$ tel que $\sigma_+(x) \in I$ et tel que $|x|_0$ est assez grand, il existe un chemin $x \xrightarrow{a_1^j} \dots \xrightarrow{a_{n_j}^j} y$ pour un $j \in \{1,2,3\}$, vers un point $y \in \mathbb{D}$ tel que $|y|_0 < |x|_0$.

Démonstration. La première condition permet de trouver un $j \in \{1,2,3\}$ tel que l'on ait l'inégalité

$$|x + c_j|_0 < |x|_0 \,,$$

dès que $|x|_0$ est assez grand.
En effet, il suffit que dans l'espace $E_0 = \mathbb{C}$ le point x soit en dehors du triangle formé par les médiatrices des segments $[0, -c_j], j = 1,2,3$.

La deuxième condition assure que le point $y := \beta^{n_j}(x + c_j)$ est dans le domaine $\mathbb{D}$, et on a $|y|_0 = |x + c_j|_0$. Et pour finir, la définition de y donne l'existence du chemin

$$x \xrightarrow{a_1^j} \dots \xrightarrow{a_{n_j}^j} y$$

dans l'automate $\mathcal{A}$. □

Voici cette stratégie, pour $c = 0.883204$, en supposant que l'on parte d'un point $x \in \mathbb{D}$ tel que $|x|_0 > 3.883201$ et $\sigma_+(x) \geq 0$, et où les intervalles sont dilatés d'un facteur 0.883204 :

[0.468990, 0.601232]	[0.601232, 0.647807]	[0.647807, 0.671454]
-1 0 -1 1	-1 -1 0 1 1	-1 -1 0 0 1 1
-1 0 -1	-1 -1 1 -1 1	-1 -1 0 1 0 -1
-1 0 0	-1 0 -1 -1 1	-1 0 -1 -1 1 -1
[0.671454, 0.685095]	[0.685095, 0.708742]	[0.708742, 0.718028]
-1 0 -1 -1 -1 1	-1 -1 0 0 0 1	-1 -1 0 0 1 -1
-1 -1 0 1 0 -1	-1 -1 0 0 1 -1	-1 0 -1 -1 -1 0
-1 0 -1 -1 0 -1	-1 0 -1 -1 0 -1	-1 0 -1 -1
[0.718028, 0.780048]	[0.780048, 0.812982]	[0.812982, 0.832782]
-1 -1 -1 1 1	-1 -1 -1 0 1 1	-1 -1 -1 0
-1 -1 -1	-1 -1 -1 0 1	-1 -1 -1 0 1 0 -1
-1 -1 0 -1 1	-1 -1 -1 1 -1 1	-1
[0.832782, 0.850270]	[0.850270, 0.883204]	[-0.468990, 0.468990]
-1 -1 -1 0 0 1 -1	-1 -1 -1 -1 1	0^n
-1 -1 -1 0 0 0	-1 -1 -1 -1	
-1 -1 -1 0 1 -1 -1	-1 -1 -1 0 0	

Si l'on part d'un point $x \in \mathbb{D}$ tel que $|x|_0 > 3.883201$ et $\sigma_+(x) < 0$, alors on déduit la stratégie de celle donnée ci-dessus : il suffit de faire l'opposé de la suite de coups de l'intervalle opposé.

Quand on arrive dans l'intervalle [-0.468990, 0.468990], il suffit de suivre suffisamment d'arêtes étiquetées par 0 pour retomber dans l'un des intervalles ci-dessus ou son opposé.

Il reste ensuite à donner la stratégie pour $|x|_0 \leq 3.883201$. Le nombre de points est alors fini : il y en a 76. Voici une stratégie pour 38 de de ces points :

$1 \to$ -1 -1 -1 -1 1	$\beta - 2 \to$ 1 -1
$\beta - 1 \to$ -1 -1 -1	$2\beta - 3 \to$ -1 -1
$\beta^2 - 3\beta + 1 \to$ 1 1 1	$\beta^2 - 3\beta + 2 \to$ 0 1
$\beta^2 - 3\beta + 3 \to$ -1	$\beta^2 - 2\beta \to$ 0 0 1
$\beta^2 - 2\beta + 1 \to$ -1	$\beta^2 - \beta - 1 \to$ -1
$2\beta^2 - 4\beta \to$ 0 1	$2\beta^2 - 4\beta + 1 \to$ -1
$2\beta^2 - 3\beta - 1 \to$ -1	$\beta^3 - 3\beta^2 + \beta + 1 \to$ 1
$\beta^3 - 3\beta^2 + 2\beta \to$ 1	$\beta^3 - 3\beta^2 + 2\beta + 1 \to$ -1 -1 -1 1 1
$\beta^3 - 3\beta^2 + 3\beta - 2 \to$ 1	$\beta^3 - 3\beta^2 + 3\beta - 1 \to$ -1 -1 0 1 1 -1
$\beta^3 - 3\beta^2 + 4\beta - 3 \to$ -1 0 -1	$\beta^3 - 2\beta^2 - \beta + 2 \to$ 0 1
$\beta^3 - 2\beta^2 \to$ 0 1	$\beta^3 - 2\beta^2 + 1 \to$ -1 0 0 -1 1
$\beta^3 - 2\beta^2 + \beta - 2 \to$ 1	$\beta^3 - 2\beta^2 + \beta - 1 \to$ 0 -1 -1 -1 1
$\beta^3 - \beta^2 - 2\beta \to$ 1 0 1 -1	$\beta^3 - \beta^2 - 2\beta + 1 \to$ -1
$\beta^3 - \beta^2 - \beta - 1 \to$ -1	$\beta^3 - 4\beta \to$ 1 1 1
$\beta^3 - 3\beta \to$ -1	$2\beta^3 - 5\beta^2 + 3\beta - 2 \to$ 1
$2\beta^3 - 5\beta^2 + 4\beta - 3 \to$ -1 1 0 1 1	$2\beta^3 - 4\beta^2 \to$ 1
$2\beta^3 - 4\beta^2 + \beta - 1 \to$ 1 -1 -1 -1	$2\beta^3 - 4\beta^2 + \beta \to$ -1 -1 -1 -1 -1 1 0 1 1
$2\beta^3 - 4\beta^2 + 2\beta - 2 \to$ -1 -1 -1 0 1	$2\beta^3 - 3\beta^2 - 2\beta \to$ 1 1
$2\beta^3 - 3\beta^2 - \beta - 1 \to$ 0 1	$2\beta^3 - 3\beta^2 - \beta \to$ -1 -1 0 -1

De la même façon que précédemment, on déduit la stratégie pour l'autre moitié des points en considérant la suite de coups opposée de l'élément de $\mathbb{Z}[\beta]$ opposé.

En suivant cette stratégie, on aboutit à l'état 0 en partant de n'importe quel point du domaine $\mathbb{D}$. Il suffit donc de vérifier chacun des cas ci-dessus pour obtenir une preuve de l'exemple. Tout ceci a été vérifié par ordinateur. □

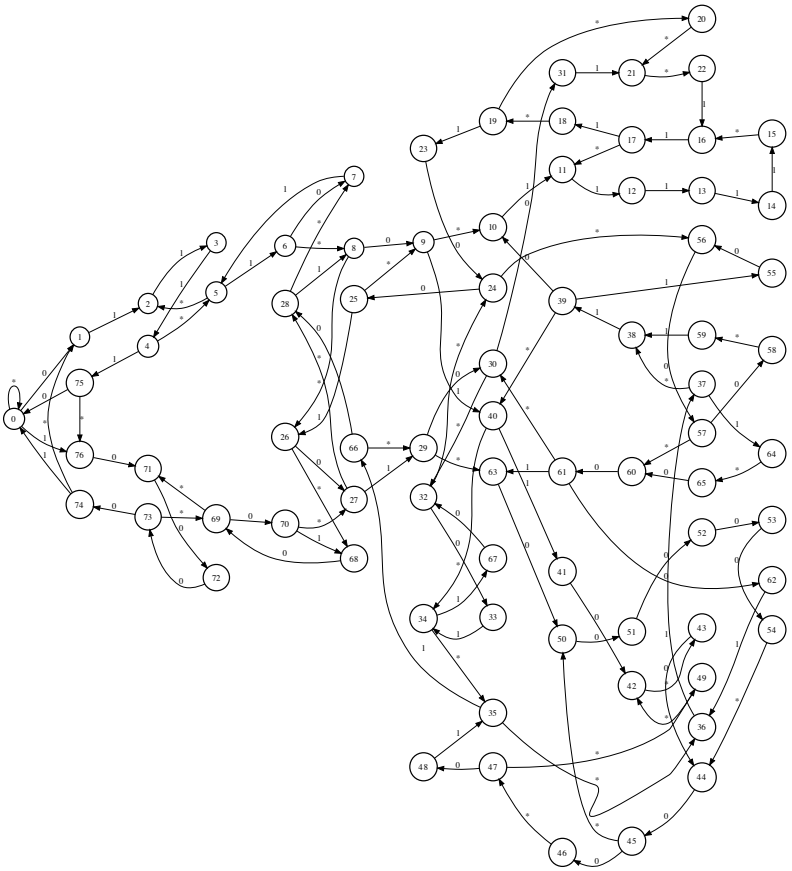
Exemple III.3.28. *En suivant la stratégie ci-dessus, en partant de $x = \beta^2 - 3$, on obtient le chemin*

$$x = \beta^2 - 3 \xrightarrow{\text{-1 0 0}} \beta^2(\beta(\beta^2 - 3) - 1) = -\beta^2 + 3\beta - 2,$$

puisque $(\beta - 1)(\beta^2 - 3) \simeq 0.4826 \in [0.468990, 0.601232]$ et $|\beta^2 - 3|_0 \simeq 3.935 > 3.883201$. L'opposé de l'élément $-\beta^2+3\beta-2$ est alors dans la liste des 38 points (puisque $|-\beta^2 + 3\beta - 2|_0 \simeq 3.75 < 3.883201$), et on a successivement (en restant parmi ces 38 points ou leur opposé) :

$$-\beta^2 + 3\beta - 2 \xrightarrow{\text{0 -1}} \beta^3 - \beta^2 - 2\beta \xrightarrow{\text{1 0 1 -1}} \beta^3 - 2\beta^2 \xrightarrow{\text{0 1}} -\beta^3 + 2\beta^2 - \beta + 1 \xrightarrow{\text{0 1 1 1 -1}} 0.$$

FIGURE III.21 – Portion de l'automate infini $\mathcal{A}^{\text{rel}}$ des relations du semi-groupe de la proposition III.3.23



Pour alléger les notations, sur la figure, on a remplacé les couples $(0,1)$ par 0, les couples $(1,0)$ par 1 et les paires de couples $(0,0)$ et $(1,1)$ par $*$.

Remarque III.3.29. *La preuve ci-dessus revient à démontrer le résultat suivant :*

Les restes dans la division euclidienne d'un polynôme $P \in \{-1,0,1\}[X]$ par le polynôme $\pi := X^4 - 2X^3 + X^2 - 2X + 1$ sont exactement les polynômes $Q \in \mathbb{Z}_3[X]$ tels que

$$|Q(\beta)| < \frac{1}{\beta - 1} \quad \text{et} \quad |Q(1/\beta)| < \frac{1}{1 - 1/\beta},$$

où $\beta > 1$ est la plus grande racine réelle de π.

La remarque suivante est due à Laurent Bartholdi.

Remarque III.3.30. *On peut montrer que le semi-groupe de l'exemple III.3.23 n'est pas de présentation fini puisqu'il contient les relations $10^{4n}1 = 011(1001)^{n-1}110$ qui ne se déduisent pas de relations plus courtes.*

Question . *Le semi-groupe de l'exemple III.3.23 est-il automatique ? A t'il un ensemble de mots réduits qui soit un langage rationnel ? Je conjecture une réponse négative à ces questions.*

III.3.4 Un exemple de semi-groupe fortement automatique et de présentation infinie

Voici un exemple explicite de semi-groupe fortement automatique dont nous montrons qu'il n'est pas de présentation finie.

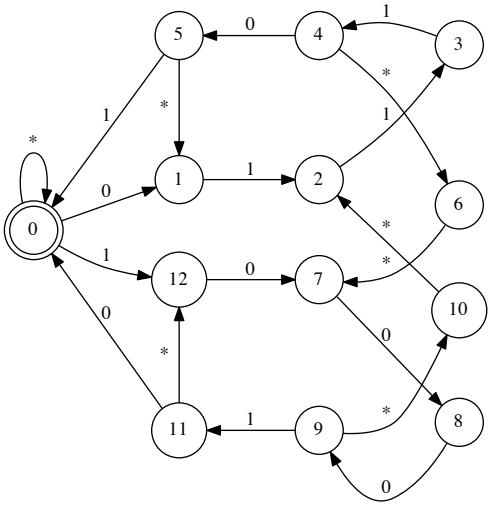
Proposition III.3.31. *Soit $\beta \simeq 1.7924023578$ la racine réelle du polynôme $X^5 - X^4 - X^3 - X^2 + X - 1$. Alors, le monoïde engendré par les deux applications*

$$\begin{cases} 0 : x & \mapsto & \beta x \\ 1 : x & \mapsto & \beta x + 1 \end{cases}$$

n'est pas de présentation finie.

Démonstration. Le nombre β n'a pas de conjugué de module 1. D'après le théorème III.3.2, le semi-groupe Γ est donc fortement automatique. Et de la preuve de ce théorème, on déduit que l'automate des relations du semi-groupe Γ est celui de la figure suivante.

FIGURE III.22 – Automate $\mathcal{A}^{\text{rel}}$ des relations du monoïde de la proposition III.3.31



Pour alléger les notations, sur la figure, on a remplacé les couples $(0,1)$ par 0, les couples $(1,0)$ par 1 et les paires de couples $(0,0)$ et $(1,1)$ par $*$.

Lemme III.3.32. *On a les relations*

$$0111(00000011)^n01 = 1000(00110000)^n10$$

pour tout entier n.

Démonstration. Cela se lit sur l'automate des relations ci-dessus. □

La proposition III.3.31 se déduit alors du lemme suivant. □

Lemme III.3.33. *Les relations données par le lemme précédent sont minimales (c'est-à-dire qu'elles ne se déduisent pas de relations plus courtes).*

Démonstration. On peut lire sur l'automate que pour toute relation minimale $u = v$, le mot u a un préfixe parmi $\begin{cases} 0111 \\ 1000**1 \\ 10001 \end{cases}$ (où les étoiles $*$ représentent chacune n'importe quelle lettre parmi 0 et 1) et a un suffixe parmi $\begin{cases} 010 \\ 101 \end{cases}$. Le mot u ne peut donc pas être un sous-mot strict du mot $0111(00000011)^n01$. □

III.4 Exemples

Cette section est consacrée à divers exemples qui rentrent dans la cadre du critère de forte automaticité des semi-groupes de développement en base β (théorème III.0.9). Nous relions nos travaux à des travaux déjà existants, et donnons des automates des relations et des valeurs exactes d'exposants critiques que nous avons pu calculer grâce à notre preuve éffective du théorème III.3.2.

Pour un semi-groupe Γ de développement en base β engendré par une partie finie G, on appellera *vitesse exponentielle de croissance* du semi-groupe le réel

$$\lambda := \limsup_{n\to\infty} \frac{1}{n} \log(\#G^n),$$

où G^n est l'ensemble des éléments de Γ de longueur n en les générateurs G.

Remarque III.4.1. *Pour un nombre $\beta \in \mathbb{C}$, si l'ensemble des générateurs G d'un semi-groupe Γ sont de la forme $x \mapsto \beta x + t$ pour $t \in \mathbb{C}$, alors l'exposant critique δ_Γ est relié à la vitesse exponentielle de croissance par*

$$\delta_\Gamma = \frac{\log(\lambda)}{|\log(\beta)|}.$$

III.4.1 Le cas où β est un nombre de Pisot

On appelle *nombre de Pisot* un réel algébrique $\beta > 1$ qui a tous ses conjugués de modules strictement inférieurs à 1. Dans son article (Lal97), Lalley s'intéresse aux semi-groupes engendrés par les transformations affines

$$x \mapsto \beta x + t$$

pout $t \in A \subset \mathbb{Z}[\beta]$, où $1/\beta$ est un nombre de Pisot et A est une partie finie de $\mathbb{Z}[\beta]$. D'après le théorème III.3.2, le semi-groupe est fortement automatique. En particulier, il existe un automate des mots réduits pour l'ordre lexicographique, par la proposition III.2.26. Lalley

donne une construction de l'automate des mots réduits (mais sans parler d'automates), mais la construction que je propose dans cette thèse est différente. Il obtient ainsi la vitesse de croissance du semi-groupe, qu'il arrive à relier à la dimension de Hausdorff de l'ensemble limite.

III.4.2 L'exemple de Kenyon

R. Kenyon étudie en détails dans son article (Ken97) le semi-groupe engendré par les trois transformations

$$\begin{cases} 0 : x & \mapsto & x/3 \\ b : x & \mapsto & x/3 & +t \\ 1 : x & \mapsto & x/3 & +1 \end{cases}$$

où $0 < t < 1$ est un réel.

D'après le théorème III.3.2, ce semi-groupe est fortement automatique pour tout réel t. La proposition suivante permet de savoir si le semi-groupe Γ est libre ou non (et donc de savoir si l'automate des relations $\mathcal{A}^{\text{rel}}$ est trivial ou non).

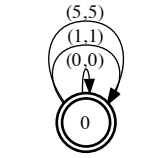
Proposition III.4.2 (Kenyon)**.** *Le semi-groupe Γ est libre si et seulement si le réel t n'est pas un rationnel de la forme $\frac{p}{q}$ avec $p+q \not\equiv 0 \mod 3$, pour $p \wedge q = 1$.*

Dans son article, Kenyon propose une construction d'automates qui est un cas particulier de la construction que je propose dans ce chapitre. Il s'intéresse à la dimension de Hausdorff de l'ensemble limite du semi-groupe Γ. Il montre que celle-ci est reliée à la vitesse exponentielle de croissance du semi-groupe (que l'on peut calculer avec l'automate des mots réduits) quand le paramètre de translation t est rationnel. C'est encore une conjecture (connue sous le nom de conjecture de Furstenberg) que l'ensemble limite est de dimension de Hausdorff 1 quand le paramètre de translation t est irrationnel. Voir (Ken97).

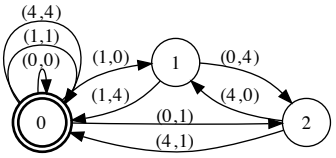
Voici quelques exemples d'automates des relations que l'on obtient pour le monoïde engendré par les 3 transformations

$$\begin{cases} 0 : & x & \mapsto & x/3, \\ a : & x & \mapsto & x/3 & + & a, \\ b : & x & \mapsto & x/3 & + & b. \end{cases}$$

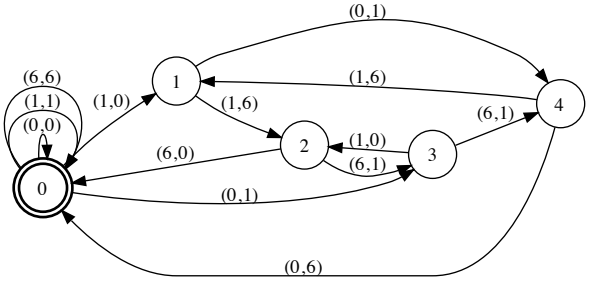
(Ce qui revient à considérer le semi-groupe de Kenyon avec $t = a/b$ et avec un élément neutre.) Cela permet de voir à quoi ressemble les premiers exemples d'automates correspondant au semi-groupe de Kenyon.



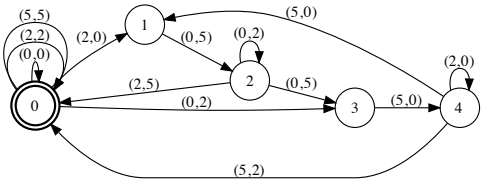
a=1 et b=5



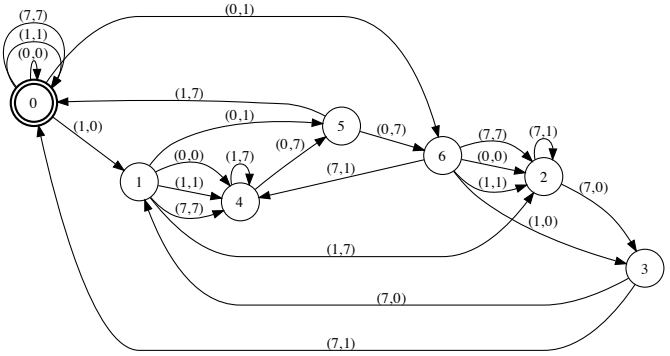
a=1 et b=4



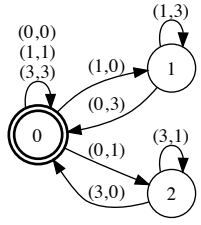
a=1 et b=6



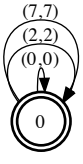
a=2 et b=5



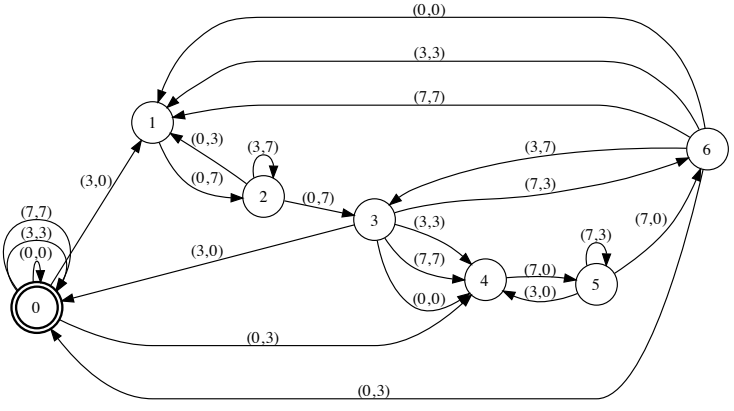
a=1 et b=7



a=1 et b=3

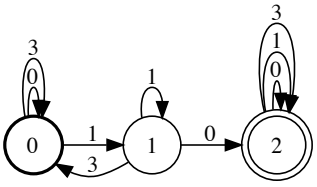


a=2 et b=7

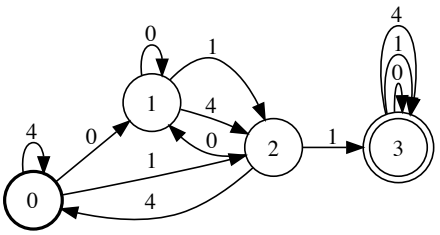


a=3 et b=7

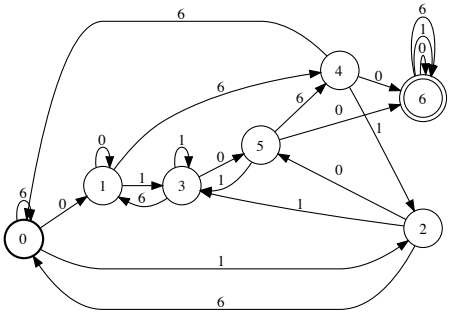
Et voici les automates minimaux des mots non réduits pour les même exemples (sauf pour $a/b = 1/5$ et $a/b = 2/7$ puisque les semi-groupes correspondant sont libres) :



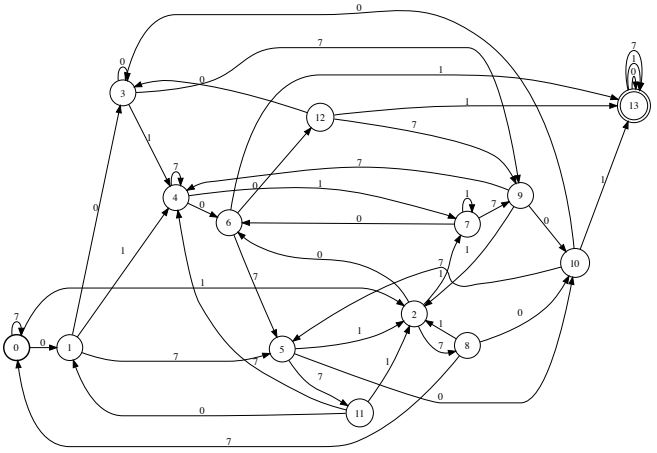
a=1 et b=3



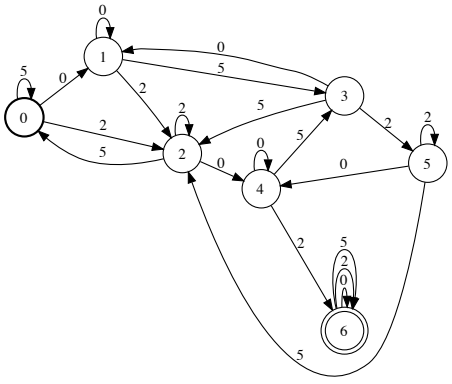
a=1 et b=4



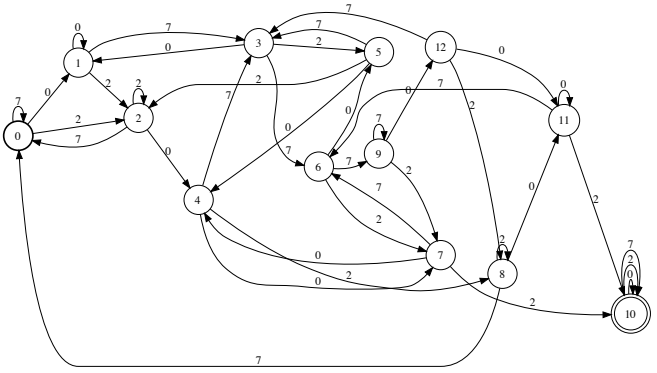
a=1 et b=6



a=1 et b=7



a=2 et b=5



a=3 et b=7

On en déduit facilement les automates des mots réduits et les vitesses de croissance de ces semi-groupes.

Voici la vitesse exponentielle de croissance λ du semi-groupe de Kenyon pour quelques valeurs du paramètre de translation t. On note π_λ le polynôme minimal de λ.

t	λ	π_λ
1/3	2.6180	$x^2 - 3x + 1$
1/4	2.6180	$x^2 - 3x + 1$
2/5	2.8019	$x^3 - 4x^2 + 3x + 1$
1/6	2.7321	$x^2 - 2x - 2$
1/7	2.7383	$x^5 - 3x^4 + x^2 + 3x - 1$
3/7	2.8794	$x^3 - 3x^2 + 1$
3/8	2.8136	$x^3 - 2x^2 - 3x + 2$
1/9	2.6180	$x^2 - 3x + 1$
2/9	2.7233	$x^6 - 3x^5 + x^3 + 3x^2 - 1$
4/9	2.8794	$x^3 - 3x^2 + 1$
1/10	2.6180	$x^2 - 3x + 1$
3/10	2.7699	$x^6 - 2x^5 - 4x^4 + x^3 + 9x^2 + 6x + 3$
2/11	2.7421	$x^5 - 4x^4 + 3x^3 + x^2 + x - 1$
3/11	2.8073	$x^9 - 4x^8 + x^7 + 7x^6 - 9x^3 - x^2 + 3x - 1$
5/11	2.9242	$x^{11} - 5x^{10} + 6x^9 - 7x^8 + 32x^7 - 32x^6 + 15x^5 - 49x^4 + 20x^3 - 13x^2 + 3x - 1$

J'ai donné ici tous les rationnels a/b dans l'intervalle $]0, 1/2[$ ayant un dénominateur inférieur ou égal à 11, avec $a + b \not\equiv 0 \mod 3$. On en déduit facilement les valeurs des vitesses exponentielles de croissance pour tous les rationnels a/b ayant un dénominateur inférieur ou égal à 11. On constate que ces vitesses de croissance sont difficiles à prévoir. Il existe cependant des suites de valeurs de a/b pour lesquelles on connait la vitesse de croissance, comme par exemple les $1/3^n$ et $1/(3^n + 1)$.

III.4.3 Développement β-adique avec ensemble de chiffres $\{0, 1\}$

Considérons le monoïde engendré par les deux transformations affines

$$\begin{cases} 0 : x \mapsto \beta x, \\ 1 : x \mapsto \beta x + 1, \end{cases}$$

où $\beta > 1$ est un réel. Si β est transcendant, le semi-groupe est libre, et donc sa structure automatique est triviale. Supposons que β est algébrique.

Définition III.4.3. *On appelle produit de Mahler (ou mesure de Mahler) d'un nombre algébrique β le produit*

$$m_\beta := \prod_{\substack{v \text{ place de } \mathbb{Q}(\beta) \\ |\gamma|_v > 1}} |\gamma|_v ,$$

où l'on considère les valeurs absolues usuelles du corps de nombres $\mathbb{Q}(\beta)$.

Autrement dit, le produit de Mahler est le produit des modules des conjugués strictements supérieurs à 1 et du coefficient dominant du polynôme minimal de β.

On sait que le semi-groupe est libre quand le nombre algébrique β a un conjugué de module supérieur ou égal à 2 (puisque le semi-groupe avec $\beta > 2$ est de Schottky). Voici une réciproque :

Proposition III.4.4. *Si le produit de Mahler m_β de β est strictement inférieur à 2, alors le semi-groupe n'est pas libre.*

Démonstration. Toutes les valeurs absolues ultramétriques de β sont inférieure ou égales à 1, puisque sinon le produit de Mahler serait trop grand. Le réel β est donc un entier algébrique. On peut donc plonger l'anneau $\mathbb{Z}[\beta]$ dans $\mathbb{R}^d$, de tel façon qu'il y soit un réseau, où d est le degré du nombre algébrique β. Si l'on considère les 2^{n+1} polynômes en β de degré n et à coefficients dans $\{0,1\}$, on remarque qu'ils sont inclus dans un domaine de $\mathbb{R}^d$ qui est de volume majoré par $P(n)m_\beta^n$, pour un certain polynôme P. Comme l'anneau des entiers est un réseau de $\mathbb{R}^d$, ceci nous donne que le nombre d'éléments du semi-groupe de longueur n est majoré par $cP(n)m_\beta^n$, pour une constante $c > 0$, ce qui est strictement inférieur à 2^{n+1} pour n assez grand. D'où l'existence d'une relation non triviale dans le semi-groupe. □

La preuve ci-dessus montre que, sous les hypothèses de la proposition, l'exposant de croissance du semi-groupe est majoré par le produit de Mahler. Dans tous les exemples vérifiant les hypothèses de la proposition que j'ai pu voir, l'exposant de croissance du semi-groupe est même égal au produit de Mahler (i.e. $\delta_\Gamma = \frac{\log(m_\beta)}{\log(\beta)}$).

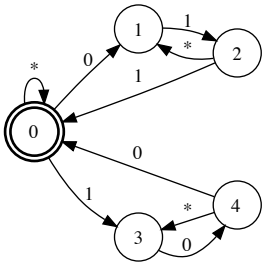
Remarque III.4.5. *Dans le cas particulier où le réel β est strictement inférieur à 2, l'étude du semi-groupe est liée à celle du système dynamique*

$$\begin{array}{rccll} T: & \mathbb{R}/\mathbb{Z} & \to & \mathbb{R}/\mathbb{Z} & \\ & x & \mapsto & \beta x & \mod 1. \end{array}$$

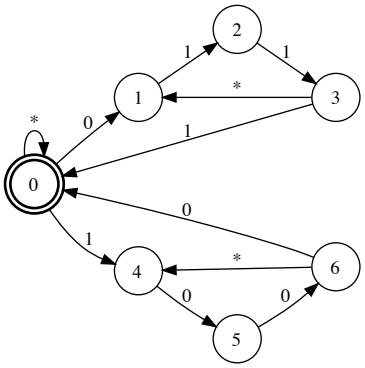
Voici quelques exemples d'automates des relations pour le monoïde engendré par les applications

$$\begin{cases} 0 : x & \mapsto & \beta x, \\ 1 : x & \mapsto & \beta x + 1, \end{cases}$$

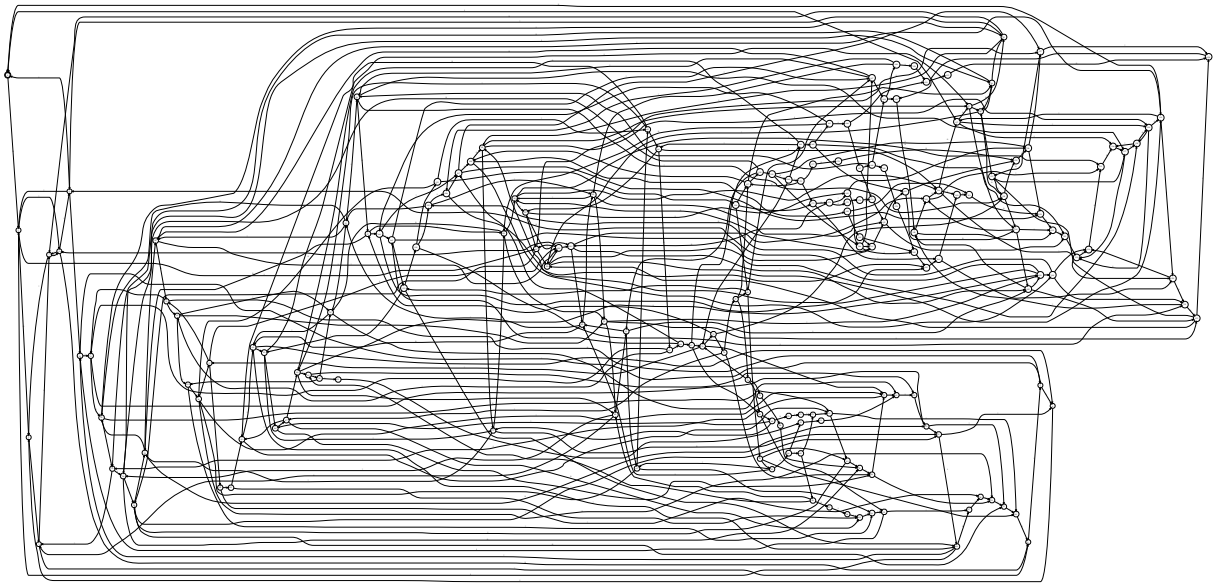
où l'étiquette 0 signifie $(0,1)$, l'étiquette 1 signifie $(1,0)$ et l'étiquette $*$ signifie que l'on a deux arêtes étiquetées respectivement par $(0,0)$ et $(1,1)$.



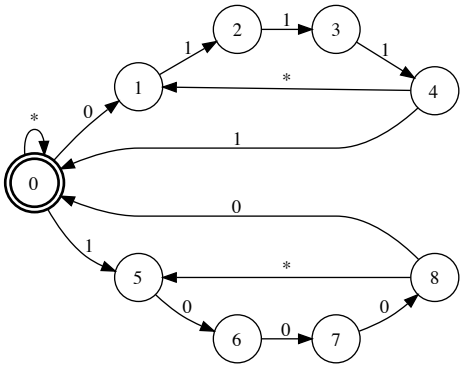
$\pi_\beta = x^2 - x - 1$



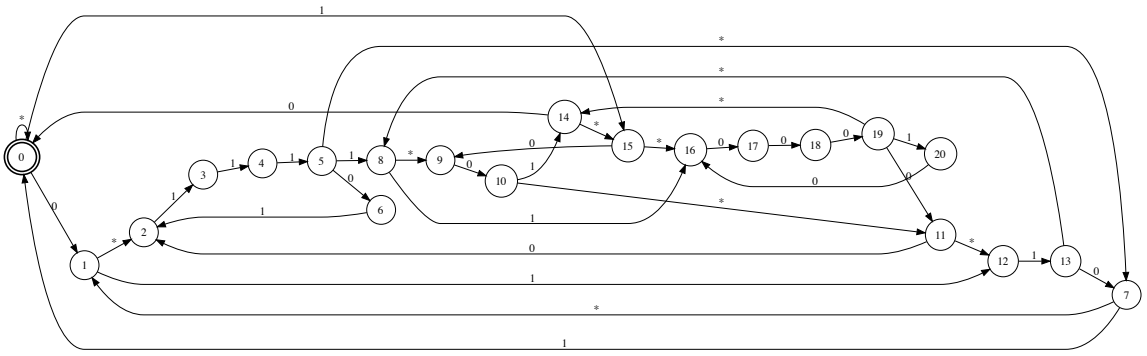
$\pi_\beta = x^3 - x^2 - x - 1$



$\pi_\beta = x^3 - x - 1$



$\pi_\beta = x^4 - x^3 - x^2 - x - 1$



$$\pi_\beta = x^4 - x^3 - x^2 + x - 1$$

Les trois premiers exemples d'automates des relations sont pour des nombres de Pisot, tandis que ce dernier exemple est pour un nombre qui n'est pas de Pisot. On peut voir que ces automates peuvent être très simples, mais aussi très compliqués même pour un des plus simples exemples de nombre de Pisot.

III.4.4 Un cas où β est un nombre transcendant

Considérons le monoïde engendré par les 3 transformations

$$\begin{cases} 0 : x & \mapsto & \beta x, \\ p : x & \mapsto & \beta x + P(\beta), \\ q : x & \mapsto & \beta x + Q(\beta), \end{cases}$$

où β est un nombre transcendant, et P et Q sont deux polynômes à coefficients entiers.

Remarque III.4.6. *On peut supposer que l'on a* $\deg P < \deg Q$ *et* $\mathrm{pgcd}(P, Q) = 1$.

En effet, si l'on a $\deg Q < \deg P$, alors il suffit d'échanger P et Q, et si $\deg P = \deg Q$, alors le monoïde engendré par les transformations

$$\begin{cases} 0 : x & \mapsto & \beta x, \\ p : x & \mapsto & \beta x + (Q - P)(\beta), \\ q : x & \mapsto & \beta x + Q(\beta), \end{cases}$$

est le même. Si maintenant on a $\deg P = \deg Q = \deg(Q - P)$, alors le semi-groupe est libre, puisque l'on ne peut avoir d'égalité non triviale

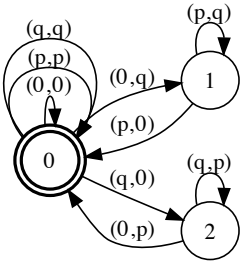
$$\sum_{i=0}^{n} \epsilon_i \beta^i = 0,$$

avec $\epsilon_i \in \{0, P, Q\} - \{0, P, Q\} = \{0, P, Q, -P, -Q, P - Q, Q - P\}$. On peut toujours supposer que les polynômes P et Q sont premiers entre eux quitte à tout diviser par le pgcd.

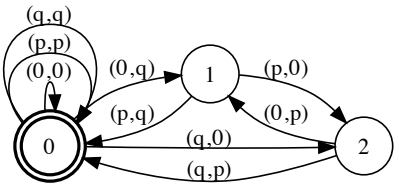
D'après la proposition III.4.2 de Kenyon, le semi-groupe est libre dès que l'on a $P(3) + Q(3) \equiv 0 \mod 3$. Et d'après la preuve du théorème III.3.2, déterminer si le semi-groupe

est libre est toujours décidable, puisque la structure fortement automatique du semi-groupe est calculable. La remarque III.4.8 donne un critère pour déterminer si le semi-groupe est libre. Mais existe-t'il un critère simple pour déterminer si le semi-groupe est libre à partir des polynômes P et Q ?

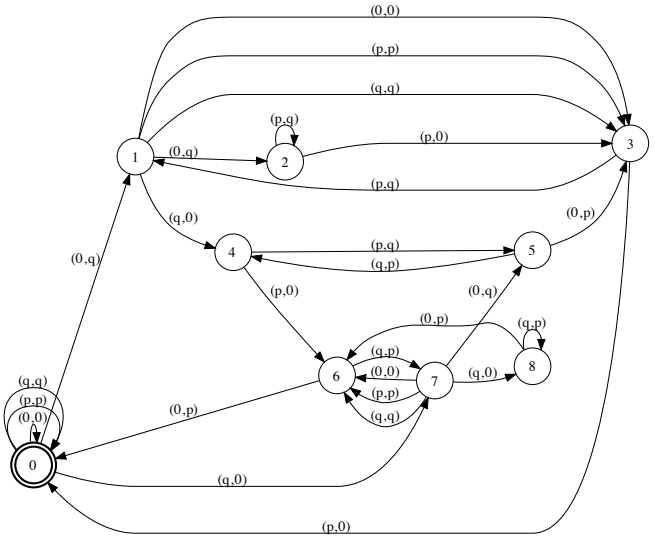
Voici quelques exemples d'automates des relations pour ce semi-groupe



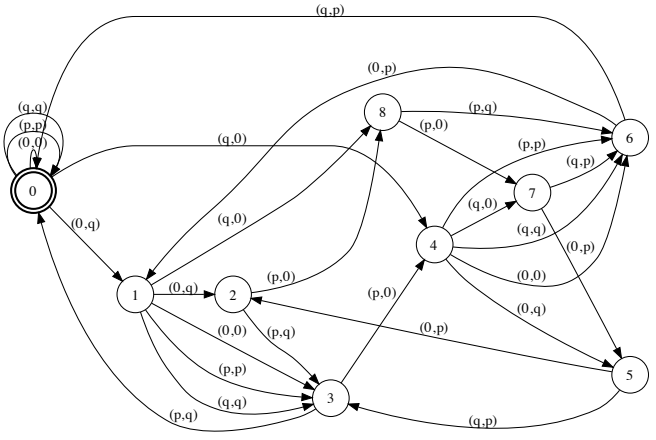
P=1 et Q=X



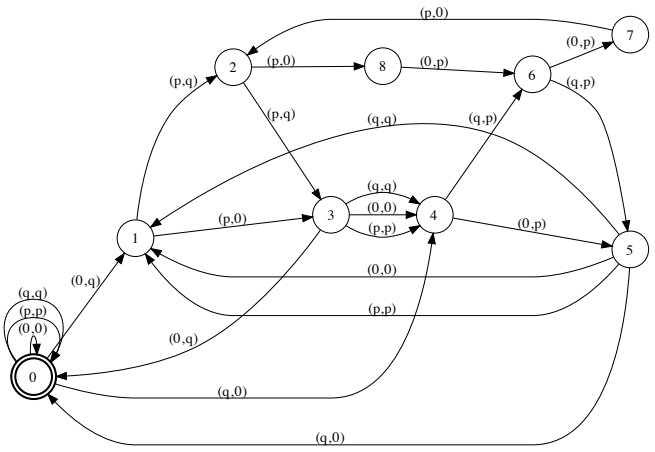
P=1 et Q=X+1



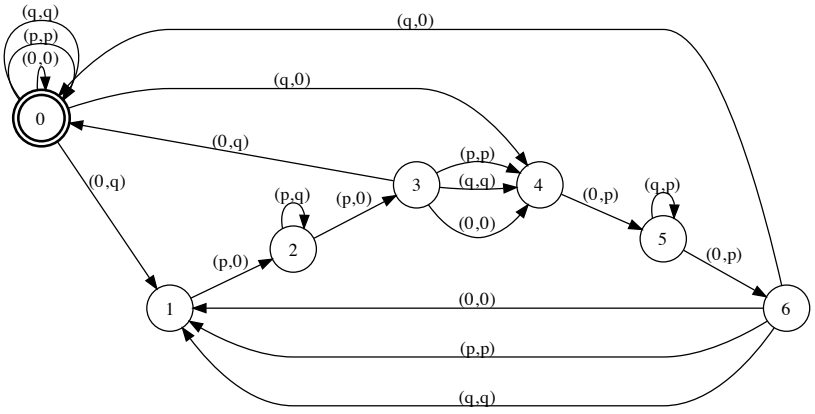
$P = 1$ et $Q = X^2$



$P = 1$ et $Q = X^2 + 1$

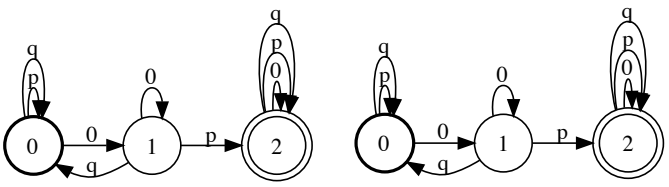


$P = X$ et $Q = X^2 + 1$

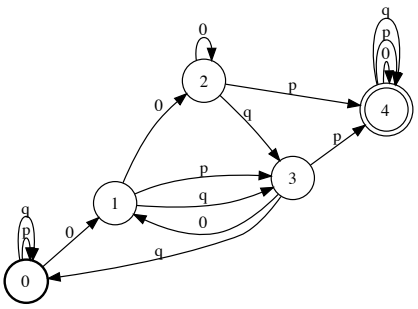


$P = X$ et $Q = X^2 - X + 1$

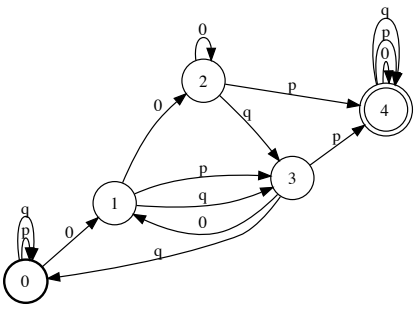
Et voici les automates des mots réduits pour les mêmes exemples :



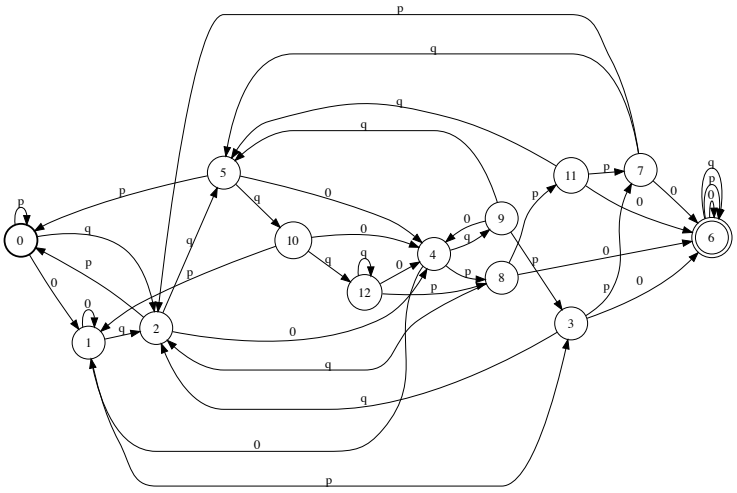
$P = 1$ et $Q = X$ $P = 1$ et $Q = X + 1$



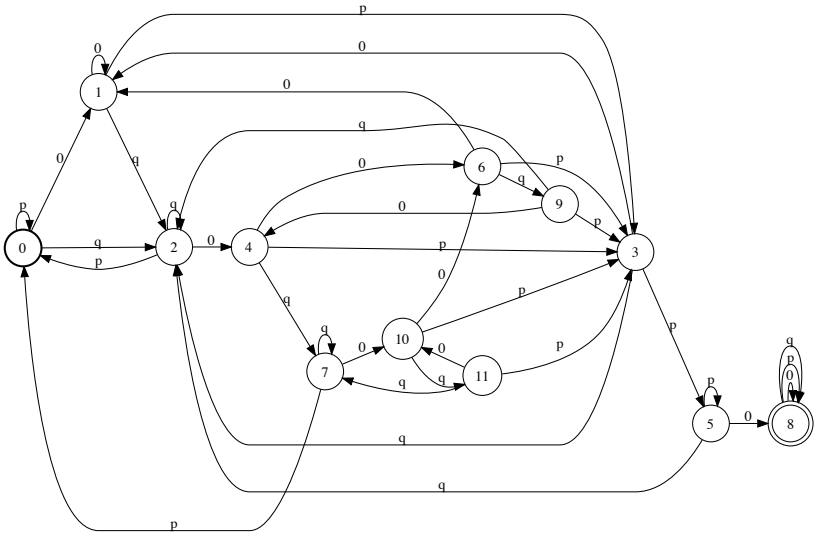
$P = 1$ et $Q = X^2$



$P = 1$ et $Q = X^2 + 1$



$P = X$ et $Q = X^2 + 1$



$P = X$ et $Q = X^2 - X + 1$

Voici les vitesses exponentielles de croissance λ pour quelques exemples, où π_λ est le polynôme minimal de λ :

P/Q	λ	π_λ
$1/X$	2.6180	x^2-3x+1
$1/(X+1)$	2.6180	x^2-3x+1
$1/(X^2-X)$	2.8794	x^3-3x^2+1
$1/(X^2-X+1)$	2.7971	$x^4-2x^3-2x^2-x+1$
$1/X^2$	2.6180	x^2-3x+1
$1/(X^2+1)$	2.6180	x^2-3x+1
$1/(X^2+X)$	2.8794	x^3-3x^2+1
$1/(X^2+X+1)$	2.7693	x^3-3x^2+x-1
$(X-1)/X^2$	2.7971	$x^4-2x^3-2x^2-x+1$
$(X-1)/(X^2+X-1)$	2.8794	x^3-3x^2+1
$1/(X^3-X^2-X)$	2.9615	x^4-3x^3+1
$1/(X^3-X^2)$	2.8584	$x^7-3x^6+3x^3+x^2-1$
$1/(X^3-X^2+1)$	2.8396	$x^{10}-3x^9+3x^6+x^5+4x^4-3x^3-3x^2+1$
$1/(X^3-X^2+X)$	2.8444	$x^{13}-3x^{12}-2x^{11}+7x^{10}-2x^9+7x^8-$ $16x^6+6x^5-6x^3+8x^2+x-2$

On remarque qu'à nouveau ces vitesses exponentielles de croissance sont difficiles à prévoir, mais qu'il y a tout de même des valeurs particulières pour lesquelles on les connait (par exemple les $1/X^n$).

Remarque III.4.7. *La vitesse exponentielle de croissance du semi-groupe pour β transcendant majore celle du semi-groupe pour β algébrique. Pour l'exemple de l'introduction (qui correspond aux polynômes $P=1$ et $Q=X$), le caractère algébrique de $1/3$ n'a aucun rôle : le semi-groupe est le même (d'un point de vue combinatoire) en prenant β transcendant plutôt que $\beta=1/3$. Cependant, les semi-groupes diffèrent quand on prend par exemple $P=X$ et $Q=X^2-X+1$ suivant que $\beta=1/3$ ou que β est transcendant.*

Remarque III.4.8. *Le semi-groupe n'est pas libre si et seulement si l'on a $P/Q=A/B$ pour deux polynômes $A,B\in\{-1,0,1\}[X]$ et avec $A-B\in\{-1,0,1\}[X]$. C'est pourquoi tous les exemples considérés ci-dessus sont de cette forme.*

Chapitre IV

Construction de fractions continues périodiques uniformément bornées

Dans ce chapitre, nous nous intéressons aux fractions continues bornées. Ces dernières sont reliées à certains semi-groupes de matrices par l'équivalence :

$$\Updownarrow \begin{matrix} \begin{pmatrix}0 & 1\\ 1 & a_1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & a_2\end{pmatrix}\dots\begin{pmatrix}0 & 1\\ 1 & a_k\end{pmatrix} = \begin{pmatrix}* & p\\ * & q\end{pmatrix} \\ \frac{q}{p} = [a_1, a_2, ..., a_k], \end{matrix}$$

qui fait correspondre à tout rationnel une matrice de $GL_2(\mathbb{Z})$.

On a aussi une correspondance entre ces mêmes matrices et les fractions continues périodiques :

$$\Updownarrow \begin{matrix} \begin{pmatrix}1\\ x\end{pmatrix} \text{ est vecteur propre de } \begin{pmatrix}0 & 1\\ 1 & a_1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & a_2\end{pmatrix}\dots\begin{pmatrix}0 & 1\\ 1 & a_k\end{pmatrix} \quad . \\ x = [\overline{a_1, a_2, ..., a_k}], \end{matrix}$$

Ainsi l'étude des conjectures suivantes se ramène à celle de certains sous-semi-groupes de type fini de $GL_2(\mathbb{Z})$.

Voici une conjecture de Zaremba sur les rationnels dont le développement en fraction continue est borné.

Conjecture IV.0.9 (Zaremba)**.** *Il existe une constante m telle que pour tout dénominateur $q \geq 1$, il existe un numérateur p premier à q tel que l'on ait*

$$\frac{p}{q} = [a_0, a_1, a_2, \dots]$$

où les entiers a_i sont entre 0 et m.

Et voici un équivalent pour les fractions continues périodiques.

Conjecture IV.0.10 (McMullen)**.** *Il existe un réel m tel que tout corps quadratique réel $\mathbb{Q}[\sqrt{\delta}]$ contient une infinité de fractions continues périodiques uniformément bornées par m.*

McMullen propose même la conjecture plus forte suivante.

Conjecture IV.0.11 (McMullen)**.** *Tout corps quadratique réel $\mathbb{Q}[\sqrt{\delta}]$ contient une infinité de fractions continues périodiques ne comportant que les entiers* 1 *et* 2*.*

Nous obtenons deux moyens de construire des fractions continues périodiques bornées dans les corps quadratiques. Le premier permet d'obtenir des suites de fractions continues périodiques uniformément bornées dans un cops quadratique réel donné, à partir d'une fraction continue périodique particulière. Plus précisément, on a le résultat suivant.

Théorème IV.0.12. *Si la fraction continue périodique quasi-palindromique*

$$[\overline{a_0, a_1, a_2, ..., a_2, a_1}]$$

est dans $\mathbb{Q}[\sqrt{\delta}]$, alors il existe deux uplets d'entiers strictement positifs $(b_1, b_2, ..., b_k)$ et $(c_1, c_2, ..., c_l)$ tels que $\mathbb{Q}[\sqrt{\delta}]$ contienne la suite non constante de fractions continues périodiques

$$[\overline{b_1, b_2, ..., b_k, (a_0, a_1, a_2, ..., a_2, a_1)^n, c_1, c_2, ..., c_l, (a_1, a_2, ..., a_2, a_1, a_0)^n}]$$

En outre, si m est un majorant des entiers a_i, alors on peut demander à ce que $2m+1$ soit un majorant des entiers b_i et c_i.

Le deuxième moyen que nous proposons, pour construire des fractions continues périodiques dans un corps quadratique donné, consiste à considérer le développement en fraction continue d'un rationnel, et fournit une fraction continue périodique dont les coefficients sont très proches de ceux du rationnel, et dans un corps quadratique qui ne dépend que du dénominateur du rationnel. Plus précisément, on a le théorème suivant.

Théorème IV.0.13. *Soient a, b, c et δ des entiers strictement positifs tels que*
- *b et c sont solution de l'équation de Pell-Fermat : $c^2 - \delta b^2 = \pm 1$,*
- *a et c sont premiers entre eux et $a \leq c$.*

Alors on a l'une des égalités

$$\frac{c - a + b\sqrt{\delta}}{c} = [\overline{1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n, 1, 1, a_n - 1, a_{n-1}, a_{n-2}, \ldots, a_2, a_1}]$$

ou

$$\frac{c - a + b\sqrt{\delta}}{c} = [\overline{1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n - 1, 1, 1, a_n, a_{n-1}, a_{n-2}, \ldots, a_2, a_1}],$$

où $[0, a_1, a_2, \ldots, a_{n-1}, a_n]$ est le développement en fraction continue du rationnel $\frac{a}{c}$.

Si l'on a des entiers nuls dans la fraction continue donnée par ce théorème (c'est le cas si $a_1 = 1$ ou $a_n = 1$), il suffit de remplacer chaque triplet $x, 0, y$ par $x + y$ pour obtenir une vraie fraction continue. Ces deux théorèmes nous permettent de petites avancées dans la résolution des conjectures de Zaremba et de McMullen, puisqu'ils permettent d'obtenir les résultats :

Théorème IV.0.14. *Il existe une infinité de corps quadratiques réels dans lesquels il existe une infinité de fraction continues périodiques bornées par* 2.

Théorème IV.0.15. *La conjecture IV.0.9 de Zaremba implique la conjecture IV.0.10 de McMullen.*

Voici le plan de ce chapitre :

Nous commençons dans la section IV.1 par donner quelques propriétés des matrices positives, qui sont les matrices de $GL_2(\mathbb{Z})$ qui correspondent à des fractions continues périodiques. Nous donnons ensuite dans la section IV.2 une preuve rapide du théorème IV.0.12 qui permet de construire des suites de fractions continues continues périodiques dans un corps quadratique donné, à partir d'une fraction continue périodique d'une forme particulière. Nous montrons dans la section IV.3 que les suites de fractions continues de la forme $[\overline{b_1, b_2, ..., b_k(a_1, a_2, ..., a_l)^n}]$ qui restent dans un corps quadratique donné, sont nécessairement triviales. Nous expliquons ensuite dans la section IV.4 pourquoi il y a beaucoup de fraction continues de la forme $[\overline{\mathsf{BAC}\,{}^t\mathsf{A}}]$ dans un corps quadratique donné, où A, B et C sont des motifs, et ${}^t\mathsf{A}$ est le motif A en ordre inverse. La section IV.5 s'intéresse aux suites de fractions continues périodiques de la forme $[\overline{\mathsf{BA}^n\mathsf{C}\,{}^t\mathsf{A}^n}]$. Nous y redémontrons le théorème IV.0.12. La section IV.6 explicite les suites de fractions continues périodiques données par le théorème IV.0.12 et donne des exemples. Nous démontrons en particulier le théorème IV.0.14. Enfin, dans la section IV.7, nous nous intéressons à la conjecture de Zaremba. Nous commençons par montrer que la conjecture est fausse si l'on se restreint à des ensembles de quotients partiels qui donnent des semi-groupes de matrices trop petit. Nous démontrons ensuite le théorème IV.0.13 permettant de construire des fractions continues périodiques dans un corps quadratique donné, à partir des développement en fractions continues de rationnels de dénominateur fixé. Nous montrons aussi le théorème IV.0.15 qui ramène la conjecture IV.0.10 de McMullen à celle IV.0.9 de Zaremba.

Mais commençons par introduire quelques notations que l'on utilisera dans tout le chapitre.

Notations

Tout réel x peut se développer en fraction continue

$$x = [a_1, a_2, a_3, ...] := a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}$$

avec des quotients partiels $a_i \in \mathbb{Z}$ et $a_i \geq 1$ si $i \geq 2$. Si le développement est périodique (c'est-à-dire s'il existe un entier p tel que pour tout i, on ait $a_i = a_{i+p}$),
on notera $x = [\overline{a_1, a_2, ..., a_p}]$.

Définition IV.0.16. *On appellera quasi-palindromique une fraction continue de la forme* $[\overline{a_0, a_1, a_2, a_3, ..., a_3, a_2, a_1}]$.

Dans cette définition, la partie symétrique $a_1, a_2, ..., a_2, a_1$ peut ou non avoir un terme médian. Dans la suite, la notation $(a_0, a_1, a_2, ..., a_{k-1}, a_k)^n$ signifie que le motif

$$a_0, a_1, a_2, ..., a_{k-1}, a_k$$

est répété n fois.

IV.1 Matrices positives

Dans cette section, on s'intéresse au semi-groupe Γ des matrices positives, qui est l'ensemble des matrices de $GL_2(\mathbb{Z})$ qui correspondent à un développement en fraction continue périodique. On démontre des propriétés qui serviront par la suite.

Définition IV.1.1. *Soit M une matrice de $M_2(\mathbb{R})$. On appelle discriminant de M le discriminant du polynôme caractéristique de M. Autrement dit, c'est le réel*

$$\mathrm{discr}(M) := (d-a)^2 + 4bc = \mathrm{Tr}(M)^2 - 4\,\mathrm{Det}(M),$$

pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Propriétés IV.1.2. *Soit M une matrice de $GL_2(\mathbb{Z})$.*

1. *Les valeurs propres de M sont dans le corps $\mathbb{Q}[\sqrt{\mathrm{discr}(M)}]$.*
2. *Les vecteurs propre de M peuvent être choisis à coefficients dans le corps $\mathbb{Q}[\sqrt{\mathrm{discr}(M)}]$.*
3. *Pour tout $n \geq 1$, $\mathrm{discr}(M)$ divise $\mathrm{discr}(M^n)$ et $\frac{\mathrm{discr}(M^n)}{\mathrm{discr}(M)}$ est un carré parfait.*

Démonstration. 1 . Les valeurs propres sont les racines du polynôme caractéristique, donc sont dans $\mathbb{Q}[\sqrt{\mathrm{discr}(M)}]$.
2 . Si l'on choisis un vecteur propre de la forme $\begin{pmatrix} 1 \\ x \end{pmatrix}$, alors x est racine du polynôme $bx^2+(a-d)x-c=0$, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Or ce polynôme a pour discriminant $\mathrm{discr}(M)$, et donc x est dans $\mathbb{Q}[\sqrt{\mathrm{discr}(M)}]$.
3 . Si λ et μ sont les deux valeurs propres de M, alors $\mathrm{discr}(M^n) = (\lambda^n - \mu^n)^2$. On a donc

$$\frac{\mathrm{discr}(M^n)}{\mathrm{discr}(M)} = (\frac{\lambda^n - \mu^n}{\lambda - \mu})^2 = (\sum_{i=0}^{n-1} \lambda^i \mu^{n-i-1})^2.$$

Or, l'expression $\sum_{i=0}^{n-1} \lambda^i \mu^{n-i-1}$ est un polynôme à coefficients entiers, symétrique en λ et μ. C'est donc aussi un polynôme à coefficients entiers en la trace et le déterminant de M. Donc le nombre complexe $\sum_{i=0}^{n-1} \lambda^i \mu^{n-i-1}$ est en fait un entier. □

IV.1.1 Notations

- On appelle *corps d'une matrice* $M \in GL_2(\mathbb{Z})$ le corps $\mathbb{Q}[\sqrt{\text{discr}(M)}]$.
- On note T_i la matrice $\begin{pmatrix} 0 & 1 \\ 1 & i \end{pmatrix}$ où i est un entier, et on note $T_{(a_1,a_2,...,a_n)}$ le produit $T_{a_1}T_{a_2}...T_{a_n}$ pour un n-uplet d'entiers $(a_1, a_2, ..., a_n)$. Cette notation est justifiée par la remarque IV.1.4.
- On note Γ l'ensemble des produits des matrices T_i pour $i \geq 1$ (Γ est donc le monoïde engendré par les matrices T_i, et il contient I_2), et Γ_n l'ensemble des produits de matrices T_i pour $1 \leq i \leq n$. On dit qu'une matrice est *positive* si c'est un élément du semi-groupe $\Gamma\backslash\{I_2\}$. En particulier, une matrice positive a tous ses coefficients positifs ou nuls.
- Étant donnée une matrice $P \in M_2(\mathbb{R})$, on note $P^\dagger$ l'unique matrice vérifiant $P+P^\dagger = \text{Tr}(P)I_2$. Si $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a donc $P^\dagger = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Et si P est inversible, on peut écrire $P^\dagger = \text{Det}(P)P^{-1}$.
  Les relations $P^\dagger Q^\dagger = (QP)^\dagger$ et $PP^\dagger = \text{Det}(P)I_2$ permettent d'obtenir l'égalité bien utile :

$$\text{Det}(P+Q) = \text{Det}(P) + \text{Det}(Q) + \text{Tr}(PQ^\dagger) \tag{IV.1}$$

- On appelle *longueur* d'une fraction continue périodique la plus petite période.

Proposition IV.1.3 (Critère de positivité)**.** *Soit* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$.

Alors les propriétés suivantes sont équivalentes :

1. $M \in \Gamma\backslash\{I_2\}$ *(i.e. M est positive)*
2. $0 \leq a \leq b \leq d$ *et* $a \leq c \leq d$
3. *Il existe un réel quadratique* $x_M > 1$*, dont le conjugué* $\overline{x_M}$ *est dans* $]-1, 0[$*, tel que* $\begin{pmatrix} 1 \\ x_M \end{pmatrix}$ *et* $\begin{pmatrix} 1 \\ \overline{x_M} \end{pmatrix}$ *soient des vecteurs propres de M, et les entiers b et d sont strictement positifs.*
4. $|b-c| < d-a$ *et les entiers a, b, c et d sont positifs ou nuls.*

Démonstration. 1 $\Rightarrow$ 2 Récurrence facile.

2 $\Rightarrow$ 1 Supposons que M vérifie ces inégalités. Démontrons que M est positive par récurrence sur ses coefficients.

Si $a = 0$, alors $bc = -\text{Det}(M) = \pm 1$, donc $b = c = 1$ et $M = \begin{pmatrix} 0 & 1 \\ 1 & d \end{pmatrix} = T_d$.

Si $a = 1$, alors M est de la forme

$$M = \begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix} = T_c T_b \text{ quand } \text{Det}(M) = 1,$$
$$M = \begin{pmatrix} 1 & b \\ c & bc-1 \end{pmatrix} = T_{c-1} T_1 T_{b-1} \text{ quand } \text{Det}(M) = -1.$$

Si $a \geq 2$, alors on a $\left\lfloor \frac{b}{a} \right\rfloor = \left\lfloor \frac{d}{c} \right\rfloor$ (cela découle de l'égalité $ad - bc = \pm 1$). Et en posant $q = \left\lfloor \frac{b}{a} \right\rfloor = \left\lfloor \frac{d}{c} \right\rfloor$, la matrice $MT_q^{-1} = \begin{pmatrix} b - qa & a \\ d - qc & c \end{pmatrix}$ vérifie encore le point 2 de la proposition : l'inégalité $b - qa \leq d - qc$ résulte de $\mathrm{Det}(M \cdot T_q^{-1}) = \pm 1$ et de $2 \leq a \leq c$, et les autres inégalités sont claires. De plus, la matrice MT_q^{-1} est strictement plus petite que M, coefficients à coefficients.

2 $\Rightarrow$ 4 Clair.

3 $\Leftrightarrow$ 4 Les réels quadratiques x_M et $\overline{x_M}$ sont les racines du polynôme $Q(X) = bX^2 + (a-d)X - c$. Si b est positif, on a donc,

$$\left\{ \begin{array}{c} x_M > 1 \\ -1 < \overline{x_M} < 0 \end{array} \right. \iff \left\{ \begin{array}{c} Q(1) < 0 \\ Q(-1) > 0 \\ Q(0) < 0 \end{array} \right. \iff \left\{ \begin{array}{c} |b-c| < d - a \\ c > 0 \end{array} \right. \tag{IV.2}$$

Et l'égalité $bc = 0$ est impossible si $|b - c| < d - a$, puisque si elle avait lieu, alors l'égalité $ad - bc = \pm 1$ et la positivité de a et de d entraîneraient que $a = d = 1$.

4 $\Rightarrow$ 3 On a $b > 0$ et $c > 0$, parce que bc est non nul. On peut donc utiliser l'équivalence (IV.2) ci-dessus pour obtenir $x_M > 1$ et $-1 < \overline{x_M} < 0$. On a ensuite $|b - c| < d - a$ qui entraîne $d > 0$.

3 $\Rightarrow$ 4 L'équivalence (IV.2) ci-dessus nous donne $|b - c| < d - a$ et $c > 0$. L'égalité $ad - bc = \pm 1$ et l'inégalité $bc > 0$ donnent alors que $ad \geq 0$, d'où $a \geq 0$.

4 $\Rightarrow$ 2 Si l'on avait $c < a$, on aurait $cd < ad = bc \pm 1$, donc $cd \leq bc$ puis $d \leq b$. Mais la différence $d - a < b - c$ des inégalités contredirai alors l'hypothèse $|b - c| < d - a$. Les autres inégalités $a \leq b$, $c \leq d$ et $b \leq d$ s'obtiennent de la même façon. □

Remarque IV.1.4. *Le réel x_M de la proposition ci-dessus qui correspond à une matrice*

$$M = T_{(a_1,a_2,a_3,\ldots,a_p)} = T_{a_1} T_{a_2} T_{a_3} \ldots T_{a_p},$$

a pour développement en fraction continue

$$x_M = [\overline{a_1, a_2, a_3, \ldots, a_p}].$$

La correspondance est bijective si l'entier p est la longueur.

Définition IV.1.5. *Une suite (A_n) de matrices est non triviale si l'ensemble des réels x_{A_n} est infini (ce qui signifie simplement que la suite de matrices correspond à une infinité de fractions continues périodiques).*

Remarque IV.1.6. *Il y a unicité de l'écriture d'une matrice de Γ comme produit de matrices T_i. En particulier, une matrice de Γ est symétrique si et seulement si son écriture comme produit de matrices T_i est symétrique.*

Les matrices positives sont toujours diagonalisables et ont des valeurs propres réelles distinctes.

Pour démontrer l'unicité de la décomposition $M = T_{i_1}T_{i_2}...T_{i_n}$ d'une matrice positive $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, il suffit de remarquer que la dernière matrice $T_{i_n} = \begin{pmatrix} 0 & 1 \\ 1 & i_n \end{pmatrix}$ s'obtient par la formule

$$i_n = \min(\left\lfloor \frac{b}{a} \right\rfloor, \left\lfloor \frac{d}{c} \right\rfloor),$$

avec la convention $\left\lfloor \frac{b}{0} \right\rfloor = \infty$. Voir la preuve de la proposition IV.1.3 pour plus de détails.

On dispose également d'un critère de positivité pour les matrices de rang 1 :

Proposition IV.1.7. *Soit* $H = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ *une matrice de rang 1 vérifiant les inégalités* $0 \leq a \leq b \leq d$ *et* $a \leq c \leq d$. *Alors il existe deux matrices* P *et* Q *dans* Γ *et un entier* $e \geq 1$ *tels que* $H = P \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} Q$. *De plus,* e *est unique, et* P *et* Q *sont uniques modulo les relations*

$$XT_nT_1 \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} Y = XT_{n+1} \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} Y$$
$$X \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} T_1T_nY = X \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} T_{n+1}Y$$

pour $X, Y \in \Gamma$.

Démonstration. On a nécessairement $e = \text{pgcd}(a, b, c, d)$, d'où son unicité. On peut supposer $e = 1$ quitte à diviser H par e. Comme H est non inversible, il existe des entiers positifs ou nuls x, y, z et t tels que $H = \begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} z & t \end{pmatrix}$ et avec x et y premiers entre eux, et z et t premiers entre eux.

La matrice P est nécessairement de la forme $P = \begin{pmatrix} u & x \\ v & y \end{pmatrix}$ pour être dans $GL_2(\mathbb{Z})$, puisque les coefficients x et y doivent être premiers entre eux. Déterminons toutes les valeurs possibles des entiers u et v pour que la matrice P soit dans Γ.

- Si $x = 0$, alors on a nécessairement $y = 1$, et donc $(u, v) = (1, 0)$ convient et est la seule solution.
- Si $x = 1$, alors les solutions sont $(u, v) = (0, 1)$ et $(u, v) = (1, y - 1)$ (le couple $(u, v) = (1, y - 1)$ est bien une solution à condition que $y \geq 2$).
- Si $x \geq 2$, alors les solutions (u, v) vérifient nécessairement les inégalités $0 \leq u < x$ et $0 \leq v < y$. Le théorème de Bézout nous donne alors l'existence et l'unicité d'une solution (u, v) vérifiant les inégalités $0 \leq u < x$ et $0 \leq v < y$ et l'équation $uy - vx = 1$, et de même pour l'équation $uy - vx = -1$. L'inégalité $u \leq v$ est alors automatiquement bien vérifiée. On a donc exactement deux solutions.

D'autre part, il est facile de vérifier que l'on a les égalités

$$T_nT_1\begin{pmatrix}0&0\\0&e\end{pmatrix}=T_{n+1}\begin{pmatrix}0&0\\0&e\end{pmatrix}\text{ et que }\begin{pmatrix}0&0\\0&e\end{pmatrix}T_1T_n=\begin{pmatrix}0&0\\0&e\end{pmatrix}T_{n+1}$$

dès que $n\geq 1$, d'où le résultat. Par transposition, on obtient également les matrices Q qui conviennent. □

IV.2 Preuve du théorème I.2.5

Dans cette partie, nous démontrons le théorème I.2.5. Pour cela, nous commençons par le reformuler en termes de matrices :

Théorème IV.2.1. *Soit $A=MN$ avec M et N deux matrices symétriques de Γ_q telles que l'une d'elles est de déterminant -1. Alors il existe des matrices B et C dans Γ_{2q+1} telles que pour tout n, le corps de $BA^nC\,{}^tA^n$ est le corps de A, et telles que la suite $BA^nC\,{}^tA^n$ est non triviale.*

Remarque IV.2.2. *Une matrice de la forme MN, avec $M,N\in\Gamma$ symétriques et $\mathrm{Det}(M)=-1$ ou $\mathrm{Det}(N)=-1$, est toujours semblable (en faisant une permutation circulaire sur les entiers strictement positifs $m_1,\dots,m_n$ qui apparaissent dans la décomposition $MN=T_{m_1}\dots T_{m_n}$) à une matrice de la forme T_kM', $k\geq 1$, $M'\in\Gamma$ symétrique. L'énoncé du théorème IV.2.1 n'est donc pas plus général que celui du théorème I.2.5.*

Toute la suite du chapitre est consacrée à la preuve du théorème IV.2.1, qui est équivalent au théorème I.2.5.

Preuve du théorème IV.2.1. Soient M et N deux matrices de Γ, avec $\mathrm{Det}(M)=-1$ (on peut toujours se ramener à ce cas, quitte à tout transposer). Pour tout entier k, posons

$$H_k:=H_k(M,N)=MS_0+(MN)^{2k},$$

où $S_0=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$.

Lemme IV.2.3. *Pour toute matrice symétrique $P\in M_2(\mathbb{R})$, on a $\mathrm{Tr}(S_0P)=0$.*

Démonstration. On a $\mathrm{Tr}(S_0P)=\mathrm{Tr}({}^t(S_0P))=\mathrm{Tr}(-PS_0)=-\mathrm{Tr}(S_0P)$. □

Lemme IV.2.4. *Pour tout entier k, H_k est de rang 1.*

Démonstration. D'après la formule (IV.1) (page 139), on a

$$\mathrm{Det}(H_k)=\mathrm{Det}(MS_0)+\mathrm{Det}((MN)^{2k})+\mathrm{Tr}(MS_0((MN)^{2k})^\dagger),$$

et ici on a $((MN)^{2k})^\dagger=(MN)^{-2k}$ puisque $\det(MN)=\pm1$.
Or on a d'une part $\mathrm{Tr}(MS_0(MN)^{-2k})=\mathrm{Tr}(S_0(MN)^{-2k}M)=0$ puisque $(MN)^{-2k}M$ est

symétrique, et d'autre part $\mathrm{Det}(MS_0) = -1$ puisque $\mathrm{Det}(M) = -1$. Et comme on a de plus $\mathrm{Det}((MN)^{2k}) = 1$, le déterminant de la matrice H_k est finalement nul. La non nullité de H_k est claire, puisque la matrice $-S_0$ n'est ni dans Γ ni dans Γ^{-1}. □

Lemme IV.2.5. *Pour toute matrice $C \in M_2(\mathbb{R})$, on a $CS_0\,{}^tC = \mathrm{Det}(C)S_0$.*

Démonstration. Vérification facile. □

Lemme IV.2.6. *Pour k assez grand, la matrice H_k s'écrit*

$$H_k = FT_i \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} T_j G$$

où i et j sont des entiers supérieurs ou égaux à 2, F et G sont des matrices de Γ et e est un entier supérieur ou égal à 1.

Démonstration. Quitte à prendre k supérieur ou égal à 3, la matrice $N(MN)^{2k-1}$ a tous ses coefficients supérieurs ou égaux à 3 (le quatrième nombre de Fibonacci) qui est strictement supérieur à 1. Et donc si l'on pose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = N(MN)^{2k-1}$, alors on a les inégalités strictes $0 < a < b < d$ et $a < c < d$. Les mêmes inégalités mais larges sont alors satisfaites pour la matrice $S_0 + N(MN)^{2k-1}$, et elles le sont donc encore pour la matrice $H_k = M(S_0 + N(MN)^{2k-1})$
(i.e. si $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = H_k$, alors on a $0 \leq a' \leq b' \leq d'$ et $a' \leq c' \leq d'$).

D'après la proposition IV.1.7, la matrice H_k s'écrit alors $H_k = P \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} Q$ pour des matrices P, Q dans Γ et un entier $e \geq 1$. On a ensuite

$$H_{k+2} = M(S_0 + N(MN)^{2k+3}) = MNMNM(S_0 + N(MN)^{2k-1})MNMN$$

ce qui donne $H_{k+2} = MNMNH_kMNMN$. Les relations données dans la proposition IV.1.7 permettent alors d'obtenir H_{k+2} de la forme annoncée (c'est-à-dire avec $i \geq 2$ et $j \geq 2$), puisque $MNMN \in \Gamma \backslash \{I_2, T_1\}$. □

On fixe k assez grand et F, G, i, j et e pour avoir $H_k = FT_i \begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix} T_j G$ comme dans le lemme IV.2.6. Introduisons les matrices suivantes

$$B = \begin{cases} {}^tGT_{(j-1,1,e-1,j)}G & \text{si} \quad \mathrm{Det}(G) = 1 \\ {}^tGT_{(j,e-1,1,j-1)}G & \text{si} \quad \mathrm{Det}(G) = -1 \end{cases}$$

$$C = \begin{cases} FT_{(i-1,1,e-1,i)}\,{}^tF & \text{si} \quad \mathrm{Det}(F) = 1 \\ FT_{(i,e-1,1,i-1)}\,{}^tF & \text{si} \quad \mathrm{Det}(F) = -1 \end{cases}$$

Lemme IV.2.7.

1. *Les matrices B et C sont dans Γ.*

2. *Chaque matrice B et C s'écrit sous la forme $N-S_0$, où N est une matrice symétrique de rang 1.*

Démonstration. 1. Si $e > 1$, les matrices B et C sont clairement dans Γ, et si $e = 1$, l'égalité $T_{(a,0,b)} = T_{a+b}$, pour des entiers a et b, montre que B et C sont encore dans Γ.

2. Pour $k \geq 1$, la matrice $T_{(k-1,1,e-1,k)} = \begin{pmatrix} e & ek+1 \\ ek-1 & ek^2 \end{pmatrix}$ s'écrit sous la forme $N - S_0$ avec N symétrique de rang 1. On a donc, pour une matrice K de Γ, ${}^tKT_{(k-1,1,e-1,k)}K = {}^tKNK - \mathrm{Det}(K)S_0$ d'après le lemme IV.2.5, et la matrice ${}^tKNK$ est encore symétrique de rang 1. On obtient donc bien le résultat.

□

Lemme IV.2.8. *Pour toute matrice $A \in M_2(\mathbb{R})$, on a les deux égalités*

$$\mathrm{Tr}(BAC\,{}^tA) = (\mathrm{Tr}(H_kA))^2 - 2\,\mathrm{Det}(A),$$

$$\mathrm{discr}(BAC\,{}^tA) = (\mathrm{Tr}(H_kA))^2((\mathrm{Tr}(H_kA))^2 - 4\,\mathrm{Det}(A)).$$

Démonstration. On peut écrire B et C sous la forme : $B = b_0\,{}^tb_0 - S_0$ et $C = c_0\,{}^tc_0 - S_0$ pour des vecteurs $b_0, c_0 \in M_{2,1}(\mathbb{R})$ définis par $b_0 = {}^tG\begin{pmatrix} \sqrt{e} \\ j\sqrt{e} \end{pmatrix}$ et $c_0 = F\begin{pmatrix} \sqrt{e} \\ i\sqrt{e} \end{pmatrix}$. On a alors $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}(b_0\,{}^tb_0Ac_0\,{}^tc_0\,{}^tA) + \mathrm{Tr}(S_0AS_0\,{}^tA)$ (les deux termes $\mathrm{Tr}(S_0Ac_0\,{}^tc_0\,{}^tA)$ et $\mathrm{Tr}(b_0\,{}^tb_0AS_0\,{}^tA)$ sont nuls puisque les matrices $Ac_0\,{}^tc_0\,{}^tA$ et ${}^tAb_0\,{}^tb_0A$ sont symétriques). On a ensuite
$\mathrm{Tr}(b_0\,{}^tb_0Ac_0\,{}^tc_0\,{}^tA) = ({}^tb_0Ac_0)^2 = \mathrm{Tr}(c_0\,{}^tb_0A)^2$, et $\mathrm{Tr}(S_0AS_0\,{}^tA) = -2\,\mathrm{Det}(A)$. On vérifie que l'on a $c_0\,{}^tb_0 = H_k$, et on a alors obtenue la première égalité.

La deuxième égalité s'en déduit alors facilement :

$$\begin{aligned}\mathrm{discr}(BAC\,{}^tA) &= \mathrm{Tr}^2(BAC\,{}^tA) - 4\,\mathrm{Det}(BAC\,{}^tA) \\ &= \mathrm{Tr}^4(H_kA) - 4\,\mathrm{Tr}^2(H_kA)\,\mathrm{Det}(A) + (4-4)\,\mathrm{Det}^2(A) \\ &= \mathrm{Tr}^2(H_kA)(\mathrm{Tr}^2(H_kA) - 4\,\mathrm{Det}(A))\end{aligned}$$

□

Lemme IV.2.9. *Pour tous entiers n et k, on a $\mathrm{Tr}(H_k(MN)^n) = \mathrm{Tr}((MN)^{n+2k})$.*

Démonstration. On a $\mathrm{Tr}(H_k(MN)^n) = \mathrm{Tr}(MS_0(MN)^n) + \mathrm{Tr}((MN)^{n+2k})$. Or, $\mathrm{Tr}(MS_0(MN)^n) = \mathrm{Tr}(S_0(MN)^nM) = 0$, parce que $(MN)^nM$ est symétrique. □

Terminons maintenant la preuve du théorème IV.2.1. On a

$$\begin{aligned}\mathrm{discr}(B(MN)^nC(NM)^n) &= \mathrm{Tr}^2(H_k(MN)^n)(\mathrm{Tr}^2(H_k(MN)^n) - 4\,\mathrm{Det}(MN)^n) \\ &= \mathrm{Tr}^2((MN)^{n+2k})(\mathrm{Tr}^2((MN)^{n+2k}) - 4\,\mathrm{Det}(MN)^n) \\ &= \mathrm{Tr}^2((MN)^{n+2k})\,\mathrm{discr}((MN)^{n+2k})\end{aligned}$$

On vérifie que les matrices B et C sont bien dans Γ_{2q+1} (voir sections IV.5 et IV.6 pour plus de détails), et en explicitant les suites obtenues, on vérifie qu'elles sont non triviales (voir section IV.6). Ceci termine la preuve du théorème IV.2.1. □

IV.3 Fractions continues de la forme $[\overline{BA^n}]$

Dans cette partie, nous expliquons pourquoi la construction précédente ne pouvait pas aboutir avec des suites de fractions continues de la forme

$$[\overline{b_1, b_2, ..., b_k(a_1, a_2, ..., a_l)^n}].$$

Nous montrons qu'il n'existe pas de suite non constante de fractions continues périodiques de la forme $[\overline{BA^n}]$ dans un corps quadratique donné, ce qui se formule matriciellement de la façon suivante :

Proposition IV.3.1. *Soit $\mathbb{Q}[\sqrt{\delta}]$ un corps quadratique réel, et soient A et B des matrices de Γ. Si pour tout n, le corps de BA^n est $\mathbb{Q}[\sqrt{\delta}]$, alors la suite BA^n est triviale (au sens de la définition IV.1.5).*

On obtient même que les matrices BA^n correspondent toutes à la même fraction continue périodique, puisque l'on va montrer qu'il existe une matrice $D \in M_2(\mathbb{R})$ telle que pour tout n, BA^n est une puissance de D.

Pour démontrer cette proposition, nous aurons besoin de quelques lemmes :

Le lemme suivant permet de ramener le fait qu'une matrice soit dans un corps donné à une égalité de traces.

Lemme IV.3.2. *Soit δ entier non carré. Alors il existe une matrice U dans $GL_2(\mathbb{Z})$ telle que les solutions positives x à l'équation de Pell-Fermat : $x^2 - \delta y^2 = \pm 4$ sont exactement les $\mathrm{Tr}(U^n), n \in \mathbb{Z}$.*

Démonstration. Ecrivons $\delta = k^2\delta'$ où δ' est sans facteur carré.

Supposons d'abord que $k = 1$. Montrons que dans ce cas les solutions x à l'équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$ sont exactement les traces des unités (c'est-à-dire des entiers de norme ± 1) du corps $\mathbb{Q}[\sqrt{\delta'}]$.

Pour un réel quadratique $z = x' + y'\sqrt{\delta'}$, la trace vaut $\mathrm{Tr}(z) = 2x'$ et la norme vaut $\mathrm{N}(z) = x'^2 - \delta' y'^2$. On a donc

$$\mathrm{Tr}^2(z) - \delta'(2y')^2 = 4\,\mathrm{N}(z),$$

et donc la trace est solution x de l'équation $x^2 - \delta' y^2 = \pm 4$ si et seulement si $N(z) = \pm 1$. On vérifie que si $N(z) = \pm 1$, alors z est un entier de $\mathbb{Q}[\sqrt{\delta'}]$ si et seulement si $\mathrm{Tr}(z)$ et $2y'$ sont des entiers, sachant que l'anneau des entiers est $\mathbb{Z}[\frac{\sqrt{\delta'}+1}{2}]$ si $\delta' \equiv 1 \pmod 4$ et est $\mathbb{Z}[\sqrt{\delta'}]$ si $\delta' \not\equiv 1 \pmod 4$. Ainsi, on obtient bien que les parties x des solutions (x, y)

entières sont exactement les traces des unités. Or, le théorème des unités de Dirichlet nous donne l'existence d'une unité fondamentale $u \in O^*_{\delta'}$ dont les puissances engendrent, au signe près, le groupe des unités.

Soit U la matrice de la multiplication par u dans la base $\{1, u\}$. Alors $U \in GL_2(\mathbb{Z})$, puisque u est dans l'anneau d'entiers et son inverse aussi, et on a pour tout n, $\mathrm{Tr}(u^n) = \mathrm{Tr}(U^n)$, d'où le résultat.

Si maintenant on ne fait plus d'hypothèse sur k, on remarque qu'un couple (x, y) est solution de l'équation $x^2 - \delta y^2 = \pm 4$ si et seulement si (x, ky) est solution de $x^2 - \delta' y^2 = \pm 4$ avec x et y entiers. Or, l'ensemble des unités $z = x' + y'\sqrt{\delta'}$ telles que $2y'$ est divisible par k est un sous-groupe du groupe des unités. Donc il existe une certaine puissance de la matrice U obtenue précédemment qui convient. □

Le lemme suivant permettra de montrer (entre autres) que si les corps des matrices BA^n sont tous les mêmes, alors la matrice A a aussi le même corps.

Lemme IV.3.3. *Soit $n_0 \in \mathbb{Z}$, soient A, B, C trois matrices de $M_2(\mathbb{R})$, avec A et C ayant chacune des valeurs propres distinctes en module, et avec C inversible, et soient a et b deux entiers. Si l'égalité $\mathrm{Tr}(BA^n) = \mathrm{Tr}(C^{an+b})$ est vraie pour tout $n \geq n_0$, alors les matrices A et C^a ont mêmes valeurs propres, et l'égalité a lieu pour tout $n \in \mathbb{Z}$.*

Démonstration. Si l'on appelle λ et $\overline{\lambda}$ les valeurs propres de A, avec $|\overline{\lambda}| < |\lambda|$, et μ et $\overline{\mu}$ les valeurs propres de C, avec $|\overline{\mu}| < |\mu|$, l'égalité des traces se réécrit : $\alpha\lambda^n + \beta\overline{\lambda}^n = \mu^{an+b} + \overline{\mu}^{an+b}$ pour certains réels α et β et pour tout entier $n \geq n_0$.

Regardons les termes dominants de part et d'autre. Si on avait $\alpha = 0$, on aurait $\overline{\lambda} = \mu^a$ et $\beta = \mu^b$, puis $\overline{\mu} = 0$, ce qui contredit l'inversibilité de C. On a donc $\alpha \neq 0$. On obtient donc $\lambda = \mu^a$ et $\alpha = \mu^b$, puis on obtient $\overline{\lambda} = \overline{\mu}^a$ et $\beta = \overline{\mu}^b$. Donc A et C ont mêmes valeurs propres et l'égalité a lieu pour tout $n \in \mathbb{Z}$. □

D'après le lemme qui suit, les matrices BA^n ont toutes pour corps $\mathbb{Q}[\sqrt{\delta}]$ dès qu'il existe deux entiers i et j tels que les matrices BA^i et BA^j ont pour corps $\mathbb{Q}[\sqrt{\delta}]$.

Lemme IV.3.4. *Soient A et C des matrices positives ayant mêmes valeurs propres, et B et D des matrices de $M_2(\mathbb{R})$ quelconques. Si la relation $\mathrm{Tr}(BA^n) = \mathrm{Tr}(DC^n)$ est vraie pour deux valeurs de n, alors elle est vraie pour tout $n \in \mathbb{Z}$.*

Démonstration. Soient λ et $\overline{\lambda}$ les deux valeurs propres distinctes de A (et donc aussi de C). La relation $\mathrm{Tr}(BA^n) = \mathrm{Tr}(DC^n)$ se réécrit $\alpha\lambda^n + \beta\overline{\lambda}^n = 0$ pour des réels α et β indépendants de n, puisque les coefficients de chacune des deux matrices BA^n et DC^n sont des combinaisons linéaires en λ^n et $\overline{\lambda}^n$. Si la relation est vraie pour deux valeurs de n, on obtient alors un système de Cramer, donc $\alpha = \beta = 0$. □

La suite de ce chapitre est consacrée à la preuve de la proposition IV.3.1.

Preuve de la proposition IV.3.1. Supposons que l'on ait une suite de matrices BA^n ayant toutes pour corps $\mathbb{Q}[\sqrt{\delta}]$, où A et B sont deux matrices positives et δ est un entier sans facteur carré. Il existe alors un entier α_n tel que le discriminant $\mathrm{discr}(BA^n) = \mathrm{Tr}(BA^n)^2 -$

$4\,\mathrm{Det}(BA^n)$ soit égal à $\delta\alpha_n^2$. Et donc $\mathrm{Tr}(BA^n)$ est solution x de l'équation de Pell-Fermat $x^2 - \delta y^2 = 4\,\mathrm{Det}(BA^n)$. D'après le lemme IV.3.2, il existe donc une matrice $U \in GL_2(\mathbb{Z})$ (indépendante de n) telle que pour tout n, il existe un entier i_n tel que $\mathrm{Tr}(BA^n) = \mathrm{Tr}(U^{i_n})$, et on a alors aussi $\mathrm{Det}(BA^n) = \mathrm{Det}(U^{i_n})$ à partir d'un certain rang. On peut alors utiliser le lemme suivant :

Lemme IV.3.5. *Soient U une matrice de $GL_2(\mathbb{Z})$ ayant des valeurs propres distinctes en module, $B \in M_2(\mathbb{R})$ une matrice, et A une matrice positive. Si (i_n) est une suite d'entiers telles que pour tout n, $\mathrm{Tr}(BA^n) = \mathrm{Tr}(U^{i_n}) \neq 0$, alors, la suite (i_n) est arithmétique.*

Démonstration. Si l'on appelle λ et μ les deux valeurs propres de la matrice positive A (avec $\lambda > 1$ et $|\mu| < 1$), alors la trace de BA^n s'écrit $e\lambda^n + f\mu^n$ pour certains réels e et f indépendants de n, et on a $\mathrm{Tr}(U^{i_n}) = \alpha^{i_n} + \beta^{i_n}$, où α et β sont les deux valeurs propres de la matrice U (avec α la plus grande valeur propre de U en module). En divisant par α^{i_n} de part et d'autre de l'égalité $e\lambda^n + f\mu^n = \alpha^{i_n} + \beta^{i_n}$, on obtient $\lim_{n\to\infty} \dfrac{e\lambda^n}{\alpha^{i_n}} = 1$. En prenant le log, on obtient alors que $\lim_{n\to\infty} i_n\ \log(\alpha) - n\ \log(\lambda) - \log(e) = 0$. On a donc $i_n = an + b + \epsilon_n$, où $\lim_{n\to\infty} \epsilon_n = 0$, $a = \dfrac{\log(\lambda)}{\log(\alpha)}$ et $b = \dfrac{\log(e)}{\log(\alpha)}$. Et comme i_n est entier, on a finalement $i_n = an + b$ à partir d'un certain rang. D'après le lemme IV.3.3, cela est alors vrai pour tout n, ce qui termine la preuve du lemme. □

Dans ce dernier lemme a et b sont des entiers, puisque i_0 et i_1 sont entiers, et le lemme IV.3.3 donne que les matrices A et U^a ont mêmes valeurs propres. On obtient donc les égalités $\mathrm{Tr}(BA^n) = \mathrm{Tr}(U^{an+b})$ et $\mathrm{Det}(BA^n) = \mathrm{Det}(U^{an+b})$ pour tout n. L'égalité des traces nous donne que dans une base dans laquelle A est diagonale, la matrice B est de la forme $\begin{pmatrix} \alpha^b & * \\ * & \beta^b \end{pmatrix}$ où α et β sont les valeurs propres de U. L'égalité des déterminants $\mathrm{Det}(B) = \mathrm{Det}(U^b) = \alpha^b\beta^b$ implique alors que B est trigonale dans la base de diagonalisation de A. Les matrices A et B sont à coefficients entiers et ont un espace propre en commun : elles sont donc simultanément diagonalisables, puisque l'on obtient le deuxième espace propre par l'élement non trivial de $Gal(\mathbb{Q}[\sqrt{\delta}]/\mathbb{Q})$. Si l'on pose D la matrice qui vaut $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ dans la base de diagonalisation de A, on a $B = D^b$ et $A = D^a$, donc la suite BA^n est triviale. Ceci termine la preuve de la proposition IV.3.1. □

IV.4 Fractions continues de la forme $[\overline{\mathsf{BAC\,{}^tA}}]$

Dans ce chapitre, nous étudions les fractions continues périodiques correspondant aux matrices de la forme $BAC\,{}^tA$. Expérimentalement, de telles fractions continues périodiques apparaissent souvent, et nous allons tenter d'expliquer pourquoi, et en même temps généraliser et donner les réciproques de résultats qui permettent d'aboutir au théorème I.2.5.

Nous allons voir dans ce chapitre que l'on peut ramener l'étude des suites de matrices de la forme $BA^nC\,{}^tA^n$ (qui est faite dans le chapitre IV.5) à l'étude de suites de la forme

HA^n pour certaines matrices H non inversibles. On se ramène donc à des suites d'une forme semblable à celles qui ont étudiées dans le chapitre précédent.

Lemme IV.4.1. *Soit B une matrice de $GL_2(\mathbb{Z})$. On a équivalence entre les deux points suivants :*

1. *$B + {}^tB$ est de rang 1,*
2. *Il existe une matrice N symétrique de rang 1 telle que $B = N \pm S_0$,*

où S_0 est la matrice définie dans le chapitre IV.2.
De plus, si l'un de ces points est satisfait, alors on a $\mathrm{Det}(B) = 1$.

Démonstration. $\Longrightarrow$ Si $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a l'égalité

$$0 = \mathrm{Det}(B + {}^tB) = 4ad - (b+c)^2 = 4\,\mathrm{Det}(B) - (b-c)^2.$$

Donc on obtient $\mathrm{Det}(B) = 1$ et $b - c = \pm 2$. Quitte à la transposer, la matrice B peut donc s'écrire $B = \begin{pmatrix} a & b'-1 \\ b'+1 & d \end{pmatrix}$, avec $ad = b'^2$.
$\Longleftarrow$ Clair. □

La proposition qui suit généralise le lemme IV.2.8.

Proposition IV.4.2. *Soient B et C deux matrices de $GL_2(\mathbb{Z})$. On a l'équivalence :*

1. *Il existe une matrice $H \in \mathbb{M}_2(\mathbb{R})$ de rang 1 et un réel λ tels que pour toute matrice $A \in M_2(\mathbb{R})$ on ait :* $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}^2(HA) + \lambda\,\mathrm{Det}(A)$.
2. *Les matrices $B + {}^tB$ et $C + {}^tC$ sont de rang* 1.

De plus, si l'un des points est satisfait, alors on a nécessairement $\lambda = \pm 2$, et on a l'égalité suivante pour toute matrice $A \in M_2(\mathbb{R})$:

$$\mathrm{discr}(BAC\,{}^tA) = \mathrm{Tr}^2(HA)(\mathrm{Tr}^2(HA) \pm 4\,\mathrm{Det}(A)).$$

Tous les exemples connus de suites de fractions continues périodiques qui restent dans un corps quadratique donné (voir par exemple (McM09), (Wil80) et le chapitre IV.6 ci-après), correspondent à des suites de matrices de la forme $BA^nC\,{}^tA^n$ avec $B + {}^tB$ et $C + {}^tC$ de rang 1. Nous ignorons si cela est toujours vrai.

L'expression du discriminant $\mathrm{discr}(BAC\,{}^tA)$ donnée par la proposition IV.4.2, donne une factorisation par un carré. Cela est favorable à ce que le corps quadratique de la matrice $BAC\,{}^tA$ soit petit et explique donc un peu pourquoi l'on observe un certain nombre de fractions continues périodiques de cette forme.

Preuve de la proposition IV.4.2. $\Longrightarrow$ Ecrivons les matrices B et C sous la forme : $B = B_0 + \beta S_0$ et $C = C_0 + \gamma S_0$, où B_0 et C_0 sont deux matrices symétriques de $M_2(\mathbb{R})$, β et γ sont deux réels et S_0 est la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On a alors $\mathrm{Tr}(S_0AC_0\,{}^tA) = \mathrm{Tr}(B_0AS_0\,{}^tA) = 0$

puisque les matrices $AC_0\,{}^tA$ et ${}^tAB_0A$ sont symétriques, et on a $\mathrm{Tr}(S_0AS_0\,{}^tA) = -2\,\mathrm{Det}(A)$. On obtient donc l'égalité $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}(B_0AC_0\,{}^tA) - 2\beta\gamma\,\mathrm{Det}(A)$. On souhaite maintenant montrer que les matrices B_0 et C_0 sont chacune de rang 1. En évaluant la forme quadratique $A \mapsto \mathrm{Tr}(BAC\,{}^tA)$ en $A = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, en $A = \begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix}$, et en les transposées, on obtient à chaque fois des formes quadratiques en x et y qui doivent être des carrés, et qui ont à chaque fois pour matrice un multiple de B_0 ou de C_0. Ceci nous donne que les matrices B_0 et C_0 sont chacune des matrices de formes quadratiques carrées. Et ni la matrice B_0 ni la matrice C_0 ne peuvent être nulles puisque la matrice H est non nulle. Donc les matrices B_0 et C_0 sont de rang 1.

$\Longleftarrow$ Si des matrices B et C de $GL_2(\mathbb{Z})$ sont telles que $B + {}^tB$ et $C + {}^tC$ sont de rang 1, d'après le lemme IV.4.1 on peut les écrire sous la forme $B = b_0\,{}^tb_0 \pm S_0$ et $C = c_0\,{}^tc_0 \pm S_0$ pour des vecteurs b_0 et c_0 de $M_{2,1}(\mathbb{R})$. On a alors $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}(b_0\,{}^tb_0Ac_0\,{}^tc_0\,{}^tA) \pm \mathrm{Tr}(S_0AS_0\,{}^tA)$, puisque les deux termes $\mathrm{Tr}(S_0Ac_0\,{}^tc_0\,{}^tA)$ et $\mathrm{Tr}(b_0\,{}^tb_0AS_0\,{}^tA)$ sont nuls, étant donné que les matrices $Ac_0\,{}^tc_0\,{}^tA$ et ${}^tAb_0\,{}^tb_0A$ sont symétriques. On a ensuite $\mathrm{Tr}(b_0\,{}^tb_0Ac_0\,{}^tc_0\,{}^tA) = ({}^tb_0Ac_0)^2 = \mathrm{Tr}(c_0\,{}^tb_0A)^2$, et $\mathrm{Tr}(S_0AS_0\,{}^tA) = -2\,\mathrm{Det}(A)$, d'où le résultat avec $H := c_0\,{}^tb_0$. L'expression du discriminant annoncée se déduit facilement du point 1. :

$$\begin{aligned}\mathrm{discr}(BAC\,{}^tA) &= \mathrm{Tr}^2(BAC\,{}^tA) - 4\,\mathrm{Det}(BAC\,{}^tA)\\ &= \mathrm{Tr}^4(HA) \pm 4\,\mathrm{Tr}^2(HA)\,\mathrm{Det}(A) + 4 - 4\,\mathrm{Det}(BC)\\ &= \mathrm{Tr}^2(HA)(\mathrm{Tr}^2(HA) \pm 4\,\mathrm{Det}(A)).\end{aligned}$$

□

Remarque IV.4.3. *Dans la proposition IV.4.2, si B est de la forme $b_0\,{}^tb_0 + \epsilon_B S_0$ et C est de la forme $c_0\,{}^tc_0 + \epsilon_C S_0$ pour des vecteurs b_0 et c_0 de $M_{2,1}(\mathbb{R})$ et des signes ϵ_B et ϵ_C de $\{-1, 1\}$, alors λ vaut $-2\epsilon_B\epsilon_C$ et H vaut (au signe près) $c_0\,{}^tb_0$ et ce sont les seules solutions.*

La proposition suivante permet de déterminer toutes les matrices $B \in \Gamma$ telles que $B + {}^tB$ est de rang 1.

Proposition IV.4.4. *Soit $B \in \Gamma$. On a l'équivalence :*

1. *$B + {}^tB$ est de rang 1,*
2. *Il existe des entiers $k \geq 1$ et $n \geq 2$, et une matrice F de Γ tels que B ou ${}^tB$ vaut $FT_{(n-1,1,k-1,n)}\,{}^tF$.*

La transposée d'une matrice positive est positive, et on a $T_{(n,1,0,n+1)} = T_{(n,n+2)}$, donc le deuxième point de la proposition IV.4.4 entraîne automatiquement que B est une matrice positive.

Démonstration. $\Longleftarrow$ Vérification facile sachant que l'on a

$$T_{(n-1,1,k-1,n)} = \begin{pmatrix} k & kn+1 \\ kn-1 & kn^2 \end{pmatrix}.$$

$\Longrightarrow$ Quitte à transposer la matrice B, on peut l'écrire sous la forme : $\begin{pmatrix} a & b+1 \\ b-1 & c \end{pmatrix}$ avec $ac = b^2$. On peut alors écrire les entiers a et c sous la forme : $a = zx^2$ et $c = z'y^2$ avec z et z' sans facteurs carrés. La condition $ac = b^2$ entraîne alors que $z = z'$ et $b = \pm xyz$. Comme la matrice B est dans Γ, on peut donc écrire

$$B = \begin{pmatrix} zx^2 & xyz+1 \\ xyz-1 & zy^2 \end{pmatrix}, \quad \text{avec} \quad x, y, z \geq 1.$$

On peut supposer que la première matrice T_i et la dernière matrice T_j qui apparaissent dans la décomposition de B en produit de matrices T_k, $k \geq 1$, sont distinctes. En effet, ni l'identité I_2 ni les matrices T_i, $i \geq 1$ ne sont de la forme $N \pm S_0$, avec N matrice symétrique de rang 1.

On a ensuite $i = \left\lfloor \dfrac{xyz-1}{zx^2} \right\rfloor$ et $j = \left\lfloor \dfrac{xyz+1}{zx^2} \right\rfloor$, puisque $\mathrm{Det}(B) = 1 > 0$ et $zx^2 > 0$. De plus, on a $i < j$ puisque l'on a $i \neq j$. Et on a les inégalités :

$$izx^2 \leq xyz - 1 < (i+1)zx^2,$$

$$jzx^2 \leq xyz + 1 < (j+1)zx^2.$$

Donc en particulier on a $(j-i-1)zx^2 < 2$. On obtient alors deux cas :

Premier cas : $x = z = 1$

On a alors $B = \begin{pmatrix} 1 & y+1 \\ y-1 & y^2 \end{pmatrix} = T_{(y-1,y+1)} = T_{(y-1,1,0,y)}$.

Deuxième cas : $xz \geq 2$ et j = i+1

On a $y - \dfrac{1}{xz} < jx \leq y + \dfrac{1}{xz}$, avec $xz \geq 2$ et comme y et jx sont des entiers, ceci entraîne que $y = jx$. Et donc finalement

$$B = \begin{pmatrix} zx^2 & jzx^2+1 \\ jzx^2-1 & zj^2x^2 \end{pmatrix} = T_{(j-1,1,zx^2-1,j)}.$$

□

Le corollaire qui suit nous permet de connaître la matrice H qui apparaît dans l'écriture $\mathrm{Tr}(BAC\,{}^t\!A) = \mathrm{Tr}^2(HA) \pm 2\,\mathrm{Det}(A)$ pour toute matrice $A \in M_2(\mathbb{R})$, en fonction des décompositions des matrices positives B et C comme produits de matrices T_k, données par la proposition précédente.

Étant fixée une matrice A positive de corps $\mathbb{Q}[\sqrt{\delta}]$, cela nous permet de ramener la recherche de matrices B et C telles que les rangs de $B + {}^tB$ et de $C + {}^tC$ sont 1, et telles que les corps des matrices $BA^nC\,{}^t\!A^n$ sont tous les mêmes, à la recherche des matrices H de rang 1 telles que $\mathrm{Tr}^2(HA)(\mathrm{Tr}^2(HA) \pm 4\,\mathrm{Det}(A))$ (c'est-à-dire le discriminant de $BAC\,{}^t\!A$) soit de la forme $\delta\alpha^2$ pour α entier.

Corollaire IV.4.5. *Si l'on a*

$$\begin{aligned} B &= MT_{(m-1,1,k-1,m)}\,{}^tM, \\ C &= NT_{(n-1,1,l-1,n)}\,{}^tN, \end{aligned}$$

pour $n, m \geq 1$, $k, l \geq 0$ et $M, N \in GL_2(\mathbb{Z})$, alors la matrice $H \in M_2(\mathbb{R})$ telle que $\mathrm{Tr}(BAC\,{}^tA) = (\mathrm{Tr}(HA))^2 \pm 2\,\mathrm{Det}(A)$ pour toute matrice $A \in M_2(\mathbb{R})$, s'écrit :

$$H = NT_n \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{kl} \end{pmatrix} T_m\,{}^tM.$$

Démonstration. On peut se ramener à $M = N = I_2$, puisque si $B = MB'\,{}^tM$ et $C = NC'\,{}^tN$, alors $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}(B'({}^tMAN)C'\,{}^t({}^tMAN))$, et $A \mapsto {}^tMAN$ décrit $M_2(\mathbb{R})$ quand A décrit $M_2(\mathbb{R})$ puisque M et N sont inversibles.
La proposition IV.4.2 donne bien l'existence d'une matrice $H \in M_2(\mathbb{R})$ telle que $\mathrm{Tr}(BAC\,{}^tA) = (\mathrm{Tr}(HA))^2 \pm 2\,\mathrm{Det}(A)$ pour toute matrice $A \in M_2(\mathbb{R})$, et d'après la remarque IV.4.3 elle est uniquement déterminée au signe près, et vaut $H = \begin{pmatrix} \sqrt{ae} & \sqrt{ah} \\ \sqrt{ed} & \sqrt{hd} \end{pmatrix}$ si $B = \begin{pmatrix} a & * \\ * & d \end{pmatrix}$ et $C = \begin{pmatrix} e & * \\ * & h \end{pmatrix}$. Or, B vaut $\begin{pmatrix} k & mk+1 \\ mk-1 & km^2 \end{pmatrix}$, et C vaut $\begin{pmatrix} l & nl+1 \\ nl-1 & ln^2 \end{pmatrix}$, d'où le résultat. □

Corollaire IV.4.6. *Soit δ un entier sans facteur carré, soit A une matrice positive, soient B et C des matrices de Γ telles que $B + {}^tB$ et $C + {}^tC$ sont de rang 1, et soit H la matrice donnée dans la proposition précédente.*
On a l'équivalence :

1. *Le corps de $BAC\,{}^tA$ ou de $BA\,{}^tC\,{}^tA$ est $\mathbb{Q}[\sqrt{\delta}]$.*
2. *L'entier $\frac{1}{\sqrt{s}}\mathrm{Tr}(HA)$ est solution x d'une équation de Pell-Fermat $sx^2 - ty^2 = \pm 4$, pour des entiers s et t tels que $\frac{1}{\sqrt{s}}H \in M_2(\mathbb{Z})$ et tels que le produit st soit de la forme δk^2.*

En particulier, il suffit que $\mathrm{Tr}(HA)$ soit solution x entière de l'équation $x^2 - \delta y^2 = \pm 4$ pour que le corps de $BAC\,{}^tA$ ou de $BA\,{}^tC\,{}^tA$ soit $\mathbb{Q}[\sqrt{\delta}]$.

Remarque IV.4.7. *Il est facile de déterminer dans ce corollaire si c'est $BAC\,{}^tA$ ou bien $BA\,{}^tC\,{}^tA$ dont le corps est $\mathbb{Q}[\sqrt{\delta}]$. Supposons que B et C s'écrivent respectivement $N_B + \epsilon_B S_0$ et $N_C + \epsilon_C S_0$ pour des matrices N_B et N_C symétriques de rang 1.*

- *Si l'entier $\frac{1}{\sqrt{s}}\mathrm{Tr}(HA)$ est solution x de l'équation de Pell-Fermat $sx^2 - ty^2 = 4\epsilon_B\epsilon_C\,\mathrm{Det}(A)$, alors la matrice $BAC\,{}^tA$ a pour corps $\mathbb{Q}[\sqrt{\delta}]$.*
- *Si l'entier $\frac{1}{\sqrt{s}}\mathrm{Tr}(HA)$ est solution x de l'équation de Pell-Fermat $sx^2 - ty^2 = -4\epsilon_B\epsilon_C\,\mathrm{Det}(A)$, alors la matrice $BA\,{}^tC\,{}^tA$ a pour corps $\mathbb{Q}[\sqrt{\delta}]$.*

Dans la suite, nous nous intéressons surtout au cas particulier où $\mathrm{Tr}(HA)$ est solution x entière de l'équation $x^2 - \delta y^2 = \pm 4$. Le cas général est plus compliqué, car les ensembles de solutions des équations de Pell-Fermat plus générales $sx^2 - ty^2 = \pm 4$ n'ont pas une structure aussi simple que pour l'équation classique où $s = 1$. On retombe quand même sur une équation de Pell-Fermat classique dans le cas où $s = \delta$ (voir les suites de type Wilson à la fin du chapitre IV.5).

Preuve du corollaire. On a pour toute matrice $A \in M_2(\mathbb{R})$, $\mathrm{Tr}(BAC\,{}^tA) = \mathrm{Tr}(HA)^2 \pm 4\,\mathrm{Det}(A)$, et on peut choisir le signe devant le terme $4\,\mathrm{Det}(A)$ quitte à transposer C. On a alors $\mathrm{discr}(BAC\,{}^tA) = \mathrm{Tr}^2(HA)(\mathrm{Tr}^2(HA) \pm 4\,\mathrm{Det}(A)) = sx^2(sx^2 \pm 4)$ où $x = \dfrac{1}{\sqrt{s}}\mathrm{Tr}(HA)$. Le corps de $BAC\,{}^tA$ est donc $\mathbb{Q}[\sqrt{\delta}]$ si et seulement si $sx^2(sx^2 \pm 4)$ est de la forme $\delta\alpha^2$, si et seulement si $sx^2 - t\alpha^2 = \mp 4$ pour un entier t tel que st est de la forme δk^2. □

Conjecture IV.4.8. *Dans tout corps quadratique réel, il existe une infinité de fractions continues périodiques d'une des formes* $[\overline{2, 1, 1, 1, \mathsf{A}, 2, 1, 1, 1, {}^t\mathsf{A}}]$ *ou* $[\overline{2, 1, 1, 1, \mathsf{A}, 1, 1, 1, 2, {}^t\mathsf{A}}]$, *formées seulement des entiers 1 et 2.*

Ici, A est un motif $a_1, a_2, ...a_k$, avec $a_i \in \{1, 2\}$, et ${}^t\mathsf{A}$ est le motif miroir.

Remarque IV.4.9. *Pour obtenir cette conjecture, il suffirait, étant donné un entier δ non carré, de trouver une infinité de matrices A dans Γ_2 telles que $\mathrm{Tr}(HA)$ soit solution x entière d'une équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$, où H est la matrice* $\begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix}$.

La conjecture IV.0.11 de McMullen revient à trouver, pour tout δ non carré, une infinité de matrices A dans Γ_2 telles que $\mathrm{Tr}(A)$ est solution x de l'équation de Pell-Fermat $x^2 - \delta y^2 = 4\,\mathrm{Det}(A)$.

La conjecture IV.4.8 se ramène donc approximativement à la conjecture IV.0.11 dans laquelle on aurait remplacé la trace par la forme linéaire $A \mapsto \mathrm{Tr}(HA)$.

Il est malheureusement impossible de recommencer tel quel ce procédé qui nous a permis de passer de la trace à la forme linéaire $A \mapsto \mathrm{Tr}(HA)$: Si l'on a $\mathrm{Tr}(HBAC\,{}^tAD) = (g(A))^2 + \lambda\,\mathrm{Det}(A)$ pour toute matrice $A \in M_2(\mathbb{R})$, alors on a $\lambda = 0$, quelles que soient les matrices $B, C, D \in GL_2(\mathbb{Z})$ et $g \in M_2(\mathbb{R})^*$, et donc cela ne donne plus de factorisation du discriminant par un carré.

Remarque IV.4.10. *La conjecture IV.4.8 est « presque » conséquence de celle de Zaremba avec une borne 2. Voir section IV.7 pour plus de détails.*

IV.5 Fractions continues de la forme $[\overline{\mathsf{BA}^n\mathsf{C}\,{}^t\mathsf{A}^n}]$

Dans ce chapitre, nous donnons une façon de construire des suites de fractions continues périodiques qui sont dans un corps quadratique donné, et qui correspondent à des suites de matrices de la forme $BA^nC\,{}^tA^n$ avec $B + {}^tB$ et $C + {}^tC$ de rang 1.

IV.5.1 Hypothèse H entière

On supposera que B et C sont deux matrices de Γ telles que $B + {}^tB$ et $C + {}^tC$ sont de rang 1. Et on supposera que la matrice H donnée par le corollaire IV.4.5 (pour ces matrices B et C) est à coefficients entiers.

La proposition suivante justifie que pour une matrice positive A fixée on cherche à obtenir une relation de la forme $\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+k})$ pour obtenir une suite de matrices $BA^nC\,{}^tA^n$ qui ont toutes le même corps. Dans le cas où A est une matrice donnée par le lemme IV.3.2, et sous l'hypothèse H entière, cela est nécessaire.

Proposition IV.5.1. *Soit $\mathbb{Q}[\sqrt{\delta}]$ un corps quadratique réel. Sous l'hypothèse H entière les deux assertions suivantes sont équivalentes :*

1. *Pour tout $n \in \mathbb{Z}$, le corps de $BA^nC\,{}^tA^n$ ou bien de $BA^n\,{}^tC\,{}^tA^n$ est $\mathbb{Q}[\sqrt{\delta}]$,*
2. *Il existe une matrice $U \in GL_2(\mathbb{Z})$ de corps $\mathbb{Q}[\sqrt{\delta}]$ et deux entiers a et b tels que $\mathrm{Tr}(HA^n) = \mathrm{Tr}(U^{an+b})$ pour tout entier $n \in \mathbb{Z}$.*

Et le corps de A est alors nécessairement $\mathbb{Q}[\sqrt{\delta}]$.

Remarque IV.5.2. *Supposons que l'on ait $B = N_B + \epsilon_B S_0$ et $C = N_C + \epsilon_C S_0$, pour des matrices N_B et N_C symétriques de rang 1, et pour des $\epsilon_B, \epsilon_C \in \{-1, 1\}$. Si l'on a $\mathrm{Tr}(HA^n) = \mathrm{Tr}(U^{an+b})$ pour tout entier $n \in \mathbb{Z}$, comme dans la proposition IV.5.1, alors*

- *la matrice $BA^nC\,{}^tA^n$ a pour corps $\mathbb{Q}[\sqrt{\delta}]$ si $\epsilon_B\epsilon_C = \mathrm{Det}(U^b)$,*
- *la matrice $BA^n\,{}^tC\,{}^tA^n$ a pour corps $\mathbb{Q}[\sqrt{\delta}]$ sinon,*

pour tout entier n.

Preuve de la proposition IV.5.1. $\Longleftarrow$ En utilisant la proposition IV.4.2, on obtient que

$$\mathrm{discr}(BA^nC\,{}^tA^n) = \mathrm{Tr}^2(HA^n)(\mathrm{Tr}^2(HA^n) + 4\epsilon)$$

pour un $\epsilon \in \{-1, 1\}$, et on peut choisir ϵ comme l'on veut quitte à transposer C.

L'entier $\mathrm{Tr}(U^{an+b})$ est solution x d'une équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$. En effet, on a d'une part que le discriminant de U^{an+b} est de la forme $\mathrm{discr}(U^{an+b}) = \delta y^2$ puisque le corps de U est $\mathbb{Q}[\sqrt{\delta}]$, et on a d'autre part les égalités $\mathrm{discr}(U^{an+b}) = \mathrm{Tr}(U^{an+b})^2 - 4\,\mathrm{Det}(U^{an+b})$, et $\mathrm{Det}(U^{an+b}) = \pm 1$.

On obtient donc, quitte à transposer C, que $\mathrm{discr}(BA^nC\,{}^tA^n)$ est de la forme δz^2, donc que le corps de $BA^nC\,{}^tA^n$ est $\mathbb{Q}[\sqrt{\delta}]$.

$\Longrightarrow$ Pour démontrer cette implication, on reprend les choses qui ont été faites pour étudier les suites de la forme AB^n (voir chapitre IV.3). Soit U la matrice donnée par le lemme IV.3.2. On a que $\mathrm{Tr}(HA^n)$ est solution x d'une équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$, donc d'après le lemme IV.3.2, il existe une suite d'entiers (i_n) telle que pour tout n, on ait $\mathrm{Tr}(HA^n) = \mathrm{Tr}(U^{i_n})$. On est alors exactement dans la situation du lemme IV.3.5, et on obtient alors que la suite (i_n) est arithmétique : il existe donc deux entiers a et b tels que pour tout n, $i_n = an + b$. D'après le lemme IV.3.3, on a de plus que les matrices A et U^a sont semblables (i.e. ont mêmes valeurs propres), donc le corps de A est $\mathbb{Q}[\sqrt{\delta}]$. □

La proposition suivante permet de ramener la recherche de matrices non inversibles et à coefficients entiers H telles que $\mathrm{Tr}(HA)$ est solution x entière de l'équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$ (A étant fixée), à la recherche de matrices S vérifiant certaines propriétés plus simples :

Proposition IV.5.3. *Soit A une matrice positive, et b un entier. Les assertions suivantes sont équivalentes :*

1. *Il existe une matrice $H \in M_2(\mathbb{Z})$ de rang 1, telle que pour tout $n \in \mathbb{Z}$,*

$$\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+b}).$$

2. *Il existe une matrice $S \in GL_2(\mathbb{Z})$ telle que*

$$\mathrm{Det}(S) = -\mathrm{Det}(A^b),\ \mathrm{Tr}(S) = 0 \text{ et } \mathrm{Tr}(SA) = 0.$$

Démonstration. $\Longrightarrow$ Soit $S = H - A^b$. On a alors bien $\mathrm{Tr}(S) = 0$ et $\mathrm{Tr}(SA) = 0$. Montrons que $S \in GL_2(\mathbb{Z})$. Si l'on diagonalise A, on voit que la condition

$$\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+b})$$

pour tout entier $n \in \mathbb{Z}$, entraîne que dans la base de diagonalisation, H est de la forme : $\begin{pmatrix} \lambda^b & * \\ * & \bar{\lambda}^b \end{pmatrix}$, où λ et $\bar{\lambda}$ sont les deux valeurs propres de A. Comme H est non inversible, on obtient l'égalité des déterminants $\mathrm{Det}(S) = -\mathrm{Det}(A^b)$. Et comme S est à coefficients entiers, on a bien $S \in GL_2(\mathbb{Z})$.

$\Longleftarrow$ Les égalités $\mathrm{Tr}(S) = 0$ et $\mathrm{Tr}(SA) = 0$ entraînent d'après le lemme IV.3.4, l'égalité $\mathrm{Tr}(SA^n) = 0$ pour tout entier n. Et par la formule IV.1 (page 139) on a

$$\mathrm{Det}(S + A^b) = \mathrm{Det}(S) + \mathrm{Det}(A^b) + \mathrm{Tr}(SA^{b\dagger}),$$

où $M^\dagger = \mathrm{Det}(M)M^{-1}$. Or on a $\mathrm{Tr}(SA^{-b}) = 0$ et $\mathrm{Det}(S) = -\mathrm{Det}(A^b)$, donc $S + A^b$ est de déterminant 0. Finalement $H = S + A^b$ convient. □

Corollaire IV.5.4. *Soit A une matrice positive, et soit S une matrice de $GL_2(\mathbb{Z})$ vérifiant les conditions $\mathrm{Tr}(S) = \mathrm{Tr}(SA) = 0$ et aussi $\mathrm{Det}(S) = -1$ si $\mathrm{Det}(A) = 1$. Alors il existe deux matrices B et C de Γ telles que les rangs de $B + {}^tB$ et de $C + {}^tC$ sont 1, et telles que les corps des matrices $BA^nC\,{}^tA^n$ sont tous les mêmes.*

Preuve du corollaire. L'existence d'une telle matrice S nous donne, par la proposition IV.5.3 l'existence d'une matrice $H \in M_2(\mathbb{Z})$ non inversible telle que pour tout entier n, $\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+k})$ (pour un k pair si $\mathrm{Det}(S) = \mathrm{Det}(A) = -1$, k impair si $\mathrm{Det}(S) = 1$ et k quelconque sinon). Quitte à prendre k assez grand, on peut supposer que les inégalités $0 \leq a < b \leq d$ et $a < c \leq d$ sont satisfaites, où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = H$, et donc la

proposition IV.1.7 nous donne que H s'écrit : $H = X\begin{pmatrix} 0 & 0 \\ 0 & e \end{pmatrix}Y$, avec $X, Y \in \Gamma$, $e \geq 1$. Et comme on a $a < b$ et $a < c$, on obtient que X et Y sont chacun dans $\Gamma\backslash\{I_2, T_1\}$. On peut donc utiliser les relations données dans la proposition IV.1.7, pour se ramener à X et Y de la forme : $X = X'T_i$ et $Y = T_jY'$, avec $i, j \geq 2$ (et on a bien $e \geq 1$). D'après le corollaire IV.4.5, il existe donc deux matrices positives B et C telles que les rangs de $B + {}^tB$ et de $C + {}^tC$ sont 1 et telles que pour toute matrice $M \in M_2(\mathbb{R})$ on ait $\mathrm{Tr}(BMC\,{}^tM) = (\mathrm{Tr}(HM))^2 - 2\,\mathrm{Det}(MA^k)$. On a alors $\mathrm{discr}(BA^nC\,{}^tA^n) = \mathrm{Tr}^2(A^{n+k})(\mathrm{Tr}^2(A^{n+k}) - 4\,\mathrm{Det}(A^{n+k})) = \mathrm{Tr}^2(A^{n+k})\,\mathrm{discr}(A^{n+k})$, donc pour tout n, le corps de $BA^nC\,{}^tA^n$ est le corps de A. □

Remarque IV.5.5. *Soient A, B et C trois matrices de Γ. Sous les trois hypothèses*

1. *que $B + {}^tB$ et $C + {}^tC$ sont de rang 1,*
2. *que la matrice H donnée par la proposition IV.4.4 et le corollaire IV.4.5 est entière,*
3. *que l'on peut prendre $U = A$ dans l'égalité $\mathrm{Tr}(HA^n) = \mathrm{Tr}(U^{an+b})$ donnée par la proposition IV.5.1,*

ceci fournit de manière exhaustive les suites de matrices $BA^nC\,{}^tA^n$ qui ont toutes le même corps.

La dernière hypothèse est automatiquement satisfaite si A est une matrice donnée par le lemme IV.3.2 (par exemple si $A = T_1$), et la première hypothèse est vérifiée pour tous les exemples connus. Il reste des suites infinies à étudier en retirant l'hypothèse H entière.

A l'aide de ce corollaire IV.5.4, on peut redémontrer rapidement le théorème IV.2.1 :

Preuve du théorème IV.2.1. Quitte à tout transposer, on peut supposer que c'est N qui est de déterminant -1. La matrice $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}N$ vérifie alors $\mathrm{Tr}(S) = \mathrm{Tr}(SMN) = 0$ (parce que NMN est symétrique), $\mathrm{Det}(S) = -1$ et $S \in GL_2(\mathbb{Z})$, donc le corollaire IV.5.4 permet de conclure. □

Voici maintenant une preuve plus longue, mais qui fait apparaître naturellement la condition sur la matrice A pour que l'on ait une suite $BA^nC\,{}^tA^n$ de matrices ayant toutes pour corps le corps de A.

Preuve du théorème IV.2.1. Étant fixée une matrice positive A, on cherche une matrice S qui vérifie les hypothèses du corollaire IV.5.4. Les condition $\mathrm{Tr}(S) = \mathrm{Tr}(SA) = 0$ imposent de chercher S sous la forme : $S = \begin{pmatrix} x & y \\ \dfrac{x(d-a) - cy}{b} & -x \end{pmatrix}$ où $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, et on doit avoir $\mathrm{Det}(S) = \pm 1$, ce qui nous donne l'équation de Pell-Fermat :

$$(2bx + (d-a)y)^2 - \mathrm{discr}(A)y^2 = \pm 4b^2$$

On va maintenant montrer que l'on peut trouver S qui s'exprime simplement en fonction de A^n. Si l'on définit les suites (u_n) et (v_n) par :

$$\begin{cases} u_0 = 1 \text{ et } u_{n+1} = au_n + bcv_n \\ v_0 = 0 \text{ et } v_{n+1} = u_n + dv_n \end{cases}$$

alors on a $A^n = \begin{pmatrix} u_n & bv_n \\ cv_n & u_n + (d-a)v_n \end{pmatrix}$, et comme on a $\mathrm{Det}(A^n) = \pm 1$, on obtient :

$$(2u_n + (d-a)v_n)^2 - \mathrm{discr}(A)v_n^2 = \pm 4$$

On voit donc que $(x, y) = (u_n, bv_n)$ fournit une solution. La dernière chose à vérifier est que la matrice S trouvée est à coefficients entiers. Or, cela est le cas si et seulement si b divise $d - a$, puisque b divise y et b est premier à x. Or, les matrices $A \in \Gamma$ qui vérifient cette relation de divisibilité sont exactement les matrices de la forme $T_k M$ avec $k \geq 1$ et $M \in \Gamma$ symétrique. Ainsi on a bien démontré le théorème IV.2.1. Et le théorème I.2.5 lui est équivalent (voir remarque IV.2.2). □

IV.6 Exemples

Dans ce chapitre, nous décrivons précisément les suites de fractions continues périodiques que donne la preuve du théorème I.2.5, et nous donnons des exemples, que nous vérifions directement.

Étant donnés une matrice A positive fixée, un entier k et une matrice H non inversible telle que pour tout n, $\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+k})$, le corollaire IV.4.5 et les propositions IV.1.7 et IV.4.2 permettent de trouver toutes les matrices B et C telles que

$$\text{pour toute matrice } M \in M_2(\mathbb{R}), \mathrm{Tr}(BMC\,{}^tM) = \mathrm{Tr}(HM)^2 \pm 2\,\mathrm{Det}(M).$$

Cela donne alors une suite de matrices $BA^nC\,{}^tA^n$ ayant toutes le même corps.

On peut déterminer explicitement quelles sont les matrices H qui sont données par la proposition IV.5.3, à partir des matrices S choisies ci-dessus dans la preuve du théorème, pour $N = T_i$. En prenant $A = MT_i$ pour $M \in \Gamma$ symétrique, $b = 2$ et $S = S_0T_i$ dans la proposition IV.5.3, on a $H = S_0T_i + MT_iMT_i$, donc on obtient :

$$H = M(\mathrm{Det}(M)S_0 + T_i)MT_i = \begin{cases} MRMT_i & \text{si} \quad \mathrm{Det}(M) = 1 \\ M\,{}^tRMT_i & \text{si} \quad \mathrm{Det}(M) = -1 \end{cases}$$

où $R := \begin{pmatrix} 0 & 0 \\ 2 & i \end{pmatrix}$.

Et l'on peut expliciter la décomposition de la matrice R donnée par la proposition IV.1.7 :

$$R = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} T_{\frac{i}{2}} \qquad \text{si } i \text{ pair,}$$
$$R = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} T_2 T_{\frac{i-1}{2}} \qquad \text{si } i \text{ impair.}$$

On choisit alors des matrices B et C de Γ qui correspondent, par le corollaire IV.4.5, aux matrices H de rang 1 ci-dessus. Par exemple, si $\mathrm{Det}(M) = 1$, si i est pair, et si $M = T_j S T_j$ pour une matrice symétrique S de Γ, on peut prendre :

$$\begin{array}{l} B = T_{(i,j)} S T_{(j,i/2-1,1,1,i/2,j)} S T_{(j,i)}, \\ C = T_j S T_{(j-1,1,1,j)} S T_j. \end{array} .$$

On obtient finalement les suites de fractions continues périodiques suivantes :

Proposition IV.6.1. *Soit $M = (a_1, a_2, ..., a_2, a_1)$ un uplet symétrique d'entiers strictement positifs et soient i et j deux entiers strictement positifs.*

Si i est pair, alors pour tout entier n,

$$[\overline{i/2-1, 1, 1, i/2, i^n, i-1, 1, 1, i, i^n}] \in \mathbb{Q}[\sqrt{i^2+4}]$$

$$[\overline{i/2-1, 1, 1, i/2, (j,i)^n, j-1, 1, 1, j, (i,j)^n}] \in \mathbb{Q}[\sqrt{(ij)^2+4ij}]$$
$$[\overline{i/2-1, 1, 1, i/2, (j, M, j, i)^n, j, M, j-1, 1, 1, j, M, j, (i, j, M, j)^n}]$$
$$\in \mathbb{Q}[\sqrt{\mathrm{discr}(T_{(j,a_1,a_2,...,a_2,a_1,j,i)})}].$$

Et si i est impair, alors pour tout n,

$$[\overline{(i-1)/2, 1, 3, (i-1)/2, i^n, i+1, i-1, i^n}] \in \mathbb{Q}[\sqrt{i^2+4}]$$

$$[\overline{(i-1)/2, 1, 3, (i-1)/2, (j,i)^n, j+1, j-1, (i,j)^n}] \in \mathbb{Q}[\sqrt{(ij)^2+4ij}]$$
$$[\overline{(i-1)/2, 1, 3, (i-1)/2, (j, M, j, i)^n, j, M, j+1, j-1, M, j, (i, j, M, j)^n}]$$
$$\in \mathbb{Q}[\sqrt{\mathrm{discr}(T_{(j,a_1,a_2,...,a_2,a_1,j,i)})}].$$

Et l'on obtient de vraies fractions continues périodiques même s'il y a des entiers nuls, en utilisant la relation $T_{(i,0,j)} = T_{i+j}$.

Ici, i^n signifie que l'entier i est répété n fois, et de même $(j, \mathsf{M}, j, i)^n$ signifie que le motif $j, a_1, a_2, ..., a_2, a_1, j, i$ est répétée n fois.

Exemple IV.6.2. *En choisissant dans la proposition précédente $i = 2$, $j = 2$ et $M = (1,1,1,1,2,1,1,1,1,1,2,1,1,1,1)$, on obtient pour tout entier n la fraction continue périodique*

$$[\overline{1, 1, 1, 2, (M, 2, 2, 2)^n, M, 3, 1, 1, 2, M, (2, 2, 2, M)^n}] \in \mathbb{Q}[\sqrt{2}]$$

de longueur $36n + 38$, et n'ayant que des 1 et des 2, à l'exception d'un 3.

Vérification. La proposition IV.6.1 donne la suite de fractions continues périodiques :

$$\overline{[0,1,1,1,(2,\mathsf{M},2,2)^n,2,\mathsf{M},1,1,1,2,\mathsf{M},2,(2,2,\mathsf{M},2)^n]}$$

qui devient par permutation circulaire et décalage des puissances :

$$\overline{[1,1,1,2,(\mathsf{M},2,2,2)^n,\mathsf{M},2,0,1,1,1,2,\mathsf{M},(2,2,2,\mathsf{M})^n]}$$

et on obtient enfin la suite annoncée en utilisant la relation $T_{(2,0,1)} = T_3$ (ce qui revient à remplacer le motif 2,0,1 par 3).
Il suffit alors de vérifier que le corps de la matrice $A = T_{(2,2,2,1,1,1,1,2,1,1,1,1,1,2,1,1,1,1)}$ est $\mathbb{Q}[\sqrt{2}]$. On a $A = \begin{pmatrix} 7918 & 12929 \\ 19159 & 31284 \end{pmatrix}$, donc $\mathrm{discr}(A) = 1536796800 = 2 \times 27720^2$. □

Remarque IV.6.3. *Il est possible de réécrire matriciellement sous une forme plus simple les suites de fractions continues données dans la proposition IV.6.1 :*

Le corps de la matrice $S_1(MT_i)^n S_2(MT_i)^n$ est $\mathbb{Q}[\sqrt{\mathrm{discr}(MT_i)}]$,

pour toute matrice symétrique M, pour tout entier $i \geq 1$, et pour tout entier n, où S_1 et S_2 sont deux symétries de $GL_2(\mathbb{Z})$, données par

$$\left\{ \begin{array}{l} S_1 = T_i^{-1} T_{i/2-1} T_1 T_1 T_{i/2} = \begin{pmatrix} -i-1 & -i^2/2 - i \\ 2 & i+1 \end{pmatrix} \\ S_2 = T_i^{-1} T_j^{-1} T_{j-1} T_1 T_1 = \begin{pmatrix} 1 & 2+i \\ 0 & -1 \end{pmatrix} \end{array} \right\} \textit{si } i \textit{ est pair,}$$

$$\left\{ \begin{array}{l} S_1 = T_i^{-1} T_{(i-1)/2} T_1 T_3 T_{(i-1)/2} = \begin{pmatrix} -2i+1 & -i^2+i \\ 4 & 2i-1 \end{pmatrix} \\ S_2 = T_i^{-1} T_j^{-1} T_{j+1} T_{j-1} T_j^{-1} = \begin{pmatrix} -1 & 1-i \\ 0 & 1 \end{pmatrix} \end{array} \right\} \textit{sinon,}$$

où j est un entier quelconque.

La proposition suivante nous donne l'existence, dans tout corps quadratique réel, d'une infinité de fractions continues périodiques qui n'utilisent que trois entiers différents.

Proposition IV.6.4. *Soit δ un entier non carré. Alors il existe un entier $s \geq 1$ tel que pour tout entier n,*

$$\overline{[2,1,1,1,(s,1,1,2,1,1)^n,s,1,2,1,1,1,1,s,(1,1,2,1,1,s)^n]} \in \mathbb{Q}[\sqrt{\delta}].$$

Corollaire IV.6.5. *Pour tout corps quadratique $\mathbb{Q}[\sqrt{\delta}]$, il existe un réel m_δ et une infinité de fractions continues périodiques $[\overline{a_0, a_1, ..., a_n}] \in \mathbb{Q}[\sqrt{\delta}]$ avec $1 \leq a_i \leq m_\delta$.*

Voici des exemples de suites de fractions continues qui ne comportent que les entiers 1 et 2 et qui restent dans un corps quadratique donné :

Exemple IV.6.6. *Pour tout entier n, la fraction continue périodique suivante est dans $\mathbb{Q}[\sqrt{7}]$:*

$$[\overline{2,1,1,1,(1,1,1,1,1,1,1,2,1,2)^n,1,1,1,1,2,1,(2,1,2,1,1,1,1,1,1,1)^n}].$$

Proposition IV.6.7. *Pour tout uplet symétrique d'entiers $\mathsf{S} = (a_1, a_2, ..., a_2, a_1)$, et pour tout entier n, la fraction continue périodique*

$$[\overline{2,1,1,1,(\mathsf{S},1,1,2,1,1)^n,\mathsf{S},1,2,1,1,1,1,\mathsf{S},(1,1,2,1,1,\mathsf{S})^n}]$$

est dans $\mathbb{Q}[\sqrt{\mathrm{discr}(T_{(a_1,a_2,...,a_2,a_1,1,1,2,1,1)})}]$.

En particulier en choisissant $\mathsf{S} = 1^{n-5}$ (c'est-à-dire l'entier 1 répété $n-5$ fois), on a des suites de fractions continues périodiques formées seulement des entiers 1 et 2 dans $\mathbb{Q}[\sqrt{f_n f_{n+2}}]$, pour tout $n \geq 3$, où $(f_n)_{n\in\mathbb{N}}$ est la suite de Fibonnacci, définie par $f_0 = 0$, $f_1 = 1$ et pour tout entier n positif ou nul $f_{n+2} = f_{n+1} + f_n$. Cela nous donne une infinité de corps quadratiques d'après le lemme suivant :

Lemme IV.6.8. *L'ensemble des corps quadratiques $\mathbb{Q}[\sqrt{f_n f_{n+2}}]$ est infini.*

Démonstration. Il est bien connu que pour tout n, les entiers f_n et f_{n+2} sont premiers entre eux. Montrons que pour tout nombre premier p, il existe un entier $n \geq 1$ tel que p divise f_n. La matrice T_1^n s'écrit : $T_1^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$, et si l'on note o l'ordre du groupe fini multiplicatif $GL_2(\mathbb{Z}/p\mathbb{Z})$, on a $T_1^o \equiv I_2 \pmod p$, donc f_o est divisible par p. Utilisons alors la propriété suivante des nombres de Fibonacci :

Propriétés IV.6.9. *Soit p un nombre premier impair, et soit $n \geq 1$ un entier. Si $q = p^k$ est la plus grande puissance de p divisant f_n, avec $k \geq 1$, alors pq est la plus grande puissance de p divisant f_{pn}.*

Démonstration. Comme $f_{n+1} = f_n + f_{n-1}$, on a $T_1^n \equiv cI_2 \pmod q$ pour $c = f_{n-1}$. On peut donc écrire $T_1^n = cI_2 + qA$, pour une matrice $A \in M_2(\mathbb{Z})$. On a alors

$$T_1^{pn} = (cI_2 + qA)^p = \sum_{i=0}^{p} \binom{p}{i} c^i (qA)^{p-i} \equiv c^p I_2 + pc^{p-1}qA \pmod{p^2 q}$$

puisque $p^2 q$ divise $\binom{p}{i} c^i (qA)^{p-i}$ dès que $i < p-1$. Donc on obtient $f_{np} \equiv pc^{p-1} f_n \pmod{p^2 q}$, et comme c est premier à p, cela donne bien que la plus grande puissance de p divisant f_{np} est qp. □

Ce dernier lemme permet d'obtenir, pour tout nombre premier p impair, un entier n pour lequel p divise le facteur sans carré de f_n et donc aussi le facteur sans carré de $f_n f_{n+2}$. On en déduit que l'ensembles des corps quadratiques $\mathbb{Q}[\sqrt{f_n f_{n+2}}]$ est infini. □

La proposition IV.6.7 est une conséquence immédiate de la proposition IV.6.1, mais voici une vérification directe :

Preuve de la proposition IV.6.7. Soient $S \in \Gamma$ symétrique, $A = ST_{(1,1,2,1,1)}$, $B = T_{(2,1,1,1)}$ et $C = ST_{(1,2,1,1,1,1)}S$. Soit alors $H = ST_1H_0$, la matrice donnée par le corollaire IV.4.5, où $H_0 = T_2 \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} T_2 = \begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix}$.

Pour obtenir le résultat, il suffit de montrer que $\mathrm{Tr}(T_1H_0M) = \mathrm{Tr}(T_{(1,1,2,1,1)}M)$, pour toute matrice M symétrique. En effet, en prenant $M = (ST_{(1,1,2,1,1)})^nS$, on obtient alors $\mathrm{Tr}(HA^n) = \mathrm{Tr}(A^{n+1})$ qui donne bien le résultat d'après la proposition IV.4.2 :

$$\begin{aligned}\mathrm{discr}(BA^nC\,{}^tA^n) &= \mathrm{Tr}^2(HA^n)(\mathrm{Tr}^2(HA^n) + 4\,\mathrm{Det}(S)\,\mathrm{Det}(A^n)) \\ &= \mathrm{Tr}^2(HA)(\mathrm{Tr}^2(A^{n+1}) - 4\,\mathrm{Det}(A^{n+1})) \\ &= \mathrm{Tr}^2(HA)\,\mathrm{discr}(A^{n+1}).\end{aligned}$$

Le signe $+\mathrm{Det}(S)$ qui apparaît devant le terme $\mathrm{Det}(A^n)$ dans la première des égalités ci-dessus est dû au fait que si B et C sont respectivement de la forme $N_B + \epsilon_B S_0$ et $N_C + \epsilon_C S_0$ pour des matrices N_B et N_C symétriques de rang 1, alors $\epsilon_B\epsilon_C = -\mathrm{Det}(S)$ (voir la remarque IV.4.3).

Or, l'égalité $\mathrm{Tr}(T_1H_0M) = \mathrm{Tr}(T_{(1,1,2,1,1)}M)$ pour toute matrice M symétrique découle simplement de la relation $T_1 \begin{pmatrix} 2 & 4 \\ 4 & 8 \end{pmatrix} - T_{(1,1,2,1,1)} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et du lemme IV.2.3. □

Vérification de l'exemple IV.6.6. On a à nouveau une suite de la forme $BA^nC\,{}^tA^n$ avec cette fois $A = T_{(1,1,1,1,1,1,1,2,1,2)}$, $B = T_{(2,1,1,1)}$ et $C = T_{(1,1,1,1,2,1)}$. On démontre pour tout n l'égalité suivante :

$$\mathrm{Tr}(H(T_{(1,1,1,1,1,1,1,2,1,2)})^n) = \mathrm{Tr}((T_{(1,1,1,4)})^{2n+1})$$

où $H = T_{(1,2)} \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} T_2 = \begin{pmatrix} 4 & 8 \\ 6 & 12 \end{pmatrix}$.

Le corps de la matrice $T_{(1,1,1,4)} = \begin{pmatrix} 2 & 9 \\ 3 & 14 \end{pmatrix}$ est bien $\mathbb{Q}[\sqrt{7}]$, donc cela donnera bien le résultat, d'après la proposition IV.5.1 et la remarque IV.5.2, et parce-qu'on est dans le cas où B et C sont toutes les deux des matrices de la forme $N+S_0$, avec N matrice symétrique de rang 1, et où $\mathrm{Det}(T_{(1,1,1,4)}) = 1$. D'après le lemme IV.3.4, comme $T_{(1,1,1,1,1,1,1,2,1,2)} = \begin{pmatrix} 47 & 128 \\ 76 & 207 \end{pmatrix}$ et $(T_{(1,1,1,4)})^2 = \begin{pmatrix} 31 & 144 \\ 48 & 223 \end{pmatrix}$ ont mêmes valeurs propres (car mêmes traces et mêmes déterminants), il suffit de démontrer cette égalité pour $n = 0$ et $n = 1$. Pour $n = 0$, on a $\mathrm{Tr}(H) = 16 = \mathrm{Tr}(T_{(1,1,1,4)})$. Pour $n = 1$, on a $\mathrm{Tr}(HT_{(1,1,1,1,1,1,1,2,1,2)}) = 4048 = \mathrm{Tr}((T_{(1,1,1,4)})^3)$. □

Preuve de la proposition IV.6.4. Il suffit de démontrer qu'étant donné un entier δ non carré, il existe un entier $s \geq 1$ tel que le corps de la matrice $T_{(1,1,2,1,1,s)}$ est $\mathbb{Q}[\sqrt{\delta}]$ (c'est ensuite un cas particulier de la proposition IV.6.7). Or, on a $\mathrm{discr}(T_{(1,1,2,1,1,s)}) = 48(s+1)(3s+4)$. Donc il suffit de prendre $s = 3y^2\delta - 1$ où (x, y) est une solution à l'équation de Pell-Fermat $x^2 - 9\delta y^2 = 1$. □

IV.6.1 Suites de type Wilson

On a vu comment l'on pouvait trouver des suites de fractions continues périodiques en cherchant les matrices H non inversibles du corollaire IV.4.5 à coefficients entiers. Cela revient à chercher $\mathrm{Tr}(HA)$ comme solution x entière de l'équation de Pell-Fermat $x^2 - \delta y^2 = \pm 4$. Un autre cas intéressant est celui où H est de la forme $\sqrt{\delta}H'$, avec H' entière, et où δ est le discriminant de la matrice A. On doit alors chercher $\mathrm{Tr}(H'A)$ comme solution y (et non plus x) de la même équation de Pell-Fermat, puisque l'on a alors $\mathrm{discr}(BAC\,{}^tA) = \delta(\mathrm{Tr}(H'A))^2(\delta(\mathrm{Tr}(H'A))^2 \pm 4)$, que l'on veut de la forme δx^2.

Wilson donne des suites qui rentrent dans ce cadre (voir (Wil80)), comme par exemple :

$$[\overline{(s(s+4)-1), 1, (s,1)^n, s+2, (s,1)^n, s+1}] \in \mathbb{Q}[\sqrt{s(s+4)}]$$

que l'on peut réécrire avec des entiers plus petits (en choisissant d'autres matrices B et C pour la même matrice H grâce au corollaire IV.4.5) :

$$[\overline{s, 1, s-1, s+1, (1,s)^n, 1, s+1, s+3, 1, (s,1)^n}] \in \mathbb{Q}[\sqrt{s(s+4)}]$$

Cependant, il sera impossible d'obtenir des suites uniformément bornées avec une borne indépendante de δ avec des suites de ce type, puisque si l'on a $H = P \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} Q$ avec $P, Q \in \Gamma$, alors la proposition IV.4.4 et le corollaire IV.4.5 montrent que l'on a nécessairement au moins un facteur T_i avec $i > \sqrt{\delta} - 1$ dans la décomposition de l'une des matrices B ou C.

IV.6.2 Réels quasi-palindromiques

À la vue du théorème I.2.5, on peut se demander quels sont les réels quasi-palindromiques, c'est-à-dire les réels qui ont un développement en fraction continue périodique quasi-palindromique. La proposition suivante, répond à la question :

Proposition IV.6.10. *Soit $x \in \mathbb{Q}[\sqrt{\delta}]$. On a équivalence entre :*

1. *x est quasi-palindromique,*
2. *$\mathrm{Tr}(x) = \lfloor x \rfloor$ et $x > 1$,*
3. *$\mathrm{Tr}(x) \in \mathbb{Z}$, $x > 1$ et $-1 < \overline{x} < 0$.*

On peut démontrer ce résultat en utilisant un lemme de É. Galois sur le miroir d'une fraction continue périodique (voir paragraphe 6, p. 83 dans (Per13)).

Les réels $\sqrt{\delta} + \left\lfloor \sqrt{\delta} \right\rfloor$ sont donc des exemples de réels palindromiques. Le résultat classique suivant donne une borne optimale sur le développement de ces réels :

Proposition IV.6.11. *Soit δ un entier positif sans facteur carré. Alors les coefficients du développement en fraction continue du réel $\sqrt{\delta} + \left\lfloor \sqrt{\delta} \right\rfloor$ sont majorés par $2\left\lfloor \sqrt{\delta} \right\rfloor$.*

Si l'on applique le théorème I.2.5 avec ce réel $\sqrt{\delta} + \left\lfloor \sqrt{\delta} \right\rfloor$, on obtient donc une infinité de fractions continues périodiques uniformément bornées par $4\left\lfloor \sqrt{\delta} \right\rfloor + 1$ dans le corps $\mathbb{Q}[\sqrt{\delta}]$. Cela améliore le résultat de Wilson, puisque la borne qu'il obtient est seulement en $O(\delta)$.

IV.7 Conjecture de Zaremba

Nous nous sommes intéressé au problème de majorer les coefficients de fractions continues périodiques. Voici une question similaire à propos des fractions continues finies. Voir (BK11) pour plus de détails.

Conjecture IV.7.1 (Zaremba). *Il existe une constante m telle que pour tout dénominateur $q \geq 1$, il existe un numérateur p premier à q tel que l'on ait*

$$\frac{p}{q} = [a_0, a_1, a_2, \dots]$$

où les entiers a_i sont entre 0 et m.

Cette conjecture est probablement vraie pour $m = 5$. Elle est sans doute même vraie pour $m = 2$, à condition d'exclure un nombre finie de dénominateurs q.

IV.7.1 Lien entre fractions continues et exposant critique

Nous nous proposons de montrer que cette conjecture de Zaremba est fausse quand on se restreint à des fractions continues ne comportant que les nombres 1 et 3. Plus généralement nous montrons le sens facile de la conjecture de Hensley, qui établit un lien entre cette conjecture de théorie des nombres et l'exposant critique de certains sous-semi-groupes de $SL(2, \mathbb{R})$.

a) Conjectures de Zaremba et de Hensley

Précisons les énoncés de la conjecture de Hensley, et du résultat que nous démontrons dans cette sous-section. Pour cela, introduisons quelques notations.

Notation . *Pour une partie $A \subseteq \mathbb{N}$, notons δ_A l'exposant critique du sous-semi-groupe Γ_A de $SL(2, \mathbb{R})$ engendré par les matrices $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ pour a décrivant A.*

Conjecture IV.7.2 (Hensley). *Soit $A \subseteq \mathbb{N}$. On a l'équivalence*

$$\delta_A > \tfrac{1}{2} \quad \Leftrightarrow \quad \begin{array}{l} \textit{Il existe deux constante } m \textit{ et } q_0 \textit{ telles que pour tout dénominateur } q \geq q_0, \textit{ il} \\ \textit{existe un numérateur } p \textit{ premier à } q \textit{ tel que le rationnel } \frac{p}{q} \textit{ ne comporte que} \\ \textit{des entiers de l'ensemble } A \textit{ dans son développement en fraction continue.} \end{array}$$

Remarque IV.7.3. *Cette conjecture implique celle de Zaremba pour $m = 2$, puisque l'on a*

$$\delta_{\{1,2\}} = 0,531280506277205141624468 6... > \frac{1}{2}.$$

Cette approximation a été obtenue grâce à Jenkinson et Pollicott, voir (JP01). Voir aussi (Hen96), p.16.

Voir (BK11) pour plus de détails sur cette conjecture. Nous allons montrer le résultat suivant, qui est le sens facile de l'équivalence donnée par la conjecture de Hensley.

Proposition IV.7.4. *Soit $A \subseteq \mathbb{N}$ une partie finie telle que $\delta_A < \frac{1}{2}$, alors il existe une infinité d'entiers q tels qu'il n'existe pas d'entier p tel que le développement en fraction continue périodique du rationnel $\frac{p}{q}$ ne comporte que des nombres de l'ensemble A.*

Autrement dit, on démontre que la conjecture de Zaremba est fausse si l'on impose que les développements en fractions continues ne comportent que des nombres dans l'ensemble fini A quand celui-ci est tel que $\delta_A < \frac{1}{2}$. Ce résultat est déjà connu depuis Hensley (voir (BK11)) mais je présente tout de même une preuve ici pour mettre en lumière le rôle de l'exposant critique.

Remarque IV.7.5. *Quand Γ_A agit sur le demi-plan de Poincaré, l'ensemble limite Λ_{Γ_A} est exactement l'ensemble des réels n'ayant que des nombres de l'ensemble A dans leur développement en fraction continue infini.*

Remarque IV.7.6. *L'ensemble des rationnels n'ayant que des nombres de l'ensemble A dans leur développement en fraction continue est presque en bijection avec l'ensemble des matrices de Γ_A par l'application :*

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \mapsto \frac{p}{q},$$

d'inverse :

$$[a_1, a_2, ..., a_n] \mapsto \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot ... \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Le fait que ce ne soit pas une bijection vient de la non unicité du développement en fraction continue d'un rationnel : il y a toujours exactement deux développements en fraction continue pour un rationnel (sauf pour 1).

On voit donc que pour compter ces nombres rationnels, il suffit de compter les points de l'orbite $\Gamma_A x$ d'un point x dans une boule. L'exposant critique va alors correspondre à la « dimension » de l'ensemble de ces rationnels.

b) Lemmes préliminaires

Soit Γ un semi-groupe. Pour démontrer la proposition IV.7.4, nous allons introduire :

Notation . *Pour une fonction $f : \Gamma \to \mathbb{R}$, on notera $c_f : \mathbb{R} \to \mathbb{R}$ la fonction définie par :*

$$\forall n \in \mathbb{R}, \quad c_f(n) = \#\{\gamma \in \Gamma | f(\gamma) \leq n\}$$

Définition IV.7.7. *Soit $\delta > 0$ un réel. On définit l'ensemble $\mathbb{F}_\delta$ des fonctions de dimension δ par :*

$$f : \Gamma \to \mathbb{R} \in \mathbb{F}_\delta \quad \Longleftrightarrow \quad \limsup_{n\to\infty} \frac{\log(c_f(n))}{\log(n)} = \delta \ .$$

On appellera dimension de f et on notera δ_f l'unique réel δ tel que la fonction f soit de dimension δ (i.e. $f \in \mathbb{F}_\delta$).

Notation . *Pour deux fonctions $f, g : \Gamma \to \mathbb{R}$, on notera $f \asymp g$ s'il existe une constante $C > 0$ telle que*

$$\frac{1}{C} f(n) \leq g(n) \leq C f(n)$$

pour n assez grand.

Lemme IV.7.8. *Pour deux fonctions $f, g : \Gamma \to \mathbb{R}$, on a*

$$f \asymp g \quad \Longrightarrow \quad \delta_f = \delta_g \ .$$

Démonstration. Supposons que l'on ait $\frac{1}{C} f(n) \leq g(n) \leq C f(n)$ pour une constante $C > 0$ et pour $n \geq n_0$. On a alors les inégalités $c_{Cf}(n) - M \leq c_g(n) \leq c_{\frac{1}{C}f}(n) + M$, pour une constante M dépendant de n_0. Cela devient :

$$c_f(\frac{n}{C}) - M \leq c_g(n) \leq c_f(Cn) + M \ .$$

En faisant un changemenent de variable, on a alors

$$\limsup_{n\to\infty} \frac{\log(c_f(\frac{n}{C})) - M}{\log(n)} = \limsup_{n\to\infty} \frac{\log(c_f(n))}{\log(Cn)} = \limsup_{n\to\infty} \frac{\log(c_f(n))}{\log(n)} = \delta_f \ ,$$

et de même avec le terme de droite. On obtient donc $\delta_f = \delta_g$. □

Lemme IV.7.9. *Si une fonction $f : \Gamma \to \mathbb{R}$ est de dimension δ, alors f^k est de dimension $\frac{1}{k}\delta$, où k est un réel strictement positif.*

Démonstration.

$$\delta_{f^k} = \limsup_{n\to\infty} \frac{\log(c_{f^k}(n))}{\log(n)} = \limsup_{n\to\infty} \frac{\log(c_f(n^{1/k}))}{\log(n)} = \limsup_{n\to\infty} \frac{\log(c_f(n))}{\log(n^k)} = \frac{1}{k}\delta_f \ .$$

□

c) Preuve de la proposition IV.7.4

Dans cette partie, on donne une preuve de la proposition IV.7.4. Dans toute la partie le semi-groupe Γ considéré sera Γ_A pour une partie finie $A \subseteq \mathbb{N}$ tel que $\delta_A < \frac{1}{2}$.

Définissons les fonctions suivantes de Γ dans $\mathbb{R}$:

$$f : \begin{pmatrix} p & r \\ q & s \end{pmatrix} \mapsto q,$$

$$\mathrm{Tr} : \begin{pmatrix} p & r \\ q & s \end{pmatrix} \mapsto p + s,$$

$$g : \gamma \mapsto \exp(d(i, \gamma i)),$$

$$h : \begin{pmatrix} p & r \\ q & s \end{pmatrix} \mapsto \sqrt{(q-r)^2 + (p+s)^2},$$

où $d(i, \gamma i)$ est la distance hyperbolique entre les points i et γi du demi-plan de Poincaré $\mathbb{H}^2_{\mathbb{R}}$.

Lemme IV.7.10. *Les fonctions $f, \mathrm{Tr}, \sqrt{g}$ et h ont même dimension.*

Démonstration. Soit $m := \max A$ et $\gamma = \begin{pmatrix} p & r \\ q & s \end{pmatrix} \in \Gamma$. On a alors les inégalités $p \geq q \geq s$ ainsi que $\frac{p}{m} \leq q \leq ms$, sauf pour un nombre fini d'éléments de Γ. On a donc

$$\frac{1}{2m}\mathrm{Tr} - M \leq f \leq \frac{1}{2}\mathrm{Tr} + M$$

pour une constante M, et donc par le lemme IV.7.8 les fonctions f et Tr ont même dimension.

De même, on a $\mathrm{Tr} \leq h \leq \sqrt{2}\,\mathrm{Tr}$, donc les fonctions h et Tr ont même dimension.

Montrons la dernière égalité. À l'aide de l'application $\begin{cases} \mathbb{H}^2_{\mathbb{R}} & \to & \mathbb{D} \\ z & \mapsto & \frac{iz+1}{z+i} \end{cases}$, on obtient à partir de γ une matrice γ' de $SU(1,1)$ qui agit par homographie sur le disque de Poincaré (et non plus sur le demi-plan) :

$$\gamma' = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \text{ où } \alpha = \frac{i(r-q) - (p+s)}{2} \text{ et } \beta = \frac{i(s-p) - (q+r)}{2}\ .$$

On a alors $d(i, \gamma i) = d_{\mathbb{D}}(0, \gamma' 0) = 2\,\mathrm{argth}(\frac{\alpha}{\beta})$, où $d_{\mathbb{D}}$ est la distance du disque de Poincaré. Comme on a l'égalité $|\alpha|^2 - |\beta|^2 = 1$, on obtient

$$d(i, \gamma i) = 2\,\mathrm{argth}(\sqrt{1 - \frac{1}{|\alpha|^2}})\ .$$

On a $2|\alpha| = h(\gamma)$, et il suffit donc pour terminer cette preuve de montrer

$$\exp(\operatorname{argth}\left(\sqrt{1-\frac{1}{|\alpha|^2}}\right)) \asymp |\alpha| \ . \tag{IV.3}$$

Pour obtenir cela, on a $\sqrt{1-\frac{1}{|\alpha|^2}} = 1 - \frac{1}{2|\alpha|^2} + O(\frac{1}{|\alpha|^4})$ qui nous donne :

$$\operatorname{argth}\left(\sqrt{1-\frac{1}{|\alpha|^2}}\right) = \frac{1}{2}\ln(\frac{2+O(\frac{1}{|\alpha|^2})}{\frac{1}{2|\alpha|^2}+O(\frac{1}{|\alpha|^4})}) = \frac{1}{2}\ln(4|\alpha|^2+O(1))$$

Ce qui donne bien la relation (IV.3) voulue. □

Lemme IV.7.11. *La dimension de la fonction $g : \gamma \mapsto \exp(d(i,\gamma i))$ est égale à l'exposant critique du semi-groupe Γ.*

Démonstration. Par définition, l'exposant critique du semi-groupe Γ est

$$\delta_\Gamma = \limsup_{n\to\infty} \frac{\log(c_g(e^n))}{n} \ ,$$

qui est égal à $\limsup_{n\to\infty} \frac{\log(c_g(n))}{\log(n)} = \delta_g$. □

Preuve de la proposition IV.7.4. D'après les lemmes IV.7.11, IV.7.10 et IV.7.9, la dimension de la fonction f est égale au double de l'exposant critique du semi-groupe Γ qui est strictement inférieur à $\frac{1}{2}$. On peut donc trouver des réels n_0 et $c < 1$ tels que pour tout réel $n \geq n_0$ on ait $\frac{\log(c_f(n))}{\log(n)} \leq c$. Soit $\mathbb{Q}_A$ l'ensemble des rationnels ne faisant apparaître que des nombre de l'ensemble A dans leur développement en fraction continue. On a alors, pour n assez grand :

$$\#\left\{\frac{p}{q} \in \mathbb{Q}_A \mid q \leq n\right\} \leq c_f(n) \leq n^c < \frac{n}{2}.$$

On en déduit alors l'existence d'un dénominateur q entre $\frac{n}{2}$ et n, pour lequel il n'existe pas de numérateur p tel que la fraction $\frac{p}{q}$ soit irréductible et dans $\mathbb{Q}_A$. □

Exemple IV.7.12. *La proposition IV.7.4 s'applique pour $A = \{1,3\}$.*

Autrement dit, la conjecture de Zaremba est fausse si l'on impose que les nombres qui apparaîssent dans les développements en fractions continues soient 1 ou 3.

Démonstration. On a $\delta_{\{1,3\}} = \dim_H(\Lambda_{\Gamma_{\{1,3\}}})$, d'après le corollaire I.2.17 et la proposition II.2.9 puisque le semi-groupe $\Gamma_{\{1,3\}}$ est contractant et séparé, et on a

$$\dim_H(\Lambda_{\Gamma_{\{1,3\}}}) \approx 0,4544890776618 < \frac{1}{2}$$

d'après (JP01). □

On aurait aussi put prendre $A = \{2, 3\}$, $A = \{2, 4\}$, etc...

IV.7.2 Lien entre fractions continues périodiques et fractions continues finies

Nous allons montrer le théorème I.2.4, qui dit que la conjecture de Zaremba sur les développements en fractions continues de rationnels dont on fixe le dénominateur implique la conjecture I.2.2 de McMullen sur les développement en fractions continues périodiques qui sont dans un corps donné. Cela découlera du résultat nouveau suivant :

Théorème IV.7.13. *Soient a, b, c et δ des entiers strictement positifs tels que*
- *b et c sont solution de l'équation de Pell-Fermat : $c^2 - \delta b^2 = \pm 1$,*
- *a et c sont premiers entre eux et $a < c$.*

Alors on a l'une des égalités

$$\frac{c - a + b\sqrt{\delta}}{c} = \overline{[1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n, 1, 1, a_n - 1, a_{n-1}, a_{n-2}, \ldots, a_2, a_1]}$$

ou

$$\frac{c - a + b\sqrt{\delta}}{c} = \overline{[1, 1, a_1 - 1, a_2, a_3, \ldots, a_{n-1}, a_n - 1, 1, 1, a_n, a_{n-1}, a_{n-2}, \ldots, a_2, a_1]},$$

où $[0, a_1, a_2, \ldots, a_{n-1}, a_n]$ est le développement en fraction continue du rationnel $\frac{a}{c}$.

Si l'on a des entiers nuls dans la fraction continue donnée par ce théorème (c'est le cas si $a_1 = 1$ ou $a_n = 1$), il suffit de remplacer chaque triplet $x, 0, y$ par $x + y$ pour obtenir une vraie fraction continue.

Preuve de Zaremba $\Rightarrow$ Conjecture I.2.2. Soit m la constante donnée par la conjecture de Zaremba, et soit δ un entier non carré. L'équation de Pell-Fermat $c^2 - \delta b^2 = 1$ admet alors une infinité de solutions (b, c). Pour chaque entier c assez grand d'un tel couple solution, on choisit alors un numérateur p, donné par la conjecture de Zaremba, tel que le développement en fraction continue du rationnel $\frac{p}{c}$ ne s'écrive qu'avec des 1 et des 2. Si l'on choisit pour a le reste de la division de p par c, alors le théorème IV.7.13 nous donne une fraction continue périodique bornée par $m + 1$ et dans le corps $\mathbb{Q}[\sqrt{\delta}]$. On obtient bien une infinité de fractions continues périodiques dans un même corps $\mathbb{Q}[\sqrt{\delta}]$, puisque pour deux rationnels $\frac{a}{c}$ distincts, le théorème donne deux fractions continues périodiques distinctes. □

Preuve du théorème IV.7.13. Remarquons que les fractions continues données par le théorème s'écrivent matriciellement sous la forme

$$BAC\,{}^tA,$$

où $A := T_{(a_1,a_2,\dots,a_n)}$ est la matrice correspondant au développement du rationnel $\frac{c}{a}$, $B := T_{(1,1,a_1-1)}{T_{a_1}}^{-1}$ et $C := \begin{cases} T_{(1,1,a_n-1)}{T_{a_n}}^{-1} \\ \text{ ou} \\ {T_{a_n}}^{-1}T_{(a_n-1,1,1)} \end{cases}$.

Un rapide calcul donne $B = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$ et $C = B$ ou ${}^tB$. Nous sommes donc dans le cadre de la proposition IV.4.2, avec $H := \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$, ce qui nous donne le discriminant

$$\operatorname{discr}(BAC\,{}^tA) = \operatorname{Tr}^2(HA)(\operatorname{Tr}^2(HA) \pm 4).$$

Or, la matrice A peut s'écrire sous la forme $A = \begin{pmatrix} u & a \\ v & c \end{pmatrix}$, pour des entiers u et v, puisque c'est la matrice correspondant au développement en fraction continue du rationnel irreductible $\frac{c}{a}$. On a donc $\operatorname{Tr}(HA) = 2c$, et donc $\operatorname{discr}(BAC\,{}^tA) = 4c^2(4c^2 \pm 4)$. En choisissant le signe, quitte à choisir $C = B$ ou $C = {}^tB$, on a donc finalement

$$\operatorname{discr}(BAC\,{}^tA) = 16c^2b^2\delta,$$

puisque (b, c) est solution de l'équation de Pell-Fermat $c^2 - \delta b^2 = \pm 1$. Ainsi, le corps de la matrice $BAC\,{}^tA$ est bien $\mathbb{Q}[\sqrt{\delta}]$ comme annoncé, quitte à transposer C.

Pour vérifier l'égalité annoncée, on vérifie que le réel quadratique $x := \frac{c-a+b\sqrt{\delta}}{c}$ correspond (par la proposition IV.1.3) à la matrice

$$BAC\,{}^tA = \begin{pmatrix} 2ac \pm 1 & 2c^2 \\ 4ac - 2a^2 \pm 2 & 4c^2 - 2ac \pm 1 \end{pmatrix}$$

c'est-à-dire que le vecteur $\begin{pmatrix} 1 \\ x \end{pmatrix}$ est bien un vecteur propre. □

Grâce au théorème IV.7.13, pour obtenir la conjecture I.2.1 de McMullen, il suffit de démontrer la variante suivante de la conjecture de Zaremba, où l'on impose en plus les premiers et le dernier entiers du développement en fraction continue.

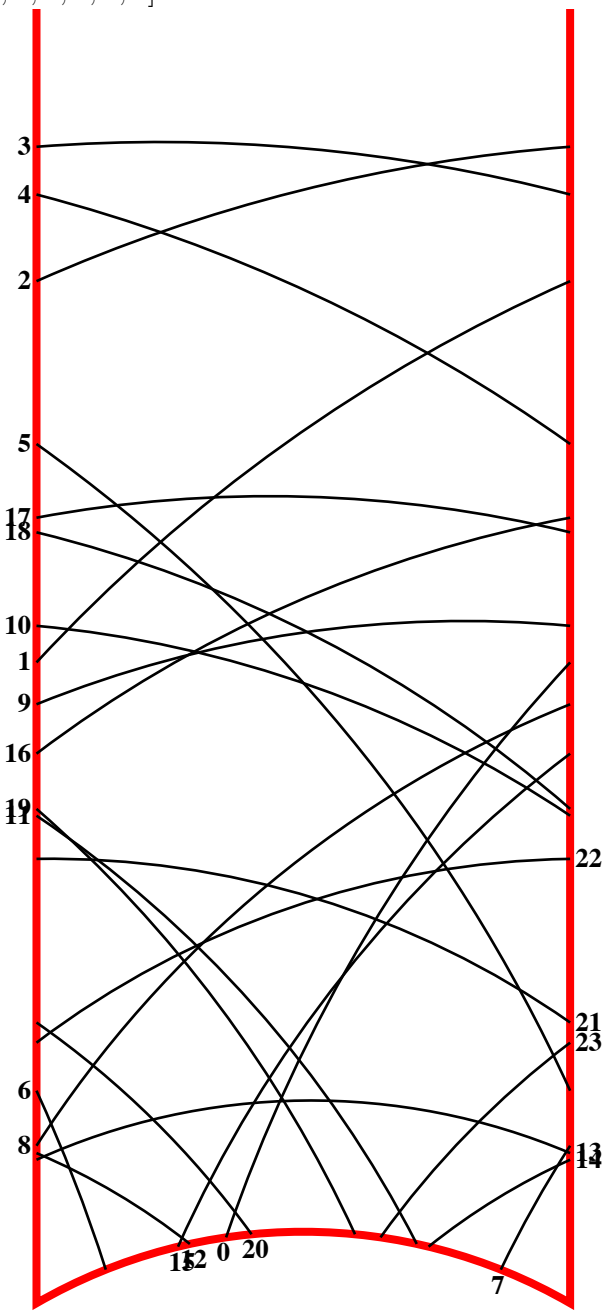
Conjecture IV.7.14. *Il existe un entier q_0 tel que pour tout entier $q \geq q_0$, il existe un entier p premier à q tel que l'on ait*

$$\frac{p}{q} = [a_0, a_1, a_2, \dots, a_{n-1}, a_n]$$

où les entiers a_i valent chacun 1 ou 2, et avec de plus les conditions $a_1 = 2$ et $a_n = 2$.

Remarque IV.7.15. *C'est en cherchant, par ordinateur, des fractions continues de la forme donnée par cette conjecture que nous sommes parvenu à vérifier la conjecture I.2.2 de McMullen pour tous les corps quadratiques $\mathbb{Q}[\sqrt{\delta}]$ pour $\delta < 127$.*

FIGURE IV.1 – Géodésique fermée de la surface modulaire qui correspond à la fraction continue périodique $[\overline{5, 1, 3, 2, 4, 3}]$.



Annexe A

Sous-semi-groupes paraboliques de $SL(2,\mathbb{R})$

Dans cette annexe, nous présentons des résultats que nous avons pu généraliser aux semi-groupes sans même avoir à changer la preuve qui existait pour les groupes. Nous notons $\mathbb{H}^2_{\mathbb{R}}$ le modèle du demi-plan de Poincaré usuel et $d(.,.)$ la distance hyperbolique usuelle. Commençons par un exemple de semi-groupe dont on connait l'exposant critique.

Lemme A.0.16. *Soit $p \in SL(2,\mathbb{R})$ un élément parabolique. Alors le semi-groupe $P :=< p >$ engendré par p a pour exposant critique $\frac{1}{2}$ et est divergent.*

Démonstration. Soit $x \in \mathbb{H}^2_{\mathbb{R}}$ un point. Montrons l'égalité :

$$d(x, p^n x) = \log(n^2)(1 + \epsilon(n)).$$

Quitte à tout conjuguer par une isométrie qui envoie le point fixe de p à l'infini, on peut se ramener à $p : z \mapsto z + r$ pour un réel r, et à $x = i \in \mathbb{H}^2_{\mathbb{R}}$. La géodésique reliant les points i et $p^n(i) = i + nr$ est alors un arc de cercle de rayon euclidien $R_n \sim \frac{nr}{2}$, et de centre euclidien $c_n \sim \frac{nr}{2}$. Soit α l'angle entre l'axe réel et le segment euclidien $[i, c_n]$. On a

$$d(i, i + nr) = \int_{\alpha}^{\pi-\alpha} \frac{dt}{\sin(t)} = 2\,\mathrm{argth}(\cos(\alpha)) = \log(\frac{2 + \epsilon(n)}{\frac{2}{n^2} + \epsilon(n)}) \sim \log(n^2).$$

La série de Poincaré $h_{Px}(x)$ est donc de même nature que la série

$$\sum_{n\geq 1} e^{-s\log(n^2)} = 2\sum_{n\geq 1} \frac{1}{|n|^{2s}}.$$

qui a pour exposant critique $\frac{1}{2}$ et diverge en $s = \frac{1}{2}$. □

Remarque A.0.17. *Cet exemple de semi-groupe montre que dans le corollaire I.2.17, l'hypothèse que l'ensemble limite du semi-groupe Γ contienne au moins deux points est*

indispensable. En effet, il s'agit d'un contre-exemple puisque l'on a

$$\frac{1}{2} = \delta_\Gamma \neq \dim_H(\Lambda_\Gamma) = 0.$$

La proposition suivante permet d'obtenir une information sur l'exposant critique simplement en sachant l'existence d'un élément parabolique dans le semi-groupe. On retrouve ce résultat dans un cadre plus général mais seulement pour les groupes : il s'agit d'un théorème de Dal'Bo-Otal-Peigné dont on peut trouver par exemple trouver l'énoncé dans (Sch04).

Proposition A.0.18. *Si Γ est un sous-semi-groupe de $SL(2,\mathbb{R})$ dont l'ensemble limite contient au moins deux points, et contenant un élément parabolique, alors on a l'inégalité stricte*

$$\delta_\Gamma > \frac{1}{2}.$$

Démonstration. L'inégalité large $\delta_\Gamma \geq \frac{1}{2}$ découle facilement du lemme précédent. Montrons l'inégalité stricte. Pour cela, on va montrer les lemmes :

Lemme A.0.19. *Le semi-groupe Γ contient un élément hyperbolique.*
De plus, si p est un élément parabolique, on peut demander à ce que le point fixe attracteur de cet élément hyperbolique soit distinct du point fixe de l'élément parabolique p.

Démonstration. Cela découle immédiatement du lemme II.3.2. □

Lemme A.0.20. *Le semi-groupe Γ contient un produit libre $P * H$, d'un semi-groupe P engendré par un élément parabolique, par un semi-groupe H engendré par un élément hyperbolique.*

Démonstration. Le semi-groupe Γ contient par hypothèse un élément parabolique p, et par le lemme précédent, il contient également un élément hyperbolique h dont le point fixe attracteur est distinct du point fixe de p. Quitte à remplacer chacun des éléments p et h par des puissances, on peut supposer qu'ils sont suffisamment contractants pour pouvoir éffectuer un ping-pong. C'est-à-dire qu'il existe deux parties A et B et un point $x \notin A \cup B$ vérifiants les propriétés :

1. Les parties A et B sont disjointes.
2. Pour tout $n \in \mathbb{N}\backslash\{0\}$, on a les inclusions

$$p^n(B \cup \{x\}) \subseteq A,$$

$$h^n(A \cup \{x\}) \subseteq B.$$

On conclut alors en remarquant que si $p^{n_1}h^{m_1}\dots p^{n_r}h^{m_r}x = x$, avec un entier $r \geq 2$ et des entiers positifs n_i et m_i non nuls sauf éventuellement m_r et n_1, alors on a $p^{n_1}h^{m_1}\dots p^{n_r}h^{m_r}x \in A \cup B$, ce qui est absurde. Donc le produit $< p > * < h >$ est libre. □

On dispose donc d'un produit libre $P * H$ dans Γ, où $P =< p >$ est engendré par un parabolique et $H =< h >$ est engendré par un hyperbolique. On peut alors écrire tout élément γ de ce produit libre $P * H$ sous la forme

$$\gamma = p_1 h^{n_1} p_2 h^{n_2} \dots p_k h^{n_k}$$

pour des éléments p_1, p_2,..., p_k de P et des entiers $n_i \in \mathbb{N}$. Pour un point $x \in \mathbb{H}^2_{\mathbb{R}}$, la série de Poincaré $h_{P*Hx}(x)$ du semi-groupe $P * H$ s'écrit donc

$$\begin{aligned}\sum_{\gamma \in P*H} e^{-sd(x,\gamma x)} &= \sum_{k=1}^{\infty} \sum_{(p_1,\dots,p_k)\in P^k} \sum_{(n_1,\dots,n_k)\in \mathbb{N}^k} e^{-sd(x,p_1 h^{n_1} p_2 h^{n_2} \dots p_k h^{n_k} x)} \\ &\geq \sum_{k=1}^{\infty} \sum_{(p_1,\dots,p_k)\in P^k} \sum_{(n_1,\dots,n_k)\in \mathbb{N}^k} e^{-sd(x,p_1 x)} e^{-sd(x,h^{n_1} x)} \dots e^{-sd(x,p_k x)} e^{-sd(x,h^{n_k} x)} \\ &= \sum_{k=1}^{\infty} \left(\sum_{p\in P} e^{-sd(x,px)} \sum_{n\in\mathbb{N}} e^{-sd(x,h^n x)} \right)^k .\end{aligned}$$

Comme le semi-groupe P a pour exposant critique $\frac{1}{2}$, on peut trouver un réel $s > \frac{1}{2}$ suffisamment proche de $\frac{1}{2}$ pour avoir

$$\sum_{p\in P} e^{-sd(x,px)} \sum_{n\in\mathbb{N}} e^{-sd(x,h^n x)} > 1.$$

On obtient alors que la série de Poincaré du semi-groupe $P * H$ et donc du semi-groupe Γ diverge. □

FIGURE A.1 – Ensemble limite d'un sous-semi-groupe de $SL(2,\mathbb{C})$ engendré par deux éléments paraboliques.

Table des figures

Bibliographie

[Ben08] Y. Benoist – « Réseaux des groupes de Lie », cours de M2 à Paris 6, 2007-2008.

[Ber79] J. Berstel – *Transductions and context-free languages*, Teubner Verlag, 1979.

[BK11] J. Bourgain & A. Kontorovich – « On Zaremba's conjecture », *arXiv* (2011).

[BL85] P. Bougerol & J. Lacroix – *Products of random matrices with applications to Schrödinger operators*, Birkhäuser, 1985.

[Bow08] L. Bowen – « Free groups in lattices », *arXiv* (2008).

[Cai05] A. Cain – « Presentations for subsemigroups of groups », Thèse, University of St Andrews, 2005.

[Car08] O. Carton – *Langages formels, calculabilité et complexité*, Vuibert, 2008.

[CI99] K. Corlette & A. Iozzi – « Limit sets of discrete groups of isometries of exotic hyperbolic spaces », *Amer. Math. Soc.* **351** (1999), no. 4, p. 1507–1530.

[CN08] J. Cassaigne & F. Nicolas – « On the decidability of semigroup freeness », 2008.

[Coo93] M. Coornaert – « Mesures de Patterson-Sullivan sur le bord d'un espace hyperbolique au sens de Gromov », *Pacific J. Math.* **159** (1993), no. 2, p. 241–270.

[Doy88] P. Doyle – « On the bass note of a Schottky group », *Acta Math.* **160** (1988), p. 249–284.

[EC+92] D. Epstein, J. Cannon et al. – *Word processing in groups*, Jones and Barlett, 1992.

[Fal89] K. Falconer – *Dimensions and measures of quasi self-similar sets*, vol. 106, Proc. Amer. Math. Soc., 1989.

[Fed69] H. Federer – *Geometric measure theory*, Springer, 1969.

[GdlH+90] E. Ghys, P. de la Harpe et al. – *Sur les groupes hyperboliques d'après Mikhael Gromov*, Progr. Math. éd., vol. 83, Birkhäuser, 1990.

[Ghy06] E. Ghys – « Poincaré et son disque », in *L'héritage scientifique de Henri Poincaré*, Belin, 2006.

[Hae12] T. Haettel – « Compactification de chabauty de l'espace des sous-groupes de cartan de $SL_n(\mathbb{R})$ », *Mathematische Zeitschrift* (2012).

[Hen96] D. Hensley – « A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets », *journal of number theory* **58** (1996), no. 58, p. 9–45.

[HLV07] I. Holopainen, U. Lang & A. Vähäkangas – « Dirichlet problem at infinity on Gromov hyperbolic metric measure spaces », *Math. Ann.* **339** (2007), p. 101–134.

[JP01] O. Jenkinson & M. Pollicott – « Computing the dimension of dynamically defined sets I : E_2 and bounded continued fractions », *Erg. Theo. Dyn. Syst.* **21** (2001), p. 1429–1445.

[Kap07] M. Kapovich – « Kleinian groups in higher dimensions », *Prog. Math.* **265** (2007), p. 485–562.

[Ken97] R. Kenyon – « Projecting the one-dimensional Sierpinski gasket », *Israel J. Math.* (1997), p. 221–238.

[Lal97] S. Lalley – « β-expansions with deleted digits for Pisot numbers β », *Trans. Amer. Math. Soc.* **349** (1997), p. 4355–4365.

[Lan70] S. Lang – *Algebraic number theory*, vol. 110, Springer, 1970.

[McM09] C. T. McMullen – « Uniformly Diophantine numbers in a fixed real quadratic field », *Compositio Math.* **145** (2009), p. 827–844.

[Mer09] P. Mercat – *Un théorème de Patterson et Sullivan*, Mémoire, É.N.S., 2009.

[Pat76] S. J. Patterson – « The limit set of a Fuchsian group », *Acta Math.* **136** (1976), p. 241–273.

[Pau97] F. Paulin – « On the critical exponent of a discrete group of hyperbolic isometries », in *Diff. Geom. and its Appl.*, vol. 7, Elsevier, 1997, p. 231–236.

[Per13] O. Perron – *Die Lehre von den Kettenbrüchen*, B.G. Teubner, 1913.

[Qui06] J.-F. Quint – « An overview of Patterson-Sullivan theorie », cours Zurich, 2006.

[Rob03] T. Roblin – *Ergodicité et équidistribution en courbure négative*, vol. 95, Mémoires Soc. Math. France, 2003.

[Rud21] W. Rudin – *Functional analysis*, McGraw Hill, 1921.

[Sak87] J. Sakarovitch – « Easy multiplications I. the realm of Kleene's theorem », *Information and Computation* **74** (1987), p. 173–197.

[Sch04] B. Schapira – « Lemme de l'ombre et non divergence des horosphères d'une variété géométriquement finie », *Ann. Inst. Fourier* **54** (2004), no. 4, p. 939–989.

[Sul79] D. Sullivan – « The density at infinity of a discrete group of hyperbolic motions », *Pub. Math. I.H.E.S.* **50** (1979), p. 171–202.

[Wil80] S. Wilson – « Limit points in the Lagrange spectrum of a quadratic field », *Bull. S.M.F.* **108** (1980), p. 137–141.

Mathématiques

Laboratoire de Topologie et dynamique
Bâtiment 425
Faculté des Sciences d'Orsay
Université Paris-Sud 11
F-91405 Orsay Cedex
FRANCE