PETITS SOUS-GROUPES DE $\mathrm{SL}(2,\mathbb{R})$

SAMUEL BRONSTEIN

Dans cet exposé, on s'intéresse aux "petits" sous-groupes de $\mathrm{SL}(2,\mathbb{R})$, et par petit nous entendons avec un petit nombre de générateurs. En particulier, on s'intéressera aux sous-groupes engendrés par 2 matrices de $\mathrm{SL}(2,\mathbb{R})$. Les ressources utilisées sont diverses sources accessibles en ligne, ainsi que les notes d'Yves Benoist sur le sujet [Ben97]. Ce texte consiste en les notes d'un exposé donné le 17 mai 2024 à l'ENS, dans le cadre de la Journée CPGE - ENS 2024.

1. Introduction à la géométrie hyperbolique

Définition 1.1 (Demi-plan de Poincaré)**.** Le demi-plan de Poincaré, noté $\mathcal{H}$, est le demi-plan supérieur de $\mathbb{C}$:

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}\,. \tag{1.1}$$

On s'intéresse à l'acion de $\mathrm{SL}(2,\mathbb{R})$ sur $\mathcal{H}$ par homographies:

Proposition 1.2. *Le groupe* $\mathrm{SL}(2,\mathbb{R})$ *agit sur le demi-plan supérieur par la formule suivante:*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}\,. \tag{1.2}$$

Cette action s'étend naturellement au bord de $\mathcal{H} = \mathbb{R} \cup \{\infty\}$.

Un attrait de cette action est qu'elle préserve les cercles de $\mathcal{H}$. Pour voir cela, nous utilisons le fait que l'inversion de $\mathbb{C}^*$ préservent les cercles ou droites de $\mathbb{C}$.

Définition 1.3 (Modèle du disque de Poincaré)**.** Le disque de Poincaré, noté $\mathbb{D}$, est le disque unité ouvert de $\mathbb{C}$. Il est difféomorphe à $\mathcal{H}$ via l'application suivante:

$$f : \begin{cases} \mathbb{D} & \to \mathcal{H} \\ z & \mapsto \frac{1}{z-i} \end{cases}\,. \tag{1.3}$$

Remark 1.1. L'application $z \mapsto \frac{1}{\bar{z}}$, définie de $\mathbb{C}^*$ vers lui-même, préserve les cercles/droites. En effet, un cercle ou une droite est caractérisé par une équation du type suivant:

$$a|z|^2 + \Re(zw) + c = 0\,,$$

avec a, c réels et $w \in \mathbb{C}$ fixé. Si $a = 0$, c'est l'équation d'une droite affine de $\mathbb{C}$, et si $b = 0$, c'est l'équation d'un cercle centré en 0. Notons $\mathcal{C}_{a,w,c}$ un tel cercle ou droite. On s'aperçoit alors que $z \in \mathcal{C}_{a,w,c}$ si et seulement si $\frac{1}{\bar{z}} \in \mathcal{C}_{c,w,a}$. Comme la conjugaison est une réflexion par rapport à l'axe des abscisses, elle préserve aussi les cercles/droites. On en déduit que les cercles/droites de $\mathbb{D}$ sont envoyés par f sur les cercles/droites de $\mathcal{H}$.

Comme corollaire, on en déduit que l'action de $\mathrm{SL}(2,\mathbb{R})$ envoie un cercle/droite sur un cercle/droite.

Date: 17 mai 2024.

Corollaire 1.4. *L'action de* $\mathrm{SL}(2,\mathbb{R})$ *envoie un cercle/droite sur un cercle/droite de* $\mathcal{H}$.

Proof. Utilisons la décomposition polaire: soit A une matrice de $\mathrm{SL}(2,\mathbb{R})$. On peut toujours la décomposition $A = R_\theta \cdot P$, avec $R_\theta \in \mathrm{SO}(2)$ la matrice de rotation d'angle θ et P une matrice triangulaire supérieure. L'action de P sur $\mathcal{H}$ correspond à une dilatation composée avec une translation, donc elle préserve bien les cercles/droites. Pour comprendre l'action de R_θ, on regarde l'action correspondante sur $\mathbb{D}$ et on remarque que sur $\mathbb{D}$ cette action est bien une rotation euclidienne d'angle θ. Encore une fois, elle préserve les cercles/droites de $\mathbb{D}$, qui sont bien envoyés sur les cercles/droites de $\mathcal{H}$ par f, donc A préserve bien les cercles/droites de $\mathcal{H}$. □

Bien sûr, si le centre de notre cercle appartient à $\mathbb{R}\cup\{\infty\}$, le centre du cercle/droite image par A aussi. Ainsi l'action de $\mathrm{SL}(2,\mathbb{R})$ préserve les cercles orthogonaux au bord de $\mathcal{H}$.

Contexte historique. Historiquement, la question de la cocircularité de 4 points complexes est considérée par l'astronome Claude Ptolémée, auteur de l'Almageste. Dans ce traité d'astronomie, il énonce la règle suivante: "Un quadrilatère admet un cercle circonscrit si et seulement si le produit des longueurs des diagonales est égal à la somme des produits des longueurs des côtés opposés." Un point de vue plus moderne sur cette question apporte la notion de birapport de 4 points complexes.

Définition 1.5 (Birapport)**.** Étant donné 4 points $a, b, c, d \in \mathbb{C}$ distincts, on définit le birapport de (a, b, c, d), noté $\zeta_{a,b,c,d}$:

$$\zeta_{a,b,c,d} = \frac{(a-b)(c-d)}{(a-d)(b-c)} \tag{1.4}$$

Fait 1.6. *4 points* a, b, c, d *sont cocirculaires ou alignés si et seulement si leur birapport est réel.*

Avec cet outil en main, on peut retrouver la règle de Ptolémée avec le calcul suivant: Soient $(a, b, c, d) \in \mathbb{C}$ 4 points distints. On a:

$$\begin{align}
|a-b||c-d| + |a-d||b-c| &= (|\zeta_{a,b,c,d}| + 1)|a-d||b-c| \tag{1.5}\\
&\geq |(\zeta+1)(a-d)(b-c)| \tag{1.6}\\
&= |a-c||b-d| \tag{1.7}
\end{align}$$

On a utilisé l'inégalité de Cauchy-Schwarz, et donc il y a égalité si et seulement si le birapport est réel positif, ce qui implique la cocircularité des 4 points. La condition sur le signe du birapport n'est là que parce que la désignation des diagonales implique un ordre (circulaire) sur les sommets du quadrilatère.

Classes de conjugaison dans $\mathrm{SL}(2,\mathbb{R})$**.** L'étude des sous-groupes monogènes de $\mathrm{SL}(2,\mathbb{R})$ se ramène à l'étude des classes de conjugaison de matrices de $\mathrm{SL}(2,\mathbb{R})$. Il y a alors une correspondance entre le polynôme caractéristique d'une matrice A et le nombre de points fixes de son action sur $\mathcal{H}$: en effet, le polynôme caractéristique de A est $X^2 - Tr(A)X + 1$ et les points fixes dans $\mathcal{H}$ sont les solutions dans $\mathcal{H}$ de l'équation $cz^2 + (d-a)z - b = 0$, avec la notation $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(1) Si $|\mathrm{Tr}(A)| < 2$, alors le polynôme caractéristique de A a discriminant négatif, et A à 2 valeurs propres complexes conjuguées de module 1. Dans ce cas, A a un unique point fixe $z \in \mathcal{H}$, et A est conjuguée à une matrice de rotation d'angle θ, donc l'action conjuguée par le difféomorphisme f est une rotation euclidienne d'angle θ. Selon la valeur de θ, le sous-groupe engendré par A est soit fini, soit dense dans $\mathrm{SO}(2)$. Un tel élément est dit elliptique.

(2) Si $\mathrm{Tr}(A) = 2$ et que A n'est pas l'identité, alors A est conjuguée dans $\mathrm{GL}(2,\mathbb{R})$ à la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Dans $\mathrm{SL}(2,\mathbb{R})$, elle est conjuguée soit à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ soit à $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. Alors l'action de A est conjuguée à une translation horizontale de $\mathcal{H}$, vers la droite ou vers la gauche. Le cas où $\mathrm{Tr}(A) = -2$ se traite de même, $-I_2$ étant dans le centre de $\mathrm{SL}(2,\mathbb{R})$. Dans tout les cas, A n' a pas de points fixes dans $\mathcal{H}$ mais en a un unique dans le bord $\mathbb{R} \cup \{\infty\}$. Le sous-groupe engendré est isomorphe à $\mathbb{Z}$. On appelle une telle matrice un élément parabolique.

(3) Finalement, si $|\mathrm{Tr}(A)| = 2$, alors A est diagonalisable et est conjuguée à une matrice de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. Au niveau des points fixes, A n'a pas de points fixes dans $\mathcal{H}$ mais en a exactement 2 dans le bord $\mathbb{R} \cup \{\infty\}$. A conjugaison près, l'action sur $\mathcal{H}$ correspond à une multiplication par λ^2. Le sous-groupe monogène est isomorphe à $\mathbb{Z}$. Un tel élément est dit loxodromique.

Groupe engendré par 2 matrices de $\mathrm{SL}(2,\mathbb{R})$. Étant donné 2 matrices $A, B \in \mathrm{SL}(2,\mathbb{R})$, on peut se demander quel est le groupe engendré par (A, B) ? C'est une question toujours ouverte en général, et la réponse varie largement selon A et B. Un cas particulier auquel on peut répondre est lorsque A et B commutent. Dans ce cas, A et B sont du même type, car ils ont le même nombre de points fixes dans $\mathcal{H}$ et dans son bord. Dans tous les cas, le groupe engendré est un sous-groupe de $\mathbb{Z}^2$, et l'étude d'un tel sous-groupe se ramène à l'étude des sous-groupes de $\mathbb{R}$ ou de $\mathbb{S}^1$ si les 2 matrices sont elliptiques et commutent.

2. Lemme du Ping-Pong et Théorème de Sanov–Brenner

Dans cette deuxième partie, nous présentons une preuve du théorème suivant:

Theorem 2.1 (Sanov, Brenner)**.** *Soient A, B deux matrices unipotentes de $\mathrm{SL}(2,\mathbb{R})$, conjuguées au couple suivant:*

$$(A, B) \sim \left(\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \right). \tag{2.1}$$

Alors si le produit $\alpha\beta$ est supérieur ou égal à 2, le groupe engendré par A, B est isomorphe à un groupe libre non-abélien engendré sur les 2 générateurs A et B. De plus, c'est un sous-groupe discret de $\mathrm{SL}(2,\mathbb{R})$.

Sanov énonce ce théorème pour $\alpha = \beta = 1$ en 1947 [San47], et Brenner [Bre55] généralise ce résultat sous cette forme en 1955.

Le groupe libre non-abélien.

Définition 2.2 (Groupe libre non-abélien)**.** Le groupe $\mathbf{F_n}$, dit groupe libre non-abélien à n-générateurs, est l'ensemble des mots en les $2n$ lettres $a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}$, muni de la loi de groupe suivante:

(1) La somme de deux mots ω, ω' est la concaténation $\omega\omega'$.
(2) Le neutre est le mot vide, $\emptyset$.
(3) L'inverse de a_i est a_i^{-1}.

C'est un groupe dénombrable, engendré par n éléments. En un certain sens, c'est le plus général possible, i.e. tout groupe G engendré par n éléments admet une surjection $\mathbf{F_n} \to \mathbf{G}$.

Le lemme du Ping-Pong. Le lemme du Ping-Pong est un outil essentiel de la preuve du théorème de Sanov–Brenner. Il permet, sous une condition combinatoire assez simple, de déduire que certaines transformations engendrent un groupe libre. Nous l'énonçons ici pour 2 générateurs, mais l'énoncé se déduit aisément pour un nombre arbitraire de générateurs.

Theorem 2.3 (Lemme du Ping-Pong)**.** *Soit X un ensemble, et A_1, A_2, B_1, B_2 4 sous-parties de X deux à deux disjointes. Supposons qu'il existe g_1, g_2 deux éléments de $\mathrm{Bij}(X)$ satisfaisant:*

$$X - B_1 \subset g_1(A_1),\ X - B_2 \subset g_2(A_2)\,. \tag{2.2}$$

Alors le groupe engendré par g_1, g_2 est isomorphe à un groupe libre abélien à 2 générateurs.

Un des premiers à utiliser le lemme du Ping-Pong fut Félix Klein, dans son études des sous-groupes discrets de $\mathrm{PSL}(2, \mathbb{C})$, en particulier des sous-groupes dits de Schottky.

Proof. Notons $\mathcal{M} = \{A_1, A_2, B_1, B_2\}$. Soit Γ le groupe engendré par g_1 et g_2. Nous avons toujours un morphisme sujectif $\Phi : \mathbf{F_2} \to \mathbf{\Gamma}$, défini par $\Phi(a_1) = g_1$ et $\Phi(a_2) = g_2$. Nous allons montrer que, sous les conditions de l'énoncé, ce morphisme est injectif, et donc un isomorphisme.

Soit donc $w \in \mathbf{F_2}$ un mot en a_1, a_2. Nous voulons montrer que $\Phi(w) \neq 1$. Pour cela, nous utilisons la forme dite librement réduite de w. Le mot w s'écrit de façon unique comme un produit $z_n^{\varepsilon_n} \dots z_2^{\varepsilon_2} z_1^{\varepsilon_1}$ avec les propriétés suivantes: $z_i \in \{a_1, a_2, a_1^{-1}, a_2^{-1}\}$, $\varepsilon_i \in \{-1, 1\}$, et si $z_i = z_{i+1}$ alors $\varepsilon_i = \varepsilon_{i+1}$. Pour montrer que $\Phi(w)$ n'est pas l'identité, nous allons trouver deux éléments R, S de $\mathcal{M}$ tel que $\Phi(w)(X - S) \subset R$. Comme $\mathcal{M}$ contient 4 éléments, $R \cup S$ n'est pas l'ensemble total X, et donc si $\Phi(w)(X - S) \subset R$, $\Phi(w)$ n'est pas l'identité.

Le choix de S se fait selon le tableau suivant:

$z_1^{\varepsilon_1} = a_1$	$S = A_1$
$z_1^{\varepsilon_1} = a_1^{-1}$	$S = B_1$
$z_1^{\varepsilon_1} = a_2$	$S = A_2$
$z_1^{\varepsilon_1} = a_2^{-1}$	$S = B_2$

Le choix de P est un peu plus délicat: Notons P_i la suite définie par récurrence comme ceci: $P_0 = X - S$, $P_1 = \Phi(z_1^{\varepsilon_1})(P_0)$, et ainsi de suite jusqu'à $P_n = \Phi(z_n^{\varepsilon_n})(P_{n-1}) = \Phi(w)(X - S)$. On montre alors l'alternative suivante, pour $l \in \{1, \dots, n\}$:

$z_l^{\varepsilon_l} = a_1$	$P_l \subset B_1$
$z_l^{\varepsilon_l} = a_1^{-1}$	$P_l \subset A_1$
$z_l^{\varepsilon_l} = a_2$	$P_l \subset B_2$
$z_l^{\varepsilon_l} = a_2^{-1}$	$P_l \subset A_2$

Cela se démontre par récurrence sur l. Pour $l = 1$, cela découle directement des hypothèses de l'énoncé. (Comme g_1 est bijective et que $g_1(X - A_1) \subset B_1$, il vient directement que $g_1^{-1}(X - B_1) \subset A_1$, et de même pour g_2). Supposons l'énoncé vrai pour $l - 1$, et montrons le pour l. Il y a 2 cas à considérer. Si $z_l \neq z_{l-1}$, alors si $z_{l-1} = a_i$ et $z_l = a_j$, par hypothèse $P_{l-1} \subset A_i \cup B_i \subset X - (A_j \cup B_j)$, et on vérifie que $P_l \subset \Phi(z_l^{\varepsilon_l})(S - (A_j \cup B_j))$ est incluse dans A_j ou B_j selon le signe de ε_l.

Si $z_l = z_{l-1}$, alors la notation utilisée pour le mot implique que $\varepsilon_l = \varepsilon_{l-1}$. Si $\varepsilon_l = 1$, et $z_l = a_i$, on a $P_{l-1} \subset B_i$ et donc $P_l = g_i(P_{l-1}) \subset g_i(X - A_i) \subset B_i$. Si $\varepsilon_l = -1$, $z_l = a_i$, on a $P_{l-1} \subset A_i$ et donc $P_l = g_i^{-1}(P_{l-1}) \subset g_i^{-1}(A_i) \subset g_i^{-1}(X - B_i) \subset A_i$, comme voulu. Cela termine cette récurrence. Lorsque $l = n$, on obtient bien un $P \in \mathcal{M}$ tel que $\Phi(w)(X-S) \subset P$, et donc $\Phi(w) \neq 1$. Comme Φ est injective et surjective, cela donne un isomorphisme entre $\mathbf{F_2}$ et Γ, démontrant le lemme du Ping-Pong. □

Théorème de Sanov–Brenner. Nous terminons par une application du lemme de Ping-Pong, permettant de démontrer le théorème de Sanov–Brenner énoncé plus haut. Soient donc A et B les matrices suivantes:

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

Ces 2 matrices agissent par homographies sur le demi-plan supérieur de la façon suivante:

$$\varphi_1(z) = z + \lambda \,\text{et}\, \varphi_2(z) = \frac{z}{z + \lambda} .$$

Nous allons construire 4 domaines disjoints de $\mathcal{H}$, notés A_1, A_2, B_1, B_2 satisfaisant les conditions du lemme de Ping-Pong pour démontrer que φ_1 et φ_2 engendrent bien un groupe libre non abélien à 2 générateurs.

Commençons par A_1 et B_1. Comme φ_1 est simplement une translation horizontale de longueur λ, nous posons les domaines suivants:

$$A_1 = \{z \in \mathcal{H}, \Re(z) < \frac{-\lambda}{2}\} ,\, B_1 = \{z \in \mathcal{H}, \Re(z) \geq \frac{\lambda}{2}\} .$$

Il est clair que A_1 et B_1 sont disjoints, et que $\varphi_1(\mathcal{H} - A_1) \subset B_1$.

Pour A_2 et B_2, nous utilisons la place qu'il nous reste dans $\mathcal{H}$ pour définir nos domaines. Posons ainsi:

$$A_2 = \{z \in \mathcal{H} : \frac{-\lambda}{2} \leq \Re(z) < 0\} ,\, B_2 = \{z \in \mathcal{H} : 0 \leq \Re(z) < \frac{\lambda}{2}\} .$$

En notant $z = x + iy$ avec $x, y \in \mathbb{R}$, on peut exprimer la partie réelle de $\varphi_2(z)$:

$$F(x, y) = \Re(\varphi_2(z)) = \frac{x + \lambda x^2 + \lambda y^2}{1 + \lambda^2 x^2 + 2\lambda x + \lambda^2 y^2} .$$

On cherche à montrer que $\varphi_2(\mathcal{H} - A_2) \subset B_2$, c'est à dire:

$$F\left(\mathbb{R} - \left[\frac{-\lambda}{2}, 0\right[\times \mathbb{R}_+^*\right) \subset \left[0, \frac{\lambda}{2}\right[.$$

Un calcul permet de montrer que $F(x, \cdot)$ est monotone sur $\mathbb{R}_+^*$, et donc de vérifier aisément que la condition énoncée est satisfaite dès que $\lambda^2 \geq 2$. Ce que l'on touche du doigt sans le dire, c'est que F, en temps que partie réelle d'une fonction holomorphe sur $\mathcal{H}$, est harmonique, et donc n'admet pas d'extréma locaux sur $\mathcal{H}$, ce qui permet de simplifier grandement l'étude de F.

Cela démontre donc que le lemme du Ping-Pong s'applique pour démontrer que le groupe engendré par φ_1 et φ_2 est un groupe libre non-abélien. En particulier, le groupe engendré par A et B est aussi un groupe libre non-abélien, ce qui est l'énoncé du théorème de Sanov–Brenner. Il n'est pas dur de se convaincre (grâce au lemme du Ping-Pong) que l'orbite d'un point de $\mathcal{H}$ n'admet pas de point d'accumulation dans $\mathcal{H}$, ce qui montre que le groupe engendré est un sous-groupe discret de $\mathrm{SL}(2, \mathbb{R})$.

Discussion plus globale. Une conséquence du résultat démontré est la suivante:

Corollaire 2.4. *Soient A, B deux matrices unipotentes de* $\mathrm{SL}(2, \mathbb{R})$*. Alors il y a l'alternative suivante:*

- *Soit A et B commutent, et le groupe engendré est un groupe abélien.*
- *Soit il existe $n > 0$ tel que A^n et B^n engendrent un groupe libre non-abélien à n générateurs.*

Ce corollaire est un cas particulier de la célèbre Alternative de Tits, qui énonce qu'un sous-groupe de $\mathrm{SL}(n, \mathbb{R})$ satisfait l'alternative suivante: soit il est virtuellement résoluble, soit il contient une copie du groupe libre non-abélien à 2 générateurs. Le lemme du Ping-Pong joue d'ailleurs un rôle essentiel dans la preuve de Tits en 1972 [Tit72].

Dans le cas où $\alpha\beta < 2$. Dans le cas où $\alpha\beta < 2$, la question reste largement ouverte en général. Lorsque $\alpha = \beta = 1$, le groupe engendré est le groupe des matrices de $\mathrm{SL}(2, \mathbb{R})$ à coefficients entiers. Lorsque λ est transcendant, on peut facilement démontrer que le morphisme Φ introduit est injectif (car un élément du noyau donne un polynôme à coefficients rationnels s'annulant en λ), et donc le groupe engendré est bien un groupe libre non-abélien à 2 générateurs, mais il n'est plus discret. On peut d'ailleurs vérifier que l'orbite d'un point est dense dans $\mathcal{H}$. Nous reférons à l'article de Chang–Jennings–Ree [CJR58] pour une discussion plus extensive du sujet.

References

[Ben97] Yves Benoist. Sous-groupes discrets des groupes de lie. *European Summer School in Group Theory*, pages 1–72, 1997.

[Bre55] Joël Lee Brenner. Quelques groupes libres de matrices. *CR Acad. Sci. Paris*, 241:1689, 1955.

[CJR58] Bomshik Chang, SA Jennings, and Rimhak Ree. On certain pairs of matrices which generate free groups. *Canadian Journal of Mathematics*, 10:279–284, 1958.

[San47] IN Sanov. A property of a representation of a free group. In *Doklady Akad. Nauk SSSR (NS)*, volume 57, page 16, 1947.

[Tit72] Jacques Tits. Free subgroups in linear groups. *Journal of algebra*, 20(2):250–270, 1972.