École Normale Supérieure, Année 2019-2020

1e année, Algèbre 1

TD n° 7 : Générateurs et relations pour $\mathrm{SL}_2(\mathbb{Z})$

Le but de cette note est de déterminer une présentation en termes de générateurs et relations du groupe $\mathrm{SL}_2(\mathbb{Z})$. La présentation est grandement inspiré du cours d'arithmétique de Serre. On montre le théorème suivant :

Théorème 1. *On a les isomorphismes suivants :*

$$\mathrm{SL}_2(\mathbb{Z}) \cong \langle x, y \mid x^2 = y^3, x^4 = 1\rangle,\ \mathrm{PSL}_2(\mathbb{Z}) \cong \langle x, y \mid x^2 = y^3 = 1\rangle$$

En particulier on se concentre sur le *groupe modulaire* $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\langle \pm \mathrm{Id}_2\rangle$, on verra que la présentation de $\mathrm{SL}_2(\mathbb{Z})$ s'en déduit immédiatement. En effet, on considère les matrices

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ U = ST = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

qui sont tels que $S^2 = -\mathrm{Id}_2$, $U^3 = -\mathrm{Id}_2$ et T est d'ordre infini. Ainsi dans $\mathrm{PSL}_2(\mathbb{Z})$, la classe de S et d'ordre 2, la classe de U est d'ordre 3 et celle de T est d'ordre infini. On montre d'abord que $\mathrm{PSL}_2(\mathbb{Z})$ est engendré par les classes de S et T, puis qu'il n'y a pas d'autres relations que celles décrites dans ce groupe en utilisant le *lemme du ping-pong*. Il est alors clair que les matrices S et T engendrent $\mathrm{SL}_2(\mathbb{Z})$. Alors S est d'ordre 4 et $S^2 = U^3$ ce qui fournit la présentation de $\mathrm{SL}_2(\mathbb{Z})$.

0.1 Action modulaire

L'idée, qu'on a déjà rencontré, est d'étudier le groupe modulaire au travers d'une action. Souvenez vous qu'on ne peut pas dire grand chose d'un groupe abstrait mais on peut dire beaucoup plus d'un groupe muni d'une action. Ici, on fait agir $\mathrm{PSL}_2(\mathbb{Z})$ sur le *demi-plan de Poincaré*, l'ensemble des nombres complexes de partie imaginaire strictement positive, $\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$. L'action est définit par homographie : pour $g \in \mathrm{SL}_2(\mathbb{Z})$ on définit

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ g \cdot z = \frac{az+b}{cz+d} \ \text{ pour tout } z \in \mathbb{H}.$$

Cette action de $\mathrm{SL}_2(\mathbb{Z})$ est bien définie, car $cz + d \neq 0$ pour $z \in \mathbb{H}$ et $c, d \in \mathbb{Z}$, et on vérifie par un calcul direct que c'est bien une action. De plus, $-\mathrm{Id}_2$ et Id_2 sont les seuls éléments qui agissent trivialement, donc l'action passe bien au quotient et on obtient une action fidèle de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathbb{H}$. On pose

$$D = \{z \in \mathbb{H} \mid |\Re(z)| \leqslant \frac{1}{2},\ \|z\| \geqslant 1\},$$

où $\Re(\cdot)$ est la partie réelle et $\|\cdot\|$ est le module complexe. On présente le lemme technique suivant :

Lemme 2. *Soit $z \in \mathbb{H}$, alors*

a) Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $z \in \mathbb{H}$ alors

$$\Im(g \cdot z) = \frac{\Im(z)}{\|cz+d\|^2}.$$

b) L'ensemble $\{\|cz+d\|^2 \mid (c,d) \in \mathbb{Z}^2 \backslash (0,0), \|cz+d\|^2 < 1\}$ est fini.

Démonstration. Le point *a)* est un calcul direct

$$\Im(g \cdot z) = \Im\left(\frac{az+b}{cz+d}\right) = \Im\left(\frac{(az+b)(\overline{cz+d})}{(cz+d)(\overline{cz+d})}\right) = \frac{1}{\|cz+d\|^2}\Im(acz\bar{z} + adz + bc\bar{z} + bd),$$

or $acz\bar{z}, bd \in \mathbb{R}$ et $\Im(adz + bc\bar{z}) = (ad - bc)\Im(z) = \Im(z)$ d'où le résultat.

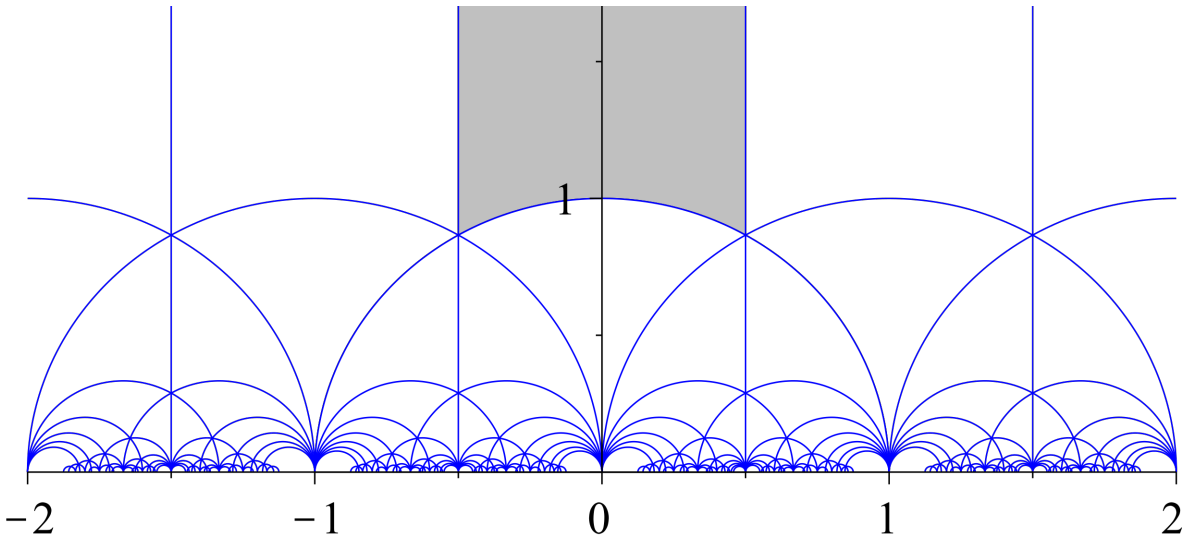

FIGURE 1 – Le demi-plan de Poincaré et ses régions sous l'action du groupe modulaire.

On montre le point b). On suppose que cet ensemble n'est pas vide. À $c \in \mathbb{Z}$ fixé, d doit être la partie entière de $-\Re(cz)$. Les conditions imposent que $c \neq 0$, on pose donc $z' = z + \frac{d}{c}$. Alors l'ensemble précédent est inclue dans

$$\{\|cz'\|^2 \mid c \in \mathbb{Z}, \|cz'\|^2 < 1\} \text{ qui est en bijection avec } \{c^2 \mid c \in \mathbb{Z},\ c^2 < \frac{1}{\|z'\|^2}\},$$

qui est fini comme intersection d'un compact avec un ensemble discret. □

L'ensemble D est la région grisée de la figure 1 ; on a en bleu les translatés sous $\mathrm{PSL}_2(\mathbb{Z})$ du bord de D. On note G' le sous-groupe de $\mathrm{PSL}_2(\mathbb{Z})$ engendré par les classes de S et T. On veut essentiellement montrer que D est un *domaine fondamental* pour l'action du groupe modulaire et l'action de G'. L'action de G' se résume essentiellement à l'action de S et T donnée pour tout $z \in \mathbb{H}$ par

$$T \cdot z = z + 1,\ S \cdot z = -\frac{1}{z}$$

On a le lemme suivant :

Proposition 3. *a) Soit $z \in \mathbb{H}$, alors il existe $g' \in G'$ tel que $g' \cdot z \in D$.*
b) Soit $z \in \mathring{D}$, l'intérieur de D, alors pour $g \in \mathrm{PSL}_2(\mathbb{Z})$, $g \cdot z \in D$ si et seulement si $g = \mathrm{Id}_2$.

Démonstration. On commence par montrer a). On cherche tout d'abord à trouver $g' \in G'$ tel que $\Im(g' \cdot z)$ soit maximal, i.e. de sorte à ce que $g' \cdot z$ soit "le plus haut possible" dans le demi-plan. Pour cela, il suffit de montrer que l'ensemble

$$\left\{\Im(g \cdot z) \mid g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G', \Im(g \cdot z) > \Im(z), \right\}$$

est fini. Or par le point a) du lemme précédent cet ensemble est en bijection avec l'ensemble

$$\{\|cz + d\|^2 \mid c, d \in \mathbb{Z}\backslash(0,0), \|cz + d\|^2 < 1\}.$$

Il existe donc $g' \in G'$ tel que $\Im(g' \cdot z)$ soit maximal. Comme $\Re((Tg') \cdot z) = \Re(g' \cdot z) + 1$ et $\Im((Tg') \cdot z) = \Im(g' \cdot z)$, quitte à multiplier g' par T, on peut supposer que $|\Re(g' \cdot z)| \leqslant \frac{1}{2}$. De plus $\|g' \cdot z\| \geqslant 1$, car en effet si on suppose que $\|g' \cdot z\| < 1$, on a par le point a) du lemme précédent

$$\Im((Sg') \cdot z) = \frac{\Im(g' \cdot z)}{\|z\|^2} > \Im(g' \cdot z),$$

d'où une contradiction avec la maximalité de $\Im(g' \cdot z)$. Ainsi on a montré que $g' \cdot z \in D$.

On montre le point b) : soit $z \in \mathring{D}$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ tels que $g \cdot z \in D$. On a deux cas

- Supposons que $c = 0$. Alors $1 = ad - cb = ad$ donc $g = T^b$ et ainsi $\Re(g \cdot z) = \Re(z) + b \in [-\frac{1}{2}, \frac{1}{2}]$. Or comme $\Re(z) \in]-\frac{1}{2}, \frac{1}{2}[$ on a $b = 0$ donc $g = \mathrm{Id}_2$.
- Supposons par l'absurde que $c \neq 0$, on peut alors supposer que $c > 0$ quitte à multiplier g par $-\mathrm{Id}_2$. Quitte à échanger $g \cdot z$ et $g^{-1} \cdot (g \cdot z)$ on peut supposer que $\Im(g \cdot z) \geqslant \Im(z)$ qui se réécrit par le point a) du lemme 2 en $\|cz+d\|^2 \leqslant 1$. Or dans ce cas $\Im(cz+d)^2 \leqslant 1$, c'est-à-dire que $c^2\Im(z)^2 \leqslant 1$. Donc $c = 1$ et on en déduit de la même façon que $d = 0$, comme $\Re(cz + d)^2 = \Re(z + d)^2 \leqslant 1$. Ainsi
$$g = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}),$$
donc $g \cdot z = a - \frac{1}{z}$. Mais comme $\left|\Re\left(\frac{1}{z}\right)\right| = \frac{1}{\|z\|^2} |\Re(z)| < \frac{1}{2}$ et $|\Re(g \cdot z)| \leqslant \frac{1}{2}$ on a $a = 0$. Ainsi $g = S$, mais c'est une contradiction car dans ce cas $g \cdot z \notin D$; en effet comme $\|z\| > 1$ on a $\|S \cdot z\| < 1$

□

Remarque 4. *On aurait pu être plus précis dans la proposition précédente et décrire ce qu'il se passe au bord. Par exemple, le second point de la proposition précédente nous dit que les stabilisateurs des éléments de $\mathring{D}$ sont triviaux. Les seuls points de D qui ont un stabilisateur sont i, ρ et $-\bar{\rho}$ les racines troisièmes de l'unité. Alors i a pour stabilisateur le groupe d'ordre 2 engendré par S. Remarquez que ρ et $-\bar{\rho}$ qui sont dans la même orbite ; leurs stabilisateurs sont les groupes d'ordre 3 engendrés par ST et TS respectivement.*

On est maintenant en mesure de conclure que $G' = \mathrm{PSL}_2(\mathbb{Z})$. Soit $z \in \mathring{D}$ quelconque. Soit $g \in \mathrm{PSL}_2(\mathbb{Z})$, alors $g \cdot z \in \mathbb{H}$ et donc par le premier point de la proposition précédente il existe $g' \in G'$ tel que $(g'g) \cdot z \in D$. Alors par le second point on a $g'g = \mathrm{Id}_2$ c'est-à-dire que $g \in G'$.

0.2 Lemme du ping-pong

On veut maintenant montrer qu'il n'y a pas de relation non triviale entre S et U, i.e. que le groupe modulaire est bien le groupe libre engendré par un élément d'ordre 3 et un élément d'ordre 2. En fait, $\mathrm{PSL}_2(\mathbb{Z})$ est même *virtuellement libre*, c'est-à-dire qu'il contient un sous-groupe libre sur 2 générateurs comme sous-groupe d'indice fini [1]. Pour montrer qu'il n'y a pas d'autres relations, on utilise une idée de la théorie géométrique des groupes qui est celle du *lemme du ping-pong*. On énonce le résultat général, ce qui nécessite une petite définition supplémentaire.

Définition 5. *Soit Γ_1, Γ_2 deux groupes définis par générateurs et relations de la forme*
$$\Gamma_1 = \langle x_1, \dots x_n \mid f_1 = \cdots = f_r = 1\rangle,\ \Gamma_2 = \langle y_1, \dots y_m \mid g_1 = \cdots = g_s = 1\rangle,$$
où les f_i sont des mots en les x_j et les g_i sont des mots en les y_j. Alors on définit le produit libre $\Gamma_1 \star \Gamma_2$ *de Γ_1 et Γ_2, en termes de générateurs et relations par*
$$\Gamma_1 \star \Gamma_2 = \langle x_1, \dots x_n, y_1, \dots y_m \mid f_1 = \cdots = f_r = g_1 = \cdots = g_s = 1\rangle.$$

C'est essentiellement la propriété de ne "pas avoir plus de relations" qui est formalisée. Ainsi, avec ces notations, on veut essentiellement montrer que $\mathrm{PSL}_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/3\mathbb{Z}$. Le lemme qui va suivre nous permet de savoir à partir d'un groupe muni d'une action sur un ensemble qui contient deux sous-groupes s'il contient le produit libre :

Lemme 6 (Lemme du ping-pong)**.** *Soit G un groupe agissant sur un ensemble X. Soit $\Gamma_1, \Gamma_2 \subset G$ deux sous-groupes contenant respectivement au moins 3 et 2 éléments. On suppose de plus qu'il existe $X_1, X_2 \subset X$ des sous-ensembles tels que X_2 n'est pas inclue dans X_1 et tels que*
$$\begin{cases} \gamma \cdot X_1 \subset X_2 & \text{pour } \gamma \in \Gamma_1,\ \gamma \neq e, \\ \gamma \cdot X_2 \subset X_1 & \text{pour } \gamma \in \Gamma_2,\ \gamma \neq e. \end{cases}$$
Alors le sous-groupe engendré par Γ_1 et Γ_2 est le sous-groupe $\Gamma = \langle \Gamma_1, \Gamma_2\rangle = \Gamma_1 \star \Gamma_2 \subset G$.

1. Le sous-groupe engendré par les matrices
$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$
est le groupe libre à deux générateurs, essentiellement par le lemme du ping-pong. Il n'est pas difficile de voir qu'il est d'indice fini.

Démonstration. Il suffit de montrer qu'un mot de Γ, le sous-groupe engendré par Γ_1 et Γ_2, contenant des éléments de $\Gamma_1\backslash\{e\}$ et $\Gamma_2\backslash\{e\}$ n'est pas le neutre. Soit w un tel mot et soit a_i une famille d'éléments de $\Gamma_1\backslash\{e\}$ et b_j une famille d'éléments de $\Gamma_2\backslash\{e\}$ intervenant dans l'écriture de w. On distingue 4 cas en fonction de si le mot w se termine ou commence par l'un des a_i ou l'un des b_j.

- Supposons que $w = a_1b_1\cdots b_{k-1}a_k$. Alors

$$w \cdot X_2 = (a_1b_1\cdots b_{k-1}a_k)\cdot X_2 \subset (a_1b_1\cdots b_{k-1})\cdot X_1 \subset \ldots a_1X_2 \subset X_1.$$

  Donc $w \cdot X_2 \subset X_1$ mais comme X_2 n'est pas inclue dans X_1 on en déduit que w n'agit pas trivialement et donc que ce n'est pas le neutre.
- Supposons que $w = b_1\cdots a_{k-1}b_k$. Alors soit $a \in \Gamma_1\backslash\{e\}$. Le point précédent montre que awa^{-1} n'est pas le neutre, donc w non plus car la conjugaison est un automorphisme.
- Supposons que $w = a_1b_1\cdots a_{k-1}b_k$. Alors, soit $a \in \Gamma_1\backslash\{e, a_1^{-1}\}$, ce qui est possible par hypothèse Γ_1 contient au moins 3 éléments. Alors par le premier point awa^{-1} n'est pas le neutre et donc w non plus comme au point précédent.
- Supposons que $w = b_1a_1\cdots a_k$. Alors, soit $a \in \Gamma_1\backslash\{e, a_k^{-1}\}$, ce qui est possible par hypothèse comme au point précédent. Alors, comme précédemment, awa^{-1} n'est pas le neutre donc w non plus, ce qui termine les 4 cas.

Ainsi on a montré que $w \neq e$, donc il n'y a, dans Γ, pas de relation non triviale entre les éléments de Γ_1 et ceux de Γ_2. □

On est maintenant en mesure de conclure que $\mathrm{PSL}_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \star \mathbb{Z}/3\mathbb{Z}$. En effet, on pose $\Gamma_1 = \langle U\rangle$, $\Gamma_2 = \langle S\rangle$, qui sont des groupes cycliques respectivement d'ordre 3 et 2, ce qui rentre dans les hyopthèses du lemme. On choisit maintenant $X = \mathbb{H}$ et

$$X_1 = \{z \in \mathbb{H} \mid \Re(z) \geqslant 0\},\ X_2 = \{z \in \mathbb{H} \mid \Re(z) \leqslant 0\}.$$

Alors il est clair que X_2 n'est pas inclue dans X_1. De plus, pour tout $z \in \mathbb{H}$, comme $U \cdot z = -\frac{1}{1+z}$ et $U^2 \cdot z = -1 - \frac{1}{z}$, on remarque que

$$\Re(U\cdot z) = -\frac{1+\Re(z)}{\|1+z\|^2},\ \Re(U^2\cdot z) = -(1+\frac{\Re(z)}{\|z\|^2}),\ \Re(S\cdot z) = -\frac{\Re(z)}{\|z\|^2}.$$

Alors $U \cdot X_1 \subset \{z \in \mathbb{H} \mid \Re(z) \leqslant 0\} = X_2$ et $U^2 \cdot X_1 \subset \{z \in \mathbb{H} \mid \Re(z) \leqslant 0\} = X_2$, ce qui donne la première condition. De même $S \cdot X_2 \subset \{z \in \mathbb{H} \mid \Re(z) \geqslant 0\} = X_1$, ce qui donne la deuxième condition. Ainsi le lemme nous donne $\langle \Gamma_1, \Gamma_2\rangle = \Gamma_1 \star \Gamma_2 \cong \mathbb{Z}/3\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z}$.

Or au paragraphe précédent on a montré que $\langle \Gamma_1, \Gamma_2\rangle = \mathrm{PSL}_2(\mathbb{Z})$ et donc on a bien

$$\mathrm{PSL}_2(\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \star \mathbb{Z}/2\mathbb{Z} \cong \langle x, y \mid x^2 = y^3 = 1\rangle.$$

Ce qui démontre finalement le théorème 1.