Générateurs de $\mathrm{SL}_2(\mathbb{Z})$

Leçons : 108 ; 182 ; 183

Références : FRANCINOU–GIANELLA–NICOLAS, *Oraux X-ENS Algèbre 1* (p.55)

Prérequis :

- Action de groupe
- Groupe engendré par des éléments
- Compréhension du repère complexe et des transformations comme la rotation et la translation

Notations :

- $\mathrm{SL}_2(\mathbb{Z})$ désigne l'ensemble des matrices 2×2 à coefficients entiers de déterminant égal à 1.
- $\Re(z)$ désigne la partie réelle de z où $z \in \mathbb{C}$.
- $\Im(z)$ désigne la partie imaginaire de z où $z \in \mathbb{C}$.

Introduction :

On va montrer que le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par seulement deux matrices. Ces deux matrices correspondent à des transformations du plan complexe quand on fait agir $\mathrm{SL}_2(\mathbb{Z})$ sur une partie du plan complexe.

Théorème 1. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Démonstration. On note $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ le demi plan de Poincaré.

On fait agir $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$.

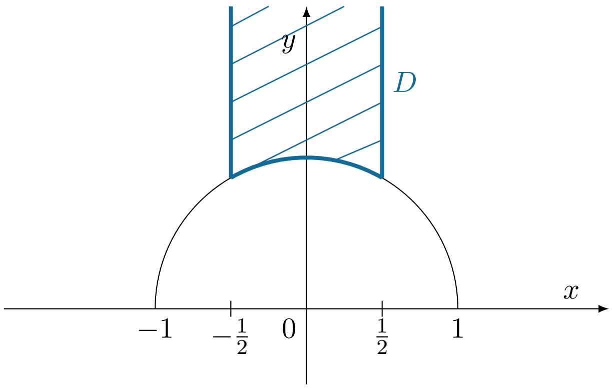
$$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \forall z \in \mathbb{H}, A \cdot z = \frac{az+b}{cz+d}$$

Il faut prouver que $\Im(A \cdot z) > 0$.

$$\begin{aligned}
\Im(A \cdot z) &= \Im\left(\frac{az+b}{cz+d}\right) \\
&= \Im\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) \\
&= \Im\left(\frac{acz\bar{z}+bd+bc\bar{z}+adz}{|cz+d|^2}\right) \\
&= \underbrace{(ad-bc)}_{=1^{1}} \frac{\Im(z)}{|cz+d|^2} > 0
\end{aligned}$$

On note $G = \langle S, T \rangle$ le sous groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par les matrices S et T et

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



On veut montrer que $\mathrm{SL}_2(\mathbb{Z}) = G$.

Lemme 1. Toute orbite de l'action restreinte à G rencontre l'ensemble D.

Démonstration. Autrement dit, on veut prouver que pour tout $z \in \mathbb{H}$, il existe une matrice $A \in G$ telle que $A \cdot z \in D$.

Soit $z \in \mathbb{H}$. On va montrer que le nombre de couple $(c, d) \in \mathbb{Z}^2$ tel que $|cz + d| \leqslant 1$ est fini.

$$|c|\Im(z) \leqslant |\Im(cz + d)| \leqslant |cz + d| \leqslant 1$$

Ainsi

$$|c| \leqslant \frac{1}{\Im(z)} \text{ et } |d| \leqslant 1 - |z||c|$$

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on a vu que $\Im(A \cdot z) = \dfrac{\Im(z)}{|cz + d|^2}$, il y a donc un nombre fini de couples (c, d) tels que

$$\Im(A \cdot z) \geqslant \Im(z)$$

II existe donc une matrice $A_1 \in G$ telle que $\Im(A_1 \cdot z)$ soit maximal.

On note $z_1 = A_1 \cdot z$.

Le but maintenant est de translater le point z_1 pour arriver dans la bande de l'ensemble D. On sait que

$$\forall u \in \mathbb{C}, \quad T \cdot u = u + 1$$

On pose $n = \lfloor \Re(z_1) + \frac{1}{2} \rfloor$ afin d'avoir

$$-\frac{1}{2} \leqslant \Re(z_1) - n = \Re(z_1 - n) = \Re(T^{-n} \cdot z_1) \leqslant \frac{1}{2}$$

et on a $\Im(T^{-n} \cdot z_1 = \Im(z_1)$.

On pose donc $z_2 = T^{-n} \cdot z_1$.

On veut montrer que $|z_2| \geqslant 1$. Supposons que l'on ait $|z_2| < 1$, on aurait alors

$$\begin{aligned} \Im(S \cdot z_2) &= \Im\left(-\frac{1}{z_2}\right) \\ &= \Im\left(-\frac{\bar{z}_2}{|z_2|^2}\right) \end{aligned}$$

1. car $A \in \mathrm{SL}_2(\mathbb{Z})$ donc $\det A = ad - bc = 1$

$$= \frac{\Im(z_2)}{|z_2|^2}$$
$$> \Im(z_2)$$

Ce qui est absurde par maximalité de $\Im(z_1) = \Im(z_2)$.

Ainsi $z_2 \in D$ et on a obtenu z_2 à partir de z qu'en faisant agir des matrices de G. Ce qui conclut la preuve du lemme. $\square$

Pour $z \in D$ fixé, on cherche à caractériser les matrices $A \in \mathrm{SL}_2(\mathbb{Z})$ telles que $A \cdot z \in D$.

Lemme 2. Soient $z \in D$ et $A \in \mathrm{SL}_2(\mathbb{Z})$ telle que $A \cdot z \in D$. Alors la matrice A est dans G.

Démonstration. On écrit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On peut se restreindre à $|cz + d| \leqslant 1$, autrement dit $\Im(A \cdot z) \geqslant \Im(z)$. En effet, supposons que $\Im(A \cdot z) < \Im(z) = \Im(A^{-1} \cdot (A \cdot z))$, on pourrait faire l'étude sur A^{-1}, et si A^{-1} est dans G alors A le sera aussi car G est un groupe.

Dans le lemme précédent, on a vu que si $|cz + d| \leqslant 1$, on avait alors

$$|c| \leqslant \frac{1}{\Im(z)} \leqslant \frac{2}{\sqrt{3}} < 2$$

car $z \in D$ donc sa partie imaginaire est supérieure à $\frac{\sqrt{3}}{2}$.

Comme $c \in \mathbb{Z}$, on peut faire une distinction de cas sur $c \in \{-1, 0, 1\}$.

☞ Si $\underline{c = 0}$, on a alors que $\det(A) = ad = 1$. Quitte à changer A en $-A$ (ce qui ne change pas la valeur de $A \cdot z$), on peut supposer $a = d = 1$. On a donc

$$A \cdot z = z + b$$

On sait que $z \in D$ et $A \cdot z \in D$, donc

— Si $\underline{|\Re(z)| < \frac{1}{2}}$, on a forcément $b = 0$. Donc $A = \pm I_2 \in G$.

— Si $\underline{\Re(z) = \frac{1}{2}}$, on a $b = 0$ ou $b = -1$. Donc $A = \pm I_2 \in G$ ou $A = \pm T^{-1} \in G$.

— Si $\underline{\Re(z) = -\frac{1}{2}}$, on a $b = 0$ ou $b = 1$. Donc $A = \pm I_2 \in G$ ou $A = \pm T \in G$.

☞ Si $\underline{c = 1}$, on a alors $|z + d| \leqslant 1$. Comme $z \in D$ et $A \cdot z \in D$, il n'y a que 3 choix possibles pour d.

(i) $d = 0$

(ii) $d = 1$ et $z = j$

(iii) $d = -1$ et $z = j + 1$

(i) Si $d = 0$, on a alors $\det(A) = -b = 1$ et $A \cdot z = a - \dfrac{1}{z}$. L'hypothèse $|cz + d| \leqslant 1$ se traduit par $|z| \leqslant 1$ et puisque $z \in D$, on a $|z| = z\bar{z} = 1$. On a donc

$$A \cdot z = a - \bar{z}$$

Comme il faut que $A \cdot z$ soit dans D et que $z \in D$, on a trois cas possibles pour a [2] :

— Si $a = 0$, on a $A = S \in G$.

— Si $a = 1$ (et $z = j$), on a $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = TS \in G$.

2. en effet, comme a est réel (même entier), on ne peut pas avoir $a > 1$

— Si $a = -1$ (et $z = 1 + j$), on a $A = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = (ST)^2 \in G$.

(ii) Si $d = 1$ et $z = j$, on a alors $\det(A) = a - b = 1$, d'où $b = a - 1$. Ainsi

$$A \cdot z = \frac{aj + a - 1}{j + 1} = a + j$$

qui n'appartient à D seulement si $a = 0$ ou $a = 1$ ce qui donne les matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = ST \in G \quad \text{ou} \quad A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = TST \in G$$

(iii) Si $d = -1$, même genre de considérations qui amènent à

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = (TS)^2 \in G \quad \text{ou} \quad A = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} = (TS)^2 S \in G$$

☞ Si $\underline{c = -1}$, on se ramène à $c = 1$ en changeant A en $-A$.

□

On sait déjà que

$$G \subset \mathrm{SL}_2(\mathbb{Z})$$

Réciproquement, prenons une matrice $A \in \mathrm{SL}_2(\mathbb{Z})$. Soit $z \in D$. On a alors $A \cdot z \in \mathbb{C}$. Par le lemme 1, on peut trouver $B \in G$ telle que $B \cdot (A \cdot z) \in D$.

Comme $z \in D$ et $BA \cdot z \in D$, par le lemme 2, on sait que $BA \in G$. En multipliant par $B^{-1} \in G$ à gauche, on trouve que la matrice A est dans G.

On peut donc conclure que

$$G = \mathrm{SL}_2(\mathbb{Z})$$

□

Astuces de l'agrégatif :

Pour le premier lemme finalement ce que l'on fait c'est que l'on remonte le point z avec des transformations dans G puis on translate ce point jusqu'à arriver dans D avec la matrice T qui translate de 1.

Peut-être qu'il peut être judicieux de mettre les produits matriciels des matrices S et T en annexe, et pendant le développement pour la distinction de cas, on dit « comme on le voit dans l'annexe, notre matrice appartient bien à G en tant que produit de S et T et de leur inverse ».

Je fais plein de dessins, notamment dans la disjonction de cas du lemme 2, pour montrer ce que fait l'action de A sur z dans chaque cas. Il peut être intéressant d'écrire la matrice A en faisant changer les coefficients au fur et à mesure de la disjonction de cas.

Questions possibles :

- Expliciter les cas non traités de la disjonction de cas.

Voir page suivant pour un schéma récapitulatif sur le lemme 2.

Schéma du lemme 2 : Dans ce schéma on représente les différents choix que l'on fait dans l'ordre c, d, a puis b.