Générateurs de $SL_2(\mathbb{Z})$ et $SL_2(\mathbb{Z}/n\mathbb{Z})$

Nico

Prérequis : Matrices à coefficiens entiers, algorithme d'Euclide
Notations :

1. N un entier plus grand que 2.
2. $SL_2(\mathbb{Z}) = \{M \in M_2(\mathbb{Z}) : \det M = 1\}$

Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors :

1. $SL_2(\mathbb{Z})$ est engendré par S et T.
2. Soit $\Gamma_N = \{M \in SL_2(\mathbb{Z}) : M \equiv I_2 \pmod N\}$, alors $SL_2(\mathbb{Z})/\Gamma_N \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$.

L'algorithme d'Euclide jouera un rôle clef dans la démonstration dans la preuve des générateurs de $SL_2(\mathbb{Z})$:

Démonstration. Soit $G =< S, T >$ le groupe engendré par S et T. On vérifie que $\det S = \det T = 1$, D'où $G \subseteq SL_2(\mathbb{Z})$. Il nous reste à montrer l'inclusion réciproque. On étudie dans un premier temps l'action naturelle de G sur $M_2(\mathbb{Z})$. Plus précisément, pour $n \in \mathbb{Z}$, on étudie comment agissent S et $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ sur $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$. On a que :

$$SM = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \text{ et } T^n M = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix} \tag{1}$$

Prenons une telle matrice M dans $SL_2(\mathbb{Z})$. Alors $1 = \det M = ad - bc$. Quitte à multiplier M par S, on peut supposer que $|a| \geq |c|$. En effet, Si $|a| < |c|$, alors la multiplication par S permute a et c à signe près.

1. Si $c = 0$, alors $ad = 1$, ce qui donne que $a = d = \pm 1$, et alors $M = \pm T^b$ ou $\pm T^{-b}$. Un tel élément est dans G car $S^2 = -I_2$, d'où $-I_2 \in G$.

2. Si $c \neq 0$, on effectue la division euclidienne de a et par c : $a = cq + r$, $q \in \mathbb{Z}$ et $|r| < |c|$. Par le calcul de $T^n M$ en (1), on a que :

$$T^{-q}M = \begin{pmatrix} a - qc & * \\ c & * \end{pmatrix} = \begin{pmatrix} r & * \\ c & * \end{pmatrix}$$

Il vient que le coefficient en $(1,1)$ est strictement inférieur à celui en $(2,1)$. En multipliant par S, On inverse la relation d'ordre. On met alors en place un algorithme :

1. On considère $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$
2. Si $|a| < |c|$, $M \leftarrow SM$
3. Si $c = 0$, retourner M.
4. Sinon, on effectue la division euclidienne de a par c : $a = cq + r$, puis $M \leftarrow T^{-q}M$.

L'algorithme prend fini car dès lors que $|a| \geq |c|$, on remplace a par un entier en valeur absolue strictement plus petit que $|c|$, puis on permute en valeur absolue a et c. Il se termine dès lors que $c = 0$, qui finit par être atteint.
Par l'étude du cas $c = 0$, la matrice retournée appartient à G. L'algorithme nous donne qu'il existe $g \in G$ tel que $gM = \pm T^m$ pour un certain $m \in \mathbb{Z}$. Donc $M = \pm g^{-1}T^m$, qui est un élément de G. □

Etablissons maintenant notre isomorphisme

Démonstration. On on applique la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ à $SL_2(\mathbb{Z})$:

$$\pi : \begin{cases} SL_2(\mathbb{Z}) & \longrightarrow & SL_2(\mathbb{Z}/N\mathbb{Z}) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \end{cases}$$

Montrons qu'une telle application est surjective. Soient $\overline{a}, \overline{b}, \overline{c}, \overline{d} \in \mathbb{Z}/N\mathbb{Z}$. On considère leurs représentants dans $\mathbb{Z}$: a, b, c, d. Par définition de $SL_2(\mathbb{Z}/N\mathbb{Z})$:

$$ad - bc \equiv 1 \pmod{N}$$

Autrement dit, par le théorème de Bézout, $\text{pgcd}(\overline{d}, \overline{c}) = \overline{1}$. Il existe alors $c', d' \in \mathbb{Z}$ tels que $|c|, |d| < N$, et modulo N :

$$c \equiv c',\ d \equiv d' \text{ et } \text{pgcd}(c', d') = 1.$$

Ainsi, quitte à renommer c en c', et d en d', on peut supposer que $\text{pgcd}\, c, d = 1$. Soit alors $k \in \mathbb{Z}$ tel que :

$$ad - bc = 1 + kN \tag{2}$$

Puisque $\text{pgcd}(c, d) = 1$, par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que :

$$ud - vc = -k \tag{3}$$

$(2) \leftarrow (2) + N(3)$ donne que :

$$d(a - Nu) - c(b - Nv) = 1$$

Notons alors $a_0 = a - Nu$ et $b_0 = c(b - Nv)$. Par construction, il vient que la matrice $M_0 = \begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, et $\pi(M_0) = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$. D'où l'application est surjective.

De plus, $\pi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv I_2 \pmod{N} \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_N$. D'où $\text{Ker}(\pi) = \Gamma_N$. Ainsi, par le premier théorème d'isomorphisme :

$$SL_2(\mathbb{Z})/\Gamma_N \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$$

□

Vu que le dév est un peu cours, je propose un bonus qui n'a pas de référence, mais qui se fait très bien. Il a le luxe de justifier la place de ce dév dans les leçons Z/nZ et Anneaux principaux.

$$[SL_2(\mathbb{Z}) : \Gamma(N)] = |SL_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

Démonstration. La stratégie est de faire appel au lemme chinois en faisant des calculs pour $N = p^\alpha$ d'une part.

1. Cas 1 : $N = p$ premier. Alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps. On sait que $|GL_2(\mathbb{F}_p)| = p(p^2 - 1)(p - 1)$. Et $\det : GL_2(\mathbb{F}_p) \to \mathbb{F}_p^*$ induit un isomorphisme de groupe $GL_2(\mathbb{F}_p)/SL_2(\mathbb{F}_p) \simeq \mathbb{F}_p^*$. D'où $|SL_2(\mathbb{F}_p)| = \dfrac{p(p^2 - 1)(p - 1)}{p - 1} = p(p^2 - 1) = p^3 - p$.
2. Cas 2 $N = p^\alpha$, $\alpha \geq 1$. On considère la surjection canonique :

$$\pi : SL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \to SL_2(\mathbb{Z}/p\mathbb{Z})$$

De noyau $\mathrm{Ker}(\pi) = \{\overline{A} \in SL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : \overline{A} \equiv \overline{I_2} \pmod p\} = \{\overline{A} = \overline{I_2} + \overline{p}B : B \in M_N(\mathbb{Z}/p^{\alpha-1}\mathbb{Z}),\ \det A \equiv 1 \pmod{p^\alpha}\}$.
D'une part, par un simple argument de comptage, $|M_2(\mathbb{Z}/p^{\alpha-1})| = p^{4(\alpha-1)}$.
D'autre part, pour tout $\overline{A} = \overline{I_2} + \overline{p}B$: [1]

$$\det \overline{A} = 1 + \overline{p}\,\mathrm{Tr}(B) + \overline{p}^2 \det B$$

D'où :

$$\det A \equiv 1 + p\,\mathrm{Tr}(B) \pmod{p^2}$$

Mais puisque $\det A \equiv 1 \pmod{p^\alpha}$, cette proposition est alors équivalente à :

$$\mathrm{Tr}(B) = 0 \text{ dans } \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$$

D'où si $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a = -d$. On a finalement que 3 coefficients à fixés : $|\mathrm{Ker}\,\pi| = p^{3(\alpha-1)}$. D'où :

$$|SL_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^{3(\alpha-1)}(p^3 - p)$$

3. Cas général : Soit $N = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Par le théorème des restes chinois, on un isomorphisme d'anneau :

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$$

D'où puisque l'application $M_n(A_1 \times A_2) \to M_n(A_1) \times M_n(A_2)$, $(a_{ij}, b_{ij})_{1\le i,j\le n} \mapsto ((a_{ij})_{1\le i,j\le n}, (b_{ij})_{1\le i,j\le n})$ est un isomorphisme, par récurrence, on obtient que :

$$M_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{i=1}^{r} M_2(\mathbb{Z}/p^{\alpha_i}\mathbb{Z})$$

Qui induit un isomorphisme de groupe sur $SL_2(\mathbb{Z}/N\mathbb{Z})$. D'où finalement :

$$|SL_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{i=1}^{r} p^{3(\alpha_i-1)}(p^3 - p) = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

□

[1]. Poser $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et calculer brutalement : $\det(I_2 + pB) = (1 + pa)(1 + pc) - p^2bd = 1 + p(a + c) + p^2(ad - bc)$.

Question 1. *Etudier :* det : $GL_2(\mathbb{Z}) \to \mathbb{Z}$. *Image ? Noyau ? Etablir un isomorphisme.*

Question 2. *Déterminer la complexité de l'algorithme permettant d'écrire un élément de $SL_2(\mathbb{Z})$ comme combinaison de S et T.*

Référence

Lesesvre, D. (2020). *131 Développements pour l'oral*. Dunod, p. 103.

Recasages

Leçon 108 : Exemples de parties génératrices d'un groupe. Applications.
Leçon 120 : Anneaux Z/nZ. Applications.
Leçon 122 : Anneaux principaux. Exemples et applications.
Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.