Générateurs de $\mathrm{SL}_2(\mathbb{Z})$ et relèvement d'une matrice de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

Notions utilisées : PGCD, division euclidienne

Motivations : Donner des générateurs de $\mathrm{SL}_2(\mathbb{Z})$ et décrire $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. $\mathrm{SL}_2(\mathbb{Z})$ apparaît par exemple dans l'étude des réseaux ou bien des homographies (c.f demi-plan de Poincarré).

Théorème 1. *1.* $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par les deux éléments* $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

2. $\forall n \in \mathbb{N}$, $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z})/\Gamma(n)$ *où* $\Gamma(n) := \{M \in \mathrm{SL}_2(\mathbb{Z}), M \equiv I_2[n]\}$

Avant tout, on remarque que les deux matrices S et T sont bien dans $\mathrm{SL}_2(\mathbb{Z})$

Etape 1 : calculs préliminaires de SM et T^nM pour $M \in \mathrm{SL}_2(\mathbb{Z})$ quelconque.

Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $n \in \mathbb{Z}$, on a

$$SM = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

$$\text{et } T^nM = \begin{pmatrix} a+cn & b+dn \\ c & d \end{pmatrix}$$

Etape 2 : Par divisions euclidiennes successives, trouver une matrice de $N \in \langle S, T\rangle$ et un entier k telle que $NM = \pm T^k$.

Tout d'abord, si $c = 0$ on montre que $M = T^b \in \langle S, T\rangle$ (c.f cas "$r = 0$" plus bas). Dans le cas général, on peut supposer $|a| \geq |c|$ quitte à multiplier à gauche par S. On effectue alors la division euclidienne de a par c ; on obtient $a = cq + r$ avec $r = 0$ ou $|r| < |c|$. On remarque par ailleurs que $T^{-q}M = \begin{pmatrix} a-cq & (\star) \\ c & (\star) \end{pmatrix} = \begin{pmatrix} r & (\star) \\ c & (\star) \end{pmatrix}$ et donc que

$$ST^{-q}M = \begin{pmatrix} -c & (\star) \\ r & (\star) \end{pmatrix}.$$

Si r est nul, on a $ST^{-q}M$ de la forme $\begin{pmatrix} -c & \beta \\ r & \alpha \end{pmatrix}$. Cette matrice étant dans $\mathrm{SL}_2(\mathbb{Z})$, l'équation du déterminant montre que $\alpha = -c \in \{\pm 1\}$. On a alors $ST^{-q}M = \pm T^\beta$. En remarquant que $S^2 = -I_2 \in \langle S, T\rangle$, on en conclut que $NM \in \langle S, T\rangle$ avec $N = ST^{-q}M$. Sinon, on répète le processus de division euclidienne, qui fournit un 0 en place $(2, 1)$ au bout d'un nombre fini d'étapes. Dans tous les cas, on

obtient une matrice $N \in \langle S, T\rangle$ telle que $NM \in \langle S, T\rangle$. Par inversibilité de N dans le groupe $\langle S, T\rangle$ on en déduit que $M \in \langle S, T\rangle$. Ceci conclut le premier point (double inclusion).

Etape 3 : description de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Pour le second point, on s'attache tout d'abord à montrer la surjectivité de l'application $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Pour cela, considérons une matrice $A = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

- **Si** $ad - bc = 1$ dans $\mathbb{Z}$ alors $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ vérifie $\varphi(M) = A$ et $M \in \mathrm{SL}_2(\mathbb{Z})$.
- **Si** $ad - bc = 1 + kn$ avec $\neq 0$: on a alors $ad - bc - kn = 1$ donc, d'après le théorème de Bézout, $pgcd(c, d, n) = 1$. Quitte à réduire modulo n, on peut supposer que c et d sont premiers entre eux. En effet, la réduction de $ad - bc - kn = 1$ modulo n donne $pgcd(c, d) \equiv 1[n]$ (théorème de Bézout). Notons $\alpha := pgcd(c, d)$ et c', d' des entiers tels que $c = \alpha c'$ et $d = \alpha d'$. D'une part, on a $c' \equiv c[n]$ et $d' \equiv d[n]$ car $\alpha \equiv 1[n]$. D'autre part, $pgcd(c', d') = 1$ dans $\mathbb{Z}$ par maximalité de α en tant que diviseur de c et d.

  Ainsi, quitte à changer c en c', d en d' on peut supposer c et d premiers entre eux. Alors d'après le théorème de Bézout, il existe u, v tels que $cu - dv = 1$. On a alors $\begin{cases} cukn - dvkn & = kn \\ ad - bc & = 1 + kn \end{cases}$ d'où, en posant $a' = a - vkn$, $b' = b + ukn$ et $M := \begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ vérifie $\varphi(M) = A$ et $det(M) = ad - bc - dvkn + cukn = 1 + kn - kn = 1$, d'où $M \in \mathrm{SL}_2(\mathbb{Z})$.

On a donc bien φ surjective. De plus, on vérifie que $Ker(\varphi) = \{(m_{i,j})_{1 \leq i,j \leq 2} \in \mathrm{SL}_2(\mathbb{Z}), m_{i,i} = 1\} = \Gamma(n)$. Ainsi, par théorème d'isomorphisme, il vient

$$\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z})/\Gamma(n)$$