Génération du groupe $\mathrm{SL}(2,\mathbb{Z})$

On note $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe de $\mathrm{GL}(2)\mathbb{R}$ constitué des matrices carrées d'ordre 2 à coefficients entiers relatifs de déterminant 1 :

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M}_2(\mathbb{Z}),\ ad - bc = 1 \right\}$$

On note[a] S et T les matrices :

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Montrer que S et T engendrent $\mathrm{SL}(2,\mathbb{Z})$.

[a] On peut aussi prendre $S' = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, en notant que $S' = -TS = TS^3$.

Commençons par remarquer que

$$S^2 = -\mathrm{I}_2 \quad \text{et} \quad (\forall n \in \mathbb{Z})\ T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

et que si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M}_2(\mathbb{Z})$, alors

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

Soit alors $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M}_2(\mathbb{Z})$.
Si $c = 0$, alors comme $M \in \mathfrak{M}_2(\mathbb{Z})$, $ad = 1$, ce qui ne laisse que deux possibilités :

$$M = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = T^m, \text{ d'ou } T^{-m} M = \mathrm{I}_2$$

ou

$$M = \begin{pmatrix} -1 & m \\ 0 & -1 \end{pmatrix} = -T^{-m}, \text{ d'ou } S^2 T^m M = \mathrm{I}_2$$

Supposons maintenant $c \neq 0$. Si $|a| \geqslant |c|$, écrivons $a = cq + r$, avec $0 \leqslant r \leqslant |c|$, la division euclidienne de a par c. La matrice $M' = T^{-q} M$ a alors un coefficient supérieur gauche $a - qc$ strictement inférieur en valeur absolue à son coefficient inférieur gauche c.
La multiplication à gauche par S échange ces deux coefficients (en changeant l'un des deux signes), de sorte que $M'' = SM' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ vérifie : $|c'| < |c|$ et $a' \neq 0$.

Répétant alors ce procédé, on aboutit nécessairement à une matrice $M^* = \begin{pmatrix} a^* & b^* \\ 0 & d^* \end{pmatrix}$ dont le coefficient inférieur gauche est nul (la suite de ces coefficients ne peut être une suite d'entiers *naturels* strictement décroissante), et on sait comment l'écrire comme produit de S et T. $\square$

Voici un exemple détaillant l'algorithme de la preuve : prenons $M = \begin{pmatrix} 19 & 8 \\ 7 & 3 \end{pmatrix}$.

- On a $19 = 2 \times 7 + 5$, donc $T^{-2}M = \begin{pmatrix} 5 & 2 \\ 7 & 3 \end{pmatrix}$, et $ST^{-2}M = \begin{pmatrix} -7 & -3 \\ 5 & 2 \end{pmatrix}$.
- $-7 = -2 \times 5 + 3$, donc $T^2ST^{-2}M = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$, et $ST^2ST^{-2}M = \begin{pmatrix} -5 & -2 \\ 3 & 1 \end{pmatrix}$.
- $-5 = -2 \times 3 + 1$, donc $T^2ST^2ST^{-2}M = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$, et[1] $ST^2ST^2ST^{-2}M = \begin{pmatrix} -3 & -1 \\ 1 & 0 \end{pmatrix}$.
- $-3 = -3 \times 1 + 0$, donc $T^3ST^2ST^2ST^{-2}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = S$.

On a alors :

$$M = T^2S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}T^3$$

et comme $S^{-1} = -S = S^2$,

$$M = -T^2ST^{-2}ST^{-2}ST^3 = S^2T^2ST^{-2}ST^{-2}ST^3$$

Référence : $\mathrm{SL}(2,\mathbb{Z})$, Keith Conrad,
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/SL(2,Z).pdf.

[1] À ce stade, on pourrait noter que $S\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}S = \begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix} = -T^{-3} = S^2T^{-3}$.