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

Aurélien Guerder

2023-2024

Source : LESESVRE, MONTAGNON, LE BARBENCHON, PIERRON, 131 développements pour l'oral

Théorème 1. *$SL_2(\mathbb{Z}) =< S, T >$ où $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

Démonstration. On fait agir $< S, T >= G$ sur $SL_2(\mathbb{Z})$ par multiplication à gauche.
Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, SM = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$ et $T^n M = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$

Soit $M \in SL_2(\mathbb{Z})$. Notons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On va procéder de manière algorithmique pour montrer que M est dans l'orbite d'un élément de G.
Quitte à multiplier par S, on peut supposer que $|a| \geq |c|$.
Tant que le coefficient en bas à gauche est non nul, on procède comme suit :
Si $c \neq 0$, soit $a = pc + r$ la division euclidienne de a par c. Alors $T^{-q} M = \begin{pmatrix} a-qc & * \\ c & * \end{pmatrix} = \begin{pmatrix} r & * \\ c & * \end{pmatrix}$
Maintenant on multiplie par S pour avoir une matrice de la forme $\begin{pmatrix} -c & * \\ r & * \end{pmatrix}$ et on est de nouveau dans le cas précédent.

Ce processus s'arrête au bout d'un moment car la suite des valeurs absolues des coefficients en bas à gauche est une suite d'entiers naturels strictement décroissante. Au bout d'un moment il vaut donc 0. On a alors une matrice de la forme $\begin{pmatrix} \epsilon & m \\ 0 & \epsilon \end{pmatrix}$ où $\epsilon = 1$ ou -1 et $m \in \mathbb{Z}$. Si $\epsilon = 1$, cette matrice vaut T^m, sinon elle vaut $-T^{-m} = S^2 T^{-m}$. Dans tous les cas, elle est bien dans G. Ainsi, $M \in G$ et finalement, $G = SL_2(\mathbb{Z})$. □

Théorème 2. *Soit $n \geq 2$. Notons $\Gamma(n) = \{M \in SL_2(\mathbb{Z}) | M \equiv I_2 \mathrm{mod} n\}$. Alors $SL_2(\mathbb{Z})/\Gamma(n) \simeq SL_2(\mathbb{Z}/n\mathbb{Z})$.*

Remarque : dans la source, cette preuve n'est pas complète : voilà une réponse possible.

Démonstration. Posons le morphisme de groupes $\begin{array}{ccccc} \phi & : & SL_2(\mathbb{Z}) & \to & SL_2(\mathbb{Z}/n\mathbb{Z}) \\ & & M & \mapsto & \overline{M} \end{array}$.
Montrons qu'il est surjectif.

Soit $M = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in SL_2(\mathbb{Z}/n\mathbb{Z})$.
On a $ad - bc = 1 \mathrm{mod} n$ donc pgcd(c, d, n)=1.
On peut en fait choisir c et d premiers entre eux : trouvons k tel que $c \wedge (d + kn) = 1$.
Si p premier divise c, on veut que p ne divise pas $d + kn$.
• Si p ne divise pas n, on peut prendre $d + kn \equiv 1 \mathrm{mod} p$ en prenant $\overline{k} = (\overline{1} - \overline{d})\overline{n}^{-1}$ modulo p.

• Si p divise n, on a $d + kn \equiv d \not\equiv 0 \mathrm{mod} p$ car p divise c et $c \wedge d = 1$. N'importe quel choix fonctionne, par exemple $k \equiv 0 \mathrm{mod} p$.
Ce choix de k est possible par le théorème des restes chinois.

Supposons à présent c et d premiers entre eux. Soit $k \in \mathbb{Z}$ tel que $ad - bc = 1 + kn$.
Comme $c \wedge d = 1$, il existe u et v entiers tels que $ud - vc = -k$.
Posons $a_0 = a + un$ et $b_0 = b + vn$ et $M_0 = \begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix}$.
On a $\det(M_0) = a_0 d - b_0 c = ad - bc + und - vnc = 1$. D'où $M = \overline{M_0}$ avec $M_0 \in SL_2(\mathbb{Z})$.
ϕ est un morphisme surjectif de noyau $\Gamma(n)$, d'où le théorème grâce au théorème d'isomorphisme. □