Générateurs de $GL_n(\mathbb{Z})$

(rédigé par Émilie Tezenas)

Leçons : 108 ; 142

Références : COGNET, *Algèbre Linéaire*

Introduction :

Le but de ce développement est d'obtenir un système de générateurs du groupe $\mathrm{GL}_n(\mathbb{Z})$, en le faisant agir sur $\mathbb{Z}^n$. On commence par exhiber une famille de représentants de l'action, avant de s'attaquer à la génération du groupe.

On considère l'action naturelle de $\mathrm{GL}_n(\mathbb{Z})$ sur $\mathbb{Z}^n$:

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Z}) \times \mathbb{Z}^n & \longrightarrow & \mathbb{Z}^n \\ (P, X) & \longmapsto & P.X \end{array}$$

On note pour $X \in \mathbb{Z}^n$, et $a \in \mathbb{Z}$,

— ω_X l'orbite de X sous l'action de $\mathrm{GL}_n(\mathbb{Z})$,

— ρ_X le pgcd des coordonnées de X,

— C_a la colonne $\begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ de $\mathbb{Z}^n$.

Introduisons également les matrices suivantes :

— $T_n(i, j, \varepsilon)$: matrice de transvection avec $\varepsilon = \pm 1$.

— $D_n(i)$: matrice de dilatation, avec un -1 à la $\mathrm{i}^{\text{ème}}$ ligne.

— $P_n(\tau)$: la matrice de permutation associée à τ, avec $\tau \in \mathfrak{S}_n$.

On note alors G_n le groupe engendré par toutes ces matrices. G_n est en particulier inclus dans $\mathrm{GL}_n(\mathbb{Z})$, car les déterminants des générateurs valent ± 1.

Théorème 1. Pour tout $X \in \mathbb{Z}^n$, $\omega_X = \omega_{C_{\rho_X}}$. Autrement dit, l'orbite de X est confondue avec l'orbite de la colonne contenant le pgcd des coordonnées de X.

Démonstration. Soit $X \in \mathbb{Z}^n$. Les orbites sous une actions sont soit disjointes, soit égales. Il nous suffit donc de trouver un élément dans l'intersection

$$\omega_X \cap \omega_{C_{\rho_X}}$$

pour montrer que ces deux orbites sont égales.
Montrons que $C_{\rho_X} \in \omega_X \cap \omega_{C_{\rho_X}}$.

On va en fait montrer un Lemme plus fort, qui nous sera utile pour trouver ensuite un système de générateurs de $\mathrm{GL}_n(\mathbb{Z})$.

Lemme 1. Pour tout $X \in \mathbb{Z}^n$, il existe $P \in G_n$ tel que $P.X = C_{\rho_X}$

Une fois ce lemme démontré, il est immédiat que C_{ρ_X} se trouve dans l'orbite de X, et donc que les deux orbites sont confondues.

□

Démonstration du Lemme. L'idée est de réaliser des opérations qui ne changent pas le pgcd, en s'inspirant de l'algorithme d'Euclide additif.

On note, pour $X \in \mathbb{Z}^n$, $S_X = \sum_{i=1}^n |x_i|$. On raisonne par récurrence sur S_X.

Pour $k \in \mathbb{N}$, on note : $HR(\mathrm{k})$: "Si $S_X = k$, alors il existe $P \in G_n$ tel que $P.X = C_{\rho_X}$"

▷ $S_X = 0$: Alors $P = I_n$ convient.

▷ Soit $k \geq 1$. Supposons $HR(\mathrm{m})$ vérifiées pour $m < k$. Soit $X \in \mathbb{Z}^n$ tel que $S_X = k$.

- Si X a un seul coefficient non nul, disons à la ligne i, ce coefficient est égal au pgcd de X. Alors si $\tau = (1, i)$, $P_n(\tau).X = C_{\rho_X}$.
- Sinon, X a au moins deux éléments non nuls, aux lignes $i < j$. Quitte à permuter ces deux lignes au moyen d'une matrice de permutation, on peut supposer que $|x_i| > |x_j|$. Soit ε tel que $|x_i + \varepsilon x_j| = |x_i| - |x_j|$ (ε vaut -1 si les deux coefficients sont de même signe, 1 sinon).

  On note $\tilde{X} = T_n(i, j, \varepsilon).X$. Alors

  $$S_{\tilde{X}} = \sum_{k=1}^{n} |\tilde{x}_k| = \sum_{k \neq i} |x_k| + |x_i + \varepsilon x_j|$$

  Or, $|x_i + \varepsilon x_j| = |x_i| - |x_j| < |x_i|$. Donc $S_{\tilde{X}} < S_X$.

  On peut donc appliquer l'hypothèse de récurrence à $\tilde{X}$. De plus, $\rho_X = \rho_{\tilde{X}}$ car pour $a, b \in \mathbb{Z}$, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a, b - a)$.

  Finalement, il existe $\tilde{P} \in G_n$ tel que $\tilde{P}.\tilde{X} = C_{\rho_{\tilde{X}}} = C_{\rho_X}$. D'où

  $$\tilde{P}.T(i, j, \varepsilon).X = C_{\rho_X}$$

  .

□

Corollaire 1. L'ensemble $(C_a)_{a \in \mathbb{Z}}$ est une famille de représentants de l'action.

Démonstration. Le théorème précédent montre que pour tout $X \in \mathbb{Z}^n$, il existe $a \in \mathbb{Z}$ tel que $\omega_X = \omega_{C_a}$.

Il reste à montrer que si $a \neq b$, alors $\omega_{C_a} \cap \omega_{C_b} = \varnothing$.

Soit a et $b \in \mathbb{Z}$ tels que $\omega_{C_a} \cap \omega_{C_b} \neq \varnothing$. Alors il existe $P \in \mathrm{GL}_n(\mathbb{Z})$ tel que $P.C_a = C_b$.

$P \in \mathrm{GL}_n(\mathbb{Z})$ donc $\det(P) = \pm 1$. En particulier, en développant par rapport à la première colonne, la valeur du déterminant donne une relation de Bézout entre les coefficients de la première colonne de P - que l'on note maintenant P_1. Donc $\rho_{P_1} = 1$.

On a alors $C_b = a.P_1$ donc $b = \rho_{C_b} = a.\rho_{P_1} = a$. Donc si $a \neq b$, les orbites sont disjointes, et on a bien trouvé un système de représentants de l'action. □

Théorème 2. $\mathrm{GL}_n(\mathbb{Z}) = G_n$

Démonstration. On procède par récurrence sur n.

▷ $n = 1$: OK, $\mathrm{GL}_n(\mathbb{Z}) = \pm 1$

▷ Soit $n \geq 2$. Supposons que le théorème soit vrai en dimension $n - 1$.

Soit $P \in \mathrm{GL}_n(\mathbb{Z})$. Le pgcd des coefficients de la première colonne vaut 1 (vu dans la preuve du corollaire). Donc il existe $G \in G_n$ tel que $G.P_1 = C_1$ (P_1 désigne la première colonne de la matrice P). Autrement dit, il existe $G \in G_n$ tel que

$$G.P = \begin{pmatrix} 1 & \star \\ \vdots & \star \\ 0 & \end{pmatrix}$$

Au moyen d'une multiplication à droite par des matrices de transvection, dont on notera le produit $\tilde{T}$, on annule les coefficients de la première ligne pour se ramener à une matrice de la forme suivante :

$$G.P.\tilde{T} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \tilde{P} & \\ 0 & & & \end{pmatrix}$$

$\tilde{P}$ est une matrice de taille $n-1 \times n-1$, donc l'hypothèse de récurrence s'y applique : $\tilde{P} \in G_{n-1}$.

La matrice $\tilde{G} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & \tilde{P} & \\ 0 & & & \end{pmatrix}$ est donc dans G_n car les matrices de transpositions, permutations et dilatations en dimenson $n-1$ donnent des matrices de transposition, permutation et dilatation en dimension n lorsqu'on leur rajoute un point fixe.

On a donc $P = G^{-1}.\tilde{G}.\tilde{T}^{-1} \in G_n$, et le théorème est démontré.

$\square$