Sous-groupes de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Projet Mathématiques - Informatique

Kevin Garnier
Charly Martin Avila

Dirigé par Olivier Brunat

Année 2023

Matrices à coefficients entier et forme normale de Hermite

Proposition

Soient $A \in \mathscr{M}_{m,n}(\mathbb{Z})$ et $Q \in GL_n(\mathbb{Z})$, alors $\operatorname{Im} AQ = \operatorname{Im} A$

Definition

Soit $A \in \mathscr{M}_{m,n}(\mathbb{Z})$. Alors, il existe une unique matrice échelonnée réduite suivant les colonnes $H \in \mathscr{M}_{m,n}(\mathbb{Z})$ telle qu'il existe $Q \in GL_n(\mathbb{Z})$ avec $H = AQ$. La matrice H s'appelle la forme normale de Hermite de A.

Example

$$\begin{pmatrix} 2 & 1 \\ 4 & 10 \\ 5 & 13 \\ 13 & 12 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_1} \begin{pmatrix} 1 & 2 \\ 10 & 4 \\ 13 & 5 \\ 12 & 13 \end{pmatrix} \xrightarrow{C_2 \leftarrow C_2 - 2C_1} \begin{pmatrix} 1 & 0 \\ 10 & -16 \\ 13 & 3 \\ 12 & -14 \end{pmatrix} \xrightarrow{C_2 \leftarrow -C_2} \begin{pmatrix} 1 & 0 \\ 10 & 16 \\ 13 & -3 \\ 12 & 14 \end{pmatrix}$$

Génération des sous-groupes

Théorème

Les seules matrices dont les colonnes génèrent un sous-groupe de $\mathbb{Z}^2/p^m\mathbb{Z} \times p^m\mathbb{Z}$ sont les matrices de la forme $H = \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix}$ avec $a \leq m$, $b \leq m$ et $j < p^b$ ou $H = \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix}$ avec $a \leq m$, $b \leq m$, $k \leq m$ et $j < p^{b-k}$

Corollaire

Soit la suite $(A_k)_{0 \leq k \leq n}$ telle que $A_0 = \{ (a, b) \mid a + b \leq m \}$

$$A_k = \left\{ (a, b) \;\middle|\; \begin{array}{l} a \leq m, b \leq m \\ a + b = m + k \end{array} \right\}$$

Alors, l'ensemble des matrices du théorème, c'est-à-dire, les matrices dont les colonnes génèrent les sous-groupes de $\mathbb{Z}^2/p^m\mathbb{Z} \times p^m\mathbb{Z}$ est $M = \bigsqcup_{k=0}^{m} M_k$ où

$$M_k = \left\{ \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix} \;\middle|\; \begin{array}{l} (a, b) \in A_k \\ 0 \leq j < p^{b-k} \end{array} \right\}$$

Énumération des sous-groupes

Théorème

Soit

$$\psi : \mathbb{N}^2 \to \mathbb{N}$$

$$(p, n) \mapsto \sum_{i=0}^{n} (n-i)p^i + \sum_{i=0}^{n} \frac{1 - p^{n-i+1}}{1-p}$$

Alors, le nombre de sous groupe de $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ est $\psi(p, m)$

Proposition

Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec p_i des nombres premiers distincts

Le nombre total de sous-groupes de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est

$$\prod_{i=0}^{k} \psi(p_i, \alpha_i) = \prod_{i}^{k} \Big(\sum_{j=0}^{\alpha_i} (\alpha_i - j)p_i^j + \sum_{j=0}^{\alpha_i} \frac{1 - p_i^{\alpha_i - j + 1}}{1 - p_i} \Big)$$

Quelques résultats générés

n	0	1	2	3	4	5	6	7	8	9	10
$\lvert\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\rvert$	∞	1	5	6	15	8	30	10	37	23	40

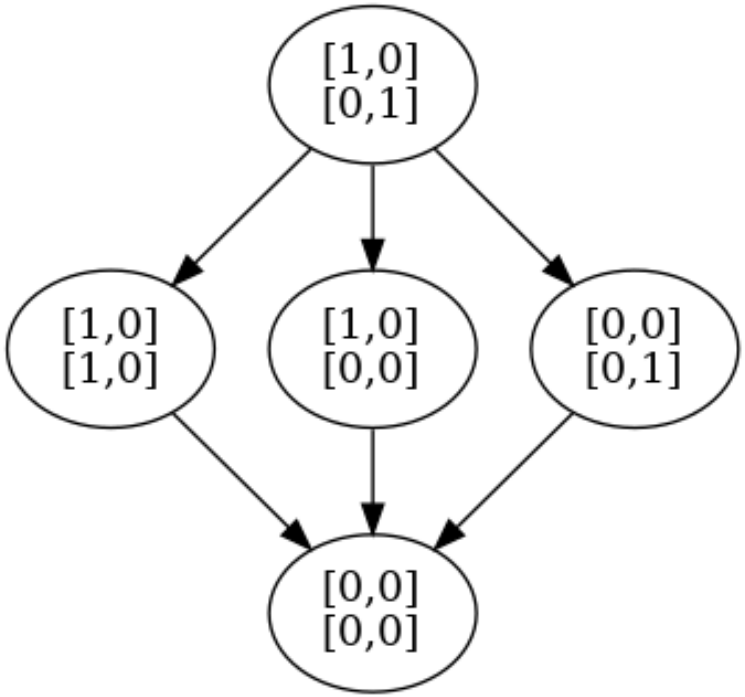

FIGURE – Treillis des sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec les formes normales de Hermite correspondantes