



UNIVERSITÉ PARIS CITÉ

PROJET MATHÉMATIQUES - INFORMATIQUE

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

*Kevin Garnier*

*Charly Martin Avila*

Dirigé par  
Olivier BRUNAT

L3 Mathématiques - Informatique  
Année 2023



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Quelques simplifications du problème</b>	<b>4</b>
2.1	Décomposition de $n$ en éléments irréductibles . . . . .	4
2.2	Simplification des sous-groupes . . . . .	5
<b>3</b>	<b>Matrices à coefficients entier et forme normales de Hermite</b>	<b>6</b>
3.1	Matrices à coefficients entier . . . . .	6
3.2	Formes normales de Hermite . . . . .	7
<b>4</b>	<b>Génération et énumération des sous-groupes</b>	<b>11</b>
4.1	Génération des sous-groupes . . . . .	11
4.2	Énumération des sous-groupes . . . . .	15
<b>5</b>	<b>Génération du treillis</b>	<b>18</b>
<b>6</b>	<b>Quelques résultats</b>	<b>19</b>
6.1	Pour $n = 2$ . . . . .	19
6.2	Pour $n = 4$ . . . . .	19
6.3	Pour $n = 20$ . . . . .	19
<b>7</b>	<b>Bibliographie</b>	<b>20</b>

# 1 Introduction

Il est très facile de décrire tous les sous-groupes d'un groupe cyclique d'ordre  $n$  : il y en a exactement un par diviseur positif de  $n$ . Pourtant, étonnamment, décrire tous les sous-groupes d'un groupe abélien est en général un problème difficile. Dans ce projet, nous nous proposons de considérer cette question pour le groupe  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  qui, de nos jours n'a pas l'air d'avoir été traitée.

D'un point de vue théorique, nous mettrons en avant la génération et la caractérisation des sous-groupes grâce aux vecteurs colonnes des matrices à coefficients entiers et en particulier aux formes normales de Hermite. Nous montrerons aussi une formule permettant de les compter.

D'un point de vue pratique, nous créerons un programme OCAML capable de générer les sous-groupes de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  ainsi que leur treillis à partir d'un entier donné en paramètres.

## 2 Quelques simplifications du problème

### 2.1 Décomposition de $n$ en éléments irréductibles

Nous pouvons tout d'abord simplifier le problème aux cas où  $n = p^m$  avec  $p$  un nombre premier et  $m \in \mathbb{N}$ . En effet la proposition suivante nous garantit que le résultat est isomorphe

**Proposition 1.** Soit  $n = \prod_i^k p_i^{\alpha_i}$ , avec  $p_i$  des nombres premiers, alors

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \simeq \prod_i^k (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2$$

*Démonstration.* Soit  $n = \prod_i^k p_i^{\alpha_i}$ . Par le théorème des restes chinois, nous avons

$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

En particulier,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \\ &\simeq (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2 \end{aligned}$$

■

En pratique, pour décomposer en entier en facteurs irréductibles, nous avons utilisé la procédure de  $\rho$ -POLLARD pour obtenir un diviseur de  $n$  :

```
1 fonction rho_pollard P n x y k i d
2   Si d <> 1:
3       Retourne d
4   Sinon:
5       x = P(x) mod n
6       d = pgcd(|y - x|, n)
7       Si i = k:
8           Alors, Retourne rho_pollard loop P n x x 2k (i + 1) d
9       Sinon Retourne rho_pollard P n x y k (i + 1) d
```

Puis nous répétons la procédure jusqu'à que les diviseurs soient premier.

En triant et en regroupant les nombres premier, nous obtenons donc les différents  $p_i^{\alpha_i}$ .

Dans notre implémentation,  $P(X) = X^2 - 1$  et  $n$  n'est pas premier.

## 2.2 Simplification des sous-groupes

**Proposition 2.**

$$\mathbb{Z}^2/n\mathbb{Z} \times n\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

*Démonstration.* Soit

$$\begin{aligned}\varphi : \mathbb{Z}^2 &\rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ (a, b) &\mapsto (\bar{a}, \bar{b})\end{aligned}$$

$\varphi$  est surjectif par définition de la classe d'équivalence de  $a$  et  $b$ . Montrons que  $\ker \varphi = n\mathbb{Z} \times n\mathbb{Z}$ .

$$\begin{aligned}(a, b) &\in \ker \varphi \\ \text{ssi } \varphi(a, b) &= (\bar{0}, \bar{0}) \\ \text{ssi } (\bar{a}, \bar{b}) &= (\bar{0}, \bar{0}) \\ \text{ssi } \bar{a} = \bar{0} \text{ et } \bar{b} &= \bar{0} \\ \text{ssi } a \in n\mathbb{Z} \text{ et } b &\in n\mathbb{Z} \\ \text{ssi } (a, b) &\in n\mathbb{Z} \times n\mathbb{Z}\end{aligned}$$

Ainsi par le premier théorème d'isomorphisme, nous avons

$$\mathbb{Z}^2/n\mathbb{Z} \times n\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

■

Ainsi le problème se résout à trouver les sous-groupes  $G$  de  $\mathbb{Z}^2$  tels que  $H = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$$\text{et } n\mathbb{Z} \times n\mathbb{Z} \subseteq G = \left\langle \begin{pmatrix} \bar{a} \\ \bar{b} \end{pmatrix}, \begin{pmatrix} \bar{c} \\ \bar{d} \end{pmatrix} \right\rangle$$

### 3 Matrices à coefficients entier et forme normales de Hermite

Nous avons vu dans la section précédente qu'il était possible de caractériser les sous-groupe de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$  par une matrice  $H = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ . Cependant, ces matrices ne sont pas uniques. C'est pourquoi, nous allons utiliser les formes normales d'Hermite. Énonçons d'abord une proposition sur les matrices à coefficients entier qui nous sera fort utile par la suite.

#### 3.1 Matrices à coefficients entier

**Proposition 3.** Soient  $A \in \mathcal{M}_{m,n}(\mathbb{Z})$  et  $Q \in GL_n(\mathbb{Z})$ , alors

$$\text{Im } AQ = \text{Im } A$$

*Démonstration.* Soit  $y \in \text{Im } AQ$ , il existe  $x \in \mathbb{Z}^n$  tel que  $y = AQx$ . Or,

$$\begin{aligned} y &= AQx \\ \implies y &= A(Qx) \\ \implies y &\in \text{Im } A \end{aligned}$$

Donc,  $\text{Im } AQ \subseteq \text{Im } A$ . Soit  $y \in \text{Im } A$ . Il existe  $x \in \mathbb{Z}^n$  tel que  $y = Ax$ . Cherchons  $z \in \mathbb{Z}^n$  tel que  $y = Ax = AQz$

$$\begin{aligned} Ax &= AQz \\ \implies A(x) &= A(Qz) \\ \implies x &= Qz \\ \implies Q^{-1}x &= z \text{ (car } Q \in GL_n(\mathbb{Z})) \end{aligned}$$

Donc, il existe bien un  $z \in \mathbb{Z}^n$  tel que  $AQz = y$ . Donc,  $y \in \text{Im } AQ$ .  
D'où  $\text{Im } AQ = \text{Im } A$

■

## 3.2 Formes normales de Hermite

Nous allons désormais énoncer la définition de la forme normale de Hermite.

**Définition 4.** Soit  $A \in \mathcal{M}_{m,n}(\mathbb{Z})$ . Alors, il existe une unique matrice échelonnée réduite suivant les colonnes  $H \in \mathcal{M}_{m,n}(\mathbb{Z})$  telle qu'il existe  $Q \in GL_n(\mathbb{Z})$  avec  $H = AQ$ . La matrice  $H$  s'appelle la forme normale de Hermite de  $A$ .

*Démonstration.* Nous admettons l'unicité.

L'algorithme suivant nous montre son existence.

```
1 Fonction hermite_aux(A, i) :
2   Pour chaque j allant de i à m :
3     Si i = j :
4       Si  $a_{ij} < 0$  : réaliser l'opération  $C_j \leftarrow -C_j$ 
5     Sinon :
6       Si  $a_{ij} < 0$  : réaliser l'opération  $C_j \leftarrow -C_j$ 
7        $k, r = \text{div\_euclide}(a_{ij}, a_{ii})$ 
8       réaliser l'opération  $C_j \leftarrow C_j - kC_i$ 
9   Si  $\forall i < j \leq m, a_{ij} = 0$  :
10    Réduire à gauche du pivot
11    Retourner A
12   Sinon
13      $d_k = \min(\{a_{ij} \mid i \leq j \leq n, a_{ij} \neq 0\})$ 
14     Permuter  $C_k$  avec  $C_i$ 
15     hermite_aux(A, i)
16
17 Fonction hermite(A) :
18   Pour chaque i allant de 1 à n :
19      $d_k = \min(\{a_{ij} \mid i \leq j \leq n, a_{ij} \neq 0\})$ 
20     Si  $d = \text{None}$  :
21       Continuer boucle
22     Sinon :
23       Permuter  $C_k$  avec  $C_i$ 
24        $A = \text{hermite\_aux}(A, i)$ 
25   vérifier signe des pivots de A
26   Retourner A
```



Montrons la terminaison de l'algorithme.

La fonction `hermite_aux` se repose sur l'algorithme d'Euclide.

En effet, pour tout  $i < j < m$ , nous réalisons la division euclidienne de  $a_{ij}$  par  $a_{ii}$ .

Si à la fin de la boucle il existe  $j$  tel que  $a_{ij} < a_{ii}$ , alors nous recommençons en permutant  $C_j$  et  $C_i$  et  $a_{ij}$  devient notre nouveau pivot.

Ainsi, par la correction de l'algorithme d'Euclide, il existe un rang  $N$  où tous les  $a_{ij}$  avec  $j > i$  sont tous nuls. Ainsi la fonction `hermite_aux` se termine. La fonction `hermite` étant seulement une boucle, elle se termine également. Donc, l'algorithme se termine bien.

Montrons la correction de l'algorithme.

La fonction `hermite_aux` se repose sur l'algorithme d'Euclide en utilisant des opérations élémentaires sur les matrices. Par la correction de l'algorithme d'Euclide, nous pouvons en déduire que pour tout  $j > i$ ,  $a_{ij} = 0$ .

De plus, avant de retourner, nous réalisons la division euclidienne des  $a_{ij}$  par  $a_{ii}$  avec  $0 < j < i$ .

Donc, les  $a_{ij}$  sont les restes des divisions euclidiennes et sont donc réduit au maximum. Nous réalisons ces opération sur toutes les lignes sans jamais revenir sur les lignes précédentes. Enfin, nous vérifions le signe de pivot et nous changeons la colonne de signe si nécessaire.

Ainsi la matrice obtenue est bien échelonnée réduite, il s'agit donc d'une forme normale de Hermite, ce qui prouve donc son existence. ■

### Exemple 5.

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

**Remarque 6.** Il existe des algorithmes beaucoup plus efficace pour calculer la forme normale de Hermite comme l'algorithme de de Domich & Ai (1989) qui réalise les calculs modulo le déterminant de  $A$  ou l'algorithme de Micciancio-Warinski. Cependant, ces algorithmes étant plus ou moins compliqué, le choix ici a été de faire nous-mêmes un algorithme à partir de la méthode naïve employée lors du calcul de la forme normale de Hermite à la main.

**Définition 7.** Soient  $A \in \mathcal{M}_{m,n}$ ,  $B \in \mathcal{M}_{m,p}$  deux formes normales de Hermite

$A \sim B$  ssi les colonnes non nulles de  $A$  sont les mêmes que les colonnes non nulles de  $B$ .

Nous allons énoncer quelques résultats utiles des formes normales de Hermite. Tout d'abord, la proposition suivante nous permet de nous restreindre à certaines matrices sous une forme particulière dont les colonnes génèrent un sous groupe de  $\mathbb{Z}^2$

**Proposition 8.** Soit  $A \in \mathcal{M}_{m,n}(\mathbb{Z})$  et soit  $H$  sa forme normale d'Hermite. Alors,

$$\text{Im } A = \text{Im } H$$

*Démonstration.* C'est une application de la proposition 3 avec  $H = AQ$  avec  $Q \in GL_n(\mathbb{Z})$  ■

Ainsi les colonnes de la forme normale de Hermite  $H$  d'une matrice  $A$  génèrent le même sous-groupe que les colonnes de  $A$ .

Nous n'avons donc plus qu'à trouver des matrices de la forme  $H = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$  telle que

$$n\mathbb{Z} \times n\mathbb{Z} \subseteq \left\langle \begin{pmatrix} \bar{a} \\ b \end{pmatrix}, \begin{pmatrix} 0 \\ \bar{c} \end{pmatrix} \right\rangle$$

**Proposition 9.** Soient  $A, B \in \mathcal{M}_{m,n}(\mathbb{Z})$ .

Soit  $H_A$  (resp.  $H_B$ ) la forme normale de Hermite de  $A$  (resp.  $B$ ). Alors,

$$H_A = H_B \Leftrightarrow \text{Im } A = \text{Im } B$$

*Démonstration.* Supposons que  $H_A = H_B$ . Par la proposition 8, nous avons

$$\text{Im } A = \text{Im } H_A = \text{Im } H_B = \text{Im } B$$

Réciproquement, supposons que  $\text{Im } A = \text{Im } B$ . Par la proposition 8, nous avons

$$\text{Im } A = \text{Im } H_A = \text{Im } H_B = \text{Im } B$$

Donc, les vecteurs colonnes de  $H_A$  qui génèrent  $\text{Im } H_A$  sont les mêmes que ceux de  $H_B$  qui génèrent  $\text{Im } H_B$ , d'où  $H_A = H_B$  ■

Cette proposition nous affirme donc qu'en traitant seulement les formes normales de Hermite, nous pourrions générer tous les sous-groupes de  $\mathbb{Z}^2$

La proposition suivante, va nous être utile pour trouver la bonne forme des matrices de Hermite ainsi que la génération du treillis.

**Proposition 10.** Soient  $A, B \in \mathcal{M}_{m,n}$  deux formes normales de Hermite et soit  $G$  (resp.  $H$ ) le groupe engendré par les colonnes de  $A$  (resp.  $B$ ). Alors,

$$G \cup H = G \Leftrightarrow \text{hermite}(A|B) \sim A$$

où  $\text{hermite}(A|B)$  est la forme normale de hermite de la matrice augmentée  $(A|B)$ .

*Démonstration.* Supposons que  $G \cup H = G$ . Alors,  $H \subseteq G$ . Donc

$$\forall x \in H, \exists y \in G, \exists \lambda \in \mathbb{Z}, x = \lambda y$$

En particulier la base de  $H$  est une combinaison linéaire de la base de  $G$ . D'où

$$\text{hermite}(A|B) = (A|0) \sim A$$

Réciproquement, soit  $\text{hermite}(A|B) \sim A$ . Alors, par définition de la relation d'équivalence,  $\text{hermite}(A|B) = (A|0)$ . Ainsi les colonnes de  $B$  sont des combinaisons linéaires des colonnes de  $A$ ,

c'est-à-dire la base de  $H$  est une combinaison linéaire de la base de  $G$ .

$$\text{D'où } H \subseteq G \text{ et } G \cup H = G$$

■

Nous avons désormais tous les outils à notre disposition pour démontrer la forme voulue des matrices ainsi que la formule permettant de compter le nombre de sous-groupe de  $\mathbb{Z}^2/n\mathbb{Z} \times n\mathbb{Z}$

## 4 Génération et énumération des sous-groupes

Nous allons voir dans cette section la forme des matrices dont les vecteurs colonnes génèrent les sous-groupes de  $\mathbb{Z}^2/n\mathbb{Z} \times n\mathbb{Z}$ , la formule permettant de les compter ainsi que quelques propositions sur leurs caractéristiques. Nous avons montré dans la section 2.1 que nous pouvons nous restreindre aux cas où  $n = p^m$  avec  $p$  un nombre premier et  $m \in \mathbb{N}$ .

Ainsi dans cette section, nous supposons que  $n = p^m$ .

### 4.1 Génération des sous-groupes

Commençons tout d'abord par montrer la forme des matrices dont les vecteurs colonnes génèrent les sous-groupes de  $\mathbb{Z}^2/p^m\mathbb{Z} \times p^m\mathbb{Z}$ . Dans la section 2.2, nous avons montré que les sous-groupes de  $\mathbb{Z}^2$  recherché sont les sous groupes  $G$  tels que  $p^m\mathbb{Z} \times p^m\mathbb{Z} \subseteq G$ , c'est-à-dire

$$G \cup p^m\mathbb{Z} \times p^m\mathbb{Z} = G$$

Par la proposition 10, cela revient à trouver les matrices  $H = \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix}$  telles que

$$(H|Mat(p^m\mathbb{Z} \times p^m\mathbb{Z})) = \begin{pmatrix} \alpha & 0 & p^m & 0 \\ \beta & \gamma & 0 & p^m \end{pmatrix} \sim \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix} = H$$

**Théorème 11.** *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*

$$H = \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix} \text{ avec } a \leq m, b \leq m \text{ et } j < p^b$$

ou

$$H = \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix} \text{ avec } a \leq m, b \leq m, k \leq m \text{ et } j < p^{b-k}$$

*Démonstration.* Montrons tout d'abord que ces matrices sont les seules qui génèrent les sous-groupe de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ .

Supposons qu'il existe  $H, H'$  deux formes normales de Hermite qui génèrent  $G$  un sous-groupe de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ . Alors, nous avons  $\text{Im } H = \text{Im } H'$  et par la proposition 9,  $H = H'$ .

Nous pouvons donc créer une classe d'équivalence pour la relation  $\sim$  où la forme normale de hermite est la représentante de ces classes.

Montrons désormais l'existence de telles matrices.

Soit  $H = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$  Nous cherchons à réaliser des opérations élémentaires telles que

$$A = \begin{pmatrix} \alpha & 0 & p^m & 0 \\ \beta & \gamma & 0 & p^m \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha & 0 & 0 & 0 \\ \beta & \gamma & 0 & 0 \end{pmatrix}$$

Annuler  $a_{13} = a_{24} = p^m$  nécessite les conditions suivante sur  $\alpha$  et  $\beta$  :

$$\begin{cases} \alpha = p^a \text{ avec } a \leq m \\ \gamma = p^b \text{ avec } a \leq m \end{cases}$$

Nous pouvons donc réaliser les opérations  $C_3 \leftarrow C_3 - p^{m-a}C_1$  et  $C_4 \leftarrow C_4 - p^{m-b}C_2$ . Ceci nous donne donc :

$$\begin{pmatrix} \alpha & 0 & p^m & 0 \\ \beta & \gamma & 0 & p^m \end{pmatrix} \xrightarrow[C_4 \leftarrow C_4 - p^{m-b}C_2]{C_3 \leftarrow C_3 - p^{m-a}C_1} \begin{pmatrix} \alpha & 0 & 0 & 0 \\ \beta & \gamma & -p^{m-a}\beta & 0 \end{pmatrix}$$

Nous cherchons désormais  $\beta$  tel que  $p^b \mid \beta p^{m-a}$ .

Tout d'abord, par la définition de la forme normale de Hermite,  $\beta < p^b$ .

Nous pouvons isoler deux cas en fonction de  $a$  et  $b$  :

- Si  $a + b \leq m$ , alors  $b \leq m - a$  et  $p^b \mid p^{m-a}$  et donc  $p^b \mid \beta p^{m-a}$ .
- Sinon  $m \leq a + b \leq 2m \implies 0 \leq a + b - m \leq n$ .  
 Nous posons  $k = a + b - m$  et nous avons donc  $0 \leq k \leq m$ .  
 Nous posons  $\beta = ip^k$  avec  $0 \leq i < p^{b-k}$ . Nous avons bien  $\forall i, \beta = ip^k < p^b$ .  
 De plus,  $p^b \mid ip^k p^{m-a}$  car  $p^b \mid p^k p^{m-a}$  car  $b = k + m - a$

Ainsi, dans les deux cas, nous pouvons annuler  $a_{23}$  et nous obtenons bien la matrice

suivante en faisant l'opérations élémentaire.  $\begin{pmatrix} \alpha & 0 & 0 & 0 \\ \beta & \gamma & 0 & 0 \end{pmatrix}$ .

Dans le premier cas, nous obtenons en posant  $j = \beta < p^b$

$$\begin{pmatrix} p^a & 0 & 0 & 0 \\ j & p^b & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix}$$

Dans le deuxième cas, nous obtenons en posant  $j = i < p^{b-k}$

$$\begin{pmatrix} p^a & 0 & 0 & 0 \\ jp^k & p^b & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} p^a & 0 \\ jp^k & p^b \end{pmatrix}$$

Ce qui démontre bien l'existence de ces matrices.

■

**Corollaire 12.** Soit la suite  $(A_k)_{0 \leq k \leq n}$  telle que

$$A_0 = \{ (a, b) \mid a + b \leq m \}$$

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

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

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

**Proposition 13.** Soit  $\pi : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2/n\mathbb{Z} \times n\mathbb{Z}$  et soit  $H \in \mathcal{M}_2$  une matrice de Hermite de la forme  $H = \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix}$ .

$$H \in M \Leftrightarrow \text{Im}(H)/p^m\mathbb{Z} \times p^m\mathbb{Z} = \pi(\text{Im } H) = \left\langle \pi \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \pi \begin{pmatrix} 0 \\ \gamma \end{pmatrix} \right\rangle$$

*Démonstration.* (admise?)

■

**Exemple 14** (Cas pour  $n = 2$ ). Nous avons  $n = 2 = 2^1$  donc  $m = 1$ .  
Calculons les matrices appartenant à

$$M_0 = \left\{ \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix} \middle| \begin{array}{l} (a, b) \in A_0 \\ 0 \leq j < p^b \end{array} \right\}$$

Nous avons  $A_0 = \{ (a, b) \mid a + b \leq 1 \} = \{ (0, 0), (0, 1), (1, 0) \}$ . Ainsi

$$M_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Calculons les matrices appartenant à

$$M_1 = \left\{ \begin{pmatrix} 2^a & 0 \\ 2j & 2^b \end{pmatrix} \middle| \begin{array}{l} (a, b) \in A_1 \\ 0 \leq j < 2^{b-1} \end{array} \right\}$$

Nous avons

$$A_1 = \left\{ (a, b) \middle| \begin{array}{l} a \leq 1, b \leq 1 \\ a + b = 2 \end{array} \right\} = \{ (1, 1) \}$$

Ainsi

$$M_0 = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\}$$

Par la proposition 13, nous pouvons réaliser la correspondances entre les matrices obtenues et les sous-groupes de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ . Nous avons donc

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\longrightarrow (Z/2\mathbb{Z})^2 \\ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} &\longrightarrow \langle \bar{1}, \bar{0} \rangle \\ \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} &\longrightarrow \langle \bar{1}, \bar{1} \rangle \\ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} &\longrightarrow \langle \bar{0}, \bar{1} \rangle \\ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} &\longrightarrow \langle \bar{0}, \bar{0} \rangle \end{aligned}$$

**Proposition 15.** soit  $H = \begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix}$  une forme normale d'Hermite. Alors

$$|Z^2 / \text{Im } H| = \det(H) = \alpha\beta$$

*Démonstration.* (admise ?) ■

**Remarque 16.** En particulier, si  $H \in M$ ,  $\text{ord}(\pi(H)) = p^{a+B}$

## 4.2 Énumération des sous-groupes

Grâce aux résultats démontrés dans la section précédente, nous pouvons donc énumérer les sous-groupes de  $\mathbb{Z}/p^m\mathbb{Z}$ . Cela nous donne le théorème suivant :

**Théorème 17.** Soit

$$\begin{aligned} \psi : \mathbb{N}^2 &\rightarrow \mathbb{N} \\ (p, n) &\mapsto \sum_{i=0}^n (n-i)p^i + \sum_{i=0}^n \frac{1-p^{n-i+1}}{1-p} \end{aligned}$$

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

*Démonstration.* Par le corollaire 12, nous savons que  $M = \bigsqcup_{k=0}^m M_k$  est l'ensemble des matrices dont les colonnes engendrent les sous-groupes de  $\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}$ . Ainsi,

$$|M| = |\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z}|$$

De plus,

$$|M| = \left| \sum_{k=0}^m M_k \right| = \sum_{k=0}^m |M_k|$$

Calculons donc le cardinal de  $M_0$  dans un premier temps, puis nous calculerons le cardinal de  $M_k$  pour  $1 < k < m$ .

Nous avons

$$M_0 = \left\{ \begin{pmatrix} p^a & 0 \\ j & p^b \end{pmatrix} \mid \begin{array}{l} (a, b) \in A_0 \\ 0 \leq j < p^b \end{array} \right\} \text{ avec } A_0 = \{ (a, b) \mid a + b \leq m \}$$

Or, pour chaque couple  $(a, b) \in A_0$ , nous avons  $p^b$  matrices différentes. De plus,  $a \leq m - b$ .



Donc, en remplaçant  $b$  par  $i$ , nous obtenons

$$|M_0| = \sum_{i=0}^m (m-i)p^i$$

Calculons maintenant le cardinal des  $M_k$ . Nous avons

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

Tout d'abord, pour tout couple  $(a, b) \in A_k$ , il y a  $p^{b-k}$  matrices différentes.

De plus, pour tout  $(a, b) \in A_k$ , nous avons  $a + b = m + k \implies b = m - a + k$ . De cela, nous en déduisons

$$\begin{aligned} 0 &\leq m - a + k \leq m \\ \implies 0 &\leq m - a \leq m - k, \text{ car } 0 \leq a \leq m \end{aligned}$$

D'où posant  $j = m - a$ , nous avons

$$\begin{aligned} |M_k| &= \sum_j^{m-k} p^{b-k} \\ &= \sum_j^{m-k} p^{m-a+k-k} \\ &= \sum_j^{m-k} p^j \\ &= \frac{1 - p^{m-k+1}}{1 - p} \end{aligned}$$

Ainsi, en remplaçant  $k$  par  $i$ , nous en déduisons le cardinal de  $M$  :

$$\begin{aligned} |M \setminus M_0| &= \sum_{i=1}^m |M_i| \\ &= \sum_{i=0}^m \frac{1 - p^{m-i+1}}{1 - p} \end{aligned}$$

D'où

$$|M| = \sum_{i=0}^n (m-i)p^i + \sum_{i=0}^m \frac{1 - p^{m-i+1}}{1 - p}$$

Enfin, il ne nous reste plus qu'à poser

$$\begin{aligned}\psi : \mathbb{N}^2 &\rightarrow \mathbb{N} \\ (p, n) &\mapsto \sum_{i=0}^n (n-i)p^i + \sum_{i=0}^n \frac{1-p^{n-i+1}}{1-p}\end{aligned}$$

■

**Proposition 18.** Soit  $n = \prod_{i=0}^k p_i^{\alpha_i}$ .

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

$$\prod_{i=0}^k \psi(p_i, \alpha_i) = \prod_i \left( \sum_{l=0}^{\alpha_i} (\alpha_i - l)p_i^l + \sum_{l=0}^{\alpha_i} \frac{1-p_i^{\alpha_i-l+1}}{1-p_i} \right)$$

*Démonstration.* Nous avons montré dans la section 2.1 que

$$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \simeq \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2$$

Par le théorème précédent,  $|(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2| = \psi(p_i, \alpha_i)$ .

Ainsi,

$$\begin{aligned}|\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| &= \left| \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2 \right| \\ &= \prod_i |(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^2| \\ &= \prod_i \psi(p_i, \alpha_i) \\ &= \prod_i \left( \sum_{l=0}^{\alpha_i} (\alpha_i - l)p_i^l + \sum_{l=0}^{\alpha_i} \frac{1-p_i^{\alpha_i-l+1}}{1-p_i} \right)\end{aligned}$$

■

## 5 Génération du treillis

## 6 Quelques résultats

6.1 Pour  $n = 2$

6.2 Pour  $n = 4$

6.3 Pour  $n = 20$

## 7 Bibliographie

- [1] COSTE Michel, *Algèbre linéaire sur les entiers*, Mars 2018
- [2] **TODO livre algo**
- [3] PERNET Clément, *Calcul de formes normales matricielles : de l'algorithmique à la mise en pratique*, Séminaire SIESTE, ENS-Lyon, 12 février 2013
- [4] BERTHURRY Grégory, *Algèbre le grand combat : Cours et exercices*, 2<sup>e</sup> édition. Paris : Calvage & Mounet, 2020. 1215 p. (Mathématiques en devenir)