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

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 se proposons de considérer cette question pour le groupe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

D'un point de vue théorique, nous mettrons en avant la générations et la caractérisations de sous-groupes grâce aux vecteurs colonne des matrices à coefficients entier 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 garantie 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, on a

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

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 ρ-Pollard pour obtenir un diviseur de n :

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

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

φ est surjective 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, on a

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

∎

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

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 propriété les matrices à coefficients entier qui nous sera forte utile par la suite.

3.1 Matrices à coefficients entier

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

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

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

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

Donc $\operatorname{Im} AQ \subseteq \operatorname{Im} A$.

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

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

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

■

3.2 Formes normales de Hermite

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

Définition 4. *Soit $A \in \mathscr{M}_{m,n}(\mathbb{Z})$. 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.*

Démonstration. Nous supposerons l'unicité admise, l'algorithme suivant nous montre son existence.

```
Fonction hermite_aux(A, i):
    Pour chaque j allant de i à m :
        Si i = j :
            Si a_ij < 0 : réaliser l'opération C_j ← -C_j
        Sinon :
            Si a_ij < 0 : réaliser l'opération C_j ← -C_j
            k,r = div_euclide(a_ij, a_ii)
            réaliser l'opération C_j ← C_j - kC_i
    Si ∀i < j <= m, a_ij = 0 :
        Réduire à gauche du pivot
        Retourner A
    Sinon
    d_k = min({ a_ij | i <= j <= na_ij ≠ 0 })
    Permuter C_k avec C_i
    hermite_aux(A, i)

Fonction hermite(A) :
    Pour chaque i allant de A à n :
        d_k = min({ a_ij | i <= j <= na_ij ≠ 0 })
        Si d = None :
            Continuer boucle
        Sinon :
            Permuter C_k avec C_i
            A = hermite_aux(A, i)
    vérifier signe des pivots de A
    Retourner A
```

Montrons la terminaison de l'algorithme. La fonction hermite_aux se repose sur l'algorithme d'euclide. En effet, pour tout $i < j < m$, on réalise 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 on recommence 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, on réalise 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.
On réalise ces opération sur toutes les lignes sans jamais revenir sur les lignes précédentes. Enfin, on vérifie le signe de pivot et on change 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-Warinshi. Cependant ces algorithmes étant plus ou moins compliqué, le choix ici a été de faire nous même un algorithme à partir de la méthode naïve employée lors du calcul de la forme normale de Hermite à la main.

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

Proposition 7. *Soit $A \in \mathscr{M}_{m,n}(\mathbb{Z})$ et soit H sa forme normale d'Hermite. Alors,*

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

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

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

4 Génération et énumération des sous-groupes

4.1 Génération des sous-groupes

4.2 Énumération des sous-groupes

5 Génération du treillis

6 Quelques résultats

6.1 Pour n = 2

6.2 Pour n = 4

6.3 Pour n = 20

7 Références

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. BERHURY Grégory, *Algèbre le grand combat : Cours et exercices*, 2^{e} édition.
   Paris : Calvage & Mounet, 2020. 1215 p. (Mathématiques en devenir)