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

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

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 $H = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$. Cependant, ces matrices ne sont pas uniques. C'est pourquoi, nous allons utiliser les formes normales d'Hermite. Énonçons d'abord quelques propriété sur les matrices à coefficients entier.

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,

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

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 $y = Ax = AQz$

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

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 quelques propriétés utiles sur les formes normales 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.*

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

```
Fonction hermite A:
    Pour chaque i <= n :
```

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