



## Rapport de stage

### Réduction de réseaux - adaptations d'idées provenant du cas polynomiale au cas entier.

*HAI001I : Stage académique*

**Lucas Noirot**

(lucas.noirot@etu.umontpellier.fr)

**Encadrant : Romain Lebreton**

(romain.lebreton@lirmm.fr)

**Date : 17 février - 26 juin 2025**

# Table des matières

<b>Notations</b>	<b>2</b>
<b>Guide de Lecture</b>	<b>3</b>
<b>1 Réseaux euclidiens et polynomiaux</b>	<b>6</b>
1.1 Généralités sur les réseaux . . . . .	6
1.1.1 Définitions et exemples . . . . .	6
1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens . . .	6
1.2 Réduction de réseaux euclidiens et polynomiaux . . . . .	7
1.2.1 Réduction de réseaux euclidiens . . . . .	7
1.2.2 Réduction de réseaux polynomiaux . . . . .	7
<b>2 Adaptation de la réduction de réseaux polynomiaux au cas entier</b>	<b>8</b>
<b>3 Réseaux définis par relations plutôt que par générateurs</b>	<b>9</b>
<b>A Rappels d'algèbre : Groupes, Anneaux et Modules</b>	<b>11</b>
A.1 Définition et propriétés des groupes . . . . .	11
A.2 Définition et propriétés des anneaux . . . . .	11
A.3 Définition et propriétés des modules . . . . .	11
A.3.1 Généralités . . . . .	11
A.3.2 Modules sur un anneau principal . . . . .	12
<b>B Rappels d'algèbre linéaire</b>	<b>13</b>
B.1 Orthonormalisation de Gram-Schmidt (GSO) . . . . .	13
<b>C Code SageMath</b>	<b>14</b>

# Notations

- $\mathbb{Z}$  : L'ensemble des entiers relatifs.
- $\mathbb{R}$  : L'ensemble des réels.
- $\mathcal{L}$  : Un réseau, désigné par une lettre majuscule calligraphiée.
- $A^T$  : La transposée de la matrice  $A$ .
- $K$  : Un corps.
- $F$  : Un corps fini.
- $F[X]$  : L'anneau des polynômes univariés à coefficients dans le corps fini  $F$ .

# Guide de Lecture

Dans ce document, chaque définition est suivie d'un exemple concret illustrant la notion en question, ainsi que d'un contre-exemple visant à en exposer les subtilités et les exceptions éventuelles. Cette approche permet de mieux comprendre les conditions et les limitations associées à chaque concept. L'objectif est de clarifier les différences entre les situations où une définition est applicable et celles où elle ne l'est pas, afin de renforcer la compréhension approfondie des théorèmes et des constructions présentés.

# Introduction

# Introduction

L'objectif de ce stage est d'explorer les réseaux euclidiens et polynomiaux, ainsi que d'analyser les techniques de réduction de réseau. L'enjeu est d'adapter les méthodes de réduction utilisées dans le cadre des réseaux polynomiaux au cas des réseaux entiers.

La réduction de réseau est un outil essentiel dans plusieurs domaines de la cryptographie, notamment dans les algorithmes de sécurité basés sur la difficulté de résoudre des problèmes liés aux réseaux. En particulier, la réduction de réseaux polynomiaux joue un rôle clé dans la recherche de solutions efficaces à ces problèmes, et l'adaptation de ces méthodes pour les réseaux entiers pourrait avoir des implications importantes pour la sécurité des systèmes cryptographiques. Ce stage vise donc à approfondir cette adaptation et à en étudier les applications pratiques.

# Chapitre 1

## Réseaux euclidiens et polynomiaux

### 1.1 Généralités sur les réseaux

#### 1.1.1 Définitions et exemples

Nous considérons un espace euclidien, c'est-à-dire un espace vectoriel réel de dimension finie muni d'un produit scalaire, noté  $\langle f, g \rangle$ . Ici, nous utiliserons le produit scalaire usuel, défini par  $\langle f, g \rangle = f \cdot g^T$  lequel induit la norme-2, donnée par  $\|f\|_2 = (f \cdot f^T)^{1/2}$ .

**Définition 1.1.** Soit  $n \in \mathbb{N}$ .  $\mathbb{Z}$  module reseau "euclidien" ?

**Définition 1.2** (WALLET s. d.). Un **réseau euclidien** est un sous-groupe discret de  $\mathbb{R}^n$

**Définition 1.3** (ALLINI 2014). Un réseau euclidien  $(\Lambda, q)$  est un  $\mathbb{Z}$ -module libre  $\Lambda$  de rang fini avec une forme quadratique définie positive  $q$  sur  $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$

*Exemple 1.1.*

def de la base d'un reseau  
def d'un plus court vecteur

**Définition 1.4** (WALLET s. d.). On appelle minimum d'un réseau  $\mathcal{L}$  la quantité

$$\lambda_1 = \min\{r > 0 : |\mathcal{B}(r) \cap \mathcal{L}| > 1\} \in \mathbb{R}_+$$

problematique -> differentes bases -> des bases avec de courts vecteurs,

#### 1.1.2 Quelques problèmes algorithmiques liés aux réseaux euclidiens

Le calcul du plus court vecteur dans un réseau est un problème difficile.

Considérons le problème suivant :

- **Shortest Vector Problem (SVP)** : Étant donnée une base  $B$  d'un réseau  $L$ , trouver un vecteur  $v \neq 0$  tel que  $\|v\| = \lambda_1(L)$ . Ce problème est **NP-complet** (Ajtai).

On s'intéresse souvent à une version approximative plus accessible :

- **SVP** $_{\gamma}$ , où  $\gamma > 0$  : Étant donnée une base  $B$  du réseau  $L$ , trouver un vecteur  $v \neq 0$  tel que  $\|v\| \leq \gamma \cdot \lambda_1(L)$ .

L'état des connaissances actuelles est le suivant :

- Pour  $\gamma = O(1)$ , le problème reste **NP-complet**.
  - Pour  $\gamma = \text{poly}(n)$ , il existe des algorithmes en **temps exponentiel**.
  - Pour  $\gamma = 2^{O(n)}$ , l'algorithme **LLL** permet de le résoudre en **temps polynomial**.
- Un autre problème important concerne la recherche de vecteurs proches dans un réseau.
- **Closest Vector Problem (CVP)** : Étant donné une cible  $t \in \mathbb{R}^m$  et un réseau  $L(B)$ , trouver un vecteur  $v \in L$  tel que

$$\|t - v\| = d(t, L) := \min\{\|t - v\| \mid v \in L\}.$$

De même, on peut considérer une version approximative :

- **CVP** $_{\gamma}$ , où  $\gamma > 0$  : Trouver un vecteur  $v \in L$  tel que

$$\|t - v\| \leq \gamma \cdot d(t, L).$$

Le problème CVP est en général difficile pour un réseau arbitraire. Cependant, pour certaines familles spécifiques de réseaux, comme  $\mathbb{Z}^n$ , des algorithmes en temps polynomial sont connus. La qualité de la base choisie joue un rôle crucial dans la résolution du problème.

## 1.2 Réduction de réseaux euclidiens et polynomiaux

### 1.2.1 Réduction de réseaux euclidiens

### 1.2.2 Réduction de réseaux polynomiaux

reseau reduit chap 16

**Définition 1.5** (LEBRETON 2014). Soit  $\mathbb{K}$  un corps et  $M \in \mathbb{K}[x]_{1 \times n}$ . On définit le **degré de ligne** du vecteur ligne  $M$  par :

$$rdeg(M) = \max(\deg(m_i))_{i \in \{1, \dots, n\}}$$

**Définition 1.6** (LEBRETON 2014). Soit  $\mathbb{K}$  un corps et  $M \in \mathbb{K}[x]_{n \times n}$ . On définit le **degré de ligne** de la matrice  $M$  par :

$$rdeg(M) = \max(rdeg(ligne_i))_{i \in \{1, \dots, n\}}$$

*Exemple 1.2.* Soit  $M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ x & 1 & x+1 & 0 \\ 1 & x^3+x^2 & x & 0 \\ x^2 & 0 & x^4+x^3 & 0 \end{pmatrix} \in \mathbb{F}_2[x]$  alors  $row\_degree(M) =$   
 $\begin{pmatrix} 0 & 1 & 3 & 4 \end{pmatrix} \in \mathbb{Z}^4$

**Définition 1.7.** Soit  $s \in \mathbb{Z}^n$ . On définit le degré de ligne décalé du vecteur ligne  $M$  par :

$$rdeg_s(M) = \max(\deg(m_i) + s_i)$$

Je cite WALLET s. d. je cite ALLINI 2014 et puis WIKIPEDIA CONTRIBUTORS Consulté en 2025 et finalement GATHEN et GERHARD 2003



## Chapitre 2

# Adaptation de la réduction de réseaux polynomiaux au cas entier

## Chapitre 3

# Réseaux définis par relations plutôt que par générateurs

# Conclusion et perspectives

# Annexe A

## Rappels d'algèbre : Groupes, Anneaux et Modules

### A.1 Définition et propriétés des groupes

### A.2 Définition et propriétés des anneaux

### A.3 Définition et propriétés des modules

#### A.3.1 Généralités

La notion de module est la généralisation naturelle de celle d'espace vectoriel. Dans toute la suite  $A$  désigne un anneau commutatif.

**Définition A.1.** Un  $A$ -module  $(M, +, \cdot)$  est un ensemble :

- muni d'une loi interne  $+$  tel que  $(M, +)$  est un groupe abélien.
- muni d'une loi externe  $A \times M \rightarrow M, (a, m) \mapsto a \cdot m$ , qu'on notera  $am$  vérifiant les quatre propriétés suivantes :

1. Distributivité :  $\alpha(m + m') = \alpha m + \alpha m'$
2. Distributivité :  $(\alpha + \beta)m = \alpha m + \beta m$
3. Associativité :  $(\alpha\beta)m = \alpha(\beta m)$
4. Neutre :  $1m = m$

pour tout  $\alpha, \beta \in A$  et  $m, m' \in M$

*Remarque A.1.* La définition d'un module peut être vue comme une généralisation de celle d'un espace vectoriel. En effet, un module est un espace vectoriel dans lequel l'hypothèse sur  $A$  est affaiblie : au lieu d'être un corps,  $A$  est un anneau, ici commutatif, on ne se soucie donc pas de la distinction entre modules à gauche ou à droite.

**Définition A.2.** Soit  $M$  un  $A$ -module. Un sous-module  $N$  de  $M$  est un sous-groupe de  $(M, +)$  stable pour la multiplication externe par tout élément de  $A$ .

**Définition A.3.** type fini

**Définition A.4.** libre

proposition : libre et type fini  $\Rightarrow$  base finie  
exemples et contre-exemple

### **A.3.2 Modules sur un anneau principal**

Dans cette partie,  $A$  désigne un anneau principal.

# Annexe B

## Rappels d'algèbre linéaire

### B.1 Orthonormalisation de Gram-Schmidt (GSO)

On se considère dans un espace euclidien. Soit  $B = (b_i)_{1 \leq i \leq n}$  une base de  $\mathbb{R}^n$ , on peut construire la **base de Gram-Schmidt (GS)** associée à cette base par le procédé récursif suivant :

$$b_1^* := b_1$$

$$b_i^* := b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*, \quad \text{avec } \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$$

où  $\mu_{i,j}$  est appelé **coefficient de Gram-Schmidt** associé au vecteur  $b_i$ .

Notons  $B^*$  la matrice des  $b_i^*$ , et  $U$  la matrice des  $\mu_{i,j}$ . Alors, on a la relation :

$$B = B^* U$$

*Remarque B.1.* —  $U$  est triangulaire avec un déterminant égal à 1.

— On ne normalise pas, sinon cela introduit des racines et on risque de passer de  $\mathbb{Q}$  à  $\mathbb{R} \setminus \mathbb{Q}$ . De plus, la normalisation impose un volume de 1 et ne conserve donc pas l'information volumique du réseau associé.

*Proposition B.1.* — Conservation du volume :  $\det L = \prod \|b_i^*\|$ .

— Propriété du plus petit vecteur\*\* :  $\lambda_1(\mathcal{L}) \geq \min \|b_i^*\|$ .

Le coût de l'algorithme de Gram-Schmidt (GSO) est en  $O(n^3)$  opérations arithmétiques dans  $\mathbb{Q}$ .

## Annexe C

### Code SageMath

# Bibliographie

- ALLINI, Elie Noumon (2014). *Théorie algorithmique des nombres*. Diaporama.
- GATHEN, Joachim Von Zur et Jorgen GERHARD (2003). *Modern Computer Algebra*. 2<sup>e</sup> éd.  
USA : Cambridge University Press. ISBN : 0521826462.
- LEBRETON, Romain (2014). *A crash course on Order Bases : Theory and Algorithms*.  
Diaporama.
- WALLET, Alexandre (s. d.). *Réseaux euclidiens et cryptographie*. Document PDF, Notes  
de cours.
- WIKIPEDIA CONTRIBUTORS (Consulté en 2025). *Réseau (géométrie)*.