RÉSEAUX EUCLIDIENS EN CRYPTOGRAPHIE
TD 1 – 2023

ALEXANDRE WALLET, QUYEN NGUYEN

Exercice 1. Soit $\mathcal{L}_1, \mathcal{L}_2$ deux réseaux de $\mathbb{R}^m$. Montrer que :
— si $\mathcal{L}_1 + \mathcal{L}_2$ est un réseau, alors $\mathrm{rk}(\mathcal{L}_1 + \mathcal{L}_2) \geq \max(\mathrm{rk}\,\mathcal{L}_1, \mathrm{rk}\,\mathcal{L}_2)$;
— $\mathcal{L}_1 \cap \mathcal{L}_2$ est un réseau et $\mathrm{rk}(\mathcal{L}_1 \cap \mathcal{L}_2) \leq \min(\mathrm{rk}\,\mathcal{L}_1, \mathrm{rk}\,\mathcal{L}_2)$.
Donner des exemples où les inégalités sont atteintes, et non atteintes.

Exercice 2. (Réseaux et non-réseaux)

(1) L'ensemble $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un réseau de $\mathbb{R}$?

(2) Soit V la droite de $\mathbb{R}^2$ engendrée par $(1, \sqrt{2})$. Quel est le rang de $\mathbb{Z}^2 \cap V$? Si π désigne la projection orthogonale sur V, l'ensemble $\pi(\mathbb{Z}^2)$ est-il un réseau de $\mathbb{R}^2$?

(3) Montrer que les sous-groupes de $\mathbb{R}$ sont soit denses, soit de la forme $\alpha\mathbb{Z}$ pour $\alpha \in \mathbb{R}$.

Exercice 3 (Problèmes algorithmiques, partie 1)**.** Le but est de donner des algorithmes pour résoudre chacun des problèmes ci-dessous. On donnera la complexité en nombre d'opérations. Dans toutes les questions, on pourra toujours supposer que les réseaux sont décrits par un système générateur.

(1) *(Base)* Soit $g_1, \ldots, g_n$ une famille génératrice d'un réseau $\mathcal{L} \subset \mathbb{R}^m$. Calculer une base de $\mathcal{L}$.

(2) *(Appartenance)* Soit $v \in \mathbb{R}^m$ et $\mathcal{L}$ un réseau de $\mathbb{R}^m$. Déterminer si $v \in \mathcal{L}$ ou non.

(3) *(Sous-réseau, égalité)* Soit $\mathcal{L}, \mathcal{L}'$ deux sous-réseaux de $\mathbb{R}^m$. Déterminer si $\mathcal{L} \subset \mathcal{L}'$, $\mathcal{L}' \subset \mathcal{L}$ ou $\mathcal{L} = \mathcal{L}'$.

(4) *(Somme de réseaux)* Donner un algorithme pour calculer une base de $\mathcal{L} + \mathcal{L}'$.

Exercice 4 (Dualité, problèmes algorithmiques, partie 2)**.** Soit $\mathcal{L} \subset \mathbb{R}^m$ un réseau et V l'espace vectoriel qu'il engendre. Le dual de $\mathcal{L}$ est l'ensemble

$$\mathcal{L}^\vee = \{u \in V \ : \ \forall\, v \in \mathcal{L}, \langle u, v\rangle \in \mathbb{Z}\}.$$

(1) Montrer que $\mathcal{L}^\vee$ est un réseau de même rang que $\mathcal{L}$. Si $\mathbf{B}$ est une base de $\mathcal{L}$, donner une base de $\mathcal{L}^\vee$.

(2) Soit $\mathcal{L}_1, \mathcal{L}_2$ deux réseaux de $\mathbb{R}^m$. Montrer que $\mathcal{L}_1^{\vee\vee} = \mathcal{L}_1$, $(\mathcal{L}_1 + \mathcal{L}_2)^\vee = \mathcal{L}_1^\vee \cap \mathcal{L}_2^\vee$ et $(\mathcal{L}_1 \cap \mathcal{L}_2)^\vee = \mathcal{L}_1^\vee + \mathcal{L}_2^\vee$.

(3) Donner un algorithme pour calculer une base de $\mathcal{L}_1 \cap \mathcal{L}_2$.

Exercice 5 (Plus difficile, faire des dessins)**.** Soit $\mathcal{L}, \mathcal{L}'$ deux réseaux de même rang.

(1) Montrer que si $\mathcal{L}' \subsetneq \mathcal{L}$, alors $\det \mathcal{L}' > \det \mathcal{L}$.

(2) Plus généralement, on veut montrer que $[\mathcal{L} : \mathcal{L}'] = \frac{\det \mathcal{L}'}{\det \mathcal{L}}$.

(a) On appelle *domaine fondamental* d'une base $\mathbf{B}$ de $\mathbb{R}^n$ l'ensemble

$$\mathcal{D}_{\mathbf{B}} = \Big\{ \sum_{i \leq n} x_i \mathbf{b}_i \ : \ x_i \in [0,1) \Big\}.$$

Montrer que $\mathbb{R}^n = \bigcup_{\mathbf{u} \in \mathcal{L}} (\mathbf{u} + \mathcal{D}_{\mathbf{B}})$, où l'union est disjointe.

(b) Soit $\mathcal{D}_{\mathbf{B}}$ et $\mathcal{D}_{\mathbf{B}'}$ des domaines fondamentaux pour $\mathcal{L}$ et $\mathcal{L}'$. Montrer que pour tout $\mathbf{u} \in \mathcal{L}$, on a $\sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathcal{D}_{\mathbf{B}})\big) = \mathrm{Vol}(\mathcal{D}_{\mathbf{B}})$.

(c) En déduire que $\mathcal{L}/\mathcal{L}'$ est fini, puis le résultat annoncé.

À noter : il existe une autre preuve, plus algorithmique mais moins visuelle, reposant sur le théorème de classification des groupes abéliens.