M2 CRYPTO
RÉSEAUX EUCLIDIENS EN CRYPTOGRAPHIE - TD 1

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. Autour des réseaux de rang 1 :
— L'ensemble $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un réseau de $\mathbb{R}$?
— L'ensemble $\mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ est-il un réseau de $\mathbb{R}^2$?
— Montrer que les sous-groupes de $\mathbb{R}$ sont soit dense, soit de la forme $\alpha\mathbb{Z}$ pour $\alpha \in \mathbb{R}$.

Exercice 3. Soit $\mathcal{L}$ un réseau de dimension n. Montrer que le nombre de vecteurs $x \in \mathcal{L}$ tels que $||x|| = \lambda_1(\mathcal{L})$ est majoré par 3^n. Ce nombre s'appelle aussi le *kissing number*. On pourra regarder le volume des boules ouvertes centrées en ces points et de rayon $\lambda_1/2$.

Exercice 4. 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.