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.

1. Solutions

1 Si $\mathcal{L}_1 + \mathcal{L}_2$ est un réseau, il contient clairement chacune des deux opérandes. On atteint par exemple l'égalité avec $\mathcal{L}_1 = 2\mathbb{Z}$ et $\mathcal{L}_2 = 3\mathbb{Z}$, dont la somme est $\mathbb{Z}$, et tous ces réseaux sont de rang 1. L'inégalité peut être stricte : prenant e_1, e_2 la base canonique de $\mathbb{R}^2$, et $\mathcal{L}_i =_i$, la somme est $\mathbb{Z}^2$ qui est de rang 2. Notons ensuite que l'intersection de réseaux est toujours un ensemble discret, et donc un réseau qui est contenu dans chaque membre décrivant l'intersection. Si $\mathcal{L}_2 \subset \mathcal{L}_1$, l'intersection est $\mathcal{L}_2$ et l'inégalité est atteinte. L'exemple $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ montre que le rang peut rester le même. Enfin, $\mathbb{Z}e_1 \cap \mathbb{Z}e_2 = \{0\}$, qui montre que l'inégalité peut être stricte.

2 Bien que $G = \mathbb{Z} + \sqrt{2}\mathbb{Z}$ soit un sous-groupe de $\mathbb{R}$, il n'est pas discret et n'est donc pas un réseau de $\mathbb{R}$. Pour le montrer, il suffit de trouver une suite de G qui tend vers 0. Une candidate est la suite de $(\sqrt{2}-1)^n$, et il suffit donc de montrer que chacun de ses termes est dans G. Comme on a $(\sqrt{2}-1)^n = \sum_{i=0}^n \binom{n}{i}\sqrt{2}^i(-1)^{n-i}$, il suffit de montrer que tous les $\sqrt{2}^i$ sont dans G. Si i est pair c'est immédiat, sinon $i = 2j+1$ avec j entier et on peut écrire $\sqrt{2}^i = 2^j\sqrt{2} \in G$.
La subtilité du deuxième point est dans l'identification qu'on fait sur $\mathbb{R}^2$, ou encore sur la représentation des objets. Si on le voit comme le groupe abélien $\mathbb{R} \oplus \mathbb{R}$ avec sa topologie produit, il est clair que $\mathcal{L} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ en est un sous-groupe discret. Si on veut raisonner en terme de l'espace Euclidien $\mathbb{R}^2$ muni de sa norme Euclidienne usuelle et de la topologie induite, on peut construire une *isométrie* φ entre $\mathcal{L}$ et le réseau (au sens du cours) $\mathbb{Z}(1,0) \oplus \mathbb{Z}(0,\sqrt{2})$, qui est bien un sous-réseau de rang 2 de $\mathbb{R}^2$. Si on s'autorise à changer la norme sur $\mathbb{R}^2$, on peut trouver d'autres isométries : par exemple, l'association $1 \mapsto (1,0)$ et $\sqrt{2} \mapsto (1,1)$ identifie $\mathcal{L}$ au réseau $\mathbb{Z}(1,0) \oplus \mathbb{Z}(1,1)$ dans l'espace $\mathbb{R}^2$ muni de la norme induite par $Q = \begin{bmatrix} 1 & -1 \\ -1 & \sqrt{2}-1 \end{bmatrix}$. Le dernier point est un classique. Soit G un sous-groupe non trivial de $\mathbb{R}$. En particulier il est non-vide, et il existe donc au moins un élément strictement positif. Ceci nous permet de définir $\alpha = \inf G \cap \mathbb{R}_+^*$. Il y a alors deux cas de figure :

- **Cas** $\alpha = 0$ **:** Dans ce cas G est dense. En effet, par la propriété de la borne inférieure et la définition de α, pour tout $\epsilon > 0$ on peut trouver $g \in G$ tel que $0 < g < \epsilon$. Soit $x \in \mathbb{R} \setminus G$ et notons $\lfloor a \rfloor$ le plus grand entier inférieur à un réel a, satisfaisant $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$. Comme G est un groupe additif, on a $\lfloor x/g \rfloor g \in G$. On a de plus $0 \leq x - \lfloor x/g \rfloor g = g(x/g - \lfloor x/g \rfloor) < \epsilon$, ce qu'on voulait démontrer.
- **Cas** $\alpha > 0$ **:** On a directement que G est discret, puisque l'intervalle $(-\alpha/2, \alpha/2)$ ne contient que 0, donc par translation par les éléments de g, les intervalles $(g - \alpha/2, g + \alpha/2)$ ne contiennent qu'un seul élément de G. Il faut montrer que $\alpha \in G$, puis que $G = \alpha\mathbb{Z}$. Deux utilisations de la propriété de la borne inférieure donnent $g, g' \in G$ tels que $\alpha \leq g < g' < 2\alpha$. Ceci entraine que $0 < g' - g \leq \alpha$, et donc par définition de α que $\alpha = g' - g \in G$. Il est ensuite clair que $\alpha\mathbb{Z} \subset G$. Pour l'autre inclusion, notons que pour tout $g \in G$, on a $g - \lfloor g/\alpha \rfloor \alpha \in G$. Par définition, ceci implique $0 \leq \alpha(g/\alpha - \lfloor g/\alpha \rfloor) < \alpha$, ce qui n'est possible que si $g = \lfloor g/\alpha \rfloor \alpha$.

3 Soit X l'ensemble des vecteurs de norme λ et considérons les boules ouvertes centrées en les points de X de rayon $\lambda/2$. Ces boules sont disjointes : en effet la distance entre deux points quelconque du réseau est plus grande que λ (sinon en translatant, on aurait un vecteur de norme plus petite). Elles sont de plus incluses dans la boule de centre 0 et de rayon $3\lambda/2$. Ainsi

$$\#X \leq \frac{\text{vol(boule de rayon } 3\lambda/2)}{\text{vol(boule de rayon } \lambda/2)} = 3^d.$$

4 (1) Soient $\mathbf{B}$ et $\mathbf{B}'$ deux bases (sous forme de matrices) de $\mathcal{L}$ et $\mathcal{L}'$ respectivement. Par hypothèse, il existe une matrice $\mathbf{U} \in \mathcal{M}_n(\mathbb{Z})$ telle que $\mathbf{B}' = \mathbf{BU}$. Comme $\mathbf{B}'$ est de rang plein, on a $\det \mathbf{U} \neq 0$. D'autre part, $\mathbf{U}$ est entière et comme $\mathcal{L}' \neq \mathcal{L}$, on a nécessairement $|\det \mathbf{U}| > 1$. On conclut par définition du déterminant d'un réseau.

(a) Soit $\mathbf{x} \in \mathbb{R}^n$, et écrivons $\mathbf{x} = \sum_i x_i \mathbf{b}_i$, où les $\mathbf{b}_i$ sont les vecteurs colonnes de $\mathbf{B}$. En notant $\lceil \cdot \rfloor$ la partie entière d'un réel et $\{\cdot\}$ sa partie fractionnaire, on peut décomposer $\mathbf{x} = \sum_i \lceil x_i \rfloor \mathbf{b}_i + \sum_i \{x_i\} \mathbf{b}_i$, où le premier vecteur est dans $\mathcal{L}$ et le second dans $\mathcal{D}_\mathbf{B}$. Montrons maintenant que cette décomposition est unique. Supposons que $\mathbf{x} \in \mathbf{u} + \mathcal{D}_\mathbf{B} \cap \mathbf{u}' + \mathcal{D}_\mathbf{B}$, de sorte que $\mathbf{x} = \mathbf{y} + \mathbf{u} = \mathbf{y}' + \mathbf{u}'$ pour $\mathbf{y}, \mathbf{y}'$ dans $\mathcal{D}_\mathbf{B}$. Ceci implique que $\mathbf{y} - \mathbf{y}' \in \mathcal{L}$. Si $(y_i)_i$, $(y_i')_i$ sont les coordonnées respectives de $\mathbf{y}, \mathbf{y}'$ dans la base $\mathbf{B}$, on remarque $\max_i |y_i - y_i'| < 1$, donc $\mathbf{y} = \mathbf{y}'$ et par extension $\mathbf{u} = \mathbf{u}'$.

(b) On se convainc par un dessin qu'il s'agit de montrer qu'il n'y a qu'une copie de $\mathcal{D}_\mathbf{B}$ dans $\mathcal{D}_{\mathbf{B}'}$ par classes de $\mathcal{L}/\mathcal{L}'$. Il s'agit ensuite d'utiliser les propriétés élémentaires du volume (ou plus généralement de la mesure de Lebèsgue) :

$$\begin{aligned}
\sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathcal{D}_\mathbf{B})\big) &= \sum_{\mathbf{u}' \in \mathcal{L}'} \mathrm{Vol}(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{x} + \mathbf{u} + \mathcal{D}_\mathbf{B})) \\
&= \sum_{\mathbf{u}' \in \mathcal{L}'} \mathrm{Vol}\big((\mathcal{D}_{\mathbf{B}'} - \mathbf{u}) \cap (\mathbf{x} + \mathcal{D}_\mathbf{B})\big) \\
&= \mathrm{Vol}(\mathbf{x} + \mathcal{D}_\mathbf{B}),
\end{aligned}$$

où on utilise l'invariance du volume par translation à la deuxième ligne, et la question (1) à la troisième. On conclut encore par invariance par translation.

(c) D'après la question (1) on a $\mathcal{D}_{\mathbf{B}'} = \bigcup_{\mathbf{u} \in \mathcal{L}} (\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_\mathbf{B}))$. Un réseau étant dénombrable, on en déduit $\mathrm{Vol}(\mathcal{D}') = \sum_{\mathbf{u} \in \mathcal{L}} \mathrm{Vol}(\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_\mathbf{B}))$. Les classes $\bar{\mathbf{u}}$ de $\mathcal{L}/\mathcal{L}'$ correspondent aux "cosets" $\mathbf{u} + \mathcal{L}'$, ce qui donne

$$\begin{aligned}
\mathrm{Vol}(\mathcal{D}') &= \sum_{\bar{\mathbf{u}} \in \mathcal{L}/\mathcal{L}'} \sum_{\mathbf{x} \in \mathbf{u} + \mathcal{L}'} \mathrm{Vol}\big((\mathcal{D}_{\mathbf{B}'} \cap (\mathbf{u} + \mathcal{D}_\mathbf{B})\big) \\
&= \sum_{\bar{\mathbf{u}} \in \mathcal{L}/\mathcal{L}'} \mathrm{Vol}(\mathcal{D}),
\end{aligned}$$

d'après la question précédente. Comme $\mathrm{Vol}(\mathcal{D}')$ est fini, $\mathcal{L}/\mathcal{L}'$ est nécessairement un groupe fini et avec la définition du déterminant d'un réseau, on obtient le résultat.