TD 5. *HNF* - Réseaux - LLL

Exercice 1 (Forme Normale de Hermite)
Étant donné un sous-module M de rang r de $\mathbb{Z}^n$, décrit par la donnée de $k \geq r$ générateurs, on considère la matrice de taille $k \times n$ formée des coordonnées (en ligne) de chacun des générateurs dans la base canonique de $\mathbb{Z}^n$. La *forme normale de Hermite* de M s'obtient à partir de cette matrice à l'aide d'opérations élémentaires sur ses lignes ; c'est la matrice qui vérifie :

(i) sur chaque ligne, l'indice de colonne du premier cœfficient non nul est strictement supérieur à celui du premier cœfficient non nul de la ligne précédente ;

(ii) ce cœfficient est > 0 et strictement supérieur à tous les cœfficients de sa colonne, lesquels sont des entiers naturels ;

(iii) les $k - r$ dernières lignes sont nulles.

1. On reprend le sous-module L de $\mathbb{Z}^2$ engendré par les vecteurs $(1, 2)$ et $(2, 7)$. Écrire la matrice correspondante et décrire l(es) opération(s) élémentaire(s) qui permet(tent) d'en déduire sa HNF. Retrouver la base de $\mathbb{Z}^2$ adaptée à L.
2. On considère le sous-module M de $\mathbb{Z}^2$ dont la matrice des générateurs est $\left(\begin{smallmatrix} 30 & -2 \\ 8 & -1 \end{smallmatrix}\right)$.
   a) Écrire une relation de Bézout liant 30 et 8 : $30u + 8v = d$;
   b) Appliquer à la matrice les opérations élémentaires $L_1 \leftarrow uL_1 + vL_2$, $L_2 \leftarrow -\frac{8}{d}L_1 + \frac{30}{d}L_2$. À la multiplication par quelle matrice ces opérations correspondent-elles ? Vérifier que son déterminant est ± 1.
   c) À ce stade, la condition (i) est satisfaite ; appliquer deux opérations élémentaires supplémentaires pour assurer la condition (ii).
   d) Peut-on en déduire une base adaptée à M ? En déduire la structure du quotient $\mathbb{Z}^2/M$.
3. Faire de même avec la matrice $\begin{pmatrix} 2 & 1 & 0 \\ 5 & -2 & 1 \\ 3 & -3 & 1 \end{pmatrix}$, en commençant par chercher une relation de Bézout liant 2 et 5. On vérifiera que le module quotient $\mathbb{Z}^3/M$ est sans torsion, en est-il de même si l'on remplace M par $2M$?

Exercice 2
Soit n un entier ≥ 1, on considère sur $\mathbb{R}^n$ la forme bilinéaire symétrique usuelle qui à $(x, y) \in \mathbb{R}^n \times \mathbb{R}^n$ associe $x \cdot y = \sum_{i=1}^{n} x_i y_i$. On note H l'hyperplan de $\mathbb{R}^n$ d'équation :

$$x_1 + \cdots + x_n = 0 \ .$$

Soit D_{n-1} le $\mathbb{Z}$-module engendré par les vecteurs $(1, -1, 0, \ldots, 0)$, $(0, 1, -1, 0, \ldots, 0)$, $\ldots$ $(0, \ldots, 0, 1, -1)$ de H, muni du produit scalaire ci-dessus.

a) Vérifier que D_{n-1} est libre de rang $n - 1$ et écrire sa matrice de Gram G_{n-1} ;

b) à l'aide de celle-ci, montrer que $\det(D_{n-1}) = \sqrt{n}$.
[On pourra chercher une relation de récurrence entre $\det(G_{n+1})$, $\det(G_n)$ *et* $\det(G_{n-1})$*.]*

Exercice 3
Soit $j \in \mathbb{C}$ une racine cubique de l'unité. On vérifie comme dans l'exercice 1. du TD4 que $\mathbb{Z}[j]$ est un $\mathbb{Z}$-module libre de rang 2, de base $(1, j)$, donc $\mathbb{Z}[j] = \{a + bj,\ a, b \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Z}j$. On pose $\mathbb{R}[j] = \mathbb{R} \oplus \mathbb{R}j$ et on définit $q : \mathbb{R}[j] \to \mathbb{R}$ par :

$$q(x + yj) = (x + yj)(x + yj^2) = x^2 - xy + y^2 \ .$$

a) Vérifier que q est une forme quadratique définie positive.

b) Écrire la matrice de Gram du réseau $(\mathbb{Z}[j], q)$, en déduire son volume. Comparer avec le déterminant de la matrice formée par les coordonnées des vecteurs de base de $\mathbb{Z}[j]$ dans la base $(1, i)$ de $\mathbb{C}$.

Exercice 4 (LLL)
On souhaite déterminer les bases LLL-réduites des sous-$\mathbb{Z}$-modules de $\mathbb{R}^n$ — muni du produit scalaire usuel — donnés par les bases suivantes.

1. On prend $n = 2$ et $b_1 = (-3, 5)$, $b_2 = (1, 3)$:
   a) calculer $\langle b_1, b_1\rangle$ et $\langle b_2, b_1\rangle$, en déduire $b_2^* = b_2 - \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} b_1$; vérifier que $\langle b_2^*, b_1\rangle = 0$ et que $\langle b_2^*, b_2^*\rangle = \frac{98}{17}$.
   b) Déterminer l'entier q le plus proche de $\frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle}$, $\mu_{2,1} = q - \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle}$ et $\hat{b}_2 = b_2 - qb_1$. Calculer $(\frac{3}{4} - \mu_{2,1}^2)\langle b_1, b_1\rangle$; $(b_1, \hat{b}_2)$ est-elle LLL-réduite ?
   c) On échange b_1 et $\hat{b}_2$: $\tilde{b}_1 = (1, 3)$, $\tilde{b}_2 = (-3, 5)$. Reprendre les opérations listées ci-dessus ; la base $(\hat{\tilde{b}}_1, \hat{\tilde{b}}_2)$ obtenue est-elle LLL-réduite ?
2. Faire de même avec $b_1 = (2, 6)$, $b_2 = (1, 2)$ *[l'échange* c) *pourra éventuellement être réitéré]* ; puis avec le sous-module de rang 2 de $\mathbb{R}^3$ engendré par $b_1 = (1, 5, -1)$ et $b_2 = (0, 9, -2)$ *[pour ceux qui n'ont pas de calculatrice : on vérifiera que* $\langle b_2^*, b_2^*\rangle = \frac{86}{27}$ *].*
3. On prend $n = 3$, suivre les étapes de l'algorithme donné en cours pour trouver la base LLL-réduite correspondant aux bases de sous-$\mathbb{Z}$-modules de $\mathbb{R}^3$ ci-dessous :
   a) $b_1 = (1, 3, 0)$, $b_2 = (-2, 6, 1)$, $b_3 = (-5, 5, -2)$;
   b) $b_1 = (1, 0, 1)$, $b_2 = (3, 1, -2)$, $b_3 = (2, -1, 0)$.