Réseaux euclidiens et leur groupe d'automorphismes

Exercice 1. Soit $B = (e_1, \ldots, e_n)$ une base d'un réseau $R \subset V$. Montrer que $B' = (e'_1, \ldots, e'_n)$ est également une base de R si et seulement si la matrice de passage P de B à B' est une matrice à coefficients entiers et de déterminant ± 1.

Exercice 2. Soit $B = (e_1 \ldots, e_n)$ une base d'un réseau euclidien $R \subset V$ et soit $B' = (e'_1, e'_2, \ldots, e'_n)$ une base d'un autre réseau euclidien $R' \subset V'$.
On appellera *matrice de Schäfli* S_B de la base $B = (e_1, \ldots, e_n)$ la matrice dans B du produit scalaire sur V.

1. Montrer que R et R' sont des réseaux euclidiens isométriques si et seulement s'il existe une base B'' de R' telle que $S_B = S_{B''}$.
2. Montrer que R et R' sont isométriques si et seulement s'il existe une matrice $n \times n$ P à coefficients entiers telle que $\det(P) = \pm 1$ et $P^t S_B P = S_{B'}$.
3. Justifier que $\mathrm{vol}(R) = \sqrt{\det(S_B)}$.
4. Trouver des bases (e_1, e_2, e_3) et (e'_1, e'_2, e'_3) de A_3 et D_3 qui ont pour matrice de Schäfli

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

5. Les réseaux euclidiens D_n et A_n sont-ils isomorphes, en général ? (On considérera l'ensemble des vecteurs non nuls de longueur minimale).

Exercice 3. On propose de calculer le groupe d'automorphismes du réseau canonique $\mathbb{Z}^n$. On rappelle que le groupe d'automorphismes $\mathrm{Aut}(R)$ d'un réseau euclidien $R \subset V$ est le sous–groupe des éléments de $O(V)$ qui préservent R.

1. Soit $R \subset V$ un réseau euclidien. Montrer que $\mathrm{Aut}(R)$ est fini.
2. On considère le réseau $R = \mathbb{Z}^n \subset \mathbb{R}^n$ muni de son produit scalaire canonique. Montrer que tout élément de $\mathrm{Aut}(R)$ permute les axes de coordonnées dans $\mathbb{R}^n$.
3. En déduire $\mathrm{Aut}(\mathbb{Z}^n)$.

Exercice 4. Dans cet exercice on considère le réseau A_n

$$A_n = \left\{(m_1, \ldots, m_{n+1}) |\, m_i \in \mathbb{Z}, \sum_{i=1}^{n+1} m_i = 0\right\}$$

muni de la restriction du produit scalaire canonique de $\mathbb{R}^{n+1}$.
On propose de calculer $\mathrm{Aut}(A_n)$.

1. Donner un sous–groupe de $\mathrm{Aut}(A_n)$ isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et un autre isomorphe à $\mathfrak{S}_{n+1}$.
2. Montrer que tout élément $\sigma \in \mathrm{Aut}(R)$ qui fixe les vecteurs $u = (1, -1, 0, \ldots, 0)$ et $v = (1, 0, -1, 0, \ldots, 0)$ est donné par une permutation des axes de coordonnées. (On pourra considérer les éléments de la forme $(1, 0, \ldots, 0, -1, 0, \ldots, 0)$).

3. En déduire $\mathrm{Aut}(A_n)$.

Exercice 5. *Isométries affines d'un réseau.* Soit V un espace euclidien (de dimension finie), et $R \subset V$ un réseau. On notera $\mathrm{Aff}(R)$ l'ensemble des bijections $f : V \to V$ de la forme

$$f : v \mapsto \phi(v) + w$$

avec $\phi \in \mathrm{GL}(V)$ et $w \in R$, telles que $f(R) = R$. On notera $\mathrm{Is}(R)$ l'ensemble des éléments de $\mathrm{Aff}(R)$ qui préservent la distance, cad. des isométries affines de V qui conservent R.

1. Montrer que $\mathrm{Aff}(R)$ et $\mathrm{Iso}(R)$ sont des sous–groupes de $\mathrm{Bij}(V)$.
2. Soit G un sous–groupe *fini* de $\mathrm{Aff}(R)$. Montrer qu'il existe un point $p \in V$ tel que $g(p) = p$ pour tout $g \in G$.
3. Soit T l'ensemble des translations $v \mapsto v + w$ dans $\mathrm{Aff}(R)$. Montrer que T est un sous–groupe abélien et distingué de $\mathrm{Aff}(R)$.
4. Soit $H \subset \mathrm{Iso}(R)$ un sous-groupe abélien et distingué. Justifier que pour tout $h \in H$ et tout $r \in R$ nous avons que
$$ht_r h t_{-r} = t_r h t_{-r} h,$$
où t_r est la translation de vecteur r. En déduire que si h s'écrit $v \mapsto \phi(v) + w$ alors
$$(\phi - \mathrm{Id})^2 = 0.$$
Conclure que $H \subset T$.

Exercice 6. *Groupes d'automorphismes des réseaux de dimension 2.*

Quels sont les groupes $\mathrm{Aut}(R)$ possibles pour R un réseau euclidien de dimension 2 ? Décrire les réseaux admettant chaque type de groupe d'automorphismes.

Exercice 7. *Réseaux de densité maximale dans* $\mathbb{R}^2$. On considère un réseau R de dimension 2, dont les vecteurs non nuls de longueur minimale ont norme 1. On cherche à minimiser le volume de R en respectant cette contrainte.

Soit e_1 un vecteur de longueur 1 dans R et e_2 un vecteur de longueur minimale parmi ceux qui ne sont pas contenus dans $\mathrm{Vect}(e_1)$.

1. Soit $v \in R$ non colinéaire à e_1 et soit v' sa projection orthogonale sur ${e_1}^{\perp}$. En considérant les vecteurs de la forme $v + ne_1$, montrer que $||v'|| \geq \frac{\sqrt{3}}{2}$.
2. Montrer que (e_1, e_2) est une base de R.
3. Justifier que la mesure de l'angle entre e_1 et e_2 est comprise entre $\frac{\pi}{3}$ et $\frac{2\pi}{3}$.
4. Justifier que le volume de R est au moins $\frac{\sqrt{3}}{2}$ et que ce volume est atteint uniquement par le réseau hexagonal engendré par deux vecteurs de longueur 1 formant un angle de mesure $\frac{\pi}{3}$.

Exercice 8. *Réseau dont les vecteurs minimaux ne forment pas une base.* On considère dans $\mathbb{R}^5$ le réseau R engendré par les éléments de la base canonique e_1, e_2, e_3, e_4 et le vecteur $v = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.

1. Montrer que tout élément non nul de R est de norme au moins 1.
2. Montrer qu'il existe dans R une famille de 5 vecteurs indépendants de norme 1 mais qu'aucune telle famille n'est une base de R.

Exercice 9. *Théorème de Minkowski.* Soit R un réseau dans $\mathbb{R}^d$ et soit C un convexe compact dans $\mathbb{R}^d$ qui est symétrique par rapport à l'origine et de volume $> 2^d \operatorname{vol}(R)$. On va montrer que C contient un point non-nul de R.

1. Soit $(e_1, \dots e_d)$ une base de R et soit $D = [0, 2[e_1 \times ...[0, 2[e_d$. Justifier que chaque élément de $\mathbb{R}^d$ est équivalent modulo $2R$ à un unique élément de D.
2. On considère l'application $C \to D$ qui envoie chaque $c \in C$ sur l'unique élément de D équivalent à c modulo $2R$. Justifier que cette application n'est pas injective.
3. Soient c_1, c_2 deux éléments de C équivalents modulo $2R$. Notant $c_2 = c_1 + 2r$ avec $r \in R$, justifier que $r \in C$.

Exercice 10. *Réseau de densité maximale dans* $\mathbb{R}^3$. Dans cet exercice, on se propose de trouver les réseaux de volume minimal parmi les réseaux de dimension 3 tels que $N(R) = 1$. On n'hésitera pas à s'appuyer sur les méthodes proposées dans l'exercice 7.

1. (*) Soit e_1 un vecteur non nul de norme minimale dans R, soit e_2 un vecteur de norme minimale dans R parmi ceux qui ne sont pas dans $\operatorname{Vect}(e_1)$ et soit e_3 un vecteur de norme minimale dans R parmi ceux qui ne sont pas dans $\operatorname{Vect}(e_1, e_2)$. Montrer que (e_1, e_2, e_3) est une base de R. Vous pouvez utiliser le résultat suivant : si R' est un réseau dans $\mathbb{R}^2$ engendré par e_1, e_2 avec $||e_1|| < ||e_2||$, alors chaque point du plan se trouve à une distance au plus $\frac{||e_2||}{\sqrt{2}}$ d'un point de R'.
2. En considérant le réseau engendré par $e_1, (1 - \epsilon_1)e_2, (1 - \epsilon_2)e_3$ montrer que e_1, e_2 et e_3 sont tous de norme 1.
3. Justifier qu'on peut supposer que S, la matrice de Schäfli de cette base, est de la forme
$$\begin{pmatrix} 1 & x & y \\ x & 1 & z \\ y & z & 1 \end{pmatrix}$$
avec $0 \leq x, y, \leq \frac{1}{2}$ et $-\frac{1}{2} \leq z \leq \frac{1}{2}$.
4. En considérant la norme de $-e_1 + e_2 + e_3$, justifier que $z \geq x + y - 1$.
5. Calculer $\det(S)$ en termes de x, y, z. (*) Montrer que si z est positif alors $\det(S) \geq \frac{1}{2}$ et qu'il y a égalité quand $x = y = z = \frac{1}{2}$.
6. (*)Montrer qu'on a toujours $\det(S) \geq \frac{1}{2}$. En déduire qu'un réseau de $\mathbb{R}^3$ engendré par trois vecteurs de norme 1 et d'angles deux-à-deux valant $\frac{\pi}{3}$ est de volume minimal parmi les réseaux de dimension 3 dont tout vecteur non nul est de norme au moins 1.