RÉSEAUX.

1 Définition

Définition 1 Soit E un espace vectoriel sur $\mathbb{R}$ de dimension finie. Une partie Λ de E est un réseau si

- Λ est sous-groupe additif de E ,
- l'espace vectoriel engendré par Λ est E tout entier,
- Λ est une partie discrète de E .

Théorème 1 de Weyl. Soit E un espace vectoriel de dimension finie sur $\mathbb{R}$. Une partie Λ de E est un réseau de E ssi il existe une base $e_1, \dots, e_n$ de E telle que $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \dots + \mathbb{Z}e_n$.

Définition 2 Soit E un e.v. de dim. finie sur $\mathbb{R}$ et Λ un réseau. On appelle base de Λ toute base $(e_1, \dots, e_n)$ de E telle que $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \dots + \mathbb{Z}e_n$.

Proposition 1 Soit E un e.v. de dim. finie sur $\mathbb{R}$, Λ un réseau et $(e_1, \dots, e_n)$, $(f_1, \dots, f_n)$ deux bases de Λ . Alors la matrice de passage A de la base $(e_1, \dots, e_n)$ à la base $(f_1, \dots, f_n)$ appartient à $GL(n, \mathbb{Z})$.

Démonstration. $f_j = \sum_i a_{ji} e_i$ où $a_{ij} \in \mathbb{Z}$ de même $e_j = \sum_i b_{ij} f_i$ où $b_{ij} \in \mathbb{Z}$ donc

$$e_j = \sum_k b_{kj} f_k = \sum_k \sum_i b_{kj} a_{ji} e_i$$

d'où $AB = Id$ avec $B = (b_{i,j})$. $\square$

Définition 3 Soit Λ un réseau de $\mathbb{R}^n$. Le déterminant de Λ est la valeur absolue du déterminant d'une base de Λ dans la base canonique de $\mathbb{R}^n$. $\det \Lambda = |\det(e_1, \dots, e_n)|$ où $e_1, \dots, e_n$ est une base de Λ .

Remarques. 1. Ce déterminant ne dépend pas de la base choisie car le déterminant d'une matrice de $GL(n, \mathbb{Z})$ vaut ± 1 .

2. Le déterminant de Λ est égale au volume du parallélépipède $\mathcal{P} = \{\sum x_i e_i : x_i \in [0, 1]\}$ défini par une quelconque base de Λ .

3. $\mathcal{P}$ est un domaine fondamental pour l'action de Λ sur $\mathbb{R}^n$.

Conséquence du théorème de Minkowski sur les convexes :

Théorème 2 Soit N une norme sur $\mathbb{R}^n$ et Λ un réseau de $\mathbb{R}^n$. Appelons $\mathcal{C}$ la boule unité. Alors la boule fermée $B(0, 2(\frac{\det \Lambda}{V(\mathcal{C})})^{1/n})$ contient au moins un point de Λ différent de 0.

Démonstration. Soit $f_1, \dots, f_n$ une base de Λ et $e_1, \dots, e_n$ la base canonique de $\mathbb{R}^n$. Appelons $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ l'application définie par $\phi(f_i) = e_i$. On a $|\det \phi| = \frac{1}{\det \Lambda}$ et $\phi(\Lambda) = \mathbb{Z}^n$ et

$$V(\phi(B(0, 2\left(\frac{\det \Lambda}{V(\mathcal{C})}\right)^{1/n})) = |\det \phi| \times V(B(0, 2\left(\frac{\det \Lambda}{V(\mathcal{C})}\right)^{1/n})) = |\det \phi| \times V(\mathcal{C}) \times 2^n \frac{\det \Lambda}{V(\mathcal{C})} = 2^n$$

donc $\phi(B(0, 2\left(\frac{\det \Lambda}{V(\mathcal{C})}\right)^{1/n}))$ contient un point de $\mathbb{Z}^n$ différent de 0. $\square$

Définition 4 Soit N une norme sur $\mathbb{R}^n$ et Λ un réseau de $\mathbb{R}^n$. Pour $k \in \{1, \dots, n\}$ on appelle $k^{\text{ième}}$ minimum de Λ pour la norme N la borne inférieure des $\lambda \geq 0$ tels que la boule fermée $B(0, \lambda)$ contienne au moins k éléments linéairement indépendants de Λ .

Notation $\lambda_k = \lambda_k(\Lambda, N) = k^{\text{ième}}$ minimum de Λ .

Remarques 1. On peut définir les minima d'une norme de $\mathbb{R}^n$ en considérant les minima du réseau canonique $\mathbb{Z}^n$ par rapport à cette norme. Ce point de vue est rattaché au précédent car si N est une norme et Λ un réseau on a

$$\lambda_k(N, \Lambda) = \lambda_k(N \circ B, \mathbb{Z}^n)$$

où B est un isomorphisme tel que $\phi(\mathbb{Z}^n) = \Lambda$.

2. λ_1 représente la longueur du plus court vecteur du réseau Λ . D'après le théorème précédent on a $\lambda_1 \leq 2\left(\frac{\det \Lambda}{V(\mathcal{C})}\right)^{1/n}$.

2 Théorème des minima successifs de Minkowski

Théorème 3 Soit N une norme sur $\mathbb{R}^n$ de boule unité $\mathcal{C}$ et Λ un réseau de $\mathbb{R}^n$. Alors

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 \dots \lambda_n V(\mathcal{C}) \leq 2^n \det \Lambda.$$

Nous allons prouver l'inégalité plus faible :

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 \dots \lambda_n V(\mathcal{C}) \leq 4^n n^{n/2} \det \Lambda.$$

Lemme 1 Il existe $x_1, \dots, x_n$ des éléments linéairement indépendants de Λ tels que pour chaque $k \in \{1, \dots, n\}$

$$x_1, \dots, x_k \in \lambda_k \mathcal{C}.$$

Démonstration. Soit $x_1, \dots, x_n$ une suite de vecteurs de Λ telle que

- x_1 est le plus court vecteur de $\Lambda \setminus \{0\}$,
- x_{k+1} est le plus court vecteurs de Λ indépendant de $x_1, \dots, x_k$.

L'existence de $x_1, \dots, x_n$ résulte du caractère discret de Λ . Montrons que pour $k = 1, \dots, n$, $N(x_k) \leq \lambda_k$. Si $N(x_k) > \lambda_k$ alors il existe des vecteurs indépendants de Λ , $y_1, \dots, y_k$ de norme $< N(x_k)$. L'un de ces vecteurs n'appartient pas à $\text{vect}(x_1, \dots, x_{k-1})$ ce qui contredit la minimalité de $N(x_k)$. Par définition des minima on a $N(x_k) = \lambda_k$. $\square$

Remarque $x_1, \dots, x_n$ ne forment en général pas une base de Λ . Ex : $\Lambda = \mathbb{Z}^4 + \frac{1}{2}(1, 1, 1, 1)\mathbb{Z}$, $x_1, \dots, x_4$ base canonique de $\mathbb{Z}^4$.

Lemme 2 Soit $x_1, \dots, x_n$ des éléments linéairement indépendants de Λ tels que pour chaque $k \in \{1, \dots, n\}$

$$x_1, \dots, x_k \in \lambda_k \mathcal{C}.$$

Soit $k \in \{2, \dots, n\}$ et $\lambda \in [0, \lambda_k[$. Si x est un élément de $\Lambda \cap \lambda \mathcal{C}$ alors x est dans l'espace vectoriel engendré par $x_1, \dots, x_{k-1}$. De même avec $k = 1$ on a $x = 0$.

Démonstration : Conséquence immédiate de la définition.

Proposition 2 Soit N une norme sur $\mathbb{R}^n$ de boule unité $\mathcal{C}$ et Λ un réseau de $\mathbb{R}^n$. Alors

$$\frac{2^n}{n!} \det \Lambda \leq \lambda_1 \dots \lambda_n V(\mathcal{C}).$$

Démonstration. Soit $x_1, \dots, x_n$ choisis comme dans les lemmes précédents. On a $y_i = \frac{1}{\lambda_i} x_i \in \mathcal{C}$. Les points $\pm y_1, \dots, \pm y_n$ sont tous de norme ≤ 1 donc les points de $K = \{\sum_i t_i y_i : \sum |t_i| \leq 1\}$ aussi de norme ≤ 1 . Or le volume de K est égale à

$$\frac{2^n}{n!} |\det(y_1, \dots, y_n)|$$

donc

$$V(\mathcal{C}) \geq V(K) = \frac{2^n}{n!} |\det(y_1, \dots, y_n)| = \frac{2^n}{n! \lambda_1 \dots \lambda_n} |\det(x_1, \dots, x_n)| \geq \frac{2^n}{n! \lambda_1 \dots \lambda_n} \det \Lambda. \square$$

Lemme 3 Si la norme N est issu d'un produit scalaire $(\cdot|\cdot)$ alors

$$\lambda_1 \dots \lambda_n V(\mathcal{C}) \leq 2^n \det \Lambda.$$

démonstration. Soit $x_1, \dots, x_n$ des éléments linéairement indépendants de Λ tels que pour chaque $k \in \{1, \dots, n\}$, $x_1, \dots, x_k \in \lambda_k \mathcal{C}$. Orthonormalisons $x_1, \dots, x_n$ on trouve une base $y_1, \dots, y_n$ orthonormale pour le produit scalaire $(\cdot|\cdot)$. Définissons un nouveau produit scalaire $(\cdot|\cdot)^*$ par $\lambda_1 y_1, \dots, \lambda_n y_n$ est une base orthonormée pour $(\cdot|\cdot)^*$ et notons $\mathcal{C}^*$ la boule unité associé a ce produit scalaire. On a

$$V(\mathcal{C}^*) = \lambda_1 \dots \lambda_n V(\mathcal{C}).$$

Appelons u l'applications linéaire définie par $u(y_i) = \frac{1}{\lambda_i^2} y_i$. On a pour tout $x \in \mathbb{R}^n$ on a

$$(x|x)^* = (u(x)|x)$$

Si $x \in \text{vect}(x_1, \dots, x_k) = \text{vect}(y_1, \dots, y_k)$ on a $N^*(x) \geq \frac{1}{\lambda_k} N(x)$. Montrons que $\lambda_1(\Lambda, N^*) \geq 1$. Soit x un élément non nul de Λ . Comme $x_1, \dots, x_n$ sont libre il existe $a_1, \dots, a_n \in \mathbb{R}$ tels que $x = \sum a_i x_i$. Appelons k le plus grand entier tel que $a_k \neq 0$. D'après le lemme 2, x ne peut pas appartenir à $\mu \mathcal{C}$ avec $\mu < \lambda_k$ donc $N(x) \geq \lambda_k$. Donc $N^*(x) \geq \frac{1}{\lambda_k} N(x) \geq 1$. Or

$$\lambda_1(\Lambda, N^*) V(\mathcal{C}^*) \leq 2^n \det \Lambda$$

donc

$$1 \times \lambda_1 \dots \lambda_n V(\mathcal{C}) \leq 2^n \det \Lambda. \square$$

Pour achever la démonstration nous allons utiliser un résultat de Jordan :

Théorème 4 Soit N une norme quelconque sur $\mathbb{R}^n$ alors il existe une norme euclidienne N' tel que

$$B_{N'}(0, 1) \subset B_N(0, 1) \subset 2\sqrt{n} B_{N'}(0, 1)$$

(En fait Jordan montre l'inclusion plus forte $B_N(0, 1) \subset \sqrt{n} B_{N'}(0, 1)$).

Démonstration. Par un argument de compacité on montre qu'il existe une norme euclidienne N' telle que $B_{N'}(0, 1) \subset B_N(0, 1)$ et le volume de $B_{N'}(0, 1)$ soit maximal. Montrons que cette norme vérifie la deuxième inclusion. Il suffit de montrer que si $N'(z) > 2\sqrt{n}$ alors $N(z) > 1$. Prenons une base orthonormée $(e_1, \dots, e_n)$ pour la norme N' dont le premier vecteur est colinéaire à z : $e_1 = pz$. On a $p \geq 2\sqrt{n}$. Supposons que $N(x) \leq 1$ alors l'enveloppe convexe H de x , $-x$ et $B_{N'}(0, 1)$ est incluse dans $B_N(0, 1)$. On voit que H contient

$$K = \{\lambda e_1 + v : v \in e_1^\perp, \frac{1}{p} |\lambda| + N'(v) \leq 1\}$$

car K est l'enveloppe convexe de x , $-x$ et $B_{N'}(0, 1) \cap e_1^\perp$. Considérons la norme euclidienne $\|\cdot\|$ définie par

$$\left\| \sum x_i e_i \right\|^2 = \left(\frac{x_1}{a}\right)^2 + \left(\frac{x_2}{b}\right)^2 + \dots + \left(\frac{x_n}{b}\right)^2.$$

Soit $x = \lambda e_1 + v$ on a

$$\frac{1}{p} |\lambda| + N'(v) \leq \|\lambda e_1 + v\| = \sqrt{\frac{\lambda^2}{a^2} + \frac{N'(v)^2}{b^2}}$$

lorsque $b = \sqrt{1 - \frac{1}{n}}$ et $a = \frac{p}{\sqrt{n}}$. En effet

$$\begin{aligned} \frac{1}{p} |\lambda| + N'(v) \leq \|\lambda e_1 + v\| &= \sqrt{\frac{\lambda^2}{a^2} + \frac{N'(v)^2}{b^2}} \iff \\ \lambda^2 \left(\frac{1}{a^2} - \frac{1}{p^2}\right) + N'^2(v) \left(\frac{1}{b^2} - 1\right) - 2\frac{1}{p} |\lambda| N'(v) &\geq 0 \end{aligned}$$

et le discriminant Δ de cette forme quadratique un λ , $N'(v)$ vaut

$$\Delta = \left(\frac{1}{a^2} - \frac{1}{p^2}\right) \left(\frac{1}{b^2} - 1\right) - \frac{1}{p^2} = \frac{1}{b^2} \left(\frac{1}{a^2} - \frac{1}{p^2}\right) - \frac{1}{a^2} = \frac{1}{p^2} \left(\frac{1}{b^2} (n-1) - (n-1)\right) \geq 0$$

car $b \leq 1$. D'autre part, grâce a une affinité on voit que

$$V(\{\|x\| \leq 1\}) = ab^{n-1} V(B_{N'}(0, 1)) = \frac{p}{\sqrt{n}} \left(1 - \frac{1}{n}\right)^{(n-1)/2} V(B_{N'}(0, 1))$$

et par maximalité de $V(B_{N'}(0, 1))$ on a

$$\frac{p}{\sqrt{n}} \left(1 - \frac{1}{n}\right)^{(n-1)/2} \leq 1,$$

d'où

$$\left(1 - \frac{1}{n}\right)^{(n-1)/2} \leq \frac{1}{2}.$$

Or par convexité ($n \geq 3$)

$$\left(1 - \frac{1}{n}\right)^{(n-1)/2} \geq 1 - \frac{n-1}{2} \times \frac{1}{n} > \frac{1}{2}. \quad \square$$

Fin de la démonstration du théorème de Minkowski.

Il reste à prouver l'inégalité $\lambda_1 \dots \lambda_n V(B_N(0, 1)) \leq 4^n n^{n/2} \det \Lambda$ pour une norme qq. N . Considérons la norme euclidienne N' fournie par le théorème de Jordan, on a $N' \geq N$ et $V(B_N(0, 1)) \leq 2^n n^{n/2} V(B_{N'}(0, 1))$. Comme $N' \geq N$ on a

$$\lambda_i(N') \geq \lambda_i(N).$$

D'après le th. sur les normes euclidienne on a

$$\lambda_1(N') \dots \lambda_n(N') V(B_{N'}(0, 1)) \leq 2^n \det \Lambda$$

donc

$$\lambda_1(N) \dots \lambda_n(N) V(B_N(0, 1)) \leq 2^n \det \Lambda \times 2^n n^{n/2}. \square$$

3 Réseau réciproque

Munissons $\mathbb{R}^n$ du produit scalaire usuel $x.y$ et notons $\|\cdot\|$ la norme associée.

Proposition 3 *Soit Λ un réseau de $\mathbb{R}^n$. Alors*

$$\Lambda^* = \{x \in \mathbb{R}^n : x.y \in \mathbb{Z}; \forall y \in \Lambda\}$$

est un réseau de déterminant $\frac{1}{\det \Lambda}$. On a aussi $\Lambda^{**} = \Lambda$. Λ^* s'appelle le réseau réciproque ou le réseau dual.

Démonstration. Soit $e_1, \dots, e_n$ une base de Λ . Appelons $e_1^*, \dots, e_n^*$ la base dual i.e. la base tel $e_i.e_j^* = \delta_{i,j}$. On vérifie facilement que $\Lambda^* = \mathbb{Z}e_1^* + \dots + \mathbb{Z}e_n^*$. Appelons A (resp A^*) la matrice dont les vecteurs colonne sont les coordonnées des e_i (resp e_i^*) dans la base canonique. On a par définition ${}^tAA^* = Id$ d'où $A^* = {}^tA^{-1}$ et $\det A^* = 1/\det A$. On en déduit que la matrice de Λ^{**} est A . $\square$

Théorème 5 (Malher 1939) *Soit Λ un réseau de $\mathbb{R}^n$. Appelons λ_i les minima de Λ et λ_i^* les minima de Λ^* . Alors pour tout $i \in \{1, \dots, n\}$,*

$$\frac{1}{C_n} \lambda_i^* \leq \frac{1}{\lambda_{n+1-i}} \leq C_n \lambda_i^*$$

où C_n est constante qui ne dépend que de la dimension.

Démonstration. Soit $x_1, \dots, x_n$ des vecteurs linéairement indépendants de Λ tels que $\|x_i\| \leq \lambda_i$. Appelons $x_1^*, \dots, x_n^*$ la base duale de $x_1, \dots, x_n$, $x_i.x_j^* = 1$. Si on appelle X la matrice dont les colonnes sont les x_i et X^* la matrice dont les colonnes sont les x_i^* alors ${}^tXX^* = Id$. Pour chaque j ${}^tXx_j^* = e_j$ et $x_j^* = {}^tX^{-1}e_j$. Appelons $X_{i,j}$ le cofacteur d'indice ij de la matrice X , on a

$$x_j^* = \frac{1}{\det X} (X_{1j}, X_{2j}, \dots, X_{nj}) = \frac{1}{\det X} \sum_i X_{ij} e_i.$$

D'après l'inégalité de Hadamard pour chaque i on a

$$|X_{ij}| \leq \prod_{k \neq j}^n \|x_k\|,$$

donc

$$\|x_j^*\| \leq \frac{1}{|\det X|} \times \sqrt{n} \times \prod_{k \neq j} \|x_k\| \leq \frac{1}{|\det X|} \times \sqrt{n} \times \prod_{k \neq j} \lambda_k.$$

Montrons que les vecteurs $y_j^* = \frac{\det X}{\det \Lambda} x_j^* \in \Lambda^*$. Appelons A la matrice d'une base du réseau Λ . Il existe une matrice B à coefficients entiers telle que $X = AB$. La matrice $(\det B)B^{-1}$ est à coefficients entiers donc

$${}^t A (\det B) X^* = {}^t (X B^{-1}) (\det B) X^* = (\det B) {}^t B^{-1} {}^t X X^* = (\det B) {}^t B^{-1} \in M_n(\mathbb{Z}).$$

Donc les y_j^* appartiennent à Λ^* . On a

$$\|y_j^*\| \leq \sqrt{n} \times \frac{|\det B|}{|\det X|} \times \prod_{k \neq j} \lambda_k = \sqrt{n} \times \frac{1}{\det \Lambda} \times \prod_{i \neq j} \lambda_i.$$

Or d'après le th. des minima

$$\det \Lambda \geq c_n \prod_{i=1}^n \lambda_i$$

donc

$$\|y_j^*\| \leq c_n \frac{1}{\lambda_j}$$

et comme les y_j^* sont indépendants on en déduit que $\lambda_j^* \leq c_n \frac{1}{\lambda_{n+1-j}}$. L'autre inégalité découle de la relation $\Lambda^{**} = \Lambda$. $\square$

Remarques. 1. Soit N une norme équivalente à la norme euclidienne avec une constante C . Alors le théorème précédent est vrai avec la constante $C^2 C_n$.

2. On ne peut pour une norme qq. trouver une inégalité ne faisant intervenir que le volume de la boule unité. En effet, considérons le réseau $\Lambda = \mathbb{Z} t e_1 \oplus \mathbb{Z} \frac{1}{t} e_2$ où (e_1, e_2) est la base canonique de $\mathbb{R}^2$ et $t \geq 1$. On a $\Lambda^* = \mathbb{Z} \frac{1}{t} e_1 \oplus \mathbb{Z} t e_2$. Soit $\langle \cdot, \cdot \rangle$ un produit scalaire tel que $t e_1, \frac{1}{t} e_2$ soient orthonormaux. Appelons N la norme associée. On a

$$\lambda_1(\Lambda, N) = \lambda_2(\Lambda, N) = 1, \quad \lambda_1(\Lambda^*, N) = \frac{1}{t}, \quad \lambda_2(\Lambda^*, N) = t \quad \text{et} \quad V(B_N(0, 1)) = 1.$$