Cours 1: Géométrie des nombres

On fixe un espace euclidien réel E de dimension finie $n \geq 1$ et on note par un point son produit scalaire. Ainsi la norme d'un élément $\mathbf{x}$ de E est donnée par

$$\|\mathbf{x}\| = (\mathbf{x} \cdot \mathbf{x})^{1/2}.$$

On fixe aussi une base orthonormée $\underline{\mathbf{e}} = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$ de E.

L'exemple le plus simple est $E = \mathbb{R}^n$ muni de son produit scalaire usuel. Mais E pourrait aussi être un sous-espace de $\mathbb{R}^m$ pour un entier $m \geq n$, avec le produit scalaire obtenu par restriction à E du produit scalaire standard de $\mathbb{R}^m$.

1. **Algèbre extérieure.** (Référence: [Bo1970])

On montre que, pour tout entier $k \geq 1$, il existe un espace vectoriel réel noté $\bigwedge^k E$ et une application multilinéaire alternée

$$\begin{array}{rccc} \varphi_k : & E^k & \longrightarrow & \bigwedge^k E \\ & (\mathbf{x}_1, \ldots, \mathbf{x}_k) & \longmapsto & \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \end{array} \tag{1.1}$$

avec la propriété universelle suivante. Pour tout espace vectoriel réel W et toute application multilinéaire alternée

$$\psi \colon E^k \to W,$$

il existe une et une seule application linéaire $T \colon \bigwedge^k E \to W$ telle que $\psi = T \circ \varphi_k$, c'est-à-dire telle que

$$\psi(\mathbf{x}_1, \ldots, \mathbf{x}_k) = T(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) \quad \text{pour tout } (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in E^k.$$

On dit que $\bigwedge^k E$ est la *puissance extérieure k-ième de E*. La propriété ci-dessus la caractérise seulement à isomorphisme près, mais en pratique cela ne pose pas de problème. Mieux, on en déduit sans trop de mal de nombreuses propriétés.

Par exemple, on montre sans peine que l'image de φ_k engendre $\bigwedge^k E$. Autrement dit, en tant qu'espace vectoriel, $\bigwedge^k E$ est engendré par les éléments de la forme $\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k$ avec $\mathbf{x}_1, \ldots, \mathbf{x}_k \in E$, qu'on appelle les *produits purs*. Par contre, les éléments de $\bigwedge^k E$ ne sont pas tous de cette forme si $2 \leq k \leq n-2$.

On montre aussi qu'il existe un et un seul produit scalaire sur $\bigwedge^k E$ tel que

$$(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) \cdot (\mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_k) = \det(\mathbf{x}_i \cdot \mathbf{y}_j) \tag{1.2}$$

pour tout choix de $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_1, \ldots, \mathbf{y}_k \in E$. De plus, pour ce produit scalaire, les vecteurs

$$\mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_k} \quad \text{avec} \quad 1 \leq i_1 < \cdots < i_k \leq n \tag{1.3}$$

forment une base orthonormée de $\bigwedge^k E$. Cela implique que

$$\dim \bigwedge^k E = \begin{cases} \binom{n}{k} & \text{si } k \leq n, \\ 0 & \text{si } k > n. \end{cases} \tag{1.4}$$

En particulier, $\bigwedge^n E$ est de dimension 1 engendré par le vecteur unitaire $\mathbf{e}_1 \wedge \cdots \wedge \mathbf{e}_n$. Alors le seul autre vecteur unitaire de $\bigwedge^n E$ est $-\mathbf{e}_1 \wedge \cdots \wedge \mathbf{e}_n$. Donc si $\underline{\mathbf{f}} = (\mathbf{f}_1, \ldots, \mathbf{f}_n)$ est une autre base othonormée de E, on a $\mathbf{f}_1 \wedge \cdots \wedge \mathbf{f}_n = \pm \mathbf{e}_1 \wedge \cdots \wedge \mathbf{e}_n$ pour un choix de signe $\pm$.

Pour $k = 1$, on fixe $\bigwedge^1 E = E$ (en prenant l'identité pour application linéaire $\varphi_1 \colon E \to E$).

On convient aussi que $\bigwedge^0 E = \mathbb{R}$. Alors la formule des dimensions (1.4) s'applique aussi pour $k = 0$ et la somme directe (externe)

$$\bigwedge E = \bigoplus_{k \geq 0} \bigwedge^k E$$

est un espace vectoriel sur $\mathbb{R}$ de dimension 2^n avec pour base l'ensemble des produits (1.3) avec $0 \leq k \leq n$. De plus, il existe une et une seule application bilinéaire

$$(\bigwedge E) \times (\bigwedge E) \to \bigwedge E$$

notée $\wedge$ telle que

$$\begin{aligned}(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) \wedge (\mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_\ell) &= \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \wedge \mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_\ell, \\ (\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) \wedge 1 &= (\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k), \\ 1 \wedge (\mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_\ell) &= \mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_\ell, \\ 1 \wedge 1 &= 1,\end{aligned}$$

quels que soient les entiers $k, \ell \geq 1$ et les vecteurs $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_1, \ldots, \mathbf{y}_\ell \in E$. Ici, 1 désigne l'unité de $\mathbb{R} = \bigwedge^0 E$. Cette forme bilinéaire munit $\bigwedge E$ d'une structure d'algèbre associative graduée avec unité 1, pour laquelle un produit pur $\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k$ est littéralement le produit des éléments $\mathbf{x}_1, \ldots, \mathbf{x}_k$ de $E = \bigwedge^1 E$, comme le suggère la notation.

Pour chaque entier $k \geq 0$, on dit que $\bigwedge^k E$ est la *partie homogène* de degré k de $\bigwedge E$. L'algèbre $\bigwedge E$ est graduée parce que si $X \in \bigwedge^k E$ et $Y \in \bigwedge^\ell E$ pour des entiers $k, \ell \geq 0$, alors $X \wedge Y \in \bigwedge^{k+\ell} E$.

Si $T \colon E \to E$ est un opérateur linéaire sur E, alors pour chaque $k = 1, \ldots, n$, il existe un et un seul opérateur linéaire $\bigwedge^k T \colon \bigwedge^k E \to \bigwedge^k E$ sur $\bigwedge^k E$ tel que

$$\bigwedge^k T(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) = T(\mathbf{x}_1) \wedge \cdots \wedge T(\mathbf{x}_k)$$

pour tout $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in E^k$. Il satisfait

$$\det(\bigwedge^k T) = \det(T)^K \quad \text{où} \quad K = \binom{n-1}{k-1}. \tag{1.5}$$

Ces n opérateurs s'étendent à un endomorphisme d'algèbre graduée $\bigwedge T \colon \bigwedge E \to \bigwedge E$ qui coïncide avec T sur $E = \bigwedge^1 E$.

Lemme 1.1. *Pour chaque $k = 0, \ldots, n$, il existe une et une seule isométrie*

$$\begin{array}{rcl} * \colon \bigwedge^k E & \longrightarrow & \bigwedge^{n-k} E \\ X & \longmapsto & X^* \end{array}$$

telle que $X \wedge Y^* = (X \cdot Y)\mathbf{e}_1 \wedge \cdots \wedge \mathbf{e}_n$ pour tout choix de $X, Y \in \bigwedge^k E$.

Comme le produit $\mathbf{e}_1 \wedge \cdots \wedge \mathbf{e}_n$ ne dépend que de E au produit près par ± 1, il en va de même de cette isométrie.

Par exemple, pour $k = 1$, on vérifie sans peine que l'application linéaire $* \colon E \to \bigwedge^{n-1} E$ qui envoie chaque $\mathbf{e}_i$ sur

$$\mathbf{e}_i^* = (-1)^{i-1} \mathbf{e}_1 \wedge \cdots \wedge \widehat{\mathbf{e}_i} \wedge \cdots \wedge \mathbf{e}_n \quad (1 \leq i \leq n)$$

est une isométrie avec la propriété requise et que c'est la seule. On laisse le cas général en exercice.

Lemme 1.2. *Soit* $\underline{\mathbf{v}} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ *une base de* E *et soit*

$$P = \{t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n \,;\, 0 \leq t_1, \dots, t_n \leq 1\}$$

le parallélépipède de E *engendré par* $\underline{\mathbf{v}}$*. Alors le volume de* P *est*

$$\mathrm{vol}(P) = \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| = \det(\mathbf{v}_i \cdot \mathbf{v}_j)^{1/2} \leq \|\mathbf{v}_1\| \cdots \|\mathbf{v}_n\|$$

avec l'égalité si et seulement si $\underline{\mathbf{v}}$ *est une base orthogonale de* E*.*

La relation $\|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| \leq \|\mathbf{v}_1\| \cdots \|\mathbf{v}_n\|$ est appelée l'inégalité d'Hadamard.

Démonstration. C'est clair si $n = 1$. Supposons maintenant $n \geq 2$ et que le résultat soit vrai en dimension $n-1$ pour le parallélépipède

$$Q = \{t_1\mathbf{v}_1 + \cdots + t_{n-1}\mathbf{v}_{n-1} \,;\, 0 \leq t_1, \dots, t_{n-1} \leq 1\}$$

de $W = \langle \mathbf{v}_1, \dots, \mathbf{v}_{n-1} \rangle_{\mathbb{R}}$ engendré par $(\mathbf{v}_1, \dots, \mathbf{v}_{n-1})$. Écrivons $\mathbf{v}_n = \mathbf{w} + \mathbf{v}$ avec $\mathbf{w} \in W$ et $\mathbf{v} \in W^{\perp}$. D'une part, on a

$$\mathrm{vol}(P) = \mathrm{vol}(Q)\|\mathbf{v}\|.$$

D'autre part, le produit extérieur étant multi-linéaire alterné, on a aussi

$$\|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| = \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_{n-1} \wedge \mathbf{v}\|.$$

D'après les formules (1.2) pour le produit scalaire, le membre de gauche de cette égalité est $\det(\mathbf{v}_i \cdot \mathbf{v}_j)^{1/2}$, et celui de droite est donné par la même formule avec $\mathbf{v}_n$ remplacé par $\mathbf{v}$. Comme $\mathbf{v} \cdot \mathbf{v}_j = \mathbf{v}_i \cdot \mathbf{v} = 0$ pour $i, j = 1, \dots, n-1$, on en déduit

$$\|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| = \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_{n-1}\| \, \|\mathbf{v}\| = \mathrm{vol}(Q)\|\mathbf{v}\| = \mathrm{vol}(P),$$

puis

$$\|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| \leq \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_{n-1}\| \, \|\mathbf{v}_n\| \leq \|\mathbf{v}_1\| \cdots \|\mathbf{v}_n\|$$

avec l'égalité partout si et seulement si $\mathbf{v}_n = \mathbf{v} \in W^{\perp}$ et que $(\mathbf{v}_1, \dots, \mathbf{v}_{n-1})$ est une base orthogonale de W, c'est-à-dire si et seulement si $\underline{\mathbf{v}}$ est une base orthogonale de E. □

Remarque 1.3. On sait qu'un opérateur linéaire T sur E multiplie les volumes par $|\det(T)|$. Comme le parallélépipède B de E engendré par $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ est de volume 1 et que le parallélépipède P du lemme 1.2 est son image sous l'opérateur linéaire T tel que $T(\mathbf{e}_i) = \mathbf{v}_i$ pour $i = 1, \dots, n$, on en déduit que

$$\mathrm{vol}(P) = |\det(T)|\mathrm{vol}(B) = |\det(\mathbf{e}_i \cdot \mathbf{v}_j)|.$$

Puisque la matrice $M = (\mathbf{e}_i \cdot \mathbf{v}_j)$ satisfait ${}^tMM = (\mathbf{v}_i \cdot \mathbf{v}_j)$, on retrouve la formule $\mathrm{vol}(P) = \det(\mathbf{v}_i \cdot \mathbf{v}_j)^{1/2}$.

Exemple 1.4. Supposons que $E = \mathbb{R}^n$ et soient $\mathbf{x} = (x_1, \dots, x_n),\ \mathbf{y} = (y_1, \dots, y_n) \in E$. En notant $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ la base canonique de E, on trouve

$$\mathbf{x} \wedge \mathbf{y} = \Big(\sum_{i=1}^{n} x_i\mathbf{e}_i\Big) \wedge \Big(\sum_{j=1}^{n} y_j\mathbf{e}_j\Big) = \sum_{1 \leq i,j \leq n} x_iy_j\mathbf{e}_i \wedge \mathbf{e}_j = \sum_{1 \leq i < j \leq n} \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} \mathbf{e}_i \wedge \mathbf{e}_j,$$

donc

$$\|\mathbf{x}\wedge\mathbf{y}\| = \Big(\sum_{1\le i<j\le n}\begin{vmatrix} x_i & x_j \\ y_i & y_j\end{vmatrix}^2\Big)^{1/2}.$$

Géométriquement, ce nombre représente l'aire du parallélogramme engendré par $\mathbf{x}$ et $\mathbf{y}$.

2. **Réseaux.** (Références: [GL1987], [Sc1980])

Un réseau de E est un sous-groupe discret de E de rang $n = \dim(E)$. De manière équivalente, c'est un sous-groupe

$$\Lambda = \langle \mathbf{v}_1,\dots,\mathbf{v}_n\rangle_{\mathbb{Z}} \tag{2.1}$$

engendré par une base $(\mathbf{v}_1,\dots,\mathbf{v}_n)$ de E. Alors, toute base de Λ sur $\mathbb{Z}$ est une base de E sur $\mathbb{R}$. Comme $P = \{t_1\mathbf{v}_1+\cdots+t_n\mathbf{v}_n\,;\,0\le t_1,\dots,t_n<1\}$ est un système de représentants de E/Λ, le *covolume* de Λ dans E est

$$\mathrm{covol}(\Lambda) = \mathrm{vol}(E/\Lambda) = \mathrm{vol}(P) = \|\mathbf{v}_1\wedge\cdots\wedge\mathbf{v}_n\|. \tag{2.2}$$

a) Le réseau de E *dual* à Λ est

$$\begin{aligned}\Lambda^* &= \{\mathbf{x}\in E\,;\,\mathbf{x}\cdot\mathbf{v}\in\mathbb{Z}\ \forall\mathbf{v}\in\Lambda\}\\ &= \langle\mathbf{v}_1^*,\dots,\mathbf{v}_n^*\rangle_{\mathbb{Z}}\end{aligned} \tag{2.3}$$

où $\underline{\mathbf{v}}^* = (\mathbf{v}_1^*,\dots,\mathbf{v}_n^*)$ est la base duale de E (avec $\mathbf{v}_i\cdot\mathbf{v}_j^* = \delta_{i,j}$). On a donc $(\Lambda^*)^* = \Lambda$ et

$$\mathrm{covol}(\Lambda^*) = \mathrm{covol}(\Lambda)^{-1}. \tag{2.4}$$

b) Pour chaque entier $k = 1,\dots,n$, on définit

$$\Lambda^{(k)} = \langle \mathbf{x}_1\wedge\cdots\wedge\mathbf{x}_k\,;\,\mathbf{x}_1,\dots,\mathbf{x}_k\in\Lambda\rangle_{\mathbb{Z}}. \tag{2.5}$$

C'est un réseau de $\bigwedge^k E$ qui admet pour base les produits $\mathbf{v}_{i_1}\wedge\cdots\wedge\mathbf{v}_{i_k}$ avec $1\le i_1<\cdots<i_k$. Son covolume est

$$\mathrm{covol}(\Lambda^{(k)}) = \mathrm{covol}(\Lambda)^K \quad\text{où}\quad K = \binom{n-1}{k-1}. \tag{2.6}$$

Soit $\mathcal{E}$ le réseau de E de base $\underline{\mathbf{e}}$. On note que $\Lambda = T(\mathcal{E})$ pour l'opérateur linéaire T de E qui applique $\mathbf{e}_i$ sur $\mathbf{v}_i$ pour $i = 1,\dots,n$. Comme le covolume de $\mathcal{E}$ est 1 et que $\Lambda^* = T^*(\mathcal{E})$ où $T^* = {}^tT^{-1}$, on en déduit la formule (2.4).

De même, comme $\mathcal{E}^{(k)}$ est engendré par une base orthonormée de $\bigwedge^k E$, son covolume dans $\bigwedge^k E$ est égal à 1. On note aussi que $\Lambda^{(k)} = \bigwedge^k T(\mathcal{E}^{(k)})$ pour le même opérateur linéaire T. Alors la formule (2.6) se déduit de (1.5).

Enfin, on retrouve essentiellement le dual de Λ en formant sa puissance extérieure $(n-1)$-ième comme le montre le lemme suivant.

Lemme 2.1. *Si $n\ge 2$, l'isométrie $*\colon \bigwedge^{n-1}E\to E$ envoie $\Lambda^{(n-1)}$ sur* $\mathrm{covol}(\Lambda)\Lambda^*$.

Démonstration. Il suffit de noter que

$$(\mathbf{v}_1\wedge\cdots\wedge\widehat{\mathbf{v}_m}\wedge\cdots\wedge\mathbf{v}_n)^* = (-1)^{n-m-1}\det(\mathbf{e}_i\cdot\mathbf{v}_j)\mathbf{v}_m^* \tag{2.7}$$

pour $m = 1,\dots,n$. □

Cette relation est cohérente avec les formules (2.4) et (2.6) car elle implique

$$\mathrm{covol}(\Lambda^{(n-1)}) \ = \mathrm{covol}(\Lambda)^n \mathrm{covol}(\Lambda^*) = \mathrm{covol}(\Lambda)^{n-1}.$$

Exemple 2.2. Si $E = \mathbb{R}^n$ et si $\Lambda = \mathbb{Z}^n$ est le réseau de $\mathbb{R}^n$ engendré par la base canonique $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$, alors $\Lambda^* = \mathbb{Z}^n$ et par suite $\mathrm{covol}(\Lambda) = \mathrm{covol}(\Lambda^*) = 1$. Par ailleurs, pour un entier k avec $1 \leq k \leq n$, on peut identifier $\bigwedge^k \mathbb{R}^n$ avec $\mathbb{R}^N$ où $N = \binom{n}{k}$ en identifiant chaque élément de $\bigwedge^k \mathbb{R}^n$ au N-uplet de ses coordonnées dans la base formée des produits (1.3) dans l'ordre lexicographique. Sous cette isométrie, $(\mathbb{Z}^n)^{(k)}$ s'identifie à $\mathbb{Z}^N$, de covolume 1 dans $\mathbb{R}^N$.

3. **Convexes symétriques.** (Références: [GL1987], [Sc1980])

Un *convexe symétrique* de E est un voisinage compact convexe $\mathcal{C}$ de 0 tel que $-\mathcal{C} = \mathcal{C}$.

On lui associe une norme $\| \ \|_{\mathcal{C}}$ sur E en posant

$$\|\mathbf{x}\|_{\mathcal{C}} = \min\{\lambda \geq 0 \, ; \, \mathbf{x} \in \lambda \mathcal{C}\}$$

pour tout $\mathbf{x} \in E$. De plus, $\mathcal{C}$ est la boule unité de E pour cette norme. Réciproquement, toute boule unité pour une norme de E est un convexe symétrique de E. Donc, de manière équivalente, on peut définir un convexe symétrique de E comme la boule unité pour une norme sur E.

Cette seconde définition a l'avantage de se transposer à tout espace vectoriel E de dimension finie sur un corps valué complet, comme $\mathbb{C}$, ou le corps $\mathbb{Q}_p$ des nombres p-adiques pour un nombre premier p, ou le corps des séries formelles $K((T))$ en une variable sur un corps K et les extensions algébriques finies de ces derniers.

L'ensemble des convexes symétriques de E est stable sous le groupe $\mathrm{GL}(V)$ des opérateurs linéaires inversibles de E.

Exemple 3.1. Le parallélépipède symétrique associé à une base $\underline{\mathbf{v}} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ de E est

$$\mathcal{P}_{\underline{\mathbf{v}}} = \big\{\mathbf{x} \in E \, ; \, |\mathbf{v}_i \cdot \mathbf{x}| \leq 1 \text{ pour } i = 1, \ldots, n\big\} = \Big\{ \sum_{i=1}^{n} t_i \mathbf{v}_i^* \, ; \, \max |t_i| \leq 1 \Big\}$$

avec $\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}}) = 2^n \|\mathbf{v}_1^* \wedge \cdots \wedge \mathbf{v}_n^*\| = 2^n \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\|^{-1}$.

Soit $\mathcal{B} = \{\mathbf{x} \in E \, ; \, \|\mathbf{x}\| = 1\}$ la boule unité de E pour la norme euclidienne. Un *ellipsoïde* E est l'image de cette boule sous un opérateur $T \in \mathrm{GL}(V)$. Pour une preuve du résultat suivant, voir [Sc1980, Theorem 2A].

Théorème 3.2 (Jordan)**.** *Pour tout convexe symétrique $\mathcal{C}$ de E, il existe $T \in \mathrm{GL}(V)$ tel que l'ellipsoïde $\mathcal{E} = T(\mathcal{B})$ satisfasse $\mathcal{E} \subseteq \mathcal{C} \subseteq \sqrt{n}\mathcal{E}$.*

Un résultat plus général de F. John de 1948 s'applique à tout compact convexe de E d'intérieur non vide.

Corollaire 3.3. *Pour tout convexe symétrique $\mathcal{C}$ de E, il existe une base $\underline{\mathbf{v}}$ de E telle que $\mathcal{P}_{\underline{\mathbf{v}}} \subseteq \mathcal{C} \subseteq n\mathcal{P}_{\underline{\mathbf{v}}}$.*

Démonstration. On note que $n^{-1/2}\mathcal{P}_{\underline{\mathbf{e}}} \subseteq \mathcal{B} \subseteq \mathcal{P}_{\underline{\mathbf{e}}}$. Alors, pour T comme dans le théorème de Jordan, on a $n^{-1/2}T(\mathcal{P}_{\underline{\mathbf{e}}}) \subseteq \mathcal{C} \subseteq n^{1/2}T(\mathcal{P}_{\underline{\mathbf{e}}})$. La conclusion suit car $n^{-1/2}T(\mathcal{P}_{\underline{\mathbf{e}}}) = \mathcal{P}_{\underline{\mathbf{v}}}$ pour une base $\underline{\mathbf{v}}$ de E. □

a) Le *convexe dual* de $\mathcal{C}$ est

$$\mathcal{C}^* = \{\mathbf{x} \in E\,;\, \mathbf{x}\cdot\mathbf{y} \leq 1 \ \forall \mathbf{y} \in \mathcal{C}\}. \tag{3.1}$$

Comme $\mathcal{C} = -\mathcal{C}$, on peut remplacer la condition $\mathbf{x}\cdot\mathbf{y} \leq 1$ par $|\mathbf{x}\cdot\mathbf{y}| \leq 1$ dans (3.1).

Exemple 3.4. Pour toute base $\underline{\mathbf{v}}$ de E, on trouve

$$\mathcal{P}^*_{\underline{\mathbf{v}}} = \Big\{ \sum_{i=1}^n t_i\mathbf{v}_i\,;\, \sum_{i=1}^n |t_i| \leq 1 \Big\} \quad\Longrightarrow\quad \frac{1}{n}\mathcal{P}_{\underline{\mathbf{v}}^*} \subseteq \mathcal{P}^*_{\underline{\mathbf{v}}} \subseteq \mathcal{P}_{\underline{\mathbf{v}}^*}$$

où $\underline{\mathbf{v}}^*$ désigne la base de E duale à $\underline{\mathbf{v}}$.

Cet exemple montre en particulier que

$$\mathcal{P}^*_{\underline{\mathbf{v}}} \asymp_n \mathcal{P}_{\underline{\mathbf{v}}^*}$$

où le symbole $\asymp_n$ signifie qu'il existe des constantes $c_1, c_2 > 0$ qui ne dépendent que de n telles que $\mathcal{P}^*_{\underline{\mathbf{v}}} \subseteq c_1\mathcal{P}_{\underline{\mathbf{v}}^*}$ et $\mathcal{P}^*_{\underline{\mathbf{v}}} \supseteq c_2\mathcal{P}_{\underline{\mathbf{v}}^*}$ (ici $c_1 = 1$ et $c_2 = 1/n$). Cette notation permet de simplifier l'écriture en faisant abstraction des valeurs des constantes. Dans le même esprit, on en déduit que

$$\mathrm{vol}(\mathcal{P}^*_{\underline{\mathbf{v}}}) \asymp_n \mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^*})$$

pour signifier cette fois qu'il existe des constantes $c_1', c_2' > 0$ qui ne dépendent que de n telles que $\mathrm{vol}(\mathcal{P}^*_{\underline{\mathbf{v}}}) \leq c_1'\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^*})$ et $\mathrm{vol}(\mathcal{P}^*_{\underline{\mathbf{v}}}) \leq c_2'\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^*})$ (par exemple $c_1' = c_1^n$ et $c_2' = c_2^n$).

Lemme 3.5. *On a* $\mathrm{vol}(\mathcal{C}^*) \asymp_n \mathrm{vol}(\mathcal{C})^{-1}$ *pour tout convexe symétrique* $\mathcal{C}$ *de* E.

Démonstration. Pour $\mathcal{C}$ et $\underline{\mathbf{v}}$ comme au corollaire 3.3, on a

$$\begin{aligned} \mathcal{C} \asymp_n \mathcal{P}_{\underline{\mathbf{v}}} \quad &\Longrightarrow \quad \mathcal{C}^* \asymp_n \mathcal{P}^*_{\underline{\mathbf{v}}} \asymp_n \mathcal{P}_{\underline{\mathbf{v}}^*} \\ &\Longrightarrow \quad \mathrm{vol}(\mathcal{C}^*) \asymp_n \mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^*}) = 4^n\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}})^{-1} \asymp_n \mathrm{vol}(\mathcal{C})^{-1}. \end{aligned}$$ □

On peut montrer que $\mathcal{C}$ est le dual de $\mathcal{C}^*$, c'est-à-dire que $(\mathcal{C}^*)^* = \mathcal{C}$ [GL, §14, Theorem 2].

b) Pour chaque entier $k = 1, \ldots, n$, on définit

$$\mathcal{C}^{(k)} = \text{enveloppe convexe des produits } \mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \text{ avec } \mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathcal{C}. \tag{3.2}$$

Pour un parallélépipède, on trouve l'estimation suivante.

Lemme 3.6. *Soit* k *un entier avec* $1 \leq k \leq n$ *et soit* $\underline{\mathbf{v}} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ *une base de* E. *On a*

$$N^{-1}\mathcal{P}_{\underline{\mathbf{v}}^{(k)}} \subseteq \mathcal{P}^{(k)}_{\underline{\mathbf{v}}} \subseteq k!\mathcal{P}_{\underline{\mathbf{v}}^{(k)}} \tag{3.3}$$

où $N = \binom{n}{k}$ *et où* $\underline{\mathbf{v}}^{(k)}$ *désigne la base de* $\bigwedge^k E$ *formée des produits* $\mathbf{v}_{i_1} \wedge \cdots \wedge \mathbf{v}_{i_k}$ *avec* $1 \leq i_1 < \cdots < i_k \leq n$.

Démonstration. Soit $X \in \mathcal{P}_{\underline{\mathbf{v}}^{(k)}}$. Il sécrit

$$X = \sum_{1 \le i_1 < \cdots < i_k \le n} a_{i_1,\ldots,i_k} \mathbf{v}_{i_1}^* \wedge \cdots \wedge \mathbf{v}_{i_k}^*$$

avec coefficients $|a_{i_1,\ldots,i_k}| = |(\mathbf{v}_{i_1} \wedge \cdots \wedge \mathbf{v}_{i_k}) \cdot X| \le 1$. Comme $\mathcal{P}_{\underline{\mathbf{v}}}$ contient les vecteurs $\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*$, le parallélépipède $\mathcal{P}_{\underline{\mathbf{v}}}^{(k)}$ contient tous les produits $\mathbf{v}_{i_1}^* \wedge \cdots \wedge \mathbf{v}_{i_k}^*$ et par suite il contient $N^{-1}X$. Cela démontre la première inclusion de (3.3).

Enfin, pour tout choix de vecteurs $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathcal{P}_{\underline{\mathbf{v}}}$ et d'entiers $1 \le i_1 < \cdots < i_k \le n$, on trouve $|(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k) \cdot (\mathbf{v}_{i_1} \wedge \cdots \wedge \mathbf{v}_{i_k})| \le k!$, donc $\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \in k! \mathcal{P}_{\underline{\mathbf{v}}^{(k)}}$. La seconde inclusion s'ensuit. □

Lemme 3.7. *Avec les notations du lemme précédant, on a*

$$\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^{(k)}}) = \mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}})^K \quad \textit{où} \quad K = \binom{n-1}{k-1}.$$

Démonstration. Soit $T \colon E \to E$ l'opérateur linéaire qui applique $\mathbf{e}_i$ sur $\mathbf{v}_i$ pour chaque $i = 1, \ldots, n$. On trouve que $\mathcal{P}_{\underline{\mathbf{v}}} = T^*(\mathcal{P}_{\underline{\mathbf{e}}})$ et que $\mathcal{P}_{\underline{\mathbf{v}}^{(k)}} = (\bigwedge^k T^*)(\mathcal{P}_{\underline{\mathbf{e}}^{(k)}})$, donc $\mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}^{(k)}}) = \det(\bigwedge^k T^*) = \det(T^*)^K = \mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}})^K$. □

On en déduit l'estimation générale suivante en procédant comme pour le Lemme 3.5.

Lemme 3.8. *Pour tout $k = 1, \ldots, n$, on a*

$$\mathrm{vol}(\mathcal{C}^{(k)}) \asymp_n \mathrm{vol}(\mathcal{C})^K \quad \textit{où} \quad K = \binom{n-1}{k-1}.$$

Enfin, pour $n \ge 2$, on a l'analogue suivant du lemme 2.1 en termes de convexes symétriques au lieu de réseaux.

Lemme 3.9. *Si $n \ge 2$, l'isométrie $* \colon \bigwedge^{n-1} E \to E$ applique $\mathcal{C}^{(n-1)}$ sur un convexe symétrique $\mathcal{K}$ de E avec $\mathcal{K} \asymp_n \mathrm{vol}(\mathcal{C})\mathcal{C}^*$.*

Démonstration. Le corollaire 3.3 fournit une base $\underline{\mathbf{v}} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ de E pour laquelle on a $\mathcal{P}_{\underline{\mathbf{v}}} \subseteq \mathcal{C} \subseteq n\mathcal{P}_{\underline{\mathbf{v}}}$. Grâce au lemme 3.6, on obtient

$$\mathcal{C}^{(n-1)} \asymp_n (\mathcal{P}_{\underline{\mathbf{v}}})^{(n-1)} \asymp_n \mathcal{P}_{\underline{\mathbf{v}}^{(n-1)}}.$$

La formule (2.7) montre que l'isométrie $*$ envoie les n éléments de $\underline{\mathbf{v}}^{(n-1)}$ sur les n vecteurs

$$(\mathbf{v}_1 \wedge \cdots \wedge \widehat{\mathbf{v}_m} \wedge \cdots \wedge \mathbf{v}_n)^* = \pm \|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\| \mathbf{v}_m^* \quad (1 \le m \le n)$$

pour un choix de signes $\pm$. Donc elle envoie $\mathcal{P}_{\underline{\mathbf{v}}^{(n-1)}}$ sur

$$\|\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_n\|^{-1} \mathcal{P}_{\underline{\mathbf{v}}^*} = 2^{-n} \mathrm{vol}(\mathcal{P}_{\underline{\mathbf{v}}}) \mathcal{P}_{\underline{\mathbf{v}}^*} \asymp_n \mathrm{vol}(\mathcal{C})\mathcal{C}^*$$

grâce aux calculs des exemples 3.1 et 3.4, donc $\mathcal{K} \asymp_n \mathrm{vol}(\mathcal{C})\mathcal{C}^*$. □

4. **Minima successifs.** (Références: [GL1987], [Sc1980])

Soit Λ un réseau de E et soit $\mathcal{C}$ un convexe symétrique de E. Pour chaque $i = 1, \dots, n$, on définit

$$\lambda_i(\mathcal{C}, \Lambda) = \text{le plus petit } \lambda > 0 \text{ tel que } \lambda\mathcal{C} \text{ contienne au moins } i \text{ éléments linéairement indépendants de } \Lambda.$$

Ce minimum existe car $\mathcal{C}$ est compact et que Λ est discret. Les nombres

$$0 < \lambda_1(\mathcal{C}, \Lambda) \leq \cdots \leq \lambda_n(\mathcal{C}, \Lambda)$$

s'appellent les *minima successifs* de $\mathcal{C}$ par rapport à Λ (ou de Λ par rapport à $\mathcal{C}$, selon le point de vue).

Lemme 4.1. *Avec les notations ci-dessus, il existe des éléments linéairement indépendants* $\mathbf{x}_1, \dots, \mathbf{x}_n$ *de* Λ *tels que*

$$\mathbf{x}_i \in \lambda_i(\mathcal{C}, \Lambda)\mathcal{C} \tag{4.1}$$

pour $i = 1, \dots, n$.

On dit que de tels vecteurs *réalisent* les minima de $\mathcal{C}$ par rapport à Λ.

Démonstration. Par définition, il existe un vecteur non nul $\mathbf{x}_1$ de Λ qui satisfait la condition (4.1) pour $i = 1$. Supposons en général que, pour un entier m avec $1 \leq m < n$, on ait construit $\mathbf{x}_1, \dots, \mathbf{x}_m \in \Lambda$ linéairement indépendants qui satisfont (4.1) pour $i = 1, \dots, m$. Par définition, le produit $\lambda_{m+1}(\mathcal{C}, \Lambda)\mathcal{C}$ contient au moins $m+1$ éléments linéairement indépendants de Λ. Donc il en contient au moins un en dehors de $\langle \mathbf{x}_1, \dots, \mathbf{x}_m \rangle_{\mathbb{R}}$. En notant ce point $\mathbf{x}_{m+1}$, on a maintenant $\mathbf{x}_1, \dots, \mathbf{x}_{m+1} \in \Lambda$ linéairement indépendants qui satisfont (4.1) pour $i = 1, \dots, m+1$. En procédant ainsi de proche en proche, on construit une suite $\mathbf{x}_1, \dots, \mathbf{x}_n$ comme requis. □

Théorème 4.2 (Minkowski, 1907)**.** *Pour tout convexe symétrique* $\mathcal{C}$ *de* E *et tout réseau* Λ *de* E*, on a*

$$\frac{2^n}{n!}\mathrm{covol}(\Lambda) \leq \mathrm{vol}(\mathcal{C}) \prod_{i=1}^{n} \lambda_i(\mathcal{C}, \Lambda) \leq 2^n \mathrm{covol}(\Lambda).$$

En particulier dans le cas important où $E = \mathbb{R}^n$ et $\Lambda = \mathbb{Z}^n$, le théorème donne

$$\frac{2^n}{n!} \leq \mathrm{vol}(\mathcal{C}) \prod_{i=1}^{n} \lambda_i(\mathcal{C}) \leq 2^n.$$

où $\lambda_i(\mathcal{C}) = \lambda_i(\mathcal{C}, \mathbb{Z}^n)$ pour $i = 1, \dots, n$. Les deux inégalités sont optimales. Celle de droite est une égalité pour la boule unité $\mathcal{C} = [-1, 1]^n$ de $\mathbb{R}^n$ relativement à la norme du maximum. Celle de gauche le devient pour la boule unité de $\mathbb{R}^n$ pour la norme L_1, le convexe dual de $[-1, 1]^n$.

Dans [Sc1980], Schmidt donne une démonstration de cette inégalité sous la forme

$$\mathrm{vol}(\mathcal{C})\lambda_1(\mathcal{C}) \cdots \lambda_n(\mathcal{C}) \asymp_n 1$$

en utilisant le théorème 3.2 de Jordan pour se ramener au cas d'un ellipsoïde. Dans [GL1987], Gruber et Lekkerkerker en donnent une démonstration complète. Le cas général du théorème 4.2 s'en déduit aisément.

Le théorème de Minkowski permet d'étudier aussi bien des questions d'approximation homogène que des questions d'approximation inhomogène. Dans le premier cas, on utilise la conséquence suivante.

Corollaire 4.3. *Soient $\mathcal{C}$ un convexe symétrique de $\mathbb{R}^n$ de volume au moins 2^n. Alors $\mathcal{C}$ contient un point non nul de $\mathbb{Z}^n$.*

Démonstration. On a $\lambda_1(\mathcal{C})^n \leq \prod_{i=1}^{n} \lambda_i(\mathcal{C}) \leq \dfrac{2^n}{\mathrm{vol}(\mathcal{C})} \leq 1$, donc $\lambda_1(\mathbb{C}) \leq 1$. □

Pour l'approximation inhomogène, c'est le dernier minimum qui entre en jeu.

Corollaire 4.4. *Soient $\mathcal{C}$ et λ comme au théorème 4.2 et soit $\mathbf{y} \in E$. Il existe $\mathbf{x} \in \Lambda$ tel que $\mathbf{y} \in \mathbf{x} + (n/2)\lambda\mathcal{C}$ où $\lambda = \lambda_n(\mathcal{C}, \Lambda)$.*

Démonstration. Par définition de λ, le produit $\lambda\mathcal{C}$ contient n points linéairement indépendants $\mathbf{x}_1, \ldots, \mathbf{x}_n$ de Λ. On peut donc écrire

$$\mathbf{y} = t_1\mathbf{x}_1 + \cdots + t_n\mathbf{x}_n$$

pour des nombres réels $t_1, \ldots, t_n$. On choisit des entiers $a_1, \ldots, a_n$ tels que $|t_i - a_i| \leq 1/2$ pour $i = 1, \ldots, n$. Alors le point

$$\mathbf{x} = a_1\mathbf{x}_1 + \cdots + a_n\mathbf{x}_n \in \Lambda$$

satisfait

$$\mathbf{y} - \mathbf{x} = \sum_{i=1}^{n} (t_i - a_i)\mathbf{x}_i \in \frac{n}{2}\lambda\mathcal{C}.$$ □

Théorème 4.5 (Malher, 1939)**.** *Soient $\mathcal{C}$ un convexe symétrique de E et Λ un réseau de E. Alors, pour $i = 1, \ldots, n$, on a*

$$1 \leq \lambda_i(\mathcal{C}^*, \Lambda^*)\lambda_{n+1-i}(\mathcal{C}, \Lambda) \leq (n!)^2.$$

Pour la démonstration, voir [GL1987, §14, Theorem 5]. Pour une démonstration sous la forme non explicite

$$\lambda_i(\mathcal{C}^*, \Lambda^*) \asymp_n \lambda_{n+1-i}(\mathcal{C}, \Lambda)^{-1} \quad (1 \leq i \leq n),$$

voir [Sc1980, Chapter IV, Theorem 4A].

Théorème 4.6 (Malher, 1955)**.** *Soient $\mathcal{C}$ un convexe symétrique de E et Λ un réseau de E. Soit $k \in \{1, \ldots, n\}$, soit $N = \binom{n}{k}$, et soit $\mu_1^{(k)}, \ldots, \mu_N^{(k)}$ la suite des N produits*

$$\lambda_{i_1}(\mathcal{C}, \Lambda) \cdots \lambda_{i_k}(\mathcal{C}, \Lambda) \quad (1 \leq i_1 < \cdots < i_k \leq n)$$

listés en ordre croissant. Alors, on a

$$c(n)\mu_j^{(k)} \leq \lambda_j(\mathcal{C}^{(k)}, \Lambda^{(k)}) \leq \mu_j^{(k)} \quad (1 \leq j \leq N),$$

pour une constante $c(n) > 0$.

Démonstration. Posons

$$\begin{aligned} \lambda_i &:= \lambda_i(\mathcal{C}, \Lambda) \qquad (1 \le i \le n), \\ \lambda_j^{(k)} &:= \lambda_j(\mathcal{C}^{(k)}, \Lambda^{(k)}) \quad (1 \le j \le N), \end{aligned} \tag{4.2}$$

et choisissons des points linéairement indépendants $\mathbf{x}_1, \dots, \mathbf{x}_n$ de Λ tels que $\mathbf{x}_i \in \lambda_i \mathcal{C}$ pour $i = 1, \dots, n$. Pour tout choix d'entiers $1 \le i_1 < \cdots < i_k \le n$, on a

$$\mathbf{x}_{i_1} \wedge \cdots \wedge \mathbf{x}_{i_k} \in \Lambda^{(k)} \cap \lambda_{i_1} \cdots \lambda_{i_k} \mathcal{C}^{(k)}.$$

Comme les N produits $\mathbf{x}_{i_1} \wedge \cdots \wedge \mathbf{x}_{i_k}$ sont linéairement indépendants, on en déduit que $\lambda_j^{(k)} \le \mu_j^{(k)}$ pour $j = 1, \dots, N$, puis que

$$\prod_{j=1}^{N} \frac{\mu_j^{(k)}}{\lambda_j^{(k)}} \asymp_n \frac{\mathrm{vol}(\mathcal{C}^{(k)})}{\mathrm{covol}(\Lambda^{(k)})} \prod_{j=1}^{N} \mu_j^{(k)} \asymp_n \frac{\mathrm{vol}(\mathcal{C})^K}{\mathrm{covol}(\Lambda)^K} \Big(\prod_{i=1}^{n} \lambda_j \Big)^K \asymp_n 1 \quad \text{où} \quad K = \binom{n-1}{k-1}.$$

On conclut que $\lambda_j^{(k)} \asymp_n \mu_j^{(k)}$ pour $j = 1, \dots, N$. □

Avec les notations (4.2), le plus petit des produits $\lambda_{i_1} \cdots \lambda_{i_k}$ avec $1 \le i_1 < \cdots < i_k \le n$ est $\mu_1^{(k)} = \lambda_1 \cdots \lambda_k$. Si $k < n$, le suivant est $\mu_2^{(k)} = \lambda_1 \cdots \lambda_{k-1} \lambda_{k+1}$. Donc le théorème de Mahler admet la conséquence suivante.

Corollaire 4.7. *Avec les notations* (4.2)*, on a*

$$\lambda_1^{(k)} \asymp_n \mu_1^{(k)} = \lambda_1 \cdots \lambda_k. \tag{4.3}$$

Si $k < n$, on a aussi

$$\lambda_2^{(k)} \asymp_n \mu_2^{(k)} = \lambda_1 \cdots \lambda_{k-1} \lambda_{k+1}. \tag{4.4}$$

On en déduit le théorème 4.2 de Minkowski aux constantes près. En effet, en dimension $n = 1$, il est facile. On a même une égalité

$$\lambda_1^{(n)} \mathrm{vol}(\mathcal{C}^{(n)}) = 2\mathrm{covol}(\Lambda^{(n)}).$$

Or le lemme 3.8 donne $\mathrm{vol}(\mathcal{C}^{(n)}) \asymp_n \mathrm{vol}(\mathcal{C})$ et on obtient $\mathrm{covol}(\Lambda^{(n)}) = \mathrm{covol}(\lambda)$ grâce à la formule (2.6), donc

$$\lambda_1 \cdots \lambda_n \mathrm{vol}(\mathcal{C}) \asymp_n \lambda_1^{(n)} \mathrm{vol}(\mathcal{C}^{(n)}) \asymp_n \mathrm{covol}(\Lambda^{(n)}) = \mathrm{covol}(\Lambda).$$

Le théorème 4.6 de Mahler redonne aussi le théorème 4.5 sur les minima du convexe dual $\mathcal{C}^*$ si $n \ge 2$. En effet, avec les mêmes notations, il livre, pour $i \in \{1, \dots, n\}$ fixé,

$$\lambda_i^{(n-1)} \asymp_n \mu_i^{(n-1)} = \lambda_1 \cdots \widehat{\lambda_{n-i+1}} \cdots \lambda_n.$$

Par ailleurs, les lemmes 2.1 et 3.9 nous apprennent que l'isométrie $*\colon \bigwedge^{(n-1)} E \to E$ applique $\Lambda^{(n-1)}$ sur $\mathrm{covol}(\Lambda)\Lambda^*$ et $\mathcal{C}^{(n-1)}$ sur un convexe symétrique $\mathcal{K}$ de E avec $\mathcal{K} \asymp_n \mathrm{vol}(\mathcal{C})\mathcal{C}^*$. On en déduit que

$$\lambda_i^{(n-1)} = \lambda_i(\mathcal{K}, \mathrm{covol}(\Lambda)\Lambda^*) \asymp_n \frac{\mathrm{covol}(\Lambda)}{\mathrm{vol}(\mathcal{C})} \lambda_i(\mathcal{C}^*, \Lambda^*).$$

Grâce au théorème de Minkowski, on conclut que

$$\lambda_i(\mathcal{C}^*, \Lambda^*) \asymp_n \frac{\mathrm{vol}(\mathcal{C})}{\mathrm{covol}(\Lambda)} \lambda_1 \cdots \widehat{\lambda_{n-i+1}} \cdots \lambda_n \asymp_n \lambda_{n-i+1}(\mathcal{C}, \Lambda)^{-1}.$$

Enfin, on retient de la preuve du théorème 4.6 que si $\mathbf{x}_1, \ldots, \mathbf{x}_n$ sont des éléments linéairement indépendants de Λ qui réalisent les minima de $\mathcal{C}$ par rapport à Λ, alors, pour $k = 1, \ldots, n$, le produit $\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \in \Lambda^{(k)}$ satisfait

$$\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_k \in \mu_1^{(k)} \mathcal{C}^{(k)} \asymp_n \lambda_1^{(k)} \mathcal{C}^{(k)}.$$

Donc il réalise le premier minimum de $\mathcal{C}^{(k)}$ par rapport à $\Lambda^{(k)}$ à un facteur près, borné supérieurement et inférieurement par des constantes positives qui ne dépendent que de n. En particulier pour $k = n$, on obtient que

$$\|\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_n\| \asymp_n \mathrm{vol}(\lambda_1^{(n)} \mathcal{C}^{(n)}) \asymp_n \mathrm{covol}(\Lambda^{(n)}) = \mathrm{covol}(\Lambda).$$

Donc $\mathbf{x}_1, \ldots, \mathbf{x}_n$ engendrent un sous-groupe de Λ d'indice fini borné par une fonction de n. On peut montrer que cet indice est au plus $n!$ [GL1987, §9, équation (13)].

References

[Bo1970] N. Bourbaki, *Algèbre*, chapitre 3, Éditions C.C.L.S., 1970.

[GL1987] P. M. Gruber et C. G. Lekkerkerker, *Geometry of Numbers*, North Holland, 1987, Chapitre 2, pp. 39–125.

[Sc1980] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics, volume 785, Springer Verlag, 1980, Chapitre IV, pp. 80–113.