CHAPITRE I Géométrie des nombres

§1 Réseaux dans un espace normé

<u>Notation</u> : V espace vectoriel de dimension finie sur $\mathbb{R}$

$$n = \dim_{\mathbb{R}}(V)$$

$\mathrm{vol}(\cdot)$ une mesure de Haar sur V

$\|\cdot\|$ une norme sur V

<u>Définition</u> 1.1 On appelle réseau dans V tout sous-ensemble de V de la forme

$$\Lambda = \{ a_1 e_1 + \dots + a_n e_n \mid (a_1, \dots, a_n) \in \mathbb{Z}^n \}$$

où $(e_i)_{i=1}^n$ est une base de V sur $\mathbb{R}$

<u>Géométrie des nombres</u> : Compter le nombres de points de réseau dans un domaine de V.

<u>Lemme</u> 1.2 (Blichfeldt) Soit $A \subset V$ un sous-ensemble borélien. Soit $N_A : V \to \mathbb{N} \cup \{+\infty\}$ la fonction

$$N_A(x) = \#(\Lambda \cap (A+x))$$

où $A + x := \{ y + x \mid y \in A \}$.

Alors la fonction N_A est Λ-périodique, et

$$\sup_{x \in V} N_A(x) \geqslant \frac{\mathrm{vol}(A)}{\mathrm{vol}(V/\Lambda)} \tag{1.1}$$

le volume d'un domaine fondamental.

<u>Remarque</u> : le membre à droite de (1.1) ne dépend pas du choix de la mesure de Haar.

Preuve Pour tout $S \subset V$, soit $\mathbb{1}_S$ la fonction indicatrice de S

$$\mathbb{1}_S(x) = \begin{cases} 1, & \text{si } x \in S \\ 0, & \text{sinon.} \end{cases}$$

On a
$$N_A(x) = \sum_{e \in \Lambda} \mathbb{1}_{A+e}(-x).$$

Donc la fonction N_A est Λ-périodique. Il existe alors une unique fonction $\tilde{N}_A$ sur V/Λ telle que

$$N_A = \tilde{N}_A \circ \pi,$$ où $\pi : V \longrightarrow V/\Lambda$ est la projection.

En outre

$$\int_{V/\Lambda} \tilde{N}_A(-x)\, \mathrm{vol}(dx) = \sum_{e \in \Lambda} \int_{D} \mathbb{1}_{A+e}(x)\, \mathrm{vol}(dx)$$

un domaine fondamental

$$= \sum_{e \in \Lambda} \mathrm{vol}(A \cap (D - e)) = \mathrm{vol}(A).$$

On en déduit

$$\sup_{x \in V} N_A(x) = \sup_{x \in V/\Lambda} \tilde{N}_A(x) \geq \frac{\mathrm{vol}(A)}{\mathrm{vol}(V/\Lambda)}$$

#

Définition 1.3 Soit Δ un sous-ensemble de V

On dit que Δ est un corps convexe s'il est convexe et compact, et si $\Delta^\circ \neq \emptyset$

On dit que Δ est symétrique si $x \in \Delta \Rightarrow -x \in \Delta$

Exemple $B_r(V, \|\cdot\|) := \{x \in V \mid \|x\| \leq r\}$

Théorème 1.4 (1er théorème de Minkowski) Soit $\Delta \subset V$ un corps convexe symétrique. On a

$$\#(\Delta \cap \Lambda) \geqslant 2^{-n} \frac{\mathrm{vol}(\Delta)}{\mathrm{vol}(V/\Lambda)}.$$

Démonstration On applique le lemme 1.2 à $A = \frac{1}{2}\Delta$ pour obtenir l'existence d'un $x \in V$ tel que

$$N_A(x) = \#(\Lambda \cap (A+x)) \geqslant \frac{\mathrm{vol}(A)}{\mathrm{vol}(V/\Lambda)} = 2^{-n} \frac{\mathrm{vol}(\Delta)}{\mathrm{vol}(V/\Lambda)}.$$

Comme Δ est convexe et symétrique. Si e et e' sont deux éléments de $\Lambda \cap (A+x)$, on a $e' - e \in \Delta \cap \Lambda$

Donc $\#(\Delta \cap \Lambda) \geqslant \#(\Lambda \cap (A+x)) \geqslant 2^{-n} \dfrac{\mathrm{vol}(\Delta)}{\mathrm{vol}(V/\Lambda)}$.

§2 Minima successifs

Définition 1.5

Caractéristique d'Euler-Poincaré

$$\chi(\Lambda, \|\cdot\|) := \log \frac{\mathrm{vol}(B_1(V, \|\cdot\|))}{\mathrm{vol}(V/\Lambda)}$$

Minima successif (logarithmiques)

$$\lambda_i(\Lambda, \|\cdot\|) = -\log \inf \{ r > 0 \mid \mathrm{rg}(B_r(V, \|\cdot\|) \cap \Lambda) \geqslant i \}$$

Remarque $\lambda_1(\Lambda, \|\cdot\|) = -\log \min \{ \|e\| \mid e \in \Lambda \setminus \{0\} \}$

$$\lambda_1(\Lambda, \|\cdot\|) \geqslant \cdots \geqslant \lambda_n(\Lambda, \|\cdot\|)$$

noté comme $\lambda_{max}(\Lambda, \|\cdot\|)$ noté comme $\lambda_{min}(\Lambda, \|\cdot\|)$

Corollaire 1.6 $n\lambda_1(\Lambda, \|\cdot\|) \geq \chi(\Lambda, \|\cdot\|) - n\log(2)$.

Preuve On applique le théorème 1.4 à $\Delta = B_{r-\varepsilon}(V, \|\cdot\|)$ où $r = e^{-\lambda_1(\Lambda, \|\cdot\|)}$ puis tend ε vers $0+$ ⁂

Définition 1.7

Filtration par les minima

$$\forall\, t \in \mathbb{R},\quad \mathcal{F}^t(V) := \mathrm{Vect}_{\mathbb{R}}\left(\left\{ e \in \Lambda \;\middle|\; \|e\| \leq \exp(-t) \right\}\right)$$

C'est une filtration décroissante dont les points de saut sont des minima successifs :

$$-d\left(\mathrm{rg}\,(\mathcal{F}^t(V))\right) = \sum_{i=1}^{n} \delta_{\lambda_i(\Lambda, \|\cdot\|)}$$

où δ_x désigne la mesure de Dirac en x.

Point de vue d'analyse fonctionnelle :

$$\forall\, x \in V,\quad \text{Soit } \lambda_{\mathcal{F}}(x) := \sup\left\{ t \in \mathbb{R} \;\middle|\; x \in \mathcal{F}^t(V) \right\} \in \mathbb{R} \cup \{+\infty\}.$$

Alors $\|x\|_{\mathcal{F}} := \exp(-\lambda_{\mathcal{F}}(x))$ est une norme ultramétrique sur V, où on considère la valeur absolue triviale sur $\mathbb{R}$

Théorème 1.8 (2ème théorème de Minkowski)

$$n\log(2)-\log(n!) \leq \chi(\Lambda,\|\cdot\|)-\sum_{i=1}^{n}\lambda_i(\Lambda,\|\cdot\|) \leq n\log(2)$$

$S_\lambda(\Lambda,\|\cdot\|)$

Démonstration (1) Soit $(e_i)_{i=1}^n$ une famille de vecteurs dans Λ qui forme une base de V et telle que

$$r_i := \|e_i\| = \exp(-\lambda_i(\Lambda,\|\cdot\|)) \text{ et } B^\circ_{r_i}(V,\|\cdot\|)\cap\Lambda \subset \mathbb{Z}e_1+\dots+\mathbb{Z}e_{i-1}$$

Soit Δ l'enveloppe convexe de $\left\{\pm\frac{e_i}{\|e_i\|},\ i=1,\dots,n\right\}$

On a $\Delta\subset B_1(V,\|\cdot\|)$. De plus,

$$\left(\prod_{i=1}^n\|e_i\|\right)\cdot\mathrm{vol}(\Delta)=\frac{2^n}{n!}\mathrm{vol}(P),$$ où P est le parallélotope engendré par $e_1,\dots,e_n$.

Il existe un entier non-nul C tel que $\frac{\mathrm{vol}(P)}{\mathrm{vol}(V/\Lambda)}=C$

$C=|\det(\text{matrice de transition entre } (e_i)_{i=1}^n \text{ et une base de } \Lambda)|$

Donc $\mathrm{vol}(P)\geq\mathrm{vol}(V/\Lambda)$. On en déduit

$$\left(\prod_{i=1}^n\|e_i\|\right)\cdot\mathrm{vol}(B_1(V,\|\cdot\|))\geq\frac{2^n}{n!}\mathrm{vol}(V/\Lambda),$$

d'où $$\chi(\Lambda,\|\cdot\|)-\sum_{i=1}^n\lambda_i(\Lambda,\|\cdot\|)\geq n\log(2)-\log(n!)$$

(2) Pour tout $i\in\{1,\dots,n\}$, soit $\Lambda_i=\mathbb{Z}e_1+\dots+\mathbb{Z}e_i$ et on désigne par $\pi_i : V\longrightarrow V/\Lambda_i$ la projection.

Observation $V/\Lambda_{i-1}\longrightarrow V/\Lambda_i$ est injectif sur

$$\pi_{i-1}\left(B^\circ_{\frac{\|e_i\|}{2}}(V,\|\cdot\|)\right)$$

avec la notation $r_i = \|e_i\|$, on obtient

$$\mathrm{vol}\left(\pi_i\left(B^\circ_{\frac{r_i}{2}}(V, \|\cdot\|)\right)\right) = \mathrm{vol}\left(\pi_{i-1}\left(B^\circ_{\frac{r_i}{2}}(V, \|\cdot\|)\right)\right)$$

<u>Lemme</u> Soit C un sous-ensemble convexe symétrique de V

$$\forall\, t \geq 1 \qquad \mathrm{vol}(\pi_i(tC)) \geq t^{n-i}\,\mathrm{vol}(\pi_i(C))$$

<u>Preuve</u> Soit V_i l'espace vectoriel engendré par Λ_i.
Quitte à choisir un complémentaire W_i de V_i dans V, on identifie V/Λ_i à $(V_i/\Lambda_i) \times W_i$.
Pour tout $w \in W_i$, $H \subset V$, on note $H_w = H \cap (V_i \times \{w\})$
Similairement, pour $\tilde{H} \subset V/\Lambda_i$, on note $\tilde{H}_w = H \cap ((V_i/\Lambda_i) \times \{w\})$
D'après le théorème de Fubini, on a

$$\mathrm{vol}(\pi_i(tC)) = \int_{w \in W_i} \mathrm{vol}(\pi_i(tC)_w)\ \mathrm{vol}(dw)$$

Comme $\pi_i(tC)_w = \pi_i((tC)_w) = \pi_i(t\, C_{t^{-1}w})$

$= t\,\pi_i(C_{t^{-1}w})$, on a

$$\mathrm{vol}(\pi_i(tC)) = \int_{w \in W_i} \mathrm{vol}(t\,\pi_i(C_{t^{-1}w}))\ \mathrm{vol}(dw)$$

$$\geq \int_{w \in W_i} \mathrm{vol}(\pi_i(C_{t^{-1}w}))\ \mathrm{vol}(dw) = t^{n-i}\,\mathrm{vol}(\pi_i(C))$$

#

D'après le lemme, on obtient

$$\mathrm{vol}\left(\pi_i\left(B^\circ_{\frac{r_i}{2}}(V, \|\cdot\|)\right)\right) \geq \left(\frac{r_i}{r_{i-1}}\right)^{n-i+1} \mathrm{vol}\left(\pi_{i-1}\left(B^\circ_{\frac{r_{i-1}}{2}}(V, \|\cdot\|)\right)\right)$$

On en déduit

$$\mathrm{vol}(V/\Lambda) \geq \mathrm{vol}\left(\pi_n\left(B^\circ_{\frac{r_n}{2}}(V, \|\cdot\|)\right)\right) \geq \frac{r_n}{r_{n-1}} \cdot \left(\frac{r_{n-1}}{r_{n-2}}\right)^2 \cdots \left(\frac{r_2}{r_1}\right)^{n-1} r_1^{\,n}\ \mathrm{vol}\left(B^\circ_{\frac{1}{2}}(V, \|\cdot\|)\right)$$

$$= \frac{r_1 \cdots r_n}{2^n}\,\mathrm{vol}(B_1(V, \|\cdot\|))$$

, d'où le résultat.

§3 Points de réseau dans la boule unité

<u>Définition</u> 1.9
$$\widehat{h}^0(\Lambda, \|\cdot\|) := \log \#\left(B_1(V, \|\cdot\|) \cap \Lambda\right)$$
$$S_\lambda^+(\Lambda, \|\cdot\|) := \sum_{i=1}^{n} \max\left(\lambda_i(\Lambda, \|\cdot\|), 0\right)$$
$$\left(= -\int_0^{+\infty} t \, d(\mathrm{rg}(\mathcal{F}^t(V))) = \int_0^{+\infty} \mathrm{rg}(\mathcal{F}^t(V)) \, dt \right)$$

Analogue du deuxième théorème de Minkowski : Comparaison entre $\widehat{h}^0(\Lambda, \|\cdot\|)$ et $S_\lambda^+(\Lambda, \|\cdot\|)$

<u>Remarque</u> : Soit Λ' le groupe engendré par $B_1(V, \|\cdot\|) \cap \Lambda$.

Alors Λ' est un réseau dans $\mathcal{F}^0(V) =: V'$.

On a $\quad S_\lambda^+(\Lambda, \|\cdot\|) = S_\lambda(\Lambda', \|\cdot\|)$ norme induite sur V'

et $\quad \widehat{h}^0(\Lambda, \|\cdot\|) = \widehat{h}^0(\Lambda', \|\cdot\|)$

<u>Proposition</u> 1.10 $\quad \widehat{h}^0(\Lambda, \|\cdot\|) \geqslant S_\lambda^+(\Lambda, \|\cdot\|) - \log(n!)$

<u>Preuve</u> D'après le théorème 1.4, on a
$$\widehat{h}^0(\Lambda', \|\cdot\|) \geqslant -n' \log(2) + \chi(\Lambda', \|\cdot\|)$$
où $n' = \mathrm{rg}_{\mathbb{Z}}(\Lambda')$.

D'après le théorème 1.8, on a
$$\chi(\Lambda', \|\cdot\|) \geqslant S_\lambda(\Lambda', \|\cdot\|) + n' \log(2) - \log(n'!).$$

D'où
$$\widehat{h}^0(\Lambda, \|\cdot\|) \geqslant S_\lambda^+(\Lambda, \|\cdot\|) - \log(n'!)$$ ※

Lemme 1.11 Soit $\tilde{\Lambda}$ un réseau de V contenu dans Λ.

(1) $\log[\Lambda : \tilde{\Lambda}] = \chi(\tilde{\Lambda}, \|\cdot\|) - \chi(\Lambda, \|\cdot\|)$

(2) $\hat{h}^\circ(\Lambda, \|\cdot\|) \leq \hat{h}^\circ(\tilde{\Lambda}, \frac{1}{2}\|\cdot\|) + \log[\Lambda : \tilde{\Lambda}]$

Preuve (1) $[\Lambda : \tilde{\Lambda}] = \mathrm{vol}(V/\tilde{\Lambda}) / \mathrm{vol}(V/\Lambda)$

(2) On suppose que $x_0, \dots, x_m$ sont des éléments distincts de $\Lambda \cap B_1(V, \|\cdot\|)$ qui sont dans la même classe de $V/\tilde{\Lambda}$.
Alors $(x_i - x_0)_{i=0}^m$ sont des éléments distincts de

$$\tilde{\Lambda} \cap B_2(V, \|\cdot\|) = \tilde{\Lambda} \cap B_1(V, \tfrac{1}{2}\|\cdot\|).$$

#

Théorème 1.12 (Henk) $\hat{h}^\circ(\Lambda, \|\cdot\|) \leq S_\lambda^+(\Lambda, \|\cdot\|) + n \log(5)$.

Démonstration Pour $i \in \{1, \dots, n\}$, soit $r_i = \exp(-\lambda_i(\Lambda, \|\cdot\|))$.
Il existe une famille de vecteurs linéairement indépendents $(u_1, \dots, u_n)$ tels que $\|u_i\| = r_i = \min\{\|u\| \mid u \in \Lambda \setminus \mathbb{R}u_1 + \dots + \mathbb{R}u_{i-1}\}$
Soit $(e_i)_{i=1}^n$ une base de Λ tel que $u_i \in \mathbb{Z}e_1 + \dots + \mathbb{Z}e_i$

On a alors $\overset{\circ}{B}_{r_i}(V, \|\cdot\|) \cap \Lambda \subset \mathbb{Z}e_1 + \dots + \mathbb{Z}e_{i-1}$

Pour tout i, soit $a_i = 1 + \lfloor \frac{2}{r_i} \rfloor$.

On a $a_1 \geq \dots \geq a_n \geq 1$

Étape 1 Il existe des entiers strictement positifs $d_1, \dots, d_n$ tels que

$$d_{i+1} \mid d_i \quad \text{et} \quad a_i \leq d_i < 2a_i$$

Construction par récurrence : $d_n = a_n$

On suppose $d_n, \dots, d_{k+1}$ construits.

Si $d_{k+1} \geq a_k$, on prend $d_k = d_{k+1}$.

Si $d_{k+1} < a_k$ alors il existe des entiers m et r,

$0 \leq r < d_{k+1}$ tels que $a_k = m d_{k+1} + r$

On prend $d_k = a_k + d_{k+1} - r$.

<u>Étape 2</u> Soit $\tilde{\Lambda} = \mathbb{Z} d_1 e_1 + \dots + \mathbb{Z} d_n e_n$.

Alors on a $[\Lambda : \tilde{\Lambda}] = d_1 \cdots d_n \leq \prod_{i=1}^{n} (2a_i - 1)$

$$\leq \prod_{i=1}^{n} \left(1 + \frac{4}{r_i}\right) \leq 5^n \prod_{i=1}^{n} \max\left(1, \frac{1}{r_i}\right)$$

En outre, on a $B_2(V, \|\cdot\|) \cap \tilde{\Lambda} = \{0\}$.

Sinon il existe $x = b_1 d_1 e_1 + \dots + b_k d_k e_k \in B_2(V, \|\cdot\|) \cap \tilde{\Lambda}$

avec $b_k \neq 0$. Alors $\frac{1}{d_k} x \in \Lambda$ et

$$\left\| \frac{x}{d_k} \right\| = \frac{1}{d_k} \|x\| \leq \frac{2}{d_k} \leq \frac{2}{a_k} < r_k$$

<u>Conclusion</u> : $\hat{h}^0(\tilde{\Lambda}, \frac{1}{2}\|\cdot\|) = 0$. Donc, par le lemme

$$\hat{h}^0(\Lambda, \|\cdot\|) \leq S_\lambda^+(\Lambda, \|\cdot\|) + n \log(5)$$

Références

[1] Blichfeldt, H.F., A new principle in the geometry of numbers, with some application, Trans. Amer. Math. Soc. 15, 227-235, 1914.

[2] Bombieri E., Vaaler J. On siegel's lemma, Invent. Math. 73, no.1, 11-32, 1983.

[3] Henk, M. Successive minima and lattice points, Rend. Circ. Mat. Palermo (2) Suppl. No. 70, part I (2002), 377-384
arXiv: 0204158v1