Séminaire BOURBAKI Octobre 2018
71e année, 2018–2019, no 1152

RÉSEAUX EUCLIDIENS, SÉRIES THÊTA ET PENTES
[d'après W. Banaszczyk, O. Regev, S. Dadush, N. Stephens-Davidowitz,...]

par **Jean-Benoît Bost**

Table des matières

1. INTRODUCTION

1.1. Réseaux euclidiens

Soit V un $\mathbb{R}$-vectoriel de dimension finie n. Un *réseau* Λ de V est un sous-groupe discret de V tel que le groupe topologique quotient V/Λ soit compact, ou de façon équivalente, tel qu'il existe une base $(e_i)_{1\leqslant i\leqslant n}$ de V telle que $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}e_i$. Le $\mathbb{R}$-vectoriel V s'identifie alors à $\Lambda_{\mathbb{R}} := \Lambda \otimes \mathbb{R}$.

Un *réseau euclidien* est la donnée $(V, \Lambda, \|.\|)$ d'un $\mathbb{R}$-vectoriel de dimension finie V, d'une structure euclidienne sur V de norme associée $\|.\|$, et d'un réseau Λ dans V.

De manière équivalente, un réseau euclidien est la donnée

$$\overline{E} := (E, \|.\|)$$

d'un $\mathbb{Z}$-module libre de rang fini E et d'une norme euclidienne $\|.\|$ sur le $\mathbb{R}$-vectoriel $E_{\mathbb{R}} := E \otimes \mathbb{R}$. (On identifiera E à son image par l'injection $(E \hookrightarrow E_{\mathbb{R}}, v \longmapsto v \otimes 1)$, qui constitue un réseau dans $E_{\mathbb{R}}$.)

Les réseaux euclidiens de dimension 3 constituent un modèle mathématique pour la configuration des atomes ou des molécules dans un solide cristallin, et ont été considérés pour cette raison depuis le dix-septième siècle (notamment par Huyghens dans son

Traité de la lumière, publié en 1690). À partir de la fin du dix-huitième siècle, le développement de la théorie des nombres a conduit à étudier les réseaux euclidiens dans une perspective « mathématique pure » : Lagrange, dans ses travaux sur les formes quadratiques entières à deux variables, considère les réseaux euclidiens de dimension 2 et leurs propriétés de « réduction » ; l'étude des formes quadratiques entières en un nombre de variables arbitraires et des corps de nombres de degré quelconque conduisent, notamment Gauss puis Hermite, à s'intéresser aux propriétés des réseaux euclidiens de rang 3 puis de rang quelconque.

À la fin du dix-neuvième siècle, l'étude des réseaux euclidiens est devenu un domaine mathématique à part entière, avec des contributions majeures de Korkin, Zolotarev, Minkowski (qui introduisit la terminologie de « géométrie des nombres »), puis Voronoi. Pour une présentation des résultats classiques de ce domaine, nous renvoyons aux ouvrages et articles d'exposition [Cas71], [RB79], [Lag95], et [Mar03].

1.2. Les invariants classiques des réseaux euclidiens

On dispose d'une notion évidente d'*isomorphisme* entre réseaux euclidiens : un isomorphisme entre deux réseaux euclidiens $\overline{E}_1 := (E_1, \|.\|_1$ et $\overline{E}_2 := (E_2, \|.\|_2)$ est un isomorphisme $\varphi : E_1 \xrightarrow{\sim} E_2$ de $\mathbb{Z}$-modules tels que l'isomorphisme de $\mathbb{R}$-vectoriels qui s'en déduit $\varphi_{\mathbb{R}} : E_{1,\mathbb{R}} \xrightarrow{\sim} E_{2,\mathbb{R}}$ soit une isométrie entre les $\mathbb{R}$-vectoriels euclidiens $(E_{1,\mathbb{R}}, \|.\|_1)$ et $(E_{2,\mathbb{R}}, \|.\|_2)$.

On attache classiquement à un réseau euclidien $\overline{E} := (E, \|.\|)$ des invariants ne dépendant que de sa classe d'isomorphisme :

- son *rang* :
$$\operatorname{rk} E = \dim_{\mathbb{R}} E_{\mathbb{R}} \in \mathbb{N};$$
- son *covolume* : si $m_{\overline{E}}$ désigne la mesure de Lebesgue[(1)] sur l'espace vectoriel euclidien $(E_{\mathbb{R}}, \|.\|)$ et si Δ est un domaine fondamental[(2)] pour l'action par translation de E sur $E_{\mathbb{R}}$, le covolume de $\overline{E}$ est défini comme
$$\operatorname{covol}(\overline{E}) := m_{\overline{E}}(\Delta) \in \mathbb{R}_+^*.$$
On observera que, si $\operatorname{rk} E = 0$, alors $\operatorname{covol}(\overline{E}) = 1$.
- son *premier minimum*, lorsque $\operatorname{rk} E > 0$:
$$\lambda_1(\overline{E}) := \min_{e \in E \setminus \{0\}} \|e\| \in \mathbb{R}_+^*.$$

(1) Elle est définie comme l'unique mesure borélienne invariante par translation sur $E_{\mathbb{R}}$ telle que, pour toute base orthonormée $(v_i)_{1 \leqslant i \leqslant n}$ de l'espace euclidien $(E_{\mathbb{R}}, \|.\|)$, on ait : $m_{\overline{E}}(\sum_{i=1}^n [0,1[v_i) = 1$. Une condition de normalisation équivalente est la suivante : $\int_{E_{\mathbb{R}}} e^{-\pi \|x\|^2} \, dm_{\overline{E}}(x) = 1$.

(2) C'est-à-dire une partie borélienne de $E_{\mathbb{R}}$ telle que $(\Delta + e)_{e \in E}$ soit une partition de $E_{\mathbb{R}}$. On vérifie aisément qu'il existe un tel domaine fondamental et que la mesure $m_{\overline{E}}(\Delta)$ est indépendante du choix de Δ.

Plus généralement, on introduit les *minima successifs* $(\lambda_i(\overline{E}))_{1\leqslant i\leqslant \operatorname{rk} E}$ de $\overline{E}$ définis par :

$$\lambda_i(\overline{E}) := \min\left\{r \in \mathbb{R}_+ \mid E \cap \overline{B}_{\|.\|}(0,r) \text{ contient une famille libre à } i \text{ éléments}\right\},$$

où $\overline{B}_{\|.\|}(0,r)$ désigne la boule fermée de centre 0 et rayon r dans l'espace vectoriel euclidien $(E_{\mathbb{R}}, \|.\|)$.

– son *rayon de recouvrement*[(3)], lorsque $\operatorname{rk} E > 0$:

$$R_{\mathrm{cov}}(\overline{E}) := \max_{x\in E_{\mathbb{R}}} \min_{e\in E} \|x-e\| = \min\{r \in \mathbb{R}_+ \mid E + \overline{B}_{\|.\|}(0,r) = E_{\mathbb{R}}\}.$$

De nombreux résultats de la théorie des réseaux euclidiens prennent la forme d'inégalités reliant ces divers invariants.

Par exemple, un résultat classique, qui remonte à Hermite et joue un rôle central en théorie algébrique des nombres, est la majoration suivante du premier minimum d'un réseau euclidien en fonction de son covolume :

Théorème 1.1 (Hermite, Minkowski). — *Pour tout entier $n > 0$, il existe $C(n)$ dans $\mathbb{R}_+^*$ tel que, pour tout réseau euclidien $\overline{E}$ de rang n,*

$$\lambda_1(\overline{E}) \leqslant C(n)(\operatorname{covol}(\overline{E}))^{1/n}. \tag{1.1}$$

Si v_n désigne la mesure de Lebesgue de la boule unité dans $\mathbb{R}^n$, on peut prendre :

$$C(n) = 2v_n^{-1/n}. \tag{1.2}$$

Comme $v_n = \pi^{n/2}/\Gamma(n/2+1)$, on déduit de la formule de Stirling que, lorsque n tend vers l'infini,

$$C(n) \sim \sqrt{2n/e\pi}. \tag{1.3}$$

Hermite a établi ce théorème par récurrence sur le rang n, en initiant ce que l'on appelle aujourd'hui la *théorie de la réduction*, dont nous rappelons les rudiments dans la section 2. Sa méthode lui permettait d'établir la majoration (1.1) avec

$$C(n) = (4/3)^{(n-1)/2}.$$

(voir paragraphe 2.4, *infra*).

Minkowski a donné dans sa *Geometrie der Zahlen* ([Min96], p. 73-76) une preuve élégante de l'inégalité de Hermite (1.1), preuve qui conduit à la valeur (1.2) pour $C(n)$ et admet une interprétation physique simple. Pensons au réseau euclidien $\overline{E} := (E, \|.\|)$ comme modélisant un cristal situé dans l'espace euclidien $(E_{\mathbb{R}}, \|.\|)$ de dimension n, dont les molécules sont représentées par les points du réseau E. Comme les boules ouvertes $\mathring{B}_{\|.\|}(v, \lambda_1(\overline{E})/2)$ de rayon $\lambda_1(\overline{E})/2$ centrées en ces points sont deux à deux disjointes, la

(3) En anglais *covering radius*. Celui-ci est noté $\mu(\overline{E})$ dans les articles de Banaszczyk et de Regev et ses collaborateurs qui font l'objet de cet exposé. Nous le notons $R_{\mathrm{cov}}(\overline{E})$, en nous inspirant de [CS99], pour éviter la confusion avec les diverses pentes $\widehat{\mu}(\overline{E})$, $\widehat{\mu}_i(\overline{E})$, $\widehat{\mu}_{KL}(\overline{E})$ associées à $\overline{E}$.

densité du cristal — définie comme le nombre de ses molécules par unité de volume — est au plus l'inverse du volume de ces boules, lequel vaut

$$v_n(\lambda_1(\overline{E})/2)^n.$$

Or cette densité n'est autre que l'inverse du covolume de $\overline{E}$. Il vient donc :

$$\mathrm{covol}(\overline{E})^{-1} \leqslant [v_n(\lambda_1(\overline{E})/2)^n]^{-1}.$$

Cette inégalité est précisément (1.1) avec $C(n)$ donnée par (1.2).

De même, en observant que la boule $\overline{B}_{\|.\|}(0, R_{\mathrm{cov}}(\overline{E}))$ contient un domaine fondamental pour l'action de E sur $E_{\mathbb{R}}$, on obtient que

$$v_n R_{\mathrm{cov}}(\overline{E})^n \geqslant \mathrm{covol}(\overline{E}),$$

ou encore :

$$R_{\mathrm{cov}}(\overline{E}) \geqslant v_n^{-1/n}\ \mathrm{covol}(\overline{E})^{1/n}. \tag{1.4}$$

Le carré $\gamma_n = C(n)^2$ de la meilleure constante dans l'inégalité d'Hermite (1.1) est classiquement appelée *constante d'Hermite*. Sa valeur exacte n'est connue que pour de petites valeurs de n (voir [CS99], [CK09]). Toutefois Minkowski a montré que l'estimation asymptotique $\gamma_n = O(n)$, conséquence de (1.3), est essentiellement optimale — à savoir, lorsque n tend vers l'infini, on a :

$$\log \gamma_n = \log n + O(1).$$

Par comparaison, l'argument de « théorie de la réduction » d'Hermite prouvait seulement la majoration :

$$\log \gamma_n \leqslant (n-1)\log(4/3).$$

Cette discussion illustre un thème central de la théorie des réseaux euclidiens, depuis Hermite et ses successeurs Korkin et Zolotarev : l'investigation des « meilleures constantes » figurant dans les inégalités comparant les invariants des réseaux, et notamment la détermination de leur comportement asymptotique lorsque ce rang tend vers l'infini.

Les travaux discutés dans cet exposé apportent des progrès spectaculaires sur ce type de question.

1.3. Quelques rappels

Avant d'énoncer les résultats de ces travaux, nous devons procéder à quelques rappels concernant les réseaux euclidiens.

1.3.1. *Suites exactes et dualité.* — Soit $\overline{E} := (E, \|.\|)$ un réseau euclidien.

Pour tout sous-$\mathbb{Z}$-module F de E, l'inclusion $F \hookrightarrow E$ détermine, par extension des scalaires, une injection canonique $F_{\mathbb{R}} \hookrightarrow E_{\mathbb{R}}$. Muni de la restriction à $F_{\mathbb{R}}$ de $\|.\|$, F (qui est encore un $\mathbb{Z}$-module libre de rang fini) définit un réseau euclidien :

$$\overline{F} := (F, \|.\|_{|F_{\mathbb{R}}}).$$

Si de plus F est *saturé* dans E — c'est-à-dire si le $\mathbb{Z}$-module E/F est sans torsion, ou de façon équivalente, si $F = F_{\mathbb{R}} \cap E$ — alors E/F est un $\mathbb{Z}$-module libre de rang fini. En outre, la suite exacte

$$0 \longrightarrow F \xrightarrow{i} E \xrightarrow{p} E/F \longrightarrow 0$$

(où i et p désignent le morphisme d'inclusion et le morphisme quotient) devient, par extension des scalaires, une suite exacte de $\mathbb{R}$-vectoriels :

$$0 \longrightarrow F_{\mathbb{R}} \xrightarrow{i_{\mathbb{R}}} E_{\mathbb{R}} \xrightarrow{p_{\mathbb{R}}} (E/F)_{\mathbb{R}} \longrightarrow 0.$$

Ainsi le $\mathbb{R}$-vectoriel $(E/F)_{\mathbb{R}}$ s'identifie-t-il au quotient de $E_{\mathbb{R}}$ par $F_{\mathbb{R}}$. En particulier, on peut le munir de la norme euclidienne quotient $\|.\|_{\mathrm{quot}}$ déduite de la norme euclidienne $\|.\|$ sur $E_{\mathbb{R}}$. On définit ainsi un réseau euclidien

$$\overline{E/F} := (E/F, \|.\|_{\mathrm{quot}}).$$

On résumera souvent cette construction en disant que le diagramme

$$0 \longrightarrow \overline{F} \xrightarrow{i} \overline{E} \xrightarrow{p} \overline{E/F} \longrightarrow 0 \tag{1.5}$$

est une *suite exacte courte admissible* de réseaux euclidiens.

Un sous-$\mathbb{Z}$-module saturé F de E est déterminé par le sous-$\mathbb{R}$-vectoriel $F_{\mathbb{R}}$ de $E_{\mathbb{R}}$, et aussi par le sous-$\mathbb{Q}$-vectoriel $F_{\mathbb{Q}} := F \otimes \mathbb{Q}$ de $E_{\mathbb{Q}} := E \otimes \mathbb{Q}$, puisque $F = F_{\mathbb{R}} \cap E = F_{\mathbb{Q}} \cap E$. L'application $(F \mapsto F_{\mathbb{Q}})$ établit en fait une bijection entre sous-$\mathbb{Z}$-modules saturés de E et sous-$\mathbb{Q}$-vectoriels de $E_{\mathbb{Q}}$. Si F est un sous-$\mathbb{Z}$-module (non nécessairement saturé) de E, on pose :

$$F^{\mathrm{sat}} := F_{\mathbb{Q}} \cap E.$$

C'est le sous-module saturé de E associé à $F_{\mathbb{Q}}$ par la bijection précédente. On a $F \subset F^{\mathrm{sat}}$ et F^{sat}/F est fini.

Par ailleurs, à tout réseau euclidien $\overline{E} := (E, \|.\|)$ est attaché son *réseau euclidien dual*

$$\overline{E}^{\vee} := (E^{\vee}, \|.\|^{\vee})$$

défini comme suit.

Son $\mathbb{Z}$-module sous-jacent $E^{\vee}$ est le $\mathbb{Z}$-module dual

$$E^{\vee} := \mathrm{Hom}_{\mathbb{Z}}(E, \mathbb{Z}),$$

qui est un $\mathbb{Z}$-module libre de même rang que E. Le $\mathbb{R}$-vectoriel $(E^{\vee})_{\mathbb{R}} := E^{\vee} \otimes \mathbb{R}$ s'identifie canoniquement à $(E_{\mathbb{R}})^{\vee} := \mathrm{Hom}_{\mathbb{R}}(E_{\mathbb{R}}, \mathbb{R})$; on le notera $E^{\vee}_{\mathbb{R}}$. On définit la norme euclidienne $\|.\|^{\vee}$ comme la norme duale de la norme $\|.\|$ sur $E_{\mathbb{R}}$. Ainsi, pour tout $\xi \in E^{\vee}_{\mathbb{R}}$, $\|\xi\|^{\vee} := \max\{|\xi(x)|; x \in \overline{B}_{\|.\|}(0,1)\}$.

On dispose d'un isomorphisme de bidualité canonique $\overline{E} \xrightarrow{\sim} \overline{E}^{\vee\vee}$. En outre, toute suite exacte courte admissible (1.5) détermine par dualité un diagramme

$$0 \longrightarrow \overline{E/F}^{\vee} \xrightarrow{{}^t i} \overline{E}^{\vee} \xrightarrow{{}^t p} \overline{F}^{\vee} \longrightarrow 0$$

qui s'identifie à la suite exacte courte admissible

$$0 \longrightarrow \overline{F}^{\perp} \longrightarrow \overline{E} \longrightarrow \overline{E^{\vee}/F^{\perp}} \longrightarrow 0$$

associé au sous-module saturé

$$F^{\perp} := \{\xi \in E^{\vee} \mid \xi_{|F} = 0\}$$

de $E^{\vee}$. Enfin, l'application $(F \mapsto F^{\perp})$ met en bijection les sous-modules saturés de E et $E^{\vee}$.

1.3.2. *Degré d'Arakelov et pente.* — Plutôt que le covolume, il est souvent plus naturel d'utiliser le *degré d'Arakelov* d'un réseau euclidien $\overline{E}$, défini comme le logarithme de sa « densité » $\operatorname{covol}(\overline{E})^{-1}$:

$$\widehat{\deg}\,\overline{E} := -\log \operatorname{covol}(\overline{E}), \tag{1.6}$$

et, lorsque $\operatorname{rk} E > 0$, sa *pente*

$$\widehat{\mu}(\overline{E}) := \frac{\widehat{\deg}\,\overline{E}}{\operatorname{rk} E} = \log(\operatorname{covol}(\overline{E})^{-1/\operatorname{rk} E}). \tag{1.7}$$

Par exemple, on vérifie aisément que, pour toute suite exacte courte admissible de réseaux euclidiens (1.5), les covolumes $\overline{E}$, $\overline{F}$ et $\overline{E/F}$ satisfont à :

$$\operatorname{covol}(\overline{E}) = \operatorname{covol}(\overline{F}).\operatorname{covol}(\overline{E/F}) \tag{1.8}$$

Les degrés d'Arakelov satisfont donc à la propriété d'additivité

$$\widehat{\deg}\,\overline{E} = \widehat{\deg}\,\overline{F} + \widehat{\deg}\,\overline{E/F}, \tag{1.9}$$

analogue à celle satisfaite par le rang :

$$\operatorname{rk} E = \operatorname{rk} F + \operatorname{rk} E/F.$$

De même, les covolumes d'un réseau euclidien $\overline{E}$ et du réseau dual satisfont à la relation

$$\operatorname{covol}(\overline{E}^{\vee}) = \operatorname{covol}(\overline{E})^{-1},$$

que l'on peut récrire sous la forme :

$$\widehat{\deg}\,\overline{E}^{\vee} = -\widehat{\deg}\,\overline{E}.$$

1.3.3. *Formule de Poisson et séries thêta.* — La notion de réseau dual joue en rôle central en cristallographie, depuis le développement de l'étude des cristaux au moyen de la diffraction des rayons X : les figures de diffraction produites par un cristal modélisé par un réseau euclidien $\overline{E}$ fournissent une image du réseau dual $\overline{E}^\vee$ (Ewald, von Laue, Bragg, 1912). Cela est une manifestation physique de la *formule de Poisson* pour le réseau euclidien $\overline{E}$, qui peut s'énoncer de la manière suivante pour un réseau euclidien de rang n arbitraire $\overline{E} := (E, \|.\|)$.

La transformation de Fourier établit un isomorphisme d'espaces vectoriels topologiques

$$\mathcal{F} : \mathcal{S}(E_\mathbb{R}) \xrightarrow{\sim} \mathcal{S}(E_\mathbb{R}^\vee)$$

entre les espaces de Schwartz de $E_\mathbb{R}$ et de son dual $E_\mathbb{R}^\vee$, défini par la formule, valable pour toute $f \in \mathcal{S}(E_\mathbb{R})$ et tout $\xi \in E_\mathbb{R}^\vee$:

$$\mathcal{F}(f)(\xi) := \int_{E_\mathbb{R}} f(x) e^{-2\pi i \xi(x)} dm_{\overline{E}}(x).$$

Elle se prolonge en un isomorphisme d'espaces vectoriels topologiques entre espaces de distributions tempérées :

$$\mathcal{F} : \mathcal{S}'(E_\mathbb{R}) \xrightarrow{\sim} \mathcal{S}'(E_\mathbb{R}^\vee).$$

La formule de Poisson affirme que les « mesures de comptage » $\sum_{v\in E} \delta_v$ et $\sum_{\xi\in E^\vee} \delta_\xi$ — qui sont des distributions tempérées sur $E_\mathbb{R}$ et sur $E_\mathbb{R}^\vee$ — se déduisent l'une de l'autre par transformation de Fourier :

$$\mathcal{F}(\sum_{v\in E} \delta_v) = (\mathrm{covol}(\overline{E}))^{-1} \sum_{\xi\in E^\vee} \delta_\xi. \tag{1.10}$$

De façon équivalente, pour toute $f \in \mathcal{S}(E_\mathbb{R})$ et tout $x \in E_\mathbb{R}$, on a :

$$\sum_{v\in E} f(x-v) = (\mathrm{covol}(\overline{E}))^{-1} \sum_{\xi\in E^\vee} \mathcal{F}(f)(\xi) e^{2\pi i \xi(x)}. \tag{1.11}$$

(Ce n'est autre que le développement en série de Fourier de la fonction E-périodique $\sum_{v\in E} f(\cdot - v)$.)

Pour tout $t \in \mathbb{R}_+^*$, on peut appliquer (1.11) à la fonction $f_t \in \mathcal{S}(E_\mathbb{R})$ définie par

$$f_t(x) := e^{-\pi t \|x\|^2},$$

dont la transformée de Fourier est donnée par :

$$(\mathcal{F} f_t)(\xi) = t^{-n/2} e^{-\pi t^{-1} \|\xi\|^2}.$$

On obtient ainsi l'identité, valable pour tout $x \in E_\mathbb{R}$:

$$\sum_{v\in E} e^{-\pi t \|x-v\|^2} = (\mathrm{covol}(\overline{E}))^{-1} t^{-n/2} \sum_{\xi\in E^\vee} e^{-\pi t^{-1}\|\xi\|^2 + 2\pi i \xi(x)}. \tag{1.12}$$

En particulier, lorsque $x = 0$, la formule de Poisson (1.12) s'écrit :

$$\theta_{\overline{E}}(t) = (\mathrm{covol}(\overline{E}))^{-1} t^{-n/2} \theta_{\overline{E}^\vee}(t^{-1}), \tag{1.13}$$

où la *fonction thêta* $\theta_{\overline{E}}$ associée à un réseau euclidien $\overline{E}$ est définie, pour tout $t \in \mathbb{R}_+^*$, par la série :

$$\theta_{\overline{E}}(t) := \sum_{v \in E} e^{-\pi t \|v\|^2}. \tag{1.14}$$

1.4. Les inégalités de transférence de Banaszczyk

Les énoncés reliant les invariants de géométrie des nombres attachés à un réseau et à son réseau dual sont classiquement connus sous le nom de *théorèmes de transférence*[(4)].

En 1993, dans son article [Ban93], Banaszczyk établit de remarquables inégalités de transférence, concernant les minima successifs et le rayon de recouvrement :

Théorème 1.2 (Banaszczyk). — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$ et pour tout $i \in \{1, \ldots, n\}$, on a :*

$$\lambda_i(\overline{E}).\lambda_{n+1-i}(\overline{E}^\vee) \leqslant n. \tag{1.15}$$

De plus,

$$R_{\mathrm{cov}}(\overline{E}).\lambda_1(\overline{E}^\vee) \leqslant n/2. \tag{1.16}$$

Comme l'observe Banaszczyk, ces majorations sont optimales, à un terme d'erreur multiplicatif borné uniformément en n près. Cela découle de l'existence, établie par Conway et Thompson, d'une suite de réseaux euclidiens $\overline{\mathrm{CT}}_n$ tels que

$$\overline{\mathrm{CT}}_n^\vee \xrightarrow{\sim} \overline{\mathrm{CT}}_n \tag{1.17}$$

et que :

$$\lambda_1(\overline{\mathrm{CT}}_n) \geqslant \sqrt{n/2\pi e}\,(1 + o(n)) \quad \text{lorsque } n \longrightarrow +\infty.$$

(Voir [MH73], Chapter II, Theorem 9.5. Les réseaux $\overline{\mathrm{CT}}_n$ sont en fait des réseaux entiers unimodulaires, dont l'existence découle de la « formule de masse » de Minkowski-Siegel.) Les réseaux $\overline{\mathrm{CT}}_n$ satisfont à :

$$\lambda_1(\overline{\mathrm{CT}}_n).\lambda_n(\overline{\mathrm{CT}}_n) \geqslant \lambda_1(\overline{\mathrm{CT}}_n)^2 \geqslant (n/2\pi e)(1 + o(n)) \quad \text{lorsque } n \longrightarrow +\infty.$$

De plus, d'après (1.17), on a :

$$\mathrm{covol}(\overline{\mathrm{CT}}_n) = 1$$

et donc, d'après (1.4) :

$$R_{\mathrm{cov}}(\overline{\mathrm{CT}}_n) \geqslant \sigma_n^{-1/n} = \sqrt{n/2\pi e}\,(1 + o(n)) \quad \text{lorsque } n \longrightarrow +\infty.$$

Par conséquent,

$$\lambda_1(\overline{\mathrm{CT}}_n).R_{\mathrm{cov}}(\overline{\mathrm{CT}}_n) \geqslant \lambda_1(\overline{\mathrm{CT}}_n)^2 \geqslant (n/2\pi e)(1 + o(n)) \quad \text{lorsque } n \longrightarrow +\infty.$$

Pour établir le théorème 1.2, Banaszczyk introduit une méthode originale, fondée sur les propriétés analytiques des séries thêta (1.14) associées aux réseaux euclidiens et sur la formule de Poisson (1.12). Les approches antérieures aux inégalités de transférence telles que (1.15) et (1.16) reposaient sur la théorie de la réduction et conduisaient à des

(4) Originellement, *Übertragungssätze* ; voir par exemple [Cas71], Chapter XI.

majorations par des constantes de l'ordre de $n^{3/2}$ et non pas de n (voir par exemple [LLS90]).

Le rôle des séries thêta $\theta_{\overline{E}}$ associées aux réseaux *entiers* — les réseaux euclidiens $\overline{E}$ dont le produit scalaire euclidien prend sur $E \times E$ des valeurs dans $\mathbb{Z}$ — n'est plus à souligner : les fonctions $\theta_{\overline{E}}$ définissent alors des formes modulaires et, via ce type de construction, la théorie des formes modulaires joue un rôle central dans l'étude et la classification des réseaux entiers (on pourra consulter [Ebe13] pour une présentation récente de ces questions et des références).

La méthode de Banaszczyk met en évidence l'importance des fonctions $\theta_{\overline{E}}$ pour l'étude fine des réseaux euclidiens généraux. Nous présentons cette méthode en section 3.

1.5. Les théorèmes de Dadush, Regev et Stephens-Davidowitz

Au cours des dernières décennies, les réseaux euclidiens sont devenus l'objet d'importants travaux en informatique théorique. Leur point de départ ont été les travaux d'Ajtai en 1996, qui a montré comment on pouvait construire des algorithmes de chiffrement à clé publique à partir de constructions mettant en jeu des réseaux euclidiens de grande dimension, pourvu que l'on sache établir la « difficulté » de certains problèmes naturels de théorie des réseaux.

Parmi ces problèmes figurent les suivants :

- un réseau $\overline{E} := (E, \|.\|)$ étant donné par une base de $E_{\mathbb{R}} = \mathbb{R}^n$ muni de la norme standard [(5)] $\|.\| = \|.\|_{\mathrm{st}}$, déterminer une famille dans E de générateurs de $E_{\mathbb{Q}}$ de normes $\leqslant an^c \lambda_n(\overline{E})$, où a et c désignent deux réels > 0 fixés ;
- construire, pour un point x de $E_{\mathbb{R}} = \mathbb{R}^n$, un point v de E tel que $\|x - v\| \leqslant an^c R_{\mathrm{cov}}(\overline{E})$.

Ces questions de cryptographie ont donné un regain d'intérêt considérable à l'étude des « meilleures constantes » dans les inégalités mettant en jeu les invariants des réseaux euclidiens de dimension arbitrairement grande.

Les techniques de Banaszczyk, reposant sur les propriétés des séries thêta (1.14) et sur la formule de Poisson (1.12), ont joué un rôle central dans les travaux suscités par ces questions, notamment dans les travaux de D. Micciancio, O. Regev, S. Dadush et N. Stephens-Davidowitz.

Ces trois derniers auteurs ont obtenu de remarquables résultats sur les invariants des réseaux et sur les inégalités qui les relient dans une série de travaux récents, notamment dans [DR16], [RSD17a] et [RSD17b]. Cet exposé a pour ambition de les présenter à des mathématiciens non-spécialistes.

Nous n'en discuterons pas les motivations, ni les applications liées à la « lattice based cryptography » — questions sur lesquelles l'ouvrage [MG02] et les articles d'exposition [MR09] et [Pei16] constituent des références accessibles à tout mathématicien de bonne

[(5)] ou de façon équivalente, avec les notations du paragraphe 2.6 *infra*, comme le réseau définissant le point $\iota_n([g])$ associé à un élément g de $GL_n(\mathbb{R})$.

volonté. Nous essaierons plutôt d'expliquer comment ces résultat se comprennent naturellement dans le cadre de l'analogie entre corps de nombres et corps de fonctions d'une variable.

Les résultats principaux des articles [DR16] et [RSD17b] peuvent s'énoncer de la manière suivante :

THÉORÈME 1.3 (Regev, Stephens-Davidowitz ; conjecture de Dadush)
Soit $\overline{E} := (E, \|.\|)$ un réseau euclidien de rang $n > 0$ tel que, pour tout sous-$\mathbb{Z}$-module F non nul de E,

$$\mathrm{covol}(F, \|.\|) \geqslant 1.$$

Alors, si $t(n) := 10(\log n + 2)$, on a :

$$\theta_{\overline{E}}(t(n)^{-2}) := \sum_{v \in E} e^{-\pi \|v\|^2 / t(n)^2} \leqslant 3/2. \tag{1.18}$$

THÉORÈME 1.4 (Dadush, Regev, Stephens-Davidowitz ; conjecture de Kannan–Lovász ℓ^2)
Pour tout réseau euclidien $\overline{E} := (E, \|.\|)$ de rang $n > 0$, on pose :

$$\widehat{\mu}_{KL}(\overline{E}) := \min_{F = F^{\mathrm{sat}} \subsetneq E} [\widehat{\mu}(\overline{E/F}) - (1/2) \log \mathrm{rk}\, E/F].$$

On a alors :

$$-c \leqslant \widehat{\mu}_{KL}(\overline{E}) - \log R(\overline{E})^{-1} \leqslant c(n), \tag{1.19}$$

où c désigne une constante universelle et où $c(n)$ désigne une fonction de n telle que

$$c(n) = O(\log \log n) \quad \textit{lorsque } n \longrightarrow +\infty.$$

Plus précisément, les majorations (1.19) sont satisfaites avec

$$c = \log \sqrt{2\pi e} \quad \text{et} \quad c(n) = \log[10(\log n + 10)^{3/2}] = (3/2) \log \log n + o(1).$$

L'intérêt d'un énoncé comme le théorème 1.3 n'est sans doute pas clair au premier regard. Formulons donc quelques commentaires à son sujet.

Tout d'abord, le théorème 1.3 est un élément essentiel de la démonstration de la conjecture de Kannan-Lovász établie dans le théorème 1.4.

Le choix de la valeur 3/2 dans le membre de droite de (1.18) est largement arbitraire. On pourrait y remplacer 3/2 par $1 + \varepsilon$, où ε désigne un quelconque élément de $\mathbb{R}_+^*$, et l'inégalité (1.18) resterait valable avec $t(n)$ remplacé par un certain $t_\varepsilon(n)$ dans $\mathbb{R}_+^*$, satisfaisant

$$\log t_\varepsilon(n) = O(\log \log n) \quad \text{lorsque } n \longrightarrow +\infty.$$

De plus, pour $\varepsilon > 0$ arbitraire, cette variante du théorème 1.3 permettrait d'établir le théorème 1.4.

Soulignons enfin que, dans ce dernier théorème, la première inégalité est une conséquence facile de la minoration (1.4). La contribution fondamentale de Dadush, Regev et Stephens-Davidowitz est d'établir la seconde inégalité dans (1.19) avec une constante $c(n)$ bornée en $O(\log \log n)$. Dans l'article original [KL88] de Kannan et Lovász, où est

conjecturé (entre autres) le théorème 1.3, les majorations (1.19) étaient établies avec $c(n) = (1/2)\log n$. Le passage d'une majoration en $\log n$ à une majoration en $\log\log n$ — dont l'ordre de grandeur lorsque n tend vers l'infini est optimal — constitue un progrès spectaculaire.

Nous renvoyons aux articles originaux [RSD17b] et [DR16] pour une discussion plus approfondie des applications des théorèmes 1.3 et 1.4.

Je remercie chaleureusement Antoine Chambert-Loir, François Charles, Javier Fresán et Vincent Lafforgue pour leurs remarques sur une première version de ce texte.

2. RÉDUCTION DES RÉSEAUX EUCLIDIENS

La théorie classique de la réduction des réseaux euclidiens a pour objet la construction de bases remarquables des réseaux euclidiens, les bases « réduites », adaptées à la détermination de leurs minima successifs (ou de ceux des réseaux duaux) et essentiellement uniques. Il s'agit là d'un sujet notoirement technique, et nous renvoyons à [vdW56], [RB79] Chapter IV, [LLS90] et [Lag95] Section 2 pour des présentations synthétiques et des références.

Dans cette section, nous présentons dans un langage géométrique une version simple d'un résultat central de cette théorie — à savoir qu'un réseau euclidien de rang $n > 0$ peut être « approché » par un réseau euclidien de la forme $\overline{L}_1 \oplus \ldots \oplus \overline{L}_n$, où $\overline{L}_1, \ldots, \overline{L}_n$ désignent des réseaux euclidiens de rang 1, avec une erreur contrôlée en fonction de n, et est donc approximativement déterminé par les n nombres réels $\mu_i := \widehat{\deg}\,\overline{L}_i$.

Puisque que les minima successifs, le rayon de recouvrement, ou la pente de Kannan-Lovász $\widehat{\mu}_{KL}$ d'une telle somme directe $\overline{L}_1 \oplus \ldots \oplus \overline{L}_n$ s'expriment aisément en termes de $(\mu_1, \ldots, \mu_n)$, cette forme simple de la théorie de la réduction implique aussitôt des versions grossières des inégalités (1.15), (1.16) et (1.19) dans les théorèmes 1.2 et 1.4, où les constantes dans les membres de droite sont remplacées par des fonctions du rang n beaucoup plus grandes.

Même si les résultats quantitatifs que permet d'atteindre la théorie classique de la réduction sont souvent dépassés par les méthodes qui font l'objet de cet exposé, les notions qui s'introduisent naturellement dans cette théorie continuent à jouer un rôle central dans l'étude des réseaux euclidiens, dans la forme raffinée des pentes de Stuhler-Grayson (*cf.* [HS97], et Section 5.1 *infra*). En outre, la théorie de la réduction reste la voie d'accès aux énoncés classiques de compacité dans les espaces de réseaux euclidiens, énoncés qui jouent un rôle crucial dans la démonstration du théorème 1.3.

2.1. Opérations sur les réseaux euclidiens

Les opérations de somme directe et de produit tensoriel sur les $\mathbb{Z}$-modules et sur les $\mathbb{R}$-vectoriels euclidiens permettent de définir des opérations analogues sur les réseaux

euclidiens. Ainsi, si $\overline{E}_1 := (E_1, \|.\|_1)$ et $\overline{E}_2 := (E_2, \|.\|_2)$ sont deux réseaux euclidiens, on pose

$$\overline{E}_1 \oplus \overline{E}_2 := (E_1 \oplus E_2, \|.\|_\oplus) \quad \text{et} \quad \overline{E}_1 \otimes \overline{E}_2 := (E_1 \otimes E_2, \|.\|_\otimes),$$

où la norme euclidienne $\|.\|_\oplus$ sur $(E_1 \oplus E_2)_\mathbb{R} \simeq E_{1,\mathbb{R}} \oplus E_{2,\mathbb{R}}$ est définie par

$$\|x_1 \oplus x_2\|_\oplus^2 := \|x_1\|_1^2 + \|x_2\|_2^2,$$

et où la norme $\|.\|_\otimes$ sur $(E_1 \otimes E_2)_\mathbb{R} \simeq E_{1,\mathbb{R}} \otimes_\mathbb{R} E_{2,\mathbb{R}}$ est caractérisée par le fait que, si $(e_{1\alpha})_{1\leqslant\alpha\leqslant n_1}$ (resp. $(e_{2\beta})_{1\leqslant\beta\leqslant n_2}$) est une base orthonormée de l'espace euclidien $(E_{1,\mathbb{R}}, \|.\|_1)$ (resp. de $(E_{2,\mathbb{R}}, \|.\|_2)$), alors $(e_{1\alpha} \otimes e_{2\beta})_{1\leqslant\alpha,\beta\leqslant n_1,n_2}$ est une base orthonormée de l'espace euclidien $(E_{1,\mathbb{R}} \otimes_\mathbb{R} E_{2,\mathbb{R}}, \|.\|_\otimes)$.

L'inclusion canonique $i : E_1 \longrightarrow E_1 \oplus E_2$ et la projection $p : E_1 \oplus E_2 \longrightarrow E_2$ font du diagramme

$$0 \longrightarrow \overline{E}_1 \xrightarrow{\ i\ } \overline{E}_1 \oplus \overline{E}_2 \xrightarrow{\ p\ } \overline{E}_2 \longrightarrow 0 \tag{2.1}$$

une suite exacte courte admissible[(6)]. En particulier, on a :

$$\widehat{\deg}\,(\overline{E}_1 \oplus \overline{E}_2) = \widehat{\deg}\,\overline{E}_1 + \widehat{\deg}\,\overline{E}_2.$$

Pour tout $t \in \mathbb{R}$, on introduit le réseau euclidien de rang 1

$$\overline{\mathcal{O}}(t) := (\mathbb{Z}, \|.\|_t),$$

où $\|.\|_t$ désigne la norme sur $\mathbb{Z}_\mathbb{R} = \mathbb{R}$ définie par $\|x\|_t := e^{-t}|x|$

Il est immédiat qu'un réseau euclidien $\overline{L}$ de rang 1 est isomorphe à $\overline{\mathcal{O}}(t)$ où $t := \widehat{\deg}\,\overline{L}$. Pour tout réseau euclidien $\overline{E} := (E, \|.\|)$, le produit tensoriel $\overline{E} \otimes \overline{\mathcal{O}}(t)$ peut être identifié au réseau euclidien $(E, e^{-t}\|.\|)$, déduit de $\overline{E}$ par un « changement d'échelle » e^{-t}.

2.2. Sommes directes de réseaux de rang 1

Les invariants des réseaux euclidiens sommes directs de réseaux de rang 1 s'évaluent facilement. Considérons en effet

$$\overline{E} := \bigoplus_{i=1}^{n} \overline{\mathcal{O}}(t_i),$$

où n est un entier > 0 et où $t_1 \geqslant \cdots \geqslant t_n$ sont des réels en ordre décroissant. On vérifie aisément que

$$\widehat{\deg}\,\overline{E} = t_1 + \ldots + t_n \quad \text{et} \quad \widehat{\mu}(\overline{E}) = \frac{t_1 + \ldots + t_n}{n},$$

$$\lambda_i(\overline{E}) = e^{-t_i} \quad \text{pour tout } i \in \{1, \ldots, n\}, \tag{2.2}$$

(6) On prendra garde que, en général, une suite exacte courte admissible de réseaux euclidiens *n'est pas* isomorphe à une telle suite exacte : l'obstruction à ce que la suite exacte courte admissible (1.5) soit scindée, c'est-à-dire isomorphe à une suite exacte courte admissible de la forme (2.1), est un élément d'un groupe d'extensions associé aux réseaux $\overline{E}$ et $\overline{E/F}$ dont les propriétés sont étroitement liées à la théorie de la réduction ; voir [BK10].

et

$$R_{\mathrm{cov}}(\overline{E}) = (1/2)(\sum_{i=1}^{n} e^{-2t_i})^{1/2}.$$

En particulier,

$$R_{\mathrm{cov}}(\overline{E}) \in [(1/2)e^{-t_n}, (\sqrt{n}/2)e^{-t_n}].$$

Par ailleurs,

$$\overline{E}^{\vee} \simeq \bigoplus_{i=1}^{n} \overline{\mathcal{O}}(-t_i).$$

Par suite :

$$\lambda_i(\overline{E}^{\vee}) = e^{t_{n+1-i}} \quad \text{pour tout } i \in \{1, \ldots, n\}.$$

2.3. Isomorphismes non-isométriques et invariants des réseaux euclidiens

Soient $\overline{E} := (E, \|.\|)$ et $\overline{E}' := (E', \|.\|')$ deux réseaux euclidiens de même rang n et soit $\varphi : E \xrightarrow{\sim} E'$ un isomorphisme des réseaux sous-jacents. L'application $\varphi_{\mathbb{R}} := \varphi \otimes Id_{\mathbb{R}} : E_{\mathbb{R}} \longrightarrow E'_{\mathbb{R}}$ est un isomorphisme de $\mathbb{R}$-vectoriels, mais n'est pas nécessairement isométrique. Le « défaut d'isométrie » de $\varphi_{\mathbb{R}}$ est contrôlé par les normes d'opérateurs $\|\varphi_{\mathbb{R}}\|$ et $\|\varphi_{\mathbb{R}}^{-1}\|$ définies au moyen des normes $\|.\|$ et $\|.\|'$ sur $E_{\mathbb{R}}$ et $E'_{\mathbb{R}}$, et l'on vérifie aisément que le covolume, les minima successifs ou le rayon de recouvrement de $\overline{E}$ et $\overline{E}'$ peuvent se comparer en termes de ces normes :

$$\|\varphi_{\mathbb{R}}^{-1}\|^{-n} \leqslant \frac{\mathrm{covol}(\overline{E}')}{\mathrm{covol}(\overline{E})} = \|\Lambda^n \varphi_{\mathbb{R}}\| \leqslant \|\varphi_{\mathbb{R}}\|^n,$$

$$\|\varphi_{\mathbb{R}}^{-1}\|^{-1} \leqslant \frac{\lambda_i(\overline{E}')}{\lambda_i(\overline{E})} \leqslant \|\varphi_{\mathbb{R}}\| \quad \text{pour tout } i \in \{1, \ldots, n\},$$

$$\|\varphi_{\mathbb{R}}^{-1}\|^{-1} \leqslant \frac{R_{\mathrm{cov}}(\overline{E}')}{R_{\mathrm{cov}}(\overline{E})} \leqslant \|\varphi_{\mathbb{R}}\|.$$

On peut reformuler ces relations comme suit :

Proposition 2.1. — *Si ψ désigne l'un des invariants $\widehat{\mu}$, $\log \lambda_i^{-1}$, or $\log R_{\mathrm{cov}}^{-1}$, on a :*

$$-\log \|\varphi_{\mathbb{R}}\| \leqslant \psi(\overline{E}') - \psi(\overline{E}) \leqslant \log \|\varphi_{\mathbb{R}}^{-1}\|. \tag{2.3}$$

En particulier, pour tout $\lambda \in \mathbb{R}$,

$$\psi(\overline{E} \otimes \overline{\mathcal{O}}(\lambda)) = \psi(\overline{E}) + \lambda. \tag{2.4}$$

2.4. Théorie de la réduction

THÉORÈME 2.2. — *Pour tout entier $n > 0$, il existe $D(n) \in \mathbb{R}_+^*$ tel que, pour tout réseau euclidien $\overline{E} := (E, \|.\|)$, il existe une $\mathbb{Z}$-base $(v_1, \ldots, v_n)$ de E telle que*

$$\prod_{i=1}^{n} \|v_i\| \leqslant D(n) \operatorname{covol} \overline{E}. \tag{2.5}$$

On peut prendre en fait :

$$D(n) = (4/3)^{n(n-1)/2}. \tag{2.6}$$

On remarquera que, avec les notations du théorème 2.2, il vient aussitôt :

$$\lambda_1(\overline{E}) \leqslant (\prod_{i=1}^{n} \|v_i\|)^{1/n} \leqslant D(n)^{1/n} \operatorname{covol} \overline{E}^{1/n}.$$

On a ainsi retrouvé l'inégalité de Hermite (1.1), avec

$$C(n) = D(n)^{1/n} = (4/3)^{(n-1)/2}.$$

Démonstration. — Le théorème se démontre par récurrence sur l'entier n.

Soit donc $\overline{E}$ un réseau euclidien de rang $n > 0$. Chosissons un élément $s \in E$ tel que $\|s\| = \lambda_1(\overline{E})$. Le sous-module $\mathbb{Z}s$ est alors saturé dans E.

Si $n = 1$, alors $E = \mathbb{Z}s$. Ainsi

$$\operatorname{covol}(\overline{E}) = \lambda_1(\overline{E})$$

et la majoration (2.5) est satisfaite par $v_1 := s$ et $D(1) = 1$.

Si $n > 1$, on peut considérer le réseau euclidien quotient $\overline{E/\mathbb{Z}s} := (E/\mathbb{Z}s, \|.\|_{\mathrm{quot}})$, de rang $n - 1$. Par récurrence, il existe une base $(w_1, \ldots, w_{n-1})$ de $E/\mathbb{Z}s$ telle que

$$\prod_{i=1}^{n-1} \|w_i\|_{\mathrm{quot}} \leqslant D(n-1) \operatorname{covol} \overline{E/\mathbb{Z}s}. \tag{2.7}$$

Si, pour tout $i \in \{0, \ldots, n-1\}$, on choisit un élément v_i dans la préimage $p^{-1}(w_i)$ de w_i par l'application quotient $p : E \longrightarrow E/\mathbb{Z}s$ et si l'on pose $v_n := s$, alors $(v_1, \ldots, v_n)$ est une base de E. De plus, pour $i \in \{0, \ldots, n-1\}$, on peut choisir pour v_i un élément de $p^{-1}(w_i)$ de norme minimale. On a alors :

$$\|v_i\| \leqslant \|v_i - s\| \quad \text{et} \quad \|v_i\| \leqslant \|v_i + s\|. \tag{2.8}$$

Par ailleurs, on a :

$$\|v_i\| \geqslant \lambda_1(\overline{E}) = \|s\|. \tag{2.9}$$

Soit $v_i^{\perp}$ l'élément de $p_{\mathbb{R}}^{-1}(w_i)$ orthogonal à s. Par définition de $\|.\|_{\mathrm{quot}}$, on a :

$$\|v_i^{\perp}\| = \|w_i\|_{\mathrm{quot}}. \tag{2.10}$$

De plus, on peut écrire :

$$v_i = v_i^{\perp} + \eta_i s$$

avec $\eta_i \in \mathbb{R}$; on a alors :

$$\|v_i\|^2 = \|v_i^\perp\|^2 + \eta_i^2 \|s\|^2.$$

D'après (2.8), on a $|\eta_i| \leqslant 1/2$. On en déduit :

$$\|v_i\|^2 \leqslant \|v_i^\perp\|^2 + (1/4)\|s\|^2,$$

puis, compte tenu de (2.9) et (2.10),

$$\|v_i\|^2 \leqslant (4/3)\|w_i\|^2_{\mathrm{quot}}. \tag{2.11}$$

Les majorations (2.11) et (2.7), jointes à la multiplicativité du covolume (1.8) montrent que :

$$\begin{aligned}\prod_{i=1}^{n} \|v_i\| &\leqslant (4/3)^{(n-1)/2} \prod_{i=1}^{n-1} \|w_i\|_{\mathrm{quot}} . \|s\| \\ &\leqslant (4/3)^{(n-1)/2} D(n-1)\, \mathrm{covol}(\overline{E/\mathbb{Z}s}).\, \mathrm{covol}(\overline{\mathbb{Z}s}) \\ &= (4/3)^{(n-1)/2} D(n-1)\, \mathrm{covol}(\overline{E}).\end{aligned}$$

Cela établit l'existence d'une base $(v_1, \ldots, v_n)$ de E satisfaisant à l'inégalité (2.5) avec $D(n) = (4/3)^{(n-1)/2} D(n-1)$, puis avec $D(n)$ donné par (2.6). □

On remarquera que la démonstration précédente fournit un algorithme[(7)] pour construire la base $(v_1, \ldots, v_n)$: les bases produites par cet algorithme sont dites *réduites au sens de Korkin-Zolotarev* (voir par exemple [LLS90]).

2.5. Théorie de la réduction et inégalités de transférence

Il est commode, dans les applications, de combiner le théorème 2.2 avec les observations suivantes.

Soit $\overline{E}$ un réseau euclidien de rang $n > 0$ et soient $L_1, \ldots, L_n$ des sous-$\mathbb{Z}$-modules de rang 1 de E dont E soit la somme directe. Considérons l'application somme :

$$\Sigma : L_1 \oplus \ldots \oplus L_n \xrightarrow{\sim} E$$

et le réseau euclidien $\overline{L}_1 \oplus \ldots \oplus \overline{L}_n$. On peut considérer les normes d'opérateurs $\|\Sigma_{\mathbb{R}}\|$, $\|\Lambda^n \Sigma_{\mathbb{R}}\|$ et $\|\Sigma_{\mathbb{R}}^{-1}\|$ définies à partir des structures euclidiennes sur $\overline{L}_1 \oplus \ldots \oplus \overline{L}_n$ et $\overline{E}$. Enfin, on peut poser :

$$\delta(\overline{E}; L_1, \ldots, L_n) := \widehat{\mu}(\overline{E}) - \frac{1}{n} \sum_{i=1}^{n} \widehat{\deg}\, \overline{L}_i \tag{2.12}$$

$$= \widehat{\mu}(\overline{E}) - \widehat{\mu}(\overline{L}_1 \oplus \ldots \oplus \overline{L}_n). \tag{2.13}$$

(7) pourvu que l'on dispose d'algorithmes pour déterminer les vecteurs de plus petite norme non nulle d'un réseau euclidien, etc.

Proposition 2.3. — *Avec les notations précédentes, on a :*

$$\delta(\overline{E}; L_1, \dots, L_n) = -\frac{1}{n} \log \|\Lambda^n \Sigma_{\mathbb{R}}\| \geqslant 0, \tag{2.14}$$

$$\log \|\Sigma_{\mathbb{R}}\| \leqslant (1/2) \log n, \tag{2.15}$$

et

$$\log \|\Sigma_{\mathbb{R}}^{-1}\| \leqslant \frac{n-1}{2} \log n + n\delta(\overline{E}; L_1, \dots, L_n). \tag{2.16}$$

Démonstration. — Les inégalités (2.14) et (2.15) découlent aisément des définitions. On en déduit (2.16) grâce aux « formules de Cramer » pour Σ^{-1}, qui identifient Σ^{-1} à $\Lambda^{n-1}\Sigma \otimes (\Lambda^n \Sigma)^{-1}$ et montrent que :

$$\begin{aligned} \log \|\Sigma_{\mathbb{R}}^{-1}\| &= \log \|\Lambda^{n-1}\Sigma_{\mathbb{R}}\| - \log \|\Lambda^n \Sigma_{\mathbb{R}}\| \\ &\leqslant (n-1) \log \|\Sigma_{\mathbb{R}}\| + n\delta(\overline{E}; L_1, \dots, L_n). \end{aligned}$$

□

Avec les notations du théorème 2.2, on peut poser $L_i := \mathbb{Z}v_i$, pour $1 \leqslant i \leqslant n$. On a alors :

$$n\delta(\overline{E}; L_1, \dots, L_n) = -\log \operatorname{covol} \overline{E} + \sum_{i=1}^{n} \log \|v_i\| \leqslant \log D(n).$$

En appliquant la proposition (2.3) à $\varphi = \Sigma$, on obtient que, si ψ désigne l'un des invariants $\log \lambda_i^{-1}$ ou $\log R_{\mathrm{cov}}^{-1}$, on a alors :

$$-\frac{n-1}{2} \log n - \log D(n) \leqslant \psi(\bigoplus_{i=1}^{n} \overline{\mathbb{Z}v_i}) - \psi(\overline{E}) \leqslant (1/2) \log n. \tag{2.17}$$

On peut également appliquer la proposition (2.3) à l'isomorphisme :

$${}^t\Sigma : E^\vee \xrightarrow{\sim} \bigoplus L_i^\vee,$$

et on obtient ainsi :

$$-(1/2) \log n \leqslant \psi(\bigoplus_{i=1}^{n} \overline{\mathbb{Z}v_i}^\vee) - \psi(\overline{E}^\vee) \leqslant \frac{n-1}{2} \log n + \log D(n). \tag{2.18}$$

Les calculs du paragraphe 2.2 permettent d'exprimer les invariants des réseaux euclidiens $\bigoplus_{i=1}^n \overline{\mathbb{Z}v_i}$ et $\bigoplus_{i=1}^n \overline{\mathbb{Z}v_i}^\vee$ en termes de la suite $(t_i)_{1 \leqslant i \leqslant n} := (\log \|v_i\|^{-1})_{i \leqslant i \leqslant n}$, où les $\|v_i\|$ sont ordonnés par ordre croissant. Combinés avec les majorations précédentes, ils conduisent à des inégalités de transférence comparant les invariants de $\overline{E}$ et de $\overline{E}^\vee$, où toutefois les constantes dépendant de n sont excessivement grandes.

Par exemple, en appliquant (2.17) avec $\psi = \log R_{\mathrm{cov}}^{-1}$ et (2.18) avec $\psi = \log \lambda_1^{-1}$, on obtient l'inégalité :

$$|\log R_{\mathrm{cov}}(\overline{E}) + \log \lambda_1(\overline{E}^\vee)| \leqslant E(n),$$

avec

$$E(n) = \frac{n+1}{2} \log n + D(n) = O(n^2).$$

2.6. Les espaces $\mathcal{R}_n$ et $\mathcal{R}_n^0$

On vérifie aisément que, pour tout entier naturel n, les classes d'isomorphismes de réseaux euclidiens de rang n constituent un ensemble et que l'on définit une bijection

$$\iota_n : GL_n(\mathbb{Z})\backslash GL_n(\mathbb{R})/O_n(\mathbb{R}) \xrightarrow{\sim} \mathcal{R}_n$$

en envoyant la (double) classe $[g]$ d'un élément g de $GL_n(\mathbb{R})$ sur le réseau euclidien $(\mathbb{R}^n, \|.\|_{\mathrm{st}}, g^{-1}\mathbb{Z}^n)$, défini par le $\mathbb{R}$-vectoriel $V = \mathbb{R}^n$ muni de la norme euclidienne standard $\|.\|_{\mathrm{st}}$ (définie par $\|(x_1, \ldots, x_n)\|_{\mathrm{st}}^2 := x_1^2 + \ldots x_n^2$) et du réseau $\Lambda := g^{-1}\mathbb{Z}^n$. Ce réseau euclidien est isomorphe, *via* g, à $(\mathbb{R}^n, \|g^{-1}.\|_{\mathrm{st}}, \mathbb{Z}^n)$, et l'on a donc :

$$\iota_n([g]) := [(\mathbb{R}^n, \|.\|_{\mathrm{st}}, g^{-1}\mathbb{Z}^n)] = [(\mathbb{R}^n, \|g^{-1}.\|_{\mathrm{st}}, \mathbb{Z}^n)].$$

Si Sym_n^+ désigne l'ouvert des matrices symétriques définies positives dans $M_n(\mathbb{R})$, on dispose d'un difféomorphisme entre variétés $\mathbb{R}$-analytiques

$$\begin{array}{ccc} GL_n(\mathbb{R})/O_n(\mathbb{R}) & \xrightarrow{\sim} & \mathrm{Sym}_n^+ \\ g & \longmapsto & g.{}^t g. \end{array}$$

Ainsi $\mathcal{R}_n$ s'identifie au quotient $GL_n(\mathbb{Z})\backslash \mathrm{Sym}_n^+$ par l'action du sous-groupe $GL_n(\mathbb{Z})$ de $GL_n(\mathbb{R})$, qui agit à gauche sur l'espace Sym_n^+ des formes quadratiques définies positives sur $\mathbb{R}^n$ par le « changement de variables » qui envoie $(\gamma, h) \in GL_n(\mathbb{Z}) \times \mathrm{Sym}_n^+$ sur ${}^t\gamma^{-1} h \gamma^{-1}$.

Rappelons que l'action de $GL_n(\mathbb{Z})$ sur Sym_n^+ est propre et que, après restriction à un sous-groupe d'indice fini assez petit, elle est libre. On munira $\mathcal{R}_n \simeq GL_n(\mathbb{Z})\backslash \mathrm{Sym}_n^+$ de la topologie quotient de la topologie usuelle de Sym_n^+ vu comme ouvert du $\mathbb{R}$-vectoriel des matrices symétriques. C'est un espace localement compact. Davantage, c'est le quotient d'une variété analytique réelle par un groupe fini d'automorphisme ; en tant que tel, $\mathcal{R}_n$ possède une structure naturelle « d'orbifold » . Dans la pratique, cela signifie que l'on peut *grosso modo* travailler sur $\mathcal{R}_n$ comme sur une variété différentiable, et faire comme si l'application quotient $p : \mathrm{Sym}_n^+ \longrightarrow \mathcal{R}_n$ était un revêtement : les fonctions C^∞ sur un ouvert U de $\mathcal{R}_n$ s'identifient aux fonctions C^∞ sur l'ouvert $p^{-1}(U)$ qui sont $GL_n(\mathbb{Z})$-invariantes, etc.

Le degré d'Arakelov des réseaux euclidiens définit une application analytique réelle :

$$\widehat{\deg} : \mathcal{R}_n \longrightarrow \mathbb{R}.$$

On pose :

$$\mathcal{R}_n^0 := \widehat{\deg}^{\,-1}(0).$$

C'est une hypersurface lisse de $\mathcal{R}_n$, et l'on dispose d'un isomorphisme analytique réel :

$$\begin{array}{ccc} \mathcal{R}_n^0 \times \mathbb{R} & \xrightarrow{\sim} & \mathcal{R}_n \\ ([\overline{E}], \lambda) & \longmapsto & [\overline{E} \otimes \overline{\mathcal{O}}(\lambda)]. \end{array}$$

Une partie de $\mathcal{R}_n$ est compacte si et seulement si c'est l'image $p(K)$ d'une partie compacte de Sym_n^+. Cette observation, jointe au théorème 2.2 et à la proposition 2.3, conduit au critère de compacité suivant :

THÉORÈME 2.4 (Critère de Mahler). — *Soit n un entier > 0. Une partie A de $\mathcal{R}_n$ est relativement compacte si et seulement s'il existe α et β dans $\mathbb{R}_+^*$ tel que, pour tout élément $[\overline{E}]$ de A,*

$$\mathrm{covol}(\overline{E}) \leqslant \alpha \quad et \quad \lambda_1(\overline{E}) \geqslant \beta.$$

On peut résumer le théorème d'Hermite 1.1 et le critère de Mahler 2.4 dans l'assertion suivante : *la fonction continue $\lambda_1^{-1} : \mathcal{R}_n^0 \longrightarrow \mathbb{R}_+$ est une fonction d'exhaustion*, c'est-à-dire une application propre de l'espace topologique $\mathcal{R}_n^0$ vers $\mathbb{R}_+$.

Une contribution majeure à l'étude des espaces $\mathcal{R}_n$, de la fonction λ_1 et des constantes de Hermite $\gamma_n = \max_{\mathcal{R}_n^0} \lambda_1^2$ est due à Voronoi. Dans son mémoire [Vor08a], il étudie notamment les réseaux euclidiens *parfaits*, à savoir les réseaux euclidiens $\overline{E}$ tels que l'image de

$$\{v \in E \mid \|v\|_{\overline{E}} = \lambda_1(\overline{E})\}$$

par l'application $(x \mapsto x^{\otimes 2})$ soit une partie génératrice du $\mathbb{R}$-vectoriel $S^2 E_{\mathbb{R}}$. Non seulement les réseaux euclidiens parfaits contiennent les réseaux euclidiens *extrêmes*, qui correspondent aux points de $\mathcal{R}_n^0$ où la fonction λ_1 atteint un maximum local, mais ils permettent à Voronoi de construire par dualité une remarquable décomposition cellulaire de $\mathcal{R}_n$, qui peut apparaître comme une forme raffinée de la théorie de la réduction (voir [RB79], [Mar03] et [Sch09] pour des expositions modernes de ces constructions).

Dans son second mémoire ([Vor08b] et [Vor09]), il étudie une autre décomposition de $\mathcal{R}_n^0$, associée à la combinatoire des domaines de Voronoi des réseaux euclidiens : si $\overline{E} := (E, \|.\|)$ est un réseau euclidien, son *domaine de Voronoi* est défini comme le polytope convexe symétrique :

$$\mathcal{V}(\overline{E}) := \{x \in E_{\mathbb{R}} \mid \forall e \in E, \|x\| \leqslant \|x - e\|\},$$

formé des points x de $E_{\mathbb{R}}$ tels que l'origine appartienne à l'ensemble (fini) des points de E minimisant la distance de x à E dans l'espace euclidien $(E_{\mathbb{R}}, \|.\|)$.

La notion de domaine de Voronoi est bien naturelle, et apparaît dès les premiers travaux mathématiques sur les réseaux euclidiens : ainsi les domaines de Voronoi apparaissent encore dans la littérature sous le nom de *domaine de Dirichlet*. Ils jouent aussi un rôle central en cristallographie et en physique du solide, domaines où ils apparaissent sous le nom de *première zone de Brillouin* ou de *cellule de Wigner-Seitz*. Ils jouent aussi un rôle fondamental dans la preuve des théorèmes 1.3 et1.4.

La profondeur et la quantité des résultats présentés dans les mémoires de Voronoi ont fait qu'ils sont restés longtemps mal étudiés, tout particulièrement le second. L'interface entre l'étude à la Voronoi des espaces $\mathcal{R}_n^0$ et des invariants classiques des réseaux et l'étude de leurs invariants définis à l'aide de séries thêta, qui font l'objet de cet exposé, apparaît comme un champ d'investigation fascinant.

3. LES INÉGALITÉS DE BANASZCZYK

Dans cette section, logiquement indépendante de la précédente, nous présentons la méthode introduite par Banaszczyk dans son article fondateur [Ban93] pour établir les inégalités de transférence optimales énoncées dans le théorème 1.2. Nous nous concentrerons sur la seconde inégalité (1.16) ; la démonstration des inégalités (1.15) utilise des arguments similaires à ceux qui conduisent à (1.16), et nous renvoyons à [Ban93], p. 631–632, pour les détails. Signalons aussi que Banaszczyk a appliqué ce type de technique à des questions voisines dans les articles [Ban95] et [Ban96].

3.1. Les majorations clés

Soit $\overline{E} := (E, \|.\|)$ un réseau euclidien de rang $n > 0$.

Sa fonction thêta $\theta_{\overline{E}}$ est clairement une fonction décroissante. Il en va de même de $\theta_{\overline{E}^\vee}$ et l'équation fonctionelle (1.13) reliant $\theta_{\overline{E}}$ et $\theta_{\overline{E}^\vee}$ montre donc que $t^{n/2}\theta_{\overline{E}}(t)$ est une fonction croissante de $t \in \mathbb{R}_+^*$.

Par ailleurs, la formule de Poisson (1.12) montre que, pour tout $x \in E_{\mathbb{R}}$ et tout $t \in \mathbb{R}_+$, on a :

$$\sum_{v\in E} e^{-\pi t\|x-v\|^2} \leqslant \sum_{v\in E} e^{-\pi t\|v\|^2}, \tag{3.1}$$

avec égalité si et seulement si $x \in E$.

Le point de départ de la méthode de Banaszczyk est la majoration suivante, qui découle aisément des observations qui précédent :

Lemme 3.1. — *Pour tout $x \in E_{\mathbb{R}}$, tout $r \in \mathbb{R}_+$ et tout $t \in]0, 1]$, on a :*

$$\sum_{v\in E,\|v-x\|\geqslant r} e^{-\pi\|v-x\|^2} \leqslant t^{-n/2} e^{-\pi(1-t)r^2} \sum_{v\in E} e^{-\pi\|v\|^2}. \tag{3.2}$$

Démonstration. — Il vient :

$$\begin{aligned}
\sum_{v\in E,\|v-x\|\geqslant r} e^{-\pi\|v-x\|^2} &= \sum_{v\in E,\|v-x\|\geqslant r} e^{-\pi(1-t)\|v-x\|^2} e^{-\pi t\|v-x\|^2} \\
&\leqslant e^{-\pi(1-t)r^2} \sum_{v\in E,\|v-x\|\geqslant r} e^{-\pi t\|v-x\|^2} \\
&\leqslant e^{-\pi(1-t)r^2} \sum_{v\in E} e^{-\pi t\|v\|^2} \qquad (3.3) \\
&\leqslant e^{-\pi(1-t)r^2} t^{-n/2} \sum_{v\in E} e^{-\pi\|v\|^2}. \qquad (3.4)
\end{aligned}$$

En effet, la majoration (3.3) découle de (3.1), et (3.4) de l'inégalité $t^{n/2}\theta_{\overline{E}}(t) \leqslant \theta_{\overline{E}}(1)$. □

Compte tenu de (3.1), la majoration (3.2) n'a d'intérêt que pour les valeurs de r telles que

$$\inf_{t\in]0,1]} t^{-n/2}e^{-\pi(1-t)r^2} < 1.$$

Un calcul élémentaire montre que cette inégalité est satisfaite précisément lorsque $r > \sqrt{n/2\pi}$, puis que, lorsque cela a lieu, si l'on pose $r = \sqrt{n/2\pi}\,\tilde{r}$ avec $\tilde{r} \in]1, +\infty[$, alors le minimum de $t^{-n/2}e^{-\pi(1-t)r^2}$ sur $]0, 1]$ est atteint en $t = t_{\min} := \tilde{r}^{-2}$ et prend comme valeur :

$$t_{\min}^{-n/2}e^{-\pi(1-t_{\min})r^2} = [\tilde{r}e^{-(1/2)(\tilde{r}^2-1)}]^n.$$

Ces considérations montrent que le lemme 3.1 peut se reformuler comme la proposition suivante, mieux adaptée aux applications, où l'on a posé :

$$\beta(\tilde{r}) := \tilde{r}e^{-(1/2)(\tilde{r}^2-1)}. \tag{3.5}$$

Proposition 3.2. — *Soit $\overline{E}$ un réseau euclidien de rang $n > 0$ et soit x un élément de $E_{\mathbb{R}}$. Pour tout $\tilde{r} \in [1, +\infty[$, si l'on pose*

$$r = \sqrt{\frac{n}{2\pi}}\tilde{r},$$

alors on a :

$$\sum_{v\in E, \|v-x\|\geqslant r} e^{-\pi\|v-x\|^2} \leqslant \beta(\tilde{r})^n \sum_{v\in E} e^{-\pi\|v\|^2}. \tag{3.6}$$

On observera que l'on définit par la formule (3.5) un homéomorphisme décroissant :

$$\beta : [1, +\infty[\xrightarrow{\sim}]0, 1].$$

On remarquera aussi que la formule de Poisson (1.12) implique les identités :

$$\begin{aligned}\sum_{v\in E} e^{-\pi\|x-v\|^2} + \sum_{v\in E} e^{-\pi\|v\|^2} &= (\operatorname{covol}\overline{E})^{-1} \sum_{\xi\in E^\vee} e^{-\pi\|\xi\|^2}[1 + \cos(2\pi\xi(x))] \\ &= 2(\operatorname{covol}\overline{E})^{-1} \sum_{\xi\in E^\vee} e^{-\pi\|\xi\|^2}\cos^2(\pi\xi(x)),\end{aligned}$$

On en déduit :

Proposition 3.3. — *Pour tout réseau euclidien $\overline{E}$ et tout point $x \in E_{\mathbb{R}}$, on a :*

$$\sum_{v\in E} e^{-\pi\|x-v\|^2} + \sum_{v\in E} e^{-\pi\|v\|^2} \geqslant 2(\operatorname{covol}\overline{E})^{-1}. \tag{3.7}$$

3.2. Démonstration de l'inégalité (1.16)

Commençons par énoncer deux corollaires des propositions 3.2 et 3.3.

En appliquant la proposition 3.2 avec $x = 0$ et $r = \lambda_1(\overline{E})$, on obtient :

COROLLAIRE 3.4. — *Soit $\overline{E}$ un réseau euclidien de rang $n > 0$ et de premier minimum $\lambda_1(\overline{E}) > \sqrt{n/2\pi}$.*

Si l'on définit $\tilde{\lambda} \in]1, +\infty[$ par l'égalité $\lambda_1(\overline{E}) = \sqrt{n/2\pi}\tilde{\lambda}$, alors on a :

$$\theta_{\overline{E}}(1) := \sum_{v \in E} e^{-\pi\|v\|^2} \leqslant (1 - \beta(\tilde{\lambda})^n)^{-1}. \tag{3.8}$$

Par ailleurs, par définition même de $R_{\mathrm{cov}}(\overline{E})$, il existe $x \in E_{\mathbb{R}}$ tel que $\|v - x\| \geqslant \rho(\overline{E})$ pour tout v dans E. Si l'on applique la proposition 3.2 à un tel point x et à $r = R_{\mathrm{cov}}(\overline{E})$, on obtient la première assertion du corollaire suivant :

COROLLAIRE 3.5. — *Soit $\overline{E}$ un réseau euclidien de rang $n > 0$ et de rayon de recouvrement $R_{\mathrm{cov}}(\overline{E}) \geqslant \sqrt{n/2\pi}$. On définit $\tilde{R} \in [1, +\infty[$ par l'égalité $R_{\mathrm{cov}}(\overline{E}) = \sqrt{n/2\pi}\tilde{R}$,*

Il existe $x \in E_{\mathbb{R}}$ tel que

$$\frac{\displaystyle\sum_{v \in E} e^{-\pi\|v-x\|^2}}{\displaystyle\sum_{v \in E} e^{-\pi\|v\|^2}} \leqslant \beta(\tilde{R})^n. \tag{3.9}$$

Par conséquent,

$$\beta(\tilde{R})^n \geqslant 2\theta_{\overline{E}^\vee}(1)^{-1} - 1. \tag{3.10}$$

Pour établir (3.10), il suffit d'observer que, d'après la proposition 3.3, le membre de gauche de l'inégalité (3.9) est minoré par $2\,\mathrm{covol}(\overline{E})^{-1}\theta_{\overline{E}}(1)^{-1} - 1$, puis de faire appel à l'équation fonctionnelle (1.13) reliant $\theta_{\overline{E}}$ et $\theta_{\overline{E}^\vee}$, qui montre que :

$$\theta_{\overline{E}}(1) = (\mathrm{covol}(\overline{E}))^{-1}\,\theta_{\overline{E}^\vee}(1).$$

Nous sommes maintenant à même de démontrer l'inégalité de transférence (1.16) :

$$R_{\mathrm{cov}}(\overline{E}).\lambda_1(\overline{E}^\vee) \leqslant n/2.$$

Soit donc $\overline{E}$ un réseau euclidien de rang $n > 0$ et définissons $\tilde{R}$ et $\tilde{\lambda}^\vee$ par les égalités

$$R_{\mathrm{cov}}(\overline{E}) = \sqrt{n/2\pi}\,\tilde{R} \quad \text{et} \quad \lambda_1(\overline{E}^\vee) = \sqrt{n/2\pi}\,\tilde{\lambda}^\vee.$$

LEMME 3.6. — *Lorsque* $\min(\tilde{\lambda}^\vee, \tilde{R}) > 1$, *on a :*

$$\beta(\tilde{R})^n + 2\beta(\tilde{\lambda}^\vee)^n \geqslant 1. \tag{3.11}$$

Démonstration. — Le corollaire 3.4, appliqué à $\overline{E}^\vee$, montre que :

$$1 - \beta(\tilde{\lambda}^\vee)^n \leqslant \theta_{\overline{E}^\vee}(1)^{-1}. \tag{3.12}$$

La majoration (3.11) découle des inégalités (3.10) et (3.12). □

Pour tout entier $n > 0$, posons :

$$t_n := \beta^{-1}(3^{-1/n}) \in]1, +\infty[.$$

Un calcul élémentaire montre que

$$t_n \leqslant 1 + \sqrt{(\log 3)/n}$$

et que

$$t_n = 1 + \sqrt{(\log 3)/n} + O(1/n) \quad \text{lorsque } n \longrightarrow +\infty.$$

À partir du lemme 3.6, on dérive une version plus précise de l'inégalité de Banaszczyk (1.16) :

PROPOSITION 3.7. — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$, on a :*

$$R_{\mathrm{cov}}(\overline{E}).\lambda_1(\overline{E}^\vee) \leqslant t_n^2 n/2\pi. \tag{3.13}$$

En fait, pour $n \geqslant 3$, $t_n \leqslant t_3 = 1,605... < \sqrt{\pi} = 1,772...$ et donc $t_n^2 n/2\pi < n/2$. Ainsi l'inégalité (3.13) implique (1.16) lorsque $n \geqslant 3$. Lorsque $n = 1$, (1.16) est triviale, et lorsque $n = 2$, elle découle de considérations élémentaires sur les bases réduites des réseaux euclidiens dans le plan.

Démonstration de la proposition 3.7. — Supposons d'abord que

$$R_{\mathrm{cov}}(\overline{E}) = \lambda_1(\overline{E}^\vee) =: t. \tag{3.14}$$

D'après le lemme 3.6, si $t > 1$, alors $\beta(t) \geqslant 3^{-1/n}$ et donc $t \leqslant t_n$. Comme $t_n > 1$, cette majoration est encore vrai lorsque $t \leqslant 1$. L'inégalité (3.13) en découle aussitôt.

La validité de (3.13) en général découle de sa validité sous l'hypothèse (3.14). En effet, lorsque l'on remplace le réseau euclidien $\overline{E}$ par $\overline{E} \otimes \overline{\mathcal{O}}(\delta)$ avec $\delta \in \mathbb{R}$ (c'est-à-dire lorsque l'on multiplie la norme euclidienne définissant $\overline{E}$ par le facteur $e^{-\delta}$), le produit $R_{\mathrm{cov}}(\overline{E}).\lambda_1(\overline{E}^\vee)$ reste inchangé, alors, que par un choix convenable de δ, la condition (3.14) est satisfaite par $\overline{E} \otimes \overline{\mathcal{O}}(\delta)$. (Cela découle aussitôt de (2.4) avec $\psi = \log \lambda_1^{-1}$ et $\psi = \log R_{\mathrm{cov}}^{-1}$.) □

4. FIBRÉS VECTORIELS SUR LES COURBES : FILTRATIONS DE HARDER-NARASIMHAN ET PENTES

Dans cette section, nous rappelons divers résultats classiques concernant les fibrés vectoriels sur les courbes algébriques. Ces résultats jouent un rôle central dans l'étude des espaces de modules classifiant ces fibrés vectoriels, et l'on pourra se reporter à [VLP85] pour une présentation synthétique et des références sur ce sujet. Nous présentons ici ces résultats en tant que « modèles » pour l'étude des réseaux euclidiens dans la suite de cet exposé. Notamment les propositions 4.1 et 4.2 ont été formulées explicitement parce qu'elles apparaîtront comme les analogues géométriques du théorème 1.3.

Soit C une courbe projective lisse et géométriquement connexe sur un corps k. On notera $K := k(C)$ le corps des fonctions rationnelles sur C.

Un *fibré vectoriel* E sur C est un faisceau cohérent localement libre sur C. Tout sous-faisceau cohérent F de E est encore un fibré vectoriel sur C. On dira que F est un *sous-fibré vectoriel* de E lorsque le faisceau quotient E/F est sans torsion, et définit donc un fibré vectoriel.

La fibre E_K de E au point générique de C — à savoir, l'espace des sections rationnelles de E sur C — est un K-vectoriel de dimension finie. Si F est un sous-faisceau cohérent de E, F_K est un sous-K-vectoriel de E_K, et cette construction met en bijection les sous-fibrés vectoriels de E et les sous-K-vectoriels de E_K.

On dispose d'opérations tensorielles sur les fibrés vectoriels : si E est un fibré vectoriel sur C, on peut définir le fibré dual $E^\vee$ et, pour tout $n \in \mathbb{N}$, la puissance tensorielle $E^{\otimes n}$ et extérieure $\bigwedge^n E$; à deux fibrés vectoriels E et F sur C, on peut associer leur produit tensoriel $E \otimes F$ et le fibré vectoriel $\mathrm{Hom}(E, F) \simeq E^\vee \otimes F$.

4.1. Invariants des fibrés vectoriels

À un fibré vectoriel E sur C sont associés les invariants suivants :

– son rang

$$\mathrm{rk}\, E := \dim_K E_K \in \mathbb{N};$$

– son degré[(8)]

$$\deg E \in \mathbb{Z}.$$

– lorsque $\mathrm{rk}\, E > 0$, sa pente :

$$\mu(E) := \frac{\deg E}{\mathrm{rk}\, E} \in \mathbb{Q}.$$

Ces invariants satisfont aux propriétés suivantes :

(i) Pour tout fibré vectoriel E sur C et tout sous-fibré vectoriel F de E,

$$\deg E = \deg F + \deg E/F; \tag{4.1}$$

(ii) Si E est un fibré vectoriel de rang > 0 et L un fibré en droites sur C, on a :

$$\mu(E \otimes L) = \mu(E) + \deg L.$$

Plus généralement, si E et F sont deux fibrés vectoriels de rang > 0 sur C, on a :

$$\mu(E \otimes F) = \mu(E) + \mu(F).$$

(iii) Si $\varphi : E \longrightarrow E'$ est un morphisme de faisceaux de $\mathcal{O}_C$-modules entre deux fibrés vectoriels qui est un isomorphisme au point générique :

$$\varphi_K : E_K \xrightarrow{\sim} E'_K,$$

(8) Rappelons que, lorsque E est de rang 1 (un *fibré en droites*), donc isomorphe au faisceau $\mathcal{O}_C(D)$ associé au diviseur $D = \sum_{i\in I} n_i P_i$ d'une section rationnelle non-nulle de E (défini par une famille $(P_i)_{i\in I}$ de points fermés de C, affectés de multiplicités $(n_i)_{i\in I} \in \mathbb{Z}^I$), on a : $\deg E = \deg \mathcal{O}_C(D) = \deg D := \sum_{i\in I} n_i[\kappa(P_i) : k]$. Pour un fibré E de rang quelconque, on se ramène aux fibrés en droites en considérant sa puissance extérieure maximale : $\deg E := \deg \bigwedge^{\mathrm{rk}\, E} E$.

alors

$$\deg E \leqslant \deg E',$$

et l'égalité a lieu si et seulement si φ est un isomorphisme.

En particulier, pour tout sous-faisceau cohérent F de E, on a

$$\deg F \leqslant \deg F^{\mathrm{sat}},$$

avec égalité si et seulement si F est un sous-fibré vectoriel de E.

(iv) Soient F_1 et F_2 deux sous-faisceaux cohérents d'un fibré vectoriel E sur C. On peut alors considérer les sous-faisceaux cohérents $F_1 \cap F_2$ et $F_1 + F_2$ de F et l'on a :

$$\deg(F_1 \cap F_2) + \deg(F_1 + F_2) = \deg F_1 + \deg F_2. \tag{4.2}$$

Si de plus F_1 et F_2 sont saturés dans E, le faisceau $F_1 \cap F_2$ l'est aussi (mais pas nécessairement $F_1 + F_2$) et l'on a :

$$\deg(F_1 \cap F_2) + \deg(F_1 + F_2)^{\mathrm{sat}} \geqslant \deg F_1 + \deg F_2. \tag{4.3}$$

(v) Pour tout fibré vectoriel E sur C, il existe $c(E)$ dans $\mathbb{R}$ tel que, pour tout sous-faisceau cohérent F de E,

$$\deg F \leqslant c(E).$$

(vi) Pour tout fibré vectoriel E sur C, de fibré vectoriel dual $E^\vee := \mathrm{Hom}(E, \mathcal{O}_C)$, on a :

$$\deg E^\vee = -\deg E.$$

De plus, si F désigne un sous-fibré vectoriel de E et si $F^\perp \subset E^\vee$ est l'annulateur de F dans $E^\vee$, on dispose d'un isomorphisme canonique :

$$F^\perp \xrightarrow{\sim} (E/F)^\vee;$$

on en déduit :

$$\deg F^\perp = \deg F - \deg E. \tag{4.4}$$

4.2. Filtration canonique et pentes d'un fibré vectoriel

On dit qu'un fibré vectoriel E de rang non nul est *semi-stable* lorsque, pour tout sous-fibré vectoriel (ou, de façon équivalente, pour tout sous-faisceau) non nul F de E, on a :

$$\mu(F) \leqslant \mu(E).$$

Harder et Narasimhan ont montré que les propriétés (i) à (v) du degré permettent d'attacher à tout fibré vectoriel E sur C de rang non nul une filtration canonique — la *filtration de Harder-Narasimhan* — de E,

$$E_0 = 0 \subsetneq E_1 \subsetneq \cdots \subsetneq E_N = E.$$

C'est l'unique filtration de longueur $N \in \mathbb{N}_{>0}$, par des sous-fibrés vectoriels E_i de E tels que les quotients E_i/E_{i-1} soient semi-stables, de pentes strictement décroissantes :

$$\mu(E_1) > \mu(E_2/E_1) > \ldots > \mu(E_N/E_{N-1}). \tag{4.5}$$

(Voir [HN75] ; cette construction est étroitement liée à la théorie de la réduction sur les corps de fonctions développée par Harder dans [Har69]. Tjurin avait introduit une construction analogue dans [Tju66].)

Nous rappelons dans l'appendice A la construction de ces filtrations canoniques, dans un cadre formel général, concernant un ensemble ordonné muni d'une fonction « rang » r et d'une fonction « degré » d idoines. On retrouve la construction de [HN75] en appliquant cette construction générale à l'ensemble ordonné $(\mathcal{E}(E), \subseteq)$ des sous-faisceaux cohérents de E munis de l'inclusion, et aux fonctions $r := \mathrm{rk}$ et $d := \deg$. On la retrouve également en appliquant le formalisme des pentes au sous-ensemble $\mathcal{E}_{\mathrm{st}}(E)$ de $\mathcal{E}(E)$ défini par les sous-fibrés vectoriels de E. Les hypothèses (2) et (3) de sous-additivité et de finitude sur lesquelles s'appuie la construction générale de l'appendice sont satisfaites ici d'après les points (iv) et (v) du paragraphe précédent.

En utilisant l'additivité (4.1) du degré dans les suites exactes courtes, on vérifie que la filtration de Harder-Narasimhan peut aussi se décrire, comme ci-dessus, en terme des sous-quotients E_i/E_{i-1} : et que les pentes successives du polygone canonique de E, construit comme dans l'appendice A en termes de l'envoppe convexe des points $(\mathrm{rk}\, F, \deg F)$ associés aux sous-fibrés vectoriels F de E, sont précisément les pentes (4.5). En particulier, la fonction P de $[0, \mathrm{rk}\, E]$ vers $\mathbb{R}$ associée par la construction de l'appendice A à $(\mathcal{E}(E), \subset, \mathrm{rk}\,, \deg)$ — son graphe est le polygone canonique de E — est affine sur chaque intervalle $[\mathrm{rk}\, E_i, \mathrm{rk}\, E_{i-1}]$ $(i \in \{1, \dots, N\})$ et satisfait

$$P(\mathrm{rk}\, E_i) = \deg E_i \quad \text{pour tout } i \in \{0, \dots, N\}.$$

On observera que E est semi-stable précisément lorsque sa filtration de Harder-Narasimhan est triviale ($N = 1$), ou encore lorsque son polygone canonique est un segment de droite. En outre, on vérifie aisément que

$$\mu_{\max}(E) := \mu(E_1) = \max_{0 \neq F \subset E} \mu(F),$$

$$\mu_{\min}(E) := \mu(E_N/E_{N-1}) = \min_{F = F^{\mathrm{sat}} \subsetneq E} \mu(E/F),$$

et que, si L est un fibré en droites sur C,

$$\mu_{\max}(E \otimes L) = \mu_{\max}(E) + \deg L,$$

$$\mu_{\min}(E \otimes L) = \mu_{\min}(E) + \deg L.$$

Enfin, comme l'application $(F \longmapsto F^{\perp})$ établit une bijection entre sous-fibrés vectoriels de E et sous-fibrés vectoriels de $E^{\vee}$, l'égalité (4.4) montre que, pour tout $x \in [0, \mathrm{rk}\, E]$, on a :

$$P_{E^{\vee}}(x) = P_E(\mathrm{rk}\, E - x) - \deg E. \tag{4.6}$$

En particulier, les pentes de $E^{\vee}$ sont les opposés des pentes de E ; notamment :

$$\mu_{\min}(E) = -\mu_{\max}(E^{\vee}).$$

4.3. Groupes de cohomologie et pentes

Si E est un fibré vectoriel sur C, les groupes de cohomologie $H^i(C,E)$ sont des k-vectoriels de dimension finie, nuls si $i>1$. On pose :

$$h^i(C,E) := \dim_k H^i(C,E).$$

Si $\omega_C := \Omega^1_{C/k}$ désigne le fibré en droite canonique de C, on dispose des isomorphismes de dualité de Serre

$$H^i(C,E) \simeq \mathrm{Hom}_k(H^{1-i}(C,E^\vee\otimes\omega_C),k)$$

et donc des égalités de dimension :

$$h^i(C,E) = h^{1-i}(C,E^\vee\otimes\omega_C). \tag{4.7}$$

Si g désigne le genre de C, défini comme $g := h^1(C,\mathcal{O}_C)$, la caractéristique d'Euler-Poincaré de E est donnée par la formule de Riemann-Roch :

$$\begin{aligned}\chi(C,E) &:= h^0(C,E) - h^1(C,E)\\ &= h^0(C,E) - h^0(C,E^\vee\otimes\omega_C) = \deg E + \mathrm{rk}\,E\,(1-g).\end{aligned} \tag{4.8}$$

La formule de Riemann-Roch implique notamment la minoration (inégalité de Riemann) :

$$h^0(C,E) \geqslant \deg E + \mathrm{rk}\,E\,(1-g). \tag{4.9}$$

En particulier, si E est non nul et si $\mu(E)+1-g>0$, alors $H^0(C,E)\neq\{0\}$. On en déduit aussitôt que *si E est un fibré vectoriel non nul sur C tel que $\mu_{\max}(E)>g-1$, alors $H^0(C,E)\neq\{0\}$.*

Inversement, *si $H^0(C,E)\neq\{0\}$,* c'est-à-dire s'il existe un morphisme injectif de faisceaux de $\mathcal{O}_C$-modules $s:\mathcal{O}_C\longrightarrow E$, *on a alors : $\mu_{\max}(E)\geqslant\mu(\mathcal{O}_C)=0$.*

Supposons maintenant que C est muni d'un diviseur D de degré 1[(9)]. Pour tout $n\in\mathbb{Z}$, nous pouvons considérer le fibré vectoriel

$$E(nD) := E\otimes\mathcal{O}_C(nD).$$

Il satisfait à

$$\mu_{\max}(E(nD)) = \mu_{\max}(E) + n.$$

Les observations précédentes, appliquées aux fibrés vectoriels $E(nD)$, impliquent aussitôt :

Proposition 4.1. — *Pour tout fibré vectoriel E de rang non nul sur C, il existe un entier $s^0(E)$ tel que, pour tout $k\in\mathbb{Z}$,*

$$H^0(C,E(-kD)) = \{0\} \Longleftrightarrow k > s^0(E).$$

(9) Un tel diviseur existe notamment lorsque le corps k est algébriquement clos (il suffit alors de prendre pour D le diviseur défini par un point de $C(k)$) et lorsque k est fini.

De plus,

$$\mu_{\max}(E) - g \leqslant s^0(E) \leqslant \mu_{\max}(E). \tag{4.10}$$

On en déduit, par dualité de Serre :

Proposition 4.2. — *Pour tout fibré vectoriel E de rang non nul sur C, il existe un entier $s^1(E)$ tel que, pour tout $k \in \mathbb{Z}$,*

$$H^1(C, E(kD)) = \{0\} \Longleftrightarrow k > s^1(E).$$

On a :

$$s^1(E) = s^0(E^\vee \otimes \omega_C)$$

et

$$-\mu_{\min}(E) + g - 2 \leqslant s^1(E) \leqslant -\mu_{\min}(E) + 2g - 2.$$

On observera que, d'après la formule de Riemann-Roch, pour tout entier $k > s^1(E)$, on a :

$$h^0(C, E(kD)) = \operatorname{rk} E(k + 1 - g) + \deg E. \tag{4.11}$$

En outre, pour tout $k \in \mathbb{Z}$,

$$s^0(E(kD)) = s^0(E) + k \quad \text{et} \quad s^1(E(kD)) = s^1(E) - k.$$

5. L'ANALOGIE ENTRE RÉSEAUX EUCLIDIENS ET FIBRÉS VECTORIELS SUR LES COURBES

L'un des avatars de l'analogie entre corps de nombres et corps de fonctions algébriques d'une variable est l'analogie entre réseaux euclidiens et fibrés vectoriels sur une courbe C, projective, lisse et géométriquement irréductible sur un corps k.

Dans cette analogie, le corps $\mathbb{Q}$ tient la place du corps $K := k(C)$, et l'ensemble des places de $\mathbb{Q}$ (qui s'identifie à la réunion disjointe des points fermés de $\operatorname{Spec}\mathbb{Z}$ — autrement dit, des nombres premiers — et de la place archimédienne de $\mathbb{Q}$, définie par la valeur absolue usuelle) tient le rôle de l'ensemble des points fermés de C.

En particulier, le $\mathbb{Q}$-vectoriel $E_{\mathbb{Q}}$ associé à un réseau euclidien $\overline{E}$ tient la place de la fibre E_K d'un fibré vectoriel E au point générique de C ; les réseaux euclidiens $\overline{F}$ associés à des sous-$\mathbb{Z}$-modules F de E (resp. à des sous-$\mathbb{Z}$-modules saturés) jouent le rôle des sous-faisceaux cohérents (resp. des sous-fibrés vectoriels) de E, et les suites exactes courtes admissibles de réseaux euclidiens (1.5) celui des suites exactes courtes de fibrés vectoriels sur C.

Sous une forme parfois vague, ces analogies sont très anciennes (voir par exemple [Wei39] et [Eic66], Chapter I). Il est remarquable qu'elles puissent être étendue dans diverses directions, et, dans cette section, nous décrivons comment les diverses constructions discutées dans la section 4 admettent des analogues, souvent étonnamment précis, concernant les réseaux euclidiens.

Il s'avère que l'invariant $s^1(E)$ associé à un fibré vectoriel E dans le paragraphe 4.3 possède comme avatar dans le monde des réseaux euclidiens l'invariant $\eta_\varepsilon(\overline{E})$ introduit par Micciancio et Regev ([MR07]) sous le nom de *smoothing parameter*, ou plutôt une version logarithmique de ce dernier :

$$s^1_{\theta,\varepsilon}(\overline{E}) := \log \eta_\varepsilon(\overline{E}). \tag{5.1}$$

Ces auteurs étaient motivés, non par l'analogie entre corps de nombres et corps de fonctions, mais par les applications des réseaux euclidiens à la cryptographie : le *smoothing parameter* $\eta_\varepsilon(\overline{E})$ d'un réseau euclidien $\overline{E} := (E, \|.\|)$ est le réel λ tel que la mesure

$$\mathrm{covol}(\overline{E}) \sum_{v \in E} \delta_v$$

sur $E_\mathbb{R}$ devienne, à un seuil $\varepsilon > 0$ fixé, « indiscernable » de la mesure de Lebesgue après convolution avec la mesure gaussienne centrée de variance $\lambda^{-2}\|.\|^2$ sur $E_\mathbb{R}$. Formellement, $\eta_\varepsilon(\overline{E})$ est défini par l'égalité :

$$\theta_{\overline{E}^\vee}(\eta_\varepsilon(\overline{E})^2) = 1 + \varepsilon. \tag{5.2}$$

L'article [MR07] montre aussi comment ce nouvel invariant intervient naturellement lorsque l'on étudie les invariants classiques des réseaux euclidiens par les techniques de Banaszczyk présentées dans la section 3.

Le « smoothing parameter » $\eta_\varepsilon(\overline{E})$ s'est ensuite imposé comme un invariant fondamental dans les travaux consacrés aux réseaux euclidiens dans une perspective cryptographique (voir [CDLP13], [DRSD14], [DR16], [RSD17b], et notamment [APSD18] pour des résultats et des références récentes).

5.1. Degré, pentes et semi-stabilité des réseaux euclidiens

Dans l'analogie entre réseaux euclidiens et fibrés vectoriels sur une courbe C, le rang des premiers correspond évidemment au rang des seconds, et le degré d'Arakelov (1.6) (resp. la pente (1.7)) au degré et la pente. L'additivité (1.9) du degré d'Arakelov dans les suites exactes courtes admissibles est analogue à l'additivité (4.1) du degré des fibrés vectoriels sur les courbes.

Aux morphismes $\varphi : E_1 \longrightarrow E_2$ de faisceaux de $\mathcal{O}_C$-modules entre deux fibrés vectoriels E_1 et E_2 sur C correspondent, deux réseaux euclidiens $\overline{E}_1 := (E_1, \|.\|_1)$ et $\overline{E}_2 := \overline{E}_2, \|.\|_2)$ étant donnés, les morphismes de $\mathbb{Z}$-modules $\varphi : E_1 \longrightarrow E_2$ tels que, pour tout $x \in E_{1,\mathbb{R}}$, on ait : $\|\varphi(x)\|_2 \leqslant \|x\|_1$. L'existence d'un morphisme tel que $\varphi_\mathbb{Q} : E_{1,\mathbb{Q}} \longrightarrow E_{2,\mathbb{Q}}$ soit un isomorphisme implique l'inégalité

$$\widehat{\deg}\, \overline{E}_1 \leqslant \widehat{\deg}\, \overline{E}_2$$

entre degrés d'Arakelov.

Bien entendu, alors que le degré des fibrés vectoriels prend des valeurs entières, le degré d'Arakelov des réseaux prend des valeurs réelles arbitraires.

Dans sa note [Stu76], Stuhler a observé que le degé d'Arakelov satisfait aussi à une propriété de sous-addivité analogue à (4.3) et que cela permet d'associer à tout réseau euclidien une filtration canonique, à la Harder-Narasimhan.

Précisément, si $\overline{E} := (E, \|.\|)$ est un réseau euclidien, alors, pour tout couple (F_1, F_2) de sous-$\mathbb{Z}$-modules de E, l'inégalité suivante est satisfaite :

$$\widehat{\deg}\,\overline{F_1 \cap F_2} + \widehat{\deg}\,\overline{F_1 + F_2} \geqslant \widehat{\deg}\,\overline{F}_1 + \widehat{\deg}\,\overline{F}_2. \tag{5.3}$$

En effet, la suite exacte courte de $\mathbb{Z}$-modules

$$0 \longrightarrow F_1 \cap F_2 \longrightarrow F_1 \oplus F_2 \longrightarrow F_1 + F_2 \longrightarrow 0,$$

définie par l'application somme de $F_1 \oplus F_2$ vers $F_1 + F_2$, détermine un isomorphisme de $\mathbb{Z}$-modules libres de rang 1 :

$$\varphi : \Lambda^{\max} F_1 \otimes \Lambda^{\max} F_2 \simeq \Lambda^{\max}(F_1 \oplus F_2) \xrightarrow{\sim} \Lambda^{\max}(F_1 \cap F_2) \otimes \Lambda^{\max}(F_1 + F_2),$$

et par définition du degré d'Arakelov, on a :

$$\widehat{\deg}\,\overline{F_1 \cap F_2} + \widehat{\deg}\,\overline{(F_1 + F_2)} - \widehat{\deg}\,\overline{F}_1 + \widehat{\deg}\,\overline{F}_2 = \log \|\varphi_{\mathbb{R}}\|^{-1},$$

où $\|\varphi_{\mathbb{R}}\|$ désigne la norme de l'isomorphisme

$$\varphi_{\mathbb{R}} : \Lambda^{\max} F_{1,\mathbb{R}} \otimes_{\mathbb{R}} \Lambda^{\max} F_{2,\mathbb{R}} \xrightarrow{\sim} \Lambda^{\max}(F_{1,\mathbb{R}} \cap F_{2,\mathbb{R}}) \otimes_{\mathbb{R}} \Lambda^{\max}(F_{1,\mathbb{R}} + F_{2,\mathbb{R}})$$

lorsque l'on muni les puissances extérieures de $F_{1,\mathbb{R}}, \ldots$ des structures euclidiennes qui se déduisent de celles définies par la norme euclidienne $\|.\|$ sur $E_{\mathbb{R}}$. Or cette norme[(10)] est toujours $\leqslant 1$, comme on le voit en l'exprimant au moyen de bases orthonormées idoines de $F_{1,\mathbb{R}}$ et $F_{2,\mathbb{R}}$.

Lorsque les sous-$\mathbb{Z}$-modules F_1 et F_2 sont saturés dans E, $F_1 \cap F_2$ l'est encore et (5.3) implique aussitôt :

$$\widehat{\deg}\,\overline{F_1 \cap F_2} + \widehat{\deg}\,\overline{(F_1 + F_2)^{\mathrm{sat}}} \geqslant \widehat{\deg}\,\overline{F}_1 + \widehat{\deg}\,\overline{F}_2. \tag{5.4}$$

Si $\overline{E}$ est un réseau euclidien de rang $n > 0$, on peut alors appliquer le formalisme des pentes présenté dans l'appendice A à l'ensemble ordonné $(\mathcal{E}(E), \subseteq)$ des sous-$\mathbb{Z}$-modules de E muni de l'inclusion et aux fonctions $r := \mathrm{rk}$ et $d := (F \mapsto \widehat{\deg}\,\overline{F})$. La propriété de monotonie (1) de l'appendice A est en effet immédiate ; l'inégalité (5.3) établit la sous-additivité (2), et la finitude (3) découle de l'interprétation de $-\widehat{\deg}\,\overline{F}$, pour un sous-$\mathbb{Z}$-module saturé F de E, comme hauteur logarithmique du point de Plücker dans $\mathbb{P}(\Lambda^{\mathrm{rk}\,F} E_{\mathbb{Q}})$ associé au sous-$\mathbb{Q}$-vectoriel $F_{\mathbb{Q}}$ de $E_{\mathbb{Q}}$.

On attache ainsi à $\overline{E}$ une application

$$P_{\overline{E}} : [0, n] \longrightarrow \mathbb{R}$$

(10) Lorsque F_1 et F_2 sont de rang 1 et que $F_1 \cap F_2 = \{0\}$, cette norme est $|\sin \alpha|$, où α désigne l'angle des deux droites $F_{1,\mathbb{R}}$ et $F_{2,\mathbb{R}}$ dans l'espace euclidien $(E_{\mathbb{R}}, \|.\|)$. En général, $\|\varphi_{\mathbb{R}}\|$ admet une interprétation géométrique analogue ; *cf.* [Sch67], Part II.

concave et affine sur chaque intervalle $[i-1,i]$, $1 \leqslant i \leqslant \operatorname{rk} E$. Le graphe de $\overline{E}$ est le *polygone canonique* de $\overline{E}$; ses sommets sont les images par l'application $(\operatorname{rk}, \widehat{\deg})$ des sous-réseaux $\overline{E}_i$, $0 \leqslant i \leqslant N$, associés à une filtration canonique de E,

$$E_0 = 0 \subsetneq E_1 \subsetneq \cdots \subsetneq E_N = E,$$

par des sous-$\mathbb{Z}$-modules saturés. On obtient encore $P_{\overline{E}}$ et la filtration canonique en appliquant le formalisme des pentes au sous-ensemble $\mathcal{E}_{\mathrm{sat}}(E)$ de $\mathcal{E}(E)$ défini comme l'ensemble des sous-$\mathbb{Z}$-modules saturés de E.

Comme dans la situation géométrique, le réseau euclidien $\overline{E}$ est dit *semi-stable* lorsque tout sous-$\mathbb{Z}$-module (ou de façon équivalente, tout sous-$\mathbb{Z}$-module saturé) non nul F de E satisfait à

$$\widehat{\mu}(\overline{F}) \leqslant \widehat{\mu}(\overline{E}),$$

c'est-à-dire lorsque la filtration canonique de E est triviale, ou encore lorsque son polygone canonique est un segment de droite. La semi-stabilité d'un réseau euclidien $\overline{E}$ est inchangée par changement d'échelle, c'est-à-dire lorsque l'on remplace $\overline{E}$ par $\overline{E} \otimes \overline{\mathcal{O}}(\lambda)$, $\lambda \in \mathbb{R}$.

Ici encore, l'additivité du degré d'Arakelov dans les suites exactes courtes admissibles (1.9) montre que les réseaux euclidiens sous-quotients $\overline{E_i/E_{i-1}}$ attachés à la filtration canonique de E sont semi-stables, de pentes strictement décroissantes :

$$\widehat{\mu}(\overline{E}_1) > \widehat{\mu}(\overline{E_2/E_1}) > \ldots > \mu(\overline{E_N/E_{N-1}}).$$

Pour tout $k \in \{1, \ldots, n\}$, la k-ième pente de $\overline{E}$ est la pente de $P_{\overline{E}}$ sur $[k-1,k]$:

$$\widehat{\mu}_k(\overline{E}) := P_{\overline{E}}(k) - P_{\overline{E}}(k-1).$$

On a par construction[(11)] :

$$\widehat{\mu}_1(\overline{E}) \geqslant \ldots \geqslant \widehat{\mu}_n(\overline{E})$$

et

$$\sum_{i=i}^{n} \widehat{\mu}_i(\overline{E}) = \widehat{\deg}\, \overline{E}.$$

On définit encore :

$$\widehat{\mu}_{\max}(\overline{E}) := \widehat{\mu}_1(\overline{E}) = \widehat{\mu}(\overline{E}_1) = \max_{0 \neq F \subset E} \widehat{\mu}(\overline{F})$$

et

$$\widehat{\mu}_{\min}(\overline{E}) := \widehat{\mu}_n(\overline{E}) = \widehat{\mu}(\overline{E}_N/\overline{E}_{N-1}) = \min_{F = F^{\mathrm{sat}} \subsetneq E} \widehat{\mu}(\overline{E/F}).$$

On voit facilement, en utilisant encore l'additivité du degré d'Arakelov, qu'une somme directe de réseaux euclidiens semi-stables de même pente μ est encore semi-stable de pente μ.

[(11)] Cette suite est la suite des pentes $\widehat{\mu}(\overline{E_i/E_{i-1}})$ de la filtration canonique, chacune répétée $\operatorname{rk}(E_i/E_{i-1})$-fois.

Les pentes des sommes directes de réseaux euclidiens de rang 1 se calculent aisément. Avec les notations du paragraphe 2.2, il vient :

$$\widehat{\mu}_k(\bigoplus_{i=1}^{n} \overline{\mathcal{O}}(t_i)) = t_k. \tag{5.5}$$

Les égalités (2.2) et (5.5) montrent ainsi que, lorsque $\overline{E}$ est une somme directe de réseaux euclidiens de rang 1, $\widehat{\mu}_k(\overline{E})$ et $\log \lambda_k(\overline{E})^{-1}$ coincident. Par ailleurs, la validité de la proposition 2.1 lorsque $\psi = \widehat{\mu}$ entraîne aisément sa validité pour chacune des pentes $\widehat{\mu}_i$, $1 \leqslant i \leqslant n$.

En faisant appel à la théorie de la réduction, comme dans le paragraphe 2.5, on en déduit que *pour tout entier $n > 0$, il existe $c(n) \in \mathbb{R}_+$, tel que, pour tout réseau euclidien $\overline{E}$ de rang n et tout $i \in \{1, \dots, n\}$, on ait* :

$$|\widehat{\mu}_i(\overline{E}) - \log \lambda_i(\overline{E})^{-1}| \leqslant c(n). \tag{5.6}$$

(Voir par exemple [Bor05]). Les pentes successives de $\overline{E}$ apparaissent ainsi comme des avatars des (logarithmes des inverses) de ses minima successifs.

Les propriétés formelles des pentes sont toutefois plus satisfaisantes que celles de ces derniers. Par exemple, en utilisant la compatibilité du degré d'Arakelov et des suites exactes courtes admissibles à la dualité (*cf.* 1.3.1 et 1.3.2), on obtient par un argument analogue à celui conduisant à (4.6) :

$$P_{\overline{E}^\vee}(x) = P_{\overline{E}}(n - x) - \widehat{\deg}\, \overline{E}.$$

Ainsi les inégalités de transférence du type (1.15) reliant les minima successifs d'un réseau euclidien et de son dual prennent la forme d'égalités entre pentes :

$$\widehat{\mu}_i(\overline{E}^\vee) = -\widehat{\mu}_{n+1-i}(\overline{E}) \quad \text{pour tout } i \in \{1, \dots, n\}.$$

En particulier, en faisant $i = n$, on trouve :

$$\widehat{\mu}_{\min}(\overline{E}^\vee) = -\widehat{\mu}_{\max}(\overline{E}).$$

Il est immédiat que, pour tout entier $n > 0$, la partie $\mathcal{S}t_n$ de $\mathcal{R}_n$ paramètrant les réseaux euclidiens semi-stables est fermée. Compte-tenu de (5.6) (avec $i = 1$), le critère de Mahler (théorème 2.4) montre que l'intersection

$$\mathcal{S}t_n^0 := \mathcal{S}t_n \cap \mathcal{R}_n^0,$$

qui paramètre les réseaux euclidiens semi-stables de rang n et de pente nulle, est *compacte*. Il est facile de décrire le bord de $\mathcal{S}t_n$ dans $\mathcal{R}_n$ (voir par exemple [Gra84]) :

Proposition 5.1. — *Soit $\overline{E}$ un réseau euclidien de rang $n > 0$ semi-stable. Les conditions suivantes sont équivalentes :*

(1) *La classe $[\overline{E}]$ de $\overline{E}$ dans $\mathcal{R}_n$ appartient au bord $\partial\mathcal{S}t_n := \mathcal{S}t_n \backslash \mathring{\mathcal{S}t}_n$ du fermé $\mathcal{S}t_n$.*
(2) *Il existe un sous-$\mathbb{Z}$-module saturé F dans E tel que*

$$0 < \operatorname{rk} F < \operatorname{rk} E \quad \textit{et} \quad \widehat{\mu}(\overline{F}) = \widehat{\mu}(\overline{E}).$$

Lorsque ces conditions sont réalisés, $\overline{F}$ et $\overline{E/F}$ sont des réseaux euclidiens semi-stables (de pente $\widehat{\mu}(\overline{E})$).

Cet énoncé reste valable lorsque l'on remplace $\mathcal{R}_n$ (resp. $\mathcal{S}t_n$) par $\mathcal{R}_n^0$ (resp. $\mathcal{S}t_n^0$). (On a alors $\widehat{\mu}(\overline{E}) = \widehat{\mu}(\overline{E/F}) = \widehat{\mu}(\overline{E}) = 0$.)

Signalons aussi que les domaines de l'espace $\mathcal{R}_n$ définis par des inégalités sur les pentes des réseaux euclidiens apparaissent dans les travaux sur la formule des traces d'Arthur-Selberg, dans le contexte plus général des quotients arithmétiques associés à des $\mathbb{Q}$-groupes réductifs arbitraires. En fait, les constructions géométriques qui sous-tendent les opérations de troncature mises en oeuvre dans la formule des traces apparaissent comme une généralisation du formalisme des pentes décrit dans ce paragraphe (voir notamment [Art78] (Section 6) et comparer à [Gra86] et [HS97] ; voir aussi [Cas04]).

Mentionnons enfin les beaux résultats de Shapira et Weiss ([SW14], [SW16]) concernant les propriétés géométriques et dynamiques du lieu semi-stable $\mathcal{S}t_n^0$ dans $\mathcal{R}_n^0$ et leurs applications à des questions classiques de géométrie des nombres.

5.2. Les invariants $h^0_{\mathrm{Ar}}(\overline{E})$, $h^0_\theta(\overline{E})$ et $h^1_\theta(\overline{E})$

Dans la littérature apparaissent plusieurs invariants des réseaux euclidiens qui jouent le rôle de la dimension $h^0(C,E)$ de l'espace des sections d'un fibré vectoriel E sur une courbe C ou de la dimension $h^1(C,E)$ de son premier groupe de cohomologie.

5.2.1. *L'invariants $h^0_{\mathrm{Ar}}(\overline{E})$.* — Avec les notations de la section 4, le k-vectoriel $H^0(C,E)$ s'identifie au k-vectoriel $\mathrm{Hom}_{\mathcal{O}_C}(\mathcal{O}_C,E)$ des morphismes de faisceaux de $\mathcal{O}_C$-modules de $\mathcal{O}_C$ vers E. Lorsque le corps k est fini, de cardinal q, c'est un ensemble fini et l'on a :

$$h^0(C,E) = \dim_k \mathrm{Hom}_{\mathcal{O}_C}(\mathcal{O}_C,E) = \frac{\log|\mathrm{Hom}_{\mathcal{O}_C}(\mathcal{O}_C,E)|}{\log q}.$$

Cela conduit à considérer l'ensemble des morphismes de $\overline{\mathcal{O}}(0) = (\mathbb{Z},|.|)$ vers un réseau euclidien $\overline{E} := (E,\|.\|)$ — il s'identifie à l'ensemble fini $E\cap\overline{B}_{\|.\|}(0,1)$ des points du réseau dans la boule unité de $(E_{\mathbb{R}},\|.\|)$ — puis à poser :

$$h^0_{\mathrm{Ar}}(\overline{E}) := \log|E\cap\overline{B}_{\|.\|}(0,1)|. \tag{5.7}$$

Cette définition apparaît implicitement chez Weil [Wei39] et Arakelov [Ara75] et plus explicitement dans les présentations de la géométrie d'Arakelov dans [Szp85] et [Man85] (voir aussi [GMS91]).

5.2.2. *Les invariants $h^0_\theta(\overline{E})$ et $h^1_\theta(\overline{E})$.* — On peut aussi former la série thêta $\theta_{\overline{E}}$ associée à un réseau euclidien $\overline{E} := (E,\|.\|)$:

$$\theta_{\overline{E}}(t) := \sum_{v\in E} e^{-\pi t\|v\|^2} \quad \text{pour tout } t\in\mathbb{R}_+^*,$$

(*cf.* 1.3.3 *supra*) et poser :

$$h^0_\theta(\overline{E}) := \log\theta_{\overline{E}}(1) = \log\sum_{v\in E} e^{-\pi\|v\|^2} \in \mathbb{R}_+. \tag{5.8}$$

Le fait que l'invariant $h^0_\theta(\overline{E})$ ainsi associé à un réseau euclidien soit l'analogue de l'invariant $h^0(C,E)$ associé à un fibré vectoriel sur une courbe est une découverte de l'école de théorie des nombres allemande, et remonte au moins à F. K. Schmidt. En effet, si l'on compare les démonstrations, dues respectivement à Hecke ([Hec17]) et à Schmidt ([Sch31]) du prolongement analytique et de l'équation fonctionnelle de la fonction zêta associée à un corps de nombres et au corps de fonctions $K := k(C)$ associé à une courbe (projective, lisse, géométriquement connexe) sur un corps fini de cardinal q, on voit que les quantités

$$\sum_{v\in E} e^{-\pi\|v\|^2}$$

associées à une réseau euclidien $\overline{E} := (E, \|.\|)$ jouent le même rôle que les expressions

$$q^{h^0(C,E)}.$$

Un point clé de la démonstration de Schmidt est en fait que la formule de Riemann-Roch pour un fibré (en droites) sur une courbe y joue un rôle comparable à la formule de Poisson (1.13), qui relie $\theta_{\overline{E}}$ et $\theta_{\overline{E}^\vee}$.

Cette formule, évaluée en $t = 1$, devient en effet :

$$\theta_{\overline{E}}(1) = (\mathrm{covol}(\overline{E}))^{-1}\theta_{\overline{E}^\vee}(1)$$

et peut encore s'écrire :

$$h^0_\theta(\overline{E}) - h^0_\theta(\overline{E}^\vee) = \widehat{\deg}\,\overline{E}. \tag{5.9}$$

Cette égalité est formellement analogue à la formule de Riemann-Roch sur une courbe C de genre 1 (donc de fibré canonique trivial), et conduit à poser :

$$h^1_\theta(\overline{E}) := h^0_\theta(\overline{E}^\vee),$$

de sorte que (5.9) deviennent la formule de « Poisson-Riemann-Roch » :

$$h^0_\theta(\overline{E}) - h^1_\theta(\overline{E}) = \widehat{\deg}\,\overline{E}. \tag{5.10}$$

Au cours des dernières décennies, ces définitions sont apparues notamment dans le journal mathématique de Quillen [Qui] (voir les entrées des 24/12/1971, 26/04/1973 et 01/04/1983), dans [Roe93], [Mor95], et plus récemment dans les articles de van der Geer et Schoof [vdGS00] et Groenewegen [Gro01].

5.2.3. *Varia.* — Il est rassurant de savoir que l'on peut réconcilier les définitions (5.7) et (5.8) des invariants $h^0_{\mathrm{Ar}}(\overline{E})$ et $h^0_\theta(\overline{E})$, l'un et l'autre candidats à tenir la place de $h^0(C,E)$ pour les réseaux euclidiens.

En premier lieu, pour tout réseau euclidien $\overline{E}$ de rang $n > 0$, on peut établir les inégalités :

$$-\pi \leqslant h^0_\theta(\overline{E}) - h^0_{\mathrm{Ar}}(\overline{E}) \leqslant (n/2)\log n + \log(1 - 1/2\pi)^{-1}.$$

La première inégalité est immédiate, et la seconde se démontre au moyen des techniques de Banaszczyk présentées en section 3 (voir [Bos15], section 3).

En outre, on peut relier $h^0_\theta(\overline{E})$ à une version « stable » de l'invariant $h^0_{\mathrm{Ar}}(\overline{E})$ et établir l'énoncé suivant par un argument de grandes déviations :

PROPOSITION 5.2 ([Bos15], Theorem 3.4.5). — *Pour tout $t \in \mathbb{R}_+^*$, posons :*

$$h^0_{\mathrm{Ar}}(\overline{E}, t) := \log |\{v \in E \mid \|v\|^2 \leqslant t\}|.$$

Alors, pour tout $t \in \mathbb{R}_+^*$, la limite suivante existe dans $\mathbb{R}_+$:

$$\tilde{h}^0_{\mathrm{Ar}}(\overline{E}, t) := \lim_{n \to +\infty} \frac{1}{n} h^0_{\mathrm{Ar}}(\overline{E}^{\oplus n}, nt).$$

De plus, les fonctions $\log \theta_{\overline{E}}(\beta) (= h^0_\theta(\overline{E} \otimes \overline{\mathcal{O}}((1/2) \log \beta^{-1}))$ et $\tilde{h}^0_{\mathrm{Ar}}(\overline{E}, t)$ se déduisent l'une de l'autre par dualité de Legendre ; à savoir, pour tout $x \in \mathbb{R}_+^*$, on a :

$$\tilde{h}^0_{\mathrm{Ar}}(\overline{E}, x) = \inf_{\beta > 0} (\pi \beta x + \log \theta_{\overline{E}}(\beta))$$

et, pour tout $\beta \in \mathbb{R}_+^*$:

$$\log \theta_{\overline{E}}(\beta) = \sup_{x > 0} (\tilde{h}^0_{\mathrm{Ar}}(\overline{E}, x) - \pi \beta x).$$

Nous renvoyons à [Bos15], Chapter 3 et Appendix A, pour la démonstration et pour divers développements de ce résultat.

Rappelons aussi que les réseaux euclidiens ne sont que le cas particulier, correspondant au corps $K = \mathbb{Q}$, des fibrés vectoriels hermitiens sur $\operatorname{Spec} \mathcal{O}_K$, attachés à un corps de nombres K. L'analogie entre fibrés vectoriels sur une courbe et réseaux euclidiens s'étend en une analogie entre fibrés vectoriels sur une courbe et fibrés vectoriels sur $\operatorname{Spec} \mathcal{O}_K$, où K est un corps de nombres arbitraire. Cela constitue en fait son cadre naturel : travailler avec des corps de nombres K arbitraires correspond à considérer des courbes C de genre $g \geqslant 1$ quelconques. Les invariants $h^i_\theta(\overline{E})$ s'étendent à ce cadre (qui était déjà en substance celui de [Hec17]). Nous renvoyons à [Bos15], Chapter 2, pour leur étude dans cette situation plus générale.

Soulignons enfin que les séries thêta (1.14) associées aux réseaux euclidiens apparaissent dans divers domaines des mathématiques et de la physique mathématique, et ont donné lieu à de multiples travaux, dans des perspectives très diverses. Citons par exemple les travaux sur les valeurs extrémales des fonctions thêta, inspirés par la théorie classique des formes modulaires ou automorphes (sur lesquels on pourra consulter [SS06] et ses références), les travaux sur le « Gaussian core model » , motivés par l'étude des empilements de sphères et la physique statistique ([CdCI16]) et divers travaux de cristallographie et de physique du solide (voir par exemple [BP17]).

5.3. Les analogies entre $h^0_\theta(\overline{E})$ et $h^0(C, E)$

Une différence, qui peut sembler de taille, entre les invariants $h^0_\theta(\overline{E})$ et $h^1_\theta(\overline{E})$ des réseaux euclidiens et des dimensions $h^0(C, E)$ et $h^1(C, E)$ des groupes de cohomologie des fibrés vectoriels est que les premiers sont réels, alors que ces derniers sont entiers, et que, lorsque $\overline{E}$ est de rang non nul, les premiers ne sont jamais nuls.

Ceci étant, les analogies entre les propriétés des uns et des autres sont particulièrement frappantes. Nous allons en décrire trois, par ordre chronologique et de difficulté croissante.

5.3.1. *Comportement asymptotique de* $\log \theta_{\overline{E}}$. — À partir de l'égalité

$$\int_{E_{\mathbb{R}}} e^{-\pi\|x\|^2}\, dm_{\overline{E}}(x) = 1,$$

en approchant l'intégrale par des « sommes de Riemann » sur le réseau $\sqrt{t}E$, où $t \in \mathbb{R}_+^*$ tend vers 0, on obtient :

$$\lim_{t \longrightarrow 0_+} \sqrt{t}^{\,\mathrm{rk}\, E} \operatorname{covol}(\overline{E}) \sum_{v \in E} e^{-\pi t\|v\|^2} = 1,$$

ou encore :

$$\log \theta_{\overline{E}}(t) = -(\mathrm{rk}\, E)/2 \log t + \widehat{\deg}\, \overline{E} + o(1) \quad \text{quand } t \longrightarrow 0_+. \tag{5.11}$$

En posant $\lambda = -1/2 \log t$, on obtient donc :

$$h^0_\theta(\overline{E} \otimes \overline{\mathcal{O}}(\lambda)) = \mathrm{rk}\, E\, \lambda + \widehat{\deg}\, \overline{E} + \varepsilon(\lambda) \quad \text{avec } \lim_{\lambda \to +\infty} \varepsilon(\lambda) = 0.$$

Ainsi reformulée, l'expression asymptotique (5.11) de $\theta_{\overline{E}}(t)$ près de 0 devient l'analogue de l'expression (4.11) pour le « polynôme de Hilbert » d'un fibré vectoriel sur une courbe de genre $g = 1$.

L'expression (5.11) est aussi une conséquence de la formule de Poisson (1.13), qui montre en outre que le terme d'erreur $\varepsilon(\lambda)$ décroit extrêmement rapidement à l'infini : il existe $c \in \mathbb{R}_+^*$ tel que, lorsque $\lambda \longrightarrow +\infty$,

$$\varepsilon(\lambda) = O(e^{-ce^{\lambda^2}}).$$

5.3.2. *Suites exactes courtes admissibles et invariants thêta.* — Une seconde analogie entre les propriétés de $h^0_\theta(\overline{E})$ et de $h^0(C, E)$ concerne leur compatibilité avec les sommes directes et, plus généralement, les suites exactes courtes :

Proposition 5.3. — 1) *Si* $\overline{E}_1$ *et* $\overline{E}_2$ *sont deux réseaux euclidiens, on a :*

$$h^0_\theta(\overline{E}_1 \oplus \overline{E}_2) = h^0_\theta(\overline{E}_1) + h^0_\theta(\overline{E}_2). \tag{5.12}$$

2) *Pour toute suite exacte courte admissible de réseaux euclidiens*

$$0 \longrightarrow \overline{F} \xrightarrow{\ i\ } \overline{E} \xrightarrow{\ p\ } \overline{E/F} \longrightarrow 0,$$

on a :

$$h^0_\theta(\overline{E}) \leqslant h^0_\theta(\overline{F}) + h^0_\theta(\overline{E/F}). \tag{5.13}$$

L'égalité (5.12) est immédiate. L'inégalité (5.13) découle aisément de (3.1), qui montre que, pour tout $\alpha \in E/F$,

$$\sum_{v \in p^{-1}(\alpha)} e^{-\pi\|v\|^2_{\overline{E}}} \leqslant e^{-\pi\|\alpha\|^2_{\overline{E/F}}} \sum_{f \in F} e^{-\pi\|f\|^2_{\overline{F}}}$$

et a été observée par Quillen ([Qui], entrée du 26/04/1973) et Groenewegen ([Gro01], Lemma 5.3).

5.3.3. *Un théorème de Regev et Stephens-Davidowitz.* — Reprenons les notations de la section 4. Soient E un fibré vectoriel sur C et F_1 et F_2 deux sous-faisceaux cohérents de E. On peut former une suite exacte courte de fibrés vectoriels sur C :

$$0 \longrightarrow F_1 \cap F_2 \longrightarrow F_1 \oplus F_2 \longrightarrow F_1 + F_2 \longrightarrow 0,$$

où le morphisme de $F_1 \oplus F_2$ vers $F_1 + F_2$ est l'application somme. On en déduit aussitôt une suite exacte de k-vectoriels de dimension finie :

$$0 \longrightarrow H^0(C, F_1 \cap F_2) \longrightarrow H^0(C, E_1) \oplus H^0(C, E_2) \longrightarrow H^0(C, F_1 + F_2),$$

puis l'inégalité suivante entre leurs dimensions :

$$h^0(C, F_1) + h^0(C, F_2) \leqslant h^0(C, F_1 \cap F_2) + h^0(C, F_1 + F_2).$$

En réponse à une question de McMurray Price (voir [MP17]), Regev et Stephens-Davidowitz ont montré qu'un telle inégalité reste valide *ne varietur* pour les réseaux euclidiens et leurs invariants h^0_θ :

Théorème 5.4 ([RSD17a]). — *Soit $\overline{E}$ un réseau euclidien et soient F_1 et F_2 deux sous-$\mathbb{Z}$-modules de E. On a alors :*

$$h^0_\theta(\overline{F}_1) + h^0_\theta(\overline{F}_2) \leqslant h^0_\theta(\overline{F_1 \cap F_2}) + h^0_\theta(\overline{F_1 + F_2}).$$

Nous renvoyons à [RSD17a] pour la démonstration, élémentaire mais extrêmement ingénieuse.

5.4. Les invariants $s^0_{\theta,\varepsilon}(\overline{E})$ et $s^1_{\theta,\varepsilon}(\overline{E})$

5.4.1. *Définitions.* — Soit $\overline{E}$ un réseau euclidien de rang > 0. Il est immédiat que la fonction $\theta_{\overline{E}}$ est un difféomorphisme analytique décroissant de $\mathbb{R}^*_+$ sur $]1, +\infty[$. Pour tout $\varepsilon > 0$, on peut donc définir

$$s^0_{\theta,\varepsilon}(\overline{E}) := \frac{1}{2} \log \theta^{-1}_{\overline{E}}(1 + \varepsilon)$$

et

$$s^1_{\theta,\varepsilon}(\overline{E}) := \frac{1}{2} \log \theta^{-1}_{\overline{E}^\vee}(1 + \varepsilon).$$

Ainsi, pour tout $\lambda \in \mathbb{R}$, on a :

$$\lambda > s^0_{\theta,\varepsilon}(\overline{E}) \Longleftrightarrow \theta_{\overline{E}}(e^{2\lambda}) < 1 + \varepsilon \Longleftrightarrow h^0_\theta(\overline{E} \otimes \overline{\mathcal{O}}(-\lambda)) < \log(1 + \varepsilon)$$

et

$$\lambda > s^1_{\theta,\varepsilon}(\overline{E}) \Longleftrightarrow \theta_{\overline{E}^\vee}(e^{2\lambda}) < 1 + \varepsilon \Longleftrightarrow h^1_\theta(\overline{E} \otimes \overline{\mathcal{O}}(\lambda)) < \log(1 + \varepsilon).$$

De plus on a :

$$s^1_{\theta,\varepsilon}(\overline{E}) = s^0_{\theta,\varepsilon}(\overline{E}^\vee)$$

et, pour tout $\delta \in \mathbb{R}$,

$$s^0_{\theta,\varepsilon}(\overline{E} \otimes \overline{\mathcal{O}}(\delta)) = s^0_{\theta,\varepsilon}(\overline{E}) + \delta \quad \text{et} \quad s^1_{\theta,\varepsilon}(\overline{E} \otimes \overline{\mathcal{O}}(\delta)) = s^1_{\theta,\varepsilon}(\overline{E}) - \delta.$$

Comme indiqué dans l'introduction de cette section, l'invariant $s^1_{\theta,\varepsilon}(\overline{E})$ est une version logarithmique du « smoothing parameter » $\eta_\varepsilon(\overline{E})$ introduit par Micciancio et Regev dans [MR07] (*cf.* (5.1) et (5.2) *supra*).

Les invariants $\eta_\varepsilon(\overline{E})$ et $s^i_{\theta,\varepsilon}$ dépendent du paramètre ε. Le choix de ce paramètre est anodin, du moins pour les applications qui en sont décrites dans cet exposé. En effet, si ε et ε' sont deux réels dans $]0,1[$, il existe $c(\varepsilon,\varepsilon') \in \mathbb{R}_+$ tel que, pour tout réseau euclidien $\overline{E}$ de rang non nul, on ait :

$$|s^i_{\theta,\varepsilon'}(\overline{E}) - s^i_{\theta,\varepsilon}(\overline{E})| \leqslant c(\varepsilon,\varepsilon').$$

Cela résulte de l'énoncé plus précis suivant :

Proposition 5.5 ([CDLP13], Section 2). — *Pour tout réseau euclidien $\overline{E}$ de rang non nul, $s^i_{\theta,\varepsilon}$ est une fonction décroissante de $\varepsilon \in \mathbb{R}^*_+$, et $s^i_{\theta,\varepsilon} - (1/2)\log\log\varepsilon^{-1}$ est une fonction croissante de $\varepsilon \in]0,1[$.*

Démonstration. — La première assertion est évidente. La seconde découle de l'inégalité, valable pour tout $x \in \mathbb{R}^*_+$ et tout $t \in [1,+\infty[$,

$$\theta_{\overline{E}}(tx) - 1 \leqslant (\theta_{\overline{E}}(x) - 1)^t.$$

□

Dans la suite, comme dans [RSD17b], nous choisirons $\varepsilon = 1/2$.

5.4.2. *Reformulation du théorème 1.3.* — En terme des invariants $s^0_{\theta,1/2}(\overline{E})$ et $s^1_{\theta,1/2}(\overline{E})$, on peut reformuler le théorème 1.3 de la manière suivante :

Théorème 5.6. — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$, on a :*

$$s^0_{\theta,1/2}(\overline{E}) \leqslant \widehat{\mu}_{\max}(\overline{E}) + t(n), \tag{5.14}$$

où l'on a posé $t(n) := \log[10(\log n + 2)]$.

De façon équivalente, on a :

$$s^1_{\theta,1/2}(\overline{E}) \leqslant -\widehat{\mu}_{\min}(\overline{E}) + t(n). \tag{5.15}$$

Le théorème 1.3 apparaît ainsi comme un avatar, concernant les réseaux euclidiens, de la seconde inégalité dans l'encadrement (4.10) de l'invariant $s^0(E)$ associé à une fibré vectoriel E sur une courbe. Observons que la première inégalité dans (4.10) se transpose aussitôt, en mimant sa démonstration, aux réseaux euclidiens : de la minoration

$$h^0_\theta(\overline{E}) \geqslant \widehat{\mu}_{\max}(\overline{E})^+,$$

conséquence de la « formule de Poisson-Riemann-Roch » (5.10) valable pour tout réseau euclidien $\overline{E}$ de rang > 0, on déduit aisément que, pour tout $\varepsilon \in \mathbb{R}^*_+$,

$$\widehat{\mu}_{\max}(\overline{E}) - \log(1+\varepsilon) \leqslant s^0_{\theta,\varepsilon}(\overline{E}). \tag{5.16}$$

Par dualité, on en déduit :

$$-\widehat{\mu}_{\min}(\overline{E}) - \log(1+\varepsilon) \leqslant s^1_{\theta,\varepsilon}(\overline{E}).$$

La dépendance en la dimension n du réseau $\overline{E}$ dans l'inégalité (5.14) est asymptotiquement d'un ordre de grandeur optimal. En effet, lorsque $\overline{E}$ est le « réseau euclidien trivial de rang n » $\overline{\mathcal{O}}(0)^{\oplus n}$, défini par le réseau $\mathbb{Z}^n$ dans $\mathbb{R}^n$ muni de la norme standard $\|.\|_{\mathrm{st}}$, on voit aisément que $\widehat{\mu}_{\max}(\overline{E}) = 0$ ($\overline{E}$ est un réseau semi-stable de pente nulle) et que

$$s^0_{\theta,1/2}(\overline{E}) = (1/2)\log\log n + O(1) \quad \text{lorsque } n \longrightarrow +\infty.$$

5.4.3. *Les invariants $s^0_{\theta,\varepsilon}(\overline{E})$ et $s^1_{\theta,\varepsilon}(\overline{E})$ et la méthode de Banaszczyk.* — Les invariants $\eta_\varepsilon(\overline{E})$ et $\eta_\varepsilon(\overline{E}^\vee)$, ou de façon équivalente $s^1_{\theta,\varepsilon}(\overline{E})$ et $s^0_{\theta,\varepsilon}(\overline{E})$, se révèlent particulièrement utiles pour formuler les inégalités sur les invariants classiques des réseaux euclidiens obtenues par la méthode de Banszczyk.

Les deux propositions suivantes illustrent ce principe.

Proposition 5.7 ([MR07], Lemma 3.2). — *Pour tout réseau euclidien de rang $n > 0$, on a :*

$$s^1_{\theta,2^{-n}}(\overline{E}) \leqslant (1/2)\log n + \log \lambda_1(\overline{E}^\vee)^{-1}. \tag{5.17}$$

Démonstration. — Si l'on pose

$$\mu := (1/2)\log n + \log \lambda_1(\overline{E}^\vee)^{-1},$$

l'inégalité (5.17) est équivalente à :

$$\theta_{\overline{E}^\vee \otimes \overline{\mathcal{O}}(-\mu)}(1) \leqslant 1 + 2^{-n}.$$

Or

$$\lambda_1(\overline{E}^\vee \otimes \overline{\mathcal{O}}(-\lambda)) = e^\lambda \, \lambda_1(\overline{E}^\vee) = \sqrt{n} > \sqrt{n/2\pi}.$$

Le corollaire (3.4) s'applique donc au réseau euclidien $\overline{E}^\vee \otimes \overline{\mathcal{O}}(-\lambda)$ et montre donc que :

$$\theta_{\overline{E}^\vee \otimes \overline{\mathcal{O}}(-\lambda)}(1) \leqslant (1 - \beta(\sqrt{2\pi})^n)^{-1}.$$

On conclut en observant que

$$\beta(\sqrt{2\pi}) = \sqrt{2\pi e}\, e^{-\pi} = 0,1786... < 1/4.$$

□

Proposition 5.8 ([RSD17b], Lemma 6.1). — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$, on a :*

$$\log R_{\mathrm{cov}}(\overline{E}) \leqslant \log(1 + \sqrt{n/2\pi}) + s^1_{\theta,1/2}(\overline{E}). \tag{5.18}$$

Démonstration. — Comme $\log R_{\mathrm{cov}}(\overline{E} \otimes \overline{\mathcal{O}}(\delta)) = \log R_{\mathrm{cov}}(\overline{E}) - \delta$ et $s^1_{\theta,\varepsilon}(\overline{E} \otimes \overline{\mathcal{O}}(\delta)) = s^1_{\theta,\varepsilon}(\overline{E}) - \delta$, il suffit de montrer que

$$R_{\mathrm{cov}}(\overline{E}) \leqslant 1 + \sqrt{n/2\pi}$$

lorsque $s^1_{\theta,1/2}(\overline{E}) \leqslant 0$, c'est-à-dire lorsque $\theta_{\overline{E}^\vee}(1) \leqslant 3/2$, ce que nous supposons désormais.

Clairement, nous pouvons aussi supposer que $R_{\mathrm{cov}}(\overline{E}) \geqslant \sqrt{n/2\pi}$, puis poser $R_{\mathrm{cov}}(\overline{E}) = \sqrt{n/2\pi}\tilde{R}$, avec $\tilde{R} \in [1, +\infty[$. L'inégalité (3.10) du corollaire (3.5) montre alors que

$$\beta(\tilde{R})^n \geqslant 2\theta_{\overline{E}^\vee}(1)^{-1} - 1 \geqslant 1/3.$$

Avec les notations du paragraphe 3.2, on en déduit que

$$\tilde{R} \leqslant \beta^{-1}(3^{-1/n}) =: t_n \leqslant 1 + \sqrt{(\log 3)n}.$$

On déduit que

$$R_{\mathrm{cov}}(\overline{E}) \leqslant \sqrt{n/2\pi} + \sqrt{\log 3/2\pi} \leqslant 1 + \sqrt{n/2\pi}.$$

□

6. À PROPOS DE LA DÉMONSTRATION DU THÉORÈME 1.3

Dans cette section, nous présentons les grandes lignes de la démonstration du théorème 1.3. Cette démonstration fait intervenir des résultats profonds de « géométrie gaussienne » concernant les propriétés des mesures gaussiennes des domaines convexes de $\mathbb{R}^n$, notamment leurs propriétés d'isopérimétrie. Nous renvoyons à l'article [Lat02] et l'exposé [Mau05] dans ce séminaire pour des présentations générales de ce sujet.

6.1. Préliminaires

6.1.1. *Mesures gaussiennnes et parties G-isotropes de* $\mathbb{R}^n$. — Pour tout entier naturel n et pour tout $s \in \mathbb{R}_+^*$, on définit la mesure de probabilité gaussienne γ_s sur $\mathbb{R}^n$ par l'égalité suivante, pour toute partie borélienne S de $E_{\mathbb{R}}$:

$$\gamma_s(S) := s^{-n} \int_S e^{-\pi\|x\|^2/s^2}\, dm(x),$$

où m désigne la mesure de Lebesgue sur $\mathbb{R}^n$. L'inégalité

$$e^{-\pi\|x\|^2/s^2} e^{-\pi\|y\|^2/s^2} \leqslant (1/2)(e^{-\pi\|y-x\|^2/s^2} + e^{-\pi\|y+x\|^2/s^2})$$

montre que, pour toute partie borélienne *symétrique* par rapport à l'origine S dans $\mathbb{R}^n$ et tout $y \in \mathbb{R}^n$, on a :

$$\gamma_s(S + y) \geqslant e^{-\pi\|y\|^2/s^2}\gamma_s(S). \tag{6.1}$$

Si $x = (x_i)_{1\leqslant i\leqslant n}$ est un élément de $\mathbb{R}^n$, vu comme vecteur colonne, on peut former la matrice symétrique

$$x \cdot {}^t x = (x_i x_j) \in M_n(\mathbb{R}).$$

On dira qu'une partie borélienne S de $\mathbb{R}^n$ est *G-isotrope de paramètre* s lorsque

$$\int_S x \cdot {}^t x\, d\gamma_s(x) := s^{-n} \int_S e^{-\pi\|x\|^2/s^2} x \cdot {}^t x\, dm(x) \in \mathbb{R}_+^* I_n,$$

où $I_n := (\delta_{ij})_{1\leqslant i,j\leqslant n}$. Cette notion est notamment étudiée dans [Bob11].

6.1.2. *Domaines de Voronoi.* — Rappelons que le domaine de Voronoi $\mathcal{V}(\overline{E})$ d'un réseau euclidien $\overline{E}$ est le polytope convexe symétrique

$$\mathcal{V}(\overline{E}) := \{x \in E_{\mathbb{R}} \mid \forall e \in E, \|x\| \leqslant \|x - e\|\}.$$

La géométrie de ces polytopes est l'un des objets d'étude des mémoires [Vor08b] et [Vor09]. Soulignons leur complexité lorsque $n := \operatorname{rk} E$ est grand : comme le montre Voronoi, $\mathcal{V}(\overline{E})$ possède au plus $(n+1)!$ sommets et $2(2^n - 1)$ faces de dimension $n-1$, et ces bornes sont atteintes. Le nombre de types combinatoires possibles pour ces polytopes, même dans la situation primitive considérée par Voronoi, augmente rapidement avec n.

Si F est une face de dimension $n-1$ de $\mathcal{V}(\overline{E})$, il existe un unique vecteur $v \in E\backslash\{0\}$ tel que F soit inclus dans l'hyperplan affine médiateur de 0 et v,

$$H_v := \{x \in E_{\mathbb{R}} \mid \|x\| = \|x - v\|\} = \{x \in E_{\mathbb{R}} \mid 2\langle v, x\rangle = \|v\|^2\}.$$

La face F contient $v/2$; la face opposée $-F$ est associée au vecteur $-v$:

$$-F \subset -H_v = H_{-v}$$

et se déduit aussi de F par la translation $(x \mapsto x - v)$:

$$F - v = -F.$$

Cela montre que F est invariante par la symétrie $(x \mapsto v - x)$ de centre $v/2$.

À un ensemble Lebesgue-négligeable (contenu dans $\partial\mathcal{V}(\overline{E})$) près, le domaine de Voronoi $\mathcal{V}(\overline{E})$ est un domaine fondamental pour l'action de E sur $E_{\mathbb{R}}$. De plus, si $\sigma : E_R/E \longrightarrow \mathcal{V}(\overline{E})$ est une section borélienne de la restriction à $\mathcal{V}(\overline{E})$ de l'application quotient $q : E_{\mathbb{R}} \longrightarrow E_R/E$, on a :

$$\|\sigma \circ q(x)\| \leqslant \|x\| \quad \text{pour tout } x \in E_{\mathbb{R}}.$$

On en déduit :

Proposition 6.1 ([RSD17b], Corollary 2.8). — *Pour tout domaine fondamental Δ pour l'action de E sur $E_{\mathbb{R}}$ et toute fonction $\varphi : \mathbb{R}_+ \longrightarrow \mathbb{R}_+$ borélienne décroissante, on a :*

$$\int_{\Delta} \varphi(\|x\|^2)\, dm_{\overline{E}}(x) \geqslant \int_{\mathcal{V}(\overline{E})} \varphi(\|x\|^2)\, dm_{\overline{E}}(x).$$

Il découle aussitôt de la définition du rayon de recouvrement que

$$R_{\mathrm{cov}}(\overline{E}) = \max_{x \in \mathcal{V}(\overline{E})} \|x\|.$$

(Ce maximum est atteint en un sommet de $R_{\mathrm{cov}}(\overline{E})$.)

La construction de $\mathcal{V}(\overline{E})$ est clairement compatible aux sommes directes de réseaux euclidiens : si $\overline{E}_1$ et $\overline{E}_2$ sont deux réseaux euclidiens, alors

$$\mathcal{V}(\overline{E}_1 \oplus \overline{\mathcal{E}}_2) = \mathcal{V}(\overline{E}_1) \oplus \mathcal{V}(\overline{E}_2).$$

En particulier, on a :

$$R_{\mathrm{cov}}(\overline{E}_1 \oplus \overline{\mathcal{E}}_2)^2 = R_{\mathrm{cov}}(\overline{E}_1)^2 + R_{\mathrm{cov}}(\overline{E}_2)^2.$$

Considérons enfin une suite exacte courte de réseaux euclidiens

$$0 \longrightarrow \overline{F} \overset{i}{\hookrightarrow} \overline{E} \overset{p}{\longrightarrow} \overline{E/F} \longrightarrow 0$$

et notons $s^\perp$ la section de $p_{\mathbb{R}} : E_{\mathbb{R}} \longrightarrow E_{\mathbb{R}}/F_{\mathbb{R}}$ d'image le supplémentaire orthogonal de $F_{\mathbb{R}}$ dans l'espace euclidien $(E_{\mathbb{R}}, \|.\|_{\overline{E}})$. L'isomorphisme

$$\begin{aligned} F_{\mathbb{R}} \oplus (E/F)_{\mathbb{R}} &\xrightarrow{\sim} E_{\mathbb{R}} \\ (x, y) &\longmapsto i(x) + s^\perp(y) \end{aligned}$$

est une isométrie qui envoie $\mathcal{V}(\overline{F}) \times \mathcal{V}(\overline{E/F})$ sur le polytope

$$\Delta := i(\mathcal{V}(\overline{F})) + s^\perp(\mathcal{V}(\overline{E/F})), \tag{6.2}$$

qui constitue ainsi un domaine fondamental (à une partie négligeable près) pour l'action de E sur$E_{\mathbb{R}}$.

Cette construction montre en outre que

$$R_{\mathrm{cov}}(\overline{E})^2 \leqslant \max_{z \in \Delta} \|z\|^2 = \max_{x \in \mathcal{V}(\overline{F})} \|x\|^2 + \max_{y \in \mathcal{V}(\overline{E/F})} \|y\|^2 = R_{\mathrm{cov}}(\overline{F})^2 + R_{\mathrm{cov}}(\overline{E/F})^2. \tag{6.3}$$

6.2. Mesure gaussienne des domaines de Voronoi

Les mesures gaussiennes γ_s et la notion de G-isotropie se transportent aussitôt sur l'espace euclidien sous-jacent à un réseau euclidien.

Soit en effet $\overline{E} := (E, \|.\|)$ un réseau euclidien. On définit la mesure de probabilité gaussienne γ_s sur $E_{\mathbb{R}}$ par l'égalité suivante, pour toute partie borélienne S de $E_{\mathbb{R}}$:

$$\gamma_s(S) := s^{-n} \int_S e^{-\pi \|x\|^2/s^2} \, dm_{\overline{E}}(x).$$

Pour tout $x \in E_{\mathbb{R}}$, on note $x \cdot {}^t x$ l'élément $x \otimes \langle x, . \rangle_{\overline{E}}$ de $\mathrm{End}_{\mathbb{R}}(E_{\mathbb{R}}) \simeq E_{\mathbb{R}} \otimes E_{\mathbb{R}}^\vee$, et l'on dit que S *est G-isotrope de paramètre s* lorsque

$$\int_S x \cdot {}^t x \, d\gamma_s(x) \in \mathbb{R}_+^* \mathrm{Id}_{E_{\mathbb{R}}}.$$

La masse $\gamma_s(\mathcal{V}(\overline{E}))$ du domaine de Voronoi $\mathcal{V}(\overline{E})$ de $\overline{E}$ relativement à la mesure γ_s est un invariant remarquable de $\overline{E}$, qui joue un rôle central dans la démonstration du théorème 1.3. Il a été considéré classiquement dans l'étude du « Gaussian channel coding problem » (voir [CS99], Chapter 3, Sections 1.3 and 1.4). Dans [CDLP13], Chung, Dadush, Liu et Peikert ont mis en évidence comment les mesures $\gamma_s(\mathcal{V}(\overline{E}))$ permettent de contrôler la fonction $\theta_{\overline{E}}$, ou de manière équivalente les invariants $\eta_\varepsilon(\overline{E}^\vee)$. Ils ont notamment établi l'inégalité suivante :

Proposition 6.2 ([CDLP13], Lemma 3.4). — *Pour tout réseau euclidien $\overline{E}$ et pour tout $s \in \mathbb{R}_+^*$, on a :*

$$\theta_{\overline{E}}(s^{-2}).\gamma_s(\mathcal{V}(\overline{E})) \leqslant 1. \tag{6.4}$$

Démonstration. — L'inégalité (6.1) montre que, pour tout $v \in E$, on a :

$$e^{-\pi s^{-2}\|v\|^2}\,\gamma_s(\mathcal{V}(\overline{E})) \leqslant \gamma_s(\mathcal{V}(\overline{E}) + v).$$

L'inégalité (6.4) en découle en sommant sur $v \in E$; en effet, comme $\mathcal{V}(\overline{E})$ est un domaine fondamental pour l'action de E sur $E_{\mathbb{R}}$, on a :

$$\sum_{v\in E} \gamma_s(\mathcal{V}(\overline{E}) + v) = \gamma_s(\mathbb{R}^n) = 1.$$

□

Les mesures $\gamma_s(\mathcal{V}(\overline{E}))$ sont par ailleurs « surmultiplicatives » relativement aux suites courtes admissibles :

Proposition 6.3 ([RSD17b], Proof of Prop. 4.14). — *Pour toute suite exacte courte admissible de réseaux euclidiens*

$$0 \longrightarrow \overline{F} \longrightarrow \overline{E} \longrightarrow \overline{E/F} \longrightarrow 0$$

et pour tout $s \in \mathbb{R}_+^*$, on a :

$$\gamma_s(\mathcal{V}(\overline{E})) \geqslant \gamma_s(\mathcal{V}(\overline{F})).\gamma_s(\mathcal{V}(\overline{E/F})). \tag{6.5}$$

Démonstration. — Appliquer la proposition 6.1 avec pour Δ le domaine fondamental (6.2) et pour φ la fonction $(t \mapsto e^{-\pi t/s^2})$. □

Le théorème 1.3 découlera de la minoration suivante de l'invariant $\gamma_{s^{-1}}(\mathcal{V}(\overline{E}))$ des réseaux euclidiens semi-stables :

Théorème 6.4. — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$ semi-stable tel que $\widehat{\deg}\,(\overline{E}) = 0$, on a :*

$$\gamma_{t(n)^{-1}}(\mathcal{V}(\overline{E})) \geqslant 2/3, \tag{6.6}$$

où l'on a posé :

$$t(n) := 10(\log n + 2).$$

La démonstration de ce théorème fait l'objet des trois prochains paragraphes. La démonstration du théorème 1.3 à partir du théorème 6.4 sera enfin exposée au paragraphe 6.6.

6.3. Différentiation des intégrales sur les domaines de Voronoi

Soit n un entier > 0 et soit $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ une fonction de classe C^1.

À tout réseau euclidien $\overline{E}$ de rang n, on peut associer le nombre réel

$$F(\overline{E}) := \mathrm{covol}(\overline{E})^{-1} \int_{\mathcal{V}(\overline{E})} f(\|x\|^2) dm_{\overline{E}}(x).$$

Si $\nu_{\overline{E}}$ désigne la mesure de Haar sur le groupe de Lie compact $E_{\mathbb{R}}/E$ normalisée par $\nu_{\overline{E}}(E_{\mathbb{R}}/E) = 1$ et si

$$\delta_{\overline{E}} : E_{\mathbb{R}}/E \longrightarrow \mathbb{R}_+$$

est la fonction définie par

$$\delta_{\overline{E}}([x]) := \min_{v \in E} \|x - v\|^2$$

pour tout $x \in E_{\mathbb{R}}$, on peut encore écrire :

$$F(\overline{E}) = \int_{E_{\mathbb{R}}/E} f \circ \delta_{\overline{E}} \, d\nu_{\overline{E}}. \tag{6.7}$$

Regev et Stephens-Davidowitz montrent que la fonction F ainsi définie est de classe C^1 sur $\mathcal{R}_n$ et calculent sa différentielle.

Notons m la mesure de Lebesgue et $\|.\|_{\mathrm{st}}$ la norme euclidienne standard sur $\mathbb{R}^n$. Tout réseau Λ dans $\mathbb{R}^n$ définit un réseau euclidien $(\mathbb{R}^n, \Lambda, \|.\|_{\mathrm{st}})$, et nous poserons :

$$\mathrm{covol}(\Lambda) := \mathrm{covol}(\mathbb{R}^n, \Lambda, \|.\|_{\mathrm{st}})$$

et

$$\mathcal{V}(\Lambda) := \mathcal{V}(\mathbb{R}^n, \Lambda, \|.\|_{\mathrm{st}}).$$

En termes élémentaires, le résultat de différentiabilité mentionné plus haut s'énonce ainsi :

Proposition 6.5. — *Soit Λ un réseau de $\mathbb{R}^n$. La fonction*

$$F_\Lambda : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}$$

définie par

$$\begin{aligned} F_\Lambda(g) &:= F(\mathbb{R}^n, g.\Lambda, \|.\|_{\mathrm{st}}) \\ &= \mathrm{covol}(\Lambda)^{-1} \, |\det g|^{-1} \int_{\mathcal{V}(g.\Lambda)} f(\|x\|_{\mathrm{st}}^2) \, dm(x) \end{aligned} \tag{6.8}$$

est de classe C^1. Sa différentielle en $g \in GL_n(\mathbb{R})$ est donnée par :

$$DF_\Lambda(g).h = 2 \, \mathrm{covol}(\Lambda)^{-1} \, |\det g|^{-1} \int_{\mathcal{V}(g.\Lambda)} f'(\|x\|_{\mathrm{st}}^2) \, {}^t x.hg^{-1}.x \, dm(x). \tag{6.9}$$

Regev et Stephens-Davidowitz établissent ce résultat par une démonstration utilisant l'expression (6.8) de F_Λ. La différentiabilité de F_Λ écrite sous cette forme est délicate à établir, car le domaine d'intégration $\mathcal{V}(g.\Lambda)$ varie avec g. Il s'avère toutefois que les « contributions du bord » dans la variation première de $F_\Lambda(g)$ se compensent, grâce aux propriétés de symétrie des faces de $\mathcal{V}(g.\Lambda)$ que nous avons évoquées au paragraphe 6.1.2.

Il est possible d'éviter ces arguments délicats en utilisant l'expression (6.7) de $F(\overline{E})$ comme intégrale sur la variété compacte sans bord $E_\mathbb{R}/E$. Une difficulté pour établir la différentiabilité de F (ou encore de F_Λ) est que la fonction $\delta_{\overline{E}}$ n'est pas de classe C^1. On s'en affranchit en observant que F_Λ est continue, puis en montrant que sa différentielle au sens des distributions est effectivement donnée par la formule (6.9) (on utilise pour cela que $\delta_{\overline{E}}$ est lipschitzienne), puis en remarquant que cette différentielle est elle aussi continue sur $GL_n(\mathbb{R})$.

Dans la suite, nous ferons appel à la proposition (6.5) avec pour f la fonction $(x \mapsto e^{-\pi x/s^2})$, où $s \in \mathbb{R}_+^*$. Elle implique aussitôt :

Corollaire 6.6. — *Pour tout $t \in \mathbb{R}_+^*$ et tout entier $n > 0$, l'invariant $\gamma_{t^{-1}}(\mathcal{V}(\overline{E}))$, considéré comme fonction de $[\overline{E}]$ décrivant $\mathcal{R}_n$, est une fonction de classe C^1 sur $\mathcal{R}_n$.*

Si $[\overline{E}]$ est un point critique de la restriction de cette fonction à $\mathcal{R}_n^0$, alors $\mathcal{V}(\overline{E})$ est G-isotrope de paramètre t dans $(E_\mathbb{R}, \|.\|_{\overline{E}})$.

6.4. Mesures gaussiennes des parties compactes convexes symétriques G-isotropes

Soit n un entier > 0 et soit $t(n) := 10(\log n + 2)$.

Théorème 6.7. — *Soit K une partie compacte convexe symétrique de $\mathbb{R}^n$ telle que $m(K) \geqslant 1$. Si $s \in]0, t(n)^{-1}]$ et si K est G-isotrope de paramètre s, alors $\gamma_s(K) \geqslant 2/3$.*

Cet énoncé découle de résultats profonds de géométrie gaussienne. Nous nous contenterons de brèves indications sur sa démonstration, en renvoyant à [RSD17b], Section 4.1, pour les détails.

D'une part, la G-isotropie de K implique que la mesure γ_s prend sur l'orbite de K sous $SL_n(\mathbb{R})$ une valeur maximale au point K :

Proposition 6.8 ([Bob11], Prop. 3.1). — *Soit K une partie compacte convexe symétrique de $\mathbb{R}^n$ et soit $s \in \mathbb{R}_+^*$ tel que K soit G-isotrope de paramètre s. Alors, pour tout $g \in SL_n(\mathbb{R})$,*

$$\gamma_s(K) \geqslant \gamma_s(g.K).$$

Cet énoncé est une conséquence du théorème de Cordero-Erausquin, Fradelizi et Maurey ([CEFM04]) affirmant, qui si l'on pose, pour $t = (t_1, \ldots, t_n) \in \mathbb{R}^n$,

$$\exp \Delta(t) := (e^{t_i}\delta_{ij})_{1 \leqslant i,j \leqslant n},$$

alors *pour toute partie compacte convexe symétrique K de $\mathbb{R}^n$, $t \mapsto \gamma_s(\exp \Delta(t).K)$ est une fonction log-concave de $t \in \mathbb{R}^n$.* (Cet énoncé établit et généralise une conjecture proposée par Banaszczyk et popularisée dans [Lat02] sous le nom de « (B) conjecture »).

On conclut la démonstration du théorème 6.7 au moyen du « théorème $\ell\ell^*$ » ([FTJ79], [Lew79], [Pis82]) qui permet de montrer que *pour toute partie compacte convexe symétrique de $\mathbb{R}^n$ tel que $m(K) = 1$, il existe $g \in SL_n(\mathbb{R})$ tel que $\gamma_{t(n)^{-1}}(g.K) \geqslant 2/3$.*

6.5. Démonstration du théorème 6.4

Comme précédemment, on désigne encore par n un entier > 0 et l'on pose $t(n) := 10(\log n + 2)$.

L'énoncé suivant découle immédiatement du corollaire 6.6 et du théorème 6.7.

Corollaire 6.9. — *Soit $[\overline{E}]$ un point de $\mathcal{R}_n^0$ en lequel $\gamma_{t(n)^{-1}}(\mathcal{V}(\overline{E}))$ atteint un extremum local. On a alors :*

$$\gamma_{t(n)^{-1}}(\mathcal{V}(\overline{E})) \geqslant 2/3. \tag{6.10}$$

La démonstration du théorème 6.4 va procéder par récurrence sur n. L'étape de récurrence fait encore appel à un résultat de géométrie gaussienne, à savoir à la conséquence suivante de l'inégalité isopérimérique gaussienne :

Lemme 6.10. — *Soit K une partie compacte convexe symétrique de $\mathbb{R}^n$ et soient t et r dans $\mathbb{R}_+^*$ tels que*

$$\gamma_{t^{-1}}(K) \geqslant 2/3 \quad \textit{et} \quad \overline{B}_{\|\cdot\|_{\mathrm{st}}}(0, r) \subset K.$$

Alors, pour tout $\tau \in \mathbb{R}_+$,

$$\gamma_{(t+\tau)^{-1}}(K) \geqslant 1 - \frac{1}{3}\, e^{-\pi r^2 \tau^2}.$$

Nous renvoyons à [RSD17b], Lemma 4.11, pour la preuve.

Démonstration du théorème 6.4. — On considère la restriction de la fonction différentiable de $[\overline{E}] \in \mathcal{R}_n^0$ définie par $\gamma_{t(n)^{-1}}(\mathcal{V}(\overline{E}))$ à la partie compacte $\mathcal{S}t_n^0$ de $\mathcal{R}_n^0$. Il suffit d'établir la minoration (6.6) lorsque cette fonction atteint son minimum en $[\overline{E}]$, ce que nous supposons désormais.

Lorsque $[\overline{E}]$ est un point intérieur de $\mathcal{S}t_n^0$ (considéré comme une partie de $\mathcal{R}_n^0$), cette minoration est un cas particulier du corollaire 6.9.

Lorsque $[\overline{E}]$ est un point du bord de $\mathcal{S}t_n^0$, il existe un sous-$\mathbb{Z}$-module saturé F de E tel que $0 < \operatorname{rk} F < \operatorname{rk} E$ et que $\overline{F}$ et $\overline{E/F}$ soient semi-stables de pente nulle (*cf.* proposition 5.1). En particulier $n > 1$. On complète alors la démonstration par récurrence, en utilisant la surmultiplicativité (6.5) de $\gamma_s(\mathcal{V}(\overline{E}))$ et en faisant appel au lemme 6.10 pour contrôler $\gamma_{t(n)^{-1}}(\overline{F})$ et $\gamma_{t(n)^{-1}}(\overline{E/F})$ à partir de $\gamma_{t(\operatorname{rk} F)^{-1}}(\overline{F})$ et $\gamma_{t(\operatorname{rk}(E/F))^{-1}}(\overline{E/F})$. □

6.6. Démonstration du théorème 1.3

Expliquons maintenant comment déduire le théorème 1.3 du theorème 6.4.

Soit donc $\overline{E}$ un réseau euclidien de rang $n > 0$.

Nous devons montrer que, lorsque $\widehat{\mu}_{\max}(\overline{E}) \leqslant 0$, alors on a :

$$\theta_{\overline{E}}(t(n)^2) \leqslant 3/2,$$

ou encore, de façon équivalente :

$$h^0_\theta(\overline{E} \otimes \overline{\mathcal{O}}(-\log t(n))) \leqslant \log 3/2.$$

Dans le cas particulier où $\overline{E}$ est semi-stable de pente 0, cela découle du théorème 6.4 et de l'inégalité (6.4).

En général, on considère la filtration canonique de $\overline{E}$,

$$E_0 = \{0\} \subset E_1 \subset \cdots \subset E_n = E,$$

et les réseaux euclidiens qui s'en déduisent comme sous-quotients et leurs pentes :

$$\overline{F}_i := \overline{E_i/E_{i-1}} \quad \text{et} \quad \mu_i := \widehat{\mu}(\overline{E_i/E_{i-1}}), \qquad i \in \{1, \ldots, N\}.$$

Par hypothèse, on a :

$$0 \geqslant \mu_1 > \ldots > \mu_N.$$

D'après les propriétés de sous-additivité (Proposition 5.3) et de croissance de h^0_θ, il vient alors, pour tout $\lambda \in \mathbb{R}$:

$$h^0_\theta(\overline{E} \otimes \overline{\mathcal{O}}(\lambda)) \leqslant \sum_{i=1}^N h^0_\theta(\overline{F}_i \otimes \overline{\mathcal{O}}(\lambda)) \leqslant \sum_{i=1}^N h^0_\theta(\overline{F}_i \otimes \overline{\mathcal{O}}(\lambda - \mu_i)) \leqslant h^0_\theta\Big(\overline{\mathcal{O}}(\lambda) \otimes \bigoplus_{i=1}^N (\overline{F}_i \otimes \overline{\mathcal{O}}(-\mu_i))\Big).$$

Comme le réseau euclidien de rang n défini par la somme directe

$$\bigoplus_{i=1}^N (\overline{F}_i \otimes \overline{\mathcal{O}}(-\mu_i))$$

est semi-stable de pente nulle, on est ramené au cas particulier précédent.

7. LA CONJECTURE DE KANNAN-LOVÁSZ ℓ^2

Dans cette section, nous expliquons comment le théorème 1.3 implique la seconde inégalité[(12)] dans le théorème 1.4 :

$$\log R_{\mathrm{cov}}(\overline{E}) \leqslant -\widehat{\mu}_{KL}(\overline{E}) + \log[10(\log n + 10)^{3/2}] \tag{7.1}$$

[(12)] Comme déjà observé, la première inégalité est une conséquence facile de la minoration (1.4).

Cette implication fait l'objet de l'article [DR16] (où elle est établie avec des constantes moins précises) ; nous en exposons la présentation simplifiée qui figure dans [RSD17b], Section 6.

Commençons par énoncer une conséquence immédiate de la proposition 5.8 et du théorème 1.3, sous la forme de l'inégalité (5.15) :

COROLLAIRE 7.1. — *Pour tout réseau euclidien $\overline{E}$ de rang $n > 0$, on a :*

$$\log R_{\mathrm{cov}}(\overline{E}) \leqslant -\widehat{\mu}_{\min}(\overline{E}) + \log[10(\log n + 2)] + \log(1 + \sqrt{n/2\pi}).$$

Pour tout entier $n > 0$, on pose :

$$c_{\mathrm{cov}}(n) := \max_{1 \leqslant d \leqslant n} \max_{[\overline{E}] \in \mathcal{S}t_n^0} (\log R_{\mathrm{cov}}(\overline{E}) - (1/2)\log d).$$

Le corollaire 7.1 montre que :

$$\begin{aligned} c_{\mathrm{cov}}(n) &\leqslant \max_{1 \leqslant d \leqslant n} \Big(\log[10(\log d + 2)] + \log(1/\sqrt{2\pi} + 1/\sqrt{n}) \Big) \\ &\leqslant \log[4(\log n + 2)]. \end{aligned}$$

L'inégalité (7.1) est une conséquence immédiate de cette majoration de $c_{\mathrm{cov}}(n)$ et de la proposition suivante :

PROPOSITION 7.2. — *Pour tout réseau euclidien de rang $n > 0$, on a :*

$$\log R_{\mathrm{cov}}(\overline{E}) \leqslant (1/2)(1 + \log 2) + (1/2)\log\lceil \log(2n) \rceil + c_{\mathrm{cov}}(n) - \widehat{\mu}_{KL}(\overline{E}).$$

La proposition 7.2 va découler de la sous-addivité du (carré du) du rayon de recouvrement (6.3) et du lemme suivant, qui constitue une forme inversée de l'inégalité entre moyenne arithmétique et moyenne géométrique :

LEMME 7.3. — *Soit N un entier > 0. Pour tout $(a_1, \ldots, a_N) \in \mathbb{R}^N$ tel que $0 < a_1 < \cdots < a_N$ et tout $(d_1, \ldots, d_n) \in \mathbb{N}^N$, on a :*

$$\sum_{i=1}^{N} d_i a_i \leqslant 2e\lceil \log(2m_1) \rceil \max_{1 \leqslant j \leqslant N} m_j \Big(\prod_{j \leqslant i \leqslant N} a_i^{d_i} \Big)^{1/m_j},$$

où, pour tout $j \in \{1, \ldots, N\}$, on a posé $m_j := \sum_{j \leqslant i \leqslant N} d_i$.

Pour établir ce lemme, on écrit $\{1, \ldots, N\}$ comme la réunion disjointe

$$\{1, \ldots, N\} = \bigcup_{l \in \mathbb{N}_{>0}} S_l$$

où

$$S_l := \{j \in \mathbb{N} \mod 1 \leqslant j \leqslant N \text{ et } \lfloor -\log a_i/a_n \rfloor = l\},$$

et l'on observe que, si $S_l \neq \varnothing$ et $j(l) := \min S_l$, alors :

$$\sum_{i \in S_l} d_i a_i \leqslant e m_{j(l)} \Big(\prod_{j(l) \leqslant i \leqslant N} a_i^{d_i} \Big)^{1/m_{j(l)}},$$

puis qu'il existe $l \in \mathbb{N}_{>0}$ tel que :

$$\lceil \log(2m_1) \rceil \sum_{i \in S_l} d_i a_i \geqslant \sum_{i=1}^{N} d_i a_i.$$

Démonstration de la proposition 7.2. — De nouveau, on considère la filtration canonique de $\overline{E}$,

$$E_0 = \{0\} \subset E_1 \subset \cdots \subset E_n = E,$$

et l'on pose :

$$\overline{F}_i := \overline{E_i/E_{i-1}} \quad \text{et} \quad \mu_i := \widehat{\mu}(\overline{E_i/E_{i-1}}), \qquad i \in \{1, \ldots, N\}.$$

D'après la sous-additivité du carré du rayon de recouvrement dans les suites exactes courtes admissibles (*cf.* (6.3)), on a :

$$R_{\mathrm{cov}}(\overline{E})^2 \leqslant \sum_{i=1}^{N} R_{\mathrm{cov}}(\overline{F}_i)^2. \tag{7.2}$$

Par ailleurs, comme chacun des réseaux euclidiens $\overline{F}_i \otimes \overline{\mathcal{O}}(-\mu_i)$ est semi-stable de pente nulle, on trouve :

$$R(\overline{F}_i)^2 \leqslant e^{c_{\mathrm{cov}}(n)} \mathrm{rk}\, F_i \, e^{-2\mu_i} \tag{7.3}$$

En appliquant le lemme 7.3 avec $a_i := e^{-2\mu_i}$ et $d_i := \mathrm{rk}\, F_i$, on obtient :

$$\begin{aligned} \sum_{i=1}^{N} \mathrm{rk}\, F_i \, e^{-2\mu_i} &\leqslant 2e\lceil \log(2n) \rceil \max_{1 \leqslant j \leqslant N} \mathrm{rk}\,(E/E_{j-1}) \exp(-2\widehat{\mu}(\overline{E/E_{j-1}})) \\ &\leqslant 2e\lceil \log(2n) \rceil \exp(-\widehat{\mu}_{KL}(\overline{E})). \end{aligned} \tag{7.4}$$

La proposition découle de la conjonction de (7.2), (7.3) et (7.4). □

On observera que l'on a établi une version légèrement plus précise de l'inégalité (7.1) : on peut y remplacer $\widehat{\mu}_{KL}(\overline{E})$ par

$$\min_{1 \leqslant i \leqslant N} (\widehat{\mu}(\overline{E/E_{i-1}}) - (1/2) \log \mathrm{rk}\, E/E_{i-1}).$$

Cet invariant n'est fonction que du polygone canonique de $\overline{E}$.

Signalons enfin que l'on peut aisément calculer la pente de Kannan-Lovász des réseaux euclidiens sommes directes de réseaux de rang 1, et montrer que la constante fonction de n dans le membre de droite de (7.1) (ou encore la constante $c(n)$ dans (1.19)) croit au moins comme $\log \log n$ lorsque n tend vers l'infini.

En effet, si n est un entier > 0 et si $\lambda_1 \leqslant \ldots \leqslant \lambda_n$ est une suite croissante de n nombres réels, on vérifie que :

$$\widehat{\mu}_{KL}(\bigoplus_{i=1}^{n} \overline{\mathcal{O}}(\lambda_i)) = \min_{1 \leqslant k \leqslant n} ((1/k) \sum_{i=1}^{k} \lambda_i - (1/2) \log k).$$

Par ailleurs, on sait que :

$$R^2_{\mathrm{cov}}(\bigoplus_{i=1}^{n}\overline{\mathcal{O}}(\lambda_i)) = (1/4)\sum_{i=1}^{n} e^{-2\lambda_i}.$$

La suite de réels $(t_i)_{i\geqslant 1}$ définie par les égalités :

$$\sum_{i=1}^{k} t_i = (k/2)\log k \quad \text{pour tout } k \geqslant 1$$

est croissante et satisfait :

$$2t_i = \log i - 1 + O(1/i) \quad \text{lorsque } i \longrightarrow +\infty,$$

et par conséquent :

$$(1/4)\sum_{i=1}^{n} e^{-2\lambda_i} = (1/4e)\log n + O(1) \quad \text{lorsque } n \longrightarrow +\infty.$$

Ainsi, si pour tout entier $n > 0$, on pose $\overline{E}_n := \bigoplus_{i=1}^{n}\overline{\mathcal{O}}(t_n)$, on a :

$$\widehat{\mu}_{KL}(\overline{E}_n) = 0 \quad \text{et} \quad \log R_{\mathrm{cov}}(\overline{E}_n) = (1/2)\log\log n + O(1) \quad \text{lorsque } n \longrightarrow +\infty.$$

APPENDICE A. LE FORMALISME DES PENTES

Dans cet appendice, nous décrivons un formalisme de pentes, qui s'applique notamment aux fibrés vectoriels sur les courbes (Tjurin, Harder-Narasimhan) et aux réseaux euclidiens (Stuhler, Grayson). Ce formalisme est rudimentaire et nous renvoyons aux articles d'André [And09] et Chen [Che10] pour des formalismes plus sophistiqués et pour des références et des applications supplémentaires.

Soit $(\mathcal{E}, \preceq)$ un ensemble ordonné réticulé. En d'autres termes, l'ensemble ordonné $(\mathcal{E}, \preceq)$ possède un élément minimal O et un élément maximal X, et tout couple $(X_1, X_2) \in \mathcal{E}$ admet une borne inférieure $X_1 \wedge X_2$ et une borne supérieure $X_1 \vee X_2$ dans $(\mathcal{E}, \preceq)$.

Soient en outre

$$r : \mathcal{E} \longrightarrow \mathbb{Z} \quad \text{et} \quad d : \mathcal{E} \longrightarrow \mathbb{R}$$

deux applications[(13)] satisfaisant aux conditions suivantes :

(1) *monotonie* : lorsque l'on munit $\mathbb{N} \times \mathbb{R}$ de l'ordre lexicographique, l'application $(r, d) : \mathcal{E} \longrightarrow \mathbb{N} \times \mathbb{R}$ est strictement croissante.

En d'autres termes, si X_1 et X_2 sont des éléments de $\mathcal{E}$ tels que $X_1 \preceq X_2$, alors $r(X_1) \leqslant r(X_2)$; si de plus $r(X_1) = r(X_2)$, alors $d(X_1) \leqslant d(X_2)$ avec égalité (si et) seulement si $X_1 = X_2$.

(2) *(sous)-additivité* : pour tout $(X_1, X_2) \in \mathcal{E}^2$, on a :

$$r(X_1) + r(X_2) = r(X_1 \wedge X_2) + r(X_1 \vee X_2)$$

[(13)] L'application r est souvent appelé *rang* et l'application d *degré*.

et

$$d(X_1) + d(X_2) \leqslant d(X_1 \wedge X_2) + d(X_1 \vee X_2).$$

(3) *finitude* : pour tout $c \in \mathbb{R}$, l'intersection $d(\mathcal{E}) \cap [c, +\infty]$ est finie.

On observera que, d'après (1), l'image $r(\mathcal{E})$ est contenue dans l'intervalle $[r(O), r(X)] \cap \mathbb{N}$ et donc finie.

Supposons de plus que

$$r(O) < r(X).$$

On peut alors procéder à la construction suivante.

Soit $\mathcal{C}$ l'ensemble des fonctions concaves

$$c : [r(O), r(X)] \longrightarrow \mathbb{R}$$

telles que, pour tout $Y \in \mathcal{E}$,

$$d(Y) \leqslant c(r(Y)).$$

Il découle aussitôt de l'hypothèse de finitude (3) que $\mathcal{C}$ possède un plus petit élément[(14)] P, qui est une fonction affine sur chaque intervalle $[i-1, i]$, où $i \in]r(0), r(X)] \cap \mathbb{N}$. De plus, il existe $N \in \mathbb{N}_{>0}$ et $(X_0, \ldots, X_N)$ dans $\mathcal{E}^{N+1}$ tels que :

- $r(X_0) = r(O) < r(X_1) < \ldots < r(X_N) = r(X)$;
- pour tout $i \in \{0, \ldots, N\}$,

$$P((r(X_i)) = d(X_i),$$

et, si $i \geqslant 1$, la fonction P est affine sur $[r(X_{i-1}), r(X_i)]$; on notera :

$$\mu_i := \frac{d(X_i) - d(X_{i-1})}{r(X_i) - r(X_{i-1})}$$

la *pente* de P sur cet intervalle ;

- la suite des pentes est strictement décroissante :

$$\mu_1 > \mu_2 > \ldots > \mu_N.$$

En faisant appel aux propriétés (1) et (2), on établit alors aisément :

Proposition A.1. — *Avec les notations ci-dessus, la suite $(X_0, \ldots, X_N)$ est uniquement déterminée et croissante :*

$$X_0 \preceq X_1 \preceq \ldots \preceq X_N.$$

De plus, l'élément X_0 est maximal dans $r^{-1}(r(O))$ et $X_N = X$.

Le graphe de P est le *polygone canonique* associé à l'ensemble ordonné $(\mathcal{E}, \preceq)$ muni des fonctions rang et degré r et d. La proposition affirme que les sommets du polygone canonique sont les images par l'application (r, d) d'une « filtration » bien déterminée de X, sa *filtration canonique*.

(14) En d'autres termes, pour tout $c \in \mathcal{C}$ et tout $x \in [r(O), r(X)]$, on a : $P(x) \leqslant c(x)$.

Souvent, dans les applications, on a $r^{-1}(0) = \{O\}$. On peut alors attacher à tout élément Y de $\mathcal{E}\backslash\{O\}$ sa pente

$$\mu(Y) := \frac{d(Y)}{r(Y)},$$

et l'on a :

$$\mu_1 = \max_{Y \in \mathcal{E}\backslash\{O\}} \mu(Y).$$

RÉFÉRENCES

[And09] Y. André. « Slope filtrations ». *Confluentes Math.*, 1(1):1–85, 2009.

[APSD18] N. Alamati, C. Peikert & N. Stephens-Davidowitz. « New (and old) proof systems for lattice problems ». In *Public-key cryptography—PKC 2018. Part II*, volume 10770 of *Lecture Notes in Comput. Sci.*, pages 619–643. Springer, Cham, 2018.

[Ara75] S. J. Arakelov. « Theory of intersections on the arithmetic surface ». In *Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974), Vol. 1*, pages 405–408. Canad. Math. Congress, Montreal, Que., 1975.

[Art78] J. G. Arthur. « A trace formula for reductive groups. I. Terms associated to classes in $G(\mathbf{Q})$ ». *Duke Math. J.*, 45(4):911–952, 1978.

[Ban93] W. Banaszczyk. « New bounds in some transference theorems in the geometry of numbers ». *Math. Ann.*, 296(4):625–635, 1993.

[Ban95] W. Banaszczyk. « Inequalities for convex bodies and polar reciprocal lattices in $\mathbf{R}^n$ ». *Discrete Comput. Geom.*, 13(2):217–231, 1995.

[Ban96] W. Banaszczyk. « Inequalities for convex bodies and polar reciprocal lattices in $\mathbf{R}^n$. II. Application of K-convexity ». *Discrete Comput. Geom.*, 16(3):305–311, 1996.

[BK10] J.-B. Bost & K. Künnemann. « Hermitian vector bundles and extension groups on arithmetic schemes. I. Geometry of numbers ». *Adv. Math.*, 223(3):987–1106, 2010.

[Bob11] S. G. Bobkov. « On Milman's ellipsoids and M-position of convex bodies ». In *Concentration, functional inequalities and isoperimetry*, volume 545 of *Contemp. Math.*, pages 23–33. Amer. Math. Soc., Providence, RI, 2011.

[Bor05] Th. Borek. « Successive minima and slopes of Hermitian vector bundles over number fields ». *J. Number Theory*, 113(2):380–388, 2005.

[Bos15] J.-B. Bost. « Theta invariants of euclidean lattices and infinite-dimensional hermitian vector bundles over arithmetic curves ». ArXiv: 1512.08946, 2015.

[BP17] L. Bétermin & M. Petrache. « Dimension reduction techniques for the minimization of theta functions on lattices ». *J. Math. Phys.*, 58(7):071902, 40, 2017.

[Cas71] J. W. S. Cassels. *An introduction to the geometry of numbers*. Springer-Verlag, Berlin-New York, 1971. Second printing, corrected, Die Grundlehren der mathematischen Wissenschaften, Band 99.

[Cas04] B. Casselman. « Stability of lattices and the partition of arithmetic quotients ». *Asian J. Math.*, 8(4):607–637, 2004.

[CdCI16] H. Cohn & M. de Courcy-Ireland. « The Gaussian core model in high dimensions ». ArXiv: 1603.09684, 2016.

[CDLP13] K.-M. Chung, D. Dadush, F.-H. Liu & C. Peikert. « On the lattice smoothing parameter problem ». In *2013 IEEE Conference on Computational Complexity—CCC 2013*, pages 230–241. IEEE Computer Soc., Los Alamitos, CA, 2013.

[CEFM04] D. Cordero-Erausquin, M. Fradelizi & B. Maurey. « The (B) conjecture for the Gaussian measure of dilates of symmetric convex sets and related problems ». *J. Funct. Anal.*, 214(2):410–427, 2004.

[Che10] H. Chen. « Harder-Narasimhan categories ». *J. Pure Appl. Algebra*, 214(2):187–200, 2010.

[CK09] H. Cohn & A. Kumar. « Optimality and uniqueness of the Leech lattice among lattices ». *Ann. of Math. (2)*, 170(3):1003–1050, 2009.

[CS99] J. H. Conway & N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, New York, third edition, 1999.

[DR16] D. Dadush & O. Regev. « Towards strong reverse Minkowski-type inequalities for lattices ». In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 447–456. IEEE Computer Soc., Los Alamitos, CA, 2016.

[DRSD14] D. Dadush, O. Regev & N. Stephens-Davidowitz. « On the closest vector problem with a distance guarantee ». In *IEEE 29th Conference on Computational Complexity—CCC 2014*, pages 98–109. IEEE Computer Soc., Los Alamitos, CA, 2014.

[Ebe13] W. Ebeling. *Lattices and codes*. Advanced Lectures in Mathematics. Springer Spektrum, Wiesbaden, third edition, 2013. A course partially based on lectures by Friedrich Hirzebruch.

[Eic66] M. Eichler. *Introduction to the theory of algebraic numbers and functions*. Translated from the German by George Striker. Pure and Applied Mathematics, Vol. 23. Academic Press, New York-London, 1966.

[FTJ79] T. Figiel & N. Tomczak-Jaegermann. « Projections onto Hilbertian subspaces of Banach spaces ». *Israel J. Math.*, 33(2):155–171, 1979.

[GMS91] H. Gillet, B. Mazur & C. Soulé. « A note on a classical theorem of Blichfeldt ». *Bull. London Math. Soc.*, 23(2):131–132, 1991.

[Gra84] D. R. Grayson. « Reduction theory using semistability ». *Comment. Math. Helv.*, 59(4):600–634, 1984.

[Gra86] D. R. Grayson. « Reduction theory using semistability. II ». *Comment. Math. Helv.*, 61(4):661–676, 1986.

[Gro01] R. P. Groenewegen. « An arithmetic analogue of Clifford's theorem ». *J. Théor. Nombres Bordeaux*, 13(1):143–156, 2001. 21st Journées Arithmétiques (Rome, 2001).

[Har69] G. Harder. « Minkowskische Reduktionstheorie über Funktionenkörpern ». *Invent. Math.*, 7:33–54, 1969.

[Hec17] E. Hecke. « Über die Zetafunktion beliebiger algebraischer Zahlkörper ». *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, 1917:77–89, 1917.

[HN75] G. Harder & M. S. Narasimhan. « On the cohomology groups of moduli spaces of vector bundles on curves ». *Math. Ann.*, 212:215–248, 1974/75.

[HS97] G. Harder & U. Stuhler. *Trieste lectures on reduction theory.* University of Bonn, 1997.

[KL88] R. Kannan & L. Lovász. « Covering minima and lattice-point-free convex bodies ». *Ann. of Math. (2)*, 128(3):577–602, 1988.

[Lag95] J. C. Lagarias. « Point lattices ». In *Handbook of combinatorics, Vol. 1, 2*, pages 919–966. Elsevier Sci. B. V., Amsterdam, 1995.

[Lat02] R. Latała. « On some inequalities for Gaussian measures ». In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 813–822. Higher Ed. Press, Beijing, 2002.

[Lew79] D. R. Lewis. « Ellipsoids defined by Banach ideal norms ». *Mathematika*, 26(1):18–29, 1979.

[LLS90] J. C. Lagarias, H. W. Lenstra, Jr. & C.-P. Schnorr. « Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice ». *Combinatorica*, 10(4):333–348, 1990.

[Man85] Yu. I. Manin. « New dimensions in geometry ». In *Workshop Bonn 1984 (Bonn, 1984)*, volume 1111 of *Lecture Notes in Math.*, pages 59–101. Springer, Berlin, 1985.

[Mar03] J. Martinet. *Perfect lattices in Euclidean spaces*, volume 327 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2003.

[Mau05] B. Maurey. « Inégalité de Brunn-Minkowski-Lusternik, et autres inégalités géométriques et fonctionnelles ». *Astérisque*, (299):Exp. No. 928, vii, 95–113, 2005. Séminaire Bourbaki. Vol. 2003/2004.

[MG02] D. Micciancio & S. Goldwasser. *Complexity of lattice problems. A cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, MA, 2002.

[MH73] J. Milnor & D. Husemoller. *Symmetric bilinear forms*. Springer-Verlag, New York-Heidelberg, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[Min96] H. Minkowski. *Geometrie der Zahlen*. Teubner-Verlag, Leipzig, Berlin, 1896.

[Mor95] M. Morishita. « Integral representations of unramified Galois groups and matrix divisors over number fields ». *Osaka J. Math.*, 32(3):565–576, 1995.

[MP17] T. McMurray Price. « Numerical cohomology ». *Algebr. Geom.*, 4(2):136–159, 2017.

[MR07] D. Micciancio & O. Regev. « Worst-case to average-case reductions based on Gaussian measures ». *SIAM J. Comput.*, 37(1):267–302, 2007.

[MR09] D. Micciancio & O. Regev. « Lattice-based cryptography ». In *Post-quantum cryptography*, pages 147–191. Springer, Berlin, 2009.

[Pei16] C. Peikert. *A decade of lattice cryptography*. Monographie disponible sur `http://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`, 2016.

[Pis82] G. Pisier. « Holomorphic semigroups and the geometry of Banach spaces ». *Ann. of Math. (2)*, 115(2):375–392, 1982.

[Qui] D. Quillen. *Quillen Notebooks 1968–2003*, edited by G. Luke and G. Segal. Published online by the Clay Mathematics Institute. `http://www.claymath.org/publications/quillen-notebooks`.

[RB79] S. S. Ryškov & E. P. Baranovskiĭ. « Classical methods of the theory of lattice packings ». *Uspekhi Mat. Nauk*, 34(4(208)):3–63, 256, 1979.

[Roe93] D. Roessler. *The Riemann-Roch theorem for arithmetic curves*. Diplomarbeit, ETH Zürich, 1993.

[RSD17a] O. Regev & N. Stephens-Davidowitz. « An inequality for Gaussians on lattices ». *SIAM J. Discrete Math.*, 31(2):749–757, 2017.

[RSD17b] O. Regev & N. Stephens-Davidowitz. « A reverse Minkowski theorem ». In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 941–953. ACM, New York, 2017.

[Sch31] F. K. Schmidt. « Analytische Zahlentheorie in Körpern der Charakteristik p ». *Math. Z.*, 33:1–32, 1931.

[Sch67] W. M. Schmidt. « On heights of algebraic subspaces and diophantine approximations ». *Ann. of Math. (2)*, 85:430–472, 1967.

[Sch09] A. Schürmann. « Enumerating perfect forms ». In *Quadratic forms—algebra, arithmetic and geometry*, volume 493 of *Contemp. Math.*, pages 359–377. Amer. Math. Soc., Providence, RI, 2009.

[SS06] P. Sarnak & A. Strömbergsson. « Minima of Epstein's zeta function and heights of flat tori ». *Invent. Math.*, 165(1):115–151, 2006.

[Stu76] U. Stuhler. « Eine Bemerkung zur Reduktionstheorie quadratischer Formen ». *Arch. Math. (Basel)*, 27(6):604–610, 1976.

[SW14] U. Shapira & B. Weiss. « A volume estimate for the set of stable lattices ». *C. R. Math. Acad. Sci. Paris*, 352(11):875–879, 2014.

[SW16] U. Shapira & B. Weiss. « Stable lattices and the diagonal group ». *J. Eur. Math. Soc. (JEMS)*, 18(8):1753–1767, 2016.

[Szp85] L. Szpiro. « Degrés, intersections, hauteurs ». *Astérisque*, (127):11–28, 1985.

[Tju66] A. N. Tjurin. « Classification of n-dimensional vector bundles over an algebraic curve of arbitrary genus ». *Izv. Akad. Nauk SSSR Ser. Mat.*, 30:1353–1366, 1966.

[vdGS00] G. van der Geer & R. Schoof. « Effectivity of Arakelov divisors and the theta divisor of a number field ». *Selecta Math. (N.S.)*, 6(4):377–398, 2000.

[vdW56] B. L. van der Waerden. « Die Reduktionstheorie der positiven quadratischen Formen ». *Acta Math.*, 96:265–309, 1956.

[VLP85] *Module des fibrés stables sur les courbes algébriques*, édité par J.-L. Verdier & J. Le Potier, volume 54 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1985.

[Vor08a] G. Voronoi. « Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites ». *J. Reine Angew. Math.*, 133:97–102, 1908.

[Vor08b] G. Voronoi. « Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs ». *J. Reine Angew. Math.*, 134:198–287, 1908.

[Vor09] G. Voronoi. « Nouvelles applications des paramètres continus à théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs ». (Seconde partie) *J. Reine Angew. Math.*, 136:67–182, 1909.

[Wei39] A. Weil. « Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques ». *Rev. Sci.*, 77:104–106, 1939.

Jean-Benoît Bost

Département de Mathématiques,
Université Paris-Sud
Bâtiment 307
91405 Orsay cedex, France
E-mail : jean-benoit.bost@math.u-psud.fr