Séminaire BOURBAKI Octobre 2018
71e année, 2018–2019, no 1151, p. 1 à 59
doi:10.24033/ast.1130

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

par **Jean-Benoît BOST**

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 $(e_i)_{1\leq i\leq n}$ 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'un réseau Λ dans V et d'une structure euclidienne sur V de norme associée $\|.\|$.

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 identifie E à son image par l'injection canonique ($E \hookrightarrow E_{\mathbb{R}}$, $v \longmapsto v \otimes 1$), 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 Voronoï. Pour une présentation des résultats classiques de ce domaine, nous renvoyons aux ouvrages et articles d'exposition [**14**], [**57**], [**36**], et [**42**].

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 $\operatorname{rk} E > 0$:
$$\lambda_1(\overline{E}) := \min_{e \in E \setminus \{0\}} \|e\| \in \mathbb{R}_+^*.$$
Plus généralement, on introduit les *minima successifs* $(\lambda_i(\overline{E}))_{1 \leq i \leq \operatorname{rk} E}$ de $\overline{E}$ définis par :

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

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

---

(1) Elle est définie comme l'unique mesure borélienne invariante par translation sur $E_{\mathbb{R}}$ telle que, pour toute base orthonormée $(v_i)_{1 \leq i \leq n}$ 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.

– 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,*

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

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

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

(voir paragraphe 2.4, *infra*).

Minkowski a donné dans sa *Geometrie der Zahlen* (**[49]**, 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 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

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

[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 **[19]**, pour éviter la confusion avec les diverses pentes $\widehat{\mu}(\overline{E})$, $\widehat{\mu}_i(\overline{E})$, $\widehat{\mu}_{KL}(\overline{E})$ associées à $\overline{E}$.

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

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

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

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

ou encore :

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

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 [**19**], [**18**]). 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 :

$$\log \gamma_n \leq (n-1) \log \sqrt{4/3}.$$

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'en présenter les résultats, il nous faut rappeler diverses constructions classiques 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.

Remarquons qu'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 le quotient F^{sat}/F est fini.

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

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