Minkowski et la geometrie des nombres «classique»

Jacques Martinet

26-27 juin 2007

Institut de Matématiques de Bordeaux
Université Bordeaux 1

Colloque :

Rencontres Arithmétiques de Caen
2007

Préhistoire

Soit $\mathbf{q(X)} = {}^{\mathbf{t}}\mathbf{X}\,\mathbf{A}\,\mathbf{X}$ une forme quadratique définie positive en $\mathbf{n}$ variables. Trouver une constante $\gamma_{\mathbf{n}}$ telle qu'il existe $\mathbf{X} \in \mathbb{Z}^{\mathbf{n}}$ avec ($\det(A)$ est le *discriminant de* q)

$$\mathbf{q(X)} \leq \gamma_{\mathbf{n}}\, \frac{\min \mathbf{q}}{\det(\mathbf{A})^{\mathbf{1/n}}}\,.$$

Lagrange (1770) : $\gamma_{\mathbf{2}} = \frac{\mathbf{2}}{\sqrt{\mathbf{3}}}$.

Gauss (1831) : $\gamma_{\mathbf{3}} = \mathbf{2}^{\mathbf{1/3}}$.

Hermite (6 août 1845, lettre à Jacobi) : $\gamma_{\mathbf{n}}$ existe, et $\gamma_{\mathbf{n}} \leq (\frac{\mathbf{4}}{\mathbf{3}})^{\mathbf{(n-1)/2}}$.

Korkine & Zolotareff (1872) : $\gamma_{\mathbf{4}} = \sqrt{\mathbf{2}}$.[a]

Korkine & Zolotareff (1877) : $\gamma_{\mathbf{5}} = \mathbf{2}^{\mathbf{3/5}}$.

Enfin Minkowski vint ...

[a] future inégalité de Mordell (1944) : $\gamma_{\mathbf{n}} \leq \gamma_{\mathbf{n-1}}^{\mathbf{(n-1)/(n-2)}}$

Réseaux permis

Soit $\mathbf{E}$ un espace euclidien. Un *réseau de* $\mathbf{E}$ est un sous-groupe de $\mathbf{E}$ possédant une $\mathbb{Z}$-base qui constitue une base de $\mathbf{E}$ (sur $\mathbb{R}$). On dit qu'un réseau $\mathbf{\Lambda}$ est *permis pour une partie* $\mathbf{A}$ *de* $\mathbf{E}$ si $\mathbf{\Lambda} \cap \mathbf{A} = \{\mathbf{0}\}$ ou $\emptyset$. La *constante de réseau* $\kappa(\mathbf{A})$ *de* $\mathbf{A}$ est la borne inférieure des déterminants des réseaux permis pour $\mathbf{A}$ (ou $+\infty$).

N.B. On pose $\det(\mathbf{\Lambda}) = \det(\mathbf{e_i} \cdot \mathbf{e_j})$ où $\mathcal{B} = (\mathbf{e_1}, \ldots, \mathbf{e_n})$ est une base de $\mathbf{\Lambda}$. C'est le **carré** du déterminant d'une base de $\mathbf{\Lambda}$ dans une base orthonormée $(\varepsilon_\mathbf{1}, \ldots, \varepsilon_\mathbf{n})$ de $\mathbf{E}$.

N.B. Aujourd'hui, l'origine sera toujours un point intérieur de $\mathbf{A} \quad \Longrightarrow \kappa(\mathbf{A}) > \mathbf{0}$.

Un point de vue révolutionnaire

Idée de base : il revient au même

- de majorer $\mathbf{q(x)/\operatorname{disc}(q)^{1/n}}$ sur $\mathbb{Z}^{\mathbf{n}}$ pour toute forme $\mathbf{q}$;
- de majorer $\mathbf{q(x)/[\operatorname{disc}(q)\det(\Lambda)]^{1/n}}$ sur $\mathbf{\Lambda}$ pour toute forme $\mathbf{q}$ et pour tout réseau $\mathbf{\Lambda}$;
- de majorer $\mathbf{q(x)/[\operatorname{disc}(q)\det(\Lambda)]^{1/n}}$ sur $\mathbf{\Lambda}$ pour tout $\mathbf{\Lambda}$, **mais pour une seule forme $\mathbf{q}$**, par exemple $\mathbf{x_1^2+x_2^2+\cdots+x_n^2}$ sur $\mathbf{E}\simeq\mathbb{R}^{\mathbf{n}}$.
- de minorer $\mathbf{\Gamma_n}=\kappa(\mathbf{B_n})$ ($\mathbf{B_n}$: boule unité de $\mathbb{R}^{\mathbf{n}}$). [On a $\mathbf{\Gamma_n}=\gamma_{\mathbf{n}}^{-\mathbf{n/2}}$, cf. *infra*.]

Minkowski remarque que si le réseau est permis pour $\mathbf{B_n}$, il empile les boules de rayon $\frac{\mathbf{1}}{\mathbf{2}}$, empilement dont la densité δ est au plus $\mathbf{1}$, et il estime δ par passage à la limite. Cela remplace la majoration exponentielle en $\mathbf{n}$ de $\gamma_{\mathbf{n}}$ due à Hermite par une majoration linéaire :

$$\left(\frac{\mathbf{4}}{\mathbf{3}}\right)^{\mathbf{(n-1)/2}} \quad \text{devient par exemple} \quad \mathbf{1}+\frac{\mathbf{n}}{\mathbf{4}}\,.$$

Plus tard, il remarque que l'argument des boules s'étend aux domaines convexes symétriques.

La majoration $\delta < \mathbf{1}$ n'est pas bonne. Bien majorer δ a conduit à d'importants progrès, d'abord par Blichfeldt.

Chabauty. *Une ménagère achetant des pommes dans* $\mathbb{R}^{\mathbf{n}}$*, lorsque* $\mathbf{n}$ *est grand, rapporte surtout du vide dans son panier*.

Empilements quelconques. Ambrose Rogers, 1964 ; Cohn & Elkies, 2003.

Joint à de la combinatoire (*designs sphériques*), ce résultat a conduit au

Théorème de Cohn & Kumar**.** $\gamma_{\mathbf{24}} = \mathbf{4}$, valeur atteinte uniquement sur le réseau de Leech.

Hermite et Minkowski : produits

Dans une lettre à Jacobi, Hermite précise sa majoration ; voici l'énoncé en termes de réseaux : un réseau $\mathbf{\Lambda}$ possède une *base* telle que

$$\big(\mathbf{N(e_1)}\cdots\mathbf{N(e_n)}\big)^{\mathbf{1/n}} \leq \big(\frac{\mathbf{4}}{\mathbf{3}}\big)^{\mathbf{(n-1)/2}} \det(\mathbf{\Lambda})\,.$$

Minkowski : il existe des vecteurs $\mathbf{e_1},\ldots,\mathbf{e_n}$ *indépendants* tels que

$$\big(\mathbf{N(e_1)}\cdots\mathbf{N(e_n)}\big)^{\mathbf{1/n}} \leq \gamma_{\mathbf{n}}\ \det(\mathbf{\Lambda})\,.$$

Fonctions distances

Il s'agit de fonctions $\mathbf{F} : \mathbf{E} \to \mathbb{R}_{\geq \mathbf{0}}$ continues, et «homogènes de degré $\mathbf{d} > \mathbf{0}$» dans le sens suivant :

$$\forall \mathbf{x} \in \mathbf{E}\,,\ \forall \lambda \in \mathbb{R}\,,\ \mathbf{F}(\lambda \mathbf{x}) = |\lambda|^{\mathbf{d}} \mathbf{F}(\mathbf{x})\,.$$

À $\mathbf{F}$, on associe $\mathbf{A} = \{\mathbf{x} \in \mathbf{E} \mid \mathbf{F}(\mathbf{x}) < \mathbf{1}\}$ et l'on étend $\mathbf{F}$ à l'espace des réseaux par

$$\mathbf{F}(\mathbf{\Lambda}) = \inf_{\mathbf{x} \in \mathbf{\Lambda} \smallsetminus \{\mathbf{0}\}} \mathbf{F}(\mathbf{x})\,.$$

On a alors

$$\kappa(\mathbf{A}) = \mathbf{F}(\mathbf{\Lambda})^{-\mathbf{n}/\mathbf{d}}\,.$$

Exemple : en prenant $\mathbf{F}(\mathbf{x}) = \mathbf{x} \cdot \mathbf{x}$ ($= \|\mathbf{x}\|^{\mathbf{2}}$, noté $\mathbf{N}(\mathbf{x})$), on obtient

$$\gamma_{\mathbf{n}} = \mathbf{\Gamma}_{\mathbf{n}}^{-\mathbf{2}/\mathbf{n}}\,.$$

Formes quadratiques indéfinies

Soit $\mathbf{F(x) = |x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2|}$.

Quid de κ pour le domaine $\mathbf{F(x) < 1}$? ($\mathbf{n = r + s}$.)

Signatures $\mathbf{(1,1)}$[a] et $\mathbf{(2,1)}$: Markoff(v), 1879, 1903

Signatures $\mathbf{(3,1)}$ et $\mathbf{(2,2)}$: Oppenheim, 1931, 1934

Conjecture (Oppenheim, 1929) ; **théorème** (Margulis, 1987). Une forme quadratique $\mathbf{q}$ indéfinie en au moins $\mathbf{3}$ variables qui n'est pas proportionnelle à une forme entière prend des valeurs arbitrairement petites.

$$\Longrightarrow \quad \kappa = +\infty \text{ si } \mathbf{n \geq 5}\,.$$

Mieux (Dani & Margulis) : $\mathbf{q}(\mathbb{Z})$ est dense dans $\mathbb{R}$.

La démonstration originale consiste à se ramener à un théorème sur les groupes de Lie : soient $\mathbf{G} = \mathrm{SL}_\mathbf{3}(\mathbb{R})$, $\mathbf{\Gamma} = \mathrm{SL}_\mathbf{3}(\mathbb{Z})$, $\mathbf{H}$ le stabilisateur de $\mathbf{q = 2x_1x_2 + x_3^2}$ dans $\mathbf{G}$. Si $\mathbf{z} \in \mathbf{G/\Gamma}$ a une orbite $\mathbf{Hz}$ relativement compacte, $\mathbf{H/H \cap G_z}$ est compact.

[a] *Sur le formes quadratiques binaires indéfinies*, Mat. Ann. **15**

Réseaux associés aux corps de nombres

En complétant un corps de nombres $\mathbf{K}$ de signature $(\mathbf{r_1}, \mathbf{r_2})$ pour une norme du maximum relativement à la valeur abolue usuelle de $\mathbb{Q}$, on obtient une $\mathbb{R}$-algèbre

$$\widehat{\mathbf{K}} \simeq_{\text{can.}} \mathbb{R} \otimes \mathbf{K} \simeq \mathbb{R}^{\mathbf{r_1}} \times \mathbb{C}^{\mathbf{r_2}} ,$$

munie de l'involution canonique induite par la conjugaison complexe, que la «trace tordue» munit d'une structure euclidienne :

$$\mathbf{x} \cdot \mathbf{y} = \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\mathbf{x}\overline{\mathbf{y}}) .$$

[**Attention:** $\mathrm{Tr}(\mathbf{z}\overline{\mathbf{z}}) = \mathbf{2}\,\mathbf{z}\overline{\mathbf{z}}$, d'où des $\mathbf{2^{r_2}}$ ici et là.]

Un sous-module $\mathbf{M}$ de $\mathbf{K}$, de rang $\mathbf{n} = [\mathbf{K} : \mathbb{Q}]$ et de type fini s'identifie à un réseau de $\widehat{\mathbf{K}}$ (on dira *réseau algébrique pour la signature* $(\mathbf{r_1}, \mathbf{r_2})$).

On pose $\mathrm{N}(\mathbf{M}) = \min_{\mathbf{x} \in \mathbf{M} \smallsetminus \{\mathbf{0}\}} |\mathrm{N}_{\mathbf{K}/\mathbb{Q}}(\mathbf{x})|$;
c'est un nombre $\mathbf{m}$ strictement positif, ce qui va permettre de construire par renormalisation des réseaux permis pour les ensembles qui suivent.

Remarque. Quid des corps gauches ?

Fonction distance et domaine associés à une signature

On prend $\mathbf{E} = \mathbb{R}^{\mathbf{n}}$, et l'on pose

$$\mathrm{N}_{\mathbf{r_1},\mathbf{r_2}}(\mathbf{x}) = \prod_{\mathbf{i}=\mathbf{1}}^{\mathbf{r_1}} |\mathbf{x_i}| \prod_{\mathbf{j}=\mathbf{1}}^{\mathbf{r_2}} (\mathbf{y_j^2} + \mathbf{z_j^2}) \,,$$

$$\mathbf{A}_{\mathbf{r_1},\mathbf{r_2}} = \{\mathbf{x} \in \mathbb{R}^{\mathbf{n}} \mid \mathrm{N}_{\mathbf{r_1},\mathbf{r_2}}(\mathbf{x}) < \mathbf{2}^{\mathbf{r_2}}\} \,,$$
$$\kappa_{\mathbf{r_1},\mathbf{r_2}} = \kappa(\mathbf{A}_{\mathbf{r_1},\mathbf{r_2}}) \,,$$
$$\mathbf{B}_{\mathbf{r_1},\mathbf{r_2}} = \{\mathbf{x} \in \mathbb{R}^{\mathbf{n}} \mid \sum|\mathbf{x_i}| + \mathbf{2}\sum(\mathbf{y_j^2} + \mathbf{z_j^2}) < \mathbf{1}\} \,.$$

On a les inclusions (inégalités arithmético-géométriques)

- $\mathbf{A}_{\mathbf{r_1},\mathbf{r_2}} \subset \mathbf{A}_{\mathbf{r_1}+\mathbf{2},\mathbf{r_2}-\mathbf{1}}$ $(\mathbf{r_2} > \mathbf{0})$.
- $\mathbf{n}\, \mathbf{2}^{\mathbf{r_2}/\mathbf{n}}\, \mathbf{B}_{\mathbf{r_1},\mathbf{r_2}} \subset \mathbf{A}_{\mathbf{r_1},\mathbf{r_2}}$.
- $\mathbf{B}(\mathbf{0}, \sqrt{\mathbf{n}}) \subset \mathbf{A}_{\mathbf{r_1},\mathbf{r_2}}$.

À l'aide de l'inclusion (2) et de son théorème sur les convexes symétriques, Minkowski démontre (lettre à Hermite, janvier 1891, publiée aux C.R.A.S.) la conjecture de Kronecker (Crelle **92**, 1882) sur les discriminants : $\mathbf{K} \neq \mathbb{Q} \Longrightarrow |\mathbf{d_k}| > \mathbf{1}$.

Théorème. Tout $\mathbf{M} \subset \mathbf{K}$ de signature $(\mathbf{r_1}, \mathbf{r_2})$ contient un élément $\mathbf{x}$ non nul tel que

$$|\mathrm{N}_{\mathbf{K}/\mathbb{Q}}(\mathbf{x})| \leq \Big(\frac{|\mathbf{d_K}(\mathbf{M})|}{\kappa_{\mathbf{r_1},\mathbf{r_2}}}\Big)^{\mathbf{1/2}},$$

$$\Longrightarrow$$

toute classe d'idéaux de $\mathbf{K}$ contient un idéal $\mathfrak{a}$ t.q.

$$\mathrm{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{a}) \leq \Big(\frac{|\mathbf{d_K}|}{\kappa_{\mathbf{r_1},\mathbf{r_2}}}\Big)^{\mathbf{1/2}}.$$

Pour prouver la conjecture de Kronecker, il n'y a plus qu'à minorer $\mathrm{N}_{\mathbf{K}/\mathbb{Q}}(\mathfrak{a})$ par $\mathbf{1}$ et $\kappa_{\mathbf{r_1},\mathbf{r_2}}$ par $\kappa(\mathbf{B}_{\mathbf{r_1},\mathbf{r_2}})$, puis cette constante par un calcul de volume.

Réseaux isolés et chaîne de Markoff

En cherchant les *minima locaux* des déterminants des réseaux permis pour un domaine $\mathbf{A}$ ($\leftrightarrow$ *maxima locaux* pour $\mathbf{F(\Lambda)/\det(\Lambda)^{d/n}}$), on rencontre souvent des *réseaux isolés* $\mathbf{\Lambda_0}$, i.e. tels dans tout voisinage assez petit de $\mathbf{\Lambda_0}$, les réseaux permis se déduisent de $\mathbf{\Lambda_0}$ par automorphisme de $\mathbf{A}$ et homothétie de rapport $\lambda \geq \mathbf{1}$.

On évite alors des raisonnements «à ε près» dans l'utilisation du théorème de compacité de Mahler.

C'est le cas du domaine associé à $\mathbf{F(x,y) = |xy|}$ (pour lequel les énoncés ont une traduction en termes d'approximation diophantienne) pour les réseaux avec $\det(\mathbf{\Lambda}) < \mathbf{9}$, ceux de la chaîne de Markoff : $\mathbf{d = 5, 8, \frac{221}{25}}$, ..., de la forme $\mathbf{9 - \frac{4}{m_n^2}}$ où le *nombre de Markoff* $\mathbf{m_n}$ est équivalent (Zagier) à $\mathbf{\frac{1}{3}\, e^{2.35234...\sqrt{n}}}$.

Du fait que $\mathbf{9}$ est un point d'accumulation, il y a «explosion» des réseaux permis de déterminant $\mathbf{9}$.

De ce point de vue, la dimension $\mathbf{2}$ pourrait être spéciale.

Corps totalement réels

$\mathbf{n = 3}$ (Cassels et Swinnerton-Dyer, 1955).

Thm 1. *Les réseaux algébriques sont* fortement *isolés.*

Fortement : les valeurs de $\mathbf{x_1 x_2 x_3}$ sont denses dans $\mathbb{R}$.

Les réseaux algébriques sont en fait isolés pour $\mathbf{n \geq 3}$ (Skubenko, 1981 ; Akramov, 1990). Cela est lié à l'égalité $\dim \mathrm{Aut}(\mathbf{F}) =$ rang des unités.

Conjecture générale. Si $\mathbf{n \geq 3}$, à automorphisme et homothétie près, tout réseau permis est algébrique.

Thm 2. Cette conjecture pour $\mathbf{n = 3}$ entraîne la

Conjecture de Littlewood :

$$\forall\, \alpha,\, \beta \in \mathbb{R},\ \liminf_{\mathbf{q} \to +\infty} \mathbf{q}\, \|\mathbf{q}\alpha\|\, \|\mathbf{q}\beta\| = \mathbf{0}\,.$$

N.B. Une démonstration fausse de la conjecture générale a été publiée par Skubenko.

Remarque. La **C. G.** entraîne vraisemblablement que les minima successifs (isolés) forment une suite tendant vers l'infini, et donc une majoration en $\mathbf{o}(\sqrt{\mathbf{d_K}})$ pour les normes minimales des idéaux dans une classe.

Corps cubiques réels

(d'après H.P.F. S.-D., 1971)

Après avoir publié en 1941 une démonstration courte du calcul de la constante de réseau, Davenport a prouvé en 1943 aux prix d'énormes difficultés que les premiers minima sont $\mathbf{7^2}$, $\mathbf{9^2}$, puis $> \mathbf{82}, \ldots$ Swinnerton-Dyer a réussi à programmer la recherche des **19** premiers minima, jusqu'à $\mathbf{296}, \ldots$: $\mathbf{7^2 = 49}$, $\mathbf{9^2 = 81}$, $\mathbf{148}$, $\mathbf{(63/5)^2 = 158,76}$ (n.p.), $\mathbf{13^2 = 169}$, $\mathbf{(91/7)^2 = 13^2}$ (n.p.), ... Il apparaît dans la liste des modules qui ne proviennent pas de classes d'idéaux.

Discriminants.

n	3	4	5	6
Minkowski	20	113	678	4199
connu	49	500	3251	14762
conject.	49	725	14641	300125

Autres signatures

Le résultat optimal n'est connu que pour $\mathbf{n = 2}$ et $\mathbf{3}$, atteint sur les réseaux associés aux entiers d'Eisenstein et au corps cubique de discriminant $\mathbf{-23}$. Une difficile démonstration avec la preuve que le réseau est «faiblement» isolé a été donnée par Davenport et Rogers en 1950.

Point de vue de Mordell. Pour les formes cubiques *binaires*, les constantes de réseau sont associées aux discriminants $\mathbf{-23}$ et $\mathbf{+49}$. Un argument de dualité permet de ramener $\mathbf{n = 3}$ à $\mathbf{n = 2}$.

Un résultat général d'isolement «faible» a été publié (en russe) par Akramov en 2002.

Discriminants (cas $r_1 \leq 1$).

n	3	4	5	6	8
Minkowski	12	43	258	985	25067
Sphere	13	64	390	2187	65536
conject.	<u>23</u>	117	1609	9747	1257728