Extrait de l'article de Wikipedia Géométrie des nombres[1]

Valeurs minimales de formes

Les deux exemples d'applications précédents font intervenir des formes algébriques (c'est-à-dire des polynômes homogènes), formes linéaires dans le premier cas[2], formes quadratiques dans le deuxième[3]. La géométrie des nombres permet plus généralement d'étudier les valeurs aux points entiers de telles formes, en particulier de majorer leurs minima[4].

Théorème - Soit $\xi_1, \xi_2, \ldots, \xi_n$ un système de n formes linéaires homogènes à n variables $x_1, x_2, \ldots, x_n$, à coefficients réels, et de déterminant non nul Δ. Alors, pour tout ensemble de n nombres positifs $\tau_1, \tau_2, \ldots, \tau_n$ tels que $\tau_1\tau_2 \ldots \tau_n = \Delta$, on peut donner aux variables x_i des valeurs entières telles que pour tout i, on ait $|\xi_i| \leq \tau_i$.

La preuve repose sur le théorème fondamental de Minkowski appliqué au parallélépipède défini par $|\xi_i| \leq \tau_i$ pour tout i, dont le volume est 2^n.

Théorème - Soit $Q(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} s_{ij}x_ix_j$ une forme quadratique définie positive à n variables et $D = \text{dét}(s_{ij})$ son déterminant. Alors il existe des entiers $u_1, u_2, \ldots, u_n$ qui ne sont pas tous nuls et tels que la valeur de la forme en ces entiers $Q(u_1, u_2, \ldots, u_n)$ soit plus petite que $\frac{4}{\pi}\left(\Gamma(1+\frac{1}{2}n)^2 D\right)^{1/n}$.

Dans cet énoncé, Γ désigne la fonction gamma, qui intervient ici parce que ses valeurs donnent les volumes des sphères en toute dimension (et de certains transformés comme les ellipsoïdes). La preuve du théorème repose encore une fois sur le théorème fondamental de Minkowski, mais appliqué cette fois à l'ellipsoïde défini par $Q(u_1, u_2, \ldots, u_n) \leq \lambda$, pour un nombre λ réel bien choisi.

[1] https://fr.wikipedia.org/wiki/G%C3%A9om%C3%A9trie_des_nombres

[2] Cas de l'application du théorème de Minkowski à l'approximation diophantienne.

[3] Cas de l'application du théorème de Minkowski pour montrer que tout entier positif est somme de 4 carrés.

[4] Voir [1], Gruber et Lekkerkerker 1987, p.43-44.

Traduction d'un court extrait de l'édition de 1971 de *Introduction to the geometry of numbers* de J.W.S. Cassels (p.64, début du troisième chapitre)[5]

Chapitre III

Théorèmes de Blichfeldt et Minkowski

III.1. Introduction. On peut dire que l'ensemble de la géométrie des nombres est née du théorème du corps convexe de Minkowski. Dans son sens le plus basique, ce théorème dit que si un ensemble de points $\mathscr{S}$ est symétrique dans l'espace euclidien à n dimensions autour de l'origine (i.e. contient $-x$ quand il contient x) et convexe [i.e. contient le segment complet

$$\lambda x + (1-\lambda)y \qquad (0 \leq \lambda \leq 1)$$

quand il contient x et y] et a un volume $V > 2^n$, alors il contient un point entier u autre que l'origine. De cette façon, on a un lien entre les propriétés "géométriques" d'un ensemble - convexité, symétrie et volume - et une propriété "arithmétique", notamment l'existence d'un point entier dans $\mathscr{S}$. Une autre forme du même théorème, qui est plus générale seulement en apparence, établit que si Λ est un réseau de déterminant $d(\Lambda)$ et $\mathscr{S}$ est convexe et symétrique autour de l'origine, comme précédemment, alors $\mathscr{S}$ contient un point de Λ autre que l'origine, si le volume V de $\mathscr{S}$ est plus grand que $2^n d(\Lambda)$. Dans le paragraphe 2, nous démontrerons le théorème de Minkowski et quelques raffinements. Nous ne suivrons pas la démonstration de Minkowski lui-même mais nous déduirons son théorème de celui de Blichfeldt, qui a d'importantes applications par lui-même et qui est intuitement pratiquement évident : si un ensemble de point $\mathscr{R}$ a un volume strictement plus grand que $d(\Lambda)$ alors il contient deux points distincts x_1 et x_2 dont la différence $x_1 - x_2$ appartient à Λ.

Les théorèmes de Blichfeldt et Minkowski peuvent être regardés comme des énoncés établis à propos de la fonction caractéristique d'un ensemble $\mathscr{S}$, qui est la fonction $\chi(x)$ qui est égale à 1 si $x \in \mathscr{S}$ et 0 sinon.

[5] Voir [2].

Traduction des pages 43 à 47 du livre "Geometry of numbers" de Peter M. Gruber et Cornelis G. Lekkerkerker

7. Généralisations du théorème de Minkowski

7.1. Siegel [7a] a donné une formule générale qui implique la vérité du théorème de Minkowski. Cette formule n'est rien de plus qu'une instance particulière du théorème de Parseval pour les séries multiples de Fourier. Elle s'obtient comme suit.

Soit K un convexe borné o-symétrique dans R^n et soit P la cellule $0 \leq x_i < 1 \quad (i = 1, ..., n)$. Soit χ la fonction caractéristique de $\frac{1}{2}K$ et, comme dans la section 6.1, posons $\varphi(x) = \sum \chi(u + x)$. Alors $\varphi(x) = \varphi(x_1, \ldots, x_n)$ est périodique en chaque variable, de période 1. Par conséquent, par le théorème de Parseval,

$$\int_P \varphi^2(x)dx = \sum_{u \in Y} |\alpha(u)|^2, \tag{1}$$

où

$$\alpha(u) = \int_P \varphi(x)e^{-2\pi iu\cdot x}dx = \int_{R^n} \chi(x)e^{-2\pi iu\cdot x}dx \qquad (i = \sqrt{-1}).$$

En particulier, $\alpha(o) = V(\frac{1}{2}K)$.

Maintenant, supposons que K ne contienne pas de point du réseau $\neq o$. Alors les domaines $\frac{1}{2}K + u, u \in Y$ sont mutuellement disjoints. Par conséquent, $\chi(x + u)\chi(x + u') = 0$ si $u \neq u'$.

Puisque $\chi^2(x) = \chi(x)$, il s'ensuit que $\varphi^2(x) = \varphi(x), \quad x \in R^n$. Alors le membre de gauche de (1) est égal à $\alpha(o) = V(\frac{1}{2}K)$. En multipliant les deux membres par $2^n/V(\frac{1}{2}K) = 4^n/V(K)$, on obtient

$$2^n = V(K) + 4^n\{V(K)\}^{-1} \sum_{u \neq 0} |\alpha(u)|^2. \tag{2}$$

Clairement, (2) implique que $V(K) \leq 2^n$. Au vu de nos hypothèses, cela prouve le théorème de Minkowski.

7.2. À partir du théorème 6.1, on peut aisément déduire la généralisation suivante du théorème de Minkowski[6].

Théorème 1. *Soit k un entier positif et soit K un convexe borné o-symétrique de volume $V(K) > 2^n k$. Alors K contient au moins k paires de points $\pm u^i \neq 0$.*

Preuve. Le convexe $\frac{1}{2}K$ a pour volume $V(\frac{1}{2}K) > k$. Par conséquent, par le théorème 6.1, il existe un point z et $k + 1$ points distincts de réseau $v^1, ..., v^{k+1}$, tels que $z + v^i \in \frac{1}{2}K$ pour $i = 1, ..., k + 1$. On peut supposer que les points v^i sont arrangés dans l'ordre lexicographique[7]. On pose maintenant $u^i = v^{i+1} - v^1 \quad (i = 1, ..., k)$. Les points u^i sont tous contenus dans $\mathscr{D}(\frac{1}{2}K) = K$. De plus, ces points sont mutuellement distincts et distincts de o, et la première coordonnée ne s'évanouissant

[6](v.d. Corput [7a] ; sec. 7.4).

[7]Deux points distincts x, y sont dits en ordre lexicographique si $y_i > x_i$, pour le plus petit indice i avec $y_i \neq x_i$.

pas de n'importe quel u^i est positive. Par conséquent, les points $\pm u^i \ \ (i = 1, \ldots, k)$ sont distincts. Cela prouve le théorème.

Dans les résultats précédents, la condition que K soit borné est superflue. En fait, soit K un convexe non borné o-symétrique. On sait déjà (sec. 1.2) qu'alors K est de volume infini. En appliquant le théorème 1 aux parties bornées de K, on trouve que K contient une infinité de points du réseau. Ainsi, dans les théorèmes 5.1 et 7.1, on peut omettre la condition que K soit borné.

Une autre remarque est que, dans le théorème 1, la condition que $V(K) > 2^n k$ peut être remplacée par $V(K) \geq 2^n k$ à la condition que K soit fermé. Cela est prouvé d'une manière similaire à celle utilisée dans le cas où $k = 1$ (voir la remarque 5.1 et la preuve du théorème 5.2).

7.3. En affaiblissant ou en généralisant les conditions de o-symétrie et de convexité, on obtient d'autres généralisations du théorème de Minkowski.

D'abord on considère des convexes bornés H contenant un voisinage de o. Pour eux, on introduit (sec. 1.4) un coefficient d'assymétrie. On prouve (voir Mahler [14a]) le

Théorème 2. *Soit H un convexe borné contenant o comme point intérieur. Soit σ son coefficient d'asymétrie et supposons que $V(H) > (1+\sigma)^n$. Alors H contient un point du réseau $\neq o$.*

Preuve. Posons $H'(1+\sigma)^{-1}H$. Alors $V(H') > 1$. Par conséquent, H' contient deux points x, y, tels que $y - x$ est un point du réseau $\neq o$. On a également $-\sigma^{-1}x \in H'$, par la définition de σ. Donc,

$$\frac{1}{1+\sigma}(y-x) = \frac{1}{1+\sigma}y + \frac{\sigma}{1+\sigma}\left(-\frac{1}{\sigma}x\right) \in H',$$

ou également $y - x \in H$. Cela prouve le théorème.

Sawyer [7a] a appliqué le théorème de Minkowski à une sous-région convenablement choisie de H et a trouvé que dans le théorème 2 la condition que $V(H) > (1+\sigma)^n$ peut être remplacée par $V(H) > (1+\sigma)^n\{1-(1-\sigma^{-1})^n\}$.

Ehrhart [7a, 7c, 7e] a traité les convexes en deux dimensions. Il a démontré que H contient un point du réseau $u \neq o$ si le centre de gravité de H coïncide avec o et si H est fermé et a un volume $V(H) \geq \frac{0}{2}$[8]. Ce résultat est le meilleur possible. De plus, Ehrhart [7b, 7d] a prouvé des résultats similaires pour des solides de révolution en trois dimensions et a dérivé les conditions selon lesquelles un corps convexe deux-dimensionnel contient une paire de points du réseau $\pm u \neq o$.

Dans la suite, considérons des solides étoilés bornés. Mordell [6a] a prouvé le

Théorème 3. *Soit S un solide étoilé borné (o-symétrique). Soit ω son coefficient de concavité et supposons que $V(S) > (2\omega)^n$. Alors S contient un point du réseau $\neq o$.*

[8] ?

Preuve. Posons $S' = (2\omega)^{-1}S$, de telle façon que $V(S') > 1$. Prenons deux points $x, y \in S'$, tels que $y - x$ est un point du réseau $\neq o$. On a nécessairement $-x \in S'$, parce que S' est o-symétrique. Par conséquent, par la définition de ω, le point $y - x = y + (-x)$ appartient à $2\omega S' = S$. Cela prouve le théorème.

7.4. Rado [7a] a considéré une matrice $n \times n$ arbitraire non singulière A et il a appelé un ensemble M dans R^n un A-ensemble s'il vérifie la propriété suivante :

$$A(x - y) \in M \quad \text{si } x, y \in M. \tag{3}$$

En d'autres termes, M est un A-ensemble si l'ensemble différence $\mathscr{D}AM$ est contenu dans M.

Un solide convexe o-symétrique est un A-ensemble, avec A la matrice diagonale d'éléments diagonaux $\frac{1}{2}$. Plus généralement, la propriété (3) est vérifiée par un solide étoilé borné de coefficient de concavité ω si pour A on prend les éléments diagonaux de la matrice diagonale $(2\omega)^{-1}$.

Les considérations précédentes peuvent s'appliquer au cas des A-ensembles. Plus précisément, une application du théorème de Blichfeldt au solide AM, avec la relation $\mathscr{D}AM \subset M$, amène immédiatement au théorème suivant :

Théorème 4. *Soit M un A-ensemble et soit k un entier positif. Supposons que $V(M) > |\det A|^{-1}k$. Alors M contient au moins k paires distinctes de points du réseau $\pm u \neq 0$.*

Dans le cas où A est une matrice diagonale avec des éléments positifs sur la diagonale, ce résultat a été obtenu par v.d. Corput [7a] et également par Hlawka [13a] qui a utilisé la méthode de Siegel. La preuve de Rado est assez différente ; l'idée est la suivante[9].

Soit χ une fonction de Riemann intégrable non négative sur R^n satisfaisant la condition

$$\chi(Ax - Ay) \geq \min\{\chi(x), \chi(y)\} \quad (x, y \in R^n). \tag{4}$$

Par des considérations élémentaires, on peut démontrer qu'une telle fonction satisfait l'inégalité suivante :

$$\chi(o) + \sum_u \chi(u) \geq 2 \sum_u \chi(A^{-1}(x + u)) \qquad (x \in R^n).$$

En intégrant sur une cellule de Y, on obtient

$$\chi(o) + \sum_u \chi(u) \geq 2 \int_{R^n} \chi(A^{-1}x)dx = 2|\det A| \int_{R^n} \chi(x)dx. \tag{5}$$

Si maintenant M satisfait les conditions du théorème 4 et χ est la fonction caractéristique de M, alors (4) est vérifiée et ainsi, on a $\chi(o) + \sum_u \chi(u) > 2k$. L'assertion du théorème 4 découle de cela, au moins dans le cas où M est o-symétrique.

[9] Voir aussi Cassels [7a] et Cassels [GN], p. 75.

En utilisant la méthode de Siegel, Cassels [7a] a démontré que, si (4) est vérifiée,

$$|\det A| \cdot V + (|\det A| \cdot V)^{-1} \sum_{u \neq o} |\alpha(u)|^2 \leq \tfrac{1}{2}\{\chi(o) + \sum_u \chi(u)\}, \tag{6}$$

où

$$V = \int_{R^n} \chi(x)dx \qquad \text{et} \qquad \alpha(u) = \int_{R^n} \chi(A^{-1}x)e^{-2\pi i u \cdot x}dx.$$

Bibliographie

[1] Peter M. Gruber et Cornelis G. Lekkerkerker, *Geometry of Numbers*, Groningen et Amsterdam, London, Wolters-Noordhoff et North-Holland, coll. "Bibliotheca Mathematica" (n° 8), 1987, 2ème éd. (1ère éd. 1969, 510 p.), 731 p.

[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 1959, Springer, Berlin.