IV. Applications aux formes quadratiques définies POSITIVES ET AUX APPROXIMATIONS DIOPHANTIENNES LINÉAIRES.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **8 (1962)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

on pose dét $(G) = |$ dét $(T)| =$ mesure (P) où P est un domaine fondamental de R^n modulo G, par exemple P est le parallèlotope formé par les $\vec{x} = \sum t_i \vec{u}_i$, $0 \leqq t_i < 1$, et le résultat obtenu ci-dessus pour le réseau Z^n se traduit pour un réseau quelconque G de R^n, par l'énoncé que nous appellerons *Théorème de Minkowski-Blichfeldt :*

Si A est un ensemble et G un réseau de R^n

$$\text{mes}\,(A) = \int_{x \varepsilon P} \text{nbre}\,((A+\vec{x}) \cap G)$$

autrement dit la valeur moyenne de nbre $((A+\vec{x}) \cap G)$ est égale à mes $(A)/$dét (G). En particulier il existe $\vec{a}$ tel que

nbre $((A+\vec{a}) \cap G) \geqq$ mes $(A)/$dét G et il existe $\vec{b}$ tel que
nbre $((A+\vec{b}) \cap G) \leqq$ mes $(A)/$dét G.

Si A est irréductible par rapport à G, ou, ce qui revient au même, si la famille des ensembles $(A+\vec{g}, \vec{g} \,\varepsilon\, G)$ est un empilement mes $(A) \leqq \det G$. Si en outre A est borné fermé, on a mes $(A) < 1$.

IV. Applications aux formes quadratiques définies positives et aux approximations diophantiennes linéaires.

Considérons dans R^n la boule de rayon unité centrée à l'origine et ouverte, $B : t_1^2 + t_2^2 + \ldots + t_n^2 < 1$ et soit Ω_n sa mesure. Nous noterons B_r celle de rayon r: $t_1^2 + t_2^2 + \ldots + t_n^2 < r^2$.

Soit G un réseau de R^n. Pour que $G \cap B_r$ se réduise à l'origine, il faut et il suffit que $B_{r/2}$ soit irréductible par rapport à G, autrement dit que les $(B_{r/2} + \vec{g}, \vec{g} \,\varepsilon\, G)$ forment un empilement. On a donc alors mes $(B_{r/2}) \leqq$ dét G, c'est-à-dire $\frac{r^n}{2^n}\,\Omega_n \leqq$ dét G. Si donc $\vec{m}$ est un point de G (autre que l'origine) ayant la distance minima à l'origine

$$|m|^2 \leqq 4\,(\text{dét}\ (G))^2/\Omega_n^{2/n}\,.$$

La constante d'Hermite satisfait donc à

$$\gamma_n \leqq 4/\Omega_n^{2/n}\,.$$

Si l'on remarque que la boule-unité $\sum t_i^2 < 1$ contient le cube $|x_1| < 1/\sqrt{n}, \ldots, |x_n| < 1/\sqrt{n}$ de côté $2/\sqrt{n}$, dont la mesure est $2^n/n^{n/2}$, il vient $\Omega_n > 2^n/n^{n/2}$ et par conséquent

$$\gamma_n < n .$$

On a naturellement un résultat un peu plus fort en utilisant la valeur exacte de Ω_n qui est donnée, à partir des valeurs bien connues $\Omega_1 = 2$, $\Omega_2 = \pi$, par la formule de récurrence $\Omega_n = 2\pi\Omega_{n-2}/n$. En particulier on peut écrire:

$$\gamma_n \leqq (1 + \varepsilon(n))\, 2n/\pi e, \quad \text{avec} \lim_n \varepsilon(n) = 0 .$$

On voit le progrès fait depuis la première majoration d'Hermite. Celle-ci donne la valeur exacte de γ pour $n = 2$, mais devient beaucoup moins bonne que celle de Minkowski pour n grand. Mais en outre la majoration, de Minkowski a été obtenue par une *méthode de portée très générale et qui s'applique non seulement aux boules mais à toute jauge.* Nous appelons ainsi tout ensemble J convexe ($\vec{a} \,\varepsilon\, J$, $\vec{b} \,\varepsilon\, J$ entraîne que le segment joignant a et b est dans J), et symétrique *par rapport à l'origine* [1]).

Pour une jauge J et un réseau G de R^n, la propriété que $J \cap G$ se réduise à l'origine équivaut encore à: $\frac{1}{2} J$ irréductible par rapport à G [2]), ou encore que les ensembles ($\frac{1}{2} J + \vec{g}$, $\vec{g} \,\varepsilon\, G$) forment un empilement, et par conséquent entraîne mes $(J) \leqq 2^n$ dét (G) et mes $(J) < 2^n$ dét G si J bornée fermée. C'est le *théorème de Minkowski sur les jauges.*

Considérons par exemple un système de formes linéaires indépendantes à coefficients réels: $a_{1,1}\, x_1 + \ldots + a_{1,n}\, x_n, \ldots, a_{n,1}\, x_1 + \ldots + a_{n,n}\, x_n$, et soit $D = |\, \text{dét} \, | a_{i,j} ||$. Si les t_i sont des constantes > 0 telles que $t_1 \times t_2 \times \ldots \times t_n = D$, le domaine H de R^n défini par les n inégalités

1) En général, on met dans les propriétés qui définissent les jauges, celles d'être un ensemble borné et d'avoir l'origine comme point intérieur. Ces conditions sont bien vérifiées dans les exemples que nous considérons.

2) $\frac{1}{2} A$ désigne l'ensemble homothétique de l'ensemble A par rapport à l'origine et dans le rapport ½.

$$|a_{1,1}x_1 + \dots + a_{1,n}x_n| \leqq t_1$$
$$\dots\dots\dots\dots\dots$$
$$|a_{n,1}x_1 + \dots + a_{n,n}x_n| \leqq t_n$$

est un parallèlotope fermé de mesure 2^n. Donc il contient un point du réseau Z^n différent de l'origine. Autrement dit les inégalités admettent au moins une solution en entiers $x_1, \dots, x_n$, non tous nuls. C'est le théorème de Minkowski sur *les formes linéaires*. Corollaire: le produit des valeurs absolues des formes est $\leqq D$ pour une infinité de systèmes d'entiers $x_1, \dots, x_n$.

En spécialisant les formes et les coefficients, on obtient le *Théorème fondamental des approximations diophantiennes linéaires:*

Pour tout $t > 1$, les inégalités

$$|x_1 - C_{1,1}y_1 - \dots - C_{1,q}y_q| \leqq 1/t^{q/p}$$
$$\dots\dots\dots\dots\dots$$
$$|x_p - C_{p,1}y_1 - \dots - C_{p,q}y_q| \leqq 1/t^{q/p}$$
$$|y_1| \leqq t, \dots, |y_q| \leqq t$$

ont au moins une solution en entiers $x_1, \dots, x_p, y_1, \dots, y_q$, les y_i étant non tous nuls.

Par exemple, pour $p = 1$, $q = 1$, on a un théorème qu'on peut écrire: pour tout nombre θ réel et toute constante $t > 1$ les inégalités

$$|y\theta - x| \leqslant \frac{1}{t}, \quad 0 < y \leqq t,$$

ont au moins une solution en entiers x, y, et par conséquent l'inégalité

$$\left|\theta - \frac{x}{y}\right| \leqq \frac{1}{y^2}$$

a une infinité de solutions en entiers x, y, avec $y \neq 0$. C'est un énoncé voisin de l'énoncé (D), moins fort par le coefficient numérique (1 au lieu de $1/\sqrt{5}$), plus fort par la présence du paramètre t.

Remarquons que si la fonction

$$f(x_1, \dots, x_n)$$
$$= (a_{1,1}x_1 + \dots + a_{1,n}x_n) \times \dots \times (a_{n,1}x_1 + \dots + a_{n,n}x_n)$$

a ses coefficients entiers, mais est rationnellement indécomposable (les a_{ij} sont donc des nombres algébriques) et si $f(1, 0, ..., 0) = 1$ le théorème du produit montre que pour un entier $h \neq 0$ convenable l'équation $f(x_1, ..., x_n) = h$ a une infinité de solutions en entiers $x_1, ..., x_n$. Si en outre $f(1, 0, ..., 0) = 1$ on peut déduire de deux solutions entières congrues mod h, une solution de $f(x_1, ..., x_n) = 1$ qui a ainsi une infinité de solutions. C'est la généralisation à n variables du résultat (B) sur l'équation de Pell-Fermat [1]).

V. Densité d'empilement de sphères: le résultat de Blichfeldt.

Mais revenons aux formes quadratiques définies. Le résultat de Minkowski, $\gamma_n \leqq n$, qui surprit tous ses contemporains par la simplicité et la généralité de la méthode de majoration utilisée, n'est en fait que la traduction du résultat intuitif que, dans un empilement $(A + \vec{g}, \vec{g} \in G)$ le quotient de l'espace occupé par l'empilement à l'espace total est $\leqq 1$. Tel quel bien entendu l'énoncé n'est pas correct puisque l'espace entier et l'espace occupé par l'empilement sont infinis, il faut se restreindre à un domaine $|x_1| \leqq l, ..., |x_n| \leqq l$, et étudier ce qui se passe quand l croit indéfiniment. On obtient alors comme limite du quotient, que nous appellerons la *densité de l'empilement*, mes $(A)/\text{dét}\, G$. Ne peut-on améliorer cette majoration triviale: densité de l'empilement $\leqq 1$? Il ne peut être question de l'améliorer pour un ensemble A quelconque, même si c'est une jauge, car si A est par exemple le cube défini par les inégalités

$$-\frac{1}{2} < x_1 < \frac{1}{2}, ..., -\frac{1}{2} < x_n < \frac{1}{2},$$

l'empilement $(A + \vec{g}, \vec{g} \in Z^n)$ recouvre l'espace, à un ensemble de mesure nulle près, donc la densité de l'empilement est égale à 1.

---

[1]) Comme les résultats sur l'équation de Pell sont équivalents à des résultats sur les « unités » du corps quadratique engendré par $\sqrt{d}$, les résultats sur l'équation $f(x_1, ..., x_n) = 1$ sont équivalents à des résultats sur les unités d'un corps de nombres algébriques de degré n, associé à f. Le cas considéré ici correspond aux corps dont tous les conjugués sont réels. Le cas général peut être traité à partir d'une extension du théorème sur les formes linéaires au cas des coefficients complexes.