10. Théorème de Hilbert. Fin de la démonstration

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

à **Q**, ainsi que son enveloppe convexe $h(S)$. Puis on considère les sous-ensembles T et T' constitués par les formes $(a_1x_1 + \ldots + a_5x_5)^{2k}$ vérifiant $a_1^2 + \ldots + a_5^2 \leqslant 1$, les a_i appartenant respectivement à **Q** et à **R**. On a l'inclusion $h(T) \subset h(S)$, cependant que $h(T)$ et $h(T')$ ont même intérieur.

On étudie ensuite l'intégrale

$$\int_{\mathscr{S}} (a_1x_1 + \ldots + a_5x_5)^{2k} \, da_1 \ldots da_5 \;/\; \int_{\mathscr{S}} da_1 \ldots da_5$$

$$(\ \mathscr{S} \text{ étant l'hypersphère } a_1^2 + \ldots + a_5^2 \leqslant 1)$$

et on établit, à l'aide d'un banal changement de variables, qu'elle est égale à $c\,(x_1^2 + \ldots + x_5^2)^k$, avec

$$c = \int_{\mathscr{S}} t_1^{2k} \, dt_1 \ldots dt_5 \;/\; \int_{\mathscr{S}} dt_1 \ldots dt_5) > 0\,.$$

La forme $f = c\,(x_1^2 + \ldots + x_5^2)^k$ se trouve par conséquent à l'intérieur de $h(T')$, donc de $h(T)$, donc de $h(S)$, ainsi d'ailleurs que toutes les formes $\lambda f (\lambda$ réel $\in [0, 1])$. Et on peut conclure en choisissant λ tel que $\lambda c \in$ **Q**.

Mais nous pouvons faire un peu mieux: en effet la forme f est à l'intérieur de $h(S)$ tandis que la forme $g = x_5^2$ est dans S donc dans la variété affine support de S; ce qui permet d'en déduire qu'il existe μ_0 réel > 0 tel que, pour tout μ réel $\in [0, \mu_0]$, la forme $f - \mu g$ se trouve dans $h(S)$, ainsi d'ailleurs que toutes les formes $\lambda f - \lambda \mu g$ (λ réel $\in [0, 1]$). Nous choisissons alors λ et μ tels que λc et $\lambda \mu$ soient rationnels et, en utilisant les résultats rappelés sur les ensembles convexes et les vecteurs à coordonnées rationnelles, nous en déduisons l'identité cherchée.

10. Théorème de Hilbert. Fin de la démonstration

Théorème. *Pour tout entier positif k il existe des entiers positifs $A = A(k)$ et $T = T(k)$ tels que tout intervalle $[\, m - A, m\,]$ contienne un nombre qui soit somme de T puissances 2k-ièmes.*

Corollaire (théorème de Hilbert). *Pour tout entier positif n, $g(n)$ est fini.*

On pourra remarquer que la recherche d'une majoration explicite de $g(2k)$ en utilisant notre démonstration dépend essentiellement des constantes M et m_i qui interviennent dans l'identité fondamentale, les autres constantes (celles que l'on trouve dans l'identité relative au problème facile de Waring comme celles qui interviendront dans la suite de la démonstration) étant aisément estimables ou majorables.

Nous allons donc montrer que, pour tout entier m, il existe $r < A$ tel que $m - r$ soit somme de T puissances $2k$-ièmes (rappelons que les diverses constantes que nous allons rencontrer: R, M, ... ont déjà été définies, soit au paragraphe 8 soit au paragraphe 9, et qu'elles dépendent toutes de k, et de k seulement). Si l^k est la plus grande puissance k-ième inférieure ou égale à $\frac{m}{RM}$, nous pouvons tout d'abord écrire

$$m = R.Ml^k + r_1 , \qquad \text{avec} \qquad \frac{1}{2}\left(\frac{m}{RM}\right)^{1/k} \leqslant l \leqslant \left(\frac{m}{RM}\right)^{1/k}$$

$$\text{et} \qquad 0 \leqslant r_1 \leqslant kRM\left(\frac{m}{RM}\right)^{(k-1)/k}$$

(la constante $\frac{1}{2}$ n'est pas essentielle; en toute rigueur, l'inégalité où elle figure n'est vérifiée que pour $m \geqslant m_0(k)$, mais il nous semble inutile d'alourdir notre démonstration avec de tels détails qui ne peuvent avoir d'importance que dans la recherche éventuelle d'une majoration explicite de $g(2k)$).

Nous pouvons maintenant, en utilisant le corollaire du lemme qui énonce l'identité fondamentale, écrire

$$m = \sum_{i=1}^{R} x_i^{2k} + \sum_{h=1}^{QR} u_h^{2k} + r_1 ,$$

les x_i étant des entiers arbitraires inférieurs ou égaux à $\frac{1}{\sqrt{2}}\left(\frac{m}{RM}\right)^{1/2k}$.

Il nous faut alors employer le lemme sur l'identité relative au problème facile de Waring. Nous supposerons que l'on a $|\beta| < |\alpha|$, ce qui est toujours possible par une translation sur n. Définissons

$$a = \max_i a_i , \quad b = \max_i |b_i/a_i|$$

de sorte que pour tout $n \leqslant \frac{1}{a}\left\{\frac{1}{\sqrt{2}}\left(\frac{m}{RM}\right)^{1/2k}\right\} - b$, nous pouvons toujours poser, pour tout i, $x_i = a_i n + b_i$. Ce qui permet d'écrire

$$m = \sum_{j=1}^{S} y_j^{2k} + \sum_{h=1}^{QR} u_h^{2k} + r_1 - (\alpha n + \beta) ,$$

la condition de majoration sur n pouvant s'écrire (ici encore pour m assez grand):

$$n \leqslant C m^{1/2k} .$$

Il est clair qu'en général r_1 est trop grand pour pouvoir être « presque annulé » par le terme $-(\alpha n+\beta)$, mais nous pouvons résoudre cette difficulté de la même manière que nous l'avons fait pour les sommes de cubes. On extraira donc la plus grande puissance $2k$-ième inférieure ou égale à r_1, puis on répétera ce processus:

$$r_1 = {z_1}^{2k} + r_2$$

$$\text{avec} \quad 0 \leqslant r_2 \leqslant k\left\{kRM\left(\frac{m}{RM}\right)^{(k-1)/k}\right\}^{(k-1)/k} = c_2 m^{\gamma^2} \left(\gamma = \frac{k-1}{k}\right)$$

$$r_2 = {z_2}^{2k} + r_3 \qquad \text{avec} \qquad 0 \leqslant r_3 \leqslant c_3 m^{\gamma^3}$$

. . . .

$$r_{t-1} = {z_{t-1}}^{2k} + r_t \qquad \text{avec} \qquad 0 \leqslant r_t \leqslant c_t m^{\gamma^t} .$$

En prenant t tel que γ^t soit supérieur à $1/2k$, il sera alors possible (toujours pour m assez grand) de choisir n de telle façon que le reste final $r = r_t - (\alpha n+\beta)$ vérifie

$$r < \alpha ,$$

et nous avons ainsi obtenu le résultat cherché: pour $A = \alpha$, il existe toujours $r < A$ tel que $m - r$ soit somme de $T = S + QR + t - 1$ puissances $2k$-ièmes.

Appendice

Tableau des valeurs ou des meilleurs encadrements de $G(k)$ et de $g(k)$ actuellement connus pour les petites valeurs de k:

k	2	3	4	5	6	7	8	9	10
$G(k)$	4	4-7	16	6-23	9-36	8-52	32-73	13-99	12-122
$g(k)$	4	9	19-30	37	73	143	279	548	1079