9. Théorème de Hilbert. L'identité fondamentale

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

Nous retiendrons cette identité sous la forme suivante:

LEMME. *Pour tout entier positif* k *il existe des entiers positifs* $R = R(k)$, $S = S(k)$, α, $a_1, \ldots, a_R$, $c_1, \ldots, c_S$, *et des entiers quelconques* β, $b_1, \ldots, b_R$, $d_1, \ldots, d_S$, *tels que l'on ait l'identité*

$$\sum_{i=1}^{R} (a_i n + b_i)^{2k} = \sum_{j=1}^{S} (c_j n + d_j)^{2k} - (\alpha n + \beta) .$$

9. Théorème de Hilbert. L'identité fondamentale

La méthode de Hilbert pour démontrer l'existence de $g(n)$ est fondée sur la donnée, pour tout k, d'une identité de même forme que celle que nous avons vue pour les sommes de bicarrés:

$$M(x_1^2 + x_2^2 + \ldots + x_5^2)^2 = \sum_{i=1}^{N} m_i (a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{i5} x_5)^{2k} .$$

Mais cette identité permet uniquement de démontrer l'existence de $g(2k)$ en supposant établie celle de $g(k)$. Hilbert a donc dû, pour montrer l'existence de $g(n)$ pour les valeurs impaires de n, imaginer un raisonnement par récurrence que nous trouvons personnellement assez compliqué. Après Hilbert, de nombreux mathématiciens se sont efforcés de simplifier sa démonstration mais les améliorations ont pratiquement toutes porté sur l'établissement de l'identité fondamentale.

Nous nous proposons ici de supprimer la seconde partie de la démonstration de Hilbert et de prouver, sans aucune récurrence, que $g(n)$ existe pour tout n pair (d'où il s'ensuit trivialement que $g(n)$ existe aussi pour tout n impair). Outre l'utilisation déjà annoncée des identités du problème facile de Waring, nous aurons besoin au préalable de préciser quelque peu l'identité fondamentale de Hilbert.

LEMME. *Pour tout entier positif* k *il existe des entiers positifs* M, $N = (2k+1) \ldots (2k+5)/24$, $m_1, \ldots, m_{N-1}$, m_N, *avec* M *et* m_N *strictement positifs, et des entiers* $a_{11}, \ldots, a_{15}$, $a_{21}, \ldots, a_{N5}$, *tels que l'on ait l'identité*

$$M(x_1^2 + \ldots + x_5^2)^k = \sum_{i=1}^{N-1} m_i (a_{i1} x_1 + \ldots + a_{i5} x_5)^{2k} + m_N x_5^{2k} .$$

(L'innovation par rapport à l'identité de Hilbert est: m_N est strictement positif).

COROLLAIRE. *Pour tout entier positif k il existe des entiers positifs $M = M(k)$ et $Q = Q(k)$ tels que, pour tout entier l et tout entier $x \leqslant \sqrt{l}$ on ait*

$$Ml^k = x^{2k} + \sum_{1}^{Q} u_h{}^{2k}$$

$$(\text{avec les } u_h \in \mathbf{Z})$$

Ce corollaire est la généralisation du résultat que nous avions utilisé pour disposer d'un « cube arbitraire ».

Pour la démonstration de notre identité, nous utiliserons la méthode de Schmidt, reprise par Ellison, qui s'appuie sur les propriétés des ensembles convexes (dans un espace vectoriel réel). Nous rappelons tout d'abord — sans démonstration — les définitions et résultats dont nous aurons besoin:

— étant donné un ensemble $S \subset \mathbf{R}^N$, on appelle enveloppe convexe (ou clôture convexe) de S et on note $h(S)$ le plus petit ensemble convexe qui contient S (i.e. l'intersection de tous les ensembles convexes qui contiennent S);

— étant donné un ensemble $S \subset \mathbf{R}^N$, tout vecteur $V \in h(S)$ peut s'écrire sous la forme $V = \sum_{i=1}^{N} m_i s_i$, avec $s_i \in S$, $m_i \in \mathbf{R}$, $m_i \geqslant 0$ et $\sum_{i=1}^{N} m_i = 1$. De plus, si tous les vecteurs de S sont à coordonnées rationnelles, et si V est également à coordonnées rationnelles, les m_i peuvent être choisis rationnels;

— le barycentre d'une masse continûment répartie dans un ensemble S borné se trouve toujours à l'intérieur de $h(S)$ (cet intérieur étant « pris » dans la plus petite variété affine support de $h(S)$ — munie de la topologie ordinaire).

Nous allons maintenant donner la démonstration de l'identité de Hilbert telle qu'elle est exposée par Ellison. Il nous suffira ensuite d'un petit complément pour obtenir la précision supplémentaire: m_N est strictement positif.

L'ensemble des formes homogènes de degré $2k$ en 5 variables et à coefficients réels constitue un espace vectoriel sur $\mathbf{R}$ de dimension $N = (2k+1) \ldots (2k+5)/24$ (N est le nombre de termes de la forme générale de degré $2k$ en $x_1, \ldots, x_5$). On considère alors dans cet espace $\mathbf{R}^N$ l'ensemble S de toutes les formes $(a_1 x_1 + \ldots + a_5 x_5)^{2k}$, les a_i appartenant à $\mathbf{Q}$, ainsi que son enveloppe convexe $h(S)$. Puis on considère les sous-ensembles T et T' constitués par les formes $(a_1x_1 + \dots + a_5x_5)^{2k}$ vérifiant $a_1^2 + \dots + a_5^2 \leqslant 1$, les a_i appartenant respectivement à $\mathbf{Q}$ et à $\mathbf{R}$. On a l'inclusion $h(T) \subset h(S)$, cependant que $h(T)$ et $h(T')$ ont même intérieur.

On étudie ensuite l'intégrale

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

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

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

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

La forme $f = c\,(x_1^2 + \dots + x_5^2)^k$ 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 $\lambda c \in \mathbf{Q}$.

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.