Astérisque

MIREILLE CAR

Le problème de Waring pour les corps de fonctions

Astérisque, tome 198-199-200 (1991), p. 77-82

<http://www.numdam.org/item?id=AST_1991__198-199-200__77_0>

LE PROBLEME DE WARING POUR LES CORPS DE FONCTIONS

Mireille CAR

Soit F_q le corps fini à q éléments. L'analogie entre l'anneau Z et l'anneau $F_q[X]$ a conduit à l'étude de nombreux problèmes additifs dans $F_q[X]$ et notemment à l'étude du problème de Waring. Sous sa forme la plus générale, le problème de Waring peut être posé dans un anneau A quelconque. Il s'énonce ainsi. Soit un entier $k \geq 2$. Soit $W(k,A)$ le plus petit entier m, s'il existe, tel que pour tout $a \in A$, l'équation

$$a = a_1^k + \cdots + a_m^k$$

admette une solution $(a_1, \cdots, a_m) \in A^m$. Récemment, L.N. VASERSTEIN a donné une majoration des nombres $W(k,A)$ pour différents anneaux A et pour des algèbres A sur un corps fini F_q, [6], [7]. Cette majoration est de l'ordre de k^3 pour un entier k non divisible par la caractéristique du corps F_q lorsque A est une algèbre sur F_q. Cette majoration est valable lorsque A est l'anneau $F_q[X]$ ou lorsque A est l'anneau des S-entiers d'un corps de fonctions algébriques sur F_q, objet de ce travail.

Toutefois, les problèmes qui m'intéressent sont d'une nature différente comme le montre le cas simple où $A = F_q[X]$.

1 Le problème de Waring pour $F_q[X]$

Pour $A \in F_q[X]$, on s'intéresse aux solutions $(A_1, \cdots, A_m) \in F_q[X]^m$ de l'équation

$$(I.1) \quad A = A_1^k + \cdots + A_m^k$$

S.M.F.
Astérisque 198-199-200 (1991)

réalisant les conditions de degré les plus restrictives possibles, c'est à dire telles que

$$(I.2) \quad degA_i \leq n \qquad \text{si} \qquad k(n-1) < degA \leq kn.$$

On désigne par $g(k)$, resp. $G(k)$, le plus petit entier m s'il existe, tel que pour tout $A \in F_q[X]$, l'équation (I.1) ait une solution vérifiant (I.2), resp. tel que pour tout $A \in F_q[X]$ de degré assez grand, (I.1) ait une solution vérifiant (I.2).

Par une méthode analogue à la méthode du cercle on établit une estimation asymptotique du nombre $r_m(A)$ de solutions de l'équation (I.1) assujetties aux conditions (I.2) valable pour des entiers $k < p$, p désignant la caractéristique du corps F_q. On obtient alors pour $k < p$:

$$(I.3) \quad G(k) \leq k2^{k-1} + 1 \quad , cf \cdot [1], [3],$$

$$(I.4) \quad G(2) \leq 4 \qquad et \qquad G(2) = 3 \quad \text{si} \quad q \geq 53, cf \cdot [2] \cdot$$

On a peu de renseignements sur $g(k)$. Jean-Pierre SERRE a établi que $g(2) = 3$ pour $q \geq 5$. Ce résultat n'a pas été publié.

2 Le problème de Waring pour les anneaux d'entiers des corps de fonctions algébriques sur F_q.

Soit L une extension algébrique finie séparable du corps $F_q(X)$.

L'analogie entre corps de nombres et corps de fonctions algébriques sur F_q laissait espérer que les méthodes introduites par C.L. SIEGEL, cf.[4], [5], pour l'étude du problème de Waring dans les corps de nombres pouvaient être adaptées à l'anneau B fermeture intégrale de $F_q[X]$ dans L. Cet espoir était raisonnable. La seule difficulté, en dehors des difficultés techniques, était de bien poser le problème. Bien poser le problème consiste à avoir des conditions faisant intervenir tous les prolongements à L de la valuation à l'infini v de $F_q(X)$ définie par $v(A/B) = degB - degA$ si A et B sont des polynômes non nuls.

Pour exploiter l'analogie entre L et les corps de nombres, on fait une distrinction entre valuations P-adiques de L et valuations prolongeant la valuation à l'infini v. Cette distinction est artificielle. En effet, soit S un ensemble fini non vide de valuations de L, soit O_S l'ensemble des S-entiers de L, i.e. l'ensemble des $a \in L$ tels que $w(a) \geq 0$ pour toute valuation $w \notin S$. Les résultats établis pour l'anneau B se généralisent à l'anneau O_S.

On s'intéresse aux représentations de $b \in O_S$ comme somme

$$(II.1) \qquad b = b_1^k + \cdots + b_m^k,$$

telles que

$$(II.2) \qquad w(b_j) \geq [w(b)/k]$$

pour tout $j \in \{1, \cdots, m\}$, tout $w \in S$.

On note $r_m(b)$ le nombre de ces représentations et on désigne par $G(k)$ le plus petit entier m, s'il existe tel que $r_m(b) > 0$ pour tout les $b \in O_S$ pour lesquels la somme

$$(II.3) \qquad h(b) = \sum_{w \in S} f_w w(b)$$

est assez petite, f_w désignant le degré de la place w.

Dans le cas où $L = F_q(X)$ et S est réduit à la seule valuation à l'infini v, $O_S = F_q[X]$, la condition (II.2) se réduit à la condition (I.2) et $h(b) = -deg(b)$. On retrouve le problème de Waring posé au paragraphe I. Dans le cas où S est l'ensemble $\{w_1, \cdots, w_r\}$ de tous les prolongements de w à L, $O_S = B$, et, pour $b \in B$, la condition (II.2) s'écrit aussi

$$(II.2)' \qquad -w_i(b_j) \leq N_i \quad \text{si} \quad k(N_i - 1) < -w_i(b) \leq kN_i,$$

ce qui est une généralisation de la condition (I.2).

On a le théorème suivant :

Théorème 2.1 *Pour* $2 \leq k < p$, *on a*

$$(II.4) \qquad G(k) \leq 1 + k2^{k-1} Card(S) .$$

La démonstration de ce théorème est basée sur la méthode du cercle. Elle est très longue. J'indique seulement les étapes importantes. Tout d'abord on démontre qu'il existe $y \in L$ possédant la propriété suivante : $F_q[y]$ est inclus dans l'anneau de valuation de w si et seulement si $w \notin S$, ce qui prouve que y est transcendant sur F_q, que L est une extension algébrique de $F_q(y)$ nécessairement finie et que O_S est la clôture entière de l'anneau $F_q[y]$. Il suffit donc de faire la démonstration lorsque $S = \{w_1, \cdots, w_r\}$ et que $O_S = B$.

On se place dans le cas où $O_S = B$. Si $\vec{N} = (N_1, \cdots, N_r) \in Z^r$, si $A \in B$, on désigne par $R(m, \vec{N}, A)$ le nombre de solutions $(A_1, \cdots, A_m) \in B^m$ de l'équation

$$A = A_1^k + \cdots + A_m^k,$$

telles que

$$-w_i(A_j) \leq N_i,$$

pour tout $i = 1, \cdots, r$, tout $j = 1, \cdots, m$. Si $\vec{N} \in Z^r$ et $A \in B$ vérifient

$$(II.5) \qquad k(N_i - 1) < -w_i(A) \leq kN_i,$$

on a

$$r_m(A) = R(m, \vec{N}, A).$$

Pour $\vec{N} \in Z^r$, soit

$$(II.6) \qquad s(\vec{N}) = \sum_{i=1}^{r} f_{w_i} N_i.$$

On note que lorsque $A \in B$ et $\vec{N} \in Z^r$ sont liés par (II.5) $s(\vec{N})$ tend vers $+\infty$ si et seulement si $h(A)$ tend vers $-\infty$. Pour démontrer le théorème on fixe un entier $m \geq 1 + k2^{k-1}Card(S)$ et on montre que pour tous les $A \in B$ pour lesquels la somme $s(\vec{N})$ est assez grande, on a $R(m, \vec{N}, A) > 0$, $\vec{N}$ et A étant toujours liés par (II.5). On ne sait pas obtenir d'estimation asymptotique des nombres $R(m, \vec{N}, A)$ pour tous les éléments A de B, mais seulement pour les éléments A vérifiant la condition supplémentaire

$$|f_{w_i} N_i - \frac{1}{r} s(\vec{N})|$$