SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

W. J. ELLISON

Waring's Problem for Fields

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 8, p. 1-8

<http://www.numdam.org/item?id=STNB_1970-1971____A8_0>

Séminaire de Théorie des Nombres
Année 1970-1971 - exposé n° 10

9 Décembre 1970

WARING'S PROBLEM FOR FIELDS

by

W. J. ELLISON

-:-:-:-

THE ORIGINAL WARING'S PROBLEM. Given a positive integer k does there exist an integer $g(k)$ such that every positive integer is a sum of at most $g(k)$ k^{th} powers of positive integers ?

This was proposed by Waring in 1770 and answered by Hilbert in 1909. The proof of the theorem is quite difficult. (See the paper in the Jan. issue of the American Math. Monthly if you wish to read about the problem ad nauseum).

It is natural to pose the same problem about other common rings, say for example, the ring of integers in an algebraic number field. The combined work of Siegel, Birch and Ramanujam show that given a number field K and a positive integer k then if we denote by $A(k)$ the subring of the ring of integers of K which can be written as a sum of k^{th} powers of integers there exists a constant $g(k)$ such that every integer in $A(k)$ is a sum of at most $g(k)$ k^{th} powers of integers. There is also a very nice paper by Joly in a recent issue of Acta Arithmetica.

The proof of this theorem is quite complicated.

Instead of asking Waring's problem about rings we ask it about fields. The following definition is useful.

DEFINITION. Let K be a field. The Waring's theorem of exposent k holds if every totally positive $\alpha \in K$ can be written in the form

$$\alpha = \sum_{i=1}^{n} a_i^k ,$$

where $a_i \in K$ for $1 \leq i \leq n \leq g(K,k) < \infty$ and

(1) The a_i are all totally positive.

(2) $g(K,k)$ depends only on K and k.

In some circumstances it is convenient to drop condition (1); then we say that the weak Waring theorem of exponent k holds.

THEOREM 1. Let K be a field with the following two properties:

(I) Every totally positive $\alpha \in K$ can be written as a sum of at most s squares in K.

(II) Let k be a fixed positive integer and suppose that for each totally positive $\alpha \in K$ there exists $\beta \in K$, depending on α, which satisfies

$$0 < \frac{s}{s+2k} \alpha < \beta^k < \alpha$$

for all orderings $<$ of K.

Then, (a) The weak Waring theorem of exponent k holds in K

(b) If the β corresponding to each $\alpha \in K$ can always be chosen to be totally positive, then Waring's theorem of exponent k holds in K.

COROLLARY. Waring's theorem holds for all exponents in Q.

Proof. - Every positive rational is a sum of at most 4 squares of rationals, so $s = 4$.

If k is a positive integer and α is a positive rational then we can always find a positive rational β such that

$$\frac{4}{4+2k}\ \alpha < \beta^k < \alpha \ .$$

Thus $g(Q,k) < \infty$ for each positive k.

We shall give some more corollaries later.

The proof of the theorem is elementary (i. e. simple), we shall need the following lemma due to Hilbert.

LEMMA. (Hilbert) - For every pair of positive integers k and s there are : an integer

$$M = \frac{(2k+3)\ \ldots\ (2k+2+s)}{s\ !}\ ;$$

positive rational numbers λ_i for $0 \le i \le M$ and integers α_{ij}, $0 \le i \le s$, $0 \le j \le M$ such that we have an identity

$$(x_o^2 + \ldots + x_s^2)^{k+1} = \sum_{j=0}^{M} \lambda_j (\alpha_{oj} x_o + \ldots + \alpha_{sj} x_s)^{2k+2} \ .$$

Proof. - See Hilbert or the Amer. Math. Monthly.

Proof of theorem 1 - Differentiate the above identity twice with respect to x_o

$$(1) \qquad (x_o^2 + \ldots + x_s^2)^k + 2k x_o^2 (x_o^2 + \ldots + x_s^2)^{k-1} = (2k+1) \Sigma \lambda_j \alpha_{oj} (\alpha_{oj} x_o + \ldots + \alpha_{sj} x_s)^{2k} .$$

If $a_i \in K$ and $1 - a_i^2 >$ for all orderings of K then by hypothesis (I) we have

$$1 - a_i^2 = b_{1i}^2 + \ldots + b_{si}^2 \ , \quad b_{ji} \in K \ .$$

Substitute $x_o = a_i$, $x_j = b_{ji}$ in (1) and obtain

$$(2) \qquad 1 + 2k a_i^2 = (2k+1) \sum_{j=0}^{M} \lambda_j \alpha_{oj}^2 (\alpha_{oj} a_i + \ldots + \alpha_{sj} b_{sj})^{2k} \ .$$

If $a \in K$ and $0 \le a < 1$ for all orderings of K, then by hypothesis (I) we have

$$a = a_1^2 + \ldots + a_s^2$$

and

$$0 \le a_i < 1 \quad \text{for} \quad 1 \le i \le s \ , \quad \text{i.e} \quad 1 - a_i^2 > 0 \quad \text{for} \quad 1 \le i \le s$$

substitute the a_i into (2) and add the resulting set of s equations to obtain

$$(3) \qquad s + 2k a = \sum_{i=1}^{s} \sum_{j=0}^{M} \lambda_j \alpha_{oj}^2 (2k+1) (\alpha_{oj} a_i + \ldots + \alpha_{sj} b_{si})^{2k} \ .$$

Let A_k = l. c. m. of the denominators of the λ_j, so that $A_k\lambda_j = \Lambda_j \in Z^+$.

$$(4) \qquad s A_k + 2k A_k a = \sum_i \sum_j \Lambda_j \alpha_{oj}^2 (2k+1)(\alpha_{oj} a_i + \ldots + \alpha_{sj} b_{si})^{2k} = \sum_{i=1}^{n} \zeta_i^{2k} ,$$

where $\zeta_i \in K$ and $n \leq (2k+1).\ s.\ \sum_{j=0}^{M} \Lambda_j \alpha_{oj}^2$.

Now if $\alpha \in K$ is totally positive then so is $\dfrac{A_k(s+2k)}{\alpha}$. Hence by hypothesis (II) there exists a $\beta \in K$ such that

$$0 < \frac{s}{s+2k} \left(\frac{A_k(s+2k)}{\alpha}\right) < \beta^k < \left(\frac{A_k(s+2k)}{\alpha}\right)$$

for all orderings $<$ of K.

Put $a = \dfrac{\alpha\beta^k - s A_k}{2k A_k}$, then $0 \leq a < 1$ and substuting into (4) we have

$$\alpha\beta^k = \sum_{i=1}^{n} \zeta_i^{2k}$$

$$\alpha = \sum_{i=1}^{n} \left(\frac{\zeta_i^2}{\beta}\right)^k .$$

The two assertions of the theorem now follow.

The upper bound for $g(K,k)$ is given by

$$g(K,k) \leq (2k+1)\, s \sum_{j=0}^{M} \Lambda_j \alpha_{oj}^2 .$$

This upper bound depends very weakly on the field K; it is a function of k and s only.

If we are interested in numerical estimates for $g(K,k)$ then we can improve this upper bound. We look at (4) again

$$(4') \qquad s A_k + 2k A_k a = \sum_{j=0}^{M} \sum_{i=1}^{s} \Lambda_j \alpha_{oj} (2k+1)(\alpha_{oj} a_i + \ldots + \alpha_{sj} b_{si})^{2k}$$

$$= \sum_{i=1}^{m} \eta_i^{2k} r_i^k , \quad \text{where } \eta_i \in K ,\ r_i \in Q^+ ,$$

and $m \leq g(Q,k)(M+1)$.

It is trivial that $g(Q,k) \leq G(k)$ and one can obtain good upper estimates for $G(k)$ by analytic methods.

COROLLARY 2. If K is an algebraic number field then Waring's theorem is true for all exponents.

Proof. - It is a classical theorem that that every totally positive algebraic number is a sum of at most 4 squares. Thus, hypothesis (I) is satisfied with $s = 4$.

If K is a totally imaginary number field, then every element of K is totally positive and we can satisfy hypothesis (II) with $\beta = 1$. Suppose now that K is not totally imaginary. Denote the real conjugate fields by $K^{(1)}, \ldots, K^{(r)}$. We need the following lemma

LEMMA. Let $\varepsilon > 0$ and $\eta_1, \ldots, \eta_r$ be given real numbers, then there exists a $\beta \in K$ such that

$$|\beta^{(i)} - \eta_i| < \varepsilon \quad \text{for} \quad 1 \le i \le r .$$

Proof. - Let $K = Q(\theta)$ so that $K^{(i)} = Q(\theta^{(i)})$ for $1 \le i \le r$. Let $f(x)$ be the polynomial of degree $(r-1)$ with real coefficients which takes the values $\eta_i + \frac{1}{2}\varepsilon$ at $x = \theta^{(i)}$ for $1 \le i \le r$.

Let $g(x)$ be a polynomial with rational coefficients and degree $(r-1)$ such that

$$|f(x)-g(x)| < \frac{1}{2}\varepsilon \quad \text{at} \quad x = \theta^{(1)}, \ldots, \theta^{(r)} .$$

Put $\beta = g(\theta)$, then $\beta^{(i)} = g(\theta^{(i)})$ for $1 \le i \le r$ and

$$|\beta^{(i)} - \eta_i| < \varepsilon \quad \text{for} \quad 1 \le i \le r .$$

If $\alpha \in K$ and α is totally positive, then $\alpha^{(i)} > 0$ for $1 \le i \le r$. To satisfy hypothesis (II) of theorem 1 we must find a $\beta \in K$ such that

$$0 < \{\frac{2}{2+k}\,\alpha^{(i)}\} < \beta^{(i)} < \{\alpha^{(i)}\}^{1/k} \quad \text{for} \quad 1 \le i \le r .$$

The existence of such a β follows from the lemma by taking

$$\eta_i = \frac{1}{2}\{(\frac{2}{2+k} \cdot \alpha^{(i)})^{1/k} + (\alpha^{(i)})^{1/k}\} \quad \text{for} \quad 1 \le i \le r$$

and ε small enough.

COROLLARY 2. If K is a non-real field of characteristic 0 (i.e. -1 is a sum of squares in K) then Waring's theorem holds for every exponent.

Proof. - Let $-1 = a_1^2 + \ldots + a_t^2$, then $\alpha \in K$ can be written as

$$\alpha = \left(\frac{\alpha+1}{2}\right)^2 - 1 \cdot \left(\frac{\alpha-1}{2}\right)^2 ,$$

$$\alpha = \left(\frac{\alpha+1}{2}\right)^2 + \sum_{i=1}^{t} \left(\frac{a_i(\alpha-1)}{2}\right)^2$$

Thus, hypothesis (I) holds with $s \leq t+1$ and hypothesis (II) is trivially satisfied.

We now look at a slightly different problem. We used hypothesis (I) quite a lot in the proof of theorem 1, but hypothesis (II) is only used at one point. The proof of theorem 1 can be used to prove the following theorem.

THEOREM 1'. Let K be a field with the following two properties

(a) Every totally positive $\alpha \in K$ can be written as a sum of at most s squares in K.

If we are given a positive integer k and a totally positive $\alpha \in K$ such that there exists a $\beta \in K$, depending on α, such that

$$0 < \frac{s}{s+2k}\left(\frac{s+2k}{\alpha}\right) < \beta^k < \frac{s+2k}{\alpha}$$

for all orderings of K, then α can be written in the form

$$\alpha = \sum_{i=1}^{n} a_i^k ,$$

where $a_i \in K$ and $n \leq g(s,k) < \infty$.

We can apply theorem 1' to fields which do not have property (II) of theorem 1, for example function fields of the type $K = K_1(X)$, where K_0, K_1 is a real field.

Suppose for example we take $K = \mathbb{R}(X_1, \ldots, X_n)$, $\mathbb{R}$ = real numbers. It is a well known theorem of Pfister that every totally positive element of $\mathbb{R}(X_1, \ldots, X_n)$ is a sum of at most 2^n squares, so $s \leq 2^n$.

If one is given a totally positive element of $\mathbb{R}(X_1,\ldots,X_n)$ then it seems to be rather difficult to check that the second condition of theorem 1' is satisfied (By the way the condition is sufficient but not necessary). One can prove the following lemma which is sometimes useful in helping to verify the existence of a β with the required properties.

LEMMA. Let $f(\underline{X})$ be a strictly positive definite, everywhere defined, continuous real valued function on $\mathbb{R}^n$. Suppose that there exist real numbers a, b, δ and a rational function $h(\underline{X}) \in (X_1,\ldots,X_n)$ such that

(0) $h(X)$ has no real poles in the region defined by $X_1^2+\ldots+X_n^2 \leq c+1$

(1) $0 < a < \dfrac{f(\underline{X})}{h^k(\underline{X})} < b < \infty$

(2) $0 < \delta \leq f(\underline{X})$

for all $X \in \mathbb{R}^n$ which satisfy $X_1+\ldots+X_n \geq c$, where $c > 1$ is a fixed real number.

Then, given $\varepsilon > 0$ there exists a function $\gamma(\underline{X}) \in \mathbb{R}(X_1,\ldots,X_n)$ such that

$$0 < (a-\varepsilon) < \frac{f(\underline{X})}{\gamma^k(\underline{X})} < (b+\varepsilon) \quad \text{for all } X \in \mathbb{R}^n .$$

The proof is straightforward and extremely boring.

In the special case $n = 1$ we can prove much more.

THEOREM 2. Let $f(\underline{X}) \in \mathbb{R}(X)$ be positive definite; a necessary and sufficient condition that $f(X)$ can be written as a sum of k^{th} powers of positive definite functions in $\mathbb{R}(X)$ is that $f(X)$ is of the form

$$f(X) = \prod_{i=1}^{n} (X-\alpha_i)^{2kr_i} \frac{G(X)}{H(X)} ,$$

where $\alpha_i \in \mathbb{R}$; $r_i \in \mathbb{Z}$; $G(X)$ and $H(X)$ are strictly definite polynomials in $\mathbb{R}[X]$ of degrees $2\ell_1 k$ and $2\ell_2 k$.

Moreover if $f(X)$ is a sum of k^{th} powers of positive definite functions in $\mathbb{R}(X)$ then $f(X)$ can be written as a sum of atmost $g(k)$ such

functions. An upper bound for $g(k)$ is $\frac{2(2k+3)(2k+4)}{2} = 2(2k+2)(2k+3)$.

The proof is straightforward.

SOME PROBLEMS

(a) If Waring's problem holds for the field K, then what is the best possible value for $g(K,k)$? Even for $K = \mathbb{Q}$ this seems to be hard. The known results are $g(\mathbb{Q},2) = 4$, $g(\mathbb{Q},3) = 3$, $g(\mathbb{Q},4) = 15$.

(b) Let K be a real field. If given integers k and n, does there exist a constant $C(K,n,k)$ such that if $f(\underline{X})$ is a sum of k^{th} powers in $K(X_1,\ldots,X_n)$ then $f(\underline{X})$ can be written as a sum of at most $C(K,n,k)$ k^{th} powers ? [This is known to be true when $K = \mathbb{R}$, $k = 2$, n arbit. and when $K = \mathbb{R}$, $n = 1$, k arbit.]

(c) If $f(X) \in K[X]$ is a sum of k^{th} powers in $K(X)$, then can $f(X)$ be written as a sum of k^{th} powers in $K[X]$?

(d) Give a "nice" description of the elements of $K(X_1,\ldots,X_n)$ which can be expressed a sum of k^{th} powers in $K(X_1,\ldots,X_n)$. [The case $k = 2$ and K a real field is Hilbert's 17^{th} problem. Artin showed that $f(\underline{X})$ is a positive definite function on K in the case when K is a subfield of the real numbers with precisely one ordering].

-:-:-:-

W. J. ELLISON
U. E. R. de Mathématiques
et d'Informatique
Université de Bordeaux 1
351, cours de la Libération
33 - T A L E N C E