ACTA ARITHMETICA
XLII (1982)

On the nonessential discriminant divisor of an algebraic number field

by

JAN ŚLIWA (Wrocław)

Let K/Q be a finite extension, R_K the ring of integers of K and θ a primitive element belonging to R_K. The index of the subring of R_K generated by θ in the ring R_K we shall call the index of θ and denote by $i(\theta)$. Obviously

$$(1) \qquad d(\theta) = i(\theta)^2 d_K,$$

where $d(\theta)$ is the discriminant of θ and d_K the discriminant of K.

The greatest common divisor of indices of all primitive integers of K is called the *nonessential discriminant divisor of* K and denoted by $i(K)$.

Let p be a rational prime and f a positive integer. Denote by $g(f)$ the number of prime ideal divisors of p in R_K which have degree f and by $s(f)$ the number of irreducible polynomials of degree f over the field of p elements.

R. Dedekind ([5]) showed that $p \mid i(K)$ if and only if there exists an f such that

$$g(f) > s(f).$$

From this criterion it follows that if $p \mid i(K)$ then $p < [K:Q]$, and, as shown by M. Bauer ([1]), if $p < n$ then there exists a field K of degree n such that $p \mid i(K)$.

Obviously, if $R_K = Z[\theta]$ with $\theta \in R_K$, then $i(K) = 1$. K. Hensel ([10]) has constructed a form (called the *indicial form of* K) of degree $n(n-1)/2$ in $n-1$ variables (where $n = [K:Q]$) such that the set of the moduli of values attained by it as the arguments vary independently over Z forms the set of all indices of integers of K.

Using this same approach, M. Hall, Jr. ([9]) proved that $I(K) = \min_{\theta \in R_K} i(\theta)$ is unbounded as K ranges over all cubic fields.

D. S. Dummit and H. Kisilevsky ([6]) investigated the values of $I(K)$ for cubic cyclic fields. They proved that $I(K)$ is unbounded as K

runs over the set of cubic subfields of the lth cyclotomic fields, where $l \equiv 1 \pmod 3$ is prime, and that there exist infinitely many cubic cyclic fields K with $I(K) = 1$. They computed also the value of $I(K)$ for many examples of cubic fields.

The same subject was considered by M. N. Gras ([8]). She gave, again in the cyclic cubic case, a criterion for $I(K)$ to be 1 in terms of solvability of some diophantine equation.

The minimal number of generators needed to generate R_K over Z was determined by P. Pleasants ([13]). To formulate his result we have to introduce some notations.

If $q = p^k$, let $\pi(q, f)$ be the number of irreducible polynomials of degree f over a finite field with q elements. For any prime ideal $\mathfrak{p}$ of R_K dividing p, denote by $m_\mathfrak{p}$ the minimal m such that

$$\pi(N_{K/Q}(\mathfrak{p}^m), \deg\mathfrak{p}) \geqslant g(\deg\mathfrak{p})$$

and let

$$m_p(K) = \max_{\mathfrak{p}|p} m_\mathfrak{p}. \tag{2}$$

Obviously $m_p = 1$ for all but a finite number of p's. Now put $m(K) = \max_p m_p(K)$.

Pleasants showed that the minimal number of generators of R_K is equal to $m(K)$, unless $m(K) = 1$, in which case two generators may be needed.

From this result it follows immediately that

$$p^{m_p(K)-1} \mid i(K),$$

but $m_p(K)-1$ need not be equal to $\varkappa_p(K)$, the highest power of p dividing $i(K)$.

In this paper we shall study $\varkappa_p(K)$ under the assumption that all prime divisors of p in R_K are unramified.

The best result in this direction was obtained by H. T. Engstrom ([7]). One of his results states that if p splits in K then this maximal power equals

$$\sum_m \left[\frac{n}{p^m}\right]\left\{n - p^m \frac{\left[\frac{n}{p^m}\right]+1}{2}\right\} \tag{3}$$

where n is the degree of the extension K/Q.

He confirmed also the conjecture of O. Ore ([12]) that $\varkappa_p(K)$ is in general not determined by the prime ideal decomposition of p.

However, from our result it will follow that if p is unramified in K then $\varkappa_p(K)$ depends only on the form of the decomposition of p. Engstrom has conjectured that $\varkappa_p(K)$ attains its maximal value if p splits in K. We confirm this conjecture under the restriction that p is unramified.

A. A. Sukallo ([14]) investigated the case in which

$$pR_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}, \quad k > p, \ \deg\mathfrak{p}_i = 1 \text{ for } i = 1, \ldots, k,$$

and proved that if $e_1 \geqslant e_2 \geqslant \ldots \geqslant e_k$, and S, T, R are determined by

$$S = \sum_{i=1}^{p} e_i, \quad [K:Q] = ST+R \quad (0 \leqslant R < S),$$

then $\varkappa_p(K) = \frac{1}{2}ST(T-1)+TR$.

For other results connected with this subject see [2], [3], [4], [15], [16].

All the facts used in the paper and most of the common notations can be found in [11].

1. Let p be a fixed rational prime and Ω_p the maximal unramified extension of Q_p. Ω_p is the composite of all $Q_p(\zeta_m)$ with $p \nmid m$, where ζ_m denotes the mth primitive root of unity. In the following v will stand for the additive valuation of Ω_p normalized by $v(p) = 1$. For any positive integer f we denote by L_f the unique subfield of Ω_p of degree f over Q_p and by R_f the ring of integers of L_f. Thus $L_f = Q_p(\zeta_{p^f-1})$ and the extension L_f/Q_p is cyclic. We shall denote by G_f the Galois group of this extension.

If we put

$$A_f = \{\gamma \in R_f \colon \gamma^{p^f} = \gamma\},$$

then $0 \in A_f$ and A_f is a set of representatives of $R_f \bmod pR_f$ because each nonzero class of R_f/pR_f contains the (p^f-1)th root of unity ([11], Corollary 2 to Theorem 5.3). Hence every element $a \in R_f$ can be uniquely represented as the sum of a convergent series

$$a = \sum_{m=0}^{\infty} \gamma_m p^m, \quad \gamma_m \in A_f \quad ([11], \text{ Theorem } 5.1).$$

If $\sigma \in G_f$ then $\sigma(A_f) = A_f$ and if $f' \mid f$ then $A_{f'} \subseteq A_f$. Observe further that if $a \in R_{f_1} \cap R_{f_2}$ and

$$a = \sum_{m=0}^{\infty} \gamma_m^{(1)} p^m = \sum_{m=0}^{\infty} \gamma_m^{(2)} p^m$$

with $\gamma_m^{(1)} \in A_{f_1}$, $\gamma_m^{(2)} \in A_{f_2}$, then

$$\gamma_m^{(1)} = \gamma_m^{(2)} \quad \text{for} \quad m = 1, 2, \ldots$$

We shall denote the unique $\gamma_m \in A_f$ in the expansion of a by $t_m(a)$ and let $s_m(a)$ denote the sum $\sum_{i=0}^{m-1} t_i(a) p^i$.

From a previous remark it follows that if $a \in R_f$ then $t_m(a)$, $s_m(a)$ do not depend on the choice of f.

Further, we have

$$\tau(t_m(\alpha)) = t_m(\tau(\alpha)) \tag{1.1}$$

for $\tau \in G_f$ and $m = 0, 1, 2, \ldots$

Indeed, as $s_k(\alpha) = \alpha + p^k\gamma_1$, $s_k(\tau(\alpha)) = \tau(\alpha) + p^k\gamma_2$ with $\gamma_1, \gamma_2 \in R_f$, we have

$$\tau(s_k(\alpha)) - s_k(\tau(\alpha)) \in p^k R_f. \tag{1.2}$$

Assume that for given $\alpha \in R_f$, $\tau \in G_f$ (1.1) hold if $m < M$. Then

$$\tau(s_{M+1}(\alpha)) - s_{M+1}(\tau(\alpha)) = p^M\big(\tau(t_M(\alpha)) - t_M(\tau(\alpha))\big),$$

and so by (1.2)

$$\tau(t_M(\alpha)) \equiv t_M(\tau(\alpha)) \pmod p.$$

Both sides of this congruence belong to A_f, and so it holds if and only if they are equal.

Let $\varphi(x) \in Z_p[x]$ be an irreducible unitary polynomial of degree f, such that its root α generates L_f over Q_p. Any such polynomial will be called unramified.

For $m \geqslant 1$ we shall write $\varphi_{m,\alpha}(x)$ for the minimal polynomial of $s_m(\alpha)$.

If β is another root of $\varphi(x)$ then α and β are conjugated and so are $s_m(\alpha)$ and $s_m(\beta)$ (this follows from (1.1)). Hence $\varphi_{m,\alpha}(x) = \varphi_{m,\beta}(x)$. Therefore to each unramified polynomial $\varphi(x)$ and a positive integer m we can attach a unique irreducible polynomial $\varphi_m(x)$, starting with any of its roots.

Let

$$G_m(\alpha) = \{\sigma \in G_f\colon \sigma(\alpha) \equiv \alpha \pmod{p^m}\} = \{\sigma \in G_f\colon s_m(\sigma(\alpha)) = s_m(\alpha)\}. \tag{1.3}$$

Then

$$\varphi_m(x) = \prod_{\tau \in G_f/G_m(\alpha)} \big(x - \tau(s_m(\alpha))\big) \equiv \prod_{\tau \in G_f/G_m(\alpha)} (x - \tau(\alpha)) \pmod{p^m}$$

and hence

$$\varphi(x) \equiv \varphi_m(x)^{|G_m(\alpha)|} \pmod{p^m}. \tag{1.4}$$

Denote by $\Phi(m, f)$ the set of all minimal polynomials of $s_m(\alpha)$ for $\alpha \in R_f$. It is a finite set and can be written as a disjoint union

$$\Phi(m, f) = \bigcup_{d|f} \Phi_d(m, f),$$

where $\Phi_d(m, f)$ consists of those polynomials in $\Phi(m, f)$ which have degree d. Obviously $\Phi_d(m, f)$ is the same for all f divisible by d; hence we shall denote it by $\Phi_d(m)$.

With each $\psi \in \Phi_d(m)$ we associate the set of all its roots, and counting

the number of elements in $R_f/p^m R_f$ we arrive at

$$p^{mf} = \sum_{d|f} d|\Phi_d(m)|;$$

thus

$$|\Phi_d(m)| = \frac{1}{d}\sum_{d_1|d} \mu(d_1) p^{md/d_1}.$$

This last number is obviously equal to $\pi(p^m, d)$ — the number of irreducible polynomials of degree d over the field of p^m elements.

Let $\Psi(m, f)$ be the subset of $\Phi(m, f)$ consisting of those polynomials whose reduction $\operatorname{mod} p$ is irreducible over Z/pZ. Obviously

$$\Psi(m, f) \subset \Phi_f(m).$$

The elements of $\Psi(m, f)$ correspond to those $\alpha \in R_f$ for which $s_1(\alpha)$ generates L_f over Q_p.

If $\varphi_1 \in \Phi(m, f)$, $\varphi_2 \in \Phi(k, f)$, $m < k$ and $\varphi_1(x)$, $\varphi_2(x)$ are minimal polynomials of $s_m(\alpha)$, $s_k(\alpha)$ with the same α, then we shall say that $\varphi_2(x)$ is an extension of $\varphi_1(x)$.

Observe that to each $\varphi(x) \in \Psi(m, f)$ there exist exactly p^f elements of $\Psi(m+1, f)$ which extend $\varphi(x)$. This gives

$$|\Psi(m, f)| = p^{(m-1)f}\pi(p, f).$$

2. Let K/Q be a finite extension and p a rational prime unramified in K and let

$$pR_K = \mathfrak{p}_1 \ldots \mathfrak{p}_\varrho, \quad \deg_{K/Q}\mathfrak{p}_i = f_i, \quad i = 1, \ldots, \varrho. \tag{2.1}$$

If $\alpha \in R_K$ is such that $K = Q(\alpha)$ and $f(x)$ is its minimal polynomial, then $f(x)$ factorizes in $Z_p[x]$:

$$f(x) = \varphi_1(x) \ldots \varphi_\varrho(x) \tag{2.2}$$

where $\varphi_i(x)$ are unramified and $\deg \varphi_i = f_i$. For $i = 1, \ldots, \varrho$ and $m \geqslant 1$ we can write

$$\varphi_i(x) \equiv \varphi_{i,m}(x)^{a_{i,m}} \pmod{p^m} \tag{2.3}$$

with unique $\varphi_{i,m}(x) \in \Phi(m, f_i)$ and $a_{i,m} = \dfrac{\deg\varphi_i}{\deg\varphi_{i,m}}$. Observe that $a_{i,m} = 1$ and $\varphi_{i,m}(x) \neq \varphi_{j,m}(x)$ for $i \neq j$, if m is large enough.

Theorem 1. *The maximal power of p dividing the discriminant of α is equal to*

$$\sum_{i=1}^{\varrho} f_i \sum_{t=1}^{m_i} (a_{i,t} - 1) + \sum_{i<j} \sum_{t=1}^{m_{ij}} \{f_j a_{i,t} + f_i a_{j,t}\},$$

where $m_i = \max\{m\colon a_{i,m} \neq 1\}$, $m_{ij} = \max\{m\colon \varphi_{i,m}(x) = \varphi_{j,m}(x)\}$.

Proof. We shall need two lemmas.

LEMMA 1. *If* $\varphi(x) \in Z_p[x]$ *is unramified of degree* f *and*

$$\varphi(x) \equiv \varphi_m(x)^{a_m} (\operatorname{mod} p^m) \quad \text{with} \quad \varphi_m(x) \in \Phi(m, f),$$

then the maximal power of p *dividing the discriminant* $d(\varphi)$ *of* φ *is equal to* $\sum_m f(a_m - 1)$.

Proof of Lemma 1. Let $\alpha \in L_f$ be a root of $\varphi(x)$. It is known that

$$d(\varphi) = \pm N_{L_f/Q_p}\big(\varphi'(\alpha)\big), \tag{2.4}$$

where $\varphi'(x)$ denotes the derivative of $\varphi(x)$. Putting

$$t = \max\{i\colon |G_i(\alpha)| \neq 1\}$$

where $G_i(\alpha)$ are defined as in (1.1), we have

$$v\big(\varphi'(\alpha)\big) = v\Big(\prod_{\sigma \in G_f \setminus \{1\}} \big(\sigma(\alpha) - \alpha\big)\Big) = \sum_{j=1}^{t-1} \sum_{\sigma \in G_j(\alpha) \setminus G_{j+1}(\alpha)} v\big(\sigma(\alpha) - \alpha\big) +$$

$$+ \sum_{\sigma \notin G_1(\alpha)} v\big(\sigma(\alpha) - \alpha\big) + \sum_{\sigma \in G_t(\alpha) \setminus \{1\}} v\big(\sigma(\alpha) - \alpha\big)$$

$$= \sum_{j=1}^{t-1} j\big(|G_j(\alpha)| - |G_{j+1}(\alpha)|\big) + t(|G_t| - 1) = \sum_{j=1}^{t} \big(|G_j(\alpha)| - 1\big).$$

Now (2.4) and (1.2) give the assertion of our lemma.

LEMMA 2. *If* $\varphi_1(x), \varphi_2(x) \in Z_p[x]$ *are unramified of degrees* f_1, f_2 *respectively,*

$$\varphi_i(x) \equiv \varphi_{i,m}(x)^{a_{i,m}} (\operatorname{mod} p^m), \quad i = 1, 2, \quad m \geqslant 1,$$

with $\varphi_{i,m}(x) \in \Phi(m, f_i)$ *and* $M = \max\{m\colon \varphi_{1,m}(x) = \varphi_{2,m}(x)\}$, *then the maximal power of* p *dividing* $R(\varphi_1, \varphi_2)$, *the resultant of* φ_1 *and* φ_2, *is equal to*

$$\sum_{m=1}^{M} a_{1,m} a_{2,m} \deg \varphi_{1,m} = f_1 \sum_{m=1}^{M} a_{2,m} = f_2 \sum_{m=1}^{M} a_{1,m}.$$

Proof of Lemma 2. Assume first that $\deg \varphi_1 = \deg \varphi_2 = f$. Let $\alpha, \beta \in L_f$ be roots of φ_1, φ_2 respectively. Put

$$B_m = \{\tau \in G_f\colon \alpha \equiv \tau(\beta) (\operatorname{mod} p^m)\}$$

and observe that $B_m = \emptyset$ or else is a coset of G_f with respect to $G_m(\beta)$. The case $B_m \neq \emptyset$ occurs if and only if there exists a $\tau \in G_f$ such that $s_m(\alpha)$ and $s_m\big(\tau(\beta)\big) = \tau\big(s_m(\beta)\big)$ are equal, e.g. when $\varphi_{1,m} = \varphi_{2,m}$. Hence $|B_m| = a_{2,m}$ for $m = 1, 2, \ldots, M$ and $|B_m| = 0$ for $m > M$. We have

$$R(\varphi_1, \varphi_2) = N_{L_f/Q_p}\Big(\prod_{\tau \in G_f} \big(\alpha - \tau(\beta)\big)\Big).$$

Proceeding as in the proof of Lemma 1, one gets

$$v\Big(\prod_{\tau \in G_f} \big(\alpha - \tau(\beta)\big)\Big) = \sum_{m=1}^{M} \sum_{\tau \in B_m \setminus B_{m+1}} v\big(\alpha - \tau(\beta)\big) = \sum_{m=1}^{M} a_{2,m};$$

hence

$$v\big(R(\varphi_1, \varphi_2)\big) = f \sum_{m=1}^{M} a_{2,m} = f \sum_{m=1}^{M} a_{1,m} = \sum_{m=1}^{M} a_{1,m} a_{2,m} \deg \varphi_{1,m}. \tag{2.5}$$

The above equalities hold since in our case

$$a_{1,m} = \frac{f}{\deg \varphi_{1,m}} = \frac{f}{\deg \varphi_{2,m}} = a_{2,m}.$$

Now we turn to the general situation. Put $t_m = \deg \varphi_{1,m} = \deg \varphi_{2,m}$, and let $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(f_1)}$ be the roots of $\varphi_1(x)$, ordered so that $s_M(\alpha^{(1)})$, $s_M(\alpha^{(2)}), \ldots, s_M(\alpha^{(t_M)})$ form the set of all roots of $\varphi_{1,M}(x)$. Do the same with the roots $\beta^{(1)}, \ldots, \beta^{(f_2)}$ of $\varphi_2(x)$.

Let φ_1', φ_2' be distinct elements of $\Phi(M+1, t_M)$, both being extensions of $\varphi_{1,M} = \varphi_{2,M}$.

Observe that

$$v\big(R(\varphi_1, \varphi_2)\big) = v\Big(\prod_{\substack{1 \leqslant i \leqslant f_1 \\ 1 \leqslant j \leqslant f_2}} (\alpha^{(i)} - \beta^{(j)})\Big)$$

$$= \frac{f_1}{t_M} \frac{f_2}{t_M} v\Big(\prod_{1 \leqslant i, j \leqslant t_M} (\alpha^{(i)} - \beta^{(j)})\Big) = \frac{f_1}{t_M} \frac{f_2}{t_M} v\big(R(\varphi_1', \varphi_2')\big).$$

As φ_1' and φ_2' have equal degrees, we can apply (2.5) to determine $v\big(R(\varphi_1', \varphi_2')\big)$. We have

$$\varphi'_{1,m} = \varphi'_{2,m} = \varphi_{1,m} = \varphi_{2,m} \quad \text{for} \quad m = 1, 2, \ldots, M, \quad \varphi'_{1,M+1} \neq \varphi'_{2,M+1},$$

and

$$\varphi_i' \equiv \varphi_{i,m}^{a_{i,m}/a_{i,M}} \quad \text{for} \quad i = 1, 2 \text{ and } 1 \leqslant m \leqslant M.$$

Further, we have

$$f_1 = t_m a_{1,m}, \quad f_2 = t_m a_{2,m}.$$

So (2.5) gives us

$$v\big(R(\varphi_1, \varphi_2)\big) = \frac{f_1}{t_M} \frac{f_2}{t_M} \sum_{m=1}^{M} \frac{a_{1,m}}{a_{1,M}} \frac{a_{2,m}}{a_{2,M}} \deg \varphi'_{1,m}$$

$$= \sum_{m=1}^{M} a_{1,m} a_{2,m} \deg \varphi_{1,m} = f_1 \sum_{m=1}^{M} a_{2,m} = f_2 \sum_{m=1}^{M} a_{1,m}.$$

Using the Lemmas 1, 2 and the formula

$$d(\alpha) = \prod_{i=1}^{\varrho} d(\varphi_i) \times \prod_{1\leqslant i<j\leqslant \varrho} R(\varphi_i, \varphi_j)^2,$$

we get the assertion of Theorem 1.

As p is unramified in K, we have $p \nmid d_K$. Hence formula (1) implies that $\varkappa_p(K)$ is equal to the minimal value of $\frac{1}{2}v\big(d(\alpha)\big)$ when α runs through primitive elements of R_K. Observe also that if $m \geqslant m_p(K)$, where $m_p(K)$ is defined as in (2), then there exists an $\alpha \in R_K$ such that the polynomials $\varphi_1, \ldots, \varphi_\varrho$ corresponding to it in (2.2) satisfy

$$m_i,\ m_{ij} \leqslant m \quad \text{for} \quad i, j = 1, 2, \ldots, \varrho.$$

An easy argument shows now that the minimal value of $v\big(d(\alpha)\big)$ is attained at one of those integers α.

Let p, ϱ, $f_1, \ldots, f_\varrho$ be as in (2.1).

LEMMA 3. *If m is a positive integer and $\psi_i \in \Phi(m, f_i)$ for $i = 1, \ldots, \varrho$ then there exists an $\alpha \in R_K$ such that if its minimal polynomial $f(x)$ has the factorization* (2.2) *in $Z_p[x]$ then*

$$\varphi_i(x) \equiv \psi_i(x)^{a_i} (\operatorname{mod} p^m)$$

where

$$a_i = \deg\varphi_i/\deg\psi_i \quad \textit{and} \quad i = 1, \ldots, \varrho.$$

Proof. Let $\alpha_i \in L_{f_i}$ be a root of $\psi_i(x)$. Choose first $\gamma \in R_K$ such that $\gamma \equiv \gamma_i (\operatorname{mod} \mathfrak{p}_i^m)$ for $i = 1, \ldots, \varrho$ and then a generator α of the extension K/Q in the form $\gamma + p^m\theta$ with $\theta \in R_K$. One easily checks that α has the required property.

COROLLARY 1. *If p is unramified in K/Q then $\varkappa_p(K)$ depends only on the type of factorization of p into prime ideals in R_K.*

The proof immediately follows from Lemma 3 and Theorem 1.

3. Now we shall give an upper bound for $\varkappa_p(K)$, which in many cases is the best possible and is strong enough to prove Engstrom's conjecture mentioned in the introduction.

A primitive integer α of K will be called *absolutely primitive* if each polynomial $\varphi_{i,m}$ corresponding to it according to (2.3) belongs to $\Psi(m, f_i)$. This means that all $a_{i,m}$'s are equal to 1. Put

$$\varkappa'_p(K) = \min\{\varkappa_p(\theta)\colon\ \theta - \text{absolutely primitive in } R_K\},$$

where $\varkappa_p(\theta) = \frac{1}{2}v\big(d(\theta)\big)$.

Obviously

(3.1) $$\varkappa_p(K) \leqslant \varkappa'_p(K).$$

THEOREM 2. *If p is a prime unramified in K/Q then*

$$\varkappa'_p(K) = \sum_f f \sum_m \left[\frac{\varrho(f)}{s(m,f)}\right] \left\{\varrho(f) - s(m,f)\,\frac{\left[\frac{\varrho(f)}{s(m,f)}\right]+1}{2}\right\}$$

where $\varrho(f)$ denotes the number of prime ideals dividing p which have degree f and $s(m,f) = p^{(m-1)f}\pi(p,f)$.

Proof. If θ is absolutely primitive then Theorem 1 gives

$$\varkappa_p(\theta) = \frac{1}{2}\sum_{i<j}\sum_{m=1}^{m_{ij}} (f_i + f_j)$$

where $m_{ij} = \max\{m\colon\ \varphi_{i,m} = \varphi_{j,m}\}$.

Obviously for $f_i \neq f_j$ the equality $\varphi_{i,m} = \varphi_{j,m}$ cannot occur. Hence we can write

$$\varkappa_p(\theta) = \sum_f A(f)$$

where

(3.2) $$A(f) = f \sum_{\substack{i<j \\ f_i = f_j = f}} m_{ij}.$$

For a given f let $\varrho(f)$ be the number of $\varphi_i(x)$ in (2.2) which have degree f and let

$$F_f(x) = \prod_{i, f_i = f} \varphi_i(x).$$

Write

$$F_f(x) \equiv V_{1,m}^{a_{1,m}}(x) \ldots V_{s(m,f),m}^{a_{s(m,f),m}}(x) \ (\operatorname{mod} p^m)$$

where $V_{i,m}(x)$ are distinct elements of $\Psi(m,f)$ and $s(m,f) = |\Psi(m,f)|$.

From (3.2) we obtain

$$A(f) = \frac{1}{2} f \sum_{m=1}^{M} \sum_{i=1}^{s(m,f)} a_{i,m}(a_{i,m} - 1)$$

where

$$M = \min\{m\colon\ a_{i,m} = 1 \text{ for } i = 1, 2, \ldots, s(m,f)\}.$$

Because of

$$\sum_{i=1}^{s(m,f)} a_{i,m} = \varrho(f)$$

we get

(3.3) $$2A(f) + f\varrho(f)M = f \sum_{m=1}^{M} \sum_{i=1}^{s(m,f)} a_{i,m}^2.$$

To obtain the minimal value of $A(f)$ we shall need the following obvious lemma.

LEMMA 4. *If $x_1, \ldots, x_s$ are nonnegative integers with $x_1+\ldots+x_s = A$, then the minimal value of $x_1^2+\ldots+x_s^2$ is attained for $x_i = [A/s]+\delta_i$, where $\delta_i = 0$ or 1, and $\sum_{i=1}^{s} \delta_i = A-[A/s]s$.*

Using Lemma 4, we find that the minimal value of $\sum_{i=1}^{s(m,f)} a_{i,m}^2$ under the restriction

$$\sum_{i=1}^{s(m,f)} a_{i,m} = \varrho(f)$$

is attained for any system $\{a_{i,m}\}$ such that

$$a_{i,m} = \left[\frac{\varrho(f)}{s(m,f)}\right]+\delta_{i,m} \tag{3.4}$$

where $\delta_{i,m} = 0$ or 1 and

$$\sum_{i=1}^{s(m,f)} \delta_{i,m} = \varrho(f)-s(m,f)\left[\frac{\varrho(f)}{s(m,f)}\right].$$

Now (3.3) gives

$$A(f) \geqslant f\sum_m \left[\frac{\varrho(f)}{s(m,f)}\right]\left\{\varrho(f)-s(m,f)\frac{\left[\frac{\varrho(f)}{s(m,f)}\right]+1}{2}\right\}. \tag{3.5}$$

To end the proof of Theorem 2 it is now enough to show that there exists an absolutely primitive $\theta \in R_K$ such that for every f the two sides of (3.5) are equal.

Because of Lemma 3 it suffices to prove that for every f there exists a θ such that there is an equality in (3.5).

LEMMA 5. *Let M be a given integer and a system of nonnegative integers*

$$(r_k^{(m)})_{1\leqslant m\leqslant M, 1\leqslant k\leqslant s(m,f)}$$

such that

$$\sum_{k=1}^{s(1,f)} r_k^{(1)} = \varrho(f) \tag{3.6}$$

and

$$\sum_{j=1}^{p^f} r_{(k-1)p^f+j}^{(m)} = r_k^{(m-1)} \quad \text{for} \quad m = 2, \ldots, M,\ k = 1, \ldots, s(m-1,f). \tag{3.7}$$

There exists an absolutely primitive $\theta \in R_K$ such that for the polynomial $F_f(x)$ corresponding to it one has

$$F_f(x) \equiv V_1^{(m)}(x)^{r_1(m)} \ldots V_{s(m,f)}^{(m)}(x)^{r_{s(m,f)}^{(m)}} (\operatorname{mod} p^m),$$

with distinct $V_i^{(m)}(x) \in \Psi(m,f)$, for $m = 1, \ldots, M$.

Proof of Lemma 5. In view of the discussion given in Section 1 and Lemma 3, it suffices to construct $\gamma_1, \ldots, \gamma_{\varrho(f)} \in R_f$ such that for every $1 \leqslant m \leqslant M$, the elements

$$s_m(\gamma_{t_i}), s_m(\gamma_{t_i+1}), \ldots, s_m(\gamma_{t_i+r_i(m)}),$$

where

$$t_i = \begin{cases} 0, & \text{if} \quad i = 1, \\ r_1^{(m)}+\ldots+r_{i-1}^{(m)}, & \text{if} \quad i = 2, 3, \ldots, s(m,f), \end{cases}$$

have the same minimal polynomial $\varphi_{i,m} \in \Psi(m,f)$, while $\varphi_{i,m} \neq \varphi_{j,m}$ for $i \neq j$.

This can be achieved by an easy recurrential argument using the properties (3.6) and (3.7) of the system $(r_k^{(m)})$ and the fact that each polynomial of $\Psi(m,f)$ has exactly p^f extensions in $\Psi(m+1,f)$.

Now we shall show that one can determine $\delta_{i,m}$ such that the system defined by (3.4) satisfies the assumptions of Lemma 5.

Suppose that we have done it already for $k < m$. Because of

$$\left[\frac{\varrho(f)}{s(m-1,f)}\right]-p^f\left[\frac{\varrho(f)}{s(m,f)}\right]+\delta_{k,m-1} \leqslant p^f,$$

we can now determine $\delta_{j,m}$ such that

$$\sum_{j=1}^{p^f} a_{(k-1)p^f+j,m}$$

$$= p^f\left[\frac{\varrho(f)}{s(m,f)}\right]+\sum_{j=1}^{p^f} \delta_{(k-1)p^f+j,m} = \left[\frac{\varrho(f)}{s(m-1,f)}\right]+\delta_{k,m-1},$$

for $k = 1, 2, \ldots, s(m-1,f)$.

COROLLARY 2. *If p is unramified in K then $\varkappa_p(K)$ attains its maximal value when p splits.*

Proof. Because of (3.1) and (3) it is enough to show that for every $m \geqslant 1$

$$\sum_f f\left[\frac{\varrho(f)}{s(m,f)}\right]\left\{\varrho(f)-s(m,f)\frac{\left[\frac{\varrho(f)}{s(m,f)}\right]+1}{2}\right\}$$

$$\leqslant \left[\frac{n}{p^m}\right]\left\{n-p^m\frac{\left[\frac{n}{p^m}\right]+1}{2}\right\}.$$

Observe that

$$\left[\frac{n}{p^m}\right]\left\{n-p^m\frac{\left[\frac{n}{p^m}\right]+1}{2}\right\} = -2n+2\sum_{i=1}^{p^m} x_i^2$$

and

$$\left[\frac{\varrho(f)}{s(m,f)}\right]\left\{\varrho(f)-s(m,f)\frac{\left[\frac{\varrho(f)}{s(m,f)}\right]+1}{2}\right\} = -2\varrho(f)+2\sum_{i=1}^{s(m,f)} x_i(f)^2$$

where x_i, $x_i(f)$ are determined so that they minimize $\sum_{i=1}^{p^m} x_i^2$, $\sum_{i=1}^{s(m,f)} x_i(f)^2$ respectively, under the restriction that

$$\sum x_i = n, \quad \sum x_i(f) = \varrho(f).$$

To end the proof note that $\sum_f f\varrho(f) = n$ and that $fs(m,f) > p^m$ holds for every f, m.

Remark. Using Theorem 1, one easily finds that the discriminant of $F_f(x)$ (defined as in the proof of Theorem 2) is divisible at least by p in the power

$$f\varrho(f)\left(\frac{p^{fM(f)}-1}{p^f-1}-M(f)\right),$$

where $M(f) = \max\{m:\ p^m \leqslant f\varrho(f)\}$.

This gives

$$\varkappa_p(K) \geqslant \frac{1}{2}\sum_f f\varrho(f)\left(\frac{p^{fM(f)}-1}{p^f-1}-M(f)\right).$$

This evaluation seems to be close to the best possible in the case where all prime ideal divisors of p have the same degree.

4. We are not yet able to give a closed formula for $\varkappa_p(K)$, but, given any field K, Theorem 1 allows us to determine its value. First, we should find the minimal value of the expression appearing in Theorem 1, under the obvious restrictions. Then it is enough to check if there exists a $\theta \in R_K$ which realizes this minimum. After checking several cases we are led to the conjecture that this minimum can always be realized.

Engstrom in his paper gave a table of values of $\varkappa_p(K)$ for K with a degree not exceeding 7. As an example of the application of our method we have determined the value of $\varkappa_p(K)$ for $8 \leqslant n \leqslant 12$, in the case where p is unramified. In the following table only those types of factorization are listed for which $\varkappa_p(K) \neq 0$ for $p = 2, 3, 5, 7$. There is one more prime p for which $\varkappa_p(K) \neq 0$ can occur if $[K:Q] \leqslant 12$. Namely $\varkappa_{11}(K) = \varkappa'_{11}(K) = 1$ if $[K:Q] = 12$ and 11 splits completely in K. If $\varkappa_p \neq \varkappa'_p$ for some p then we give in brackets the corresponding value of $\varkappa'_p$.

$$pR_K = \mathfrak{p}_1 \ldots \mathfrak{p}_\varrho, \quad \deg\mathfrak{p} = f_i.$$

Degree of field	Type of decomposition of pR_K $[f_1, f_2, \ldots, f_\varrho]$	2 $\varkappa_2$	3 $\varkappa_3$	5 $\varkappa_5$	7 $\varkappa_7$
1	2	3	4	5	6
8	[11111111]	16	7	3	3
	[2111111]	8	3	1	
	[221111]	3 (4)	1		
	[22211]	5 (6)			
	[2222]	4 (12)	1 (2)		
	[311111]	5	2		
	[41111]	2	1		
	[5111]	1			
	[3221]	1 (2)			
	[32111]	1			
	[422]	1 (2)			
9	[111111111]	23	9	4	2
	[21111111]	12	4	2	
	[2211111]	7	2		
	[222111]	6 (7)			
	[22221]	6 (12)	1 (2)		
	[3111111]	8	3	1	
	[33111]	1			
	[333]	3			
	[321111]	2	1		
	[32211]	2			
	[3222]	2 (6)			
	[411111]	5	2		
	[42111]	1			
	[4221]	1 (2)			
	[51111]	2	1		
	[522]	1 (2)			
	[6111]	1			
10	[1111111111]	30	13	5	3
	[211111111]	16	7	3	1
	[22111111]	10	3	1	
	[2221111]	8	1		
	[222211]	8 (12)	2 (4)		
	[31111111]	12	4	2	
	[331111]	2	1		
	[3331]	3			
	[3211111]	5	2		
	[322111]	3			
	[32221]	3 (6)			
	[3322]	1 (2)			
	[4111111]	8	3	1	
	[421111]	2	1		
	[42211]	2			
	[4222]	2 (6)			
	[43111]	1			
	[511111]	5	2		

1	2	3	4	5	6
	[52111]	1			
	[5221]	1 (2)			
	[61111]	2	1		
	[622]	1 (2)			
	[7111]	1			
11	[11111111111]	43	17	7	4
	[2111111111]	23	9	4	2
	[221111111]	14	4	2	
	[22211111]	11	2		
	[2222111]	9 (13)	2		
	[222221]	19 (22)	2 (4)		
	[311111111]	16	7	3	1
	[3311111]	5	2		
	[33311]	3			
	[32111111]	8	3	1	
	[3221111]	7	2		
	[322211]	5 (6)			
	[32222]	4 (12)	1 (2)		
	[332111]	1			
	[33221]	1 (2)			
	[3332]	3			
	[41111111]	12	4	2	
	[44111]	1			
	[4211111]	5	2		
	[422111]	3	3		
	[42221]	3 (6)			
	[431111]	2	1		
	[4322]	1 (2)			
	[5111111]	8	3	1	
	[521111]	2	1		
	[52211]	2			
	[5222]	2 (6)			
	[53111]	1			
	[611111]	5	2		
	[62111]	1			
	[6221]	1 (2)			
	[71111]	2	1		
	[722]	1 (2)			
	[8111]	1			
12	[111111111111]	46	21	9	5
	[21111111111]	30	13	5	3
	[2211111111]	18	7	3	1
	[222111111]	14	3	1	
	[22221111]	7 (14)	3		
	[2222211]	12 (22)	3 (4)		
	[222222]	14 (34)	3 (6)		
	[3111111111]	23	9	4	2
	[33111111]	8	3	1	
	[333111]	4			
	[3333]	6			
	[321111111]	12	4	2	
	[32211111]	7	2		
	[3222111]	6 (7)			
	[322221]	6 (12)	1 (2)		
	[3321111]	2	1		
	[332211]	2			
	[33222]	2 (6)			
	[33321]	3			
	[411111111]	16	7	3	1
	[441111]	2	1		
	[42111111]	8	3	1	
	[4221111]	3 (4)	1		
	[422211]	5 (6)			
	[42222]	4 (12)	1 (2)		
	[4311111]	5	2		
	[432111]	1			
	[43221]	1 (2)			
	[51111111]	12	4	2	
	[5211111]	5	2		
	[522111]	3			
	[52221]	3 (6)			
	[531111]	2	1		
	[5322]	1 (2)			
	[6111111]	8	3	1	
	[621111]	2	1		
	[62211]	2			
	[6222]	2 (6)			
	[63111]	1			
	[711111]	5	2		
	[72111]	1			
	[7221]	1 (2)			
	[81111]	2	1		
	[822]	1 (2)			
	[9111]	1			

References

[1] M. Bauer, *Über die ausserwesentliche Diskriminantenteiler einer Gattung*, Math. Ann. 64 (1907), pp. 572–576.

[2] R. Bungers, *Über Zahlkörper mit gemeinsamen ausserwesentlichen Diskriminantenteilern*, Jber. Deutsch. Math.-Verein. 46 (1936), pp. 93–96.

[3] L. Carlitz, *On abelian fields*, Trans. Amer. Math. Soc. 35 (1933), pp. 122–136.

[4] — *A note on common index divisors*, Proc. Amer. Math. Soc. 3 (1952), pp. 688–692.

[5] R. Dedekind, *Über Zusammenhang zwischen der Theorie der Ideale und der Theorie der höhere Kongruenzen*, Abh. König. Ges. der Wissen. zu Göttingen, 23 (1878), pp. 1–23.
[6] D. S. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields*, in: *Number Theory and Algebra*, Academic Press, New York 1977, pp. 29–42.
[7] H. T. Engstrom, *On the common index divisor of an algebraic field*, Trans. Amer. Math. Soc. 32 (1930), pp. 223–237.
[8] M. N. Gras, *Sur les corps cubiques cycliques dont l'anneau des entiers est monogène*, C. R. Acad. Sci., Paris, 278 (1974), pp. 59–62.
[9] M. Hall, *Indices in cubic fields*, Bull. Amer. Math. Soc. 43 (1937), pp. 104–108.
[10] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamer ausserwesentlicher Diskriminantenteiler einer Gattung*, Journal für Mathematik 113 (1894), pp. 128–160.
[11] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN, Warszawa 1974.
[12] O. Ore, *Über der Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körper*, Math. Ann. 96 (1926), pp. 313–352.
[13] P. A. B. Pleasants, *The number of generators of the integers of a number field*, Mathematika 21 (1974), pp. 160–167.
[14] A. A. Sukallo, *On determination of the index of a field of algebraic numbers*, Rostov. Gos. Univ. Uč. Zap., Fiz.-Mat. Fak., 32 (1955), pp. 37–42.
[15] L. Tornheim, *Minimal basis and inessential discriminant divisors for a cubic field*, Pacific J. Math. 5 (1955), pp. 621–631.
[16] E. Zylinsky, *Zur Theorie der ausserwesentlicher Diskriminantenteiler algebraischer Körper*, Math. Ann. 73 (1913), pp. 273–274.

Received on 24.11.1980 (1233)

ACTA ARITHMETICA
XLII (1982)

Some new estimates for $G(k)$ in Waring's problem

by

K. Thanigasalam (Monaca, Penn.)

1. Introduction. In a recent paper [3], some new estimates were obtained for $G(k)$ when $k \geqslant 9$. In this paper they will be improved a little further. For large k the method does not give significant results.

Theorem. $G(9) \leqslant 88$, $G(10) \leqslant 104$, $G(11) \leqslant 119$, $G(12) \leqslant 134$, $G(13) \leqslant 150$, $G(14) \leqslant 165$, $G(15) \leqslant 181$, $G(16) \leqslant 197$, $G(17) \leqslant 213$, $G(18) \leqslant 229$, $G(19) \leqslant 245$, $G(20) \leqslant 262$.

When $k = 8$ the argument gives $G(8) \leqslant 73$ which is the same as that obtained by Davenport's method.

As in [3] we take

$$2P = N^{1/k}, \quad P_0 = \sqrt{P}, \quad \tau = P^{k-1+\delta} \tag{1}$$

where N is a large positive integer and δ is a small positive constant. Let

$$\eta = \frac{1}{2k-1}, \quad P_1 = P_0^{1-\eta}, \quad P_2 = P_0^{1+\eta}, \tag{2}$$

let $\mathscr{U}$ denote the set of numbers u of the form

$$u = \sum_{i=1}^{s_2} x_i^k$$

with

$$P_1^{k-\delta} < u < s_2 2^k P_1^{k-\delta}, \tag{3}$$

and let

$$U_1 = \operatorname{card} \mathscr{U}. \tag{4}$$

Suppose further that $\mathscr{P}$ is the set of primes v with

$$\tfrac{1}{2} P_2^{1-\delta/2} \leqslant v \leqslant P_2^{1-\delta/2}. \tag{5}$$