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 $\theta$ a primitive element belonging to $R_K$. The index of the subring of $R_K$ generated by $\theta$ in the ring $R_K$ we shall call the index of $\theta$ and denote by $i(\theta)$. Obviously

$$d(\theta) = i(\theta) d_K,$$

where $d(\theta)$ is the discriminant of $\theta$ 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 $p | i(K)$ if and only if there exists an $f$ such that

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

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

Obviously, if $R_K = Z[\theta]$ with $\theta \in R_K$, then $i(K) = 1$. K. Honsel ([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 $I(K) = \min_{\theta} i(\theta)$ 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 $k$th cyclotomic fields, where $l = 1 \pmod{3}$ 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 $\mathbb{Z}$ was determined by P. Pleasants ([13]). To formulate their result we have to introduce some notations.

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

$$\pi(K^0 \cap \{p^{m}\}, \deg p) \geq g(\deg p)$$

and let

$$m_p(K) = \max_{p} m_p.$$  

(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

$$m_p(K) \leq \pi(g, f),$$

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

In this paper we shall study $\pi(g, f)$ 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

$$\sum_{m=1}^{\infty} \left[ \frac{n}{m^m} \right] \left\lfloor \frac{n}{m^m} \right\rfloor + 1$$

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

He confirmed also the conjecture of O. Ore ([12]) that $\pi(g, f)$ 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 $\pi(g, f)$ depends only on the form of the decomposition of $p$. Engstrom has conjectured that $\pi(g, f)$ attains its maximal value if $p$ splits in $K$.

We confirm this conjecture under the restriction that $p$ is unramified.

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

$$pR_K = p^1 \cdots p^k, \ h > p, \ deg p_i = 1 \ for \ i = 1, \ldots, k,$$

and proved that if $\epsilon_1 \geq \epsilon_2 \geq \ldots \geq \epsilon_r$, and $S, T, R$ are determined by

$$S = \sum_{i=1}^{r} \epsilon_i, \ \ [K:Q] = ST + R \ \ (0 \leq R < S),$$

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

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].

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

If we put

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

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

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

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 $a \in R_{f_2} \cap R_{f_3}$ and

$$a = \sum_{m=0}^{\infty} \gamma_m p^m = \sum_{m=0}^{\infty} \gamma_m p^m$$

with $\gamma_m(0) \in A_{f_2}, \gamma_m(1) \in A_{f_3}$, then

$$\gamma_m(1) = \gamma_m(0) \ \text{for} \ \ m = 1, 2, \ldots$$

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 $\sum_{m=1}^{\infty} t_m(a)p^f$.

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

\[(1.1) \quad \tau(t_m(a)) = t_m(\tau(a))\]

for \(\tau \in T_f\) and \(m = 0, 1, 2, \ldots\)

Indeed, as \(s_{\epsilon}(a) = a + p^\epsilon \gamma_1\), \(s_{\epsilon}(\tau(a)) = \tau(a) + p^\epsilon \gamma_2\) with \(\gamma_1, \gamma_2 \in R_f\), we have

\[(1.2) \quad \tau(s_m(a)) - s_m(\tau(a)) \in p^M R_f\]

Assume that for given \(a \in R_f\), \(m < M\) hold if \(m \leq M\). Then

\[\tau(s_{M+1}(a)) - s_{M+1}(\tau(a)) = p^M \{\tau(t_M(a) - t_M(\tau(a))\},\]

and so by (1.2)

\[\tau(t_M(a)) = t_M(\tau(a)) \mod p\]

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

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

For \(m \geq 1\) we shall write \(\phi_{m,a}(x)\) for the minimal polynomial of \(s_m(a)\).

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

Let

\[(1.3) \quad G_m(a) = \{\sigma \in T_f : \sigma(a) = a \mod p^m\} = \{\sigma \in T_f : s_m(\sigma(a)) = s_m(a)\} \]

Then

\[\phi_{m,a}(x) = \prod_{\sigma \in G_m(a)} (x - \tau(s_m(\alpha))) = \prod_{\sigma \in G_m(a)} (x - \tau(\tau(a) \mod p^m))\]

and hence

\[\phi(a) = \phi_{m,a}(x) \mod \phi_{m,a}(x)\]

where \(\phi_i(a)\) are unramified and \(deg \phi_i = f_i\). For \(i = 1, \ldots, \epsilon\) and \(m \geq 1\) we can write

\[\phi_{i,m}(x) = \phi_{i,m}(x) \mod \phi_{m,a}(x)\]

with unique \(\phi_{i,m}(x) \in \Phi(m, f_i)\) and \(a_{i,m} = \frac{deg \phi_i}{deg \phi_{i,m}}\). Observe that

\[a_{i,m} = 1 \quad \text{and} \quad \phi_{i,m}(a) = \phi_{j,m}(a) \quad \text{for} \quad i \neq j, \quad \text{if} \quad m \quad \text{is large enough.}\]

Theorem 1. The maximal power of \(p\) dividing the discriminant of \(a\) is equal to

\[\sum_{i=1}^{c} f_i \sum_{l=1}^{m} (a_i l - 1) + \sum_{l=1}^{m} \sum_{i=1}^{m} (f_i a_i l + f_i a_i l)\]

where \(m_i = \max \{m : a_{i,m} \neq 1\}\), \(m_i = \max \{m : \phi_{i,m}(x) = \phi_{j,m}(x)\}\).
LEMMA 1. If \( \varphi(x) \in \mathbb{Z}_p[x] \) is unramified of degree \( f \) and
\[
\varphi(x) = a_m x^m \pmod{p^n}, \quad \text{with} \quad a_m(x) \in \mathcal{O}(m, \beta),
\]
then the maximal power of \( p \) dividing the discriminant \( \Delta(\varphi) \) of \( \varphi \) is equal to
\[
\sum_{m=1}^{M} f(a_m - 1).
\]

Proof of Lemma 1. Let \( a \in \mathbb{Z}_p \) be a root of \( \varphi(x) \). It is known that
\[
\Delta(\varphi) = \pm N_{\mathbb{Z}_p/\mathbb{Z}_p}^{\mathbb{Z}_p}(\varphi'(a)),
\]
where \( \varphi'(x) \) denotes the derivative of \( \varphi(x) \). Putting
\[
\ell = \max \{ i : |\theta_i(a)| \neq 1 \}
\]
where \( \theta_i(a) \) are defined as in (1.1), we have
\[
\nu(\varphi'(a)) = \nu \left( \prod_{i \neq j} (\sigma(a) - a) \right) = \sum_{i=1}^{\ell-1} \sum_{a \in \theta_i(a)} \nu(\sigma(a) - a) + \sum_{a \in \theta_i(a)} \nu(\sigma(a) - a)
\]
\[
= \sum_{i=1}^{\ell-1} \nu(\theta_{i+1}(a) - |\theta_i(a)|) + \ell \nu(\theta_1(a) - 1) = \sum_{i=1}^{\ell} \nu(\theta_i(a) - 1).
\]

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

LEMMA 2. If \( \varphi_1(x), \varphi_2(x) \in \mathbb{Z}_p[x] \) are unramified of degrees \( f_1, f_2 \), respectively,
\[
\varphi_i(x) = a_{i,m} x^m \pmod{p^n}, \quad i = 1, 2, \quad m \geq 1,
\]
with \( a_{i,m}(x) \in \mathcal{O}(m, f_i) \) and \( M = \max \{ m : \varphi_1(x) = \varphi_2(x) \} \), then the maximal power of \( p \) dividing \( R(\varphi_1, \varphi_2) \), the resultant of \( \varphi_1 \) and \( \varphi_2 \), 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 \( a, b \in \mathbb{Z}_p \) be roots of \( \varphi_1, \varphi_2 \) respectively. Put
\[
B_{m} = \{ r \in \mathcal{O} : a - r(b) \pmod{p^n} \}
\]
and observe that \( B_m = \emptyset \) or else is a coset of \( \mathcal{O} \) with respect to \( \mathcal{O}(\beta) \). The case \( B_m = \emptyset \) occurs if and only if there exists a \( r \in \mathcal{O} \) such that \( s_m(a) = s_m(b) \). Hence \( B_m \neq \emptyset \) for \( m = 1, 2, \ldots, M \) and \( |B_m| = 0 \) for \( m > M \). We have
\[
R(\varphi_1, \varphi_2) = N_{\mathbb{Z}_p/\mathbb{Z}_p}^{\mathbb{Z}_p}(a - \tau(b)).
\]

Proceeding as in the proof of Lemma 1, one gets
\[
\nu \left( \prod_{i \neq j} (a - \tau(b)) \right) = \sum_{m=1}^{M} \nu(a_m \tau(b)) = \sum_{m=1}^{M} a_{2,m} i_m,
\]
hence
\[
\nu(R(\varphi_1, \varphi_2)) = f_1 \sum_{m=1}^{M} a_{2,m} = f_2 \sum_{m=1}^{M} a_{1,m} \deg \varphi_{1,m}.
\]

The above equalities hold since in our case
\[
a_{i,m} = \frac{f_i}{\deg \varphi_{i,m}} = \frac{f_2}{\deg \varphi_{2,m}} = a_{2,m}.
\]

Now we turn to the general situation. Put \( t_m = \deg \varphi_{1,m} = \deg \varphi_{2,m} \), and let \( a = \alpha^{(0)}, \alpha^{(e)}, \ldots, \alpha^{(e)} \) be the roots of \( \varphi_1(x) \), ordered so that \( s_M(a^{(0)}), s_M(a^{(e)}), \ldots, s_M(a^{(e)}) \) form the set of all roots of \( \varphi_{1,M}(x) \). Do the same with the roots \( \beta^{(0)}, \beta^{(e)}, \ldots, \beta^{(e)} \) of \( \varphi_2(x) \).

Let \( \varphi_1, \varphi_2 \) be distinct elements of \( \mathcal{O}(M + 1, f_m) \), both being extensions of \( \varphi_{1,M} = \varphi_{2,M} \).

Observe that
\[
\nu(R(\varphi_1, \varphi_2)) = \nu \left( \prod_{1 \leq i < 0 \leq M} (a^{(0)} - \beta^{(0)}) \right) = f_1 f_2 \nu(R(\varphi_1, \varphi_2)).
\]

As \( \varphi_1 \) and \( \varphi_2 \) have equal degrees, we can apply (2.5) to determine \( \nu(R(\varphi_1, \varphi_2)) \).

We have
\[
\varphi_{1,m} = \varphi_{2,m} = \varphi_{1,m} = \varphi_{2,m} \quad \text{for} \quad m = 1, 2, \ldots, M, \quad \varphi_{1,M+1} = \varphi_{2,M+1},
\]
and
\[
\varphi_i = \varphi_i^{(0)} \varphi_i^{(e)}. \quad \text{for} \quad i = 1, 2 \quad \text{and} \quad 1 \leq m \leq M.
\]

Further, we have
\[
f_1 = t_m a_{1,m}, \quad f_2 = t_m a_{2,m}.
\]

So (2.5) gives us
\[
\nu(R(\varphi_1, \varphi_2)) = f_1 f_2 \sum_{m=1}^{M} a_{1,m} a_{2,m} \deg \varphi_{1,m} = f_1 f_2 \sum_{m=1}^{M} a_{1,m} a_{2,m} = f_1 f_2 \sum_{m=1}^{M} a_{1,m} a_{2,m}.
\]
Using the Lemmas 1, 2 and the formula
\[
d(a) = \prod_{i=1}^{g} d(q_i) \times \prod_{1 \leq i < j \leq e} R(q_i, q_j)^{5},
\]
we get the assertion of Theorem 1.

As \( p \) is unramified in \( K \), we have \( p \not\in \mathcal{D}_K \). Hence formula (1) implies that \( \kappa_p(K) \) is equal to the minimal value of \( \frac{1}{\nu} \nu(d(a)) \) when \( a \) runs through primitive elements of \( R_K \). Observe also that if \( m \geq m_{ij}(K) \), where \( m_{ij}(K) \) is defined as in (2), then there exists an \( a \in R_K \) such that the polynomials \( q_i, \ldots, q_e \) corresponding to it in (2.2) satisfy
\[
m_{ij} \leq m \quad \text{for} \quad i, j = 1, 2, \ldots, e.
\]

An easy argument shows that the minimal value of \( \nu(d(a)) \) is attained at one of those integers \( a \).

Let \( q_i, q_j, f_i, \ldots, f_e \) be as in (2.1).

**Lemma 3.** If \( m \) is a positive integer and \( q_i, q_j, f_i, \ldots, f_e \) then there exists an \( a \in R_K \) such that its minimal polynomial \( f(x) \) has the factorization (2.2) in \( \mathbb{Z}_p[x] \) then
\[
q_i(x) = q_i(x^{a_i} \mod p^m)
\]
where
\[
a_i = \deg q_i / \deg q_i \quad \text{and} \quad i = 1, \ldots, e.
\]

**Proof.** Let \( a_i \in \mathbb{Z}_p \) be a root of \( q_i(x) \). Choose first \( \gamma \in R_K \) such that \( \gamma = q_i^{a_i} \mod p^m \) for \( i = 1, \ldots, e \) and then a generator \( a \) of the extension \( K/Q \) in the form \( \gamma + p^m \theta \) with \( \theta \in R_K \). One easily checks that \( a \) has the required property.

**Corollary 1.** If \( p \) is unramified in \( K/Q \) then \( \kappa_p(K) \) 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 \( \kappa_p(K) \), which in many cases is the best possible and is strong enough to prove Engstrom's conjecture mentioned in the introduction.

A primitive integer \( a \in K \) will be called absolutely primitive if each polynomial \( q_i(x) \) corresponding to it according to (2.3) belongs to \( \mathcal{P}(m, f) \). This means that all \( a_i(m) \)'s are equal to 1. Put

\[
k_p'(K) = \min \{ \kappa_p(\theta) : \theta \text{ absolutely primitive in } R_K \},
\]

where \( \kappa_p(\theta) = \frac{1}{\nu} \nu(d(\theta)) \).

Obviously
\[
\kappa_p(K) \leq k_p'(K).
\]

**Theorem 2.** If \( p \) is a prime unramified in \( K/Q \) then
\[
k_p'(K) = \sum_{i,j} \sum_{m} \left[ \frac{\nu(f)}{s(m,f)} \right] \left( \frac{[\nu(f)]}{s(m,f)} + 1 \right)
\]
where \( \nu(f) \) denotes the number of prime ideals dividing \( p \) which have degree \( f \) and \( s(m,f) = p^{m-1} \nu_a(p,f) \).

**Proof.** If \( \theta \) is absolutely primitive then Theorem 1 gives
\[
k_p(\theta) = \frac{1}{2} \sum_{i \neq j} \sum_{m} \left( f_i + f_j \right)
\]
where \( m_{ij} = \max \{ m : q_i(m) = q_j(m) \} \).

Obviously for \( f_i \neq f_j \) the equality \( q_i(m) = q_j(m) \) cannot occur. Hence we can write
\[
k_p(\theta) = \sum_{f} A(f)
\]
where
\[
A(f) = f \sum_{i \leq f} m_{ij}.
\]

For a given \( f \) let \( \nu(f) \) be the number of \( q_i(m) \) in (2.2) which have degree \( f \) and let
\[
F_f(x) = \prod_{i,j,f} q_i(x).
\]

Write
\[
F_f(x) = V_{1,m}^{a_1}(x) \ldots V_{e,m}^{a_e}(x) \mod p^m
\]
where \( V_{i,m}(x) \) are distinct elements of \( \mathcal{P}(m, f) \) and \( s(m,f) = |\mathcal{P}(m,f)| \).

From (3.2) we obtain
\[
A(f) = \frac{1}{2} \sum_{m} \sum_{i \leq f} a_i(m) a_{i,m} - 1
\]
where
\[
M = \min \{ m : a_i(m) = 1 \text{ for } i = 1, 2, \ldots, s(m,f) \}.
\]

Because of
\[
\sum_{i \leq f} a_i(m) = \nu(f)
\]
we get
\[
2A(f) + f \nu(f) M = \sum_{m} \sum_{i \leq f} a_i(m).
\]
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 \( \sum \delta_i = A - [A/s]s \).

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

\[
\sum_{i=1}^{s(m,f)} \alpha_{i,m} = e(f)
\]

is attained for any system \( \{\alpha_{i,m}\} \) such that

\[
\alpha_{i,m} = \left[ \frac{e(f)}{s(m,f)} \right] + \delta_{i,m}
\]

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

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

Now (3.3) gives

\[
A(f) \geq f \sum_m \left( \left[ \frac{e(f)}{s(m,f)} \right] - 1 \right) \left[ \frac{e(f)}{s(m,f)} \right] = \frac{s(m,f)}{2} + 1.
\]

To end the proof of Theorem 2 it is now enough to show that there exists an absolutely primitive \( \theta \in \mathbb{K} \) 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 \( \theta \) such that there is an equality in (3.5).

**Lemma 5.** Let \( M \) be a given integer and a system of nonnegative integers

\[
(r_k^{(m)})_{1 \leq m \leq M, 1 \leq k \leq s(m,f)}
\]

such that

\[
\sum_{k=1}^{s(m,f)} r_k^{(m)} = e(f)
\]

and

\[
\sum_{k=1}^{s(m,f)} r_k^{(m)} = r_k^{(m-1)} \quad \text{for} \quad m = 2, \ldots, M, \quad k = 1, \ldots, s(m-1,f).
\]

There exists an absolutely primitive \( \theta \in \mathbb{K} \) such that for the polynomial \( P_f(x) \) corresponding to \( \theta \) one has

\[
P_f(x) = x^{s(m,f)}x^{(m)} \cdots V_1^{(m)}(x)^{r_1^{(m)}} \cdots V_{s(m,f)}^{(m)}(x)^{r_{s(m,f)}^{(m)}} \mod p^m,
\]

with distinct \( V_i^{(m)}(x) \in \mathbb{V}(m,f) \), 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 \( \gamma_1, \ldots, \gamma_{s(f)} \in \mathbb{K} \) such that for every \( 1 \leq m \leq M \), the elements

\[
\gamma_m(\gamma_{m+1}), \ldots, \gamma_{s(m,f)+r(m)}(\gamma_{s(m,f)+r(m)}),
\]

where

\[
t_i = \begin{cases} 0, & i = 1, \\ r_i^{(m)} + \cdots + r_{i-1}^{(m)}, & i = 2, 3, \ldots, s(m,f),
\end{cases}
\]

have the same minimal polynomial \( q_{i,m} \in \mathbb{V}(m,f) \), while \( q_{i,m} \neq q_{j,m} \) for \( i \neq j \).

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

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

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

we can now determine \( \delta_{k,m} \) such that

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

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

**Corollary 2.** If \( p \) is unramified in \( \mathbb{K} \) then \( \kappa(\mathbb{K}) \) attains its maximal value when \( p \) splits.

**Proof.** Because of (3.1) and (3.3) it is enough to show that for every \( m \geq 1 \)

\[
\sum_f \left[ \frac{e(f)}{s(m,f)} \right] \left[ \frac{e(f)}{s(m,f)} \right] + 1
\]

\[
\leq \left[ \frac{n}{p^m} \right] \left[ \frac{n}{p^m} \right] + 1
\]

\[
= -2n + 2 \sum_{i=1}^{n} i.
\]

Observe that

\[
\left[ \frac{n}{p^m} \right] \left[ \frac{n}{p^m} \right] + 1
\]

\[
= -2n + 2 \sum_{i=1}^{n} i
\]
and
\[
\left[ \frac{a(f) - s(m, f)}{s(m, f)} \right] + 1 = -2g(f) + 2 \sum_{i=1}^{s(m, f)} a_i(f)^2
\]

where \(a_0, a_1(f)\) are determined so that they minimize \(\sum_{i=0}^{s(m, f)} a_i(f)^2\) respectively, under the restriction that
\[
\sum_{i=1}^{s(m, f)} a_i(f) = 2g(f).
\]

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

**Remark.** Using Theorem 1, one easily finds that the discriminant of \(F_j(x)\) (defined as in the proof of Theorem 2) is divisible at least by \(p\) in the power
\[
f(f) \left( \frac{p^{f(n+1)} - 1}{p^f - 1} - M(f) \right),
\]

where \(M(f) = \max \{m : p^m \leq f(f)\}\).

This gives
\[
x_p(K) \geq \frac{1}{2} \sum_f f(f) \left( \frac{p^{f(n+1)} - 1}{p^f - 1} - M(f) \right).
\]

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 \(x_p(K)\), 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 \(x_p(K)\) for \(K\) with a degree not exceeding 7. As an example of the application of our method we have determined the value of \(x_p(K)\) for \(8 \leq n \leq 12\), in the case where \(p\) is unramified. In the following table only those types of factorization are listed for which \(x_p(K) \neq 0\) for \(p = 2, 3, 5, 7\). There is one more prime \(p\) for which \(x_p(K) \neq 0\) can occur if \([K:Q] \leq 12\). Namely \(x_1(K) = x_0(K) = 1\) if \([K:Q] = 12\) and 11 splits completely in \(K\). If \(x_p \neq x_p\) for some \(p\) then we give in brackets the corresponding value of \(x_p\).

\[
pR_K = p_1 \cdots p_e, \quad \deg p = f_i.
\]
<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>[211111111]</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[211111111]</td>
<td>43</td>
<td>17</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>[211111111]</td>
<td>22</td>
<td>9</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[211111111]</td>
<td>14</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[321111111]</td>
<td>11</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>22</td>
<td>10</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[322111111]</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>[331111111]</td>
<td>48</td>
<td>21</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>30</td>
<td>13</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>18</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>16</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>7</td>
<td>14</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>12</td>
<td>22</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>14</td>
<td>34</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>23</td>
<td>9</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>[331111111]</td>
<td>8</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

References

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

by

K. Thanigasalam (Monaco, Penn.)

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

Theorem. $G(9) \leq 88$, $G(10) \leq 104$, $G(11) \leq 119$, $G(12) \leq 134$, $G(13) \leq 150$, $G(14) \leq 165$, $G(15) \leq 181$, $G(16) \leq 197$, $G(17) \leq 213$, $G(18) \leq 219$, $G(19) \leq 245$, $G(20) \leq 262$.

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

As in [3] we take

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

where $N$ is a large positive integer and $\delta$ is a small positive constant. Let

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

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

\[ u = \sum_{i=1}^{n} a_i^k \]

with

\[ P_1^{k-\delta} < u < \eta_2P_1^{k-\delta}, \]

and let

\[ U_\gamma = \text{card } \mathcal{U}. \]

Suppose further that $\mathcal{P}$ is the set of primes $\mathfrak{p}$ with

\[ \frac{1}{2} P_2^{k-\delta} \leq \mathfrak{p} \leq P_1^{k-\delta}. \]