Czechoslovak Mathematical Journal

Juraj Kostra

Remark on the minimum discriminant of normal fields

Czechoslovak Mathematical Journal, Vol. 39 (1989), No. 4, 555–558

Persistent URL: http://dml.cz/dmlcz/102328

CZECHOSLOVAK MATHEMATICAL JOURNAL

Mathematical Institute of the Czechoslovak Academy of Sciences

V. *39* (*114*), PRAHA 20. 12. 1989, No 4

REMARK ON THE MINIMUM DISCRIMINANT OF NORMAL FIELDS

JURAJ KOSTRA, Bratislava

(Received March 3, 1986)

In the present paper we shall determine the minimum discriminants of normal algebraic number fields of a prime degree over the rational field Q. Let D be the discriminant of an algebraic number field K of a degree n over Q. The problem of finding the lowest absolute value of D if K runs over all fields of the degree n with a given number of real and imaginary conjugate fields is not solved in general. The highest degree for which this problem is solved is $n = 5$ ([2], J. Hunter). The case when all conjugated fields are real (totally real case) is known at most for $n = 7$ ([6], M. Pohst). For greater n the minimum discriminants are not known. In the following we shall show that this problem is simpler when we look for the minimum discriminant of the normal fields a prime degree p over Q. Apart from the case $p = 2$ we need not consider the absolute value of D, because all fields are totally real and so $D > 0$.

By K_m we shall denote the cyclotomic field generated byan m-th primitive rooth from the unit. Often we shall need the following results:

Leopold [4], Narkiewicz [5]: (A1) *Let K be an Abelian algebraic number field and let the degree of the extension K/Q be n. Then the following conditions are equivalent*:

(a) *The field K has an integral normal basis.*

(b) *The field K can be embedded into K_m, where m is not divisible by any square of prime.*

(c) *The discriminant $d(K)$ is not divisible by any n-th power of prime.*

Hilbert [1]: (A2) *An Abelian algebraic number field K, the discriminant of which is prime to the degree of the extension K/Q, has an integral normal basis.*

Narkiewicz [5]: (A3) *If L/Q is finite and $Q \subset K \subset L$, then $d(L)$ is divisible by $d(K)^{[L:K]}$.*

(A4) *If K/Q is a normal extension of a prime degree p, then $d(K)$ is a $(p - 1)$-st power.*

(A5) *Let L_i/Q $(i = 1, 2)$ be a finite extension of degree n_i let $(d(L_1), d(L_2)) = 1$*

and let $K = L_1 . L_2$ be the sum of L_1, L_2. Then $[K : Q] = n_1 n_2$ and

$$d(K) = d(K_1)^{n_2}\, d(L_2)^{n_1} .$$

(A6) *If K is the sum of L_1, L_2 with $[L_i : Q] = n_i$, $i = 1, 2$ then $d(K)$ divides*

$$d(L_1)^{n_2}\, d(L_2)^{n_1} .$$

Lemma 1. *Let $K \subset K_m$, where $m = p_1^{k_1} \dots p_s^{k_s}$ and let there be an i, $1 \leqq i \leqq s$ such that $(d(K), p_i) = 1$. Then $K \subset K_{m_i}$, where*

$$m_i = \frac{m}{p^{k_i}} .$$

Proof. Proof is by contradiction. Suppose $K \not\subset K_{m_i}$. We have

$$K_m = K_{p_i}^{k_i} K_{m_i} ,$$

where by (A5)

$$[K_m : Q] = [K_{p_i}^{k_i} : Q]^{[K_{m_i}:Q]}\, [K_{m_i} : Q]^{[K_{p_i}^{k_i}:Q]} = \varphi(p_i^{k_i})^{\varphi(m_i)}\, \varphi(m_i)^{\varphi(p^{k_i})} .$$

Since $t = [KK_{m_i} : Q] > \varphi(m_i)$, and by (A6)

$$(d(K_{p_i}^{k_i}), d(KK_{m_i})) = 1 ,$$

by (A5) we obtain

$$[K_m : Q] = \varphi(p_i^{k_i})^t\, t\, \varphi(p_i^{k_i}) > \varphi(p_i^{k_i})^{\varphi(m_i)}\, \varphi(m_i)^{\varphi(p_i^{k_i})} = [K_m : Q] ,$$

which is a contradiction. Hence $K \subset K_{m_i}$.

Proposition 1. *Let p be a prime and let q be the smallest prime of the form $kp + 1$. Then the minimum discriminant D of the normal extension of the field of rational numbers Q with an integral normal basis of the degree p over Q is*

$$|D| = q^{p-1} .$$

Proof. First we show that there is a field K with an integral normal basis of the degree p over Q with the discriminant

$$|d(K)| = q^{p-1} .$$

Take the field K_q. Clearly $[K_q : Q] = kp$ and the Galois group $G(K_q/Q)$ is a cyclic group of the order kp. Hence there is $G_0 \subset G(K_q/Q)$ of the order k leaving fixed the field K, $[K : Q] = p$. From the fact that q is the only prime dividing $d(K_q)$ we get by (A3) that q is the only prime dividing $d(K)$. According to (A4), $d(K)$ is a $(p-1)$-st power and by (A1) we get $|d(K)| = q^{p-1}$.

Now we shall prove that $|D| = q^{p-1}$ is the minimum discriminant. This we shall show by contradiction. Let there be a normal algebraic number field K_0 with an integral normal basis of the degree p over Q such that

$$|d(K_0)| < q^{p-1} . \tag{1}$$

Due to (A1), $K_0 \subset K_m$, where m is not divisible by any square of prime. By (A4), $d(K_0)$ is a $(p-1)$-st power. Hence from (1) and from the fact that q is the smallest prime of the form $kp + 1$, using Lemma 1 we conclude that $K_0 \subset K_s$, where $s \mid m$ and s is not divisible by any prime of the form $kp + 1$. Therefore $p \nmid [K_s : Q]$ and this is a contradiction with the assumption that $[K_0 : Q] = p$. Proposition 1 is proved.

Lemma 2. *Let $K \subset K_{p^n}$ and $[K : Q] = p$. Then $p^{2(p-1)} \mid d(K)$.*

Proof. By (A4), $d(K)$ is a $(p-1)$-st power and therefore it is sufficient to prove that $p^p \mid d(K)$. We shall prove it by contradiction. Let $p^p \nmid d(K)$. According to (A3) p is the unique prime divisor of $d(K)$ and therefore (A1) implies $K \subset K_m$, where m is not divisible by any square of prime. Using Lemma 1 we get that $K \subset K_p$, which is a contradiction, because $[K : Q] > [K_p : Q]$. Hence $p^p \mid d(K)$.

Proposition 2. *Let p be a prime. Then the minimum discriminant D of a normal extension of the field of rational numbers Q without an integral normal basis of the degree p over Q is*

$$|D| = p^{2(p-1)}.$$

Proof. First we shall show that there is a field K without an integral normal basis of the degree p over Q with the discriminant

$$|d(K)| = p^{2(p-1)}.$$

Let $K \subset K_{p^2}$. According to Lemma 2, K has no integral normal basis and it is sufficient to show that $p^{3(p-1)} \nmid d(K)$. We shall prove it by contradiction. Let $p^{3(p-1)} \mid d(K)$. Then by (A3)

$$p^{3(p-1)^2} \mid |d(K_{p^2})| = p^{2p^2-3p}.$$

It means that $(p-2)^2 + p - 1 \leqq 0$, which is a contradiction. Hence $|d(K)| = p^{2(p-1)}$.

Now we shall show that $|F| = p^{2(p-1)}$ is the minimum discriminant. Proof is by contradiction. Let there be a normal field of algebraic numbers K_0 without an integral normal basis of the degree p over Q such that $|d(K_0)| < p^{2(p-1)}$. According to (A2), $p \mid d(K_0)$ and therefore by (A4) $d(K_0)$ is not divisible by any prime $q > p$. Hence Lemma 1 yields $K_0 \subset K_{mp^n}$, where m is not divisible by any prime $q \geqq p$ and $n \geqq 2$, because $n = 1$ would imply $p \nmid [K_{mp} : Q]$. According to Lemma 2 $K_0 \not\subset K_{p^n}$ and therefore $K_0 \cap K_{p^n} = Q$. Clearly $K_0 \cap K_m = Q$. Hence

$$[K_0 K_m : Q] = p[K_m : Q]$$

and by ([3], p. 224)

$$K_0 K_m \cap K_{p^n} = K',$$

where $[K' : Q] = p$. By Lemma 2, $p^{2(p-1)} \mid d(K')$ and using (A3) we get

$$p^{2(p-1)[K_m:Q]} \mid d(K_0 K_m). \tag{2}$$

According to (A6)

$$d(K_0 K_m) \mid d(K_m)^p \, d(K_0)^{[K_m:Q]},$$

where $(d(K_m), p) = 1$ and

$$p^{2(p-1)} \nmid d(K_0),$$

which is contradiction with (2). Proposition 2 is proved.

As a corollary from Proposition 1, 2 we get

Theorem. *Let p be a prime. Then the minimum discriminant D of a normal algebraic number field of the degree p over Q is*

1. $|D| = q^{p-1}$, *where q is the smallest prime of the form $kp + 1$, if there exists a prime of this form less than p^2.*
2. $|D| = p^{2(p-1)}$, *if there is no prime of the form $kp + 1$ less than p^2.*

Remark. It is known that there exist infinitely many primes p for which there is a prime $q = kp + 1$ and $q < p^2$. It is not known if there exists a prime p not having this property.

References

[1] *Hilbert, D.:* Die Theorie der algebraischen Zahlkörper. Jber. Deutsch. Math. Verein. *4*, 1897.

[2] *Hunter, J.:* The minimum discriminant of quintic fields. Proc. Glasgow Math. Assoc. *3*, 1957.

[3] *Lang, S.:* Algebra (Russian). MIR, Moscow 1968.

[4] *Leopoldt, H. W.:* Zur Arithmetik in abelschen Zahlkörpern. J. Reine Angew. Math. *209*, 1962.

[5] *Narkiewicz, W.:* Elementary and analytic theory of algebraic numbers. PWN, Warszawa 1974.

[6] *Pohst, M.:* The minimum discriminant of seventh degree totally real algebraic number fields. Number theory and algebra. Zassenhaus. Academic Press 1977.

Author's address: 814 73 Bratislava, Obrancov mieru 49, Czechoslovakia (MÚ SAV).