S. Oka
Nagoya Math. J.
Vol. 160 (2000), 181–186

ON THE UNRAMIFIED COMMON DIVISOR OF DISCRIMINANTS OF INTEGERS IN A NORMAL EXTENSION

SATOMI OKA

Abstract. Let F be an algebraic number field of a finite degree, and K be a normal extension over F of a finite degree n. Let $\mathfrak{p}$ be a prime ideal of F which is unramified in K/F, $\mathfrak{P}$ be a prime ideal of K dividing $\mathfrak{p}$ such that $N_{K/F}\mathfrak{P} = \mathfrak{p}^f$, $n = fg$. Denote by $\delta(K/F)$ the greatest common divisor of discriminants of integers of$K$ with respect to K/F. Then, $\mathfrak{p}$ divides $\delta(K/F)$ if and only if $\Sigma_{d|f}\mu(\frac{f}{d})N\mathfrak{p}^d < n$.

§1. Introduction

Let F be an algebraic number field of a finite degree, and K be an extension over F of a finite degree. A basic theorem in the general theory of algebraic number fields says that the greatest common divisor of differents of integers of K with respect to K/F is equal to the different $\mathfrak{d}(K/F)$ of K/F. Therefore, the greatest common divisor $\delta(K/F)$ of discriminants of integers of K with respect to K/F, as an ideal of F, is divisible by the discriminant $d(K/F) = N_{K/F}\mathfrak{d}(K/F)$. It is known, however, that $d(K/F)$ is not always equal to $\delta(K/F)$. In the present paper, we assume that K/F is a normal extension, and will give a necessary and sufficient condition for a prime ideal $\mathfrak{p}$, which is unramified in K/F, to divide $\delta(K/F)$. The main theorem is in Section 3.

A prime divisor of $\delta(K/F)$ which does not divide $d(K/F)$ was called "*Ausserwesentlicher Diskriminantenteiler*" (Dedekind [1]).

§2. Preliminaries

1. Throughout the paper, we use standard terminology of number theory as in [2] and [3].

Let F be an algebraic number field of a finite degree, and K be an extension over F of a finite degree n. The different $\mathfrak{d}(\alpha, K/F)$ of an element

Received October 26, 1999.
2000 Mathematics Subject Classification: Primary:11R04, Secondary:11R29.

α of K with respect to F is then defined by $f'(\alpha) = \mathfrak{d}(\alpha, K/F)$ where $f(X)$ is the characteristic polynomial of $\alpha = \alpha^{(1)}$ with respect to K/F. If $\alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$ are conjugates of α with respect to K/F, the equality $\mathfrak{d}(\alpha, K/F) = \prod_{i\neq 1}(\alpha^{(1)} - \alpha^{(i)})$ holds. Furthermore,

$$\begin{aligned} d(\alpha, K/F) &= \begin{vmatrix} 1 & \alpha^{(1)} & \cdots & \alpha^{(1)n-1} \\ 1 & \alpha^{(2)} & \cdots & \alpha^{(2)n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{(n)} & \cdots & \alpha^{(n)n-1} \end{vmatrix}^2 \\ &= \prod_{i>j}(\alpha^{(i)} - \alpha^{(j)})^2 \\ &= (-1)^{n(n-1)/2}\prod_{i\neq j}(\alpha^{(i)} - \alpha^{(j)}) \\ &= (-1)^{n(n-1)/2} N_{K/F}\mathfrak{d}(\alpha, K/F) \end{aligned}$$

implies the relation

$$d(\alpha, K/F) = (-1)^{n(n-1)/2} N_{K/F}\mathfrak{d}(\alpha, K/F)$$

between the different of α and the relative discriminant $d(\alpha, K/F)$ of α with respect to K/F.

2. We insert here some elementary facts concerning finite fields.

Let K_1 be a finite field, and K_f be an extension of K_1 of degree f. Then, the Galois group Z of K_f/K_1 is cyclic of order f, and, for a divisor d of f, there is a unique subfield K_d of K_f of degree d over K_1. Denote by C_d the set of elements γ of K_f such that $K_1(\gamma) = K_d$, and by c_d the number of elements of C_d. Then, $\cup_{d|f} C_d = K_f$ implies $\sum_{d|f} c_d = q^f$, where $q = c_1$ is the number of elements of K_1. Thus, Möbius' inversion formula yields

$$c_f = \sum_{d|f} \mu\left(\frac{f}{d}\right) q^d.$$

Every f elements of C_f are mutually conjugate under the action of the Galois group Z. So, denoting the set of such conjugacy classes of C_f by $\tilde{C}_f$, the number of elements of $\tilde{C}_f$ is $c_f/f = M(q, f)$ with

$$M(q, f) = \frac{1}{f}\sum_{d|f} \mu\left(\frac{f}{d}\right) q^d. \tag{1}$$

§3. Main theorem

In this article, we assume that K/F is normal with $G = \mathrm{Gal}(K/F)$. Here, as before, F is an algebraic number field of a finite degree, and K is an extension over F of a finite degree n. Let now $\mathfrak{o}_K$ and $\mathfrak{o}_F$ be ring of integers of K and F, respectively, $\mathfrak{p}$ a prime ideal of F which is unramified in K, and $\mathfrak{P}$ be a prime ideal of K dividing $\mathfrak{p}$. Moreover, let Z be the decomposition group of $\mathfrak{P}$, f be the order of Z, and $\sigma_1, \sigma_2, \cdots, \sigma_g$ be a system of representatives of $Z\backslash G$ fixed once for all with $fg = n$. We then apply (1) to the case where $K_f = \mathfrak{o}_K/\mathfrak{P}$ and $K_1 = \mathfrak{o}_F/\mathfrak{p}$. We write $C(\mathfrak{P})$ for C_f and $\tilde{C}(\mathfrak{P})$ for $\tilde{C}_f$ and can see that

$$M(N\mathfrak{p}, f) = \frac{1}{f}\sum_{d|f} \mu\left(\frac{f}{d}\right) N\mathfrak{p}^d \tag{2}$$

is the number of elements of $\tilde{C}(\mathfrak{P})$. Since $\mathfrak{P}$ is an arbitrary divisor of $\mathfrak{p}$ in K, $C(\mathfrak{P}^\sigma)$ and $\tilde{C}(\mathfrak{P}^\sigma)$ for any $\sigma \in G$ are as well-defined as $C(\mathfrak{P})$ and $\tilde{C}(\mathfrak{P})$, and the number of element of $\tilde{C}(\mathfrak{P}^\sigma)$ is equal to that of $C(\mathfrak{P})$ given by (2).

Our main theorem is stated as follows:

THEOREM. *Let F be an algebraic number field of a finite degree, and K be a normal extension over F of a finite degree n. Let $\mathfrak{p}$ be a prime ideal of F which is unramified in K/F, $\mathfrak{P}$ be a prime ideal of K dividing $\mathfrak{p}$ such that $N_{K/F}\mathfrak{P} = \mathfrak{p}^f$, $n = fg$. Denote by $\delta(K/F)$ the greatest common divisor of discriminants of integers of K with respect to K/F, and $M(N\mathfrak{p}, f)$ be as in* (2). *Then, $\mathfrak{p}$ divides $\delta(K/F)$ if and only if $M(N\mathfrak{p}, f) < g$, or equivalently if and only if $\sum_{d|f}\mu(\frac{f}{d})N\mathfrak{p}^d < n$.*

Proof. Meanings of symbols Z and σ_i being as above, we say that a residue classes represented by $\alpha_i \bmod \mathfrak{P}^{\sigma_i}$ and by $\alpha_j \bmod \mathfrak{P}^{\sigma_j}$, $(\alpha_i, \alpha_j \in \mathfrak{o}_K)$, are conjugate, when there exists an element σ of $G = \mathrm{Gal}(K/F)$ such that $\mathfrak{P}^{\sigma_i\sigma} = \mathfrak{P}^{\sigma_j}$ and $\alpha_i^\sigma \equiv \alpha_j \pmod{\mathfrak{P}^{\sigma_j}}$. In this situation, $\sigma \in \sigma_i^{-1}Z\sigma_j$ necessarily holds. For each σ_i, the sets $C(\mathfrak{P}^{\sigma_i})$ and $\tilde{C}(\mathfrak{P}^{\sigma_i})$ are as well-defined as $C(\mathfrak{P})$ and $\tilde{C}(\mathfrak{P})$ above, and the set of all $C(\mathfrak{P}^{\sigma_i})$ is divided into $M(N\mathfrak{p}, f)$ conjugacy classes. In particular, the set of conjugacy classes of one $C(\mathfrak{P}^{\sigma_i})$ coincides with $\tilde{C}(\mathfrak{P}^{\sigma_i})$, and this set consists of $M(N\mathfrak{p}, f)$ elements either.

Assume now $M \geq g$. Then, there are integers $\alpha_1, \alpha_2, \cdots, \alpha_g$ in $\mathfrak{o}_K$ such that the residue class $\alpha_i \bmod \mathfrak{P}^{\sigma_i}$ belongs to $C(\mathfrak{P}^{\sigma_i})$ and that $\alpha_i \bmod \mathfrak{P}^{\sigma_i}$

and α_j mod $\mathfrak{P}^{\sigma_j}$ are not conjugate whenever $i \neq j$. Using these integers, we find an integer $\alpha \in \mathfrak{o}_K$ satisfying simultaneously

$$\alpha \equiv \alpha_i \pmod{\mathfrak{P}^{\sigma_i}}, \quad (i = 1, 2, \cdots, g).$$

Suppose that

$$\alpha^{\sigma} \equiv \alpha \pmod{\mathfrak{P}^{\sigma_j}} \tag{3}$$

holds for an element $\sigma \in G$, $(\sigma \neq 1)$, and for some j. Then, taking σ_i with $\sigma_i \sigma = \xi \sigma_j$, $(\xi \in Z)$, we have

$$\alpha_i^{\sigma_i^{-1} \xi \sigma_j} \equiv \alpha_j \pmod{\mathfrak{P}^{\sigma_j}},$$

contrary to the choice of $\alpha_1, \alpha_2, \cdots, \alpha_g$. Thus, $\alpha - \alpha^{\sigma}$ is not divisible by any $\mathfrak{P}^{\sigma_j}$, and therefore is prime to $\mathfrak{p}$. From this follows that $\mathfrak{p}$ does not divide $\delta(K/F)$.

Assume conversely $M < g$. Then (3) should hold for $\sigma = \sigma_i^{-1} \xi \sigma_j$ with some σ_i, σ_j, $(i \neq j)$ and $\xi \in Z$, whenever α is an integer in $\mathfrak{o}_K$ such that α mod $\mathfrak{P}_i$ belongs to $C(\mathfrak{P}^{\sigma_i})$ for every i. This means that the discriminant of such an α with respect to K/F is divisible by $\mathfrak{p}$. If α is an integer in $\mathfrak{o}_K$, and α mod $\mathfrak{P}^{\sigma_i}$ does not belong to $C(\mathfrak{P}^{\sigma_i})$ for some i, then

$$\alpha^{\sigma_i^{-1} \xi \sigma_i} \equiv \alpha \pmod{\mathfrak{P}^{\sigma_i}}$$

holds with an element ξ of Z, $(\xi \neq 1)$, which implies (3) with $\sigma = \sigma_i^{-1} \xi \sigma_i \neq 1$. From all these arguments, we can conclude that the discriminant of an integer α in $\mathfrak{o}_K$ is divisible by $\mathfrak{p}$ regardless of its residue class $\bmod\, \mathfrak{p}$. Hence, $\mathfrak{p}$ divides $\delta(K/F)$.

COROLLARY 1. *Assume that the prime ideal in the Theorem decomposes completely in K. Then, $\mathfrak{p}$ divides $\delta(K/F)$ if and only if $N\mathfrak{p} < n$.*

Proof. In this case, $f = 1$, and $\sum_{d|f} \mu(\frac{f}{d}) N\mathfrak{p}^d = N\mathfrak{p}$.

COROLLARY 2. *If the prime ideal $\mathfrak{p}$ in the Theorem satisfies $N\mathfrak{p} \geq n$, then $\mathfrak{p}$ dose not divide $\delta(K/F)$.*

Proof. Put $N\mathfrak{p} = q$. Then,

$$\sum_{d|f} \mu\left(\frac{f}{d}\right) q^d \geq q^f - \sum_{d|f, d<f} q^d \geq q^f - (q^{f-1} + q^{f-2} + \cdots + q)$$
$$= q - q\frac{q^{f-1} - 1}{q - 1} \geq q^f - q(q^{f-1} - 1) = q \geq n.$$

§4. Examples

1. Let K be a composite of a finite number (>1) of quadratic fields over $\mathbf{Q} = F$ in which 2 is unramified. Then, the degree f of a prime factor of 2 in K is either 1 or 2, and $n = (K : \mathbf{Q}) \geq 4$. If $f = 1$, then Corollary 1 shows that 2 divides $\delta(K/\mathbf{Q})$. If $f = 2$, then the number $M(N\mathfrak{p}, f)$ in the Theorem is $\frac{1}{2}(2^2 - 2) = 1$. Since $g = \frac{n}{2} \geq 2$, the Theorem implies that 2 divides $\delta(K/\mathbf{Q})$. Namely, 2 always divides $\delta(K/\mathbf{Q})$, whenever K is a composite of quadratic fields in which 2 is unramified.

2. Let p be a prime number, and l be a prime number dividing $p^3 - 1$. Then, p decomposes completely in the subfield K of the cyclotomic field $\mathbf{Q}(e^{(2\pi i)/l})$ with the property $(K : \mathbf{Q}) = \frac{1}{3}(l-1)$. If here moreover $\frac{1}{3}(l-1) > p$, then it follows from Corollary 1 that p divides $\delta(K/\mathbf{Q})$.

A few actual numerical examples are:

p	3	5	7	11	13
l	13	31	-	-	61

3. Let $K/\mathbf{Q}$ be normal of degree 4. If $K/\mathbf{Q}$ is not cyclic and 2 is unramified, then example 1 shows that 2 divides $\delta(K/\mathbf{Q})$. Even if $K/\mathbf{Q}$ is cyclic, $\sum_{d|f} \mu(\frac{f}{d})2^d$ is 2 for $f = 1$ and 2. Therefore, 2 divides $\delta(K/\mathbf{Q})$, unless 2 remains prime in K. If 3 is completely decomposed in K, then Corollary 1 implies that 3 divides $\delta(K/\mathbf{Q})$. But, if 3 is not completely decomposed and unramified, then $\sum_{d|f} \mu(\frac{f}{d})3^d = 3^4 - 3^2$ or $3^2 - 3$, and is bigger than 4. So, by the Theorem, 3 does not divide $\delta(K/\mathbf{Q})$. The unramified primes bigger than 3 do not divide $\delta(K/\mathbf{Q})$ as a consequence of Corollary 2.

Acknowledgements. The author expresses her thanks to Professor Tomio Kubota for his advice and encouragement.

References

[1] R. Dedekind, *Über den Zusammenhang zwuschen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abh.der König. Gesell. der Wiss. zu Göttingen, **23** (1878), 1-23, Complete works, Chelsea, 1969.

[2] S. Lang, Algebraic number theory, Addison-Wesley, 1970.

[3] E. Weiss, Algebraic number theory, AcGraw-Hill, 1963.

Department of Mathematics
Meijo University
Shiogamaguchi 1-501, Tenpakuku
Nagoya, 468-8502, Japan
d3991001@meijo-u.ac.jp