TSUKUBA J. MATH.
Vol. 26 No. 1 (2002), 69-78

ON THE COMMON DIVISOR OF DISCRIMINANTS OF INTEGERS

By

Satomi OKA

Abstract. Let F be an algebraic number field of a finite degree, and let K be an extension of F of a finite degree. Denote by $\delta(K/F)$ the greatest common divisor of the discriminants of integers of K with respect to K/F. Then, $\delta(K/F)$ is divisible by the discriminant $d(K/F)$ of K/F.

Let $\mathfrak{p}$ be an arbitrary prime ideal of F, let $\mathfrak{p} = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\cdots\mathfrak{q}_g^{e_g}$ be the decomposition of $\mathfrak{p}$ in K into primes, and let f_i be the degree of $\mathfrak{q}_i$. The set of indices $\{1,2,\ldots,g\}$ is then divided into the union of maximal subsets I such that $f_i = f_j$ whenever i and j belong to a common I. We write f_I instead of f_i for $i \in I$, and denote by g_I the number of elements in I. Put on the other hand $c(I) = \sum_{d|f_I} \mu(f_I/d)N\mathfrak{p}^d$, where μ is the *Möbius* function. Then, $\mathfrak{p}$ divides $\delta(K/F)d(K/F)^{-1}$ if and only if there exists an I such that $c(I) < f_I g_I$.

§ 1. Introduction

Let F be an algebraic number field of a finite degree, and K 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 $d(K/F) = N_{K/F}\mathfrak{d}(K/F)$ of K/F. It is known, however, that $d(K/F)$ is not always equal to $\delta(K/F)$. In the present paper, we will give a necessary and sufficient condition in a simple, elementary

Primary: 11R04 Algebraic numbers; rings of algebraic integers.
Secondary: 11R29 Class numbers, class groups, discriminants.
Received August 10, 2000.
Revised November 30, 2000.

form for an arbitrary prime ideal $\mathfrak{p}$ of F to divide $\delta(K/F)d(K/F)^{-1}$. The main theorem is in §4. 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 [4].

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 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 $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ 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,

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

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 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, $\bigcup_{d|f} C_d = K_f$ 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

$$
c_f = c(q, f), \tag{1}
$$

where $c(q,f)$ is defined by

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

for any two natural numbers q,f. Every f elements of C_f are mutually conjugate under the action of the Galois group Z. So, denoting the set of such conjugate classes of C_f by $\tilde{C}_f$, the number of elements of $\tilde{C}_f$ is

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

3. Let, as in 1, F be an algebraic number field of a finite degree, and K an extension over F of a finite degree n. Assume that $\mathfrak{p}$ is a prime ideal of F, and L is a normal extension over F of a finite degree containing K. For instance, we may take as L the Galois closure of K/F.

Put

$$Gal(L/F)=G,\quad Gal(L/K)=H,$$

and let Z be the decomposition group of a prime factor $\mathfrak{P}$ of $\mathfrak{p}$ in L. Then, $\mathfrak{P}^\sigma$ and $\mathfrak{P}^{\sigma'}$, $(\sigma,\sigma'\in G)$, divide a common prime ideal $\mathfrak{q}$ of K if and only if σ and σ' belong to a common double coset of $Z\backslash G/H$. Fixing the representatives $\sigma_1=1$, $\sigma_2,\ldots,\sigma_g$ of the double cosets so that

$$G=\bigcup_{i=1}^{g}Z\sigma_i H$$

holds, the decomposition of $\mathfrak{p}$ in K is of the form

$$\mathfrak{p}=\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\cdots\mathfrak{q}_g^{e_g}, \tag{2}$$

where $\mathfrak{q}_i$ is the prime ideal of K divisible by $\mathfrak{P}^{\sigma_i}$. Since $\mathfrak{P}^{\sigma_i}=\mathfrak{P}^{\sigma_i\eta}$, $(\eta\in H)$, is equivalent to $\sigma_i\eta\sigma_i^{-1}\in Z$, the number of different prime factors of $\mathfrak{q}_i$ in L is $(H:\sigma_i^{-1}Z\sigma_i\cap H)$. The product of the degree and the ramification exponent of $\mathfrak{P}^{\sigma_i}$ over K is $(\sigma_i^{-1}Z\sigma_i\cap H:1)$. Therefore, the degree f_i and the ramification exponent e_i of $\mathfrak{q}_i$ over F is given by

$$e_i f_i=(\sigma_i^{-1}Z\sigma_i:\sigma_i^{-1}Z\sigma_i\cap H)$$

and

$$e_i=(\sigma_i^{-1}T\sigma_i:\sigma_i^{-1}T\sigma_i\cap H),$$

where T is the inertia group of $\mathfrak{P}$.

§3. Isomorphisms between Residue Class Fields

In the investigation of the different, it is basically enough to treat one single prime ideal of the extention field. But, in the investigation of the discriminant, it is required to handle all those prime ideals of the extension field at the same time which divide a prime ideal of the base field. Actually, the discriminant is of a semi-local nature. From this point of view, we summarize in this article some propositions; they are effectively used in the proof of the main theorem.

In this article, as before, F is an algebraic number field of a finite degree, and K is an extension over F of a finite degree n. In addition, we employ same notation and symbols as in 3 of §2. Let now $\mathfrak{o}_L$, $\mathfrak{o}_K$ and $\mathfrak{o}_F$ be the ring of integers of L, K and F, respectively, $\mathfrak{p}$ a prime ideal of F, and $\mathfrak{P}$ a prime ideal of L dividing $\mathfrak{p}$. Moreover, let Z be the decomposition group of $\mathfrak{P}$. Then, corresponding to the decomposition (2) of $\mathfrak{p}$ in K, we put

$$\mathfrak{o}_F/\mathfrak{p} = K(\mathfrak{p}), \quad \mathfrak{o}_K/\mathfrak{q}_i = K(\mathfrak{q}_i)$$

and

$$G(\mathfrak{q}_i) = Gal(K(\mathfrak{q}_i)/K(\mathfrak{p})), \tag{3}$$

so that

$$(K(\mathfrak{q}_i) : K(\mathfrak{p})) = f_i, \quad N\mathfrak{q}_i = q^{f_i}, \quad q = N\mathfrak{p}.$$

For every divisor d of f_i, the finite field $K(\mathfrak{q}_i)$ has a unique subfield of degree d over $K(\mathfrak{p})$, which will be denoted by $K(\mathfrak{q}_i)_d$. In particular, $K(\mathfrak{q}_i) = K(\mathfrak{q}_i)_{f_i}$ and $K(\mathfrak{q}_i)_1 = K(\mathfrak{p})$. We denote by $C(\mathfrak{q}_i)$ the set of elements γ of $K(\mathfrak{q}_i)$ such that γ generates $K(\mathfrak{q}_i)$ over $K(\mathfrak{p})$, and by $c(\mathfrak{q}_i)$ the number of elements of $C(\mathfrak{q}_i)$. The elements of $C(\mathfrak{q}_i)$ are divided into conjugate classes under the action of $G(\mathfrak{q}_i)$, and every conjugate class consists of f_i elements. The set of such conjugate classes will be denoted by $\tilde{C}(\mathfrak{q}_i)$. Considering $K(\mathfrak{q}_i)$, $K(\mathfrak{q}_i)_d$, f_i, and $q = N\mathfrak{p}$ as to be K_f, K_d, f, and q in 2 of §2, we have $c(\mathfrak{q}_i) = c(q, f_i)$, or

$$c(\mathfrak{q}_i) = \sum_{d|f_i} \mu\left(\frac{f_i}{d}\right) N\mathfrak{p}^d \tag{4}$$

by (1). Accordingly, the number of elements of $\tilde{C}(\mathfrak{q}_i)$ is $\frac{1}{f_i}c(\mathfrak{q}_i)$.

We write an element of $K(\mathfrak{q}_i)$ in the form $\alpha \bmod \mathfrak{q}_i$, $(\alpha \in \mathfrak{o}_K)$, and we say that $\alpha \bmod \mathfrak{q}_i \in K(\mathfrak{q}_i)$ and $\beta \bmod \mathfrak{q}_j \in K(\mathfrak{q}_j)$ are weakly conjugate, if there is an element σ in $\sigma_i^{-1} Z \sigma_j$ such that

$$\alpha^\sigma \equiv \beta \pmod{\mathfrak{P}^{\sigma_j}}. \tag{5}$$

Here, α^{σ} need not belong to K. This definition of weak conjugation does not depend on the choice of σ_i. In fact, suppose

$$\sigma_i' = \xi_i \sigma_i \eta_i, \quad \sigma_j' = \xi_j \sigma_j \eta_j, \quad (\xi_i, \xi_j \in Z, \eta_i, \eta_j \in H),$$

and put $\sigma' = \eta_i^{-1} \sigma \eta_j$. Then, σ' belongs to $\sigma_i'^{-1} Z \sigma_j'$, and $\mathfrak{P}^{\sigma_j'} = \mathfrak{P}^{\sigma_j \eta_j}$. Hence, it follows from (5) that

$$\alpha^{\sigma} = \alpha^{\eta_i \sigma' \eta_j^{-1}} = \alpha^{\sigma' \eta_j^{-1}} \equiv \beta \pmod{\mathfrak{P}^{\sigma_j}},$$

which implies

$$\alpha^{\sigma'} \equiv \beta \pmod{\mathfrak{P}^{\sigma_j'}}.$$

The weak conjugation determines a relation between the residue classes $\alpha \bmod \mathfrak{q}_i$ and $\beta \bmod \mathfrak{q}_j$, which proves to be an equivalence relation. Firstly the self-equivalence is clear by $\alpha \equiv \alpha \pmod{\mathfrak{P}^{\sigma_i}}$ for any $\alpha \in \mathfrak{o}_K$. To see the reflectivity, we note that $\mathfrak{P}^{\sigma_j \sigma^{-1}} = \mathfrak{P}^{\sigma_i}$, if $\sigma^{-1} \in \sigma_j^{-1} Z \sigma_i$. From this and from (5) follows $\beta^{\sigma^{-1}} \equiv \alpha \pmod{\mathfrak{P}^{\sigma_i}}$. Assume now

$$\alpha^{\sigma} \equiv \beta \pmod{\mathfrak{P}^{\sigma_j}}, \quad \beta^{\tau} \equiv \gamma \pmod{\mathfrak{P}^{\sigma_k}}, \quad (\alpha, \beta, \gamma \in \mathfrak{o}_K),$$

with $\sigma \in \sigma_i^{-1} Z \sigma_j$, $\tau \in \sigma_j^{-1} Z \sigma_k$. Then, $\sigma\tau \in \sigma_i^{-1} Z \sigma_k$ and $\mathfrak{P}^{\sigma_j \tau} = \mathfrak{P}^{\sigma_k}$. Thus, we get the transitivity

$$\alpha^{\sigma\tau} \equiv \beta^{\tau} \equiv \gamma \pmod{\mathfrak{P}^{\sigma_k}}.$$

An isomorphism between $K(\mathfrak{q}_i)$ or their subfields will be called a weak conjugating isomorphism, if it maps each residue class to a weakly conjugate one.

PROPOSITION 1. *Every element of* $G(\mathfrak{q}_i)$ *in* (3) *is a weak conjugating isomorphism of* $K(\mathfrak{q}_i)$ *onto itself.*

PROOF. By definition, a weak conjugating isomorphism of $K(\mathfrak{q}_i)$ is an automorphism of $K(\mathfrak{q}_i)/K(\mathfrak{p})$ induced by an element of $\sigma_i^{-1} Z \sigma_i$. Put here $K(\mathfrak{P}^{\sigma_i}) = \mathfrak{o}_L/\mathfrak{P}^{\sigma_i}$. Then, $\sigma_i^{-1} Z \sigma_i$ is the Galois group of $K(\mathfrak{P}^{\sigma_i})/K(\mathfrak{p})$, and $K(\mathfrak{q}_i)$ is a subfield of $K(\mathfrak{P}^{\sigma_i})/K(\mathfrak{p})$. Therefore, every element of $G(\mathfrak{q}_i)$ is induced by an element of $\sigma_i^{-1} Z \sigma_i$, and is a weak conjugating isomorphism. (q.e.d.)

PROPOSITION 2. *If two elements* $x \in K(\mathfrak{q}_i)$ *and* $y \in K(\mathfrak{q}_j)$ *are weakly conjugate, then* x *belongs to* $K(\mathfrak{q}_i)_d$ *and* y *belongs to* $K(\mathfrak{q}_j)_d$, *where* d *is the g.c.d. of* $f_i = (K(\mathfrak{q}_i) : K(\mathfrak{p}))$ *and* $f_j = (K(\mathfrak{q}_j) : K(\mathfrak{p}))$.

PROOF. The fields generated by x and y over $K(\mathfrak{p})$ have a common degree d' over $K(\mathfrak{p})$. So, $d'|d$, and the both fields must be contained in $K(\mathfrak{q}_i)_d$ and $K(\mathfrak{q}_j)_d$, respectively, because a finite field has a unique extension field with a given degree. (q.e.d.)

PROPOSITION 3. *Notation being as in Prop. 2, there exists a weak conjugating isomorphism from $K(\mathfrak{q}_i)_d$ onto $K(\mathfrak{q}_j)_d$, and the number of different such isomorphism is d.*

PROOF. The element $\sigma_i^{-1}\sigma_j$ of G maps $K(\mathfrak{P}^{\sigma_i}) = \mathfrak{o}_L/\mathfrak{P}^{\sigma_i}$ onto $K(\mathfrak{P}^{\sigma_j}) = \mathfrak{o}_L/\mathfrak{P}^{\sigma_j}$. The image by $\sigma_i^{-1}\sigma_j$ of the subfield $K(\mathfrak{q}_i)_d$ of $K(\mathfrak{P}_i)$ must coincide with $K(\mathfrak{q}_j)_d$, because a finite field has a unique extension field with a given degree. This proves the first assertion. The second assertion follows now from Prop. 1. (q.e.d.)

Under the equivalence relation determined by the weak conjugation, the union $\bigcup_{i=1}^{g} K(\mathfrak{q}_i)$ as well as the union $\bigcup_{i=1}^{g} C(\mathfrak{q}_i)$ is divided into equivalence classes, which will be called weak conjugate classes.

PROPOSITION 4. *The weak conjugate classes of $C(\mathfrak{q}_i)$ are same as classes in $\tilde{C}(\mathfrak{q}_i)$.*

PROOF. This follows immediately from Prop. 1. (q.e.d.)

If I is a maximal subset of indices $\{1, 2, \ldots, g\}$ in (2) such that $f_i = f_j$ for every $i, j \in I$, then we write f_I instead of f_i for $i \in I$, and will denote by g_I the number of indices in I. We call I a component of indices. Clearly, $\sum_I g_I = g$.

PROPOSITION 5. *Let I be a component of indices. Then, the number of weak conjugate classes in the union $\bigcup_{i \in I} C(\mathfrak{q}_i)$ is given by $c(I)/f_I = (1/f_I)\sum_{d|f_I} \mu(f_I/d) N\mathfrak{p}^d$, which is equal to the number of elements in $\tilde{C}(\mathfrak{q}_i)$, $(i \in I)$.*

PROOF. This follows from Prop. 3, Prop. 4, and (4).

§4. Application of the Local Theory

To prove our main theorem, it is convenient to apply some properties of local fields.

Notation being as in 3 of §2, we denote by $K_{(i)}$ the $\mathfrak{q}_i$-completion of K, by $L_{(i)}$ the $\mathfrak{P}^{\sigma_i}$-completion of L, and by $F_\mathfrak{p}$ the $\mathfrak{p}$-completion of F. Moreover, we denote by $\mathfrak{o}_{(i)}$, $\mathfrak{O}_{(i)}$, and $\mathfrak{o}_\mathfrak{p}$ the rings of integers of $K_{(i)}$, $L_{(i)}$, and $F_\mathfrak{p}$, respectively. Since no confusion is possible, the maximal ideal of $\mathfrak{o}_{(i)}$ will be denoted by $\mathfrak{q}_i$. Similarly, $\mathfrak{P}^{\sigma_i}$ and $\mathfrak{p}$ will stand for maximal ideals of $\mathfrak{O}_{(i)}$ and $\mathfrak{o}_\mathfrak{p}$, respectively.

We have isomorphisms

$$\mathfrak{o}_{(i)}/\mathfrak{q}_i \cong \mathfrak{o}_K/\mathfrak{q}_i = K(\mathfrak{q}_i), \quad \mathfrak{o}_\mathfrak{p}/\mathfrak{p} \cong \mathfrak{o}_F/\mathfrak{p} = K(\mathfrak{p})$$

and

$$\mathfrak{O}_{(i)}/\mathfrak{P}^{\sigma_i} \cong \mathfrak{o}_L/\mathfrak{P}^{\sigma_i} = K(\mathfrak{P}^{\sigma_i}),$$

where the meanings of $K(\mathfrak{q}_i)$, $K(\mathfrak{p})$, and $K(\mathfrak{P}^{\sigma_i})$ are same as in §3. Accordingly, every terminology concerning $\alpha \bmod \mathfrak{q}_i$, $(\alpha \in \mathfrak{o}_K)$, $\alpha \bmod \mathfrak{p}$, $(\alpha \in \mathfrak{o}_F)$, or $\alpha \bmod \mathfrak{P}^{\sigma_i}$, $(\alpha \in \mathfrak{o}_L)$ can be used for $\alpha \bmod \mathfrak{q}_i$, $(\alpha \in \mathfrak{o}_{(i)})$, $\alpha \bmod \mathfrak{p}$, $(\alpha \in \mathfrak{o}_\mathfrak{p})$, or $\alpha \bmod \mathfrak{P}^{\sigma_i}$, $(\alpha \in \mathfrak{O}_{(i)})$, without change. In particular, the notion of weak conjugation introduced in §3 makes sense also for residue classes $\alpha_i \bmod \mathfrak{q}_i$, $(\alpha_i \in \mathfrak{o}_{(i)})$ and $\alpha_j \bmod \mathfrak{q}_j$, $(\alpha_j \in \mathfrak{o}_{(j)})$.

As is known in the theory of local fields, $K_{(i)}/F_\mathfrak{p}$ has a unique unramified maximal intermediate field, which we will denote by $K_{(i),0}$. The extension $K_{(i),0}/F_\mathfrak{p}$ is cyclic, cyclotomic, and $K_{(i)}/K_{(i),0}$ is fully ramified, so that

$$(K_{(i)} : K_{(i),0}) = e_i, \quad (K_{(i),0} : F_\mathfrak{p}) = f_i.$$

Denoting by $\mathfrak{o}_{(i),0}$ the ring of integers of $K_{(i),0}$, we have furthermore

$$\mathfrak{o}_{(i)}/\mathfrak{q}_i \cong \mathfrak{o}_{(i),0}/\mathfrak{q}_i \cap \mathfrak{o}_{(i),0} \cong \mathfrak{o}_{(i),0}/\mathfrak{p}.$$

To go forward, we quote here a basic theorem in the theory of local fields without proof. We state it in the form of next proposition fitting to the present situation.

PROPOSITION 6. *Notation being as above and as in* 3 *of* §2, *let* π_i *be a prime element of* $\mathfrak{q}_i$ *in* $\mathfrak{o}_{(i)}$. *Then, the* $\mathfrak{q}_i$*-exponent of the different* $\mathfrak{D}(K/F)$ *of* K/F *is equal to the* $\mathfrak{q}_i$*-exponent of*

$$\prod_\sigma (\pi_i - \pi_i^\sigma), \quad \sigma \in \sigma_i^{-1} T \sigma_i \cap H \backslash \sigma_i^{-1} T \sigma_i, \quad \pi_i^\sigma \neq \pi_i.$$

PROPOSITION 7. *Notation being as in Prop.* 6 *and in* §3, *let an element* $\alpha_{i,0}$ *of* $\mathfrak{o}_{(i),0}$ *be given for each* i, $(i = 1, 2, \ldots, g)$, *such that*

a) $\alpha_{i,0} \bmod \mathfrak{q}_i$ *belongs to* $C(\mathfrak{q}_i)$,

and that

b) $\alpha_{i,0} \bmod \mathfrak{q}_i$ *and* $\alpha_{j,0} \bmod \mathfrak{q}_j$, $(i \neq j)$, *are not weakly conjugate.*

Put

$$\alpha_i = \alpha_{i,0} + \pi_i,$$

and let σ *be an element of* G *which does not belong to the union* $\bigcup_i H \cdot \sigma_i^{-1} T \sigma_i$. *Then, a conguruence of the form*

$$\alpha_i^{\sigma} \equiv \alpha_j \pmod{\mathfrak{P}^{\sigma_j}} \tag{6}$$

can not hold for any i, j.

PROOF. Fix one arbitrary i, and assume first $\sigma \in \sigma_i^{-1} Z \sigma_i$. Then, $\pi_i - \pi_i^{\sigma} \equiv 0 \pmod{\mathfrak{P}^{\sigma_i}}$. On the other hand, we see by the local theory that $\sigma_i^{-1} Z \sigma_i / \sigma_i^{-1} T \sigma_i$ is the Galois group of $K_{(i),0}/F_{\mathfrak{p}}$. This means that σ induces a non-trivial automorphism of $K(\mathfrak{q}_i)$ unless it belongs $\sigma_i^{-1} T \sigma_i$. So, $\alpha_{i,0}^{\sigma} - \alpha_{i,0} \equiv 0 \pmod{\mathfrak{P}^{\sigma_i}}$ can not hold by the assumption. Hence, (6) can not hold.

Assume next $\sigma \notin \sigma_i^{-1} Z \sigma_i$. Then, $\mathfrak{P}^{\sigma_i \sigma} = \mathfrak{P}^{\sigma_j \eta}$ with some σ_j and $\eta \in H$. In this case, $\pi_i^{\sigma} - \pi_j^{\eta} \equiv 0 \pmod{\mathfrak{P}^{\sigma_j \eta}}$, and $\sigma' = \sigma \eta^{-1} \in \sigma_i^{-1} Z \sigma_j$, $(\sigma \eta^{-1} \neq 1)$. Accordingly, $\pi_i^{\sigma'} - \pi_j \equiv 0 \pmod{\mathfrak{P}^{\sigma_j}}$, and therefore (6) would imply $\alpha_{i,0}^{\sigma'} - \alpha_{j,0} \equiv 0 \pmod{\mathfrak{P}^{\sigma_j}}$. But, this is impossible by the definition of the weak conjugation and by the assumption of the proposition. (q.e.d.)

The converse statement of Prop. 7 is also valid. For the sake of convenience, we state it separately.

PROPOSITION 8. *Notation being as in Prop.* 7, *assume either that*

a′) $\alpha_{i,0} \bmod \mathfrak{q}_i$ *does not belongs to* $C(\mathfrak{q}_i)$,

or

b′) $\alpha_{i,0} \bmod \mathfrak{q}_i$ *and* $\alpha_{j,0} \bmod \mathfrak{q}_j$, $(i \neq j)$, *are weakly conjugate. Then,* (6) *holds with some* $\sigma \in \sigma_i^{-1} Z \sigma_j$, *and, if* a′) *is the cases, with* $i = j$ *and* $\sigma \notin H \cdot \sigma_i^{-1} T \sigma_i$.

PROOF. The first part of the proposition concerning a′) is, as the corresponding part of Prop. 7, a consequence of the fact that σ induces a non-trivial autmorphism of $K(\mathfrak{q}_i)$.

To prove the second, it is enough to recall that $\alpha_{i,0}^{\sigma} \equiv \alpha_{j,0} \pmod{\mathfrak{q}_j}$, $(\sigma \in \sigma_i^{-1} Z \sigma_j)$, is the definition of the weak conjugation. (q.e.d.)

§5. Main Theorem

Using the terminology "*component of indices*" introduced in prior to Prop. 5, our main theorem is stated as follows:

THEOREM. *Let F be an algebraic number field of a finite degree, and K an extension over F of a finite degree n. Let $\mathfrak{p}$ be a prime ideal of F, and let $d(K/F)$ be the discriminant of K/F. Denote on the other hand by $\delta(K/F)$ the greatest common divisor of discriminants of integers of K with respect to K/F. Then, $\mathfrak{p}$ divides $\delta(K/F)d(K/F)^{-1}$ if and only if $c(I) < f_I g_I$, or equivalentry*

$$\frac{1}{f_I}\sum_{d|f_I}\mu\left(\frac{f_I}{d}\right)(N\mathfrak{p})^d < g_I,$$

is the case for at least one component I of indices, where μ is the Möbius' function.

PROOF. Notation being as in §4, we investigate an integer α in $\mathfrak{o}_K$ together with a system $\alpha_1, \alpha_2, \ldots, \alpha_g$ of local integers in $\mathfrak{o}_{(i),0}$ satisfying

$$\alpha \equiv \alpha_i \pmod{\mathfrak{q}_i^{e_i(N+1)}}, \quad (i = 1, 2, \ldots, g), \tag{7}$$

where N is the $\mathfrak{p}$-exponent of $d(K/F)$.

Assume first the inequality $c(I) \geq f_I g_I$ holds for every components I of indices. Then, by Prop. 5, we can choose $\alpha_{i,0} \in \mathfrak{o}_{(i),0}$ such that $\alpha_i \bmod \mathfrak{q}_i$ belongs to $C(\mathfrak{q}_i)$ and such that $\alpha_{i,0} \bmod \mathfrak{q}_i$ and $\alpha_{j,0} \bmod \mathfrak{q}_j$ are not weakly conjugate as far as i and j belong to the same I. If here i and j belong to different components of indices, then $\alpha_{i,0} \bmod \mathfrak{q}_i$ and $\alpha_{j,0} \bmod \mathfrak{q}_j$ cannot be weakly conjugate because the field generated by them have different degree over $K(\mathfrak{p})$.

Let π_i be, as in Prop. 7, a prime element of $\mathfrak{q}_i$. Put

$$\alpha_i = \alpha_{i,0} + \pi_i,$$

and let α be as in (7). Then, Prop. 6 implies that the $\mathfrak{q}_i$-exponent of

$$\prod_\sigma(\alpha - \alpha^\sigma), \quad \sigma \in H\backslash H \cdot \sigma_i^{-1} Z \sigma_i,$$

is equal to the $\mathfrak{q}_i$-exponent of $\mathfrak{D}(K/F)$, and Prop. 7 implies that $\prod_\sigma(\alpha - \alpha^\sigma)$, $(\sigma \in H\backslash G)$, is prime to $\mathfrak{p}$ whenever $\sigma \notin \bigcup_i H \cdot \sigma_i^{-1} T \sigma_i$. Therefore, the $\mathfrak{q}_i$-exponent of $\mathfrak{D}(\alpha, K/F)$ coincides with that of $\mathfrak{D}(K/F)$ for every i. Hence, the $\mathfrak{p}$-components of $d(\alpha, K/F)$ and $d(K/F)$ are same. From this follows that $\mathfrak{p}$ does not divide $\delta(K/F)$.

Assume conversely $c(I) < f_I g_I$ for some I, and denote in general by $\alpha_{i,0}$

an element of $\mathfrak{o}_{(i),0}$ and by π_i a prime element of $\mathfrak{q}_i$ in $\mathfrak{o}_{(i)}$. Since then $\sigma \in \sigma_i^{-1} Z \sigma_j$, $(i \neq j)$, does not belong to any $H \cdot \sigma_i^{-1} T \sigma_i$, Prop. 8 implies that there exists $\sigma \in G$ with $\sigma \notin H \cdot \sigma_i^{-1} T \sigma_i$ at least one i such that (6) holds under any choice of $\alpha_{i,0}$. This shows that the $\mathfrak{p}$-exponent of $d(\alpha, K/F)$ exceeds N as far as α is determined by (7) with $\alpha_i = \alpha_{i,0} + \pi_i$.

Thus, there remains only to observe the case where α_i is not of this form. This case occurs merely when $e_i > 1$ and $\alpha_i = \alpha_{i,0} + \rho_i$ with $\rho_i \equiv 0 \pmod{\mathfrak{q}_i^2}$. But, in this case, the $\mathfrak{q}_i$-exponent of

$$\prod_{\sigma}(\rho_i - \rho_i^{\sigma}), \quad \sigma \in \sigma_i^{-1} T \sigma_i \cap H \backslash \sigma_i^{-1} T \sigma_i,$$

exceeds the $\mathfrak{q}_i$-exponent of $\mathfrak{D}(K/F)$ due to Prop. 6. Consequently, the $\mathfrak{p}$-exponent of $d(\alpha, K/F)$ exceeds N. Hence, $\mathfrak{p}$ divides $\delta(K/F)$ whenever $c(I) < f_I g_I$.

(q.e.d.)

REMARK 1. The statement of the theorem does not concern the ramification.

REMARK 2. The arguments in the present paper are based upon the idea announced in [3] in a very special case.

Acknowledgement

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

References

[1] R. Dedekind, Über den Zusammenhang zwischen 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] S. Oka, On the unramified common divisor of discriminants of integers in a normal extension, Nagoya Math. J., 160, 2000.
[4] E. Weiss, Algebraic number theory, AcGraw-Hill, 1963.

Department of Mathematics
Meijo University
Shiogamaguchi 1-501, Tenpakuku
Nagoya, 468-8502, Japan