A COHOMOLOGICAL INVESTIGATION OF THE DISCRIMINANT OF A NORMAL ALGEBRAIC NUMBER FIELD

HIDEO YOKOI

Dedicated to the memory of Professor TADASI NAKAYAMA

1. Let F be an algebraic number field of finite degree, and let K/F be a normal extension of degree n. Denote by O_K the ring of all integers in K. In [1][1] we proved the following:

THEOREM 1. *The relative traces of all integers of K to F constitute an integral ideal $\mathfrak{a}$ of F and the ideal $\mathfrak{a}$ is characterized as the smallest ideal of F dividing the relative different $\mathfrak{D}_{K/F}$.*

In other words,

THEOREM 1'. *The 0-dimensional Galois cohomology group of O_K with respect to K/F is trivial if and only if K/F is tamely ramified at every prime ideal of F*[2].

Moreover we obtained there the following:

THEOREM 2. *If K/F is tamely ramified at every prime ideal of F, then the Galois cohomology group of O_K with respect to K/M is trivial for every dimension and for any intermediate field M of K/F*[3].

Namely, so far as we consider only the ring of all integers in an algebraic number field, the Galois cohomology group is trivial for every dimension whenever the normal extension is tamely ramified at every prime ideal. Therefore, we now consider more generally ambiguous ideals[4] instead of the ring of all integers in a normal extension field, and generalizing the theorem 1 we chara-

Received May 24, 1965.

1) Cf. [1] p. 83, Theorem 1.

2) Cf. [1] p. 86, Corollary 1.

3) Cf. [1] p. 86, Corollary 1, Corollary 2, [2] and [3].

4) This means ideals invariant under the operator of the Galois group.

cterize the discriminant (different) of the normal extension field by the 0-dimensional Galois cohomology groups of ambiguous ideals.

2. Let $\mathfrak{P}$ be any prime ideal of K and $\mathfrak{p}$ be the prime ideal of F contained in $\mathfrak{P}$. Denote by $K_{\mathfrak{P}}$ and $F_{\mathfrak{p}}$ the $\mathfrak{P}$-adic completion of K and the $\mathfrak{p}$-adic completion of F respectively. The following proposition is a generalization of Lemma 2 in [1].

PROPOSITION 1. *Let $e \geqq 1$ be the ramification order of $\mathfrak{P}$ with respect to $K_{\mathfrak{P}}/F_{\mathfrak{p}}$, and represent the relative different $\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$ of $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ in the form*

$$\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}}) = \mathfrak{P}^{er+s} = \mathfrak{p}^r\mathfrak{P}^s \qquad (r \geqq 0,\ 0 \leqq s < e).$$

Then we have

$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s+1} = \cdots = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{0} = \cdots = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s-1} = \mathfrak{p}^r,$$

$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s+1} = \cdots = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e} = \cdots = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{2e-s-1} = \mathfrak{p}^{r+1}, \text{ etc.},$$

where $tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{\lambda}$ means for every rational integer λ the image of $\mathfrak{P}^{\lambda}$ by the trace mapping from $K_{\mathfrak{P}}$ to $F_{\mathfrak{p}}$.

Proof. Since it is clear that

$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s} \supseteqq tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s+1} \supseteqq \cdots \supseteqq tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s-1},$$
$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s} \supseteqq tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s+1} \supseteqq \cdots \supseteqq tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{2e-s-1}, \text{ etc.}$$

hold and the elements in $tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{\lambda}$ constitute an ideal of $F_{\mathfrak{p}}$ for every rational integer λ, it will be enough to prove the following relations:

(1) $tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s} \subseteqq \mathfrak{p}^r$, $\quad tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s} \subseteqq \mathfrak{p}^{r+1}$, ...

(2) $tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s-1} \nsubseteqq \mathfrak{p}^{r+1}$, $\quad tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{2e-s-1} \nsubseteqq \mathfrak{p}^{r+2}$, ...

However, the relative different $\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$ of $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is characterized as the highest power of $\mathfrak{P}$ such that $tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\alpha \equiv 0 \bmod \mathfrak{p}^n$ holds for any fixed natural number n and for every number α in $K_{\mathfrak{P}}$ with $\alpha \equiv 0 \bmod \mathfrak{p}^n/\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$[5]. Here, if we consider the cases of $n = r, r+1, \ldots$, then we have at once

$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{-s} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{p}^r/\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}}) \subseteqq \mathfrak{p}^r,$$
$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{p}^{r+1}/\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}}) \subseteqq \mathfrak{p}^{r+1}, \text{ etc.}$$

[5] Cf. [1] p. 84, Lemma 1.

Hence (1) is proved. Moreover, from the above characterization of the relative different $\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}})$ for the cases of $n=r+1, r+2, \cdots$, it follows

$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{e-s-1} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{p}^{r+1}/\mathfrak{P}\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}}) \subsetneqq \mathfrak{p}^{r+1},$$
$$tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{P}^{2e-s-1} = tr(K_{\mathfrak{P}}/F_{\mathfrak{p}})\mathfrak{p}^{r+2}/\mathfrak{P}\mathfrak{D}(K_{\mathfrak{P}}/F_{\mathfrak{p}}) \subsetneqq \mathfrak{p}^{r+2}, \text{ etc.}$$

These are the same relations as in (2).

We denote by $[\mathfrak{D}_{K/F}]_{\mathfrak{P}_i}$ and $[\mathfrak{D}_{K/F}]_{\mathfrak{p}}$ the $\mathfrak{P}_i$-component and the $\mathfrak{p}$-component of the relative different $\mathfrak{D}_{K/F}$ respectively. Then the following proposition is a generalization of theorem 1.

PROPOSITION 2. *Let* $\mathfrak{p}=(\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$ *be the decomposition of a prime ideal* $\mathfrak{p}$ *of* F *into powers of distinct prime ideals of* K, *and put* $[\mathfrak{D}_{K/F}]_{\mathfrak{P}_i}=\mathfrak{P}_i^{er+s}$; $r\geqq 0$, $0\leqq s<e$, $i=1, 2, \cdots, g$. *Then we have*

(1) $$\mathfrak{p}^r // tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^o, \cdots, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1}$$

i.e. $tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^o, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i), \cdots, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1} \subseteqq \mathfrak{p}^r$, *but* $\subsetneqq \mathfrak{p}^{r+1}$,

(2) $$\mathfrak{p}^{r+1} // tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s}, \cdots, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{2e-s-1}$$

i.e. $tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s}, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s+1}, \cdots, tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{2e-s-1} \subseteqq \mathfrak{p}^{r+1}$, *but* $\subsetneqq \mathfrak{p}^{r+2}$

Proof. From the product theorem of different and proposition 1, it follows that $tr(K_{\mathfrak{P}_i}/F_{\mathfrak{p}})\alpha \equiv 0 \bmod \mathfrak{p}^r$ for every $i=1, 2, \cdots, g$ and for any α in $(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1}$, and hence for any α in $(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1}$ we obtain the following congruence:

$$tr(K/F)\alpha = \sum_{i=1}^{g} tr(K_{\mathfrak{P}_i}/F_{\mathfrak{p}})\alpha \equiv 0 \bmod \mathfrak{p}^r.$$

On the other hand, by proposition 1 there exists β in $\mathfrak{P}_1^{e-s-1}$ such that $tr(K_{\mathfrak{P}_1}/F_{\mathfrak{p}})\beta \not\equiv 0 \bmod \mathfrak{p}^{r+1}$, and by the strong approximation theorem there exists γ in O_K such that $\gamma \equiv \beta \bmod \mathfrak{P}_1^{e-s}$, $\gamma \equiv 0 \bmod \mathfrak{P}_j^{e-s}$ $(j=2, 3, \ldots, g)$, that is,

$$tr(K_{\mathfrak{P}_1}/F_{\mathfrak{p}})\gamma \equiv tr(K_{\mathfrak{P}_1}/F_{\mathfrak{p}})\beta \bmod \mathfrak{p}^{r+1},$$
$$tr(K_{\mathfrak{P}_j}/F_{\mathfrak{p}})\gamma \equiv 0 \bmod \mathfrak{p}^{r+1} \qquad (j=2, \ldots, g).$$

Consequently γ belongs to $(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1}$ and

$$tr(K/F)\gamma = \sum_{i=1}^{g} tr(K_{\mathfrak{P}_i}/F_{\mathfrak{p}})\gamma \not\equiv 0 \mod \mathfrak{p}^{r+1}.$$

This fact means $tr(K/F)(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-s-1} \not\equiv \mathfrak{p}^{r+1}$, and the rest of this proposition 2 can be proved similarly.

THEOREM 3. *Let F be an algebraic number field of finite degree and let K/F be a normal extension of degree n. For any prime ideal $\mathfrak{p}$ in F we denote by $\mathfrak{a}_{\mathfrak{p}} = \prod_{i=1}^{g}\mathfrak{P}_i$ the ambiguous ideal in K which is the product of all distinct prime divisors $\mathfrak{P}_i$ of $\mathfrak{p}$ in K. If we assume $\mathfrak{p}^k // tr(K/F)\mathfrak{a}_{\mathfrak{p}}^o$, $tr(K/F)\mathfrak{a}_{\mathfrak{p}}$, $\cdots$, $tr(K/F)\mathfrak{a}_{\mathfrak{p}}^{t-1}$ and $tr(K/F)\mathfrak{a}_{\mathfrak{p}}^t \subseteq \mathfrak{p}^{k+1}$, then $k \geqq 0$, $1 \leqq t \leqq e$, $\mathfrak{p}^{k+1} // tr(K/F)\mathfrak{a}_{\mathfrak{p}}^t$ and the $\mathfrak{p}$-component of the relative different $\mathfrak{D}_{K/F}$ of K/F may be represented in the following form:*

$$[\mathfrak{D}_{K/F}]_{\mathfrak{p}} = \mathfrak{p}^{k+1}/\mathfrak{a}_{\mathfrak{p}}^t = \mathfrak{p}^k(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-t},$$

where e is the ramification order of $\mathfrak{p}$ in K/F, namely, $\mathfrak{p} = (\prod_{i=1}^{g}\mathfrak{P}_i)^e$.

Proof. From the assumption and proposition 2, it follows immediately $k = r$, $t = e - s$ and hence $k \geqq 0$, $1 \leqq t \leqq e$, $\mathfrak{p}^{k+1} // tr(K/F)\mathfrak{a}_{\mathfrak{p}}^t$. Consequently, for the $\mathfrak{p}$-component $[\mathfrak{D}_{K/F}]_{\mathfrak{p}}$ of the relative different $\mathfrak{D}_{K/F}$ of K/F we have

$$[\mathfrak{D}_{K/F}]_{\mathfrak{p}} = \mathfrak{p}^r(\prod_{i=1}^{g}\mathfrak{P}_i)^s = \mathfrak{p}^k(\prod_{i=1}^{g}\mathfrak{P}_i)^{e-t} = \mathfrak{p}^{k+1}/\mathfrak{a}_{\mathfrak{p}}^t.$$

THEOREM 4. *Let K be a normal extension field of degree n of the rational number field $\mathbf{Q}$, and let $G = G(K/\mathbf{Q})$ be the Galois group of $K/\mathbf{Q}$. For any rational prime p, we denote by $\mathfrak{a}_{\mathfrak{p}} = \prod_{i=1}^{g}\mathfrak{P}_i$ the ambiguous ideal in K which is the product of all distinct prime divisors $\mathfrak{P}_i$ of p in K, and we denote by $H^o(G, \mathfrak{a}_p^\lambda)$ and $[H^o(G, \mathfrak{a}_p^\lambda)]_p$ the 0-dimensional Galois cohomology group of the ambiguous ideal $\mathfrak{a}_p^\lambda$ and the p-component of the order of the group $H^o(G, \mathfrak{a}_p^\lambda)$ respectively.*

If we assume that

$$[H^o(G, \mathfrak{a}_p)]_p = [H^o(G, \mathfrak{a}_p^2)]_p = \cdots = [H^o(G, \mathfrak{a}_p^{t-1})]_p < [H^o(G, \mathfrak{a}_p^o)]_p$$

and

$$[H^o(G, \mathfrak{a}_p^t)]_p \geqq [H^o(G, \mathfrak{a}_p^o)]_p = p^k,$$

then we have $k \geqq 0$, $1 \leqq t \leqq e$, $[H^o(G, \mathfrak{a}_p)]_p = [H^o(G, \mathfrak{a}_p^2)]_p = \cdots = [H^o(G, \mathfrak{a}_p^{t-1})]_p = p^{k-1}$, $[H^o(G, \mathfrak{a}_p^t)]_p = [H^o(G, \mathfrak{a}_p^o)]_p = p^k$ and the p-component $[D_K]_p$ of the discriminant D_K of K may be represented in the following form:

$$[D_K]_p = p^{n(k+1-t/e)},$$

where e is the ramification order of p with respect to $K/\mathbf{Q}$, namely, $p = \mathfrak{a}_p^e$.

Proof. We denote by $(\mathfrak{a}_p^\lambda)^G$ the G-invariant maximal submodule of G-module $\mathfrak{a}_p^\lambda$. Then for every $\lambda = 1, 2, \cdots, e$ we can easily verify that $(\mathfrak{a}_p^\lambda)^G$ is equal to the integral principal ideal (p) of $\mathbf{Q}$ and $(\mathfrak{a}_p^0)^G$ is equal to the ring of all rational integers, and hence from proposition 2 it follows at once

$$[H^0(G, \mathfrak{a}_p^0)]_p = p^r,\ [H^0(G, \mathfrak{a}_p)]_p = [H^0(G, \mathfrak{a}_p^2)]_p = \cdots = [H^0(G, \mathfrak{a}_p^{e-s-1})]_p = p^{r-1}$$

and $[H^0(G, \mathfrak{a}_p^{e-s})]_p = p^r$. Therefore, by assumption of this theorem 4 we obtain at once $k = r$, $e - s = t$ and so $k \geqq 0$, $1 \leqq t \leqq e$, $[H^0(G, \mathfrak{a}_p)]_p = \cdots = [H^0(G, \mathfrak{a}_p^{t-1})]_p = p^{r-1} = p^{k-1}$, $[H^0(G, \mathfrak{a}_p^t)]_p = p^r = p^k$. Moreover, for the discriminant D_K of K we obtain by theorem 3

$$[D_K]_p = N_K[\mathfrak{D}_{K/\mathbf{Q}}]_p = p^{nk+(e-t)n/e} = p^{n(k+1-t/e)}.$$

This concludes the proof.

References

[1] H. Yokoi, On the ring of integers in an algebraic number field as a representation module of Galois group, Nagoya Math. J. **16** (1960), 83-90.

[2] H. Yokoi, On the Galois cohomology group of the ring of integers in an algebraic number field, Acta Arithmetica **8** (1963), 243-250.

[3] H. Yokoi, A note on the Galois cohomology group of the ring of integers in an algebraic number field, Proc. Japan Akad. **40** (1964), 245-246.

Mathematical Institute
Nagoya University