TOKYO J. MATH.
VOL. 6, NO. 2, 1983

On the Genus Field in Algebraic Number Fields

Mitsuko HORIE

Tokyo Metropolitan University

Introduction

In 1951, Hasse [7] started from the principal genus theorem of Gauss and gave a class field-theoretic interpretation of the genus theory of quadratic number fields. Subsequently, Leopoldt [11] extended the theory to abelian fields, and Fröhlich [1] generalized it to arbitrary number fields. In his paper [11], Leopoldt studied the "Auflösung" of groups of numerical characters and gave an ideal-theoretic characterization of genus fields and a genus number formula of abelian fields. By origin, the principal genus in the Gauss' classical theory is defined as the kernel of numerical characters which are called the genus characters. Hasse [9] asserted that Leopoldt's characterization of genus fields of abelian fields can restated as the following: the principal genus of an abelian field is the kernel of norm residue symbols. And recently, Gold [3] showed that the principal genus in the wide sense of a relative Galois extension is also characterized as the kernel of norm residue symbols. On the other hand, Furuta [2], using idele, obtained a genus number formula in the wide sense of relative Galois extensions. The genera that the above authors except Furuta and Gold treated in their papers were in the narrow sense.

The genus field, the genus number and the principal genus are defined as follows.

DEFINITION. Let K/k be an arbitrary extension of finite algebraic number fields. The narrow (wide) genus field K^* of K/k is the maximal extension of K, which satisfies the following conditions:

(i) K^* is a composite of K and an abelian extension of k,

(ii) no finite (and no infinite) prime in K ramifies in K^*/K.

The genus number of K/k is the degree $[K^*: K]$. Clearly, the genus field K^* is a class field over K, and we call the ideal group of K corresponding to K^* the principal genus.

Received November 18, 1982

In 1971, Goldstein gave in [4] a genus number formula of relative abelian extensions by using a method similar to Furuta [2]. Recently, Gurak [5] extended an analogy of Leopoldt's theory and showed that the principal genus in the narrow sense of a relative abelian or Galois extension is characterized by norm residue symbols, and obtained a genus number formula.

In the works mentioned above, the authors always drew a line between the two senses, i.e., the narrow and the wide ones. We show in the present paper that such distinction is not essential. For that purpose, we use the generalized notation of genus fields as follows.

DEFINITION. Let K/k be an arbitrary extension of finite algebraic number fields, $\mathfrak{M}$ an integral divisor of K and $K(\mathfrak{M})$ the ray class field of K mod $\mathfrak{M}$. Let E be the maximal abelian subextension of $K(\mathfrak{M})/k$. Set

$$K^*(\mathfrak{M})=KE\,,$$

$$g_{K/k}(\mathfrak{M})=[K^*(\mathfrak{M}):K]\,.$$

We call $K^*(\mathfrak{M})$ the genus field and $g_{K/k}(\mathfrak{M})$ the genus number of K/k mod $\mathfrak{M}$. The principal genus is the ideal group of K corresponding to $K^*(\mathfrak{M})$.

In this definition, if $\mathfrak{M}$ is the integer ring of K (the product of all the infinite primes of K respectively), then we have the wide (resp. the narrow) genus fields. An idele-theoretic investigation of the above genus fields was already made by Furuta and he obtained genus number formulas (cf. Remark 2). But his results are yet unpublished. In the present paper, we make a further study of the genus fields using ideal-theoretic methods. Our purpose in this paper is to generalize Leopoldt-Gurak theory to the genus field of a relative extension with modulus. Especially, we give a generalization of "Auflösung" in Leopoldt's paper [11] and construct an abelian extension $K^{**}(\mathfrak{m})$ over K attached to an integral divisor $\mathfrak{m}$ of k (see §3). By comparing the genus field $K^*(\mathfrak{M})$ with $K^{**}(\mathfrak{m})$, we can see that for any given abelian extension K/k and for any integral divisor $\mathfrak{M}$ of K, there exists an integral divisor $\mathfrak{m}$ of k such that $K^*(\mathfrak{M})=K^{**}(\mathfrak{m})$, i.e., the principal genus of a relative abelian extension K/k with modulus can be completely characterized by norm residue symbols and an integral divisor of k (Theorem 2 and its corollary). In §1, we study groups of numerical characters of a finite algebraic number field, in §2, we are concerned with two special numerical character groups related to the genus fields, in §3, we in-

troduce another generalization of genus fields determined by "Auflösung" and in final section §4, we will compare $K^*(\mathfrak{M})$ with $K^{**}(\mathfrak{m})$ and prove Theorem 2 and its corollary.

I express my hearty gratitude to Prof. Y. Furuta for giving me the chance to read his notes on nilpotent extensions, and to Prof. M. Ishida for his valuable suggestions. My gratitude also extends to Prof. T. Hayashida, Prof. G. Fujisaki, Prof. M. Fujiwara and Prof. H. Miki for their warm encouragements.

We use the following notations in this paper.

k, K and L: finite algebraic number fields.

$\mathfrak{p}$, $\mathfrak{P}$ and $\mathfrak{P}_L$: prime of k, K and L respectively such that $\mathfrak{P}$ and $\mathfrak{P}_L$ divide $\mathfrak{p}$.

$L_{\mathfrak{P}_L}$ (or simply $\bar{L}$ when the prime $\mathfrak{P}_L$ is fixed): the completion of L at $\mathfrak{P}_L$.

M (resp. $M_{\mathfrak{P}}$ or simply $\bar{M}$): the maximal abelian subextension of K/k (resp. $K_{\mathfrak{P}}/k_{\mathfrak{p}}$).

$G(K/k)$ (resp. $G(\bar{K}/\bar{k})$): the Galois group of K/k (resp. $\bar{K}/\bar{k}$) when the extension is Galois.

$\hat{G}(K/k)$ (resp. $\hat{G}(\bar{K}/\bar{k})$): the character group of $G(K/k)$ (resp. $G(\bar{K}/\bar{k})$) when the extension is abelian.

$\mathfrak{f}(K/k)$ (resp. $\mathfrak{f}(\bar{K}/\bar{k})$): the conductor of an abelian extension K/k (resp. $\bar{K}/\bar{k}$).

$\mathfrak{O}_k$: the integer ring of k.

U_k: the unit group of k.

$k^{\mathfrak{m}}=\{\alpha \in k^{\times}: \alpha \equiv 1 (\mathrm{mod}\ \mathfrak{m})\}$ for an integral divisor $\mathfrak{m}$ of k.

$A^{\mathfrak{m}}=\{\alpha \in A: \alpha \equiv 1 (\mathrm{mod}\ \mathfrak{m})\}$ for a subset A of k.

$(A)_{\mathfrak{f}}$: the elements of A which are relatively prime to an integral divisor $\mathfrak{f}$ of k, where A is a subset of k.

P_L: for fixed k, a full representative set of the primes of k, consisting of primes of L such that for any prime $\mathfrak{p}$ of k there is a unique prime $\mathfrak{P}$ in P_L dividing $\mathfrak{p}$.

We call P_L (or simply P when there is no confusion) a P-set of L.

I_k: the group of all the fractional ideals of k.

$H(L/K)$: the ideal group of K corresponding to an abelian extension L/K.

$i(\alpha)=(\alpha)$: the principal ideal of k generated by an element α of k.

$S_k(\mathfrak{m})=i(k^{\mathfrak{m}})$: the ray mod $\mathfrak{m}$ of k.

$k(\mathfrak{m})$: the ray class field of k mod $\mathfrak{m}$.

$U_{\bar{k}}^{(i)}=\{\alpha \in \bar{k}: \alpha \equiv 1 (\mathrm{mod}\ \mathfrak{p}^i)\}$.

$V_{\bar{K}/\bar{k}}^{(i)}=\{\sigma \in G(\bar{K}/\bar{k}): \alpha^{\sigma} \equiv \alpha (\mathrm{mod}\ \mathfrak{P}^{i+1})$ for all $\alpha \in \bar{K}\}$: the i-th ramification

group of a Galois extension $\bar{K}/\bar{k}$.

$\psi_{\bar{K}/\bar{k}}(u)$: the Hasse's function for a Galois extension $\bar{K}/\bar{k}$ of non-archimedean local fields (see §2).

§1. Numerical characters of an algebraic number field.

Let $\mathfrak{f}$ be an integral divisor of k. A mapping $\chi: (k^\times)_\mathfrak{f} \to \boldsymbol{C}$ is called a numerical character of $k \bmod \mathfrak{f}$ when the following conditions are satisfied.

(i) $\chi(x) \neq 0$ for any x in $(k^\times)_\mathfrak{f}$,

(ii) if $x \equiv y (\bmod \mathfrak{f})$, then $\chi(x) = \chi(y)$,

(iii) $\chi(xy) = \chi(x)\chi(y)$.

Let χ be a numerical character of $k \bmod \mathfrak{f}$, then for any $\mathfrak{f}'$ which is divided by $\mathfrak{f}$, χ is also a numerical character $\bmod \mathfrak{f}'$. For any proper divisor $\mathfrak{f}_1$ of $\mathfrak{f}$, if there are x and y in $(k^\times)_\mathfrak{f}$ such that $x \equiv y (\bmod \mathfrak{f}_1)$ and $\chi(x) \neq \chi(y)$, then $\mathfrak{f}$ is called the conductor of χ and symbolized by $\mathfrak{f}(\chi)$. Let $\mathfrak{G}$ be an arbitrary group of numerical characters of $k \bmod \mathfrak{f}$. Put

$$\mathfrak{f}(\mathfrak{G}) = \text{l. c. m.}\{\mathfrak{f}(\chi): \chi \in \mathfrak{G}\} .$$

We call $\mathfrak{f}(\mathfrak{G})$ the conductor of $\mathfrak{G}$.

For a group $\mathfrak{G}$ of numerical characters of $k \bmod \mathfrak{f}$, set the restriction of $\mathfrak{G}$ to $k^\mathfrak{m}$

$$\mathfrak{G}_\mathfrak{m} = \{\chi|_{k^\mathfrak{m}}: \chi \in \mathfrak{G}\} ,$$

and set

$$a(\mathfrak{G}_\mathfrak{m}) = \{x \in (k^\mathfrak{m})_\mathfrak{f}: \chi(x) = 1 \quad \text{for all} \quad \chi \in \mathfrak{G}\} .$$

The restriction $\mathfrak{G}_\mathfrak{m}$ of a numerical character group $\mathfrak{G} \bmod \mathfrak{f}$ can be regarded as a character group of $\overline{\mathfrak{D}_k^\mathfrak{m}}$, where the notation $\overline{\mathfrak{D}_k^\mathfrak{m}}$ stands for the subgroup of $(\mathfrak{D}_k/\mathfrak{f})^\times$ which is generated by the classes represented by the elements of $\mathfrak{D}_k^\mathfrak{m}$. By the duality, there is an inverting correspondence between the subgroups of $\overline{\mathfrak{D}_k^\mathfrak{m}}$ and $\mathfrak{G}_\mathfrak{m}$'s, and the correspondence is given by

$$\mathfrak{G}_\mathfrak{m} \longleftrightarrow \overline{a(\mathfrak{G}_\mathfrak{m})} ,$$

where $\overline{a(\mathfrak{G}_\mathfrak{m})}$ is the classes of $\overline{\mathfrak{D}_k^\mathfrak{m}}$ represented by the elements of $a(\mathfrak{G}_\mathfrak{m})$.

Lemma 1 below is elementary.

LEMMA 1. *Let $\mathfrak{G}$ and $\mathfrak{G}'$ be groups of numerical characters of k.*

Put $\mathfrak{f}=\mathfrak{f}(\mathfrak{S}), \mathfrak{f}'=\mathfrak{f}(\mathfrak{S}')$. *If* $\mathfrak{S}_{\mathfrak{m}}\supset\mathfrak{S}'_{\mathfrak{m}}$ *on* $(k^{\mathfrak{m}})_{\mathfrak{ff}'}$, *then* $\mathfrak{f}'$ *divides* l. c. m.$(\mathfrak{f}, \mathfrak{m})$. *Therefore, in that case,*

$$\mathfrak{S}_{\mathfrak{m}}\supset\mathfrak{S}'_{\mathfrak{m}} \quad on \quad (k^{\mathfrak{m}})_{\mathfrak{f}} .$$

PROOF. Put

$$\mathfrak{n}=\text{l. c. m.}(\mathfrak{f}, \mathfrak{m})=\prod_{\mathfrak{p}}\mathfrak{p}^{s_{\mathfrak{p}}},$$

$$\mathfrak{f}'=\prod_{\mathfrak{p}}\mathfrak{p}^{t_{\mathfrak{p}}} .$$

Suppose that there is a prime $\mathfrak{p}$ such that $s_{\mathfrak{p}}<t_{\mathfrak{p}}$. Then, by the definition of the conductor of numerical character groups, we can take a character χ in $\mathfrak{S}'$ and an element α of $(k^{\times})_{\mathfrak{f}'}$ such that

$$\alpha\equiv 1(\text{mod g. c. d.}(\mathfrak{f}', \mathfrak{n})) , \tag{1}$$

$$\chi(\alpha)\neq 1 . \tag{2}$$

From the congruence (1), it follows that there is an element β in $k^{\times}$ such that

$$\beta\equiv\alpha \ (\text{mod}\ \mathfrak{f}') , \tag{3}$$

$$\beta\equiv 1 \ (\text{mod}\ \mathfrak{n}) . \tag{4}$$

Clearly, β is in $(k^{\mathfrak{m}})_{\mathfrak{ff}'}$. Therefore, the congruence (4) and the assumption of the lemma imply $\chi(\beta)=1$. From (2) and (3), it follows that $\chi(\beta)\neq 1$. It is a contradiction. Thus we have $s_{\mathfrak{p}}\geqq t_{\mathfrak{p}}$. And the lemma was proved.

In the next section, we will be concerned with two special numerical character groups of k related to the genus fields.

§ 2. The groups $\mathfrak{S}(K)_{\mathfrak{m}}$ and $\mathfrak{S}^*(K; P_K)_{\mathfrak{m}}$.

In this section, we will give a generalization of "Auflösung" in Leopoldt's paper [11]. We start from the definition of the group $\mathfrak{S}(K)$.

For an arbitrary finite extension K of a fixed finite algebraic number field k, we define the subgroup $\mathfrak{S}(K)$ of the group of all the numerical characters of k mod $\mathfrak{f}(M/k)$. Put

$$\mathfrak{S}(K)=\left\{\chi: \chi(x)=\overline{\chi}\left(\frac{M/k}{(x)}\right) \quad \text{for some} \quad \overline{\chi}\in\hat{G}(M/k)\right\} ,$$

where $((M/k)/\mathfrak{a})$ is the Artin symbol of the maximal abelian subextension M/k of K/k. The group $\mathfrak{S}(K)$ is defined on $(k^{\times})_{\mathfrak{f}(M/k)}$. We see $\mathfrak{f}(\mathfrak{S}(K))=$

$\mathfrak{f}(K/k)$. Moreover, for the character group $\mathfrak{G}(K)_{\mathfrak{m}}$, the following Lemma 2 holds.

LEMMA 2. *Let M be the maximal abelian subextension of K/k. Then*

$$\mathfrak{G}(K)_{\mathfrak{m}} \cong G(M/k(\mathfrak{m}) \cap M) .$$

PROOF. This lemma can be proved similarly to (i) of Proposition of Gurak [5].

Now, to generalize "Auflösung", we introduce the following notations.

$$\mathfrak{f}(K/k; P_K) = \prod_{\mathfrak{P} \in P_K} f(M_{\mathfrak{P}}/k_{\mathfrak{p}}) .$$

We call it the locally abelian conductor of K/k at P_K, where P_K is a P-set of K. The subgroup $\mathfrak{G}^{\mathfrak{P}}(K)$ (resp. $\mathfrak{G}^*(K; P_K)$) of the group of all the numerical characters of $k \bmod \mathfrak{f}(M_{\mathfrak{P}}/k_{\mathfrak{p}})$ (resp. $\bmod \mathfrak{f}(K/k; P_K)$) is as follows.

$$\mathfrak{G}^{\mathfrak{P}}(K) = \left\{ \chi : \chi(x) = \bar{\chi}\left(\frac{x, M_{\mathfrak{P}}/k_{\mathfrak{p}}}{\mathfrak{p}}\right) \text{ for some } \bar{\chi} \in \hat{G}(M_{\mathfrak{P}}/k_{\mathfrak{p}}) \text{ on } (k^{\times})_{\mathfrak{p}} \right\} .$$

$$\mathfrak{G}^*(K; P_K) = \prod_{\mathfrak{P} \in P_K} \mathfrak{G}^{\mathfrak{P}}(K) \quad \text{(direct)} .$$

We can easily see that $\mathfrak{f}(K/k; P)$ is not depend on the choice of P in case K/k is a Galois extension. So we write $\mathfrak{G}^*(K) = \mathfrak{G}^*(K; P)$ when K/k is Galois.

The group $\mathfrak{G}^*(K; P)$ is defined on $(k^{\times})_{\mathfrak{f}(K/k;P)}$ and its conductor $\mathfrak{f}(\mathfrak{G}^*(K; P))$ is equal to the locally abelian conductor of K/k at P. The restriction $\mathfrak{G}^*(K; P)_{\mathfrak{m}}$ is a generalization of "Auflösung". Actually, if k is the rational number field, K is an abelian field and $\mathfrak{m}$ is the product of all the infinite primes of k, then $\mathfrak{G}^*(K; P)_{\mathfrak{m}}$ is "Auflösung" in [11]. We will show later in final section that, for any abelian extension K/k and for any integral divisor $\mathfrak{M}$ of K, there exists an integral divisor $\mathfrak{m}$ of k such that the genus field $K^*(\mathfrak{M})$ is characterlized by $\mathfrak{G}^*(K)_{\mathfrak{m}}$.

On the connection between groups $\mathfrak{G}(K)_{\mathfrak{m}}$ and extension K/k, Lemma 3 and Theorem 1 below are elementary and essential (cf. (ii) of Proposition and Theorem 3 in [5]).

LEMMA 3. *Let K_0 and L_0 be the maximal abelian subextensions of K/k and L/k respectively. If $k(\mathfrak{m})K_0 \supset L_0 \supset K_0$, then $\mathfrak{G}(K)_{\mathfrak{m}} = \mathfrak{G}(L)_{\mathfrak{m}}$ on $(k^{\mathfrak{m}})_{\mathfrak{f}(K_0/k)}$.*

PROOF. This lemma can also be proved similarly to Gurak's Pro-

position (ii) in [5].

THEOREM 1. *Let $\mathfrak{G}$ be a group of numerical characters* mod $\mathfrak{f}(\mathfrak{G})$ *of k, which is trivial on $U_k^{\mathfrak{m}}$. Then there is a unique abelian extension L of k such that $L \supset k(\mathfrak{m})$ and*

$$\mathfrak{G}(L)_{\mathfrak{m}} = \mathfrak{G}_{\mathfrak{m}} \quad on \quad (k^{\mathfrak{m}})_{\mathfrak{f}(\mathfrak{G})} .$$

Moreover, in that case, the ideal group of k corresponding to L is $i(a(\mathfrak{G}_{\mathfrak{m}}))$.

PROOF. This theorem is a generalization of Theorem 3 in [5]. Lemma 1 and an analogy of the proof of the theorem of Gurak prove the theorem.

In Lemmas 1, 2 and 3 and Theorem 1, if we replace $k^{\mathfrak{m}}$ by a subgroup A of $k^{\times}$ such that $i(A)$ is an ideal group of k and $k(\mathfrak{m})$ by the class field over k corresponding to $i(A)$, analogous results are obtained. The reason why we restrict our discussion to $A = k^{\mathfrak{m}}$ is the fact that there is a simple formula for the number of the elements of $\mathfrak{G}^*(K; P)_{\mathfrak{m}}$.

To make a simple description of the the number of elements of $\mathfrak{G}^*(K)_{\mathfrak{m}}$, we introduce the Hasse's function $\psi_{\bar{K}/\bar{k}}$ for a Galois extension $\bar{K}/\bar{k}$ of non-archimedean local fields.

Let $V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_r = 1$ be all the ramification groups of $\bar{K}/\bar{k}$ and $-1 = v_0 < v_1 < \cdots < v_r < \infty$ be all the ramification numbers i.e. v_{j+1} is the maximal exponent such that

$$\begin{aligned} V_j &= V_{\bar{K}/\bar{k}}^{(v_j+1)} = \cdots = V_{\bar{K}/\bar{k}}^{(v_j+1)} \\ &= \{\sigma \in G(\bar{K}/\bar{k}) : \alpha^{\sigma} \equiv \alpha \pmod{\mathfrak{P}^{v_j+1+1}} \quad \text{for all} \quad \alpha \in \bar{K}\} . \end{aligned}$$

We define v_{r+1} as ∞, and put

$$u_j = v_0 + \frac{n_0}{n_0}(v_1 - v_0) + \cdots + \frac{n_{j-1}}{n_0}(v_j - v_{j-1})$$

for $j = 0, 1, \cdots, r+1$, where $n_j = \# V_j$. The Hasse's function $\psi_{\bar{K}/\bar{k}}$ is defined as

$$\psi_{\bar{K}/\bar{k}}(u) = v_j + \frac{n_0}{n_j}(u - u_j) \quad \text{for} \quad u_j \leqq u < u_{j+1} .$$

The following propositions are known (see [8], [10] and [12]).

I. *The Hasse's function is strictly monotone increasing and if u is a rational integer, then $\psi_{\bar{K}/\bar{k}}(u)$ is also a rational integer. The inverse image $u_j = \psi_{\bar{K}/\bar{k}}^{-1}(v_j)$ of a ramification number v_j is not always a rational*

integer, but if $\bar{K}/\bar{k}$ is abelian, u_j is a rational integer for $j=0, 1, \cdots, r$.

II. *Let $\bar{K}/\bar{k}$ be abelian. If α runs through all the elements of $U_{\bar{k}}^{(u)}$ for an integer u such that $u_j<u\leqq u_{j+1}$, then*

$$\left(\frac{\alpha, \bar{K}/\bar{k}}{\mathfrak{p}}\right)$$

runs through all the elements of $V_j=V_{\bar{K}/\bar{k}}^{(v_j+1)}$.

LEMMA 4. *Let $\mathfrak{P}$ be a prime of K, $\mathfrak{p}$ the prime of k divided by $\mathfrak{P}$ and let $u_\mathfrak{p}$ be the $\mathfrak{p}$-exponent of an integral divisor $\mathfrak{m}$ of k. Then*

$$\#\mathfrak{G}^{\mathfrak{P}}(K)_{\mathfrak{m}}=\begin{cases}\#V_{\bar{M}/\bar{k}}^{(\psi_{\bar{M}/\bar{k}}(u_\mathfrak{p}))} & \text{if } \mathfrak{P} \text{ is finite}\\ 2 & \text{if } \mathfrak{P} \text{ is imaginary infinite and } \mathfrak{p}\nmid\mathfrak{m}\\ 1 & \text{otherwise,}\end{cases}$$

where $\bar{k}=k_\mathfrak{p}$ and $\bar{M}$ is the maximal abelian subextension of $\bar{K}/\bar{k}$.

PROOF. In case $\mathfrak{P}$ is infinite, $\mathfrak{P}$ is imaginary and $\mathfrak{p}$ is real. So the statement is obvious. Let $\mathfrak{P}$ be a finite prime. The mapping $\hat{G}(\bar{M}/\bar{k})\to\mathfrak{G}^{\mathfrak{P}}(K)_{\mathfrak{m}}: \bar{\chi}\mapsto\chi$ is a surjective homomorphism and $\bar{\chi}$ is in the kernel of the homomorphism if and only if

$$\bar{\chi}\left(\frac{U_{\bar{k}}^{(u_\mathfrak{p})}, \bar{M}/\bar{k}}{\mathfrak{p}}\right)=1.$$

From II, it follows that

$$\left(\frac{U_{\bar{k}}^{(u_\mathfrak{p})}, \bar{M}/\bar{k}}{\mathfrak{p}}\right)=V_{\bar{M}/\bar{k}}^{(\psi_{\bar{M}/\bar{k}}(u_\mathfrak{p}))}.$$

So the kernel of the homomorphism is $\hat{G}(\bar{M}^{(\psi_{\bar{M}/\bar{k}}(u_\mathfrak{p}))}/\bar{k})$, where $\bar{M}^{(i)}$ is the i-th ramification field of $\bar{M}/\bar{k}$. By the duality, we have Lemma 4.

REMARK 1. Let K/k be Galois. If $\mathfrak{m}$ is the product of all the infinite primes of k, then for any ramifying prime $\mathfrak{P}$,

$$\#\mathfrak{G}^{\mathfrak{P}}(K)_{\mathfrak{m}}=\begin{cases}\text{the ramification number of } \bar{M}/\bar{k} \text{ if } \mathfrak{P} \text{ is finite}\\ 1 \quad \text{if } \mathfrak{P} \text{ is infinite.}\end{cases}$$

If $\mathfrak{m}$ be the integer ring $\mathfrak{O}_k$ of k, then

$\#\mathfrak{G}^{\mathfrak{P}}(K)_{\mathfrak{m}}=$the ramification number of $M_\mathfrak{P}/k_\mathfrak{p}$ for all $\mathfrak{P}$.

§3. The field $K^{**}(P_K; \mathfrak{m})$.

We first, in this section, give a definition of ideal group $H(K; P_K; \mathfrak{m})$ and the field $K^{**}(P_K; \mathfrak{m})$.

DEFINITION. Let K be an arbitrary finite extension over k, $\mathfrak{m}$ an integral divisor of k and P_K a P-set of K. Let E^* be the class field over k corresponding to the ideal group $i(a(\mathfrak{S}^*(K; P_K)_\mathfrak{m}))$. The field $K^{**}(P_K: \mathfrak{m})$, the ideal group $H(K; P_K; \mathfrak{m})$ and the number $g'_{K/k}(P_K; \mathfrak{m})$ are defined as follows.

$$K^{**}(P_K; \mathfrak{m}) = KE^* ,$$

$$H(K; P_K; \mathfrak{m}) = H(K^{**}(P_K; \mathfrak{m})/K) ,$$

$$g'_{K/k}(P_K; \mathfrak{m}) = [K^{**}(P_K; \mathfrak{m}): K] .$$

In case K/k is Galois, we write $K^{**}(\mathfrak{m}) = K^{**}(P_K; \mathfrak{m})$, $H(K; \mathfrak{m}) = H(K; P_K; \mathfrak{m})$.

The above definition can be rewritten as follows. $H(K; P_K; \mathfrak{m})$ is the group of all the ideals $\mathfrak{A} \in I_K$ satisfying the following conditions:

(i) there is an element α in $k^\mathfrak{m}$ such that

$$N_{K/k}(\mathfrak{A}) = (\alpha) ,$$

(ii) there is a unit ε in $U_k^\mathfrak{m}$ such that

$$\left(\frac{\alpha, K_\mathfrak{P}/k_\mathfrak{p}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon, K_\mathfrak{P}/k_\mathfrak{p}}{\mathfrak{p}}\right) \quad \text{for all} \quad \mathfrak{P} \in P_K .$$

And $\mathfrak{S}(K^{**}(P_K; \mathfrak{m}))_\mathfrak{m}$ is the subgroup of $\mathfrak{S}^*(K; P_K)_\mathfrak{m}$ corresponding to the subgroup $\overline{a(\mathfrak{S}^*(K; P_K)_\mathfrak{m})U_k^\mathfrak{m}}$ of $\overline{\mathfrak{D}_k^\mathfrak{m}}$ represented by the elements of $a(\mathfrak{S}^*(K; P_K)_\mathfrak{m})U_k^\mathfrak{m}$.

The number $g'_{K/k}(P; \mathfrak{m}) = [K^{**}(P; \mathfrak{m}): K]$ can easily be computed.

PROPOSITION 1. *Let $u_\mathfrak{p}$ be the $\mathfrak{p}$-exponent of an integral divisor $\mathfrak{m}$ of k, $h_\mathfrak{m} = [k(\mathfrak{m}): k]$, and*

$$U_{K/k}^\mathfrak{m}(P) = \{\varepsilon \in U_k^\mathfrak{m}: \varepsilon \text{ is a norm from } K_\mathfrak{P} \text{ for all } \mathfrak{P} \in P\} ,$$

$$e'_\mathfrak{P} = \begin{cases} \#V_{\overline{M}/\overline{k}}^{(\psi_{\overline{M}/\overline{k}}(u_\mathfrak{p}))} & \text{if } \mathfrak{P} \text{ is finite} \\ 1 & \text{if } \mathfrak{P} \text{ is infinite and } \mathfrak{p}|\mathfrak{m} \\ 2 & \text{if } \mathfrak{P} \text{ is imaginary infinite } p \nmid \mathfrak{m} . \end{cases}$$

Then

$$g'_{K/k}(P; \mathfrak{m}) = \frac{h_\mathfrak{m} \prod_{\mathfrak{P} \in P} e'_\mathfrak{P}}{[M: k](U_k^\mathfrak{m}: U_{K/k}^\mathfrak{m}(P))} ,$$

where M is the maximal abelian subextension of K/k.

PROOF. From Lemma 2, it follows that

$$\mathfrak{G}(K^{**}(P;\mathfrak{m}))_{\mathfrak{m}} \cong G(M^*(P)/k(\mathfrak{m}) \cap M^*(P)) ,$$

where $M^*(P)$ is the maximal abelian subextension of $K^{**}(P;\mathfrak{m})/k$. Therefore, it follows that

$$\begin{aligned} g'_{K/k}(P;\mathfrak{m}) &= [K^{**}(P;\mathfrak{m}): K] \\ &= [M^*(P): M] \\ &= \frac{[M^*(P): k(\mathfrak{m})][k(\mathfrak{m}): k]}{[M: k]} \\ &= \frac{\#\mathfrak{G}(K^{**}(P;\mathfrak{m}))_{\mathfrak{m}} \cdot h_{\mathfrak{m}}}{[M: k]} . \end{aligned}$$

Since $\mathfrak{G}(K^{**}(P;\mathfrak{m}))_{\mathfrak{m}}$ is trivial on $U_k^{\mathfrak{m}}$, it follows that

$$\mathfrak{G}^*(K;P)_{\mathfrak{m}}/\mathfrak{G}(K^{**}(P;\mathfrak{m}))_{\mathfrak{m}} \cong U_k^{\mathfrak{m}}/U_{K/k}^{\mathfrak{m}}(P)$$

from the duality. Lemma 4 and the above prove the proposition.

The field $K^{**}(P;\mathfrak{m})$ is another generalization of the genus field K^* of K/k.

§4. The fields $K^*(\mathfrak{M})$ and $K^{**}(P_K;\mathfrak{m})$.

We consider the relation between $K^*(\mathfrak{M})$ and $K^{**}(P_K;\mathfrak{m})$. For that purpose, we introduce the notations $D_1(\mathfrak{M})$ and $D_2(\mathfrak{M})$ for a fixed integral divisor $\mathfrak{M}$ of K.

$D_1(\mathfrak{m})$: *the set of integral divisors $\mathfrak{m}$ of k such that if $\alpha \equiv 1 (\mathrm{mod}\, \mathfrak{M})$, then $N_{K/k}(\alpha) \equiv 1 \pmod{\mathfrak{m}}$.*

Let $\mathfrak{P}$ be a prime of K and $\mathfrak{p} = \mathfrak{P} \cap k$. Set $\bar{M}^*$ (resp. $\bar{M}$) the maximal abelian subextension of $\overline{K^*(\mathfrak{M})}/\bar{k}$ (resp. $\bar{K}/\bar{k}$), where $\bar{K} = K_{\mathfrak{P}}$, $\bar{k} = k_{\mathfrak{p}}$ and $\overline{K^*(\mathfrak{M})}$ is a localization of $K^*(\mathfrak{M})$ which contains $\bar{K}$. Moreover, let $u(\mathfrak{P})$ be the exponent of the conductor of $\bar{M}^*/\bar{M}$, and let $m(\mathfrak{P})$'s the rational numbers such that

$$u(\mathfrak{P}) - 1 < m(\mathfrak{P}) . \tag{5}$$

Since $K^*(\mathfrak{M})/K$ is abelian, the rational numbers $m(\mathfrak{P})$'s depend only on $\mathfrak{P}$. For $\mathfrak{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}}$, the notation of $D_2(\mathfrak{M})$ is as follows.

$D_2(\mathfrak{M})$: *the set of integral divisors $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ of k satisfying the*

following conditions:

(i) *if* $\mathfrak{p}$ *is infinite, then* $u_{\mathfrak{p}}=m_{\mathfrak{P}}$ *for some real* $\mathfrak{P}|\mathfrak{p}$,

(ii) *if* $\mathfrak{p}$ *is finite, then* $u_{\mathfrak{p}}$ *is a rational integer such that*

$$\psi_{\bar{M}/\bar{k}}(u_{\mathfrak{p}}-1)<m(\mathfrak{P})\leqq\psi_{\bar{M}/\bar{k}}(u_{\mathfrak{p}})$$

for some $\mathfrak{P}|\mathfrak{p}$ *and for some* $m(\mathfrak{P})$ *satisfying* (5).

For fixed $\mathfrak{m}$ in $D_2(\mathfrak{M})$, let $P_K(\mathfrak{m})$ be a P-set of K which contains $\mathfrak{P}$, used to define $\mathfrak{m}$ in the above definition. Then for each finite prime $\mathfrak{P}$ in $P_K(\mathfrak{m})$, there are rational numbers $m(\mathfrak{P})$'s such that

$$(6)\qquad \begin{cases} u(\mathfrak{P})-1<m(\mathfrak{P}) \\ \psi_{\bar{M}/\bar{k}}(u_{\mathfrak{p}}-1)<m(\mathfrak{P})\leqq\varphi_{\bar{M}/\bar{k}}(u_{\mathfrak{p}})\,. \end{cases}$$

Moreover, let $\boldsymbol{P}_K$ be the set of P-sets of K such that any $\mathfrak{P}$ in P_K satisfies

$$\left(\frac{N_{K/k}(\alpha),\ M_{\mathfrak{P}}/k_{\mathfrak{p}}}{\mathfrak{p}}\right)=1$$

for all α in $K^{\times}$ prime to $\mathfrak{p}$.

On the sets $D_1(\mathfrak{M})$ and $D_2(\mathfrak{M})$, Lemmas 5 and 6 below are essential.

LEMMA 5. *Let* L/k *be an abelian extension. Then, for any* $\mathfrak{m}_1\in D_1(\mathfrak{M})$ *and for any* $P_K\in\boldsymbol{P}_K$, $\mathfrak{G}(L)_{\mathfrak{m}_1}\subset\mathfrak{G}^*(K;\ P_K)_{\mathfrak{m}_1}$ *on* $(k^{\mathfrak{m}_1})_{\mathfrak{f}(K/k)}$ *implies* $L\subset K^*(\mathfrak{M})$.

PROOF. We can assume $L\supset k(\mathfrak{m}_1)$ without loss of generality by Lemma 3. Then, by Theorem 1, we see that L is the class field over k corresponding to the ideal group $i(a(\mathfrak{G}(L)_{\mathfrak{m}_1}))$. From $\mathfrak{G}(L)_{\mathfrak{m}_1}\subset\mathfrak{G}^*(K;\ P_K)_{\mathfrak{m}_1}$, it follows that

$$i(a(\mathfrak{G}(L)_{\mathfrak{m}_1}))\supset i(a(\mathfrak{G}^*(K;\ P_K)_{\mathfrak{m}_1}))\,.$$

On the other hand, by the translation theorem of the class field theory, an ideal $\mathfrak{A}$ of K is in $H(KL/K)$ if and only if the ideal $N_{K/k}(\mathfrak{A})$ of k is in $i(a(\mathfrak{G}(L)_{\mathfrak{m}_1}))$. Let $\mathfrak{A}\in S_K(\mathfrak{M})$, i.e., $\mathfrak{A}=(\alpha)$ for some $\alpha\equiv1(\mathrm{mod}\ \mathfrak{M})$. From the definition of $D_1(\mathfrak{M})$, it follows that $N_{K/k}(\alpha)\equiv1(\mathrm{mod}\ \mathfrak{m}_1)$. And from the definition of $\boldsymbol{P}_K$, $(N_{K/k}(\alpha))$ is in $i(a(\mathfrak{G}^*(K;\ P_K)_{\mathfrak{m}_1}))$. Therefore, we obtain $S_K(\mathfrak{M})\subset H(KL/K)$ i.e., $L\subset K(\mathfrak{M})$.

LEMMA 6. *Let* $K\subset L\subset K^*(\mathfrak{M})$. *Then there are P-sets* $P_K(\mathfrak{m}_2)$ *and* $P_L(\mathfrak{m}_2)$ *of* K *and* L *respectively such that*

$$\mathfrak{G}^*(K;\ P_K(\mathfrak{m}_2))_{\mathfrak{m}_2}=\mathfrak{G}^*(L;\ P_L(\mathfrak{m}_2))_{\mathfrak{m}_2} \quad on \quad (k^{\mathfrak{m}_2})_{\mathfrak{f}(K/k,P_K(\mathfrak{m}_2))}\ ,$$

for all $\mathfrak{m}_2 \in D_2(\mathfrak{M})$.

To prove Lemma 6, we enumerate the necessary properties of the Hasse's function of a Galois extension $\bar{K}/\bar{k}$ (see [8], [10] and [12]).

III (the conductor theorem). *Let* $\bar{K}/\bar{k}$ *be abelian and let* $\mathfrak{f}(\bar{K}/\bar{k})$ *be the conductor of* $\bar{K}/\bar{k}$, *then*

$$\mathfrak{f}(\bar{K}/\bar{k})=\mathfrak{p}^{\psi^{-1}_{\bar{K}/\bar{k}}(v(\bar{K}/\bar{k}))+1}\ ,$$

where $v(\bar{K}/\bar{k})$ *is the last ramification number of* $\bar{K}/\bar{k}$.

IV (Herbrand's theorem). *Let* $\bar{L}/\bar{k}$ *and* $\bar{K}/\bar{k}$ *be Galois extensions and let* $\bar{L}$ *contain* $\bar{K}$. *Then*

$$V^{(u)}_{\bar{K}/\bar{k}} \cong V^{(v)}_{\bar{L}/\bar{k}} G(\bar{L}/\bar{K})/G(\bar{L}/\bar{K})$$

for $\psi^{(u-1)}_{\bar{L}/\bar{K}} < v \leqq \psi_{\bar{L}/\bar{K}}(u)$.

PROOF OF LEMMA 6. Let $P_K(\mathfrak{m}_2)$ be a P-set of K satisfying (6) and $P_L(\mathfrak{m}_2)$ a P-set of L such that $P_K(\mathfrak{m}_2)$ is contained in $\{\mathfrak{P}_L \cap K: \mathfrak{P}_L \in P_L(\mathfrak{m}_2)\}$. Then, clearly,

$$\mathfrak{G}^*(L;\ P_L(\mathfrak{m}_2))_{\mathfrak{m}_2} \supset \mathfrak{G}^*(K;\ P_K(\mathfrak{m}_2))_{\mathfrak{m}_2} \quad \text{on} \quad (k^{\mathfrak{m}_2})_{\mathfrak{f}(L/k,P_L(\mathfrak{m}_2))}\ .$$

Let $\mathfrak{P}_L$ be in $P_L(\mathfrak{m}_2)$ and let $\mathfrak{P}=\mathfrak{P}_L \cap K$ and $\mathfrak{p}=\mathfrak{P}_L \cap k$. Put $\bar{L}=L_{\mathfrak{P}_L}$, $\bar{K}=K_{\mathfrak{P}}$, $\bar{k}=k_{\mathfrak{p}}$ and $\bar{L}_0$ (resp. $\bar{K}_0$) the maximal abelian subextension of $\bar{L}/\bar{k}$ (resp. $\bar{K}/\bar{k}$). Considering the conductor theorem III, we obtain by the choice of $P_K(\mathfrak{m}_2)$ that

$$V^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}_{\bar{L}_0/\bar{K}_0} = V^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}-1)+1)}_{\bar{L}_0/\bar{K}_0} = 1\ ,$$

where $u_\mathfrak{p}$ is the $\mathfrak{p}$-exponent of $\mathfrak{m}_2$. On the other hand, from the definition of the ramification groups, it follows that

$$V^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}_{\bar{L}_0/\bar{K}_0} = V^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}_{\bar{L}_0/\bar{k}} \cap G(\bar{L}_0/\bar{K}_0)\ .$$

Therefore, we obtain

$$\bar{L}_0 = \bar{L}_0^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}\bar{K}_0\ ,$$

where $\bar{L}_0^{(i)}$ is the i-th ramification field of $\bar{L}_0/\bar{k}$. By Herbrand's theorem IV,

$$[\bar{K}_0: \bar{K}_0^{(\psi_{\bar{K}_0/\bar{k}}(u_\mathfrak{p}))}] = [\bar{K}_0: \bar{K}_0 \cap \bar{L}_0^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}]$$
$$= [\bar{L}_0^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}\bar{K}_0: \bar{L}_0^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}]$$
$$= [\bar{L}_0: \bar{L}_0^{(\psi_{\bar{L}_0/\bar{k}}(u_\mathfrak{p}))}] .$$

Lemma 4 and the above imply

$$(7) \qquad \#\mathfrak{G}^{\mathfrak{P}}(K)_{\mathfrak{m}_2} = \#\mathfrak{G}^{\mathfrak{P}_L}(L)_{\mathfrak{m}_2}$$

for all infinite prime $\mathfrak{G}_L$ in $P_L(\mathfrak{m}_2)$. In case $\mathfrak{P}_L \in P_L(\mathfrak{m}_2)$ is infinite, the equality (7) also holds. And, by Lemma 1, we obtain Lemma 6.

The following Proposition 2 is a consequence of Lemmas 5 and 6.

PROPOSITION 2. (i) *For any P-set P_K in $\boldsymbol{P}_K$ and for any $\mathfrak{m}_1 \in D_1(\mathfrak{M})$,*

$$K^{**}(P_K; \mathfrak{m}_1) \subset K^*(\mathfrak{M}) .$$

(ii) *For any $\mathfrak{m}_2 \in D_2(\mathfrak{M})$, there is a P-set $P_K(\mathfrak{m}_2)$ such that*

$$K^*(\mathfrak{M}) \subset K^{**}(P_K(\mathfrak{m}_2); \mathfrak{m}_2) .$$

Especially, if $\mathfrak{m}$ is in $D_1(\mathfrak{M}) \cap D_2(\mathfrak{M})$ and if $P_K(\mathfrak{m})$ is in $\boldsymbol{P}_K$, then

$$K^*(\mathfrak{M}) = K^{**}(P_K(\mathfrak{m}); \mathfrak{m}) .$$

PROOF. Let $P_K(\mathfrak{m}_2)$ satisfy (6) for all finite primes in $P_K(\mathfrak{m}_2)$. We obtain $\mathfrak{G}(K^*(\mathfrak{M}))_{\mathfrak{m}_2} \subset \mathfrak{G}^*(K; P_K(\mathfrak{m}_2))_{\mathfrak{m}_2}$ by Lemma 6. Since $\mathfrak{G}(K^*(\mathfrak{M}))_{\mathfrak{m}_2}$ is trivial on $U_k^{\mathfrak{m}_2}$,

$$\boldsymbol{a}(\mathfrak{G}(K^*(\mathfrak{M}))_{\mathfrak{m}_2}) \supset \boldsymbol{a}(\mathfrak{G}^*(K; P_K(\mathfrak{m}_2))_{\mathfrak{m}_2}) U_k^{\mathfrak{m}_2} .$$

From the definition of $K^{**}(P_K(\mathfrak{m}); \mathfrak{m})$, it follows that

$$K^*(\mathfrak{M}) \subset K^{**}(P_K(\mathfrak{m}_2); \mathfrak{m}_2) .$$

The statement (i) is an immediate consequence of Lemma 5.

In the rest of the paper, we assume that the extension K/k is a Galois extension.

Put $\mathfrak{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}}$ and let $u_{\mathfrak{P}}$ is the rational integer satisfying

$$\psi_{K_{\mathfrak{P}}/k_\mathfrak{p}}(u_{\mathfrak{P}} - 1) < m_{\mathfrak{P}} \leqq \psi_{K_{\mathfrak{P}}/k_\mathfrak{p}}(u_{\mathfrak{P}})$$

for a finite prime $\mathfrak{P}$. For a real infinite prime $\mathfrak{P}$, put

$$u_{\mathfrak{P}} = \begin{cases} 1 & \text{if } \mathfrak{P} \mid \mathfrak{M} \\ 0 & \text{if } \mathfrak{P} \nmid \mathfrak{M} . \end{cases}$$

For any imaginary infinite prime $\mathfrak{P}$, we do not define $u_{\mathfrak{P}}$. Put

$$u_{\mathfrak{p}}^{*}=\min\{u_{\mathfrak{P}}: \mathfrak{P}|\mathfrak{p}\} ,$$

$$\mathfrak{m}^{*}=\prod_{\mathfrak{p}}\mathfrak{p}^{u_{\mathfrak{p}}^{*}} \tag{8}$$

where the product $\prod_{\mathfrak{p}}$ runs through all the finite primes and all the real infinite primes of k.

From the following Proposition V, we easily see

$$\mathfrak{m}^{*}\in D_{1}(\mathfrak{M}) .$$

V (cf. [8], [10] and [12]). *Let u be a non-negative integer, then, for any integer v such that $\psi_{\bar{K}/\bar{k}}(u-1)<v\leqq\psi_{\bar{K}/\bar{k}}(u)$,*

$$N_{\bar{K}/\bar{k}}(U_{\bar{K}}^{(v)})\subset U_{\bar{k}}^{(u)} .$$

Hereafter, we will be concerned with sufficient conditions for $\mathfrak{m}^{*}\in D_{2}(\mathfrak{M})$.

LEMMA 7. *Let $\bar{K}/\bar{k}$ (resp. $\bar{L}/\bar{k}$) be a Galois (resp. abelian) extension of non-archimedean local fields. Put $v(\bar{K}/\bar{k})$ the last ramification number of $\bar{K}/\bar{k}$. And put*

$$\mathfrak{f}(\bar{K}\bar{L}/\bar{K})=\mathfrak{P}^{u(\bar{K}\bar{L}/\bar{K})+1} , \quad \mathfrak{f}(\bar{L}/\bar{k})=\mathfrak{p}^{u(\bar{L}/\bar{k})+1} .$$

If $v(\bar{K}/\bar{k})\leqq u(\bar{K}\bar{L}/\bar{K})$, then $u(\bar{L}/\bar{k})$ is the rational integer such that

$$\psi_{\bar{K}/\bar{k}}(u(\bar{L}/\bar{k}))<u(\bar{K}\bar{L}/\bar{K})+1\leqq\psi_{\bar{K}/\bar{k}}(u(\bar{L}/\bar{k})+1) .$$

PROOF. From the conductor theorem III, it follows that

$$V_{\bar{K}\bar{L}/\bar{K}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K})))}\neq 1 ,$$

i.e.,

$$V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K})))}\cap G(\bar{K}\bar{L}/\bar{K})\neq 1 .$$

The above implies

$$V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K})))}\not\subset G(\bar{K}\bar{L}/\bar{L}) . \tag{9}$$

We obtain by Herbrand's theorem IV that if $\psi_{\bar{K}/\bar{k}}(u)<u(\bar{K}\bar{L}/\bar{K})+1$,

$$V_{\bar{L}/\bar{k}}^{(\psi_{\bar{L}/\bar{k}}(u))}\supset V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K})))}G(\bar{K}\bar{L}/\bar{L})/G(\bar{K}\bar{L}/\bar{L}) . \tag{10}$$

By (9) and (10),

(11) $$V_{\bar{L}/\bar{k}}^{(\psi_{\bar{L}/\bar{k}}(u))} \neq 1 .$$

On the other hand, from $v(\bar{K}/\bar{k}) \leqq u(\bar{K}\bar{L}/\bar{K})$, it follows that

$$\begin{aligned} 1 &= V_{\bar{K}/\bar{k}}^{(u(\bar{K}\bar{L}/\bar{K})+1)} \\ &= V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K}))+1)} G(\bar{K}\bar{L}/\bar{K})/G(\bar{K}\bar{L}/\bar{K}) , \end{aligned}$$

i.e.,

$$V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K}))+1)} \subset G(\bar{K}\bar{L}/\bar{K}) .$$

Since we defined $u(\bar{K}\bar{L}/\bar{K})+1$ as the exponent of the conductor of $\bar{K}\bar{L}/\bar{K}$,

$$1 = V_{\bar{K}\bar{L}/\bar{k}}^{(\psi_{\bar{K}\bar{L}/\bar{K}}(u(\bar{K}\bar{L}/\bar{K}))+1)} \cap G(\bar{K}\bar{L}/\bar{K}) .$$

So we obtain by Herbrand's theorem IV that if $u(\bar{K}\bar{L}/\bar{K})+1 \leqq \psi_{\bar{K}/\bar{k}}(u)$,

(12) $$V_{\bar{L}/\bar{k}}^{(\psi_{\bar{L}/\bar{k}}(u)+1)} = 1 .$$

(11) and (12) prove the lemma.

LEMMA 8. *Let $\bar{L}/\bar{k}$ and $\bar{K}/\bar{k}$ be Galois extensions and let $\bar{L}/\bar{K}$ be abelian. If $\bar{L}/\bar{K}$ is tamely ramified, then*

$$\psi_{\bar{K}/\bar{K}_0}(u(\bar{L}_0/\bar{K}_0)) < u(\bar{L}/\bar{K})+1 ,$$

where $\bar{K}_0$ (resp. $\bar{L}_0$) is the maximal abelian subextension of $\bar{K}/\bar{k}$ (resp. $\bar{L}/\bar{k}$) and $\mathfrak{f}(\bar{L}_0/\bar{K}_0) = \mathfrak{P}_0^{u(\bar{L}_0/\bar{K}_0)+1}$, $\mathfrak{f}(\bar{L}/\bar{K}) = \mathfrak{P}^{u(\bar{L}/\bar{K})+1}$ and $\mathfrak{P}_0$ (resp. $\mathfrak{P}$) is the prime of $\bar{K}_0$ (resp. $\bar{K}$).

PROOF. Take the inertia fields $\bar{T}$ and $\bar{T}_0$ of $\bar{L}/\bar{K}$ and $\bar{L}_0/\bar{K}_0$ respectively. Then we can easily see that $\bar{T} = \bar{T}_0\bar{K}$. Comparing the degrees $[\bar{L}_0 : \bar{T}_0]$ and $[\bar{L} : \bar{T}]$, we obtain the lemma.

The above Lemma 8 is a generalization of the lemma in [5].

THEOREM 2. *Let K/k be a Galois extension of finite algebraic number fields. For a fixed integral divisor $\mathfrak{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}}$, set $\mathfrak{m}^*$ as in (8). Suppose that any finite prime $\mathfrak{P}$ of K satisfies one of the following conditions:*

(i) *$\overline{K(\mathfrak{M})}/\bar{K}$ is tamely ramified,*

(ii) *the last ramification number $v(\bar{K}/\bar{M})$ of $\bar{K}/\bar{M}$ does not exceed $m_{\mathfrak{P}}-1$.*

Then the genus field $K^*(\mathfrak{M})$ is characterized by $\mathfrak{S}^*(K)_{\mathfrak{m}^*}$, i.e.,

$$H(K^*(\mathfrak{M})/K)=H(K;\mathfrak{m}^*)\ .$$

PROOF. Since K/k is Golois, $K^*(\mathfrak{M})/k$ is also Galois. So, the conductor of $\overline{K^*(\mathfrak{M})}/\bar{K}$ does not depend on the choice of $\mathfrak{P}$ dividing $\mathfrak{p}$. Set $m_\mathfrak{p}^*=\min\{m_\mathfrak{P}:\mathfrak{P}|\mathfrak{p}\}$ and $\mathfrak{M}'=\prod_\mathfrak{p}(\mathfrak{P}^{(1)}\mathfrak{P}^{(2)}\cdots)^{m_\mathfrak{p}^*}$ where $\mathfrak{P}^{(i)}(i=1, 2, \cdots)$ are all the primes of K dividing $\mathfrak{p}$. Then

$$K^*(\mathfrak{M})\subset K(\mathfrak{M}')\ . \tag{13}$$

There is an integer $u(\mathfrak{p})$ such that

$$\psi_{\bar{K}|\bar{M}}(u(\mathfrak{p})-1)<m_\mathfrak{p}^*\leqq\psi_{\bar{K}|\bar{M}}(u(\mathfrak{p}))\ . \tag{14}$$

From (13) and (14), it follows that $u(\mathfrak{p})$ is not less than the exponent of the conductor of $\bar{M}^*/\bar{M}$ (c.f. the definition of $D_2(\mathfrak{M})$ and Lemmas 7 and 8). On the other hand, from the choice of $\mathfrak{m}^*$, it follows that

$$\psi_{\bar{K}|\bar{k}}(u_\mathfrak{p}^*-1)<m_\mathfrak{p}^*\leqq\psi_{\bar{K}|\bar{k}}(u_\mathfrak{p}^*)\ .$$

Therefore, we obtain

$$\mathfrak{m}^*\in D_2(\mathfrak{M})\ .$$

So, Proposition 2 prove the theorem.

The following corollary is an immediate consequence of Theorem 2 and Proposition 1.

COROLLARY. *Let K/k be an abelian extension of finite algebraic number fields. Then, for an arbitrary integral divisor $\mathfrak{M}$ of K, the principal genus $H(K^*(\mathfrak{M})/K)$ is the ideal group of all the ideals $\mathfrak{A}\in I_K$ such that*

(i) $N_{K/k}(\mathfrak{A})=(\alpha)$ *for some* $\alpha\in k^{\mathfrak{m}^*}$,

(ii) $\left(\frac{\alpha, K_\mathfrak{P}/k_\mathfrak{p}}{\mathfrak{p}}\right)=\left(\frac{\varepsilon, K_\mathfrak{P}/k_\mathfrak{p}}{\mathfrak{p}}\right)$ *for some* $\varepsilon\in U_k^{\mathfrak{m}^*}$ *and for all* $\mathfrak{p}$ *ramifying in* K/k.

And the genus number $g_{K/k}(\mathfrak{M})$ is given by the formula

$$g_{K/k}(\mathfrak{M})=\frac{h_{\mathfrak{m}^*}\prod_\mathfrak{p}' e_\mathfrak{p}'}{[K:k](U_k^{\mathfrak{m}^*}:U_{K/k}^{\mathfrak{m}^*})} \tag{15}$$

where the product $\prod_\mathfrak{p}'$ runs through all the primes of k ramifying in K/k and $\mathfrak{m}^*$ is as in (8), $m_\mathfrak{p}^*=\min\{\mathfrak{P}\text{-exponent of }\mathfrak{M};\ \mathfrak{P}|\mathfrak{p}\}$,

$$e'_{\mathfrak{p}}=\begin{cases}\#V_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}^{(m_{\mathfrak{p}}^*)} & \text{if } \mathfrak{p} \text{ is finite} \\ 1 & \text{if } \mathfrak{p} \text{ is infinite and } \mathfrak{p}\mid\mathfrak{m}^* \\ 2 & \text{if } \mathfrak{p} \text{ is infinite and } \mathfrak{p}\nmid\mathfrak{m}^*, \end{cases}$$

$$h_{\mathfrak{m}^*}=[k(\mathfrak{m}^*): k]$$

and $U_{K/k}^{\mathfrak{m}^*}$ *is all the units in* $U_k^{\mathfrak{m}^*}$ *which are norms from* $K_{\mathfrak{P}}$ *for all primes* $\mathfrak{P}$ *of* K.

REMARK 2. For an arbitrary extension, a genus number formula similar to Satz 1 of Halter-Koch [6] has been obtained by Furuta. He also obtained a genus number formula similar to (15) in the case when K/k is EL-abelian. The latter genus number formula of Furuta follows from our Propositions 1 and 2.

REMARK 3. The theorem of Gold [3] is the case when $\mathfrak{M}$ is the integer ring of K in our Theorem 2. The genus number formula of Furuta [2] follows from Theorem 2 and Proposition 1. Theorem 7 of Gurak [5] is the case when $\mathfrak{M}$ is the product of all the real infinite primes of K. And Leopoldt's formula in [11] and the theorem in Hasse [9] are the case when k is the rational number field, K is an abelian field and $\mathfrak{M}$ is the product of all the real infinite primes of K in Corollary to Theorem 2.

References

[1] A. FRÖHLICH, The genus field and genus group in finite number fields I, II, Mathematika, **6** (1959), 40–46, 142–146.

[2] Y. FURUTA, The genus field and genus number in algebraic number fields, Nagoya Math. J., **29** (1967), 281–285.

[3] R. GOLD, Genera in normal extensions, Pacific J. Math., **63** (1976), 397–400.

[4] L. J. GOLDSTEIN, On prime discriminants, Nagoya Math. J., **45** (1971), 119–127.

[5] S. J. GURAK, Ideal-theoretic characterization of the relative genus field, J. Reine Angew. Math., **296** (1977), 119–124.

[6] F. HALTER-KOCH, Zur Geschlechtertheorie algebraischer Zahlkörper, Arch. Math., **31** (1978), 137–142.

[7] H. HASSE, Zur Geschlechtertheorie in quadratischer Zahlkörpern, J. Math. Soc. Japan, **3** (1951), 45–51.

[8] H. HASSE, Vorlesungen über Klassenkörpertheorie, Phisica-Verlag, Würzburg, 1967.

[9] H. HASSE, A supplement to Leopoldt's theory of genera in abelian number fields, J. Number Theory, **1** (1967), 4–7.

[10] S. IYANAGA, Number Theory, Iwanami Shoten, Tokyo, 1969, (in Japanese).

[11] H. W. LEOPOLDT, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. **9** (1953), 351–362.

[12] J.-P. SERRE, Corps Locaux, Hermann, Paris, 1962.

Present Address:
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCES
TOKYO METROPOLITAN UNIVERSITY
FUKAZAWA, SETAGAYA-KU, TOKYO 158