ON THE PRINCIPAL GENUS THEOREM CONCERNING THE ABELIAN EXTENSIONS

FUMIYUKI TERADA

(Received May 31, 1952)

Introduction

The principal genus theorem in a cyclic extension plays an important role in the study of the class field theory. A generalization of this theorem in the case of an abelian extension will be shown in this note. It was a long standing conjecture of Professor Tadao Tannaka.

Let K be an abelian extension of an algebraic number field k, and $\mathfrak{f}$ and $\mathfrak{F}$ be the conductor and the "Geschlechtermodul" of K/k respectively. Let $\mathfrak{m}$ be an integral module in k. Let us denote the ray ("Strahl") mod. $\mathfrak{mf}$ in k and mod. $\mathfrak{mF}$ in K by $R_k(\mathfrak{mf})$ and $R_K(\mathfrak{mF})$, respectively. H. Hasse proved the following so-called principal genus theorem for a cyclic extension (Cf. [1], pp. 304–310):

If K/k is a cyclic extension, following two conditions concerning an ideal $\mathfrak{A}$ of K are equivalent:

(1) $$N_{Kk}\mathfrak{A} \in R_k(\mathfrak{mf}),$$

(2) $$\mathfrak{A} = \mathfrak{B}^{1-\sigma}(A),\ (A) \in R_K(\mathfrak{mF}),$$

where σ is a generator of Galois group G of K/k.

The generalization in quite the same form seems to be difficult, and we take up the transformation set instead of the norm in (1). Namely, starting from a given ideal $\mathfrak{A}$, define an ideal $\mathfrak{A}(\sigma^a)$ corresponding to each element σ^a of G as the following:

$$\mathfrak{A}(1) = 1, \qquad \mathfrak{A}(\sigma) = \mathfrak{A}, \qquad \mathfrak{A}(\sigma^a) = \mathfrak{A}(\sigma)^{\sigma^{a-1}}\mathfrak{A}(\sigma^{a-1}) \qquad (0 < a < e,\ \sigma^e = 1).$$

Then, on the one hand, the condition (1) is equivalent to the condition

(3) $$\mathfrak{A}(\rho)^{\tau}\mathfrak{A}(\tau)\mathfrak{A}(\rho\tau)^{-1} \in R_k(\mathfrak{mf})$$

for all ρ, τ in G. And, on the other hand, the condition (2) is equivalent to the existence of an ideal $\mathfrak{B}$ such that

(4) $$\mathfrak{A}(\rho) = \mathfrak{B}^{1-\rho}(A(\rho)),\ (A(\rho)) \in R_K(\mathfrak{mF})$$

for any ρ in G. Moreover, these numbers $A(\rho)$ satisfy the condition:

(5) $A(\rho)^{\tau}A(\tau)A(\rho\tau)^{-1} \equiv 1$ mod. $\mathfrak{mf}$, and is contained in k

for any ρ, τ in G. So that, in the case of a cyclic extension, the assertion (1)→(2) is equivalent to the assertion (3)→(4), (5).

In an arbitrary abelian extension K/k, we shall deal with a generalization in this form. Let us denote by $\{\mathfrak{A}(\rho)\}$ a system of ideals in K corresponding to the elements of Galois group G of K/k. The main theorem in this note

is the following generalization of Hasse's result.

THEOREM 1. *In an arbitrary abelian extension, a necessary and sufficient condition for a system* $\{\mathfrak{A}(\rho)\}$ *to satisfy the condition* (3) *is that there exist an ideal* $\mathfrak{B}$ *and numbers* $A(\rho)$ *in* K *such that the conditions* (4) *aud* (5) *are satisfied.*[1]

As a sufficient condition to get (3), the conditions (4), (5) are not an actual generalization of the condition (2)—— we get (3) from (4), (5) immediately, although we have to use Lemma 2 in §1 in order to get (1) from (2). In this respect, we may have to take Theorem 1′, which is shown in §1, instead of Theorem 1 as a direct generalization of the Hasse's result.

In the case in which we do not consider the classification of numbers in K, a generalization of the principal genus theorem of a cyclic extension was proved by E. Noether making use of the theory of algebras (See [5]). If K/k is unramified abelian, and if $\mathfrak{m}=1$, our Theorem 1 is equivalent to Noether's result. As for the proof of our theorem, it depends only upon arithmetical results, and will be given in §1. The preceding Hasse's result is translated to a group-theoretical one by Artin's law of reciprocity, and this is directed from a property of a meta-abelian group (Cf. [3], [4]). In our case, however, the condition (3) is not a property of classes mod. $\mathfrak{m}\mathfrak{F}$, and we are not able to translate it to a group-theoretical one.

In §2 we first prove the following theorem which was proved by H. Hasse in the case of the fields of prime degree (Cf. [1], pp 298–302).

THEOREM 2.[2] *By a cyclic extension* K/k, *the following two conditions concerning a number* A *of* K *are equivalent to each other*:

$$N_{Kk}A \equiv 1 \bmod. \mathfrak{m}\mathfrak{f}, \tag{6}$$

$$A \equiv B^{1-\sigma} \bmod. \mathfrak{m}\mathfrak{F}, \tag{7}$$

where σ *is a generator of Galois group of* K/k[3].

This will be used in §1 to obtain Theorem 1 without proof there.

Moreover, we may consider naturally a generalization of this theorem in an arbitrary abelian extension. Concerning this, we have

THEOREM 3. *If* $\{A(\sigma)\}$ *is a system of numbers in* K *corresponding to the elements of* G *such that*

$$A(\rho)^{\tau}A(\tau)A(\rho\tau)^{-1} \equiv 1 \bmod. \mathfrak{m}\mathfrak{f}, \tag{8}$$

$$A(\rho)^{\tau-1} = A(\tau)^{\rho-1} \tag{9}$$

for all ρ, τ *in* G, *then there exist a number* B *such that*

1) In proving the necessity of the conditions (4) and (5), we do not assume that the principal ideals $\mathfrak{A}(\rho)^{\tau}\mathfrak{A}(\tau)\mathfrak{A}(\rho\tau)^{-1}$ are generated by elements which form a factor set. But after proving (4) and (5), it is shown that they are generated by a factor set which splits into a transformation set $A(\rho)$ with $\equiv 1$ mod. $\mathfrak{m}\mathfrak{F}$

2) Perhaps this result may have been proved already by some one. But I am not able to find the proof anywhere.

3) It is not necessary for A to be prime to the module $\mathfrak{m}\mathfrak{f}$.

(10) $$A(\rho) \equiv B^{1-\rho} \bmod \mathfrak{m}\mathfrak{F}$$

for all ρ in G.

This Theorem 3 is equivalent to the following result.

THEOREM 3'. *Let $\{a(\rho,\tau)\}$ be a factor set in K, satisfying the condition*

$$a(\rho,\tau) \equiv 1 \bmod \mathfrak{m}\mathfrak{f}, \quad a(\rho,\tau) = a(\tau,\rho)^{4)}$$

for all ρ,τ in G. Then, if $\{a(\rho,\tau)\}$ splits into a transformation set $\{A(\rho)\}$ in K, it splits into a transformation set such that $\equiv 1 \bmod \mathfrak{m}\mathfrak{F}$.

This will be proved also in § 2.

The author wishes to express his thank to Professor Tadao Tannaka who have conjectured the above generalization of the principal genus theorem and encouraged me during my study of these theorems.

§ 1

1. Lemmas. Let K be an abelian extension of degree m over an algebraic number field k. Let $\mathfrak{p}$ be a prime divisor in k, and V_i $(i = 1, 2, \cdots)$ be the Hilbert's sequence of subgroups of G corresponding to $\mathfrak{p}$, V_1 being the inertia group of $\mathfrak{p}$. Let $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e = \mathfrak{P}^e$ be the decomposition of $\mathfrak{p}$ in K. Denote the order of the group V_i by N_i $(i = 1, 2, \cdots)$, especially $N_1 = e$. For a finite prime spot $\mathfrak{p}$, the $\mathfrak{p}$-component $\mathfrak{D}(K/k)_\mathfrak{p}$ of the different $\mathfrak{D}(K/k)$ of K/k is given by $\mathfrak{P}^{\Sigma(N_i-1)}$ $(i = 1, 2, \cdots)$. In imitation of this formula, for an infinite prime $\mathfrak{p}_\infty$ in k, we define a module $\mathfrak{D}(K/k)_{\mathfrak{p}_\infty}$ by

$$\mathfrak{D}(K/k)_{\mathfrak{p}_\infty} = \begin{cases} \mathfrak{P}_\infty (= \mathfrak{P}_{\infty,1} \cdots \mathfrak{P}_{\infty,m/2}) & \text{if } \mathfrak{p}_\infty \text{ real and } \mathfrak{P}_\infty \text{ imaginary,} \\ 1 & \text{otherweise.} \end{cases}$$

In this note, we shall denote $\Pi_\mathfrak{p} \mathfrak{D}(K/k)_\mathfrak{p} \cdot \Pi_{\mathfrak{p}_\infty} \mathfrak{D}(K/k)_{\mathfrak{p}_\infty}$ by $\mathfrak{D}(K/k)$, and call it the different of K/k.

Let v be the number with $N_{v+1} \neq 1$, $N_{v+2} = 1$, and u be an integer defined by $u + 1 = \frac{1}{N_1} \Sigma_{i=1}^{v+1} N_i$. The $\mathfrak{p}$-component of the conductor $\mathfrak{f}(K/k)$ and of the "Geschlechtermodul" $\mathfrak{F}(K/k)$ are given by

(11) $$\mathfrak{f}(K/k)_\mathfrak{p} = \mathfrak{p}^{u+1}, \quad \mathfrak{F}(K/k)_\mathfrak{p} = \mathfrak{P}^{v+1}$$

respectively. Then it follows from the above definition of $\mathfrak{D}(K/k)$ and from these formulas that $\mathfrak{f}(K/k) = \mathfrak{D}(K/k) \cdot \mathfrak{F}(K/k)$.

LEMMA 1. *If K' is an intermediate field of K/k, we have*

(12) $$\mathfrak{F}(K/K')\mathfrak{f}(K/k) = \mathfrak{D}(K'/k)\mathfrak{F}(K/k)\mathfrak{f}(K/K'),$$

(13) $$\mathfrak{F}(K'/K)\mathfrak{f}(K/k) = \mathfrak{D}(K/K')\mathfrak{F}(K/k)\mathfrak{f}(K'/k).$$

PROOF.
$$\begin{aligned} \mathfrak{F}(K/K')\mathfrak{f}(K/k) &= \mathfrak{F}(K/K')\mathfrak{F}(K/k)\mathfrak{D}(K/k) \\ &= \mathfrak{F}(K/K')\mathfrak{D}(K/K')\mathfrak{F}(K/k)\mathfrak{D}(K'/k) \\ &= \mathfrak{f}(K/K')\mathfrak{F}(K/k)\mathfrak{D}(K'/k), \end{aligned}$$

which is (12), and we have also (13) by the same way, q. e. d.

LEMMA 2. *Let K/k be an abelian extension and $\mathfrak{m}$ and $\mathfrak{n}$ be integral modules in k. Denote the numbers in K by A and numbers in k by a. Then*

4) If a factor set $a(\rho,\tau)$ in K satisfies the condition $a(\rho,\tau) = a(\tau,\rho)$, then it is shown easily by a simple computation that all the numbers $a(\rho,\tau)$ lie in k.

1. *if* $A \equiv 1 \bmod. \mathfrak{m}\mathfrak{f}$, *we have* $N_{K_k}A \equiv 1 \bmod. \mathfrak{m}\mathfrak{f}$;

2. *if* $a \equiv 1 \bmod. \mathfrak{m}\mathfrak{f}$, *there exists* A *such that* $a \equiv N_{K_k}A \bmod. \mathfrak{m}\mathfrak{n}\mathfrak{f}$ *and* $A \equiv 1 \bmod. \mathfrak{m}\mathfrak{F}$.

PROOF. Let a_λ and A_η be elements in k and K respectively with $a_\lambda \equiv 1 \bmod. \mathfrak{p}^\lambda$ and $A_\eta \equiv 1 \bmod. \mathfrak{P}^\eta$. Then it follows from Hasse's result concerning the norm residue (See [2], pp. 210~223) that

$$N_{Kk}A_{v+re+1} \subset a_{u+r+1} \qquad (r \geqq 0), \tag{14}$$

$$N_{Kk}A_{v+re}\, a_{u+r+1} = a_{u+r} \qquad (r \geqq 1). \tag{15}$$

The first statement of our lemma follows from (11) and (14) immediately. As for the second statement, applying (15) successively to the given number a, we can find a number $A_\mathfrak{p}$ such that

$$A_\mathfrak{p} \equiv 1 \bmod. (\mathfrak{m}\mathfrak{F})_\mathfrak{p}, \quad a \equiv N_{K_k}A_\mathfrak{p} \bmod. (\mathfrak{m}\mathfrak{n}\mathfrak{f})_\mathfrak{p};$$

then a number A such that $A \equiv A_\mathfrak{p} \bmod. (\mathfrak{m}\mathfrak{n}\mathfrak{F})_\mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{n}\mathfrak{f}$ will satisfy the desired condition. q. e. d.

LEMMA 3. *In a* $\mathfrak{p}$*-adic case, any number* a *in* $k_\mathfrak{p}$ *such that* $\equiv 1 \bmod. \mathfrak{m}\mathfrak{f}$ *is the norm of a number* A *in* $K_\mathfrak{p}$ *such that* $\equiv 1 \bmod. \mathfrak{m}\mathfrak{F}$.

PROOF. This follows from the successive application of (14), which are also true in a $\mathfrak{p}$-adic case, immediately. q. e. d.

Now let us decompose Galois group of K/k into cyclic subgroups $G_1, \cdots, G_n$. Denote a generator of G_i by σ_i, and a corresponding subfield of K by K_i. For the sake of simplicity of the description, we shall use the following notations:

$$\Delta_i = 1 - \sigma_i, \quad M_i = 1 + \sigma_i \cdots + \sigma_i^{m_i-1} \qquad (i = 1, \cdots, n),$$

where m_i is the order of the group G_i. These symbols will be used in this note without further mention.

LEMMA 4. *If a system* $\{A_i\,;\, i = 1, \cdots, n\}$ *of numbers in* K *satisfy the following conditions*:

$$N_{K|K_i} A_i \ (= A_i^{M_i}) = 1 \qquad (i = 1, \cdots, n), \tag{16}$$

$$A_i^{\Delta_j} = A_j^{\Delta_i} \qquad (i, j = 1, \cdots, n), \tag{17}$$

then there exists a number A *in* K *such that* $A_i = A^{\Delta_i}$ $(i = 1, \cdots n)$. *This is also true for ideals instead of numbers. Moreover, if these elements* A_i *satisfy the additional condition*

$$A_i \equiv 1 \bmod. (\mathfrak{m})\mathfrak{M} \qquad (i = 1, \cdots, n), \tag{18}$$

where m *is the order of the group* G *and* $\mathfrak{M}$ *is an arbitrary integral module in* K, *such that* $\mathfrak{M}^\sigma = \mathfrak{M}$, *then we may select the preceding number* A *as it satisfies the following additional condition*:

$$A \equiv 1 \bmod. \mathfrak{M}. \tag{19}$$

PROOF. Let us arrange the groups G_i in a fixed order. For each element $\sigma = \sigma_{i_1}^{a_1} \cdots \sigma_{i_r}^{a_r}$ $(0 < a_j < m_{i_j})$ of G, define a number $A(\sigma)$ in K by

$$A(1) = 1. \quad A(\sigma_i) = A_i, \quad A(\sigma) = A(\sigma_{i_1}^{\sigma_1 - 1}\, \sigma_{i_2}^{a_2} \cdots \sigma_{i_r}^{\gamma}\tau)^{\sigma_{i_1}} A(\sigma_{i_1}).$$

Then it follows from (16) and (17) that

$$A(\sigma)^{\tau}\, A(\tau) A(\sigma\tau)^{-1} = 1$$

for all σ, τ in G. Let θ be an arbitrary generator of the extension K/k. Then we may find a number $A \neq 0$ under the following m numbers: $B_i = \Sigma_\sigma A(\sigma)\theta^{\sigma i}$ $(i = 0, \cdots, m-1)$, which satisfy $B_i^{\sigma} A(\sigma) = B_i$ (Speiser's lemma). Now, if $\{A_i\}$ satisfies (18), so does $\{A(\sigma)\}$. Let $f \neq 0$ be a rational number such that $f\theta$ is divisible by $(\mathfrak{m})\mathfrak{M}$. Then, $\theta' = 1 + f\theta$ is also a generator of the extension K/k and $\equiv 1 \bmod.(\mathfrak{m})\mathfrak{M}$. Therefore, all the numbers $B_i' = \Sigma A(\sigma)\theta'^{\sigma i}$ $(i = 1, \cdots, m)$ satisfy the following condition

$$B_i' \equiv \Sigma 1 = m \mod^{+}(\mathfrak{m})\mathfrak{M}.$$

This shows that we may find our number A with (19) under the m numbers B_i'/m. q. e. d.

2. Modification of Theorem 1. The assertion that (3) follows from (4) and (5) is trivial, as it was mentioned in the introduction, and we are interested only in the necessity of the conditions (4) and (5).

After putting $\rho = \sigma_i$ and $\tau = \sigma_i^{\eta}$ into (3), take the product letting a run from 0 to $m_i - 1$. Then we have, for $\mathfrak{A}(\sigma_i) = \mathfrak{A}_i$,

$$\mathfrak{A}_i^{M_i} = (a_i), \quad (a_i) \in R_k(\mathfrak{m}\dagger) \qquad (i = 1, \cdots, n). \tag{20}$$

Moreover, also in (3), let $\rho = \sigma_i$, $\tau = \sigma_j$ on the one hand, and $\rho = \sigma_j$, $\tau = \sigma_i$ on the other hand. Canceling $\mathfrak{A}(\sigma_i \sigma_j)$ in these two relations out, we have

$$\mathfrak{A}_i^{A_j} = \mathfrak{A}_j^{A_i}(a_{i,j}), \quad (a_{i,j}) \in R_k(\mathfrak{m}\dagger) \qquad (i, j = 1, \cdots, n).$$

Since $\Delta_i M_i = 0$ $(i = 1, \cdots, n)$, we have from this by operating $M_i M_j$

$$(a_{i,j})^{M_i M_j} = (a_{i,j})^{m_i m_j} = 1 \qquad (i, j = 1, \cdots n,),$$

which means $(a_{i,j}) = 1$. Therefore we have the following:

$$\mathfrak{A}_i^{A_j} = \mathfrak{A}_j^{A_i} \qquad (i, j = 1, \cdots, n). \tag{21}$$

To prove our assertion getting (4), (5) from (3), we need only prove the following:

THEOREM 1.[5] *A necessary and sufficient condition for a system* $\{\mathfrak{A}_i\}$ *of ideals in* K *to satisfy the condition* (20), (21) *is that there exist an ideal* $\mathfrak{B}$ *and numbers* A_i *in* K *such that*

$$\mathfrak{A}_i = \mathfrak{B}^{A_i}(A_i), \quad A_i \equiv 1 \bmod.\mathfrak{m}\mathfrak{F}(K/k)\mathfrak{D}(K/L_i) \qquad (i = 1, \cdots, n), \tag{22}$$

$$A_i^{A_j} = A_j^{A_i} \qquad (i, j = 1, \cdots, n), \tag{23}$$

$$A_i = A_i' A_i'', \quad A_i' \in L_i, \quad A_i'' \equiv 1 \bmod.\mathfrak{m}\mathfrak{F}(K/k)\,\mathfrak{D}(K/k) \quad (i = 1, \cdots, n), \tag{24}$$

where L_i *is a subfield of* K *corresponding to the subgroup* $G_1 \times \cdots \times G_{i-1} \times$

5) The statement (3)→(4), (5) is actually a generalization of the statement (1)→(2). In the case of $n = 1$, i.e., if K/k is a cyclic extension, the conditions (21), (23) and (24) in Theorem 1′ have no meaning, and Theorem 1′ is exactly the Hasse's result.

$G_{i+1}\times\cdots\times G_n$ *of* G.

In fact, we get Theorem 1 if we can prove the statement (20), (21)$\rightarrow$(22)$\sim$(24), as it is shown in the following.

Firstly, *it may be shown that* A_i *satisfies the following*

(25) $$A_i^{M_i}\equiv 1 \mod \mathfrak{m}\mathfrak{f}(K/k) \quad \textit{and} \in k, \qquad (i=1,\cdots,n).$$

PROOF. From (22) and (24) the number $A'\in L_i$ satisfies the condition

$$A_i'\equiv 1 \mod \mathfrak{m}\mathfrak{F}(K/k)\mathfrak{D}(K/L_i),$$

and then it follows from (13) in Lemma 1 that

$$A_i'\equiv 1 \mod \mathfrak{m}\mathfrak{f}(K/k)\mathfrak{F}(L_i/k)/\mathfrak{f}(L_i/k) \qquad (i=1,\cdots,n).$$

Applying Lemma 2 to the cyclic extension L_i/k and to the number $A_i'\in L_i$,

$$A_i'^{M_i}\equiv 1 \mod \mathfrak{m}\mathfrak{f}(K/k) \qquad (i=1,\cdots,n).$$

Applying the above method also to the cyclic extension K/K_i and to the number A_i'', which is $\equiv 1 \mod \mathfrak{m}\mathfrak{F}(K/k)\mathfrak{D}(K/k)$, we have

$$A_i''^{M_i}\equiv 1 \mod \mathfrak{m}\mathfrak{f}(K/k) \qquad (i=1,\cdots,n).$$

These two results show the first part of (25). On the other hand, operating M_i to the equality (23), we have $A_i^{M_i\Delta_j}=1$, which shows that $A_i^{M_i}$ is in $K_1\cap\cdots\cap K_{i-1}\cap K_{i+1}\cap\cdots\cap K_n$, and we have the second part of (25) as well as the fact that $A_i^{M_i}$ lies in K_i.

Now, for an arbitrary element $\rho=\sigma_{i_1}^{a_1}\cdots\sigma_{i_r}^{a_r}=\sigma_{i_1}\cdot\tau$ in G, we obtain by using (3)

$$\mathfrak{A}(\rho)\equiv\mathfrak{A}_{i_1}^{\tau}\,\mathfrak{A}(\tau) \mod R_k(\mathfrak{m}\mathfrak{f}(K/k)).$$

Using this, it is easy to derive (4) from (22) by an inductive method, and we do not go deep into its detail. In this process, the elements $A(\rho)$ in (4) may be constructed from A_i as we did in the proof of Lemma 4, and the relations (23), (25) shows the additional condition (5).

Thus we need only to prove the previous Theorem 1'. In this time also, the sufficiency of the conditions (22)$\sim$(24) is proved easily. That is, on the one hand, since (25) was derived from (22)$\sim$(24) only, we get (20) from (22) taking (25) into consideration; on the other hand, (22) and (23) show the condition (21). So that, we are interested only in the necessity of the conditions (22), (23) and (24). Concerning this, we shall proceed to a more simplified modification.

Let $\mathfrak{n}$ be an arbitrary integral module in k. Applying Lemma 2 to the cyclic extension L_i/k and to the element a_i in (20), we may find a number A_i' in L_i such that

(26) $$A_i'^{M_i}\equiv a_i \mod \mathfrak{m}\mathfrak{n}\mathfrak{f}(K/k),$$

(27) $$A_i'\equiv 1 \mod \mathfrak{m}\mathfrak{F}(L_i/k)\mathfrak{f}(K/k)/\mathfrak{f}(L_i/k)=\mathfrak{m}\mathfrak{F}(K/k)\mathfrak{D}(K/L_i).$$

These n elsments A_i' also satisfy

$$A_i'^{\Delta_j} = A_j'^{\Delta_i} \ (=1) \tag{28}$$

for all $i,j = 1, \cdots, n$. These elements A_i' are just the elements which we described A_i' in Theorem 1'. It follows from (20), (21), (26) and (28), that the ideals $\mathfrak{A}_i' = \mathfrak{A}_i/(A_i')$ satisfy the following conditions

$$\mathfrak{A}_i'^{M_i} = (a_i'), \quad a_i' \equiv 1 \bmod. \mathfrak{mf}(K/k), \quad a_i' \in k \qquad (i = 1, \cdots, n), \tag{20'}$$

$$\mathfrak{A}_i'^{\Delta_j} = \mathfrak{A}_j'^{\Delta_i} \qquad (i,j = 1, \cdots, n). \tag{21'}$$

Now, if we can prove from these, for a sufficiently large $\mathfrak{n}$, the following relations:

$$\mathfrak{A}_i' = \mathfrak{B}'^{\Delta_i}(A_i''), \quad A_i'' \equiv 1 \bmod. \mathfrak{m}\mathfrak{F}(K/k)\mathfrak{d}(K/k) \qquad (i = 1, \cdots, n), \tag{22'}$$

$$A_i''^{\Delta_j} = A_j''^{\Delta_i} \qquad (i,j = 1, \cdots, n), \tag{23'}$$

where $\mathfrak{d}(K/k) = N_{Kk}\mathfrak{D}(K/k)$, then we have the desired relations (22)~(24) taking (27), (28) in mind at the same time. Moreover, as the module $\mathfrak{n}$ can be taken sufficiently large, the module $\mathfrak{m}\mathfrak{d}(K/k)$ in (22') may be denoted again $\mathfrak{m}$, and consequently, we concern only with the following

THEOREM 1''. *If a system $\{\mathfrak{A}_i\}$ of ideals in K satisfies the conditions*

$$\mathfrak{A}_i^{M_i} = (a_i), \quad a_i \equiv 1 \bmod. \mathfrak{mf}(K/k), \quad a_i \in k \qquad (i = 1, \cdots, n), \tag{20''}$$

$$\mathfrak{A}_i^{\Delta_j} = \mathfrak{A}_j^{\Delta_i} \qquad (i,j = 1, \cdots, n) \tag{21''}$$

for a sufficiently large integral module $\mathfrak{n}$ in k, then there exist an ideal $\mathfrak{B}$ and numbers A_i such that

$$\mathfrak{A}_i = \mathfrak{B}^{\Delta_i}(A_i), \quad A_i \equiv 1 \bmod. \mathfrak{m}\mathfrak{F}(K/k) \qquad (i = 1, \cdots, n), \tag{22''}$$

$$A_i^{\Delta_j} = A_j^{\Delta_i} \qquad (i,j = 1, \cdots, n). \tag{23''}$$

3. **Proof of Theorem 1''.** Now, we shall proceed to the proof of Theorem 1''. From now on, we shall repeatedly use the relation (12) in Lemma 1, especially the following

$$\mathfrak{F}(K/k)\mathfrak{D}(K_i/k) = \mathfrak{F}(K/K_i)\mathfrak{f}(K/k)/\mathfrak{f}(K/K_i). \tag{12'}$$

This will be used by applying Lemma 2 to several cyclic extensions, and we do not notice in each time.

I. *We may assume that all the ideals $\mathfrak{A}_i$ are prime to* $\mathfrak{mf}(K/k)$.

PROOF. Let us decompose $\mathfrak{A}_i = \mathfrak{A}_i'\mathfrak{A}_i''$, where $\mathfrak{A}_i'$ is prime to $\mathfrak{mf}(K/k)$ and $\mathfrak{A}_i''$ consists of only the prime divisors of $\mathfrak{mf}(K/k)$. Then it follows especially from (20'') and (21'') that these ideals $\mathfrak{A}_i''$ satisfy the conditions $\mathfrak{A}_i''^{M_i} = 1$, $\mathfrak{A}_i''^{\Delta_j} = \mathfrak{A}_j''^{\Delta_i}$. Therefore, by Lemma 4, there exists an ideal $\mathfrak{B}''$ such that $\mathfrak{A}_i'' = \mathfrak{B}''^{\Delta_i}$. This shows that we need only prove (22'') and (23'') concerning the ideals $\mathfrak{A}_i'$ which are prime to $\mathfrak{mf}(K/k)$. q. e. d.

II. *We may find an ideal $\mathfrak{B}$, which is prime to* $\mathfrak{mf}(L/k)$, *and a number A_1 such that*

(29) $\mathfrak{A}_1 = \mathfrak{B}^{\Delta_1}(A_1),\ A_1 \equiv 1 \bmod. \mathfrak{m}\mathfrak{n}\mathfrak{F}(K/k)\mathfrak{D}(K_1/k).$ [6]

(30) $A_1^{M_1} \in k.$

PROOF. Let us apply Hasse's result described in the introduction to the cyclic extension K/K_1 and to the ideal $\mathfrak{A}_1$, Then we get such a relation as (29) immediately. Moreover, operating M_1 to (29), it follows from (20″) that

(31) $$1 \equiv A_1^{M_1} = a_1 \varepsilon_1 \equiv \varepsilon_1 \mod. \mathfrak{m}\mathfrak{n}\mathfrak{f}(K/k),$$

where ε_1 is an unit in K_1. Since ε_1 is a norm residue in the cyclic extension K/K_1, there exists a number B_1 in K such that

(32) $$\varepsilon_1 = B_1^{M_1}, \qquad (B_1) = \mathfrak{B}_1^{\Delta_1}$$

The latter in obtained from the so-called Hilbert's lemma (Lemma 4 in the case of $n = 1$). Then, it follows from (31), (32) especially that $B_1^{M_1} \equiv 1$ mod. $\mathfrak{m}\mathfrak{n}\mathfrak{f}(K/k)$, from which it follows from Theorem 2 that there exists a number C in K such that

(33) $$B_1 \equiv C^{\Delta_1} \mod. \mathfrak{m}\mathfrak{n}\mathfrak{F}(K/k)\mathfrak{D}(K_1/k).$$

Now, the number $A_1C^{\Delta_1}/B_1$ satisfies both (29) and (30), which means that $A_1C^{\Delta_1}/B_1$ is a desired one. That we can assume $(\mathfrak{B}, \mathfrak{m}\mathfrak{n}\mathfrak{f}) = 1$ is an immediate consequence of (29).

III. We shall conclude the proof of Theorem 1″ by an inductive method. Let the module $\mathfrak{n}$, which can be taken sufficiently large, be as large as to be divisible by $(m)^n\mathfrak{d}(K/k)^{2n}$, where m is the order of the group G and $\mathfrak{d} = \mathfrak{d}(K/k) = N_{Kk}\mathfrak{D}(K/k)$. [7] And define a module $\mathfrak{n}_r = \mathfrak{n}/(m)^r\mathfrak{d}^{2r}$ $(r = 0, 1, \cdots, n)$ in k.

Now let us assume, concerning $\mathfrak{A}_1, \cdots, \mathfrak{A}_r$ $(r < n)$, that there exist an ideal $\mathfrak{B}$, which is prime to $\mathfrak{m}\mathfrak{n}\mathfrak{f}(K/k)$, and elements $A_1, \cdots A_r$ such that

(34) $$\mathfrak{A}_i = \mathfrak{B}^{\Delta_i}(A_i),\ A_i \equiv 1 \bmod. \mathfrak{m}\mathfrak{n}_r\mathfrak{F}(K/k) \qquad (i = 1, \cdots, r),$$

(35) $$A_i^{M_i} \in k \qquad (i = 1, \cdots, r),$$

(36) $$A_i^{\Delta_j} = A_j^{\Delta_i} \qquad (i, j = 1, \cdots, r).$$

In the case of $r = 1$, these conditions are fulfilled, that is, the conditions (29) and (30) are just (34) (35), respectively, and (36) has no meaning at this time. Moreover, in the case of $r = n$, these conditions are just the desired conditions (22″) and (23″). Accordingly, we may prove our result by an inductive method, that is, we need only prove (34)~(36) concerning $\mathfrak{A}_1, \cdots, \mathfrak{A}_{r+1}$ under the preceding assumption (34)~(36) concerning $\mathfrak{A}_1, \cdots, \mathfrak{A}_r$.

PROOF OF THE INDUCTION. According to the conditions (34)~(36), the numbers $B_i = A_i^{\Delta_{r+1}}$ $(i = 1, \cdots, r)$ satisfy the following conditions

$$B_i \equiv 1 \bmod. \mathfrak{m}\mathfrak{n}_r\mathfrak{F}(K/k),\ B_i^{M_i} = 1,\ B_i^{\Delta_j} = B_j^{\Delta_i} \qquad (i, j, = 1, \cdots, r).$$

Applying Lemma 4 to the abelian extension $K/K_1 \cap \cdots \cap K_r$ and to these

6) As the module $\mathfrak{n}$ may be taken as large as we desire, it is not necessary to give it explicitly, and also to describe $\mathfrak{D}(K/k)$, $\mathfrak{d}(K/k)$, (m) in (29), (33), etc. I give only a rough bound of $\mathfrak{n}$.

7) Cf. 4).

numbers $B_1, \cdots, B_r$, there exists a number B such that

$$A_i^{\Delta_{r+1}} = B_i = B^{\Delta_i} \qquad (i = 1, \cdots, r), \tag{37}$$

$$B \equiv 1 \bmod. \mathfrak{m}_r \mathfrak{F}(K/k)/(m). \tag{38}$$

Then, it follows from (21″), (34) and (37),

$$\mathfrak{A}_{r+1}^{\Delta_i} = \mathfrak{A}_i^{\Delta_{r+1}} = (\mathfrak{B}^{\Delta_{r+1}}(B))^{\Delta_i} \qquad (i = 1, \cdots, r).$$

Therefore, if $\mathfrak{C}$ is an ideal defined by

$$\mathfrak{A}_{r+1} = \mathfrak{B}^{\Delta_{r+1}}(B)\mathfrak{C}, \tag{39}$$

it satisfies $\mathfrak{C}^{\Delta_i} = 1$ $(i = 1, \cdots, r)$. As the ideals $\mathfrak{A}_{r+1}, \mathfrak{B}$ and (B) are prime to $\mathfrak{f}(K/k)$, so also is $\mathfrak{C}$, whence $\mathfrak{C}$ is an ideal in $K_1 \cap \cdots \cap K_r$. Operating M_{r+1} to (39), it follows from (20″) that

$$(a_{r+1}) = (B^{M_{r+1}})\ \mathfrak{C}^{M_{r+1}}, \quad (a_{r+1}) \in R_k(\mathfrak{m}\mathfrak{f}). \tag{40}$$

Now, on the one hand, operating M_{r+1} to (37), we get $B^{M_{r+1}\Delta_i} = 1$ $(i = 1, \cdots, r)$, which shows

$$B^{M_{r+1}} \in K_1 \cap \cdots \cap K_r \cap K_{r+1}. \tag{41}$$

On the other hand, operating M_{r+1} to (38), we get

$$B^{M_{r+1}} \equiv 1 \bmod. \mathfrak{m}_r \mathfrak{f}(K/k)/(m)\mathfrak{d} = \mathfrak{m}_{r+1}\mathfrak{f}(K/k)\mathfrak{d}. \tag{42}$$

Therefore, the ideal $\mathfrak{C}$ in $K_1 \cap \cdots \cap K_r$ satisfies the condition

$$\mathfrak{C}^{M_{r+1}} \in R_{K_1} \cap \cdots \cap K_{r+1}(\mathfrak{m}_{r+1}\mathfrak{f}(\mathfrak{F}/k)\mathfrak{d}).$$

We may apply Hasse's result to the cyclic extension $K_1 \cap \cdots \cap K_r/K_1 \cap \cdots \cap K_{r+1}$ and to the ideal $\mathfrak{C}$. This shows that there exist an ideal $\mathfrak{B}'$ and a number B' in $K_1 \cap \cdots \cap K_r$ such that

$$\mathfrak{C} = \mathfrak{B}'^{\Delta_{r+1}}(B'), \quad B' \equiv 1 \bmod. \mathfrak{m}_{r+1}\mathfrak{F}(K/k)\cdot\mathfrak{d}, \tag{43}$$

whereby we used the result of the following computation which follows from Lemma 1:

$$[\mathfrak{f}(K/k)/\mathfrak{f}(K_1 \cap \cdots \cap K_r/K_1 \cap \cdots \cap K_{r+1})] \cdot \mathfrak{F}(K_1 \cap \cdots \cap K_r/K_1 \cap \cdots \cap K_{r+1})$$
$$= [\mathfrak{D}(K/k)/\mathfrak{D}(K_1 \cap \cdots \cap K_r/K_1 \cap \cdots \cap K_{r+1})]\cdot\mathfrak{F}(K/k).$$

It follows from (38), (39) and (43)

$$\mathfrak{A}_{r+1} = (\mathfrak{B}\mathfrak{B}')^{\Delta_{r+1}}(BB'), \quad BB' \equiv 1 \bmod. \ \mathfrak{m}_{r+1}\mathfrak{F}(K/k)\cdot\mathfrak{d}. \tag{44}$$

Now, the followings are just analogously as we get (30) from (29). Since $B' \in K_1 \cap \cdots \cap K_r$ and B satisfies (41), $(BB')^{M_{r+1}} \in K_1 \cap \cdots \cap K_{r+1}$. Then, analogous to (31), we get from (20″) and (44),

$$1 \equiv (BB')^{M_{r+1}} = a_{r+1}\cdot\varepsilon_{r+1} \equiv \varepsilon_{r+1} \bmod. \mathfrak{m}_{r+1}\cdot\mathfrak{f}(K/k), \tag{45}$$

where ε_{r+1} is an unit in $K_1 \cap \cdots \cap K_{r+1}$. Consequently we may find a number B'' and an ideal $\mathfrak{B}''$ in $K_1 \cap \cdots \cap K_r$ such that

$$\varepsilon_{r+1} = B''^{M_{r+1}}, \quad (B'') = \mathfrak{B}''^{\Delta_{r+1}}, \quad B'' \equiv 1 \bmod. \mathfrak{m}_{r+1}\cdot\mathfrak{F}(K/k). \tag{46}$$

We have consequently, on the one hand, from (44), (46)

$$\mathfrak{A}_{r+1} = (\mathfrak{B}\mathfrak{B}'\mathfrak{B}'')^{\Delta_{r+1}}(BB'/B''), \quad BB'/B'' \equiv 1 \bmod. \ \mathfrak{m}_{r+1}\cdot\mathfrak{F}(K/k),$$

and on the other hand, as $\mathfrak{B}'$, $\mathfrak{B}''$ are in $K_1 \cap \cdots \cap K_r$, we get from (34)

$$\mathfrak{A}_i = (\mathfrak{B}\mathfrak{B}'\mathfrak{B}'')^{\Delta_i}(A_i), \quad A_i \equiv 1 \bmod. \mathfrak{m}\cdot\mathfrak{n}_r\mathfrak{F}(K/k),$$

whence $\bmod. \mathfrak{m}\mathfrak{n}_{r+1}\mathfrak{F}(K/k)$, for $i = 1, \ldots, n$. These two relations show that (34) is also true for $r+1$ ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_{r+1}$ making use of the ideal $\mathfrak{B}\mathfrak{B}'\mathfrak{B}''$ and numbers $A_1, \ldots, A_r$, $A_{r+1} = BB'/B''$. In addition, since B', $B'' \in K_1 \cap \cdots \cap K_r$, it follows from (37)

$$A_i^{\Delta_{r+1}} = (BB'/B'')^{\Delta_i} \qquad (i = 1, \ldots, r),$$

which shows, together with the conditions (36) concerning $A_1, \ldots A_r$, the desired relation (36) for $A_1, \ldots, A_{r+1}$. And finally, it follows from (45), (46) that $(BB'/B'')^{M_{r+1}} = a_{r+1} \in k$, which is nothing but (35) for $A_{r+1} = BB'/B''$.

Thus we conclude our induction.

§ 2.

4. Proof of Theorem 2. In this section we shall prove Theorem 2 which was assumed by proving Theorem 1. The sufficiency of the condition (7) is an immediate consequence of Lemma 2, and we are interested only in its necessity.

I. *We can confine our attention to a number A which is prime to the module* $\mathfrak{m}\mathfrak{f}$.

PROOF. Let us suppose that A is not prime to $\mathfrak{m}\mathfrak{f}$. Then the ideal (A) is decomposable into a part $\mathfrak{A}$ which is prime to $\mathfrak{m}\mathfrak{f}$ and a part $\mathfrak{A}'$ which consists of prime divisions of $\mathfrak{m}\mathfrak{f}$. It follows from (6) especially that $N_{Kk}A$ is prime to $\mathfrak{m}\mathfrak{f}$, and the ideal $\mathfrak{A}'$ satisfies $N_{Kk}\mathfrak{A}' = 1$. Then the so-called Hilbert's lemma shows that there exists an ideal $\mathfrak{B}$ such that $\mathfrak{A}' = \mathfrak{B}^{1-\sigma}$. Now, take a number A' such that $\mathfrak{B}' = \mathfrak{B}(A')$ is prime to $\mathfrak{m}\mathfrak{f}$, and it is shown easily that $AA'^{1-\sigma}$ satisfies (6) and is also prime to $\mathfrak{m}\mathfrak{f}$. This shows the preceding statement. q. e. d.

II. It is shown easily that we may reduce our Theorem 2 to one concerning the prime-component of the modules, that is, we need only prove the following

THEOREM 2'. *Let $\mathfrak{p}$ be a prime divisior in k. If a number A satisfies the condition*

$$N_{Kk} = a \equiv 1 \bmod. (\mathfrak{m}\mathfrak{f})_{\mathfrak{p}}, \tag{6'}$$

then there exists a number B such that

$$A = B^{1-\sigma} \bmod. (\mathfrak{m}\mathfrak{F})_{\mathfrak{p}}, \tag{7'}$$

where the sign $(\ )_{\mathfrak{p}}$ means the $\mathfrak{p}$-components of these modules.

III. *We may confine our attention to the case in which the ground field k is the splitting field of $\mathfrak{p}$.*

PROOF. Let us denote

K_z the splitting field of $\mathfrak{p}$, G_z the splitting group of $\mathfrak{p}$,
$\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_g = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ the decomposition of $\mathfrak{p}$ in K_z and in K respectively,
A number in K prime to $(\mathfrak{m}\mathfrak{f})_p$ with $N_{Kk} A \equiv 1 \bmod (\mathfrak{m}\mathfrak{f})_p$,
B_0 number in K with $B_0^{1-\sigma}$ prime to $(\mathfrak{m}\mathfrak{f})_p$,
B number in K prime to $(\mathfrak{m}\mathfrak{f})_p$,
C number in $K \equiv 1 \bmod (\mathfrak{m}\mathfrak{F})_p$,
a number in $k \equiv 1 \bmod (\mathfrak{m}\mathfrak{f})_p$,
and we occasionally understand by the same symbols $A, \cdots$ also groups generated by them, respectively. Since $B_0^{1-\sigma} C \subset A$, we need only prove the following

$$(B : B_0^{1-\sigma} C) \leqq (B : A). \tag{47}$$

Now, on the one hand, a correspondence $B/C \to N_{Kk} B \cdot a/a$ shows that $(B : A) = (N_{Kk} B\, a : a)$, which is equal to $\varphi_k((\mathfrak{m}\mathfrak{f})_p)/e$, where φ_k is the Euler's function $\bmod (\mathfrak{m}\mathfrak{f})_p$ in k. On the other hand, we have

$$(B : B^{1-\sigma} C) = (B : B^{1-\sigma} C)/(B_0^{1-\sigma} C : B^{1-\sigma} C) = (D : C)/(B_0^{1-\sigma} C : B^{1-\sigma} C),$$

where D is a number in K such that $D^{1-\sigma} \equiv 1 \bmod (\mathfrak{m}\mathfrak{F})_p$ and is prime to $(\mathfrak{m}\mathfrak{f})_p$. Let Π and π be numbers in K and k with $\mathfrak{P}_i \| \Pi$ $(i = 1, \cdots, g)$ and $\mathfrak{p} \| \pi$ respectively. Then, for each number B_0, there exists an integer a such that B_0/Π^a is prime to $(\mathfrak{m}\mathfrak{f})_p$, i.e., $B_0/\Pi^a \subset B$. Accordingly, the quotient group $B_0^{1-\sigma} \cdot C/B^{1-\sigma} \cdot C$ is a cyclic group generated by the class of $\Pi^{1-\sigma}$. Since $\Pi^e = \pi B$, the order e^* of the preceding quotient group is a divisor of e. Hence, the inequality (47) which we wish to prove is reduced to the following

$$(D : C)/e^* \leqq \varphi_k((\mathfrak{m}\mathfrak{f})_p)/e, \tag{48}$$

where e^* is the least positive integer such that

$$(\Pi^{e^*})^{1-\sigma} \equiv B^{1-\sigma} \bmod (\mathfrak{m}\mathfrak{F})_p. \tag{49}$$

Let us now assume that we have proved Theorem 2′ concerning K/K_z and prime divisors $\mathfrak{p}_i$ $(i = 1, \cdots, g)$ of $\mathfrak{p}$ in K_z. In this case, let us denote all the preceding symbols $A, C, \cdots, e^*, \cdots$ by $A_{z,i}, C_{z,i}, \cdots, e^*_{z,i}, \cdots$, where we may assume $\Pi_{z,i} = \Pi$ $(i = 1, \cdots, g)$. Then it follows from our assumption that

$$(D_{z,i} : C_{z,i})/e^*_{z,i} \leqq \varphi_{Kz}((\mathfrak{m}\mathfrak{f})_{\mathfrak{p}_i})/e \qquad \text{for all } i = 1, \cdots g. \tag{50}$$

We have of course $\mathfrak{f}(K/K_z)_p = \mathfrak{f}(K/k)_p$ and $\mathfrak{F}(K/K_z)_p = \mathfrak{F}(K/k)_p$, and we denote them by $\mathfrak{f}_p$ and $\mathfrak{F}_p$ respectively in the following. Since σ^g is a generator of G_z, $e^*_{z,i}$ is the least positive integer such that $(\Pi^{e^*_{z,i}})^{1-\sigma^g} \equiv B_{z,i}^{1-\sigma^g} \bmod (\mathfrak{m}\mathfrak{f})_{\mathfrak{p}_i}$. By operating σ, it is shown easily that $e^*_{z,i}$ does not depend on i, and we may denote it by e^*_z. Now operating $1 + \sigma + \cdots + \sigma^{g-1}$ to (49), we get

$$(\Pi^{e^*})^{1-\sigma^g} \equiv B^{1-\sigma^g} \bmod (\mathfrak{m}\mathfrak{F})_{\mathfrak{p}_i} \qquad (i = 1, \cdots, g),$$

which shows especially

(51) $$e_z^* \leqq e^*.$$

Next, it can be shown that

(52) $$(D:C) \leqq (D_{z,1}:C_{z,1}).$$

In fact, it follows from the definition of D that $D^{1-\sigma_g} \equiv 1 \bmod.(\mathfrak{m}\mathfrak{F})_{\mathfrak{p}_i}$ $(i=1, \cdots, g)$, and this means $D \subset D_{z,i}$ $(i=1, \cdots, g)$. That is to say, D is contained at most in $(D_{z,1}:C_{z,1})$ classes mod. $(\mathfrak{m}\mathfrak{F})_{\mathfrak{p}_1}$. Moreover, if $D^{(1)} \equiv D^{(2)} \bmod.(\mathfrak{m}\mathfrak{F})_{\mathfrak{p}_1}$, we get from the definition of D that $D^{(1)} \equiv D^{(2)} \bmod.(\mathfrak{m}\mathfrak{F})_{\mathfrak{p}_i}$ for all $\mathfrak{p}_i$ $(i=2, \cdots, g)$, which shows $D^{(1)} \equiv D^{(2)} \bmod.(\mathfrak{m}\mathfrak{F})_p$. Accordingly also D is contained at most in $(D_{z,1}:C_{z,1})$ classes mod. $(\mathfrak{m}\mathfrak{F})_p$. Thus we get the inequality (52).

Now it follows from (50), (52)

$$(D:C)/e^* \leqq (D_{z,1}:C_{z,1})/e_z^* \leqq \varphi_{Kz}((\mathfrak{m}\mathfrak{F})_{\mathfrak{P}_1})/e = \varphi_k((\mathfrak{m}\mathfrak{f})_{\mathfrak{p}})/e.$$

This is the desired relation (48), and we have gotten the preceding statement. q. e. d.

IV. Thus we may confine our attention to the case in which the ground field is the splitting field of p, Then it is easy to see that we may reduce our Theorem 2′ to one concerning p-adic number field, and in this case the statement follows from Lemma 3. That is to say, for the number a in (6′), there exists a number C such that

$$N_{Kk}A = a = N_{Kk}C, \qquad C \equiv 1 \bmod.\ (\mathfrak{m}\mathfrak{F})_p,$$

and it follows from Hilbert's lemma that we may find such a number as $A/C = B^{1-\sigma}$

This completes the proof of Theorem 2′ and accordingly Theorem 2.

5. **Proof of Theorem 3.** We may prove Theorem 3 quite analogously as by the proof of Theorem 1. All the arguments of the proof of Theorem 1 in which ideals are replaced by numbers hold true after some amendent which is seen easily, and we does not refer to the minute detail of this proof. As for the condition (9), we must assume it in order to get (21) and $A_{\sigma_i}^{M_i} \in k$. Moreover we get Theorem 3′ if we describe $A(\rho)^\tau A(\tau)A(\rho\tau)^{-1}$ in Theorem 3 by $a(\rho, \tau)$.

BIBLIOGRAPHY

[1] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkorper I_a, Jahr. der Deut. Math., 27(1926).
[2] H. HASSE, Klassenkörpertheorie, Marburg, 1932.
[3] J. HERBRAND, Sur les théorèmes du genre principal et des ideaux principaux, Abh. a. d. Hamb. Math. Sem., 8(1933).
[4] S. IYANAGA, Zur Theorie der Geschlechtermodul, Crelle's Journal, 171(1934).
[5] E. NOETHER, Der Hauptgeschlechtssatz für relativ galoissche Zahlkorper, Math. Ann., 108(1933).

MATHEMATICAL INSTITUTE, TÔHOKU UNIVERSITY, SENDAI.