ON THE PRINCIPAL GENUS THEOREM

HIDEO KUNIYOSHI and SHUICHI TAKAHASHI

(Received July 20, 1953)

Recently, Mr. F. Terada has proved the principal genus theorem for abelian extension fields [2]. It is the purpose of this paper to investigate the same problem for non abelian cases. Though our theorem is slightly different from Terada's formulation, both coincide in cyclic cases.

Let K be a normal extension field of a number field k, with the galois group $\mathfrak{G}$. We denote by $\mathfrak{D}$ the relative different of K/k, and by $\mathfrak{f}$ the conductor[1] of K/k. Our theorem is stated as follows:

THEOREM 1. *Let $\{\mathfrak{A}_\sigma, \sigma \in \mathfrak{G}\}$ be a system of ideals of K which satisfies the following conditions:*

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

(2) $\mathrm{A}_{\sigma,\tau} \equiv 1 \qquad \text{mod. } \mathfrak{f}\mathfrak{D}$,

(3) $\{\mathrm{A}_{\sigma,\tau}\}$ *is a factor set of K/k.*

Then, there exists an ideal $\mathfrak{C}$ such that

(4) $\mathfrak{A}_\sigma = \mathfrak{C}^{1-\sigma}(C_\sigma)$,

where $C_\sigma \equiv 1 \quad \text{mod. } \mathfrak{f}$.

To prove the theorem by employing idèles, we restate it in terms of them.

THEOREM 1′. *Let $\{\mathfrak{A}_\sigma, \sigma \in \mathfrak{G}\}$ be a system of idèles in K which satisfies the following conditions :*

(1′) $\mathfrak{A}_\tau^\sigma \mathfrak{A}_{\sigma\tau}^{-1} \mathfrak{A}_\tau = A_{\sigma,\tau} \mathfrak{U}_{\sigma,\tau}$,

(2′) $\mathfrak{U}_{\sigma,\tau} \equiv 1$[2] $\qquad$ mod. $\mathfrak{f}\mathfrak{D}$,

(3′) $\{\mathrm{A}_{\sigma,\tau}\}$ *is a principal idèle factor set.*

Then, there exists an idèle $\mathfrak{C}$ such that

(4′) $\mathfrak{A}_\sigma = \mathfrak{C}^{1-\sigma}\mathfrak{B}_\sigma$,

where $\mathfrak{B}_\sigma \equiv 1 \qquad \text{mod. } \mathfrak{f}$.

PROOF OF THE EQUIVALENCE OF THEOREM 1 AND THEOREM 1′. In the assumption of Theorem 1, for the primes $\mathfrak{P}$ of k dividing $\mathfrak{f}$, the $\mathfrak{p}$-components of $\mathfrak{A}_\sigma$ form an ideal crossed character (one dimensional ideal cocycle), and it

1) Let $\mathfrak{P}$ be a prime spot of K. We denote by $\mathfrak{G}_i$ the i-th ramification group of $\mathfrak{P}$ for K/k, i. e., $\mathfrak{G}_i = \{\sigma \in \mathfrak{G}, A^\sigma \equiv A \text{ mod } \mathfrak{P}^{i+1}$ for all integers A of $K\}$ and by $\mathfrak{G}_r$ the last $\mathfrak{G}_i \neq 1$. Then, we define the $\mathfrak{P}$ conductor $\mathfrak{f}_{\mathfrak{P}}$ of K/k formally as $\mathfrak{P}^f$, $f = \sum_{i=0}^{r} [\mathfrak{G}_i : 1]$. The ideal $\mathfrak{f} = \Pi \mathfrak{f}_{\mathfrak{P}}$ of K is called the conductor of K/k. As $\mathfrak{f}_{\mathfrak{P}} = \mathfrak{f}_{\mathfrak{P}'}$, for each canjugate $\mathfrak{P}'$ of $\mathfrak{P}$, $\mathfrak{f}$ is invariant under automorphisms of K/k.

2) $\mathfrak{A} \mathrel{\underline{\equiv}} 1$ (mod. $\mathfrak{m}$) means $\mathfrak{A} \equiv 1$ (mod. $\mathfrak{m}$) and $\mathfrak{A}_{\mathfrak{P}}$ are $\mathfrak{P}$-units at $\mathfrak{P} \nmid \mathfrak{m}$.

is of the form $\mathfrak{C}^{1-\sigma}$ (an ideal coboundary). Translating these factors into the right side of (4), we may assume that $\mathfrak{A}_\sigma$ are all prime to $\mathfrak{f}\mathfrak{D}$.

As $\mathfrak{f}$ and $\mathfrak{D}$ are invariant under automorphisms in $\mathfrak{G}$, $\mathfrak{G}$ is an operator domain of ideal and idèle class groups modulo $\mathfrak{f}$, (res. $\mathfrak{f}\mathfrak{D}$). Under the usual isomorphism between these two groups, theorems 1 and 1′ are transformable into each other.

In the following, german letters should mean idèles instead of ideals.

We begin the proof with local considerations.

LEMMA 1. *Let $K_{\mathfrak{P}}$ be a normal extension field of a $\mathfrak{p}$-adic number field $k_{\mathfrak{p}}$. Let $\mathfrak{D}_{\mathfrak{P}}$, $\mathfrak{f}_{\mathfrak{P}}$ be its relative different and conductor*[1]*, respectively.*

Then, a factor set $U_{\sigma,\tau}$ in the ray (Strahl) of $\mathfrak{D}_{\mathfrak{P}}\mathfrak{f}_{\mathfrak{P}}$

$$U_{\sigma,\tau} \equiv 1 \qquad \text{mod. } \mathfrak{D}_{\mathfrak{P}}\mathfrak{f}_{\mathfrak{P}}$$

is a splitting factor set.

Furthermore, it splits in the ray of $\mathfrak{f}_{\mathfrak{P}}$, i.e., there exists $\{B_\sigma\}$ in the ray of $\mathfrak{f}_{\mathfrak{P}}$

$$B_\sigma \equiv 1 \qquad \text{mod. } \mathfrak{f}_{\mathfrak{P}}$$

such that

$$U_{\sigma,\tau} = B_\tau^\sigma B_{\sigma\tau}^{-1} B_\sigma.$$

PROOF. It holds obviously for unramified $K_{\mathfrak{P}}/k_{\mathfrak{p}}$.

For a ramified extension we prove the lemma in a generalized form.

Let us put

$$s = \min_{A \in K_{\mathfrak{P}}} \text{Ord. } \frac{S(A)}{A},$$

$S(A)$ being the trace of A concerning $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Obviously $s \geq 0$.

If the factor set $U_{\sigma,\tau}$ is in the ray of $\mathfrak{P}^x$, $x > 2s$

$$U_{\sigma,\tau} \equiv 1 \qquad \text{mod. } \mathfrak{P}^x \qquad x > 2s$$

it splits in the ray of $\mathfrak{P}^{x-s}$, i.e.,

$$U_{\sigma,\tau} = B_\tau^\sigma B_{\sigma\tau}^{-1} B_\sigma,$$

$$B_\sigma \equiv 1 \qquad \text{mod. } \mathfrak{P}^{x-s}.$$

In fact, we take $A_0 \in K_{\mathfrak{P}}$ which attains the minimum value s, and put

$$U_{\sigma,\tau} = 1 + V_{\sigma,\tau}, \qquad V_{\sigma,\tau} \equiv 0 \text{ mod. } \mathfrak{P}^x,$$

$$B'_\sigma = \frac{1}{S(A_0)} \sum_{\tau \in \mathfrak{G}} \sigma\tau(A_0)\ V_{\sigma,\tau},$$

and

$$B_\sigma^{(x)} = 1 + B'_\sigma.$$

Then it follows from the definitions of B_σ' and A_0

$$B_\sigma^{(x)} \equiv 1 \qquad \text{mod. } \mathfrak{P}^{x-s}.$$

As $x > 2s > 0$, we know that

$$U_{\sigma,\tau}\ (B_\tau^\sigma B_{\sigma\tau}^{-1} B_\sigma)^{-1} \equiv 1 \qquad \text{mod. } \mathfrak{P}^{x+1}.$$

Repeating this process, we have a converging infinite product $\prod_{y \geq x} B_{\sigma}^{(y)}$ which is a desired solution B_{σ}.

Finally, from the definition, $s <$ Ord. $\mathfrak{D}_{\mathfrak{P}} <$ Ord. $\mathfrak{f}_{\mathfrak{P}}$.[1] Therefore, we may take Ord. $\mathfrak{D}_{\mathfrak{P}}$ + Ord. $\mathfrak{f}_{\mathfrak{P}}$ as x and get a solution in the ray of $\mathfrak{P}^{x-s}$ which is contained in the ray of $\mathfrak{f}_{\mathfrak{P}}$.

LEMMA 2. *Let $U_{\sigma,\tau}$ be an idèle factor set and*

$$U_{\sigma,\tau} \equiv 1 \qquad \text{mod. } \mathfrak{f}\mathfrak{D}.$$

Then, there exists a system $\{B_{\sigma}\}$ of idèles in K, such that

$$U_{\sigma,\tau} = B_{\tau}^{\sigma} \; B_{\sigma\tau}^{-1} \; B_{\sigma}$$

$$B_{\sigma} \equiv 1 \qquad \text{mod. } \mathfrak{f}.$$

PROOF. We prove the lemma for each component of $\mathfrak{p}$ of k, and combine them to get the seeking B_{σ}. As components are always $\mathfrak{P}$- units, the resulting B_{σ} is an idèle.

We shall restrict ourselves to the $\mathfrak{p}$-component idèles $I_{\mathfrak{p}}$. It is the product of $\mathfrak{P}$ components,

$$I_{\mathfrak{p}} = \prod_{\mathfrak{P} | \mathfrak{p}} I_{\mathfrak{P}},$$

where $\mathfrak{P}$ mean prime factors of $\mathfrak{p}$ in K. We denote by $R(\mathfrak{f})_{\mathfrak{P}}$ the ray of $\mathfrak{f}_{\mathfrak{P}}$, as a subgroup of $K_{\mathfrak{P}}^*$, and $R(\mathfrak{f})_{\mathfrak{p}}$ the direct product of $R(\mathfrak{f})_{\mathfrak{P}}$ where $\mathfrak{P}$ ranges over $\mathfrak{P} | \mathfrak{p}$, which is a subgroup of $I_{\mathfrak{p}}$. Similar notations $R(\mathfrak{D}\mathfrak{f})_{\mathfrak{P}}$, $R(\mathfrak{D}\mathfrak{f})_{\mathfrak{p}}$ are used analogously. The automorphism σ in $\mathfrak{G}$ induces automorphisms in $R(\mathfrak{f})_{\mathfrak{p}}$ and $R(\mathfrak{D}\mathfrak{f})_{\mathfrak{p}}$. From Shapiro's lemma [1], we have onto isomorphisms

$$H^2(\mathfrak{G}, R(\mathfrak{f})_{\mathfrak{p}}) \longrightarrow H^2(\mathfrak{G}_{\mathfrak{P}}, R(\mathfrak{f})_{\mathfrak{P}}),$$

$$H^2(\mathfrak{G}, R(\mathfrak{f}\mathfrak{D})_{\mathfrak{p}}) \longrightarrow H^2(\mathfrak{G}_{\mathfrak{P}}, R(\mathfrak{D}\mathfrak{f})_{\mathfrak{P}}).$$

Furthermore, the following diagram is commutative.

$$\begin{tikzcd} H^2(\mathfrak{G}, R(\mathfrak{f})_{\mathfrak{p}}) \arrow[d] & H^2(\mathfrak{G}, R(\mathfrak{f}\mathfrak{D})_{\mathfrak{p}}) \arrow[l, "\varphi"'] \arrow[d] \\ H^2(\mathfrak{G}_{\mathfrak{P}}, R(\mathfrak{f})_{\mathfrak{P}}) & H^2(\mathfrak{G}_{\mathfrak{P}}, R(\mathfrak{f}\mathfrak{D})_{\mathfrak{P}}), \arrow[l, "\psi"] \end{tikzcd}$$

where φ and ψ are induced by injection maps

$$R(\mathfrak{f})_{\mathfrak{p}} \longleftarrow R(\mathfrak{f}\mathfrak{D})_{\mathfrak{p}},$$

$$R(\mathfrak{f})_{\mathfrak{P}} \longleftarrow R(\mathfrak{f}\mathfrak{D})_{\mathfrak{P}}.$$

The image of ψ is (0) from lemma 1, and hence the image of φ is also (0). This shows the lemma for the $\mathfrak{p}$-component.

PROOF OF THEOREM 1′.

From lemma 2 we have

$$\mathfrak{U}_{\sigma,\tau} = \mathfrak{B}_{\tau}^{\sigma} \; \mathfrak{B}_{\sigma\tau}^{-1} \; \mathfrak{B}_{\sigma},$$

$$\mathfrak{B}_{\sigma} \equiv 1 \quad \text{mod. } \mathfrak{f}.$$

Therefore, $\{A_{\sigma,\tau}\}$ is an everywhere splitting factor set. From, Hasse's norm theorem, it splits as a global factor set. i. e.,

$$A_{\sigma,\tau} = C_{\tau}^{\sigma} \; C_{\sigma\tau}^{-1} \; C_{\sigma}.$$

Hence, $\left\{\dfrac{\mathfrak{A}_\sigma}{\mathfrak{B}_\sigma\ C_\sigma}\right\}$ is a one-dimensional idèle cocycle which is always a coboundary

$$\frac{\mathfrak{A}_\sigma}{\mathfrak{B}_\sigma\ C_\sigma} = \mathfrak{C}^{1-\sigma}.$$

REFERENCES

[1] G. HOCHSCHILD-T. NAKAYAMA; Cohomology in class field theory, Ann. of Math. 55(1952), 348-366.

[2] F. TERADA; On the principal genus theorem concerning the Abelian extensions, Tôhoku Math. Journ. 4 (1952), 141-152.

MATHEMATICAL INSTITUTE, TÔHOKU UNIVERSITY, SENDAI.