S. Shirai
Nagoya Math. J.
Vol. 71 (1978), 61-85

ON THE CENTRAL CLASS FIELD mod $\mathfrak{m}$ OF GALOIS EXTENSIONS OF AN ALGEBRAIC NUMBER FIELD

SUSUMU SHIRAI

Introduction

Let k be the rational number field, K/k be an Abelian extension defined mod $\tilde{m}$ whose degree is some power of a prime ℓ, and let $\mathfrak{A}$ be the module of K belonging to $\tilde{m}$ in the sense of Fröhlich [1, p. 239]. Denote by $\hat{K}$ (resp. K^*) the maximal central (resp. genus) ℓ-extension of K/k contained in the ray class field mod $\mathfrak{A}$ of K. Fröhlich [1, Theorem 3] proved that if $(m, 16) \neq 8$, then the Galois group of $\hat{K}$ over K^* is isomorphic to the Schur multiplicator of the Galois group of K over k, and using this theorem, he gave a complete characterization of all fields whose Galois groups over the rational number field are of nilpotency class two.

In the present paper, we generalize the above result to the case where the base field k is an arbitrary algebraic number field of finite degree and K/k any finite Galois extension.

§§ 1, 2 contain a generalization of the conductor and the Geschlechtermodul, which, the author thinks, plays an important role in a study of nilpotent extensions. In § 3 we define the central class field mod $\mathfrak{m}$ of a Galois extension and prove our main theorem which may be viewed as a direct generalization of the principal genus theorem for a cyclic extension (Theorem 29). In §§ 4, 5, and 6 we apply our main theorem to some cases.

The author wishes to express his hearty thanks to Professor Y. Furuta for his valuable advice and encouragement.

§ 1. The Galois conductor of a local Galois extension

Throughout this section, k is always a field complete with respect to a discrete prime divisor $\mathfrak{p}$ of a global field, and some basic notation

Received June 10, 1977.

is listed below.

$k^\times$ the multiplicative group of all non-zero elements of k.

$U_k^{(i)}$ the group of all elements a in $k^\times$ such that $a \equiv 1 \bmod \mathfrak{p}^i$, in particular, $U_k^{(0)}$ is the unit group of k.

Let K/k be a finite Galois extension. Then:

$N_{K/k}$ the Norm of K to k.

$G(K/k)$ the Galois group of K over k.

$V_{K/k}^{(i)}$ the i-th ramification group of K/k with $V_{K/k}^{(-1)} = G(K/k)$.

$\mathscr{V}(K/k)$ the last ramification number of K/k, in other words, $V_{K/k}^{(\mathscr{V}(K/k))} \neq 1$ and $V_{K/k}^{(\mathscr{V}(K/k)+1)} = 1$.

$\varphi_{K/k}(i)$ the Hasse's function for K/k.

It is well-known that Hasse [9] proved that if K/k is a finite Galois extension, then

$$N_{K/k}U_K^{(\varphi_{K/k}(i-1)+1)} \subset U_k^{(i)} \qquad \text{for } i \geqq 0 \tag{1}$$

and moreover, if K/k is Abelian and $\mu(K/k)$ the $\mathfrak{p}$-exponent of the conductor of K/k, then

$$\mu(K/k) = \varphi_{K/k}^{-1}(\mathscr{V}(K/k)) + 1 \tag{2}$$

and

$$N_{K/k}U_K^{(\varphi_{K/k}(i-1)+1)} = U_k^{(i)} \qquad \text{for } i \geqq \mu(K/k)\,. \tag{3}$$

In this direction we define the Galois conductor of a finite Galois extension.

DEFINITION. Let K/k be a finite Galois extension, and let $\mu(K/k)$ be the least integer i such that $\varphi_{K/k}(i-1) \geqq \mathscr{V}(K/k)$, namely, the least integer i such that $V_{K/k}^{(\varphi_{K/k}(i-1)+1)} = 1$. Then we define the *Galois conductor of* K/k to be $\mathfrak{f}(K/k) = \mathfrak{p}^{\mu(K/k)}$. Needless to say, this coincides with the ordinary one when K/k is Abelian.

LEMMA 1. *Let K/k be a finite Galois extension. Then:*

(i) *If $\varphi_{K/k}^{-1}(\mathscr{V}(K/k))$ is an integer, then $\mu(K/k) = \varphi_{K/k}^{-1}(\mathscr{V}(K/k)) + 1$, and if not, $\mu(K/k) = [\varphi_{K/k}^{-1}(\mathscr{V}(K/k))] + 2$, [ ] being the Gauss symbol.*

(ii) *K/k is unramified if and only if $\mu(K/k) = 0$.*

(iii) *K/k is tamely ramified if and only if $\mu(K/k) \leqq 1$.*

Proof. Immediate from the definition.

LEMMA 2. *Let K/k be a finite Galois extension, and let $\mathfrak{D}(K/k)$ be the different of K/k. Then*

$$\mathfrak{f}(K/k) = \mathfrak{D}(K/k)\cdot\mathfrak{P}^{\varphi_{K/k}(\mu(K/k)-1)+1},$$

here $\mathfrak{P}$ denotes the prime ideal of K.

Proof. Let N_i be the order of $V^{(i)}_{K/k}$. Then we have

$$\mu(K/k) = \sum_{i=0}^{\varphi_{K/k}(\mu(K/k)-1)} N_i/N_0 = \sum_{i=0}^{\nu(K/k)} N_i/N_0 + \sum_{i=\nu(K/k)+1}^{\varphi_{K/k}(\mu(K/k)-1)} 1/N_0$$

and hence

$$\begin{aligned} e\cdot\mu(K/k) &= \sum_{i=0}^{\nu(K/k)} N_i + \varphi_{K/k}(\mu(K/k)-1) - \nu(K/k) \\ &= \sum_{i=0}^{\nu(K/k)} (N_i - 1) + \varphi_{K/k}(\mu(K/k)-1) + 1, \end{aligned}$$

where $e = N_0$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. According to Hilbert's formula, the $\mathfrak{P}$-exponent of $\mathfrak{D}(K/k)$ is given by $\sum_{i=0}^{\nu(K/k)}(N_i - 1)$. This completes the proof.

LEMMA 3. *Let $L \supset K \supset k$ be a tower of Galois extensions. Then:*

(i) $\mu(K/k) \leqq \mu(L/k)$.

(ii) *If $\mu(L/K) \leqq \varphi_{K/k}(\mu(K/k) + m - 1) + 1$ with $m \geqq 0$, then $\mu(L/k) \leqq \mu(K/k) + m$.*

Proof. From $V^{(\varphi_{L/k}(\mu(L/k)-1)+1)}_{L/k} = 1$, we have $V^{(\varphi_{K/k}(\mu(L/k)-1)+1)}_{K/k} = 1$ by Herbrand's theorem on ramification groups (see Serre [17]).

(ii) Let $i_0 = \mu(K/k) + m$, then $i_0 \geqq \mu(K/k)$, $\varphi_{K/k}(i_0 - 1) + 1 \geqq \mu(L/K)$, and hence $V^{(\varphi_{L/k}(i_0-1)+1)}_{L/K} = 1$. By Herbrand's theorem, the image of $V^{(\varphi_{L/k}(i_0-1)+1)}_{L/k}$, under the natural homomorphism of $G(L/k)$ onto $G(K/k)$, is $V^{(\varphi_{K/k}(i_0-1)+1)}_{K/k} = 1$. This implies $V^{(\varphi_{L/k}(i_0-1)+1)}_{L/k} \subset G(L/K)$. Therefore $V^{(\varphi_{L/k}(i_0-1)+1)}_{L/k} = V^{(\varphi_{L/k}(i_0-1)+1)}_{L/K} = 1$.

LEMMA 4. *Let $L \supset K \supset k$ be a tower of Galois extensions, and suppose that L/K is Abelian. Then:*

(i) $\mu(L/K) \leqq \varphi_{K/k}(\mu(L/k) - 1) + 1$.

(ii) *If $\mu(L/k) \leqq \mu(K/k) + m$ with $m \geqq 0$, then $\mu(L/K) \leqq \varphi_{K/k}(\mu(K/k) + m - 1) + 1$.*

Proof. (i) From $V^{(\varphi_{L/k}(\mu(L/k)-1)+1)}_{L/k} = 1$, we have $V^{(\varphi_{L/k}(\mu/k)-1)+1)}_{L/K} = 1$.

Since L/K is Abelian, we have, by Hasse's formula (2),

$$\varphi_{L/K}(\mu(L/K) - 1) = \mathfrak{v}(L/K) \leqq \varphi_{L/k}(\mu(L/k) - 1) ,$$

and hence $\mu(L/K) \leqq \varphi_{K/k}(\mu(L/k) - 1) + 1$.

(ii) Immediate from (i).

LEMMA 5. *Let K/k be a finite Galois extension, and let k'/k be an Abelian extension. If $\mu(k'/k) \leqq m$, then $\mu(K \cdot k'/K) \leqq \varphi_{K/k}(m - 1) + 1$.*

Proof. Since k'/k is Abelian, we have, by Hasse's formulas (3) and (1), $N_{k'/k}U_{k'}^{(\varphi_{k'/k}(m-1)+1)} = U_k^{(m)} \supset N_{K/k}U_K^{(\varphi_{K/k}(m-1)+1)}$, and hence, by the translation theorem in local class field theory,

$$N_{K\cdot k'/K}(K \cdot k')^{\times} \supset U_K^{(\varphi_{K/k}(m-1)+1)} .$$

Since $K \cdot k'/K$ is also Abelian, this completes the proof.

LEMMA 6. *Let K/k be a finite Galois extension, then*

$$N_{K/k}U_K^{(\varphi_{K/k}(i-1)+1)} = U_k^{(i)} \qquad \text{for } i \geqq \mu(K/k) .$$

Proof. The proof depends on the solubility of the local Galois group $G(K/k)$. Let $K_0 = k, K_1$ be the inertia field of K/k, and let $K_2 \subset \cdots \subset K_r = K$ be the distinct ramification fields of K/k. Then K_j/k is Galoisian, each K_{j+1}/K_j Abelian, and evidently, $\mathfrak{v}(K/K_j) = \mathfrak{v}(K/k)$ for $0 \leqq j < r$. Let $i \geqq \mu(K/k)$, then $\varphi_{K/k}(i - 1) \geqq \mathfrak{v}(K/k) = \mathfrak{v}(K/K_j)$. Since $\mathfrak{v}(K/K_j) \geqq \varphi_{K/K_{j+1}}(\mathfrak{v}(K_{j+1}/K_j))$ by Herbrand's theorem, we have

$$\varphi_{K_j/k}(i - 1) \geqq \varphi_{K_{j+1}/K_j}^{-1}(\mathfrak{v}(K_{j+1}/K_j)) = \mu(K_{j+1}/K_j) - 1 .$$

Thus, by Hasse's formula (3),

$$N_{K_{j+1}/K_j}U_{K_{j+1}}^{(\varphi_{K_{j+1}/k}(i-1)+1)} = U_{K_j}^{(\varphi_{K_j/k}(i-1)+1)}$$

for $j = 0, 1, \cdots, r - 1$. This shows $N_{K/k}U_K^{(\varphi_{K/k}(i-1)+1)} = U_k^{(i)}$.

For later use, we treat here the -1 dimensional cohomology group of $U_K^{(\varphi_{K/k}(i-1)+1)}$ with $i \geqq \mu(K/k)$, which appears in our main theorem.

The next exact sequence on cohomology groups was proved by Furuta [6].

PROPOSITION 7 (Furuta [6, Prop. 6]). *Let G be a finite group, H be a normal subgroup of G, and let A be a G-module. Then the sequence*

$$H^{-1}(H, A) \xrightarrow{\text{Inj}} H^{-1}(G, A) \xrightarrow{\tilde{N}_H} H^{-1}(G/H, N_H A) \longrightarrow 0$$

is exact, where Inj *denotes the injection map,* N_H *the trace map, namely,* $N_H(a) = \sum_{\sigma \in H} \sigma a$ *for an element* a *of* A, *and* $\tilde{N}_H$ *the corresponding induced map.*

LEMMA 8. *Let* K/k *be a finite Galois extension, and let* T *be the inertia field of* K/k. *If* K/T *is Abelian, then the sequence*

$$H^{-1}(G(K/T), U_K^{(\varphi_{K/k}(i-1)+1)}) \xrightarrow{\text{Inj}} H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) \longrightarrow 0$$

is exact for $i \geqq \mu(K/k)$. *In particular, if* $G(K/T)$ *is cyclic, then*

$$1^{\#} H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) = 0 \qquad \text{for } i \geqq \mu(K/k)\ ,$$

where $1 : U_K^{(\varphi_{K/k}(i-1)+1)} \to K^\times$ *denotes the inclusion map and* $1^{\#}$ *the induced cohomology map.*

Proof. Let $i \geqq \mu(K/k)$, then we have, by Lemma 4, $\mu(K/T) \leqq \varphi_{T/k}(i-1) + 1$. Since $\varphi_{T/k}(i-1) = i - 1$, we have, by Lemma 6, $N_{K/T} U_K^{(\varphi_{K/k}(i-1)+1)} = U_T^{(i)}$. It is known that $U_T^{(i)}$ is cohomologically trivial as a $G(T/k)$-module. Then Proposition 7 leads to the exact sequence in Lemma 8. The latter half follows from the following commutative diagram:

$$\begin{array}{ccc} H^{-1}(G(K/T), U_K^{(\varphi_{K/k}(i-1)+1)}) & \xrightarrow{\text{Inj}} & H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) \\ \downarrow 1^{\#} & & \downarrow 1^{\#} \\ 0 = H^{-1}(G(K/T), K^\times) & \xrightarrow{\text{Inj}} & H^{-1}(G(K/k), K^\times)\ . \end{array}$$

LEMMA 9. *If* K/k *is both totally and tamely ramified, then* $U_K^{(\varphi_{K/k}(i-1)+1)}$ *with* $i \geqq \mu(K/k)$ *is cohomologically trivial as a* $G(K/k)$*-module.*

Proof. In this case, $\mu(K/k) = 1$ and $\varphi_{K/k}(i) = ei$ for $i \geqq 0$, here $e = [K : k]$, the extension degree. For $i \geqq 1$, take $a \in U_K^{(\varphi_{K/k}(i-1)+1)} \cap k^\times$, then $\nu_\mathfrak{p}(a - 1) \geqq i - 1 + 1/e$, $\nu_\mathfrak{p}$ denoting the normalized exponential valuation of k, and hence $a \in U_k^{(i)}$. Thus

$$U_K^{(\varphi_{K/k}(i-1)+1)} \cap k^\times \subset U_k^{(i)} = N_{K/k} U_K^{(\varphi_{K/k}(i-1)+1)}$$

This implies $H^0(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) = 0$. On the other hand, it is well-

known that the Herbrand's quotient of $U_K^{(0)}$ is one, and hence the Herbrand's quotient of $U_K^{(\varphi_{K/k}(i-1)+1)}$ is also one. This completes the proof.

LEMMA 10. *Let K/k be a finite Galois extension. If the first ramification group of K/k is cyclic, then*

$$1^{\#}H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) = 0 \qquad \text{for } i \geqq \mu(K/k) .$$

Proof. Let T, V be the inertia field, the ramification field of K/k, respectively. Since $G(V/T)$ is cyclic, we have, by Lemmas 3 and 4,

$$\begin{aligned}\mu(V/T) &\leqq \varphi_{T/k}(\mu(V/k) - 1) + 1 \leqq \varphi_{T/k}(\mu(K/k) - 1) + 1 \\ &\leqq \varphi_{T/k}(i - 1) + 1 ,\end{aligned}$$

and hence, by Lemma 9, $H^{-1}(G(V/T), U_V^{(\varphi_{V/k}(i-1)+1)}) = 0$. Moreover it is known that $U_T^{(i)}$ with $i \geqq 0$ is cohomologically trivial as a $G(T/k)$-module. Therefore, according to Prop. 7, we have $H^{-1}(G(V/k), U_V^{(\varphi_{V/k}(i-1)+1)}) = 0$. Again, by Lemma 4,

$$\mu(K/V) \leqq \varphi_{V/k}(\mu(K/k) - 1) + 1 \leqq \varphi_{V/k}(i - 1) + 1 ,$$

and hence Prop. 7 leads to that

$$\mathrm{Inj} : H^{-1}(G(K/V), U_K^{(\varphi_{K/k}(i-1)+1)}) \to H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)})$$

is epimorphic. Then our assertion in Lemma 10 follows from the following commutative diagram:

$$\begin{array}{ccc} H^{-1}(G(K/V), U_K^{(\varphi_{K/k}(i-1)+1)}) & \xrightarrow{\mathrm{Inj}} & H^{-1}(G(K/k), U_K^{(\varphi_{K/k}(i-1)+1)}) \\ \downarrow 1^{\#} & & \downarrow 1^{\#} \\ 0 = H^{-1}(G(K/V), K^{\times}) & \xrightarrow{\mathrm{Inj}} & H^{-1}(G(K/k), K^{\times}) . \end{array}$$

We consider more special cases which correspond to the cases where $(m, 16) \neq 8$ and $(\mathfrak{f}(K/Q), 16) = 8$ in Theorem 3 of Fröhlich [1].

Let Q_2 be the 2-adic number field, T/Q_2 be a finite unramified extension, ζ_ν be a primitive 2^ν-th root of unity, and let $K_\nu = T(\zeta_\nu)$.

THEOREM 11. *Let $R = T(\zeta_\nu + \zeta_\nu^{-1})$, and let σ be a generator of the cyclic Galois group $G(R/T)$. Assume $\nu \geqq 3$. If $N_{R/T}\varepsilon = 1$ for $\varepsilon \in U_R^{(4)}$, then*

$$\varepsilon \in (N_{K_\nu/R}K_\nu^{\times})^{\sigma-1} .$$

The proof is elementary but slightly complicated. The details will appear elsewhere.

Ramification groups of R/T are as follows, where $V^{(i)} = V^{(i)}_{R/T}$.

order	ramification groups	number of $V^{(i)}$
$2^{\nu-2}$	$V^{(0)} = V^{(1)} = V^{(2)}$	3
$2^{\nu-3}$	$V^{(3)} = V^{(4)}$	2
$2^{\nu-4}$	$V^{(5)} = \cdots = V^{(8)}$	4
$\vdots$	$\vdots$	$\vdots$
$2^{\nu-k+1}$	$V^{(2^{k-3}+1)} = \cdots = V^{(2^{k-2})}$	2^{k-3}
$\vdots$	$\vdots$	$\vdots$
2	$V^{(2^{\nu-3}+1)} = \cdots = V^{(2^{\nu-2})}$	$2^{\nu-3}$
1	$V^{(2^{\nu-2}+1)}$	$(4 \leqq k \leqq \nu)$

Therefore $\mathfrak{f}(R/T) = 2^{\nu-2}$, and $\mu(R/T) = \nu$ by Hasse's formula (2).

LEMMA 12.

$$\varphi_{R/T}(i-1) = 2^{\nu-2}(i-\nu+1) \qquad \textit{for } i \geqq \nu\,.$$

Proof. Let $i \geqq \nu$. Then $\varphi(i-1) \geqq \varphi(\nu-1) = \mathfrak{f}(R/T)$. Hence

$$i = \sum_{j=0}^{\varphi(i-1)} N_j/N_0 = \nu + \sum_{j=2^{\nu-2}+1}^{\varphi(i-1)} 1/N_0 = \nu + \frac{1}{2^{\nu-2}}(\varphi(i-1) - 2^{\nu-2})\,,$$

here N_j denotes the order of $V^{(j)}_{R/T}$.

LEMMA 13. *If* $\nu \geqq 3$, *then*

$$1^{\#}H^{-1}(G(K_\nu/Q_2),\ U^{(\varphi_{K\nu/Q_2}(i-1)+1)}_{K_\nu}) = 0 \qquad \textit{for } i \geqq \mu(K_\nu/Q_2) = \nu,\ i \neq 3\,.$$

Proof. Let $i \geqq \mu(K_\nu/Q_2) = \nu$. We have the following commutative diagram in which the first row is exact by Lemma 8:

$$\begin{array}{ccccc} H^{-1}(G(K_\nu/T),\ U^{(\varphi_{K\nu/Q_2}(i-1)+1)}_{K_\nu}) & \xrightarrow{\text{Inj}} & H^{-1}(G(K_\nu/Q_2),\ U^{(\varphi_{K\nu/Q_2}(i-1)+1)}_{K_\nu}) & \longrightarrow & 0 \\ \Big\downarrow 1^{\#} & & \Big\downarrow 1^{\#} & & \\ H^{-1}(G(K_\nu/T),\ K_\nu^\times) & \xrightarrow{\text{Inj}} & H^{-1}(G(K_\nu/Q_2),\ K_\nu^\times)\,. & & \end{array}$$

Thus it is enough to show that the image of $1^{\#}$ of the left hand side is 0 when $i \neq 3$. By Lemma 12,

$$\begin{aligned} \varphi_{R/Q_2}(i-1)+1 &= \varphi_{R/T}(i-1)+1 \\ &= 2^{\nu-2}(i-\nu+1)+1 \geqq 2^{\nu-2}+1 \geqq 3 > 2 = \mu(K_\nu/R)\,, \end{aligned}$$

and hence, by Lemma 6,

$$N_{K_\nu/R}U_{K_\nu}^{(\varphi_{K_\nu/Q_2}(i-1)+1)} = U_R^{(\varphi_{R/Q_2}(i-1)+1)} .$$

Therefore we have the following commutative diagram in which the rows are exact by Prop. 7:

$$\begin{array}{ccccc} H^{-1}(G(K_\nu/T), U_{K_\nu}^{(\varphi_{K_\nu/Q_2}(i-1)+1)}) & \longrightarrow & H^{-1}(G(R/T), U_R^{(\varphi_{R/Q_2}(i-1)+1)}) & \longrightarrow & 0 \\ & \overset{1^\#}{\searrow} & \downarrow{\scriptstyle 1^\#} & & \\ 0 = H^{-1}(G(K_\nu/R), K_\nu^\times) & \to & H^{-1}(G(K_\nu/T), K_\nu^\times) & \to & H^{-1}(G(R/T), N_{K_\nu/R}K_\nu^\times) \to 0 . \end{array}$$

We know that $\varphi_{R/Q_2}(i-1)+1 = 3$ if and only if $i = \nu = 3$. Hence, if $i \geqq \nu$ and $i \neq 3$, then Theorem 11 shows that the image of $1^\#$ of the right hand side is 0, from which it follows that the image of $1^\#$ of the left hand side is also 0. This completes the proof.

Remark. If k is a field complete with respect to an archimedean prime divisor, then we define, as usual,

$$\mu(K/k) = \begin{cases} 1 & \text{when } k \text{ is real and } K \text{ imaginary,} \\ 0 & \text{otherwise.} \end{cases}$$

Artin's conductors. Let K/k be a finite Galois extension with the Galois group $G = G(K/k)$, and let χ be a character of G. Artin defined the conductor of χ whose $\mathfrak{p}$-exponent is given by

$$\nu(\chi) = \sum_{i=0}^{\infty} \frac{N_i}{N_0}(\chi(1) - \chi(V_{K/k}^{(i)})) ,$$

where $N_i = \mathrm{Card}\,(V_{K/k}^{(i)})$ and $\chi(V_{K/k}^{(i)}) = N_i^{-1}\sum_{\sigma\in V_{K/k}^{(i)}}\chi(\sigma)$ is the "mean value" of χ on $V_{K/k}^{(i)}$.

It is known that if χ is of degree one and Z_χ the subfield of K corresponding to $\mathrm{Ker}\,\chi$, then $\nu(\chi)$ is equal to the $\mathfrak{p}$-exponent of the conductor of Z_χ/k as a cyclic extension:

$$\nu(\chi) = \mu(Z_\chi/k) .$$

In connection with the above result, we have, in general,

PROPOSITION 14. *Let χ be the character of a representation A of G, and let Z_χ be the subfield of K corresponding to* $\mathrm{Ker}\,A$. *Then*

$$\nu(\chi) \geqq \mu(Z_\chi/k) .$$

Proof. In virtue of Serre [17, p. 158, Prop. 4], we may assume that χ is faithful. Then $Z_\chi = K$. Since $\chi(V^{(i)}_{K/k})$ is the multiplicity of the unit character contained in the restriction of A on $V^{(i)}_{K/k}$, $\chi(1) = \chi(V^{(i)}_{K/k})$ if and only if $\operatorname{Ker}\chi \supset V^{(i)}_{K/k}$, and hence this is equivalent to $V^{(i)}_{K/k} = 1$, namely, $\mathfrak{r}(K/k) < i$. Thus $\nu(\chi) \geqq \sum_{i=0}^{\mathfrak{r}(K/k)} \frac{N_i}{N_0}$. On the other hand, since it is known that $\nu(\chi)$ is a non-negative integer, we have

$$\nu(\chi) = \sum_{i=0}^{\varphi_{K/k}(\nu(\chi)-1)} \frac{N_i}{N_0} .$$

Hence $\varphi_{K/k}(\nu(\chi) - 1) \geqq \mathfrak{r}(K/k)$, which shows $\nu(\chi) \geqq \mu(K/k)$.

We note that there exists an irreducible character χ of degree greater than one such that $\nu(\chi) > \mu(Z_\chi/k)$ by a suitable choice of K/k.

§ 2. The Galois conductor of a Galois extension of an algebraic number field

In this section, we define the Galois conductor of a Galois extension of an algebraic number field of finite degree.

From now on, k is always an algebraic number field of finite degree, and a completion at a prime divisor $\mathfrak{p}$ of k is denoted by $k_\mathfrak{p}$.

DEFINITION. (i) Let K/k be a finite Galois extension, $\mathfrak{p}$ be a prime divisor of k, and let $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in K. Then $\mu(K_\mathfrak{P}/k_\mathfrak{p})$ defined in § 1 does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$, and $\mu(K_\mathfrak{P}/k_\mathfrak{p}) = 0$ when $\mathfrak{p}$ is unramified in K. We set

$$\mathfrak{f}(K/k) = \prod_\mathfrak{p} \mathfrak{f}(K_\mathfrak{P}/k_\mathfrak{p}) = \prod_\mathfrak{p} \mathfrak{p}^{\mu(K_\mathfrak{P}/k_\mathfrak{p})} ,$$

where $\mathfrak{p}$ runs through all finite and infinite prime divisors of k, and we call this the *Galois conductor of* K/k.

(ii) Let K/k be a finite Galois extension, and let $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{i_\mathfrak{p}}$ be a module of k which may contain infinite prime divisors. Set

$$\mathfrak{g}_{K/k}(\mathfrak{m}) = \prod_\mathfrak{P} \mathfrak{P}^{\varphi_{K_\mathfrak{P}/k_\mathfrak{p}}(i_\mathfrak{p}-1)+1} ,$$

where $\mathfrak{p}$ denotes the restriction of $\mathfrak{P}$ on k and $\mathfrak{P}$ runs through all finite and infinite prime divisors of K. Since $i_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$, $\mathfrak{g}_{K/k}(\mathfrak{m})$ is really a module of K. Put $\mathfrak{F}(K/k) = \mathfrak{g}_{K/k}(\mathfrak{f}(K/k))$, and call it the

generalized Geschlechtermodul of K/k, which is equal to the ordinary one when K/k is Abelian. Furthermore, if K/k is an Abelian extension of prime power degree, then $\mathfrak{g}_{K/k}(\mathfrak{m})$ coincides with ${}_*\mathfrak{M}_{\Delta}(\tilde{\mathfrak{m}})$ in [1, p. 239].

We often omit the subscript of $\mathfrak{g}_{K/k}(\mathfrak{m})$ and write briefly $\mathfrak{g}(\mathfrak{m})$ or $\mathfrak{g}_K(\mathfrak{m})$.

LEMMA 15. *Let K/k be a finite Galois extension, and let $\mathfrak{m}$ be a module of k. Then $\mathfrak{g}_{K/k}(\mathfrak{m}\mathfrak{f}(K/k)) = \mathfrak{m}\mathfrak{F}(K/k)$.*

Proof. Let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{i_{\mathfrak{p}}}$. Then the $\mathfrak{P}$-exponent of the left hand side is $\varphi_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(i_{\mathfrak{p}} + \mu(K_{\mathfrak{P}}/k_{\mathfrak{p}}) - 1) + 1$, which is, by the definition of $\mu(K_{\mathfrak{P}}/k_{\mathfrak{p}})$, equal to $i_{\mathfrak{p}}e(\mathfrak{P}/\mathfrak{p}) + \varphi_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mu(K_{\mathfrak{P}}/k_{\mathfrak{p}}) - 1) + 1$, $e(\mathfrak{P}/\mathfrak{p})$ being the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, and hence this is the $\mathfrak{P}$-exponent of the right hand side.

LEMMA 16. *Let $L \supset K \supset k$ be a tower of Galois extensions, and let $\mathfrak{m}$ be a module of k. Then $\mathfrak{g}_{L/K}(\mathfrak{g}_{K/k}(\mathfrak{m})) = \mathfrak{g}_{L/k}(\mathfrak{m})$.*

Proof. Immediate from the fact that the Hasse's function is transitive.

Next, we express some Lemmas in § 1 in terms of $\mathfrak{f}(K/k)$ or $\mathfrak{g}_{K/k}(\mathfrak{m})$. By Lemma 1, we have

LEMMA 17. *Let K/k be a finite Galois extension. Then $\mathfrak{p}$ is ramified in K if and only if $\mathfrak{p} \mid \mathfrak{f}(K/k)$.*

Lemma 2 gives

PROPOSITION 18. *Let K/k be a finite Galois extension, and let $\mathfrak{D}(K/k)$ be the different of K/k. Then*

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

According to Lemmas 3, 4, and 5, we have the following three Lemmas.

LEMMA 19. *Let $L \supset K \supset k$ be a tower of Galois extensions, and let $\mathfrak{f}(K/k) \mid \mathfrak{m}$. Then:*

(i) $\mathfrak{f}(K/k) \mid \mathfrak{f}(L/k)$.

(ii) *If $\mathfrak{f}(L/K) \mid \mathfrak{g}_{K/k}(\mathfrak{m})$, then $\mathfrak{f}(L/k) \mid \mathfrak{m}$. In particular, if $\mathfrak{f}(L/K) \mid \mathfrak{F}(K/k)$, then $\mathfrak{f}(L/k) = \mathfrak{f}(K/k)$.*

LEMMA 20. *Let $L \supset K \supset k$ be a tower of Galois extensions, L/K*

be Abelian, and let $\mathfrak{f}(K/k) \mid \mathfrak{m}$. *Then*:

(i) $\mathfrak{f}(L/K) \mid \mathfrak{g}_{K/k}(\mathfrak{f}(L/k))$.

(ii) *If* $\mathfrak{f}(L/k) \mid \mathfrak{m}$, *then* $\mathfrak{f}(L/K) \mid \mathfrak{g}_{K/k}(\mathfrak{m})$. *In particular, if* $\mathfrak{f}(L/k) = \mathfrak{f}(K/k)$, *then* $\mathfrak{f}(L/K) \mid \mathfrak{F}(K/k)$.

LEMMA 21. *Let* K/k *be a finite Galois extension, and let* k'/k *be an Abelian extension. If* $\mathfrak{f}(k'/k) \mid \mathfrak{m}$, *then* $\mathfrak{f}(K \cdot k'/K) \mid \mathfrak{g}_{K/k}(\mathfrak{m})$.

For later use, we treat here subgroups of the group of total norm residues.

Let K/k be a finite Galois extension, $\mathfrak{m}$ be a module of k, and let $S(\mathfrak{m})$ be the group of all numbers a in k such that $a \equiv 1 \bmod \mathfrak{m}$, and $S(\mathfrak{g}_K(\mathfrak{m}))$ is similarly defined in K.

LEMMA 22. *Notation being as above, we have*

$$S(\mathfrak{g}_K(\mathfrak{m})) \cap k^\times \supset S(\mathfrak{m}) .$$

Proof. Let $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{i_\mathfrak{p}}$, $\mathfrak{P}$ be any prime factor of $\mathfrak{p}$ in K, and let $e(\mathfrak{P}/\mathfrak{p})$ be the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$. Take $a \in S(\mathfrak{m})$. Since $i_\mathfrak{p} e(\mathfrak{P}/\mathfrak{p}) \geqq \varphi_{K_\mathfrak{P}/k_\mathfrak{p}}(i_\mathfrak{p} - 1) + 1$, the $\mathfrak{P}$-exponent of $a - 1$ is equal to or more than $\varphi_{K_\mathfrak{P}/k_\mathfrak{p}}(i_\mathfrak{p} - 1) + 1$. This implies $a \in S(\mathfrak{g}_K(\mathfrak{m}))$.

Let K/k be a finite Galois extension, $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{i_\mathfrak{p}}$ be a module of k, and let H be the group of total norm residues of K/k. Denote by $H_\mathfrak{m}$ the group of all numbers a in H such that

$$a \in N_{K_\mathfrak{P}/k_\mathfrak{p}} U_{K_\mathfrak{P}}^{(\varphi_{K_\mathfrak{P}/k_\mathfrak{p}}(i_\mathfrak{p}-1)+1)} \qquad \text{for all } i_\mathfrak{p} > 0 .$$

In virtue of Hasse's formula (1), we note $H_\mathfrak{m} \subset S(\mathfrak{m})$.

LEMMA 23.

$$S(\mathfrak{g}_K(\mathfrak{m})) \cap k^\times \supset H_\mathfrak{m} .$$

Proof. By Lemma 22, the left hand side contains $S(\mathfrak{m})$.

LEMMA 24. *Let* K/k *be a finite Galois extension, and let* $\mathfrak{f}(K/k) \mid \mathfrak{m}$. *Then*

$$H \cap S(\mathfrak{m}) = H_\mathfrak{m} .$$

Proof. Take $a \in H \cap S(\mathfrak{m})$, then $a \equiv 1 \bmod \mathfrak{m}$. Thus $\mathfrak{f}(K/k) \mid \mathfrak{m}$ and Lemma 6 give our assertion.

§ 3. The central class field mod $\mathfrak{m}$

In this section, we define the central class field mod $\mathfrak{m}$ of a finite Galois extension, and prove our main theorem. The following notation will be used.

$S(\mathfrak{m}), S(\mathfrak{g}_K(\mathfrak{m})), H, H_{\mathfrak{m}}$ as given in § 2.

Z the ring of rational integers.

E_k the unit group of k.

$k(\mathfrak{m})$ the ray class field mod $\mathfrak{m}$ of k, $K(\mathfrak{g}_K(\mathfrak{m}))$ similarly defined in K.

(A) the principal ideal group induced from a number group A.

Let K/k be a finite Galois extension. Then:

$I_{\mathfrak{g}_K(\mathfrak{m})}$ the ideal group of K prime to (the finite part of) $\mathfrak{g}_K(\mathfrak{m})$.

$I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$ the subgroup of $I_{\mathfrak{g}_K(\mathfrak{m})}$ consisting of all ideals whose norms to k belong to $(S(\mathfrak{m}))$.

$I^D_{\mathfrak{g}_K(\mathfrak{m})}$ the subgroup of $I_{\mathfrak{g}_K(\mathfrak{m})}$ generated by all ideals $\mathfrak{a}^{\sigma-1}$ such that $\mathfrak{a} \in I_{\mathfrak{g}_K(\mathfrak{m})}$ and $\sigma \in G(K/k)$, in other words, D is the augmentation ideal of the group ring of $G(K/k)$ over Z.

LEMMA 25. *Let K/k be a finite Galois extension, $\mathfrak{m}$ be a module of k, and let $\mathfrak{f}(K/k) \mid \mathfrak{m}$. Then*

$$H^{-1}(G(K/k), I_{\mathfrak{g}_K(\mathfrak{m})}) = 0 .$$

This implies that for $\mathfrak{a} \in I_{\mathfrak{g}_K(\mathfrak{m})}$, $N_{K/k}\mathfrak{a} = 1$ if and only if $\mathfrak{a} \in I^D_{\mathfrak{g}_K(\mathfrak{m})}$.

Proof. Let S be the union of the infinite primes of K and the finite primes dividing $\mathfrak{g}_K(\mathfrak{m})$, J_K be the idele group of K, and let

$$J_S = \prod_{\mathfrak{P} \in S} K_{\mathfrak{P}}^{\times} \cdot \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}} ,$$

here $U_{\mathfrak{P}}$ is the unit group of $K_{\mathfrak{P}}$. Then we have the following exact sequence:

$$1 \longrightarrow J_S \xrightarrow{1} J_K \longrightarrow I_{\mathfrak{g}_K(\mathfrak{m})} \cdot \longrightarrow 1 .$$

This gives the following exact sequence of cohomology groups:

$$H^{-1}(G(K/k), J_S) \xrightarrow{1^{\#}_{-1}} H^{-1}(G(K/k), J_K) \longrightarrow H^{-1}(G(K/k), I_{\mathfrak{g}_K(\mathfrak{m})})$$
$$\longrightarrow H^0(G(K/k), J_S) \xrightarrow{1^{\#}_0} H^0(G(K/k), J_K) .$$

Using semi-local theory and the fact that $\mathfrak{P}$ is unramified over k when

$\mathfrak{P} \in S$, it is easy to see that

$$H^{-1}(G(K/k), J_S) \approx \sum_{\mathfrak{P} \in S} H^{-1}(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times}) \approx H^{-1}(G(K/k), J_K) ,$$

where $G_{\mathfrak{P}}$ denotes the decomposition group of $\mathfrak{P}$ over k and the sum runs over non-conjugate primes in S. Similarly,

$$H^0(G(K/k), J_S) \approx \sum_{\mathfrak{P} \in S} H^0(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times})$$

and

$$H^0(G(K/k), J_K) \approx \sum_{\mathfrak{P} \in S} H^0(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times}) + \sum_{\mathfrak{P} \notin S} H^0(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times}) .$$

Therefore we conclude that $1_{-1}^{\#}$ is isomorphic and $1_0^{\#}$ injective, which implies $H^{-1}(G(K/k), I_{\mathfrak{g}_K(\mathfrak{m})}) = 0$.

Let $L \supset K \supset k$ be a tower of Galois extensions. Then L is called a *central extension of* K/k if $G(L/K)$ is contained in the center of $G(L/k)$, and is called a *genus extension of* K/k if it is obtained from K composing an Abelian extension over k.

LEMMA 26. *Let* $\mathfrak{m}$ *be a module of* k, *and let* K/k *be a finite Galois extension with* $\mathfrak{f}(K/k) \mid \mathfrak{m}$. *If* L_1, L_2 *are central (resp. genus) extensions of* K/k *with* $\mathfrak{f}(L_i/k) \mid \mathfrak{m}$ *for* $i = 1, 2$, *then the composite field* L_1L_2 *is also a central (resp. genus) extension of* K/k *with* $\mathfrak{f}(L_1L_2/k) \mid \mathfrak{m}$.

Proof. By Lemma 20, we have $\mathfrak{f}(L_i/K) \mid \mathfrak{g}_K(\mathfrak{m})$, and hence $L_i \subset K(\mathfrak{g}_K(\mathfrak{m}))$. This shows $\mathfrak{f}(L_1L_2/K) \mid \mathfrak{g}_K(\mathfrak{m})$. Then our assertion follows from Lemma 19.

DEFINITION. Let K/k be a finite Galois extension with $\mathfrak{f}(K/k) \mid \mathfrak{m}$. Then we denote by $\hat{K}_{\mathfrak{m}}$ (resp. $K_{\mathfrak{m}}^*$) the maximal central (resp. genus) extension L of K/k with $\mathfrak{f}(L/k) \mid \mathfrak{m}$, which is equal to the maximal central (resp. genus) extension of K/k contained in the ray class field mod $\mathfrak{g}_K(\mathfrak{m})$ by Lemmas 19 and 20, and call it the *central class field* (resp. the *genus field*) mod $\mathfrak{m}$ *of* K/k.

LEMMA 27. *If* K/k *is a finite Galois extension with* $\mathfrak{f}(K/k) \mid \mathfrak{m}$, *then*

$$K_{\mathfrak{m}}^* = K \cdot k(\mathfrak{m})$$

and so

$$G(K_{\mathfrak{m}}^*/K) \approx N_{K/k} I_{\mathfrak{g}_K(\mathfrak{m})} / N_{K/k} I_{\mathfrak{g}_K(\mathfrak{m})} \cap (S(\mathfrak{m})) .$$

Proof. By Lemma 21, we have $\mathfrak{f}(K\cdot k(\mathfrak{m})/K)\,|\,\mathfrak{g}_K(\mathfrak{m})$, $K\cdot k(\mathfrak{m})\subset K(\mathfrak{g}_K(\mathfrak{m}))$, and hence $K\cdot k(\mathfrak{m})\subset K^*_{\mathfrak{m}}$. To prove the converse, let A be the maximal Abelian extension contained in $K(\mathfrak{g}_K(\mathfrak{m}))$, then $K^*_{\mathfrak{m}}=K\cdot A$. By Lemma 19, $\mathfrak{f}(K(\mathfrak{g}_K(\mathfrak{m}))/k)\,|\,\mathfrak{m}$, and hence $\mathfrak{f}(A/k)\,|\,\mathfrak{m}$. This shows $A\subset k(\mathfrak{m})$. The latter half follows from the "Abschliessungssatz" in class field theory:

$$\begin{aligned} G(K^*_{\mathfrak{m}}/K) &\approx G(k(\mathfrak{m})/K\cap k(\mathfrak{m}))\approx (S(\mathfrak{m}))\cdot N_{K/k}I_{\mathfrak{g}_K(\mathfrak{m})}/(S(\mathfrak{m}))\\ &\approx N_{K/k}I_{\mathfrak{g}_K(\mathfrak{m})}/N_{K/k}I_{\mathfrak{g}_K(\mathfrak{m})}\cap (S(\mathfrak{m}))\ .\end{aligned}$$

LEMMA 28. *If K/k is a finite Galois extension with $\mathfrak{f}(K/k)\,|\,\mathfrak{m}$, then*

$$\begin{aligned} G(\hat{K}_{\mathfrak{m}}/K^*_{\mathfrak{m}}) &\approx I_{\mathfrak{g}_K(\mathfrak{m}),K/k}/I^D_{\mathfrak{g}_K(\mathfrak{m})}\cdot(S(\mathfrak{g}_K(\mathfrak{m})))\\ &\approx (H\cap S(\mathfrak{m}))/(N_{K/k}S(\mathfrak{g}_K(\mathfrak{m})))\ .\end{aligned}$$

Proof. By Lemma 27 and the translation theorem in class field theory, $K^*_{\mathfrak{m}}$ corresponds to the ideal group $I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$ of K. Moreover it can be checked that $\hat{K}_{\mathfrak{m}}$ corresponds to the ideal group $I^D_{\mathfrak{g}_K(\mathfrak{m})}\cdot(S(\mathfrak{g}_K(\mathfrak{m})))$. This indicates the first isomorphism. To prove the second isomorphism, for $\mathfrak{a}\in I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$, set $N_{K/k}\mathfrak{a}=(a)$, $a\in S(\mathfrak{m})$. Then $a\in H$, since $\mathfrak{f}(K/k)\,|\,\mathfrak{m}$. Conversely, take $a\in H\cap S(\mathfrak{m})$. Since $\mathfrak{p}$ is unramified in K when $\mathfrak{p}\nmid\mathfrak{m}$, $\nu_{\mathfrak{p}}(a)$ is a multiple of the degree of $\mathfrak{p}$ in K, where $\nu_{\mathfrak{p}}$ denotes the normalized exponential valuation at $\mathfrak{p}$, and hence (a) is a norm from $I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$. Therefore $N_{K/k}$ is an epimorphism of $I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$ to $(H\cap S(\mathfrak{m}))$. Assume $N_{K/k}\mathfrak{a}\in(N_{K/k}S(\mathfrak{g}_K(\mathfrak{m})))$. Then there exists a number $\alpha\in S(\mathfrak{g}_K(\mathfrak{m}))$ such that $N_{K/k}\mathfrak{a}(\alpha)=1$. We have, by Lemma 25, $\mathfrak{a}\in I^D_{\mathfrak{g}_K(\mathfrak{m})}\cdot(S(\mathfrak{g}_K(\mathfrak{m})))$, and the proof is complete.

Furthermore we have

$$\begin{aligned} (H\cap S(\mathfrak{m}))/(N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))) &\approx H\cap S(\mathfrak{m})/[H\cap S(\mathfrak{m})\cap E_k]\cdot N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))\\ &\approx H\cap S(\mathfrak{m})/[S(\mathfrak{m})\cap E_k]\cdot N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))\\ &\approx \frac{H\cap S(\mathfrak{m})/N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))}{[S(\mathfrak{m})\cap E_k]\cdot N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))/N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))}\ ,\end{aligned}$$

and hence the sequence

$$\begin{aligned} 1\to E_k\cap S(\mathfrak{m})/E_k\cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))&\to H\cap S(\mathfrak{m})/N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))\\ &\to G(\hat{K}_{\mathfrak{m}}/K^*_{\mathfrak{m}})\to 1\end{aligned}$$

is exact, because $N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))\subset S(\mathfrak{m})$ by Hasse's formula (1).

Continuously we give a relationship between $H\cap S(\mathfrak{m})/N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))$ and the Schur multiplicator of $G=G(K/k)$. Let

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{i_\mathfrak{p}}, \quad \mathfrak{g}(\mathfrak{m}) = \prod_{\mathfrak{P}} \mathfrak{P}^{\mu_\mathfrak{P}}, \quad \mu_\mathfrak{P} = \varphi_{K_\mathfrak{P}/k_\mathfrak{p}}(i_\mathfrak{p} - 1) + 1,$$

J_K be the idele group of K, and let

$$J_K(\mathfrak{g}(\mathfrak{m})) = \prod_{\mathfrak{P}|\mathfrak{g}(\mathfrak{m})} U_\mathfrak{P}^{(\mu_\mathfrak{P})} \cdot \prod_{\mathfrak{P}\nmid\mathfrak{g}(\mathfrak{m})}' K_\mathfrak{P}^\times,$$

here we wrote $U_\mathfrak{P}^{(i)}$ instead of $U_{K_\mathfrak{P}}^{(i)}$ and $\prod'$ denotes the restricted direct product of $K_\mathfrak{P}^\times$ with respect to $U_\mathfrak{P}^{(0)}$. Then we have, by the approximation theorem, $J_K = K^\times \cdot J_K(\mathfrak{g}(\mathfrak{m}))$, and $S(\mathfrak{g}(\mathfrak{m})) = K^\times \cap J_K(\mathfrak{g}(\mathfrak{m}))$. Thus the sequence

$$1 \longrightarrow S(\mathfrak{g}(\mathfrak{m})) \xrightarrow{i} J_K(\mathfrak{g}(\mathfrak{m})) \xrightarrow{j} C_K \longrightarrow 1$$

is exact, where C_K is the idele class group of K. Passing to cohomology, we have the following exact sequence:

$$H^{-1}(G, J_K(\mathfrak{g}(\mathfrak{m}))) \xrightarrow{j^\#} H^{-1}(G, C_K)$$
$$\longrightarrow S(\mathfrak{g}(\mathfrak{m})) \cap k^\times / N_{K/k} S(\mathfrak{g}(\mathfrak{m})) \xrightarrow{i^\#} H^0(G, J_K(\mathfrak{g}(\mathfrak{m}))).$$

Using semi-local theory, we have

$$H^0(G, J_K(\mathfrak{g}(\mathfrak{m}))) \approx \sum_{\mathfrak{P}|\mathfrak{m}} H^0(G_\mathfrak{P}, U_\mathfrak{P}^{(\mu_\mathfrak{P})}) + \sum_{\mathfrak{P}\nmid\mathfrak{m}} H^0(G_\mathfrak{P}, K_\mathfrak{P}^\times),$$

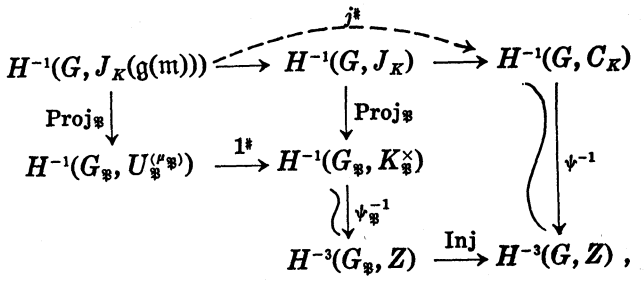
where $G_\mathfrak{P}$ is the decomposition group of $\mathfrak{P}$ over k and the sums run over non-conjugate primes in K. Therefore we obtain, by Lemmas 23 and 24,

$$\begin{aligned} \operatorname{Ker} i^\# &= S(\mathfrak{g}(\mathfrak{m})) \cap k^\times \cap H_\mathfrak{m}/N_{K/k} S(\mathfrak{g}(\mathfrak{m})) = H_\mathfrak{m}/N_{K/k} S(\mathfrak{g}(\mathfrak{m})) \\ &= H \cap S(\mathfrak{m})/N_{K/k} S(\mathfrak{g}(\mathfrak{m})). \end{aligned}$$

Similarly,

$$\begin{aligned} H^{-1}(G, J_K(\mathfrak{g}(\mathfrak{m}))) &\approx \sum_{\mathfrak{P}|\mathfrak{m}} H^{-1}(G_\mathfrak{P}, U_\mathfrak{P}^{(\mu_\mathfrak{P})}) + \sum_{\mathfrak{P}\nmid\mathfrak{m}} H^{-1}(G_\mathfrak{P}, K_\mathfrak{P}^\times) \\ &= \sum_{\mathfrak{P}|\mathfrak{m}} H^{-1}(G_\mathfrak{P}, U_\mathfrak{P}^{(\mu_\mathfrak{P})}). \end{aligned}$$

Denoting by $\mathrm{Proj}_\mathfrak{P}$ the projection of $H^{-1}(G, J_K(\mathfrak{g}(\mathfrak{m})))$ to $H^{-1}(G_\mathfrak{P}, U_\mathfrak{P}^{(\mu_\mathfrak{P})})$, we have the following commutative diagram:



where $1: U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})} \to K_{\mathfrak{P}}^{\times}$ denotes the inclusion map and $\psi, \psi_{\mathfrak{P}}$ are the Tate isomorphisms in class field theory. From this, we obtain

$$\mathrm{Im}\, j^{\#} = \psi\Big(\sum_{\mathfrak{P}|\mathfrak{m}} \mathrm{Inj}_{G_{\mathfrak{P}}/G} \psi_{\mathfrak{P}}^{-1} 1^{\#} H^{-1}(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})})\Big) .$$

Thus we have proved the following main

THEOREM 29. *Let* $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{i_{\mathfrak{p}}}$ *be a module of* k, *and let* K/k *be a finite Galois extension with* $\mathfrak{f}(K/k) | \mathfrak{m}$. *Denote by* $\hat{K}_{\mathfrak{m}}$ *the central class field* mod $\mathfrak{m}$ *and by* $K_{\mathfrak{m}}^{*}$ *the genus field* mod $\mathfrak{m}$ *of* K/k. *Then we have the following exact sequence*

$$1 \to E_k \cap S(\mathfrak{m})/E_k \cap N_{K/k} S(\mathfrak{g}_K(\mathfrak{m})) \\ \to H^{-3}(G(K/k), Z)/F(K/k)_{\mathfrak{m}} \to G(\hat{K}_{\mathfrak{m}}/K_{\mathfrak{m}}^{*}) \to 1 ,$$

where

$$F(K/k)_{\mathfrak{m}} = \sum_{\mathfrak{P}|\mathfrak{m}} \mathrm{Inj}_{G_{\mathfrak{P}}/G(K/k)} \psi_{\mathfrak{P}}^{-1} 1^{\#} H^{-1}(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})}) ,$$

$\mu_{\mathfrak{P}} = \varphi_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(i_{\mathfrak{p}} - 1) + 1$,
$U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})}$ *the* $\mu_{\mathfrak{P}}$*-th unit group of* $K_{\mathfrak{P}}$,
$G_{\mathfrak{P}}$ *the decomposition group of* $\mathfrak{P}$ *over* k,
$1^{\#}$ *the cohomology map induced from the inclusion map* $1: U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})} \to K_{\mathfrak{P}}^{\times}$,
$\psi_{\mathfrak{P}}$ *the Tate isomorphism of* $H^{-3}(G_{\mathfrak{P}}, Z)$ *to* $H^{-1}(G_{\mathfrak{P}}, K_{\mathfrak{P}}^{\times})$,

and the sum runs over non-conjugate prime factors of $\mathfrak{m}$ *in* K.

COROLLARY 30. *If* K/k *is a cyclic extension with* $\mathfrak{f}(K/k) | \mathfrak{m}$, *then we have*

$$H \cap S(\mathfrak{m}) = N_{K/k} S(\mathfrak{g}_K(\mathfrak{m}))$$

and

$$E_k \cap S(\mathfrak{m}) = E_k \cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))\ .$$

Lemma 10 gives

THEOREM 31. *Let K/k be a finite Galois extension with $\mathfrak{f}(K/k)|\mathfrak{m}$.*

(i) *If all first ramification groups of K/k are cyclic, then the sequence*

$$1 \to E_k \cap S(\mathfrak{m})/E_k \cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m})) \to H^{-3}(G(K/k), Z) \to G(\hat{K}_{\mathfrak{m}}/K^*_{\mathfrak{m}}) \to 1$$

is exact.

(ii) *If K/k is tamely ramified, then the above sequence is exact.*

(iii) *If K/k is unramified, then the above sequence is exact even if $\mathfrak{m} \neq 1$.*

From Lemmas 10 and 13, we obtain

THEOREM 32. *Let m be a positive integer such that $(m, 16) \neq 8$, and let K be the m-th cyclotomic field of the rational number field Q. Then*

$$G(\hat{K}_{mp_\infty}/K) \approx H^{-3}(G(K/Q), Z)\ ,$$

where p_∞ denotes the real prime divisor of Q.

This is a generalization of Fröhlich [1, Theorem 3] to a cyclotomic field of the rational number field.

Remark. (i) Hasse [8] proved the so-called principal genus theorem as follows: Let K/k be a cyclic extension with $\mathfrak{f}(K/k)|\mathfrak{m}$, and let σ be a generator of $G(K/k)$. If $N_{K/k}\mathfrak{a} \in (S(\mathfrak{m}))$, namely, $\mathfrak{a} \in I_{\mathfrak{g}_K(\mathfrak{m}),K/k}$, then there exists an ideal $\mathfrak{b}$ in $I_{\mathfrak{g}_K(\mathfrak{m})}$ such that $\mathfrak{a}\cdot\mathfrak{b}^{1-\sigma} \in (S(\mathfrak{g}_K(\mathfrak{m})))$, namely, $\mathfrak{a} \in I^D_{\mathfrak{g}_K(\mathfrak{m})}\cdot(S(\mathfrak{g}_K(\mathfrak{m})))$. Thus our main Theorem 29 combined with Lemma 28 may be viewed as a direct generalization of the principal genus theorem to a Galois extension. For other generalizations of this theorem, see Herbrand [10], Iyanaga [11], Kuniyoshi and Takahashi [12], Noether [14], and Terada [19], [20].

(ii) For a finite extension K/k, Fröhlich [2], [3] defined the genus field K^* of K/k to be the maximal unramified extension of K which is obtained from K by composing an Abelian extension of k, and studied the genus number $[K^*:K]$ in the case where the base field k is the

rational number field. Furuta [4] gave an explicit formula for the genus number in number fields. Masuda [13] treated an EL-Abelian and central extension of a Galois extension K/k, and expressed its Galois group over K in idele language. Using this result, Furuta [5] obtained an explicit formula for the central class number of K which is the extension degree of the maximal unramified central extension of K/k over K. Moreover Furuta [6] gave a cohomological expression of the Galois group of the maximal EL-Abelian and central extension contained in an Abelian extension M of K over the maximal genus extension contained in M, and determined the reduction formula for the central class field tower contained in an EL-Abelian extension of K/k. Fröhlich [1] studied fields of class two over the rational number field as in Introduction, and in its conclusion, he stated, "The methods used in this paper can be generalized, so as to become applicable to a study of fields at most (C2) over an arbitrary algebraic number field. But they become extremely cumbersome, and it is desirable to replace them by less elementary, but more powerful, tools."

§ 4. The ℓ-class field mod $\mathfrak{m}$

DEFINITION. Let ℓ be a rational prime, $\mathfrak{m}$ be a module of an algebraic field number field k of finite degree, and let K/k be a finite ℓ-extension with $\mathfrak{f}(K/k) \mid \mathfrak{m}$. Denote by $\hat{K}_{\mathfrak{m},\ell}$ (resp. $K^*_{\mathfrak{m},\ell}$) the maximal central (resp. genus) ℓ-extension L of K/k with $\mathfrak{f}(L/k) \mid \mathfrak{m}$, which is equal to the maximal central (resp. genus) ℓ-extension of K/k contained in the ray class field mod $\mathfrak{g}_K(\mathfrak{m})$ of K by Lemmas 19 and 20, and call it the *ℓ-class field* (resp. the *ℓ-genus field*) mod $\mathfrak{m}$ *of* K/k.

In the case where k is the rational number field and K/k an Abelian ℓ-extension, Fröhlich [1, Theorem 3] treated the Galois group of the ℓ-class field mod $\tilde{m}$ of K/k over the ℓ-genus field mod $\tilde{m}$. In this section, we generalize this result to the case where k is an arbitrary algebraic number field and K/k a finite ℓ-extension.

LEMMA 33. *Let K/k be a finite ℓ-extension with $\mathfrak{f}(K/k) \mid \mathfrak{m}$, and let $k(\mathfrak{m})_\ell$ be the maximal ℓ-extension contained in the ray class field $k(\mathfrak{m})$. Then*

$$K^*_{\mathfrak{m},\ell} = K \cdot k(\mathfrak{m})_\ell .$$

Proof. Similar to the proof of Lemma 27.

LEMMA 34. *Notation being as above, we have*

$$\hat{K}_{\mathfrak{m},\ell} \cap K^*_{\mathfrak{m}} = K^*_{\mathfrak{m},\ell} , \qquad \hat{K}_{\mathfrak{m},\ell} \cdot K^*_{\mathfrak{m}} = \hat{K}_{\mathfrak{m}} ,$$

and so

$$G(\hat{K}_{\mathfrak{m},\ell}/K^*_{\mathfrak{m},\ell}) \approx G(\hat{K}_{\mathfrak{m}}/K^*_{\mathfrak{m}}) .$$

Proof. By Lemmas 27 and 33, we have

$$K^*_{\mathfrak{m}} = K \cdot k(\mathfrak{m}) = K \cdot k(\mathfrak{m})_\ell \cdot k(\mathfrak{m}) = K^*_{\mathfrak{m},\ell} \cdot k(\mathfrak{m}) .$$

Thus $[K^*_{\mathfrak{m}} : K^*_{\mathfrak{m},\ell}]$ divides $[k(\mathfrak{m}) : k(\mathfrak{m})_\ell]$ and hence is prime to ℓ. Since $K^*_{\mathfrak{m}} \supset \hat{K}_{\mathfrak{m},\ell} \cap K^*_{\mathfrak{m}} \supset K^*_{\mathfrak{m},\ell}$, we have $\hat{K}_{\mathfrak{m},\ell} \cap K^*_{\mathfrak{m}} = K^*_{\mathfrak{m},\ell}$. Next, since $G(\hat{K}_{\mathfrak{m}}/K^*_{\mathfrak{m}})$ is a homomorphic image of the Schur multiplicator $H^{-3}(G(K/k), Z)$, $[\hat{K}_{\mathfrak{m}} : K^*_{\mathfrak{m}}]$ is some power of ℓ, and hence $[\hat{K}_{\mathfrak{m}} : \hat{K}_{\mathfrak{m},\ell} \cdot K^*_{\mathfrak{m}}]$ is so. On the other hand, since $[\hat{K}_{\mathfrak{m}} : \hat{K}_{\mathfrak{m},\ell}]$ is prime to ℓ, $[\hat{K}_{\mathfrak{m}} : \hat{K}_{\mathfrak{m},\ell} \cdot K^*_{\mathfrak{m}}]$ is also prime to ℓ. Thus $\hat{K}_{\mathfrak{m},\ell} \cdot K^*_{\mathfrak{m}} = \hat{K}_{\mathfrak{m}}$.

From the above Lemma and Theorem 29, we obtain

THEOREM 35. *Let K/k be a finite ℓ-extension with $\mathfrak{f}(K/k) \mid \mathfrak{m}$. Then the sequence*

$$\begin{aligned} 1 \to E_k \cap S(\mathfrak{m})/E_k \cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m})) \\ \to H^{-3}(G(K/k), Z)/F(K/k)_{\mathfrak{m}} \to G(\hat{K}_{\mathfrak{m},\ell}/K^*_{\mathfrak{m},\ell}) \to 1 \end{aligned}$$

is exact, where $F(K/k)_{\mathfrak{m}}$ is as in Theorem 29.

COROLLARY 36 (Fröhlich [1, Theorem 3]). *Let K be a finite Abelian ℓ-extension of the rational number field Q, and let m be a rational module such that $\mathfrak{f}(K/Q) \mid m$ and $(m, 16) \neq 8$ when $(\mathfrak{f}(K/Q), 16) = 8$. Then*

$$G(\hat{K}_{m,\ell}/K^*_{m,\ell}) \approx H^{-3}(G(K/Q), Z) .$$

Proof. When $\ell \neq 2$, all inertia groups of K are cyclic. Then Lemma 8 gives $F(K/Q)_m = 0$. When $\ell = 2$, Lemmas 8 and 13 show $F(K/Q)_m = 0$ under the hypotheses.

§ 5. The ℓ-class field tower mod $\mathfrak{m}$

Let $\mathfrak{m}$ be a module of an algebraic number field $k = K_0$ of finite degree, K_1 be the maximal ℓ-extension contained in the ray class field

$k(\mathfrak{m})$, and let K_n be the ℓ-class field mod $\mathfrak{m}$ of K_{n-1}/k. Then the sequence of fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n \subset \cdots$$

will be called the *ℓ-class field tower* mod $\mathfrak{m}$ *of* k. It is obvious that $\mathfrak{f}(K_n/k) \mid \mathfrak{m}$ for $n \geqq 0$. Conversely,

LEMMA 37. *Let $k_\ell^{(\mathfrak{m})} = \bigcup_{n=0}^{\infty} K_n$, and let K'/k be a finite ℓ-extension with $\mathfrak{f}(K'/k) \mid \mathfrak{m}$. Then $k_\ell^{(\mathfrak{m})} \supset K'$, in other words, $k_\ell^{(\mathfrak{m})}$ is the composite field of all finite ℓ-extensions over k whose Galois conductors divide $\mathfrak{m}$.*

Proof. Let $k = K_0' \subset K_1' \subset \cdots \subset K_r' = K'$ be the subfields corresponding to the lower central series of $G(K'/k)$. Clearly $K_1' \subset K_1$. Suppose $K_{i-1}' \subset K_{i-1}$. From $\mathfrak{f}(K_i'/k) \mid \mathfrak{m}$, we obtain $\mathfrak{f}(K_i'/K_{i-1}') \mid \mathfrak{g}_{K_{i-1}'}(\mathfrak{m})$ by Lemma 20. Since K_i'/K_{i-1}' is Abelian and $\mathfrak{g}_{K_{i-1}/K_{i-1}'}(\mathfrak{g}_{K_{i-1}'}(\mathfrak{m})) = \mathfrak{g}_{K_{i-1}}(\mathfrak{m})$, we have, by Lemma 21, $\mathfrak{f}(K_i' \cdot K_{i-1}/K_{i-1}) \mid \mathfrak{g}_{K_{i-1}}(\mathfrak{m})$. It can be easily checked that $G(K_i' \cdot K_{i-1}/K_{i-1})$ is contained in the center of $G(K_i' \cdot K_{i-1}/k)$. Therefore $K_i' \subset K_i' \cdot K_{i-1} \subset \widehat{(K_{i-1})}_{\mathfrak{m}} = K_i$, which completes the proof.

Continuously we generalize a famous result of Golod-Šafarevič [7] on the unramified ℓ-class field towers to the case of the tamely ramified ℓ-class field towers. The following notation will be used.

$d_\ell(M)$ the ℓ-rank of a module M.
$I_{\mathfrak{m}}$ the ideal group of k prime to $\mathfrak{m}$.
k' the number group of k prime to $\mathfrak{m}$.
V the subgroup of k' consisting of all numbers a such that $(a) \in I_{\mathfrak{m}}^\ell$, where ( ) denotes the principal ideal.
ρ the ℓ-rank of the ideal class group of k.
$r = r_1 + r_2 - 1$, where r_1 is the number of real and r_2 the number of complex prime divisors of k.
δ is equal to 1 if k contains an ℓ-th root of unity and to 0 if not.

LEMMA 38. $(k') \cap I_{\mathfrak{m}}^\ell \cdot (S(\mathfrak{m})) = (V \cdot S(\mathfrak{m}))$.

Proof. Immediate.

LEMMA 39. *Let $\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$, $N_{k/Q}\mathfrak{p}_i \equiv 1 \bmod \ell$ for $i = 1, \cdots, t$, and let K_1 be the maximal ℓ-extension contained in the ray class field $k(\mathfrak{m})$. Then*

$$d_\ell(G(K_1/k)) = t + \rho - d_\ell(V/V \cap k'^{\ell} \cdot S(\mathfrak{m})) .$$

In particular,

$$d_\ell(G(K_1/k)) \geqq t - (r + \delta) .$$

Proof. In the exact sequence

$$1 \to I_{\mathfrak{m}}^{\ell} \cdot (k')/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m})) \to I_{\mathfrak{m}}/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m})) \to I_{\mathfrak{m}}/I_{\mathfrak{m}}^{\ell} \cdot (k') \to 1 ,$$

all groups are elementary. Thus

$$\begin{aligned} d_\ell(G(K_1/k)) &= d_\ell(I_{\mathfrak{m}}/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m}))) = d_\ell(I_{\mathfrak{m}}/I_{\mathfrak{m}}^{\ell} \cdot (k')) + d_\ell(I_{\mathfrak{m}}^{\ell} \cdot (k')/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m}))) \\ &= \rho + d_\ell(I_{\mathfrak{m}}^{\ell} \cdot (k')/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m}))) . \end{aligned}$$

By Lemma 38, we have

$$\begin{aligned} I_{\mathfrak{m}}^{\ell} \cdot (k')/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m})) &= (k') \cdot I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m}))/I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m})) \\ &\approx (k')/(k') \cap I_{\mathfrak{m}}^{\ell} \cdot (S(\mathfrak{m})) = (k')/(V \cdot S(\mathfrak{m})) \approx k'/V \cdot S(\mathfrak{m}) \end{aligned}$$

and hence the exact sequence in which all groups are elementary:

$$1 \to V/V \cap k'^{\ell} \cdot S(\mathfrak{m}) \approx V \cdot S(\mathfrak{m})/k'^{\ell} \cdot S(\mathfrak{m}) \to k'/k'^{\ell} \cdot S(\mathfrak{m}) \to k'/V \cdot S(\mathfrak{m}) \to 1 .$$

Since $d_\ell(k'/k'^{\ell} \cdot S(\mathfrak{m}))$ is equal to the ℓ-rank of the group of prime residue classes mod $\mathfrak{m}$, we have

$$t = d_\ell(k'/V \cdot S(\mathfrak{m})) + d_\ell(V/V \cap k'^{\ell} \cdot S(\mathfrak{m}))$$

and hence

$$d_\ell(G(K_1/k)) = t + \rho - d_\ell(V/V \cap k'^{\ell} \cdot S(\mathfrak{m})) .$$

The latter half follows from $d_\ell(V/V \cap k'^{\ell} \cdot S(\mathfrak{m})) \leqq d_\ell(V/k'^{\ell}) = \rho + r + \delta$, for which see Šafarevič [16, p. 131].

THEOREM 40. *Let* $\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$, $N_{k/Q}\mathfrak{p}_i \equiv 1 \mod \ell$ *for* $i = 1, \cdots, t$. *If*

$$t + \rho \geqq d_\ell(V/V \cap k'^{\ell} \cdot S(\mathfrak{m})) + 2 + 2\sqrt{r + \delta + 1} ,$$

then the ℓ-class field tower $k_\ell^{(\mathfrak{m})}$ which is tamely ramified is infinite. In particular, if $t \geqq r + \delta + 2 + 2\sqrt{r + \delta + 1}$, then $k_\ell^{(\mathfrak{m})}$ is infinite.

Proof. In virtue of Lemma 1, K_n/k is tamely ramified. Thus we have, by Lemma 8 and Theorem 35, the exact sequence

$$1 \to E_k \cap S(\mathfrak{m})/E_k \cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))$$
$$\to H^{-3}(G(K_n/k), Z) \to G(K_{n+1}/K_n) \to 1 .$$

It is clear that

$$d_\ell(E_k \cap S(\mathfrak{m})/E_k \cap N_{K/k}S(\mathfrak{g}_K(\mathfrak{m}))) \leqq d_\ell(E_k \cap S(\mathfrak{m})) \leqq d_\ell(E_k) = r + \delta ,$$

and it is well-known that (see, Roquette [15])

$$d_\ell(H^{-3}(G(K_n/k), Z)) > \tfrac{1}{4}d^2 - d , \qquad \text{where } d = d_\ell(G(K_1/k)) .$$

By Lemma 39, $d \geqq 2 + 2\sqrt{r + \delta + 1}$, and hence $\frac{1}{4}d^2 - d \geqq r + \delta$. Therefore

$$|G(K_{n+1}/K_n)| \equiv 0 \mod \ell \qquad \text{for } n \geqq 0 ,$$

here $|\ |$ denotes the number of elements.

Remark. If $t = 0$, then $V = V \cap k'^{\ell}S(\mathfrak{m})$. Thus the condition in Theorem 40 coincides with Roquette [15, Remark to Theorem 3] in case of the unramified ℓ-class field towers.

§ 6. The central class field tower mod $\mathfrak{m}$

Let $\mathfrak{m}$ be a module of an algebraic number field $k = K_0$ of finite degree, $K_1 = k(\mathfrak{m})$ be the ray class field mod $\mathfrak{m}$ of k, and let K_n be the central class field mod $\mathfrak{m}$ of K_{n-1}/k. Then the sequence of fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n \subset \cdots$$

will be called the *central class field tower* mod $\mathfrak{m}$ *of* k. The extension degree $z_n = [K_{n+1} : K_n]$ will be called the *central class number* mod $\mathfrak{m}$ *of* K_n *over* k. It is obvious that $\mathfrak{f}(K_n/k) | \mathfrak{m}$ for $n \geqq 0$, and the same procedure as the proof of Lemma 37 yields

LEMMA 41. *Let* $k^{(\mathfrak{m})} = \bigcup_{n=0}^{\infty} K_n$, *and let* K'/k *be a finite nilpotent extension with* $\mathfrak{f}(K'/k) | \mathfrak{m}$. *Then* $k^{(\mathfrak{m})} \supset K'$, *in other words,* $k^{(\mathfrak{m})}$ *is the composite field of all finite nilpotent extensions over* k *whose Galois conductors divide* $\mathfrak{m}$.

Finally we generalize a result of our previous paper [18] to the case of the central class field tower mod $\mathfrak{m}$.

It follows from [18, Lemma 4] the following

LEMMA 42. *Let* G *be a finite nilpotent group of class* $n > 1$, *and let*

$$(4) \qquad G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = 1$$

be the lower central series of G. *Then*

$$|H^{-3}(G/G_{n-1}, Z)| \cdot |G_{n-1}|^{d(G/G_1)-1} \equiv 0 \mod |H^{-3}(G, Z)| ,$$

where $d(M)$ *denotes the rank of a module* M, *that is, the minimal number of generators of* M.

Now, let $k^{(\mathfrak{m})} = \bigcup_{n=0}^{\infty} K_n$ be the central class field tower mod $\mathfrak{m}$. We denote by G the Galois group of K_n over k. Suppose $z_{n-1} \neq 1$. Then G is a finite nilpotent group of class n, and the lower central series (4) of G corresponds to the sequence of fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n .$$

Thus $|G_{n-1}| = [K_n : K_{n-1}] = z_{n-1}$. By Theorem 29, we have

$$|H^{-3}(G, Z)| = z_n \cdot [E_k \cap S(\mathfrak{m}) : E_k \cap N_{K_n/k} S(\mathfrak{g}_{K_n}(\mathfrak{m}))] \cdot |F(K_n/k)_{\mathfrak{m}}|$$

and

$$|H^{-3}(G/G_{n-1}, Z)| = z_{n-1} \cdot [E_k \cap S(\mathfrak{m}) : E_k \cap N_{K_{n-1}/k} S(\mathfrak{g}_{K_{n-1}}(\mathfrak{m}))] \cdot |F(K_{n-1}/k)_{\mathfrak{m}}| .$$

Therefore, if $n > 1$, then we have, by Lemma 42,

$$z_{n-1}^{d(G/G_1)} \cdot |F(K_{n-1}/k)_{\mathfrak{m}}| \equiv 0 \mod z_n \cdot |F(K_n/k)_{\mathfrak{m}}| ,$$

where G/G_1 is isomorphic to the ideal class group mod $\mathfrak{m}$ of k.

Next, set $n = 1$. Then G is an Abelian group of order z_0. Hence it follows from [18, p. 392] that

$$z_0^{z_0(d(G)-1)} \equiv 0 \mod |H^{-3}(G, Z)| .$$

Therefore, by Theorem 29,

$$z_0^{z_0(d(G)-1)} \equiv 0 \mod z_1 \cdot |F(K_1/k)_{\mathfrak{m}}| .$$

Thus we have proved the following

THEOREM 43. *Let* z_n *be the central class number* mod $\mathfrak{m}$ *of* K_n *over* k, *and let* d *be the rank of the ideal class group* mod $\mathfrak{m}$ *of* k. *Then*

$$z_0^{z_0(d-1)d^{n-1}} \equiv 0 \mod z_n \quad \text{for } n \geqq 1 .$$

COROLLARY 44. *Let* $z_0 = \ell_1^{e_1} \cdots \ell_t^{e_t}$, $e_i > 0$ *for* $i = 1, \cdots, t$ *be the*

factorization of z_0 in Z. Then

$$k^{(\mathfrak{m})} = k_{\ell_1}^{(\mathfrak{m})} \cdots k_{\ell_t}^{(\mathfrak{m})} ,$$

where $k_{\ell_i}^{(\mathfrak{m})}$ is the ℓ_i-class field tower mod $\mathfrak{m}$ *of k in* § 5.

Proof. $\supset$: Immediate from Lemma 41.

$\subset$: Let $k^{(\mathfrak{m})} = \bigcup_{n=0}^{\infty} K_n$. According to Theorem 43, the distinct prime factors of $[K_n : k] = z_0 z_1 \cdots z_{n-1}$ are $\ell_1, \ell_2, \cdots, \ell_t$, and a finite nilpotent group is a direct product of all its Sylow subgroups. Thus we have, by Lemma 37, $K_n \subset k_{\ell_1}^{(\mathfrak{m})} \cdots k_{\ell_t}^{(\mathfrak{m})}$.

Furthermore by the same procedure as the proof of [18, Theorem 5], we obtain

THEOREM 45. *Notation being as above, we have*

$$d(G(K_{n+1}/K_n)) \leqq (d+1) \cdot d(G(K_n/K_{n-1})) + \sum_{\mathfrak{P}|\mathfrak{m}} d(1^{\#}H^{-1}(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu_{\mathfrak{P}})})) + r_1 + r_2 \qquad \textit{for } n > 1$$

and

$$d(G(K_2/K_1)) \leqq d \cdot z_0 \qquad \textit{for } n = 1 ,$$

where the sum runs over non-conjugate prime factors of $\mathfrak{m}$ in K.

REFERENCES

[1] A. Fröhlich, On fields of class two, Proc. London Math. Soc. (3), **4** (1954), 235–256.

[2] ——, The genus field and genus group in finite number fields, Mathematika, **6** (1959), 40–46.

[3] ——, The genus field and genus group in finite number fields, II, Mathematika, **6** (1959), 142–146.

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

[5] ——, Über die zentrale Klassenzahl eines relativ-galoisschen Zahlkörpers, J. Number Theory, **3** (1971), 318–322.

[6] ——, On nilpotent factors of congruent ideal class groups of Galois extensions, Nagoya Math. J., **62** (1976), 13–28.

[7] E. S. Golod and I. R. Šafarevič, On class field towers (Russian), Izv. Akad. Nauk. SSSR, **28**, 261–272. English translation in Amer. Math. Soc. Transl., (2), **48**, 91–102.

[8] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper Ia, Jahr. der Deutschen Math. Ver., **36** (1927).

[9] ——, Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, Journ. Fac. Sci. Tokyo Imp. Univ., **2** (1934), 477–498.

[10] J. Herbrand, Sur les théorèmes du genre principal et des idéaux principaux, Abh. a. d. Hamb. Math. Sem., **8** (1933), 84–92.

[11] S. Iyanaga, Zur Theorie der Geschlechtermoduln, J. reine angew. Math., **171** (1934), 12–18.
[12] H. Kuniyoshi and S. Takahashi, On the principal genus theorem, Tôhoku Math. J., (2), **5** (1953), 128–131.
[13] K. Masuda, An application of the generalized norm residue symbol, Proc. Amer. Math. Soc., **10** (1959), 245–252.
[14] E. Noether, Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper, Math. Ann., **108** (1933), 411–419.
[15] P. Roquette, On class field towers, Proc. instr. conf. at Brighton (Algebraic Number Theory), (1967), 231–249.
[16] I. R. Šafarevič, Extensions with given points of ramification (Russian), Inst. Hautes Etudes Sci. Publ. Math., **18** (1963), 71–95. English translation in Amer. Math. Soc. Transl., (2), **59**, 128–149.
[17] J. P. Serre, Local class field theory, Proc. instr. conf. at Brighton (Algebraic Number Theory), (1967), 128–161.
[18] S. Shirai, Central class numbers in central class field towers, Proc. Japan Acad., **51** (1975), 389–393.
[19] F. Terada, On the principal genus theorem concerning the abelian extensions, Tôhoku Math. J., (2), **4** (1952), 141–152.
[20] ——, A note on the principal genus theorem, Tôhoku Math. J., (2), **5** (1953), 211–213.

Toyama Medical and Pharmaceutical University