Japan. J. Math.
Vol. 20, No. 2, 1994

The Hasse norm principle modulo $\mathfrak{m}$ of finite Galois extensions of algebraic number fields and a generalization of a theorem of Fröhlich on the ℓ-divisibility of the class numbers of ℓ-abelian fields*

By Teruo TAKEUCHI

(Received September 29, 1992)
(Revised May 31, 1993)

Introduction

Let ℓ be a prime number. About forty years ago A. Fröhlich [1] determined the Galois group of the narrow central field of an abelian ℓ-extension over $\mathbf{Q}$ which coincides with it's narrow genus field, by generators and relations. As an application of this result he [2] also determined the abelian ℓ-extensions over $\mathbf{Q}$ whose narrow class numbers are prime to ℓ. These results appear in his recent book [3] in a more modern fashion. Recently S. V. Ullom and S. B. Watt [19] determined the abelian ℓ-extensions over imaginary quadratic fields whose class numbers are prime to ℓ, which is considered as a generalization of the Fröhlich's result. The proof by Ullom and Watt is based on properties of number knots, and is more direct than that of Fröhlich.

The purpose of this paper is to generalize the argument used by Ullom and Watt to that over an arbitrary algebraic number field of finite degree. Since the Fröhlich's results depend essentially on the triviality of units of base fields, it is no longer possible to generalize the results as they are. We treat this problem as the Ray class number problem modulo suitable $\mathfrak{m}$. Since the narrow class number is the Ray class number modulo infinite primes, this approach may be a natural one. For this purpose we study the genus theory and central extensions modulo $\mathfrak{m}$ somewhat generally from our point of view.

Section 1 studies the genus group modulo $\mathfrak{m}$ generally. The purpose of this section is to prove Theorem 1.1. This is a rank formula for the genus group modulo $\mathfrak{m}$ from which the ordinary genus number formula is obtained as a corollary.

Section 2 concerns with a theorem of Leopoldt on the genus theory over $\mathbf{Q}$.

*This research was partially supported by Grant-in-Aid for Scientific Research (03640026), Ministry of Education, Science and Culture.

This theorem of Leopoldt asserts that the narrow genus field of an abelian extension of $\mathbf{Q}$ is a composite field of abelian fields with prime power conductors. Since the Fröhlich's result is based on this theorem, we need to provide a similar result over an algebraic number field of finite degree. Theorem 2.1 gives a generalization of the result of Leopoldt using a modulus $\mathfrak{m}$ which satisfies suitable conditions. Theorem 2.2 assures the existence of such an $\mathfrak{m}$.

Section 3 is devoted to central extensions modulo $\mathfrak{m}$. The goal of this section is Theorem 3.3. Ullom and Watt [19] used some properties on number knots as a key fact. Theorem 3.3 provides a key fact to our case with certain modulus $\mathfrak{m}$.

The final section 4 deals with the Hasse norm principle modulo $\mathfrak{m}$ and a generalization of the Fröhlich's result. From a general viewpoint the result of Ullom and Watt is naturally considered as a result on the Hasse norm principle rather than that on ℓ-divisibility of the class numbers. From Theorem 3.3 we first deduce Theorem 4.1, which states a condition for the Hasse norm principle modulo $\mathfrak{m}$ to hold for fields of certain type. Using Theorem 4.1 with the results of Section 2 we finally prove the main theorem of this paper, Theorem 4.2, which gives a desired generalization of the Fröhlich's result over an algebraic number field.

1. The Genus group modulo $\mathfrak{m}$

In this section we study the genus group modulo $\mathfrak{m}$. The main result is Theorem 1.1. This gives a rank formula for the genus group from which the ordinary genus number formula follows as a corollary. This generalizes the result of [14] for the genus group modulo $\mathfrak{m}$, and also gives a refinement of results of Horie [11] from our view point.

1.1. Preliminaries from local fields. Let $\mathfrak{p}$ be a prime of an algebraic number field. Let k be the completion of the field with respect to $\mathfrak{p}$. We first consider the case where $\mathfrak{p}$ is finite. Let K/k be a Galois extension of finite degree and let K'/k denote the maximal abelian subextension of K/k. Let $\mathfrak{P}$ (resp. $\mathfrak{P}'$) be the prime divisor of $\mathfrak{p}$ in K (resp. in K'). Using the Hasse's function ψ of $\mathfrak{P}$ with respect to K/k, we define a function $v_{K/k}$ by

$$v_{K/k}(x) = \psi(x-1)+1. \tag{D1.1}$$

Hence in particular, we have $v_{K/k}(0) = 0$ and $v_{K/k}(1) = 1$. (For the properties of the Hasse's function, we refer to Iyanaga [12] and Serre [17].) Furthermore from the convexity of the Hasse's function we also have

$$v_{K/k}(x) \leqq \psi(x). \tag{1.1}$$

Moreover from the transitivity of the Hasse's functions, the transitivity of $v_{K/k}$ follows, i.e., for a tower of Galois extensions $k \subset L \subset K$ we see

$$v_{K/k} = v_{K/L} \circ v_{L/k}. \tag{1.2}$$

In what follows for simplicity we also use the notation $v(x)$, $v'(x)$, $v''(x)$ instead of $v_{K/k}(x)$, $v_{K'/k}(x)$, $v_{K/K'}(x)$, respectively.

Let $\mathfrak{m} = \mathfrak{p}^e$ be a modulus of k, i.e., a finite product of $\mathfrak{p}$. Then we define the lifting modulus $\mathfrak{m}^*_{K/k}$ of $\mathfrak{m}$ from k to K by

$$\mathfrak{m}^* = \mathfrak{m}^*_{K/k} = \mathfrak{P}^{v(e)}. \tag{D1.2}$$

Since v is transitive, this lifting is also transitive, namely, for a tower of Galois extensions $k \subset L \subset K$ we have

$$\mathfrak{m}^*_{K/k} = (\mathfrak{m}^*_{L/k})^*_{K/L}. \tag{1.3}$$

Let

$$U(K) = U(K)^{(0)} \tag{D1.3}$$

denote the group of units of K, and for $j \geqq 1$ put

$$U(K)^{(j)} = \{x \in U(K) \mid x \equiv 1 \mod \mathfrak{P}^j\}. \tag{D1.4}$$

Then we have

$$N_{K/k}(U(K)^{(v(e))}) \subset U(k)^{(e)}, \tag{1.4}$$

$$N_{K/k}(U(K)) = N_{K/k}(K^\times) \cap U(k), \tag{1.5}$$

$$N_{K/k}(U(K)^{(1)}) = N_{K/k}(K^\times) \cap U(k)^{(1)}, \tag{1.6}$$

$$N_{K'/k}(U(K')^{(v'(e))}) = N_{K'/k}(K'^\times) \cap U(k)^{(e)}. \tag{1.7}$$

$$U(k)^{(e)}/N_{K'/k}(U(K')^{(v'(e))}) \cong V'(v'(e)), \tag{1.8}$$

where $V'(j)$ denotes the j-th ramification group of $\mathfrak{P}'$ with respect to K'/k, i.e.,

$$V'(j) = \{\sigma \in \mathrm{Gal}\,(K'/k) \mid \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}'^{j+1} \quad \text{for all } \alpha \in \mathfrak{O}'\},$$

where $\mathfrak{O}'$ denotes the valuation ring of K'.

Indeed, (1.4), (1.5), (1.7), and (1.8) are well known (e.g., see [12] and [17]). Furthermore (1.6) follows from (1.5) and the fact $U(K)^{(0)} = W \cdot U(K)^{(1)}$ (direct), where W denotes the group of those roots of unity in K whose orders divide $N(\mathfrak{P}) - 1$.

Now we make the following assumption:

$$N_{K/k}(U(K)^{(v(e))}) = N_{K/k}(K^\times) \cap U(k)^{(e)}. \tag{A1.1}$$

Under the assumption (A1.1) we obtain from (1.7)

$$N_{K/k}(U(K)^{(v(e))}) = N_{K'/k}(K'^{\times}) \cap U(k)^{(e)} \tag{1.9}$$

because $N_{K/k}(K^{\times}) = N_{K'/k}(K'^{\times})$; therefore from (1.8) we also have

$$U(k)^{(e)}/N_{K/k}(U(K)^{(v(e))}) \cong V'(v'(e)). \tag{1.10}$$

The following lemma gives sufficient conditions of the assumption (A1.1).

LEMMA 1.1. *Each one of the following conditions* (1), (2), (3), *and* (4) *implies* (A1.1).

(1) $v'(e) \geqq \min\{j \mid V''(v''(j)) = \{1\}\}$, *where* $V''(i)$ *denotes the* i*-th ramification group of* $\mathfrak{P}$ *with respect to* K/K'.

(2) K/k *is an abelian extension.*

(3) $e = 0$ *or* 1.

(4) K/k *is tamely ramified or unramified.*

PROOF. (1) Let K_0 be the inertia field of K/K' with respect to $\mathfrak{P}$, and K_i the i-th ramification field of K/K' for $i = 1, 2, \cdots$. Then each K_i/K_{i-1} is an abelian extension and $K_r = K$ for some integer r. Let $v_i' = v_{K_i/K'}$ and $v_i = v_{K/K_i}$ be the functions defined by (D1.1). Take an integer j_0 such that

$$j_0 \geqq \min\{j \mid V''(v''(j)) = \{1\}\}. \tag{1.11}$$

Now the Herbrand's theorem asserts that the $v_i'(j_0)$-th ramification group of K_i/K_{i-1} is $V''(v''(j_0))V''(i)/V''(i)$. However by the choice of j_0 in (1.11), this group is trivial. Hence by [17, Chap. V, Cor. 3 of Proposition 9] we have

$$N_{K_i/K_{i-1}}(U(K_i)^{(v_i'(j_0))}) = U(K_{i-1})^{(v_{i-1}'(j_0))}$$

for $i = 1$ to r, and therefore

$$N_{K/K_0}(U(K)^{(v''(j_0))}) = U(K_0)^{(v_0'(j_0))}.$$

On the other hand, clearly

$$N_{K_0/K'}(U(K_0)^{(v_0'(j_0))}) = U(K')^{(j_0)}$$

because K_0/K' is unramified. Hence

$$N_{K/K'}(U(K)^{(v''(j_0))}) = U(K')^{(j_0)}.$$

In particular, for the case $j_0 = v'(e)$, we have

$$N_{K/K'}(U(K)^{(v(e))}) = U(K')^{(v'(e))}.$$

Thus using (1.7) we see

$$\begin{aligned} N_{K/k}(U(K)^{(v(e))}) &= N_{K'/k}(K'^{\times}) \cap U(k)^{(e)} \\ &= N_{K/k}(K^{\times}) \cap U(k)^{(e)}. \end{aligned}$$

This proves that (1) implies (A1.1).

The assertion about (2) is trivial by (1.7). For (3) the assertion follows from (1.5) and (1.6). Finally, assume that (4) is satisfied. Then K/K' is also tamely ramified or unramified, so that $V''(v''(1)) = \{1\}$. Hence if $e \geqq 1$ then the assertion follows from (1), and if $e = 0$ then the assertion follows from (3). This completes the proof.

We next consider the the case where $\mathfrak{p}$ is infinite. If $\mathfrak{p}$ is infinite, then a modulus $\mathfrak{m}$ of k means a product $\mathfrak{p}^e$ with $e = 0$ or 1. Furthermore we define the function v by $v(e) = e$ for $e = 0, 1$. Then the lifting modulus $\mathfrak{m}^*$ of $\mathfrak{m} = \mathfrak{p}^e$ is defined as $\mathfrak{P}^{v(e)}$. Finally we set $V(0) =$ inertia group, $V(1) = \{1\}$, $U(k)^{(0)} = k^{\times}$, and $U(k)^{(1)} = k^{\times}$ or the group of positives of k according as $\mathfrak{p}$ is complex or real. Under these interpretations, all of (1.2) $\sim$ (1.10) clearly hold.

1.2. The Genus fields modulo $\mathfrak{m}$. Hereafter in this paper we deal with global number fields. Let k be an algebraic number field of finite degree. Let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ be a modulus of k, i.e., a finite product of primes $\mathfrak{p}$ of k such that $e(\mathfrak{p}) \geqq 0$ in the case when $\mathfrak{p}$ is finite, and $e(\mathfrak{p}) = 0$ or 1 in the case when $\mathfrak{p}$ is infinite. Denote the $\mathfrak{p}$-component of $\mathfrak{m}$ by $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}^{e(\mathfrak{p})}$ and call $e(\mathfrak{p})$ the $\mathfrak{p}$-exponent of $\mathfrak{m}$. Let K/k be a finite Galois extension. For a prime $\mathfrak{p}$ of k and for a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ of K, let $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$ denote the completions of K and of k by $\mathfrak{P}$ and by $\mathfrak{p}$, respectively. Let $\mathfrak{m}^*_{\mathfrak{P}}$ be the lifting modulus of $\mathfrak{m}_{\mathfrak{p}}$ from $k_{\mathfrak{p}}$ to $K_{\mathfrak{P}}$ defined locally in (D1.2). Then the global lifting modulus of $\mathfrak{m}$ from k to K is defined by

$$\mathfrak{m}^* = \prod_{e(\mathfrak{p})>0} \mathfrak{m}^*_{\mathfrak{P}}, \tag{D1.5}$$

where the product is taken over all of prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in K for all of primes $\mathfrak{p}$ of k with $e(p) > 0$. Then $\mathfrak{m}^*$ is a Galois modulus, i.e., for $\sigma \in \mathrm{Gal}\,(K/k)$ we have

$$\mathfrak{m}^{*\sigma} = \mathfrak{m}^*. \tag{1.12}$$

Using this $\mathfrak{m}^*$, we define the genus field of K/k modulo $\mathfrak{m}$.

Definition 1.1. Let $K'(\mathfrak{m})$ be the maximal abelian extension of k contained in the ray class field over K modulo $\mathfrak{m}^*$. Then we call $K \cdot K'(\mathfrak{m})$ the genus field $K^*(\mathfrak{m})$ of K/k modulo $\mathfrak{m}$, $\mathrm{Gal}\,(K^*(\mathfrak{m})/K)$ the genus group of K/k modulo $\mathfrak{m}$, and $[K^*(\mathfrak{m}) : K]$ the genus number of K/k modulo $\mathfrak{m}$, respectively.

This definition is due to S. Shirai [18].

Let J_k denote the idele group of k. For a modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ of k, we put

$$W_{k\mathfrak{m}} = \prod_{e(\mathfrak{p})>0} U(k_{\mathfrak{p}})^{(e(\mathfrak{p}))} \cdot \prod_{e(\mathfrak{p})=0} U(k_{\mathfrak{p}}) \tag{D1.6}$$

and

$$J_{k\mathfrak{m}} = \prod_{e(\mathfrak{p})>0} U(k_{\mathfrak{p}})^{(e(\mathfrak{p}))} \cdot \prod_{e(\mathfrak{p})=0}' k_{\mathfrak{p}}^{\times}, \tag{D1.7}$$

where $\prod'$ denotes the restricted product. Using these notations we can describe the class group of $K'(\mathfrak{m})$ over k. We start with the following lemma, which is well known; we omit the proof of it (for the proof, e.g., see Y. Furuta [4]).

LEMMA 1.2. *Let the notation be as above. Then $K'(\mathfrak{m})$ is the class field over k corresponding to*

$$J_k/k^{\times} N_{K/k}(W_{K\mathfrak{m}^*}),$$

where $\mathfrak{m}^*$ denotes the lifting modulus of $\mathfrak{m}$ from k to K.

Let $k_{(\mathfrak{m})}$ denote the ray number group modulo $\mathfrak{m}$ of k, i.e.,

$$k_{(\mathfrak{m})} = \{x \in k^{\times} \mid x \equiv 1 \mod \mathfrak{m}\}. \tag{D1.8}$$

Then by the approximation theorem we know $J_k \subset k^{\times} J_{k\mathfrak{m}}$, and thus

$$J_k/k^{\times} N_{K/k}(W_{k\mathfrak{m}^*}) \cong J_{k\mathfrak{m}}/k_{(\mathfrak{m})} N_{K/k}(W_{K\mathfrak{m}^*}). \tag{1.13}$$

We often use the expression on the right hand side hereafter rather than the one on the left.

The group structure of the genus group is determined by its ℓ-parts for each prime number ℓ. Therefore we study the structure of the ℓ-part of the genus group.

Let ℓ be a fixed prime number. For a finite abelian group A written multiplicatively, let $\operatorname{rank}_i(A)$ denote the ℓ^i-rank of A, i.e., the $\mathbb{F}_\ell$-dimension of $A^{\ell^{i-1}}/A^{\ell^i}$. For ℓ^i-rank we have the following:

LEMMA 1.3. *Let*

$$1 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 1$$

be an exact sequence of finite abelian groups ($N \subset M$). For an integer $i \geqq 0$, put $N_i = N \cap M^{\ell^i}$. Then

$$\begin{aligned}\operatorname{rank}_i(M) &= \operatorname{rank}_i(L) + \operatorname{rank}_1(N_{i-1}/N_i)\\ &= \operatorname{rank}_i(L) + \log_\ell\{\#(N_{i-1}/N_i)\}.\end{aligned}$$

PROOF. By the definition of ℓ^i-rank , we see $\operatorname{rank}_i(L) = \operatorname{rank}_1(L^{\ell^{i-1}}/L^{\ell^i}) = \operatorname{rank}_1(M^{\ell^{i-1}}N/M^{\ell^i}N)$. We also have

$$\begin{aligned}\#(M^{\ell^{i-1}}N/M^{\ell^i}N) &= \#(M^{\ell^{i-1}}/M^{\ell^{i-1}} \cap N)/\#(M^{\ell^i}/M^{\ell^i} \cap N)\\ &= \#(M^{\ell^{i-1}}/M^{\ell^i})/\#(N_{i-1}/N_i).\end{aligned}$$

Since N_{i-1}/N_i is an elementary abelian ℓ-group, this proves the lemma.

To apply the above lemma we need some notations. For each non negative integer i, put

$$\mathcal{N}_i = W_{k\mathfrak{m}}^{\ell^i} N_{K/k}(W_{K\mathfrak{m}^*}) \tag{D1.9}$$

and

$$\mathcal{F}_i = W_{k\mathfrak{m}} \cap J_{k\mathfrak{m}}^{\ell^i} k_{(\mathfrak{m})}. \tag{D1.10}$$

PROPOSITION 1.1. *Let the notation be as above. Then for each positive integer i we have*

$$\begin{aligned}\operatorname{rank}_i(\operatorname{Gal}(K'(\mathfrak{m})/k)) = {} & \operatorname{rank}_i(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}})\\ & + \operatorname{rank}_i(W_{k\mathfrak{m}}/N_{K/k}(W_{K\mathfrak{m}^*}))\\ & + \log_\ell\left\{\frac{\#(\mathcal{F}_{i-1}/(\mathcal{F}_{i-1}\cap\mathcal{N}_{i-1}))}{\#(\mathcal{F}_i/(\mathcal{F}_i\cap\mathcal{N}_i))}\right\}.\end{aligned}$$

PROOF. We apply Lemma 1.3 to the exact sequence

$$\begin{aligned}1 \longrightarrow k_{(\mathfrak{m})}W_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*}) \longrightarrow\\ J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{k\mathfrak{m}^*}) \longrightarrow J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}} \longrightarrow 1.\end{aligned}$$

Let N_i be as in Lemma 1.3, i.e.,

$$\begin{aligned}N_i = {} & (k_{(\mathfrak{m})}W_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*}))\\ & \cap (J_{k\mathfrak{m}}^{\ell^i}k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})).\end{aligned}$$

Then from the definition of $\mathcal{F}_i$ it follows that

$$N_i \cong \mathcal{F}_i N_{K/k}(W_{K\mathfrak{m}^*})/E_{k(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*}), \tag{1.14}$$

where $E_{k(\mathfrak{m})}$ denotes the ray subgroup of units E_k of k modulo $\mathfrak{m}$, i.e., $E_{k(\mathfrak{m})} = \{\varepsilon \in E_k \mid \varepsilon \equiv 1 \mod \mathfrak{m}\}$. Hence we have

$$N_{i-1}/N_i \cong \mathcal{F}_{i-1}N_{K/k}(W_{K\mathfrak{m}^*})/\mathcal{F}_i N_{K/k}(W_{k\mathfrak{m}^*}),$$

and consequently

$$\begin{aligned}\#(N_{i-1}/N_i) &= \frac{\#(\mathcal{F}_{i-1}N_{K/k}(W_{K\mathfrak{m}^*})/N_{i-1})}{\#(\mathcal{F}_i N_{K/k}(W_{K\mathfrak{m}^*})/N_i)}\#(\mathcal{N}_{i-1}/\mathcal{N}_i)\\ &= \frac{\#(\mathcal{F}_{i-1}/(\mathcal{F}_{i-1}\cap\mathcal{N}_{i-1}))}{\#(\mathcal{F}_i/(\mathcal{F}_i\cap\mathcal{N}_i))}\#(\mathcal{N}_{i-1}/\mathcal{N}_i).\end{aligned}$$

Furthermore, since

$$\mathcal{N}_{i-1}/\mathcal{N}_i = W_{k\mathfrak{m}}^{\ell^{i-1}}N_{K/k}(W_{K\mathfrak{m}^*})/W_{k\mathfrak{m}}^{\ell^i}N_{K/k}(W_{k\mathfrak{m}^*}),$$

we see

$$\log_\ell\{\#(\mathcal{N}_{i-1}/\mathcal{N}_i)\} = \operatorname{rank}_i(W_{k\mathfrak{m}}/N_{K/k}(W_{k\mathfrak{m}^*})).$$

Thus it follows that

$$\begin{aligned}\log_\ell\{\#(N_{i-1}/N_i)\} = \log_\ell&\left\{\frac{\#(\mathcal{F}_{i-1}/(\mathcal{F}_{i-1}\cap\mathcal{N}_{i-1}))}{\#(\mathcal{F}_i/(\mathcal{F}_i\cap\mathcal{N}_i))}\right\}\\ &+\operatorname{rank}_i(W_{k\mathfrak{m}}/N_{K/k}(W_{k\mathfrak{m}^*})).\end{aligned}$$

Hence the assertion follows from Lemma 1.3 and Lemma 1.2 with (1.13).

Now, let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ be a modulus of k, and let K/k be a finite Galois extension. For a prime $\mathfrak{p}$ of k ramified in K, choose a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K. Let $(K_{\mathfrak{P}})'/K_{\mathfrak{p}}$ be the maximal abelian subextension of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Let $\mathfrak{f}_{\mathfrak{P}}$, $V'_{\mathfrak{P}}(j)$, and $v'_{\mathfrak{P}}$ denote the conductor of $(K_{\mathfrak{P}})'/k_{\mathfrak{p}}$, j-th ramification group of $\mathfrak{P}' = \mathfrak{P}\cap(K_{\mathfrak{P}})'$, and the function $v'_{\mathfrak{P}}$ defined by (D1.1) , respectively. Since K/k is a Galois extension, it follows that $\mathfrak{f}_{\mathfrak{P}}$, $V'_{\mathfrak{P}}(j)$, and $v'_{\mathfrak{P}}$ do not depend on the choice of a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K. Therefore we denote them by $\mathfrak{f}_{\mathfrak{p}}$, $V'(j)$, and $v'_{\mathfrak{p}}$, respectively. Furthermore, we denote the product of local abelian conductors of K/k by $\mathfrak{f} = \mathfrak{f}_{K/k}$, i.e.,

$$\text{(D1.11)}\qquad \mathfrak{f} = \mathfrak{f}_{K/k} = \prod_{\mathfrak{p}:\text{ramified}} \mathfrak{f}_{\mathfrak{p}}.$$

If K/k is abelian, then $\mathfrak{f}_{K/k}$ is just the conductor of K/k.

We give an ℓ^i-rank formula for the genus group of $K/k \mod \mathfrak{m}$.

THEOREM 1.1. *Let the notation be as above. Assume that $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ satisfies* (A1.1) *for each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ and each prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K. Then for each positive integer i, we have*

$$\begin{aligned}\operatorname{rank}_i(\operatorname{Gal}(K'(\mathfrak{m})/k)) &= \operatorname{rank}_i(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) \\ &\quad + \sum_{\mathfrak{p}|\mathfrak{f}} \operatorname{rank}_i(V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p})))) \\ &\quad + \log_\ell \left\{ \frac{\#(\mathcal{F}_{i-1}/(\mathcal{F}_{i-1}\cap\mathcal{N}_{i-1}))}{\#(\mathcal{F}_i/(\mathcal{F}_i\cap\mathcal{N}_i))} \right\}.\end{aligned}$$

PROOF. By Lemma 1.1 we see that for each prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, and each prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K, K/k satisfies (A1.1). Therefore, by the above assumption we see that (A1.1) holds for every prime $\mathfrak{p}$ of k, and every prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K. Hence from (D1.6) and (1.10) it follows that

$$\begin{aligned}W_{k\mathfrak{m}}/N_{K/k}(W_{K\mathfrak{m}^*}) &\cong \prod_{\mathfrak{p}} (U(k_{\mathfrak{p}})^{(e(\mathfrak{p}))}/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(k_{\mathfrak{P}})^{(v(e(\mathfrak{p})))})) \\ &\cong \prod_{\mathfrak{p}} V'_{\mathfrak{p}}(V'_{\mathfrak{p}}(e(\mathfrak{p})))\end{aligned}$$

where we put $e(\mathfrak{p}) = 0$ if $\mathfrak{p}$ does not divide $\mathfrak{m}$. Since $V'_{\mathfrak{p}}(e(\mathfrak{p})) = \{0\}$ for a prime $\mathfrak{p}$ of k which is unramified in K, we have

$$\prod_{\mathfrak{p}} V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))) \cong \prod_{\mathfrak{p}|\mathfrak{f}} V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))).$$

Thus we have

$$W_{k\mathfrak{m}}/N_{K/k}(W_{K\mathfrak{m}^*}) \cong \prod_{\mathfrak{p}|\mathfrak{f}} V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))).$$

Hence Proposition 1.1 implies the assertion.

The genus number formula of modulo $\mathfrak{m}$ is a direct consequence of the theorem.

COROLLARY 1 (Genus number formula of modulo $\mathfrak{m}$, cf. M. Horie [11]). *Let the notations and the assumptions be as in Theorem* 1.1. *Then*

$$[K^*(\mathfrak{m}) : K] = \frac{\#(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) \cdot \prod_{\mathfrak{p}|\mathfrak{f}} \#(V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))))}{[K' : k] \cdot [E_{k(\mathfrak{m})} : E_{k(\mathfrak{m})} \cap N_{K'/k}(J_{K'\mathfrak{m}^*})]}$$

where K' denote the maximal abelian subextension of K/k and $E_{k(\mathfrak{m})} = \{\varepsilon \in E_k \mid \varepsilon \equiv 1 \mod \mathfrak{m}\}$.

PROOF. Since we know $N_i = 1$ for sufficiently large i and j (independent of ℓ) with the notation of (1.14), we have

$$\mathcal{F}_i/(\mathcal{F}_i \cap \mathcal{N}_i) \cong E_{k(\mathfrak{m})}/(E_{k(\mathfrak{m})} \cap \mathcal{N}_i) \cong E_{k(\mathfrak{m})}/(E_{k(\mathfrak{m})} \cap \mathcal{N}_j).$$

Moreover taking a product for all ℓ, we have

$$E_{k(\mathfrak{m})}/(E_{k(\mathfrak{m})} \cap N_{K'/k}(J_{K'\mathfrak{m}^*})) \cong \prod_{\ell} E_{k(\mathfrak{m})}/(E_{k(\mathfrak{m})} \cap \mathcal{N}_j),$$

where j is a sufficiently large number independent of ℓ. Thus by the formulae in the above theorem for all ℓ and j, we obtain

$$[K'(\mathfrak{m}) : K] = \frac{\#(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) \cdot \prod_{\mathfrak{p}|\mathfrak{f}} \#(V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))))}{[E_{k(\mathfrak{m})} : E_{k(\mathfrak{m})} \cap N_{K'/k}(J_{K'\mathfrak{m}^*})]}.$$

Therefore from the obvious equality

$$[K^*(\mathfrak{m}) : K] = [K'(\mathfrak{m}) : K'] = [K'(\mathfrak{m}) : k]/[K' : k],$$

the corollary follows.

In general, the genus group modulo $\mathfrak{m}$ is not determined only by $\mathrm{Gal}\,(K'(\mathfrak{m})/k)$ and $\mathrm{Gal}\,(K/k)$. However if K/k does not contain unramified subextension, then the genus group modulo $\mathfrak{m}$ is completely determined.

COROLLARY 2. *Let the notations and the assumptions be as in Theorem* 1.1. *Furthermore suppose that there exists a finite set T of primes $\mathfrak{p}$ of k relatively prime to $\mathfrak{m}$ such that* $\mathrm{Gal}\,(K'/k) = \prod_{\mathfrak{p}\in T} T_{\mathfrak{p}}$ *(direct product), where $T_{\mathfrak{p}}$ denotes the inertia group of $\mathfrak{p}$ in K'/k. Then*

$$\begin{aligned}
&\mathrm{rank}_i(\mathrm{Gal}\,(K^*(\mathfrak{m})/K)) \\
&\quad = \mathrm{rank}_i(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) + \sum_{\mathfrak{p}|\mathfrak{f}} \mathrm{rank}_i(V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p})))) \\
&\qquad + \log_\ell \left\{ \frac{\#(\mathcal{F}_{i-1}/(\mathcal{F}_{i-1} \cap \mathcal{N}_{i-1}))}{\#(\mathcal{F}_i/(\mathcal{F}_i \cap \mathcal{N}_i))} \right\} - \mathrm{rank}_i(\mathrm{Gal}\,(K'/k)).
\end{aligned}$$

PROOF. For each $\mathfrak{p} \in T$, choose a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in $K'(\mathfrak{m})$; and let $T_{\mathfrak{P}}$ denote the inertia group of $\mathfrak{P}$ in $K'(\mathfrak{m})/k$. Since $\mathfrak{P}$ is unramified in $K'(\mathfrak{m})/K'$, it follows that $T_{\mathfrak{P}}$ is isomorphic to $T_{\mathfrak{p}}$ by the restriction from $K'(\mathfrak{m})$ to K'. Therefore we obtain an isomorphism:

$$\prod_{\mathfrak{p}\in T} T_{\mathfrak{P}} \cong \prod_{\mathfrak{p}\in T} T_{\mathfrak{p}} = \mathrm{Gal}\,(K'/k);$$

in particular, we see $\#(\prod_{\mathfrak{p}\in T} T_{\mathfrak{P}}) = [K' : k]$. Thus we have

$$\mathrm{Gal}\,(K'(\mathfrak{m})/k) = \mathrm{Gal}\,(K'(\mathfrak{m})/K') \cdot \prod_{\mathfrak{p}\in T} T_{\mathfrak{P}} \cong \mathrm{Gal}\,(K'(\mathfrak{m})/K') \oplus \mathrm{Gal}\,(K'/k).$$

From this and Theorem 1.1 the corollary follows.

2. A generalization of a theorem of Leopoldt on the genus theory over Q

H. W. Leopoldt [13] proved that the character group of the narrow genus field of a finite abelian extension $K/\mathbf{Q}$ is decomposed as a direct product of the groups of local components of the character group of $K/\mathbf{Q}$. Several authors attempted to generalize this theory over a finite algebraic number field k as the base field. In the general situation, however, we can only obtain weaker results than those over $\mathbf{Q}$ because the result of Leopoldt is based on the triviality of the positive units of $\mathbf{Q}$.

In this section we choose a modulus $\mathfrak{m}$ which satisfies certain conditions and generalize Leopoldt's theory to the genus theory modulo such an $\mathfrak{m}$ in precise form for an arbitrary algebraic number field k and its finite abelian extension K.

2.1. A generalization of a theorem of Leopoldt on the genus theory over Q. Let k be an algebraic number field. Let N be a positive integer and fix it throughout this section. For each positive integer n denote

$$F_n = \{x \in k^\times \mid (x) \in I_k^n\}, \tag{D2.1}$$

where I_k is the ideal group of k.

Let $\mathfrak{m}$ be a modulus of k that satisfies the following three conditions:

(A2.1) $\mathfrak{m}$ is prime to N.

(A2.2) $\mathfrak{m}$ is a product of distinct primes of k.

(A2.3) For each positive integer n dividing N it holds that

$$F_{n(\mathfrak{m})} \subset k^{\times n},$$

where $F_{n(\mathfrak{m})} = F_n \cap k_{(\mathfrak{m})}$.

In the next subsection 2.2 we prove that such a modulus $\mathfrak{m}$ exists under certain conditions. In the case where $k = \mathbf{Q}$, of course, $\mathfrak{m} = \infty$ satisfies the above assumptions for any N.

For such an $\mathfrak{m}$ we can show that the genus theory modulo $\mathfrak{m}$ also has some good properties in the same way as the narrow genus theory over $\mathbf{Q}$ does.

Let K/k be a finite abelian extension of exponent n dividing N. Let $\mathfrak{f}$ be the conductor of K/k and $S = S_K$ denote the set of primes that divide $\mathfrak{f}$ and are prime to $\mathfrak{m}$, i.e.,

$$S = S_K = \{\mathfrak{p} \mid \mathfrak{p} \text{ divides } \mathfrak{f}, \text{ and } \mathfrak{p} \text{ is prime to } \mathfrak{m}\}. \tag{D2.2}$$

Let ℓ be a prime number. By Theorem 1.1 we can calculate the ℓ-part of $\mathrm{Gal}\,(K^*(\mathfrak{m})/k) = \mathrm{Gal}\,(K'(\mathfrak{m})/k)$. First, since $\mathfrak{m}$ is prime to N the prime divisors of $\mathfrak{m}$ are at most tamely ramified in K/k. Hence we see for each prime divisor $\mathfrak{p}$ of $\mathfrak{f}$

$$V_{\mathfrak{p}}(v_{\mathfrak{p}}(e(\mathfrak{p}))) = \begin{cases} \{1\} & \text{if} \quad \mathfrak{p} \notin S, \\ V_{\mathfrak{p}}(0) & \text{if} \quad \mathfrak{p} \in S. \end{cases} \tag{2.1}$$

Furthermore we can prove the following.

LEMMA 2.1. *Let K/k be a finite abelian extension of exponent n dividing N. Let ℓ be a prime number and let the notations be as in* (D1.9) *and* (D1.10). *Then we have*

$$\mathcal{F}_i \subset \mathcal{N}_i,$$

i.e.,

$$W_{k\mathfrak{m}} \cap J_{k\mathfrak{m}}^{\ell^i} k_{(\mathfrak{m})} \subset W_{k\mathfrak{m}}^{\ell^i} N_{K/k}(W_{K\mathfrak{m}^*})$$

for every non negative integer i.

PROOF. We know by (1.8) that the exponent of $W_{k\mathfrak{m}}/N_{K/k}(W_{K\mathfrak{m}^*})$ divides n. Therefore, if ℓ does not divide n, then the assertion of the lemma is clear. Now we assume that ℓ divides n.

First we consider the case where ℓ^i divides n. Let $\alpha \in W_{k\mathfrak{m}} \cap J_{k\mathfrak{m}}^{\ell^i} k_{(\mathfrak{m})}$. Then we can write $\alpha = \beta^{\ell^i} x$ for $\beta \in J_{k\mathfrak{m}}$ and $x \in k_{(\mathfrak{m})}$; so $x = \alpha\beta^{-\ell^i} \in F_{\ell^i(\mathfrak{m})}$. Therefore by (A2.3) we see $x = y^{\ell^i}$ for some $y \in k$. Hence $\alpha = (\beta y)^{\ell^i}$. Since $\mathfrak{m}$ is a product of distinct primes of k and $\alpha \in W_{k\mathfrak{m}}$, it follows that $\alpha \in W_{k\mathfrak{m}}^{\ell^i}$. This completes the proof of the first case.

Next consider the case where ℓ divides n but ℓ^i dose not divides n. Let j denote the maximal integer such that ℓ^j divides n. Let $\alpha \in W_{k\mathfrak{m}} \cap J_{k\mathfrak{m}}^{\ell^i} k_{(\mathfrak{m})}$. Then by the result of the first case we have $\alpha \in W_{k\mathfrak{m}}^{\ell^j}$. On the other hand, the exponent of $W_{k\mathfrak{m}}/N_{K/k}(W_{k\mathfrak{m}^*})$ divides n, and $\mathcal{F}_i\mathcal{N}_i/\mathcal{N}_i$ is a ℓ-group. Since ℓ^j is the ℓ-part of n, we have $\alpha \in \mathcal{N}_i$. This completes the proof.

By this lemma we see the last term of the formula in Theorem 1.1 vanishes. Since this holds for every prime number ℓ, we have

$$\mathrm{Gal}\,(K^*(\mathfrak{m})/k) \cong (J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) \oplus \sum_{\mathfrak{p}\in S} V_{\mathfrak{p}}(0)$$

by (2.1). This isomorphism is expressed more explicitly using character groups as follows:

PROPOSITION 2.1. *Let $S = S_K$ denote the set of primes that divide the conductor $\mathfrak{f}$ of K/k, and are prime to $\mathfrak{m}$. Put*

$$U(K/k)_S = \prod_{\mathfrak{p}\in S} U(k_{\mathfrak{p}}),$$
$$\overline{U}(K/k)_S = \prod_{\mathfrak{p}\in S} U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}})),$$

where $\mathfrak{P}$ denotes a prime divisor of $\mathfrak{p}$ in K. Let

$$\overline{f} : \overline{U}(K/k)_S \longrightarrow J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})$$

be the natural homomorphism induced from the inclusion map

$$f : U(K/k)_S \longrightarrow J_{k\mathfrak{m}}.$$

Then we have the following.

(1) *$\overline{f}$ is injective.*

(2) *$\overline{f}(\overline{U}(K/k)_S)$ is a pure subgroup of $J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})$.*

PROOF. (1) Let $\alpha \in U(K/k)_S$ and assume $f(\alpha) = x \cdot \beta$ with $x \in k_{(\mathfrak{m})}$ and $\beta \in N_{K/k}(W_{K\mathfrak{m}^*})$. Since $x = f(\alpha)\beta^{-1}$ is a unit idele, we see that x is a unit of k. Therefore, for any positive integer m, it holds that $x \in F_{m(\mathfrak{m})}$; in particular, $x \in F_{N(\mathfrak{m})}$. Hence by (A2.3) we have $x = y^N$ for some $y \in k^\times$. Since x is a unit, y is also a unit. Moreover the exponent of $\mathrm{Gal}\,(K/k)$ divides N. Hence by (1.8) and (1.6) we can write $x = N_{K/k}(\gamma)$ with $\gamma \in W_{K\mathfrak{m}^*}$ and so $f(\alpha) \in N_{K/k}(W_{K\mathfrak{m}^*})$. This shows $\alpha \in \prod_{\mathfrak{p}\in S} N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))$, which proves (1).

(2) Since the exponent of $J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})$ divides N, it suffices to prove, for each prime factor ℓ of N and each positive integer i with $\ell^i \mid N$, that

$$\begin{aligned} J_{k\mathfrak{m}}^{\ell^i} \cap (f(U(K/k)_S) \cdot k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})) \\ \subset f(U(K/k)_S)^{\ell^i} \cdot k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*}). \end{aligned}$$

Assume $\gamma^{\ell^i} = f(\alpha)\cdot x\cdot\beta$ for $\gamma \in J_{k\mathfrak{m}}$, $\alpha \in U(K/k)_S$, $x \in k_{(\mathfrak{m})}$ and $\beta \in N_{K/k}(W_{K\mathfrak{m}^*})$. Since $f(\alpha)\cdot\beta$ is a unit idele, we see that $x = f(\alpha^{-1})\cdot\beta^{-1}\cdot\gamma^{\ell^i} \in F_{\ell^i} \cap k_{(\mathfrak{m})}$. Hence by (A2.3) $x = y^{\ell^i}$ for some $y \in k^\times$. Therefore we have

$$(\gamma y^{-1})^{\ell^i} = f(\alpha)\cdot\beta,$$

and γy^{-1} is a unit idele. Let γ' and β' be the S-component of γy^{-1} and β, respectively. Then $\gamma', \beta' \in U(K/k)_S$, and

$$\gamma'^{\ell^i} = \alpha\cdot\beta', \text{ i.e., } \quad f(\gamma')^{\ell^i} = f(\alpha)\cdot f(\beta').$$

Thus we have

$$\gamma^{\ell^i} = f(\gamma')^{\ell^i} f(\gamma'^{-1})^{\ell^i} f(\alpha) \cdot x \cdot \beta = f(\gamma')^{\ell^i} \cdot x \cdot f(\beta'^{-1}) \cdot \beta$$
$$\in f(U(K/k)_S)^{\ell^i} \cdot k_{(\mathfrak{m})} N_{K/k}(W_{K\mathfrak{m}^*}).$$

This completes the proof of (2).

By this proposition we see that there exists a subgroup $H_{\mathfrak{m}}$ of $J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})$ such that

$$J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*}) = H_{\mathfrak{m}} \oplus \overline{f}(\overline{U}(K/k)_S) \cong H_{\mathfrak{m}} \oplus \overline{U}(K/k)_S. \tag{2.2}$$

Now we fix such $H_{\mathfrak{m}}$. Then using (1.10) we have

$$H_{\mathfrak{m}} \cong J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})f(U(K/k)_S) \cong J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}},$$

because the prime divisors of $\mathfrak{m}$ are at most tamely ramified in K/k.

DEFINITION 2.1. For a finite abelian extension L/k, let $\mathfrak{X}(L/k)$ denote the character group of $J_k/k^\times N_{L/k}(J_L)$.

Let $L/L_1/k$ be a tower of finite abelian extensions, then it holds that

$$\mathfrak{X}(L_1/k) \subset \mathfrak{X}(L/k)$$

because $N_{L/k}(J_L) \subset N_{L_1/k}(J_{L_1})$. Therefore if $k^{(\mathfrak{m})}$ and $L^*(\mathfrak{m})$ denote the ray class field of k modulo $\mathfrak{m}$ and the genus field of L/k, respectively, then we have

$$\mathfrak{X}(k^{(\mathfrak{m})}/k) \cdot \mathfrak{X}(L/k) \subset \mathfrak{X}(L^*(\mathfrak{m})/k).$$

Now let K/k be a finite abelian extension whose exponent divides N as above. Let $\chi \in \mathfrak{X}(K^*(\mathfrak{m})/k)$. By (1.13) $\mathfrak{X}(K^*(\mathfrak{m})/k)$ is considered as the character group of $J_{k\mathfrak{m}}/k_{(\mathfrak{m})}N_{K/k}(W_{K\mathfrak{m}^*})$. Hence using the direct decomposition (2.2) χ is decomposed uniquely as follows:

$$\chi = \chi_H \cdot \prod_{\mathfrak{p} \in S} \chi_{\mathfrak{p}},$$

where χ_H is the $H_{\mathfrak{m}}$-component of χ, and $\chi_{\mathfrak{p}}$ is the $U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))$-component of χ for each $\mathfrak{p} \in S$.

Then χ_H is considered as a character of $J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}} \cong H_{\mathfrak{m}}$; hence if K_{χ_H} denotes the class field over k corresponding to the kernel of χ_H, then K_{χ_H} is a subfield of the ray class field of k modulo $\mathfrak{m}$. Similarly, for each $\mathfrak{p} \in S$, $\chi_{\mathfrak{p}}$ is a

character of $U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))$. Hence if $K_{\chi_{\mathfrak{p}}}$ denotes the class field over k corresponding to the kernel of $\chi_{\mathfrak{p}}$, then, at the most, only prime divisors of $\mathfrak{m}$ are ramified in $K_{\chi_{\mathfrak{p}}}$ outside $\mathfrak{p}$, and $\mathfrak{p}$ is totally ramified in $K_{\chi_{\mathfrak{p}}}$.

DEFINITION 2.2. Let

$$\mathfrak{X}(K/k)_{\mathfrak{p}} = \{\chi_{\mathfrak{p}} \mid \chi \in \mathfrak{X}(K^*(\mathfrak{m})/k)\}.$$

Then $\mathfrak{X}(K/k)_{\mathfrak{p}}$ is a subgroup of $\mathfrak{X}(K^*(\mathfrak{m})/k)$.

Now we can prove the following theorem, which gives a generalization of Leopoldt's theorem on the genus theory over $\mathbf{Q}$ in a precise form.

THEOREM 2.1. *Let N and $\mathfrak{m}$ be a positive integer and a modulus of k which satisfy* (A2.1) $\sim$ (A2.3). *Let K/k be a finite abelian extension such that the exponent of* $\mathrm{Gal}(K/k)$ *divides N. Then*

$$\mathfrak{X}(K^*(\mathfrak{m})/k) = \mathfrak{X}(k^{(\mathfrak{m})}/k) \oplus \prod_{\mathfrak{p}\in S} \mathfrak{X}(K/k)_{\mathfrak{p}}.$$

PROOF. By the definition of $\mathfrak{X}(K/k)_{\mathfrak{p}}$, it is clear that

$$\mathfrak{X}(K^*(\mathfrak{m})/k) \supset \mathfrak{X}(k^{(\mathfrak{m})}/k) \oplus \prod_{\mathfrak{p}\in S} \mathfrak{X}(K/k)_{\mathfrak{p}}. \tag{2.3}$$

Furthermore, by the direct decomposition (2.2) we know that $\mathfrak{X}(K/k)_{\mathfrak{p}}$ is the character group of $U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))$; in particular, $\#(\mathfrak{X}(K/k)_{\mathfrak{p}}) = \#(U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}})))$. On the other hand by (1.10) we have $\#(U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))) = \#(V_{\mathfrak{p}}(0))$. Hence

$$\begin{aligned}
&\#(\mathfrak{X}(k^{(\mathfrak{m})}/k) \oplus \prod_{\mathfrak{p}\in S} \mathfrak{X}(K/k)_{\mathfrak{p}}) \\
&\qquad = \#(\mathfrak{X}(k^{(\mathfrak{m})}/k)) \cdot \prod_{\mathfrak{p}\in S} \#(U(k_{\mathfrak{p}})/N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U(K_{\mathfrak{P}}))) \\
&\qquad = \#(\mathfrak{X}(k^{(\mathfrak{m})}/k)) \cdot \prod_{\mathfrak{p}\in S} \#(V_{\mathfrak{p}}(0)).
\end{aligned}$$

Thus from Corollary 1 of Theorem 1.1 with (2.3) the assertion follows. This completes the proof.

Finally hereafter in this subsection suppose that $\mathfrak{m}$ satisfies the following assumption (A2.4) in addition to (A2.1) $\sim$ (A2.3).

(A2.4) For each prime number ℓ dividing N it holds that

$$P_k(\mathfrak{m}) \subset I_k(\mathfrak{m})^{\ell} P_{k(\mathfrak{m})},$$

where $P_k(\mathfrak{m})$, $I_k(\mathfrak{m})$ and $P_{k(\mathfrak{m})}$ denote the group of principal ideals of k prime to $\mathfrak{m}$, the group of ideals of k prime to $\mathfrak{m}$, and the ray ideal group of k modulo $\mathfrak{m}$, respectively.

LEMMA 2.2. *Suppose that k, N, and $\mathfrak{m}$ satisfy* (A2.1) $\sim$ (A2.4). *Let ℓ be a prime factor of N. If the class number $h(k)$ of k is prime to ℓ, then the ray class number $h(k,\mathfrak{m})$ of k modulo $\mathfrak{m}$ is also prime to ℓ.*

PROOF. Since $h(k)$ is prime to ℓ, we have $I_k^\ell P_k = I_k$, where I_k and P_k denote the ideal group of k and the principal ideal group of k. Hence $I_k(\mathfrak{m})^\ell P_k(\mathfrak{m}) = I_k(\mathfrak{m})$, where $I_k(\mathfrak{m})$ and $P_k(\mathfrak{m})$ denote the group of ideals of k prime to $\mathfrak{m}$ and the group of principal ideals of k prime to $\mathfrak{m}$, respectively. Furthermore (A2.4) implies that $I_k(\mathfrak{m})^\ell P_k(\mathfrak{m}) = I_k(\mathfrak{m})^\ell P_{k(\mathfrak{m})}$. Therefore we see that $I_k(\mathfrak{m})^\ell P_{k(\mathfrak{m})} = I_k(\mathfrak{m})$, which gives $\ell \nmid \#(I_k(\mathfrak{m})/P_{k(\mathfrak{m})})$. This completes the proof.

By this lemma we have the following corollary of Theorem 2.1.

COROLLARY OF THEOREM 2.1. *Let the notations and the assumptions be as in Theorem* 2.1. *Furthermore, assume that $\mathfrak{m}$ satisfies* (A2.4) *and N is prime to the class number $h(k)$ of k. Let $\mathfrak{X}'(K^*(\mathfrak{m})/k)$ denote the N-part of $\mathfrak{X}(K^*(\mathfrak{m})/k)$. Then we have*

$$\mathfrak{X}'(K^*(\mathfrak{m})/k) = \prod_{\mathfrak{p}\in S} \mathfrak{X}(K/k)_{\mathfrak{p}}.$$

2.2. Existence of a modulus with (A2.1) $\sim$ (A2.4). In this subsection we prove that there exists a modulus which satisfies (A2.1) $\sim$ (A2.4) under certain conditions.

Let k be an algebraic number field of finite degree, and let N be an odd positive integer. Let N^* denote the product of distinct prime factors of N. Let ζ_N denote a primitive N-th root of unity, and put $k_N = k(\zeta_N)$.

Now we consider the following condition:

(A2.5) $[k_{N^*} : k]$ is prime to N.

If N is a power of a prime number, then (A2.5) always holds.

LEMMA 2.3. *Assume k and N satisfy* (A2.5). *Then we have*

$$k^\times \cap k_N^{\times N} = k^{\times N}.$$

PROOF. It suffices to show $k^\times \cap k_N^{\times N} \subset k^{\times N}$. Furthermore we note that if k and N satisfy (A2.5), then for any finite extension $\widetilde{k}/k$, $\widetilde{k}$ and N satisfy (A2.5). Let $N = \prod_{i=1}^m p_i^{e_i}$ denote the prime decomposition of N with distinct odd prime numbers p_i. We prove the assertion by induction on the number m of prime factors of N. If $m = 1$, then the assertion is true by Hasse [8, Satz 1].

Assume that the assertion is valid for N; and $N \cdot M$ is prime to $[k_{N^*p} : k]$, where $M = p^e$ is a power of an odd prime number p prime to N. Then we must prove

$$k^\times \cap k_{NM}^{\times NM} = k^{\times NM}.$$

Let $x \in k^\times \cap k_{NM}^{\times NM}$. Then $x = \alpha^{NM}$ for some $\alpha \in k_{NM}^\times$. Put $y = \alpha^M$. Then $x = y^N$. Let σ be a generator of a cyclic group $\mathrm{Gal}\,(k_{NM}/k_{Np})$. Since $\sigma(\alpha^{NM}) = \sigma(x) = x = \alpha^{NM}$, we can write $\sigma(\alpha) = \zeta \cdot \alpha$ for some NM-th root of unity ζ, i.e., $\zeta^{NM} = 1$. Therefore, $\sigma(y) = \sigma(\alpha^M) = \zeta^M \cdot \alpha^M = \zeta^M \cdot y$. Furthermore, $\sigma(\zeta^M) = \zeta^M$ since $\zeta^M \in k_N$. Hence for every positive integer j, we see that $\sigma^j(y) = \sigma^{j-1}(\zeta^M y) = \zeta^M \sigma^{j-1}(y) = \cdots = \zeta^{jM} y$. In particular, if p^i is the order of σ, then $y = \sigma^{p^i}(y) = \zeta^{p^i M} y$, i.e., $\zeta^{p^i M} = 1$. On the other hand we know that $\zeta^{NM} = 1$ and N is prime to p. Hence we have $\zeta^M = 1$, so that $\sigma(y) = y$. Thus $y \in k_{Np}$. Since $x = y^N$, by the induction assumption we can write $x = w^N = y^N$ for some $w \in k_p$.

Next put $z = \alpha^N$. Then $x = z^M$. Let τ be any element of $\mathrm{Gal}\,(k_{NM}/k_{MN^*})$. Then we can write $\tau(\alpha) = \eta \cdot \alpha$ for some NM-th root of unity η, i.e., $\eta^{NM} = 1$. Therefore $\tau(z) = \tau(\alpha^N) = \eta^N z$ and $\tau(\eta^N) = \eta^N$ since $\eta^N \in k_M$. Let t denote the order of τ. Then $z = \tau^t(z) = \eta^{tN} z$, and $\eta^{tN} = 1$. Since $\eta^{tN} = 1$ and t is prime to M, we have $\eta^N = 1$. Hence $\tau(z) = z$. Since τ is any element of $\mathrm{Gal}\,(k_M/k_{MN^*})$, it follows that $z \in k_{MN^*}$. Therefore from $x = z^M$, using the result of the case $m = 1$, we can write $x = v^M$ for some $v \in k_{pN^*}$.

Thus we see that $x = w^N = v^M$ for some $w, v \in k_{pN^*}$. Since N is prime to M, this implies that $x = u^{NM}$ for some $u \in k_{pN^*}$. Hence taking norm from k_{pN^*} to k we have $x^c = x_0^{NM}$ where $x_0 = N_{k_{pN^*}/k}(u)$ and $c = [k_{pN^*} : k]$. Since c is prime to NM by (A2.5), it follows that $x = x_1^{NM}$ for some $x_1 \in k$. This completes the proof.

The purpose of this subsection is to prove the following theorem.

THEOREM 2.2 (1) *Suppose that k and N satisfy* (A2.5). *Then there exist infinitely many ideals of k that satisfy* (A2.1) $\sim$ (A2.3).

(2) *Let ℓ be an odd prime and let N be a power of ℓ. Then there exist infinitely many ideals of k that satisfy* (A2.1) $\sim$ (A2.4).

(3) *Let k and N satisfy* (A2.5). *Assume that the class number of k is prime to N. Then there exist infinitely many ideals of k that satisfy* (A2.1) $\sim$ (A2.4).

PROOF. (1) Let $(I_k/P_k)'$ denote the N-part of I_k/P_k, i.e., the subgroup of the ideal class group I_k/P_k of k that consists of all of the elements whose order divide N. Choose prime ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ of k such that $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ are prime to N and represent a basis of $(I_k/P_k)'$. For $j = 1, \ldots, t$ let C_j denote the order of $\mathfrak{a}_j$ in I_k/P_k. Then $a_j^{C_j} = (\alpha_j)$ for some $\alpha_j \in k^\times$. Let E_k be the group of units of k, and let $\alpha_{t+1}, \ldots, \alpha_{t+r}$ be a system of fundamental units of k, i.e., a basis of the free part of E_k. Let $W = W_k$ denote the torsion part of E_k and α_{t+r+1} be a generator of W.

Put $F' = \langle \alpha_1, \alpha_2, \dots, \alpha_{t+r+1} \rangle$, to be the subgroup of $k^\times$ generated by $\alpha_1, \alpha_2, \dots, \alpha_{t+r+1}$. Then

$$F' \cong \mathbb{Z}^{t+r} \oplus W. \tag{2.4}$$

Furthermore, we have

$$F_n \subset F' k^{\times n} \quad \text{for every factor } n \text{ of } N. \tag{2.5}$$

In fact, let $a \in F_n$, then we can write $(a) = \mathfrak{a}^n$ for an ideal $\mathfrak{a}$ of k. Since the order of $\mathfrak{a}$ in I_k/P_k divides N, $\mathfrak{a}$ represents an element of $(I_k/P_k)'$. Hence $\mathfrak{a}$ is written in the form

$$\mathfrak{a} = (b) \prod_{j=1}^{t} \mathfrak{a}_j^{e_j}$$

for integers e_j and some $b \in k^\times$. Thus

$$(a) = \mathfrak{a}^n = (b^n) \prod_{j=1}^{t} \mathfrak{a}_j^{e_j n}. \tag{2.6}$$

Since $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ represent a basis of N-part of I_k/P_k and $C_1, \dots, C_t$ denote the orders of them, it follows that C_i divides $e_j n$ for $j = 1, \dots, t$. Put $f_j = e_j n / C_j$. Then by (2.6) we have

$$(a) = \prod_{j=1}^{t} \mathfrak{a}_j^{e_j n} (b^n) = \prod_{j=1}^{t} (\alpha_j)^{f_j} (b^n). \tag{2.7}$$

Hence we can write

$$a = \prod_{i=1}^{t} \alpha_i^{f_i} b^n \varepsilon.$$

with some $\varepsilon \in E_k = \langle \alpha_{t+1}, \dots, \alpha_{t+r}, \dots, \alpha_{t+r+1} \rangle$. This shows (2.5).

We next prove that

$$F' \cap k^{\times n} = F'^n \quad \text{for every factor } n \text{ of } N. \tag{2.8}$$

It suffices to prove that $F' \cap k^{\times n} \subset F'^n$. Let $x \in F' \cap k^{\times n}$. Then x is of the form

$$x = y^n = \prod_{j=1}^{t+r+1} \alpha_j^{e_j}$$

for some $y \in k^\times$ and some integers e_j. Hence by the choice of α_j, we obtain that

$$(y)^n = \prod_{j=1}^{t} \mathfrak{a}_j^{C_j e_j}.$$

Since $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ are distinct prime ideals, we have

$$(y) = \prod_{j=1}^{t} \mathfrak{a}_j^{f_j},$$

for integers f_j with $f_j n = C_j e_j$. Since $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ represent a basis of $(I_k/P_k)'$, the order C_j of the class of $\mathfrak{a}_j$ divides f_j for $j = 1, \dots, t$. Hence we have

$$(y) = \prod_{j=1}^{t} (\alpha_j)^{f_j/C_j}.$$

Thus

$$y^{-1} \prod_{j=1}^{t} \alpha_j^{f_j/C_j} \in E_k, \quad \text{and} \quad y^{-1} \prod_{j=1}^{t} \alpha_j^{f_j/C_j} = \prod_{j=t+1}^{t+r+1} \alpha_j^{g_j}$$

for some integers g_j. This implies that $y \in F'$, and $x = y^n \in F'^n$, which proves (2.8).

From (2.8) and Lemma 2.3 we can prove for every factor n of N that

$$F'/F'^n \cong F'k^{\times n}/k^{\times n} \cong F'k_n^{\times n}/k_n^{\times n}, \tag{2.9}$$

which is a key fact for our proof of the theorem. Indeed, (2.8) shows that

$$F'/F'^n \cong F'/(F' \cap k^{\times n}) \cong F'k^{\times n}/k^{\times n}.$$

Furthermore, by Lemma 2.3 we see that $F' \cap k_n^{\times n} = F' \cap k^{\times n}$. Thus we have

$$F'/(F' \cap k^{\times n}) = F'/(F' \cap k_n^{\times n}) \cong F'k_n^{\times n}/k_n^{\times n}.$$

This proves (2.9).

Now, let $N' = GCD(N, \#(W))$, $M = k_N(\sqrt[N]{F'})$, and $M' = k(\sqrt[N']{F'})$. Furthermore, for $j = 1, 2, \dots, t+r$ let

$$L_j = k_N(\sqrt[N]{\alpha_1}, \dots, \sqrt[N]{\alpha_{j-1}}, \sqrt[N]{\alpha_{j+1}}, \dots, \sqrt[N]{\alpha_{t+r+1}})$$

and

$$L' = k(\sqrt[N']{\alpha_1}, \dots, \sqrt[N']{\alpha_{t+r}}).$$

Then (2.4) and (2.9) imply that

$$\mathrm{Gal}\,(M/k_N) \cong F'/F'^N \cong (\mathbb{Z}/N\mathbb{Z})^{t+r} \oplus (\mathbb{Z}/N'\mathbb{Z}).$$

Hence by Čebotarev density theorem we can choose $t+r$ prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_{t+r}$ of k, and in the case $N' > 1$, another $\mathfrak{q}_{t+r+1}$ which satisfy the following conditions (1), (2), and (3).

(1) All $\mathfrak{q}_j$ are prime to $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ and N.

(2) For $j = 1, \dots, t+r$, $\mathfrak{q}_j$ is unramified in M, and the decomposition field of a prime divisor of $\mathfrak{q}_j$ in M is L_j. (Since L_j/k is a Galois extension, it follows that the decomposition field of any prime divisor of $\mathfrak{q}_j$ in M coincides with L_j.)

(3) In the case when $N' > 1$, q_{t+r+1} is unramified in M', and the decomposition field of a prime divisor of $\mathfrak{q}_{t+r+1}$ in M' is L'.

Put $\mathfrak{m} = \mathfrak{q}_1 \dots q_{t+r}$ if $N' = 1$, and $\mathfrak{m} = \mathfrak{q}_1 \dots \mathfrak{q}_{t+r+1}$ if $N' > 1$. We prove that this $\mathfrak{m}$ satisfies the condition (A2.1) $\sim$ (A2.3). Clearly $\mathfrak{m}$ satisfies (A2.1) and (A2.2). Hence it suffices to prove that $\mathfrak{m}$ satisfies (A2.3).

For this we first show the following assertion:

(2.10) Let n (> 1) be a positive integer dividing N. For each pair of indices i and j, $1 \leqq i \leqq t+r$ and $1 \leqq j \leqq t+r+1$ with $i \neq j$, α_j is n-th power residue modulo $\mathfrak{q}_i$, i.e., there exists $\beta \in k^\times$ such that $\alpha_j \equiv \beta^n \mod \mathfrak{q}_i$. Furthermore α_i represents a generator of a cyclic group $k(\mathfrak{q}_i)/k(\mathfrak{q}_i)^n k_{(\mathfrak{q}_i)}$ of order n, where $k(\mathfrak{q}_i)$ denotes the subgroup of $k^\times$ consisting of those elements prime to $\mathfrak{q}_i$.

In fact, $\mathfrak{q}_i$ is completely decomposed in L_i/k; in particular, so is in $k_n(\sqrt[n]{\alpha_j})/k$. Let $\mathfrak{Q}_i$ be a prime divisor of $\mathfrak{q}_i$ in k_n. Then by Hasse [9, Teil Ia, §9, IX] there exists an element $\gamma \in k_n$ such that $\alpha_j \equiv \gamma^n \mod \mathfrak{Q}_i$. Moreover $\mathfrak{q}_i$ is completely decomposed in k_n. Therefore we can choose an element $\beta \in k^\times$ with $\beta \equiv \gamma \mod \mathfrak{Q}_i$. Thus we have $\alpha \equiv \beta^n \mod \mathfrak{q}_i$, which proves the first part of (2.10). Next we prove the second part. Assume $\alpha_i^m \equiv \delta^n \mod \mathfrak{q}_i$ for $\delta \in k(\mathfrak{q}_i)$ and $m \mid n$. Then $\alpha_i^m \equiv \delta^n \mod \mathfrak{Q}_i$. Hence $\mathfrak{Q}_i$ is completely decomposed in $k_n(\sqrt[n]{\alpha_i^m})$. Since by the choice of $\mathfrak{q}_i$, $\mathfrak{Q}_i$ is inert in $k_n(\sqrt[n]{\alpha_i})$, this implies $k_n(\sqrt[n]{\alpha_i^m}) = k_n$. Thus we have $m = n$. This proves (2.10).

In the case when $N' > 1$, moreover, we have similarly the following:

(2.11) Let $N' > 1$ and put $i = t+r+1$. Let $1 \leqq j \leqq t+r$. Then α_j is N'-th power residue modulo $\mathfrak{q}_i$. Furthermore, α_i represents a generator of a cyclic group $k(\mathfrak{q}_i)/k(\mathfrak{q}_i)^{N'} k_{(\mathfrak{q}_i)}$.

Using (2.5), (2.10) and (2.11) we can prove (A2.3). Let n be a positive integer dividing N and let $x \in F_{n(\mathfrak{m})}$. Then by (2.5) x is written in the form:

$$x = \prod_{j=1}^{t+r+1} \alpha_j^{e_j} y^n, \tag{2.12}$$

for some integers e_j and an element y of k. Since x and $\alpha_1, \dots, \alpha_{t+r+1}$ are prime to $\mathfrak{m}$, y is also prime to $\mathfrak{m}$. Furthermore, by (2.10) it follows that α_j is n-th power residue modulo $\mathfrak{q}_i$ for $1 \leqq i \leqq t+r$, $1 \leqq j \leqq t+r+1$, and $i \neq j$. On the other hand, we have $x \equiv 1 \mod \mathfrak{m}$, and in particular, we see that x is n-th power

residue modulo $\mathfrak{q}_i$ for $1 \leqq i \leqq t+r$. Hence $\alpha_i^{e_i}$ is also n-th power residue modulo $\mathfrak{q}_i$ for $1 \leqq i \leqq t+r$. Therefore using the second part of (2.10) we obtain the fact that n divides e_i for $1 \leqq i \leqq t+r$. Next we consider the case $i = t+r+1$. Let $n' = GCD(n, N') = GCD(n, \#(W))$. Then using the second part of (2.11) we obtain similarly the fact that n' divides e_{t+r+1}. Since α_{t+r+1} is a generator of a cyclic group W, we can write $\alpha_{t+r+1}^{e_{t+r+1}} = \alpha_{t+r+1}^{nb}$ for some integer b. Thus we have

$$x = \left(\prod_{j=1}^{t+r} \alpha_j^{e_j/n} \alpha_{t+r+1}^{b} y\right)^n,$$

which shows (A2.3). This completes the proof of (1).

(2) We use the notations and the results in the proof of (1). Let $\mathfrak{m}$ be the ideal chosen in (1) in the case when N is a power of ℓ. Then by the result of (1) it suffices to prove (A2.4).

Let $(x) \in P_k(\mathfrak{m})$. Then by the second part of (2.10) and (2.11), we can choose integers a_i and elements b_i of k such that $x \equiv \alpha_i^{a_i} b_i^{\ell} \mod \mathfrak{q}_i$ for $1 \leqq i \leqq t+r+1$. Put

$$y = \prod_{j=1}^{t+r+1} \alpha_j^{a_j}.$$

Then by (2.10) and (2.11) we have

$$x^{-1}y \equiv b_i^{-\ell}\alpha_i^{-a_i} \prod_{j=1}^{t+r+1} \alpha_j^{a_j} \equiv b_i^{-\ell} \prod_{j=1, j\neq i}^{t+r+1} \alpha_j^{a_j} \equiv c_i^{\ell} \mod \mathfrak{q}_i$$

for $1 \leqq i \leqq t+r+1$. Therefore, there are elements z and w of k such that $x = yz^{\ell}w$ with $z \in k(\mathfrak{m})$ and $w \equiv 1 \mod \mathfrak{m}$. On the other hand, by the definition, the order C_j of $\mathfrak{a}_j$ in I_k/P_k is a power of N. Hence we have

$$(y) = \prod_{j=1}^{t} (\alpha_j)^{a_j} = \prod_{j=1}^{t} \mathfrak{a}_j^{C_j a_j} \in I_k(\mathfrak{m})^{\ell}.$$

Thus $(x) \in I_k(\mathfrak{m})^{\ell} P_{k(\mathfrak{m})}$. This proves (A2.4).

(3) Let ℓ be a prime dividing N. Let y be as in the proof of (2). If the class number of k is prime to N, then in the proof of (1) the number t of ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ equals to 0. Hence in this case y is a unit. Thus we can prove (A2.4) similarly as for the case (2). This completes the proof of the theorem.

3. Central extensions modulo $\mathfrak{m}$

In this section we study central extensions modulo $\mathfrak{m}$ of a finite Galois extension K over a finite algebraic number field k and the ray class number modulo $\mathfrak{m}$

of K in connection with the Hasse norm principle modulo $\mathfrak{m}$ of K/k. The purpose of this section is to prove Theorem 3.3.

3.1. Central extensions modulo $\mathfrak{m}$ of finite Galois extensions K/k. Let k be an algebraic number field of finite degree. Let $\mathfrak{m}$ be a modulus of k. Let K/k be a finite Galois extension. In this subsection we give some general results on central extensions modulo $\mathfrak{m}$ as preliminaries to the next subsection .

We start with the definition of the central class extension of K/k modulo $\mathfrak{m}$.

DEFINITION 3.1. Let K/k be a finite Galois extension. Let $\mathfrak{m}$ be a modulus of k. Let $\mathfrak{m}^*$ denote the lifting modulus of $\mathfrak{m}$ from k to K defined in (D1.5). Let $\widehat{K}(\mathfrak{m})$ be the maximal central extension of K/k contained in the ray class field over K modulo $\mathfrak{m}^*$. We call $\widehat{K}(\mathfrak{m})$ the central extension modulo $\mathfrak{m}$ of K/k.

From the definition it follows that $K^*(\mathfrak{m}) \subset \widehat{K}(\mathfrak{m})$. We study the abelian group structure of the Galois group of $\widehat{K}(\mathfrak{m})/K^*(\mathfrak{m})$. Since the approximation theorem implies $J_K \subset K^\times J_{K\mathfrak{m}^*}$, we have a natural isomorphism: $J_K/K^\times \cong J_{K\mathfrak{m}^*}/K_{(\mathfrak{m}^*)}$. Therefore, there is a natural correspondence between the class fields over K and the subgroups of $J_{K\mathfrak{m}^*}$ which contains $K_{(\mathfrak{m}^*)}$.

The following lemma is well known and is proved by standard class field theory; we omit the proof of it. For the proof, e.g., see M. Razar [15, Proposition 1].

LEMMA 3.1. (1) *Let H_G be the subgroup of $J_{K\mathfrak{m}^*}$ corresponding to the genus field of K/k modulo $\mathfrak{m}$ (i.e., in particular, $J_{K\mathfrak{m}^*}/H_G \cong \mathrm{Gal}\,(K^*(\mathfrak{m})/K)$). Then we have*

$$H_G = N_{K/k}^{-1}(k_{(\mathfrak{m})} N_{K/k}(W_{K\mathfrak{m}^*})),$$

where $N_{K/k}$ denotes the norm map from $J_{K\mathfrak{m}^*}$ to $J_{k\mathfrak{m}}$.

(2) *Let H_C be the subgroup of $J_{K\mathfrak{m}^*}$ corresponding to the central class field of K/k modulo $\mathfrak{m}$ (i.e., in particular, $J_{K\mathfrak{m}^*}/H_C \cong \mathrm{Gal}\,(\widehat{K}(\mathfrak{m})/K)$). Then we have*

$$H_C = J_{K\mathfrak{m}^*}^D K_{(\mathfrak{m}^*)} W_{K\mathfrak{m}^*},$$

where $J_{K\mathfrak{m}^*}^D = \langle \alpha^{\sigma-1} \mid \alpha \in J_{K\mathfrak{m}^*}, \sigma \in \mathrm{Gal}\,(K/k)\rangle$.

From this lemma we can prove the following theorem. A. Scholz [16] first obtained the results of this type, and in the case $\mathfrak{m} = 1$ or $\mathfrak{m} = \infty$, this theorem is classical. S. Shirai [18] proved this theorem for some $\mathfrak{m}$. F. P. Heider [10] obtained the results of this type in the general situation. Here we give a direct proof from Lemma 3.1.

THEOREM 3.1. *There is a homomorphism*

$$\phi : k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}) \longrightarrow \mathrm{Gal}\,(\widehat{K}(\mathfrak{m})/K^*(\mathfrak{m}))$$

such that the sequence

$$1 \longrightarrow (E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/(E_{k(\mathfrak{m})} \cap N_{K/k}(K_{(\mathfrak{m}^*)})) \longrightarrow$$
$$(k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \xrightarrow{\phi} \mathrm{Gal}\,(\widehat{K}(\mathfrak{m})/K^*(\mathfrak{m})) \longrightarrow 1$$

is exact.

PROOF. We first define an epimorphism ψ:

$$H_G \longrightarrow (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/(E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))N_{K/k}(K_{(\mathfrak{m}^*)})$$

as follows. Let $x \in H_G$. Then by Lemma 3.1 for some $y \in k_{(\mathfrak{m})}$ and $w \in W_{K\mathfrak{m}^*}$ we can write $N_{K/k}(x) = yN_{K/k}(w)$. Since $y = N_{K/k}(xw^{-1}) \in N_{K/k}(J_{K\mathfrak{m}^*})$, we have $y \in k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*})$. Then we define $\psi(x)$ using y as follows:

$$\psi(x) = y \mod (E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))N_{K/k}(K_{(\mathfrak{m}^*)}).$$

It is easy to check that ψ is well defined and an epimorphism.

Now, we prove the kernel of ψ is H_C. Let $x \in H_C$. Then by Lemma 3.1 we can write $x = wyv$ for some $w \in J^D_{K\mathfrak{m}^*}$, $y \in K_{(\mathfrak{m}^*)}$, and $v \in W_{K\mathfrak{m}^*}$. Since $N_{K/k}(w) = 1$, we see that $N_{K/k}(x) = N_{K/k}(y)N_{K/k}(v)$. Hence by the definition of ψ, we have

$$\psi(x) = N_{K/k}(y) \mod (E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))N_{K/k}(K_{(\mathfrak{m}^*)}) = 1.$$

This shows $H_C \subset \ker\psi$. Conversely, assume $\psi(x) = 1$ for $x \in H_G$. Then there exist $z \in (E_{K(\mathfrak{m})} \cap N_{K/k}(J_{k\mathfrak{m}^*}))$, $v \in K_{(\mathfrak{m}^*)}$, and $w \in W_{K\mathfrak{m}^*}$ such that $N_{K/k}(x) = zN_{K/k}(v)N_{K/k}(w)$. Furthermore using (1.5) we can write $z = N_{K/k}(u)$ for some $u \in W_{K\mathfrak{m}^*}$. Hence we have $xu^{-1}v^{-1}w^{-1} \in J_{K\mathfrak{m}^*}$ and $N_{K/k}(xu^{-1}v^{-1}w^{-1}) = 1$. On the other hand by semilocal theory we know

$$\begin{aligned} H^{-1}(G, J_{K\mathfrak{m}^*}/W_{K\mathfrak{m}^*}) &= H^{-1}(G, \sum_{\substack{\mathfrak{P}\nmid\mathfrak{m}^* \\ \mathfrak{P}:\text{finite}}} K^\times_{\mathfrak{P}}/U(K_{\mathfrak{P}})) \\ &= \sum_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}:\text{finite}}} H^{-1}(G_{\mathfrak{p}}, K^\times_{\mathfrak{P}}/U(K_{\mathfrak{P}})) = \sum_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}:\text{finite}}} H^{-1}(G_{\mathfrak{p}}, \mathbb{Z}) = 1, \end{aligned}$$

where $G = \mathrm{Gal}\,(K/k)$, $\mathfrak{P}$ is a prime of K, $\mathfrak{p}$ is the prime of k divided by $\mathfrak{P}$, and $G_{\mathfrak{p}}$ is the decomposition group of a prime factor $\mathfrak{P}$ of $\mathfrak{p}$. Thus we can write $xu^{-1}v^{-1}w^{-1} = st$ for some $s \in J^D_{K\mathfrak{m}^*}$ and $t \in W_{K\mathfrak{m}^*}$. Hence by Lemma 3.1 we have $x = uvwst \in H_C$. This proves $\ker\psi = H_C$ and consequently $\ker\psi = H_C$. Thus we have proved that

$$H_G/H_C \cong (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/(E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))N_{K/k}(K_{(\mathfrak{m}^*)}).$$

Now by class field theory we know $H_G/H_C \cong \mathrm{Gal}\,(\widehat{K}(\mathfrak{m})/K^*(\mathfrak{m}))$. Therefore from the exact sequence

$$\begin{aligned} 1 \longrightarrow\ & (E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/(E_{k(\mathfrak{m})} \cap N_{K/k}(K_{(\mathfrak{m}^*)})) \longrightarrow \\ & (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \longrightarrow \\ & \quad (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/(E_{k(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))N_{K/k}(K_{(\mathfrak{m}^*)}) \longrightarrow 1 \end{aligned}$$

the theorem follows. This completes the proof.

From the theorem together with Corollary 1 of Theorem 1.1 we have the following Corollary 1, which gives a central class number formula modulo $\mathfrak{m}$.

COROLLARY 1. *Let the notations and the assumptions be the same as in Theorem* 1.1. *Then*

$$\begin{aligned} [\widehat{K}(\mathfrak{m}) : K] &= \#(J_{k\mathfrak{m}}/k_{(\mathfrak{m})}W_{k\mathfrak{m}}) \\ &\times \frac{\prod_{\mathfrak{p}|\mathfrak{f}} \#(V'_{\mathfrak{p}}(v'_{\mathfrak{p}}(e(\mathfrak{p}))))[(k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*})) : N_{K/k}(K_{(\mathfrak{m}^*)})]}{[K' : k][E_{k(\mathfrak{m})} : (E_{k(\mathfrak{m})} \cap N_{K/k}(K_{(\mathfrak{m}^*)}))]}. \end{aligned}$$

This corollary generalizes the central class number formula of Y. Furuta [5, Satz 1] to that of modulo $\mathfrak{m}$.

From Theorem 3.1 we can also deduce a relation between Hasse norm principle modulo $\mathfrak{m}$ and the central extension $\widehat{K}(\mathfrak{m})$. We define the Hasse norm principle modulo $\mathfrak{m}$ of K/k as follows.

DEFINITION 3.2. Let $\mathfrak{m}$ be a modulus of k. If

$$k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}) = N_{K/k}(K_{(\mathfrak{m}^*)}),$$

then we say that K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$.

Moreover, if

$$E_{k(\mathfrak{m})} \cap N_{K/k}(J_{k\mathfrak{m}^*}) = E_{k(\mathfrak{m})} \cap N_{K/k}(K_{\mathfrak{m}^*}),$$

then we say that K/k satisfies the Hasse norm principle for units modulo $\mathfrak{m}$.

In the case $\mathfrak{m} = 1$ the above definition coincides with the ordinary Hasse norm principle. Under this definition the following corollary is immediately obtained.

COROLLARY 2. *K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$ if and only if $\widehat{K}(\mathfrak{m}) = K^*(\mathfrak{m})$ and K/k satisfies the Hasse norm principle for units modulo $\mathfrak{m}$.*

Let ℓ be a prime number. In the case where the ray class number modulo $\mathfrak{m}$ of k is prime to ℓ and K/k is an ℓ-extension, we have a relation between the Hasse norm principle modulo $\mathfrak{m}$ of K/k and the ray class number of K modulo $\mathfrak{m}^*$.

DEFINITION 3.3. Let $\mathfrak{m}$ be a modulus of k and let K/k be a finite Galois extension. Let $\mathfrak{m}^*$ denote the lifting modulus of $\mathfrak{m}$ from k to K. We denote the ray class number of K modulo $\mathfrak{m}^*$ by $h(K, \mathfrak{m}^*)$, and call it the $\mathfrak{m}^*$-*class number of* K.

COROLLARY 3. *Let ℓ be a prime number. Let K/k be a finite Galois ℓ-extension such that $[K^*(\mathfrak{m}) : K]$ is prime to ℓ. Then K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$ if and only if $h(K, \mathfrak{m}^*)$ is prime to ℓ and K/k satisfies the Hasse norm principle for units modulo $\mathfrak{m}$.*

PROOF. Since $[K : k]$ is a power of ℓ, $k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*})/N_{K/k}(K_{(\mathfrak{m}^*)})$ is an ℓ-group. Hence by our theorem, $\mathrm{Gal}\,(\widehat{K}(\mathfrak{m})/K^*(\mathfrak{m}))$ is also an ℓ-group. Therefore, by Corollary 2, it suffices to prove that $\ell \mid h(K, \mathfrak{m}^*)$ if and only if $\ell \mid [\widehat{K}(\mathfrak{m}) : K^*(\mathfrak{m})]$. We use the notation of Lemma 3.1. Put $R = J_{K\mathfrak{m}^*}/K_{(\mathfrak{m}^*)}W_{K\mathfrak{m}^*}$, $\overline{H}_G = H_G/K_{(\mathfrak{m}^*)}W_{K\mathfrak{m}^*}$, and $\overline{H}_C = H_C/K_{(\mathfrak{m}^*)}W_{K\mathfrak{m}^*}$. Then by Lemma 3.1 R is a finite abelian group and $\overline{H}_C = R^D$, where $D = \{\Sigma n_\sigma \sigma \mid \Sigma n_\sigma = 0\} \subset \mathbb{Z}[G]$ and $G = \mathrm{Gal}\,(K/k)$. Moreover we have $\#(R) = h(K, \mathfrak{m}^*)$, $[\widehat{K}(\mathfrak{m}) : K^*(\mathfrak{m})] = \#(\overline{H}_G/\overline{H}_C)$, and $[K^*(\mathfrak{m}) : K] = \#(R/\overline{H}_G)$. Since R is a finite abelian group, it holds that $\ell \mid \#(R)$ if and only if $\ell \mid \#(R/R^D)$. On the other hand $\#(R/R^D) = \#(R/\overline{H}_G)\#(\overline{H}_G/\overline{H}_C)$ and $\ell \nmid \#(R/H_G)$ by the assumption; therefore, we see that $\ell \mid \#(R/R^D)$ if and only if $\ell \mid [\widehat{K}(\mathfrak{m}) : K^*(\mathfrak{m})]$. Thus we have $\ell \mid h(K, \mathfrak{m}^*)$ if and only if $\ell \mid [\widehat{K}(\mathfrak{m}) : K^*(\mathfrak{m})]$. This proves the corollary.

3.2. The Hasse norm principle modulo $\mathfrak{m}$ and finite Galois extensions. In this subsection we study the Hasse norm principle modulo $\mathfrak{m}$ for finite Galois extensions; in particular , for finite abelian extensions.

Let $\mathfrak{m}$ be a modulus of k satisfying (A2.2), i.e., $\mathfrak{m}$ is a product of distinct primes of k. Let K/k be a finite Galois extension such that $[K : k]$ is prime to $\mathfrak{m}$. Then the number knot modulo $\mathfrak{m}^*$, $(k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)})$, is expressed by the decomposition groups $G(\mathfrak{p})$ of the primes $\mathfrak{p}$ ramified in K/k.

THEOREM 3.2. *Let $\mathfrak{m}$ be a modulus of k such that $\mathfrak{m}$ is a product of distinct primes of k. Let K/k be a finite Galois extension such that $[K : k]$ is prime to $\mathfrak{m}$. Put $G = \mathrm{Gal}\,(K/k)$ and let S denote the set of those primes of k which are prime to $\mathfrak{m}$ and ramified in K/k. For every prime $\mathfrak{p} \in S$ we choose a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K and denote the decomposition group of $\mathfrak{P}$ in K/k by $G(\mathfrak{P})$. Then we have*

$$(k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \cong \mathrm{Coker}\Big(\sum_{\mathfrak{p}\in S} H^{-3}(G(\mathfrak{P}), \mathbb{Z}) \to H^{-3}(G, \mathbb{Z})\Big),$$

where $\sum_{\mathfrak{p}\in S} H^{-3}(G(\mathfrak{P}), \mathbb{Z}) \to H^{-3}(G, \mathbb{Z})$ is the homomorphism induced from the corestriction maps.

PROOF. Let C_K denote the idele class group of K, i.e., $C_K = J_K/K^\times = J_{K\mathfrak{m}^*}/K_{(\mathfrak{m}^*)}$. We start with a following exact sequence.

$$1 \longrightarrow K_{(\mathfrak{m}^*)} \xrightarrow{i} J_{K\mathfrak{m}^*} \xrightarrow{j} C_K \longrightarrow 1$$

Taking Tate cohomology groups we have the following exact sequence.

$$H^{-1}(G, J_{K\mathfrak{m}^*}) \xrightarrow{j^\#} H^{-1}(G, C_K) \xrightarrow{\delta^\#} H^0(G, K_{(\mathfrak{m}^*)}) \xrightarrow{i^\#} H^0(G, J_{K\mathfrak{m}^*})$$

By definition we have

$$\begin{aligned} H^0(G, K_{(\mathfrak{m}^*)}) &= (k \cap K_{(\mathfrak{m}^*)})/N_{K/k}(K_{(\mathfrak{m}^*)}), \quad \text{and} \\ H^0(G, J_{K\mathfrak{m}^*}) &= (J_k \cap J_{K\mathfrak{m}^*})/N_{K/k}(J_{K\mathfrak{m}^*}). \end{aligned}$$

Therefore we see that

$$\operatorname{Ker} i^\# = k \cap K_{(\mathfrak{m}^*)} \cap N_{K/k}(J_{K\mathfrak{m}^*})/N_{K/k}(K_{(\mathfrak{m}^*)}).$$

Furthermore, since $\mathfrak{m}$ is a product of distinct primes of k by assumption, we see that $k \cap K_{(\mathfrak{m}^*)} \cap N_{K/k}(J_{K\mathfrak{m}^*}) = k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*})$, and hence

$$\operatorname{Ker} i^\# = (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}).$$

Thus we have

$$\begin{aligned} (k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) &= \operatorname{Ker} i^\# = \operatorname{Im} \delta^\# \\ &\cong H^{-1}(G, C_K)/j^\#(H^{-1}(G, J_{K\mathfrak{m}^*})). \end{aligned} \tag{3.1}$$

The key part of our proof is to calculate $j^\#(H^{-1}(G, J_{K\mathfrak{m}^*}))$. Let $\mathfrak{p}$ be a prime of k dividing $\mathfrak{m}$. We choose a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in K, and denote its decomposition group in K/k by $G(\mathfrak{P})$.Then it holds that

$$H^{-1}(G(\mathfrak{P}), U(K_\mathfrak{P})^{(1)}) = 1. \tag{3.2}$$

Indeed, let $T(\mathfrak{P})$ and K_T denote the inertia group and the inertia field of $\mathfrak{P}$ in $K_\mathfrak{P}/k_\mathfrak{p}$, respectively. Since $\mathfrak{m}$ is prime to $[K : k]$ by assumption, we see that $K_\mathfrak{P}/K_T$ is at most tamely ramified, and $T(\mathfrak{P})$ is cyclic. Therefore, by Lemma 1.1 and (1.10) it follows that

$$N_{K_\mathfrak{P}/K_T}(U(K_\mathfrak{P})^{(1)}) = U(K_T)^{(1)} = K_T \cap U(K_\mathfrak{P})^{(1)}.$$

This means, in particular, $H^0(T(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) = 1$. Hence we have the following exact Corestriction-Deflation sequence (see e.g., E. Weiss [20, Theorem 1]).

$$\begin{aligned} H^{-1}(T(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) &\xrightarrow{\text{Cor}} H^{-1}(G(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) \\ &\xrightarrow{\text{Defl}} H^{-1}(G(\mathfrak{P})/T(\mathfrak{P}), U(K_T)^{(1)}) \longrightarrow 1. \end{aligned}$$

On the other hand, since $K_T/k_{\mathfrak{p}}$ is unramified, we have

$$N_{K_T/k_{\mathfrak{p}}}(U(K_T)^{(1)}) = U(k_{\mathfrak{p}})^{(1)} = k_{\mathfrak{p}} \cap U(K_T)^{(1)},$$

and $H^0(G(\mathfrak{P})/T(\mathfrak{P}), U(K_T)^{(1)}) = 1$. Since $G(\mathfrak{P})/T(\mathfrak{P})$ is cyclic, we can take the Herbrand quotient and see that $H^{-1}(G(\mathfrak{P})/T(\mathfrak{P}), U(K_T)^{(1)}) = 1$. Thus we have the following exact sequence.

$$H^{-1}(T(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) \xrightarrow{\text{Cor}} H^{-1}(G(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) \longrightarrow 1 \tag{3.3}$$

Since $T(\mathfrak{P})$ is a cyclic group and $H^0(T(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) = 1$, we see that $H^{-1}(T(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) = 1$ by taking Herbrand quotient. Therefore, by (3.3) we have $H^{-1}(G(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) = 1$. This proves (3.2).

Now for a prime $\mathfrak{p}$ of k put

$$U(K_{\mathfrak{p}})^{(1)} = \prod_{\mathfrak{P}|\mathfrak{p}} U(K_{\mathfrak{P}})^{(1)}, \quad K_{\mathfrak{p}}^{\times} = \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}^{\times}.$$

Then by semilocal theory we know

$$\begin{aligned} H^{-1}(G, K_{\mathfrak{p}}^{\times}) &\cong H^{-1}(G(\mathfrak{P}), K_{\mathfrak{P}}^{\times}), \\ H^{-1}(G, U(K_{\mathfrak{p}})^{(1)}) &\cong H^{-1}(G(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}). \end{aligned}$$

If $\mathfrak{p} \nmid \mathfrak{m}$ and $\mathfrak{p} \notin S$, then $\mathfrak{p}$ is unramified ; hence $H^{-1}(G, K_{\mathfrak{p}}^{\times}) \cong H^{-1}(G(\mathfrak{P}), K_{\mathfrak{P}}^{\times}) = 1$. Furthermore, if $\mathfrak{p} \mid \mathfrak{m}$, then $H^{-1}(G, U(K_{\mathfrak{p}})^{(1)}) \cong H^{-1}(G(\mathfrak{P}), U(K_{\mathfrak{P}})^{(1)}) = 1$ by (3.2). Thus we obtain $H^{-1}(G, J_{K\mathfrak{m}^*}) \cong \sum_{\mathfrak{p}\in S} H^{-1}(G(\mathfrak{P}), K_{\mathfrak{P}}^{\times})$. For simplicity we consider $H^{-1}(G(\mathfrak{P}), K_{\mathfrak{P}}^{\times})$ a subgroup of $H^{-1}(G, J_{K\mathfrak{m}^*})$. Thus from (3.1) it follows that

$$\begin{aligned} &(k_{(\mathfrak{m})} \cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \\ &\quad \cong H^{-1}(G, C_K)/j^{\#}\Big(\sum_{\mathfrak{p}\in S} H^{-1}(G(\mathfrak{P}), K_{\mathfrak{P}}^{\times})\Big). \end{aligned} \tag{3.4}$$

Now class field theory gives the following commutative diagram.

$$
\begin{array}{ccc}
H^{-3}(G(\mathfrak{P}),\mathbb{Z}) & \xrightarrow{\text{Cor}} & H^{-3}(G,\mathbb{Z}) \\
\wr\| & & \wr\| \\
H^{-1}(G(\mathfrak{P}),K_{\mathfrak{P}}^{\times}) & \xrightarrow{j^{\#}} & H^{-1}(G,C_K),
\end{array}
\tag{3.5}
$$

where $H^{-1}(G(\mathfrak{P}),K_{\mathfrak{P}}^{\times})$ is naturally considered as a subgroup of $H^{-1}(G,J_{K\mathfrak{m}^*})$. Let ϕ denote the homomorphism of the direct sum $\sum_{\mathfrak{p}\in S} H^{-3}(G(\mathfrak{P}),\mathbb{Z})$ to $H^{-3}(G,\mathbb{Z})$ induced from corestriction maps. Then (3.4) with (3.5) becomes

$$
\begin{aligned}
&(k_{(\mathfrak{m})}\cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \\
&\qquad\cong H^{-3}(G,\mathbb{Z})/\phi\Big(\sum_{\mathfrak{p}\in S} H^{-3}(G(\mathfrak{P}),\mathbb{Z})\Big).
\end{aligned}
$$

This completes the proof.

In the case where K/k is an abelian extension, the right hand of the formula in the theorem above is expressed more explicitly.

THEOREM 3.3. *Let the assumptions and the notations be as in Theorem* 3.2. *Furthermore assume that K/k is a finite abelian extension. Then we have*

$$
\begin{aligned}
&(k_{(\mathfrak{m})}\cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)}) \\
&\qquad\cong \operatorname{Coker}\Big(\sum_{\mathfrak{p}\in S}\Lambda^2(G(\mathfrak{P}))\to\Lambda^2(G)\Big),
\end{aligned}
$$

where $\Lambda^2(G(\mathfrak{P}))$ and $\Lambda^2(G)$ denote the second exterior products of $G(\mathfrak{P})$ and G, respectively.

This theorem gives a generalization of M. Razar [15, Theorem 3] .

PROOF. Let the notations be as in the proof of Theorem 3.2. Let $\Lambda^2(G(\mathfrak{P}))$ and $\Lambda^2(G)$ denote the second exterior products of $G(\mathfrak{P})$ and G, respectively. Then by Hopf's formula these are naturally isomorphic to Schur multiplicators $H_2(G(\mathfrak{P}),\mathbb{Z}) = H^{-3}(G(\mathfrak{P}),\mathbb{Z})$ and $H_2(G,\mathbb{Z}) = H^{-3}(G,\mathbb{Z})$, respectively. Let $\psi_{\mathfrak{P}}$ denote the natural homomorphism $\Lambda^2(G(\mathfrak{P}))$ to $\Lambda^2(G)$. Then the following diagram commutes.

$$
\begin{array}{ccc}
\Lambda^2(G(\mathfrak{P})) & \xrightarrow{\psi_{\mathfrak{P}}} & \Lambda^2(G) \\
\wr\| & & \wr\| \\
H^{-3}(G(\mathfrak{P}),\mathbb{Z}) & \xrightarrow{\text{Cor}} & H^{-3}(G,\mathbb{Z})
\end{array}
$$

Let ψ denote the homomorphism of the direct sum $\sum_{\mathfrak{p}\in S}\Lambda^2(G(\mathfrak{P}))$ to $\Lambda^2(G)$ induced from $\psi_{\mathfrak{P}}$. Then (3.4) with (3.5) becomes

$$(k_{(\mathfrak{m})}\cap N_{K/k}(J_{K\mathfrak{m}^*}))/N_{K/k}(K_{(\mathfrak{m}^*)})$$
$$\cong \Lambda^2(G)/\psi\Big(\sum_{\mathfrak{p}\in S}\Lambda^2(G(\mathfrak{P}))\Big),$$

which proves our theorem.

In the case where K/k is abelian, all of the decomposition groups of prime divisors of a prime $\mathfrak{p}$ of k in K coincide. In what follows, therefore, we use the notation $G(\mathfrak{p})$ for the decomposition group instead of $G(\mathfrak{P})$.

From the definition of the Hasse norm principle modulo $\mathfrak{m}$ the following corollary follows immediately.

COROLLARY 1. *K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$ if and only if $\psi:\sum_{\mathfrak{p}\in S}\Lambda^2(G(\mathfrak{p}))\longrightarrow\Lambda^2(G)$ is surjective.*

Using properties of the second exterior products we can prove the following corollaries by arguments similar to M. Razar [15, §4].

COROLLARY 2. *If K/k is a cyclic extension, then K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$.*

COROLLARY 3. *Let M/k be a subextension of K/k. If K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$, then M/k also satisfies the Hasse norm principle modulo $\mathfrak{m}$.*

COROLLARY 4. *Let K_1 and K_2 be the subfields of K such that $K=K_1K_2$ and $[K_1:k]$ is prime to $[K_2:k]$. Then K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$ if and only if K_1/k and K_2/k satisfy the Hasse norm principle modulo $\mathfrak{m}$.*

COROLLARY 5. *Let ℓ be a prime number. Let K/k be a finite abelian ℓ-extension and let K_0/k be it's maximal elementary subextension. Then K/k satisfies the Hasse norm principle modulo $\mathfrak{m}$ if and only if K_0/k satisfies the Hasse norm principle modulo $\mathfrak{m}$.*

4. The Hasse norm principle and a generalization of a theorem of Fröhlich

D. Garbanati [6] studied the Hasse norm principle over $\mathbf{Q}$ and pointed out that there is an intimate relationship between the Hasse norm principle and the ℓ-divisibility of the class numbers of composite fields of finite abelian ℓ-extensions with prime power conductors.

The purpose of this section is to determine the fields which satisfy the Hasse norm principle modulo $\mathfrak{m}$ for a suitable $\mathfrak{m}$ in some classes of finite abelian ℓ-extensions K/k. As an application of this result we also determine the fields whose $\mathfrak{m}^*$-class number is prime to ℓ in some classes of finite abelian ℓ-extensions K/k. These give generalizations of the results of Fröhlich and Garbanati.

4.1. The Hasse norm principle and elementary abelian ℓ-extensions. By corollaries of Theorem 3.3 it suffices to study the Hasse norm principle modulo $\mathfrak{m}$ for elementary abelian ℓ-extensions for every prime number ℓ. Let $\mathfrak{m}$ be a finite product of primes of k and assume that the $\mathfrak{m}$-class number $h(k, \mathfrak{m})$ of k is prime to ℓ. The purpose of this subsection is to give a criterion for certain elementary abelian ℓ-extensions K/k to satisfy the Hasse norm principle modulo $\mathfrak{m}$.

DEFINITION 4.1. Let K/k be a finite abelian ℓ-extension. If the conductor of K/k is a power $\mathfrak{p}^e$ of a prime ideal $\mathfrak{p}$ of k up to factors of $\mathfrak{m}$, then we say that K/k has a prime power conductor $\mathfrak{p}^e$ modulo $\mathfrak{m}$.

We assume that $h(k, \mathfrak{m})$ is prime to ℓ; therefore, $\mathfrak{p}$ is totally ramified in K/k if K/k has a prime power conductor $\mathfrak{p}^e$ modulo $\mathfrak{m}$.

For the rest of this section let K/k denote a composite field of elementary abelian ℓ-extensions of k with a prime power conductor modulo $\mathfrak{m}$, i.e., let

$$K = \prod_{j=1}^{m} K_j, \tag{4.1}$$

where K_j have prime power conductors $\mathfrak{p}_j^{e_j}$ modulo $\mathfrak{m}$, and $\mathfrak{p}_j$ are distinct prime ideals of k prime to $\mathfrak{m}$.

The purpose of this subsection is to determine those extensions of this type which satisfy the Hasse norm principle modulo $\mathfrak{m}$. Put $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$; this is the set of those primes of k which are prime to $\mathfrak{m}$ and ramified in K/k. In the case where K_j/k is cyclic for $1 \leqq j \leqq m$, we define a character

$$[K/k, \ ; \mathfrak{p}_j] : k(\mathfrak{p}_j) \to \mathbb{Z}/\ell\mathbb{Z}$$

as follows, where $k(\mathfrak{p}_j)$ denotes the subgroup of $k^\times$ consisting of those elements prime to $\mathfrak{p}_j$. Let $T_j = T(\mathfrak{p}_j)$ denote the inertia group of $\mathfrak{p}_j$ in K/k. Then by assumption T_j is cyclic and isomorphic to $\mathrm{Gal}\,(K_j/k)$ by the restriction map. Choose a generator t_j of $\mathrm{Gal}\,(K_j/k)$ and fix it. We also consider t_j as a generator of T_j. Let

$$(K/k, \ ; \mathfrak{p}_j) : k^\times \to \mathrm{Gal}\,(K/k)$$

be the norm residue symbol of K/k at $\mathfrak{p}_j$. Then $(K/k; \mathfrak{p}_j)$ induces an epimorphism from $k(\mathfrak{p}_j)$ to T_j. Now for $x \in k(\mathfrak{p}_j)$ we define $[K/k, x; \mathfrak{p}_j]$ as an integer modulo ℓ

such that $(K/k, x; \mathfrak{p}_j) = t_j^{[K/k,x;\mathfrak{p}_j]}$. Similarly we define $[K_j/k, x; \mathfrak{p}_j]$ starting from K_j. Since $\mathfrak{p}_j$ is unramified in $\prod_{j\neq i} K_i$, $[K/k, x; \mathfrak{p}_j]$ coincides with $[K_j/k, x; \mathfrak{p}_j]$. Hence we may write $[K_j, x]$ instead of $[K/k, x; \mathfrak{p}_j]$. Then we have for $x \in k(\mathfrak{p}_j)$

$$(K/k, x; \mathfrak{p}_j) = (K_j/k, x; \mathfrak{p}_j) = t_j^{[K_j,x]}. \tag{4.2}$$

Furthermore, for $\mathfrak{p}_i \in S$, choose an element $\pi_i \in k$ such that

$$\mathfrak{p}_i^{h(k,\mathfrak{m})} = (\pi_i) \quad \text{and} \quad \pi_i \equiv 1 \mod \mathfrak{m}. \tag{4.3}$$

Since $\pi_i \in k(\mathfrak{p}_j)$ for $i \neq j$, $[K_j, \pi_i]$ is defined if K_j/k is cyclic. Furthermore $[K : k] = \prod_{j=1}^m \#(T_j)$ by (4.1); hence it follows from Corollary 1 to Theorem 1.1 that $\ell \nmid [K^*(\mathfrak{m}) : K]$ and $E_{k(\mathfrak{m})} \subset N_{K/k}(J_{K\mathfrak{m}^*})$. Hence for $\varepsilon \in E_{k(\mathfrak{m})}$ we have $[K_j, \varepsilon] = 0$. Thus $[K_j, \pi_i]$ does not depend on the choice of π_i satisfying (4.3). Using $[K_j, \pi_i]$ for $1 \leqq i, j \leqq m$ we can obtain a criterion for K/k to satisfy the Hasse norm principle modulo $\mathfrak{m}$.

We first note that the second exterior product $\Lambda^2(G)$ of an elementary abelian ℓ-group G has a simple group structure, i.e., if G has rank r, then $\Lambda^2(G)$ is an elementary abelian ℓ-group of rank $r(r-1)/2$. We use additive notation for $\Lambda^2(G)$ though G is written multiplicatively, and consider $\Lambda^2(G)$ as a vector space over $\mathbb{Z}/\ell\mathbb{Z}$. We start with a simple criterion obtained from calculating the dimensions over $\mathbb{Z}/\ell\mathbb{Z}$.

Let $[K : k] = \ell^v$ and $[K_j : k] = \ell^{u_j}$ for $j = 1, \dots, m$. Let $G(\mathfrak{p}_j)$ denote the decomposition group of a prime divisor of $\mathfrak{p}_j$ in K. Then $\sum_{j=1}^m u_j = v$. Furthermore $\operatorname{rank}(G(\mathfrak{p}_j)) \leqq u_j + 1$ because $G(\mathfrak{p}_j)/T(\mathfrak{p}_j)$ is cyclic. Hence

$$\dim\Big(\sum_{j=1}^m \Lambda^2(G(\mathfrak{p}_j))\Big) \leqq \sum_{j=1}^m \frac{u_j(u_j+1)}{2}.$$

On the other hand

$$\dim(\Lambda^2(G)) = \frac{v(v-1)}{2} = \sum_{j=1}^m \frac{u_j(v-1)}{2}.$$

Therefore if $u_j + 1 \leqq v - 1$ for $j = 1, \dots, m$ and $u_i + 1 < v - 1$ for some i $(1 \leqq i \leqq m)$, then $\dim(\sum_{j=1}^m \Lambda^2(G(\mathfrak{p}_j))) < \dim(\Lambda^2(G))$. Consequently ψ is not surjective, which implies by Corollary 1 of Theorem 3.3 that K/k dose not satisfy the Hasse norm principle modulo $\mathfrak{m}$. In particular we have the following.

(4.4) K/k dose not satisfy the Hasse norm principle modulo $\mathfrak{m}$ in the cases where
- (i) $m \geqq 4$,
- (ii) $m = 3$ and $v \geqq 4$,
- (iii) $m = 2$, $v = u_1 + u_2 \geqq 5$, and $u_j \geqq 2$ $(j = 1, 2)$.

We next prove a relation between $G(\mathfrak{p}_i)$ and $T(\mathfrak{p}_i)$ under some conditions. Let i be a positive integer with $1 \leqq i \leqq m$ and assume that $[K_j : k] = \ell$ for each $j \neq i$. Then $[K_j, \pi_i]$ and t_j are defined for each $j \neq i$. Put $s_i = \prod_{\substack{j=1 \\ j\neq i}}^{m} t_j^{[K_j,\pi_i]}$. Then we have

$$G(\mathfrak{p}_i) = \langle s_i \rangle \cdot T(\mathfrak{p}_i). \tag{4.5}$$

Indeed, since the image of $k^\times$ (resp. $k(\mathfrak{p}_i)$) by the norm residue symbol $(K/k; \mathfrak{p}_i)$ coincides with $G(\mathfrak{p}_i)$ (resp. $T(\mathfrak{p}_i)$), $G(\mathfrak{p}_i)$ is generated by $(K/k, \pi_i; \mathfrak{p}_i)$ and $T(\mathfrak{p}_i)$. Since, at most, only prime divisors of $\mathfrak{m} \cdot \prod_{j=1}^{m} \mathfrak{p}_j$ are ramified in K/k, by the product formula we have

$$\prod_{j=1}^{m} (K/k, \pi_i; \mathfrak{p}_j) \cdot \prod_{\mathfrak{q}|\mathfrak{m}} (K/k, \pi_i; \mathfrak{q}) = 1.$$

Since the divisors of $\mathfrak{m}$ are at most tamely ramified in K/k and $\pi_i \equiv 1 \mod \mathfrak{m}$, it follows that $\prod_{\mathfrak{q}|\mathfrak{m}} (K/k, \pi_i; \mathfrak{q}) = 1$. Hence $(K/k, \pi_i; \mathfrak{p}_i) = \prod_{\substack{j=1 \\ j\neq i}}^{m} (K/k, \pi_i; \mathfrak{p}_j)^{-1}$; this with (4.2) implies (4.5).

Now we divide the problem into several cases according to the number $\#(S)$.

I. *The case where* $\#(S) = 1$. *Then* K/k *satisfies the Hasse norm principle modulo* $\mathfrak{m}$.

PROOF. Let $S = \{\mathfrak{p}_1\}$. Then $K = K_1$, and $\mathfrak{p}_1$ is totally ramified in K/k. Therefore in this case $G(\mathfrak{p}_1) = T_1 = T(\mathfrak{p}_1) = G$. Hence $\psi : \Lambda^2 G(\mathfrak{p}_1) \to \Lambda^2 G$ is surjective.

II. *The case where* $\#(S) = 2$. *Let* $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$.

(1) *If* $[K : k] = \ell^2$, *i.e.*, $[K_1 : k] = [K_2 : k] = \ell$, *then* K/k *satisfies the Hasse norm principle modulo* $\mathfrak{m}$ *if and only if* $\operatorname{rank}([K_1, \pi_2], [K_2, \pi_1]) \geqq 1$.

(2) *If* $[K : k] \geqq \ell^3$, *then* K/k *satisfies the Hasse norm principle modulo* $\mathfrak{m}$ *just in the following two cases* (i) *and* (ii).

(i) $[K_1 : k] = \ell$ *and* $[K_1, \pi_2] \neq 0$.

(ii) $[K_2 : k] = \ell$ *and* $[K_2, \pi_1] \neq 0$.

PROOF. In this case, if $[K_j : k] = \ell$ for $\{i, j\} = \{1, 2\}$, then by (4.5) we have

$$\begin{aligned} G(\mathfrak{p}_i) &= T(\mathfrak{p}_i) && \text{if} \quad [K_j, \pi_i] = 0, \\ G(\mathfrak{p}_i) &= \langle t_j \rangle T(\mathfrak{p}_i) = G && \text{if} \quad [K_j, \pi_i] \neq 0. \end{aligned} \tag{4.6}$$

(1) Suppose $\operatorname{rank}([K_1, \pi_2], [K_2, \pi_1]) = 0$. Then $[K_1, \pi_2] = [K_2, \pi_1] = 0$. Hence by (4.6) we see that $G(\mathfrak{p}_1) = T(\mathfrak{p}_1) = \langle t_1 \rangle$ and $G(\mathfrak{p}_2) = T(\mathfrak{p}_2) = \langle t_2 \rangle$, which

implies $\sum_{j=1,2}\Lambda^2(G(\mathfrak{p}_j))=0$. On the other hand we have $\dim\Lambda^2(G)=2(2-1)/2=1$ because $G=\langle t_1,t_2\rangle$ in this case. Thus we have that ψ is not surjective.

Conversely, suppose rank $([K_1,\pi_2],[K_2,\pi_1])\geqq 1$. Then at least one of $[K_1,\pi_2]$ and $[K_2,\pi_1]$ is not zero. Let $[K_1,\pi_2]\neq 0$ for instance, then by (4.6) it follows that $G(\mathfrak{p}_2)=G$. Thus ψ is surjective.

(2) Suppose $[K_1:k]=\ell$. Then $[K_2:k]=\ell^u$ with $u\geqq 2$ by assumption. If $[K_1,\pi_2]\neq 0$, then $G(\mathfrak{p}_2)=G$ by (4.6), and hence ψ is surjective. Conversely if $[K_1,\pi_2]=0$, then $G(\mathfrak{p}_2)=T(\mathfrak{p}_2)$ by (4.6). On the other hand we have rank $(G(\mathfrak{p}_1))\leqq 2$ because $G(\mathfrak{p}_1)/T(\mathfrak{p}_1)$ is a cyclic group. Therefore, $\dim(\sum_{i=1,2}\Lambda^2(G(\mathfrak{p}_i)))\leqq\frac{2(2-1)}{2}+\frac{u(u-1)}{2}$. Furthermore, we have $\dim(\Lambda^2(G))=\frac{(u+1)u}{2}=\frac{2u}{2}+\frac{u(u-1)}{2}$. Hence $\dim(\sum_{i=1,2}\Lambda^2(G(\mathfrak{p}_i)))<\dim(\Lambda^2(G))$ and ψ is not surjective. In the case where $[K_2:k]=\ell$ similar argument holds. Hence if either $[K_1:k]=\ell$ or $[K_2:k]=\ell$, then the assertion is valid. We next consider the case where $[K_j:k]=\ell^{u_j}$ with $u_j\geqq 2$ for $j=1,2$. If $u_1>2$ or $u_2>2$, then by (4.4) ψ is not surjective. Finally we consider the case $u_1=2$ and $u_2=2$. If $G(\mathfrak{p}_1)=T(\mathfrak{p}_1)$ or $G(\mathfrak{p}_2)=T(\mathfrak{p}_2)$, then similarly to the above we see that ψ is not surjective. Hence the remaining case is the case rank $(G(\mathfrak{p}_1))=$ rank $(G(\mathfrak{p}_2))=3$. Since rank $(G)=4$, it follows that rank $(G(\mathfrak{p}_1)\cap G(\mathfrak{p}_2))=2$, so that

$$\dim(\Lambda^2(G(\mathfrak{p}_1))\cap\Lambda^2(G(\mathfrak{p}_2)))\geqq 1.$$

Hence we have

$$\dim\Big(\sum_{i=1,2}\Lambda^2(G(\mathfrak{p}_i))\Big)\leqq\frac{3\cdot 2}{2}+\frac{3\cdot 2}{2}-1<\dim(\Lambda^2(G))=\frac{4\cdot 3}{2}=6,$$

which shows that ψ is not surjective.

III. *The case where* $\#(S)=3$ *and* $[K:k]=\ell^3$. *Then* $[K_j:k]=\ell$ *and* $[K_j,\pi_i]$ *is defined for* $i,j=1,2,3$. *Then* K/k *satisfies the Hasse norm principle modulo* $\mathfrak{m}$ *if and only if*

$$\operatorname{rank}\begin{pmatrix}-[K_2,\pi_1], & -[K_3,\pi_1], & 0\\ [K_1,\pi_2], & 0, & -[K_3,\pi_2]\\ 0, & [K_1,\pi_3], & [K_2,\pi_3]\end{pmatrix}=3.$$

Proof. We use the notation in (4.5). Then $G(\mathfrak{p}_j)=\langle s_j\rangle\cdot\langle t_j\rangle$, and $\Lambda^2(G(\mathfrak{p}_j))=\langle s_j\wedge t_j\rangle$ for $j=1,2,3$. Moreover since $G=\langle t_1,t_2,t_2\rangle$, it follows that $t_1\wedge t_2$, $t_1\wedge t_3$, $t_2\wedge t_3$ form a basis of $\Lambda^2(G)$. Thus ψ is surjective if and only if $s_j\wedge t_j$ for $j=1,2,3$ are lineally independent over $\mathbb{Z}/\ell\mathbb{Z}$. On the other hand from (4.5) we have

$$s_1\wedge t_1=(t_2^{[K_2,\pi_1]}\cdot t_3^{[K_3,\pi_1]})\wedge t_1$$

$$
\begin{aligned}
&= [K_2, \pi_1](t_2 \wedge t_1) + [K_3, \pi_1](t_3 \wedge t_1) \quad \text{written additively} \\
&= -[K_2, \pi_1](t_1 \wedge t_2) - [K_3, \pi_1](t_1 \wedge t_3), \\
s_2 \wedge t_2 &= [K_1, \pi_2](t_1 \wedge t_2) - [K_3, \pi_2](t_2 \wedge t_3), \\
s_3 \wedge t_3 &= [K_1, \pi_3](t_1 \wedge t_3) + [K_2, \pi_3](t_2 \wedge t_3).
\end{aligned}
$$

Hence

$$
\begin{pmatrix} s_1 \wedge t_1 \\ s_2 \wedge t_2 \\ s_2 \wedge t_2 \end{pmatrix} = \begin{pmatrix} -[K_2, \pi_1], & -[K_3, \pi_1], & 0 \\ [K_1, \pi_2], & 0 & -[K_3, \pi_2] \\ 0, & [K_1, \pi_3], & [K_2, \pi_3] \end{pmatrix} \begin{pmatrix} t_1 \wedge t_2 \\ t_1 \wedge t_3 \\ t_2 \wedge t_3 \end{pmatrix}.
$$

Thus $s_j \wedge t_j$ for $j = 1, 2, 3$ are linearly independent over $\mathbb{Z}/\ell\mathbb{Z}$ if and only if

$$
\operatorname{rank} \begin{pmatrix} -[K_2, \pi_1], & -[K_3, \pi_1], & 0 \\ [K_1, \pi_2], & 0, & -[K_3, \pi_2] \\ 0, & [K_1, \pi_3], & [K_2, \pi_3] \end{pmatrix} = 3,
$$

which proves our assertion.

The following cases IV and V are contained in (4.4).

IV. *The case where* $\#(S) = 3$ *and* $[K : k] \geqq \ell^4$. *Then* K/k *does not satisfy the Hasse norm principle modulo* $\mathfrak{m}$.

V. *The case where* $\#(S) = 4$. *Then* K/k *does not satisfy the Hasse norm principle modulo* $\mathfrak{m}$.

Summarizing the cases I,... ,V we have the following theorem.

THEOREM 4.1. *Let the notation be as above. Let* K/k *be a composite field of elementary abelian* ℓ*-extensions of* k *with a prime power conductor modulo* $\mathfrak{m}$. *Then* K/k *satisfies the Hasse norm principle modulo* $\mathfrak{m}$ *if and only if* K/k *is in one of the following cases.*

I. $\#(S) = 1$.

II. $\#(S) = 2$ *and*

(i) $[K_1 : k] = \ell$ *and* $[K_1, \pi_2] \neq 0$,

or

(ii) $[K_2 : k] = \ell$ *and* $[K_2, \pi_1] \neq 0$.

III. $\#(S) = 3$, $[K : k] = \ell$, *and*

$$
\operatorname{rank} \begin{pmatrix} -[K_2, \pi_1], & -[K_3, \pi_1], & 0 \\ [K_1, \pi_2], & 0, & -[K_3, \pi_2] \\ 0, & [K_1, \pi_3], & [K_2, \pi_3] \end{pmatrix} = 3.
$$

4.2. A generalization of a theorem of Fröhlich. In this subsection we give a generalization of Fröhlich's theorem on the ℓ-divisibility of the class numbers of ℓ-abelian fields as an application of Theorem 2.1 and Theorem 4.1.

Let ℓ be a prime number and N a power of ℓ. Let k be an algebraic number field of finite degree and assume $\ell \nmid h(k)$. Let $\mathfrak{m}$ be a modulus of k satisfying (A2.1) $\sim$ (A2.4). Then by Lemma 2.2 we see that $\ell \nmid h(k, \mathfrak{m})$. Let K/k be a finite abelian ℓ-extension whose exponent divides N. Now we give a criterion for the $\mathfrak{m}^*$-class number $h(K, \mathfrak{m}^*)$ of K to be prime to ℓ.

If $\ell \mid [K^*(\mathfrak{m}) : K]$, then $\ell \mid h(K, \mathfrak{m}^*)$ by the definition of the genus field modulo $\mathfrak{m}$. Hence it suffices to consider the case where $\ell \nmid [K^*(\mathfrak{m}) : K]$. By Theorem 2.1 we can write $K^*(\mathfrak{m}) = k^{(\mathfrak{m})} \cdot \prod_{j=1}^{m} K_j$, where $k^{(\mathfrak{m})}$ denotes the ray class field of k modulo $\mathfrak{m}$ and K_j are fields with distinct prime power conductors modulo $\mathfrak{m}$. Therefore the assumptions $\ell \nmid h(k, \mathfrak{m})$ and $\ell \nmid [K^*(\mathfrak{m}) : K]$ imply $K = \prod_{j=1}^{m} K_j$, i.e., K is a composite field of abelian ℓ-extensions with prime power conductors modulo $\mathfrak{m}$. Though K is not assumed to be elementary, Fröhlich's results suggests that the essential part is in the elementary case. Indeed, similarly to the Hasse norm principle modulo $\mathfrak{m}$ (Corollary 5 of Theorem 3.3), the problem of the ℓ-divisibility of $\mathfrak{m}^*$-class numbers is reduced to the elementary case as we now see it.

For the technical reason we state the result in a slightly more general situation.

PROPOSITION 4.1. *Let ℓ be a prime number, k an algebraic number field of finite degree, and $\mathfrak{m}$ a finite product of distinct primes of k prime to ℓ. Let F/k be a finite abelian ℓ-extension. For $j = 1, \dots, m$, let L_j/F be a finite abelian ℓ-extension which is also abelian over k, and let L'_j/F be the maximal elementary subextension of L_j/F. Assume that L_j satisfies the following conditions* (1), (2), *and* (3) *for $j = 1, \dots, m$;*

(1) *there is a prime $\mathfrak{p}_j$ of F such that $\mathfrak{p}_j$ is prime to $\mathfrak{m}$ and ramified in L_j/F,*

(2) *all primes of F which are prime to $\mathfrak{m}$ and ramified in L_j/F are totally ramified in L_j/F,*

(3) *all primes of F which are prime to $\mathfrak{m}$ and ramified in L_j/F are unramified in L_j/F for every $i \neq j$.*

Then

$$\ell \nmid h\left(\prod_{j=1}^{m} L_j, \mathfrak{m}^*\right) \quad \textit{if and only if} \quad \ell \nmid h\left(\prod_{j=1}^{m} L'_j, \mathfrak{m}^*\right).$$

PROOF. We first note that $\mathfrak{m}^*$ is a finite product of distinct primes in any abelian extension over k because $\mathfrak{m}$ is a finite product of distinct primes of k by the assumption made. We prove by induction on m.

I. The case $m = 1$. (i) We first consider the case where L_1/F is cyclic. If $\ell \mid h(L'_1, \mathfrak{m}^*)$, then clearly $\ell \mid h(L_1, \mathfrak{m}^*)$ because there is a prime of F which is prime to $\mathfrak{m}^*$ and totally ramified in L_1.

Conversely, assume $\ell \mid h(L_1, \mathfrak{m}^*)$. Let L/L_1 be the ℓ-part of the ray class field over L_1 modulo $\mathfrak{m}^*$. Since there is a prime of F which is prime to $\mathfrak{m}^*$ and totally ramified in L_1, the Galois extension L/F is not cyclic. Therefore, there is a cyclic extension N/F of degree ℓ such that $N \subset L$ and $N \cap L_1 = F$. If $\ell \nmid h(L_1', \mathfrak{m}^*)$, then there is a prime $\mathfrak{P}$ of L_1' which is prime to $\mathfrak{m}$ and ramified in $L_1'N/L_1'$. Let $\mathfrak{p}$ be the prime of F below $\mathfrak{P}$. Since $\mathfrak{p}$ is ramified in L/F and the prime divisors of $\mathfrak{p}$ in L are unramified in L/L_1, it follows that $\mathfrak{p}$ is ramified in L_1/F; hence by the assumption (2) $\mathfrak{p}$ is totally ramified in L_1; consequently $\mathfrak{p}$ is totally ramified in L_1'. Hence $\mathfrak{p}$ is totally ramified in $L_1'N/F$. Let $\mathfrak{P}'$ be the prime divisor of $\mathfrak{p}$ in N. Since L_1N/N is a cyclic extension and $\mathfrak{P}'$ is ramified in $L_1'N/N$, it follows that $\mathfrak{P}'$ is totally ramified in L_1N/N. Thus $\mathfrak{p}$ is totally ramified in L_1N/F; in particular, the prime divisor of $\mathfrak{p}$ in L_1 is ramified in L_1N/L_1, which contradicts $N \subset L$. Thus we have $\ell \mid h(L_1', \mathfrak{m}^*)$, which proves the assertion in our case.

(ii) We prove the general case (for $m = 1$) by induction on rank $(\mathrm{Gal}\,(L_1/F))$. Assume that the assertion holds for the case rank $(\mathrm{Gal}\,(L_1/F)) = r$. We must prove the assertion holds for the case rank $(\mathrm{Gal}\,(L_1/F)) = r+1$. Let rank $(\mathrm{Gal}\,(L_1/F)) = r+1$. If $\ell \mid h(L_1', \mathfrak{m}^*)$, then similarly to (i) we have $\ell \mid h(L_1, \mathfrak{m}^*)$. Conversely assume $\ell \mid h(L_1, \mathfrak{m}^*)$. Then we can take extensions L_{11} and L_{12} of F such that $L_1 = L_{11} \cdot L_{12}$, $L_{11} \cap L_{12} = F$, and L_{12}/F is cyclic. Let L_{12}' be the maximal elementary subextension of L_{12}/F, i.e., the subextension of L_{12}/F of degree ℓ. Then $L_{11}L_{12}'/L_{11}$ is the maximal elementary subextension of L_1/L_{11}. Hence by (i) (with $F = L_{11}$) we have $\ell \mid h(L_{11}L_{12}', \mathfrak{m}^*)$. Next let L_{11}' be the maximal elementary subextension of L_{11}/F. Then by the assumption of the induction it follows that $\ell \mid h(L_{11}'L_{12}', \mathfrak{m}^*)$ since $L_{11}'L_{12}'$ is the maximal elementary subextension of L_1L_{12}'/L_{12}'. Since $L_{11}'L_{12}' = L_1'$, this completes the proof in our case.

II. Assume the proposition holds for the case $m = r$. Let us consider the case $m = r+1$. If $\ell \nmid h(\prod_{j=1}^{r+1} L_j, \mathfrak{m}^*)$, then $\ell \nmid h(\prod_{j=1}^{r+1} L_j', \mathfrak{m}^*)$ since there is a prime of $\prod_{j=1}^{r} L_j$ prime to $\mathfrak{m}^*$ which is totally ramified in $\prod_{j=1}^{r+1} L_j$ by the assumption (1), (2), and (3). Conversely suppose $\ell \mid h(\prod_{j=1}^{r+1} L_j, \mathfrak{m}^*)$. Since $\mathrm{Gal}\,(\prod_{j=1}^{r+1} L_j / \prod_{j=1}^{r} L_j) \cong \mathrm{Gal}\,(L_{r+1}/F)$ and the primes of F which are prime to $\mathfrak{m}$ and ramified in L_{r+1} are unramified in $\prod_{j=1}^{r} L_j$ by the assumption made, we see that the primes of $\prod_{j=1}^{r} L_j$ which are prime to $\mathfrak{m}$ and ramified in $\prod_{j=1}^{r+1} L_j$ are totally ramified in $\prod_{j=1}^{r+1} L_j$. Hence by the result I (with $F = \prod_{j=1}^{r} L_j$) we have $\ell \mid h((\prod_{j=1}^{r} L_j) \cdot L_{r+1}', \mathfrak{m}^*)$. On the other hand the extension $(\prod_{j=1}^{r} L_j)L_{r+1}' = \prod_{j=1}^{r}(L_jL_{r+1}')$ of L_{r+1}' satisfies the assumption of the proposition with $F = L_{r+1}'$ and $m = r$. Hence by the assumption of the induction it follows that $\ell \mid h(\prod_{j=1}^{r} L_j'L_{r+1}', \mathfrak{m}^*)$, i.e., $\ell \mid h(\prod_{j=1}^{r+1} L_j, \mathfrak{m}^*)$. This completes the proof.

The following corollary is a special case of the above proposition.

COROLLARY. *Let ℓ be a prime number and N a power of ℓ. Let k be an*

algebraic number field. Let $\mathfrak{m}$ *be a modulus of* k *satisfying* (A2.1) $\sim$ (A2.4). *Let* K *be a composite field of abelian* ℓ*-extensions with a prime power conductor modulo* $\mathfrak{m}$ *whose exponent divides* N. *Let* K' *be the maximal elementary subextension of* K/k. *Then* $\ell \mid h(K, \mathfrak{m}^*)$ *if and only if* $\ell \mid h(K', \mathfrak{m}^*)$.

By this corollary it is sufficient to determine the elementary abelian ℓ-extensions K/k whose $\mathfrak{m}^*$-class number $h(K, \mathfrak{m}^*)$ is prime to ℓ.

Now by Corollary 3 of Theorem 3.1 and Theorem 4.1 we have immediately the following result.

THEOREM 4.2. *Let* K/k *be a composite field of elementary abelian* ℓ*-extensions of* k *with a prime power conductor modulo* $\mathfrak{m}$.

(1) *In the following cases* I, II, III *it holds that* $\ell \nmid h(K, \mathfrak{m}^*)$.

(2) *If* K/k *satisfies the Hasse norm principle for units modulo* $\mathfrak{m}$, *then* $\ell \nmid h(K, \mathfrak{m}^*)$ *in exactly the following cases* I, II, III.

I. $\#(S) = 1$.

II. $\#(S) = 2$ *and either*

(i) $[K_1 : k] = \ell$ *and* $[K_1, \pi_2] \neq 0$,

or

(ii) $[K_2 : k] = \ell$ *and* $[K_2, \pi_1] \neq 0$.

III. $\#(S) = 3$, $[K : k] = \ell^3$, *and*

$$\operatorname{rank}\begin{pmatrix} -[K_2, \pi_1], & -[K_3, \pi_1], & 0 \\ [K_1, \pi_2], & 0, & -[K_3, \pi_2] \\ 0, & [K_1, \pi_3], & [K_2, \pi_3] \end{pmatrix} = 3.$$

In the case when $k = \mathbf{Q}$ let $\mathfrak{m} = \infty$ or 1 according to $\ell = 2$ or $\ell > 2$. Then $\ell \nmid \#(E_{k\mathfrak{m}})$; consequently, the Hasse norm principle for units modulo $\mathfrak{m}$ is satisfied. Hence in this case , (2) in the above theorem coincides with the Fröhlich's result in [2]. Similarly in the case where k is an imaginary quadratic field with $\ell \nmid h(k)$ and $\ell \nmid \#(E_k)$, (2) gives the result of Ullom and Watt [19].

References

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

[2] A. Fröhlich, On the absolute class group of Abelian fields, J. London Math. Soc., **29** (1954), 211–217.

[3] A. Fröhlich, Central extensions, Galois groups, and ideal class group of number fields, Contemporary Math., vol. 24, American Math. Soc., Providence·Rhode Island, 1983.

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

[5] Y. Furuta, Über die Zentrale Klassenzahl eines Relativ-Galoisschen Zahlkörpers, J. Number Theory, **3** (1971), 318–322.

[6] D. Garbanati, The Hasse norm theorem for non-cyclic extensions of the rationals, Proc. London Math. Soc., **37** (1978), 143–164.

[7] R. Gold, The principal genus and Hasse's norm theorem, Indiana Univ. Math. J., **26** (1977), 183–189.

[8] H. Hasse, Zum Existensatz von Grunwald in der Klassenkörpertheorie, J. Reine. Angew. Math., **188** (1950), 40–64.

[9] H. Hasse, Bericht über neuere Untersuchengen und Problem aus der Theorie der algebraischen Zahlkörper, Physica-Verlag Würzburg-Wien, 1970.

[10] F. P. Heider, Strahlknoten und Geschlechterkörper mod m, J. Reine Angew. Math., **320** (1980), 52–67.

[11] M. Horie, On the genus field in algebraic number fields, Tokyo J. Math., **6** (1983), 363–380.

[12] S. Iyanaga, The theory of numbers (North-Holland mathematical library; 8), North-Holland, Amsterdam, 1975.

[13] H. W. Leopoldt, Zur Geschlechtertheorie in abelischen Zahlkörpern, Math. Nachr., **9** (1953), 351–362.

[14] T. Takeuchi, Genus group of finite Galois extensions, Proc. Amer. Math. Soc., **98** (1986), 211–214.

[15] M. Razar, Central and genus class fields and the Hasse norm theorem, Compositio Math., **35** (1977), 281– 298.

[16] A. Scholz, Totale Normreste, die keine Normen sind, als Erzeuger nicht abelscher Körperweiterungen. I, J. Reine Angew. Math., **172** (1936), 100-107; II, J. Reine Angew. Math., **182** (1940), 217–234.

[17] J. P. Serre, Local fields (Graduate text in mathematics; 67) Springer, New York, 1979.

[18] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.

[19] S. V. Ullom and S. B. Watt, Class number restrictions for certain ℓ-extensions of imaginary quadratic fields, Illinois J. Math., **32** (1988), 422–427.

[20] E. Weiss, A deflation map, J. Math. Mech., **8** (1959), 309–330.

DEPARTMENT OF MATHEMATICS
FACULTY OF GENERAL EDUCATION
NIIGATA UNIVERSITY
NIIGATA 950-21
JAPAN

PRESENT ADDRESS
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
NIIGATA UNIVERSITY
NIIGATA 950-21
JAPAN