

RESTRICTED RAMIFICATION FOR IMAGINARY QUADRATIC NUMBER FIELDS AND A MULTIPLICATOR FREE GROUP¹

BY

STEPHEN B. WATT

ABSTRACT. Let K be an imaginary quadratic number field with unit group E_K and let ℓ be a rational prime such that $\ell \nmid |E_K|$. Let S be any finite set of finite primes of K and let $K(\ell, S)$ denote the maximal ℓ -extension of K (inside a fixed algebraic closure of K) which is nonramified at the finite primes of K outside S . We show that the finitely generated pro- ℓ -group $\Omega(\ell, S) = \text{Gal}(K(\ell, S)/K)$ has the property that a complete set of defining relations for $\Omega(\ell, S)$ as a pro- ℓ -group can be obtained by lifting the nontrivial abelian or torsion relations in the maximal abelian quotient group $\Omega(\ell, S)^{\text{ab}}$. In addition we use the key idea of the proof to derive some interesting results on towers of fields over K with restricted ramification.

Introduction. If L/K is a Galois extension of fields and E is a Galois extension of K containing L , then E is said to be a central extension of L/K if $\text{Gal}(E/L)$ is a subgroup of the centre of $\text{Gal}(E/K)$. The study of central extensions of Galois extensions of number fields leads to several arithmetic applications (see [4, Chapter 3]) many of which stem from an early paper of Fröhlich [2]. In particular a theorem of Fröhlich [4, Theorem 4.11] gives a complete description in terms of topological generators and relations of the Galois group of the maximal ℓ -extension of $\mathbb{Q}$ (ℓ any prime, $\mathbb{Q}$ the field of rational numbers) which is nilpotent of class two with ramification restricted to a finite set of primes. This, in turn, leads to another result of Fröhlich [4, Theorem 5.2] which characterizes, in rational terms, all abelian ℓ -extensions L of $\mathbb{Q}$ for which ℓ does not divide the narrow class number of L .

Taking the previous discussion as motivation we see that it is important to consider the pro- ℓ -group $\Omega(\ell, S) = \text{Gal}(K(\ell, S)/K)$, where S is a finite set of finite primes of the number field K , and $K(\ell, S)$ is the maximal ℓ -extension of K (inside a fixed algebraic closure of K) which is nonramified at the finite primes of K outside S . The main difficulty in describing $\Omega(\ell, S)$ is the determination of a complete set of defining relations for $\Omega(\ell, S)$ as a pro- ℓ -group. When $K = \mathbb{Q}$ Fröhlich shows that a complete set of defining relations can be obtained by lifting the nontrivial abelian or torsion relations of the maximal abelian quotient group $\Omega(\ell, S)^{\text{ab}}$. We explain this idea more precisely in §1.

Our main result shows that $\Omega(\ell, S)$ also has the lifting property when K is an imaginary quadratic number field, S is any finite set as above and $\ell \nmid |E_K|$, where E_K

Received by the editors December 27, 1983 and, in revised form, August 17, 1984.

1980 *Mathematics Subject Classification*. Primary 12A65.

¹ This represents part of the author's Ph.D. dissertation written under the direction of Professor Stephen V. Ullom at the University of Illinois at Urbana.

©1985 American Mathematical Society
0002-9947/85 \$1.00 + \$.25 per page

is the group of units of K . In addition we are able to derive some interesting results on towers of fields over K with restricted ramification. For example, we show that if L is a finite ℓ -extension of an imaginary quadratic number field K such that $\ell \nmid |E_K|$ and $\text{Gal}(L/K)$ has ℓ -rank at least 4, then there is a strictly increasing infinite tower of ℓ -extensions $K \subset L \subset E_1 \subset E_2 \subset \cdots$ such that for each n the only primes of K ramified in E_n are ramified in L . As a corollary we obtain easily the known result that K has an infinite ℓ -class-tower if its ideal class group has ℓ -rank at least 4.

We note here that the other main approach to the determination of relations for pro- ℓ -groups is a cohomological one based on the fact that the relation rank of a pro- ℓ -group Ω is the dimension of the $\mathbb{F}_\ell$ -vector space $H^2(\Omega, \mathbb{F}_\ell)$, where $\mathbb{F}_\ell$ denotes the field of ℓ elements and Ω acts trivially on $\mathbb{F}_\ell$. This approach is discussed briefly in [3, p. 609] and in detail in [5].

In §1 we review the structure of finitely generated abelian pro- ℓ -groups and define the torsion relations. We also define the term “multiplicator free” and introduce the important notion of the realizability of the Schur multiplicator. The main result is proved in §2 and the key idea in the proof is then used in §3 to prove some results on towers as mentioned above.

1. Preliminaries. Suppose Ω is a finitely generated pro- ℓ -group. Then Ω^{ab} is a module over the ring $\mathbb{Z}_\ell$ of ℓ -adic integers and we write

$$\Omega^{\text{ab}} = \mathbb{Z}_\ell x_1 \oplus \cdots \oplus \mathbb{Z}_\ell x_n.$$

Suppose the torsion submodule of Ω^{ab} is generated by x_i , $i = 1, \dots, r$ ($r \leq n$), and that x_i has order ℓ^{n_i} . We call the equations $x_i^{\ell^{n_i}} = 1$ ($i = 1, \dots, r$) the torsion relations of Ω^{ab} . For each $i = 1, \dots, r$ choose a lift, ω_i , of x_i to Ω . Now $x_1, \dots, x_n$ is a minimal set of generators for Ω^{ab} so $\omega_1, \dots, \omega_n$ is a minimal set of generators for Ω by the Burnside Basis Theorem for pro- ℓ -groups [7, Proposition 24, p. 73]. Furthermore

$$(1.1) \quad \omega_i^{\ell^{n_i}} \in (\Omega, \Omega) \quad (i = 1, \dots, r).$$

(If A and B are subgroups of a profinite group Ω , we write (A, B) to denote the closure of the commutator subgroup generated by A and B .) The relations in Ω given by (1.1) are the relations lifted from the torsion relations in Ω^{ab} .

Now suppose Γ is a finite group. We denote its Schur multiplicator, $H_2(\Gamma, \mathbb{Z})$, by $M(\Gamma)$. A profinite group Ω is said to be multiplicator free if and only if for each open normal subgroup H of Ω the canonical surjective homomorphism (see [4, Proposition 3.1])

$$M(\Omega/H) \rightarrow \frac{H \cap (\Omega, \Omega)}{(H, H)}$$

is an isomorphism. The importance for us of multiplicator free groups stems from the following result.

PROPOSITION 1.2 [4, PROPOSITION 4.3]. *Let Ω be a finitely generated pro- ℓ -group. If Ω is multiplicator free, then a complete set of defining relations for Ω as a pro- ℓ -group is obtained by lifting the torsion relations of Ω^{ab} .*

Our aim then is to prove that $\Omega = \Omega(\ell, S)$ is multiplier free when K is an imaginary quadratic number field such that $\ell \nmid |E_K|$ and S is any finite set of finite primes of K , and then appeal to Proposition 1.2.

Next we discuss the important notion of the realizability of the Schur multiplier. Henceforth L/K will be a finite Galois extension of number fields with Galois group Γ . Fix an algebraic closure, K^{ac} , of K and let $\Omega = \text{Gal}(K^{\text{ac}}/K)$. Suppose E/K is a Galois extension such that $L \subseteq E \subseteq K^{\text{ac}}$. Let $\Lambda = \text{Gal}(K^{\text{ac}}/L)$ and $H = \text{Gal}(K^{\text{ac}}/E)$. Then [4, Proposition 3.1] we get the canonical commutative diagram:

$$(1.3) \quad \begin{array}{ccc} & & \frac{\Lambda \cap (\Omega, \Omega)}{(\Lambda, \Omega)} \\ & \nearrow g & \downarrow \\ M(\Gamma) & & \\ & \searrow g_H & \\ & & \frac{\Lambda/H \cap (\Omega/H, \Omega/H)}{(\Lambda/H, \Omega/H)} \end{array}$$

The map g of (1.3) is an isomorphism [4, Theorem 3.3]. We say that E realizes $M(\Gamma)$ if g_H is also an isomorphism.

PROPOSITION 1.4 [4, PROPOSITION 3.2]. *If L/K is a finite Galois extension of number fields and $\Gamma = \text{Gal}(L/K)$, then there exists a central extension E of L/K such that E is of finite degree over K and E realizes $M(\Gamma)$. Furthermore, if L/K is an ℓ -extension and E realizes $M(\Gamma)$, then the maximal ℓ -extension of K in E also realizes $M(\Gamma)$.*

Now let $X(C_L)$ denote the torsion subgroup of the Pontryagin dual of C_L , the idele class group of L . Give C_L its usual left Γ -module structure [6, p. 152]. Then $X(C_L)$ is a left Γ -module with $(\gamma\phi)(a) = \phi(\gamma^{-1}a)$ for $\gamma \in \Gamma$, $\phi \in X(C_L)$, and $a \in C_L$. Let $X(C_L)^\Gamma$ denote the fixed points of $X(C_L)$ by Γ and if E/L is finite abelian let $\Phi(E/L)$ denote the finite subgroup $X(C_L/N_{E/L}(C_E))$ of $X(C_L)$. Now we can state the test we will need to determine whether a given central extension of L/K which is of finite degree over K realizes $M(\Gamma)$. There is an exact sequence [4, (3.11)]

$$(1.5) \quad X(C_K) \xrightarrow{\hat{N}_{L/K}} X(C_L)^\Gamma \xrightarrow{r} X(\hat{H}^{-1}(\Gamma, C_L)) \rightarrow 1,$$

where $\hat{N}_{L/K}$ is the dual of the norm map $N_{L/K}: C_L \rightarrow C_K$.

PROPOSITION 1.6 [4, PROPOSITION 3.4]. *Suppose E/L is finite abelian and E/K is Galois. Then E is a central extension of L/K if and only if $\Phi(E/L) \subseteq X(C_L)^\Gamma$. Furthermore, E realizes $M(\Gamma)$ if and only if $r(\Phi(E/L)) = \text{Im}(r)$.*

2. The main result. We prove the following theorem.

THEOREM 2.1. *Let K be an imaginary quadratic number field and ℓ a prime such that $\ell \nmid |E_K|$. Then the pro- ℓ -group $\text{Gal}(K(\ell, S)/K)$ is multiplier free for any finite set S of finite primes of K .*

First we consider a local question. Let $\mathfrak{p}$ be a finite prime of K and let $L_{\mathfrak{p}}^x = \prod L_P^x$, where P runs over all primes of L above $\mathfrak{p}$ and L_P denotes the completion of L at P . Then $X(L_{\mathfrak{p}}^x)$ can be identified with $\prod X(L_P^x)$ and is a left Γ -module. Thus, if $\phi = (\phi_P)_P \in X(L_{\mathfrak{p}}^x)$ and $\gamma \in \Gamma$, then $(\gamma\phi)_P = \gamma \cdot \phi_{\gamma^{-1}P}$ as functions on L_P^x . Now let $\hat{N}_{P|\mathfrak{p}}$ denote the dual of the local norm map $N_{P|\mathfrak{p}}: L_P^x \rightarrow K_{\mathfrak{p}}^x$. The proof of the next result is straightforward. (Use [4, (3.14)] and Hilbert's Theorem 90.)

PROPOSITION 2.2. *Let $\mathfrak{p}$ be a finite prime of K which is nonramified in L . If $(\phi_P)_P \in X(L_{\mathfrak{p}}^x)^\Gamma$, then there exists a character $\lambda_{\mathfrak{p}}$ in $X(K_{\mathfrak{p}}^x)$ such that $\phi_P = \hat{N}_{P|\mathfrak{p}}(\lambda_{\mathfrak{p}})$ for all P above $\mathfrak{p}$.*

Now suppose S is any finite set of finite primes of K that contains all the finite primes which ramify in L . The set S could be empty. The group $X(C_L)$ is a left Γ -module and $X_{\ell}(C_L)$, its ℓ -torsion subgroup, is a Γ -submodule. We define a Γ -submodule of $X_{\ell}(C_L)$ by

$$X_{\ell}(C_L)_S = \left\{ \phi \in X_{\ell}(C_L) \mid \phi_P \text{ is nonramified for all finite primes } P \text{ of } L \text{ above primes of } K \text{ outside } S \right\}.$$

(Recall that if we view a character ϕ in $X(C_L)$ as a character on J_L , the idele group of L , and denote its P -local component, the restriction of ϕ to L_P^x , by ϕ_P , then we say that ϕ_P is nonramified or that ϕ is nonramified at P if $\phi_P(U_P) = 1$, where U_P is the group of local units in L_P^x .) We also define a subgroup of $X_{\ell}(C_K)$ by

$$X_{\ell}(C_K)^S = \left\{ \phi \in X_{\ell}(C_K) \mid \phi_{\mathfrak{p}} \text{ is nonramified for all } \mathfrak{p} \text{ in } S \right\}.$$

Now we can state and prove the main result we need to prove Theorem 2.1. It is an extension of [4, Theorem 3.13] to an imaginary quadratic basefield.

THEOREM 2.3. *Let K be an imaginary quadratic number field and let ℓ be a prime such that $\ell \nmid |E_K|$. Let L/K be a finite Galois extension with Galois group Γ and let S be any finite set of finite primes of K that contains all those primes of K ramified in L . Then*

$$(2.4) \quad X_{\ell}(C_L)^\Gamma = X_{\ell}(C_L)_S^\Gamma \cdot \hat{N}_{L/K}(X_{\ell}(C_K)^S).$$

Further, if ℓ does not divide the class number of K , then

$$X_{\ell}(C_L)_S^\Gamma \cap \hat{N}_{L/K}(X_{\ell}(C_K)^S) = 1$$

so that if (2.4) holds then the product is direct.

PROOF. First note that the dual norm map $\hat{N}_{L/K}$ maps $X_{\ell}(C_K)^S$ into $X_{\ell}(C_L)^\Gamma$ for any S (see (1.5)) and so $X_{\ell}(C_L)^\Gamma$ contains the two groups on the right-hand side of (2.4). Now suppose $\phi \in X_{\ell}(C_L)^\Gamma$. We show that there is a character ψ in $X_{\ell}(C_K)^S$ such that

$$\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \in X_{\ell}(C_L)_S^\Gamma.$$

Then $\phi = [\phi \cdot \hat{N}_{L/K}(\psi^{-1})][\hat{N}_{L/K}(\psi)]$, which proves (2.4).

We begin by defining a character θ of $U_f(K)$, the subgroup of finite unit ideles of J_K consisting of unit ideles with 1 at the infinite prime of K . Let $\mathfrak{p}$ be a finite prime

of K . First note that $\phi \in X_\ell(C_L)^\Gamma$ implies $(\phi_P)_{P|p} \in X(L_p^x)^\Gamma$. Now suppose $p \notin S$. Then p is nonramified in L so, by Proposition 2.2, there exists a character λ_p in $X(K_p^x)$ such that

$$(2.5) \quad \hat{N}_{P|p}(\lambda_p) = \phi_P \quad \text{for all } P \text{ above } p.$$

Define θ as follows.

$$\begin{aligned} \theta|_{U_p} &= 1 \quad \text{if } p \in S \text{ or } \phi_P \text{ is nonramified for all } P|p. \\ \theta|_{U_p} &= \lambda_p|_{U_p} \quad \text{if both } p \notin S \text{ and } \phi_P \text{ is ramified for some } P|p. \end{aligned}$$

(We note that if $p \notin S$ and ϕ_P is ramified for some P above p , then (2.5) implies that ϕ_P is ramified for all P above p .) The condition that ϕ_P is nonramified for all P above p holds for almost all p of K so $\theta|_{U_p} = 1$ for almost all p . Thus [1, p. 324], θ is a well-defined character of $U_f(K)$. We want to lift θ to an appropriate character ψ , as specified earlier.

Note that if $(x_p)_p \in U_f(K)$, then

$$(2.6) \quad \theta((x_p)_p) = \prod \lambda_p(x_p),$$

where p runs over the finite set

$$T = \{ p | p \notin S \text{ and } \phi_P \text{ is ramified for some } P \text{ above } p \}.$$

In order to lift θ to a character in $X(C_K)$ it is sufficient [4, (2.28)] to show that $\theta(x_f) = 1$ for all x in E_K , where x_f is the idele in $U_f(K)$ with 1 at the infinite prime and x elsewhere. Thus, we must show that $\prod \lambda_p(x) = 1$ ($p \in T$) for all x in E_K . We do this by showing that $\lambda_p(x) = 1$ for all x in E_K and all p in T .

Let $p \in T$. Then $p \notin S$ so p is nonramified in L . Therefore $N_{P|p}(U_P) = U_p$ for each P above p . Let $x_p \in U_p$. Then $x_p = N_{P|p}(y_P)$ for some y_P in U_P so $\lambda_p(x_p) = \phi_P(y_P)$. But ϕ has ℓ -power order so ϕ_P also has ℓ -power order and hence

$$(2.7) \quad \lambda_p(x_p) \text{ has } \ell\text{-power order for all } x_p \text{ in } U_p \text{ and } p \text{ in } T.$$

It follows from (2.6) and (2.7) that θ has ℓ -power order. In addition, if $x \in E_K$, then $\lambda_p(x)$ has order dividing $|E_K|$. Therefore $\lambda_p(x) = 1$ for all p in T , as required. Now we can lift θ to a character ψ in $X(C_K)$. Furthermore, we can write $\psi = \psi_\ell \psi'$, where ψ_ℓ and ψ' are in $X(C_K)$, ψ_ℓ is of ℓ -power order and ψ' is of order prime to ℓ . Thus, we may replace ψ by ψ_ℓ and call this ψ again. Now we have $\psi \in X_\ell(C_K)$ and $\psi|_{U_f(K)} = \theta$. Also, if $p \in S$, then $\psi|_{U_p} = \theta|_{U_p} = 1$, by definition of θ . Therefore ψ is nonramified at each p in S and so $\psi \in X_\ell(C_K)^S$. This character is the ψ announced at the beginning of the proof.

Next we show that $\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \in X_\ell(C_L)^\Gamma$. The character ψ has ℓ -power order and so, therefore, does $\hat{N}_{L/K}(\psi^{-1})$. Also, ϕ has ℓ -power order since $\phi \in X_\ell(C_L)$. Therefore $\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \in X_\ell(C_L)$. Now let p be a finite prime of K not in S . We show that $\phi \cdot \hat{N}_{L/K}(\psi^{-1})$ is nonramified at each prime of L above p . There are two cases to consider.

Case I. $p \notin S$ and ϕ_P is nonramified for all P above p . In this case, $\psi|_{U_p} = \theta|_{U_p} = 1$, by definition of θ . Therefore $\psi^{-1}|_{U_p} = 1$, so $\hat{N}_{L/K}(\psi^{-1})$ is nonramified at each P

above $\mathfrak{p}$. But ϕ_P is nonramified for all P above $\mathfrak{p}$ by hypothesis. Therefore $\phi \cdot \hat{N}_{L/K}(\psi^{-1})$ is nonramified for all P above $\mathfrak{p}$.

Case II. $\mathfrak{p} \notin S$ and ϕ_P is ramified for some P above $\mathfrak{p}$. We have $\hat{N}_{P|\mathfrak{p}}(\lambda_{\mathfrak{p}}) = \phi_P$ for all P above $\mathfrak{p}$. Let $x_P \in U_P$. Then an easy calculation shows that

$$\left[\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \right]_P(x_P) = \phi_P(X_P) \left[\psi_{\mathfrak{p}}(N_{P|\mathfrak{p}}(x_P)) \right]^{-1} = 1$$

for all P above $\mathfrak{p}$. Thus $\phi \cdot \hat{N}_{L/K}(\psi^{-1})$ is nonramified at each P above $\mathfrak{p}$ in Case II also.

We have shown that $\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \in X_{\ell}(C_L)_S$. But $\phi \cdot \hat{N}_{L/K}(\psi^{-1})$ is fixed by each element of Γ since both ϕ and $\hat{N}_{L/K}(\psi^{-1})$ are. Therefore $\phi \cdot \hat{N}_{L/K}(\psi^{-1}) \in X_{\ell}(C_L)_S^{\Gamma}$. This completes the proof of the first part of the theorem.

Now let h_K denote the class number of K and suppose that $\ell \nmid h_K$ (although not necessarily that $\ell \nmid |E_K|$). Suppose $\psi \in X_{\ell}(C_K)^S$ and that $\hat{N}_{L/K}(\psi) \in X_{\ell}(C_L)_S^{\Gamma}$. We first show that ψ is nonramified at each finite prime $\mathfrak{p}$ of K . Certainly $\psi \in X_{\ell}(C_K)^S$ implies ψ is nonramified at each $\mathfrak{p}$ in S . Now suppose $\mathfrak{p} \notin S$ and choose P above $\mathfrak{p}$. Then P is nonramified so $U_{\mathfrak{p}} = N_{P|\mathfrak{p}}(U_P)$. But $\hat{N}_{L/K}(\psi) \in X_{\ell}(C_L)_S^{\Gamma}$ implies $\hat{N}_{L/K}(\psi)$ is nonramified at P and hence ψ is nonramified at $\mathfrak{p}$. Therefore ψ is nonramified at all finite primes of K . But ψ is an idele class character of finite order so, viewing ψ as a character on J_K , $\psi(K^{\times}J_K(1)) = 1$, where $J_K(1)$ denotes the connected component of the identity in J_K . Therefore $\psi(K^{\times}J_K(1)U_f(K)) = 1$. Let $\text{Cl}(K)$ denote the ideal class group of K . Now $J_K/K^{\times}J_K(1)U_f(K) \cong \text{Cl}(K)$ [6, p. 141]. We identify these two groups. Then $\psi \in X_{\ell}(\text{Cl}(K))$. But $\ell \nmid h_K$ so $X_{\ell}(\text{Cl}(K)) = 1$. This completes the proof.

REMARKS. (i) If K is an imaginary quadratic number field it follows from Theorem 2.3 and the Primary Decomposition Theorem that

$$X'(C_L)^{\Gamma} = X'(C_L)_S^{\Gamma} \cdot \hat{N}_{L/K}(X'(C_K)^S),$$

where $X'(C_L)$ denotes the subgroup of $X(C_L)$ of characters of odd order if $K \neq Q(\sqrt{-3})$ and of order prime to 6 if $K = Q(\sqrt{-3})$.

(ii) The second part of Theorem 2.3, which is not used in the sequel, holds in general. That is, if K is a number field and ℓ does not divide the narrow class number of K , then $X_{\ell}(C_L)_S^{\Gamma} \cap \hat{N}_{L/K}(X_{\ell}(C_K)^S) = 1$. In fact we have the following result. The proof is easy and we omit it.

PROPOSITION 2.8. *If L/K is a Galois extension of number fields, then the following are equivalent.*

- (a) $X_{\ell}(C_L)_S^{\Gamma} \cap \hat{N}_{L/K}(X_{\ell}(C_K)^S) = 1$.
- (b) *The maximal ℓ -extension of K in its narrow Hilbert class field is contained in L .*

We are now almost ready to prove Theorem 2.1. The following easy result will be useful. We omit the proof (which is shorter than the statement).

LEMMA 2.9. *Suppose r is a homomorphism from an abelian torsion group G onto the group $\bar{G}$. Suppose also that G_1 and G_2 are subgroups of G such that $G = G_1G_2$ and $G_2 \subseteq \text{Ker}(r)$. If H is a finite subgroup of G such that $r(H) = \bar{G}$, then there exists a finite subgroup H_1 of G_1 such that $r(H_1) = \bar{G}$.*

PROOF OF THEOREM 2.1. Let $\Omega = \text{Gal}(K^{\text{ac}}/K)$ and $A = \text{Gal}(K^{\text{ac}}/K(\ell, S))$. Then $\Omega/A \cong \text{Gal}(K(\ell, S)/K)$ as topological groups. We need to show that Ω/A is multiplier free. Let Λ/A be an open normal subgroup of Ω/A , where Λ is an open normal subgroup of Ω which contains A . Let L be the fixed field of Λ so L is a finite ℓ -extension of K contained in $K(\ell, S)$. Let $\Gamma = \text{Gal}(L/K)$. Then $\Omega/\Lambda \cong \Gamma$ and by Proposition 1.4 there is a central ℓ -extension E of L/K which is of finite degree over K and realizes $M(\Gamma)$. From (1.5) we have a map

$$r: X_{\ell}(C_L)^{\Gamma} \rightarrow X(\hat{H}^{-1}(\Gamma, C_L)).$$

Now $X_{\ell}(C_L)^{\Gamma} = X_{\ell}(C_L)_S^{\Gamma} \cdot \hat{N}_{L/K}(X_{\ell}(C_K)^S)$ by Theorem 2.3, and $\Phi(E/L) \subseteq X_{\ell}(C_L)^{\Gamma}$ since E is a central ℓ -extension of L/K . Also, $r(\Phi(E/L)) = X(\hat{H}^{-1}(\Gamma, C_L))$ by Proposition 1.6. Now apply Lemma 2.9 with $G = X_{\ell}(C_L)^{\Gamma}$, $G_1 = X_{\ell}(C_L)_S^{\Gamma}$, $G_2 = \hat{N}_{L/K}(X_{\ell}(C_K)^S)$, $\bar{G} = X(\hat{H}^{-1}(\Gamma, C_L))$ and $H = \Phi(E/L)$. Note that $G_2 \subseteq \text{Ker}(r)$ here since r is just the restriction of characters map

$$X_{\ell}\left(\frac{C_L}{I_{\Gamma}C_L}\right) \xrightarrow{r} X\left(\frac{\text{Ker } N_{L/K}}{I_{\Gamma}C_L}\right),$$

where I_{Γ} denotes the augmentation ideal of the integral group ring of Γ . Thus, from Lemma 2.9 we get a finite subgroup of characters, H_1 , in $X_{\ell}(C_L)_S^{\Gamma}$ such that $r(H_1) = X(\hat{H}^{-1}(\Gamma, C_L))$. Since H_1 is finite we may write $H_1 = \Phi(F/L)$ for some finite abelian extension F of L by the classification theorem of global class field theory [4, p. 5]. Now the inclusion $\Phi(F/L) \subseteq X_{\ell}(C_L)_S^{\Gamma}$ implies F is a central ℓ -extension of L/K such that F/K is nonramified at all primes of K outside S . Since $r(\Phi(F/L)) = X(\hat{H}^{-1}(\Gamma, C_L))$, F also realizes $M(\Gamma)$ by Proposition 1.6. Thus we have realized $M(\Gamma)$ "without additional ramification".

Now let $B = \text{Gal}(K^{\text{ac}}/F)$. Then $A \subseteq B$ and we get the canonical commutative diagram (2.10), where the maps g_A and g_B are as in (1.3).

$$(2.10) \quad \begin{array}{ccc} & \frac{\Lambda/A \cap (\Omega/A, \Omega/A)}{(\Lambda/A, \Omega/A)} & \\ g_A \nearrow & & \downarrow \\ M(\Omega/\Lambda) & & \\ g_B \searrow & & \frac{\Lambda/B \cap (\Omega/B, \Omega/B)}{(\Lambda/B, \Omega/B)} \end{array}$$

We need to show that g_A is an isomorphism. All the maps in (2.10) are surjective and g_B is an isomorphism since F realizes $M(\Gamma)$. Therefore g_A is injective and hence is an isomorphism. This completes the proof.

REMARK. Theorem 2.3 is proved under the hypothesis that K is an imaginary quadratic number field and $\ell \nmid |E_K|$, but Theorem 2.1 will be valid whenever the conclusion of Theorem 2.3 holds.

3. Some applications. The following key result may be extracted from the proof of Theorem 2.1.

THEOREM 3.1. *Let K be an imaginary quadratic number field and ℓ a prime such that $\ell \nmid |E_K|$. Suppose L is a finite ℓ -extension of K with Galois group Γ and S is any finite set of finite primes of K that contains all primes of K ramified in L . Then there is a finite central ℓ -extension E of L/K such that E realizes $M(\Gamma)$ and E/K is nonramified at the primes of K outside S .*

Let $d(A)$ denote the ℓ -rank of A when A is a finite abelian group or a finite ℓ -group. The next result shows the existence of an infinite “S-class-tower”.

COROLLARY 3.2. *Suppose L is an ℓ -extension of an imaginary quadratic number field K with $\ell \nmid |E_K|$. If $d(\text{Gal}(L/K)) \geq 4$, then there is a strictly increasing infinite tower of ℓ -extensions*

$$K \subset L \subset E_1 \subset E_2 \subset \cdots$$

such that for each n the only primes of K ramified in E_n are ramified in L .

PROOF. First recall [1, Lemma 9, p. 236] that if G is a finite ℓ -group with relation rank $r(G)$, then

$$(3.3) \quad d(M(G)) = r(G) - d(G).$$

Also [1, Theorem 10, p. 237],

$$(3.4) \quad r(G) > d(G)^2/4.$$

It follows from (3.3) and (3.4) that $d(M(G)) \neq 0$ if $d(G) \geq 4$.

Now consider the extension L/K . Let S be the set of primes of K ramified in L . By Theorem 3.1 there is a finite central ℓ -extension E_1 of L/K such that E_1 realizes $M(\text{Gal}(L/K))$ and E_1/K is nonramified at the primes of K outside S . Let $\Gamma_1 = \text{Gal}(E_1/K)$. Now

$$d(\text{Gal}(E_1/L)) \geq d(M(\text{Gal}(L/K))) > 0$$

so E_1 is a proper extension of L . Also,

$$d(\Gamma_1) \geq d(\text{Gal}(L/K)) \geq 4$$

so we may repeat the procedure starting with the extension E_1/K . Thus, the tower is constructed by iteration.

We can now get a new and easy proof of the following known result (see [1, Theorem 3, p. 233]).

COROLLARY 3.5. *If K is an imaginary quadratic number field with $\ell \nmid |E_K|$, then K has an infinite ℓ -class-tower if $d(\text{Cl}(K)) \geq 4$.*

PROOF. Let L denote the ℓ -part of the Hilbert class field of K . Then no primes of K are ramified in L and the result follows from Corollary 3.2.

Now suppose

$$(3.6) \quad 1 \rightarrow \Lambda \rightarrow \Omega \rightarrow \Gamma \rightarrow 1$$

is a short exact sequence of finite groups. Then there is a surjective homomorphism $M(\Gamma) \rightarrow \Lambda \cap (\Omega, \Omega)/(\Lambda, \Omega)$. Recall that (3.6) is called a stem extension of Γ if it is a central extension and $\Lambda \subseteq (\Omega, \Omega)$. Then we have a surjective homomorphism $M(\Gamma) \rightarrow \Lambda$. If, further, this surjection is an isomorphism of $M(\Gamma)$ onto Λ , then (3.6) is called a stem cover of Γ .

THEOREM 3.7. *Suppose K is an imaginary quadratic number field with $\ell \nmid |E_K|$. Suppose L/K is a finite ℓ -extension such that $K^{\text{ab}}(\ell, S) \subseteq L \subseteq K(\ell, S)$ for some finite set S of finite primes of K . (Here $K^{\text{ab}}(\ell, S)$ denotes the maximal abelian extension of K in $K(\ell, S)$.) Then there is an increasing sequence of subfields of $K(\ell, S)$,*

$$L = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots$$

such that E_n is a finite ℓ -extension of K and the canonical extension

$$1 \rightarrow \text{Gal}(E_{n+1}/E_n) \rightarrow \text{Gal}(E_{n+1}/K) \rightarrow \text{Gal}(E_n/K) \rightarrow 1$$

is a stem cover of $\text{Gal}(E_n/K)$ for each $n \geq 0$.

PROOF. Let $\Gamma = \text{Gal}(L/K)$. By Theorem 3.1 there is a finite central ℓ -extension E_1 of L/K such that $E_1 \subseteq K(\ell, S)$ and E_1 realizes $M(\Gamma)$. Now the canonical extension

$$(3.8) \quad 1 \rightarrow \text{Gal}(E_1/L) \rightarrow \text{Gal}(E_1/K) \rightarrow \Gamma \rightarrow 1$$

is a stem extension of Γ since $E_1 \supseteq L \supseteq K^{\text{ab}}(\ell, S)$, so there is a surjective homomorphism

$$(3.9) \quad M(\Gamma) \rightarrow \text{Gal}(E_1/L).$$

Also, $M(\Gamma)$ is isomorphic to a subgroup of $\text{Gal}(E_1/L)$ since E_1 realizes $M(\Gamma)$. Therefore the surjection (3.9) is an isomorphism and the extension (3.8) is a stem cover of Γ . The procedure may now be repeated starting with the extension E_1/K .

REFERENCES

1. J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Thompson, Washington, D. C., 1967.
2. A. Fröhlich, *On fields of class two*, Proc. London Math. Soc. **4** (1954), 235–256.
3. ———, *Algebraic number fields*, Academic Press, London, 1977.
4. ———, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. **24** (1983).
5. H. Koch, *Galoissche Theorie der p -Erweiterungen*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1970.
6. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
7. S. S. Shatz, *Profinite groups, arithmetic, and geometry*, Princeton Univ. Press, Princeton, N. J., 1972.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KANSAS 66506

Current address: Department of Mathematics, University of Iowa, Iowa City, Iowa 52242