ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

CLASS NUMBER RESTRICTIONS FOR CERTAIN l-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

BY

STEPHEN V. ULLOM AND STEPHEN B. WATT

Dedicated to the memory of Irving Reiner

Introduction

Fix a rational prime l and suppose K is an imaginary quadratic field in which l divides neither the class number h_K of K nor the order of the group of units of K. We characterize those abelian l-extensions L/K for which l does not divide h_L (Theorem 2.4) in terms of the mutual congruence behavior of the primes of K which are ramified in L. For abelian extensions of the rationals Q, Fröhlich [4] solved the corresponding problem as a corollary of his description by generators and relations of the Galois group of the maximal S-ramified class two l-extension of Q. We used the same approach in the first version of this paper and found a result completely analogous to Theorem 5.1 of [5], which gives generators and relations for a certain class two l-group. In [5] Fröhlich presents a more modern account of [4]; in [3] Cornell and Rosen characterize abelian l-extensions L/Q for which l does not divide h_L (odd l).

1. Background from class field theory

Fix a prime l and let L be a finite abelian l-extension of a number field K. One of our major goals will be to obtain a criterion for the class number h_L of L to be relatively prime to l in case K is an imaginary quadratic field with $(l, h_K|E_K|) = 1$; here E_K denotes the unit group of K. Let $G(L/K)$ (resp. $Z(L/K)$) denote the genus field (resp. central class field) of L with respect to K and let $g(L/K) = (G(L/K)\colon L)$. Recall that $G(L/K)$ is the maximal unramified extension of L which is an abelian extension of K and $Z(L/K)$ is the maximal unramified extension of L such that the Galois group $\mathrm{Gal}(Z(L/K)/L)$ is contained in the center of $\mathrm{Gal}(Z(L/K)/K)$. The key

Received September 30, 1987

observation is that $(l, h_L) = 1$ if and only if $((Z(L/K)\colon L), l) = 1$; compare Lemma 3.9 of [5].

Let Cl_K be the ideal class group of K, J_K the idele group of K, K_v the completion of K at a prime v, U_v the unit group of K_v, and let $U_K = \prod U_v$, product taken over all primes (finite and infinite) of K. From class field theory $\mathrm{Gal}(G(L/K)/K)$ is isomorphic via the reciprocity map to $J_K/K^x(NU_L)$, where N denotes the (idele) norm from L to K; e.g., see Prop. 2.4 of [5]. There is an exact sequence of abelian groups

$$(1.1)\quad 1 \to E_K/E_K \cap NJ_L \to \prod U_v/NU_w \to J_K/K^x(NU_L) \to Cl_K \to 1.$$

For each prime v of K, a prime w of L above v is selected and U_w denotes the unit group of L_w; recall the ramification index $e_v = (U_v : NU_w)$. This sequence gives Furuta's formula [6]

$$(1.2)\qquad g(L/K) = h_K \prod e_v/(L : K)m(L/K),$$

where $m(L/K) = (E_K\colon E_K \cap NJ_L)$. Define

$$A(L/K) = \text{local norms/global norms} = K^x \cap NJ_L/NL^x$$

and subgroup

$$B(L/K) = E_K \cap NJ_L/E_K \cap NL^x.$$

From [7] or Theorems 3.6 and 3.11 of [5],

$$\mathrm{Gal}(Z(L/K)/G(L/K)) \cong A(L/K)/B(L/K)$$

for a Galois extension L/K.

Let D_v (resp. T_v) be the decomposition (resp. inertia) subgroup of a prime of L dividing v. One can show that (e.g., see Tate [1]) for a Galois extension L/K,

$$(1.3)\qquad A(L/K) \cong \mathrm{cok}\left(\coprod_v H_2(D_v, \mathbf{Z}) \to H_2(\mathrm{Gal}(L/K), \mathbf{Z})\right).$$

The mapping, say φ, is given by corestriction in homology and v ranges over all the primes of K. Furthermore if X is a finite abelian group one knows

$$H_2(X, \mathbf{Z}) \cong (\text{the second exterior power of } X) = \wedge^2 X.$$

It follows that

$$\mathrm{cok}\,\varphi \cong \mathrm{cok}\left(\coprod_v \wedge^2 D_v \to \wedge^2 \mathrm{Gal}(L/K)\right)$$

where the mapping is induced by the inclusions $D_v \to \mathrm{Gal}(L/K)$.

For a finite abelian l-group X define rk $X = \dim(X/lX)$, dimension taken over $\mathbf{F}_l$. The following proposition can easily be extracted from Prop. 9 of [8].

(1.4) PROPOSITION. *Let L/K be a finite abelian l-extension and L_1 the maximal elementary abelian l-extension of K in L. Then*

$$\operatorname{rk} A(L/K) = \operatorname{rk} A(L_1/K).$$

COROLLARY. *Let K be an imaginary quadratic field with $(l, |E_K|) = 1$. Then*

$$\operatorname{rk} \operatorname{Gal}(Z(L/K)/G(L/K)) = \operatorname{rk} \operatorname{Gal}(Z(L_1/K)/G(L_1/K)).$$

Remark. See [3] for a proof without homology of a closely related result for $K = Q$ and l an odd prime. We do not need (1.4) for what follows.

2. Central class fields

In this section K is an imaginary quadratic extension of Q satisfying $(l, h_K|E_K|) = 1$, L/K is an abelian l-extension, and we assume $(g(L/K), l) = 1$. Then we determine exactly when $(h_L, l) = 1$. Note the composite of L and the Hilbert class field of K is a subfield of the genus field $G(L/K)$, so $(h_K, l) = 1$ is a reasonable hypothesis; one could also handle the case l divides $|E_K|$, but the analysis would be longer. Under this hypothesis it follows from (1.1) that $(g(L/K), l) = 1$ if and only if Gal(L/K) is the direct product $\prod T_v$. Let S be the set of primes of K ramifying in L; let v_λ (and if necessary v'_λ) be the divisors of l in K. We shall use v for any prime of K and $\mathfrak{p}_v$ for the prime ideal. Note if an inertia subgroup T_v of Gal(L/K) is not cyclic, then v divides l and l is not split in K. Thus there is at most one noncyclic inertia group and it is denoted T_λ.

Let $\Gamma = \operatorname{Gal}(L/K)$, $d = \operatorname{rk}\Gamma$, $s = |S|$, so $s \le d$. Let $t = \operatorname{rk} T_\lambda$ $(1 \le t \le 3)$, so $d = t + s - 1$. (If $v_\lambda \notin S$, set $t = 1$). Note $t = 3$ occurs only when $\lambda|2$ and λ is the unique prime dividing 2. There is a lower bound for

$$\operatorname{rk}\operatorname{cok}\varphi = \operatorname{rk} A(L/K).$$

From the fact that rk $\wedge^2\Gamma = \binom{d}{2}$ and the quotient D_v/T_v is cyclic, we have by (1.3) (compare Prop. 2 of [2]),

$$\operatorname{rk}\operatorname{cok}\varphi \ge \binom{d}{2} - \binom{t+1}{2} - (s-1).$$

Using $t \le 3$, we have the interesting result

$$\operatorname{rk}\operatorname{cok}\varphi \ge 2 \quad \text{if } d \ge 5. \tag{2.1}$$

When $s \leq 1$ there is the well known push down result due to Iwasawa; e.g., see Theorem 10.4 of [10].

(2.2) PROPOSITION. *Let L/K be a Galois extension of l power degree in which at most one prime ramifies. Then l divides h_L implies l divides h_K.*

Thus we are left with the cases $2 \leq s \leq d \leq 4$. We need to introduce some notation that will allow us to compute cok φ and in particular to determine when cok $\varphi = 0$. For each $v \in S$ prime to l fix $x_v \in O_v$, the valuation ring of K_v, generating $(O_v/\mathfrak{p}_v O_v)^x$ and define $[v, z] \in \mathbf{Z}_l$ by

$$z \equiv x_v^{[v,z]} \mod \mathfrak{p}_v O_v,\ z \in U_v.$$

Let N be the local norm $L_w \to K_v$. Now suppose v divides l; assume $T_v \cong U_v/N(U_w)$ is cyclic and fix a generator $x_v \in U_v$ of the quotient group. For $z \in U_v$, write

$$z \equiv x_v^{[v,z]} \mod N(U_w).$$

Of course $[v, z]$ is not uniquely determined by these congruences, but that ambiguity causes no difficulty in what follows. Since we assumed $(l, h_K) = 1$, for each prime ideal $\mathfrak{p}_v$ of K there is a smallest positive integer h_v, prime to l, such that $\mathfrak{p}_v^{h_v} = (\tilde{\pi}_v)$, $\tilde{\pi}_v \in K$.

(2.3) PROPOSITION. *Let K be an imaginary quadratic field with $(l, h_K|E_K|) = 1$. Suppose that L/K is an abelian l-extension in which only v_1, v_2 ramify,*

$$\Gamma = \mathrm{Gal}(L/K) = T_{v_1} \oplus T_{v_2},$$

and the l-primary part of $U_{v_2}, (U_{v_2})_l$, is pro-cyclic. Then $\Gamma = D_{v_1}$ if and only if $[v_2, \tilde{\pi}_1] \not\equiv 0 \bmod l$.

Proof. Let E be the subfield of L fixed by T_{v_1}. The prime v_2 is totally ramified in E/K and no other prime ramifies in E/K. Thus E is contained in the ray class field over K of conductor $\mathfrak{p}_2^r$, some $r \geq 1$. Since $(l, h_K) = 1$, $\mathrm{Gal}(E/K) \cong$ quotient of $(O_K/\mathfrak{p}_2^r)^x$.

If v_2 does not divide l, then $r = 1$. Otherwise v_2 divides l and l is split in K/Q since $(U_{v_2})_l$ is assumed pro-cyclic; thus $O_K/\mathfrak{p}_2^r \cong \mathbf{Z}_l/(l^r)$. In both cases,

$$\begin{aligned}
\Gamma = D_{v_1} \quad & \text{iff } v_1 \text{ inert in } E/K \\
& \text{iff Frobenius of } v_1 \text{ generates } \mathrm{Gal}(E/K) \\
& \text{iff } \tilde{\pi}_1 \not\equiv x^l \bmod \mathfrak{p}_2^r \quad (\text{use } (l, |E_K|) = 1) \\
& \text{iff } [v_2, \tilde{\pi}_1] \not\equiv 0 \bmod l.
\end{aligned}$$

Q.E.D.

In this paragraph we define a matrix $M(L)$ whose entries are to be viewed modulo l. For notational convenience we restrict to the case where all the inertia subgroups T_v of Γ are cyclic, though this is not necessary. Let w be a prime of L above $v \in S$ and define $\sigma_v \in \mathrm{Gal}(L_w/K_v)$ as a lifting of the local Artin symbol $(L_w/K_v, \tilde{\pi}_v)$; then $\sigma_v^{h_v}$ lifts the inverse of the Frobenius automorphism on the maximal unramified extension of K_v in L_w. Choose τ_v in the inertia subgroup of $\mathrm{Gal}(L_w/K_v) \cong D_v$ which lifts the local Artin symbol $(L_w/K_v, x_v)$. We are identifying local Galois groups with appropriate subgroups of $\mathrm{Gal}(L/K)$. The column indices of the matrix $M(L)$ are pairs $(v, v') \in S \times S$, $v \neq v'$, and exactly one of (v, v') and (v', v) appears. Since we are assuming $\Gamma = \prod T_v$, the columns are indexed by $\tau_v \wedge \tau_{v'}$ for pairs (v, v') as above. The image of φ is isomorphic to the subgroup of $\wedge^2\Gamma$ generated by $\{\tau_v \wedge \sigma_v : v \in S\}$, since T_v and D_v/T_v are cyclic groups with generators τ_v and $\sigma_v \bmod T_v$ respectively. As in [9], for $v' \in S$, write in additive notation

$$\sigma_{v'} = \sum a_{v'v}\tau_v, \quad \text{summation over } v \in S, v \neq v';$$

thus $\tau_{v'} \wedge \sigma_{v'} = \sum a_{v'v}(\tau_{v'} \wedge \tau_v)$. In $M(L)$ the entry in row v and column (v, v') (resp. in row v' and column (v, v')) is $a_{vv'}$ (resp. $-a_{vv'}$) taken modulo l. Other entries are zero. This completes the description of $M(L)$.

We claim $a_{v'v} \equiv -[v, \tilde{\pi}_{v'}] \bmod l$. In fact $\Gamma \cong \prod U_v/NU_w$. The reciprocity map sends the idele $\alpha \in J_K$ with $\tilde{\pi}_{v'}$ in position v' and ones elsewhere to $\sigma_{v'} \in \Gamma$. From (1.1), α corresponds in $\prod U_v/NU_w$ to $\prod x_v^{-[v, \tilde{\pi}_{v'}]}$; the second product is taken over $v \in S$, $v \neq v'$. For example, for $d = s = 3$,

$$M(L) = \begin{bmatrix} -[v_2, \tilde{\pi}_1] & -[v_3, \tilde{\pi}_1] & 0 \\ [v_1, \tilde{\pi}_2] & 0 & -[v_3, \tilde{\pi}_2] \\ 0 & [v_1, \tilde{\pi}_3] & [v_2, \tilde{\pi}_3] \end{bmatrix}.$$

Let S be the set of primes of K ramified in L. If l is not split in K/Q, let $S' = \{v \in S \mid v \text{ divides } l\}$; otherwise $S' = \varnothing$. Let S'' be the complement of S' in S.

(2.4) THEOREM. *Let K be an imaginary quadratic field with $(l, h_K|E_K|) = 1$. Let L/K be an abelian l-extension with $(g(L/K), l) = 1$. Then $(l, h_L) = 1$ in exactly the following cases* (a)–(d).

(a) $s = 1$.

(b) $d = 2$, $S = \{v_1, v_2\}$ *and either*

  (i) $S = S''$ *and* $[v_1, \tilde{\pi}_2] \not\equiv 0$ *or* $[v_2, \tilde{\pi}_1] \not\equiv 0 \bmod l$,

  or

  (ii) $v_1 \in S'$ *and v_2 does not divide l and either* $[v_2, \tilde{\pi}_1] \not\equiv 0$ *or* $\tilde{\pi}_2$ *generates* $U_{v_1}/N(U_{w_1})$

(c) $d = 3$, *and either*
  (i) $S = \{v_1, v_2\}$ *with* v_2 *not dividing* l *and* $v_1 \in S'$ *and* $[v_2, \tilde{\pi}_1] \not\equiv 0$, *or*
  (ii) $s = 3$ *and* $\det M(L) \not\equiv 0 \bmod l$
(d) $d = 4$, $S = \{v_1, v_2\}$ with v_2 not dividing l and $[v_2, \tilde{\pi}_1] \not\equiv 0$.

Proof. In all cases we have $\Gamma = \prod T_v$, product over $v \in S$.

(a) Use (2.2). In (b) clearly $\operatorname{cok} \varphi = 0$ iff $\Gamma = D_{v_1}$ or $\Gamma = D_{v_2}$. In case (i) we may apply (2.3) twice (by interchanging v_1 and v_2 everywhere). In case (ii), $\Gamma = D_{v_2}$ iff Frobenius of v_2 generates $\mathrm{Gal}(E/K)$ where E is the fixed field of T_{v_2} iff $\tilde{\pi}_2$ generates $U_{v_1}/N(U_{w_1})$.

Case (c) (i) follows from (2.3). If $d = 4$, so $\operatorname{rk} \wedge^2\Gamma = 6$, we see $\operatorname{rk}(\operatorname{im} \varphi) \leq 5$ for $s = 3, 4$. For $s = 2$, we apply (2.3) again. Only the case $d = s = 3$ remains. But $\det M(L) \not\equiv 0 \bmod l$ iff $\operatorname{cok} \varphi = 0$. This completes the proof of the theorem.

Remark 1. We could have studied $\operatorname{im} \varphi$ in all cases via the matrix $M(L)$, but we avoided this more computational approach except in case (c) (ii).

Remark 2. Such extensions L with $g(L/K) = 1$ are obtained from the l-part of ray class fields over K with appropriate conductor.

References

1. J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, San Diego, California, 1967.
2. G. Cornell and M. Rosen, *The l-rank of the real class group of cyclotomic fields*, Compositio Math., vol. 53 (1984), pp. 133–141.
3. G. Cornell and M. Rosen, *The class group of an absolutely abelian l-extension*, Illinois J. Math., vol. 32 (1988), pp. 453–461 (this issue).
4. A. Fröhlich, *On fields of class two*, Proc. London Math. Soc., vol. 4 (1954), pp. 235–256.
5. ______, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math., vol. 24, Amer. Math. Soc., Providence, Rhode Island, 1984.
6. Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J., vol. 29 (1967), 281–285.
7. ______, *On class field towers and the rank of ideal class groups*, Nagoya Math. J., vol. 48 (1972), 147–157.
8. M. Razar, *Central and genus class fields and the Hasse norm theorem*, Compositio Math., vol. 35 (1977), pp. 281–298.
9. S. Ullom and S. Watt, *Generators and relations for certain class two Galois groups*, J. London Math. Soc. (2), vol. 34 (1986), pp. 235–244.
10. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.

University of Illinois
Urbana, Illinois
8 Sheffield Street
Palmerston North, New Zealand