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

THE CLASS GROUP OF AN ABSOLUTELY ABELIAN l-EXTENSION

BY

GARY CORNELL[1] AND MICHAEL ROSEN[2]

In Memoriam Irving Reiner

Introduction

Let $K/\mathbf{Q}$ be an Abelian l-extension, l a prime. In a series of papers written in the 1950's, A. Fröhlich investigated the l-class group of K through the use of the central class field of K. (The central class field of K is the maximal extension L of K such that L/K is Abelian and unramified, $L/\mathbf{Q}$ is Galois and $gal(L/K)$ is in the center of $gal(L/\mathbf{Q})$. It was first introduced by Scholz in the 1930's.) One of the most striking consequences of this general theory was his determination of all such fields K with l not dividing the class number of K. He recently gave a more modern exposition of these results in [3].

In this paper we reconsider this problem from a somewhat different point of view. For simplicity we assume throughout that l is an odd prime. Well-known results allow us to reduce the problem to the case where the Galois group of K over $\mathbf{Q}$, $gal(K/\mathbf{Q})$, is equal to the direct product of its ramification groups. Our next reduction allows us to simplify to the case when $gal(K/\mathbf{Q})$ is an elementary Abelian l-group. This reduction theorem allows us to develop a simple algorithm for computing the rank of the central class field of many Abelian l-extensions K by means of matrices with coefficients from the finite field with l elements.

We would like to thank the Mathematical Sciences Research Institute for its hospitality during the period when the research on this paper was carried out.

Received December 16, 1986.

[1]Partially supported by a grant from the Vaughn Foundation. Research at MSRI sponsored by a grant from the National Science Foundation.

[2]Partially supported by grants from the Vaughn Foundation and the National Science Foundation.

Section 1

If $K/\mathbf{Q}$ is Abelian, the genus field K_G of K is the maximal unramified extension of K which is Abelian over $\mathbf{Q}$. Let $K/\mathbf{Q}$ be of odd degree n and $e_1, e_2, \ldots, e_t$ be the ramification indices for the primes in $\mathbf{Q}$ that ramify in K. H. Leopoldt proved that

$$[K_G : K] = e_1 e_2 \ldots e_t / n.$$

It follows that if $K/\mathbf{Q}$ is an Abelian l-extension then so is K_G/K. (This can also be directly proved in an elementary manner without Leopoldt's theorem.) In any case, unless $K_G = K$, l will divide the class number h_K of K. This in turn can only happen when $e_1 e_2 \ldots e_t = n$, or $gal(K/\mathbf{Q})$ is the direct product of its ramification subgroups. Hence forth we will assume that K satisfies these (equivalent) conditions.

We will let K_C be the central class field of K. (Again K_C is the maximal l-extension K_C of K such that K_C/K is Abelian and unramified, $K_C/\mathbf{Q}$ is Galois and $gal(K_C/K)$ is in the center of $gal(K_C/\mathbf{Q})$.) Clearly, the genus field $K_G \subseteq K_C$. Furuta determined the structure of $gal(K_G/K_C)$; for example, see [4]. In our case the answer is that it is a group

$$\mathscr{A}(K/\mathbf{Q}) = \mathbf{Q}^* \cap \mathbf{N}_{K/Q} I_K / \mathbf{N}_{K/Q} K^*,$$

where I_K is the idele group of K and $\mathbf{N}$ is the norm map. J. Tate had previously given a cohomological interpretation of this group. For Tate's theorem set $G = gal(K/\mathbf{Q})$ and let G_i, $1 \le i \le t$, be the decomposition groups of the primes in $\mathbf{Q}$ ramified in K. Then

$$\mathscr{A}(K/\mathbf{Q}) \cong H^{-3}(G, \mathbf{Z}) \text{ modulo the sum of the images of } H^{-3}(G_i, \mathbf{Z}) \text{ under corestriction.}$$

We will analyze this group further in Section 2. For now we note that if G is an l-group so is $\mathscr{A}(K/\mathbf{Q}) \cong gal(K_C/K_G)$.

Since an l-group must have a lower central series that terminates in the identity, one sees that $l \nmid h_K$ if and only if $l \nmid |K_C : K|$. We refine the field K_C a little by taking a slightly smaller field C, where C is the maximal elementary l-extension of K such that C/K is unramified, C/K is Galois, and $gal(C/K)$ is in the center of $gal(C/\mathbf{Q})$. We will call C the *l-elementary central class field* of K. Clearly, C is the fixed field of K_C under the action of $gal(K_C/K)^l$. Thus

$$\operatorname{rank}_l[gal(K_C/K)] = \operatorname{rank}_l[gal(C/K)].$$

Our investigation of $gal(C/K)$ is made much easier by the following theorem —which may be of independent interest.

THEOREM 1. *Let $K/\mathbf{Q}$ be an Abelian l-extension with the genus field of K satisfying, $K_G = K$. Let $\mathbf{Q} \subset K_1 \subset K$ be the maximal intermediate extension between $\mathbf{Q}$ and K such that $gal(K_1/\mathbf{Q})$ is an elementary l-group. Then the l-rank of the central class field of K is equal to the l-rank of the central class field of K_1.*

Our proof of this reduction theorem needs the following lemma from group theory.

LEMMA. *Let G be a finite group and Z the center of G. Suppose that the commutator subgroup $[G, G] \subseteq Z$ and $[G, G]^m = e$, the identity of G, for some integer m. Then $G^m \subseteq Z$.*

Proof. Define $[a, b] = a^{-1}b^{-1}ab$. If $a, b, c \in G$ we have

$$[ab, c] = b^{-1}[a, c]b[b, c].$$

If $[G, G] \subseteq \mathbf{Z}$ then for $g \in G$, the map $x \mapsto [x, g]$ is a homomorphism from G to $[G, G]$. If $[G, G]^m = e$, then $[x^m, g] = e$ for all x in G. Thus $G^m \subseteq Z$.

Remark. If $a, b \in G$ and $c = a^{-1}b^{-1}ab$ is in the center of G, it is easy to see by induction that $a^ib^i = (ab)^ic^{i(i-1)/2}$. If m is odd, it follows that $a^mb^m = (ab)^m$ which shows that under our hypothesis G^m is a subgroup of Z. We do not need this fact.

Proof of Theorem 1. Let C and C_1 be the l-elementary central class fields of K and K_1 respectively. Consider the following diagram:

$$\begin{tikzcd}
 & C \\
K \arrow[ur, dash] \arrow[dd, dash] & \\
 & C_1 \\
K_1 \arrow[ur, dash] \arrow[d, dash] & \\
\mathbf{Q} &
\end{tikzcd}$$

We will show that (i) $K \cap C_1 = K_1$ and (ii) $KC_1 = C$. It follows from this that $gal(C/K) \cong gal(C_1/K_1)$ which proves the theorem.

Let p be a prime of $\mathbf{Q}$ ramified in K and let $T_{K/\mathbf{Q}}(p)$ be the common ramification group of the primes above p in K. By our hypothesis that $K = K_G$, $gal(K/\mathbf{Q}) = G = \Pi T_{K/\mathbf{Q}}(p)$; where the direct product is over the ramified primes.

Now $gal(K/K_1) = G^l = \prod T_{K/\mathbf{Q}}(p)^l$. Define $T_{K/K_1}(p)$ in the obvious way. Then

$$T_{K/K_1}(p) = T_{K/\mathbf{Q}}(p) \cap G^l = T_{K/\mathbf{Q}}(p)^l$$

and so $gal(K/K_1) = \prod T_{K/K_1}(p)$. This implies that K_1 has no unramified extensions in K and it follows that $K \cap C_1 = K_1$. This establishes (i).

Let p be a prime in $\mathbf{Q}$ ramified in K, and $\mathscr{P}_1$ a prime of C lying above p. Let $\mathscr{G}$ be $gal(C/\mathbf{Q})$ and let $T(\mathscr{P}_1) \subseteq \mathscr{G}$ be the ramification group of $\mathscr{P}_1$ in $\mathscr{G}$. Since C/K is unramified we know that restriction to K gives an isomorphism of Abelian groups:

$$T(\mathscr{P}_1) \cong T_{K/\mathbf{Q}}(p) \quad \text{and} \quad T(\mathscr{P}_1)^l \cong T_{K/K_1}(p).$$

Suppose $\mathscr{P}_2$ is another prime of C above p. Then there is a $g \in \mathscr{G}$ such that

$$g^{-1}T(\mathscr{P}_1)g = T(\mathscr{P}_2).$$

We now use the lemma. Since $[\mathscr{G}, \mathscr{G}] \subseteq gal(C/K)$ which is in the center of $\mathscr{G}$, and $gal(C/K)^l = e$, we find that $T(\mathscr{P}_1)^l = T(\mathscr{P}_2)^l$ is a subgroup of the center of $\mathscr{G}$. Write $T(\mathscr{P}_1)^l = T_{C/K_1}(p)$. It is the common ramification group in $gal(C/K_1)$ of *any* prime of C lying above p.

For each ramified prime $\mathscr{P}$, we have defined a subgroup $T_{C/K_1}(p)$ which is the same for all $\mathscr{P}$ above p. It is also a subgroup of the center of $gal(C/K_1)$ and so $\prod T_{C/K_1}(p)$ is a subgroup of $gal(C/K_1)$. Let C_1' be the fixed field of this product. C_1' is unramified over K_1 so by the remark made above, $C_1' \cap K = K_1$. It now follows that $gal(C/K)$ maps onto $gal(C_1'/K_1)$. This implies that $gal(C_1'/K_1)$ is also elementary Abelian and central in $gal(C_1'/Q)$. Since $C_1 \subseteq C_1'$ is maximal with this property, we must have $C_1 = C_1'$.

From $[C:K_1] = [C:K][K:K_1] = [C:C_1][C_1:K_1]$ we deduce

$$[C:K] \cdot \prod \left|T_{K/K_1}(p)\right| \leq [C_1:K_1] \cdot \prod \left|T_{C/K_1}(p)\right|.$$

Recalling that $T_{C/K_1}(p) \cong T_{K/K_1}(p)$ we find that $[C:K] \leq [C_1:K_1]$.

On the other hand, $KC_1 \subseteq C$, so

$$[C:K] \geq [KC_1:K] = [C_1:C_1 \cap K] = [C_1:K_1].$$

Thus $[C:K] = [C_1:K_1]$ and so $[C:K] = [KC_1:K]$ implying $KC_1 = C$. This establishes (ii) and we're done.

Section 2

In this section we suppose that $gal(K/\mathbf{Q}) \cong (\mathbf{Z}/l\mathbf{Z})^m$, where as usual l is an odd prime. Suppose $p_1, p_2, \ldots, p_t$ are the primes ramifying in K with inertia groups T_i and decomposition groups G_i. As before K_G and K_C will be the genus field of K and the central class field of K respectively. As mentioned in Section 1, since l is odd, Furuta's theorem implies that $gal(K_C/K_G) \cong \mathscr{A}(K/\mathbf{Q})$, the group of non-zero rationals which are local norms everywhere modulo global norms. Also, as mentioned before, Tate's theorem implies that $\mathscr{A}(K/\mathbf{Q})$ is the cokernel of the natural map from $\oplus_{i=1}^{t} H^{-3}(G_i, \mathbf{Z})$ to $H^{-3}(G, \mathbf{Z})$ induced by co-restriction. It is well known that $H^{-3}(G, \mathbf{Z}) \cong \Lambda^2(G)$, the second exterior power of G. (For a direct proof see [5] or for a proof in a more general setting see Brown [1]. This identification is functorial and we have:

THEOREM. *$gal(K_C/K_G)$ is isomorphic to the cokernel of the natural map from $\oplus_{i=1}^{t}\Lambda^2(G_i)$ to $\Lambda^2(G)$.*

For a proof see Razar's paper [5].

This theorem when combined with our reduction theorem lends itself to computations. For these see Section 3. However first note that the dimension of $\Lambda^2(G)$ over $\mathbf{Z}/l\mathbf{Z}$ is $m(m-1)/2$ and since the decomposition group $G_i \cong \mathbf{Z}/l\mathbf{Z}$ or $(\mathbf{Z}/l\mathbf{Z})^2$, the dimension of $\Lambda^2(G_i)$ is zero or one. Thus we have:

COROLLARY. *The dimension of $gal(K_C/K_G)$ is greater than or equal to $m(m-1)/2 - t$ where t is the number of ramified primes. When $t = m$, we have $K_G = K$ and $\dim_l(gal(K_C/K)) \geq m(m-3)/2$. So in this case $l \mid h_K$ as soon as $m \geq 4$.*

For more details see Cornell-Rosen [2].

This corollary shows that $m = 2$ and $m = 3$ are the key cases for Fröhlich's theorem. The case when $m = 2$ is easily disposed of:

PROPOSITION 2. *Suppose $m = 2$ and $p_i \neq l$ for $i = 1, 2$. Then $l \mid h_K$ if and only if $x^l \equiv p_1\ (p_2)$ and $x^l \equiv p_2\ (p_1)$ are both solvable, i.e., iff they are mutual l-th power residues.*

Proof. $\Lambda^2(G)$ is of dimension one in this case. So $gal(K_C/K)$ is non-trivial if and only if $G_i = T_i$ for $i = 1, 2$. This holds iff the stated congruences are solvable. For more details see Proposition 4 of [2]. We must modify this proposition slightly when one of the primes is l.

PROPOSITION 3. *Suppose $m = 2$ and l and p are the only primes ramified in K. Then $l | h_K$ if and only if $x^l \equiv l\ (p)$ and $p^{l-1} \equiv 1\ (l^2)$.*

We leave the proof of this to the reader.

To deal with the case $m = 3$ we need the following lemma which is stated without proof in [5]. For completeness we will give the proof.

LEMMA. *Let V be a three-dimensional vector space over a field F. Let $V_i \subset V$ for $i = 1, 2, 3$ be proper subspaces. The natural map from $\oplus_{i=1}^{3} \Lambda^2(V_i)$ to $\Lambda^2 V$ is onto if and only if:*

(i) $\dim V_i = 2$ *and* $V_i \neq V_j$ *for* $i \neq j$;

(ii) *if* $V_i \cap V_j = \langle x_{ij} \rangle$ *for* $i \neq j$, *then* x_{12}, x_{13} *and* x_{23} *is a basis for* V.

Proof. The pairing Φ: $\Lambda^2(V) \times V \to \Lambda^3(V) \cong F$ given by

$$\Phi(x \wedge y, z) = x \wedge y \wedge z$$

is non-degenerate. Assume that $\oplus_{i=1}^{3} \Lambda^2(V_i) \to V$ is onto. Then clearly each of the V_i has dimension 2 and $V_i \neq V_j$ for $i \neq j$. Thus condition (i) is satisfied. Write $V_1 = \langle x_{12}, u \rangle$, $V_2 = \langle x_{12}, v \rangle$, and $V_3 = \langle x_{13}, w \rangle$. By hypothesis, $x_{12} \wedge u$, $x_{12} \wedge v$ and $x_{13} \wedge w$ is a basis of $\Lambda^2(V)$. From the non-degeneracy of Φ we see $x_{12} \wedge x_{13} \wedge w \neq 0$. Thus x_{12} and x_{13} are linearly independent and $V_1 = \langle x_{12}, x_{13} \rangle$. Similarly, $V_2 = \langle x_{12}, x_{23} \rangle$, $V_3 = \langle x_{13}, x_{23} \rangle$. We now take $w = x_{23}$ so $x_{12} \wedge x_{13} \wedge x_{23} \neq 0$ which gives condition (ii).

Conversely suppose (i) and (ii) are satisfied. From (i) and (ii) we see $V_1 = \langle x_{12}, x_{13} \rangle$, $V_2 = \langle x_{12}, x_{23} \rangle$, $V_3 = \langle x_{13}, x_{23} \rangle$. Thus the image of $\oplus_{i=1}^{3} \Lambda^2(V_i)$ is generated by $x_{12} \wedge x_{13}$, $x_{12} \wedge x_{23}$ and $x_{13} \wedge x_{23}$ which is a basis of $\Lambda^2(V)$ by (ii).

THEOREM 2. *Suppose $m = 3$ and there are three ramified primes. Let D_i, $i = 1, 2, 3$, be the decomposition field of p_i, i.e., the fixed field of G_i. Then $l \nmid h_K$ if and only if $[D_i : \mathbf{Q}] = l$ for each i and $D_1 D_2 D_3 = K$.*

Proof. We know $l \nmid h_K$ if and only if $K_C = K$. By the previous remarks this happens if and only if the map $\oplus \Lambda^2(G_i) \to \Lambda^2(G)$ is onto. By the lemma this is true if and only if $\dim G_i = 2$, $G_i \neq G_j$ for $i \neq j$ and $G_1 \cap G_2$, $G_1 \cap G_3$ and $G_2 \cap G_3$ generate G. In terms of fields these conditions are

(i) $[D_i : \mathbf{Q}\} = l$ for each i and $D_i \neq D_j$ for $i \neq j$

and

(ii) $D_1 D_2 \cap D_1 D_3 \cap D_2 D_3 = \mathbf{Q}$.

Suppose (i) and (ii) hold. It follows easily that $D_1 = D_1 D_2 \cap D_1 D_3$ so that $D_1 \cap D_2 D_3 = \mathbf{Q}$. This implies that $D_1 D_2 D_3 = K$. Conversely if $D_1 D_2 D_3 = K$

and $[D_1 : \mathbf{Q}] = l$ for each i, then we must have

$$D_1 \cap D_2D_3 = \mathbf{Q} \quad \text{and} \quad D_1 = D_1D_2 \cap D_1D_3$$

so both (i) and (ii) hold.

Theorem 2 has a pleasing symmetry about it but the field-theoretic condition given there isn't easy to verify. So we are still left with finding an algorithm for determining whether $l|h_K$ or not. In the next section we will give such an algorithm and leave to the reader the task of relating our approach to that of Fröhlich in [3].

Section 3

In this section K is a field such that $G = gal(K/\mathbf{Q}) \cong (\mathbf{Z}/l\mathbf{Z})^m$ and exactly m primes ramify from $\mathbf{Q}$ to K. For simplicity we will assume l is not ramified in K. The modifications for this case are simple and we leave them to the reader. Let K_i be the fixed field of $\prod_{j \neq i} T_j$ where T_j is the inertia group of p_j. K_i is the unique Abelian extension of $\mathbf{Q}$ ramified only at p_i of degree l. (So of course $p_i \equiv 1\ (l)$). This in turn implies that K_i is the unique subfield of $\mathbf{Q}(\zeta_{p_i})$ of degree l over $\mathbf{Q}$. Let $N = p_1 p_2 \dots p_m$. Then K is the maximal elementary Abelian l-extension of $\mathbf{Q}$ contained in $\mathbf{Q}(\zeta_N)$. Let $G_N \cong (\mathbf{Z}/N\mathbf{Z})^*$ be the Galois group of $\mathbf{Q}(\zeta_N)$ over $\mathbf{Q}$. $G \cong G_N/G_N^l$. We will do our calculations in G_N but then interpret the results modulo l in order to descend to G. The first step is to provide explicit generators for T_i and G_i. For this we need some notation. For any integer n, we let $\bar{n}$ be the reduction of n modulo N *and* then modulo l-th powers. Thus $\bar{n}$ can be considered as an element of G. Let τ_i be a primitive root mod p_i and choose $t_i \equiv \tau_i\ (p_i)$ and $t_i \equiv 1\ (p_j)$ for $j \neq i$. Then $\bar{t}_i$ generates T_i. Now choose s_i such that $s_i \equiv 1\ (p_i)$ and $s_i \equiv p_i\ (p_j)$ for $j \neq i$. Then $\bar{t}_i$ and $\bar{s}_i$ generate G_i. These assertions follow from the basic arithmetic properties of cyclotomic fields.

By hypothesis, $\bar{t}_1, \bar{t}_2, \dots \bar{t}_m$ is a vector space basis for G. Thus

$$\bar{s}_i = \bar{t}_1^{a_{i1}} \bar{t}_2^{a_{i2}} \dots \bar{t}_m^{a_{im}}, \quad i = 1, \dots m,$$

where the a_{ij} are uniquely determined modulo l. These integers a_{ij} are fundamental to our algorithm so we note that they are easily calculated. Consider

$$s_i \equiv t_1^{a_{i1}} t_2^{a_{i2}} \dots t_m^{a_{im}} \quad (N);$$

reducing mod p_i yields $1 \equiv \tau_i^{a_{ii}}\ (p_i)$. Thus $a_{ii} = 0$. Reducing modulo p_j for $j \neq i$ gives $p_i \equiv \tau_j^{a_{ij}}\ (p_j)$. Thus to find $\bar{a}_{ij}$, calculate the index of p_i modulo p_j

for the base τ_j then reduce modulo l. This is most easily done using a table of indices or a short computer program.

We hope to make matters less confusing now by writing the operation in G additively, and omitting the bars. Then

(i) $s_i = \Sigma_j a_{ij} t_j$

and

(ii) $s_i \wedge t_i = \Sigma a_{ij} t_j \wedge t_i$.

The set $\{t_i \wedge t_j | i < j\}$ is a basis for $\Lambda^2(G)$. Using equation (ii) we can express $s_i \wedge t_i$ as linear combination of these basis elements. The rank of the resulting coefficient matrix is the dimension of the image of $\oplus \Lambda^2(G_i)$ in $\Lambda^2(G)$. Call this number r. Then

$$\dim_l(gal(K_C/K)) = m(m-1)/2 - r.$$

In the case $m = 3$ the matrix in question is

$$(**) \qquad \begin{pmatrix} -a_{12} & -a_{13} & 0 \\ a_{21} & 0 & -a_{23} \\ 0 & a_{31} & a_{32} \end{pmatrix}.$$

Since $m(m-1)/2 = 3$ in this case we have $l \nmid h_K$ only if the matrix $(**)$ is non-singular. We finish this paper by giving examples when $l = 3$ which show that r, the rank of $(**)$, can take on any value between zero and three.

For a matrix of rank three, take $p_1 = 7$, $p_2 = 13$, and $p_3 = 19$ with corresponding primitive roots 3, 2, and 2. The matrix entries a_{ij} corresponding to this choice of primitive roots are

$$a_{12} = 11, \quad a_{13} = 6, \quad a_{21} = 3, \quad a_{23} = 5, \quad a_{31} = 5, \quad a_{32} = 5.$$

Reducing modulo 3 and substituting into $(**)$ yields

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 2 & 2 \end{pmatrix}$$

which is of rank 3. It follows that the maximal 3-extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_{7\cdot 13\cdot 19})$ has class number prime to 3.

For a matrix of rank 2, take $p_1 = 7$, $p_2 = 13$, and $p_3 = 43$ with corresponding primitive roots 3, 2, and 3. The a_{ij} are

$$a_{12} = 11, \quad a_{13} = 25, \quad a_{21} = 3, \quad a_{23} = 32, \quad a_{31} = 0, \quad a_{32} = 2.$$

Reducing modulo 3 and substituting into $(**)$ yields

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

which has rank 2. It follows that the central class field of the maximal 3-extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_{7\cdot 13\cdot 43})$ has rank equal to 1.

For a matrix of rank 1, take $p_1 = 7$, $p_2 = 13$, and $p_3 = 421$ with corresponding primitive roots 3, 2, and 2. The a_{ij} are

$$a_{12} = 11, \quad a_{13} = 366, \quad a_{21} = 3, \quad a_{23} = 63, \quad a_{31} = 0, \quad a_{32} = 9.$$

Reducing modulo 3 and substituting into $(**)$ yields

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

which has rank 1. It follows that the central class field of the maximal 3-extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_{7\cdot 13\cdot 421})$ has rank 2.

Finally, take $p_1 = 7$, $p_2 = 181$, and $p_3 = 673$ with corresponding primitive roots 3, 2, and 5. The a_{ij} are

$$a_{12} = 5, \quad a_{13} = 486, \quad a_{21} = 3, \quad a_{23} = 531, \quad a_{31} = 0, \quad a_{32} = 141.$$

Since all these numbers are divisible by 3, the matrix under consideration is the zero matrix which, of course, has rank zero. Thus the central class field of the maximal 3-extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_{7\cdot 181\cdot 673})$ has the maximal possible rank, namely 3.

References

1. K. Brown, *Cohomology of Groups*, Springer Verlag, New York, 1982.
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. A. Fröhlich, *Central extensions, Galois groups, and the ideal class groups of number fields*, Contemp. Math., vol. 24, Amer. Math. Soc., Providence, Rhode Island, 1983.
4. Y. Furuta, *On class field towers and the rank of ideal class groups*, Nagoya Math. J., vol. 48 (1972), pp. 147–157.
5. M. Razar, *Central and genus class fields and the Hasse norm theorem*; Compositio Math., vol. 35 (1977), pp. 281–298.

University of Connecticut
Storrs, Connecticut
Brown University
Providence, Rhode Island