NUMBER FIELDS WITH PRESCRIBED
l-CLASS GROUPS¹
FRANK GERTH III

ABSTRACT. Let G be any finite elementary abelian l-group, where
l is a rational prime. We show that there exist infinitely many number
fields whose l-class groups are isomorphic to G.

1. Introduction. Let \( \mathbb{Q} \) denote the field of rational numbers, and let \( F \)
be a finite extension field of \( \mathbb{Q} \). It is well known that the ideal class group
of the number field \( F \) is a finite abelian group. We pose the following
question: Given any finite abelian group \( G \), does there exist a number field
\( F \) whose ideal class group is isomorphic to \( G \)? Fröhlich [2], Hasse [4], and
others have shown that there is a number field \( F \) whose ideal class group
has a factor group (and a subgroup) isomorphic to \( G \). However, the question
we have posed appears to be much more difficult and is unsolved at the pre-
sent time. A related question is the following: Given a finite abelian l-
group \( G \), where \( l \) is a rational prime, does there exist a number field \( F \) whose
l-class group is isomorphic to \( G \)? (By the l-class group, we mean the Sylow
l-subgroup of the ideal class group.) In this paper we provide a partial
answer to this question by showing that every finite elementary abelian l-
group is isomorphic to the l-class group of some number field.

2. Cases where \( l \) is an odd prime. Let \( p_1, \ldots, p_n \) be distinct rational
primes with \( p_i \equiv 1 \pmod{l} \) for each \( i \), where \( l \) is an odd prime. Let \( F \) be a
cyclic extension of \( \mathbb{Q} \) of degree \( l \) whose discriminant is divisible by \( p_1, \ldots, p_n \) and by no other rational primes. Let \( H_i \) be the cyclic extension of
\( \mathbb{Q} \) of degree \( l \) whose discriminant is divisible only by \( p_i, 1 \leq i \leq n \). Let \( K_i = F \cdot H_i \) for \( 1 \leq i \leq n \), and let \( K = K_1 \cdots K_n = F \cdot H_1 \cdots H_n \) (in fact, \( K = H_1 \cdots H_n \) since \( F \subseteq H_1 \cdots H_n \)). Then \( K_i \) is a cyclic extension of \( F \) of
degree \( l \) (if \( n \geq 2 \)), and \( K \) is an abelian extension of \( F \) whose Galois group

¹This research was supported in part by NSF Grant GP-28488A2.
is an elementary abelian \( l \)-group of rank \( n - 1 \). Moreover \( K \) is unramified over \( F \), and hence each \( K_i \) is unramified over \( F \) [5, Theorem 1]. Let \( C_F \) denote the ideal class group of \( F \), and let \( \tau \) be a generator of the cyclic \( l \)-group \( \text{Gal}(F/Q) \). Then

\[
\text{Gal}(K/F) \simeq C_F/C_F^{1-\tau}, \quad \text{where} \quad C_F^{1-\tau} = \{a^{1-\tau} \mid a \in C_F\},
\]

since \( K \) is the genus field of \( F/Q \) [5, Theorem 1].

Let \( C_F^{(\tau)} = \{a \in C_F \mid a^\tau = a\} \). If \( a \in C_F^{(\tau)} \), then

\[
a^\tau = a^{1+\tau+\cdots+\tau^{l-1}} = 1,
\]

since \( a^{1+\tau+\cdots+\tau^{l-1}} \) is the norm of the ideal class \( a \) (hence an element of \( C_Q \)), and the ideal class group \( C_Q \) of \( Q \) is trivial. So \( C_F^{(\tau)} \) is an elementary abelian \( l \)-group. From the exact sequence

\[
1 \to C_F^{(\tau)} \to C_F^\tau \to C_F/C_F^{1-\tau} \to 1,
\]

where \( \beta(a) = a^{1-\tau} \) for \( a \in C_F \), we see that \( C_F^{(\tau)} \) and \( C_F/C_F^{1-\tau} \) have the same order. So both are elementary abelian \( l \)-groups of rank \( n - 1 \).

Now let

\[
\Psi: C_F^{(\tau)} \to C_F^\tau \to C_F/C_F^{1-\tau} \simeq \text{Gal}(K/F),
\]

where the first map is the natural inclusion, the second map is the natural projection, and the third map is the canonical isomorphism. Note that

\[
\ker \Psi = C_F^{(\tau)} \cap C_F^{1-\tau} \quad \text{and} \quad \text{im} \Psi \simeq (C_F^{(\tau)} \cdot C_F^{1-\tau})/C_F^{1-\tau}.
\]

Next let \( \mathfrak{P}_i \) denote the unique prime in \( F \) which divides \( p_i \), \( 1 \leq i \leq n \). Let \( S \) be the free abelian group generated by \( \mathfrak{P}_1, \cdots, \mathfrak{P}_n \), and define a map

\[
S \to C_F^{(\tau)}, \quad \mathfrak{P} \mapsto \text{cl}(\mathfrak{P}),
\]

where \( \text{cl}(\mathfrak{P}) \) denotes the ideal class of the ideal \( \mathfrak{P} \) in \( F \). It can be easily proved [3, §13] that the cokernel of this map is isomorphic to \((E_Q \cap NF^*)/NE_F^\tau\), where \( E_Q \) (resp. \( E_F \)) denotes the group of units of \( Q \) (resp. \( F \)), \( F^* = F - \{0\} \), and \( N \) denotes the norm map from \( F \) to \( Q \). Since \([F:Q] = l \) is odd, then \( NE_F = E_Q \), and hence the map \( S \to C_F^{(\tau)} \) is surjective. Since \( \text{cl}(\mathfrak{P}_i)^l = \text{cl}(p_i) = 1 \) for each \( i \), the map \( S \to C_F^{(\tau)} \) induces a surjective map \( S/S^l \to C_F^{(\tau)} \). We let \( \phi \) be the composite map

\[
\phi: S/S^l \to C_F^{(\tau)} \to \text{Gal}(K/F),
\]

where \( (\mathfrak{P}, K/F) \) denotes the Artin symbol.
We may view $\phi$ as a linear map from the vector space $S/S^l$ of dimension $n$ over the finite field $F$ to the vector space $\text{Gal}(K/F)$ of dimension $n - 1$ over $F$. Using the basis $\mathfrak{p}_1 \mod S^l, \ldots, \mathfrak{p}_n \mod S^l$ for $S/S^l$ and the isomorphism

$$\text{Gal}(K/F) \cong \text{Gal}(K_1/F) \times \cdots \times \text{Gal}(K_{n-1}/F),$$

$$(\mathfrak{p}_j, K/F) \mapsto (\mathfrak{p}_j, K_1/F) \times \cdots \times (\mathfrak{p}_j, K_{n-1}/F),$$

we see that the matrix of $\phi$ has $ij$th element $(\mathfrak{p}_j, K_i/F), 1 \leq i \leq n - 1, 1 \leq j \leq n$. Applying class field theory when $i \neq j$, we see that $(\mathfrak{p}_j, K_i/F)$ is trivial $\iff \mathfrak{p}_j$ decomposes in $K_i$ $\iff p_j$ decomposes in $H_i$ $\iff p_j$ is an $l$th power residue modulo $p_i$.

**Theorem 1.** Let $r$ be any nonnegative integer, $n = r + 1$, and $l$ an odd prime. Let $p_1, \ldots, p_n$ be rational primes such that $p_i \equiv 1 \pmod{l}$ for $1 \leq i \leq n$. Furthermore assume $p_2$ is an $l$th power nonresidue modulo $p_1$, and for $3 \leq m \leq n$, $p_m$ is an $l$th power residue modulo $p_1, \ldots, p_{m-1}$ but an $l$th power nonresidue modulo $p_{m-2}$. Let $F$ be a cyclic extension of $Q$ of degree $l$ with discriminant divisible by $p_1, \ldots, p_n$ but by no other rational primes. Then the $l$-class group of $F$ is an elementary abelian $l$-group of rank $r$.

**Remark.** By Dirichlet's theorem on primes in an arithmetic progression, there exist primes $p_1, \ldots, p_n$ which satisfy the hypothesis of the theorem (e.g., $p_m$ can be chosen from a congruence modulo $l p_1 \cdots p_{m-1}$). In fact there exist infinitely many such primes $p_1, \ldots, p_n$.

**Corollary.** Let $G$ be any finite elementary abelian $l$-group. Then there exist infinitely many cyclic fields of degree $l$ over $Q$ whose $l$-class groups are isomorphic to $G$.

**Proof of Theorem 1.** We use the notation previously defined in this section. Our first claim is that $\phi$ is surjective for the choice of $p_1, \ldots, p_n$ in the statement of the theorem. This follows from the fact that $\text{rank}((\mathfrak{p}_j, K_i/F)) = n - 1$, where $((\mathfrak{p}_j, K_i/F))$ denotes the $(n - 1) \times n$ matrix of $\phi$. (To see that the rank of this matrix is $n - 1$, use the fact that if $i \neq j$, then $(\mathfrak{p}_j, K_i/F)$ is trivial $\iff p_j$ is an $l$th power residue modulo $p_i$.)

Since $\phi$ is surjective, then $\Psi$ is surjective, and hence $(C_F^r) \cdot C_F^{1-r}/C_F^{1-r} = C_F/C_F^{1-r}$. Since $\text{cl}(\mathfrak{p}_1), \text{cl}(\mathfrak{p}_2), \ldots, \text{cl}(\mathfrak{p}_n)$ generate $C_F^r$, then the images of $\text{cl}(\mathfrak{p}_1), \text{cl}(\mathfrak{p}_2), \ldots, \text{cl}(\mathfrak{p}_n)$ in $C_F/C_F^{1-r}$ generate $C_F/C_F^{1-r}$. Since $l | (1 - r)_l$,
NUMBER FIELDS WITH PRESCRIBED \( l \)-CLASS GROUPS

\[
\text{cl}(\mathfrak{P}_1), \text{cl}(\mathfrak{P}_1)^{1-r}, \ldots, \text{cl}(\mathfrak{P}_1)^{(1-r)^{l-1}}, \text{cl}(\mathfrak{P}_2), \text{cl}(\mathfrak{P}_2)^{1-r}, \ldots, \\
\text{cl}(\mathfrak{P}_2)^{(1-r)^{l-1}}, \ldots, \text{cl}(\mathfrak{P}_n), \text{cl}(\mathfrak{P}_n)^{1-r}, \ldots, \text{cl}(\mathfrak{P}_n)^{(1-r)^{l-1}}
\]
generate the Sylow \( l \)-subgroup of \( C_F \). But \( \text{cl}(\mathfrak{P}_i)^{1-r} = 1 \) for all \( i \) since \( \mathfrak{P}_i = \mathfrak{P}_i \). So \( \text{cl}(\mathfrak{P}_1), \text{cl}(\mathfrak{P}_2), \ldots, \text{cl}(\mathfrak{P}_n) \) generate the \( l \)-class group of \( F \). Since the group generated by \( \text{cl}(\mathfrak{P}_1), \text{cl}(\mathfrak{P}_2), \ldots, \text{cl}(\mathfrak{P}_n) \) is also \( C_F^{(r)} \), an elementary abelian \( l \)-group of rank \( n - 1 \), the theorem is proved.

3. Case \( l = 2 \).

**Theorem 2.** Let \( r \) be any nonnegative integer, and let \( n = r + 1 \). Let \( p_1, \ldots, p_n \) be rational primes such that \( p_i \equiv 1 \mod 4 \) for \( 1 \leq i \leq n \).

Furthermore assume \( p_2 \) is a quadratic nonresidue modulo \( p_1 \), and for \( 3 \leq m \leq n \), \( p_m \) is a quadratic residue modulo \( p_1, \ldots, p_{m-2} \) but a quadratic nonresidue modulo \( p_{m-1} \). Let \( F \) be the quadratic extension of \( \mathbb{Q} \) with discriminant \( p_1 \cdots p_n \). Then the 2-class group (in the strict sense and in the wide sense) of \( F \) is an elementary abelian 2-group of rank \( r \).

**Remark.** Again Dirichlet’s theorem shows that there exist infinitely many primes which satisfy the hypothesis of the theorem.

**Corollary.** Let \( G \) be any finite elementary abelian 2-group. Then there exist infinitely many quadratic extensions of \( \mathbb{Q} \) whose 2-class groups are isomorphic to \( G \).

**Proof of Theorem 2.** Let \( C_{F,s} \) (resp. \( C_{F,w} \)) denote the ideal class group of \( F \) in the strict (resp. wide) sense. We recall that \( C_{F,s} \cong C_{F,w} \) if \(-1\) is the norm of a unit of \( F \), and \( |C_{F,s}| = 2|C_{F,w}| \) otherwise \([1, p. 240]\).

For the 2-class group in the strict sense, there is a proof of Theorem 2 that is analogous to the proof of Theorem 1. On the other hand, it appears that we cannot use the same proof for the 2-class group in the wide sense because we do not know a priori that \( \text{cl}(\mathfrak{P}_1), \ldots, \text{cl}(\mathfrak{P}_n) \) generate \( C_{F,w}^{(r)} \); in fact, \( \text{cl}(\mathfrak{P}_1), \ldots, \text{cl}(\mathfrak{P}_n) \) generate \( C_{F,w}^{(r)} \iff -1 \) is the norm of a unit of \( F \).

However, with the choice of \( p_1, \ldots, p_n \) in the statement of Theorem 2, the matrix of

\[
\phi: S/S' \to C_{F,w}^{(r)} \to \text{Gal}(K/F), \quad \mathfrak{P} \mod S' \mapsto \text{cl}(\mathfrak{P}) \mapsto (\mathfrak{P}, K/F)
\]

has rank \( n - 1 \), which implies that the map \( S/S' \to C_{F,w}^{(r)} \) must be surjective because \( C_{F,w}^{(r)} \) is an elementary abelian 2-group of rank \( n - 1 \). Hence
\( \text{cl}(\mathbb{P}_1), \ldots, \text{cl}(\mathbb{P}_n) \) generate \( C^{(\alpha)}_{F_{\mathcal{O}}} \), and Theorem 2 can be proved in a manner similar to that of Theorem 1.

Remark. It follows from the above proof that \(-1\) is the norm of a unit of \( F \). So there exist real quadratic fields whose discriminants are divisible by arbitrarily many rational primes but whose fundamental units have norm equal to \(-1\). (See also [6], [7], and [8].)

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PENNSYLVANIA 19174

*Current address*: Department of Mathematics, University of Texas, Austin, Texas 78712