PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 2, June 1975

NUMBER FIELDS WITH PRESCRIBED l-CLASS GROUPS[1]

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 $\mathbf{Q}$ denote the field of rational numbers, and let F be a finite extension field of $\mathbf{Q}$. 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 present 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 $p_1, \cdots, p_n$ 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 $\mathbf{Q}$ of degree l whose discriminant is divisible by $p_1, \cdots, p_n$ and by no other rational primes. Let H_i be the cyclic extension of $\mathbf{Q}$ 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

Received by the editors April 23, 1974.

AMS (MOS) subject classifications (1970). Primary 12A35, 12A65; Secondary 12A25.

Key words and phrases. Ideal class group, l-class group, elementary abelian l-group.

[1] This 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 τ be a generator of the cyclic l-group $\mathrm{Gal}(F/\mathbf{Q})$. Then

$$\mathrm{Gal}(K/F) \cong C_F/C_F^{1-\tau}, \qquad \text{where } C_F^{1-\tau} = \{a^{1-\tau} \mid a \in C_F\},$$

since K is the genus field of $F/\mathbf{Q}$ [5, Theorem 1].

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

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

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

$$1 \to C_F^{(\tau)} \to C_F \xrightarrow{\beta} C_F \to C_F/C_F^{1-\tau} \to 1,$$

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

$$\Psi\colon C_F^{(\tau)} \to C_F \to C_F/C_F^{1-\tau} \xrightarrow{\sim} \mathrm{Gal}(K/F),$$

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

$$\ker \Psi = C_F^{(\tau)} \cap C_F^{1-\tau} \quad \text{and} \quad \mathrm{im}\, \Psi \cong (C_F^{(\tau)} \cdot C_F^{1-\tau})/C_F^{1-\tau}.$$

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

$$S \to C_F^{(\tau)}, \qquad \mathfrak{P} \mapsto \mathrm{cl}(\mathfrak{P}),$$

where $\mathrm{cl}(\mathfrak{P})$ 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 $(E_{\mathbf{Q}} \cap NF^*)/NE_F$, where $E_{\mathbf{Q}}$ (resp. E_F) denotes the group of units of $\mathbf{Q}$ (resp. F), $F^* = F - \{0\}$, and N denotes the norm map from F to $\mathbf{Q}$. Since $[F\colon \mathbf{Q}] = l$ is odd, then $NE_F = E_{\mathbf{Q}}$, and hence the map $S \to C_F^{(\tau)}$ is surjective. Since $\mathrm{cl}(\mathfrak{P}_i)^l = \mathrm{cl}(p_i) = 1$ for each i, the map $S \to C_F^{(\tau)}$ induces a surjective map $S/S^l \to C_F^{(\tau)}$. We let ϕ be the composite map

$$\phi\colon S/S^l \to C_F^{(\tau)} \xrightarrow{\Psi} \mathrm{Gal}(K/F),$$

$$\mathfrak{P} \bmod S^l \mapsto \mathrm{cl}(\mathfrak{P}) \mapsto (\mathfrak{P}, K/F),$$

where $(\mathfrak{P}, K/F)$ denotes the Artin symbol.

We may view ϕ as a linear map from the vector space S/S^l of dimension n over the finite field $\mathbf{F}_l$ to the vector space $\mathrm{Gal}(K/F)$ of dimension $n-1$ over $\mathbf{F}_l$. Using the basis $\mathfrak{P}_1 \bmod S^l, \cdots, \mathfrak{P}_n \bmod S^l$ for S/S^l and the isomorphism

$$\mathrm{Gal}(K/F) \xrightarrow{\sim} \mathrm{Gal}(K_1/F) \times \cdots \times \mathrm{Gal}(K_{n-1}/F),$$
$$(\mathfrak{P}, K/F) \mapsto (\mathfrak{P}, K_1/F) \times \cdots \times (\mathfrak{P}, K_{n-1}/F),$$

we see that the matrix of ϕ has ijth element $(\mathfrak{P}_j, K_i/F)$, $1 \le i \le n-1$, $1 \le j \le n$. Applying class field theory when $i \neq j$, we see that $(\mathfrak{P}_j, K_i/F)$ is trivial $\Leftrightarrow$ $\mathfrak{P}_j$ decomposes in K_i $\Leftrightarrow$ p_j decomposes in H_i $\Leftrightarrow$ p_j is an lth power residue mod p_i.

Theorem 1. *Let r be any nonnegative integer, $n = r+1$, and l an odd prime. Let $p_1, \cdots, p_n$ be rational primes such that $p_i \equiv 1 \pmod{l}$ for $1 \le i \le n$. Furthermore assume p_2 is an lth power nonresidue modulo p_1, and for $3 \le m \le n$, p_m is an lth power residue modulo $p_1, \cdots, p_{m-2}$ but an lth power nonresidue modulo p_{m-1}. Let F be a cyclic extension of $\mathbf{Q}$ of degree l with discriminant divisible by $p_1, \cdots, p_n$ 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 $p_1, \cdots, p_n$ which satisfy the hypothesis of the theorem (e.g., p_m can be chosen from a congruence modulo $lp_1 \cdots p_{m-1}$). In fact there exist infinitely many such primes $p_1, \cdots, p_n$.

Corollary. *Let G be any finite elementary abelian l-group. Then there exist infinitely many cyclic fields of degree l over $\mathbf{Q}$ 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 ϕ is surjective for the choice of $p_1, \cdots, p_n$ in the statement of the theorem. This follows from the fact that $\mathrm{rank}((\mathfrak{P}_j, K_i/F)) = n-1$, where $((\mathfrak{P}_j, K_i/F))$ denotes the $(n-1) \times n$ matrix of ϕ. (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 $\Leftrightarrow$ p_j is an lth power residue modulo p_i.) Since ϕ is surjective, then Ψ is surjective, and hence $(C_F^{(\tau)} \cdot C_F^{1-\tau})/C_F^{1-\tau} = C_F/C_F^{1-\tau}$. Since $\mathrm{cl}(\mathfrak{P}_1), \mathrm{cl}(\mathfrak{P}_2), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ generate $C_F^{(\tau)}$, then the images of $\mathrm{cl}(\mathfrak{P}_1), \mathrm{cl}(\mathfrak{P}_2), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ in $C_F/C_F^{1-\tau}$ generate $C_F/C_F^{1-\tau}$. Since $l \mid (1-\tau)^l$, then

$$\mathrm{cl}(\mathfrak{P}_1), \mathrm{cl}(\mathfrak{P}_1)^{1-\tau}, \cdots, \mathrm{cl}(\mathfrak{P}_1)^{(1-\tau)^{l-1}}, \mathrm{cl}(\mathfrak{P}_2), \mathrm{cl}(\mathfrak{P}_2)^{1-\tau}, \cdots,$$
$$\mathrm{cl}(\mathfrak{P}_2)^{(1-\tau)^{l-1}}, \cdots, \mathrm{cl}(\mathfrak{P}_n), \mathrm{cl}(\mathfrak{P}_n)^{1-\tau}, \cdots, \mathrm{cl}(\mathfrak{P}_n)^{(1-\tau)^{l-1}}$$

generate the Sylow l-subgroup of C_F. But $\mathrm{cl}(\mathfrak{P}_i)^{1-\tau} = 1$ for all i since $\mathfrak{P}_i^{\tau} = \mathfrak{P}_i$. So $\mathrm{cl}(\mathfrak{P}_1), \mathrm{cl}(\mathfrak{P}_2), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ generate the l-class group of F. Since the group generated by $\mathrm{cl}(\mathfrak{P}_1), \mathrm{cl}(\mathfrak{P}_2), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ is also $C_F^{(\tau)}$, 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 $p_1, \cdots, p_n$ be rational primes such that $p_i \equiv 1 \pmod 4$ 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 $p_1, \cdots, p_{m-2}$ but a quadratic nonresidue modulo p_{m-1}. Let F be the quadratic extension of $\mathbf{Q}$ 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 $\mathbf{Q}$ 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 $\mathrm{cl}(\mathfrak{P}_1), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ generate $C_{F,w}^{(\tau)}$; in fact, $\mathrm{cl}(\mathfrak{P}_1), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ generate $C_{F,w}^{(\tau)} \Leftrightarrow -1$ is the norm of a unit of F. However, with the choice of $p_1, \cdots, p_n$ in the statement of Theorem 2, the matrix of

$$\phi: S/S^l \to C_{F,w}^{(\tau)} \to \mathrm{Gal}(K/F), \qquad \mathfrak{P} \bmod S^l \mapsto \mathrm{cl}(\mathfrak{P}) \mapsto (\mathfrak{P}, K/F)$$

has rank $n-1$, which implies that the map $S/S^l \to C_{F,w}^{(\tau)}$ must be surjective because $C_{F,w}^{(\tau)}$ is an elementary abelian 2-group of rank $n-1$. Hence

$\mathrm{cl}(\mathfrak{P}_1), \cdots, \mathrm{cl}(\mathfrak{P}_n)$ generate $C^{(r)}_{F,w}$, 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

1. Z. I. Borevič and I. Šafarevič, *Number theory*, "Nauka", Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR 30 #1080; 33 #4001.

2. A. Fröhlich, *On non-ramified extensions with prescribed Galois group*, Mathematika 9 (1962), 133–134. MR 26 #3701.

3. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*. Ia, Jber. Deutsch. Math.-Verein. 36 (1927), 233–311.

4. ———, *Eine Folgerung aus H.-W. Leopoldts Theorie der Geschlechter abelscher Zahlkörper*, Math. Nachr. 42 (1969), 261–262. MR 41 #5330.

5. C. S. Herz, *Construction of class fields*, Seminar on complex multiplication, Lecture Notes in Math., no. 21, Springer-Verlag, Berlin and New York, 1966. MR 34 #1278.

6. S. Iyanaga, *Sur les classes d'idéaux dans les corps quadratiques*, Exposés Mathématiques VIII, Actualités Sci. Indust., no. 197, Hermann, Paris, 1935.

7. L. Rédei, *Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie*, Acta. Math. Acad. Sci. Hungar. 4 (1953), 1–29. MR 16, 450.

8. ———, *Die 2-Ringklassengruppe des quadratishen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta. Math. Acad. Sci. Hungar. 4 (1953), 31–87. MR 16, 450.

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

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