MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 132
OCTOBER 1975, PAGES 1135–1137

A Note on l-Class Groups of Number Fields*

By Frank Gerth III

Abstract. Let F be a number field and K a cyclic extension of degree l over F, where l is a rational prime. The l-class group of K is analyzed as a Gal(K/F)-module in the case where the l-class group of F is trivial. The resulting structure theorem is used to compute the structure of the 3-class groups of certain cyclic cubic fields that are discussed in a paper of D. Shanks.

1. Structure of l-Class Groups. Let F be a finite extension field of the rational numbers $\mathbf{Q}$, and let K be a cyclic extension of F of degree l, where l is a rational prime. Let $G = \mathrm{Gal}(K/F)$, and let τ be a generator of the cyclic group G. Let A denote the l-class group of K (i.e., the Sylow l-subgroup of the ideal class group of K). Then A is a finite abelian l-group. For convenience of notation, we shall write the operation in A as addition. Now A is a module over the ring of l-adic integers $\mathbf{Z}_l$ and also a module over G. So A is a $\mathbf{Z}_l[G]$ module. Assume that the l-class group B of F is trivial. Then for each $x \in A$, $(1 + \tau + \ldots + \tau^{l-1})x = 0$ since $(1 + \tau + \ldots + \tau^{l-1})x \in B$. Hence A is a module over $\mathbf{Z}_l[G]/(1 + \tau + \ldots + \tau^{l-1})\mathbf{Z}_l[G]$. But $\mathbf{Z}_l[G]/(1 + \tau + \ldots + \tau^{l-1})\mathbf{Z}_l[G] \cong \mathbf{Z}_l[\zeta]$, where ζ is a primitive lth root of unity (the isomorphism is induced by $\tau \mapsto \zeta$). Let Λ denote $\mathbf{Z}_l[\zeta]$. Then A is a finitely generated torsion module over the principal ideal domain Λ. The nontrivial ideals of Λ are $(1 - \zeta)\Lambda, (1 - \zeta)^2\Lambda, (1 - \zeta)^3\Lambda, \ldots$. Hence by applying the well-known structure theorem for finitely generated modules over a principal ideal domain, we obtain the following theorem.

THEOREM 1. $A \cong \Lambda/(1 - \zeta)^{i_1}\Lambda \oplus \Lambda/(1 - \zeta)^{i_2}\Lambda \oplus \ldots \oplus \Lambda/(1 - \zeta)^{i_n}\Lambda$, *where* $i_1, i_2, \ldots, i_n$ *are positive integers,* $n = \dim_{\mathbf{F}_l}(A/(1 - \zeta)A)$, *and* $\mathbf{F}_l$ *is the finite field of* l *elements.*

Remark. Let $A^G = \{x \in A \mid \tau x = x\}$. The exact sequence

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{1 - \tau} A \longrightarrow A/(1 - \tau)A \longrightarrow 0$$

shows that $\dim_{\mathbf{F}_l}(A/(1 - \tau)A) = \dim_{\mathbf{F}_l} A^G$. Since $A/(1 - \tau)A \cong A/(1 - \zeta)A$, then the integer n in Theorem 1 satisfies $n = \dim_{\mathbf{F}_l} A^G$.

Next we want to show how to obtain the invariants of A as an abelian group from the invariants $(1 - \zeta)^i\Lambda$ of A as a Λ module. Now in Λ, $(1 - \zeta)^{l-1}\Lambda = l\Lambda$. We write $i = (l - 1)r + s$, where r and s are nonnegative integers with $0 \leqslant s < l - 1$. Then $(1 - \zeta)^i\Lambda = (1 - \zeta)^s l^r \Lambda$. Since Λ is a free module of rank $l - 1$ over $\mathbf{Z}_l$, then

$$\Lambda/(1 - \zeta)^i\Lambda \cong (\mathbf{Z}_l/l^{r+1}\mathbf{Z}_l)^s \oplus (\mathbf{Z}_l/l^r\mathbf{Z}_l)^{l-1-s}$$

Received November 21, 1974.
AMS (MOS) subject classifications (1970). Primary 12A30, 12A35; Secondary 13C05.
*This research was supported by NSF Grant GP 28488A3.

Copyright © 1975, American Mathematical Society

as $\mathbf{Z}_l$ modules. If we let $\mathbf{Z}$ denote the ring of rational integers, then as abelian groups

$$\mathbf{Z}_l/l^{r+1}\mathbf{Z}_l \cong \mathbf{Z}/l^{r+1}\mathbf{Z} \quad \text{and} \quad \mathbf{Z}_l/l^r\mathbf{Z}_l \cong \mathbf{Z}/l^r\mathbf{Z}.$$

Hence as an abelian group, $\Lambda/(1-\zeta)^i\Lambda$ is isomorphic to the direct sum of s cyclic groups of order l^{r+1} and $l-1-s$ cyclic groups of order l^r. We summarize our results in the following theorem.

THEOREM 2. *Suppose A is decomposed as a direct sum of cyclic Λ modules as in Theorem* 1. *Let r_j and s_j be nonnegative integers such that $i_j = (l-1)r_j + s_j$ with $0 \leqslant s_j < l-1$. Then as abelian groups,*

$$A \cong \bigoplus_{j=1}^{n} [(\mathbf{Z}/l^{r_j+1}\mathbf{Z})^{s_j} \oplus (\mathbf{Z}/l^{r_j}\mathbf{Z})^{l-1-s_j}].$$

Remark. Results equivalent to Theorem 2 have been obtained by Gras [1], Inaba [3] and Zink [5].

In Theorem 2 let v denote the number of j's such that $r_j \neq 0$, and let $w = \Sigma' s_j$, where the sum is taken over all j's such that $r_j = 0$. Then if we view A as an abelian l-group, we obtain the following results from Theorem 2.

COROLLARY 1. Rank $A = (l-1)v + w$. *Moreover, A is the direct sum of an elementary abelian l-group of rank w and an abelian l-group of rank $(l-1)v$.*

COROLLARY 2. *If* rank $A < l-1$, *then A is an elementary abelian l-group.*

Remark. The results of this section can be generalized in various ways, and we shall present such results in other papers.

2. Applications to a Paper of D. Shanks. In [4] Shanks investigates the ideal class groups of certain cubic fields. In particular, [4, Section 7] discusses certain cyclic cubic fields whose discriminants D satisfy two conditions: (1) $D = N^2$, where $N = a^2 + 3a + 9$ for some $a \in \mathbf{Z}$, and (2) N is divisible by exactly two rational primes. Table 4 of [4] lists examples of some cyclic cubic fields of this type whose 3-class groups have rank 2. Shanks was able to determine the structure of the ideal class groups of all but five of the fields in Table 4 of [4]. For these five examples, he lists the class numbers. By using the results from Section 1 with $l = 3$, we shall determine the structures of the ideal class groups for four of these five examples. (In the other example, the problem is to determine the 2-class group.)

We let K represent a cyclic cubic field whose discriminant is divisible by t rational primes. Next we let A denote the 3-class group of K. If $G = \mathrm{Gal}(K/\mathbf{Q})$, then A^G is an elementary abelian 3-group of rank $t-1$ (cf. [1] or [2]). According to Theorem 1 and the remark following it, A is a direct sum of $t-1$ cyclic $\mathbf{Z}_3[\zeta]$ modules, where ζ is a primitive cube root of unity. We now specialize to the case $t = 2$ of [4, Section 7]. Then A is a cyclic $\mathbf{Z}_3[\zeta]$ module. If A has order 3^m, then Theorem 2 implies

$$A \cong (\mathbf{Z}/3^{m/2}\mathbf{Z})^2 \qquad \text{if } m \text{ is even,}$$

$$\cong (\mathbf{Z}/3^{(m+1)/2}\mathbf{Z}) \oplus (\mathbf{Z}/3^{(m-1)/2}\mathbf{Z}) \qquad \text{if } m \text{ is odd.}$$

This fact, together with the class numbers in Table 4 of [4] and the Theorem in [4, Section 4], gives the structure of the ideal class groups for the four examples. We list the results using the notation of [4].

a	N	$Q(\rho)$
338	$73 \cdot 1579$	9×27
341	$7 \cdot 16759$	18×18
351	$9 \cdot 13807$	9×63
382	$19 \cdot 7741$	18×18

The entries under $Q(\rho)$ indicate the orders of the cyclic factors of the ideal class group.

Shanks raises another question in [4, Section 7] with the example $N = 9 \cdot 73$ and $a = 24$. The 3-class group A of this cyclic cubic field with discriminant $(9 \cdot 73)^2$ is the direct sum of two cyclic groups of order 3. So A has four subgroups of order 3. From a group-theoretic point of view, one would expect no significant differences among these subgroups. However, Shanks shows that the prime ideals of this number field are distributed in one of these subgroups in a manner different from the way they are distributed in the other three subgroups. So there is one exceptional subgroup. The existence of this exceptional subgroup can be anticipated if we consider A as a module over $\mathbf{Z}_3[\zeta]$. Then A is a cyclic $\mathbf{Z}_3[\zeta]$ module, and there is a unique subgroup of A of order 3 which is also a $\mathbf{Z}_3[\zeta]$ module. It is this subgroup of order 3 which is the exceptional subgroup. In fact, the manner in which the prime ideals are distributed in A reflects the action of $\mathbf{Z}_3[\zeta]$ on A (more precisely, it reflects the action on A of a generator τ of G, and then $\mathbf{Z}_3[\zeta]$ acts on A by means of the isomorphism $\mathbf{Z}_3[G]/(1 + \tau + \tau^2)\mathbf{Z}_3[G] \cong \mathbf{Z}_3[\zeta]$ induced by $\tau \mapsto \zeta$).

Remark. For additional results on cyclic extensions of degree l whose discriminants are divisible by exactly two distinct primes, see the thesis of W. Zink [5].

Department of Mathematics
The University of Texas
Austin, Texas 78712

1. G. GRAS, *Sur les l-Classes d'Idéaux dans les Extensions Cycliques Relative de Degré Premier l*, Thesis, Grenoble, 1972.

2. C. S. HERZ, *Construction of Class Fields*, Seminar on Complex Multiplication, Lecture Notes in Math., vol. 21, Springer-Verlag, Berlin and New York, 1966.

3. E. INABA, "Über die Struktur der l-Klassengruppe zyklischer Zahlkörper von Primzahlgrad l," *J. Fac. Sci. Imp. Univ. Tokyo Sect.* I, v. 4, 1940, pp. 61–115. MR 2, 147.

4. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.

5. W. ZINK, Thesis, Akademie der Wissenschaften der DDR, Berlin.