PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 78, Number 3, March 1980

THE IDEAL CLASS GROUPS OF TWO CYCLOTOMIC FIELDS

FRANK GERTH III

ABSTRACT. It is known that there are exactly two cyclotomic fields with class numbers equal to 8, namely the fields of 29th and 68th roots of unity. We show by elementary methods how to determine the structure of the ideal class groups of these fields.

In [2] Masley indicates that there are exactly two cyclotomic fields that have class numbers equal to 8. These fields are $\mathbf{Q}(\zeta_{29})$ and $\mathbf{Q}(\zeta_{68})$, where $\mathbf{Q}$ denotes the field of rational numbers, and ζ_{29} (resp., ζ_{68}) is a primitive 29th (resp., 68th) root of unity. Masley remarks that it is known that the ideal class group of $\mathbf{Q}(\zeta_{29})$ has exponent 2 but that the structure of the ideal class group of $\mathbf{Q}(\zeta_{68})$ is unknown. In this paper we show by elementary methods how to determine the structure of the ideal class groups of $\mathbf{Q}(\zeta_{29})$ and $\mathbf{Q}(\zeta_{68})$, given that their class numbers are equal to 8.

We let K be a finite extension of $\mathbf{Q}$, and we let L be an extension of K of degree 2. We let σ be the generator of $\mathrm{Gal}(L/K)$. We let C_K (resp., C_L) denote the ideal class group of K (resp., L) and h_K (resp., h_L) the class number of K (resp., L). We shall suppose that $h_K = 1$.

LEMMA 1. *If $a \in C_L$, then $a^{1+\sigma} = 1$.*

PROOF. Let N: $C_L \to C_K$ be the map induced by the norm map from ideals of L to ideals of K, and let i: $C_K \to C_L$ be the map induced by the inclusion map from ideals of K to ideals of L. Then $a^{1+\sigma} = i(Na) = 1$ since $Na \in C_K$ and $h_K = 1$.

Next we let $B_L = \{a \in C_L | a^2 = 1\}$ and $A_L = \{a \in C_L | a^\sigma = a\}$. If $a \in A_L$, then $a^2 = a^{1+\sigma} = 1$ by Lemma 1, and hence $A_L \subseteq B_L$. On the other hand, if $a \in B_L$, then $a^2 = 1$ implies $a = a^{-1}$. From Lemma 1, $a^\sigma = a^{-1}$. So $a^\sigma = a$, and hence $a \in A_L$. So we have proved the following lemma.

LEMMA 2. *$B_L = A_L$.*

LEMMA 3. *$|A_L| = 2^{d-1-(r+1-q)}$ where $|A_L|$ denotes the order of A_L, d is the number of ramified primes in L/K, q satisfies $2^q = |(E_K \cap N_{L/K}L^*)/E_K^2|$ with E_K the group of units of K and $N_{L/K}$ the norm map from L to K, and r is the rank of the free abelian part of E_K.*

PROOF. This result is a classical result proved in [1, Theorem 13].

REMARK. $r + 1 - q \geqslant 0$ in Lemma 3.

Received by the editors February 15, 1979 and, in revised form, April 24, 1979.
AMS (MOS) subject classifications (1970). Primary 12A35, 12A50.

Now we consider $K = \mathbf{Q}(\zeta_{17})$ and $L = \mathbf{Q}(\zeta_{68}) = K(\sqrt{-1})$. It is well known that $h_K = 1$. We shall apply Lemma 3 to $L = \mathbf{Q}(\zeta_{68})$. It is easy to see that the only primes of K which ramify in L are the primes of K that are above the rational prime 2. A simple calculation shows that the order of 2 modulo 17 is 8. Hence 2 decomposes in $\mathbf{Q}(\sqrt{17})$, but the primes above 2 in $\mathbf{Q}(\sqrt{17})$ remain inert in $\mathbf{Q}(\zeta_{17})$. So there are exactly 2 primes of K which ramify in L. So $d = 2$ in Lemma 3, and we see that $|A_L| \leqslant 2$. Since $h_L = 8$ by [2], then $|B_L| > 1$. So $|B_L| = |A_L| = 2$, and hence C_L is a cyclic group of order 8. So we have proved the second part of the following theorem.

THEOREM 1. *The ideal class group of* $\mathbf{Q}(\zeta_{29})$ *is an elementary abelian* 2-*group of order* 8, *and the ideal class group of* $\mathbf{Q}(\zeta_{68})$ *is a cyclic group of order* 8.

REMARK. Although the first part of Theorem 1 was already known, we briefly indicate how to prove that result. We let $K = \mathbf{Q}(\sqrt{29})$, and we let L be the subfield of $\mathbf{Q}(\zeta_{29})$ of degree 2 over K. In applying Lemma 3, calculations show that $d = 3$ (the prime above 29 and the two real archimedean primes of K ramify in L/K), $r = 1$, and $q = 0$. So $|A_L| = 1$, and hence $|B_L| = 1$. Next we let $M = \mathbf{Q}(\zeta_{29})$, and we let C_M denote the ideal class group of M. We define $B_M = \{a \in C_M | a^2 = 1\}$, and $A_M = \{a \in B_M | a^\tau = a\}$. Here τ is a generator of $\mathrm{Gal}(M/L)$, which is a cyclic group of order 7. Now we note that $|A_M| = 1$. (If $a \in A_M$, then $a = a^7 = a^{1+\tau+\tau^2+\cdots+\tau^6} = 1$.) But $|B_M| \neq 1$ since $|C_M| = 8$. Hence τ is a automorphism of B_M of degree 7, which forces $|B_M| = |C_M| = 8$.

REMARK. For certain facts about cyclotomic fields that are used in this paper, see [3].

REFERENCES

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

2. J. Masley, *Solution of small class number problems for cyclotomic fields*, Compositio Math. **33** (1976), 179–186.

3. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TEXAS, AUSTIN, TEXAS 78712