93. On the Ideal Class Groups of Some Cyclotomic Fields

By Koichi TATEYAMA
Department of Mathematics, University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 13, 1982)

1. **Introduction.** Let K_m be the cyclotomic field of m-th roots of unity, and K_m^+ its maximal real subfield. Let $C(m)$, $C^+(m)$ denote the ideal class groups of K_m, K_m^+ respectively. Let j denote the automorphism of K_m, mapping each element in K_m to its complex-conjugate. Let $C^-(m)$ denote the kernel of the norm map $1+j: C(m) \to C^+(m)$.

In a paper of 1853, Kummer proved that $C^-(p)$ is cyclic for every prime $p<100$ and $p \neq 29, 41$. Furthermore, $C^-(29)$ and $C^-(41)$ are abelian groups of type $(2,2,2)$ and $(11,11)$ respectively (see [2], [5]).

Recently, Gerth [1] determined the structure of $C(68)$ by using the ambiguous class group of $C(68)$. Now we determine the structure of $C(m)$ when the order of $C(m)$ is smaller than 10^4, as well as the structure of $C^-(p)$ when p is a prime number smaller than 227 except for seven cases. Our results are shown in Tables I and II. They are obtained using the computational results due to Masley and Schrutka ([6]–[9]).

Notations. h_m and h_m^- denote the orders of $C(m)$ and $C^-(m)$ respectively. For any algebraic number field L, we denote by C_L the ideal class group of L, and h_L the order of C_L (i.e. the class number of L). When L is an imaginary abelian number field, C_L^-, h_L^- are defined as obvious generalization of $C^-(m)$, h_m^-.

2. **The structure of $C(m)$.**

Table I ($h_m<10^4$)

m	h_m	type	
29	2^3	$(2,2,2)$	(Kummer)
31	3^2	(3^2)	(Kummer)
41	11^2	$(11,11)$	(Kummer)
57	3^2	(3^2)	
65	2^6	(?)	
68	2^3	(2^3)	(Gerth)
77	$2^8\cdot 5$	(?)	
87	$2^9\cdot 3$	(?)	
93	$3^2\cdot 5\cdot 151$	$(3^2, 5, 151)$	
96	3^2	$(3,3)$	

99	$3\cdot 31^2$	$(3, 31, 31)$
104	$3^3\cdot 13$	$(3, 3, 3, 13)$
112	$2^2\cdot 3^2\cdot 13$	$(2^2, 3, 3, 13)$
120	2^2	(2^2)
144	$3\cdot 13^2$	$(3, 13, 13)$
156	$2^2\cdot 3\cdot 13$	$(?)$
168	$2^2\cdot 3\cdot 7$	$(2^2, 3, 7)$
180	$3\cdot 5^2$	$(3, 5, 5)$
240	$2^8\cdot 5^2$	$(?, 5, 5)$

The proof depends on the following lemmas.

Lemma 1. *Let k be an algebraic number field and K be an extension of k of degree 2. Let $a(K/k)$ denote the order of the ambiguous class group of K over k. If h_k is odd, then $a(K/k)=2^r\cdot n$, $(n,2)=1$, where we denote by r the rank of the 2-Sylow subgroup of C_K* (see [1]).

Lemma 2. *Suppose that K/k is a cyclic extension of degree n. Let p be a prime such that $p\nmid nh_L$, for any field L with $k\subset L\subsetneqq K$. Then the p-rank of C_K is a multiple of the order of p modulo n* (Masley [7]).

Lemma 3. *Let p be an odd prime, and K/k an abelian extension of type $(2,2)$. Let K_i and S_i $(i=1,2,3)$ denote the intermediate fields of K/k and the p-Sylow subgroup of C_{K_i} respectively. If $S_3=1$, then the p-Sylow subgroup of C_K is isomorphic to $S_1\times S_2$.*

Lemma 4. *Let p be a prime number and K/k be a cyclic extension of degree p, and S_K the p-Sylow subgroup of C_K. We set $S_k=N_{K/k}S_K$ and suppose that the canonical homomorphism $S_k\to S_K$ is injective. If $(S_K:S_k)=p^a$ and $a<p-1$, then $S_k=S_K^p$.*

Remark. The injectivity of $S_k\to S_K$ is well-known in our cases (see [4]).

3. The structure of $C^-(p)$.

Table II $(71\leqq p\leqq 211)$

p	square factors of h_p^-	type	
71	7^2	(7^2)	(Kummer)
101	5^5	$(5^2, 5^3)$	
113	2^3	$(2, 2, 2)$	
131	$3^3\cdot 5^2$	$(3, 3, 3, 5^2)$	
137	17^2	(17^2)	
139	$3^2\cdot 47^2\cdot 277^2$	$(3^2, ?, 277, 277)$	
149	3^2	$(3, 3)$	
151	11^2	$(11, 11)$	
157	$13^2\cdot 157^2$	$(13^2, 157, 157)$	(Iwasawa-Sims)
163	2^2	$(2, 2)$	

197	2^3	$(2,2,2)$
199	3^4	(3^4)
211	$3^2\cdot 7^2\cdot 281^2$	$(3^2, 7^2, 281, 281)$

To determine the structure of $C^-(p)$, we must modify Lemmas 2 and 4 into Lemmas 5 and 6.

Lemma 5. *Suppose that K/k is a cyclic extension of degree n, and that k, K are both imaginary abelian fields. Let p be an odd prime such that $p\nmid nh_L^-$ for any field with $k\subset L\subsetneqq K$. Then the p-rank of C_K^- is a multiple of the order of p modulo n.*

Lemma 6. *Let p be a prime number, K/k be a cyclic extension of degree p, and k, K be imaginary abelian. We denote by S_K the p-Sylow subgroup of C_K^-, and $S_k=N_{K/k}S_K$. We assume that the canonical homomorphism $S_k\to S_K$ is injective. If $(S_K:S_k)=p^a$ and $a<p-1$, then $S_k=S_K^p$.*

The following lemma is trivial, but useful.

Lemma 7. *Let K be an extension field over k, and p be a prime number such that $p\nmid[K:k]$. We denote by S_K the p-Sylow subgroup of C_K, and $S_k=N_{K/k}S_K$. Then S_k is a direct summand of S_K.*

References

[1] F. Gerth: The ideal class groups of two cyclotomic fields. Proc. Amer. Math. Soc., **78**(3), 321–322 (1980).

[2] K. Iwasawa: A note on ideal class groups. Nagoya Math. J., **27-1**, 239–247 (1966).

[3] K. Iwasawa and C. C. Sims: Computation of invariants in the theory of cyclotomic fields. J. Math. Soc. Japan, **18**(1), 86–96 (1966).

[4] Y. Kida: *L*-extension of *CM*-fields and cyclotomic invariants. J. Number Theory, **12**(4), 519–528 (1980).

[5] E. Kummer: Über die Irregularitat der Determinaten. Monatsber. Akad. d. Wissensch., Berlin, pp. 194–200 (1853).

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

[7] ——: Class numbers of real cyclic number fields with small conductors. ibid., **37**(3), 297–319 (1978).

[8] ——: Cyclotomic fields with class number less than one million (preprint).

[9] G. Schrutka v. Rechtenstamm: Tabelle der (relative-) Klassenzahlen von Kreiskörpern. Abh. Deutsche Akad. Wiss. Berlin, Math. Nat., nr. 2 (1964).