PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 9, September 1995

ON THE 2-CLASS GROUPS OF CYCLOTOMIC FIELDS WHOSE MAXIMAL REAL SUBFIELDS HAVE ODD CLASS NUMBERS

KUNIAKI HORIE AND MITSUKO HORIE

(Communicated by William Adams)

ABSTRACT. This paper first makes a simple remark about the structure as a group of the ideal class group of any algebraic number field, then studies the 2-rank of the ideal class group of any cyclotomic field whose maximal real subfield has odd class number, and finally determines the structure of the ideal class groups of some cyclotomic fields.

In this paper, we first state a result concerning the ideal class groups of algebraic number fields, which follows immediately from the study of the natural action of Galois groups on ideal class groups (cf. Theorem 2.14 of [7] and Theorem 10.8 of [12]). Next we study the 2-ranks of the ideal class groups of cyclotomic fields whose maximal real subfields have odd class numbers, by using one of the index formulae in [10] that was obtained naturally from the analytic class number formula. In the last section of the paper, the structure of the ideal class groups, as abelian groups, of some cyclotomic fields will be determined by means of well-known results on class numbers and the results of the preceding sections, but there we shall not deal in principle with any ideal class group whose structure is already determined (cf. [11]).

1

Let $\mathbb{Q}$ denote the rational field, $\mathbb{Z}$ the additive group of (rational) integers, and $\mathbb{N}$ the set of positive integers. The Euler function will be denoted by φ as usual.

Let K be any finite extension over $\mathbb{Q}$ contained in the complex field, and let p be any prime number. Let A denote the p-class group of K, i.e., the Sylow p-subgroup of the ideal class group of K, and let X denote the set of subfields k of K such that K is a cyclic extension over k, p does not divide $[K : k]$, and p does not divide the class number of any intermediate field of K/k other than K. Noting that K belongs to X, let f denote the least common multiple of the orders of p modulo $[K : k]$ for all $k \in X$. We understand that $f = 1$

Received by the editors January 20, 1994.
1991 *Mathematics Subject Classification.* Primary 11R18, 11R29; Secondary 11R27.
Supported in part by Grant-in-Aid for Scientific Research (No. 06640080), Ministry of Education, Science and Culture, Japan.

if $X = \{K\}$. Let t be the non-negative integer such that $|A| = p^t$. For each finite abelian group M, let $r(M)$ denote the rank of M. We then have

Theorem 1. *The positive integer f divides t, and*

$$\begin{aligned} A &\cong (\mathbb{Z}/p^{t/f}\mathbb{Z})^f && \text{in case } r(A) = f \\ &\cong (\mathbb{Z}/p^2\mathbb{Z})^f \oplus (\mathbb{Z}/p\mathbb{Z})^{t-2f} && \text{in case } r(A) = t - f. \end{aligned}$$

Proof. Let n be any non-negative integer. Let A_n denote the factor group of A modulo the group of the p^n-th powers of all ideal classes in A. Then Theorem 2.14 of [7] implies that $r(A_n)$ is divisible by the order of p modulo $[K : k]$ for every $k \in X$. Thus

$$f \mid r(A_n).$$

We therefore see that A is isomorphic to a direct sum of f copies of a finite abelian p-group. From this, the theorem follows immediately. It is also clear that $t \geq 2f$ if $r(A) = t - f$.

Remark. Even though f is replaced by any positive divisor f' of f, Theorem 1 still holds and the condition that $r(A) = f'$ or $t - f'$ implies $f' = f$. Of course, $A \cong (\mathbb{Z}/p\mathbb{Z})^t$ if $r(A) = t$.

2

With the notation of the preceding section retained, we shall assume throughout the following that $p = 2$ and that K is a cyclotomic field different from $\mathbb{Q}$. Let $\zeta_n = e^{2\pi i/n}$ for each $n \in \mathbb{N}$, and let m denote the conductor of K;

$$K = \mathbb{Q}(\zeta_m), \qquad m \not\equiv 2 \pmod 4, \qquad m > 1.$$

Let g be the number of distinct prime divisors of m. For each $n \in \mathbb{N}$ and each $q \in \mathbb{Q}$, let $R_n(q)$ denote the set of positive integers prime to n and less than q:

$$R_n(q) = \{a \in \mathbb{N} \mid (a, n) = 1,\ a < q\}.$$

Note that

$$|R_n(n)| = \varphi(n) \qquad \text{for} \quad n \in \mathbb{N},\quad n > 1.$$

We put

$$\begin{aligned} S &= \{n \in \mathbb{N} \mid n \mid m,\ (n, \tfrac{m}{n}) = 1,\ n > 1\}, \\ S_0 &= \{n \in S \mid 2 \mid n\}, \quad S_1 = \{n \in S \mid 2 \nmid n\}, \\ T &= \{n \in S \mid n \text{ is not a prime-power}\}. \end{aligned}$$

Let $\mathbb{F}_2$ denote as usual the field with 2 elements such that the additive group of $\mathbb{F}_2$ is $\mathbb{Z}/2\mathbb{Z}$. Let, for each $z \in \mathbb{Z}$,

$$z + 2\mathbb{Z} = \{z + 2y \mid y \in \mathbb{Z}\},$$

and let V be the vector space over $\mathbb{F}_2$ consisting of all row vectors of size $\frac{\varphi(m)}{2}$ with components in $\mathbb{F}_2$. For each $n \in S$ and each $a \in R_n(\frac{n}{2})$, we let $v_{n,a}$, v_n, $w_{n,a}$ denote respectively the vectors in V whose $|R_b(m)|$-th components, for each $b \in R_m(\frac{m}{2})$, are equal to

$$\left[\frac{ab}{n}\right] - \left[\frac{b}{n}\right] + 2\mathbb{Z}, \quad \left[\frac{b}{n}\right] + 2\mathbb{Z}, \quad \left[\frac{2ab}{n}\right] + 2\mathbb{Z}.$$

Here, for each $q \in \mathbb{Q}$, $[q]$ denotes the maximal integer not exceeding q. Let u denote the vector in V whose components all equal $1+2\mathbb{Z}$. We next define a subset B of V as follows: when $g=1$ or $2 \nmid m$, we put

$$B = \{u\} \cup \left(\bigcup_{n \in S} \{v_{n,a} \mid a \in R_n(\tfrac{n}{2})\} \right) \cup \{v_n \mid n \in T,\ n \neq m\};$$

when $g \geq 2$ and $2 \mid m$, we put

$$B = \{u\} \cup \left(\bigcup_{n \in S_0 \cup (S \setminus T)} \{v_{n,a} \mid a \in R_n(\tfrac{n}{2})\} \right) \cup \{v_n \mid n \in S_0 \cap T,\ n \neq m\}$$
$$\cup \left(\bigcup_{n \in S_1 \cap T} \{w_{n,a} \mid a \in R_n(\tfrac{n}{2})\} \right).$$

Now, we define d to be the dimension of the subspace of the vector space V spanned by B over $\mathbb{F}_2$. Let K^+ denote the maximal real subfield of K: $K^+ = \mathbb{Q}(\cos \frac{2\pi}{m})$. We write h for the class number of K and h^+ for that of K^+.

Theorem 2. *Assume that h^+ is odd. Then the following assertions hold:*

(i) $g \leq 4$,

(ii) $r(A) = \dfrac{\varphi(m)}{2} - d$ *if* $g = 1$,

(iii) $r(A) = \dfrac{\varphi(m)}{2} - d - 1$ *if* $g = 2$ *or* 3,

(iv) $r(A) = \dfrac{\varphi(m)}{2} - d - 2$ *or* $\dfrac{\varphi(m)}{2} - d - 1$ *if* $g = 4$.

Proof. The assertion (i) is nothing but Theorem A of [1]. We shall prove (ii), (iii), and (iv). Let E be the unit group of K, E^+ the unit group of K^+, E^* the group of all totally positive elements of E^+, and E' the group of all elements of E^+ contained in the image of the norm map $K \longrightarrow K^+$;

$$E \supseteq E^+ \supseteq E^* \supseteq E', \qquad [E : E'] < \infty, \qquad \{\varepsilon^2 \mid \varepsilon \in E^+\} \subseteq E'.$$

Note that just one or no prime ideal of K^+ is ramified in K according as $g = 1$ or $g \geq 2$. Since h^+ is odd by the assumption, the group of ambiguous ideal classes for K/K^+ in A coincides with $\{c \in A \mid c^2 = 1\}$. Therefore, by the well-known formula for the number of ambiguous ideal classes,

$$r(A) = \frac{\varphi(m)}{2} - r(E^+/E') \qquad \text{if} \quad g = 1,$$
$$= \frac{\varphi(m)}{2} - r(E^+/E') - 1 \qquad \text{if} \quad g \geq 2.$$

We further obtain $E' = E^*$ from Hasse's norm theorem and product formula, because at most one prime ideal of K^+ is ramified in K. Thus

$$(1) \qquad r(A) = \frac{\varphi(m)}{2} - r(E^+/E^*) \ \text{ or } \ \frac{\varphi(m)}{2} - r(E^+/E^*) - 1$$

according as $g = 1$ or $g \geq 2$.

Let C and C^+ denote respectively the groups of circular units of K and K^+ in the sense of Sinnott [10], namely, let

$$C = P \cap E, \qquad C^+ = C \cap E^+,$$

where P is the subgroup of the multiplicative group of K generated by $1-\zeta_m^a$ for all $a \in \mathbb{Z}$ with $m \nmid a$. Let W be the group of roots of unity in K so that W is a cyclic group generated by $-\zeta_m$. Note that $W \subseteq C$, and put $W^2 = \{\xi^2 \mid \xi \in W\}$. Let x denote the homomorphism $C \longrightarrow W$ such that $x(\varepsilon) = \varepsilon/\bar{\varepsilon}$ for every $\varepsilon \in C$, $\bar{\varepsilon}$ being the complex conjugate of ε. Then $x^{-1}(W^2) = C^+W$, whence x induces an injective homomorphism $C/C^+W \longrightarrow W/W^2$. Therefore, $[C : C^+W]$ does not exceed 2 and we see from $x(W) = W^2$ that $[C : C^+W] = 2$ if and only if $-\zeta_m = x(\eta)$ for some $\eta \in C$. Now, in the case $g \geq 2$, we have $1-\zeta_m \in C$, $-\zeta_m = x(1-\zeta_m)$, and thus $[C : C^+W] = 2$. If we assume in the case $g = 1$ that $-\zeta_m = x(\eta)$ for some $\eta \in C$, then it follows that $\eta^{-1}(1-\zeta_m)$ lies in K^+ although $\eta^{-1}(1-\zeta_m)$ generates a prime ideal of K fully ramified for $K/\mathbb{Q}$; which is obviously impossible. Consequently,

$$[C : C^+W] = 1 \text{ or } 2 \tag{2}$$

according as $g = 1$ or $g \geq 2$ (for this paragraph, see sections 1 and 4 of [10]).

Given any prime number l and any a, $n \in \mathbb{N}$, one has

$$1-\zeta_{ln}^a = \prod_{j=1}^{l}(1-\zeta_{l^2n}^{a+jln}).$$

It is easy to see from this that the subset of E

$$\{-\zeta_m\} \cup \left(\bigcup_{n \in S \setminus T} \left\{ \frac{1-\zeta_n^a}{1-\zeta_n} \;\middle|\; a \in R_n(\tfrac{n}{2}) \right\} \right) \cup \left(\bigcup_{n \in T} \{1-\zeta_n^a \mid a \in R_n(\tfrac{n}{2})\} \right)$$

generates C as a group. Therefore, if $g \geq 2$ and $2 \nmid m$, then C is generated by

$$\{-\zeta_m\} \cup \left(\bigcup_{n \in S} \left\{ \frac{\zeta_{2n}^a - \zeta_{2n}^{-a}}{\zeta_{2n} - \zeta_{2n}^{-1}} \;\middle|\; a \in R_n(\tfrac{n}{2}) \right\} \right) \cup \{1-\zeta_n \mid n \in T\},$$

whence (almost similarly as discussed in [3] for the case $m = 65$) we know from (2) that C^+ is generated by

$$\{-1,\ |1-\zeta_m|^2\} \cup \left(\bigcup_{n \in S} \left\{ \frac{\sin\frac{\pi a}{n}}{\sin\frac{\pi}{n}} \;\middle|\; a \in R_n(\tfrac{n}{2}) \right\} \right) \cup \left\{ \frac{\sin\frac{\pi}{n}}{\sin\frac{\pi}{m}} \;\middle|\; n \in T,\ n \neq m \right\}.$$

In the case $g = 1$, it is clear from (2) that

$$\{-1\} \cup \left\{ \frac{\sin\frac{\pi a}{m}}{\sin\frac{\pi}{m}} \;\middle|\; a \in R_m(\tfrac{m}{2}) \right\}$$

generates C^+. If $g \geq 2$ and $2 \mid m$, then C is generated by

$$\{-\zeta_m\} \cup \left(\bigcup_{n \in S_0 \cup (S \setminus T)} \left\{ \frac{\zeta_{2n}^a - \zeta_{2n}^{-a}}{\zeta_{2n} - \zeta_{2n}^{-1}} \;\middle|\; a \in R_n(\tfrac{n}{2}) \right\} \right)$$

$$\cup \{1-\zeta_n \mid n \in S_0 \cap T\} \cup \left(\bigcup_{n \in S_1 \cap T} \{\zeta_4(\zeta_n^a - \zeta_n^{-a}) \mid a \in R_n(\tfrac{n}{2})\} \right)$$

so that C^+ is generated by

$$\{-1, |1-\zeta_m|^2\} \cup \left(\bigcup_{n \in S_0 \cup (S \setminus T)} \left\{ \frac{\sin \frac{\pi a}{n}}{\sin \frac{\pi}{n}} \;\middle|\; a \in R_n(\tfrac{n}{2}) \right\} \right)$$

$$\cup \left\{ \frac{\sin \frac{\pi}{n}}{\sin \frac{\pi}{m}} \;\middle|\; n \in S_0 \cap T,\ n \neq m \right\} \cup \left(\bigcup_{n \in S_1 \cap T} \{ 2 \sin \tfrac{2\pi a}{n} \mid a \in R_n(\tfrac{n}{2}) \} \right).$$

The definition of B therefore implies

$$d = r(C^+/C^*), \tag{3}$$

where C^* denotes the group of totally positive elements of C^+: $C^* = C^+ \cap E^*$. On the other hand, it is shown in [10] that

$$[E^+ : C^+] = h^+ \text{ or } 2h^+$$

according as $g \leq 3$ or $g = 4$. Since h^+ is odd and $\{\varepsilon^2 \mid \varepsilon \in C^+\} \subseteq C^*$, we obtain from this formula and (3) that

$$\begin{aligned} r(E^+/E^*) &= d && \text{if } g \leq 3, \\ r(E^+/E^*) &= d \text{ or } d+1 && \text{if } g = 4. \end{aligned}$$

Hence, by (1), the assertions (ii), (iii), (iv) are proved.

3

We shall see in this section how Theorems 1 and 2 are used to determine the structure of the ideal class groups of some cyclotomic fields. For each $n \in \mathbb{N}$, $\mathfrak{C}_n$ will denote the ideal class group of $\mathbb{Q}(\zeta_n)$.

By definition, d equals the rank of a matrix whose rows coincide with the vectors in B. We can therefore compute the value of d in an elementary manner as long as m is relatively small. For instance, if $m = 65 = 5 \cdot 13$, then we have $d = 19$ (cf. [3]), and we know $h^+ = 1$ from Example 4.4 of [7]; so $r(A) = 4$ by Theorem 2 while $h = 2^6$, $\mathfrak{C}_{65} = A$, and $f = 2$ in virtue of the calculations in [2, 5]. Therefore, by Theorem 1,

$$\mathfrak{C}_{65} \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^2.$$

We next deal with the case where $m = 77 = 7 \cdot 11$. In this case, our computations show $d = 25$. On the other hand, Theorem 4.5 of [7] implies $h^+ = 1$, so that $h = 2^8 \cdot 5$ and $f = 4$ (cf. [2, 5]). Furthermore, Theorem 2 shows that $r(A) = 4$ follows from $d = 25$ and $h^+ = 1$. Hence $A \cong (\mathbb{Z}/4\mathbb{Z})^4$ by Theorem 1. Thus

$$\mathfrak{C}_{77} \cong (\mathbb{Z}/4\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z}).$$

Similarly, in the case where $m = 87 = 3 \cdot 29$, we obtain

$$h^+ = 1, \quad h = 2^9 \cdot 3, \quad f = 3, \quad d = 24, \quad \text{and} \quad A \cong (\mathbb{Z}/8\mathbb{Z})^3$$

from some results of [2, 5, 7] and Theorems 1, 2:

$$\mathfrak{C}_{87} \cong (\mathbb{Z}/8\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z}).$$

If $m \in \{91, 95, 111, 116, 124, 156\}$, then $h^+ = 1$ by Theorem 3 of [6] and $d = 33, 34, 34, 24, 27$, or 39 according as $m = 91, 95, 111, 116, 124$, or 156. We therefore see from several results in [2, 5, 9] and Theorems 1, 2 that

$$\mathfrak{C}_{91} \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/7\mathbb{Z}) \oplus (\mathbb{Z}/13\mathbb{Z}) \oplus (\mathbb{Z}/37\mathbb{Z}),$$
$$\mathfrak{C}_{95} \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/13\mathbb{Z}) \oplus (\mathbb{Z}/19\mathbb{Z}) \oplus (\mathbb{Z}/109\mathbb{Z}),$$
$$\mathfrak{C}_{116} \cong (\mathbb{Z}/8\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/7\mathbb{Z}),$$
$$\mathfrak{C}_{156} \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/13\mathbb{Z}).$$

At the same time, we find that the class numbers of

$$\mathbb{Q}(\zeta_3,\ (1-\zeta_{37})(1-\zeta_{37}^{10})(1-\zeta_{37}^{26})), \quad \mathbb{Q}(\zeta_3,\ |(1-\zeta_{37})(1-\zeta_{37}^{6})|^2),$$
$$\mathbb{Q}(\zeta_4,\ (1-\zeta_{31})(1-\zeta_{31}^{5})(1-\zeta_{31}^{25}))$$

equal $2^2 \cdot 3$, $3^2 \cdot 19$, $3 \cdot 41$, respectively (see [13] as well). Hence, with the help of Lemmas 4 and 7 in [11], we further have

$$\mathfrak{C}_{111} \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/9\mathbb{Z}) \oplus (\mathbb{Z}/19\mathbb{Z})^2 \oplus (\mathbb{Z}/37\mathbb{Z}),$$
$$\mathfrak{C}_{124} \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/9\mathbb{Z}) \oplus (\mathbb{Z}/31\mathbb{Z}) \oplus (\mathbb{Z}/41\mathbb{Z}).$$

In the case where $m = 95$ or 111, we can prove again that $A \cong \mathbb{Z}/4\mathbb{Z}$, combining $h^+ = 1$ with the fact that the ideal class group of $\mathbb{Q}(\sqrt{-m})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}$. In the case $m = 124$, the fact that $f = t = 2$ also proves $A \cong (\mathbb{Z}/2\mathbb{Z})^2$.

We now consider the case where $m = 204 = 4 \cdot 3 \cdot 17$. Let $F = \mathbb{Q}(\zeta_{68} + \zeta_{68}^{-1}) = \mathbb{Q}(\cos\frac{\pi}{34})$. It follows from Theorem 3 of [6] that the class number of F equals 1. Since the principal ideal of F generated by 3 is the unique prime ideal of F ramified in the quadratic extension K^+ over F, the second theorem, II, of [4] implies $2 \nmid h^+$ and hence t equals 4 by the table of [9]. On the other hand, we have $d = 30$. Therefore, by Theorem 2, $r(A) = 1$ so that $A \cong \mathbb{Z}/16\mathbb{Z}$.

Remark. It should be added here that, in virtue of II of [4], one can easily find for each $a \in \{1, 2, 3\}$ infinitely many examples of K satisfying $g = a$ and $2 \nmid h^+$.

Finally, assume $g \geq 4$. Then 4 divides h by Lemmas 5 and 6 in [8]. The proof there of Lemma 6 actually implies that 4 divides the class number of every subfield k of K with $2 \nmid [K : k]$ (cf. Sätze 26, 31, and 34 of [2]). In particular, we have $X = \{K\}$. The following result is therefore obtained.

Proposition. *If $g \geq 4$, then $f = 1$.*

In the case where $m = 420 = 4 \cdot 3 \cdot 5 \cdot 7$, we can verify $2 \nmid h^+$ and we also have $d = 44$, whence Theorem 2 implies that $r(A) = 2$ or 3.

References

1. G. Cornell and M. I. Rosen, *The l-rank of the real class group of cyclotomic fields*, Compositio Math. **53** (1984), 133–141.
2. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952; Springer-Verlag, Berlin, Heidelberg, New York, and Tokyo, 1985.
3. K. Horie, *On the exponents of ideal class groups of cyclotomic fields*, Proc. Amer. Math. Soc. **119** (1993), 1049–1052.
4. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

5. E. E. Kummer, *Über die Klassenzahl der aus n-ten Einheitswurzeln gebildeten complexen Zahlen*, Monatsber. Akad. Wiss. Berlin (1861), 1051–1053; *Collected papers*, I, pp. 883–885.
6. F. J. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.
7. J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), 297–319.
8. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.
9. G. Schrutka von Rechtenstamm, *Tabelle der Relativ-Klassenzahlen der Kreiskörper, deren ϕ-Funktion des Wurzelexponenten (Grad) nicht grösser als* 256 *ist*, Abh. Deutschen Akad. Wiss. Berlin Kl. Math. Phys. **2** (1964), 1–64.
10. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. (2) **108** (1978), 107–134.
11. K. Tateyama, *On the ideal class groups of some cyclotomic fields*, Proc. Japan Acad. Ser. A Math. Sci. **58** (1982), 333–335.
12. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, Heidelberg, and Berlin, 1982.
13. K. Yoshino and M. Hirabayashi, *On the relative class number of the imaginary abelian number field* I, Mem. College Liberal Arts Kanazawa Medical Univ. **9** (1981), 5–53.

Department of Mathematics, Tokai University, 1117 Kitakaname, Hiratsuka 259-12, Japan

Department of Mathematics, Ochanomizu University, Otsuka, Bunkyo-ku, Tokyo 112, Japan

E-mail address: horie@math.ocha.ac.jp