PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 119, Number 4, December 1993

# ON THE EXPONENTS OF IDEAL CLASS GROUPS OF CYCLOTOMIC FIELDS

KUNIAKI HORIE

(Communicated by William Adams)

ABSTRACT. It will be proved that the ideal class group of the cyclotomic field of 65th roots of unity is of type $(4, 4, 2, 2)$, and remarks on the exponents of ideal class groups of cyclotomic fields will be made.

Let $\mathbb{Q}$ be the rational field, $\mathbb{Z}$ the additive group of (rational) integers, and $\mathbb{N}$ the set of positive integers. We shall assume all algebraic extensions over $\mathbb{Q}$ dealt with hereafter to be contained in the complex field. The exponent of each finite group $G$ will be denoted by $\exp G$. For any $m \in \mathbb{N}$, let $C_m$ denote the ideal class group of the cyclotomic field $\mathbb{Q}(e^{2\pi i/m})$. We then note that $\mathbb{Q}(e^{2\pi i/m'}) = \mathbb{Q}(e^{2\pi i/m})$ for some $m' \in \mathbb{N}$ less than $m$ if and only if $m \equiv 2 \pmod 4$.

In this paper, we shall prove the following results.

**Proposition 1.** *$C_{65}$ is isomorphic as an abelian group to the direct sum of two copies of $\mathbb{Z}/4\mathbb{Z}$ and two copies of $\mathbb{Z}/2\mathbb{Z}$:*

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

**Proposition 2.** *Let $m$ be a positive integer $\not\equiv 2 \pmod 4$. Then:*

(i) $\exp C_m = 2^n$ *does not hold for any $n \in \mathbb{N}$ exceeding 3,*
(ii) $\exp C_m = 8$ *is equivalent with $m = 68$,*
(iii) $\exp C_m = 4$ *is equivalent with $m = 65$ or 120,*
(iv) $\exp C_m = 2$ *is equivalent with $m = 29$, 39, or 56.*

*Remark.* It is well known that for $m$ in Proposition 2, $\exp C_m = 1$, i.e., $C_m = \{1\}$ if and only if $m \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$ (cf. [9]).

## 1

Let us prove Proposition 1. We put

$$K = \mathbb{Q}(\zeta) \quad \text{where } \zeta = e^{2\pi i/65}.$$

Received by the editors April 2, 1992.
1991 *Mathematics Subject Classification*. Primary 11R18, 11R29; Secondary 11R27, 11R37.
Supported in part by Grant-in-Aid for Scientific Reserch (No. 04640066), Ministry of Education, Science and Culture, Japan.

The class number of $K$ equals $2^6$ by [2, 6, 8]: $|C_{65}| = 2^6$. For any finite abelian group $A$, let $r(A)$ denote the rank of $A$. We shall first show $r(C_{65}) = 4$ and then show $r(C_{65}^2) = 2$.

Let $H$ be the maximal unramified abelian extension over $K$, $k$ the maximal real subfield of $K$, and $L$ the maximal abelian extension over $k$ in which no finite prime of $k$ is ramified. Note that $k \subseteq K \subseteq L \subseteq H$. The integral group ring of $\mathrm{Gal}(K/k)$ acts on both $C_{65}$ and $\mathrm{Gal}(H/K)$ in the obvious manner. Let $L'$ be the maximal unramified abelian extension over $K$ such that $\exp \mathrm{Gal}(L'/K) \leq 2$, i.e., the intermediate field of $H/K$ such that $\mathrm{Gal}(H/L') = \mathrm{Gal}(H/K)^2$. Let $j$ be the complex conjugation of $K$, i.e., the generator of $\mathrm{Gal}(K/k)$: $\langle j \rangle = \mathrm{Gal}(K/k)$. Since the class number of $k$ equals 1 (cf. [8]), we then have $C_{65}^{1+j} = \{1\}$ so that, by class field theory,

$$\mathrm{Gal}(H/K)^{1-j} = \mathrm{Gal}(H/K)^2 = \mathrm{Gal}(H/L').$$

Hence $L'$ is a Galois extension over $k$ and

$$\mathrm{Gal}(L'/k) = \langle j' \rangle \times \mathrm{Gal}(L'/K)$$

where $j'$ is the complex conjugation of $L'$. It therefore follows that $L'$ is an abelian extension over $k$ in which no finite prime of $k$ is ramified. This fact means

$$L' \subseteq L. \tag{1}$$

Now, let $E$ be the unit group of $K$, $E^+$ the unit group of $k$, $k_+$ the subgroup of the multiplicative group $k^\times$ consisting of all totally positive numbers in $k$, $P$ the group of principal ideals of $k$, and $\mathscr{O}$ the ring of algebraic integers in $k$;

$$P = \{\alpha\mathscr{O} \mid \alpha \in k^\times\}.$$

Let $P_+$ denote the subgroup of $P$ defined by

$$P_+ = \{\beta\mathscr{O} \mid \beta \in k_+\}.$$

Then, letting each $\alpha \in k^\times$ correspond to $\alpha\mathscr{O}$, we obtain homomorphisms

$$k^\times \longrightarrow P, \qquad k_+ \longrightarrow P_+.$$

These obviously induce an exact sequence

$$\{1\} \longrightarrow E^+/E_+ \longrightarrow k^\times/k_+ \longrightarrow P/P_+ \longrightarrow \{1\},$$

where $E_+$ denotes the group of totally positive units in $E^+$: $E_+ = E^+ \cap k_+$. As the class number of $k$ equals 1, we obtain $\mathrm{Gal}(L/k) \cong P/P_+$. In particular, $L \subseteq L'$ so that $L' = L$ by (1). Hence it follows from $k^\times/k_+ \cong (\mathbb{Z}/2\mathbb{Z})^{[k:\mathbb{Q}]}$ that

$$r(\mathrm{Gal}(L'/K)) = r(P/P_+) - 1 = [k:\mathbb{Q}] - 1 - r(E^+/E_+).$$

Consequently,

$$r(C_{65}) = 23 - r(E^+/E_+). \tag{2}$$

The main result of [10] (based on the analytic class number formula) implies that since just two distinct prime numbers are ramified in $K$ and since the class number of $k$ equals 1, $E$ is contained in the subgroup of $K^\times$ generated by $1 - \zeta^u$ for all $u \in \mathbb{Z}$ with $65 \nmid u$, whence $E$ is generated by $-\zeta$, $1 - \zeta^a$ for all

$a \in \{1, \ldots, 32\}$ prime to 65, $(1-\zeta^{5b})/(1-\zeta^5)$ for all $b \in \{2, 3, 4, 5, 6\}$, and $(1-\zeta^{26})/(1-\zeta^{13})$:

$$E = \left\langle -\zeta\,,\, 1-\zeta^a\,,\, \frac{1-\zeta^{5b}}{1-\zeta^5}\,,\, \frac{1-\zeta^{26}}{1-\zeta^{13}} \right\rangle_{1\le a\le 32,\ (a,65)=1;\ 2\le b\le 6}.$$

Let $E'$ be the subgroup of $E^+$ with generators $-1$, $(1-\zeta)(1-\zeta^{-1}) = |1-\zeta|^2$, $\sin\frac{2\pi a}{65}/\sin\frac{2\pi}{65} = (\zeta^a-\zeta^{-a})/(\zeta-\zeta^{-1})$ for all $a \in \{2, \ldots, 32\}$ prime to 65, $\sin\frac{2\pi b}{13}/\sin\frac{2\pi}{13}$ for all $b \in \{2, \ldots, 6\}$, and $\sin\frac{4\pi}{5}/\sin\frac{2\pi}{5}$. Then

$$(1-\zeta)^2 = -\zeta(1-\zeta)(1-\zeta^{-1}) \in \langle -\zeta\rangle E', \qquad E = \langle 1-\zeta\,,\, -\zeta\rangle E';$$

so the index $[E : \langle -\zeta\rangle E']$ does not exceed 2. However, $[E : \langle -\zeta\rangle E^+] = 2$ as is well known. Thus $\langle -\zeta\rangle E' = \langle -\zeta\rangle E^+$. It is now easy to see $E' = E^+$:

$$(3)\qquad E^+ = \left\langle -1\,,\, |1-\zeta|^2\,,\, \frac{\sin\frac{2\pi a}{65}}{\sin\frac{2\pi}{65}}\,,\, \frac{\sin\frac{2\pi b}{13}}{\sin\frac{2\pi}{13}}\,,\, \frac{\sin\frac{4\pi}{5}}{\sin\frac{2\pi}{5}} \right\rangle_{2\le a\le 32,\ (a,65)=1;\ 2\le b\le 6}.$$

Next, for any $n \in \mathbb{N}$, let $n^*$ denote the number of distinct positive integers $\le n$ prime to 65. With $c$ varying through the positive integers $\le 32$ prime to 65, put

$$\begin{aligned}
f(1, c^*) &= 1 + 2\mathbb{Z},\\
f(a^*, c^*) &= \left[\frac{2ac}{65}\right] + 2\mathbb{Z} \quad \text{for } a \in \{2, \ldots, 32\},\ (a, 65) = 1,\\
f(b+23, c^*) &= \left(\left[\frac{2bc}{13}\right] - \left[\frac{2c}{13}\right]\right) + 2\mathbb{Z} \quad \text{for } b \in \{2, \ldots, 6\},\\
f(30, c^*) &= \left(\left[\frac{4c}{5}\right] - \left[\frac{2c}{5}\right]\right) + 2\mathbb{Z}.
\end{aligned}$$

Here $[q]$ denotes for each $q \in \mathbb{Q}$ the maximal integer $\le q$ and we understand that, for each $u \in \mathbb{Z}$, $u + 2\mathbb{Z} = \{u + 2v \mid v \in \mathbb{Z}\}$ belongs to $\mathbb{F}_2$, the field whose additive group is $\mathbb{Z}/2\mathbb{Z}$. We can then define a matrix

$$M = \left(f(s, t)\right)_{1\le s\le 30,\ 1\le t\le 24}$$

of size $(30, 24)$ with coefficients in $\mathbb{F}_2$. Furthermore, we readily see from (3) that $r(E^+/E_+)$ equals the rank of $M$ while elementary calculations show that the rank of $M$ equals 19. Therefore we obtain $r(C_{65}) = 4$ from (2).

Now, let $F$ be the subfield of $K$ such that $[K : F] = 3$, and let $\sigma$ be a generator of $\mathrm{Gal}(K/F)$. As the class number of $F$ equals 1 (cf. [2, 8]), we have

$$(4)\qquad C_{65}^{1+\sigma+\sigma^2} = \{1\},$$

viewing $C_{65}$ as a module over the integral group ring of $\mathrm{Gal}(K/F)$. On the other hand, we have $r(C_{65}^2) = 1$ or 2 by $|C_{65}| = 2^6$ and $r(C_{65}) = 4$. In particular, there exists an element $x$ of $C_{65}$ with $x^2 \notin C_{65}^4$. If $r(C_{65}^2) = 1$ or equivalently $C_{65}^2/C_{65}^4 \cong \mathbb{Z}/2\mathbb{Z}$, then $x^{2\sigma}C_{65}^4 = x^2C_{65}^4$ so that

$$x^2 \in x^6C_{65}^4 = x^{2(1+\sigma+\sigma^2)}C_{65}^4.$$

This conclusion contradicts (4), however (for a general argument, cf. [12, Theorem 10.8]). Hence

$$r(C_{65}^2) = 2, \quad \text{namely, } C_{65} \cong (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^2.$$

## 2

It is proved in [3] that if $m$ is a positive integer $\not\equiv 2 \pmod 4$ different from 29, 39, 56, 65, 68, 120, then $|C_m|$ either equals 1 or has an odd prime divisor. Proposition 2 therefore follows from Proposition 1 and the well-known facts below (cf. [1, 4, 5, 8, 11]).

$$C_{29} \cong (\mathbb{Z}/2\mathbb{Z})^3, \quad C_{39} \cong C_{56} \cong \mathbb{Z}/2\mathbb{Z}, \quad C_{68} \cong \mathbb{Z}/8\mathbb{Z}, \quad C_{120} \cong \mathbb{Z}/4\mathbb{Z}.$$

*Remark.* Modifying the proof of Proposition 1, we can further find other facts such as

$$C_{77} \cong (\mathbb{Z}/4\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z}), \quad C_{87} \cong (\mathbb{Z}/8\mathbb{Z})^3 \oplus (\mathbb{Z}/3\mathbb{Z}), \quad C_{156} \cong \mathbb{Z}/4 \cdot 3 \cdot 13\mathbb{Z}\ ;$$

but we omit the details here.


## Acknowledgment

The author thanks his wife Mitsuko for helpful conversations.


## References


1. F. Gerth, *The ideal class groups of two cyclotomic fields*, Proc. Amer. Math. Soc. **78** (1980), 321–322.
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 class numbers of cyclotomic fields*, Manuscripta Math. **65** (1989), 465–477.
4. K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J. **27** (1966), 239–247.
5. E. E. Kummer, *Über die Irregularität von Determinanten*, Monatsber. Akad. Wiss. Berlin (1853), 194–200; *Collected Papers*, I, 539–545.
6. ———, *Über die Klassenzahl der aus n-ten Einheitswurzeln gebildeten complexen Zahlen*, Monatsber. Akad. Wiss. Berlin (1861), 1051–1053 ; *Collected Papers*, I, 883–885.
7. S. Louboutin, *Détermination des corps quartiques cycliques totalement imaginaires à groupe des classes d'idéaux d'exposant* $\leq 2$, Manuscripta Math. **77** (1992), 385–404.
8. J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), 297–319.
9. J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.
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 **58** (1982), 333–335.
12. L. C. Washington, *Introduction to cyclotomic fields*, Springer Verlag, New York, Heidelberg, and Berlin, 1982.



Department of Mathematics, Nara Women's University, Kita-uoya Nishimachi, Nara 630, Japan

*Current address*: Department of Mathematics, Tokai University, 1117 Kitakaname, Hiratsuka, Kanagawa 259-12, Japan