S. Shirai
Nagoya Math. J.
Vol. 75 (1979), 133-143

ON THE CENTRAL IDEAL CLASS GROUP OF CYCLOTOMIC FIELDS

SUSUMU SHIRAI

Introduction

Let $\boldsymbol{Q}$ be the rational number field, $K/\boldsymbol{Q}$ be a finite Galois extension with the Galois group G, and let C_K be the ideal class group of K in the wider sense. We consider C_K as a G-module. Denote by I the augmentation ideal of the group ring of G over the ring of rational integers. Then $C_K/I(C_K)$ is called the central ideal class group of K, which is the maximal factor group of C_K on which G acts trivially. A. Fröhlich [3, 4] rationally determined the central ideal class group of a complete[1] Abelian field over $\boldsymbol{Q}$ whose degree is some power of a prime. The proof is based on Theorems 3 and 4 of Fröhlich [2]. D. Garbanati [6] recently gave an algorithm which will produce the ℓ-invariants of the central ideal class group of an Abelian extension over $\boldsymbol{Q}$ for each prime ℓ dividing its order.

In the present paper we determine the central ideal class group of a cyclotomic field over $\boldsymbol{Q}$ in terms of generators and relations by refining upon the methods used in [3, 4] (§ 3, Theorem 5). The proof is based on Theorem 32 of our preceding paper [10], which is a generalization of Fröhlich [2, Theorem 3] to the case of a cyclotomic field over $\boldsymbol{Q}$.

Notation

Throughout this paper the following notation will be used.

$\boldsymbol{Q}$ the field of rational numbers as in Introduction.

$\boldsymbol{Z}$ the ring of rational integers on which a finite group acts trivially.

Received August 4, 1978.

1) Cf. Fröhlich [3, p. 212] and [4, pp. 73-77]. When $[K:\boldsymbol{Q}] = \ell^{\alpha}$, this implies that $K_0^* = K$ or $K^* = K$ according as $\ell = 2$, K real or otherwise, where K_0^* is the maximal real, unramified, Abelian 2-extension of K which is still Abelian over $\boldsymbol{Q}$, and K^* is the maximal, unramified, Abelian ℓ-extension of K which is still Abelian over $\boldsymbol{Q}$.

Z_n	the cyclic group of order n.
$\langle A\rangle$	the subgroup generated by A when A is a subset in a group.
(a, b)	the commutator $aba^{-1}b^{-1}$ of a and b when a, b are elements in a group.
(A, B)	the subgroup generated by the commutators (a, b) of all $a \in A$, $b \in B$ when A, B are subsets in a group.
$A \times B$	the direct product of A by B when A, B are groups.
$G(K/k)$	the Galois group of K over k.
$(\ \ , K/k)$	the norm residue symbol for K/k when K/k is a local Abelian extension.
$\left(\frac{\ \ , K}{p}\right)$	the norm residue symbol for K when K is a finite Abelian extension over $\boldsymbol{Q}$.
$C_K/I(C_K)$	the central ideal class group of K defined in Introduction when K is a finite Galois extension over $\boldsymbol{Q}$.
$\psi(n)$	the Euler's function, i.e. the number of positive integers not exceeding n which are relatively prime to n.
(m, n)	the $G. C. D.$ of m and n when m, n are rational integers.

Moreover we will use the results and notation of the preceding paper [10].

§1. The Schur multiplicator of a finite Abelian group

The structure of the Schur multiplicator $H^{-3}(G, Z)$ of a finite Abelian group G is well-known (cf. [7], [8], [9]). In this section we describe $H^{-3}(G, Z)$ in terms of generators and relations.

LEMMA 1. *If* $G = Z_{n_1} \times \cdots \times Z_{n_r}$, *then*

$$|H^{-3}(G, Z)| = \prod_{1 \leq i < j \leq r} (n_i, n_j)\ .$$

Proof. We proceed by induction on r. For any Abelian group A, and any integer q, we denote by $A(q)$ the subgroup comprising all those elements a of A such that $a^q = 1$. Then it follows from R. C. Lyndon [7, Lemma 8.2] that

$$\begin{aligned} H^{-3}(G, Z) &\cong H^3(G, Z) \\ &\cong H^3(Z_{n_r}, Z) \times \prod_{0<k<3} H^k(Z_{n_1} \times \cdots \times Z_{n_{r-1}}, Z)(n_r) \\ &\qquad \times H^3(Z_{n_1} \times \cdots \times Z_{n_{r-1}}, Z) \\ &\cong (Z_{n_1} \times \cdots \times Z_{n_{r-1}})(n_r) \times H^3(Z_{n_1} \times \cdots \times Z_{n_{r-1}}, Z)\ , \end{aligned}$$

because $H^1(G, Z) = 1$ and $H^2(G, Z) \cong G$ for any finite Abelian group G.

Thus by induction hypothesis,

$$|H^{-3}(G, Z)| = \prod_{1\leqq i<j\leqq r-1} (n_i, n_j)\cdot(n_1, n_r) \cdots (n_{r-1}, n_r)$$
$$= \prod_{1\leqq i<j\leqq r} (n_i, n_j) . \qquad \text{Q.E.D.}$$

LEMMA 2. *Let* $G = Z_{n_1} \times \cdots \times Z_{n_r}$, *and let*

$$1 \longrightarrow (\Omega, \Omega) \longrightarrow \Omega \xrightarrow{f} G \longrightarrow 1$$

be an exact sequence in which Ω *is a finite nilpotent group of class two such that* $(\Omega, \Omega) \cong H^{-3}(G, Z)$. *Denote by* ω_i *an element of* Ω *such that* $f(\omega_i)$ *is a generator of* $Z_{n_i}(\subset G)$ *for* $i = 1, \cdots, r$. *Then* (Ω, Ω) *is generated by* $\binom{r}{2}$ *elements*

$$(\omega_i, \omega_j) , \qquad 1 \leqq i < j \leqq r ,$$

and completely determined by the relations

$$(1) \qquad \begin{cases} (\omega_i, \omega_j)(\omega_k, \omega_l) = (\omega_k, \omega_l)(\omega_i, \omega_j) , & \text{all } i, j, k, l , \\ (\omega_i, \omega_j)^{(n_i, n_j)} = 1 , & 1 \leqq i < j \leqq r . \end{cases}$$

Proof. Since Ω is of class two, it is obvious that the elements (ω_i, ω_j), $1 \leqq i < j \leqq r$ generate (Ω, Ω), and satisfy the above relations (1). Furthermore the order of (Ω, Ω) is $\prod_{1\leqq i<j\leqq r} (n_i, n_j)$ by Lemma 1. Conversely the group which is generated by $\binom{r}{2}$ elements and satisfies the above relations (1) is an Abelian group of order $\prod_{1\leqq i<j\leqq r} (n_i, n_j)$. Hence (Ω, Ω) is completely described by the relations (1). Q.E.D.

§ 2. Inertia groups

Let p be a rational prime, $\boldsymbol{Q}_p$ be the p-adic number field, $T/\boldsymbol{Q}_p$ be a finite unramified extension, ζ be a primitive p^ν-th root of unity, and let $K = T(\zeta)$. Denote by $\hat{K}$ a central extension of $K/\boldsymbol{Q}_p$ such that the p-exponent $\mu(\hat{K}/\boldsymbol{Q}_p)$ of the Galois conductor[2)] of $\hat{K}/\boldsymbol{Q}_p$ does not exceed ν.

LEMMA 3. *Let* $p = 2$, *and let*

$$\sigma = (2, K/\boldsymbol{Q}_2)^{-1} , \quad \tau^* = (-1, K/\boldsymbol{Q}_2) , \quad \tau = (5, K/\boldsymbol{Q}_2) .$$

Denote by $\tilde{\sigma}, \tilde{\tau}^*$, *and* $\tilde{\tau}$ *any extensions of* σ, τ^*, *and* τ *to* $\hat{K}$, *respectively.*

2) See [10, §1].

Then the inertia group of $\hat{K}/K$ is generated by the elements $(\tilde{\tau}, \tilde{\tau}^*)$, $(\tilde{\tau}, \tilde{\sigma})$, $(\tilde{\tau}^*, \tilde{\sigma})$.

Proof. Let F be the inertia field of $\hat{K}/K$, and let D be the fixed field of $\langle(\tilde{\tau}, \tilde{\tau}^*), (\tilde{\tau}, \tilde{\sigma}), (\tilde{\tau}^*, \tilde{\sigma})\rangle$. Since $G(\hat{K}/\boldsymbol{Q}_2)$ is of class two and $\{\tilde{\sigma}, \tilde{\tau}^*, \tilde{\tau}\}$ is a system of generators of $G(\hat{K}/\boldsymbol{Q}_2)$, the commutator group of $G(\hat{K}/\boldsymbol{Q}_2)$ is generated by the elements $(\tilde{\tau}, \tilde{\tau}^*)$, $(\tilde{\tau}, \tilde{\sigma})$, $(\tilde{\tau}^*, \tilde{\sigma})$. Thus $D/\boldsymbol{Q}_2$ is the maximal Abelian extension contained in $\hat{K}$. Hence $D \supset F$, because $F/\boldsymbol{Q}_2$ is an Abelian extension.

To prove the converse let T' be the inertia field of $D/\boldsymbol{Q}_2$. Since $\mu(D/\boldsymbol{Q}_2) \leqq \mu(\hat{K}/\boldsymbol{Q}_2) \leqq \nu$ by [10, Lemma 3], it follows from local class field theory that $G(D/T')$ is a homomorphic image of the group of prime residue classes mod 2^ν. We have $[D: T'] \leqq \psi(2^\nu) = 2^{\nu-1}$, and hence $D = T'K$, because of $T' \cap K = T$, $[T'K: T'] = [K: T] = 2^{\nu-1}$. We conclude that D/K is unramified, which implies $F \supset D$. Q.E.D.

By the same procedure as the proof of Lemma 3, we obtain

LEMMA 4. *Let $p \neq 2$, g be a primitive root* mod p^ν, *and let*

$$\sigma = (p, K/\boldsymbol{Q}_p)^{-1}\,, \qquad \tau = (g, K/\boldsymbol{Q}_p)\,.$$

Denote by $\tilde{\sigma}$ and $\tilde{\tau}$ any extensions of σ and τ to, $\hat{K}$, respectively. Then the inertia group of $\hat{K}/K$ is generated by the single element $(\tilde{\tau}, \tilde{\sigma})$.

§ 3. The central ideal class group of cyclotomic fields

Let $m = 2^\nu p_1^{\nu_1} \cdots p_r^{\nu_r}$ be a positive integer, K be the m-th cyclotomic field over $\boldsymbol{Q}$, and let $\hat{K}$ be the central class field mod mp_∞ in the sense of [10, § 3], where p_∞ is the real prime divisor of $\boldsymbol{Q}$. Then $\hat{K}$ is a central extension of $K/\boldsymbol{Q}$, and hence it is a nilpotency class two extension over $\boldsymbol{Q}$. Moreover it follows from the definition of the central class field mod $\mathfrak{m}$ that any rational prime not contained in mp_∞ is unramified in $\hat{K}$. We have already proved in [10, Theorem 32] that if $(m, 16) \neq 8$, then

$$(G(\hat{K}/\boldsymbol{Q}), G(\hat{K}/\boldsymbol{Q})) = G(\hat{K}/K) \cong H^{-3}(G(K/\boldsymbol{Q}), \boldsymbol{Z})\,. \tag{2}$$

For use of this result we distinguish the following three cases:

$$\text{(a)}\ \ \nu = 0\,, \qquad \text{(b)}\ \ \nu = 2\,, \qquad \text{(c)}\ \ \nu \geqq 4\,.$$

In the present paper we will prove our main Theorem for (a) and state the corresponding results for (b) and (c).

Assume $\nu = 0$. Let g_i be a primitive root $\bmod p_i^{\nu_i}$, and let

$$\sigma_i = \left(\frac{p_i, K}{p_i}\right)^{-1}, \qquad \tau_i = \left(\frac{g_i, K}{p_i}\right), \qquad i = 1, \cdots, r .$$

Since $G(K/Q)$ is isomorphic to the group of prime residue classes mod m, $G(K/Q) \cong Z_{\psi(p_1^{\nu_1})} \times \cdots \times Z_{\psi(p_r^{\nu_r})}$, and $\{\tau_1, \cdots, \tau_r\}$ is a system of generators of $G(K/Q)$. For each i, we choose elements $\tilde{\sigma}_i$ and $\tilde{\tau}_i$ in the decomposition group of a prime factor $\mathfrak{P}_i$ of p_i in $\hat{K}$, which under the natural homomorphism of $G(\hat{K}/Q)$ onto $G(K/Q)$ are mapped onto σ_i and τ_i, respectively. Since $G(\hat{K}/K)$ is contained in the center of $G(\hat{K}/Q)$, the inertia group of $\mathfrak{P}_i$ over K does not depend on the choice of $\mathfrak{P}_i$ over p_i, and it is generated by the element $(\tilde{\tau}_i, \tilde{\sigma}_i)$, as we can see by Lemma 4.

According to Lemma 2 and (2), $G(\hat{K}/K)$ is generated by $\binom{r}{2}$ elements

$$(\tilde{\tau}_i, \tilde{\tau}_j) , \qquad 1 \leqq i < j \leqq r ,$$

and completely determined by the relations

$$(\tilde{\tau}_i, \tilde{\tau}_j)(\tilde{\tau}_k, \tilde{\tau}_l) = (\tilde{\tau}_k, \tilde{\tau}_l)(\tilde{\tau}_i, \tilde{\tau}_j) , \qquad \text{all } i, j, k, l,$$
$$(\tilde{\tau}_i, \tilde{\tau}_j)^{(\psi(p_i^{\nu_i}), \psi(p_j^{\nu_j}))} = 1 , \qquad 1 \leqq i < j \leqq r .$$

Let C_K be the ideal class group[3] of K, and let U be the Abelian extension of K corresponding to $I(C_K)$ in the sense of class field theory. Then U is the maximal central extension of K/Q which is unramified over K, and is contained in $\hat{K}$, as we can see by going back to the definition of the central class field mod $\mathfrak{m}$. We conclude that U is the subfield of $\hat{K}$ corresponding to $\langle(\tilde{\tau}_1, \tilde{\sigma}_1), \cdots, (\tilde{\tau}_r, \tilde{\sigma}_r)\rangle$ in the sense of Galois theory. Hence

$$C_K/I(C_K) \cong G(U/K) \cong G(\hat{K}/K)/\langle(\tilde{\tau}_1, \tilde{\sigma}_1), \cdots, (\tilde{\tau}_r, \tilde{\sigma}_r)\rangle .$$

We next express $(\tilde{\tau}_i, \tilde{\sigma}_i)$ in terms of $\tilde{\tau}_1, \cdots, \tilde{\tau}_r$. Define the symbols[4] $[j, i]$, $[0, i]^*$, $[0, i]$ by putting

$$(3) \qquad \begin{cases} p_i \equiv g_j^{[j,i]} \bmod p_j^{\nu_j} , & i = 0, 1, \cdots, r, \ j = 1, \cdots, r , \\ p_i \equiv (-1)^{[0,i]^*} 5^{[0,i]} \bmod 2^{\nu} , & i = 1, \cdots, r , \\ [i, i] = 0 , & i = 1, \cdots, r , \end{cases}$$

3) In this case the ideal class groups in the narrow and the wider sense coincide, because no real prime divisor exists in K.

4) Cf. Fröhlich [2, pp. 237–238].

where $p_0 = 2$, namely, $[j, i]$ is the index of p_i for the modulus $p_j^{\nu_j}$ relative to the primitive root g_j, and $[0, i]^*$, $[0, i]$ are the indices of p_i for the modulus 2^ν relative to the basis $\{-1, 5\}$. Then we have

$$\sigma_i = \prod_{j=1}^{r} \tau_j^{[j,i]} \qquad \text{for } i = 1, \cdots, r ,$$

because of $\prod_{\text{all } p} \left(\frac{p_i, K}{p}\right) = 1$, the product formula in class field theory. Therefore

$$(\tilde{\tau}_i, \tilde{\sigma}_i) = \tilde{\tau}_i\tilde{\sigma}_i\tilde{\tau}_i^{-1}\tilde{\sigma}_i^{-1} = \left(\tilde{\tau}_i, \prod_{j=1}^{r} \tilde{\tau}_j^{[j,i]}\right)$$
$$= \prod_{j=1}^{r} (\tilde{\tau}_i, \tilde{\tau}_j)^{[j,i]} ,$$

because $G(\hat{K}/K)$ is contained in the center of $G(\hat{K}/\boldsymbol{Q})$ and $G(\hat{K}/\boldsymbol{Q})$ is of class two. Thus[5] we have proved the following main

THEOREM 5. *Let $m = 2^\nu p_1^{\nu_1} \cdots p_r^{\nu_r}$ be a positive integer, K be the m-th cyclotomic field over $\boldsymbol{Q}$, and let $C_K/I(C_K)$ be the central ideal class group of K. Then:*

(a) $\nu = 0$. *$C_K/I(C_K)$ is generated by $\binom{r}{2}$ elements x_{ij}, $1 \leqq i < j \leqq r$, and completely determined by the relations*

$$x_{ij}x_{kl} = x_{kl}x_{ij} , \qquad \textit{all } i, j, k, l ,$$
$$\prod_{j=1}^{r} x_{ij}^{[j,i]} = 1 , \qquad i = 1, \cdots, r ,$$
$$x_{ij}^{(\psi(p_i^{\nu_i}), \psi(p_j^{\nu_j}))} = 1 , \qquad 1 \leqq i < j \leqq r ,$$

with the convention $x_{ji} = x_{ij}^{-1}$.

(b) $\nu = 2$. *$C_K/I(C_K)$ is generated by $\binom{r+1}{2}$ elements x_{ij}, $0 \leqq i < j \leqq r$, and completely determined by the relations*

$$x_{ij}x_{kl} = x_{kl}x_{ij} , \qquad \textit{all } i, j, k, l ,$$
$$\prod_{j=1}^{r} x_{0j}^{[j,0]} = 1 ,$$
$$x_{0i}^{-[0,i]^*} \prod_{j=1}^{r} x_{ij}^{[j,i]} = 1 , \qquad i = 1, \cdots, r ,$$
$$x_{0i}^2 = 1 , \qquad i = 1, \cdots, r ,$$

5) As regards computation in the cases (b) and (c), cf. [11, §3]. See also Fröhlich [3, Theorem 2] and [4, Theorem 3].

$$x_{ij}^{(\psi(p_i^{\nu_i}),\psi(p_j^{\nu_j}))}=1\,,\qquad 1\leqq i<j\leqq r\,,$$

with the convention $x_{ji}=x_{ij}^{-1}$.

(c) $\nu\geqq 4$. *$C_K/I(C_K)$ is generated by* $\binom{r+2}{2}-1$ *elements* x_{ij}, $-1\leqq i<j\leqq r$, $(i,j)\neq(-1,0)$, *and completely determined by the relations*

$$\begin{aligned}
&x_{ij}x_{kl}=x_{kl}x_{ij}\,, && \text{all } i,j,k,l\,,\\
&\prod_{j=1}^{r}x_{ij}^{[j,0]}=1\,, && i=-1,0\,,\\
&x_{-1i}^{-[0,i]}x_{0i}^{-[0,i]^*}\prod_{j=1}^{r}x_{ij}^{[j,i]}=1\,, && i=1,\cdots,r\\
&x_{-1i}^{(2^{\nu-2},\psi(p_i^{\nu_i}))}=1\,, && i=1,\cdots,r\,,\\
&x_{0i}^{2}=1\,, && i=1,\cdots,r\,,\\
&x_{ij}^{(\psi(p_i^{\nu_i}),\psi(p_j^{\nu_j}))}=1\,, && 1\leqq i<j\leqq r\,,
\end{aligned}$$

with the convention $x_{ji}=x_{ij}^{-1}$, *where* $[j,i]$, $[0,i]^*$, $[0,i]$ *are the indices defined by* (3).

§4. Applications

Y. Furuta [5, Theorem 4] proved the following result: Let ℓ be any rational prime and m be a rational integer. Assume that the number of different prime divisors p of m such that $p\equiv 1 \bmod \ell$ is equal to or greater than 8 (this number should be replaced by 9, only when $\ell=2$ and $m\not\equiv 0 \bmod 4$). Then the class number of the m-th cyclotomic field is always divisible by ℓ and moreover the m-th cyclotomic field admits an infinite unramified ℓ-extension.

The first half of this result can be sharpen as follows.

THEOREM 6[6]. *Let* $m=2^{\nu}p_1^{\nu_1}\cdots p_r^{\nu_r}$ *be a positive integer, K be the m-th cyclotomic field over* $\boldsymbol{Q}$, ρ_ℓ *be the ℓ-rank of* $C_K/I(C_K)$, *and let t be the number of different primes* p_i *of m such that* $p_i\equiv 1 \bmod \ell$. *Then*:

(a) $\nu=0$. $\qquad\rho_\ell\geqq\frac{1}{2}t(t-3)$.

In particular $\qquad\rho_2\geqq\frac{1}{2}r(r-3)$.

(b) $\nu=2$. $\qquad\rho_\ell\geqq\frac{1}{2}t(t-3)$, $\qquad\ell\neq 2$,

$\qquad\rho_2\geqq\frac{1}{2}(r+1)(r-2)$.

(c) $\nu\geqq 4$. $\qquad\rho_\ell\geqq\frac{1}{2}t(t-3)$, $\qquad\ell\neq 2$,

$\qquad\rho_2\geqq\frac{1}{2}(r^2+r-4)$.

Proof. (a) Suppose the primes p_i to be so numbered that $p_i\equiv 1 \bmod \ell$ for $i=1,\cdots,t$. Set $m'=p_1^{\nu_1}\cdots p_t^{\nu_t}$, and denote by C' the central

6) Cf. Fröhlich [3, Lemmas 2 and 3] and [4, Lemmas 4 and 5].

ideal class group of the m'-th cyclotomic field over $\boldsymbol{Q}$. By virtue of Theorem 5, (a), C' is generated by $\binom{t}{2}$ elements y_{ij}, $1 \leqq i < j \leqq t$, and completely determined by the relations

$$\begin{aligned} &y_{ij}y_{kl} = y_{kl}y_{ij}\,, && \text{all } i, j, k, l\,, \\ (4) \qquad &\prod_{j=1}^{t} y_{ij}^{[j,i]} = 1\,, && i = 1, \cdots, t\,, \\ &y_{ij}^{(\psi(p_i^{\nu_i}),\psi(p_j^{\nu_j}))} = 1\,, && 1 \leqq i < j \leqq t\,, \end{aligned}$$

where $y_{ji} = y_{ij}^{-1}$. We define a homomorphism $C_K/I(C_K) \to C'$ by putting $x_{ij} \to y_{ij}$ for $1 \leqq i < j \leqq t$, $x_{ij} \to 1$ otherwise. Then the homomorphism is epimorphic. Hence denoting the ℓ-rank of C' by ρ'_ℓ, we have

$$\rho_\ell \geqq \rho'_\ell\,.$$

It follows from the assumption that

$$(\psi(p_i^{\nu_i}), \psi(p_j^{\nu_j})) \equiv 0 \bmod \ell \qquad \text{for } 1 \leqq i < j \leqq t\,.$$

Noting the convention $y_{ji} = y_{ij}^{-1}$, we denote by A the matrix of coefficients in the additively written equations (4) on generators y_{ij} and by $r(A)$ its rank as a matrix in $GF(\ell)$. Since A is *a* $(t, \frac{1}{2}t(t-1))$ matrix, we have $r(A) \leqq t$. Hence

$$\rho'_\ell = \tfrac{1}{2}t(t-1) - r(A) \geqq \tfrac{1}{2}t(t-3)\,.$$

Q.E.D.

COROLLARY 7. *Let $m = 2^\nu p_1^{\nu_1} \cdots p_r^{\nu_r}$ be a positive integer, h be the class number of the m-th cyclotomic field over $\boldsymbol{Q}$, and let t be the number of different primes p_i of m such that $p_i \equiv 1 \bmod \ell$ for an odd prime ℓ. Then:*

(a) $\nu = 0$. *If $r \geqq 4$, then $2^2|h$.*
If $t \geqq 4$, then $2^2\ell^2|h$.

(b) $\nu = 2$. *If $r \geqq 3$, then $2^2|h$.*
If $t \geqq 4$, then $2^5\ell^2|h$.

(c) $\nu \geqq 4$. *If $r \geqq 2$, then $2|h$.*
If $t \geqq 4$, then $2^8\ell^2|h$.

In any case h is divisible by 4 if $r \geqq 4$, and by $2^2\ell^2$ if $t \geqq 4$.

Finally we state a result concerning the invariants of the central ideal class group of cyclotomic fields. The following Lemma can be easily verified[7].

LEMMA 8. *For any prime p and any integer a prime to p, let*

$$o(p^\nu, a) = \text{the order of } a \bmod p^\nu \text{ for } \nu \geqq 1,$$
$$q(p, a) = \text{the highest exponent of } p \text{ dividing } a^{p-1} - 1.$$

Then we have: (i) *If* $p \neq 2$ *and* $\alpha = q(p, a)$, *then*

$$o(p, a) = o(p^2, a) = \cdots = o(p^\alpha, a) ,$$
$$o(p^{\alpha+i}, a) = p^i o(p, a) \qquad \text{for } i \geqq 1 .$$

(ii) $p = 2$. *If* $\alpha = q(2, a) > 1$, *i.e.* $a \equiv 1 \bmod 4$, *then*

$$o(2, a) = o(2^2, a) = \cdots = o(2^\alpha, a) = 1 ,$$
$$o(2^{\alpha+i}, a) = 2^i \qquad \text{for } i \geqq 1 ,$$

and if $\alpha = 1$, *i.e.* $a \equiv 3 \bmod 4$, *then*

$$o(2^2, a) = o(2^3, a) = \cdots = o(2^\beta, a) = 2 ,$$
$$o(2^{\beta+i}, a) = 2^{i+1} \qquad \text{for } i \geqq 1 ,$$

where $\beta =$ *the highest exponent of* 2 *dividing* $a^2 - 1$. *Note* $\beta \geqq 3$, *which implies that the group of prime residue classes* mod 2^ν *is not cyclic when* $\nu \geqq 3$.

Denote by B the matrix of coefficients in the additively written equations on generators x_{ij} in Theorem 5, (a), noting $x_{ji} = x_{ij}^{-1}$. Then B is a $(\frac{1}{2}r(r+1), \frac{1}{2}r(r-1))$ matrix. Let e_i be the elementary divisors of B in the domain of rational integers such that $e_1|e_2| \cdots |e_s, e_i > 0, i = 1, \cdots, s$. Then $C_K/I(C_K)$ can be written in the form, as a product of cyclic groups,

$$C_K/I(C_K) \cong Z_{e_1} \times \cdots \times Z_{e_s} . \tag{5}$$

Each e_i can be computed by the following rule: Let $D_i(B)$ be the G.C.D. of all i-th minors in $\det B$. Then

$$D_i(B) = e_1 e_2 \cdots e_i , \qquad 1 \leqq i \leqq s .$$

Hence

$$\begin{aligned} e_1 &= \text{the G.C.D. of all entries of } B \\ &= \text{G.C.D. } \{(\psi(p_i^{\nu_i}), \psi(p_j^{\nu_j}), [j, i], [i, j]) \mid 1 \leqq i < j \leqq r\} \\ &= \text{G.C.D. } \left\{\left(\frac{\psi(p_i^{\nu_i})}{o(p_i^{\nu_i}, p_j)}, \frac{\psi(p_j^{\nu_j})}{o(p_j^{\nu_j}, p_i)}\right) \middle| 1 \leqq i < j \leqq r\right\} . \end{aligned}$$

7) See also L. E. Dickson [1, Chapter VII].

Thus by virtue of Lemma 8 we obtain

THEOREM 9. *Let* $m = p_1^{\nu_1} \cdots p_r^{\nu_r}, p_1, \cdots, p_r$ *distinct odd primes, and let* $C_K/I(C_K)$ *be the central ideal class group of the m-th cyclotomic field over* $\boldsymbol{Q}$. *Then the first elementary divisor* e_1 *of* $C_K/I(C_K)$ *in* (5) *becomes constant for all* ν_i *sufficiently large. In fact if we put* $\alpha_{ij} = q(p_i, p_j)$ *and take* $\nu_i > \max\{\alpha_{ij} | j = 1, \cdots, r\}$ *for* $i = 1, \cdots, r$, *then*

$$e_1 = \text{G.C.D.}\left\{\left(\frac{\psi(p_i^{\alpha_{ij}})}{o(p_i, p_j)}, \frac{\psi(p_j^{\alpha_{ji}})}{o(p_j, p_i)}\right)\middle| 1 \leqq i < j \leqq r\right\}.$$

EXAMPLE. For $m = 5^{\nu_1} 11^{\nu_2}, \nu_1 \geqq 2, \nu_2 \geqq 2$, we have $C_K/I(C_K) \cong \boldsymbol{Z}_2$.

Remark. Let K be a finite Galois extension over $\boldsymbol{Q}, f(K)$ be its Galois conductor in the sense of [10, § 2], and let m be a rational module such that $f(K)|m$. We denote by $\hat{K}_m$ the central class field mod m and by K_m^* the genus field mod m of $K/\boldsymbol{Q}$ in the sense of [10, § 3]. Then it follows from [10, Theorem 31] that if all first ramification groups of $K/\boldsymbol{Q}$ are cyclic, then

$$G(\hat{K}_m/K_m^*) \cong H^{-3}(G(K/\boldsymbol{Q}), \boldsymbol{Z}).$$

Thus the method leading up to main Theorem 5 can be applicable to determine the central ideal class group of Abelian extensions over $\boldsymbol{Q}$ whose first ramification groups are cyclic, because it is based on Lemma 2 and (2).

REFERENCES

[1] L. E. Dickson, History of the Theory of Numbers, vol. **1**, Washington 1919.
[2] A. Fröhlich, On fields of class two, Proc. London Math. Soc. (3), **4** (1954), 235–256.
[3] ——, On the absolute class-group of Abelian fields, J. London Math. Soc., **29** (1954), 211–217.
[4] ——, On the absolute class-group of Abelian fields (II), J. London Math. Soc., **30** (1955), 72–80.
[5] Y. Furuta, On class field towers and the rank of ideal class groups, Nagoya Math. J., **48** (1972), 147–157.
[6] D. Garbanati, Invariants of the ideal class group and the Hasse norm theorem, J. reine angew. Math., **297** (1978), 159–171.
[7] R. C. Lyndon, The cohomology theory of group extensions, Duke Math. J., **15** (1948), 271–292.
[8] I. Schur, Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. reine angew. Math., **127** (1904), 20–50.
[9] I. Schur, Untersuchungen über die Darstellung der endlichen Gruppen durch

gebrochene lineare Substitutionen, ibid., **132** (1907), 85–137.
[10] S. Shirai, On the central class field mod $\mathfrak{m}$ of Galois extensions of an algebraic number field, Nagoya Math. J., **71** (1978), 61–85.
[11] ——, On Galois groups of class two extensions over the rational number field, Nagoya Math. J., **75** (1979), 121–131.

Toyama Medical and Pharmaceutical University