Kangweon-Kyungki Math. Jour. **5** (1997), No. 1, pp. 61–74

# GENERATORS OF COHOMOLOGY GROUPS OF CYCLOTOMIC UNITS

Jae Moon Kim and Seung Ik Oh

Abstract. Let $d$ be a positive integer with $d \not\equiv 2 \bmod 4$, and let $K = \mathbb{Q}(\zeta_{pd})$ for an odd prime $p$ such that $p \equiv 1 \mod d$. Let $K_\infty = \bigcup_{n\geq 0} K_n$ be the cyclotomic $\mathbb{Z}_p$-extension of $K = K_0$. In this paper, explicit generators for the Tate cohomology group $\widehat{H}^{-1}(G_{m,n}$ are given when $d = qr$ is a product of two distinct primes, where $G_{m,n}$ is the Galois group $\mathrm{Gal}(K_m/K_n)$ and $C_m$ is the group of cyclotomic units of $K_m$. This generalizes earlier results when $d = q$ is a prime.

## 1. Introduction

Let $K$ be a number field and $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$, where $p$ is an odd prime. That is $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, the additive group of the ring of $p$-adic integers. For each closed subgroup $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$, there corresponds a subfield $K_n$ of $K_\infty$ such that $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$, a cyclic group of order $p^n$. Thus we have a tower of field extensions $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \cup_{n\geq 0} K_n$.

For each integer $n \geq 1$, we choose a primitive $n$th root $\zeta_n$ of 1 so that $\zeta_m^{\frac{m}{n}} = \zeta_n$ whenever $n|m$. For an integer $d$ with $d \not\equiv 2 \mod 4$, let $K = K_0 = \mathbb{Q}(\zeta_{pd})$, $K_n = \mathbb{Q}(\zeta_{p^{n+1}d})$ and $K_\infty = \cup_{n\geq 0} K_n$, where $p$ is a prime satisfying $p \equiv 1 \mod d$. Then $K_\infty$ is a $\mathbb{Z}_p$-extension of $K$. The following theorem tells us the growth of the order of the Sylow $p$-subgroup of the ideal class group of $K_n$.

Theorem A (Iwasawa, Ferrero, Washington [2], [8]). *Let $p^{e_n}$ be the order of the Sylow $p$-subgroup of the ideal class group of*

---

1991 Mathematics Subject Classification: 11R23, 11R18.

Key words and phrases: cyclotomic units, $\mathbb{Z}_p$-extension, Tate cohomology groups.

This paper was supported by research fund of Inha University, 1995.

*$K_n$. Then there exist integers $\lambda \geq 0$ and $\nu$ such that $e_n = \lambda n + \nu$ for all sufficiently large $n$.*

For an arbitrary number field $K$ and its $\mathbb{Z}_p$-extension $K_\infty$, $e_n$ behaves like $e_n = \mu p^n + \lambda n + \nu$ for $n \gg 0$. These constants $\mu$, $\lambda$ and $\nu$ are called the Iwasawa invariants. It is proved by Ferrero and Washington that $\mu$ vanishes when the base field $K$ is abelian and $K_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $K$ as in our case.

By the action of complex conjugation on the ideal class groups, we have the decompositions $e_n = e_n^+ + e_n^-$, $\lambda = \lambda^+ + \lambda^-$ and $\nu = \nu^+ + \nu^-$. And $p^{e_n^+}$ is the order of the Sylow $p$-subgroup of the ideal class group of $K_n^+$, where $K_n^+ = \mathbb{Q}(\zeta_{p^{n+1}d} + \zeta_{p^{n+1}d}^{-1})$ is the maximal real subfield of $K_n$.

The minus parts (e.g. $e_n^-, \lambda^-$) of the ideal class groups are much better understood than the plus parts mainly because of the action of complex conjugation. What we want to do in this paper is to study the plus parts of the ideal class group of $K_n$. When dealing with the plus part, one usually looks at cyclotomic units and that is exactly what we are going to work with. The greatest advantage of cyclotomic units, perhaps, is that the generators of the group of cyclotomic units are given so explicitly that one can play around with them. Another feature of cyclotomic units is the following index theorem:

THEOREM B (W. SINNOTT [7]). *Let $E(C)$ be the group of units (cyclotomic units) of the cyclotomic field $\mathbb{Q}(\zeta_n)$. Let $g$ be the number of distinct prime divisors of $n$. Then $[E : C] = 2^b h^+$, where $b = 0$ if $g = 1$ and $b = 2^{g-2} + 1 - g$ if $g > 1$, and $h^+$ is the class number of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

Let $E_n(C_n)$ be the group of units(cyclotomic units) of $K_n$ and let $A_n(B_n)$ be the Sylow $p$-subgroup of the ideal class group of $K_n^+$ ($E_n/C_n$, respectively). Then the index theorem of W. Sinnott says that $\#A_n = \#B_n$. So it is natural to ask if $A_n$ is isomorphic to $B_n$. This question is still open. In [3], it is proved to be affirmative when $d = 1$ under certain assumptions.

In order to generalize those results in [3] to arbitrary $d$, one needs to compute the Tate cohomology groups of cyclotomic units and to prove the injectivity of the induced map $\widehat{H}^i(G_n, C_n) \longrightarrow \widehat{H}^i(G_n, E_n)$, where $G_n$ is the Galois group $\mathrm{Gal}(K_n/K_0)$. Tate cohomology groups for cyclotomic units are computed in [4], and we review the results briefly. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ and $D$ be the decomposition subgroup for $p$ of $\Delta$. Let $l = \#(\Delta/\pm D)$. Then for any $m > n$, we have

$$\widehat{H}^i(G_{m,n}, C_m) \simeq \begin{cases} (\mathbb{Z}/p^{m-n}\mathbb{Z})^l \text{ if } i \text{ is odd} \\ (\mathbb{Z}/p^{m-n}\mathbb{Z})^{l-1} \text{ if } i \text{ is even,} \end{cases}$$

where $G_{m,n} = \mathrm{Gal}(K_m/K_n)$. In particular, $H^1(G_n, C_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l$.

Above results were computed theoretically without providing explicit generators for $H^1(G_n, C_n)$. But if one wants to study the injectivity of $H^1(G_n, C_n) \longrightarrow H^1(G_n, E_n)$, it is better to have explicit generators of $H^1(G_n, C_n)$. In [5], explicit generators are given when $d = q$ is a prime. And in the same paper and in a later paper [6], several applications are studied concerning the plus part of the ideal class groups and $\lambda^+$.

The aim of the present paper is to provide explicit generators of $H^1(G_{m,n}, C_m)$ when $d = qr$ is a product of two distinct primes. Hopefully these generators yield similar applications to the ideal class groups as in [5] and [6]. We also hope to be able to find out explicit generators for arbitrary $d$ by modifying our proof.

We finish this section by introducing a theorem of V. Ennola([1]) on relations among cyclotomic units.

Theorem C (V. Ennola [1]). *Let $\chi$ be a character of conductor $f$ belonging to $\mathbb{Q}(\zeta_n)$. For each cyclotomic unit $\delta = \prod_{0<a<n} (1-\zeta_n^a)^{x_a}$, define $Y(\chi,\delta)$ by*

$$Y(\chi,\delta) = \sum_{\substack{d \\ f|d|n}} \frac{1}{\varphi(d)} T(\chi, d, \delta) \prod_{p|d} (1 - \overline{\chi}(p)),$$

*where $T(\chi, d, \delta) = \sum_{\substack{a=1 \\ (a,d)=1}}^{d-1} \chi(a) x_{\frac{n}{d}a}$. Then for every even character $\chi \neq 1$, $Y(\chi, \delta) = 0$ if $\delta$ is a root of 1.*

## 2. Preliminary

In this section, we set up notations and prove several lemmas which we will use in the next section.

As in the introduction, $p$ is a prime satisfying $p \equiv 1 \mod d$, where $d = qr$ is a product of two distinct odd primes. Let $\Delta$, $\Delta_q$ and $\Delta_r$ be the Galois groups $\mathrm{Gal}(\mathbb{Q}(\zeta_{qr})/\mathbb{Q})$, $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ respectively. Let $S_q^+(S_r^+)$ be a set of coset representatives of $\Delta_q/\{\pm 1\}$ ($\Delta_r/\{\pm 1\}$, respectively) and let $S_q^- = \Delta_q - S_q^+$ and $S_r^- = \Delta_r - S_r^+$. For convenience, we assume that identity elements of $\Delta_q$ and $\Delta_r$ are in $S_q^+$ and $S_r^+$, respectively. Elements of $S_q^+(S_r^+)$ will be denoted by $\tau_q(\tau_r)$ and those of $S_q^-(S_r^-)$ will be denoted by $\widetilde{\tau}_q(\widetilde{\tau}_r)$. Thus $\{\widetilde{\tau}_q\} = \{-\tau_q\}$, where $-$ is the complex conjugation on $\mathbb{Q}(\zeta_q)$ sending $\zeta_q$ to $\zeta_q^{-1}$. Under the natural isomorphism $\Delta \simeq \Delta_q \times \Delta_r$, let $\Delta^+ = \{\tau_q\tau_r \mid \tau_q \in S_q^+ - \{\mathrm{id}\},\ \tau_r \in S_r^+ - \{\mathrm{id}\}\}$ and $\Delta^- = \{\tau_q\widetilde{\tau}_r \mid \tau_q \in S_q^+,\ \tau_r \in S_r^+\}$. Note that $\Delta \neq \Delta^+ \cup \Delta^-$, since $\#\Delta^+ = (\frac{1}{2}\varphi(q) - 1)(\frac{1}{2}\varphi(r) - 1)$ and $\#\Delta^- = \frac{1}{4}\varphi(q)\varphi(r)$, and thus $\#(\Delta^+ \cup \Delta^-) = \frac{1}{2}\varphi(qr) - \frac{1}{2}\varphi(q) - \frac{1}{2}\varphi(r) + 1$. For later use, we put $\#\Delta^+ = s$, $\#\Delta^- = t$ and $\#(\Delta^+ \cup \Delta^-) = m$.

Nontrivial even (odd) characters of $\Delta_q$ are denoted by $\psi_q$($\theta_q$, respectively) and we use similar notations $\psi_r, \theta_r$ for $\Delta_r$. Thus even characters of $\Delta$ of conductor $qr$ are of the form either $\psi_q\psi_r$ or $\theta_q\theta_r$. Note that$\#\{\psi_q\psi_r\} = (\frac{1}{2}\varphi(q) - 1)(\frac{1}{2}\varphi(r) - 1) = \#\Delta^+ = s$ and that $\#\{\theta_q\theta_r\} = \frac{1}{4}\varphi(qr) = \#\Delta^- = t$.

LEMMA 1. *Let $m$ be as before and let $A$ be an $m \times m$ matrix with entries $\chi(\delta)$, where $\{\chi\}$ is the set of all even characters of $\Delta$ of conductor $qr$ and $\{\delta\} = \Delta^+ \cup \Delta^-$. Then* $\det A \not\equiv 0 \mod p$.

*Proof.* By arranging rows and columns of $A$ suitably, we may assume that $A$ is of the form

$$A = \begin{array}{cc} & \begin{array}{cc} \overbrace{\hphantom{\psi_q(\tau_q)\psi_r(\tau_r)}}^{s} & \overbrace{\hphantom{\psi_q(\tau_q)\psi_r(\widetilde{\tau}_r)}}^{t} \end{array} \\ \begin{array}{c} s\{ \\ t\{ \end{array} & \left(\begin{array}{c|c} \psi_q(\tau_q)\psi_r(\tau_r) & \psi_q(\tau_q)\psi_r(\widetilde{\tau}_r) \\ \hline \theta_q(\tau_q)\theta_r(\tau_r) & \theta_q(\tau_q)\theta_r(\widetilde{\tau}_r) \end{array}\right) \end{array}.$$

Since $\psi_r(\widetilde{\tau}_r) = \psi_r(\tau_r)$ and $\theta_r(\widetilde{\tau}_r) = -\theta_r(\tau_r)$, by adding suitable columns of $A$ to other columns, we have

$$A' = \left( \begin{array}{c|c} 2\psi_q(\tau_q)\psi_r(\tau_r) & \psi_q(\tau_q)\psi_r(\tau_r) \\ \hline \mathbf{0} & -\theta_q(\tau_q)\theta_r(\tau_r) \end{array} \right).$$

Hence $\det A = \det A' = 2^s(-1)^t \det M \det N$, where $M$ is the $s \times s$ matrix with entries $\psi_q(\tau_q)\psi_r(\tau_r)$ and $N$ is the $t \times t$ matrix with entries $\theta_q(\tau_q)\theta_r(\tau_r)$. Note that $M$ and $N$ can be written as tensor products of matrices of smaller sizes as follows:

$$M = (\psi_q(\gamma_q)) \otimes (\psi_r(\gamma_r)), \; N = (\theta_q(\gamma_q)) \otimes (\theta_r(\gamma_r)).$$

Finally one can easily check that these four matrices have nonzero determinants modulo $p$ by applying lemma 1.2 of [5]. □ □

The following Lemma on cyclotomic units follows immediately from V. Ennola's theorem which was introduced in Section 1.

LEMMA 2. *Let $\chi \neq 1$ be an even character of $\mathbb{Q}(\zeta_n)$ and $\delta_1, \delta_2, \delta$ be cyclotomic units in $\mathbb{Q}(\zeta_n)$. Then*

(i) $Y(\chi, \delta_1\delta_2) = Y(\chi, \delta_1) + Y(\chi, \delta_2)$
(ii) *If (root of 1)$\times\delta_1$ =(root of 1)$\times\delta_2$, then* $Y(\chi, \delta_1) = Y(\chi, \delta_2)$
(iii) *For any* $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $Y(\chi, \delta^\sigma) = \chi(\sigma)Y(\chi, \delta)$
(iv) $Y(\chi, \delta^{\sigma-1}) = (\chi(\sigma) - 1)Y(\chi, \delta)$.

## 3. Generators of $H^1(G_{m,n}, C_m)$

Let $K = K_0 = \mathbb{Q}(\zeta_{pd})$, $K_n = \mathbb{Q}(\zeta_{p^{n+1}d})$ and $K_\infty = \cup_{n\geq 0} K_n$ where $d = qr$ and $p \equiv 1 \mod d$. We denote the Galois group $\mathrm{Gal}(K_m/K_n)$ by $G_{m,n}$ and $\mathrm{Gal}(K_n/K_0)$ by simply $G_n$ instead of $G_{n,0}$. And we denote the norm map from $K_m$ to $K_n$ by $N_{m,n}$ and that from $K_n$ to $K_0$ by $N_n$. In this section we will find explicit generators of the cohomology groups $H^1(G_{m,n}, C_m)$ and $H^1(G_n, C_n)$ for $m > n > 0$, where $C_n$ is the group of cyclotomic units of $K_n$. Theoretically, it is known ([4]) that $H^1(G_{m,n}, C_m) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^l$, where $l = \frac{1}{2}\varphi(d)$ is the number of prime ideals of $\mathbb{Q}(\zeta_d + \zeta_d^{-1})$ above $p$.

Let $\sigma$ be the topological generator of the Galois group $\mathrm{Gal}(K_\infty/K_0)$ which sends $\zeta_{p^n}$ to $\zeta_{p^n}^{1+p}$ for all $n \geq 1$. Let $R = \{w \in \mathbb{Z}_p \mid w^{p-1} = 1\}$ be the set of roots of 1 in $\mathbb{Z}_p$. Then $R$ can be thought of as the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ or as any Galois group isomorphic to it. For example $R \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}_n)$, where $\mathbb{Q}_n$ is the subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree $p^n$ over $\mathbb{Q}$.

We need some more notations which we use throughout this section:

$$\begin{aligned}
T_n^+ &= \left\{ \prod_{w\in R} (\zeta_{p^{n+1}}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r}) \mid \tau_q\tau_r \in \Delta^+ \right\} \\
T_n^- &= \left\{ \prod_{w\in R} (\zeta_{p^{n+1}}^w - \zeta_q^{\tau_q}\zeta_r^{\widetilde{\tau}_r}) \mid \tau_q\widetilde{\tau}_r \in \Delta^- \right\} \\
T_{n,q} &= \left\{ \prod_{w\in R} (\zeta_{p^{n+1}}^w - \zeta_q^{\tau_q}) \mid \tau_q \in S_q^+ - \{\mathrm{id}\} \right\} \\
T_{n,r} &= \left\{ \prod_{w\in R} (\zeta_{p^{n+1}}^w - \zeta_r^{\tau_r}) \mid \tau_r \in S_r^+ - \{\mathrm{id}\} \right\} \\
T^+ &= T_1^+,\ T^- = T_1^-,\ T_q = T_{1,q},\ T_r = T_{1,r}.
\end{aligned}$$

Elements of $T_n^+$, $T_n^-$, $T_{n,q}$ and $T_{n,r}$ are denoted by $\delta_n^+$, $\delta_n^-$, $\delta_{n,q}$ and $\delta_{n,r}$ respectively. Thus, for example, $T_n^+ = \{\delta_n^+\}$. We also abbreviate elements of $T^+$, $T^-$, $T_q$ and $T_r$ by $\delta^+$, $\delta^-$, $\delta_q$ and $\delta_r$.

It is easy to check that $\#(T_n^+ \cup T_n^- \cup T_{n,q} \cup T_{n,r}) = \#(\Delta^+ \cup \Delta^-) + (\frac{1}{2}\varphi(q) - 1) + (\frac{1}{2}\varphi(r) - 1) = \frac{1}{2}\varphi(qr) - 1 = l - 1$. By applying the norm map $N_n$ from $K_n$ to $K_0$ to each $\delta$'s, we get 1. For example,

$$\begin{aligned} N_n(\delta_n^+) &= N_n\left(\prod_{w\in R}(\zeta_{p^{n+1}}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r})\right) \\ &= \prod_{w\in R} N_n(\zeta_{p^{n+1}}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r}) \\ &= \prod_{w\in R}(\zeta_p^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r}) \\ &= \frac{1-\zeta_q^{p\tau_q}\zeta_r^{p\tau_r}}{1-\zeta_q^{\tau_q}\zeta_r^{\tau_r}} \\ &= 1. \end{aligned}$$

The last equality holds since $p \equiv 1 \mod qr$. Thus we have $l-1$ cyclotomic units in $C_n$ whose norms to $K_0$ are 1. These elements together with $\pi_n^{\sigma-1}$ will yield a set of generators of $H^1(G_n, C_n)$, where $\pi_n = \zeta_{p^{n+1}} - 1$. We will denote $\pi_1$ by $\pi$.

THEOREM 1. *$H^1(G_1, C_1)$ is generated by $T^+ \cup T^- \cup T_q \cup T_r \cup \{\pi^{\sigma-1}\}$.*

*Proof.* Suppose

$$\begin{aligned} \eta = &\left(\prod_{\delta^+\in T^+}(\delta^+)^{a_{\delta^+}}\right)\left(\prod_{\delta^-\in T^-}(\delta^-)^{a_{\delta^-}}\right)\times \\ &\left(\prod_{\delta_q\in T_q}\delta_q^{a_{\delta_q}}\right)\left(\prod_{\delta_r\in T_r}\delta_r^{a_{\delta_r}}\right)(\pi^{\sigma-1})^b = \xi^{\sigma-1} \qquad (*) \end{aligned}$$

for some $\xi \in C_1$ and for some integers $a_{\delta^+}, a_{\delta^-}, a_{\delta_q}, a_{\delta_r}$ and $b$. Since we know that $H^1(G_1, C_1) \simeq (\mathbb{Z}/p\mathbb{Z})^l$, it is enough to show that $a_{\delta^+} \equiv a_{\delta^-} \equiv a_{\delta_q} \equiv a_{\delta_r} \equiv b \equiv 0 \mod p$. Since we apply $\sigma - 1$ to $\xi$ after all, we may assume that $\xi$ is of the form

$$\xi = \prod_{i,j,k}(\zeta_{p^2}^{\sigma^i w^j} - \zeta_{qr}^k)^{c_{i,j,k}} \times (\text{root of } 1)$$

for some integers $c_{i,j,k}$ with $0 \le i < p, 0 \le j < p-1$ and $0 < k < qr$. By applying Lemma 2 to (*), we have

$$Y(\chi, \eta) = Y(\chi, \xi^{\sigma-1})$$

for every even character $\chi \neq 1$.

The strategy of proving this theorem is as follows. First, we compute both sides when $\chi$ is of the form $\chi = \psi\chi_{qr}$, where $\psi$ is a fixed nontrivial character of $\mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q})$ and $\chi_{qr}$ is an even character of $\Delta$ of conductor $qr$. So $\chi_{qr} = \chi_q\chi_r$ is of the form either $\psi_q\psi_r$ or $\theta_q\theta_r$ under the notation in section 2. By letting $\chi_{qr}$ vary over all such characters, we somehow end up with $a_{\delta^+} \equiv a_{\delta^-} \equiv 0 \mod p$ for all $\delta^+ \in T^+$ and $\delta^- \in T^-$. Then (*) reads as

$$\left(\prod_{\delta_q \in T_q} \delta_q^{a_{\delta_q}}\right)\left(\prod_{\delta_r \in T_r} \delta_r^{a_{\delta_r}}\right)(\pi^{\sigma-1})^b = \xi_1^{\sigma-1}$$

for some $\xi_1 \in C_1$. Then use the same method with characters of the form $\chi = \psi\chi_q$ to prove that $a_{\delta_q} \equiv 0 \mod p$, where $\chi_q$ is a nontrivial even character of $\mathbb{Q}(\zeta_q)$. Similarly, $a_{\delta_r} \equiv 0 \mod p$. Therefore we have

$$(\pi^{\sigma-1})^b = \xi_2^{\sigma-1}$$

for some $\xi_2 \in C_1$. Then, finally, we see that $b \equiv 0 \mod p$.

Thus, the proof of this theorem is going to be a long computation. However we will perform only the first step of the proof. Namely we will only show that $a_{\delta^+} \equiv a_{\delta^-} \equiv 0 \mod p$. The rest of the proof is similar to the first step. And actually the essence of the generalization to the case $d = qr$ of theorem 1 of [5] which treats the case $d = q$ lies in the first step.

So we are going to compute both sides of $Y(\chi, \eta) = Y(\chi, \xi^{\sigma-1})$ when $\chi$ is of the form $\chi = \psi\chi_{qr}$. By applying Theorem $C$ in Section 1, we easily see that $Y(\chi, \delta_q) = Y(\chi, \delta_r) = Y(\chi, \pi^{\sigma-1}) = 0$. Thus by Lemma 2, we get

$$Y(\chi, \eta) = \sum_{\delta^+ \in T^+} a_{\delta^+} Y(\chi, \delta^+) + \sum_{\delta^- \in T^-} a_{\delta^-} Y(\chi, \delta^-).$$

And

$$\begin{aligned} Y(\chi, \delta^+) &= Y(\psi\chi_{qr}, \prod_{w \in R}(\zeta_{p^2}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r})) \\ &= \sum_w Y(\psi\chi_{qr}, \zeta_{p^2}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r}). \end{aligned}$$

Since $\zeta_{p^2}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r} = \zeta_{p^2}^w(1-\zeta_{p^2qr}^{-wqr+p^2r\tau_q+p^2q\tau_r})$, we have

$$\begin{aligned}Y(\psi\chi_{qr}, \zeta_{p^2}^w - \zeta_q^{\tau_q}\zeta_r^{\tau_r}) &= \frac{1}{\varphi(p^2qr)}\psi\chi_{qr}(-wqr+p^2r\tau_q+p^2q\tau_r) \\ &= \frac{1}{\varphi(p^2qr)}\psi(qr)\chi_q(p^2r\tau_q)\chi_r(p^2q\tau_r).\end{aligned}$$

Since $p \equiv 1 \mod qr$, $\chi_q(p) = \chi_r(p) = 1$. Therefore

$$\begin{aligned}Y(\chi, \delta^+) &= \sum_w \frac{1}{\varphi(p^2qr)}\psi(qr)\chi_q(r)\chi_r(q)\chi_{qr}(\tau_q\tau_r) \\ &= (p-1)\frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2qr)}\chi_{qr}(\tau_q\tau_r).\end{aligned}$$

Similarly,

$$Y(\chi, \delta^-) = (p-1)\frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2qr)}\chi_{qr}(\tau_q\widetilde{\tau}_r).$$

Hence

$$\begin{aligned}Y(\chi, \eta) =&(p-1)\frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2qr)}\times \\ &\left(\sum_{\delta^+\in T^+} a_{\delta^+}\chi_{qr}(\tau_q\tau_r) + \sum_{\delta^-\in T^-} a_{\delta^-}\chi_{qr}(\tau_q\widetilde{\tau}_r)\right).\end{aligned}$$

On the other hand,

$$\begin{aligned}Y(\chi, \xi^{\sigma-1}) &= (\chi(\sigma)-1)Y(\chi, \xi) \\ &= (\chi(\sigma)-1)\sum_{i,j,k} c_{i,j,k}Y(\chi, \zeta_{p^2}^{\sigma^i w^j} - \zeta_{qr}^k).\end{aligned}$$

If $(k, qr) \neq 1$, then $Y(\chi, \zeta_{p^2}^{\sigma^i w^j} - \zeta_{qr}^k) = 0$ when $\chi = \psi\chi_{qr}$. Therefore, in the above sum, we may assume $(k, qr) = 1$ and so we may write

$k = mq + nr$ with $1 \le m \le p-1,\ 1 \le n \le q-1$. Thus

$$\begin{aligned}
Y(\chi, \zeta_{p^2}^{\sigma^i w^j} - \zeta_{qr}^{k}) &= Y(\psi\chi_{qr}, \zeta_{p^2}^{\sigma^i w^j} - \zeta_q^n \zeta_r^m) \\
&= Y(\psi\chi_{qr}, 1 - \zeta_{p^2 qr}^{-\sigma^i w^j qr + p^2 nr + p^2 mq}) \\
&= \frac{1}{\varphi(p^2 qr)} \psi\chi_{qr}(-\sigma^i w^j qr + p^2 nr + p^2 mq) \\
&= \frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2 qr)} \psi(\sigma^i)\chi_q(n)\chi_r(m).
\end{aligned}$$

Therefore

$$\begin{aligned}
Y(\chi, \xi^{\sigma-1}) = (\chi(\sigma) - 1) &\frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2 qr)} \times \\
&\sum_{i,j,m,n} c_{i,j,m,n} \psi(\sigma^i)\chi_q(n)\chi_r(m).
\end{aligned}$$

Put $\sum_{i,j,m,n} c_{i,j,m,n}\psi(\sigma^i)\chi_q(n)\chi_r(m) = \beta(\chi_{qr})$, an algebraic integer depending on $\chi_{qr}$. Then

$$Y(\chi, \xi^{\sigma-1}) = (\chi(\sigma) - 1)\frac{\psi(qr)\chi_q(r)\chi_r(q)}{\varphi(p^2 qr)} \beta(\chi_{qr}).$$

By equating the two results for $Y(\chi, \eta)$ and $Y(\chi, \xi^{\sigma-1})$, we obtain

$$\begin{aligned}
(p-1)\left(\sum_{\delta^+ \in T^+} a_{\delta^+}\chi_{qr}(\tau_q\tau_r) + \sum_{\delta^- \in T^-} a_{\delta^-}\chi_{qr}(\tau_q\widetilde{\tau}_r)\right)& \\
= (\chi(\sigma) - 1)\beta(\chi_{qr}) = (\psi(\sigma) - 1)\beta(\chi_{qr}).&
\end{aligned}$$

By letting $\chi_{qr}$ vary over all nontrivial even characters of conductor $qr$, we have a system of linear equations

$$(p-1)A \begin{pmatrix} \vdots \\ a_{\delta^+} \\ \vdots \\ a_{\delta^-} \\ \vdots \end{pmatrix} = (\psi(\sigma) - 1) \begin{pmatrix} \vdots \\ \beta(\chi_{qr}) \\ \vdots \end{pmatrix},$$

where $A$ is the matrix in Lemma 1. Since the principal ideal $(\psi(\sigma)-1)$ lies above $p$ and since $\det A \not\equiv 0 \mod p$ by Lemma 1, we must have

$$\begin{pmatrix} \vdots \\ a_{\delta^+} \\ \vdots \\ a_{\delta^-} \\ \vdots \end{pmatrix} \equiv \begin{pmatrix} \vdots \\ 0 \\ \vdots \end{pmatrix} \mod p.$$

Therefore $a_{\delta^+} \equiv a_{\delta^-} \equiv 0 \mod p$ as desired. □ □

Now we generalize Theorem 1 to the case $H^1(G_n, C_n)$ for $n \geq 1$.

THEOREM 2. *$H^1(G_n, C_n)$ is generated by $T_n^+ \cup T_n^- \cup T_{n,q} \cup T_{n,r} \cup \{\pi_n^{\sigma-1}\}$.*

*Proof.* We prove this by induction on $n$. Theorem 1 takes case of the case $n = 1$. So we will prove the theorem for $n$ with assuming the result for $n-1$. Thus $H^1(G_{n-1}, C_{n-1})$ is generated by $T_{n-1}^+ \cup T_{n-1}^- \cup T_{n-1,q} \cup T_{n-1,r} \cup \{\pi_{n-1}^{\sigma-1}\}$.

As in the proof of Theorem 1, suppose that

$$(**) \quad \begin{aligned} \eta = &\left(\prod_{\delta_n^+ \in T_n^+} (\delta_n^+)^{a_{\delta_n^+}}\right) \left(\prod_{\delta_n^- \in T_n^-} (\delta_n^-)^{a_{\delta_n^-}}\right) \times \\ &\left(\prod_{\delta_{n,q} \in T_{n,q}} (\delta_{n,q})^{a_{\delta_q}}\right) \left(\prod_{\delta_{n,r} \in T_{n,r}} (\delta_{n,r})^{a_{\delta_r}}\right) (\pi_n^{\sigma-1})^b = \xi^{\sigma-1} \end{aligned}$$

for some $\xi \in C_n$. We have to show that $a_{\delta_n^+} \equiv a_{\delta_n^-} \equiv a_{\delta_q} \equiv a_{\delta_r} \equiv b \equiv 0 \mod p^n$.

Since $N_{n,n-1}(\delta_n^{\pm}) = \delta_{n-1}^{\pm}$, $N_{n,n-1}(\delta_{n,q}) = \delta_{n-1,q}$, $N_{n,n-1}(\delta_{n,r}) =$

$\delta_{n-1,r}$ and $N_{n,n-1}(\pi_n)=\pi_{n-1}$, we have

$$\begin{aligned}N_{n,n-1}(\eta) = &\left(\prod_{\delta^+_{n-1}\in T^+_{n-1}}(\delta^+_{n-1})^{a_{\delta^+_n}}\right)\left(\prod_{\delta^-_{n-1}\in T^-_{n-1}}(\delta^-_{n-1})^{a_{\delta^-_n}}\right)\times\\ &\left(\prod_{\delta_{n-1,q}\in T_{n-1,q}}(\delta_{n-1,q})^{a_{\delta_q}}\right)\left(\prod_{\delta_{n-1,r}\in T_{n-1,r}}(\delta_{n-1,r})^{a_{\delta_r}}\right)(\pi^{\sigma-1}_{n-1})^b\\ = &(N_{n,n-1}\xi)^{\sigma-1}.\end{aligned}$$

Hence $a_{\delta^+_n}\equiv a_{\delta^-_n}\equiv a_{\delta_q}\equiv a_{\delta_r}\equiv b\equiv 0 \mod p^{n-1}$ by the induction hypothesis. So we can write $a_{\delta^+_n}=p^{n-1}a_+$, $a_{\delta^-_n}=p^{n-1}a_-$, $a_{\delta_q}=p^{n-1}a_q$, $a_{\delta_r}=p^{n-1}a_r$ and $b=p^{n-1}c$ for some integers $a_+,a_-,a_q,a_r$ and $c$. Note that

$$\begin{aligned}(\delta^+_n)^{p^{n-1}} &= \prod_w(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)^{p^{n-1}}\\ &= \prod_w\left(N_{n,1}(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)\frac{(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)^{p^{n-1}}}{N_{n,1}(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)}\right)\\ &= \prod_w(\zeta^w_{p^2}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)\prod_w\prod_{\substack{t\\0\le t<p^{n-1}}}\left(\frac{\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r}{(\zeta^{w\sigma^{tp}}_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)}\right)\\ &= \delta^+_1\prod_w\prod_t(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)^{1-\sigma^{tp}}\\ &= \delta^+_1u^{\sigma-1}_{\delta^+_n},\end{aligned}$$

where $u_{\delta^+_n}=\prod_w\prod_t(\zeta^w_{p^{n+1}}-\zeta^{\tau_q}_q\zeta^{\tau_r}_r)^{\frac{1-\sigma^{tp}}{\sigma-1}}\in C_n$. Similarly, $(\delta^-_n)^{p^{n-1}}=\delta^-_1u^{\sigma-1}_{\delta^-_n}$, $(\delta_{n,q})^{p^{n-1}}=\delta_{1,q}u^{\sigma-1}_{\delta_{n,q}}$, $(\delta_{n,r})^{p^{n-1}}=\delta_{1,r}u^{\sigma-1}_{\delta_{n,r}}$ and $\pi^{p^{n-1}}_n=\pi_1u_\pi$ for some $u_{\delta^-_n},u_{\delta_{n,q}},u_{\delta_{n,r}}$ and $u_\pi\in C_n$. Hence (**) reads

$$\begin{aligned}&\left(\prod_{\delta^+_1\in T^+_1}(\delta^+_1)^{a_+}\right)\left(\prod_{\delta^-_1\in T^-_1}(\delta^-_1)^{a_-}\right)\left(\prod_{\delta_{1,q}\in T_{1,q}}(\delta_{1,q})^{a_q}\right)\times\\ &\left(\prod_{\delta_{1,r}\in T_{1,r}}(\delta_{1,r})^{a_r}\right)(\pi^{\sigma-1}_1)^c={\xi'}^{\sigma-1}\end{aligned}$$

for some $\xi' \in C_n$. Therefore, we have an element in $C_1$ whose norm to $K_0$ equals 1, which also lies in $C_n^{\sigma-1}$. But since the inflation map $H^1(G_1, C_1) \to H^1(G_n, C_n)$ is injective, the left hand side of the above equation must be in $C_1^{\sigma-1}$. In this case, we already know that $a_+ \equiv a_- \equiv a_q \equiv a_r \equiv c \equiv 0 \mod p$ by theorem 1. Therefore $a_{\delta_n^+} \equiv a_{\delta_n^-} \equiv a_{\delta_q} \equiv a_{\delta_r} \equiv b \equiv 0 \mod p^n$. □ □

Finally, we generalize Theorem 2 to arbitrary case.

THEOREM 3. *Let* $\sigma_n = \frac{\sigma^{p^n}-1}{\sigma-1} = 1+\sigma+\sigma^2+\cdots+\sigma^{p^n-1}$. *For* $m > n$, *define* $(T_m^+)^{\sigma_n}$ *by* $(T_m^+)^{\sigma_n} = \{(\delta_m^+)^{\sigma_n} \mid \delta_m^+ \in T_m^+\}$. *And we define* $(T_m^-)^{\sigma_n}$, $T_{m,q}^{\sigma_n}$ *and* $T_{m,r}^{\sigma_n}$ *similarly. Then* $H^1(G_{m,n}, C_m)$ *is generated by*

$$(T_m^+)^{\sigma_n} \cup (T_m^-)^{\sigma_n} \cup T_{m,q}^{\sigma_n} \cup T_{m,r}^{\sigma_n} \cup \{\pi_m^{\sigma^{p^n}-1}\}.$$

*Proof.* Since $H^1(G_{m,n}, C_m) \simeq \mathrm{Im}(H^1(G_m, C_m) \overset{\mathrm{res}}{\to} H^1(G_{m,n}, C_m))$, $H^1(G_{m,n}, C_m)$ is generated by $\mathrm{res}\{T_m^+ \cup T_m^- \cup T_{m,q} \cup T_{m,r} \cup \{\pi_m^{\sigma-1}\}\}$. Applying restriction maps to various $\delta$'s is same as applying $\sigma_n$ to $\delta$'s, *i.e.*, $\mathrm{res}(\delta_m^+) = (\delta_m^+)^{\sigma_n}$. Therefore $H^1(G_{m,n}, C_m)$ is generated by the set given in the theorem. □ □

## References


1. V. Ennola, *On relations between cyclotomic units*, J. Number Theory **4** (1972), 236–247.
2. B. Ferrero and L. Washington, *The Iwasawa invariant $\mu_p$ vanishes for abelian number fields*, Ann. Math. **109** (1979), 377–395.
3. J.M. Kim, S. Bae, I.S. Lee, *Cyclotomic units in $\mathbb{Z}_p$-extensions*, Israel J. Math. **75** (1991), 161–165.
4. J.M. Kim, *Cohomology group of cyclotomic units*, J. Algebra **152** (1992), 514–519.
5. J.M. Kim, *Units and Cyclotomic units in $\mathbb{Z}_p$-extensions*, Nagoya Math. J. **140** (1995), 101–116.
6. J.M. Kim, *Class numbers of certain real abelian fields*, Acta Arith. **LXXII 4** (1995), 335–345.
7. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. Math. **(2) 108** (1978), 107–134.

8. L. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1980.

Department of Mathematics
Inha University
Incheon 402-751, Korea
*E-mail*: jmkim@munhak.inha.ac.kr