Tohoku Math. J.
51 (1999), 305–313

CIRCULAR UNITS IN THE Z_p-EXTENSIONS OF REAL ABELIAN FIELDS OF PRIME CONDUCTOR

JAE MOON KIM

(Received March 16, 1998, revised November 6, 1998)

Abstract. The aim of this paper is to compute the cohomology groups of circular units in the $\boldsymbol{Z}_p$-extensions of a real abelian field of prime conductor. Even though the generators of circular units are described very complicatedly, their cohomology groups turn out to be as simple as one can expect compared to the cohomology groups of full unit group found by Iwasawa.

1. Introduction and notation. Let ζ_n be a primitive n-th root of 1 and P_n the multiplicative subgroup of $\boldsymbol{Q}(\zeta_n)^\times$ generated by $\{\pm 1\}$ and $\{1 - \zeta_n^a | 0 < a < n\}$. Then the group $C_{\boldsymbol{Q}(\zeta_n)}$ of cyclotomic units of $\boldsymbol{Q}(\zeta_n)$ is defined to be

$$C_{\boldsymbol{Q}(\zeta_n)} = E_{\boldsymbol{Q}(\zeta_n)} \cap P_n\,,$$

where $E_{\boldsymbol{Q}(\zeta_n)}$ is the unit group of $\boldsymbol{Q}(\zeta_n)$. The group of cyclotomic units enjoys many important properties such as the index theorem (cf. [7]). In general, for an abelian field F, Sinnott [6] defines the group of circular units of F as follows: For each $n > 2$, let

$$F'_n = F \cap \boldsymbol{Q}(\zeta_n) \quad \text{and} \quad C_{F'_n} = N_{\boldsymbol{Q}(\zeta_n)/F'_n}(C_{\boldsymbol{Q}(\zeta_n)})\,.$$

Then the group C_F of circular units of F is defined to be the multiplicative subgroup of $F^\times$ generated by $C_{F'_n}$ for all $n > 2$ together with -1. Note that if n is prime to the conductor of F, then $F'_n = \boldsymbol{Q}$ and so $C_{F'_n} = \{1\}$. Thus there are only finitely many n's to be considered in the definition of C_F.

Let k be a real subfield of $\boldsymbol{Q}(\zeta_q)$ for an odd prime q and $k_\infty = \bigcup_{n\geq 0} k_n$ the $\boldsymbol{Z}_p$-extension of $k = k_0$ for an odd prime p with $(p, q) = 1$. Here, k_n means the n-th layer of the $\boldsymbol{Z}_p$-extension, not $k \cap \boldsymbol{Q}(\zeta_n)$. For each $n \geq 0$, we denote the group of circular units of k_n by C_n. Then the index theorem of Sinnott says the following:

INDEX THEOREM (Sinnott [6]). *Let E_n be the unit group of k_n, and h_n the class number of k_n. Then $[E_n : C_n] = 2^{c_n} h_n$ for some integer c_n.*

For each integer $s \geq 1$, we choose a primitive s-th root ζ_s of 1 so that $\zeta_t^{t/s} = \zeta_s$ if $s|t$. Let $K = \boldsymbol{Q}(\zeta_q)$, $F = \boldsymbol{Q}(\zeta_p)$ and $K' = \boldsymbol{Q}(\zeta_{pq})$. We denote their cyclotomic $\boldsymbol{Z}_p$-extensions by K_∞, F_∞, and K'_∞, respectively. Let σ be the topological generator of the Galois group $\Gamma = \mathrm{Gal}(K'_\infty/K')$ which maps ζ_{p^n} to $\zeta_{p^n}^{1+p}$ for all $n \geq 1$. Restrictions of σ to various subfields are also denoted by σ. Let $k_{(p)}$ be the decomposition subfield of k

1991 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R18.
This paper was supported by Korea Research Foundation 1996.

for p and let $\Delta = \mathrm{Gal}(K/k)$, $\bar{\Delta} = \mathrm{Gal}(K/\boldsymbol{Q})$, $\Delta_p = \mathrm{Gal}(K/k_{(p)})$, $\Delta_k = \mathrm{Gal}(k/\boldsymbol{Q})$ and $\Delta_{k,p} = \mathrm{Gal}(k_{(p)}/\boldsymbol{Q})$. Let $[k : \boldsymbol{Q}] = d$ and $[k_{(p)} : \boldsymbol{Q}] = l$, so there are l prime ideals in k above p. Elements of Δ, $\bar{\Delta}$ or Δ_p will be denoted by τ's, and those of Δ_k and $\Delta_{k,p}$ by ρ's. The Frobenius automorphism of K for p or its restriction to k is denoted by τ_p. Let R be the set of all roots of 1 in the ring of the p-adic integers, i.e., $R = \{\omega \in \boldsymbol{Z}_p | \omega^{p-1} = 1\}$. Then R can be regarded as the Galois group $\mathrm{Gal}(F/\boldsymbol{Q})$ or any Galois group isomorphic to it such as $\mathrm{Gal}(F_n/\boldsymbol{Q}_n)$, where $\boldsymbol{Q}_n$ is the subfield of F_n of degree p^n over $\boldsymbol{Q}$. For $m > n$, let $G_{m,n}$ be the Galois group $\mathrm{Gal}(K'_m/K'_n)$ and $N_{m,n}$ the norm map $N_{K'_m/K'_n}$ from K'_m to K'_n. We will abbreviate $G_{m,0}$ and $N_{m,0}$ by G_m and N_m, respectively. $G_{m,n}$ will also mean the Galois groups $\mathrm{Gal}(k_m/k_n)$, $\mathrm{Gal}(F_m/F_n)$ and $\mathrm{Gal}(\boldsymbol{Q}_m/\boldsymbol{Q}_n)$. Similarly, $N_{m,n}$ will have various meanings. Finally we fix a generator ψ_n of the character group of $\mathrm{Gal}(\boldsymbol{Q}_n/\boldsymbol{Q})$ such that $\psi_n(\sigma) = \zeta_{p^n}$. In this paper, we will compute the following cohomology groups of circular units.

THEOREM. *Suppose $p \nmid d = [k : \boldsymbol{Q}]$. Then, for $m > n \geq 0$, we have the following.*

$$C_m^{G_{m,n}} = C_n, \tag{1}$$

$$\hat{H}^0(G_{m,n}, C_m) \simeq (\boldsymbol{Z}/p^{m-n}\boldsymbol{Z})^{l-1}, \tag{2}$$

$$\hat{H}^{-1}(G_{m,n}, C_m) \simeq (\boldsymbol{Z}/p^{m-n}\boldsymbol{Z})^{l}. \tag{3}$$

Since $G_{m,n}$ is cyclic, all the other Tate cohomology groups are isomorphic to one of (2) and (3). Cohomology groups of circular units over arbitrary real abelian fields are still unknown except when k is a real quadratic field (cf. [4]) and when $k = \boldsymbol{Q}(\zeta_q + \zeta_q^{-1})$ is the maximal real subfield of $\boldsymbol{Q}(\zeta_q)$ (cf. [3]).

We finish this section with a theorem of Ennola on relations of cyclotomic units which will be useful in subsequent sections.

THEOREM (Ennola [1]). *Suppose $\delta = \prod_{1 \leq a < n}(1 - \zeta_n^a)^{x_a}$ is a root of 1 for some integers x_a. Then for any even character χ of conductor n, $Y(\chi, \delta) = 0$, where $Y(\chi, \delta) = \sum_{1 \leq a < n} \chi(a) x_a$.*

2. Lemmas. In this section, we prove a series of lemmas that we need in the proof of the theorem in Section 1.

LEMMA 1. *Let χ be an even character of conductor n, and δ_1, δ_2, δ cyclotomic units in $\boldsymbol{Q}(\zeta_n)$. Then*

$$Y(\chi, \delta_1\delta_2) = Y(\chi, \delta_1) + Y(\chi, \delta_2), \tag{1}$$

$$Y(\chi, \delta^\gamma) = \chi(\gamma) Y(\chi, \delta) \textit{ for any } \gamma \in \mathrm{Gal}(\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}). \tag{2}$$

PROOF. These two follow immediately from the definition of Y.

In computing cohomology groups, we will often see circular units of k_n of the forms

$$\prod_{\omega \in R, \tau \in \Delta} (\zeta_{p^{n+1}}^{a\omega} - \zeta_q^{b\tau}), \qquad \prod_{\omega \in R, \tau \in \Delta_p} (\zeta_{p^{n+1}}^{a\omega} - \zeta_q^{b\tau}), \quad \text{and} \quad \prod_a \prod_{\omega \in R} (\zeta_{p^{n+1}}^{a\omega} - 1)^{x_a}.$$

We summarize their values $Y(\chi\psi_n^j, *)$ for $\chi \in \widehat{\Delta_k}$ or $\chi \in \widehat{\Delta_{k,p}}$ in the following lemma.

LEMMA 2. *For $\chi \neq 1$ and for every $1 \leq j \leq p^n$ with $(j, p) = 1$, we have*

(1)

$$Y\left(\chi\psi_n^j, \prod_{\omega\in R,\tau\in\Delta}(\zeta_{p^{n+1}}^{a\omega} - \zeta_q^{b\tau})\right) = (p-1)\#(\Delta)\chi(bp^{n+1})\psi_n^j(aq) \quad \textit{for } \chi \in \widehat{\Delta_k}$$

(2)

$$Y\left(\chi\psi_n^j, \prod_{\omega\in R,\tau\in\Delta_p}(\zeta_{p^{n+1}}^{a\omega} - \zeta_q^{b\tau})\right) = (p-1)\sharp(\Delta_p)\chi(b)\psi_n^j(aq) \quad \textit{for } \chi \in \widehat{\Delta_{k,p}}$$

(3)

$$Y\left(\chi\psi_n^j, \prod_a\prod_{\omega\in R}(\zeta_{p^{n+1}}^{a\omega} - 1)^{x_a}\right) = 0 \quad \textit{for } \chi \in \widehat{\Delta_k}\,.$$

PROOF. Since the proofs for (2) and (3) are similar to that of (1), we will only prove (1).

Note that

$$\begin{aligned}\prod_{\omega\in R,\tau\in\Delta}(\zeta_{p^{n+1}}^{a\omega} - \zeta_q^{b\tau}) &= \prod_{\omega\in R,\tau\in\Delta}\zeta_{p^{n+1}}^{a\omega}(1 - \zeta_{p^{n+1}}^{-a\omega}\zeta_q^{b\tau})\\ &= (\text{root of } 1) \times \prod_{\omega\in R,\tau\in\Delta}(1 - \zeta_{p^{n+1}q}^{-a\omega q + b\tau p^{n+1}})\,.\end{aligned}$$

Since $Y(\chi\psi_n^j$, root of 1) $= 0$, we have

$$\begin{aligned}Y\left(\chi\psi_n^j, \prod_{\omega\in R,\tau\in\Delta}(\zeta_{p^n+1}^{a\omega} - \zeta_q^{b\tau})\right) &= \sum_{\omega\in R,\tau\in\Delta} Y(\chi\psi_n^j, 1 - \zeta_{p^{n+1}q}^{-a\omega q + b\tau p^{n+1}})\\ &= \sum_{\omega\in R,\tau\in\Delta}\chi\psi_n^j(-a\omega q + b\tau p^{n+1})\\ &= \sum_{\omega\in R,\tau\in\Delta}\chi(bp^{n+1})\psi_n^j(aq)\\ &= (p-1)\#(\Delta)\chi(bp^{n+1})\psi_n^j(aq)\,.\end{aligned}$$

In the following lemma we solve a system of linear equations involving characters of $\mathrm{Gal}(k_n/\boldsymbol{Q})$.

LEMMA 3. *Suppose that integers $a_{l,k,i}$ satisfy*

$$\sum_{\substack{0\leq l<p^n\\ 0\leq k<p\\ \rho_i\in\Delta_k}} a_{l,k,i}\psi_{n+1}^j(\sigma^{l+kp^n})\chi(\rho_i) = 0$$

for all j with $1 \leq j < p^{n+1}$, $(j, p) = 1$ *and for all nontrivial characters* $\chi \in \widehat{\Delta_k}$. *Then*

$$a_{l,k,i} = \begin{cases} e_{0,i} + e & \text{if } l = k = 0, \\ e_{l,i} & \text{otherwise} \end{cases}$$

for some integers $e_{l,i}$ *and* e.

PROOF. Write the equation as

$$\sum_{\rho_i \in \Delta_k} \left(\sum_{\substack{0 \leq l < p^n \\ 0 \leq k < p}} a_{l,k,i} \psi^j_{n+1}(\sigma^{l+kp^n}) \right) \chi(\rho_i) = 0 .$$

Let $b_i = \sum_{l,k} a_{l,k,i} \psi^j_{n+1}(\sigma^{l+kp^n})$. As χ runs through all the nontrivial characters of $\widehat{\Delta_k}$, we have $d - 1$ equations in d unknowns $b_1, \cdots, b_d$. Since the $(d-1) \times d$ matrix with entries $\chi(\rho_i)$ is of rank $d - 1$, the solution space is of one-dimensional. Since $b_1 = \cdots = b_d = 1$ is a solution, the general solution is of the form $b_1 = \cdots = b_d = e$ for some e.

Fix i and put $a_{l,k,i} = c_{l,k}$. Then we have

$$\sum_{\substack{0 \leq l < p^n \\ 0 \leq k < p}} c_{l,k} \psi^j_{n+1}(\sigma^{l+kp^n}) = e .$$

As j varies, this gives a system of $p^{n+1} - p^n$ linear equations in p^{n+1} unknowns $\{c_{l,k} \mid 0 \leq l < p^n,\ 0 \leq k < p\}$. Let A be the $(p^{n+1} - p^n) \times p^{n+1}$ matrix with entries $\psi^j_{n+1}(\sigma^{l+kp^n})$. Then the equation reads $AX = E$, where $X = (\cdots, c_{l,k}, \cdots)^t$ and $E = (e, \cdots, e)^t$. Clearly, $X_0 = (e, 0, \cdots, 0)^t$ is a solution of $AX = E$. So the general solution for $AX = E$ is given by $X = X_0 + Y$ with $AY = \boldsymbol{O}$. Since the rank of A is $p^{n+1} - p^n$, the rank of solutions of $AY = \boldsymbol{O}$ must be p^n. For each s, $0 \leq s \leq p^n$, let $Y_s = (\cdots, f_{l,k}, \cdots)^t$ be such that

$$f_{l,k} = \begin{cases} 0 & \text{if } l \neq s , \\ 1 & \text{if } l = s . \end{cases}$$

Then Y_s is a solution since $\sum_{0 \leq k < p} \psi^j_{n+1}(\sigma^{s+kp^n}) = 0$ for all j. Since $\{Y_s \mid 0 \leq s < p^n\}$ is independent, this set provides all the solutions to $AY = \boldsymbol{O}$. Hence, the solutions for $AX = E$ is

$$X = X_0 + \sum_{0 \leq s < p^n} e_s Y_s .$$

Therefore

$$a_{l,k,i} = c_{l,k} = \begin{cases} e_{0,i} + e & \text{if } l = k = 0, \\ e_{l,i} & \text{otherwise} . \end{cases}$$

In the next two lemmas, we examine C_n for $n \geq 0$.

LEMMA 4. *For* $m > n \geq 0$, $C_n = C_0 N_{m,n} C_m$.

PROOF. Clearly, $C_n \supset C_0 N_{m,n} C_m$. To prove the converse, note that an element u of C_n can be written as $u = u_0 u_1 \cdots u_n$, where for each $k \geq 1$, u_k is of the form

$$u_k = \prod_{\omega \in R, \tau \in \Delta} (\zeta_{p^{k+1}}^{\omega} - \zeta_q^{\tau})^{\sum_{i, \rho_j \in \Delta_k} a_{i,j} \sigma^i \rho_j} \prod_{\omega \in R} (\zeta_{p^{k+1}}^{\omega} - 1)^{\sum_i b_i \sigma^i} .$$

Since

$$N_{m,k} \left(\prod_{\omega, \tau} (\zeta_{p^{m+1}}^{\omega} - \zeta_q^{\tau}) \right) = \prod_{\omega, \tau} (\zeta_{p^{k+1}}^{\omega} - \zeta_q^{\tau p^{m-k}}) ,$$

we have

$$\begin{aligned} \prod_{\omega, \tau} (\zeta_{p^{k+1}}^{\omega} - \zeta_q^{\tau}) &= \prod_{\omega, \tau} (\zeta_{p^{k+1}}^{\omega} - \zeta_q^{\tau p^{m-k}})^{\tau_p^{k-m}} \\ &= N_{m,k} \left(\prod_{\omega, \tau} (\zeta_{p^{m+1}}^{\omega} - \zeta_q^{\tau}) \right)^{\tau_p^{k-m}} \\ &= N_{m,n} \left(\prod_{\omega, \tau} (\zeta_{p^{m+1}}^{\omega} - \zeta_q^{\tau}) \right)^{\tau_p^{k-m} \sum_{0 \leq i < p^{n-k}} \sigma^{i p^k}} . \end{aligned}$$

Similarly,

$$\prod_{\omega \in R} (\zeta_{p^{k+1}}^{\omega} - 1) = N_{m,k} \left(\prod_{\omega \in R} (\zeta_{p^{m+1}}^{\omega} - 1) \right) = N_{m,n} \left(\prod_{\omega \in R} (\zeta_{p^{m+1}}^{\omega} - 1) \right)^{\sum_{0 \leq i < p^{n-k}} \sigma^{i p^k}} .$$

So $u_k \in N_{m,n} C_m$ for each $k \geq 1$ and thus $u \in C_0 N_{m,n} C_m$.

LEMMA 5. $\operatorname{rank} N_{k/k_{(p)}} C_0 = l - 1$.

PROOF. Note that the group of circular units of $k_{(p)}$ is generated by -1 and $N_{k/k_{(p)}} C_0$. Thus $N_{k/k_{(p)}} C_0$ is of finite index in the full unit group $E_{k_{(p)}}$ of $k_{(p)}$ by the index theorem of Sinnott [6]. Therefore, $\operatorname{rank} N_{k/k_{(p)}} C_0 = \operatorname{rank} E_{k_{(p)}} = l - 1$.

3. Computation of $C_m^{G_{m,n}}$.

Clearly, $C_n \subset C_m^{G_{m,n}}$. For the converse, it is enough to check when $m = n + 1$, i.e., $C_{n+1}^{G_{n+1,n}} \subset C_n$. Take $u \in C_{n+1}^{G_{n+1,n}}$. We can write u as

$$u = u_n \prod_{\substack{\omega \in R, \tau \in \Delta \\ 0 \leq l < p^n, 0 \leq k < p \\ \rho_i \in \Delta_k}} (\zeta_{p^{n+2}}^{\sigma^{l+kp^n} \omega} - \zeta_q^{\rho_i \tau})^{a_{l,k,i}} \prod_{\omega, l, k} (\zeta_{p^{n+2}}^{\sigma^{l+kp^n} \omega} - 1)^{b_{l,k}}$$

for some $u_n \in C_n$ and integers $a_{l,k,i}, b_{l,k}$. Since $u^{\sigma^{p^n}} = u$, we may assume $u_n = 1$. Now apply Lemma 1 and Lemma 2 to the relation $u^{\sigma^{p^n}} = u$ with characters of the form $\psi_{n+1}^j \chi$ with $1 \leq j \leq p^{n+1}$, $(j, p) = 1$ and nontrivial characters $\chi \in \widehat{\Delta_k}$ to obtain

$$\sum_{\omega, \tau, l, k, i} a_{l,k,i} \psi_{n+1}^j (\sigma^{l+kp^n} q) \chi(p^{n+2} \rho_i) = 0 .$$

Therefore

$$\sum_{l,k,i} a_{l,k,i}\psi_{n+1}^{j}(\sigma^{l+kp^n})\chi(\rho_i)=0\,.$$

Hence by Lemma 3,

$$a_{l,k,i}=\begin{cases} e_{0,i}+e & \text{if } l=k=0\,,\\ e_{l,i} & \text{otherwise}\,.\end{cases}$$

Thus

$$\begin{aligned} u={}&\prod_{\substack{l\neq 0\\ k,\omega,\tau,i}}(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega}-\zeta_q^{\rho_i\tau})^{e_{l,i}}\prod_{\substack{k\neq 0,l=0\\ i,\omega,\tau}}(\zeta_{p^{n+2}}^{\sigma^{kp^n}\omega}-\zeta_q^{\rho_i\tau})^{e_{0,i}}\prod_{\substack{l=k=0\\ i,\omega,\tau}}(\zeta_{p^{n+2}}^{\omega}-\zeta_q^{\rho_i\tau})^{e_{0,i}+e}\\ &\times\prod_{\omega,l,k}(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega}-1)^{b_{l,k}}\\ ={}&\prod_{\substack{l\neq 0\\ k,\omega,\tau,i}}(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega}-\zeta_q^{\rho_i\tau})^{e_{l,i}}\prod_{\substack{0\leq k<p\\ i,\omega,\tau}}(\zeta_{p^{n+2}}^{\sigma^{kp^n}\omega}-\zeta_q^{\rho_i\tau})^{e_{0,i}}\prod_{i,\omega,\tau}(\zeta_{p^{n+2}}^{\omega}-\zeta_q^{\rho_i\tau})^{e}\\ &\times\prod_{\omega,l,k}(\zeta_{p^{n+2}}^{\sigma^{l+kp^n}\omega}-1)^{b_{l,k}}\,.\end{aligned}$$

Note that the first two products in the above expression are elements in C_n, while the last two are in $\boldsymbol{Q}_{n+1}$. Hence $u=v_nv_{n+1}$ for some v_n in C_n, v_{n+1} in $\boldsymbol{Q}_{n+1}$. Then apply Lemma 1 and Lemma 2 again to get $u_{n+1}\in\boldsymbol{Q}_n$ after similar computation.

4. Computations of $\hat{H}^0(G_{m,n},C_m)$. Since $C_n=C_0N_{m,n}C_m$ by Lemma 4, the natural map

$$C_0\to C_n\to C_n/N_{m,n}C_m$$

is surjective. Thus

$$\hat{H}^0(G_{m,n},C_m)=C_n/N_{m,n}C_m\simeq C_0/C_0\cap N_{m,n}C_m\,.$$

Let C_m' be the subgroup of C_m generated by circular units of the form $\prod_{\omega\in R,\tau\in\Delta}(\zeta_{p^{m+1}}^{a\omega}-\zeta_q^{b\tau})$ with $p^{m+1}\nmid a$. Then clearly $C_m=C_0C_m'$ and $N_{m,n}C_m'=C_n'$. Hence $N_{m,n}C_m=C_0^{p^{m-n}}C_n'$. Therefore

$$\hat{H}^0(G_{m,n},C_m)\simeq C_0/C_0\cap C_0^{p^{m-n}}C_n'=C_0/C_0^{p^{m-n}}(C_0\cap C_n')\,.$$

Next we claim that

$$C_0^{\tau_p-1}\subset C_0\cap C_n'\subset {}_NC_0=\{u\in C_0\,|\,N_{k/k_{(p)}}u=1\}\,.$$

The first inclusion follows from the equality $(1-\zeta_q)^{\tau_p-1}=\prod_{\omega\in R}(\zeta_p^{\omega}-\zeta_q)$. To check the second one, take $u\in C_0\cap C_n'$ and write u as

$$u=\prod_{a,b}\prod_{\omega\in R,\tau\in\Delta}(\zeta_{p^{n+1}}^{a\omega}-\zeta_q^{b\tau})^{f(a,b)}$$

for some integers $f(a,b)$. By taking N_n, we have

$$u^{p^n}=\prod_{d,\omega,\tau}(\zeta_p^{\omega}-\zeta_q^{d\tau})^{g(d)}=\prod_{d,\tau}(1-\zeta_q^{d\tau})^{g(d)(\tau_p-1)}$$

for some integers $g(d)$. Therefore $N_{k/k_{(p)}}u^{p^n} = 1$ and the second inclusion follows. Since ${}_NC_0/C_0^{\tau_p - 1}$ is annihilated by $[k : \boldsymbol{Q}]$, which is prime to p, we obtain

$$\hat{H}^0(G_{m,n}, C_m) \simeq C_0/C_0^{p^{m-n}}(C_0 \cap C_n') = C_0/C_0^{p^{m-n}}\,{}_NC_0 \,.$$

For convenience, we denote $N_{k/k_{(p)}}$ simply by N. By Lemma 5, we know that NC_0 modulo $\{\pm 1\}$ is a free abelian group of rank $l-1$. Let $\xi_1, \xi_2, \cdots, \xi_{l-1}$ be elements of C_0 such that $\{N(\xi_1), N(\xi_2), \cdots, N(\xi_{l-1})\}$ generates NC_0 modulo $\{\pm 1\}$, and let D_0 be the subgroup of C_0 generated by $\{\xi_1, \xi_2, \cdots, \xi_{l-1}\}$. Then

$$[C_0 : D_0{}_NC_0] = [NC_0 : ND_0][{}_NC_0 : {}_NC_0] = 1 \text{ or } 2 \,.$$

Therefore

$$\hat{H}^0(G_{m,n}, C_m) \simeq \frac{\langle \xi_1, \cdots, \xi_{l-1}\rangle_N C_0}{\langle \xi_1, \cdots, \xi_{l-1}\rangle^{p^{m-n}}{}_NC_0} \simeq (\mathbf{Z}/p^{m-n}\mathbf{Z})^{l-1}$$

as desired.

5. Computation of $\hat{H}^{-1}(G_{m,n}, C_m)$. Let $\{\rho_1, \cdots, \rho_{l-1}, \rho_l = \mathrm{id}\}$ be a set of coset representatives of $\bar{\Delta}/\Delta_p$. For each $1 \le i \le l-1$, let

$$\delta_{n,i} = \prod_{\substack{\omega\in R\\ \tau\in\Delta_p}} (\zeta_{p^{n+1}}^{\omega} - \zeta_q^{\tau\rho_i}) \quad \text{and} \quad \pi_n = \prod_{\omega\in R}(\zeta_{p^{n+1}}^{\omega} - 1)\,.$$

Then

$$N_{n,n-1}\delta_{n,i} = \prod_{\substack{\omega\in R\\ \tau\in\Delta_p}} (\zeta_{p^n}^{\omega} - \zeta_q^{\tau\rho_i p}) = \prod_{\substack{\omega\in R\\ \tau\in\Delta_p}} (\zeta_{p^n}^{\omega} - \zeta_q^{\tau\rho_i})^{\tau_p} = \delta_{n-1,i}$$

and

$$N_n\delta_{n,i} = \prod_{\substack{\omega\in R\\ \tau\in\Delta_p}} (\zeta_p^{\omega} - \zeta_q^{\tau\rho_i p^n}) = \prod_{\tau\in\Delta_p} (1 - \zeta_q^{\tau\rho_i p^n})^{\tau_p - 1} = 1\,,$$

since τ_p permutes Δ_p. Also, obviously $N_n(\pi_n^{\sigma-1}) = 1$.

We claim that $\hat{H}^{-1}(G_n, C_n) \simeq (\mathbf{Z}/p^n\mathbf{Z})^l$ and is generated by $\{\delta_{n,1}, \cdots, \delta_{n,l-1}, \pi_n^{\sigma-1}\}$. Then from the inflation-restriction sequence

$$0 \to H^1(G_n, C_m^{G_{m,n}}) \xrightarrow{\text{inf}} H^1(G_m, C_m) \xrightarrow{\text{res}} H^1(G_{m,n}, C_m)\,,$$

we obtain

$$0 \to (\mathbf{Z}/p^n\mathbf{Z})^l \to (\mathbf{Z}/p^m\mathbf{Z})^l \to H^1(G_{m,n}, C_m)\,,$$

since the first cohomology group H^1 is isomorphic to $\hat{H}^{-1}$ by the cyclicity of the Galois groups. Thus $(\mathbf{Z}/p^{m-n}\mathbf{Z})^l$ injects into $H^1(G_{m,n}, C_m)$. Since the Herbrand quotient for the unit group E_m is $\#(G_{m,n}) = p^{m-n}$ and since E_m/C_m is a finite group, the Herbrand quotient for C_m is also p^{m-n} (cf. [5]). Thus $\#(\mathbf{Z}/p^{m-n}\mathbf{Z})^l = \#H^1(G_{m,n}, C_m) = p^{(m-n)l}$. Therefore $\hat{H}^{-1}(G_{m,n}, C_m) \simeq (\mathbf{Z}/p^{m-n}\mathbf{Z})^l$ and is generated by

$$\langle \mathrm{res}(\delta_{m,1}), \cdots, \mathrm{res}(\delta_{m,l-1}),\ \mathrm{res}(\pi_m^{\sigma-1})\rangle = \langle \delta_{m,1}^{(\sigma^{p^n}-1)/(\sigma-1)}, \cdots, \delta_{m,l-1}^{(\sigma^{p^n}-1)/(\sigma-1)}, \pi_m^{\sigma^{p^n}-1}\rangle\,.$$

It remains to justify the claim: If $\delta_{n,1}^{a_1} \cdots \delta_{n,l-1}^{a_{l-1}} \pi_n^{(\sigma-1)a_l} = u_n^{\sigma-1}$ for some $u_n \in C_n$, then $a_1 \equiv \cdots \equiv a_l \equiv 0 \bmod p^n$.

We will prove this by induction on n. For simplicity, write δ_i for $\delta_{1,i}$, and suppose that $\delta_1^{a_1} \cdots \delta_{l-1}^{a_{l-1}} \pi_1^{(\sigma-1)a_l} = u^{\sigma-1}$ for some $u \in C_1$. As in the proof of Lemma 4, we can write $u = u_0 u_1$, where $u_0 \in C_0$ and u_1 is of the form

$$u_1 = \prod_{\omega \in R, \tau \in \Delta} (\zeta_{p^2}^{\omega} - \zeta_q^{\tau})^{\sum_{i,\rho_j \in \Delta_k} a_{i,j} \sigma^i \rho_j} \pi_1^{(\sigma-1) \sum_i b_i \sigma^i} .$$

We apply Ennola's theorem with the character $\psi_1 \chi$, $\chi \in \widehat{\Delta_{k,p}}$, to the equation $\delta_1^{a_1} \cdots \delta_{l-1}^{a_{l-1}} \pi_1^{(\sigma-1)a_l} = u_1^{\sigma-1}$ to obtain

$$\sum_{1 \le i \le l-1} a_i Y(\psi_1 \chi, \delta_i) = (\psi_1(\sigma) - 1) Y(\psi_1 \chi, u_1) .$$

Thus by Lemma 2,

$$(p-1)\#(\Delta_p)\psi_1(q) \sum_{1 \le i \le l-1} a_i \chi(\rho_i) = (\psi(\sigma) - 1)(p-1)\#(\Delta)\alpha(\chi)$$

for some algebraic integer $\alpha(\chi)$ depending on χ. Since $p \nmid \#(\Delta_p/\Delta)$, we get

$$\sum_{1 \le i \le l-1} a_i \chi(\rho_i) \equiv 0 \bmod (\zeta_p - 1) .$$

By letting χ vary over all nontrivial characters of $\Delta_{k,p}$, we have a linear equation $MA \equiv \boldsymbol{O} \bmod (\zeta_p - 1)$, where M is the $(l-1) \times (l-1)$ matrix with entries $\chi(\rho_i)$ and $A = (a_1, \cdots, a_{l-1})^t$. Let N be the $(l-1) \times (l-1)$ matrix with entries $\chi(\rho_i^{-1})$. Then since $\det(NM^t) = l^{l-2}$, $p \nmid \det M$. Therefore $A \equiv \boldsymbol{O} \bmod (\zeta_p - 1)$, and hence mod p. Since each $a_i \equiv 0 \bmod p$ for $1 \le i \le l-1$, we get $\pi_1^{(\sigma-1)a_l} = v_1^{\sigma-1}$ for some v_1 in C_1. This implies that $\pi_1^{a_l} = v_1 \alpha_0$ for some $\alpha_0 \in k$. As ideals, we have $(\pi_1^{a_l}) = (\alpha_0)$, which is impossible unless $a_l \equiv 0 \bmod p$, since primes of k above p ramify totally in k_1. This proves the claim for $n = 1$.

Now we prove the claim for n assuming the result for $n-1$. Suppose

$$\delta_{n,1}^{a_1} \cdots \delta_{n,l-1}^{a_{l-1}} \pi_n^{(\sigma-1)a_l} = u_n^{\sigma-1}$$

for some $u_n \in C_n$. By applying $N_{n,n-1}$ to both sides, we have

$$\delta_{n-1,1}^{a_1} \cdots \delta_{n-1,l-1}^{a_{l-1}} \pi_{n-1}^{(\sigma-1)a_l} = (N_{n,n-1} u_n)^{\sigma-1} \in C_{n-1}^{\sigma-1} .$$

Then by the induction hypothesis, $a_1 \equiv \cdots \equiv a_l \equiv 0 \bmod p^{n-1}$. Let $a_i = p^{n-1} b_i$ for $1 \le i \le l$. Note that

$$\delta_{n,i}^{p^{n-1}} = (N_{n,1}\delta_{n,i}) \frac{\delta_{n,i}^{p^{n-1}}}{(N_{n,1}\delta_{n,i})} = \delta_{1,i} \left(\delta_{n,i}^{\sum_{0 \le k < p^{n-1}} (1-\sigma^{kp})/(\sigma-1)} \right)^{\sigma-1}$$

and

$$\pi_n^{p^{n-1}(\sigma-1)} = \pi_1^{\sigma-1} \left(\pi_n^{\sum_k (1-\sigma^{kp})} \right)^{\sigma-1} .$$

Therefore $\delta_{n,1}^{a_1}\cdots\delta_{n,l-1}^{a_{l-1}}\pi_n^{(\sigma-1)a_l}=u_n^{\sigma-1}$ reads

$$\delta_{1,1}^{b_1}\cdots\delta_{1,l-1}^{b_{l-1}}\pi_1^{(\sigma-1)b_l}=v_n^{\sigma-1}$$

for some $v_n\in C_n$. By the injectivity of the inflation map

$$\hat{H}^{-1}(G_1,C_1)\simeq H^1(G_1,C_1)\xrightarrow{\text{inf}}H^1(G_n,C_n)\simeq\hat{H}^{-1}(G_n,C_n),$$

$\delta_{1,1}^{b_1}\cdots\delta_{1,l-1}^{b_{l-1}}\pi_1^{(\sigma-1)b_l}$ must be in $C_1^{\sigma-1}$. Thus $b_1\equiv\cdots\equiv b_l\equiv 0 \bmod p$ and so $a_1\equiv\cdots\equiv a_l\equiv 0 \bmod p^n$. This finishes the proof.

REMARK. Let $\Gamma=\mathrm{Gal}(k_\infty/k)=\varprojlim G_n$ and $C_\infty=\bigcup_{n\geq 0}C_n$. Then by taking the limit under the inflation maps, we have $H^1(\Gamma,C_\infty)\simeq(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^l$. On the other hand, Iwasawa [2] found that $H^1(\Gamma,E_\infty)=(\boldsymbol{Q}_p/\boldsymbol{Z}_p)^l\oplus M$ for some finite group M, where $E_\infty=\bigcup_{n\geq 0}E_n$. Therefore the cohomology groups of circular units are as simple as one can expect. Moreover, the natural inclusion $C_\infty\to E_\infty$ induces a homomorphism $H^1(\Gamma,C_\infty)\to H^1(\Gamma,E_\infty)$ and it is natural to ask if this map is injective. Recently, however, this map was found not to be injective in general (cf. [4]). The kernel of this homomorphism seems to be related with the capitulation, but not well understood by the author so far.

REFERENCES

[1] V. ENNOLA, On relations between cyclotomic units, J. Number Theory 4 (1972), 236–247.

[2] K. IWASAWA, On cohomology groups of units for Z_p-extensions, Amer. J. Math. 105 (1983), 189–200.

[3] J. M. KIM, Units and cyclotomic units in Z_p-extensions, Nagoya Math. J. 140 (1995), 101–116.

[4] J. M. KIM, Class numbers of real quadratic fields, Bull. Austral. Math. Soc. 57 (1998), 261–274.

[5] S. LANG, Algebraic Number Theory, Addison-Wesley, 1970.

[6] W. SINNOTT, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980), 181–234.

[7] L. WASHINGTON, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, No.83, Springer-Verlag, New York, 1980.

DEPARTMENT OF MATHEMATICS
INHA UNIVERSITY
INCHON
KOREA

E-mail address: jmkim@math.inha.ac.kr