Comm. Korean Math. Soc. 9 (1994), No. 1, pp. 27–36

CYCLOTOMIC UNITS OF NORM 1 IN $\mathbb{Z}_p$-EXTENSIONS

JAE MOON KIM

§1. Introduction

Let K be a number field (a finite extension of $\mathbb{Q}$) and let p be a fixed odd prime. By a $\mathbb{Z}_p$-extension of K, we mean a tower of field extensions $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset \cup_{n\geq 0} K_n$ such that K_n is a cyclic extension of K of degree p^n. Put $K_\infty = \cup_{n\geq 0} K_n$. Since the Galois group $\mathrm{Gal}(K_\infty/K) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$, the additive group of the ring of p-adic integers, one often says that K_∞ is a $\mathbb{Z}_p$-extension of K.

For each integer $n \geq 1$, we choose a primitive n-th root ζ_n of 1 so that $\zeta_m^{\frac{m}{n}} = \zeta_n$ whenever $n|m$. Let $K_0 = \mathbb{Q}(\zeta_p)$ and $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$. Then K_∞ is an example of a $\mathbb{Z}_p$-extension of K_0. Since $\mathrm{Gal}(K_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$, K_n has a unique subfield $\mathbb{Q}_n$ which is cyclic over $\mathbb{Q}$ of degree p^n. Thus $\mathbb{Q}_\infty$ over $\mathbb{Q}$ is another example of a $\mathbb{Z}_p$-extension. In general, for each number field K, if we let $K_n = K\mathbb{Q}_n$, then K_∞ is a $\mathbb{Z}_p$-extension of K and such a $\mathbb{Z}_p$-extension is called the basic (or cyclotomic) $\mathbb{Z}_p$-extension of K.

One of the fundamental results on the theory of $\mathbb{Z}_p$-extension is a theorem of K. Iwasawa ([**4**]).

THEOREM (K. IWASAWA). *Let K_∞ be a $\mathbb{Z}_p$-extension of $K = K_0$. Let p^{e_n} be the order of Sylow p-subgroup of the ideal class group of K_n. Then there exist integers μ, λ and ν such that $e_n = \mu p^n + \lambda n + \nu$ for all sufficiently large n.*

The constants μ, λ and ν are called the Iwasawa invariants of K. In 1979, Ferrero and Washington proved that $\mu = 0$ if K is abelian over $\mathbb{Q}$ (see [**2**]). But little is known about λ-invariant. In [**3**], R. Greenberg produced some examples such that $\lambda = 0$ and it is conjectured that $\lambda = 0$ for any totally real number field. When the base field K is real

Received June 5, 1993.
This paper was supported by research fund of Inha University, 1992.

abelian, one often studies cyclotomic units for the study of the ideal class group because of the following algebraic interpretation of the class number formula:

THEOREM (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 $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real subfield of $\mathbb{Q}(\zeta_n)$.*

This index theorem illustrates some relationship between the group of cyclotomic units and the class number. And we are especially interested in the structure of the group E/C. Because the orders are same, it is quite natural to ask whether or not the group E/C is isomorphic to the ideal class group. The answer is no. We refer [**8**] for a counterexample. When working with $\mathbb{Z}_p$-extensions, however, one is more interested in the Sylow p-subgroups of E/C and that of the ideal class group rather than the full groups. To be more precise, let $K = K_0 = \mathbb{Q}(\zeta_{pd})$, where d is an integer prime to p such that $d \not\equiv 2$ (4). Consider the basic $\mathbb{Z}_p$-extension of K_0. Thus the nth layer of this extension is $K_n = \mathbb{Q}(\zeta_{p^{n+1}d})$. Let $E_n(C_n)$ be the group of units (cyclotomic units, respectively) of K_n and let $A_n(B_n)$ be the Sylow p-subgroup of the ideal class group (E_n/C_n, respectively). Then the index theorem of W. Sinnott says $\#A_n = \#B_n$. So we ask once again if A_n is isomorphic to B_n. This question is still open and only some partial results are known so far. In [**5**], it is proved that they are isomorphic when $d = 1$ under certain assumptions. In the same paper, it is also proved that the direct and inverse limits of B_n produce the Iwasawa λ-invariant of K_0 just as the limits of A_n do.

In order to generalize those results in [**5**] to arbitrary base field $K_0 = \mathbb{Q}(\zeta_{pd})$, one needs to compute the Tate cohomology groups of cyclotomic units and to prove the injectivity of the map $\widehat{H}^i(G_n, C_n) \to \widehat{H}^i(G_n, E_n)$, where G_n is the Galois group $\mathrm{Gal}(K_n/K_0)$. Tate cohomology groups for cyclotomic units are computed in [**6**], and we list the result briefly. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ and let D be the decomposition subgroup for p of Δ. Let $l = \#(\Delta/\pm D)$, so l is the number of prime ideals of $\mathbb{Q}(\zeta_d + \zeta_d^{-1})$ above p. Then for any $m > n$,

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

,where $G_{m,n} = \mathrm{Gal}(K_m/K_n)$. In particular, $H^1(G_n, C_n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^l$, and by taking the direct limit under the inflation maps, we have $H^1(\Gamma, C_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l$. Here $C_\infty = \bigcup_{n\geq 0} C_n$ and $\Gamma = \mathrm{Gal}(K_\infty/K)$. On the other hand, K. Iwasawa found that $H^1(\Gamma, E_\infty) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^l \oplus M$ for some finite group M, where $E_\infty = \bigcup_{n\geq 0} E_n$. Thus $H^1(\Gamma, C_\infty)$ seems to control the p-divisible part of $H^1(\Gamma, E_\infty)$ and it is very likely that the map $H^1(\Gamma, C_\infty) \to H^1(\Gamma, E_\infty)$ is injective. But no one could provide a complete proof of the injectivity of this map.

The aim of this paper is to describe all the elements of $H^1(\Gamma, C_\infty)$ when $d = q$ is a prime such that $p \equiv 1 \bmod q$. This restriction $p \equiv 1 \bmod q$ can be eliminated by suitable modification of proofs in sections 2 and 3. But this restriction simplifies a lot of notations. For instance, since p splits completely in $\mathbb{Q}(\zeta_q)$, $D = \{1\}$ and $l = \frac{q-1}{2}$. Section 2 is preliminary. We will review V. Ennola's results on the relations of cyclotomic units briefly and prove several lemmas that we use in section 3. In section 3, we will exhibit l cyclotomic units of K_n which generate $H^1(G_n, C_n)$. Hopefully this could serve as groundwork for the study of the injectivity of $H^1(\Gamma, C_\infty) \to H^1(\Gamma, E_\infty)$ and of the structure of the group B_n.

§2. Preliminary

In this section, we review relations among cyclotomic units and set up notations. We first introduce V. Ennola's theorem:

THEOREM (V. ENNOLA [1]). *Let χ be a character of conductor f belonging to $\mathbb{Q}(\zeta_n)$. For each cyclotomic unit $\delta = \prod_{1\leq a<n} (1-\zeta_n^a)^{x_a}$, 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 $T(\chi,d,\delta) = \sum_{a=1}^{d-1} \chi(a) x_{\frac{n}{d}a}$. Then for every even character $\chi \neq 1$, $Y(\chi,\delta) = 0$ if δ is a root of 1.*

This statement is somewhat different from what appears in [**1**]. We seemingly modified his result so that we can apply it to our situation. The following properties of Y can be easily justified from the definition of Y.

LEMMA 1. *Let $\chi \neq 1$ be an even character belonging to $\mathbb{Q}(\zeta_n)$ and let $\delta_1, \delta_2, \delta$ 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) $Y(\chi, \delta^{\sigma-1}) = (\chi(\sigma) - 1)Y(\chi, \delta)$.

Let $K_0 = \mathbb{Q}(\zeta_{pd})$ and K_∞ be its $\mathbb{Z}_p$-extension as in section 1. Fix a topological generator σ of the Galois group $\Gamma = \mathrm{Gal}(K_\infty/K_0)$. The restrictions of σ to various subfields of K_∞ such as $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{p^n})$, $\mathbb{Q}_\infty$ and $\mathbb{Q}_\infty(\zeta_d)$ will also be denoted by σ. We even use σ for its restriction to finite levels of $\mathbb{Z}_p$-tower such as K_n. Let ω be a generator of the cyclic group $\mathrm{Gal}(K_\infty/\mathbb{Q}_\infty(\zeta_d))$. Again the restrictions of ω to various subfields are also denoted by ω. Thus $\langle\omega\rangle = \mathrm{Gal}(K_\infty/\mathbb{Q}_\infty(\zeta_d)) \simeq \mathrm{Gal}(K_n/\mathbb{Q}_n(\zeta_d)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}_n)$. Characters belonging to the field $\mathbb{Q}(\zeta_d)$ will be denoted by γ_d. Finally we fix a generator ψ_n of the character group of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ in such a way that $\psi_n(\sigma) = \zeta_{p^n}$. Thus ψ_n is an even character of conductor p^{n+1} of order p^n, and $\psi_{n+1}^p = \psi_n$.

Now we compute $Y(\chi, \delta)$ for special cyclotomic unit δ. First of all, note that $\zeta_{p^{n+1}} - \zeta_d$ is a cyclotomic unit in K_n since

$$\zeta_{p^{n+1}} - \zeta_d = \zeta_d^{-1}(\zeta_{p^{n+1}}\zeta_d^{-1} - 1) = \zeta_d^{-1}(\zeta_{p^{n+1}d}^{d-p^{n+1}} - 1).$$

Similarly, elements of K_n of the form $\prod_{x,y}(\zeta_{p^{n+1}}^x - \zeta_d^y)^{b_{x,y}}$ for some integers $x, y, b_{x,y}$ are also in C_n except for obviously bad choice such that $x = y = 0$.

LEMMA 2. *Let $\xi = $ (root of 1) $\times \prod_{i,j,k}\left(\zeta_{p^{n+1}}^{\sigma^i\omega^j} - \zeta_d^k\right)^{c_{i,j,k}}$ for some integers $c_{i,j,k}$ with $0 \leq i < p^n$, $0 \leq j < p-1$, $0 < k < d$. Then for an even* *character* χ *of the form* $\chi = \psi_n \gamma_d$, we have

$$Y(\chi, \xi^{\sigma-1}) = \frac{\psi_n(d)}{\varphi(p^{n+1}d)}(\psi_n(\sigma) - 1) \sum_{i,j,k} c_{i,j,k} \psi_n(\sigma)^i \gamma_d(kp^{n+1}).$$

(Proof) By Lemma 1,

$$\begin{aligned} Y(\chi, \xi^{\sigma-1}) &= (\chi(\sigma) - 1) Y(\chi, \xi) \\ &= (\psi_n(\sigma) - 1) \sum_{i,j,k} c_{i,j,k} Y(\chi, \zeta_{p^{n+1}}^{\sigma^i \omega^j} - \zeta_d^k). \end{aligned}$$

Since $\zeta_{p^{n+1}}^{\sigma^i \omega^j} - \zeta_d^k = (\text{root of } 1) \times (1 - \zeta_{p^{n+1}d}^{d\sigma^i \omega^j - kp^{n+1}})$, we have

$$\begin{aligned} Y(\chi, \zeta_{p^{n+1}}^{\sigma^i \omega^j} - \zeta_d^k) &= \frac{1}{\varphi(p^{n+1}d)} T(\psi_n \gamma_d, p^{n+1}d, 1 - \zeta_{p^{n+1}d}^{d\sigma^i \omega^j - kp^{n+1}}) \\ &= \frac{1}{\varphi(p^{n+1}d)} (\psi_n \gamma_d)(d\sigma^i \omega^j - kp^{n+1}) \\ &= \frac{1}{\varphi(p^{n+1}d)} \psi_n(d) \psi_n(\sigma^i) \gamma_d(kp^{n+1}). \end{aligned}$$

Hence

$$\begin{aligned} Y(\chi, \xi^{\sigma-1}) &= (\psi_n(\sigma) - 1) \sum_{i,j,k} c_{i,j,k} \frac{1}{\varphi(p^{n+1}d)} \psi_n(d) \psi_n(\sigma^i) \gamma_d(kp^{n+1}) \\ &= \frac{\psi_n(d)}{\varphi(p^{n+1}d)} (\psi_n(\sigma) - 1) \sum_{i,j,k} c_{i,j,k} \psi_n(\sigma)^i \gamma_d(kp^{n+1}). \end{aligned}$$

§3. Generators of $H^1(G_n, C_n)$

We keep all the notations in sections 1 and 2. Let $d = q$ be a prime such that $p \equiv 1 \pmod{q}$. So $D = \{1\}$ and $l = \frac{q-1}{2}$. Let $\{\tau_1, \tau_2, \dots, \tau_l = \mathrm{id}\} \subset \Delta$ be a set of coset representatives of Δ modulo $\langle \pm 1 \rangle$. In this section, we will find l cyclotomic units which generate $H^1(G_n, C_n)$. For brevity, we write $N_{t,s}$ for the norm map from K_t to K_s and N_n for $N_{n,0}$.

We will use the following equation quite often: for $m > n$, $N_{m,n}(\zeta_{p^{m+1}} - \zeta_d) = \zeta_{p^{n+1}} - \zeta_d$.

For each k, $1 \le k \le l$, let $\delta_k = \prod_{1\le j\le p-1} \left(\zeta_{p^{n+1}}^{\omega^j} - \zeta_q^{\tau_k}\right)$. Then

$$N_n(\delta_k) = \prod_{1\le j\le p-1} N_n(\zeta_{p^{n+1}}^{\omega^j} - \zeta_q^{\tau_k}) = \prod_{1\le j\le p-1} \left(\zeta_p^{\omega^j} - \zeta_q^{\tau_k}\right) = \frac{1-\zeta_q^{p\tau_k}}{1-\zeta_q^{\tau_k}} = 1$$

since $p \equiv 1 \bmod q$. Hence we have l cyclotomic units $\delta_1, \delta_2, \dots, \delta_l$ in K_n whose norms to K_0 equal 1. This set, however, is not always the right set of generators of $H^1(G_n, C_n)$. We have to change this set a little. We throw away any one of these, say δ_l, and instead we throw in $\pi_n^{\sigma-1}$ to this set, where $\pi_n = \zeta_{p^{n+1}} - 1$, which is a uniformizing parameter of the prime ideal of $\mathbb{Q}(\zeta_{p^{n+1}})$ above p. $\pi_n^{\sigma-1}$ is obviously a cyclotomic unit in C_n of norm 1.

THEOREM. *$H^1(G_n, C_n)$ is generated by $\{\delta_1, \delta_2, \dots, \delta_{l-1}, \pi_n^{\sigma-1}\}$.*

First, we need a lemma.

LEMMA 3. *Let A be the $(l-1)\times(l-1)$ matrix with $\gamma_i(\tau_j)$ in the ijth entry for $1 \le i,j \le l-1$, where $\{\gamma_0 = 1, \gamma_1, \dots, \gamma_{l-1}\}$ is the set of characters of $Gal(\mathbb{Q}(\zeta_q)^+/\mathbb{Q})$. Then prime ideals of $\mathbb{Q}(\gamma_i(\tau_j))$ above p cannot divide the ideal $(\det A)$, where $\mathbb{Q}(\gamma_i(\tau_j))$ is the field obtained by adjoining to $\mathbb{Q}$ the values $\gamma_i(\tau_j)$ for $1 \le i,j \le l-1$.*

Proof. Let $A^* = (\gamma_i(\tau_j))_{0\le i,j\le l-1}$. Then by rearranging rows and columns of A^* suitably, we may assume that A^* is a Vandermonde matrix. Since $\gamma_i(\tau_j)$ is an lth root of 1, $\det A^*$ is a product of elements of the form $1-\zeta_l^t$ for some t. Hence primes above p cannot divide $(\det A^*)$. Also note that each row sum except the first one of A^* is zero since it is of the form $\sum_{0\le j\le l-1} \gamma_i(\tau_j)$. Hence

$$\det A^* = \det \left(\begin{array}{c|ccc} l & 0 & \cdots & 0 \\ \hline 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array}\right) = l \det A.$$

And the conclusion follows from this.

Proof of theorem. Suppose $\delta_1^{a_1}\cdots\delta_{l-1}^{a_{l-1}}\pi_n^{(\sigma-1)a_l}=\xi^{\sigma-1}$ for some $\xi\in C_n$. Since we already know that $H^1(G_n,C_n)\simeq(\mathbb{Z}/p^n\mathbb{Z})^l$, it is enough to show that $a_1\equiv\cdots\equiv a_l\equiv 0 \bmod p^n$. We will show this by induction on $n\geq 1$. To treat the case when $n=1$, suppose $\delta_1^{a_1}\cdots\delta_{l-1}^{a_{l-1}}\pi_1^{(\sigma-1)a_l}=\xi^{\sigma-1}$ for some $\xi\in C_1$, where $\delta_k=\prod_j(\zeta_{p^2}^{\omega^j}-\zeta_d^{\tau_k})$. Since we will take $\sigma-1$ to ξ after all, we may assume that ξ is of the form

$$\xi=\prod_{\substack{0\leq i<p\\0\leq j<p-1\\0<k<q}}(\zeta_{p^2}^{\sigma^i\omega^j}-\zeta_q^k)^{c_{i,j,k}}\times(\text{root of }1)$$

for some integers $c_{i,j,k}$. Let $\delta=\delta_1^{a_1}\cdots\delta_{l-1}^{a_{l-1}}\pi_1^{(\sigma-1)a_l}$. By lemma 1, we have $Y(\chi,\delta)=Y(\chi,\xi^{\sigma-1})$ for every even character $\chi\neq 1$. Compute both sides when χ is of the form $\chi=\psi_1\gamma_q$, where $\gamma_q\neq 1$ is an even character belonging to $\mathbb{Q}(\zeta_q)$. By lemma 1 again, we get

$$Y(\chi,\delta)=\sum_{k=1}^{l-1}a_kY(\chi,\delta_k)+a_lY(\chi,\pi_1^{\sigma-1}).$$

One can easily check that $Y(\chi,\pi_1^{\sigma-1})=0$. For $Y(\chi,\delta_k)$, we use lemma 2 and the fact that $\gamma_q(p)=1$ since $p\equiv 1 \bmod q$. Then we have

$$\begin{aligned}Y(\chi,\delta_k)&=\sum_{0\leq j<p-1}Y(\chi,\zeta_{p^2}^{\omega^j}-\zeta_d^{\tau_k})\\&=\sum_j\frac{1}{\varphi(p^2q)}\psi_1(q)\gamma_q(\tau_k)\\&=\frac{p-1}{\varphi(p^2q)}\psi_1(q)\gamma_q(\tau_k).\end{aligned}$$

Thus

$$Y(\chi,\delta)=\frac{(p-1)\psi_1(q)}{\varphi(p^2q)}\sum_{k=1}^{l-1}a_k\gamma_q(\tau_k).$$

On the other hand, by lemma 2, we have

$$Y(\chi,\xi^{\sigma-1})=\frac{1}{\varphi(p^2q)}(\psi_1(\sigma)-1)\,\psi_1(q)\sum_{i,j,k}c_{i,j,k}\psi_1(\sigma)^i\gamma_q(k).$$

Therefore, by comparing both sides, we obtain

$$(p-1)\sum_{k=1}^{l-1} a_k\gamma_q(\tau_k) = (\psi_1(\sigma)-1)\,\alpha(\gamma_q),$$

where $\alpha(\gamma_q) = \sum_{i,j,k} c_{i,j,k}\psi_1(\sigma)^i\gamma_q(k)$, which is an algebraic integer depending on γ_q. By letting $\gamma_q \neq 1$ vary over all nontrivial even characters belonging to $\mathbb{Q}(\zeta_q)$, we have a linear system of equations

$$(p-1)A\begin{pmatrix} a_1 \\ \vdots \\ a_{l-1}\end{pmatrix} = (\psi_1(\sigma)-1)\begin{pmatrix} \vdots \\ \alpha(\gamma_q) \\ \vdots\end{pmatrix},$$

where A is the $(l-1)\times(l-1)$ matrix with entries $\gamma_q(\tau_k)$. Hence A is a matrix of type given in lemma 3, so prime ideals above p can not divide $(\det A)$. Let $\wp$ be one of the prime ideals of $\mathbb{Q}(\zeta_p, \alpha(\gamma_q))$ above p. Since $\psi_1(\sigma)-1 = \zeta_p - 1$ is divisible by $\wp$, we have

$$\begin{pmatrix} a_1 \\ \vdots \\ a_{l-1}\end{pmatrix} \equiv \begin{pmatrix} 0 \\ \vdots \\ 0\end{pmatrix} \bmod \wp.$$

Hence $a_i \in \wp\cap\mathbb{Z} = (p)$, which means that $a_1 \equiv \cdots \equiv a_{l-1} \equiv 0 \bmod p$.

From the equation $\delta_1^{a_1}\cdots\delta_{l-1}^{a_{l-1}}\pi_1^{(\sigma-1)a_l} = \xi^{\sigma-1}$, we have $\pi_1^{(\sigma-1)a_l} = u^{\sigma-1}$ for some $u\in C_1$ since $\delta_k^p \in C_1^{\sigma-1}$ for each $k = 1,\ldots,l-1$. Thus $\pi_1^{a_l} = u\beta_0$ for some $\beta_0\in K_0$. As ideals, we have $(\pi_1)^{a_l} = (\beta_0)$. But this is impossible unless $a_l \equiv 0 \bmod p$, since primes of K_0 above p totally ramify in K_1. This finishes the first step of the induction argument.

Now we will prove the theorem for n with assuming the result for $n-1$. In the proof, we will use the fact that the inflation map $H^1(G_1,C_1)\to H^1(G_n,C_n)$ is injective. By taking $N_{n,n-1}$ on both sides of the equation $\delta_1^{a_1}\cdots\delta_{l-1}^{a_{l-1}}\pi_n^{(\sigma-1)a_l} = \xi^{\sigma-1}$, we have

$$\left(\prod_j \zeta_{p^n}^{w^j} - \zeta_q^{\tau_1}\right)^{a_1}\cdots\left(\prod_j \zeta_{p^n}^{w^j} - \zeta_q^{\tau_{l-1}}\right)^{a_{l-1}}\pi_{n-1}^{(\sigma-1)a_l} = (N_{n,n-1}\xi)^{\sigma-1}.$$

Hence $a_1 \equiv \cdots \equiv a_l \equiv 0 \bmod p^{n-1}$ by the induction hypothesis. Let $a_k = p^{n-1}b_k$ for $k = 1, 2, \ldots, l$. For each k, $1 \le k \le l-1$,

$$\begin{aligned}
\delta_k^{p^{n-1}} &= \prod_j \left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right)^{p^{n-1}} \\
&= \prod_j N_{n,1}\left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right) \frac{\left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right)^{p^{n-1}}}{N_{n,1}\left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right)} \\
&= \prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_k}\right) \times \prod_j \prod_{0 \le t < p^{n-1}} \left(\frac{\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}}{\zeta_{p^{n+1}}^{w^j\sigma^{tp}} - \zeta_q^{\tau_k}}\right) \\
&= \prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_k}\right) \times \prod_j \prod_t \left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right)^{1-\sigma^{tp}} \\
&= \prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_k}\right) \times u_k^{\sigma-1},
\end{aligned}$$

where $u_k = \prod_j \prod_t \left(\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}\right)^{\frac{1-\sigma^{tp}}{\sigma-1}} \in C_n$. Also,

$$\pi_n^{p^{n-1}} = (N_{n,1}\pi_n) \times \frac{\pi_n^{p^{n-1}}}{N_{n,1}\pi_n} = \pi_1 u_l$$

where $u_l = \prod_{0 \le t < p^{n-1}} (\zeta_{p^{n+1}} - 1)^{(1-\sigma^{tp})} \in C_n$. Hence we can rewrite the equation

$$\delta_1^{a_1} \cdots \delta_{l-1}^{a_{l-1}} \pi_n^{(\sigma-1)a_l} = \xi^{\sigma-1}$$

as

$$\prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_1}\right)^{b_1} \cdots \prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_{l-1}}\right)^{b_{l-1}} \pi_1^{(\sigma-1)b_l} \cdot u_1^{\sigma-1} \cdots u_l^{\sigma-1} = \xi^{\sigma-1}.$$

Therefore we have

$$\prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_1}\right)^{b_1} \cdots \prod_j \left(\zeta_{p^2}^{w^j} - \zeta_q^{\tau_{l-1}}\right)^{b_{l-1}} \pi_1^{(\sigma-1)b_l} = u^{\sigma-1},$$

where $u = \xi u_1^{-1} \cdots u_l^{-1} \in C_n$. Let δ be the left hand side of the above equation. Then $\delta \in C_1$, $N_1 \delta = 1$ and $\delta \in C_n^{\sigma - 1}$. But since the inflation map $H^1(G_1, C_1) \to H^1(G_n, C_n)$ is injective, δ is in $C_1^{\sigma-1}$. In this case, we already know that $b_1 \equiv \cdots \equiv b_l \equiv 0 \bmod p$. Therefore $a_1 \equiv \cdots \equiv a_l \equiv 0 \bmod p^n$. This finishes the proof.

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 μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.
3. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
4. K. Iwasawa, *On some invariants of cyclotomic fields*, Amer. J. Math. **80** (1958), 773–783.
5. J. M. Kim, S. Bae, I. S. Lee, *Cyclotomic units in $\mathbb{Z}_p$-extensions*, Israel J. Math. **75** (1991), 161–165.
6. J. M. Kim, *Cohomology group of cyclotomic units*, J. Algebra **152**(1992), 514–519.
7. W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. Math. **109** (1979), 377–395.
8. L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math., vol. 83, Springer-Verlag, Berlin-New York, 1982.

Department of Mathematics
Inha University
Incheon 402–751, Korea