J. M. Kim
Nagoya Math. J.
Vol. 140 (1995), 101–116

UNITS AND CYCLOTOMIC UNITS IN $\mathbf{Z}_p$-EXTENSIONS

JAE MOON KIM[1]

Introduction

Let p be an odd prime and d be a positive integer prime to p such that $d \not\equiv 2 \bmod 4$. For technical reasons, we also assume that $p \nmid \varphi(d)$. For each integer $n \geq 1$, we choose a primitive nth root ζ_n of 1 so that $\zeta_m^{\frac{m}{n}} = \zeta_n$ whenever $n \mid m$. Let $K = K_0 = \mathbf{Q}(\zeta_{pd})$ and $K_\infty = \cup_{n \geq 0} K_n$ be its cyclotomic $\mathbf{Z}_p$-extension, where $K_n = \mathbf{Q}(\zeta_{p^{n+1}d})$ is the nth layer of this extension. For $n \geq 1$, we denote the Galois group $\mathrm{Gal}(K_n/K_0)$ by G_n, the unit group of the ring of integers of K_n by E_n, and the group of cyclotomic units of K_n by C_n. For the definition and basic properties of cyclotomic units such as the index theorem, we refer [6] and [7]. In this paper we examine the injectivity of the homomorphism $H^1(G_n, C_n) \to H^1(G_n, E_n)$ between the first cohomology groups induced by the inclusion $C_n \to E_n$.

In [4], it is shown that the Tate cohomology group $\hat{H}^i(G_{m,n}, C_m)$ depends on the splitting of p in $\mathbf{Q}(\zeta_d)$ where $G_{m,n} = \mathrm{Gal}(K_m/K_n)$ for $m > n$. To be more precise, let k be the decomposition field of p in $\mathbf{Q}(\zeta_d)$. Then

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

where

$$l = \begin{cases} [k:\mathbf{Q}] & \text{if } k \text{ is real} \\ \frac{1}{2}[k:\mathbf{Q}] & \text{otherwise.} \end{cases}$$

In particular, $H^1(G_n, C_n) \simeq (\mathbf{Z}/p^n\mathbf{Z})^l$ and by taking the direct limit under the inflation maps, we have $H^1(\Gamma, C_\infty) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^l$, where $C_\infty = \cup_{n \geq 0} C_n$ and $\Gamma = \varprojlim G_n = \mathrm{Gal}(K_\infty/K_0)$.

Received April 4, 1994.
Revised October 31, 1994.

[1] This work was supported by KOSEF, 931-0100-003-2.

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

It is interesting to compare this result to that of K. Iwasawa. In [3], he proved that $H^1(\Gamma, E_\infty) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^l \oplus M$ for some finite group M, where $E_\infty = \cup_{n\geq 0} E_n$. Thus $H^1(\Gamma, C_\infty)$ seems to control the p-divisible part of $H^1(\Gamma, E_\infty)$. However the injectivity is still unknown. The aim of this paper is to examine the injectivity when $d = q$ is a prime. Later in Section 3 of this paper, we will give a criterion of the injectivity of this map via generalized Bernoulli numbers. This paper is organized as follows. In Section 1, we find explicit generators $\{\delta_{n,1}, \ldots, \delta_{n,l}\}$ of $\hat{H}^{-1}(G_n, C_n) \simeq H^1(G_n, C_n)$. For each i, $1 \leq i \leq l$, the sequence $\{\delta_{n,i}\}_{n\geq 0}$ produces a Coates-Wiles series $h_i(x)$. This series $h_i(x)$ is studied in [5]. In Section 2, we briefly review $h_i(x)$ and establish a criterion of the injectivity of the map $H^1(G_n, C_n) \to H^1(G_n, E_n)$ in terms of the determinant of a certain matrix. We then express the determinant by Bernoulli numbers.

§1. Generators of $\hat{H}^{-1}(G_n, C_n)$

In [4], it is shown that $\hat{H}^{-1}(G_n, C_n) \simeq (\mathbf{Z}/p^n\mathbf{Z})^l$, where l is the number of prime ideals of $\mathbf{Q}(\zeta_d)^+ = \mathbf{Q}(\zeta_d + \zeta_d^{-1})$ above p. The proof of this theorem, however, is theoretical and it does not provide generators of $\hat{H}^{-1}(G_n, C_n)$. In this section, we will exhibit generators of this cohomology group explicitly when $d = q$ is a prime. For this we need a theorem of V. Ennola on the relations among cyclotomic units (see [1]). But instead of quoting his theorem in detail, we just state what is necessary for us.

THEOREM (V. Ennola). *Suppose $\delta = \Pi_{1\leq a<n}(1-\zeta_n^a)^{x_a}$ is a root of 1 for some integers x_a. Then for every even character $\chi \neq 1$ of conductor f belonging to $\mathbf{Q}(\zeta_n)$, $Y(\chi, \delta) = 0$, where*

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

and

$$T(\chi, d, \delta) = \sum_{\substack{a=1 \\ (a,d)=1}}^{d-1} \chi(a) x_{\frac{n}{d}a}.$$

The following properties of Y can be justified from the definition of Y, so we omit the proofs.

LEMMA 1.1. *Let $\chi \neq 1$ be an even character belonging to $\mathbf{Q}(\zeta_n)$ and δ_1, δ_2, δ be cyclotomic units in $\mathbf{Q}(\zeta_n)$. Then*

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

(i) $Y(\chi, \delta_1\delta_2) = Y(\chi, \delta_1) + Y(\chi, \delta_2)$.

(ii) *If* (*root of* 1) $\times$ δ_1 = (*root of* 1) $\times$ δ_2, *then* $Y(\chi, \delta_1) = Y(\chi, \delta_2)$.

(iii) *For any* $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$, $Y(\chi, \delta^{\sigma}) = \chi(\sigma) Y(\chi, \delta)$.

(iv) $Y(\chi, \delta^{\sigma-1}) = (\chi(\sigma) - 1) Y(\chi, \delta)$.

From now on, we fix an odd prime q and consider the $\mathbf{Z}_p$-extension K_∞ over $K_0 = \mathbf{Q}(\zeta_{pq})$ such that $p \nmid \varphi(q)$. We fix a topological generator σ of the Galois group $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ such that $\zeta_{p^n}^{\sigma} = \zeta_{p^n}^{1+p}$ for any $n \geq 1$. The restrictions of σ to various subfields of K_∞ such as $\mathbf{Q}(\zeta_{p^\infty}) = \cup_{n\geq 0} \mathbf{Q}(\zeta_{p^n})$, $\mathbf{Q}_\infty$ and $\mathbf{Q}_\infty(\zeta_q)$ will also be denoted by σ. Here, $\mathbf{Q}_\infty$ is the $\mathbf{Z}_p$-extension of $\mathbf{Q}$. We even use σ for its restrictions to finite layers of $\mathbf{Z}_p$-tower such as K_n. Let w be a generator of the cyclic group $\mathrm{Gal}(K_\infty/\mathbf{Q}_\infty(\zeta_q))$. Again, the restrictions of w to various subfields are also denoted by w. Thus $\langle w \rangle = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty(\zeta_q)) \simeq \mathrm{Gal}(K_n/\mathbf{Q}_n(\zeta_q)) \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q}_n)$. Nontrivial even characters belonging to the field $\mathbf{Q}(\zeta_q)$ will be denoted by γ_q. Finally we fix a generator ψ_n of the character group of $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$ 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 $\psi_{n+1}^p = \psi_n$.

For later use, we compute $Y(\chi, \delta)$ for an even character $\chi = \psi_n \gamma_q$ and for some cyclotomic unit δ in K_n. First of all, note that $\zeta_{p^{n+1}} - \zeta_q$ is a cyclotomic unit in K_n since

$$\zeta_{p^{n+1}} - \zeta_q = \zeta_q(\zeta_{p^{n+1}}\zeta_q^{-1} - 1) = \zeta_q(\zeta_{p^{n+1}q}^{q-p^{n+1}} - 1).$$

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

Let ξ = (root of 1) $\times$ $\Pi_{i,j,k} (\zeta_{p^{n+1}}^{\sigma^i w^j} - \zeta_q^k)^{c_{i,j,k}}$ for some integers $c_{i,j,k}$ with $0 \leq i < p^n$, $0 \leq j < p - 1$, $0 < k < q$. For an even character χ of the form $\chi = \psi_n \gamma_q$, we have

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

by Lemma 1. Since

$$(\zeta_{p^{n+1}}^{\sigma^i w^j} - \zeta_q^k) = (\text{root of } 1) \times (1 - \zeta_{p^{n+1}q}^{q\sigma^i w^j - kp^{n+1}}),$$

we have

$$Y(\chi, \zeta_{p^{n+1}}^{\sigma^i w^j} - \zeta_q^k) = \frac{1}{\varphi(p^{n+1}q)} T(\chi, p^{n+1}q, 1 - \zeta_{p^{n+1}q}^{q\sigma^i w^j - kp^{n+1}})$$

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

$$= \frac{1}{\varphi(p^{n+1}q)} \psi_n \gamma_q (q\sigma^i w^j - kp^{n+1})$$
$$= \frac{1}{\varphi(p^{n+1}q)} \psi_n(q\sigma^i) \gamma_q(kp^{n+1}).$$

Hence

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

where $\alpha(\gamma_q) = \sum_{i,j,k} c_{i,j,k}\psi_n(\sigma^i)\gamma_q(k)$, which is an algebraic integer depending on γ_q.

Now we describe l elements of C_n which generate $\hat{H}^{-1}(G_n, C_n)$. Let Δ be the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$, or any Galois group isomorphic to it such as $\mathrm{Gal}(K_\infty/\mathbf{Q}(\zeta_{p^\infty}))$. Let D be the decomposition subgroup of Δ for p, and k be its fixed subfield of $\mathbf{Q}(\zeta_q)$. Let $\{\tau_1, \tau_2, \ldots, \tau_l = \mathrm{id}\} \subset \Delta$ be a set of coset representatives of Δ modulo $\langle -1, D\rangle$. Notice that this l coincides with the earlier l in the introduction. For brevity, we write $N_{t,s}$ for the norm map from K_t to K_s, N_n for $N_{n,0}$, and N_D for the norm map from K_0 to k or from K_n to $k(\zeta_{p^{n+1}})$. We shall use the following equation quite often: for $m > n$,

$$N_{m,n}(\zeta_{p^{n+1}} - \zeta_q) = \zeta_{p^{n+1}} - \zeta_q^{p^{m-n}}.$$

For each k, $1 \le k \le l$, let

$$\eta_{n,k} = \eta_k = \prod_{1\le j\le p-1} (\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k}), \text{ and } \delta_{n,k} = \delta_k = N_D(\eta_k).$$

Then

$$N_n(\delta_k) = N_D \circ N_n(\eta_k) = N_D\Big(\prod_j \zeta_p^{w^j} - \zeta_q^{p^n\tau_k}\Big) = N_D\Big(\frac{1 - \zeta_q^{q^{n+1}\tau_k}}{1 - \zeta_q^{q^n\tau_k}}\Big) = 1$$

since D is generated by p.

Hence we have l cyclotomic units $\delta_1, \delta_2, \ldots, \delta_l$ 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. Namely 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 generator of the prime ideal of $\mathbf{Q}(\zeta_{p^{n+1}})$ above p. $\pi_n^{\sigma-1}$ is obviously a cyclotomic unit in C_n whose norm to K_0 is 1.

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

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

First, we need a lemma.

LEMMA 1.2. *Let F be an abelian field of degree m over $\mathbf{Q}$. Let $\{\tau_0 = \mathrm{id}, \tau_1, \dots, \tau_{m-1}\}$ and $\{\gamma_0 = 1, \gamma_1, \dots, \gamma_{m-1}\}$ be the set of $\mathrm{Gal}(F/\mathbf{Q})$ and its character group $\mathrm{Gal}(F/\mathbf{Q})^\wedge$ respectively. Let A be the $(m-1) \times (m-1)$ matrix with $\gamma_i(\tau_j)$ for the ijth entry for $1 \leq i, j \leq m-1$. Then the only prime ideals of the field $\mathbf{Q}(\gamma_i(\tau_j))$ that can divide the ideal $(\det A)$ are those above the prime factors of m, where $\mathbf{Q}(\gamma_i(\tau_j))$ is the field obtained by adjoining to $\mathbf{Q}$ the value $\gamma_i(\tau_j)$ for $1 \leq i, j \leq m-1$.*

Proof. Let B be the $(m-1) \times (m-1)$ matrix with $\gamma_i(\tau_j^{-1})$ for the ijth entry for $1 \leq i, j \leq m-1$. Then since $\sum_{1 \leq k \leq m-1} \gamma_i(\tau_k^{-1})\gamma_j(\tau_k) = |G|\,\delta_{i,j} - 1$,

$$\det(B^tA) = \det\begin{pmatrix} m-1 & & & \\ & m-1 & & -1 \\ -1 & & \ddots & \\ & & & m-1 \end{pmatrix} = m^{m-2}.$$

Hence prime ideals of $\mathbf{Q}(\gamma_i(\tau_j))$ that can divide $(\det A)$ are prime factors of m.

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

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

for some integers $c_{i,j,k}$ with $0 \leq i < p$, $0 \leq j < p-1$, $0 < k < q$. Let $\delta = \delta_1^{a_1} \cdots \delta_{l-1}^{a_{l-1}}\pi_1^{(\sigma-1)a_l}$. By Lemma 1.1, 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 k. By (i) of Lemma 1.1, we get

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

One can easily check that $Y(\chi, \pi_1^{\sigma-1}) = 0$. For $Y(\chi, \delta_k)$, we use earlier computa-

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

tion in the middle of this section and the facts that D is generated by p and $\gamma_q(p) = 1$ to obtain

$$Y(\chi, \delta_k) = \sum_{\substack{i,j \\ 0 \leqslant j < p-1 \\ 0 \leqslant i < |D|}} Y(\chi, \zeta_{p^2}^{w^j} - \zeta_q^{\tau_k p^i}) = \sum_{i,j} \frac{1}{\varphi(p^2 q)} \psi_1(q) \gamma_q(\tau_k p^{2+i})$$
$$= \frac{(p-1)\,|\,D\,|\,\psi_1(q)}{\varphi(p^2 q)} \gamma_q(\tau_k).$$

Thus

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

On the other hand, from earlier computation, we have

$$Y(\chi, \xi^{\sigma-1}) = \frac{1}{\varphi(p^2 q)} (\psi_1(\sigma) - 1) \psi_1(q) \alpha(\gamma_q).$$

Therefore, by comparing both sides, we obtain

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

By letting γ_q vary over all nontrivial even characters belonging to k, we have a system of linear equations

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

where A is the $(l-1) \times (l-1)$ matrix with entries $\gamma_q(\tau_k)$. Hence A is a matrix of the type given in Lemma 1.2, so prime ideals above p can not divide $(\det A)$ since p is prime to $\varphi(q)$ and $l \mid \varphi(q)$. Let $\wp$ be one of the prime ideals of $\mathbf{Q}(\zeta_p, \alpha(\gamma_q))$ above p. Since $\psi_1(\sigma) - 1 = \zeta_p - 1$ is divisible by $\wp$ and since $p \nmid |\,D\,|$, we have

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

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

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 $\alpha_l \equiv 0 \bmod p$, since primes of K_0 above p totally ramify in K_1. This finishes the first step of the induction argument. Notice that $H^1(G_1, C_1)$ is also generated by $\{\delta_1', \ldots, \delta_{l-1}', \pi_1^{\sigma-1}\}$ where $\delta_k' = N_D\,(\Pi_{1 \le j \le p-1}\,(\zeta_{p^2}^{w^j} - \zeta_q^{t\tau_k}))$ for any integer t prime to q.

Now we will prove the theorem for n with assuming the result for $n-1$. Thus we assume that $H^1(G_{n-1}, C_{n-1})$ is generated by $\{\delta_1', \ldots, \delta_{l-1}', \pi_{n-1}^{\sigma-1}\}$, where $\delta_k' = N_D\,(\Pi_{1 \le j \le p-1}\,(\zeta_{p^n}^{w^j} - \zeta_q^{t\tau_k}))$ for any integer t prime to q, in particular, when $t = p$. In the proof, we will use the fact 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

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

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, $1 \le k \le l-1$,

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

where $u_k = N_D\Bigl(\prod_j \prod_t (\zeta_{p^{n+1}}^{w^j} - \zeta_q^{\tau_k})^{\frac{1-\sigma^{tp}}{\sigma-1}}\Bigr) \in C_n$. 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 $u_l = \Pi_{0 \le t \le p^{n-1}}\,(\zeta_{p^{n-1}} - 1)^{(1-\sigma^{tp})} \in C_n$. 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

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

Therefore we have

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

where $u = \xi u_1^{-b_1} \cdots u_l^{-b_l} \in C_n$.

Let $\delta = N_D(\Pi_j (\zeta_{p^2}^{w^j} - \zeta_q^{p^{n-1}\tau_1}))^{b_1} \cdots N_D(\Pi_j (\zeta_{p^2}^{w^j} - \zeta_q^{p^{n-1}\tau_{l-1}}))^{b_{l-1}} \pi_1^{(\sigma-1)b_l}$. 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.

COROLLARY. *For* $m \geq n$, $\langle \delta_{m,1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \ldots, \delta_{m,l-1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \pi_m^{\sigma^{p^n}-1} \rangle$ *generates* $\hat{H}^{-1}(G_{m,n}, C_m) \simeq H^1(G_{m,n}, C_m)$.

Proof. Since $C_m^{G_{m,n}} = C_n$ (see [2]), we have the following exact sequence:

$$0 \to H^1(G_n, C_n) \xrightarrow{\text{inflation}} H^1(G_m, C_m) \xrightarrow{\text{restriction}} H^1(G_{m,n}, C_m).$$

Since ${}^{\#}H^1(G_n, C_n) = p^{nl}$, ${}^{\#}H^1(G_m, C_m) = p^{ml}$ and ${}^{\#}H^1(G_{m,n}, C_m) = p^{(m-n)l}$, the restriction map must be surjective. Hence

$$\begin{aligned} H^1(G_{m,n}, C_m) &= \operatorname{Im}(H^1(G_m, C_m) \xrightarrow{\text{restriction}} H^1(G_{m,n}, C_m)) \\ &= \langle \operatorname{res}(\delta_{m,1}), \ldots, \operatorname{res}(\delta_{m,l-1}), \operatorname{res}(\pi_m^{\sigma-1}) \rangle \\ &= \langle \delta_{m,1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \ldots, \delta_{m,l-1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \pi_m^{\sigma^{p^n}-1} \rangle. \end{aligned}$$

§2. Injectivity of $H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$

In the section we will find a criterion of the injectivity of $H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$. Since $H^1(\Gamma, C) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^l$ and $H^1(\Gamma, E) \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^l \oplus$ finite group (see [3], [4]), the map is likely to be injective. And the following proposition shows that the Greenberg's conjecture on the vanishing of the Iwasawa λ-invariant for a totally real field implies the injectivity for $m > n \gg 0$.

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

Proposition 2. *Suppose the Iwasawa invariant λ^+ for the field $K_0 = \mathbf{Q}(\zeta_{pd})$ is zero (equivalently, the Sylow p-subgroup of E/C is a finite group). Then $H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$ is injective for $m > n \gg 0$.*

Proof. Let B_n be the Sylow p-subgroup of E_n/C_n. It is known that $B_n \to B_m$ is injective for $m > n$ (see [2]). Since we are assuming the Greenberg's conjecture, $\varinjlim B_n = B$ is finite, and hence is obtained at some finite layer K_{n_0}. That is, $B_{n_0} \simeq B_m \simeq B$ for all $m \geq n_0$. Therefore $G_{m,n}$ acts trivially on B_m for $m > n \geq n_0$. From the short exact sequence $0 \to C_m \to E_m \to E_m/C_m \to 0$, we obtain the long exact sequence of cohomology groups:

$$0 \to C_m^{G_{m,n}} \to E_m^{G_{m,n}} \to (E_m/C_m)^{G_{m,n}} \to H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m) \to \cdots.$$

In this sequence, $C_m^{G_{m,n}} = C_n$ (see [2]) and $E_m^{G_{m,n}} = E_n$. Thus we have:

$$0 \to E_n/C_n \to (E_m/C_m)^{G_{m,n}} \to H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$$

Hence, if $m > n \geq n_0$, $H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$ must be injective since $B_n \simeq B_m$.

Now we discuss the injectivity of the map when $d = q$ is an odd prime without assuming the Greenberg's conjecture. We assume that $p \equiv 1 \bmod q$ so that p splits completely in $\mathbf{Q}(\zeta_q)$ and $l = \frac{1}{2}\varphi(q)$.

Let $R = \{w \in \mathbf{Z}_p \mid w^{p-1} = 1\}$ be the group of $p - 1$th roots of 1 in the ring of p-adic integers $\mathbf{Z}_p$. Let $h_t(x) = \Pi_{w \in R}((1+x)^w - t)$ in $\mathbf{Z}_p[t][[x]]$. The following expansion of $h_t(x)$ as a power series in x with coefficients in $\mathbf{Z}_p[t]$ plays an important role in our discussion of the injectivity.

Theorem (see [5]). *$h_t(x) = \Pi_w((1+x)^w - t) = (1-t)^{p-1} + g(t)x^{p-1} +$ higher terms, where $g(t) \equiv (1-t)^{p-2} + \frac{1}{2}(1-t)^{p-3} + \cdots + \frac{1}{p-1} \pmod{p}$.*

For each n, let us fix a prime ideal $\wp_n$ of K_n in such a way that $\wp_m$ lies above $\wp_n$ for $m > n$. Then the set $\{\wp_n^\tau\}$ is the set of all prime ideals of K_n above p when τ runs over $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$. For $\tau \in \Delta$, let $K_{n,\wp_n^\tau}$ be the completion of K_n at the prime ideal $\wp_n^\tau$ and let $\varphi_\tau : K_n \to K_{n,\wp_n^\tau}$ be the natural embedding. Put $s_\tau = \varphi_\tau(\zeta_q)$ be the image of ζ_q in $K_{n,\wp_n^\tau}$. For brevity, we write s for $s_{\mathrm{id}} = \varphi_{\mathrm{id}}(\zeta_q)$. Let $p(\tau)$ be the integer modulo q corresponding to τ under the identification of Δ with $(\mathbf{Z}/q\mathbf{Z})^\times$. Then $s_\tau^{p(\tau)} = \varphi_\tau(\zeta_q)^{p(\tau)} = \varphi_\tau(\zeta_q^{p(\tau)}) = \varphi_\tau(\zeta_q^\tau)$. Since the completion of K_n^τ at the prime ideal $\wp_n^\tau$ is the same as the completion of K_n at $\wp_n$, we have $s_\tau^{p(\tau)} = \varphi_\tau(\zeta_q^\tau) = \varphi_{\mathrm{id}}(\zeta_q) = s$. Therefore $s_\tau = s^{p(\tau^{-1})}$ and $s_\tau^{p(\tau')} = s^{p(\tau^{-1})p(\tau')} = s^{p(\tau^{-1}\tau')}$

for any τ, $\tau' \in \varDelta$.

Proposition 3. *Let $g(t) \in \mathbf{Z}_p[t]$ be the polynomial introduced above and τ_i, $\tau_j \in \varDelta$. Let $\delta_{n,\tau_j} = \Pi_{w\in R}\,(\zeta_{p^{n+1}}^{w} - \zeta_q^{\tau_j})$. Then, in $K_{n,\wp_n^{\tau_i}}$,*

$$\delta_{n,\tau_j} \equiv 1 + g(s^{p(\tau_i^{-1}\tau_j)})\pi_n^{p-1} \bmod (\pi_n^p),$$

where $\pi_n = \zeta_{p^{n+1}} - 1$.

Proof. In $K_{n,\wp_n^{\tau_i}}$,

$$\begin{aligned}\delta_{n,\tau_j} &= \prod_{w\in R}\,(\zeta_{p^{n+1}}^{w} - s_{\tau_i}^{p(\tau_j)})\\ &= \prod_{w\in R}\,(\zeta_{p^{n+1}}^{w} - s^{p(\tau_i^{-1}\tau_j)})\\ &= h_{s^{p(\tau_i^{-1}\tau_j)}}(\zeta_{p^{n+1}} - 1)\\ &= (1 - s^{p(\tau_i^{-1}\tau_j)})^{p-1} + g(s^{p(\tau_i^{-1}\tau_j)})\pi_n^{p-1} \bmod (\pi_n^p)\end{aligned}$$

by the above theorem. Since $(1 - s^{p(\tau_i^{-1}\tau_j)})^{p-1} \equiv 1 \bmod p$, we obtain the congruence.

Let $S = \{\tau_1, \tau_2, \ldots, \tau_{l-1}, \tau_l = \mathrm{id}\}$ be a set of coset representatives of $\varDelta$ modulo $\{\pm 1\}$. Let $A = (a_{ij})$ be the $l \times l$ matrix with entries in $\mathbf{Z}_p$ such that

$$a_{ij} = \begin{cases} g(s^{p(\tau_i^{-1}\tau_j)}) & \text{if } j \leq l-1 \\ 1 & \text{if } j = l. \end{cases}$$

Theorem 2. *$H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$ is injective for all $m > n \geq 0$ if* $\det A \not\equiv 0 \bmod p$.

First, we prove a lemma which reduces the theorem to the case when $m = n + 1$.

Lemma 2.1. *Suppose $H^1(G_{s+1,s}, C_{s+1}) \to H^1(G_{s+1,s}, E_{s+1})$ is injective for all $s \geq 0$, then $H^1(G_{t,s}, C_t) \to H^1(G_{t,s}, E_t)$ is injective for all $t > s \geq 0$.*

Proof. Fix s, and write $t = s + k$. We use an induction on k. If $k = 1$, then there is nothing to prove. We will prove the injectivity when $t = s + k + 1$ assuming the result for $t = s + k$. Consider the following commutative diagram:

$$\begin{tikzcd}
H^1(G_{s+k,s}, C_{s+k}) \arrow[r] \arrow[d, "\text{inflation}"] & H^1(G_{s+k,s}, E_{s+k}) \arrow[d, "\text{inflation}"] \\
H^1(G_{s+k+1,s}, C_{s+k+1}) \arrow[r] \arrow[d, "\text{restiction}"] & H^1(G_{s+k+1,s}, E_{s+k+1}) \arrow[d, "\text{restiction}"] \\
H^1(G_{s+k+1,s+k}, C_{s+k+1}) \arrow[r] & H^1(G_{s+k+1,s+k}, E_{s+k+1})
\end{tikzcd}$$

Note that inflation-restriction sequences are exact and that inflation maps are injective. By hypothesis the top and the bottom of the diagram are also injective. With these in mind, one can easily check the injectivity of the middle map.

Proof of theorem. By the lemma, we may assume that $m = n + 1$. We know that, from the corollary of Theorem 1, $\{\delta_{m,1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \ldots, \delta_{m,l-1}^{\frac{\sigma^{p^n}-1}{\sigma-1}}, \pi_m^{\sigma^{p^n}-1}\}$ generates $H^1(G_{m,n}, C_m)$ where $\delta_{m,i} = \Pi_{w\in R}\, \zeta_{p^{m+1}}^w - \zeta_q^{\tau_i}$. Suppose $\delta_{m,1}^{\frac{\sigma^{p^n}-1}{\sigma-1}a_1} \cdots \delta_{m,l-1}^{\frac{\sigma^{p^n}-1}{\sigma-1}a_{l-1}} \pi_m^{(\sigma^{p^n}-1)a_l} = \eta_m^{\sigma^{p^n}-1}$ for some integers $a_1, \ldots, a_l$ and for some η_m in E_m. Since $m = n + 1$, it is enough to show that $a_1 \equiv \cdots \equiv a_l \equiv 0 \pmod p$. We write the above equation as $(\delta_{m,1}^{a_1} \cdots \delta_{m,l-1}^{a_{l-1}} \pi_m^{(\sigma-1)a_l})^{\sigma^{p^n}-1} = \eta_m^{(\sigma-1)(\sigma^{p^n}-1)}$. Thus $\delta_{m,1}^{a_1} \cdots \delta_{m,l-1}^{a_{l-1}} \pi_m^{(\sigma-1)a_l} = \eta_m^{\sigma-1} u_n$ for some unit $u_n \in E_n$. We read this equation in $K_{m,\wp_m^{\tau_i}}$. Since $\delta_{m,j}$, $\pi_m^{\sigma-1}$ and $\eta_m^{\sigma-1}$ are all congruent to 1 modulo π_m, $u_n - 1 \in (\pi_m) \cap K_{n,\wp_n^{\tau_i}} = (\pi_n) = (\pi_m)^p$. Hence by reading the above equation in consequence modulo $(\pi_m)^p$, we have

$$\delta_{m,1}^{a_1} \cdots \delta_{m,l-1}^{a_{l-1}} \pi_m^{(\sigma-1)a_l} \equiv \eta_m^{\sigma-1} \bmod (\pi_m^p).$$

By Proposition 3, $\delta_{m,j}^{a_j} \equiv (1 + g(s^{p(\tau_i^{-1}\tau_j)})\pi_m^{p-1})^{a_j} \equiv 1 + a_j g(s^{p(\tau_i^{-1}\tau_j)})\pi_m^{p-1} \bmod (\pi_m^p)$. It is easy to check that $\pi_m^{\sigma-1} \equiv 1 + \pi_m^{p-1} \bmod (\pi_m^p)$ and that $\eta_m^{\sigma-1} \equiv 1 \bmod (\pi_m^p)$. Therefore we get

$$a_1 g(s^{p(\tau_i^{-1}\tau_1)}) + a_2 g(s^{p(\tau_i^{-1}\tau_2)}) + \cdots + a_{l-1} g(s^{p(\tau_i^{-1}\tau_{l-1})}) + a_l \equiv 0 \bmod p.$$

Since this equation is true for all i, $1 \leq i \leq l$, we have a system of linear equations

$$A \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} \equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \bmod p.$$

But since $\det A \not\equiv 0 \bmod p$, $a_1 \equiv \cdots \equiv a_l \equiv 0 \bmod p$.

Finally, we interpret $\det A$ in terms of generalized Bernoulli numbers. We fix an embedding φ from $\bar{\mathbf{Q}}$ (algebraic closure of $\mathbf{Q}$) to $\mathbf{C}_p$ (completion of the algebraic

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

closure of $\mathbf{Q}_p$) such that $\varphi(\zeta_q) = s$ and we drop φ. So, for example, $g(\zeta_g^{\tau})$ should be understood as $g(s^{p(\tau)})$.

Lemma 2.2. $\det A = \prod_{\substack{\chi\in\hat{\Delta},\text{ even}\\ \chi\neq 1}} \sum_{\tau_j\in S} \chi(\tau_j) g(\zeta_q^{\tau_j})$.

We omit the proof of this lemma since it is a simple consequence of the following well known fact (see [7]): If f is a function on a finite abelian group G with values in some field of characteristic 0, then $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\hat{G}} \sum_{\sigma\in G} \chi(\sigma) f(\sigma)$.

Theorem 3. *Let ω be the character of* $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\times}$ *such that $\omega(a) \equiv a \bmod p$ for all integers a with $(a, p) = 1$. Then we have*

$$\det A \equiv \left(\frac{q}{2}\right)^{l-1} \frac{1}{\sqrt{\operatorname{disc} \mathbf{Q}(\zeta_q)^{+}}} \prod_{\substack{\chi\in\hat{\Delta},\text{ even}\\ \chi\neq 1}} B_{1,\chi\omega^{-1}} \bmod p$$

Proof. Let $\chi \in \hat{\Delta}$ be a nontrivial even character. We will show that $\sum_{\tau_j\in S} \chi(\tau_j) g(\zeta_q^{\tau_j}) \equiv \frac{q}{2\tau(\bar{\chi})} B_{1,\bar{\chi}\omega^{-1}} \bmod (\zeta_{p^2} - 1)$, where $\tau(\bar{\chi}) = \sum_{a \bmod q} \bar{\chi}(a) \zeta_q^a$ is the Gauss sum of $\bar{\chi}$. Since $\prod_{\chi} \tau(\chi) = \sqrt{\operatorname{disc} \mathbf{Q}(\zeta_q)^{+}}$, the theorem follows immediately from Lemma 2.2. Let $s \neq 1$ be a qth root of 1 in $\mathbf{C}_p$. Since $\prod_{\omega\in R}((1 + x)^{w} - s) \equiv 1 + g(s)x^{p-1} \bmod (p, x^{p})$, we have

$$\prod_{\omega\in R} (\zeta_{p^2}^{w} - s) \equiv 1 + g(s)(\zeta_{p^2} - 1)^{p-1} \bmod (\zeta_p - 1).$$

Hence, by taking p-adic logarithm, we obtain

$$\log_p\left(\prod_{\omega\in R} (\zeta_{p^2}^{w} - s)\right) \equiv \log_p(1 + g(s)(\zeta_{p^2} - 1)^{p-1}) \bmod (\zeta_p - 1).$$

By expanding out the right hand side, we get

$$\sum_{\omega\in R} \log_p(\zeta_{p^2}^{w} - s)$$
$$\equiv g(s)(\zeta_{p^2} - 1)^{p-1} - \frac{1}{2}(g(s)(\zeta_{p^2} - 1)^{p-1})^2 + \cdots + \frac{1}{p}(g(s)(\zeta_{p^2} - 1)^{p-1})^p - \cdots.$$

In this expression every term except $\frac{1}{p}(g(s)(\zeta_{p^2} - 1)^{p-1})^p$ is congruent to 0 modulo $(\zeta_{p^2} - 1)$. And one can easily check that $(\zeta_{p^2} - 1)^{(p-1)p}/p \equiv -1 \bmod (\zeta_{p^2} - 1)$. Thus, $\sum_{\omega\in R} \log_p(\zeta_{p^2}^{w} - s) \equiv -g(s) \bmod (\zeta_{p^2} - 1)$. Therefore,

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

$$(*)\qquad -\sum_{\tau_j\in S}\chi(\tau_j)g(\zeta_q^{\tau_j}) \equiv \sum_{\substack{\omega\in R\\ \tau_j\in S}}\chi(\tau_j)\log_p(\zeta_{p^2}^{w}-\zeta_q^{\tau_j}) \bmod (\zeta_{p^2}-1)$$

Let $\psi=\psi_1$ be the character of $\mathrm{Gal}(\mathbf{Q}_1/\mathbf{Q})$ as in Section 1 so that $\psi(\sigma)=\zeta_p$ for the generator σ of $\mathrm{Gal}(\mathbf{Q}_1/\mathbf{Q})\simeq\mathrm{Gal}(K_1/K_0)$. For $0\le i\le p-1$, $0\le k\le p-1$, let

$$T_i=\sum_{\substack{\omega\in R\\ \tau_j\in S}}\chi(\tau_j)\log_p(\zeta_{p^2}^{w\sigma^i}-\zeta_q^{\tau_j})$$

and

$$S_k=\sum_{i=0}^{p-1}\psi^k(\sigma^i)T_i.$$

When $k=0$,

$$\begin{aligned}
S_0&=\sum_{i=0}^{p-1}T_i\\
&=\sum_{\tau_j\in S}\chi(\tau_j)\sum_{\substack{0\le i\le p-1\\ w\in R}}\log_p(\zeta_{p^2}^{w\sigma^i}-\zeta_q^{\tau_j})\\
&=\sum_{\tau_j\in S}\chi(\tau_j)\log_p\frac{1-\zeta_q^{\tau_jp^2}}{1-\zeta_q^{\tau_jp}}\\
&=0,
\end{aligned}$$

since $p\equiv 1 \bmod q$.
When $k\neq 0$,

$$\begin{aligned}
S_k&=\sum_{i,w,\tau_j}\chi\psi^k(\tau_j\sigma^i)\log_p(\zeta_{p^2}^{w\sigma^i}-\zeta_q^{\tau_j})\\
&=\frac{1}{2}\sum_{i,w,\tau_j}\chi\psi^k(\tau_j\sigma^i w)\,(\log_p(\zeta_{p^2}^{w\sigma^i}-\zeta_q^{\tau_j})+\log_p(\zeta_{p^2}^{w\sigma^i}-\zeta_q^{-\tau_j}))\\
&=\frac{1}{2}\sum_{1\le b\le p^2q}\chi\psi^k(b)\log_p(1-\zeta_{p^2q}^{b})\\
&=-\frac{1}{2}\frac{p^2q}{\tau(\overline{\chi\psi^k})}L_p(1,\overline{\chi\psi^k}).
\end{aligned}$$

Thus we have a system of linear equations:

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

$$\begin{pmatrix} \psi^0(\sigma^0) & \psi^0(\sigma^1) & \cdots & \psi^0(\sigma^{p-1}) \\ \psi^1(\sigma^0) & \psi^1(\sigma^1) & \cdots & \psi^1(\sigma^{p-1}) \\ \vdots & & & \\ \psi^{p-1}(\sigma^0) & \psi^{p-1}(\sigma^1) & \cdots & \psi^{p-1}(\sigma^{p-1}) \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \\ \vdots \\ T_{p-1} \end{pmatrix} = -\frac{p^2 q}{2} \begin{pmatrix} 0 \\ \dfrac{L_p(1, \overline{\chi\psi})}{\tau(\overline{\chi\psi})} \\ \vdots \\ \dfrac{L_p(1, \overline{\chi\psi^{p-1}})}{\tau(\overline{\chi\psi^{p-1}})} \end{pmatrix}.$$

By solving this equation, we obtain

$$\begin{aligned} T_0 &= \sum_{\substack{w \in R \\ \tau_j \in S}} \chi(\tau_j) \log_p (\zeta_{p^2}^w - \zeta_q^{\tau_j}) \\ &= -\frac{pq}{2} \sum_{1 \le k \le p-1} \frac{1}{\tau(\overline{\chi\psi^k})} L_p(1, \overline{\chi\psi^k}). \end{aligned}$$

For the Gauss sum $\tau(\overline{\chi\psi^k})$, we have

$$\begin{aligned} \tau(\overline{\chi\psi^k}) &= \sum_{\substack{a \bmod p^2 q \\ (a,pq)=1}} \overline{\chi\psi^k}(a) \zeta_{p^2 q}^a \\ &= \sum_{\substack{x,y \\ x \bmod q \ (x,q)=1 \\ y \bmod p^2 \ (y,p)=1}} \overline{\chi\psi^k}(xp^2 + yq) \zeta_{p^2 q}^{xp^2+yq} \\ &= (\sum_x \bar{\chi}(x) \zeta_q^x)(\sum_y \psi^k(qy) \zeta_{p^2}^y) \\ &= \tau(\bar{\chi}) \overline{\psi^k}(q) \tau(\overline{\psi^k}). \end{aligned}$$

Since $\psi^k(q)\overline{\psi^k}(q) = 1$ and $\tau(\overline{\psi^k})\tau(\psi^k) = p^2$, we get

$$\begin{aligned} T_0 &= -\frac{pq}{2\tau(\bar{\chi})} \sum_{1 \le k \le p-1} \frac{1}{\overline{\psi^k}(q) \tau(\overline{\psi^k})} L_p(1, \overline{\chi\psi^k}) \\ &= -\frac{q}{2\tau(\bar{\chi})} \sum_k \psi^k(q) \frac{\tau(\psi^k)}{p} L_p(1, \overline{\chi\psi^k}). \end{aligned}$$

Note that $\tau(\psi^k)/p$ is a root of 1, hence, in particular, integral. Let $f_{\bar{\chi}}$ be the Iwasawa power series giving rise to the p-adic L-function i.e., $f_{\bar{\chi}}(\zeta(1+pq)^s - 1) = L_p(s, \overline{\chi\psi^k})$ for a suitable p-th root ζ of 1 depending on ψ^k. Since $f_{\bar{\chi}}$ has integral coefficients, $L_p(1, \overline{\chi\psi^k}) = f_{\bar{\chi}}(\zeta(1+pq) - 1) \equiv f_{\bar{\chi}}(0) = L_p(0, \bar{\chi}) = -B_{1,\bar{\chi}\omega^{-1}}$ mod $(\zeta_p - 1)$. Therefore

$$T_0 \equiv -\frac{q}{2\tau(\bar{\chi})} \sum_{1 \le k \le p-1} \psi^k(q) \frac{\tau(\psi^k)}{p} (-B_{1,\bar{\chi}\omega^{-1}}) \bmod (\zeta_p - 1)$$

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

$$\equiv \frac{q}{2\tau(\bar{\chi})} B_{1,\bar{\chi}\omega^{-1}} \sum_{1 \leq k \leq p-1} \frac{\tau(\psi^k)}{p} \bmod (\zeta_p - 1).$$

Now, we examine the sum $\displaystyle\sum_{1 \leq k \leq p-1} \frac{\tau(\psi^k)}{p}$.

$$\begin{aligned} \sum_{1 \leq k \leq p-1} \frac{\tau(\psi^k)}{p} &= \sum_{1 \leq k \leq p-1} \frac{1}{p} \sum_{\substack{a \bmod p^2 \\ (a,p)=1}} \psi^k(a) \zeta_{p^2}^a \\ &= \sum_{\substack{1 \leq k \leq p-1 \\ w \in R \\ 0 \leq i \leq p-1}} \frac{1}{p} \psi^k(\sigma^i) \zeta_{p^2}^{w\sigma^i} \\ &= \sum_{w,i} \frac{1}{p} \zeta_{p^2}^{w\sigma^i} \left(\sum_k \psi^k(\sigma^i) \right) \\ &= \sum_w \frac{1}{p} \zeta_{p^2}^w (p-1) + \sum_{\substack{w \\ i \neq 0}} \frac{1}{p} \zeta_{p^2}^{w\sigma^i} (-1) \\ &= \sum_w \zeta_{p^2}^w - \frac{1}{p} \sum_{i,w} \zeta_{p^2}^{w\sigma^i} \\ &= \sum_w \zeta_{p^2}^w \end{aligned}$$

Hence,

$$\begin{aligned} T_0 &\equiv \frac{q}{2\tau(\bar{\chi})} B_{1,\bar{\chi}\omega^{-1}} \sum_w \zeta_{p^2}^w \bmod (\zeta_p - 1) \\ &\equiv \frac{q}{2\tau(\bar{\chi})} B_{1,\bar{\chi}\omega^{-1}} (p-1) \bmod (\zeta_{p^2} - 1). \end{aligned}$$

Therefore,

$$(**) \qquad \sum_{\substack{w \in R \\ \tau_j \in S}} \chi(\tau_j) \log_p (\zeta_{p^2}^w - \zeta_q^{\tau_j}) \equiv - \frac{q}{2\tau(\bar{\chi})} B_{1\bar{\chi}\omega^{-1}} \bmod (\zeta_{p^2} - 1)$$

From (*) and (**), we obtain the desired congruence equation, and this finishes the proof of the theorem.

COROLLARY. *Let* $L = \mathbf{Q}(\zeta_q^+, \zeta_p)$ *and* $L^+ = \mathbf{Q}(\zeta_q^+, \zeta_p^+)$, *where* $\zeta_q^+ = \zeta_q + \zeta_q^{-1}$ *and* $\zeta_p^+ = \zeta_p + \zeta_p^{-1}$. *If* $p \nmid \dfrac{h_L^-}{h_p^-}$, *then* $H^1(G_{m,n}, C_m) \to H^1(G_{m,n}, E_m)$ *is injective for all* $m \geq n \geq 0$. *Here* h_L^- *is the relative class number of* L, *i.e.*, $h_L^- = h_L / h_L^+$. *Similarly* h_p^- *is the relative class number of* $\mathbf{Q}(\zeta_p)$.

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press

Proof. From the class number formula, we have

$$\begin{aligned} h_p^- &= Q\omega \prod_{\rho \text{ odd}} \left(-\frac{1}{2} B_{1,\rho}\right) \\ &= 2^t h_p^- \prod_{\substack{\chi \in \hat{\Delta} \text{ even} \\ \chi \neq 1}} B_{1,\chi\omega^{-1}} \cdot B_{1,\chi\omega^{-3}} \bullet \cdots \bullet B_{1,\chi\omega^{-(p-2)}}) \end{aligned}$$

for a suitable integer t. Hence if $p \nmid \dfrac{h_L^-}{h_p^-}$, then $\prod_{\substack{\chi \in \hat{\Delta}, \text{ even} \\ \chi \neq 1}} B_{1,\chi\omega^{-1}} \not\equiv 0 \bmod p$. By Theorems 2 and 3, we obtain the injectivity.

COROLLARY. *Suppose* $\prod_{\substack{\chi \in \hat{\Delta}, \text{ even} \\ \chi \neq 1}} B_{1,\chi\omega^{-1}} \not\equiv 0 \bmod p$. *Suppose also the class number of* $\mathbf{Q}(\zeta_{pq})^+$ *is prime to* p. *Then, the class number of* $\mathbf{Q}(\zeta_{p^m q})^+$ *is prime to* p *for every* m.

Proof. It is enough to show that $p \nmid [E_m : C_m]$ for every m (see[6]). From the short exact sequence $0 \to C_m \to E_m \to E_m / C_m \to 0$, we have a long exact sequence

$$0 \to C_0 \to E_0 \to (E_m / C_m)^{G_m} \to H^1(G_m, C_m) \to H^1(G_m, E_m).$$

Since $H^1(G_m, C_m) \to H^1(G_m, E_m)$ is injective by Theorems 2 and 3, we have $(E_m / C_m)^{G_m} \simeq E_0 / C_0$. Thus $(E_m / C_m)^{G_m} \otimes \mathbf{Z}_p \simeq E_0 / C_0 \otimes \mathbf{Z}_p = \{0\}$. Therefore $p \nmid [E_m : C_m]$.

REFERENCES

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

[2] Gold, R., Kim, J. M., Bases for cyclotomic units, Compositio Math., **71** (1989), 13–28.

[3] Iwasawa, K., On Cohomology groups of units for $\mathbf{Z}_p$-extensions, Amer. J. Math., **105** No.1 (1983), 189–200.

[4] Kim, J. M., Cohomology groups of cyclotomic units, J. Algebra, **152**, no.2 (1992), 514–519.

[5] ——, Coates-Wiles series and Mirimanoff's polynomial, J. Number Theory, **54**, No.2 (1995), 173–179.

[6] Sinnott, W., On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math., (2) **108** (1978), 107–134.

[7] Washington, L., Introduction to Cyclotomic Fields, G. T. M., Springer-Verlag, New York, 1980.

Department of Mathematics
Inha University, Inchon, Korea
(e-mail) jmkim@munhak.inha.ac.kr

https://doi.org/10.1017/S0027763000005432 Published online by Cambridge University Press