Hokkaido Mathematical Journal Vol. 44 (2015) p. 397–407

Semi-local units at p of a cyclotomic $\mathbb{Z}_p$-extension congruent to 1 modulo $\zeta_p - 1$

Humio Ichimura

(Received May 29, 2013; Revised November 21, 2014)

Abstract. Let p be a prime number. Let K be an abelian number field with $p \nmid [K:\mathbb{Q}]$ and $\zeta_p \in K$, K_∞/K the cyclotomic $\mathbb{Z}_p$-extension, and K_n the nth layer with $K_0 = K$. Let $\mathcal{U}_n$ be the group of semi-local principal units of K_n at the prime p, and $\mathcal{U}_n^{(1)}$ the elements u of $\mathcal{U}_n$ satisfying the congruence $u \equiv 1$ modulo $\zeta_p - 1$. The Galois module structure of $\mathcal{U}_n$ is well understood. The purpose of this paper is to determine the Galois module structure of $\mathcal{U}_n^{(1)}$.

Key words: semi-local units, cyclotomic $\mathbb{Z}_p$-extension, Galois module structure.

1. Introduction

Let p be a prime number. Let K be an abelian number field with $p \nmid [K:\mathbb{Q}]$ and $\zeta_p \in K$, where ζ_p is a primitive pth root of unity. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension, and K_n the nth layer with $K_0 = K$. We denote by $\mathcal{U}_n$ the product of the groups of principal units of the completions of K_n at the primes over p. Namely, $\mathcal{U}_n$ is the group of semi-local principal units of K_n at the prime p. Let $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$ be the projective limit with respect to the relative norms $K_m \to K_n$ $(m > n)$, and $\mathcal{V}_n$ the image of the projection $\mathcal{U}_\infty \to \mathcal{U}_n$. Denote by $\mathcal{U}_n^{(1)}$ the elements u of $\mathcal{U}_n$ satisfying the congruence $u \equiv 1$ modulo $\zeta_p - 1$, and put $\mathcal{V}_n^{(1)} = \mathcal{U}_n^{(1)} \cap \mathcal{V}_n$. We see that $\mathcal{U}_0^{(1)} = \mathcal{U}_0$ as $p \nmid [K:\mathbb{Q}]$. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $\Gamma = \mathrm{Gal}(K_\infty/K)$. We can regard these groups $\mathcal{U}_n$, $\mathcal{V}_n$, $\mathcal{U}_n^{(1)}$, $\mathcal{V}_n^{(1)}$ as modules over the Galois groups Δ and Γ. Let χ be a fixed $\bar{\mathbb{Q}}_p$-valued character of Δ, and $\mathcal{O} = \mathcal{O}_\chi$ the subring of $\bar{\mathbb{Q}}_p$ generated by the values of χ over $\mathbb{Z}_p$. Here, $\mathbb{Z}_p$ is the ring of p-adic integers and $\bar{\mathbb{Q}}_p$ is a fixed algebraic closure of the p-adic rationals $\mathbb{Q}_p$. Choosing a generator γ of Γ, we identify as usual the completed group ring $\mathcal{O}[[\Gamma]]$ with the power series ring $\Lambda = \Lambda_\chi = \mathcal{O}[[s]]$ by the correspondence $\gamma \leftrightarrow 1+s$. Then we can naturally regard the χ-parts $\mathcal{U}_\infty(\chi)$, $\mathcal{U}_n(\chi)$, *etc.* as modules over Λ. The Λ-module structures of the χ-parts $\mathcal{U}_n(\chi)$ and $\mathcal{V}_n(\chi)$

2010 Mathematics Subject Classification : Primary 11S23; Secondary 11R18, 11R23.

are well understood by some results in Iwasawa [8], Coleman [2] and Gillard [3]. Usually, $\mathcal{U}_n(\chi) = \mathcal{V}_n(\chi)$ and there is an isomorphism $\mathcal{V}_n(\chi) \cong \Lambda/w_n$ as Λ-modules where $w_n = w_n(s) = (1+s)^{p^n} - 1$. In [4], we determined the ideal $J_{n,\chi}$ of Λ corresponding to the submodule $\mathcal{V}_n^{(1)}(\chi)$ via this isomorphism for the case $p \geq 3$ when p does not split in K and χ is even. Here, we say that χ is even when $\chi(-1) = 1$ regarding χ as a primitive Dirichlet character. Further, in [4], [5], we applied this structure result for a normal integral basis problem on an unramified Kummer extension over K_n of degree p. In this paper, we determine the Λ-module structure of $\mathcal{V}_n^{(1)}(\chi)$ for the general case where $p \nmid [K : \mathbb{Q}]$ and χ is not necessarily even including the case $p = 2$. The result will be used in our further study [7] on normal integral basis.

2. Theorem

To state the main theorem, we recall some fundamental facts on $\mathcal{U}_n(\chi)$ and $\mathcal{V}_n(\chi)$ mainly from [3, Section 2]. Here, χ is a fixed $\bar{\mathbb{Q}}_p$-valued character of Δ. Let

$$e_\chi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \mathrm{Tr}(\chi(\sigma^{-1}))\sigma$$

be the idempotent of $\mathbb{Z}_p[\Delta]$ associated to χ. Here, Tr denotes the trace map from $\mathbb{Q}_p(\chi)$ to $\mathbb{Q}_p$, $\mathbb{Q}_p(\chi)$ being the quotient field of $\mathcal{O}_\chi$. For a $\mathbb{Z}_p[\Delta]$-module M such as $\mathcal{U}_n$ and $\mathcal{V}_n$, the χ-part $M(\chi)$ is defined to be M^{e_χ} (or $e_\chi M$). Let $\tilde{p} = 2p$ or p according as $p = 2$ or $p \geq 3$. Denote by q the least common multiple of $\tilde{p}$ and the conductor of χ. Identifying Γ with the Galois group $\mathrm{Gal}(K_\infty(\zeta_{\tilde{p}})/K(\zeta_{\tilde{p}}))$ in a natural way, we choose and fix a generator γ of Γ so that $\zeta^\gamma = \zeta^{1+q}$ for all p-power-th roots ζ of unity. (Here, $\zeta_{\tilde{p}}$ is a primitive $\tilde{p}$th root of unity.) We identify the subring $e_\chi \mathbb{Z}_p[\Delta] = \mathbb{Z}_p[\Delta](\chi)$ of $\mathbb{Z}_p[\Delta]$ with $\mathcal{O} = \mathcal{O}_\chi$ via the mapping $\sigma \to \chi(\sigma)$, and regard the completed group ring $\mathcal{O}[[\Gamma]]$ as a subring of $\mathbb{Z}_p[\Delta][[\Gamma]]$. As in Section 1, we identify $\mathcal{O}[[\Gamma]]$ with the power series ring $\Lambda = \Lambda_\chi = \mathcal{O}[[s]]$ by the correspondence $\gamma \leftrightarrow 1 + s$. Thus, the groups $\mathcal{U}_\infty(\chi), \mathcal{U}_n(\chi)$ *etc.* are regarded as Λ-modules. Let $\omega_{\tilde{p}}$ be the Teichmüller character of conductor $\tilde{p}$. We regard χ and its dual character $\chi^* = \omega_{\tilde{p}}\chi^{-1}$ also as primitive Dirichlet characters. We divide the character χ into the following three types:

$$\text{(A) } \chi(p) \neq 1 \text{ and } \chi^*(p) \neq 1, \quad \text{(B) } \chi^*(p) = 1, \quad \text{(C) } \chi(p) = 1.$$

As $p \nmid [K:\mathbb{Q}]$, type (B) does not occur when $p=2$. It is known that

$$\mathcal{U}_n(\chi) = \mathcal{V}_n(\chi) \quad \text{for type (A) or (B).}$$

For type (C), it is known that

$$N_{n/0}\mathcal{V}_n(\chi) = \mathcal{V}_0(\chi) = \mathrm{Tor}_{\mathbb{Z}}\,\mathcal{U}_0(\chi) \cong \mathcal{O}/2 \tag{1}$$

and that

$$\mathcal{U}_0(\chi)/\mathcal{V}_0(\chi) \cong \mathcal{U}_n(\chi)/\mathcal{V}_n(\chi). \tag{2}$$

In (1), $N_{n/0}$ denotes the norm map from K_n to K_0, and $\mathrm{Tor}_{\mathbb{Z}}(*)$ the $\mathbb{Z}$-torsion subgroup. Note that $\mathcal{O}/2$ is trivial when $p \geq 3$. The isomorphism (2) is induced from the natural lifting map $\mathcal{U}_0 \to \mathcal{U}_n$ (see [9, p. 695]). These are consequences of local class field theory. Even for type (C), it is enough to study $\mathcal{V}_n^{(1)}(\chi)$ for understanding $\mathcal{U}_n^{(1)}(\chi)$ because of (2) and $\mathcal{U}_0 = \mathcal{U}_0^{(1)}$. It is known that for type (B), the Λ-torsion submodule $\mathbb{T}$ of $\mathcal{U}_\infty(\chi)$ is isomorphic to $\Lambda/(\dot{s})$, where

$$\dot{s} = (1+q)(1+s)^{-1} - 1.$$

Let $\mathbb{T}_n$ be the projection of $\mathbb{T}$ to $\mathcal{U}_n(\chi)$. It is known that

$$\mathcal{U}_\infty(\chi) \cong \begin{cases} \Lambda, & \text{for type (A) or (C),} \\ \Lambda \oplus \mathbb{T}, & \text{for type (B)} \end{cases} \tag{3}$$

as Λ-modules. Let $\widetilde{\mathcal{V}}_n(\chi) = \mathcal{V}_n(\chi)$ for type (A) or (C), and $\widetilde{\mathcal{V}}_n(\chi) = \mathcal{V}_n(\chi)/\mathbb{T}_n$ for type (B). It is known that the above isomorphism (3) induces

$$\widetilde{\mathcal{V}}_n(\chi) \cong \begin{cases} \Lambda/(w_n), & \text{for type (A) or (B),} \\ \Lambda/(w_n, 2w_n/s), & \text{for type (C).} \end{cases} \tag{4}$$

For (3) and (4), see [3, Propositions 1, 2]. Let $\widetilde{\mathcal{V}}_n^{(1)}(\chi) = \mathcal{V}_n^{(1)}(\chi)$ for type (A) or (C), and $\widetilde{\mathcal{V}}_n^{(1)}(\chi) = \mathcal{V}_n^{(1)}(\chi)\mathbb{T}_n/\mathbb{T}_n$ for type (B). Now, we define the ideal $J_{n,\chi}$ of Λ containing w_n (resp. w_n and $2w_n/s$)) for type (A) or (B) (resp. type (C)) so that the above isomorphism (4) induces

$$\widetilde{\mathcal{V}}_n^{(1)}(\chi) \cong \begin{cases} J_{n,\chi}/(w_n), & \text{for type (A) or (B),} \\ J_{n,\chi}/(w_n, 2w_n/s), & \text{for type (C).} \end{cases} \tag{5}$$

We define the ideal $I_{n,\chi}$ of Λ by

$$I_{n,\chi} = \begin{cases} \langle p^n,\, p^{n-1-k}s^{p^k} \mid 0 \le k \le n-1\rangle, & \text{for type (A) or (C),} \\ \langle p^{n-1-k}s^{p^k-1} \mid 0 \le k \le n-1\rangle, & \text{for type (B),} \end{cases} \tag{6}$$

when $n \geq 1$. We put $I_{0,\chi} = \Lambda$. The following is the main result of this paper.

Theorem *Under the above setting, we have $J_{n,\chi} = I_{n,\chi}$ for all $n \geq 0$ and χ.*

In [4, Proposition 1], we proved this assertion for the case $p \geq 3$ when p does not split in K and χ is even, by showing both the inclusions $I_{n,\chi} \subseteq J_{n,\chi}$ and $J_{n,\chi} \subseteq I_{n,\chi}$. The method in [4] can be applied also to the case where $p \geq 3$, $p \nmid [K : \mathbb{Q}]$ and χ is an even character of type (A). We showed the first inclusion $I_{n,\chi} \subseteq J_{n,\chi}$ in a direct way. However, to show the second one, we needed some subtle treatment of the twisted logarithm of the "Coleman power series" associated to each element of $\mathcal{U}_\infty(\chi)$ combined with the structure theorem ([3, Theorems 1, 2]) on semi-local units modulo cyclotomic units. Thus, the method in [4] is rather complicated, and in particular can not be applied for odd characters χ. In this paper, we show Theorem by showing (i) $I_{n,\chi} \subseteq J_{n,\chi}$ for each χ associated to K and (ii) that the product $\prod_\chi |\Lambda_\chi/I_{n,\chi}|$ equals $\prod_\chi |\Lambda_\chi/J_{n,\chi}|$ in quite an elementary way.

3. Proof

We denote by $B(m, n) = {}_mC_n$ the binomial coefficient. The following lemma is easy to show (see [4, Lemma 4]).

Lemma 1 *The binomial coefficient $B(p^n, j)$ is divisible by p^{n-k} for any k and j with $0 \leq k \leq n-1$ and $p^k \leq j \leq p^{k+1}-1$.*

Lemma 2 *When $p \geq 3$ (resp. $p = 2$), $B((1+q)^{p^n}, j)$ is divisible by p for $2 \leq j \leq p^{n+1}-1$ (resp. $2 \leq j \leq p^{n+2}-1$), but not divisible by p when $j = p^{n+1}$ (resp. p^{n+2}).*

Proof. When $p \geq 3$, the assertion was shown in [4, Lemma 7]. It is shown similarly for the case $p = 2$. $\square$

We fix a prime divisor v of K_∞ over p. We also denote by v the restriction of v to each subfield K_n. Let K_n^v be the completion of K_n at v, U_n^v the group of principal units of K_n^v, $U_\infty^v = \varprojlim U_n^v$ the projective limit with respect to the relative norms $K_m^v \to K_n^v$ $(m > n)$, and V_n^v the image of the projection $U_\infty^v \to U_n^v$. Let $D \subseteq \Delta$ be the decomposition group of the prime p in $K/\mathbb{Q}$, and $\chi_{|D}$ the restriction of χ to D. The groups U_n^v and V_n^v are naturally regarded as modules over $\mathbb{Z}_p[D \times \Gamma]$. We have an isomorphism

$$\mathcal{U}_n \cong U_n^v \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[\Delta]$$

of $\mathbb{Z}_p[\Delta \times \Gamma]$-modules. This induces isomorphisms

$$\mathcal{U}_n(\chi) \cong U_n^v(\chi_{|D}) \otimes \mathcal{O}_\chi \quad \text{and} \quad \mathcal{V}_n(\chi) \cong V_n^v(\chi_{|D}) \otimes \mathcal{O}_\chi \tag{7}$$

of Λ-modules where the tensor products are taken over the ring $\mathcal{O}_\psi$ with $\psi = \chi_{|D}$. By (3), we can choose and fix an element $\boldsymbol{u} = (\boldsymbol{u}_n)_{n\geq 0} \in \mathcal{U}_\infty(\chi)$ so that the correspondence

$$\boldsymbol{u}_n^g \leftrightarrow g \bmod (w_n) \text{ or } (w_n,\, 2w_n/s) \tag{8}$$

induces the isomorphism (4). We denote by K_{-1} the maximal subextension of $K/\mathbb{Q}$ unramified at p. Then we have $K = K_{-1}(\zeta_p)$ as $p \nmid [K : \mathbb{Q}]$. We naturally identify $\Delta_{-1} = \mathrm{Gal}(K_{-1}/\mathbb{Q})$ with $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$. We put

$$\mathcal{R} = \prod_w O_w$$

where w runs over the prime divisors of K_{-1} over p, and O_w is the ring of integers of the completion of K_{-1} at w. We choose and fix a primitive p^{n+1}st root $\zeta_{p^{n+1}}$ of unity so that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for all n, and put $\pi_n = \zeta_{p^{n+1}} - 1$ or $\zeta_{p^{n+2}} - 1$ according as $p \geq 3$ or $p = 2$. Then $\pi_n \in K_n(\zeta_{\tilde{p}})$, and $N_{n,n-1}(\pi_n) = \pi_{n-1}$ where $N_{n,n-1}$ is the norm map from $K_n(\zeta_{\tilde{p}})$ to $K_{n-1}(\zeta_{\tilde{p}})$. For each norm coherent system $u = (u_n)_{n\geq 0} \in \mathcal{U}_\infty$, there exists a unique power series $f_u(t)$ in $\mathcal{R}[[t]]$ with $f_u(0) \equiv 1 \bmod p$ such that $u_n^{\varphi^n} = f_u(\pi_n)$ for all n by Coleman [1]. Here, $\varphi \in \Delta_{-1}$ is the Frobenius automorphism at p, which naturally acts on $\mathcal{U}_n$. We denote by $\mathfrak{f}(t) = f_{\boldsymbol{u}}(t) \in \mathcal{R}[[t]]$ the Coleman power series associated to the fixed element $\boldsymbol{u} \in \mathcal{U}_\infty(\chi)$. The Galois group $\Delta \times \Gamma$ naturally acts on $\mathcal{R}$ through the surjection $\Delta \times \Gamma \to \Delta_{-1}$. The completed group ring $\mathbb{Z}_p[\Delta][[\Gamma]]$ acts on each power series $f \in \mathcal{R}[[t]]$ with $f(0) \equiv 1 \bmod p$ by

$$f^\sigma(t) = f_\sigma((1+t)^{\kappa(\sigma)} - 1) \quad (\sigma \in \Delta \times \Gamma)$$

and $\mathbb{Z}_p$-linearlity. Here, f_σ is the power series obtained from f by the Galois action of σ on its coefficients, and $\kappa : \Delta \times \Gamma \to \mathbb{Z}_p^\times$ denotes the character representing the Galois action on all the p-power-th roots of unity. In particular, we have

$$f^\gamma(t) = f((1+t)^{1+q} - 1).$$

We can easily show that

$$f^\alpha(\pi_n) = f(\pi_n)^\alpha \tag{9}$$

for $\alpha \in \mathbb{Z}_p[\Delta][[\Gamma]]$.

Proof of Theorem for type (B). Putting $\psi = \chi^*$, we have $\chi = \omega_p \psi^{-1}$ and $\psi(p) = 1$. As $\psi(p) = 1$, we may as well assume that p splits completely in K_{-1} and that $\chi_{|D} = \omega_p$. In [6], we have shown Theorem when the base field is the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ for the character ω_p of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Therefore, the assertion for the general case follows from (7) since the completion K^v of $K = K_{-1}(\zeta_p)$ equals $\mathbb{Q}_p(\zeta_p)$. □

Lemma 3 *We have* $I_{n,\chi} \subseteq J_{n,\chi}$ *for any* n *and* χ.

Proof. It suffices to deal with type (A) or (C). First, assume that $p \geq 3$. We have shown the assertion in [4, Lemma 8] using Lemmas 1 and 2, under the additional assumptions that p does not split in K and χ is even. The assertion is shown quite similarly without the additional assumptions.

We assume that $p = 2$. We first show that

$$\mathfrak{f}^{s^{2^m}} \equiv 1 \bmod (2,\, t^{2^{m+2}}) \tag{10}$$

holds for any $m \geq 0$. We easily see from Lemma 2 that

$$(1+t)^{(1+q)^{2^m}} - 1 \equiv t \bmod (2,\, t^{2^{m+2}})$$

for any $m \geq 0$. It follows that

$$\mathfrak{f}^{\gamma^{2^m}}(t) = \mathfrak{f}((1+t)^{(1+q)^{2^m}} - 1) \equiv \mathfrak{f}(t) \bmod (2,\, t^{2^{m+2}}). \tag{11}$$

Letting $m = 0$, we have $\mathfrak{f}^{\gamma} \equiv \mathfrak{f} \bmod (2,\, t^{2^2})$. Hence

$$\mathfrak{f}^{s} = \mathfrak{f}^{\gamma - 1} \equiv 1 \bmod (2,\, t^{2^2})$$

and (10) holds when $m = 0$. Let $m \geq 1$. Assume that $\mathfrak{f}^{s^{2^k}} \equiv 1$ modulo $(2,\, t^{2^{k+2}})$ for all k with $0 \leq k \leq m-1$. Raising to the 2^{m-k}th power, we obtain

$$\mathfrak{f}^{s^{2^k} \cdot 2^{m-k}} \equiv 1 \bmod (2,\, t^{2^{m+2}}) \tag{12}$$

for $0 \leq k \leq m-1$. On the other hand,

$$\mathfrak{f}^{\gamma^{2^m} - 1} \equiv 1 \bmod (2,\, t^{2^{m+2}}) \tag{13}$$

holds by (11). Further, we have

$$s^{2^m} = (\gamma^{2^m} - 1) - \sum_{k=0}^{m-1} \left(\sum_{j=2^k}^{2^{k+1}-1} B(2^m,\, j) s^j \right),$$

and $B(2^m,\, j)$ is divisible by 2^{m-k} when $2^k \leq j \leq 2^{k+1} - 1$ by Lemma 1. Therefore, we see from (12) and (13) that the assertion (10) holds also for m.

Now, let us show the lemma (for $p = 2$). By (4), (8) and $\mathfrak{f}(\pi_n) = \boldsymbol{u}_n^{\varphi^n}$, we see that it suffices to show that $\mathfrak{f}(\pi_n)^{\alpha} \equiv 1 \bmod 2$ for $\alpha = 2^n$ and $2^{n-1-k} s^{2^k}$ with $0 \leq k \leq n-1$. We note that $\pi_n = \zeta_{2^{n+2}} - 1$ and $(\pi_n)^{2^{n+1}} = (2)$. As the abelian extension $K/\mathbb{Q}$ is of odd degree, it is unramified at the prime 2. It follows that

$$\mathfrak{f}(\pi_0) = \mathfrak{f}(\zeta_4 - 1) = \boldsymbol{u}_0 \equiv 1 \bmod 2.$$

This implies that $\mathfrak{f}(t) \equiv 1 \bmod (2,\, t^2)$. Therefore, $\mathfrak{f}(\pi_n) \equiv 1$ modulo $(\pi_n)^2 =$

(π_{n-1}), and hence

$$\mathfrak{f}(\pi_n)^{2^n} \equiv 1 \bmod (\pi_{n-1})^{2^n} = (2).$$

By (9) and (10), we have

$$\mathfrak{f}(\pi_n)^{s^{2^k}} = \mathfrak{f}^{s^{2^k}}(\pi_n) \equiv 1 \bmod (\pi_n)^{2^{k+2}}.$$

Hence, we observe that

$$\mathfrak{f}(\pi_n)^{2^{n-1-k}s^{2^k}} \equiv 1 \bmod (\pi_n)^{2^{n+1}} = (2). \qquad \square$$

We denote by $\mathbb{Q}_p(\chi)$ the quotient field of $\mathcal{O} = \mathcal{O}_\chi$ and put $d_\chi = [\mathbb{Q}_p(\chi) : \mathbb{Q}_p]$. Let $\mathrm{ord}_p(*)$ be the additive valuation on $\mathbb{Q}_p$ with $\mathrm{ord}_p(p) = 1$.

Lemma 4 *We have*

$$\mathrm{ord}_p(|\Lambda_\chi/I_{n,\chi}|) = \begin{cases} d_\chi \dfrac{p^n-1}{p-1}, & \text{for type (A) or (C)}, \\ d_\chi\left(\dfrac{p^n-1}{p-1} - n\right), & \text{for type (B)}. \end{cases}$$

Proof. For type (A) or (C), we see from the definition of $I_{n,\chi}$ that

$$\Lambda_\chi/I_{n,\chi} \cong \mathcal{O}/p^n \oplus \bigoplus_{k=0}^{n-2} (\mathcal{O}/p^{n-1-k})^{\oplus p^k(p-1)}.$$

Hence, it follows that

$$\frac{1}{d_\chi}\mathrm{ord}_p(|\Lambda_\chi/I_{n,\chi}|) = n + (p-1)\sum_{k=0}^{n-2}(n-1-k)p^k = \frac{p^n-1}{p-1}.$$

The assertion follows similarly for type (B). $\square$

Lemma 5 *We have*

$$|\mathcal{U}_n(\chi)/\mathcal{U}_n^{(1)}(\chi)| = \begin{cases} |\mathcal{V}_n(\chi)/\mathcal{V}_n^{(1)}(\chi)|, & \text{for type (A) or (C)}, \\ |\widetilde{\mathcal{V}}_n(\chi)/\widetilde{\mathcal{V}}_n^{(1)}(\chi)| \times p^{nd_\chi}, & \text{for type (B)}. \end{cases}$$

Proof. The assertion is obvious for type (A). First, let us deal with type (B). We have a filtration

$$\mathcal{U}_n(\chi) \supseteq \mathcal{U}_n^{(1)}(\chi)\mathbb{T}_n \supseteq \mathcal{U}_n^{(1)}(\chi).$$

The natural map $\mathcal{U}_n(\chi) \to \widetilde{\mathcal{V}}_n(\chi)/\widetilde{\mathcal{V}}_n^{(1)}(\chi)$ induces an isomorphism

$$\mathcal{U}_n(\chi)/\mathcal{U}_n^{(1)}(\chi)\mathbb{T}_n \cong \widetilde{\mathcal{V}}_n(\chi)/\widetilde{\mathcal{V}}_n^{(1)}(\chi).$$

Further, we have

$$\mathcal{U}_n^{(1)}(\chi)\mathbb{T}_n/\mathcal{U}_n^{(1)}(\chi) \cong \mathbb{T}_n/(\mathbb{T}_n \cap \mathcal{U}_n^{(1)}(\chi)) = \mathbb{T}_n/\mathbb{T}_0.$$

From these, we obtain the assertion.

Next, we deal with type (C). From (2), we see that

$$\begin{aligned}\mathcal{U}_n(\chi)/\mathcal{U}_n^{(1)}(\chi) &= (\mathcal{V}_n(\chi)\mathcal{U}_0(\chi))/(\mathcal{V}_n^{(1)}(\chi)\mathcal{U}_0(\chi)) \\ &\cong \mathcal{V}_n(\chi)/(\mathcal{V}_n(\chi) \cap (\mathcal{V}_n^{(1)}(\chi)\mathcal{U}_0(\chi))). \qquad (14)\end{aligned}$$

For $x \in \mathcal{V}_n^{(1)}(\chi)$ and $y \in \mathcal{U}_0(\chi)$, assume that $xy \in \mathcal{V}_n(\chi)$. Then, as $y \in \mathcal{V}_n(\chi)$, it follows from (1) that $y^{2p^n} = N_{n,0}(y)^2 = 1$. Hence, y is contained in the $\mathbb{Z}$-torsion part $\mathrm{Tor}_{\mathbb{Z}}\,\mathcal{U}_0(\chi)$. By (1), we have $\mathrm{Tor}_{\mathbb{Z}}\,\mathcal{U}_0(\chi) = \mathcal{V}_0(\chi) \subseteq \mathcal{V}_n(\chi)$. Therefore, we see that $xy \in \mathcal{V}_n^{(1)}(\chi)$ as $\mathcal{U}_0 = \mathcal{U}_0^{(1)}$, and hence

$$\mathcal{V}_n(\chi) \cap (\mathcal{V}_n^{(1)}(\chi)\mathcal{U}_0(\chi)) = \mathcal{V}_n^{(1)}(\chi).$$

Thus we obtain the assertion from (14). □

Proof of Theorem. As $p \nmid [K : \mathbb{Q}]$, the ramification index of p in K equals $p-1$, and $\zeta_p - 1$ is a local parameter of a prime ideal of K over p. Let $(\zeta_p - 1) = \prod_{i=1}^{g} \mathfrak{P}_i$ be the prime decomposition of $\zeta_p - 1$ in K, and let f be the residue class degree of $\mathfrak{P}_i$. We have $(p-1)fg = [K : \mathbb{Q}]$. Denote by $\mathfrak{P}_{i,n}$ the unique prime ideal of K_n over $\mathfrak{P}_i$, and $\mathcal{O}_n$ the ring of integers of K_n. Letting $\mathfrak{A}_n = \prod_{i=1}^{g} \mathfrak{P}_{i,n}$, we see that $\mathcal{U}_n/\mathcal{U}_n^{(1)}$ is isomorphic to the group

$$\{x \in \mathcal{O}_n \mid x \equiv 1 \bmod \mathfrak{A}_n\}/\{x \in \mathcal{O}_n \mid x \equiv 1 \bmod \mathfrak{A}_n^{p^n}\}.$$

The order of this group equals

$$\prod_{i=1}^{g} |\mathfrak{P}_{i,n}/\mathfrak{P}_{i,n}^{p^n}| = \prod_{i=1}^{g} |\mathcal{O}_n/\mathfrak{P}_{i,n}^{p^n-1}| = p^{fg(p^n-1)}.$$

It follows that

$$\mathrm{ord}_p(|\mathcal{U}_n/\mathcal{U}_n^{(1)}|) = [K:\mathbb{Q}] \times \frac{p^n-1}{p-1}.$$

On the other hand, it follows from Lemma 5 that

$$|\mathcal{U}_n/\mathcal{U}_n^{(1)}| = \prod_{\chi} |\Lambda_\chi/J_{n,\chi}| \times \prod_{\chi}{}^{*} p^{nd_\chi}.$$

Here, in the first product $\prod_\chi$ (resp. the second product $\prod_\chi{}^{*}$), χ runs over a complete set of representatives of the $\mathbb{Q}_p$-conjugacy classes of all the $\bar{\mathbb{Q}}_p$-valued characters of Δ (resp. of those of type (B)). Thus, we obtain

$$\sum_{\chi} \mathrm{ord}_p(|\Lambda_\chi/J_{n,\chi}|) = [K:\mathbb{Q}] \times \frac{p^n-1}{p-1} - \sum_{\chi}{}^{*} nd_\chi.$$

We see from Lemma 4 that

$$\sum_{\chi} \mathrm{ord}_p(|\Lambda_\chi/I_{n,\chi}|) = [K:\mathbb{Q}] \times \frac{p^n-1}{p-1} - \sum_{\chi}{}^{*} nd_\chi.$$

by noting that $\sum_\chi d_\chi = [K:\mathbb{Q}]$. Now, we obtain Theorem from the above two formulas because we already know that $I_{n,\chi} \subseteq J_{n,\chi}$ by Lemma 3. $\square$

References

[1] Coleman R., *Division values in local fields.* Invent. Math., **53** (1979), 91-116.

[2] Coleman R., *Local units modulo circular units.* Proc. AMS., **89** (1983), 1–7.

[3] Gillard R., *Unités cyclotomiqués, unités semi-locales et $\mathbb{Z}_\ell$-extensions II.* Ann. Fourier Inst., **29** (1979), 1–15.

[4] Ichimura H., *On p-adic L-functions and normal bases of rings of integers.* J. Reine Angew. Math., **462** (1995), 169–184.

[5] Ichimura H., *On a normal integral basis problem over cyclotomic $\mathbb{Z}_p$-extensions.* J. Math. Soc. Japan, **48** (1996), 689–703.

[6] Ichimura H., *On some congruences for units of local p-cyclotomic fields.* Abh. Math. Semin. Univ. Hamburg, **66** (1996), 273–279.

[7] Ichimura H. and Sumida-Takahashi H., *Normal integral basis of an unramified quadratic extension over a cyclotomic $\mathbb{Z}_2$-extension.* J. Théor. Nombres Bordeaux, in press.

[8] Iwasawa K., *On some modules in the theory of cyclotomic fields.* J. Math. Soc. Japan, **16** (1964), 42–82.

[9] Sumida H., *Greenberg's conjecture and the Iwasawa polynomial.* J. Math. Soc. Japan, **49** (1997), 689–711.

[10] Washington L. C., *Introduction to Cyclotomic Fields (2nd ed.).* Springer, New York, 1997.

Faculty of Science
Ibaraki University
Bunkyo 2-1-1, Mito, 310-8512, Japan
E-mail: humio.ichimura.sci@vc.ibaraki.ac.jp