On the r-ramified r-abelian extension associated to a real abelian field of prime conductor

Humio Ichimura

Abstract

We fix an integer $n \geq 1$, a prime number ℓ with $\ell \nmid 2n$ and an integer $e \geq 0$. We deal with a prime number p of the form $p = 2n\ell^f + 1$. For $0 \leq t \leq f$, let K_t be the real cyclic field of degree ℓ^t contained in the pth cyclotomic field. For a prime number $r \neq \ell$, let $K_t^{(r)}/K_t$ be the cyclotomic $\mathbb{Z}_r$-extension and $\Omega_t/K_t^{(r)}$ the maximal r-ramified pro-r abelian extension. When the conductor of the decomposition field of r in $\mathbb{Q}(\zeta_{\ell^\infty})$ equals ℓ^e, we show that $\Omega_{f-1}K_f^{(r)} = \Omega_f$ if p (or f) is large enough with respect to n, ℓ and e.

1 Introduction

We fix an integer $n \geq 1$ and a prime number ℓ with $\ell \nmid 2n$. We deal with a prime number p of the form $p = 2n\ell^f + 1$. For such a prime number p and an integer t with $0 \leq t \leq f$, let K_t be the real cyclic field of degree ℓ^t contained in the pth cyclotomic field $\mathbb{Q}(\zeta_p)$:

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_t \subset \cdots \subset K_f.$$

Here, for an integer $m \geq 2$, ζ_m denotes a primitive mth root of unity. Let r be a prime number with $r \neq \ell$, and let $K_t^{(r)}/K_t$ be the cyclotomic $\mathbb{Z}_r$-extension, where $\mathbb{Z}_r$ denotes the (additive group of the) ring of r-adic integers. Let

2020 Mathematics Subject Classfication. Primary 11R23; Secondary 11R18.

$\Omega_t/K_t^{(r)}$ be the maximal r-ramified pro-r abelian extension. In other words, $\Omega_t/K_t^{(r)}$ is the maximal pro-r abelian extension unramified outside r. We have $\Omega_0 = K_0^{(r)}$ by [9, Lemma 1], and we have a tower

$$\Omega_0 K_f^{(r)} = K_f^{(r)} \subseteq \cdots \subseteq \Omega_t K_f^{(r)} \subseteq \cdots \subseteq \Omega_f.$$

Let $s \geq 0$ be an integer. In [10, Theorem 1.4], we dealt with the case where r is a primitive root modulo ℓ^2 and showed that $\Omega_{f-(s+1)} K_f^{(r)} = \Omega_f$ when $p = 2n\ell^f + 1$ (or f) is large enough with respect to n, ℓ and s. In particular, the following assertion holds when $s = 0$.

Theorem 1.1 ([10])**.** *Fix an integer $n \geq 1$ and a prime number ℓ with $\ell \nmid 2n$, and let r be a prime number which is a primitive root modulo ℓ^2. For a prime number $p = 2n\ell^f + 1$ with $f \geq 2$, the equality $\Omega_{f-1} K_f^{(r)} = \Omega_f$ holds when*

$$p = 2n\ell^f + 1 > (2(rn-1))^{\phi(2n\ell)}. \tag{1.1}$$

Here, $\phi(*)$ denotes the Euler function.

In this paper, we deal with the general case where r is not necessarily a primitive root modulo ℓ^2. Let D_r be the decomposition field of r in $\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}$. For $e \geq 0$, let P_e be the set of prime numbers r such that the conductor of D_r equals ℓ^e. Theorem 1.1 deals with those prime numbers r in P_0. The following is a generalization of Theorem 1.1 to the case $e \geq 1$.

Theorem 1.2. *Let n and ℓ be as in Theorem 1.1. Let $e \geq 1$ be an integer, and let r be a prime number with $r \in P_e$. For a prime number $p = 2n\ell^f + 1$ with $f > e$, the equality $\Omega_{f-1} K_f^{(r)} = \Omega_f$ holds when*

$$p = 2n\ell^f + 1 > (r\ell^e n - 2)^{\phi(2n\ell^e)}. \tag{1.2}$$

For $0 \leq t \leq f$, let h_t be the class number of K_t in the ordinary sense. It is known that h_t is divisible by h_{t-1} (Washington [14, Theorem 10.1]). The following assertion on the ratio h_f/h_{f-1} is an immediate consequence of Theorem 1.2. (For this, see [10, Remark 3.1].)

Proposition 1.1. *Let n, ℓ, $e \geq 1$ and $r \in P_e$ be as in Theorem 1.2. For a prime number $p = 2n\ell^f + 1$ with $f > e$, h_f/h_{f-1} is not divisible by r when the inequality (1.2) holds.*

Remark 1.1. (I) Let $\mathbb{B}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_\ell$-extension, and $\mathbb{B}_\infty^{(r)}/\mathbb{B}_\infty$ the cyclotomic $\mathbb{Z}_r$-extension. Regarding the pair $(K_f/\mathbb{Q}, K_f^{(r)})$ as analog of $(\mathbb{B}_\infty/\mathbb{Q}, \mathbb{B}_\infty^{(r)})$, assertions such as Theorems 1.1 and 1.2 correspond to some results in Friedman [1] and [8]. For details, see [10, Remark 1.2].

(II) For a prime number $r \neq \ell$, Horie [6, 7] studied the r-part of the class number in $\mathbb{B}_\infty$; for $r \in P_0$ in [6] and for a general r in [7]. Theorems 1.1 and 1.2 are shown by modifying some arguments in [6] and in [7], respectively.

(III) In contrast to the $\mathbb{Z}_\ell$-extension $\mathbb{B}_\infty/\mathbb{Q}$, the conductors of the layers K_t $(1 \leq t \leq f)$ of the finite ℓ-tower $K_f/\mathbb{Q}$ are obviously the same. This bothers us to study under what condition on $p = 2n\ell^f + 1$ or f, the equality $\Omega_t K_f^{(r)} = \Omega_f$ holds in the general case where $t < f - 1$ and $e \geq 1$, with the method in this paper.

(IV) An assertion similar to Theorem 1.1 holds also when $f = 1$ for a prime number r which is a primitive root modulo ℓ ([9, Theorem 1]). In Theorem 1.2, the inequality (1.2) does not hold when $f \leq e$.

Remark 1.2. Let $n = 1$ and $\ell = 3$. Using a method in Grau, Oller-Marcén and Sadornil [5], Shoichi Fujima computed, upon the request of the author, that for $f \leq 2000$, $p = 2 \cdot 3^f + 1$ is a prime number when

$$\begin{aligned} f \;=\; & 1, 2, 4, 5, 6, 9, 16, 17, 30, 54, 57, 60, 65, 132, 180, 320, \\ & 696, 782, 822, 897, 1252, 1454. \end{aligned}$$

For this type of prime numbers p, we dealt with in [10, Remark 1.1] the ratios $h_f/h_{f-(s+1)}$ $(s = 0, 1, 2)$.

A prime number r is contained in P_0 (resp. P_1) when $r \equiv 2, 5 \bmod 9$ (resp. $r \equiv 4, 7 \bmod 9$). When $r = 2$, 5 and 11, we see that the inequality (1.1) holds and hence $\Omega_{f-1} K_f^{(r)} = \Omega_f$ for all $f \geq 2$, $f \geq 4$ and $f \geq 5$, respectively. For a prime number $r \in P_0$ with $23 \leq r \leq 83$ (resp. $101 \leq r \leq 4637$), (1.1) holds for $f \geq 9$ (resp. $f \geq 16$). When $r = 7$ and 13, we see that (1.2) holds and hence $\Omega_{f-1} K_f^{(r)} = \Omega_f$ for $f \geq 5$ and $f \geq 6$, respectively. For a prime number $r \in P_1$ with $31 \leq r \leq 61$ (resp. $67 \leq r \leq 3067$), (1.2) holds for $f \geq 9$ (resp. $f \geq 16$).

We organize this paper as follows similarly to [10, Sections 2–6] where we showed [10, Theorem 1.4]. In Section 2, we recall several lemmas from [9, 10]. In Section 3, we derive an r-adic congruence on certain cyclotomic units of K_f assuming that $\Omega_{f-1} K_f^{(r)} \subsetneq \Omega_f$. In Section 4, we show that the

congruence does not hold under the assumption of Theorem 1.2, and obtain the theorem.

Lemmas in Sections 3 and 4 are similar to those in [10]. For some of them, we omit or only outline their proofs. However, we give full proofs of three lemmas in Section 3 (Lemmas 3.1–3.3) on the above mentioned cyclotomic units of K_f, because they contain new aspects caused by the general setting $r \in P_e$ with $e \geq 1$. A point of the aspects is the formula (3.1) in Section 3 on r-adic characters of $\mathrm{Gal}(K_f/\mathbb{Q})$, and the above mentioned cyclotomic units are defined by using (3.1). The formula is peculiar to the case $e \geq 1$, and it does not hold when $e = 0$ (the case we dealt with in [10]). In the proof of Lemma 3.1, we use the equality (3.1), and in the proof of Lemma 3.3, we use a property of an integer "a_0" related to the right hand side of (3.1).

2 Lemmas

In this section, we recall several lemmas from [9, 10] using the same notation as in [10].

Let Δ be a finite abelian group, and let r be a prime number with $r \nmid |\Delta|$. Let $\bar{\mathbb{Q}}_r$ be a fixed algebraic closure of the r-adic rational number field $\mathbb{Q}_r$. For a $\bar{\mathbb{Q}}_r$-valued character χ of Δ, let

$$e_\chi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \mathrm{Tr}_{\mathbb{Q}_r(\chi)/\mathbb{Q}_r}(\chi(\delta^{-1}))\delta \tag{2.1}$$

be the idempotent of the group ring $\mathbb{Z}_r[\Delta]$ associated to χ. Here, $\mathbb{Q}_r(\chi)$ is the subfield of $\bar{\mathbb{Q}}_r$ generated by the values of χ over $\mathbb{Q}_r$, and Tr denotes the trace map. Let $\mathcal{O}_\chi$ be the ring of integers of $\mathbb{Q}_r(\chi)$. For a module M over $\mathbb{Z}_r[\Delta]$, we denote by $M(\chi) = e_\chi M$ (or M^{e_χ}) the χ-part of M. We naturally regard $M(\chi)$ as a module over $\mathcal{O}_\chi$ as in [10, Section 2]. Let Φ_Δ be a complete set of representatives of the $\mathbb{Q}_r$-conjugacy classes of the $\bar{\mathbb{Q}}_r$-valued characters of Δ. Then, we have a canonical decomposition

$$M = \bigoplus_{\chi \in \Phi_\Delta} M(\chi). \tag{2.2}$$

Let K be a real abelian field and let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. Let r be a prime number with $r \nmid |\Delta|$, and let $K^{(r)}/K$ be the cyclotomic $\mathbb{Z}_r$-extension. Let $\Omega_K/K^{(r)}$ be the maximal pro-r abelian extension unramified outside r, and

put $\mathcal{G}_K = \mathrm{Gal}(\Omega_K/K^{(r)})$. Identifying $\mathrm{Gal}(K^{(r)}/\mathbb{Q}^{(r)})$ with Δ, we can naturally regard $\mathcal{G}_K$ as a module over $\mathbb{Z}_r[\Delta]$. Let χ be a nontrivial $\bar{\mathbb{Q}}_r$-valued character of Δ, which is also regarded as a primitive Dirichlet character of conductor f_χ. Let $\tilde{r} = 4$ or r according as $r = 2$ or $r \geq 3$, and let q be the least common multiple of f_χ and $\tilde{r}$. Iwasawa [11, §6] constructed a power series $g_\chi(T) \in \mathcal{O}_\chi[[T]]$ related to the r-adic L-function $L_r(s, \chi)$ by

$$g_\chi((1+q)^s - 1) = \frac{1}{2} L_r(s, \chi)$$

for $s \in \mathbb{Z}_r$. We denote by λ_χ^* the lambda invariant of the power series g_χ as in [10, Section 2]. For the trivial character χ_0 of Δ, we simply set $\lambda_{\chi_0}^* = 0$. The following lemma is a consequence of the Iwasawa main conjecture proved by Mazur and Wiles [12] and Greither [4], and is known to specialists. For a proof of this lemma, see [10, Lemma 2.1].

Lemma 2.1. *Under the above notation, the $\mathcal{O}_\chi$-module $\mathcal{G}_K(\chi)$ is isomorphic to λ_χ^* copies of $\mathcal{O}_\chi$.*

Remark 2.1. Under the above notation, let $r = 2$. Then, by Greenberg [3, Theorem 1], we have $\lambda_\chi^* \geq 1$ when $\chi(2) = 1$ and $\chi \neq \chi_0$.

Now, let n, ℓ be as in Theorem 1.1, and let $r \neq \ell$ be a prime number. Let $p = 2n\ell^f + 1$ be a prime number with $f \geq 1$, and let K_t, $K_t^{(r)}$, Ω_t with $0 \leq t \leq f$ be as in Section 1. We put $\Delta_f = \mathrm{Gal}(K_f/\mathbb{Q})$ and $\mathcal{G}_f = \mathcal{G}_{K_f} = \mathrm{Gal}(\Omega_f/K_f^{(r)})$. We naturally regard $\mathcal{G}_f$ as a module over $\mathbb{Z}_r[\Delta_f]$. Let Φ_t be a complete set of representatives of the $\mathbb{Q}_r$-conjugacy classes of the $\bar{\mathbb{Q}}_r$-valued characters of Δ_f with order ℓ^t. We write characters in Φ_t as χ_t with subscript t. Then, all the characters $\chi_t \in \Phi_t$ for all $0 \leq t \leq f$ constitute a complete set of representatives of the $\mathbb{Q}_r$-conjugacy classes of the $\bar{\mathbb{Q}}_r$-valued characters of Δ_f.

Lemma 2.2. *Under the above notation, let s be an integer with $0 \leq s \leq f-1$. Then, $\Omega_{f-(s+1)} K_f^{(r)} = \Omega_f$ holds if and only if $\lambda_{\chi_t}^* = 0$ for every $\chi_t \in \Phi_t$ with every $f - s \leq t \leq f$.*

Proof. This lemma was shown in [10, Lemma 3.2] (combined with [10, Lemma 3.3(A)]) when r is a primitive root modulo ℓ^2. Since it is shown similarly in the general case, we only outline its proof. Let τ be a generator of the cyclic

group $\Delta_f = \mathrm{Gal}(K_f^{(r)}/K_0^{(r)})$ of order ℓ^f. In the proof of [10, Lemma 3.2], we have seen that

$$\mathrm{Gal}(\Omega_f/\Omega_{f-(s+1)}K_f^{(r)}) = \mathcal{G}_f^{\tau^{\ell^{f-(s+1)}}-1_f},$$

where 1_f is the identity element of Δ_f. By (2.2), we have a decomposition

$$\mathcal{G}_f^{\tau^{\ell^{f-(s+1)}}-1_f} = \bigoplus_{t=0}^{f} \bigoplus_{\chi_t \in \Phi_t} \mathcal{G}_f(\chi_t)^{\chi_t(\tau)^{\ell^{f-(s+1)}}-1}.$$

From this and Lemma 2.1, we obtain the assertion similarly to [10, Lemma 3.2]. □

For a number field F, let $\widehat{F} = \prod_{\mathcal{R}} F_{\mathcal{R}}$ be the product of the completions $F_{\mathcal{R}}$ of F for all prime ideals $\mathcal{R}$ of F over r. The field F is diagonally embedded in the ring $\widehat{F}$; $F \subset \widehat{F}$. Let $\mathcal{U}_F\,(\subset \widehat{F}^\times)$ be the group of semi-local units of F at r.

We put $\mathcal{U}_f = \mathcal{U}_{K_f}$. Let C_f be the group of cyclotomic units of K_f in the sense of Sinnott [13, page 209], and let $\mathcal{C}_f$ be the topological closure of $C_f \cap \mathcal{U}_f$ in $\mathcal{U}_f$. The groups $\mathcal{U}_f$ and $\mathcal{C}_f$ are naturally regarded as modules over $\mathbb{Z}_r[\Delta_f]$. The following lemma is a consequence of a theorem of Gillard [2, Theorem 2] on semi-local units modulo cyclotomic units, and is known to specialists. For a proof of this lemma, see [10, Lemma 2.2].

Lemma 2.3. *Under the above notation, let $1 \le t \le f$ and $\chi_t \in \Phi_t$, and assume that $\chi_t(2) \ne 1$ when $r = 2$. Then, we have $\lambda_{\chi_t}^* \ge 1$ if and only if $\mathcal{C}_f(\chi_t) \subseteq \mathcal{U}_f(\chi_t)^r$.*

We put $L_f = \mathbb{Q}(\zeta_p)$. When $r \ne p$, we can define the Frobenius automorphism $\gamma = \gamma_r$ of L_f at r. Then, $\alpha^\gamma \equiv \alpha^r \bmod r\mathcal{O}_{L_f}$ for an integer α of L_f. The following lemma was shown in [9, Lemma 4].

Lemma 2.4. *Let $r \ne p$. For an integer α of L_f, the congruence $\alpha^\gamma \equiv \alpha^r \bmod r^2\mathcal{O}_{L_f}$ holds when α is an rth power in $\widehat{L}_f$.*

Let L_f^+ be the maximal real subfield of L_f. Then, $\zeta_p + \zeta_p^{-1}$ is a cyclotomic unit of L_f^+, and $K_t \subseteq L_f^+$. We define a cyclotomic unit ϵ_t of K_t by

$$\epsilon_t = \mathrm{N}_{L_f^+/K_t}(\zeta_p + \zeta_p^{-1}),$$

where N denotes the norm map. The following lemma was shown in [10, Lemma 4.1].

Lemma 2.5. *For $1 \le t \le f$, we have $\epsilon_t = \pm 1$ if and only if $2^{2n\ell^{f-t}} \equiv 1 \bmod p$.*

3 Congruence on cyclotomic units

Let n, ℓ, $e \geq 1$ and $r \in P_e$ be as in Theorem 1.2, and let $p = 2n\ell^f + 1$ be a prime number with $f > e$. Under this setting, the extreme case $r = p$ is excluded (see Lemma 2.4); because if $r = p = 2n\ell^f + 1$, then r splits completely in $\mathbb{Q}(\zeta_{\ell^f})$, but $r \in P_e$ and $f > e$. We use the same notation as in the previous sections. Let L_0 be the subfield of $L_f = \mathbb{Q}(\zeta_p)$ of degree $2n$, so that we can identify the Galois group $\Delta_f = \mathrm{Gal}(K_f/\mathbb{Q})$ with $\mathrm{Gal}(L_f/L_0)$. We fix an arbitrary primitive root g modulo p. Let $\sigma = \sigma_g$ be the automorphism of L_f sending ζ_p to ζ_p^g, and set

$$\tau = \sigma^{2n}.$$

The Galois groups Δ_f and $\mathrm{Gal}(L_f/K_f)$ are generated by τ and σ^{ℓ^f}, respectively. Let $\mathfrak{D}_e = \Delta_f^{\ell^{f-e}} = \langle \tau^{\ell^{f-e}} \rangle$ be the subgroup of Δ_f of order ℓ^e. In the rest of this section, we *fix* a character $\chi_f \in \Phi_f$. Let $\psi = \chi_{f|\mathfrak{D}_e}$ be the restriction of χ_f to $\mathfrak{D}_e$, whose order is ℓ^e. As $r \in P_e$ and $e \geq 1$, the degree of the extension $\mathbb{Q}_r(\chi_f) = \mathbb{Q}_r(\zeta_{\ell^f})$ over $\mathbb{Q}_r(\zeta_{\ell^e})$ equals ℓ^{f-e}. Hence, for $0 \leq i \leq \ell^f - 1$, noting that $\chi_f(\tau^i)$ is an ℓ^eth root of unity if and only if ℓ^{f-e} divides i, we see that

$$\mathrm{Tr}_{\mathbb{Q}_r(\chi_f)/\mathbb{Q}_r}(\chi_f(\tau^i)) = \begin{cases} \ell^{f-e}\mathrm{Tr}_{\mathbb{Q}_r(\zeta_{\ell^e})/\mathbb{Q}_r}(\chi_f(\tau^i)), & \text{when } \ell^{f-e}|i, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, we see from the definition (2.1) of the idempotent associated to a $\bar{\mathbb{Q}}_r$-valued character that

$$e_{\chi_f} = e_\psi \in \mathbb{Z}_r[\mathfrak{D}_e]. \tag{3.1}$$

We choose and fix an element

$$\tilde{e}_\psi = \sum_{i=0}^{\ell^e-1} d_i \cdot \tau^{\ell^{f-e} \cdot i} \in \mathbb{Z}[\mathfrak{D}_e] \quad \text{with} \quad d_i \in \mathbb{N} \tag{3.2}$$

such that $\tilde{e}_\psi \equiv e_\psi \bmod r\mathbb{Z}_r[\mathfrak{D}_e]$ and

$$\sum_{i=0}^{\ell^e-1} d_i \equiv 0 \bmod 2r. \tag{3.3}$$

The cyclotomic unit ϵ_f of K_f, which appeared at the end of Section 2, is expressed as follows:

$$\epsilon_f = \mathrm{N}_{L_f^+/K_f}(\zeta_p + \zeta_p^{-1}) = \prod_{j=0}^{n-1}(\zeta_p^{g^{\ell f \cdot j}} + \zeta_p^{-g^{\ell f \cdot j}}).$$

We put

$$\pi_f = \epsilon_f^{\tilde{e}_\psi} \tag{3.4}$$

and

$$\eta_f = \prod_{j=0}^{n-1}(\zeta_p^{g^{\ell f \cdot j}} + 1) \quad \text{and} \quad \xi_f = \eta_f^{\tilde{e}_\psi}. \tag{3.5}$$

The cyclotomic unit ξ_f of L_f, which depends on χ_f, plays a role for showing Theorem 1.2.

Lemma 3.1. *Assume that $2^{2n} \equiv 1 \bmod p$ or $\lambda^*_{\chi_f} \geq 1$. Then, the congruence $\xi_f^\gamma \equiv \xi_f^r \bmod r^2\mathcal{O}_{L_f}$ holds.*

Proof. As we mentioned at the beginning of this section, we have $r \neq p$. Let ϱ be the Frobenius automorphism of L_f at the prime 2. Then, as $r \neq p$, we can write $\eta_f^\varrho = \zeta_p^{ar}\epsilon_f$ with some $a \in \mathbb{Z}$. It follows that $\xi_f^\varrho = \zeta_p^{br}\pi_f$ with some $b \in \mathbb{Z}$. Therefore, because of Lemma 2.4, it suffices to show that π_f is an rth power in $\widehat{L}_f$.

When $2^{2n} \equiv 1 \bmod p$, we have $\epsilon_f = \pm 1$ by Lemma 2.5, and hence $\pi_f = 1$ by (3.2), (3.3) and (3.4). The condition $2^{2n} \not\equiv 1 \bmod p$ is equivalent to $\chi_f(2) \neq 1$. Noting this, we see that when $2^{2n} \not\equiv 1 \bmod p$ and $\lambda^*_{\chi_f} \geq 1$, π_f is an rth power in $\widehat{L}_f$ by (3.1), (3.4) and Lemma 2.3. □

Let I (resp. J) be the set of integers i (resp. j) with $0 \leq i \leq \ell^e - 1$ (resp. $0 \leq j \leq n-1$), and set $H = I \times J$. For a pair $(a, b) \in H$, let $H_{a,b} = H \backslash \{(a, b)\}$ and let $\Theta_{a,b}$ be the set of maps from $H_{a,b}$ to $\{0, 1\}$. We write a map in $\Theta_{a,b}$ as $\theta_{a,b}$, $\rho_{a,b}$ with subscripts a, b. We put $\mathbf{v} = \mathbf{v}_{f,e} = (2n\ell^{f-e}, \ell^f)$, and for a pair $(i, j) \in H$, we set

$$\mathbf{v} \cdot (i, j) = 2n\ell^{f-e}i + \ell^f j.$$

For a pair $(a,b) \in H$, a map $\theta_{a,b} \in \Theta_{a,b}$ and an integer k with $1 \leq k \leq r-1$, we put

$$B(\theta_{a,b}) = B((a,b),\theta_{a,b}) = \sum_{(i,j)\in H_{a,b}} \theta_{a,b}((i,j))g^{\mathbf{v}\cdot(i,j)},$$

$$A(k,\theta_{a,b}) = A(k,(a,b),\theta_{a,b}) = kg^{\mathbf{v}\cdot(a,b)} + rB(\theta_{a,b}),$$

and

$$c_k = \frac{1}{r}\cdot {}_rC_k.$$

Here, ${}_rC_k$ is the binomial coefficient. Then, Lemma 3.1 is rephrased as follows.

Lemma 3.2. *Assume that* $2^{2n} \equiv 1 \bmod p$ *or* $\lambda^*_{\chi_f} \geq 1$. *Then, the congruence*

$$\sum_{k=1}^{r-1} \sum_{(a,b)\in H} \sum_{\theta_{a,b}} c_k d_a \zeta_p^{A(k,\theta_{a,b})} \equiv 0 \bmod r\mathcal{O}_{L_f} \tag{3.6}$$

holds. Here, in the third sum, $\theta_{a,b}$ *runs over the maps in* $\Theta_{a,b}$.

Proof. Noting that $\tau = \sigma^{2n}$, we see from (3.2) and (3.5) that

$$\xi_f = \prod_{i=0}^{\ell^e-1}\prod_{j=0}^{n-1}\left((\zeta_p^{g^{\ell f\cdot j}}+1)^{\tau^{\ell f - e\cdot i}}\right)^{d_i} = \prod_{(i,j)\in H}(\zeta_p^{g^{\mathbf{v}\cdot(i,j)}}+1)^{d_i}. \tag{3.7}$$

It follows that

$$\xi_f^{\gamma} = \prod_{(i,j)\in H}(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)^{d_i}. \tag{3.8}$$

For an integer $b \geq 1$, we can show that

$$(T+1)^{rb} \equiv (T^r+1)^{b-1} \times \left((T^r+1) + rb\sum_{k=1}^{r-1} c_k T^k\right) \bmod r^2\mathbb{Z}[T]$$

by induction on b. Then, we see from (3.7) that

$$\xi_f^r \equiv \prod_{(i,j)\in H}\left\{(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)^{d_i-1} \times \left((\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1) + rd_i\sum_{k=1}^{r-1} c_k\zeta_p^{kg^{\mathbf{v}\cdot(i,j)}}\right)\right\}$$

modulo $r^2\mathcal{O}_{L_f}$. Now, assume that $2^{2n} \equiv 1 \bmod p$ or $\lambda^*_{\chi_f} \geq 1$. Then, $\xi_f^\gamma \equiv \xi_f^r \bmod r^2\mathcal{O}_{L_f}$ by Lemma 3.1. Therefore, we observe from (3.8) and the above congruence on ξ_f^r that

$$\begin{aligned}\prod_{(i,j)\in H}(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1) &\equiv \prod_{(i,j)\in H}\left((\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)+rd_i\sum_{k=1}^{r-1}c_k\zeta_p^{kg^{\mathbf{v}\cdot(i,j)}}\right)\\ &\equiv \prod_{(i,j)\in H}(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)+rX \bmod r^2\mathcal{O}_{L_f}\end{aligned}$$

with

$$X=\sum_{(a,b)\in H}\sum_{k=1}^{r-1}\left(d_ac_k\zeta_p^{kg^{\mathbf{v}\cdot(a,b)}}\times\prod_{(i,j)\in H_{a,b}}(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)\right).$$

It follows that $X \equiv 0 \bmod r\mathcal{O}_{L_f}$. We easily see that

$$\prod_{(i,j)\in H_{a,b}}(\zeta_p^{rg^{\mathbf{v}\cdot(i,j)}}+1)=\sum_{\theta_{a,b}}\zeta_p^{rB(\theta_{a,b})}.$$

Therefore, we see from the above that

$$X=\sum_{k=1}^{r-1}\sum_{(a,b)\in H}\sum_{\theta_{a,b}}c_kd_a\zeta_p^{A(k,\theta_{a,b})}\equiv 0 \bmod r\mathcal{O}_{L_f},$$

and we obtain the assertion. □

Since $\tilde{e}_\psi \not\equiv 0 \bmod r\mathbb{Z}_r[\mathfrak{D}_e]$, we can choose and fix an integer $a_0 = a_0(\chi_f) \in I$ with $r \nmid d_{a_0}$. We see that a_0 actually depends on χ_f or $\psi = \chi_{f|\mathfrak{D}_e}$ in Remark 3.1 at the end of this section.

Lemma 3.3. *Let $a_0 = a_0(\chi_f)$. Assume that there exists a map $\varphi_{a_0,0} \in \Theta_{a_0,0}$ such that*

$$A(k,\theta_{a,b}) \not\equiv A(1,\varphi_{a_0,0}) \bmod p$$

for all triples $(k,(a,b),\theta_{a,b}) \neq (1,(a_0,0),\varphi_{a_0,0})$. Then, $2^{2n} \not\equiv 1 \bmod p$ and $\lambda^*_{\chi_f} = 0$.

Proof. Assume to the contrary that $2^{2n} \equiv 1 \bmod p$ or $\lambda^*_{\chi_f} \geq 1$. Then, the congruence (3.6) in Lemma 3.2 holds. Dividing the both sides of (3.6) by $\zeta_p^{A(1,\varphi_{a_0,0})}$, we see that

$$Y=c_1d_{a_0}+{\sum}'c_kd_a\zeta_p^{A(k,\theta_{a,b})-A(1,\varphi_{a_0,0})}\equiv 0 \bmod r\mathcal{O}_{L_f}.$$

Here, in the sum $\sum'$, the symbols k, (a,b) and $\theta_{a,b}$ run over the triples $(k,(a,b),\theta_{a,b}) \neq (1,(a_0,0),\varphi_{a_0,0})$. Since the exponents of ζ_p in the sum $\sum'$ are not divisible by p, we see that

$$\begin{aligned}\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Y) &= c_1 d_{a_0}(p-1) - \sum{}' c_k d_a = c_1 d_{a_0} p - \sum_k \sum_{(a,b)} \sum_{\theta_{a,b}} c_k d_a \\ &= c_1 d_{a_0} p - (\sum_k c_k)\cdot(\sum_a d_a)\cdot n \cdot 2^{\ell^e n-1} \equiv 0 \bmod r.\end{aligned}$$

Then, it follows from (3.3) that $c_1 d_{a_0} p = d_{a_0} p \equiv 0 \bmod r$. Since we have chosen a_0 so that $r \nmid d_{a_0}$, we obtain $r = p$. However, this is impossible as we mentioned at the beginning of this section. □

Remark 3.1. (I) When $r \nmid (\ell-1)$, we can choose $a_0 = 0$. Actually, $\ell^e \cdot d_0 \equiv [\mathbb{Q}_r(\zeta_{\ell^e}) : \mathbb{Q}_r] \bmod r$ by the definition of the idempotent e_ψ and (3.2), and $[\mathbb{Q}_r(\zeta_{\ell^e}) : \mathbb{Q}_r]$ is a divisor of $\ell - 1$ as $r \in P_e$ and $e \geq 1$. It follows that $r \nmid d_0$ when $r \nmid (\ell-1)$.

(II) In general, the integer a_0 depends on (the $\mathbb{Q}_r$-conjugacy class of) the character χ_f or $\psi = \chi_{f|\mathfrak{D}_e}$. Actually, let $\ell = 17$ and $r = 2$. Then, $2 \in P_1$ and the order of 2 mod 17 is 8. We choose a primitive ℓth root $\zeta = \zeta_\ell$ of unity in $\bar{\mathbb{Q}}_2$ and a square root $\sqrt{\ell}$ in $\mathbb{Q}_2$ so that

$$\mathrm{Tr}_{\mathbb{Q}_2(\zeta)/\mathbb{Q}_2}(\zeta) = \frac{-1+\sqrt{\ell}}{2} \equiv 0 \bmod 2\mathbb{Z}_2.$$

Then, for i with $\ell \nmid i$, $\mathrm{Tr}_{\mathbb{Q}_2(\zeta)/\mathbb{Q}_2}(\zeta^i) \equiv 0$ or 1 modulo $2\mathbb{Z}_2$ according as i is a square modulo ℓ or not. Let ρ be a generator of the cyclic group $\mathfrak{D}_1$ of order ℓ, and let ψ_1 (resp. ψ_2) be the character of $\mathfrak{D}_1$ sending ρ to ζ (resp. ζ^3). Then, we see that ψ_1 and ψ_2 are not conjugate over $\mathbb{Q}_2$ and that

$$e_{\psi_1} \equiv \sum_i{}' \rho^i \bmod 2\mathbb{Z}_2[\mathfrak{D}_1] \quad \text{and} \quad e_{\psi_2} \equiv \sum_i{}'' \rho^i \bmod 2\mathbb{Z}_2[\mathfrak{D}_1],$$

where in the first (resp. second) sum, i runs over the integers $1 \leq i \leq 16$ which are non-square (resp. square) modulo ℓ.

4 Proof of Theorem 1.2

Let n, ℓ, $e \geq 1$ and $r \in P_e$ be as in Theorem 1.2, and we use the same notation as in the previous sections. Let ζ_{ℓ^e} (resp. ζ_{2n}) be a fixed primitive ℓ^eth (resp.

$2n$th) root of unity in the complex field $\mathbb{C}$. In this section, we work in the $2n\ell^e$th cyclotomic field $M = \mathbb{Q}(\zeta_{\ell^e}, \zeta_{2n})$ contained in $\mathbb{C}$. In the following, k and m denote integers in the range $[1, r-1]$, (a, b) and (c, d) denote pairs in H, and $\theta_{a,b}$ and $\rho_{c,d}$ denote maps in $\Theta_{a,b}$ and $\Theta_{c,d}$, respectively. We put

$$\beta(\theta_{a,b}) = \beta((a,b), \theta_{a,b}) = \sum_{(i,j)\in H_{a,b}} \theta_{a,b}((i,j))\zeta_{\ell^e}^i \zeta_{2n}^j$$

and

$$\alpha(k, \theta_{a,b}) = \alpha(k, (a,b), \theta_{a,b}) = k\zeta_{\ell^e}^a \zeta_{2n}^b + r\beta((a,b), \theta_{a,b}).$$

On these integers of M, the following assertions hold.

Lemma 4.1. *Let $(m, (c,d)) \neq (k, (a,b))$. Then, $\alpha(m, \rho_{c,d}) \neq \alpha(k, \theta_{a,b})$ for any $\rho_{c,d} \in \Theta_{c,d}$ and any $\theta_{a,b} \in \Theta_{a,b}$.*

Lemma 4.2. *For each $u \in I$, there exists a map $\varphi_{u,0} \in \Theta_{u,0}$ such that $\alpha(1, \theta_{u,0}) \neq \alpha(1, \varphi_{u,0})$ for any map $\theta_{u,0} \in \Theta_{u,0}$ with $\theta_{u,0} \neq \varphi_{u,0}$.*

Lemma 4.1 is shown similarly to [10, Lemma 6.1(II)]. Lemma 4.2 is shown using [6, Lemma 7] similarly to [10, Lemmas 6.3, 6.4].

For a positive integer T, let $\mathrm{Supp}(T)$ be the finite set of prime numbers dividing T. For each $u \in I$, we choose and fix a map $\varphi_{u,0} \in \Theta_{u,0}$ as in Lemma 4.2, and we define a set

$$\mathbb{P}_u = \mathbb{P}_{n,\ell,e,r,\varphi_{u,0}}$$

to be the union of the sets

$$\mathrm{Supp}\left(\mathrm{N}_{M/\mathbb{Q}}(\alpha(k, \theta_{a,b}) - \alpha(1, \varphi_{u,0}))\right)$$

for all triples $(k, (a,b), \theta_{a,b}) \neq (1, (u,0), \varphi_{u,0})$. By Lemmas 4.1 and 4.2, $\mathbb{P}_u$ is actually a finite set of prime numbers.

Lemma 4.3. *We have $p < (r\ell^e n - 2)^{\phi(2n\ell^e)}$ for every prime number $p \in \mathbb{P}_u$ with every $u \in I$.*

Proof. We put $x = \alpha(k, \theta_{a,b}) - \alpha(1, \varphi_{u,0})$. Then, similarly as in the proof of [10, Lemma 6.5], we can show that $|\iota(x)| \leq r\ell^e n - 2$ for every embedding $\iota : M \hookrightarrow \mathbb{C}$. The assertion follows from this. □

Lemma 4.4. *Let n, ℓ, $e \geq 1$ and $r \in P_e$ be as in Theorem 1.2. Let $p = 2n\ell^f + 1$ be a prime number with $f > e$, and let $\chi_f \in \Phi_f$ with $a_0 = a_0(\chi_f)$. Then, we have $2^{2n} \not\equiv 1 \bmod p$ and $\lambda^*_{\chi_f} = 0$ when $p \notin \mathbb{P}_{a_0}$.*

Proof. It suffices to show that the assumption of Lemma 3.3 is satisfied. As $f > e$, $p \equiv 1 \bmod 2n\ell^e$ and so p splits completely in M. We fix a prime ideal $\mathfrak{P}$ of M over p. Then, the condition $p \notin \mathbb{P}_{a_0}$ implies that

$$\alpha(k, \theta_{a,b}) \not\equiv \alpha(1, \varphi_{a_0,0}) \bmod \mathfrak{P} \tag{4.1}$$

for all triples $(k, (a, b), \theta_{a,b}) \neq (1, (a_0, 0), \varphi_{a_0,0})$. Re-choosing a primitive root g modulo p in Section 3 so that $g^{2n\ell^{f-e}} \equiv \zeta_{\ell^e}$ and $g^{\ell^f} \equiv \zeta_{2n}$ modulo $\mathfrak{P}$, we can show from (4.1) that the assumption of Lemma 3.3 is satisfied exactly similarly as in the proof of [10, Theorem 6.1]. □

Proof of Theorem 1.2. Assume that a prime number $p = 2n\ell^f + 1$ with $f > e$ satisfies the inequality (1.2). Then, by Lemma 4.3, $p \notin \mathbb{P}_{a_0}$ with $a_0 = a_0(\chi_f)$ for every $\chi_f \in \Phi_f$. Therefore, we obtain the assertion from Lemma 2.2 with $s = 0$ and Lemma 4.4. □

Acknowledgement. The author thanks S. Fujima for the computation on the prime numbers of the form $p = 2 \cdot 3^f + 1$, which is referred to in Remark 1.2. The author is grateful to the referees for several valuable comments which improved the presentation of the paper.

References

[1] E. Friedman: *Ideal class groups in basic $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extensions of abelian number fields,* Invent. Math. **65** (1982), 425–440.

[2] R. Gillard: *Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions,* Ann. Inst. Fourier (Grenoble) **29** (1977), 1–15.

[3] R. Greenberg: *On 2-adic L-functions and cyclotomic invariants,* Math. Z. **159** (1978), 37–45.

[4] C. Greither: *Class groups of abelian fields, and the main conjecture,* Ann. Inst. Fourier (Grenoble) **42** (1992), 449–499.

[5] J. M. Grau, A. M. Oller-Marcén and D. Sadornil: *A primarity test for $Kp^n + 1$ numbers,* Math. Comp. **84** (2015), 505–512.

[6] K. Horie: *Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field,* J. London Math. Soc. **66** (2002), 257–275.

[7] K. Horie: *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field,* Tohoku Math. J. **57** (2005), 375–394.

[8] H. Ichimura: *On the class group of a cyclotomic $\mathbb{Z}_p \times \mathbb{Z}_\ell$-extension,* Acta Arith. **150** (2011), 263–283.

[9] H. Ichimura: *Triviality of Iwasawa module associated to some abelian field of prime conductor,* Abh. Math. Semin. Univ. Hambg. **88** (2018), 51–66.

[10] H. Ichimura: *On class numbers inside the real pth cyclotomic field,* Kodai Math. J. **47** (2024), 11–33.

[11] K. Iwasawa: Lectures on p-Adic L-Functions, Annals of Mathematical Studies, vol. 74, Princeton Univ. Press, Princeton, 1972.

[12] B. Mazur and A. Wiles: *Class fields of abelian extensions of $\mathbb{Q}$,* Invent. Math. **76** (1984), 179–330.

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

[14] L. C. Washington: Introduction to Cyclotomic Fields, second edition, Springer, New York, 1997.

Humio Ichimura
Professor Emeritus, Ibaraki University
4-31-19, Imanari
Kawagoe, 350-1105
Japan
E-mail: humio.ichimura.sci@vc.ibaraki.ac.jp