Normal integral basis of an unramified quadratic extension over a cyclotomic $\mathbb{Z}_2$-extension

Humio Ichimura and Hiroki Sumida-Takahashi

Abstract

Let ℓ be an odd prime number. Let $K/\mathbb{Q}$ be a real cyclic extension of degree ℓ, A_K the 2-part of the ideal class group of K, and H/K the class field corresponding to A_K/A_K^2. Let K_n be the nth layer of the cyclotomic $\mathbb{Z}_2$-extension over K. We consider the questions (Q1) "does H/K has a normal integral basis ?", and (Q2) "if not, does the pushed-up extension HK_n/K_n has a normal integral basis for some $n \geq 1$?" Under some assumptions on ℓ and K, we answer these questions in terms of the 2-adic L-function associated to the base field K. We also give some numerical examples.

1 Introduction

We fix an odd prime number ℓ. Let $K/\mathbb{Q}$ be a real cyclic extension of degree ℓ, and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. We denote by K_∞/K the cyclotomic $\mathbb{Z}_2$-extension, and by K_n the nth layer of K_∞/K with $K_0 = K$. Let $A_n = Cl_{K_n}(2)$ be the 2-part of the ideal class group of K_n, and H/K the class field corresponding to the quotient A_0/A_0^2. We say that a Galois extension N/F of a number field F with group G has a normal integral basis (NIB for short) when $\mathcal{O}_N$ is cyclic over the group ring $\mathcal{O}_F[G]$. Here, $\mathcal{O}_F$ denotes the ring of integers of F. In this paper, we deal with the following two questions:

Q 1. Does the extension H/K has a NIB ?

Q 2. If not, does the pushed-up extension HK_n/K_n has a NIB for some $n \geq 1$?

The first question is of classical nature. Some fundamental results on this type of questions are given in Brinkhuis [1] and Childs [3]. One of them asserts that an unramified abelian extension N/F of a totally real number field F has a NIB only when it is a composite of quadratic extensions of F ([1, Corollary 2.10]). This is a reason that we deal with the class field H corresponding to A_0/A_0^2 and not the whole Hilbert class field of K. It is conjectured that the ideal class group A_0 capitulates in K_n for some n (Greenberg's conjecture). The second one is an analogous question for the integer ring $\mathcal{O}_H$ of H. For some topics/results closely related to these two questions, see Remarks 1 and 2 at the end of this section.

We work under the assumptions:

A 1. The prime number 2 is a primitive root modulo ℓ.

A 2. The prime number 2 remains prime in K.

We fix a nontrivial $\bar{\mathbb{Q}}_2$-valued character χ of Δ, which we often regard as a primitive Dirichlet character. Because of the assumption (A1), all such characters are conjugate over $\mathbb{Q}_2$ with each other. The assumption (A2) implies that $\chi(2) \neq 1$. Let $\mathcal{O}_\chi = \mathbb{Z}_2[\zeta_\ell]$ be the subring of $\bar{\mathbb{Q}}_2$ generated over $\mathbb{Z}_2$ by the values of χ. Here, $\mathbb{Z}_2$ is the ring of 2-adic integers, $\mathbb{Q}_2$ the field of 2-adic rationals and $\bar{\mathbb{Q}}_2$ a fixed algebraic closure of $\mathbb{Q}_2$. Further, for an integer $m \geq 2$, ζ_m denotes a primitive mth root of unity. For a module M over $\mathbb{Z}_2[\Delta]$ and a $\bar{\mathbb{Q}}_2$-valued character ψ of Δ, $M(\psi)$ denotes the ψ-component of M. Then, because of (A1), M is decomposed as

$$M = M(\chi_0) \oplus M(\chi), \tag{1}$$

where χ_0 is the trivial character of Δ. Further, we can naturally regard the $\mathbb{Z}_2[\Delta]$-module $M(\chi)$ as a module over $\mathcal{O}_\chi$. It is well known that $A_n(\chi_0)$ is trivial for all $n \geq 0$ (see Washington [26, Theorem 10.4(b)]). Hence, we have

$$A_n = A_n(\chi). \tag{2}$$

Because of the assumption (A1), we have $\mathcal{O}_\chi \cong \mathbb{Z}_2^{\oplus(\ell-1)}$ as $\mathbb{Z}_2$-modules. It follows that

$$|A_0| = |A_0(\chi)| = 2^{\kappa(\ell-1)}$$

for some $\kappa \geq 0$. Let f_χ be the conductor of χ. By Iwasawa, there exists a unique power series $g_\chi(t) \in \mathcal{O}_\chi[[t]]$ related to the 2-adic L-function $L_2(s, \chi)$ by

$$g_\chi((1+4f_\chi)^{1-s} - 1) = \frac{1}{2} L_2(s, \chi).$$

We denote by $P_\chi(t) \in \mathcal{O}_\chi[t]$ the distinguished polynomial associated to $g_\chi(t)$, and put $\lambda_\chi = \deg P_\chi$. By a theorem of Ferrero and Washington [26, Theorem 7.15], $g_\chi(t)$ is not divisible by a prime element of $\mathcal{O}_\chi$. Hence, $g_\chi(t)$ equals $P_\chi(t)$ times a unit of $\mathcal{O}_\chi[[t]]$.

Lemma 1. *Under the assumptions* (A1) *and* (A2)*, the class group A_0 is nontrivial* (*i.e.*, $\kappa \geq 1$) *if and only if $\lambda_\chi \geq 1$.*

We denote by H_{nib} the composite of the subextensions of H/K with NIB. Then we see that H_{nib}/K has a NIB by a well known theorem of rings of integers (see Theorem (2.13) in Chapter 3 of Fröhlich and Taylor [5]). Namely, H_{nib}/K is the maximal subextension of H/K having a NIB. Clearly H_{nib} is Galois over $\mathbb{Q}$, and hence $\mathrm{Gal}(H_{nib}/K) = \mathrm{Gal}(H_{nib}/K)(\chi)$ is naturally regarded as an $\mathcal{O}_\chi$-module. Here, the equality holds because of (1) and (2). Using some result in the above mentioned paper [3], we can show that $\mathrm{Gal}(H_{nib}/K) \cong \mathcal{O}_\chi/2$ if it is nontrivial (see Lemma 8 in §3). Here and in what follows, we abbreviate as $\mathcal{O}_\chi/\alpha = \mathcal{O}_\chi/\alpha\mathcal{O}_\chi$ for an element $\alpha \in \mathcal{O}_\chi$.

Theorem 1. *Under the assumptions* (A1) *and* (A2)*, let $|A_0| = 2^{\kappa(\ell-1)}$ for some $\kappa \geq 1$. Then the following two assertions hold.*

(I) *We have $2^\kappa | P_\chi(0)$.*

(II) *The extension H_{nib}/K is nontrivial if and only if $P_\chi(0) \equiv 0 \bmod 2^{\kappa+1}$.*

From now on, we assume that

A 3. $A_0 \cong \mathcal{O}_\chi/2^\kappa$ with some $\kappa \geq 1$.

Under this assumption, we have $\mathrm{Gal}(H/K) \cong \mathcal{O}_\chi/2$ and $H_{nib} = H$ or K. The following is an immediate consequence of Theorem 1.

Theorem 2. *Under the assumptions* (A1)-(A3)*, the $\mathcal{O}_\chi/2$-extension H/K has a NIB if and only if $P_\chi(0) \equiv 0 \bmod 2^{\kappa+1}$.*

In view of Theorem 2, we assume that

A 4. $2^\kappa \| P_\chi(0)$

for dealing with the capitulation problem (Q2). Further, we assume the following stronger version of Greenberg's conjecture.

A 5. $|A_0| = |A_1|$.

Let ${}_2A_0$ be the elements $c \in A_0$ with $c^2 = 1$. We can show that (A5) implies that $|A_0| = |A_n|$ for all $n \geq 1$ and that ${}_2A_0$ is contained in the kernel of the natural lifting map $A_0 \to A_1$, using Nakayama's lemma (see Fukuda [4]).

When $\lambda_\chi = 1$ and $2^\kappa \| P_\chi(0)$, we have $P_\chi(t) = t + 2^\kappa\theta$ for some unit $\theta \in \mathcal{O}_\chi^\times$.

Theorem 3. *Under the assumptions* (A1)-(A5)*, assume further that* $\lambda_\chi = 1$.

(I) *The case* $\kappa = 1$. *When* $\theta \equiv 1 \bmod 2$*,* HK_1/K_1 *has a NIB. When* $\theta \not\equiv 1 \bmod 2$*,* HK_n/K_n *has no NIB for any* n.

(II) *The case* $\kappa \geq 2$. *The extension* HK_n/K_n *has no NIB for any* $n \geq 1$.

Theorem 4. *Under the assumptions* (A1)-(A5)*, assume further that* $\lambda_\chi \geq 2$.

(I) *The case* $\kappa = 1$. *The pushed-up extension* HK_2/K_2 *has a NIB, while* HK_1/K_1 *has no NIB.*

(II) *The case* $\kappa \geq 2$. *The extension* HK_1/K_1 *has a NIB.*

We prove these theorems in §3 and 4 after introducing several lemmas in §2.

In §5, we let $\ell = 3$, and handle a cyclic cubic field K of a prime conductor p with $p \equiv 1 \bmod 3$ and $p < 10^4$. We computed the class groups A_0, A_1, and the values λ_χ, $v_0 = \mathrm{ord}_2(P_\chi(0))$, $v_1 = \mathrm{ord}_2(P_\chi(-2))$ for each such K when it satisfies (A2). Here, $\mathrm{ord}_2(*)$ denotes the additive 2-adic valuation on $\bar{\mathbb{Q}}_2$ with $\mathrm{ord}_2(2) = 1$. The value v_1 is necessary when we apply Theorem 3. Actually, under the setting of Theorem 3(I), we have the following equivalence:

$$\theta \equiv 1 \bmod 2 \Longleftrightarrow v_1 \geq 2.$$

We give a table of these data for those p with $|A_0| > 1$, from which we can immediately check whether or not each condition in Theorems 3 and 4 is satisfied.

Remark 1. Let p be an *odd* prime number. Theorem 1 is quite analogous to a theorem of Taylor [23] (resp. Srivastav and Venkataraman [22]) which deals with an unramified cyclic extension of degree p over the p-cyclotomic field $\mathbb{Q}(\zeta_p)$ (resp. an unramified quadratic extension over a real quadratic field). Let F be an imaginary abelian field with $\zeta_p \in F$ with $p \nmid h_F^+$ satisfying some additional conditions, and F_n the nth layer of the cyclotomic $\mathbb{Z}_p$-extension F_∞/F. Here, h_F^+ is the class number of the maximal real subfield of F. Let $Cl_{F_n}^-$ be the "minus" class group of F_n, and H_n/F_n the class field corresponding to the quotient $Cl_{F_n}^-/(Cl_{F_n}^-)^p$. In [8, 9], we studied normal integral basis problems for H_n/F_n for each $n \geq 0$ corresponding to (Q1) and (Q2) in connection with the p-adic L-functions associated to F.

Remark 2. In [16], Kawamoto and Odai studied the question (Q1) when $\ell = 3$ without the assumption (A2). Let h_K and M be the class number and the Hilbert class field of K, respectively. When $h_K > 1$, they showed that M/K has a NIB if and only if $h_K = 4$ and a generator of the group of units $\mathcal{O}_K^\times$ of K satisfies some condition, and determined all cyclic cubic fields K with $f_K < 10^4$ satisfying the conditions mainly using some numerical data in Gras [7]. Here, f_K is the conductor of K.

2 Lemmas

Let F be a real abelian field. Let $E = E_F = \mathcal{O}_F^\times$ be the group of units of F, $E^+ = E_F^+$ the subgroup consisting of totally positive units, and $E^* = E_F^*$ the subgroup consisting of units ϵ satisfying the congruence $\epsilon \equiv u^2 \bmod 4$ for some $u \in F$. For a unit $\epsilon \in E$, the following equivalence is well known:

$$F(\epsilon^{1/2})/F \text{ is unramified at all finite primes} \Longleftrightarrow \epsilon \in E^*. \tag{3}$$

For this, see [26, Exercise 9.3]. It follows that $F(\epsilon^{1/2})/F$ is unramified at all primes (including the infinite ones) if and only if $\epsilon \in E^+ \cap E^*$.

Lemma 2. *Let L/F be a quadratic extension unramified at all finite primes.*

(I) *The extension L/F has a NIB if and only if $L = F(\epsilon^{1/2})$ for some unit $\epsilon \in E_F$ with $\epsilon \equiv 1 \bmod 4$.*

(II) *When the prime number 2 is unramified in F, L/F has a NIB if and only if $L = F(\epsilon^{1/2})$ for some unit $\epsilon \in E_F$.*

Proof. The assertion (I) is due to Childs [3, Theorem A]. Let us show (II). Let ϵ be a unit of F, and assume that the extension $F(\epsilon^{1/2})/F$ is unramified at all finite primes. Then, by (3), we have $\epsilon \equiv u^2 \bmod 4$ for some $u \in F^\times$. Let d be the residue class degree of a prime ideal of the abelian field F over 2. By replacing ϵ with ϵ^{2^d-1}, we have $\epsilon \equiv 1 \bmod 4$. This is because $u^{2^d-1} \equiv 1 \bmod 2$ since the prime number 2 is unramified in F. Therefore, the assertion (II) follows from (I). $\square$

We denote by A_F (resp. $\widetilde{A}_F$) the 2-part of the ideal class group of F in the ordinary (resp. narrow) sense. The first assertion in the following lemma was shown in Oriat [19, Théorème 2], and the second one in Taylor [23, Assertion (*)]. (For the latter, see also [12, Theorem 2].)

Lemma 3. *Let $F/\mathbb{Q}$ be a cyclic extension of prime degree p (≥ 3), and ψ a nontrivial $\bar{\mathbb{Q}}_2$-valued character of* $\mathrm{Gal}(F/\mathbb{Q})$. *Assume that* $-1 \equiv 2^a \bmod p$ *for some a. Then the following assertions hold.*

(I) *$A_F(\psi)$ is trivial if and only if $\widetilde{A}_F(\psi)$ is trivial.*

(II) $(E^+/E^2)(\psi) = ((E^+ \cap E^*)/E^2)(\psi) = (E^*/E^2)(\psi)$.

In what follows, we work under the notation of §1, and assume that the conditions (A1) and (A2) are satisfied.

Proof of Lemma 1. We put $k = \mathbb{Q}(\sqrt{-1})$ and $L = Kk = K(\sqrt{-1})$. Clearly K is the maximal real subfield of L. For an imaginary abelian field M with the maximal real subfield M^+, let h_M^- be the relative class number, and A_M^- the kernel of the norm map $A_M \to A_{M^+}$. We can naturally regard the minus class group A_L^- as a $\mathbb{Z}_2[\Delta]$-module, and we have $A_L^- = A_L^-(\chi)$ because of (1) and $A_L^-(\chi_0) = A_k^- = \{0\}$. By Lemma 3(I) and the assumption (A1), $A_0 = A_K(\chi)$ is trivial if and only if so is the narrow class group $\widetilde{A}_K(\chi)$. As $\chi(2) \neq 1$ (the assumption (A2)), we see that $\widetilde{A}_K(\chi)$ is trivial if and only if so is the minus class group $A_L^-(\chi)$ by [10, Corollary 2]. As the degree $[L : k]$ is odd, the unit index Q_L of L is equal to that of k (cf. [10, Lemma 4]). Therefore, from $h_k^- = 1$ and the analytic class number formula [26, Theorem 4.17], it follows that

$$h_L^- = \prod_{\chi} \left(-\frac{1}{2} B_{1,\omega_4\chi} \right). \tag{4}$$

Here, ω_4 is the Teichmüller character of conductor 4 and χ runs over the nontrivial $\bar{\mathbb{Q}}_2$-valued characters of Δ. By [26, Theorem 5.11], we have

$$\frac{1}{2} B_{1,\omega_4\chi} = \frac{1}{2} L_2(0, \chi) = g_\chi(4f_\chi).$$

Hence, by the formula (4), we observe that $A_L^- = A_L^-(\chi)$ is trivial if and only if g_χ is a unit of the power series ring Λ (namely, $\lambda_\chi = 0$). Thus we obtain the assertion. □

Let $\mathcal{U}_n$ be the group of principal units of the completion $\hat{K}_n$ of K_n at the unique prime divisor of K_n over 2, $\mathcal{U}_n^{(1)}$ the subgroup of $\mathcal{U}_n$ consisting of local units $u \in \mathcal{U}_n$ with $u \equiv 1 \bmod 2$, and $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$ the projective limit with respect to the relative norms $K_m \to K_n$ $(m > n)$. Identifying the Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ with $\mathrm{Gal}(K_\infty(\zeta_4)/K(\zeta_4))$ in a natural way, we choose and fix a topological generator γ of Γ so that $\zeta^\gamma = \zeta^{1+4f_\chi}$ for all 2-power-th roots ζ of unity. We identify as usual the completed group ring $\mathcal{O}_\chi[[\Gamma]]$ with the power series ring $\Lambda = \mathcal{O}_\chi[[t]]$ by the correspondence $\gamma \leftrightarrow 1+t$. Then we can naturally regard the χ-components $\mathcal{U}_\infty(\chi)$, $\mathcal{U}_n(\chi)$ as modules over Λ. It is well known that $\mathcal{U}_\infty(\chi) \cong \Lambda$ as Λ-modules ([6, Proposition 1]). We choose and fix a generator $\boldsymbol{u} = (\boldsymbol{u}_n)_{n\geq 0}$ of $\mathcal{U}_\infty(\chi)$ over Λ. We put $w_n = w_n(t) = (1+t)^{2^n} - 1$. Then, by [6, Proposition 2], we have an isomorphism

$$\mathcal{U}_n(\chi) \cong \Lambda/(w_n); \quad \boldsymbol{u}_n^g \leftrightarrow g \bmod w_n \tag{5}$$

of Λ-modules. Here and in what follows, we denote by $(*, **, \cdots)$ the ideal of Λ generated by $*, **, \cdots \in \Lambda$. When we refer to the isomorphism (5) with $n=m$, we shall often call it $(5)_m$ in what follows. We denote by I_n the ideal of Λ with $w_n \in I_n$ corresponding to $\mathcal{U}_n^{(1)}(\chi)$ via the isomorphism $(5)_n$:

$$\mathcal{U}_n^{(1)}(\chi) \cong I_n/(w_n).$$

The following assertion was shown in [11].

Lemma 4. *The ideal I_n is generated over Λ by the elements 2^n and $2^{n-1-j}t^{2^j}$ for all j with $0 \leq j \leq n-1$.*

The following assertion is well known.

Lemma 5. *Let $m > n$. Via the isomorphism* (5)*, the natural lifting map $\mathcal{U}_n(\chi) \to \mathcal{U}_m(\chi)$ corresponds to the homomorphism*

$$\Lambda/(w_n) \to \Lambda/(w_m); \quad g \bmod w_n \to g \times \nu_{m,n} \bmod w_m$$

with

$$\nu_{m,n}(t) = w_m(t)/w_n(t) = \sum_{j=0}^{2^{m-n}-1} (1+t)^{2^n j}.$$

Let $E_n = E_{K_n}$ be the group of units of K_n, and C_n the subgroup consisting of cyclotomic units in the sense of Sinnott [20, page 209] or Gillard [6, §4]. Let $\mathcal{E}_n$ and $\mathcal{C}_n$ be the topological closures of $E_n \cap \mathcal{U}_n$ and $C_n \cap \mathcal{U}_n$ in $\mathcal{U}_n$, respectively. The following was shown in [6, Theorem 2].

Lemma 6. *The isomorphism $(5)_n$ induces*

$$\mathcal{U}_n(\chi)/\mathcal{C}_n(\chi) \cong \Lambda/(P_\chi(t), w_n).$$

Here, let us recall some consequences of the Leopoldt conjecture proved by Brumer [2] for real abelian fields. A nice reference on this conjecture is [26, §5.5]. A well known consequence asserts that

$$\gcd(P_\chi(t),\, w_n(t)) = 1 \tag{6}$$

for all $n \geq 0$. We can easily show this using [26, Corollary 5.30] combined with [26, Theorem 7.10]. Then it follows from Lemma 6 that $\mathcal{U}_n(\chi)/\mathcal{C}_n(\chi)$ is a finite abelian group for all $n \geq 0$. In particular, we have $P_\chi(0) \neq 0$. Put $E'_n = E_n \cap \mathcal{U}_n$. The following is a consequence of the Leopoldt conjecture for K_n.

Lemma 7. *For each $n \geq 0$ and $a \geq 1$, the inclusion map $E'_n \to \mathcal{E}_n$ induces an isomorphism $E'_n/{E'_n}^{2^a} \to \mathcal{E}_n/\mathcal{E}_n^{2^a}$.*

It is know that

$$|A_n(\chi)| = |(E_n/C_n)(\chi)| \tag{7}$$

for all $n \geq 0$ by virtue of Kuz'min [17, Theorem 9.2] (and the assumption (A2)), which is a consequence of the Iwasawa main conjecture. Here, $(E_n/C_n)(\chi)$ is the χ-component of $\mathbb{Z}_2[\Delta]$-module $(E_n/C_n) \otimes \mathbb{Z}_2$, the tensor product being taken over $\mathbb{Z}$. For this formula, see Remark 3 below. As we mentioned before, the assumption (A5) implies that $|A_n| = |A_0| = 2^{\kappa(\ell-1)}$ for all n. Therefore, from (7) and Lemma 7, we obtain

$$|\mathcal{E}_n(\chi)/\mathcal{C}_n(\chi)| = |\mathcal{O}_\chi/2^\kappa| \tag{8}$$

for all $n \geq 0$ if we further assume (A5).

Remark 3. Put $G_n = \mathrm{Gal}(K_n/\mathbb{Q}) = \Delta \times (\Gamma/\Gamma^{2^n})$, and $R_n = \mathbb{Z}[G_n]$. We denote by U_n the R_n-submodule of $\mathbb{Q}[G_n]$ defined in Corollary of [20, Proposition 2.2]. Regarding the tensor products $R_n \otimes \mathbb{Z}_2$ and $U_n \otimes \mathbb{Z}_2$ over $\mathbb{Z}$ as modules over $\mathbb{Z}_2[\Delta]$, let $R_n(\chi)$ and $U_n(\chi)$ be the respective χ-components. Then Kuz'min's theorem [17, Theorem 9.2] reads

$$|(E_n/C_n)(\chi)| = |A_n(\chi)| \times (R_n(\chi) : U_n(\chi)).$$

Using [20, Proposition 2.3] and the assumption (A2) (i.e., $\chi(2) \neq 1$), we can easily show that $R_n(\chi) = U_n(\chi)$, and obtain the formula (7).

3 Proof of Theorem 1

We work under the setting of §1. In particular, H/K denotes the class field corresponding to A_0/A_0^2. We denote by V the subgroup of $K^\times/(K^\times)^2$ such that

$$H = K(v^{1/2} \mid [v] \in V),$$

which we can naturally regard as a $\mathbb{Z}_2[\Delta]$-module. As $K/\mathbb{Q}$ is unramified at 2, we may and shall choose a representative v of a class $[v]$ in V or E_K/E_K^2 so that $v \equiv 1 \bmod 2$, by replacing v with v^{2^d-1} if necessary. Here, d is the residue class degree of a prime ideal of K over 2. Assume that the condition (A1) is satisfied. Then, from (1) and (2), we see that $V = V(\chi) = V(\chi^{-1})$ and that the same holds for any Galois invariant submodule U of V. Let $E_0^* = E_{K_0}^*$ and $E_0^+ = E_{K_0}^+$ be the subgroups of $E_0 = E_{K_0}$ defined in §2. We see that $(E_0/E_0^2)(\chi) \cong \mathcal{O}_\chi/2$ by a theorem of Minkowsky on units of a Galois extension over $\mathbb{Q}$ (cf. Narkiewicz [18, Theorem 3.26a]). Hence, we have $(E_0^*/E_0^2)(\chi) \cong \mathcal{O}_\chi/2$ if it is nontrivial. From (3) and Lemma 3(II), we see that

$$\begin{aligned}(E_0(K_0^\times)^2/(K_0^\times)^2) \cap V &= (E_0^+ \cap E_0^*)(K_0^\times)^2/(K_0^\times)^2 = (E_0^+ \cap E_0^*)/E_0^2 \\ &= ((E_0^+ \cap E_0^*)/E_0^2)(\chi) = (E_0^*/E_0^2)(\chi). \end{aligned} \tag{9}$$

For each $[v] \in V$, we have $v\mathcal{O}_{K_0} = \mathfrak{A}^2$ for some ideal $\mathfrak{A}$ of K_0. By mapping $[v]$ to the ideal class $[\mathfrak{A}]$, we obtain from (9) the following exact sequence:

$$\{0\} \to (E_0^*/E_0^2)(\chi) \to V = V(\chi) \to A_0 = A_0(\chi). \tag{10}$$

We see from (9) and Lemma 2(II) that

$$H_{nib} = K(\epsilon^{1/2} \mid [\epsilon] \in (E_0^*/E_0^2)(\chi)). \tag{11}$$

From this, we immediately obtain

Lemma 8. *Assume that the condition* (A1) *is satisfied. If H_{nib}/K is nontrivial, then* $\mathrm{Gal}(H_{nib}/K) \cong \mathcal{O}_\chi/2$.

Proof of Theorem 1. We have $\mathcal{U}_0(\chi) \cong \mathcal{O}_\chi$ by $(5)_0$, and $\mathcal{U}_0(\chi) \supseteq \mathcal{E}_0(\chi) \supseteq \mathcal{C}_0(\chi)$. By Lemma 6,

$$\mathcal{U}_0(\chi)/\mathcal{C}_0(\chi) \cong \mathcal{O}_\chi/P_\chi(0). \tag{12}$$

Since $\mathcal{U}_0(\chi) \cong \mathcal{O}_\chi$, it follows from (7) and Lemma 7 that

$$\mathcal{E}_0(\chi)/\mathcal{C}_0(\chi) \cong \mathcal{O}_\chi/2^\kappa. \tag{13}$$

The assertion (I) follows immediately from (12) and (13). To show the assertion (II), by virtue of (11), it suffices to show that $(E_0^*/E_0^2)(\chi) = (E_0/E_0^2)(\chi)$ if and only if $P_\chi(0) \equiv 0 \mod 2^{\kappa+1}$. Let $[\epsilon]$ be a nontrivial element in $(E_0/E_0^2)(\chi)$ with $\epsilon \in E_0$. We may as well assume that $\epsilon \in \mathcal{E}_0(\chi)$. By (9), we have $[\epsilon] \in (E_0^*/E_0^2)(\chi)$ if and only if the extension $K(\epsilon^{1/2})/K$ is unramified at all primes (including the infinite ones). We see that the last condition is equivalent to $\epsilon \in \mathcal{U}_0(\chi)^2$. This is because the prime ideal of K over 2 splits completely in the class field H/K since it is principal by (A2). Now from the above, we obtain (II) using (12) and (13). □

The following generalization of (13) is needed in the proof of Theorem 4.

Lemma 9. *Assume that the conditions* (A1), (A2) *and* (A5) *are satisfied. Then*

$$\mathcal{E}_n(\chi)/\mathcal{C}_n(\chi) \cong \mathcal{O}_\chi/2^\kappa$$

for all $n \geq 0$.

Proof. Because of (13), it suffices to show that the inclusion $\mathcal{U}_0 \to \mathcal{U}_n$ induces an isomorphism

$$\mathcal{E}_0(\chi)/\mathcal{C}_0(\chi) \cong \mathcal{E}_n(\chi)/\mathcal{C}_n(\chi).$$

To prove this, it suffices to show that $\mathcal{E}_0(\chi) \cap \mathcal{C}_n(\chi) \subseteq \mathcal{C}_0(\chi)$ by virtue of the equality (8). Let c be an arbitrary element of $\mathcal{C}_n(\chi)$. Because of Lemma 6, we see that the local unit c corresponds to $P_\chi(t)x(t)$ for some power series $x(t) \in \Lambda$ via the isomorphism $(5)_n$. Assume that $c \in \mathcal{E}_0(\chi)$. Then we have $c^{\gamma-1} = c^t = 1$, which is equivalent to $t \times P_\chi(t)x(t) \equiv 0 \mod w_n(t)$. As $w_n(t) = t\nu_{n,0}(t)$, it follows from (6) that $\nu_{n,0}$ divides $x(t)$. Let c_0 be an element of $\mathcal{C}_0(\chi)$ corresponding to $P_\chi(t)x(t)/\nu_{n,0}(t)$ via $(5)_0$. Then by Lemma 5 we have $c = c_0$. □

4 Proofs of Theorems 3 and 4

4.1 Preliminary

In the following, we work under the assumptions (A1)-(A5). Then, by Theorem 2 and (11), we have $(E_0^*/E_0^2)(\chi) = \{0\}$. Let L/K be a fixed quadratic subextension of H/K. As $\mathrm{Gal}(H/K) \cong \mathcal{O}_\chi/2$, we see that HK_n/K_n has a NIB if and only if LK_n/K_n has a NIB. Write $L = K(\sqrt{a})$ ($\subseteq H$) for some $a \in K^\times$. We have $a\mathcal{O}_K = \mathfrak{A}^2$ for some ideal $\mathfrak{A}$ of K, which is nonprincipal by the exact sequence (10) and $(E_0^*/E_0^2)(\chi) = \{0\}$. By the assumption (A5), the ideal $\mathfrak{A}$ capitulates in K_1; $\mathfrak{A} = b\mathcal{O}_{K_1}$ for some $b \in K_1^\times$. We have $a = b^2\epsilon$ for some global unit ϵ of K_1, and $LK_1 = K_1(\epsilon^{1/2})$. We may as well assume that $\epsilon \in \mathcal{E}_1(\chi)$. Since the prime ideal of K_1 over 2 is principal and $K_1(\sqrt{\epsilon})/K_1$ is unramified, we see that

$$\epsilon = u^2 \tag{14}$$

for some $u \in \mathcal{U}_1(\chi)$. In the rest of this section, we work under this setting.

Lemma 10. *For an integer $n \geq 1$, the quadratic extension LK_n/K_n has a NIB if and only if $u \in \mathcal{E}_n(\chi)\mathcal{U}_n^{(1)}(\chi)$.*

Proof. We see immediately from Lemma 2 that $LK_n = K_n(\epsilon^{1/2})$ has a NIB if and only if $\epsilon \equiv \eta^2 \bmod 4$ for some global unit $\eta \in \mathcal{E}_n(\chi)$. As $\epsilon = u^2$, the last condition is equivalent to $u \in \mathcal{E}_n(\chi)\mathcal{U}_n^{(1)}(\chi)$. □

The following lemma also follows immediately from Lemma 2 and (14).

Lemma 11. *If $\mathcal{E}_1(\chi) \cap \mathcal{U}_1(\chi)^2 \subseteq (\mathcal{U}_1^{(1)})^2$, then LK_1/K_1 has a NIB.*

Lemma 12. *For any $n \geq 1$, $u \notin \mathcal{E}_n(\chi)$.*

Proof. If $u \in \mathcal{E}_n(\chi)$, then we have $\epsilon = u^2 \in \mathcal{E}_n^2$, and hence $\epsilon \in E_n^2$ by Lemma 7. Therefore, $LK_n = K_n(\epsilon^{1/2}) = K_n$, which is a contradiction. □

Remark 4. It is known that an unramified quadratic extension N/F has a power integral basis (PIB for short) if and only if $N = F(\epsilon^{1/2})$ for some unit ϵ of F ([21, Theorem 3], and that it has a PIB if it has a NIB ([3, Theorem B], [21, Theorem 2]). Therefore, we see that, under the setting and the assumptions of Theorem 3, LK_n/K_n has a PIB but not a NIB for all $n \geq 1$ if (i) $\kappa = 1$ and $\theta \not\equiv 1 \bmod 2$ or (ii) $\kappa \geq 2$. Here, L/K is an arbitrary quadratic subextension of H/K. For some related topics on an unramified cyclic extension having a PIB but not a NIB, see [14] and some references therein.

4.2 Proof of Theorem 3

Proof of Theorem 3(I). Let $e = \mathrm{ord}_2(\theta - 1) \geq 0$. Then we can easily show that

$$\mathrm{ord}_2((1-2\theta)^{2^n} - 1) = n + e + 1. \tag{15}$$

As $P_\chi(t) = t + 2\theta$, it follows from Lemma 6 that

$$\mathcal{U}_n(\chi)/\mathcal{C}_n(\chi) \cong \Lambda/(t+2\theta,\, w_n) \cong \mathcal{O}_\chi/((1-2\theta)^{2^n} - 1) = \mathcal{O}_\chi/2^{n+e+1}$$

via the isomorphism $(5)_n$. Then, as $\kappa = 1$, we observe from (8) that

$$\mathcal{E}_n(\chi) \cong (2^{n+e},\, t+2\theta,\, w_n)/(w_n) \tag{16}$$

via $(5)_n$. In particular, when $n = 1$, we see from Lemma 4 that

$$\begin{array}{ccl} \mathcal{U}_1^{(1)}(\chi) & \cong & (2,\, t)/(w_1), \\ \cup & & \cup \\ \mathcal{E}_1(\chi) & \cong & (2^{e+1},\, t+2\theta,\, w_1)/(w_1). \end{array} \tag{17}$$

Let $u \in \mathcal{U}_1(\chi)$ be the local unit in (14).

Assume that $e = 0$. To show that LK_n/K_n has no NIB for all n, assume to the contrary that LK_m/K_m has a NIB for some $m \geq 1$. Let $g \in \Lambda$ be a power series corresponding to the local unit u via the isomorphism $(5)_1$. Then, we see from Lemma 5 that, regarding u as an element of $\mathcal{U}_m(\chi)$, it corresponds to $g \times \nu_{m,1}(t)$ via $(5)_m$. As LK_m/K_m has a NIB by the assumption, it follows from Lemma 10 and (16) that $g \times \nu_{m,1}$ is contained in the ideal of Λ generated by 2^{m+e}, $t + 2\theta$ and I_m. Using Lemma 4, we can easily show that the last ideal equals $(2^m,\, t+2\theta)$. It follows that $g(-2\theta)\nu_{m,1}(-2\theta) \equiv 0 \bmod 2^m$. On the other hand, we have $\mathrm{ord}_2(\nu_{m,1}(-2\theta)) = m - 1$ by (15). Thus we obtain $g(-2\theta) \equiv 0 \bmod 2$, and hence $g \in (2,\, t)$. Therefore, we see from (17) and $e = 0$ that $u \in \mathcal{U}_1^{(1)}(\chi) = \mathcal{E}_1(\chi)$, which contradicts Lemma 12.

Finally, let us deal with the case $e \geq 1$. Let $g(t)$ be a power series corresponding to the local unit u via $(5)_1$. Then, from (14) and (17), we see that $2g(t)$ is contained in the ideal $J = (2^{e+1},\, t+2\theta,\, w_1)$ of Λ. We see that the ideal J equals $(2^{e+1},\, t+2)$ because $e = \mathrm{ord}_2(\theta - 1)$ and $w_1 = t(t+2)$. Therefore, we obtain

$$2g(t) = 2^{e+1}x(t) + (t+2)y(t)$$

for some power series $x(t),\, y(t) \in \Lambda$. It is clear that $y(t) = 2z(t)$ for some $z(t) \in \Lambda$. Hence, $g(t) = 2^e x(t) + (t+2)z(t)$ is contained in $(2,\, t)$ as $e \geq 1$.

Therefore, $u \equiv 1 \bmod 2$ by (17), and hence $\epsilon = u^2 \equiv 1 \bmod 4$. Thus we see that LK_1/K_1 has a NIB by Lemma 2(I). □

Proof of Theorem 3(II). From Lemma 6, we obtain

$$\mathcal{U}_n(\chi)/\mathcal{C}_n(\chi) \cong \Lambda/(t + 2^\kappa\theta,\, w_n) = \mathcal{O}/((1 - 2^\kappa\theta)^{2^n} - 1) = \mathcal{O}/2^{\kappa+n}$$

via the isomorphism $(5)_n$. Here, the last equality holds because $\kappa \geq 2$. Hence, by (8), we obtain

$$\mathcal{E}_n(\chi) \cong (2^n,\, t + 2^\kappa\theta,\, w_n)/(w_n). \tag{18}$$

In particular, we have

$$\mathcal{U}_1^{(1)}(\chi) = \mathcal{E}_1(\chi) \cong (2,\, t)/(w_1).$$

Using this and (18), we can show the assertion in a way similar to Theorem 3(I), the case $e = 0$. □

4.3 Proof of Theorem 4

Assume that the conditions (A1)-(A5) are satisfied and that $\lambda_\chi \geq 2$. We put $X = (P_\chi(t),\, w_1(t))$. Denote by Y the ideal of Λ with $w_1 \in Y$ such that $\mathcal{E}_1(\chi) \cong Y/(w_1)$ via the isomorphism $(5)_1$. The following is an immediate consequence of Lemma 11.

Lemma 13. *Under the above setting, the extension LK_1/K_1 has a NIB if*

$$Y \cap (2,\, w_1) \subseteq (2I_1,\, w_1).$$

To deal with the module Y, we need some information on $X = (P_\chi(t),\, w_1(t))$. We write

$$P_\chi(t) = w_1(t)Q(t) + \alpha t + \beta$$

for some polynomial $Q(t) \in \mathcal{O}_\chi[t]$ and some $\alpha,\, \beta \in \mathcal{O}_\chi$. Then we have

$$X = (\alpha t + \beta,\, w_1(t)).$$

By (A4), we have $2^\kappa \| \beta$. Letting $f'(t)$ denote the formal derivative of a polynomial $f(t) \in \mathcal{O}_\chi[t]$, we have

$$P'_\chi(t) = (2t + 2)Q(t) + w_1(t)Q'(t) + \alpha.$$

We see that $P'_\chi(0) \equiv 0 \bmod 2$ as $\lambda_\chi \geq 2$, and hence 2 divides α from the above. If 2^κ divides α, then $2^{-\kappa}(\beta + \alpha t)$ is a unit of Λ. If $2^\nu \| \alpha$ for some ν with $1 \leq \nu \leq \kappa - 1$, we have $\alpha t + \beta = v \times 2^\nu(t + 2^{\kappa-\nu}\vartheta)$ for some units v, $\vartheta \in \mathcal{O}_\chi^\times$. Thus we see that

$$X = \begin{cases} (2^\kappa,\, w_1(t)), & \text{when } 2^\kappa | \alpha \\ (2^\nu(t + 2^{\kappa-\nu}\vartheta),\, w_1(t)), & \text{when } 2^\nu \| \alpha \text{ with } 1 \leq \nu \leq \kappa - 1 \end{cases}$$

for some $\vartheta \in \mathcal{O}_\chi^\times$. From the above, the case $X = (2^\nu(t + 2^{\kappa-\nu}\vartheta),\, w_1)$ can occur only when $\kappa \geq 2$.

Lemma 14. *Let $X = (2^\kappa,\, w_1(t))$. Then we have an isomorphism*

$$\Lambda/X \cong \mathcal{O}_\chi/2^\kappa \oplus \mathcal{O}_\chi/2^\kappa$$

of $\mathcal{O}_\chi$-modules via the correspondence $a + bt \bmod X \leftrightarrow (a,\, b)$.

Lemma 15. *Let $X = (2^\nu(t+2^{\kappa-\nu}\vartheta),\, w_1(t))$ with $1 \leq \nu \leq \kappa-1$ and $\vartheta \in \mathcal{O}_\chi^\times$. We put $e = \mathrm{ord}_2(\vartheta - 1)$. The ideal X contains $2^{e+\kappa+1}$ (resp. $2^{\kappa+1}$) when $\nu = \kappa - 1$ (resp. $1 \leq \nu \leq \kappa - 2$). Further, we have an isomorphism*

$$\Lambda/X \cong \begin{cases} \mathcal{O}_\chi/2^{e+\kappa+1} \oplus \mathcal{O}_\chi/2^{\kappa-1}, & \text{when } \nu = \kappa - 1 \\ \mathcal{O}_\chi/2^{\kappa+1} \oplus \mathcal{O}_\chi/2^{\nu}, & \text{when } 1 \leq \nu \leq \kappa - 2 \end{cases}$$

of $\mathcal{O}_\chi$-modules via the correspondence $a + b(t + 2^{\kappa-\nu}\vartheta) \bmod X \leftrightarrow (a,\, b)$.

As Lemma 14 is quite easily shown, we do not give its proof. We give a proof of Lemma 15 at the end of this section.

By Lemma 9, the quotient Y/X is isomorphic to $\mathcal{O}_\chi/2^\kappa$ as an $\mathcal{O}_\chi$-module. Hence we observe that $Y = (\varpi,\, X)$ for some $\varpi \in \Lambda$ such that

$$\varpi \bmod X \text{ is of order } 2^\kappa \tag{19}$$

and

$$t\varpi \equiv \sigma\varpi \bmod X \tag{20}$$

with some $\sigma \in \mathcal{O}_\chi$.

Lemma 16. *The ideal Y is not contained in $(2,\, w_1(t))$.*

Proof. Assume that $Y \subseteq (2,\, w_1(t))$. Then it follows that $\mathcal{E}_1(\chi) \subseteq \mathcal{U}_1^2$. This implies, in particular, that for a unit $\epsilon \in E_0 \setminus E_0^2$ with $[\epsilon] \in (E_0/E_0^2)(\chi)$, the quadratic extension $K_1(\epsilon^{1/2})/K_1$ is unramified at all finite primes. On the other hand, the group $(E_0^*/E_0^2)(\chi)$ is trivial because of (11) and Theorem 2. Hence, $K_0(\epsilon^{1/2})/K_0$ is ramified at the prime 2. Further, both the extensions $K_1 = K_0(2^{1/2})$ and $K_0((2\epsilon)^{1/2})$ over K_0 are ramified at 2. Therefore, it follows that the (2, 2)-extension $K_1(\epsilon^{1/2})/K_0$ is fully ramified at 2. This implies that $K_1(\epsilon^{1/2})/K_1$ is ramified at 2, a contradiction. □

To prove Theorem 4, we deal with the following three cases separately in view of Lemmas 14 and 15; the case (A) where $X = (2^\kappa,\, w_1)$, the case (B) where $X = (2^{\kappa-1}(t+2\vartheta),\, w_1)$ and the case (C) where $X = (2^\nu(t+2^{\kappa-\nu}\vartheta),\, w_1)$ with $1 \le \nu \le \kappa - 2$. Here, ϑ is a unit of $\mathcal{O}_\chi$. As we mentioned just before Lemma 14, the cases (B) and (C) concern only with the case $\kappa \ge 2$ (Theorem 4(II)).

Proof of Theorem 4; the case (A). In this case, we have $X = (2^\kappa,\, w_1)$. By Lemma 14, an element $\varpi \in \Lambda$ with $Y = (\varpi,\, X)$ satisfying (19) and (20) is of the form $1 + bt$ or $t + 2b$ modulo X for some $b \in \mathcal{O}_\chi$, up to a multiplication of a unit of $\mathcal{O}_\chi$. If $\varpi \equiv 1 + bt \bmod X$, then it follows that $Y = \Lambda$ and hence $\Lambda/X \cong \mathcal{O}_\chi/2^\kappa$, which contradicts Lemma 14. Thus we see that

$$Y = (t + 2b,\, 2^\kappa,\, w_1(t))$$

with some $b \in \mathcal{O}_\chi$.

Let us deal with the case $\kappa = 1$. Then we have $Y = (2,\, t) = I_1$. It follows that $\mathcal{E}_1(\chi) = \mathcal{U}_1^{(1)}(\chi)$. Let u be the local unit in (14). If LK_1/K_1 has a NIB, then it follows from Lemma 10 and the above that $u \in \mathcal{E}_1(\chi)\mathcal{U}_1^{(1)}(\chi) = \mathcal{E}_1(\chi)$, which contradicts Lemma 12. Thus LK_1/K_1 has no NIB. To show that LK_2/K_2 has a NIB, take a power series $g(t)$ corresponding to u via the isomorphism $(5)_1$. Regarding u as an element of $\mathcal{U}_2(\chi)$, we see from Lemma 5 that the power series

$$g(t) \times (1 + (1+t)^2) = g(t) \times (2 + 2t + t^2)$$

corresponds to u via $(5)_2$. We see that the ideal $(P_\chi(t), I_2)$ equals $(2,\, t^2)$ because $\lambda_\chi \ge 2$, $2 \| P_\chi(0)$ and $I_2 = (4,\, 2t,\, t^2)$ by Lemma 4. Thus $2 + 2t + t^2$ is contained in $(P_\chi(t),\, I_2)$, which implies that $u \in \mathcal{E}_2(\chi)\mathcal{U}_2^{(1)}(\chi)$ by Lemma 6. Hence, LK_2/K_2 has a NIB by Lemma 10.

Next, let $\kappa \geq 2$. Let $f(t) \in \Lambda$ be a power series contained in $Y \cap (2, w_1)$. Then we have

$$f(t) = (t + 2b)x(t) + 2^{\kappa}y(t) = 2z(t) + w_1(t)w(t)$$

for some power series $x(t)$, $y(t)$, $z(t)$, $w(t) \in \Lambda$. Letting $t = -2b$, we observe that $z(-2b) \equiv 0 \bmod 2$ as $\kappa \geq 2$. This implies that $z(t) \in I_1 = (2, t)$. Thus we see that LK_1/K_1 has a NIB by Lemma 13. □

Proof of Theorem 4(II); the case (B). In this case, we have

$$X = (2^{\kappa-1}(t + 2\vartheta), w_1)$$

with some $\vartheta \in \mathcal{O}_\chi^\times$. By Lemma 15, an element $\varpi \in \Lambda$ with $Y = (\varpi, X)$ satisfying (19) and (20) is of the form $\varpi_b = 2^{e+1} + b(t + 2\vartheta)$ modulo X for some $b \in \mathcal{O}_\chi$, up to a multiplication of a unit of $\mathcal{O}_\chi$. From Lemma 16 and $\kappa \geq 2$, we see that b is a unit $\mathcal{O}_\chi$. Then, because of (20), a power series $f(t) \in Y \cap (2, w_1)$ is written in the form

$$f(t) = \varpi_b\sigma + 2^{\kappa-1}(t + 2\vartheta)x(t) = 2y(t) + w_1(t)z(t) \tag{21}$$

for some $\sigma \in \mathcal{O}_\chi$ and some power series $x(t)$, $y(t)$, $z(t) \in \Lambda$. To show Theorem 4(II) in this case, it suffices to show that $y(t) \in (2, t)$ by virtue of Lemma 13. Letting $t = -2\vartheta$ in (21), we obtain

$$2^{e+1}\sigma = 2y(-2\vartheta) + w_1(-2\vartheta)z(-2\vartheta). \tag{22}$$

We have $w_1(-2\vartheta) = 4\vartheta(\vartheta - 1) \sim 2^{e+2}$, where for 2-adic rationals ξ_1 and ξ_2, we write $\xi_1 \sim \xi_2$ when ξ_1/ξ_2 is a 2-adic unit. Then for the case $e \geq 1$, we see immediately from (22) that $2y(-2\vartheta) \equiv 0 \bmod 4$, which implies that $y(t) \in (2, t)$.

Let us deal with the case $e = 0$. By (22) and $w_1(-2\vartheta) \sim 2^2$, we have

$$\sigma \equiv y(-2\vartheta) \equiv y(0) \bmod 2. \tag{23}$$

Letting $t = 0$ in (21), we see that

$$(2 + 2\vartheta b)\sigma + 2^{\kappa}\vartheta x(0) = 2y(0).$$

As $\kappa \geq 2$, it follows that

$$(1 + \vartheta b)\sigma \equiv y(0) \bmod 2.$$

From the above two congruences, we obtain $b\vartheta\sigma \equiv 0 \bmod 2$, and hence $2|\sigma$ since ϑ and b are units of $\mathcal{O}_\chi$. Therefore, we see from (23) that $y(0) \equiv 0 \bmod 2$ and hence $y(t) \in (2, t)$. □

Proof of Theorem 4(II); the case (C). By Lemma 15, an element $\varpi \in \Lambda$ with $Y = (\varpi, X)$ satisfying (19) and (20) is of the form $\varpi_b = 2 + b(t + 2^{\kappa-\nu}\vartheta)$ modulo X for some $b \in \mathcal{O}_\chi$, up to a multiplication of a unit of $\mathcal{O}_\chi$. By Lemma 16, we have $b \in \mathcal{O}_\chi^\times$. Then a power series $f(t) \in Y \cap (2, w_1)$ is written in the form

$$f(t) = \varpi_b\sigma + 2^\nu(t + 2^{\kappa-\nu}\vartheta)x(t) = 2y(t) + w_1(t)z(t)$$

for some $\sigma \in \mathcal{O}_\chi$ and $x(t), y(t), z(t) \in \Lambda$. Letting $t = -2^{\kappa-\nu}\vartheta$ and $t = 0$ in this formula, we obtain congruences

$$\sigma \equiv y(-2^{\kappa-\nu}\vartheta) \equiv y(0) \bmod 2^{\kappa-\nu}$$

and

$$(1 + 2^{\kappa-\nu-1}b\vartheta)\sigma \equiv y(0) \bmod 2^{\kappa-\nu}$$

similarly to the case $\nu = \kappa - 1$. From these, we can show that $2|\sigma$ using $\vartheta, b \in \mathcal{O}_\chi^\times$, and obtain $y(t) \in (2, t)$. □

Proof of Lemma 15. First, we deal with the case $\nu = \kappa - 1$. We Consider the following $\mathcal{O}_\chi$-homomorphism

$$\varphi : \mathcal{O}_\chi \oplus \mathcal{O}_\chi \to \Lambda/X;\ (a, b) \to a + b(t + 2\vartheta) \bmod X.$$

As $w_1 = t^2 + 2t \in X$, we see that it is surjective by [26, Proposition 7.2]. To prove Lemma 15 in this case, it suffices to show that $(a, b) \in \mathcal{O}_\chi \oplus \mathcal{O}_\chi$ is contained in $\ker\varphi$ if and only if $2^{e+\kappa+1}|a$ and $2^{\kappa-1}|b$. We have

$$w_1(t) = (t + 2\vartheta)Q(t) + w_1(-2\vartheta)$$

and $w_1(-2\vartheta) \sim 2^{2+e}$. Therefore, if $2^{e+\kappa+1}|a$, then there exists an element $\alpha \in \mathcal{O}_\chi$ such that $2^{\kappa-1}\alpha w_1(-2\vartheta) = a$, and hence

$$a = -2^{\kappa-1}(t + 2\vartheta) \times \alpha Q(t) + 2^{\kappa-1}\alpha w_1(t) \in X.$$

From this we obtain the "if"-part of the assertion. To show the "only if"-part, take an element (a, b) in $\ker\varphi$. Then we have

$$a + b(t + 2\vartheta) = 2^{\kappa-1}(t + 2\vartheta)x(t) + w_1(t)y(t) \tag{24}$$

for some $x, y \in \Lambda$. We show that

$$2^{2+e+i}|a \quad \text{and} \quad 2^i|b \tag{25}$$

for each i with $0 \le i \le \kappa - 1$. Letting $t = -2\vartheta$ in (24), we obtain $a = w_1(-2\vartheta)y(-2\vartheta)$. Then, as $w_1(-2\vartheta) \sim 2^{e+2}$, the assertion (25) holds when $i = 0$. Assume that (25) holds for some i with $0 \le i \le \kappa - 2$. Then, by (24), we have $2^i | y(t)$. Dividing (24) by 2^i and putting $y_1(t) = y(t)/2^i$, we obtain

$$\frac{a}{2^i} + \frac{b}{2^i}(t + 2\vartheta) = 2^{\kappa - i - 1}(t + 2\vartheta)x(t) + w_1(t)y_1(t). \tag{26}$$

Letting $t = 0$ in (26), we have

$$\frac{a}{2^i} + \frac{b}{2^i} \times 2\vartheta = 2^{\kappa - i}\vartheta x(0).$$

We see that 4 divides $a/2^i$ because $2^{2+e+i}|a$ by the assumption on induction, and that 4 divides $2^{\kappa-i}$ as $i \le \kappa - 2$. Therefore, it follows from the above that $2^{i+1}|b$, and hence $2|y_1(t)$ by (26). Dividing (26) by 2 and putting $y_2(t) = y_1(t)/2$, we have

$$\frac{a}{2^{i+1}} + \frac{b}{2^{i+1}}(t + 2\vartheta) = 2^{\kappa - i - 2}(t + 2\vartheta)x(t) + w_1(t)y_2(t).$$

Letting $t = -2\vartheta$, we see from $w_1(-2\vartheta) \sim 2^{e+2}$ that $a/2^{i+1}$ is divisible by 2^{e+2} and hence $2^{e+2+(i+1)}|a$. Thus, (25) holds also for $i + 1$. Therefore, (25) holds for all i in the range, and hence the "only if"-part is shown.

Let us deal with the case $1 \le \nu \le \kappa - 2$. Consider the following surjective homomorphism over $\mathcal{O}_\chi$:

$$\varphi : \mathcal{O}_\chi \oplus \mathcal{O}_\chi \to \Lambda/X;\ (a,\, b) \to a + b(t + 2^{\kappa-\nu}\vartheta) \bmod X.$$

We show that $(a,\, b) \in \ker\varphi$ if and only if $2^{\kappa+1}|a$ and $2^{\nu}|b$. We have $w_1(-2^{\kappa-\nu}\vartheta) \sim 2^{\kappa-\nu+1}$ as $1 \le \nu \le \kappa - 2$. Using this, we can show the "if"-part similarly to the case $\nu = \kappa - 1$. Conversely assume that $(a,\, b)$ is contained in $\ker\varphi$. Then we have

$$a + b(t + 2^{\kappa-\nu}\vartheta) = 2^{\nu}(t + 2^{\kappa-\nu}\vartheta)x(t) + w_1(t)y(t)$$

for some $x,\, y \in \Lambda$. Using this, we can show that for each $0 \le i \le \nu$, $2^{\kappa-\nu+1+i}|a$ and $2^i|b$ inductively similarly to the case $\nu = \kappa - 1$. Thus we obtain the assertion. □

5 Numerical result

In this section, we let $\ell = 3$, and deal with a cyclic cubic field K of a prime conductor p with $p \equiv 1 \bmod 3$ and $p < 10^4$. Clearly, $\ell = 3$ satisfies the condition (A1). First, we explain our computational result. In the range $p < 10^4$, there are 411 cubic fields K of conductor p satisfying (A2). Let χ be a nontrivial $\bar{\mathbb{Q}}_2$-valued character of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. For each of them, we computed λ_χ, $v_0 = \mathrm{ord}_2(P_\chi(0))$, and $v_1 = \mathrm{ord}_2(P_\chi(-2))$. There are 48 ones with $\lambda_\chi \geq 1$. By Lemma 1, the condition $\lambda_\chi \geq 1$ is equivalent to $A_0 \neq \{0\}$. The table at the end of this section gives the conductor p, and the data of A_i, v_i with $i = 0$, 1 and λ_χ for these 48 cubic fields. The number a_i (resp. two numbers a_i, b_i) in the row "A_i" means that $A_i \simeq \mathcal{O}_\chi/a_i$ (resp. $A_i \simeq \mathcal{O}_\chi/a_i \oplus \mathcal{O}_\chi/b_i$). The number a in the row "NIB" means that HK_n/K_n has a NIB for $n \geq a$ but HK_n/K_n has no NIB for $n < a$. The mark $*$ in the row "NIB" means that HK_n/K_n has no NIB for all $n \geq 0$. We obtained these explicit result on the questions (Q1) and (Q2) immediately from our data and Theorems 2, 3 and 4. There are 4 cubic fields K with no mark in the row "NIB". The first three K's satisfy the conditions (A2)-(A4) but not (A5), and hence H/K has no NIB by Theorem 2. The 4th K with $p = 7687$ does not satisfy (A3), and hence H/K has no NIB by Lemma 8. For these 4 ones, we can not answer the capitulation problem (Q2) by the method of this paper.

In what follows, we explain how we obtained the data in the table. Letting χ be a nontrivial $\bar{\mathbb{Q}}_2$-valued character of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, we write the Iwasawa power series $g_\chi(t)$ as

$$g_\chi(t) = \sum_{i \geq 0} c_i t^i \in \Lambda = \mathcal{O}_\chi[[t]].$$

Since $g_\chi(t)$ is not divisible by a prime element of $\mathcal{O}_\chi$ ([26, Theorem 7.15]), the lambda invariant λ_χ equals the smallest integer i with $c_i \in \mathcal{O}_\chi^\times$. As usual, we put $\chi^* = \omega_4 \chi^{-1}$ and $\dot{t} = (1+4p)(1+t)^{-1} - 1$. By [26, §7], we have the following approximation formula for $g_\chi(t)$:

$$g_\chi(t) \equiv -\frac{1}{2^{j+3}p} \sum_{a=1}^{2^{j+2}p} a\chi^*(a)^{-1}(1+\dot{t})^{-\gamma_j(a)}$$

modulo the ideal $I_j(t) = ((1+\dot{t})^{2^j} - 1)$ of Λ for $j \geq 0$. Here, a runs over the odd integers with $1 \leq a \leq 2^{j+2}p$ and $p \nmid a$, and $\gamma_j(a)$ is the integer satisfying

$0 \leq \gamma_j(a) < 2^j$ and $(1+4p)^{\gamma_j(a)} \equiv a$ or $-a \mod 2^{j+2}$ according as $a \equiv 1$ or $-1 \mod 4$. In the range $p < 10^4$, there are 411 cubic fields K satisfying (A2). Applying the above formula with $j = 2$ for those 411 ones, we were able to compute the values λ_χ, v_0 and v_1 using UBASIC [25]. It turned out that the maximal values of λ_χ and v_i are 3. This assures the validity of our choice $j = 2$ because $I_2(t) \subseteq (2, t^{2^2})$ and $I_2(0) = I_2(-2) = 2^4\mathcal{O}_\chi$, where $I_j(2\alpha)$ is the ideal of $\mathcal{O}_\chi$ generated by $f(2\alpha)$ for all $f(t) \in I_j(t)$. In the above range, there are 48 fields K such that $\lambda_\chi \geq 1$.

For these 48 cubic fields, we computed the groups A_0 and A_1 as follows. Our method is quite similar to the one in [13, Section 3]. Let B_i be the 2-part of E_i/C_i. Since $A_i(\chi_0) = \{0\}$, we see that $B_i(\chi_0)$ is also trivial using [20, Theorems 4.1, 5.1] and the definition of C_i given in page 209 of [20]. Hence, we have $|A_i| = |B_i|$ by (1) and (7). We first deal with the group B_i since it is easier to attack than the ideal class group A_i. For a finite set L of prime numbers, we consider the map

$$\phi = \phi_L : E_i \to X_L = \prod_{l \in L} \prod_{\mathcal{L}|l} (\mathcal{O}_{K_i}/\mathcal{L})^\times; \quad \epsilon \to (\epsilon \bmod \mathcal{L})_{\mathcal{L}|l \in L},$$

where $\mathcal{L}$ runs over the prime ideals of K_i dividing some prime number l in L. We see that the map ϕ induces an isomorphism $B_i \cong (\phi_L(E_i)/\phi_L(C_i))(2)$ if the set L satisfies the condition

$$\dim_{\mathbb{F}_2} \phi_L(C_i)/\phi_L(C_i)^2 = \mathrm{rank}_{\mathbb{Z}} E_i, \tag{27}$$

where $\mathbb{F}_2$ is the finite field with 2 elements. Since we know a set of explicit generators of C_i, we can obtain that of $\phi_L(C_i) \bmod X_L^{2^e}$ for any e, and can compute exact values $r_1, r_2, \cdots$ such that

$$X_L/\phi_L(C_i)X_L^{2^e} \cong A_{L,e} := \mathbb{Z}/2^{r_1} \oplus \mathbb{Z}/2^{r_2} \oplus \cdots$$

by elementary row operation. When L satisfies (27) and r_i's are smaller than e, we see that B_i is isomorphic to a subgroup of $A_{L,e}$. In this sense, the group $A_{L,e}$ is an "upper bound" of the group B_i. We chose some L's with $|L| = 10$ and $l \equiv 1 \bmod 2^{i+2}p$ for all $l \in L$, and computed using UBASIC an upper bound B_i' of B_i in the above sense as small as possible. As A_0 is nontrivial, we clearly have

$$|B_i'| \geq |B_i| = |A_i| \geq |\mathcal{O}_\chi/2| = 4.$$

When $|B_i'| = 4$, we immediately see that $A_i = \mathcal{O}_\chi/2$. We obtained $|B_i'| = 4$, except for the 11 cases where $A_i \not\cong \mathcal{O}_\chi/2$ in the table. For these exceptional ones, we computed the structure of A_i as an abelian group using Kash3 [15], and obtained the data given in the table. It turned out that for these ones, $|A_i| = |B'_i|$. From this and (7), it follows that $B_i = B'_i$. As a consequence, we obtained isomorphisms $A_0 \cong (E_0/C_0)(\chi)$ and $A_1 \cong (E_1/C_1)(\chi)$ as $\mathcal{O}_\chi$-modules except for the case where $p = 7687$ and $i = 0$. In this case, we have $(E_0/C_0)(\chi) \cong \mathcal{O}_\chi/4$ but $A_0 \cong \mathcal{O}_\chi/2 \oplus \mathcal{O}_\chi/2$.

Our computation was carried out with UBASIC and Kash3 on a PC with Intel Core i5-2410M CPU and 8 GB memory. The total time of computation with UBASIC (resp. Kash3) was about five minutes (resp. two hours).

Table: $p < 10000$ and $\lambda_\chi > 0$.

p	A_0	A_1	v_0	v_1	λ_χ	NIB	p	A_0	A_1	v_0	v_1	λ_χ	NIB
163	2	2	1	1	2	2	4789	2	2	1	1	1	$*$
349	2	2	1	1	1	$*$	4801	2	2	1	1	2	2
547	2	2	1	1	2	2	5479	2	2	1	1	1	$*$
607	2	2	1	2	1	1	5659	2	2	1	1	1	$*$
709	2	2,2	1	1	2		5779	2	2	1	1	1	$*$
853	2	2	1	1	1	$*$	6247	4	4	2	2	2	1
937	2	2	1	1	1	$*$	6553	2	2,2	3	3	2	0
1009	2	2	3	1	1	0	6637	2	2	1	1	1	$*$
1879	2	2,2	1	1	3		6709	2	2	1	1	1	$*$
1951	2	2	1	2	1	1	7027	2	4	2	2	2	0
2131	2	2	1	1	1	$*$	7297	2	2	1	1	2	2
2311	2	2	1	1	2	2	7489	2	2	1	2	1	1
2797	2	2	1	3	1	1	7687	2,2	2,4	2	3	2	
2803	2	2	1	1	1	$*$	7879	2	2	1	1	2	2
3037	2	2	1	1	2	2	8209	2	2	1	1	1	$*$
3517	2	2	1	1	2	2	8647	2	2	1	1	1	$*$
3727	2	2	1	1	1	$*$	8731	2	2	1	1	1	$*$
4099	2	2	1	2	1	1	8887	2	2	1	1	2	2
4219	2	4	1	1	1		9283	2	2	2	1	1	0
4261	2	2	1	1	2	2	9319	2	2	1	1	1	$*$
4297	4	4	2	1	1	$*$	9337	2	2	1	1	1	$*$
4357	2	2	2	1	1	0	9391	2	2	1	1	1	$*$
4561	2	2	2	1	1	0	9421	2	2	1	1	2	2
4639	2	2	3	1	1	0	9601	2	2	1	1	1	$*$

References

[1] J. Brinkhuis, Unramified abelian extensions of CM-fields and their Galois module structure, Bull. London Math. Soc., **24** (1992), 236-242.

[2] A. Brumer, On the units of algebraic number fields, Mathematika, **14** (1967), 121-124.

[3] L. N. Childs, The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc., **35** (1977), 407-422.

[4] T. Fukuda, Remarks on $\mathbb{Z}_p$-extensions of number fields, Proc. Japan Acad., **70** (1994), 264-266.

[5] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge Univ. Press, Cambridge, 1993.

[6] R. Gillard, Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions, II, Ann. Inst. Fourier, **24** no. 4 (1979), 1-15.

[7] M. N. Gras, Méthods et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, J. Reine Angew. Math., **277** (1975), 89-116.

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

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

[10] H. Ichimura, Class number parity of a quadratic twist of a cyclotomic field of prime power conductor, Osaka J. Math., **50** (2013), 563-572.

[11] H. Ichimura, Semi-local units at p of a cyclotomic $\mathbb{Z}_p$-extension congruent to 1 modulo $\zeta_p - 1$, to appear in Hokkaido Math. J.

[12] H. Ichimura, On a duality of Gras between totally positive and primary cyclotomic units, to appear in Math. J. Okayama Univ.

[13] H. Ichimura, S. Nakajima and H. Sumida-Takahashi, On the Iwasawa lambda invariant of an imaginary abelian field of conductor $3p^{n+1}$, J. Number Theory, **133** (2013), 787-801.

[14] H. Ichimura and H. Sumida, A note on integral bases of unramified cyclic extensions of prime degree, II, Manus. Math., **104** (2001), 201-210.

[15] KANT/Kash3, http://page.math.tu-berlin.de/~kant/kash.html

[16] F. Kawamoto and Y. Odai, Normal integral bases of ∞-ramified abelian extensions of totally real number fields, Abh. Math. Sem. Univ. Hamburg, **72** (2002), 217-233.

[17] L. V. Kuz'min, On formulas for the class number of real abelian fields, Izv. Math., **60** (1996), 695-761.

[18] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers (3rd ed.), Springer, Berlin, 2004.

[19] B. Oriat, Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps nombres, Bull. Soc. Math. France, **104** (1976), 301-307.

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

[21] A. Srivastav and S. Venkataraman, Relative Galois module structure of quadratic extensions, Indian J. Pure Appl. Math., **25** (1994), 473-488.

[22] A. Srivastav and S. Venkataraman, Unramified quadratic extensions of real quadratic fields, normal integral bases, and 2-adic L-functions, J. Number Theory, **67** (1997), 139-145.

[23] M. J. Taylor, Galois module structure of classgroups and units, Mathematika, **22** (1975), 156-160.

[24] M. J. Taylor, The Galois module structure of certain arithmetic principal homogeneous spaces, J. Algebra, **153** (1992), 203-214.

[25] UBASIC, http://www.rkmath.rikkyo.ac.jp/~kida/ubasic.htm (in Japanese).

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