JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Humio ICHIMURA et Hiroki SUMIDA-TAKAHASHI

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

Tome 28, nº 2 (2016), p. 325-345.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_2_325_0>

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 325–345

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

par Humio ICHIMURA et Hiroki SUMIDA-TAKAHASHI

Résumé. Soit ℓ un nombre premier impair. Soient $K/\mathbb{Q}$ une extension cyclique réelle de degré ℓ, A_K la 2-partie du groupe des classes d'idéaux de K, et H/K le corps des classes correspondant à A_K/A_K^2. Soit K_n la n-ème couche de la $\mathbb{Z}_2$-extension cyclotomique sur K. Nous considérons les questions (Q1) "existe-il une base intégrale normale pour H/K ?" et (Q2) "sinon, l'extension induite HK_n/K_n a-t-elle une base intégrale normale pour un certain $n \geq 1$?" Sous quelques hypothèses sur ℓ et K, nous répondrons à ces questions en termes de la fonction L 2-adique associée au corps K de base. De plus, nous donnons quelques exemples numériques.

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

Manuscrit reçu le 28 février 2014, révisé le 20 décembre 2014, accepté le 17 février 2015.
Mathematics Subject Classification. 11R33, 11R23.
Mots-clefs. Normal integral basis, unramified quadratic extension, cyclotomic $\mathbb{Z}_2$-extension.

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 [3] and Childs [5]. One of them asserts that an unramified abelian extension N/F of a totally real number field F never has a NIB, with the possible exception of a composite of quadratic extensions of F ([3, 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 1.6 and 1.7 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.

These conditions imply that 2 remains prime in $K(\zeta_\ell)$. Here, for an integer $m \geq 2$, ζ_m denotes a primitive mth root of unity. 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 $\mathbb{Q}_2$. For a module M over $\mathbb{Z}_2[\Delta]$ and a $\bar{\mathbb{Q}}_2$-valued character ψ of Δ, $M(\psi) = M^{e_\psi}$ (or $e_\psi M$) denotes the ψ-component of M, where

$$e_\psi = \frac{1}{\ell} \sum_{\sigma \in \Delta} \mathrm{Tr}_{\mathbb{Q}_2(\psi)/\mathbb{Q}_2}(\psi(\sigma))\sigma^{-1}$$

is the idempotent of $\mathbb{Z}_2[\Delta]$ associated to ψ. Here, $\mathbb{Q}_2(\psi)$ is the field generated by the values of ψ over $\mathbb{Q}_2$, and Tr is the trace map. Then, because of (A1), M is decomposed as

$$M = M(\chi_0) \oplus M(\chi), \tag{1.1}$$

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

$$A_n = A_n(\chi). \tag{1.2}$$

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. It is known that there exists a unique power series $g_\chi(t) \in \Lambda = \mathcal{O}_\chi[[t]]$ related to the 2-adic L-function $L_2(s,\, \chi)$ by

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

For this, see [26, Theorem 5.11]. 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 $\mathcal{O}_\chi$. Namely, $2 \nmid g_\chi(t)$. Hence, $g_\chi(t)$ equals $P_\chi(t)$ times a unit of Λ.

Lemma 1.1. *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 on rings of integers (see Theorem (2.13) in Chapter 3 of Fröhlich and Taylor [6]). 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 (1.1) and (1.2). Using some result in the above mentioned paper [5], we can show that $\mathrm{Gal}(H_{nib}/K) \cong \mathcal{O}_\chi/2$ if it is nontrivial (see Lemma 3.1 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 1.2. *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*

$$P_\chi(0) \equiv 0 \mod 2^{\kappa+1}.$$

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 1.2.

Theorem 1.3. *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 1.3, 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. $|A_0| = |A_1|$.

There are many cases where this condition is satisfied (see a table in §5). 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 [7] or Kraft-Schoof [18]).

Results on the question (Q2) are quite different when $\lambda_\chi = 1$ and when $\lambda_\chi > 1$. We state them in two different theorems for clarity. 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 1.4. *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 1.5. *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 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 $\mathrm{ord}_2(2) = 1$. By Lemma 1.1, the class group A_0 is nontrivial if and only if $\lambda_\chi \geq 1$. In the range of our computation, there are 48 fields K which satisfy (A2) and $|A_0| > 1$. The value v_1 is necessary when we apply Theorem 1.4. Actually, under the setting of Theorem 1.4(I), we have the following equivalence:

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

For these 48 p's, we computed the class groups A_0 and A_1, and give a table of these data at the end of §5. Among them, we find that 44 ones satisfy the further conditions (A3)-(A5). By Theorems 1.3-1.5, we can completely answer the questions (Q1) and (Q2) for them. The four patterns in Theorems 1.4 and 1.5 actually occur. The exceptional $4 = 48 - 44$ primes are

$p = 709$, 1879, 4219 and 7687. For these, we find that H/K has no NIB, but we can not answer (Q2) by the results of this paper.

Remark 1.6. Let p be an *odd* prime number. Theorem 1.2 is quite analogous to a theorem of Taylor [25] (resp. Srivastav and Venkataraman [23]) 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 [10, 11], 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 1.7. In [17], 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 [9]. 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 $\epsilon \equiv u^2 \bmod 4\mathcal{O}_F$ for some $u \in F$. For a unit $\epsilon \in E$, the following equivalence is well known:

$$F(\epsilon^{1/2})/F \text{ is unramified at all finite primes} \Longleftrightarrow \epsilon \in E^*. \tag{2.1}$$

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 2.1. *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 $\epsilon \equiv 1 \bmod 4\mathcal{O}_F$.*

(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 [5, 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 (2.1), we have $\epsilon \equiv u^2 \bmod 4\mathcal{O}_F$ 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 $\epsilon \equiv 1 \bmod 4\mathcal{O}_F$. This is because $u^{2^d-1} \equiv 1 \bmod 2\mathcal{O}_F$ since the prime number 2 is unramified in F. Therefore, the assertion (II) follows from (I). □

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 [20, Théorème 2], and the second one in Taylor [24, Assertion (*)]. (For the latter, see also [14, Theorem 2].)

Lemma 2.2. *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 1.1. 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 (1.1) and $A_L^-(\chi_0) = A_k^- = \{0\}$. By Lemma 2.2(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 [12, Corollary 2]. As the degree $[L : k]$ is odd, the unit index Q_L of L is equal to that of k (cf. [12, Lemma 4]). Therefore, from $h_k^- = 1$ and the analytic class number formula [26, Theorem 4.17], it follows that

$$h_L^- = \prod_\chi \left(-\frac{1}{2}B_{1,\omega_4\chi}\right). \tag{2.2}$$

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 (2.2), 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 (Gillard [8, 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 [8, Proposition 2], we have an isomorphism

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

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 $(\star)$ with $n = m$, we shall often call it $(\star)_m$ 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 $(\star)_n$:

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

We have $\mathcal{U}_0^{(1)} = \mathcal{U}_0$ as 2 is unramified in K, and hence $I_0 = \Lambda$. The following assertion was shown in [13].

Lemma 2.3. *When $n \geq 1$, 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 2.4. *Let $m > n$. Via the isomorphism $(\star)$, 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 [21, page 209] or [8, §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 [8, Theorem 2].

Lemma 2.5. *The isomorphism $(\star)_n$ 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 [4] for real abelian fields. A nice reference on this conjecture is [26, §5.5]. A well known consequence asserts that

$$\gcd(P_\chi(t),\, w_n(t)) = 1 \tag{2.3}$$

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 2.5 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 2.6. *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 well known that E_n/C_n is a finite abelian group ([21, Theorem 4.1]). We denote by B_n the 2-primary part of E_n/C_n. Then we see that

$$|B_n| = |A_n| \tag{2.4}$$

for all $n \geq 0$ from Corollary to Theorem 4.1 and Theorem 5.3 of [21]. Similarly, we see that $|B_n(\chi_0)| = |A_n(\chi_0)|$ $(= 1)$. Hence, it follows that

$$|A_n(\chi)| = |B_n(\chi)| \tag{2.5}$$

from (1.1). As we mentioned before, the assumption (A5) implies that $|A_n| = |A_0| = 2^{\kappa(\ell-1)}$ for all n. Therefore, from (1.2), (2.5) and Lemma 2.6, we obtain

$$|\mathcal{E}_n(\chi)/\mathcal{C}_n(\chi)| = |\mathcal{O}_\chi/2^\kappa| \tag{2.6}$$

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

3. Proof of Theorem 1.2

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. Assume that the condition (A1) is satisfied. Then, from (1.1) and (1.2), 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. (Recall that we have set $K_0 = K$.) 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 [19, Theorem 3.26a]). Hence, we have

$(E_0^*/E_0^2)(\chi) \cong \mathcal{O}_\chi/2$ if it is nontrivial. From (2.1) and Lemma 2.2(II), we see that

$$(3.1)\quad \begin{aligned}(E_0(K_0^\times)^2/(K_0^\times)^2) \cap V &= (E_0^+ \cap E_0^*)(K_0^\times)^2/(K_0^\times)^2 \cong (E_0^+ \cap E_0^*)/E_0^2 \\ &= ((E_0^+ \cap E_0^*)/E_0^2)(\chi) = (E_0^*/E_0^2)(\chi).\end{aligned}$$

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 (3.1) the following exact sequence:

$$(3.2)\qquad \{0\} \to (E_0^*/E_0^2)(\chi) \to V = V(\chi) \to A_0 = A_0(\chi).$$

We see from (3.1) and Lemma 2.1 (II) that

$$(3.3)\qquad H_{nib} = K(\epsilon^{1/2} \mid [\epsilon] \in (E_0^*/E_0^2)(\chi)).$$

From this, we immediately obtain

Lemma 3.1. *Assume that the condition* (A1) *is satisfied. If H_{nib}/K is nontrivial, then* $\mathrm{Gal}(H_{nib}/K) \cong \mathcal{O}_\chi/2$.

In the above, we have used a classical argument for showing “Spiegelung Satz”, which is found for instance in [20] or [26, §10.2].

Proof of Theorem 1.2. We have $\mathcal{U}_0(\chi) \cong \mathcal{O}_\chi$ by $(\star)_0$, and $\mathcal{U}_0(\chi) \supseteq \mathcal{E}_0(\chi) \supseteq \mathcal{C}_0(\chi)$. By Lemma 2.5,

$$(3.4)\qquad \mathcal{U}_0(\chi)/\mathcal{C}_0(\chi) \cong \mathcal{O}_\chi/P_\chi(0).$$

Since $\mathcal{U}_0(\chi) \cong \mathcal{O}_\chi$, it follows from (2.5) and Lemma 2.6 that

$$(3.5)\qquad \mathcal{E}_0(\chi)/\mathcal{C}_0(\chi) \cong \mathcal{O}_\chi/2^\kappa.$$

The assertion (I) follows immediately from (3.4) and (3.5). To show the assertion (II), by virtue of (3.3), it suffices to show that $(E_0^*/E_0^2)(\chi) = (E_0/E_0^2)(\chi)$ if and only if $P_\chi(0) \equiv 0 \bmod 2^{\kappa+1}$. Let $[\epsilon]$ be a nontrivial element in $(E_0/E_0^2)(\chi)$ with $\epsilon \in E_0$. We may as well assume that $\epsilon \in \mathcal{E}_0(\chi)$ and that ϵ generates $\mathcal{E}_0(\chi)$ over $\mathcal{O}_\chi$. By (3.1), 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 $\epsilon \in \mathcal{U}_0(\chi)^2$ (i.e. $\mathcal{E}_0(\chi) \subseteq \mathcal{U}_0(\chi)^2$). 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 (3.4) and (3.5). □

The following generalization of (3.5) is needed in the proof of Theorem 1.5.

Lemma 3.2. *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 (3.5), 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 (2.6). Let c be an arbitrary element of $\mathcal{C}_n(\chi)$. Because of Lemma 2.5, 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 $(\star)_n$. Assume that $c \in \mathcal{E}_0(\chi)$. Then we have $c^{\gamma-1} = c^t = 1$, which is equivalent to $t \times P_\chi(t)x(t) \equiv 0 \bmod w_n(t)$. As $w_n(t) = t\nu_{n,0}(t)$, it follows from (2.3) that $\nu_{n,0}$ divides $x(t)$. Let c_0 be the element of $\mathcal{C}_0(\chi)$ corresponding to $P_\chi(t)x(t)/\nu_{n,0}(t)$ via $(\star)_0$. Then by Lemma 2.4 we have $c = c_0$. □

4. Proofs of Theorems 1.4 and 1.5

4.1. Preliminary. In the following, we work under the assumptions (A1)-(A5). Then, by Theorem 1.3 and (3.3), 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 $L = K(a^{1/2})$ $(\subseteq H)$ for some $a \in K^\times$ with $[a] \in V = V(\chi)$. We have $a\mathcal{O}_K = \mathfrak{A}^2$ for some ideal $\mathfrak{A}$ of K, which is nonprincipal by the exact sequence (3.2) 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 $\epsilon \in E_1$ with $[\epsilon] \in (E_1/E_1^2)(\chi)$, 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 $K_1(\epsilon^{1/2})/K_1$ is unramified, we see that

$$\epsilon = u^2 \tag{4.1}$$

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

Lemma 4.1. *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 2.1 that $LK_n = K_n(\epsilon^{1/2})$ has a NIB if and only if $\epsilon \equiv \eta^2 \bmod 4\mathcal{O}_{K_n}$ 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 2.1 and (4.1).

Lemma 4.2. *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 4.3. *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 2.6. Therefore, $LK_n = K_n(\epsilon^{1/2}) = K_n$, which is a contradiction. □

Remark 4.4. It is known (a) 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 ([22, Theorem 3]), and (b) that it has a PIB if it has a NIB ([5, Theorem B], [22, Theorem 2]). From the first assertion (a), we see that, under the setting and the assumptions of Theorem 1.4, 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. Thus, the converse of the assertion (b) does not hold in general. For some related topics on an unramified cyclic extension having a PIB but not a NIB, see [16] and some references therein.

4.2. Proof of Theorem 1.4.

Proof of Theorem 1.4(I). Let $n \geq 1$. We put $e = \mathrm{ord}_2(\theta - 1)$. Then we can easily show that

$$\mathrm{ord}_2((1-2\theta)^{2^n} - 1) = n + e + 1. \tag{4.2}$$

As $P_\chi(t) = t + 2\theta$, it follows from Lemma 2.5 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 $(\star)_n$. Then, as $\kappa = 1$, we observe from (2.6) that

$$\mathcal{E}_n(\chi) \cong (2^{n+e},\, t+2\theta,\, w_n)/(w_n) \tag{4.3}$$

via $(\star)_n$. In particular, when $n = 1$, we see from Lemma 2.3 that

$$\begin{array}{ccc} \mathcal{U}_1^{(1)}(\chi) & \cong & (2,\, t)/(w_1), \\ \cup & & \cup \\ \mathcal{E}_1(\chi) & \cong & (2^{e+1},\, t+2\theta,\, w_1)/(w_1). \end{array} \tag{4.4}$$

Let $u \in \mathcal{U}_1(\chi)$ be the local unit in (4.1).

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 $(\star)_1$. Then, we see from Lemma 2.4 that, regarding u as an element of $\mathcal{U}_m(\chi)$, it corresponds to $g \times \nu_{m,1}(t)$ via $(\star)_m$. As LK_m/K_m has a NIB by the assumption, it follows from Lemma 4.1 and (4.3) 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 2.3, 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 (4.2). Thus we obtain $g(-2\theta) \equiv 0 \bmod 2$, and hence $g \in (2,\, t)$. Therefore, we see from (4.4) and $e = 0$ that $u \in \mathcal{U}_1^{(1)}(\chi) = \mathcal{E}_1(\chi)$, which contradicts Lemma 4.3.

Finally, let us deal with the case $e \geq 1$. Let $g(t)$ be a power series corresponding to the local unit u via $(\star)_1$. Then, from (4.1) and (4.4), 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 (4.4), and hence $\epsilon = u^2 \equiv 1 \bmod 4$. Thus we see that LK_1/K_1 has a NIB by Lemma 2.1(I). □

Proof of Theorem 1.4(II). From Lemma 2.5, we obtain

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

via the isomorphism $(\star)_n$. Here, the last equality holds because $\kappa \geq 2$. Hence, by (2.6), we obtain

$$\mathcal{E}_n(\chi) \cong (2^n,\, t + 2^\kappa\theta,\, w_n)/(w_n). \tag{4.5}$$

In particular, we have

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

Using this and (4.5), we can show the assertion in a way similar to Theorem 1.4(I), the case $e = 0$. □

4.3. Proof of Theorem 1.5. 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 $X \subseteq Y$ such that $\mathcal{E}_1(\chi) \cong Y/(w_1)$ via the isomorphism $(\star)_1$. The following is an immediate consequence of Lemma 4.2.

Lemma 4.5. *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 $X = (P_\chi(t),\, w_1)$. 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 α, $\beta \in \mathcal{O}_\chi$. 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 $1 \le \nu \le \kappa - 1$, we have $\alpha t + \beta = \upsilon \times 2^{\nu}(t + 2^{\kappa-\nu}\vartheta)$ for some units $\upsilon, \vartheta \in \mathcal{O}_{\chi}^{\times}$. Thus we see that

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

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 $\kappa \ge 2$.

Lemma 4.6. *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 4.7. *Let* $X = (2^{\nu}(t + 2^{\kappa-\nu}\vartheta), w_1(t))$ *with* $1 \le \nu \le \kappa - 1$ *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.* $1 \le \nu \le \kappa - 2$). *Further, we have an isomorphism*

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

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

As Lemma 4.6 is quite easily shown, we do not give its proof. We give a proof of Lemma 4.7 at the end of this section.

By Lemma 3.2, 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

$$\varpi \bmod X\ (\in \Lambda/X) \text{ is of order } 2^{\kappa} \tag{4.6}$$

and

$$t\varpi \equiv \sigma\varpi \bmod X \tag{4.7}$$

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

Lemma 4.8. *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 $\eta \in E_0 \setminus E_0^2$ with $[\eta] \in (E_0/E_0^2)(\chi)$, the quadratic extension $K_1(\eta^{1/2})/K_1$ is unramified at all finite primes. On the other hand, the group $(E_0^*/E_0^2)(\chi)$ is trivial because of (3.3) and Theorem 1.3. Hence, $K_0(\eta^{1/2})/K_0$ is ramified at the prime over 2. Further, both the extensions $K_1 = K_0(2^{1/2})$ and $K_0((2\eta)^{1/2})$ over K_0 are ramified at 2. Therefore, it follows that the (2, 2)-extension $K_1(\eta^{1/2})/K_0$ is fully ramified at 2. This implies that $K_1(\eta^{1/2})/K_1$ is ramified at 2, a contradiction. □

To prove Theorem 1.5, we deal with the following three cases separately in view of Lemmas 4.6 and 4.7; 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 4.6, the cases (B) and (C) concern only with the case $\kappa \ge 2$ (Theorem 1.5(II)).

Proof of Theorem 1.5; the case (A). In this case, we have $X = (2^\kappa, w_1)$. By Lemma 4.6, an element $\varpi \in \Lambda$ with $Y = (\varpi, X)$ satisfying (4.6) and (4.7) 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 $\mathcal{O}_\chi$. This is because an element (a, b) of $\mathcal{O}_\chi/2^\kappa \oplus \mathcal{O}_\chi/2^\kappa$ is of order 2^κ if and only if (i) $a \in \mathcal{O}_\chi^\times$ or (ii) $2|a$ and $b \in \mathcal{O}_\chi^\times$. 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 4.6. 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 (4.1). If LK_1/K_1 has a NIB, then it follows from Lemma 4.1 and the above that $u \in \mathcal{E}_1(\chi)\mathcal{U}_1^{(1)}(\chi) = \mathcal{E}_1(\chi)$, which contradicts Lemma 4.3. 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 $(\star)_1$. Regarding u as an element of $\mathcal{U}_2(\chi)$, we see from Lemma 2.4 that the power series

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

corresponds to u via $(\star)_2$. 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 2.3. 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 2.5. Hence, LK_2/K_2 has a NIB by Lemma 4.1.

Next, let $\kappa \ge 2$. 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 $\kappa \ge 2$. This implies that $z(t) \in I_1 = (2, t)$. Thus we see that LK_1/K_1 has a NIB by Lemma 4.5. $\square$

Proof of Theorem 1.5(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 4.7, an element $\varpi \in \Lambda$ with $Y = (\varpi, X)$ satisfying (4.6) and (4.7) 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 4.8 and

$\kappa \geq 2$, we see that b is a unit $\mathcal{O}_\chi$. Then, because of (4.7), a power series $f(t) \in Y \cap (2, w_1)$ is written in the form

$$f(t) = \varpi_b\sigma + 2^{\kappa-1}(t + 2\vartheta)x(t) = 2y(t) + w_1(t)z(t) \tag{4.8}$$

for some $\sigma \in \mathcal{O}_\chi$ and some power series $x(t)$, $y(t)$, $z(t) \in \Lambda$. To show Theorem 1.5(II) in this case, it suffices to show that $y(t) \in (2, t)$ by virtue of Lemma 4.5. Letting $t = -2\vartheta$ in (4.8), we obtain

$$2^{e+1}\sigma = 2y(-2\vartheta) + w_1(-2\vartheta)z(-2\vartheta). \tag{4.9}$$

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 (4.9) 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 (4.9) and $w_1(-2\vartheta) \sim 2^2$, we have

$$\sigma \equiv y(-2\vartheta) \equiv y(0) \bmod 2. \tag{4.10}$$

Letting $t = 0$ in (4.8), 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 (4.10) that $y(0) \equiv 0 \bmod 2$ and hence $y(t) \in (2, t)$. □

Proof of Theorem 1.5(II); the case (C). By Lemma 4.7, an element $\varpi \in \Lambda$ with $Y = (\varpi, X)$ satisfying (4.6) and (4.7) 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 4.8, we have $b \in \mathcal{O}_\chi^\times$. Then, because of (4.7), 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 $x(t)$, $y(t)$, $z(t) \in \Lambda$. By Lemma 4.5, it suffices to show that $y(t) \in (2, t)$. 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 ϑ, $b \in \mathcal{O}_\chi^\times$, and obtain $y(t) \in (2, t)$. □

Proof of Lemma 4.7. 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 4.7 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

$$a + b(t + 2\vartheta) = 2^{\kappa-1}(t + 2\vartheta)x(t) + w_1(t)y(t) \tag{4.11}$$

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

$$2^{2+e+i}|a \quad \text{and} \quad 2^i|b \tag{4.12}$$

for each i with $0 \le i \le \kappa - 1$. Letting $t = -2\vartheta$ in (4.11), we obtain $a = w_1(-2\vartheta)y(-2\vartheta)$. Then, as $w_1(-2\vartheta) \sim 2^{e+2}$, the assertion (4.12) holds when $i = 0$. Assume that (4.12) holds for some i with $0 \le i \le \kappa - 2$. Then, by (4.11), we have $2^i|y(t)$. Dividing (4.11) by 2^i and putting $y_1(t) = y(t)/2^i$, we obtain

$$\frac{a}{2^i} + \frac{b}{2^i}(t + 2\vartheta) = 2^{\kappa-i-1}(t + 2\vartheta)x(t) + w_1(t)y_1(t). \tag{4.13}$$

Letting $t = 0$ in (4.13), 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 (4.13). Dividing (4.13) 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, (4.12) holds also for $i + 1$. Therefore, (4.12) 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 $\lambda_\chi \ge 1$. By Lemma 1.1, the condition $\lambda_\chi \ge 1$ is equivalent to $A_0 \ne \{0\}$. 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 $n \ge a$ 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 $n \ge 0$. We obtained these explicit result on the questions (Q1) and (Q2) immediately from our data and Theorems 1.3, 1.4 and 1.5. 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 H/K has no NIB by Theorem 1.3. The 4th K with $p = 7687$ does not satisfy (A3), and H/K has no NIB by Lemma 3.1. For these 4 ones, we can not answer the capitulation problem (Q2) by the results 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

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

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 [2]. 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 [15, Section 3]. As in §2, let B_i be the 2-part of E_i/C_i. We have $|B_i| = |A_i|$ by (2.4). 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

$$\dim_{\mathbb{F}_2}\phi_L(C_i)/\phi_L(C_i)^2 = \mathrm{rank}_{\mathbb{Z}}E_i, \tag{5.1}$$

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 (5.1) 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 $A_i \ncong \mathcal{O}_\chi/2$ in the table. For these exceptional ones, we computed the structure of A_i as an abelian group using Kash3 [1], and obtained the data given in the table. It turned out that for these ones, $|A_i| = |B_i'|$. From this and (2.4), it follows that $B_i \cong B_i'$. As a consequence, we obtained isomorphisms

$$A_0 \cong (E_0/C_0)(\chi) \quad \text{and} \quad A_1 \cong (E_1/C_1)(\chi)$$

as $\mathcal{O}_\chi$-modules except for the case where $p = 7687$ and $i = 0$. In this case, we have

$$(E_0/C_0)(\chi) \cong \mathcal{O}_\chi/4 \quad \text{but} \quad A_0 \cong \mathcal{O}_\chi/2 \oplus \mathcal{O}_\chi/2.$$

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	$*$

Acknowlegdements. The authors are grateful to the referee for several valuable comments which improved the presentation of the paper. The second author was partially supported by JSPS KAKENHI Grant Number 25400013.

References

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

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

[3] J. Brinkhuis, "Unramified abelian extensions of CM-fields and their Galois module structure", *Bull. London Math. Soc.* **24** (1992), no. 3, p. 236-242.

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

[5] L. N. Childs, "The group of unramified Kummer extensions of prime degree", *Proc. London Math. Soc. (3)* **35** (1977), no. 3, p. 407-422.

[6] A. Fröhlich & M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993, xiv+355 pages.

[7] T. Fukuda, "Remarks on $\mathbf{Z}_p$-extensions of number fields", *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), no. 8, p. 264-266.

[8] R. Gillard, "Unités cyclotomiques, unités semi-locales et $\mathbf{Z}_l$-extensions. II", *Ann. Inst. Fourier (Grenoble)* **29** (1979), no. 4, p. viii, 1-15.

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

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

[11] ———, "On a normal integral bases problem over cyclotomic $\mathbf{Z}_p$-extensions", *J. Math. Soc. Japan* **48** (1996), no. 4, p. 689-703.

[12] ———, "Class number parity of a quadratic twist of a cyclotomic field of prime power conductor", *Osaka J. Math.* **50** (2013), no. 2, p. 563-572.

[13] ———, "Semi-local units at p of a cyclotomic $\mathbb{Z}_p$-extension congruent to 1 modulo $\zeta_p - 1$", *Hokkaido Math. J.* **44** (2015), p. 397-407.

[14] ———, "On a duality of Gras between totally positive and primary cyclotomic units", *Math. J. Okayama Univ.* **58** (2016), p. 125-132.

[15] H. Ichimura, S. Nakajima & H. Sumida-Takahashi, "On the Iwasawa lambda invariant of an imaginary abelian field of conductor $3p^{n+1}$", *J. Number Theory* **133** (2013), no. 2, p. 787-801.

[16] H. Ichimura & H. Sumida, "A note on integral bases of unramified cyclic extensions of prime degree. II", *Manuscripta Math.* **104** (2001), no. 2, p. 201-210.

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

[18] J. S. Kraft & R. Schoof, "Computing Iwasawa modules of real quadratic number fields", *Compositio Math.* **97** (1995), no. 1-2, p. 135-155, Special issue in honour of Frans Oort.

[19] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004, xii+708 pages.

[20] B. Oriat, "Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres", *Bull. Soc. Math. France* **104** (1976), no. 3, p. 301-307.

[21] W. Sinnott, "On the Stickelberger ideal and the circular units of an abelian field", *Invent. Math.* **62** (1980/81), no. 2, p. 181-234.

[22] A. Srivastav & S. Venkataraman, "Relative Galois module structure of quadratic extensions", *Indian J. Pure Appl. Math.* **25** (1994), no. 5, p. 473-488.

[23] ———, "Unramified quadratic extensions of real quadratic fields, normal integral bases, and 2-adic L-functions", *J. Number Theory* **67** (1997), no. 2, p. 139-145.

[24] M. Taylor, "Galois module structure of classgroups and units", *Mathematika* **22** (1975), no. 2, p. 156-160.

[25] ———, "The Galois module structure of certain arithmetic principal homogeneous spaces", *J. Algebra* **153** (1992), no. 1, p. 203-214.

[26] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, xiv+487 pages.

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

Hiroki Sumida-Takahashi
Faculty of Engineering
Tokushima University
2-1 Minami-josanjima-cho,
Tokushima, 770-8506, Japan
E-mail: hirokit@tokushima-u.ac.jp