JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Takashi MIURA, Kazuaki MURAKAMI, Keiji OKANO et Rei OTSUKI

On the Cyclicity of the Unramified Iwasawa Modules of the Maximal Multiple $\mathbb{Z}_p$-Extensions Over Imaginary Quadratic Fields

Tome 34, nº 3 (2022), p. 881-902.

https://doi.org/10.5802/jtnb.1232

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **34** (2022), 881–902

On the Cyclicity of the Unramified Iwasawa Modules of the Maximal Multiple $\mathbb{Z}_p$-Extensions Over Imaginary Quadratic Fields

par Takashi MIURA, Kazuaki MURAKAMI, Keiji OKANO et Rei OTSUKI

Résumé. Pour un nombre premier impair p, on s'intéresse au nombre de générateurs des modules d'Iwasawa non ramifiés des $\mathbb{Z}_p$-extensions multiples maximales sur l'algèbre d'Iwasawa. Dans notre article précédent, sous plusieurs hypothèses sur un corps quadratique imaginaire, nous avons obtenu une condition nécessaire et suffisante de cyclicité du module d'Iwasawa sur l'algèbre d'Iwasawa. Le présent travail fournit des méthodes de calcul et des exemples numériques des modules d'Iwasawa qui sont cycliques en tant que modules sur l'algèbre d'Iwasawa. Nous remarquons que nos méthodes ne supposent pas la véracité de la conjecture de Greenberg généralisée.

Abstract. For an odd prime number p, we study the number of generators of the unramified Iwasawa modules of the maximal multiple $\mathbb{Z}_p$-extensions over the Iwasawa algebra. In our previous paper, under several assumptions for an imaginary quadratic field, we obtained a necessary and sufficient condition for the cyclicity of the Iwasawa module over the Iwasawa algebra. The present work provides computational methods and numerical examples of Iwasawa modules that are cyclic as modules over the Iwasawa algebra. We remark that our methods do not require the assumption that Greenberg's generalized conjecture holds.

1. Introduction

Let p be a prime number, $\mathbb{Z}_p$ the ring of p-adic integers, K an algebraic number field of finite degree, and K_∞^{c} the cyclotomic $\mathbb{Z}_p$-extension of K. One of the most important objects in classical Iwasawa theory is the Galois group $X_{K_\infty^{\mathrm{c}}}$ of the maximal unramified abelian pro-p extension of K_∞^{c}. The Galois group $\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$ acts on $X_{K_\infty^{\mathrm{c}}}$ by the inner automorphism, and it is well known that $X_{K_\infty^{\mathrm{c}}}$ is a finitely generated torsion $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!]$-module. We introduce here a well-known fact which we can reduce the computation of the number of generators of $X^{\mathrm{c}}_{K_\infty}$ to the computation of only the p-Sylow subgroup A_K of the ideal class group of K. If p does not split

Manuscrit reçu le 4 juillet 2021, révisé le 24 décembre 2021, accepté le 1er avril 2022.
2020 *Mathematics Subject Classification.* 11R23.
Mots-clefs. Iwasawa modules, Imaginary quadratic fields, Multiple $\mathbb{Z}_p$-extensions.

in K and is totally ramified in K_∞^{c}/K, then the $\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$-coinvariant of $X_{K_\infty^{\mathrm{c}}}$ is isomorphic to A_K, and hence Nakayama's lemma tells us that the number of generators of $X_{K_\infty^{\mathrm{c}}}$ as a $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!]$-module coincides with $\dim_{\mathbb{F}_p}(A_K/pA_K)$ (see [15, Proposition 13.22]). In particular, $X_{K_\infty^{\mathrm{c}}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!]$-module if and only if A_K is cyclic as an abelian group.

The objective of our study is to generalize the basic facts to the case of multiple $\mathbb{Z}_p$-extensions. In other words, for the Galois group $X_{\widetilde{K}}$ of the maximal unramified abelian pro-p extension of the maximal multiple $\mathbb{Z}_p$-extension $\widetilde{K}$ of K, we aim to describe the number of generators of $X_{\widetilde{K}}$ as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module, and also to determine the conditions under which $X_{\widetilde{K}}$ is $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic. There is an important conjecture called Greenberg's generalized conjecture, which states that $X_{\widetilde{K}}$ would be pseudo-null as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module. Much evidence supporting the validity of this conjecture has been reported. However, this important conjecture does not seem to give the number of generators of $X_{\widetilde{K}}$. Therefore, we considered that it would be worthwhile to describe the number of generators of $X_{\widetilde{K}}$ as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module, to give necessary and sufficient conditions for $X_{\widetilde{K}}$ to be $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic, to provide these numerical examples and so on. We expect that these studies will help us to gain a deeper understanding of various other properties of $X_{\widetilde{K}}$.

In our previous paper [10], we gave some conditions under which $X_{\widetilde{K}}$ will be $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic for imaginary quadratic fields K. In this paper, we provide methods for computing such conditions and many examples. In the remainder of this section, we will prepare the notation and introduce the theorems in [10] (Theorems 1.1, 1.2). In Section 2, we describe our method for computing the conditions in Theorem 1.1 and provide some examples to which we can apply Theorem 1.1. In Section 3, we introduce the result of Sumida, which consists of a classification of the Iwasawa modules of $\mathbb{Z}_p$-rank 2. In Section 4, we describe a method for computing the conditions in Theorem 1.2 and provide some examples to which we can apply Theorem 1.2.

1.1. Conditions for $X_{\widetilde{K}}$ to be $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic. Let p be an odd prime number, and K an imaginary quadratic field in which p does not split. Denote by K_∞^{c} and K_∞^{an} the cyclotomic $\mathbb{Z}_p$-extension and the anti-cyclotomic $\mathbb{Z}_p$-extension of K, respectively. Let $\widetilde{K} = K_\infty^{\mathrm{c}}K_\infty^{\mathrm{an}}$. Then $\widetilde{K}$ is the maximal multiple $\mathbb{Z}_p$-extension over K and $\mathrm{Gal}(\widetilde{K}/K) \cong \mathbb{Z}_p^2$. Fix a topological generator $\widetilde{\sigma}$ (resp. $\widetilde{\tau}$) of $\mathrm{Gal}(\widetilde{K}/K_\infty^{\mathrm{an}})$ (resp. $\mathrm{Gal}(\widetilde{K}/K_\infty^{\mathrm{c}})$). Then there exists a ring isomorphism between the complete group ring $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$ and the formal power series ring $\mathbb{Z}_p[\![S,T]\!]$ by sending $\widetilde{\sigma}$

and $\widetilde{\tau}$ to $1+S$ and $1+T$, respectively. Note that this ring isomorphism depends on the choice of topological generators $\widetilde{\sigma}$ and $\widetilde{\tau}$. Also, we have the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!] & \xrightarrow{\sim} & \mathbb{Z}_p[\![S,T]\!] \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!] & \xrightarrow{\sim} & \mathbb{Z}_p[\![S]\!], \end{array}$$

where the left vertical arrow is induced by the projection $\mathrm{Gal}(\widetilde{K}/K) \to \mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$, the right vertical arrow is defined by substituting $T=0$, and the lower horizonal arrow is induced by sending $\widetilde{\sigma}|_{K_\infty^{\mathrm{c}}}$ to $1+S$. We identify $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$ (resp. $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!]$) with $\mathbb{Z}_p[\![S,T]\!]$ (resp. $\mathbb{Z}_p[\![S]\!]$) via the isomorphism above. For any algebraic number field F, denote by X_F the Galois group of the maximal unramified abelian pro-p extension L_F of F. If F is a finite extension of the rational number field $\mathbb{Q}$, denote by A_F the p-Sylow subgroup of the ideal class group of F.

It is known that, for any $\mathbb{Z}_p$-extension K_∞ of K, X_{K_∞} is a finitely generated torsion $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$-module. Similarly, $X_{\widetilde{K}}$ is a finitely generated torsion $\mathbb{Z}_p[\![S,T]\!]$-module by Greenberg [5]. Moreover, for the cyclotomic $\mathbb{Z}_p$-extension K_∞^{c}, $X_{K_\infty^{\mathrm{c}}}$ is a finitely generated free $\mathbb{Z}_p$-module by Ferrero and Washington [2] and by [15, Proposition 13.28]. By Nakayama's lemma, the number of generators of $X_{K_\infty^{\mathrm{c}}}$ (resp. $X_{\widetilde{K}}$) as a $\mathbb{Z}_p[\![S]\!]$-module (resp. a $\mathbb{Z}_p[\![S,T]\!]$-module) coincides with $\dim_{\mathbb{F}_p} X_{K_\infty^{\mathrm{c}}}/(p,S)X_{K_\infty^{\mathrm{c}}}$ (resp. $\dim_{\mathbb{F}_p} X_{\widetilde{K}}/(p,S,T)X_{\widetilde{K}}$). Furthermore, since p does not split in K, we have

$$\dim_{\mathbb{F}_p} X_{K_\infty^{\mathrm{c}}}/(p,S)X_{K_\infty^{\mathrm{c}}} = \dim_{\mathbb{F}_p} A_K/pA_K.$$

We introduce the Iwasawa invariants and the characteristic ideals. Let $\mathcal{O}$ be the ring of integers of a finite extension over the field $\mathbb{Q}_p$ of p-adic numbers, and M a finitely generated torsion $\mathcal{O}[\![S]\!]$-module. By the structure theorem of $\mathcal{O}[\![S]\!]$-modules, there is an $\mathcal{O}[\![S]\!]$-homomorphism

$$\varphi\colon M \to \left(\bigoplus_i \mathcal{O}[\![S]\!]/(\pi^{m_i})\right) \oplus \left(\bigoplus_j \mathcal{O}[\![S]\!]/(f_j(S)^{n_j})\right)$$

with finite kernel and finite cokernel, where m_i, n_j are non-negative integers, π is a prime element in $\mathcal{O}$, and $f_j(S) \in \mathcal{O}[S]$ are distinguished irreducible polynomials. We let

$$\mathrm{char}(M) = \left(\prod_i \pi^{m_i} \prod_j f_j(S)^{n_j}\right),$$

which is an ideal in $\mathcal{O}[\![S]\!]$ and called the characteristic ideal of M. We define the Iwasawa μ-invariant $\mu(K_\infty/K)$ and the Iwasawa λ-invariant $\lambda(K_\infty/K)$

of a $\mathbb{Z}_p$-extension K_∞ by $\sum_i m_i$ and $\sum_j n_j \deg f_j$ for $M = X_{K_\infty}$, which is regarded as a $\mathbb{Z}_p[\![S]\!]$-module.

Now we introduce the theorems in [10] which give conditions for $X_{\widetilde{K}}$ to be $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic.

Theorem 1.1 ([10, Theorem 1.6]). *Let p be an odd prime number and K an imaginary quadratic field such that p does not split.*

(i) (trivial case) *Assume that $L_K \cap \widetilde{K} = K$, then*

$$\dim_{\mathbb{F}_p}(X_{\widetilde{K}}/(p, S, T)X_{\widetilde{K}}) = \dim_{\mathbb{F}_p}(A_K/pA_K).$$

(ii) *Suppose that $L_K \cap \widetilde{K} \neq K$, and that $\dim_{\mathbb{F}_p}(A_K/pA_K) = 1$.*
  (ii-a) *If $\lambda(K_\infty^{\mathrm{c}}/K) = 1$, then $\dim_{\mathbb{F}_p}(X_{\widetilde{K}}/(p, S, T)X_{\widetilde{K}}) = 1$.*
  (ii-b) *If $\lambda(K_\infty^{\mathrm{c}}/K) \geq 2$, then*

$$\dim_{\mathbb{F}_p}(X_{\widetilde{K}}/(p, S, T)X_{\widetilde{K}}) = \begin{cases} 1 & \text{if } L_K \subset \widetilde{K}, \\ 2 & \text{otherwise.} \end{cases}$$

Theorem 1.2 ([10, Theorem 5.12]). *Let p be an odd prime number, and K an imaginary quadratic field such that p does not split. Assume that both $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ and $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$ are non-trivial. Suppose the following conditions:*

- *$\dim_{\mathbb{F}_p}(A_K/pA_K) = 2$ and $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ is a direct summand of $\mathrm{Gal}(L_K/K)$.*
- *$\lambda(K_\infty^{\mathrm{c}}/K) = 2$.*
- *Let $\alpha, \beta \in \overline{\mathbb{Q}_p}$ be the roots of the distinguished polynomial generating $\mathrm{char}(X_{K_\infty^{\mathrm{c}}})$. Then $\alpha \neq \beta$.*

We denote by ord the normalized additive valuation on the valuation ring $\mathcal{O}$ of $\mathbb{Q}_p(\alpha, \beta)$. We may assume that $\mathrm{ord}(\alpha) \leq \mathrm{ord}(\beta)$. Let $x_2 \in X_{K_\infty^{\mathrm{c}}}$ be a preimage of a generator of $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ by the map $X_{K_\infty^{\mathrm{c}}} \to \mathrm{Gal}(L_K/K)$. Also, we denote by the vector (μ_{21}, μ_{22}) the image of $x_2 \otimes 1$ under the injective map

$$X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O} \to \mathcal{O}[\![S]\!]/(S-\alpha) \oplus \mathcal{O}[\![S]\!]/(S-\beta)$$

defined in Section 3. We regard $\mu_{21}, \mu_{22} \in \mathcal{O}$ by the natural isomorphisms of $\mathcal{O}$-algebras $\mathcal{O}[\![S]\!]/(S-\alpha) \cong \mathcal{O}$ and $\mathcal{O}[\![S]\!]/(S-\beta) \cong \mathcal{O}$. Then, $X_{\widetilde{K}}$ is $\mathbb{Z}_p[\![S, T]\!]$-cyclic if and only if one of the following holds:

(i) $k > 0$, $\mathrm{ord}(\beta - \alpha) - k < \mathrm{ord}(\alpha)$,
(ii) $k > 0$, $\mathrm{ord}(\beta - \alpha) - k = \mathrm{ord}(\alpha)$, $\mathrm{ord}(\mu_{21}) = 0$,
(iii) $k = 0$, $\mathrm{ord}(\beta - \alpha) = \mathrm{ord}(\alpha)$, $n_1 < n_2$, $\mathrm{ord}(\mu_{21}) = 0$,
(iv) $k = 0$, $\mathrm{ord}(\beta - \alpha) = \mathrm{ord}(\alpha)$, $n_1 \geq n_2$, $\begin{cases} \mathrm{ord}(\mu_{21}) = 0, \\ \mathrm{ord}(\mu_{22}) = \mathrm{ord}(\beta) - \mathrm{ord}(\alpha), \end{cases}$

where each n_1 and n_2 is defined by

$$p^{n_1} = \#\,\mathrm{Gal}(L_K \cap \widetilde{K}/K) \quad \textit{and} \quad p^{n_2} = \#\,\mathrm{Gal}(L_K/L_K \cap \widetilde{K}),$$

respectively, and k will be defined in Section 3.

Remark 1.3 (Erratum)**.** In [10], the definition of $\mathcal{O}$ (see p. 423 and Theorem 5.12 in [10]) needs to be corrected as above. Also, the assumption that both $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ and $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$ are non-trivial and the assumption that $\mathrm{ord}(\alpha) \leq \mathrm{ord}(\beta)$ are dropped in Theorem 5.12 of [10].

Acknowlegdments. We would like to express our sincere gratitude to Professor Masato Kurihara. His brilliant idea in [7], which appeared in the argument about reducing the refined class number formula to the Gross' conjecture, inspired the series of studies described in this paper and our previous one [10]. He always encouraged us, gave helpful suggestions, and kindly answered our many questions. We would also like to express our thanks to Professor Satoshi Fujii for his useful comments. We are really grateful to the anonymous referee for their patient review of the first version of the manuscript and giving a lot of useful comments. Their very important suggestions help us improve our results of the fisrt version. In particular, we could refine Theorems 4.2 and 4.3, and obtain quite satisfactory results thanks to the helpful advice of the referee.

2. Examples of Theorem 1.1

In this section, we will give examples of Theorem 1.1. As in the previous section, let p be an odd prime number, and K an imaginary quadratic field in which p does not split. We denote by $\mathfrak{X}_K$ the Galois group of the maximal abelian pro-p extension M_K/K unramified outside the primes lying above p. Let E_K be the unit group of K. Let $E_K^{(1)} = \{u \in E_K \mid u \equiv 1 \bmod \mathfrak{p}\}$, where $\mathfrak{p}$ is the prime of K lying above p. Note that $E_K^{(1)}$ is trivial unless $K = \mathbb{Q}(\sqrt{-3})$ and $p = 3$. By class field theory, we have the following exact sequence:

$$0 \to \mathrm{Tor}_{\mathbb{Z}_p}\left(U_{\mathfrak{p}}^{(1)}/\overline{\varphi(E_K^{(1)})}\right) \to \mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_K \to \mathrm{Gal}(L_K/L_K \cap \widetilde{K}) \to 0,$$

where $U_{\mathfrak{p}}^{(1)}$ is the group of the principal units in the completion of K with respect to $\mathfrak{p}$, $\varphi\colon E_K^{(1)} \to U_{\mathfrak{p}}^{(1)}$ is the natural homomorphism, and $\overline{\varphi(E_K^{(1)})}$ is the closure of $\varphi(E_K^{(1)})$ in $U_{\mathfrak{p}}^{(1)}$. We know $L_K \cap \widetilde{K} \subset K_\infty^{\mathrm{an}}$. Combining the exact sequence above with the following lemma, we can determine the integer n such that $L_K \cap \widetilde{K} = K_n^{\mathrm{an}}$.

Lemma 2.1 (Fujii [3, Lemma 4.3])**.** *Let $I_K(p)$ be the group of fractional ideals of K prime to p and $S_K(p^n)$ the Strahl group of K modulo p^n, which* *consists of all fractional principal ideals* (α) *of* K *satisfying* $\alpha \equiv 1 \bmod p^n$. *Let* $p^N = p\exp(A_K)$, *where* $\exp(A_K)$ *is the exponent of* A_K. *If*

$$(I_K(p)/S_K(p^n)) \otimes \mathbb{Z}_p \cong A \oplus \mathbb{Z}/p^{N_1}\mathbb{Z} \oplus \mathbb{Z}/p^{N_2}\mathbb{Z}$$

for some abelian group A *and some integers* N_1, N_2 *satisfying* $N+2 \leq n, N < N_i$ $(i=1,2)$, *then we have* $\mathrm{Tor}_{\mathbb{Z}_p} \mathfrak{X}_K \cong A$, *non-canonically.*

We also use the following criterion to determine whether $L_K \subset \widetilde{K}$.

Lemma 2.2 (Minardi [9, Corollary of Proposition 6.B])**.** *Let* $K = \mathbb{Q}(\sqrt{-d})$ *with a square-free positive integer* d. *If* $p=3$ *and* $d \not\equiv 3 \bmod 9$, *then* $L_K \subset \widetilde{K}$ *if and only if the class number of* $\mathbb{Q}(\sqrt{3d})$ *is not divisible by* 3.

Using Lemmas 2.1, 2.2 above and referring to Fukuda's table for the λ-invariants of imaginary quadratic fields ([4]), we get the following examples.

Example 2.3. Let $p=7$ and $K = \mathbb{Q}(\sqrt{-71})$. Then the prime 7 is inert in K. In this case we have $\lambda(K_\infty^{\mathrm{c}}/K) = 1$. We can check that $A_K \cong \mathbb{Z}/7\mathbb{Z}$ and that $L_K \cap \widetilde{K} = K$ by Lemma 2.1. Hence $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.1 (i).

Example 2.4. Let $p=3$ and $K = \mathbb{Q}(\sqrt{-61})$. Then the prime 3 is inert in K. In this case we have $\lambda(K_\infty^{\mathrm{c}}/K) = 1$. We can check that $A_K \cong \mathbb{Z}/3\mathbb{Z}$ and $L_K \subset \widetilde{K}$ by Lemma 2.2. Hence $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.1 (ii-a).

Example 2.5. Let $p=3$ and $K = \mathbb{Q}(\sqrt{-1207})$. Then the prime 3 is inert in K. In this case we have $\lambda(K_\infty^{\mathrm{c}}/K) = 2$. We can check that $A_K \cong \mathbb{Z}/3^2\mathbb{Z}$ and that $L_K \subset \widetilde{K}$ by Lemma 2.2. Hence $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.1 (ii-b).

Example 2.6. Let $p=3$ and $K = \mathbb{Q}(\sqrt{-186})$. Then the prime 3 is ramified in K. In this case we have $\lambda(K_\infty^{\mathrm{c}}/K) = 2$. We can check that $A_K \cong \mathbb{Z}/3\mathbb{Z}$ and that $L_K \subset \widetilde{K}$ by Lemma 2.2. Hence $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.1 (ii-b).

Example 2.7. Let $p=3$ and $K = \mathbb{Q}(\sqrt{-6382})$. Then the prime 3 is inert in K. In this case we have $\lambda(K_\infty^{\mathrm{c}}/K) = 2$. We can check that $A_K \cong \mathbb{Z}/3^2\mathbb{Z}$ and that $K \neq L_K \cap \widetilde{K}$ and $L_K \not\subset \widetilde{K}$. Hence $X_{\widetilde{K}}$ is not cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.1 (ii-b).

3. The results of Sumida

In this section, we prepare the notation to provide examples of Theorem 1.2. Assume that $\lambda(K_\infty^{\mathrm{c}}/K) = 2$. Let $\alpha, \beta \in \overline{\mathbb{Q}_p}$ be the roots of the distinguished polynomial $f(S)$ generating $\mathrm{char}(X_{K_\infty^{\mathrm{c}}})$. In the following, we denote $\mathbb{Q}_p(\alpha,\beta)$ by E. Let $\mathcal{O}_E$, π_E, and ord_E be the ring of integers in E, a prime element of E, and the normalized additive valuation on E such that $\mathrm{ord}_E(\pi_E) = 1$, respectively. Then

$$f(S) = (S-\alpha)(S-\beta) \in \mathcal{O}_E[S], \quad \alpha, \beta \in \pi_E\mathcal{O}_E.$$

We let $\Lambda_E := \mathcal{O}_E[\![S]\!]$, the ring of formal power series over $\mathcal{O}_E$.

For a finitely generated torsion Λ_E-module M, we denote the Λ_E-isomorphism class of M by $[M]_E$.

We consider finitely generated torsion Λ_E-modules whose characteristic ideals are $(f(S))$, and define the set $\mathcal{M}^E_{f(S)}$ by

$$\mathcal{M}^E_{f(S)} = \left\{ [M]_E \,\middle|\, \begin{array}{l} M \text{ is a finitely generated torsion } \Lambda_E\text{-module,} \\ \mathrm{char}(M) = (f(S)) \text{ and } M \text{ is free over } \mathcal{O}_E \end{array} \right\}.$$

Sumida [14] classified all the elements of $\mathcal{M}^E_{f(S)}$ for any given separable and reduceble distinguished polynomial $f(S)$ of degree 2. (For more complete classification for any given distinguished polynomial of degree 2, see Koike [6].)

Let us introduce a special case of their results. Assume that α and β are distinct. Let $[M]_E$ be an element of $\mathcal{M}^E_{f(S)}$. Since M has no non-trivial finite Λ_E-submodule, there exists an injective Λ_E-homomorphism

$$\varphi\colon M \hookrightarrow \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta)$$

with finite cokernel. For each isomorphic class $[M]_E$, we fix a representative $M \in [M]_E$ and φ as above, and regard M as a submodule in $\Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta)$. By using the canonical isomorphism $\Lambda_E/(S-\alpha) \cong \mathcal{O}_E$ $(g(S) \mapsto g(\alpha))$, we define an isomorphism

$$\iota\colon \mathcal{E} = \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta) \longrightarrow \mathcal{O}_E^{\oplus 2}$$

by $(g_1(S), g_2(S)) \mapsto (g_1(\alpha), g_2(\beta))$. We identify $\mathcal{E}$ with $\mathcal{O}_E^{\oplus 2}$ via ι. Thus an element in $\mathcal{E}$ is expressed as $(a_1, a_2) \in \mathcal{O}_E^{\oplus 2}$. Since the rank of M as an $\mathcal{O}_E$-module is equal to two, we can write M of the form

$$M = \langle (a,b), (c,d) \rangle_{\mathcal{O}_E} \ \subset \ \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta),$$

where $\langle * \rangle_{\mathcal{O}_E}$ is the $\mathcal{O}_E$-submodule generated by $*$. Furthermore, using this notation, we can express the action of S by

$$S(a,b) = (\alpha a, \beta b).$$

Then Sumida proved the following:

Proposition 3.1 (Sumida [14, Proposition 10]). *Let $f(S)$ be the polynomial in the above. Then we have*

$$\mathcal{M}^E_{f(S)} = \{ [M(k)]_E \mid 0 \le k \le \mathrm{ord}_E(\beta - \alpha) \},$$

where

$$M(k) = \langle (1,1), (0, \pi_E^k) \rangle_{\mathcal{O}_E} \subset \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta).$$

Furthermore, we have

$$M(k) \cong M(k') \Longleftrightarrow k = k'.$$

The integer k in the above proposition is defined up to Λ_E-isomorphism. Consider the isomorphism class $[X_{K_\infty^c} \otimes_{\mathbb{Z}_p} \mathcal{O}_E]_E$. Then there exists a unique integer k such that $[X_{K_\infty^c} \otimes_{\mathbb{Z}_p} \mathcal{O}_E]_E = [M(k)]_E$. We define the integer k in Theorem 1.2 in this way.

The following result is well-known, but we give a proof for convenience.

Corollary 3.2. *Using the same notation as above, the condition* $k = \mathrm{ord}_E(\beta - \alpha)$ *holds if and only if* M *is* Λ_E*-cyclic.*

Proof. We have only to show that if $k = \mathrm{ord}_E(\beta - \alpha)$, then $M(k)$ is Λ_E-cyclic. In fact, then the converse follows simultaneously from Proposition 3.1, since the Λ_E-isomorphism class of Λ_E-cyclic in $\mathcal{M}^E_{f(S)}$ is only $[\Lambda_E/(f(S))]$. Assume that $k = \mathrm{ord}_E(\beta - \alpha)$. Then

$$(S - \alpha)(1, 1) = (0, \beta - \alpha) = (p\text{-adic unit}) \cdot (0, \pi_E^k),$$

so $M(k)$ is generated by the single element $(1, 1)$. □

In the remainder of this section, we introduce a method to compute k in Proposition 3.1 for a given element of $\mathcal{M}^E_{f(S)}$ by the higher Fitting ideals, which is briefly introduced in Kurihara [8].

For a commutative ring R and a finitely presented R-module M, we consider the following exact sequence:

$$R^m \xrightarrow{f} R^n \to M \to 0,$$

where m and n are positive integers. For an integer $i \geq 0$ such that $0 \leq i < n$, the i-th Fitting ideal of M is defined to be the ideal of R generated by all $(n - i) \times (n - i)$ minors of the matrix corresponding to f. We denote the i-th Fitting ideal of M by $\mathrm{Fitt}_{i,R}(M)$. This definition does not depend on the choice of the exact sequence above (see [12]).

Let M be a Λ_E-module satisfying $[M]_E \in \mathcal{M}^E_{f(S)}$ and $[M]_E = [M(k)]_E$ for some non-negative integer k with $0 \leq k \leq \mathrm{ord}_E(\beta - \alpha)$. Since $(1, 1)$ and $(0, \pi_E^k)$ constitute an $\mathcal{O}_E$-basis of $M(k)$ by Proposition 3.1 and

$$\begin{aligned} S(1,1) &= (\alpha, \beta) \\ &= \alpha(1,1) + (\beta - \alpha)\pi_E^{-k}(0, \pi_E^k), \\ S(0, \pi_E^k) &= \beta(0, \pi_E^k), \end{aligned}$$

we have an exact sequence of Λ_E-modules

$$0 \to \Lambda_E^{\oplus 2} \xrightarrow{h} \Lambda_E^{\oplus 2} \to M(k) \to 0$$

such that the matrix A_h corresponding to the Λ_E-homomorphism h is of the form

$$A_h = \begin{pmatrix} S-\alpha & (\beta-\alpha)\pi_E^{-k} \\ 0 & S-\beta \end{pmatrix}.$$

Therefore

$$\mathrm{Fitt}_{0,\Lambda_E}(M(k)) = ((S-\alpha)(S-\beta)),\ \mathrm{Fitt}_{1,\Lambda_E}(M(k)) = (S-\alpha, (\beta-\alpha)\pi_E^{-k}).$$

Now, let $M = X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E$ and $\omega_n(S) := (1+S)^{p^n} - 1 \in \mathbb{Z}_p[S]$. Then the above exact sequence induces an exact sequence of $\Lambda_E/(\omega_n(S))$-modules

$$(\Lambda_E/(\omega_n(S)))^{\oplus 2} \to (\Lambda_E/(\omega_n(S)))^{\oplus 2} \to (X_{K_\infty^{\mathrm{c}}}/\omega_n(S)X_{K_\infty^{\mathrm{c}}}) \otimes_{\mathbb{Z}_p} \mathcal{O}_E \to 0.$$

Therefore we have the following:

Proposition 3.3. *Using the same notation as above,*

$$\begin{aligned}\mathrm{Fitt}_{1,\Lambda_E/(\omega_n(S))}&\left((X_{K_\infty^{\mathrm{c}}}/\omega_n(S)X_{K_\infty^{\mathrm{c}}}) \otimes_{\mathbb{Z}_p} \mathcal{O}_E\right) \\ &= \left(S-\alpha,\ (\beta-\alpha)\pi_E^{-k},\ \omega_n(S)\right)/(\omega_n(S)).\end{aligned}$$

If we take sufficiently large n, then we can get k in Proposition 3.1 by the equation in Proposition 3.3. Indeed, in Section 4, we compute k in Proposition 3.1 for some Iwasawa modules associated with imaginary quadratic fields.

4. Examples of Theorem 1.2

In this section, we give examples of Theorem 1.2. We use the same notation as in the previous section and suppose that the assumption in Theorem 1.2 holds.

4.1. Setting. We let $\Lambda = \mathbb{Z}_p[\![S]\!]$ and $K = \mathbb{Q}(\sqrt{-d})$, where d is a positive square-free integer. For each $n \geq 0$, we denote by K_n^{c} the intermediate field of the cyclotomic $\mathbb{Z}_p$-extension K_∞^{c} such that K_n^{c} is the unique cyclic extension over K of degree p^n. Let $A_{K_n^{\mathrm{c}}}$ be the p-Sylow subgroup of the ideal class group of K_n^{c}. Then, by class field theory, we have $X_{K_\infty^{\mathrm{c}}} \cong \varprojlim A_{K_n^{\mathrm{c}}}$, where the inverse limit is taken with respect to the relative norms. As in Section 1, $X_{K_\infty^{\mathrm{c}}}$ is a finitely generated torsion Λ-module via a fixed isomorphism

$$\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)]\!] \cong \mathbb{Z}_p[\![S]\!] \qquad (\sigma \leftrightarrow 1+S), \tag{4.1}$$

where σ is a topological generator of $\mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$. Let $f(S)$ be the distinguished polynomial which generates $\mathrm{char}(X_{K_\infty^{\mathrm{c}}})$. Since it is known that $X_{K_\infty^{\mathrm{c}}}$ is a free $\mathbb{Z}_p$-module, we have $[X_{K_\infty^{\mathrm{c}}}]_{\mathbb{Q}_p} \in \mathcal{M}_{f(S)}^{\mathbb{Q}_p}$. We can calculate the polynomial $f(S)$ mod p^n for small n numerically by Mizusawa's program Iwapoly.ub [11, Research, Programing, Approximate Computation of Iwasawa Polynomials by UBASIC].

Let $E = \mathbb{Q}_p(\alpha, \beta)$. Note that $f(S)$ is separable by the assumption in Theorem 1.2.

Hence, as in Proposition 3.1, there exists an integer k with $0 \leq k \leq \mathrm{ord}_E(\beta - \alpha)$, which depends only on the isomorphism class of $X_{K_\infty^{\mathrm{c}}}$, and an $\mathcal{O}_E$-basis $\mathbf{e}_1, \mathbf{e}_2$ of $X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E$ such that the homomorphism on Λ_E-modules

$$\begin{aligned} X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E &\hookrightarrow \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta); \\ \mathbf{e}_1 &\mapsto (1,1),\ \mathbf{e}_2 \mapsto (0, \pi_E^k) \end{aligned} \tag{4.2}$$

is injective. In the case of $k = 0$, we have $X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta)$. In this case we use the standard basis $\{(1,0),(0,1)\}$ instead of $\{(1,1),(0,1)\}$ and *redefine* $\mathbf{e}_1$, $\mathbf{e}_2$ so that

$$\mathbf{e}_1 \mapsto (1,0), \quad \mathbf{e}_2 \mapsto (0,1)$$

by the map (4.2). We regard $X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E$ as a Λ_E-submodule of $\Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta)$ by the above injection. We also regard $X_{K_\infty^{\mathrm{c}}} \subset X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E$ by the injection $x \mapsto x \otimes 1$. We can take generators x_1 and x_2 of $X_{K_\infty^{\mathrm{c}}}$ satisfying the following condition (CG) (see [10, Section 4]):

Condition of generator (CG).

- x_1 and x_2 generate $X_{K_\infty^{\mathrm{c}}}$ as a $\mathbb{Z}_p$-module.
- The image of x_1 in $\mathrm{Gal}(L_K/K)$ maps to a generator of $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$ by the natural projection. The image of x_2 in $\mathrm{Gal}(L_K/K)$ becomes 0 in $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$.

We assumed that $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ is a direct summand of $\mathrm{Gal}(L_K/K)$ as in Theorem 1.2. In other words, there exists an isomorphism

$$\mathrm{Gal}(L_K/K) \cong \mathrm{Gal}(L_K \cap \widetilde{K}/K) \oplus \mathrm{Gal}(L_K/L_K \cap \widetilde{K}). \tag{4.3}$$

Write A_K as $A_K \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2}\mathbb{Z}$ for some positive integers n_1, n_2. By exchanging n_1 and n_2 with each other if necessary, we may assume that the order of $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$ is p^{n_1} as in Theorem 1.2. Moreover, as Section 5 in [10], we may assume that the order of the projection of x_1 in $\mathrm{Gal}(L_K/K)$ is just p^{n_1} by (4.3). Then we have

$$A_K \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \mathcal{O}_E/\pi_E^{N_1}\mathcal{O}_E \oplus \mathcal{O}_E/\pi_E^{N_2}\mathcal{O}_E, \tag{4.4}$$

where $N_i = en_i$ $(i = 1, 2)$ and e is the ramification index in $E/\mathbb{Q}_p$. Note that the projection of x_2 in $\mathrm{Gal}(L_K/K)$ generates $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ whose order is p^{n_2}.

We denote by (μ_{11}, μ_{12}) (resp. (μ_{21}, μ_{22})) the image of $x_1 \otimes 1$ (resp. $x_2 \otimes 1$) under the map (4.2). Then we can write

$$\begin{aligned} x_1 &= \lambda_{11}\mathbf{e}_1 + \lambda_{12}\mathbf{e}_2 = (\mu_{11}, \mu_{12}), \\ x_2 &= \lambda_{21}\mathbf{e}_1 + \lambda_{22}\mathbf{e}_2 = (\mu_{21}, \mu_{22}) \end{aligned}$$

for some $\lambda_{ij} \in \mathcal{O}_E$. Note that $\lambda_{21} = \mu_{21}$ in both cases where $k = 0$ and those where $k > 0$, and that $\lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21} \in \mathcal{O}_E^\times$. Moreover, if $k = 0$, then $\lambda_{ij} = \mu_{ij}$ $(i, j = 1, 2)$ since we take $\mathbf{e}_1 = (1, 0), \mathbf{e}_2 = (0, 1)$.

We can easily check the condition (i) in Theorem 1.2. On the other hand, it is not easy to check the condition (ii), (iii), and (iv) in Theorem 1.2. Indeed, we need to compute the p-adic valuations of μ_{21} and μ_{22}. In the following subsections, we consider the method of computation of $\mathrm{ord}_E(\mu_{21})$ and $\mathrm{ord}_E(\mu_{22})$.

4.2. Computing $\mathrm{ord}_E(\mu_{21})$ and $\mathrm{ord}_E(\mu_{22})$ in Theorem 1.2.

Lemma 4.1. *Using the same notation as in Section 4.1, we have the following:*

(i) *If $k > 0$, we have*

$$Sx_1 = \frac{\alpha\lambda_{11}\lambda_{22} - \beta\lambda_{12}\lambda_{21} - \gamma\lambda_{11}\lambda_{21}}{\det(\lambda_{ij})_{ij}} x_1 + \frac{(\beta - \alpha)\lambda_{11}\lambda_{12} + \gamma\lambda_{11}^2}{\det(\lambda_{ij})_{ij}} x_2,$$
$$Sx_2 = \frac{(\alpha - \beta)\lambda_{21}\lambda_{22} - \gamma\lambda_{21}^2}{\det(\lambda_{ij})_{ij}} x_1 + \frac{-\alpha\lambda_{12}\lambda_{21} + \beta\lambda_{11}\lambda_{22} + \gamma\lambda_{11}\lambda_{21}}{\det(\lambda_{ij})_{ij}} x_2,$$

where $\gamma := (\beta - \alpha)\pi_E^{-k}$.

(ii) *If $k = 0$, we have*

$$Sx_1 = \frac{\alpha\lambda_{11}\lambda_{22} - \beta\lambda_{12}\lambda_{21}}{\det(\lambda_{ij})_{ij}} x_1 + \frac{(\beta - \alpha)\lambda_{11}\lambda_{12}}{\det(\lambda_{ij})_{ij}} x_2,$$
$$Sx_2 = \frac{(\alpha - \beta)\lambda_{21}\lambda_{22}}{\det(\lambda_{ij})_{ij}} x_1 + \frac{-\alpha\lambda_{12}\lambda_{21} + \beta\lambda_{11}\lambda_{22}}{\det(\lambda_{ij})_{ij}} x_2.$$

Proof. Let $\delta = 0$ or 1 according to whether or not $k = 0$. Then we have

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{pmatrix}, \qquad S \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{pmatrix} = \begin{pmatrix} \alpha & \gamma\delta \\ 0 & \beta \end{pmatrix} \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{pmatrix}.$$

Therefore we have

$$S \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \begin{pmatrix} \alpha & \gamma\delta \\ 0 & \beta \end{pmatrix} \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix}^{-1} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

We obtain the results from this equation. □

Let A be the coefficient of x_1 in the right hand side of each equation of Sx_2 in Lemma 4.1:

$$A = \begin{cases} \dfrac{(\alpha - \beta)\lambda_{21}\lambda_{22} - \gamma\lambda_{21}^2}{\det(\lambda_{ij})_{ij}} & \text{if } k > 0 \\ \dfrac{(\alpha - \beta)\mu_{21}\mu_{22}}{\det(\mu_{ij})_{ij}} & \text{if } k = 0. \end{cases}$$

Note that $A \in \mathbb{Z}_p$, since x_1, x_2 are elements in the $\mathbb{Z}_p[\![S]\!]$-module $X_{K_\infty^c}$. Then, we obtain the following theorem, which reduces computing $\mathrm{ord}_E(\mu_{21})$ and $\mathrm{ord}_E(\mu_{22})$ in Theorem 1.2 (ii)(iii)(iv) to computing $\mathrm{ord}_E(A)$.

Theorem 4.2. *Using the same notation as above, we assume that* $\mathrm{ord}_E(\alpha) \le \mathrm{ord}_E(\beta)$ *as in Theorem 1.2.*

(a) *Suppose that* $k > 0$. *Then* $\mathrm{ord}_E(\mu_{21}) = 0$ *if and only if*

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta - \alpha) - k.$$

(b) *Suppose that* $k = 0$ *and* $\mathrm{ord}_E(\beta - \alpha) = \mathrm{ord}_E(\alpha)$.

(b-i) *Assume that* $n_1 < n_2$. *Then* $\mathrm{ord}_E(\mu_{21}) = 0$ *if and only if*

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\alpha).$$

(b-ii) *Assume that* $n_1 \ge n_2$. *Then* $\mathrm{ord}_E(\mu_{21}) = 0$ *and* $\mathrm{ord}_E(\mu_{22}) = \mathrm{ord}_E(\beta) - \mathrm{ord}_E(\alpha)$ *if and only if*

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta).$$

Proof.

(a). Suppose that $k > 0$. Note that $\lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21} \in \mathcal{O}_E^\times$. Hence

$$\begin{aligned}\mathrm{ord}_E(A) &= \mathrm{ord}_E(\lambda_{21}) + \mathrm{ord}_E((\alpha - \beta)\lambda_{22} - (\beta - \alpha)\lambda_{21}\pi_E^{-k}) \\ &= \mathrm{ord}_E(\lambda_{21}) + \mathrm{ord}_E(\alpha - \beta) - k + \mathrm{ord}_E(\lambda_{21} + \lambda_{22}\pi_E^k).\end{aligned}$$

Assume that $\mathrm{ord}_E(\mu_{21}) = \mathrm{ord}_E(\lambda_{21}) = 0$. Then $\mathrm{ord}_E(\lambda_{21} + \lambda_{22}\pi_E^k) = 0$ since $k > 0$, and hence

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\alpha - \beta) - k.$$

Conversely, if $\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta - \alpha) - k$, then we have

$$\mathrm{ord}_E(\lambda_{21}) + \mathrm{ord}_E(\lambda_{21} + \lambda_{22}\pi_E^k) = 0.$$

This implies that $\mathrm{ord}_E(\mu_{21}) = \mathrm{ord}_E(\lambda_{21}) = 0$.

(b). Similarly, if we suppose that $k = 0$ and $\mathrm{ord}_E(\beta - \alpha) = \mathrm{ord}_E(\alpha)$, then we obtain

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\mu_{21}) + \mathrm{ord}_E(\mu_{22}) + \mathrm{ord}_E(\alpha). \tag{4.5}$$

On the other hand, using [10, Lemma 5.2], we have

$$A_K \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \mathcal{O}_E/\alpha\mathcal{O}_E \oplus \mathcal{O}_E/\beta\mathcal{O}_E. \tag{4.6}$$

(b-i). Suppose that $n_1 < n_2$. Comparing (4.4) with (4.6), we have $N_1 = \mathrm{ord}_E(\alpha) < N_2 = \mathrm{ord}_E(\beta)$, since we assumed that $\mathrm{ord}_E(\alpha) \le \mathrm{ord}_E(\beta)$. This induces $\mathrm{ord}_E(\mu_{12}) > 0$. In fact [1], if $\mu_{12} \in \mathcal{O}_E^\times$, then the $\mathcal{O}_E$-submodule generated by the projection of $x_1 = (\mu_{11}, \mu_{12}) \in \Lambda_E/(S-\alpha) \oplus \Lambda_E/(S-\beta)$ in $A_K \otimes_{\mathbb{Z}_p} \mathcal{O}_E$ is isomorphic to $\mathcal{O}_E/\pi_E^{N_2}$. On the other hand, by our assumption

[1] The same argument appears in [10, Lemma 5.10].

of x_1 (see the paragraph following the condition (CG)), the projection of x_1 in $\mathrm{Gal}(L_K/K)$ generates a subgroup which is isomorphic to $\mathbb{Z}/p^{n_1}\mathbb{Z}$. This implies $N_1 = N_2$, which is a contradiction. Thus, $\mathrm{ord}_E(\mu_{12}) > 0$. This implies that, in the case (b-i),

$$\mathrm{ord}_E(\mu_{22}) = 0$$

holds, since $\mu_{11}\mu_{22} - \mu_{12}\mu_{21} \in \mathcal{O}_E^\times$. Combining (4.5) with this, it follows immediately that $\mathrm{ord}_E(\mu_{21}) = 0$ if and only if $\mathrm{ord}_E(A) = \mathrm{ord}_E(\alpha)$.

(b-ii). Suppose that $n_1 \geq n_2$. If $\mathrm{ord}_E(\mu_{21}) = 0$ and $\mathrm{ord}_E(\mu_{22}) = \mathrm{ord}_E(\beta) - \mathrm{ord}_E(\alpha)$ hold, then

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta)$$

by (4.5). Conversely, assume that $\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta)$. Then

$$\mathrm{ord}_E(\mu_{21}) + \mathrm{ord}_E(\mu_{22}) = \mathrm{ord}_E(\beta) - \mathrm{ord}_E(\alpha)$$

by (4.5). Since $\mu_{11}\mu_{22} - \mu_{12}\mu_{21} \in \mathcal{O}_E^\times$, we have only to consider two cases where $\mathrm{ord}_E(\mu_{21}) = 0$ and where $\mathrm{ord}_E(\mu_{22}) = 0$. If $\mathrm{ord}_E(\mu_{21}) = 0$, then $\mathrm{ord}_E(\mu_{22}) = \mathrm{ord}_E(\beta) - \mathrm{ord}_E(\alpha)$. Next, we consider the case where $\mathrm{ord}_E(\mu_{22}) = 0$. Since we assumed that $\mathrm{ord}_E(\alpha) \leq \mathrm{ord}_E(\beta)$, we have $N_1 = \mathrm{ord}_E(\beta) \geq N_2 = \mathrm{ord}_E(\alpha)$. This induces

$$\mathrm{ord}_E(\alpha) = \mathrm{ord}_E(\beta).$$

In fact[2], since $N_2 = \mathrm{ord}_E(\alpha)$, we know that $\alpha x_2 \in SX_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E$. Therefore, there exist some $s, t \in \mathcal{O}_E$,

$$\alpha(\mu_{21}, \mu_{22}) = S(s(1,0) + t(0,1)) = s(\alpha, 0) + t(0, \beta).$$

Hence $\alpha\mu_{22} = t\beta$. Combining $\mu_{22} \in \mathcal{O}_E^\times$ with this and $\mathrm{ord}_E(\beta) \geq \mathrm{ord}_E(\alpha)$, we have $\mathrm{ord}_E(\alpha) = \mathrm{ord}_E(\beta)$. Therefore we obtain

$$\mathrm{ord}_E(\mu_{21}) = \mathrm{ord}_E(\beta) - \mathrm{ord}_E(\alpha) = 0.$$

This completes the proof. □

Our strategy is to compute A modulo some power of p by calculating the Galois action on ideal classes of a large enough intermediate subfield and to compare its order $\mathrm{ord}_E(A)$ with $\mathrm{ord}_E(\beta - \alpha) - k$, etc.

4.3. A method of computing. In this section, we give a method of computing $\mathrm{ord}_E(A)$ in Theorem 4.2. Since p does not split in K, we have Λ-isomorphisms

$$\psi_n \colon X_{K_\infty^{\mathrm{c}}}/\omega_n(S)X_{K_\infty^{\mathrm{c}}} \xrightarrow{\sim} A_{K_n^{\mathrm{c}}}$$

for any non-negative integers n, where $\omega_n(S) = (1+S)^{p^n} - 1$ (see [15, Proposition 13.22]). We fix a non-negative integer n which satisfies the following condition $(\mathrm{C}K_n^{\mathrm{c}})$:

[2]The same argument appears in [10, Lemma 5.11].

Condition of K_n^{c} (CK_n^{c}).

- If $k > 0$, then $0 < \mathrm{ord}_E(\beta - \alpha) - k < \mathrm{ord}_E(p^{n_1+n})$.
- If $k = 0$ and $n_1 < n_2$, then $0 < \mathrm{ord}_E(\alpha) < \mathrm{ord}_E(p^{n_1+n})$.
- If $k = 0$ and $n_1 \geq n_2$, then $0 < \mathrm{ord}_E(\beta) < \mathrm{ord}_E(p^{n_1+n})$.

Here, $\mathrm{ord}_E(\beta - \alpha) - k \neq 0$ by Corollary 3.2. Recall that the Iwasawa λ-invariant of K_∞^{c}/K is 2. Hence $A_{K_n^{\mathrm{c}}}$ is generated by two elements as a $\mathbb{Z}_p$-module. Since the order of $\mathrm{Gal}(L_K \cap \widetilde{K}/K)$ is p^{n_1}, we have $L_K \cap \widetilde{K} = K_{n_1}^{\mathrm{an}}$, where $K_{n_1}^{\mathrm{an}}$ is the n_1-th layer of the anti-cyclotomic $\mathbb{Z}_p$-extension K_∞^{an}/K.

For a fractional ideal $\mathfrak{a}$ in K_n^{c}, we denote its ideal class by $[\mathfrak{a}]$. Also, for readability, we denote additively the operation on $A_{K_n^{\mathrm{c}}}$. We take generators $[\mathfrak{b}_1]$, $[\mathfrak{b}_2]$ of $A_{K_n^{\mathrm{c}}}$ satisfying the following:

(i) $[\mathfrak{b}_1] = s[\mathfrak{Q}_1]$, $[\mathfrak{b}_2] = t[\mathfrak{L}_1]$ for some non-negative integers s, t and for some prime ideals $\mathfrak{Q}_1, \mathfrak{L}_1$.
(ii) $\mathfrak{Q}_1, \mathfrak{L}_1$ are prime ideals in K_n^{c} lying above primes q, ℓ, respectively.
(iii) q and ℓ split completely in $K_n^{\mathrm{c}}/\mathbb{Q}$, respectively.

In fact, the Chebotarev density theorem ensures the existence of such prime ideals $\mathfrak{Q}_1$, $\mathfrak{L}_1$. Let $\mathfrak{q}$, $\bar{\mathfrak{q}}$, $\mathfrak{l}$, and $\bar{\mathfrak{l}}$ be prime ideals in K such that $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$ and $\ell\mathcal{O}_K = \mathfrak{l}\bar{\mathfrak{l}}$. We write

$$q\mathcal{O}_{K_n^{\mathrm{c}}} = \mathfrak{Q}_1\overline{\mathfrak{Q}_1}\cdots\mathfrak{Q}_{p^n}\overline{\mathfrak{Q}_{p^n}}, \quad \mathfrak{Q}_i \mid \mathfrak{q}, \quad \overline{\mathfrak{Q}_i} \mid \bar{\mathfrak{q}} \quad (i = 1, \ldots, p^n),$$
$$\ell\mathcal{O}_{K_n^{\mathrm{c}}} = \mathfrak{L}_1\overline{\mathfrak{L}_1}\cdots\mathfrak{L}_{p^n}\overline{\mathfrak{L}_{p^n}}, \quad \mathfrak{L}_i \mid \mathfrak{l}, \quad \overline{\mathfrak{L}_i} \mid \bar{\mathfrak{l}} \quad (i = 1, \ldots, p^n),$$

where $\mathfrak{Q}_i$, $\overline{\mathfrak{Q}_i}$, $\mathfrak{L}_i$, and $\overline{\mathfrak{L}_i}$ are prime ideals in $\mathcal{O}_{K_n^{\mathrm{c}}}$. Since the norm map $N_{K_n^{\mathrm{c}}/K} \colon A_{K_n^{\mathrm{c}}} \to A_K$ is surjective, we have

$$\mathrm{Gal}(L_K/K) = \left\langle \left(\frac{L_K/K}{\mathfrak{q}}\right)^s, \left(\frac{L_K/K}{\mathfrak{l}}\right)^t \right\rangle, \tag{4.7}$$

where $\left(\frac{L_K/K}{\mathfrak{q}}\right)$, $\left(\frac{L_K/K}{\mathfrak{l}}\right)$ are the Frobenius endomorphism of $\mathfrak{q}, \mathfrak{l}$, respectively. By our assumption (4.3), there exist non-negative integers u, v such that $s \mid u$, $t \mid v$ and

$$\mathrm{Gal}(L_K/L_K \cap \widetilde{K}) = \mathrm{Gal}(L_K/K_{n_1}^{\mathrm{an}}) = \left\langle \left(\frac{L_K/K}{\mathfrak{q}}\right)^u, \left(\frac{L_K/K}{\mathfrak{l}}\right)^v \right\rangle. \tag{4.8}$$

Let Q be the field corresponding to the subgroup generated by $\left(\frac{L_K/K}{\mathfrak{q}}\right)^s$. Then, by exchanging $[\mathfrak{b}_1]$ and $[\mathfrak{b}_2]$ with each other if necessary, we may assume that $L_K = QK_{n_1}^{\mathrm{an}}$. Furthermore, by using the commutative diagram

$$\begin{array}{ccc} X_{K_\infty^{\mathrm{c}}} & & \\ \downarrow & & \\ X_{K_\infty^{\mathrm{c}}}/\omega_n(S)X_{K_\infty^{\mathrm{c}}} & \xrightarrow[\psi_n]{\sim} & A_{K_n^{\mathrm{c}}} \\ \downarrow & & \downarrow N_{K_n^{\mathrm{c}}/K} \\ X_{K_\infty^{\mathrm{c}}}/SX_{K_\infty^{\mathrm{c}}} & \xrightarrow[\psi_0]{\sim} & A_K, \end{array}$$

we know that there exist $x_1, x_2 \in X_{K_\infty^{\mathrm{c}}}$ such that

$$\psi_n(x_1 \bmod \omega_n(S)) = s[\mathfrak{Q}_1], \quad \psi_n(x_2 \bmod \omega_n(S)) = u[\mathfrak{Q}_1] + v[\mathfrak{L}_1].$$

By Nakayama's lemma and our assumptions, we obtain $X_{K_\infty^{\mathrm{c}}} = \langle x_1, x_2 \rangle$ and $A_{K_n^{\mathrm{c}}} = \langle s[\mathfrak{Q}_1], u[\mathfrak{Q}_1] + v[\mathfrak{L}_1] \rangle$.

These x_1 and x_2 satisfy the condition (CG). Moreover, the projection of x_1 in $\mathrm{Gal}(L_K/K)$ generates $\mathrm{Gal}(L_K/Q) \cong \mathbb{Z}/p^{n_1}\mathbb{Z}$. So we adopt these x_1 and x_2, which we have constructed up to modulo $\omega_n(S)$ computationally, as those taken in Section 4.1.

Finally, because $\mathbb{Z}_p[\mathrm{Gal}(K_n^{\mathrm{c}}/K)] \cong \Lambda/\omega_n(S)\Lambda$, we get some $A', B' \in \mathbb{Z}_p \cap \mathbb{Q}$ such that

$$\overline{S}([u\mathfrak{Q}_1 + v\mathfrak{L}_1]) = A'(s[\mathfrak{Q}_1]) + B'(u[\mathfrak{Q}_1] + v[\mathfrak{L}_1]) \tag{4.9}$$

in $A_{K_n^{\mathrm{c}}}$, where $\overline{S} = S \bmod \omega_n(S)$. Since

$$A_{K_n^{\mathrm{c}}} \cong \mathbb{Z}/p^{n_1+n}\mathbb{Z} \oplus \mathbb{Z}/p^{n_2+n}\mathbb{Z}$$

by [6, Proposition 2.2], the order of $s[\mathfrak{Q}_1]$ in the ideal class group $A_{K_n^{\mathrm{c}}}$ is p^{n_1+n}. Therefore, A' is determined up to mod p^{n_1+n}. In particular, if $A' \equiv 0 \bmod p^{n_1+n}$, then we may assume that $A' = 0$. Since the image of x_1 in $A_{K_n^{\mathrm{c}}}$ by the commutative diagram above is $s[\mathfrak{Q}_1]$, we know that A in Section 4.2 satisfies $A \equiv A' \bmod p^{n_1+n}$. Hence, if $A' \not\equiv 0 \bmod p^{n_1+n}$, then $\mathrm{ord}_E(A')$ is uniquely determined and

$$\mathrm{ord}_E(A) = \mathrm{ord}_E(A') < \mathrm{ord}_E(p^{n_1+n}).$$

On the other hand, if $A' \equiv 0 \bmod p^{n_1+n}$, then $\mathrm{ord}_E(A')$ is infinity by the choice of A'. Then we have the following.

Theorem 4.3. *Using the same notation as above, we suppose the assumption in Theorem 1.2. We fix a non-negative integer n which satisfies the condition (CK$_n^{\mathrm{c}}$). Then $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module if and only if one of the following holds:*

(i) $k > 0, \quad \mathrm{ord}_E(\beta - \alpha) - k < \mathrm{ord}_E(\alpha)$,
(ii) $k > 0, \quad \mathrm{ord}_E(\beta - \alpha) - k = \mathrm{ord}_E(\alpha), \quad \mathrm{ord}_E(A') = \mathrm{ord}_E(\beta - \alpha) - k$,
(iii) $k = 0, \quad \mathrm{ord}_E(\beta - \alpha) = \mathrm{ord}_E(\alpha),\ n_1 < n_2, \quad \mathrm{ord}_E(A') = \mathrm{ord}_E(\alpha)$,

(iv) $k = 0$, $\mathrm{ord}_E(\beta - \alpha) = \mathrm{ord}_E(\alpha)$, $n_1 \geq n_2$, $\mathrm{ord}_E(A') = \mathrm{ord}_E(\beta)$, *where* A' *is given by* (4.9)*.*

Proof. The condition (i) is the same as in Theorem 1.2 (i). Consider the case (ii). By Theorem 1.2 (ii) and Theorem 4.2 (a), we have only to show that $\mathrm{ord}_E(A') = \mathrm{ord}_E(\beta-\alpha)-k$ if and only if $\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta-\alpha)-k$. First, suppose that $\mathrm{ord}_E(A') = \mathrm{ord}_E(\beta - \alpha) - k$ holds. If $A \equiv 0 \bmod p^{n_1+n}$, then we obtain $A' \equiv 0 \bmod p^{n_1+n}$ and $\mathrm{ord}_E(A') = \infty$ by the above definition, which contradicts the assumption. Hence $A \not\equiv 0 \bmod p^{n_1+n}$ and $\mathrm{ord}_E(A) = \mathrm{ord}_E(A') = \mathrm{ord}_E(\beta-\alpha)-k$. Conversely, suppose $\mathrm{ord}_E(A) = \mathrm{ord}_E(\beta-\alpha)-k$ holds. Then, by the assumption about $\mathrm{ord}_E(\beta-\alpha)-k$, we have $A \not\equiv 0 \bmod p^{n_1+n}$. Hence $\mathrm{ord}_E(A') = \mathrm{ord}_E(A) = \mathrm{ord}_E(\beta - \alpha) - k$.

The rest is the same as in (ii). □

4.4. Examples of Theorem 1.2.

Example 4.4. Let $p = 3$ and $K = \mathbb{Q}(\sqrt{-12394})$. Using PARI/GP [13], we have $A_K \cong \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. By Lemma 2.1, we have $L_K \cap \widetilde{K} = K_2^{\mathrm{an}}$. Indeed, we have $(I(3)/S(3^5)) \otimes \mathbb{Z}_3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^4\mathbb{Z} \oplus \mathbb{Z}/3^6\mathbb{Z}$. Hence we get $\mathrm{Gal}(L_K/L_K \cap \widetilde{K}) \cong \mathbb{Z}/3\mathbb{Z}$. This implies that $L_K \cap \widetilde{K} = K_2^{\mathrm{an}}$. Moreover, using [1, Theorem 2], we obtain

$$S^{18} + 18S^{16} + 1069S^{14} - 4372S^{12} + 152180S^{10} - 1347136S^8 + 2053184S^6 + 36414976S^4 - 166023168S^2 + 203063296$$

as a defining polynomial of K_2^{an} over $\mathbb{Q}$. By Mizusawa's program Iwapoly.ub, we have

$$f(S) \equiv S^2 + 90S + 189 \bmod 3^5.$$

Let E be the minimal splitting field of $f(S)$. We let $f(S) = (S-\alpha)(S-\beta)$, where α and $\beta \in E$. Then we have $\alpha + \beta \equiv -90 \bmod 3^5$. Thus we get $(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta \equiv 90^2 - 4 \cdot 189 \equiv 2^4 \cdot 3^3 \cdot 17 \bmod 3^5$. Since the discriminant of $f(S)$ is $2^4 \cdot 3^3 \cdot 17 \bmod 3^5$, $E/\mathbb{Q}_p$ is a ramified extension and we get $\mathrm{ord}_E(\alpha - \beta) = 3$. By the table in [6], we obtain

$$X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \langle (1, 1), (0, \pi_E^2) \rangle_{\mathcal{O}_E},$$

which implies that $k = 2$ in Theorem 1.2. Since we have $\mathrm{ord}_E(\alpha - \beta) = 3$, we obtain $\mathrm{ord}_E(\alpha - \beta) - k = 1 < 3$.

Therefore $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.2 (i).

We can also obtain the same result as above by the following.

Proposition 4.5. *We use the same notation as in Section 4.3. Suppose the following conditions:*

(i) $A_K \cong \mathbb{Z}/p^{m_1}\mathbb{Z} \oplus \mathbb{Z}/p^{m_2}\mathbb{Z}$ $(m_1 < m_2)$,

(ii) $L_K \cap \widetilde{K} = K_{m_2}^{\mathrm{an}}$,

(iii) $\mathrm{ord}_E(\alpha) = \mathrm{ord}_E(\beta)$.

Then $X_{\widetilde{K}}$ *is cyclic as a* $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$*-module.*

Proof. Using [10, Lemma 5.2], we have

$$A_K \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \begin{cases} \mathcal{O}_E/\alpha\mathcal{O}_E \oplus \mathcal{O}_E/\beta\mathcal{O}_E & \text{if } \mathrm{ord}_E(\beta-\alpha)-k \geq m, \\ \mathcal{O}_E/(\beta-\alpha)\pi_E^{-k}\mathcal{O}_E \oplus \mathcal{O}_E/\frac{\alpha\beta}{(\beta-\alpha)\pi_E^{-k}}\mathcal{O}_E. & \text{if } \mathrm{ord}_E(\beta-\alpha)-k < m, \end{cases}$$

where $m = \min\{\mathrm{ord}_E(\alpha), \mathrm{ord}_E(\beta)\}$. This implies that $k > 0$ by assumptions (i) and (iii). Hence we have $\mathrm{ord}_E(\beta-\alpha)-k < m$. Moreover, $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ is a direct summand of $\mathrm{Gal}(L_K/K)$ by (ii). By Theorem 1.2 (i), we get the conclusion. □

By Proposition 4.5 and Table 4.2, which is obtained by Mizusawa's program Iwapoly.ub, we obtain Table 4.1. The second, the third and the fifth columns in Table 4.1 imply that the examples in the table satisfy (i), (ii) and (iii) in Proposition 4.5, respectively.

TABLE 4.1.

d	A_K	$L_K \cap \widetilde{K}$	$E/\mathbb{Q}_3$	$(\mathrm{ord}_E(\alpha), \mathrm{ord}_E(\beta))$	$\mathrm{ord}_E(\alpha-\beta)$	k	$X_{\widetilde{K}}$
5703	$(3,9)$	K_2^{an}	ramified	(3,3)	3	2	cyclic
12394	$(3,9)$	K_2^{an}	ramified	(3,3)	3	2	cyclic
50293	$(3,9)$	K_2^{an}	ramified	(3,3)	3	2	cyclic
54931	$(3,9)$	K_2^{an}	ramified	(3,3)	3	2	cyclic
89269	$(3,27)$	${K_3}^{\mathrm{an}}$	unramified	(2,2)	3	2	cyclic

(The integer k is defined by (4.2).)

TABLE 4.2.

d	a generator of $\mathrm{char}(X_{K_\infty^{\mathrm{c}}}) \bmod 3^5$
5703	$S^2 + 63S + 135$
12394	$S^2 + 63S + 27$
50293	$S^2 + 54S + 189$
54931	$S^2 + 135S + 216$
89269	$S^2 + 63S + 81$

The following example is a case in which $X_{\widetilde{K}}$ is not cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module.

Example 4.6. Let $p = 3$ and $K = \mathbb{Q}(\sqrt{-42619})$. Using PARI/GP, we have $A_K \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. We have $L_K \cap \widetilde{K} = K_1^{\mathrm{an}}$. Hence $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ is a direct summand of $\mathrm{Gal}(L_K/K)$. We get

$$f(S) \equiv S^2 + 573S + 981 \bmod 3^7.$$

By Hensel's Lemma, there exist $\alpha, \beta \in \mathbb{Z}_p$ such that $f(S) = (S-\alpha)(S-\beta)$. Then we have $\alpha+\beta \equiv -573 \bmod 3^7$. Thus we get $(\alpha-\beta)^2 = (\alpha+\beta)^2 - 4\alpha\beta \equiv 573^2 - 4 \cdot 981 \equiv 3^6 \bmod 3^7$. Hence we have the p-adic order $\mathrm{ord}_p(\alpha-\beta) = 3$. In this case, although [6] could not determine the isomorphism class of $X_{K_\infty^{\mathrm{c}}}$, we can determine it using the method in Section 3 as follows.

We compute

$$A_{K_2^{\mathrm{c}}} = \mathbb{Z}/27\mathbb{Z}\ [\mathfrak{b}_1] \oplus \mathbb{Z}/27\mathbb{Z}\ [\mathfrak{b}_2]$$

for some ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$ in $\mathcal{O}_{K_2^{\mathrm{c}}}$. Take a generator $\bar{\rho}$ of $\mathrm{Gal}(K_2^{\mathrm{c}}/K)$. These $\mathfrak{b}_1$, $\mathfrak{b}_2$, and $\bar{\rho}$ are computed by PARI/GP. We will not describe the complicated computation of $\bar{\rho}$ due to space limitations. There is a topological generator $\rho \in \mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$ such that ρ is an extension of $\bar{\rho}$. Note that we have the isomorphism (4.1) by fixing the topological generator σ, and that we regard $X_{K_\infty^{\mathrm{c}}}$ as a $\mathbb{Z}_p[\![S]\!]$-module by the isomorphism. We can easily check that $\mathrm{ord}_p(\alpha)$, $\mathrm{ord}_p(\beta)$, $\mathrm{ord}_p(\alpha-\beta)$, and $\mathcal{M}_{f(S)}^{\mathbb{Q}_p}$ do not depend on the choice of σ, although $f(S)$ depends on the choice of σ. Therefore, since we do not use the form of $f(S)$ in the rest of this example, we may replace σ with ρ. We also compute that

$$\overline{\sigma}[\mathfrak{b}_1] = 4[\mathfrak{b}_1], \quad \overline{\sigma}[\mathfrak{b}_2] = 4[\mathfrak{b}_2].$$

Hence we have

$$\mathrm{Fitt}_{1,\mathbb{Z}_p[\![S]\!]/(\omega_2(S))}(X_{K_\infty^{\mathrm{c}}}/\omega_2(S)X_{K_\infty^{\mathrm{c}}}) = (S-3, 27, \omega_2(S))/(\omega_2(S)).$$

Using Proposition 3.3, we obtain $k = 0$. Indeed, applying Proposition 3.3 for $n = 2$, we have

$$\begin{aligned}(S-\alpha, (\beta-\alpha)\pi^{-k}, \omega_2(S))/(\omega_2(S)) &= (S-3, 27, \omega_2(S))/(\omega_2(S)) \\ &= (S-3, 27, \omega_2(3))/(\omega_2(S)) \\ &= (S-3, 27)/(\omega_2(S)),\end{aligned}$$

since $\mathrm{ord}_p(\omega_2(3)) = 3$. Thus we have $\mathrm{ord}_p((\beta-\alpha)\pi^{-k}) \geq 3$ and $k = 0$.

We can easily check that none of the conditions in Theorem 1.2 holds. Therefore $X_{\widetilde{K}}$ is not cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module by Theorem 1.2.

By the same methods as in Example 4.6 for $p = 3$ and by Table 4.4, which is obtained by Mizusawa's program Iwapoly.ub, we obtain Table 4.3.

On the other hand, using Theorems 1.2 (iv) and 4.3 (iv), we obtain the following example in which $X_{\widetilde{K}}$ is cyclic as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-module.

Table 4.3.

d	A_K	$L_K \cap \widetilde{K}$	$E/\mathbb{Q}_3$	$(\mathrm{ord}_E(\alpha), \mathrm{ord}_E(\beta))$	$\mathrm{ord}_E(\alpha-\beta)$	k	$X_{\widetilde{K}}$
32137	$(3,3)$	K_1^{an}	$E=\mathbb{Q}_p$	(1,1)	2	0	non-cyclic
34989	$(3,3)$	K_1^{an}	ramified	(2,2)	5	3	non-cyclic
42619	$(3,3)$	K_1^{an}	$E=\mathbb{Q}_p$	(1,1)	3	0	non-cyclic

(The integer k is defined by (4.2).)

Table 4.4.

d	a generator of $\mathrm{char}(X_{K_\infty^{\mathrm{c}}})$ mod 3^7
32137	$S^2+1047S+1386$
34989	$S^2+66S+117$
42619	$S^2+573S+981$

Example 4.7. Let $p=3$ and $K=\mathbb{Q}(\sqrt{-2437})$. We will prove that $X_{\widetilde{K}}$ is a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}/K)]\!]$-cyclic module using PARI/GP. In this case we have $\mathrm{Cl}_K \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathrm{Cl}_{K_1^{\mathrm{c}}} \cong \mathbb{Z}/3906\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. Hence we have $A_K \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $A_{K_1^{\mathrm{c}}} \cong \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. On the other hand, we have

$$f(S) \equiv S^2+9S+9 \bmod 3^3$$

by Mizusawa's program Iwapoly.ub. Let E be the minimal splitting field of $f(S)$. We set $f(S)=(S-\alpha)(S-\beta)$, where α and $\beta \in E$. Since the discriminant of $f(S)$ is 45 mod 3^3, $E/\mathbb{Q}_p$ is an unramified extension and we get $\mathrm{ord}_E(\alpha-\beta)=1$. By the table in [6], we obtain

$$X_{K_\infty^{\mathrm{c}}} \otimes_{\mathbb{Z}_p} \mathcal{O}_E \cong \langle (1,0),(0,1) \rangle_{\mathcal{O}_E},$$

which implies that $k=0$ in Theorem 1.2.

By Lemma 2.1, we have $L_K \cap \widetilde{K} = K_1^{\mathrm{an}}$. Indeed, we have $(I(3)/S(3^4)) \otimes \mathbb{Z}_3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^3\mathbb{Z} \oplus \mathbb{Z}/3^4\mathbb{Z}$. Hence $\mathrm{Gal}(L_K/L_K \cap \widetilde{K})$ is a direct summand of $\mathrm{Gal}(L_K/K)$. Using [1, Theorem 2], we obtain

$$x^6-20x^4+100x^2+38992$$

as a defining polynomial of K_1^{an} over $\mathbb{Q}$. We can check that both 53 and 251 are primes which split completely in $K_1^{\mathrm{c}}/\mathbb{Q}$. We set

$$\mathfrak{q} = (251,\ -18+\sqrt{-2437}),$$
$$\mathfrak{l} = (53,\ 1+\sqrt{-2437}),$$

which are prime ideals in K lying above $251, 53$, respectively. Using PARI/GP, we compute prime ideals $\mathfrak{Q}_i, \overline{\mathfrak{Q}_i}, \mathfrak{L}_i, \overline{\mathfrak{L}_i}$ in $\mathcal{O}_{K_1^{\mathrm{c}}}$ $(i=1,2,3)$

which satisfy

$$251\mathcal{O}_{K_1^{\mathrm{c}}} = \mathfrak{Q}_1\overline{\mathfrak{Q}_1}\cdots\mathfrak{Q}_3\overline{\mathfrak{Q}_3},$$
$$53\mathcal{O}_{K_1^{\mathrm{c}}} = \mathfrak{L}_1\overline{\mathfrak{L}_1}\cdots\mathfrak{L}_3\overline{\mathfrak{L}_3}$$

and $\mathfrak{Q}_i \mid \mathfrak{q}$, $\overline{\mathfrak{Q}_i} \mid \bar{\mathfrak{q}}$, $\mathfrak{L}_i \mid \mathfrak{l}$, $\overline{\mathfrak{L}_i} \mid \bar{\mathfrak{l}}$ for $i = 1, 2, 3$. We also compute

$$\mathrm{Cl}_{K_1^{\mathrm{c}}} = \mathbb{Z}/(434 \cdot 9)\mathbb{Z}\ [\mathfrak{c}_1] \oplus \mathbb{Z}/9\mathbb{Z}\ [\mathfrak{c}_2]$$

for some ideals $\mathfrak{c}_1$ and $\mathfrak{c}_2$ in $\mathcal{O}_{K_1^{\mathrm{c}}}$, which was computed by PARI/GP. Pick one of $\mathfrak{Q}_i \mid \mathfrak{q}$ (resp. $\mathfrak{L}_i \mid \mathfrak{l}$) and we may assume that it is $\mathfrak{Q}_1$ (resp. $\mathfrak{L}_1$). As in Section 4.3, we take generators $\{434[\mathfrak{Q}_1], 434[\mathfrak{L}_1]\}$ of $A_{K_1^{\mathrm{c}}}$; in other words,

$$A_{K_1^{\mathrm{c}}} = \mathbb{Z}/9\mathbb{Z}\ 434[\mathfrak{Q}_1] \oplus \mathbb{Z}/9\mathbb{Z}\ 434[\mathfrak{L}_1].$$

This implies that both s and t in Section 4.3 are 434.

Now, to obtain a representation as (4.9), we consider the Galois action of $\mathrm{Gal}(K_1^{\mathrm{c}}/K)$ to $[\mathfrak{Q}_1]$ and $[\mathfrak{L}_1]$. Write $[\mathfrak{Q}_1]$ and $[\mathfrak{L}_1]$ as linear forms of $[\mathfrak{c}_1]$ and $[\mathfrak{c}_2]$:

$$[\mathfrak{Q}_1] = 2677[\mathfrak{c}_1] + [\mathfrak{c}_2], \quad [\mathfrak{L}_1] = 3004[\mathfrak{c}_1] + 8[\mathfrak{c}_2].$$

On the other hand, we can compute

$$\begin{aligned}\mathrm{Gal}(L_K/K_1^{\mathrm{an}}) &= \left\langle \left(\frac{L_K/K}{\mathfrak{q}}\right) \cdot \left(\frac{L_K/K}{\mathfrak{l}}\right) \right\rangle \\ &= \left\langle \left(\frac{L_K/K}{\mathfrak{q}}\right)^{434} \cdot \left(\frac{L_K/K}{\mathfrak{l}}\right)^{434} \right\rangle;\end{aligned}$$

in other words, both u and v in Section 4.3 are 434. Let $\bar{\rho}$ be a generator of $\mathrm{Gal}(K_1^{\mathrm{c}}/K)$, which was computed by PARI/GP. We will not describe the complicated computation of $\bar{\rho}$ due to space limitations. Then, by computation of $\bar{\rho}[\mathfrak{c}_1]$ and $\bar{\rho}[\mathfrak{c}_2]$, we can write $\bar{\rho}[\mathfrak{Q}_1]$ and $\bar{\rho}[\mathfrak{L}_1]$ as linear forms of $[\mathfrak{c}_1]$ and $[\mathfrak{c}_2]$:

$$\bar{\rho}[\mathfrak{Q}_1] = 2659[\mathfrak{c}_1] + 4[\mathfrak{c}_2],$$
$$\bar{\rho}[\mathfrak{L}_1] = 1318[\mathfrak{c}_1] + 8[\mathfrak{c}_2].$$

Take a topological generator $\rho \in \mathrm{Gal}(K_\infty^{\mathrm{c}}/K)$ such that ρ is an extension of $\bar{\rho}$. As in Example 4.6, we may replace σ, which gives the isomorphism (4.1), with ρ, since $\mathrm{ord}_p(\alpha)$, $\mathrm{ord}_p(\beta)$, $\mathrm{ord}_p(\alpha - \beta)$, and $\mathcal{M}_{f(S)}^{\mathbb{Q}_p}$ do not depend on the choice of σ and we do not use the form of $f(S)$ in the rest of this example. Since $\mathbb{Z}_p[\mathrm{Gal}(K_1^{\mathrm{c}}/K)] \cong \Lambda/\omega_1(S)\Lambda$, we get

$$\overline{S}[\mathfrak{Q}_1] = -\frac{9156}{18412}[\mathfrak{Q}_1] + \frac{8049}{18412}[\mathfrak{L}_1],$$

$$\overline{S}[\mathfrak{L}_1] = -\frac{13488}{18412}[\mathfrak{Q}_1] + \frac{1686}{18412}[\mathfrak{L}_1],$$

where $\overline{S} = S \bmod \omega_1(S)$. Using the commutative diagram before Theorem 4.2, we can take $x_1, x_2 \in X_{K_\infty^{\mathrm{c}}}$ such that

$$\psi_1(x_1 \bmod \omega_1(S)) = 434[\mathfrak{Q}_1], \quad \psi_1(x_2 \bmod \omega_1(S)) = 434[\mathfrak{Q}_1] + 434[\mathfrak{L}_1].$$

These equations imply that (4.9) becomes

$$Sx_2 \bmod \omega_1(S) = -\frac{32379}{18412}x_1 + \frac{9735}{18412}x_2 \bmod \omega_1(S).$$

Thus A' in Section 4.3 is $-\frac{32379}{18412}$. We have $\mathrm{ord}_E\left(\frac{32379}{18412}\right) = 1 = \mathrm{ord}_E(\beta)$. This means that $X_{\widetilde{K}}$ is a cyclic $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{K}/K)]]$-module by Theorem 4.3 (iv).

By the same methods as in Example 4.7 and Table 4.6, which are obtained by [1, Theorem 2] and PARI/GP, respectively, we obtain Table 4.5.

Table 4.5.

d	A_K	$L_K \cap \widetilde{K}$	$E/\mathbb{Q}_3$	$(\mathrm{ord}_E(\alpha), \mathrm{ord}_E(\beta))$	$\mathrm{ord}_E(\alpha-\beta)$	k	$X_{\widetilde{K}}$
2437	$(3,3)$	K_1^{an}	unramified	(1,1)	1	0	cyclic
3886	$(3,3)$	K_1^{an}	$E = \mathbb{Q}_p$	(1,1)	1	0	cyclic
4027	$(3,3)$	K_1^{an}	$E = \mathbb{Q}_p$	(1,1)	1	0	cyclic
7977	$(3,3)$	K_1^{an}	unramified	(1,1)	1	0	cyclic

(The integer k is defined by (4.2).)

Table 4.6.

d	Defining polynomial of K_1^{an}
2437	$x^6 - 20x^4 + 100x^2 + 38992$
3886	$x^6 - 66x^4 + 1089x^2 + 62176$
4027	$x^6 - 44x^4 + 484x^2 + 4027$
7977	$x^6 - 2x^5 - 53x^4 + 126x^3 + 8634x^2 - 1944x + 1296$

References

[1] D. Brink, “Prime decomposition in the anti-cyclotomic extensions”, *Math. Comput.* **76** (2007), no. 260, p. 2127-2138.

[2] B. Ferrero & L. C. Washington, “Iwasawa invariant μ_p vanishes for abelian number fields”, *Ann. Math.* **109** (1979), p. 377-395.

[3] S. Fujii, “Pseudo-null submodules of the unramified Iwasawa module for $\mathbb{Z}_p^2$-extensions”, *Interdiscip. Inf. Sci.* **16** (2010), p. 55-66.

[4] T. Fukuda, “Iwasawa λ-invariants of imaginary quadratic fields”, *J. College Industrial Technology Nihon Univ.* **27** (1994), p. 35-88.

[5] R. Greenberg, “The Iwasawa invariants of Γ-extensions of a fixed number field”, *Am. J. Math.* **95** (1973), p. 204-214.

[6] M. Koike, “On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$”, *J. Math. Sci., Tokyo* **6** (1999), no. 2, p. 371-396.

[7] M. KURIHARA, "On Brumer-Stark conjecture and Gross' conjecture", Proceeding of the 20th Summer School on Number Theory — Stark's conjecture, `https://www.ma.noda.tus.ac.jp/u/ha/SS2012/Data/kurihara.pdf`.

[8] ———, "Iwasawa theory and Fitting ideals", *J. Reine Angew. Math.* **561** (2003), p. 39-86.

[9] J. MINARDI, "Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields", PhD Thesis, University of Washington, 1986.

[10] T. MIURA, K. MURAKAMI, K. OKANO & R. OTSUKI, "Galois coinvariants of the unramified Iwasawa modules of multiple $\mathbb{Z}_p$-extensions", *Ann. Math.* **45** (2021), no. 2, p. 407-431.

[11] Y. MIZUSAWA, `http://mizusawa.web.nitech.ac.jp/index.html`.

[12] D. G. NORTHCOTT, *Finite free resolutions*, Cambridge Tracts in Mathematics, vol. 71, Cambridge University Press, 1976.

[13] THE PARI GROUP, "PARI/GP version `2.13.2`", 2021, available from `http://pari.math.u-bordeaux.fr/`.

[14] H. SUMIDA, "Greenberg's conjecture and the Iwasawa polynomial", *J. Math. Soc. Japan* **49** (1997), no. 4, p. 689-711.

[15] L. C. WASHINGTON, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, Springer, 1997.

Takashi MIURA
Department of Creative Engineering, National Institute of Technology,
Tsuruoka College,
104 Sawada, Inooka, Tsuruoka, Yamagata 997-8511, Japan
E-mail: `t-miura@tsuruoka-nct.ac.jp`

Kazuaki MURAKAMI
Department of Information Science,
Toho University,
2-2-1 Miyama, Funabashi-shi, Chiba 274-8510 Japan
E-mail: `murakami@is.sci.toho-u.ac.jp`

Keiji OKANO
Department of Teacher Education,
Tsuru University,
3-8-1 Tahara, Tsuru-shi, Yamanashi 402-0054, Japan
E-mail: `okano@tsuru.ac.jp`

Rei OTSUKI
Department of Mathematics,
Keio University,
3-14-1 Hiyoshi, Kouhoku-ku, Yokohama 223-8522, Japan
E-mail: `ray_otsuki@math.keio.ac.jp`