Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Satoshi FUJII et Tsuyoshi ITOH

Some remarks on pseudo-null submodules of tamely ramified Iwasawa modules

Tome 30, nº 2 (2018), p. 533-555.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_533_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 533–555

Some remarks on pseudo-null submodules of tamely ramified Iwasawa modules

par Satoshi FUJII et Tsuyoshi ITOH

Résumé. Nous donnons diverses observations sur la structure des modules d'Iwasawa modérément ramifiés pour une $\mathbb{Z}_p$-extension (ou une $\mathbb{Z}_p$-extension multiple) d'un corps de nombres. Dans cet article, nous considérons la question de savoir si un module d'Iwasawa modérément ramifié possède un sous-module fini (ou pseudo-nul) non-nul ou non. Pour la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$ (avec p impair), nous pouvons obtenir une solution complète à cette question. Nous donnons également des conditions suffisantes pour avoir un sous-module pseudo-nul non-nul pour la $\mathbb{Z}_p^{\oplus 2}$-extension d'un corps quadratique imaginaire. Et nous donnons aussi une application de nos résultats à la « théorie d'Iwasawa non-abélienne » dans le sens d'Ozaki.

Abstract. We will give several observations about the structure of tamely ramified Iwasawa modules for a $\mathbb{Z}_p$-extension (or a multiple $\mathbb{Z}_p$-extension) of an algebraic number field. In the present paper, we consider the question whether a given tamely ramified Iwasawa module has a non-trivial finite (or pseudo-null) submodule or not. For the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (with odd p), we can obtain a complete answer to this question. We also give sufficient conditions for having a non-trivial pseudo-null submodule for the case of the $\mathbb{Z}_p^{\oplus 2}$-extension of an imaginary quadratic field. We also give an application of our results to the "non-abelian Iwasawa theory" in the sense of Ozaki.

1. Introduction

We recall some basic facts on "tamely ramified Iwasawa modules". (For the details of this paragraph, see [12].) Let p be an odd prime number. Firstly, we will consider the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^c$ over the field $\mathbb{Q}$ of rational numbers. Take a finite set S of finite primes of $\mathbb{Q}$ which *does not* contain p. Let $L_S(\mathbb{Q}^c)$ be the maximal abelian pro-p extension of $\mathbb{Q}^c$ which is unramified outside S. (The term "unramified outside S" denotes that every prime of $\mathbb{Q}^c$ lying above $\ell \notin S$ or the infinite prime of $\mathbb{Q}$ is

Manuscrit reçu le 28 octobre 2016, révisé le 12 janvier 2018, accepté le 19 janvier 2018.

2010 *Mathematics Subject Classification.* 11R23.

Mots-clefs. Iwasawa modules, finite submodules, pseudo-null submodules.

The authors express their thanks to Yasushi Mizusawa for his comment, and to Takenori Kataoka for informing his result. The authors also express their thanks to the referee for careful reading the manuscript and giving suggestions. This work was partly supported by JSPS KAKENHI Grant Number JP15K04791.

unramified.) Put $X_S(\mathbb{Q}^c) = \mathrm{Gal}(L_S(\mathbb{Q}^c)/\mathbb{Q}^c)$. We also put $\Gamma = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$, and $\Lambda_1 = \mathbb{Z}_p[\![\Gamma]\!]$ (the completed group ring). Note that $X_S(\mathbb{Q}^c)$ is a finitely generated torsion Λ_1-module because $p \notin S$. $X_S(\mathbb{Q}^c)$ is called the S-ramified Iwasawa module. We note that a prime number $q \in S$ which satisfies $q \not\equiv 1 \pmod{p}$ does not have an effect on the structure of $X_S(\mathbb{Q}^c)$. Thus, it is convenient to add the assumption that

(C1.1) the congruence $q \equiv 1 \pmod{p}$ is satisfied for every $q \in S$.

Greenberg's conjecture [8] says that the "unramified" Iwasawa module (i.e., the case when $S = \emptyset$) of the cyclotomic $\mathbb{Z}_p$-extension of a totally real number field is always finite. Contrary to this, it is known that $X_S(\mathbb{Q}^c)$ can be infinite (see [19]). Note also that $X_S(\mathbb{Q}^c)$ is finitely generated as a $\mathbb{Z}_p$-module, and a formula of the $\mathbb{Z}_p$-rank of $X_S(\mathbb{Q}^c)$ is also known (see [12]). Hence a naive analog of Greenberg's conjecture does not hold for general S. However, we can obtain the following:

Theorem 1.1. *Assume that S is not empty and satisfies* (C1.1)*. Then $X_S(\mathbb{Q}^c)$ always contains a non-trivial finite Λ_1-submodule.*

We shall give two proofs of Theorem 1.1 in Section 2. One is based on Ozaki's method (given in [23]) for studying the unramified Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension of a totally real field. The other is an extension of the argument given in [12].

One may expect to generalize this theorem for other situations (e.g., the cyclotomic $\mathbb{Z}_p$-extension of a totally real field). However, Y. Mizusawa remarked that the same assertion does not hold for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. That is, for a certain set S of finite primes of $\mathbb{Q}$ (which does not contain 2), the S-ramified Iwasawa module of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$ is infinite and does not contain a non-trivial finite submodule (see [18, Theorem 7.3]). It was also found (after Mizusawa's remark) that there are an odd prime p, a totally real number field H, and a finite set S of finite primes of H (which does not contain any prime lying above p) such that the S-ramified Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension of H is infinite and does not contain a non-trivial finite submodule. However, the details about such an example will be given in another paper. (In the present paper, we shall treat only the "having case".)

We are also concerned with whether the similar assertion to Theorem 1.1 is satisfied for the case of multiple $\mathbb{Z}_p$-extensions or not. Let F be an arbitrary algebraic number field and S a finite set of finite primes of F which does not contain any prime lying above p. Let $\widetilde{F}/F$ be the composite of all $\mathbb{Z}_p$-extension of F. Then it is well known that $\mathrm{Gal}(\widetilde{F}/F) \cong \mathbb{Z}_p^{\oplus d}$ as a $\mathbb{Z}_p$-module with a certain positive integer d. We put $\Gamma_d = \mathrm{Gal}(\widetilde{F}/F)$ and $\Lambda_d = \mathbb{Z}_p[\![\Gamma_d]\!]$. Let $L_S(\widetilde{F})$ be the maximal abelian pro-p extension of $\widetilde{F}$ unramified outside S, and put $X_S(\widetilde{F}) = \mathrm{Gal}(L_S(\widetilde{F})/\widetilde{F})$. We can show that

$X_S(\widetilde{F})$ is a finitely generated torsion Λ_d-module by using the argument given in [7].

Greenberg's generalized conjecture (GGC) says that $X_\emptyset(\widetilde{F})$ is a pseudo-null Λ_d-module, that is, the annihilator ideal of Λ_d for $X_\emptyset(\widetilde{F})$ has height at least 2 (see [10, Conjecture (3.5)]). For the case of tamely ramified Iwasawa modules, we consider the following:

Question 1.2. When does $X_S(\widetilde{F})$ have a non-trivial pseudo-null Λ_d-submodule?

When $S = \emptyset$, this question is weaker than GGC, and there are several relating works (see, e.g., [2, 4, 29]).

Note that $X_S(\widetilde{F})$ also can be a non-pseudo-null Λ_d-module when $S \neq \emptyset$ and $d = 2$ (see Section 7). We found that there are many cases such that $X_S(\widetilde{F})$ contains a non-trivial pseudo-null submodule when the base field is an imaginary quadratic field. One more main purpose of the present paper is to state such cases. This will be done in Sections 3 and 4.

In the following, we denote by k an imaginary quadratic field, and S a finite set of finite primes of k which does not contain any prime lying above p (note that p is odd). In this case, $\widetilde{k}/k$ is a $\mathbb{Z}_p^{\oplus 2}$-extension. Similar to the case of $\mathbb{Q}^c/\mathbb{Q}$, any prime $\mathfrak{q} \in S$ satisfying $N\mathfrak{q} \not\equiv 1 \pmod{p}$ does not have an effect on the structure of $X_S(\widetilde{k})$, where $N\mathfrak{q}$ is the absolute norm of $\mathfrak{q}$ (see also, e.g., [12, 13]). Hence, it is sufficient to consider S satisfying the following condition.

(C1.2) $\qquad N\mathfrak{q} \equiv 1 \pmod{p}$ is satisfied for every $\mathfrak{q} \in S$.

Take a prime $\mathfrak{q} \in S$, and let q be the rational prime lying below $\mathfrak{q}$. Then, under the condition (C1.2), q satisfies either of

(1) $q \equiv 1 \pmod{p}$, or
(2) $q \equiv -1 \pmod{p}$, and q is inert in k.

We put

$$S_1 = \{\mathfrak{q} \in S \mid q \text{ satisfies (1)}\} \quad \text{and} \quad S_2 = \{\mathfrak{q} \in S \mid q \text{ satisfies (2)}\}.$$

In Section 3, we consider Question 1.2 for the case that p splits in k. When $S = \emptyset$, the first author [4] gave a $\mathbb{Z}_p^{\oplus 2}$-extension analog of Ozaki's result given in [23]. We will give an S-ramified version of this result. However, we only show it under a (somewhat strict) condition on S, because we could not imitate the original argument in general.

Theorem 1.3. *Assume that p splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}'$ in k. Let $M_{S,\mathfrak{p}}(\widetilde{k})$ be the maximal abelian pro-p extension of $\widetilde{k}$ unramified outside $S \cup \{\mathfrak{p}\}$. Assume also that S satisfies (C1.2) and $S_1 = \emptyset$. Then $X_S(\widetilde{k})$ contains a non-trivial pseudo-null submodule if and only if* $\mathrm{Gal}(M_{S,\mathfrak{p}}(\widetilde{k})/L_S(\widetilde{k}))$ *is non-trivial.*

Note that for the case $S = \emptyset$, the above theorem is just the first author's original result [4, Theorem 1].

In Section 4, we will consider Question 1.2 for the case that p does not split in k (recall that k is an imaginary quadratic field). One of our results is a sufficient condition for having a non-trivial pseudo-null submodule. Before stating this, we will introduce a condition on S.

(C1.3) For $\mathfrak{q} \in S$, if the rational prime q below $\mathfrak{q}$ splits in k, S contains all primes above q.

(Roughly speaking, S comes from a set of rational primes.)

Theorem 1.4. *Assume that p does not split in k. Let S be a finite set of primes of k satisfying the conditions* (C1.2) *and* (C1.3)*. If $S_1 \neq \emptyset$, then $X_S(\tilde{k})$ contains a non-trivial pseudo-null submodule.*

We also mention that further observations are given in Sections 3 and 4. In particular, relating Question 1.2, the structure of S-ramified Iwasawa modules of the "$\mathfrak{p}$-ramified" $\mathbb{Z}_p$-extension is also considered in Section 3.

From our results in the present paper, it can be expected that an analog of Theorem 1.1 for imaginary quadratic fields (with odd p) holds without a few exceptional cases. However, we need more observations to clarify this. (Actually, when we were preparing the present paper, an example such that $X_S(\tilde{k})$ is not trivial and it does not contain a non-trivial pseudo-null submodule was found. The details also will be given in another paper.)

In Section 5, we shall give an application to "non-abelian Iwasawa theory" in the sense of Ozaki [26]. We will show some results on the structure of the Galois group of the maximal S-ramified pro-p extension of $\mathbb{Q}^c$ (or the cyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field). Section 6 is an appendix. We will discuss a certain assertion stated in Section 3. Section 7 is an additional section to remark Kataoka's recent result.

We will define some notations and symbols which will be used. In the following of the present paper, p always denotes an odd prime number. Let $\nu_p(\,\cdot\,)$ be the additive p-adic valuation of $\mathbb{Q}$ which satisfies $\nu_p(p) = 1$. For a finite set A, we denote by $|A|$ its number of elements. Let G be a pro-p group which is topologically isomorphic to the additive group of $\mathbb{Z}_p$. For a $\mathbb{Z}_p[[G]]$-module X, let X^G (resp. X_G) be the G-invariant submodule (resp. the G-coinvariant quotient) of X. For an algebraic number field F, let O_F be the ring of integers of F. As we have already done, we often identify a finite prime of F with the corresponding prime ideal of O_F (or the corresponding prime number when $F = \mathbb{Q}$). We also denote by $F^c = F\mathbb{Q}^c$ the cyclotomic $\mathbb{Z}_p$-extension over F.

We also define some notations concerning extensions with restricted ramification. In this paragraph, k denotes $\mathbb{Q}$ or an imaginary quadratic field.

Let S be a finite set of finite primes of k which does not contain any prime lying above p, and $\mathcal{K}/k$ an algebraic extension. We denote by $L_S(\mathcal{K})$ the maximal abelian pro-p extension over $\mathcal{K}$ unramified outside S, and put $X_S(\mathcal{K}) = \mathrm{Gal}(L_S(\mathcal{K})/\mathcal{K})$. We also denote by $M_{S,p}(\mathcal{K})$ the maximal abelian pro-p extension over $\mathcal{K}$ unramified outside $S \cup \{\text{primes lying above } p\}$, and put $\mathfrak{X}_{S,p}(\mathcal{K}) = \mathrm{Gal}(M_{S,p}(\mathcal{K})/\mathcal{K})$. When k is an imaginary quadratic field in which p splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}'$, we define $M_{S,\mathfrak{p}}(\mathcal{K})$ similarly (unramified outside $S \cup \{\mathfrak{p}\}$). We also put $\mathfrak{X}_{S,\mathfrak{p}}(\mathcal{K}) = \mathrm{Gal}(M_{S,\mathfrak{p}}(\mathcal{K})/\mathcal{K})$.

2. Finite submodules of the S-ramified Iwasawa modules for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$

In this section, let S be a finite set of finite primes of $\mathbb{Q}$ satisfying (C1.1), and assume also that S is not empty. Recall that $\Gamma = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ and $\Lambda_1 = \mathbb{Z}_p[\![\Gamma]\!]$. We shall restate the notations given in [12]. For each positive integer n, we put $\zeta_{p^n} = e^{\frac{2\pi\sqrt{-1}}{p^n}}$. Recall that $\mathbb{Q}^c(\zeta_p) = \bigcup_n \mathbb{Q}(\zeta_{p^n})$ is the cyclotomic $\mathbb{Z}_p$-extension over $\mathbb{Q}(\zeta_p)$. We take a topological generator γ of $\mathrm{Gal}(\mathbb{Q}^c(\zeta_p)/\mathbb{Q}(\zeta_p))$ which satisfies $\zeta_{p^n}^{\gamma} = \zeta_{p^n}^{1+p}$. We also put $\gamma' = \gamma|_{\mathbb{Q}^c}$. As usual, we fix an isomorphism $\Lambda_1 \to \mathbb{Z}_p[\![T]\!]$ satisfying $\gamma' \mapsto 1+T$. Since $X_S(\mathbb{Q}^c)$ is a finitely generated torsion Λ_1-module, the characteristic ideal $\mathrm{char}_{\Lambda_1} X_S(\mathbb{Q}^c) \subseteq \mathbb{Z}_p[\![T]\!]$ can be defined.

We put $r = \max_{q \in S} \nu_p(q-1)$. (From our assumption, $r \geq 1$.) For $i = 1, \ldots, r$, we denote by n_i the number of $q \in S$ satisfying $\nu_p(q-1) = i$. (Note that $n_i \geq 0$, $n_r \geq 1$, and $n_1 + \cdots + n_r = |S|$.) We put $P_i = p^{i-1}$. From the results of [12], we can see that $\mathrm{char}_{\Lambda_1} X_S(\mathbb{Q}^c)$ is generated by $F(T)$, where

$$F(T) = \left(\prod_{i=1}^{r} \left\{ (1+T)^{P_i} - (1+p)^{P_i} \right\}^{n_i} \right) / \left\{ (1+T)^{P_r} - (1+p)^{P_r} \right\}.$$

(Although this is not explicitly written in [12], we can easily deduce this fact from the arguments given there. Especially, see Lemma 2.1, Lemma 2.2, the proof of Lemma 2.3, and Theorem 3.1 of [12].)

We note that Ozaki's arguments given in [23] are also applicable to our situation. Since $F(T)$ is not divisible by T, we can show that $X_S(\mathbb{Q}^c)^{\Gamma} = (X_S(\mathbb{Q}^c)_{\mathrm{fin}})^{\Gamma}$, where $X_S(\mathbb{Q}^c)_{\mathrm{fin}}$ is the maximal finite Λ_1-submodule of $X_S(\mathbb{Q}^c)$ (see the proof of [23, Proposition 2]). Hence, to see Theorem 1.1, it is sufficient to show that $X_S(\mathbb{Q}^c)^{\Gamma}$ is not trivial.

First proof of Theorem 1.1. The following is an analog of Ozaki's result [23, Proposition 2].

Lemma 2.1. *$X_S(\mathbb{Q}^c)^{\Gamma} \cong \mathrm{Gal}(M_{S,p}(\mathbb{Q}^c)/L_S(\mathbb{Q}^c))_{\Gamma}$.*

Proof. This lemma can be shown by using the same argument given in [23]. Hence we only give an outline of the proof.

We claim that the following holds.

(a) As a $\mathbb{Z}_p$-module, $\mathfrak{X}_{S,p}(\mathbb{Q}^c)$ is finitely generated and free.
(b) The prime lying above p is unramified in $M_{S,p}(\mathbb{Q})/\mathbb{Q}^c$.
(c) $\mathfrak{X}_{S,p}(\mathbb{Q}^c)_\Gamma$ is finite.

By using the argument given in the proof of [12, Lemma 3.2], we can show (a). The argument which is given in the proof of [23, Proposition 1] shows (b). Note that $\mathfrak{X}_{S,p}(\mathbb{Q}^c)_\Gamma$ is isomorphic to $\mathrm{Gal}(M_{S,p}(\mathbb{Q})/\mathbb{Q}^c)$. Then the assertion (c) follows from the fact that the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(M_{S,p}(\mathbb{Q})/\mathbb{Q})$ is just 1.

To see the assertion of this lemma, we consider the following exact sequence

$$0 \to \mathrm{Gal}(M_{S,p}(\mathbb{Q}^c)/L_S(\mathbb{Q}^c)) \to \mathfrak{X}_{S,p}(\mathbb{Q}^c) \to X_S(\mathbb{Q}^c) \to 0,$$

and evaluate the Γ-invariant and the Γ-coinvariant of each term. From (a) and (c), we can see that $\mathfrak{X}_{S,p}(\mathbb{Q}^c)^\Gamma$ is trivial. Moreover, from (b), we see that $\mathfrak{X}_{S,p}(\mathbb{Q}^c)_\Gamma \cong X_S(\mathbb{Q}^c)_\Gamma$. The lemma follows from these facts. □

The following is also an analog of Ozaki's result [23] (see also [4, Theorem B]).

Corollary 2.2. *$X_S(\mathbb{Q}^c)$ has a non-trivial finite Λ_1-submodule if and only if $\mathrm{Gal}(M_{S,p}(\mathbb{Q}^c)/L_S(\mathbb{Q}^c))$ is non-trivial.*

The above corollary follows from Lemma 2.1 and Nakayama's lemma. Moreover, by using this, we obtain the following:

Corollary 2.3. *If there is a subset S' of S such that $X_{S'}(\mathbb{Q}^c)$ has a non-trivial finite Λ_1-submodule, then $X_S(\mathbb{Q}^c)$ also has.*

Proof. Note that $M_{S',p}(\mathbb{Q}^c)$ is a subfield of $M_{S,p}(\mathbb{Q}^c)$. Hence, if $\mathrm{Gal}(M_{S',p}(\mathbb{Q}^c)/L_{S'}(\mathbb{Q}^c))$ is not trivial, then $\mathrm{Gal}(M_{S,p}(\mathbb{Q}^c)/L_S(\mathbb{Q}^c))$ is also not trivial. □

Remark 2.4. Since $X_{S'}(\mathbb{Q}^c)$ is a *quotient* of $X_S(\mathbb{Q}^c)$, the above corollary seems a non-trivial result.

Under these preparations, we shall show Theorem 1.1. Take a prime $q \in S$. By using [12, Theorem 3.1] and the fact that $q \equiv 1 \pmod{p}$, we see that $X_{\{q\}}(\mathbb{Q}^c)$ is non-trivial and finite. From Corollary 2.3, $X_S(\mathbb{Q}^c)$ has a non-trivial finite Λ_1-submodule. □

Second proof of Theorem 1.1. Recall that $F(T)$ is prime to T. Then it is well known that

$$|X_S(\mathbb{Q}^c)^\Gamma| \cdot p^{\nu_p(F(0))} = |X_S(\mathbb{Q}^c)_\Gamma|$$

(see, e.g., [28, Exercise 13.12]). We shall compute both $\nu_p(F(0))$ and $|X_S(\mathbb{Q}^c)_\Gamma|$ to show that $X_S(\mathbb{Q}^c)^\Gamma$ is non-trivial.

Since

$$F(0) = \left(\prod_{i=1}^{r} \left\{ 1 - (1+p)^{P_i} \right\}^{n_i} \right) / \left\{ 1 - (1+p)^{P_r} \right\}$$

and $\nu_p(1-(1+p)^{P_i}) = i$, we see that

$$\nu_p(F(0)) = \left(\sum_{i=1}^{r} n_i i \right) - r.$$

Note that only one prime ramifies in $\mathbb{Q}^c/\mathbb{Q}$, and it is totally ramified. Hence, we can see that

$$X_S(\mathbb{Q}^c)_\Gamma \cong X_S(\mathbb{Q}) \tag{2.1}$$

(see the below remark 2.5). It is easy to see that

$$\nu_p(|X_S(\mathbb{Q})|) = \sum_{i=1}^{r} n_i i.$$

These computations imply that $|X_S(\mathbb{Q}^c)^\Gamma| = p^r > 1$. Then we can conclude that $X_S(\mathbb{Q}^c)$ contains a non-trivial finite Λ_1-submodule. □

Remark 2.5. The proof of (2.1) is quite similar to the case of (usual) unramified Iwasawa modules (see, e.g., [28, Chapter 13]). Note also that more general results are already stated in some earlier papers, e.g., [1, 15]. (However, it seems that a few places of Section 3 of [1] need slight correction.)

3. Question 1.2 for imaginary quadratic fields in which p splits

Let k be an imaginary quadratic field, and $\widetilde{k}/k$ the unique $\mathbb{Z}_p^{\oplus 2}$-extension. We put $\Gamma_2 = \mathrm{Gal}(\widetilde{k}/k)$, and $\Lambda_2 = \mathbb{Z}_p[[\Gamma_2]]$. In this section, let S be a finite set of finite primes of k which does not contain any prime lying above p and satisfying (C1.2).

We shall give some sufficient conditions such that $X_S(\widetilde{k})$ has a non-trivial pseudo-null submodule. In the rest of this section, we assume the following:

(C3.1) p splits into two distinct primes $\mathfrak{p}$ and $\mathfrak{p}'$ in k.

Firstly, we shall show Theorem 1.3 (stated in Section 1).

Proof of Theorem 1.3. This also can be shown by imitating the original argument given in [4]. (We remark that $X_S(k^c)$ is finitely generated as a $\mathbb{Z}_p$-module (see [12]), and both $\mathfrak{X}_{S,p}(\widetilde{k})$ and $\mathfrak{X}_{S,\mathfrak{p}}(\widetilde{k})$ are finitely generated Λ_2-modules.) It is sufficient to confirm the following facts. In this proof, we will use a "$\mathbb{Z}_p$-extension" $\widetilde{k}/k^c$.

(a) The equality $M_{S,\mathfrak{p}}(k^c) = L_S(k^c)$ holds under the assumption that $S_1 = \emptyset$ (cf. [4, Lemma 2]).

(b) $\mathfrak{X}_{S,p}(\widetilde{k})$ has Λ_2-rank 1, and does not have a non-trivial pseudo-null Λ_2-submodule.

(c) $\mathfrak{X}_{S,\mathfrak{p}}(\widetilde{k})$ does not have a non-trivial pseudo-null Λ_2-submodule.

Note that under the assumption that $S_1 = \emptyset$, we see that both $M_{S,p}(k^c)$ and $L_S(k^c)$ are Galois extensions over $\mathbb{Q}^c$. Hence $\mathrm{Gal}(k^c/\mathbb{Q}^c)$ acts on $\mathfrak{X}_{S,p}(k^c)$. As usual, we can decompose

$$\mathfrak{X}_{S,p}(k^c) \cong \mathfrak{X}_{S,p}(k^c)^+ \oplus \mathfrak{X}_{S,p}(k^c)^-$$

with respect to the action of $\mathrm{Gal}(k^c/\mathbb{Q}^c)$. We also see that $\mathfrak{X}_{S,p}(k^c)^+$ is isomorphic to $\mathfrak{X}_{S^\dagger,p}(\mathbb{Q}^c)$, where $S^\dagger$ is the set of rational primes lying below S. In this case, we can see that $\mathfrak{X}_{S^\dagger,p}(\mathbb{Q}^c) = \mathfrak{X}_{\emptyset,p}(\mathbb{Q}^c)$ because $S_1 = \emptyset$ (see also the proof of [12, Lemma 3.2]), and then it is trivial. From this, we can use the argument given in the proof of [4, Lemma 2], and then (a) follows. The assertion (b) is well known (see, e.g., [21, Théorème 3,1], [11, Theorem 4], [20, 9.3.2 Corollary]). Finally, we can see (c) from (b) by using arguments given in [27] and [4]. The remaining part of the proof is quite similar to that of the original proof given in [4] (when $S = \emptyset$). □

Remark 3.1. In the above proof, the assumption that $S_1 = \emptyset$ is crucial. Actually, the assertion (a) does not hold for general S (see Section 6).

Similar to Corollary 2.3, we can obtain the following:

Corollary 3.2. *Assume that k and p satisfy (C3.1), and S satisfies (C1.2). Assume also that $S_1 = \emptyset$. If there exists a subset S' of S (including the case when $S' = \emptyset$) such that $X_{S'}(\widetilde{k})$ has a non-trivial pseudo-null Λ_2-submodule, then $X_S(\widetilde{k})$ also has.*

In particular, if $X_\emptyset(\widetilde{k})$ is not trivial and GGC holds, then $X_S(\widetilde{k})$ has a non-trivial pseudo-null Λ_2-submodule for every S which satisfies $S_1 = \emptyset$. For example, when the class number of k is prime to p and the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension k^c/k is greater than 1, these conditions are satisfied from Minardi's result [17, Proposition 3.A].

We shall give a sufficient condition such that $X_S(\widetilde{k})$ has a non-trivial pseudo-null submodule. Let $k^{\mathfrak{p}}/k$ be the unique $\mathbb{Z}_p$-extension unramified outside $\mathfrak{p}$. Minardi [17] used $k^{\mathfrak{p}}/k$ to give a sufficient condition for the validity of GGC. We also use this $\mathbb{Z}_p$-extension, however, our argument is somewhat different from Minardi's one.

We put $\Gamma_{\mathfrak{p}} = \mathrm{Gal}(k^{\mathfrak{p}}/k)$, and $\Lambda_{\mathfrak{p}} = \mathbb{Z}_p[\![\Gamma_{\mathfrak{p}}]\!]$. We can see that both $X_S(k^{\mathfrak{p}})$ and $\mathfrak{X}_{S,\mathfrak{p}}(k^{\mathfrak{p}})$ are finitely generated torsion $\Lambda_{\mathfrak{p}}$-modules. Take a topological generator $\gamma_{\mathfrak{p}}$ of $\Gamma_{\mathfrak{p}}$, and fix an isomorphism $\Lambda_{\mathfrak{p}} \to \mathbb{Z}_p[\![T_*]\!]$ with $\gamma_{\mathfrak{p}} \mapsto 1 + T_*$. As usual, we also consider $X_S(k^{\mathfrak{p}})$ and $\mathfrak{X}_{S,\mathfrak{p}}(k^{\mathfrak{p}})$ as $\mathbb{Z}_p[\![T_*]\!]$-modules.

Lemma 3.3. *Suppose that k and p satisfy* (C3.1)*. Assume that S satisfies* (C1.2)*, and $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}/k$. Then*

$$X_S(k^{\mathfrak{p}})^{\Gamma_{\mathfrak{p}}} \cong \mathrm{Gal}(M_{S,\mathfrak{p}}(k^{\mathfrak{p}})/L_S(k^{\mathfrak{p}}))_{\Gamma_{\mathfrak{p}}}.$$

Proof. The proof is quite similar to that of Lemma 2.1 (and hence it is also based on Ozaki's argument). It is sufficient to check the following assertions.

(a) $\mathfrak{X}_{S,\mathfrak{p}}(k^{\mathfrak{p}})$ has no non-trivial finite $\Lambda_{\mathfrak{p}}$-submodule.
(b) The prime lying above $\mathfrak{p}$ is unramified in $M_{S,\mathfrak{p}}(k)/k^{\mathfrak{p}}$.
(c) $\mathfrak{X}_{S,\mathfrak{p}}(k^{\mathfrak{p}})_{\Gamma_{\mathfrak{p}}}$ is finite.

The assertion (a) can be shown by using the argument given in [9, p. 91–94]. By using class field theory, we see that the $\mathbb{Z}_p$-rank of $\mathfrak{X}_{S,\mathfrak{p}}(k)$ is 1. The assertion (c) follows from this. Note that the inertia subgroup of $\mathfrak{X}_{S,\mathfrak{p}}(k)$ for $\mathfrak{p}$ is a cyclic $\mathbb{Z}_p$-module. Since $\mathfrak{p}$ is ramified in $k^{\mathfrak{p}}/k$, the assertion (b) follows. (Remark also that (c) implies that a generator of the characteristic ideal $\mathrm{char}_{\Lambda_{\mathfrak{p}}}\mathfrak{X}_{S,\mathfrak{p}}(k^{\mathfrak{p}}) \subseteq \mathbb{Z}_p[[T_*]]$ is not divisible by T_*.) □

Corollary 3.4. *Suppose that k and p satisfy* (C3.1)*. Assume that S satisfies* (C1.2)*, and $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}/k$.*

(1) *$X_S(k^{\mathfrak{p}})$ contains a non-trivial finite $\Lambda_{\mathfrak{p}}$-submodule if and only if $\mathrm{Gal}(M_{S,\mathfrak{p}}(k^{\mathfrak{p}})/L_S(k^{\mathfrak{p}}))$ is not trivial.*
(2) *If there exists a subset S' of S such that $X_{S'}(k^{\mathfrak{p}})$ has a non-trivial finite $\Lambda_{\mathfrak{p}}$-submodule, then $X_S(k^{\mathfrak{p}})$ also has.*
(3) *Assume that $S_1 = \emptyset$. If there exists a subset S' of S such that $X_{S'}(k^{\mathfrak{p}})$ has a non-trivial finite $\Lambda_{\mathfrak{p}}$-submodule, then $X_S(\widetilde{k})$ has a non-trivial pseudo-null Λ_2-submodule.*

Proof. Recall the argument given in Section 2. Let $X_S(k^{\mathfrak{p}})_{\mathrm{fin}}$ be the maximal finite $\Lambda_{\mathfrak{p}}$-submodule of $X_S(k^{\mathfrak{p}})$. Then we can show that $X_S(k^{\mathfrak{p}})^{\Gamma_{\mathfrak{p}}} \cong (X_S(k^{\mathfrak{p}})_{\mathrm{fin}})^{\Gamma_{\mathfrak{p}}}$. By using Lemma 3.3 and Nakayama's lemma, the assertion (1) follows. The proof of (2) is similar to that of Corollary 2.3, hence we omit it here. We will show (3). Assume that $X_{S'}(k^{\mathfrak{p}})$ has a non-trivial finite $\Lambda_{\mathfrak{p}}$-submodule. By (1), we see that $\mathrm{Gal}(M_{S',\mathfrak{p}}(k^{\mathfrak{p}})/L_{S'}(k^{\mathfrak{p}}))$ is not trivial. Since every prime lying above $\mathfrak{p}$ does not ramify in $\widetilde{k}/k^{\mathfrak{p}}$, we see that $M_{S',\mathfrak{p}}(k^{\mathfrak{p}})L_S(\widetilde{k})/L_S(\widetilde{k})$ is a non-trivial extension. This implies that $\mathrm{Gal}(M_{S,\mathfrak{p}}(\widetilde{k})/L_S(\widetilde{k}))$ is not trivial because $S' \subset S$. The assertion follows from Theorem 1.3. □

For an integer $n \geq 0$, let $k_n^{\mathfrak{p}}$ be the nth layer of $k^{\mathfrak{p}}/k$.

Corollary 3.5. *Suppose that k and p satisfy* (C3.1)*. Assume that S satisfies* (C1.2)*, and $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}/k$. We denote by $D_S(k_n^{\mathfrak{p}})$ the decomposition subgroup of $X_S(k_n^{\mathfrak{p}})$ for the prime lying above $\mathfrak{p}$. If there exists* *a subset S' of S such that $D_{S'}(k^{\mathfrak{p}}_{n_1})$ is not trivial for some $n_1 \geq 0$, then the following assertions hold.*

(1) *$X_S(k^{\mathfrak{p}})$ has a non-trivial finite submodule.*

(2) *Moreover, if $S_1 = \emptyset$, then $X_S(\widetilde{k})$ has a non-trivial pseudo-null submodule.*

Proof. We will only show the assertion (1), because (2) directly follows from this and Corollary 3.4(3).

We mention that some standard tools obtained in the studies of Greenberg's conjecture for totally real fields (e.g., [8, 23]) are also usable for our situation (see also [5] for the case of $k^{\mathfrak{p}}/k$ with $S' = \emptyset$).

Let $\mathfrak{m}$ be the product of all prime ideals of k contained in S'. (We identify a finite prime of k and the corresponding prime ideal of O_k. We put $\mathfrak{m} = O_k$ when $S' = \emptyset$.) We denote by $\mathfrak{m}_n$ the extension of $\mathfrak{m}$ in $k^{\mathfrak{p}}_n$. Let $A_{S'}(k^{\mathfrak{p}}_n)$ be the Sylow p-subgroup of the ray class group of $k^{\mathfrak{p}}_n$ modulo $\mathfrak{m}_n$. (If $S' = \emptyset$, then $A_{S'}(k^{\mathfrak{p}}_n)$ is the Sylow p-subgroup of the ideal class group.) By class field theory, we see that $X_{S'}(k^{\mathfrak{p}}_n)$ is isomorphic to $A_{S'}(k^{\mathfrak{p}}_n)$ because S' does not contain any prime lying above p. Under this isomorphism, $D_{S'}(k^{\mathfrak{p}}_n)$ can be identified with the subgroup of $A_{S'}(k^{\mathfrak{p}}_n)$ which consists of the classes containing a power of the prime ideal lying above $\mathfrak{p}$.

We put

$$B_{S'}(k^{\mathfrak{p}}_n) = \{c \in A_{S'}(k^{\mathfrak{p}}_n) \mid c^{\gamma} = c \ \text{ for } \gamma \in \mathrm{Gal}(k^{\mathfrak{p}}_n/k)\}$$

(cf. [8]). Recall that $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}_n/k$, and it is the unique ramified prime. From this, we can see that $|B_{S'}(k^{\mathfrak{p}}_n)| = |A_{S'}(k)|$ (see also [8, p. 269]). Hence $|B_{S'}(k^{\mathfrak{p}}_n)|$ is bounded with respect to n. Since $D_{S'}(k^{\mathfrak{p}}_n)$ is contained in $B_{S'}(k^{\mathfrak{p}}_n)$, the order of $D_{S'}(k^{\mathfrak{p}}_n)$ is also bounded.

We will mention one more fact. The essential part of the arguments in this paragraph is due to [22]. For integers $m > n \geq 0$, let $i_{n,m}$ be the natural mapping $A_{S'}(k^{\mathfrak{p}}_n) \to A_{S'}(k^{\mathfrak{p}}_m)$ which comes from the extension mapping of ideals. We also consider the restriction mapping $p_n : X_{S'}(k^{\mathfrak{p}}) \to X_{S'}(k^{\mathfrak{p}})/\omega_n X_{S'}(k^{\mathfrak{p}})$, where $\omega_n = (1+T_*)^{p^n} - 1 \in \mathbb{Z}_p[\![T_*]\!]$. Since $\mathfrak{p}$ is the unique ramified prime in $k^{\mathfrak{p}}/k$ and it is totally ramified, we can see that

$$X_{S'}(k^{\mathfrak{p}})/\omega_n X_{S'}(k^{\mathfrak{p}}) \cong X_{S'}(k^{\mathfrak{p}}_n) \ (\cong A_{S'}(k^{\mathfrak{p}}_n))$$

(see also Remark 2.5). Let $X_{S'}(k^{\mathfrak{p}})_{\mathrm{fin}}$ be the maximal finite $\Lambda_{\mathfrak{p}}$-submodule of $X_{S'}(k^{\mathfrak{p}})$. Then, for all sufficiently large m, we see that the kernel of $i_{n,m}$ is isomorphic to $p_n(X_{S'}(k^{\mathfrak{p}})_{\mathrm{fin}})$ by using the same argument given in the proof of [22, p. 218, Proposition]. Hence, if the kernel of $i_{n,m}$ is not trivial, then $X_{S'}(k^{\mathfrak{p}})$ has a non-trivial finite submodule.

Under these preparations, we shall show the assertion (1). Recall that $|D_{S'}(k^{\mathfrak{p}}_n)|$ is bounded with respect to n. Hence, by using a similar argument as given in [8, p. 267] (the proof of Corollary to Proposition 1), we see that the image of $D_{S'}(k^{\mathfrak{p}}_{n_1})$ by i_{n_1,n_2} is trivial for a sufficiently large $n_2(> n_1)$. This implies that $A_{S'}(k^{\mathfrak{p}}_{n_1})$ contains a ray class which becomes trivial in $k^{\mathfrak{p}}_{n_2}$. Hence, from the above mentioned fact, $X_{S'}(k^{\mathfrak{p}})$ has a non-trivial finite submodule. By using Corollary 3.4 (2), we see that $X_S(k^{\mathfrak{p}})$ also has a non-trivial finite submodule. □

When $D_{\emptyset}(k)$ is not trivial (that is, the order of the ideal class of k containing $\mathfrak{p}$ is divisible by p) and $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}/k$, then $X_S(\widetilde{k})$ contains a non-trivial pseudo-null submodule for every S satisfying (C1.2). If otherwise, we can obtain the following:

Theorem 3.6. *Suppose that k and p satisfy* (C3.1)*. Assume that $\mathfrak{p}$ is totally ramified in $k^{\mathfrak{p}}/k$. There are infinitely many finite primes $\mathfrak{q}$ of k such that $X_{\{\mathfrak{q}\}}(\widetilde{k})$ contains a non-trivial pseudo-null submodule. In particular, we can take $\mathfrak{q}$ such that $S_1 = \emptyset$ for $S = \{\mathfrak{q}\}$.*

Proof. Let q be an odd prime number which is inert in k, and satisfies $q \equiv -1 \pmod{p}$. Let $\mathfrak{q}$ be the unique prime k lying above q. In this case, we can decompose $A_{\{\mathfrak{q}\}}(k) \cong A_{\{\mathfrak{q}\}}(k)^+ \oplus A_{\{\mathfrak{q}\}}(k)^-$ with respect to the action of $\mathrm{Gal}(k/\mathbb{Q})$. Since $q \not\equiv 1 \pmod{p}$, it follows that $A_{\{q\}}(\mathbb{Q})$ is trivial. This implies that $A_{\{\mathfrak{q}\}}(k) \cong A_{\{\mathfrak{q}\}}(k)^-$. Since $\mathfrak{p}$ and $\mathfrak{p}'$ are conjugate over $\mathbb{Q}$, if the subgroup of $A_{\{\mathfrak{q}\}}(k)$ generated by powers of $\mathfrak{p}$ and $\mathfrak{p}'$ is non-trivial, then $D_{\{\mathfrak{q}\}}(k)$ is also non-trivial. If we put $S = \{\mathfrak{q}\}$, then $S_1 = \emptyset$. By Corollary 3.5, if $D_{\{\mathfrak{q}\}}(k)$ is non-trivial, then we can conclude that $X_{\{\mathfrak{q}\}}(\widetilde{k})$ has a non-trivial pseudo-null submodule. We show that infinitely many such prime numbers q exist.

Let $E_{\{p\}}$ be the group of p-units of k, that is, the group of units in $O_k[\frac{1}{p}]$. Since p splits in k, the $\mathbb{Z}$-rank of $E_{\{p\}}$ is 2. Let $E_{\{p\}}/E_{\{p\}}^p = (E_{\{p\}}/E_{\{p\}}^p)^+ \oplus (E_{\{p\}}/E_{\{p\}}^p)^-$ be the decomposition with respect to the action of $\mathrm{Gal}(k/\mathbb{Q})$. We remark that $(E_{\{p\}}/E_{\{p\}}^p)^-$ is a non-trivial cyclic group. Let π be an element of $E_{\{p\}}$ whose class modulo $E_{\{p\}}^p$ is trivial in $(E_{\{p\}}/E_{\{p\}}^p)^+$ and generates $(E_{\{p\}}/E_{\{p\}}^p)^-$. Fix a primitive pth root ζ_p of unity. We note that π is not a pth power in $k(\zeta_p)$ because the degree $[k(\zeta_p) : k]$ is prime to p. By Kummer theory, we have an isomorphism

$$\mathrm{Gal}\left(k\left(\zeta_p, \sqrt[p]{\pi}\right)/k(\zeta_p)\right) \cong \mathrm{Hom}((E_{\{p\}}/E_{\{p\}}^p)^-, \langle \zeta_p \rangle)$$

of $\mathrm{Gal}(k(\zeta_p)/\mathbb{Q})$-modules. From natural restriction mappings of Galois groups, we have an isomorphism

$$\mathrm{Gal}(k(\zeta_p)/\mathbb{Q}) \cong \mathrm{Gal}(k/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

Choose an element σ of $\mathrm{Gal}(k(\zeta_p)/\mathbb{Q})$ such that $\sigma|_k$ generates $\mathrm{Gal}(k/\mathbb{Q})$, and that $\sigma|_{\mathbb{Q}(\zeta_p)}$ is the complex conjugation. Let F be the subfield fixed by σ. (Actually, F is the maximal real subfield of $k(\zeta_p)$.) By the choice of

σ, one sees that $k(\zeta_p, \sqrt[p]{\pi})/F$ is abelian, and hence is a cyclic extension of degree $2p$. Let $\widetilde{\sigma}$ be a generator of $\mathrm{Gal}(k(\zeta_p, \sqrt[p]{\pi})/F)$.

By the Čebotarev density theorem, there exist infinitely many prime numbers q such that q splits completely in F and

$$\widetilde{\sigma} = \left[\frac{k(\zeta_p, \sqrt[p]{\pi})/F}{\mathfrak{Q}}\right]$$

for some prime $\mathfrak{Q}$ of $k(\zeta_p, \sqrt[p]{\pi})$ lying above q, where the right-hand-side is the Frobenius element of $\mathfrak{Q}$ at the extension $k(\zeta_p, \sqrt[p]{\pi})/F$. Then one sees that q is inert in k and that $q \equiv -1 \pmod p$. Let $\mathfrak{q}$ be the prime of k lying above q. Since a prime lying below $\mathfrak{Q}$ is inert in $k(\zeta_p, \sqrt[p]{\pi})/k(\zeta_p)$, π mod $\mathfrak{q}$ is not in $\{(O_k/\mathfrak{q})^\times\}^p$. Also, since the p-primary part of $(O_k/\mathfrak{q})^\times$ can be embedded into $A_{\{\mathfrak{q}\}}(k)$, we see that $D_{\{\mathfrak{q}\}}(k)$ is not trivial. This completes the proof. □

4. Question 1.2 for imaginary quadratic fields in which p does not split

Let k be an imaginary quadratic field. In this section, we shall consider Question 1.2 for the case when p does not split in k. Let S be a finite set of finite primes of k which does not contain the prime lying above p. Some notations defined in Section 3 are also used in this section.

Minardi [17] gave examples such that the unramified Iwasawa module $X_\emptyset(\tilde{k})$ has a non-trivial pseudo-null submodule when p is inert in k by showing that the decomposition subgroup for a prime lying above p is not trivial. (See also [2].) The same idea can be applicable to our tamely ramified case.

Throughout this section, we assume that k and p satisfy the following condition.

(C4.1) $\qquad$ p does not split in k.

Let $\mathcal{K}$ be an intermediate field of $\tilde{k}/k$. For a prime $\mathfrak{P}$ of $\mathcal{K}$ lying above p, we denote by $D_S(\mathcal{K})_{\mathfrak{P}}$ the decomposition subgroup of $X_S(\mathcal{K})$ for $\mathfrak{P}$. Put $D_S(\mathcal{K}) = \sum_{\mathfrak{P}} D_S(\mathcal{K})_{\mathfrak{P}}$, where $\mathfrak{P}$ runs over all primes lying above p. (Note that there are only finitely many primes lying above p in $\mathcal{K}$.) The following lemma plays a fundamental role in this section.

Lemma 4.1. *Assume that k and p satisfy (C4.1). Let S be a finite set of primes of k satisfying (C1.2). Then the following assertions hold.*

(1) *(See also [17].) $D_S(\tilde{k})$ is a pseudo-null Λ_2-module.*

(2) *For a finite subextension F/k contained in $\tilde{k}$, if $D_S(F)$ is not trivial, then $X_S(\tilde{k})$ contains a non-trivial pseudo-null submodule.*

Proof. Note that $D_S(\tilde{k})$ is a Λ_2-submodule and it is finitely generated as a $\mathbb{Z}_p$-module. Hence (1) follows.

We shall show (2). Let k' be the inertia field of $\widetilde{k}/k$ for the unique prime $\mathfrak{p}$ lying above p. We remark that $\mathfrak{p}$ splits completely in k', because k'/k is an unramified abelian p-extension and the order of $\mathfrak{p}$ in the ideal class group of k is not divisible by p. Of course, every prime lying above p is totally ramified in $\widetilde{k}/k'$. From this fact, if $D_S(F)$ is non-trivial, then $D_S(\tilde{k})$ is also. Combining with the result in (1), we obtain (2). □

In particular, if $D_S(k)$ is not trivial, then $X_S(\widetilde{k})$ has a non-trivial pseudo-null submodule. Apart from this, we can obtain the following:

Proposition 4.2. *Assume that k is $\mathbb{Q}$, or an imaginary quadratic field satisfying* (C4.1). *Assume also that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$. Let $\mathfrak{q}$ be a finite prime of k satisfying $N\mathfrak{q} \equiv 1 \pmod{p}$. When k is an imaginary quadratic field, suppose that $\mathfrak{q}$ is a principal ideal generated by q. Let K/k a $\mathbb{Z}_p$-extension which is totally ramified at the prime lying above p. For an integer $n \geq 0$, we denote by K_n the nth layer of K/k. Let $D_{\{\mathfrak{q}\}}(K_n)$ be the decomposition subgroup of $X_{\{\mathfrak{q}\}}(K_n)$ for the unique prime lying above p. If $X_{\{\mathfrak{q}\}}(K)$ has a non-trivial finite $\mathbb{Z}_p[\![\mathrm{Gal}(K/k)]\!]$-submodule, then $D_{\{\mathfrak{q}\}}(K_n)$ is not trivial for some $n \geq 0$.*

To show this proposition, we mainly use the techniques given in [8] (especially, the proof of Theorem 1). However, our case is slightly complicated. We need some lemmas. Put $G_n = \mathrm{Gal}(K_n/k)$, and fix a generator γ of G_n. In the following, we denote by (a) the principal ideal of K_n generated by a.

Lemma 4.3. *Let the assumptions be as in Proposition 4.2. We put*

$$V_n = \{a \in K_n^\times \mid (a) \text{ is prime to } (q)\}, V_n' = \{a \in K_n^\times \mid a \equiv 1 \pmod{(q)}\}.$$

Then, both $H^1(G_n, V_n)$ and $H^1(G_n, V_n')$ are trivial.

Proof. The assertion essentially comes from Hilbert's Theorem 90. We denote by $N_{K_n/k}$ the norm mapping from K_n to k. Take $a \in V_n$ satisfying $N_{K_n/k}a = 1$, then there exists an element b of $K_n^\times$ satisfying $b^{\gamma-1} = a$. We write $(b) = \mathfrak{Q}\mathfrak{A}$ such that $\mathfrak{Q}$ is a product of prime ideals lying above $\mathfrak{q}$ and $\mathfrak{A}$ is prime to (q). Since $(b^{\gamma-1})$ is prime to (q), we see that $\mathfrak{Q}^\gamma = \mathfrak{Q}$. From this, we can write $\mathfrak{Q} = (q)^m$ with an integer m. Hence $c = bq^{-m}$ is contained in V_n and satisfies $c^{\gamma-1} = a$. This implies that $H^1(G_n, V_n)$ is trivial.

To show the remaining part, we consider the following exact sequence.

$$0 \to V_n' \to V_n \to (O_{K_n}/(q))^\times \to 0.$$

We claim that $H^1(G_n, (O_{K_n}/(q))^\times)$ is trivial. Let K_d be the decomposition field of K_n/k for $\mathfrak{q}$ $(0 \leq d \leq n)$. Take a prime $\mathfrak{q}'$ of K_d lying above $\mathfrak{q}$, and denote by $\mathfrak{q}'_n$ the extension of $\mathfrak{q}'$ in K_n. Then, by using Shapiro's lemma, we see

$$H^1(G_n, (O_{K_n}/(q))^\times) \cong H^1(\mathrm{Gal}(K_n/K_d), (O_{K_n}/\mathfrak{q}'_n)^\times).$$

Since $\mathfrak{q}'$ does not decompose in K_n, the right hand side is trivial. The claim follows. We also see that $\hat{H}^0(G_n, (O_{K_n}/(q))^\times)$ is trivial (where $\hat{H}^0$ is the 0th Tate cohomology group). This implies that $H^1(G_n, V'_n) \cong H^1(G_n, V_n)$, and then $H^1(G_n, V'_n)$ is also trivial. □

Lemma 4.4. *Let the assumptions be as in Proposition 4.2. We put*

$$S_n = \{(a) \mid a \in V'_n\}.$$

Then $H^1(G_n, S_n)$ is trivial.

Proof. We can obtain the following exact sequence

$$0 \to E'_n \to V'_n \to S_n \to 0,$$

where E'_n is the group of units in K_n which are congruent to 1 modulo (q). Since the unit group of k is finite and its order is prime to p, we see $\hat{H}^0(G_n, E'_n)$ is trivial. Then there is a surjective homomorphism

$$H^1(G_n, V'_n) \to H^1(G_n, S_n).$$

The assertion follows from Lemma 4.3. □

Lemma 4.5. *Let the assumptions be as in Proposition 4.2. We denote by $A_{\{\mathfrak{q}\}}(K_n)$ the Sylow p-subgroup of the ray class group of K_n modulo (q). We put*

$$B_{\{\mathfrak{q}\}}(K_n) = \{c \in A_{\{\mathfrak{q}\}}(K_n) \mid c^\gamma = c\},$$

$$B'_{\{\mathfrak{q}\}}(K_n) = \{c \in A_{\{\mathfrak{q}\}}(K_n) \mid c \textit{ contains an ideal } \mathfrak{A} \textit{ satisfying } \mathfrak{A}^\gamma = \mathfrak{A}\}.$$

Then $B_{\{\mathfrak{q}\}}(K_n) = B'_{\{\mathfrak{q}\}}(K_n)$.

Proof. We can imitate the argument given in the proof of [8, Theorem 1]. (We use the previous lemma instead of Hilbert's Theorem 90.)

It is sufficient to show that $B_{\{\mathfrak{q}\}}(K_n) \subseteq B'_{\{\mathfrak{q}\}}(K_n)$. Take a ray class $c \in B_{\{\mathfrak{q}\}}(K_n)$ and an ideal $\mathfrak{A}$ contained in c. Then $\mathfrak{A}^\gamma = (a)\mathfrak{A}$ with some $a \in V'_n$. We also see that $(N_{K_n/k}a) = (1)$. By lemma 4.4, there exists an element $b \in V'_n$ satisfing $(b)^{\gamma-1} = (a)$. Then the ideal $\mathfrak{A}(b^{-1})$ is invariant under γ, and contained in the same ray class c. The assertion follows. □

Let $i_{0,n}$ be the mapping which comes from the extension mapping of ideals from $A_{\{\mathfrak{q}\}}(k)$ to $A_{\{\mathfrak{q}\}}(K_n)$ (see also Section 3).

Lemma 4.6. *Let the assumptions be as in Proposition 4.2. If $X_{\{\mathfrak{q}\}}(K)$ has a non-trivial finite submodule, then the kernel of $i_{0,n}$ is not trivial for some $n > 0$.*

Proof. This can be shown by using the arguments given in [22] and [23]. However, we need a slight modification.

We put $\Gamma_* = \mathrm{Gal}(K/k)$. In our situation, we obtain the isomorphisms

$$X_{\{\mathfrak{q}\}}(K)_{\Gamma_*} \cong X_{\{\mathfrak{q}\}}(k) \cong A_{\{\mathfrak{q}\}}(k).$$

Let $p_0 : X_{\{\mathfrak{q}\}}(K) \to X_{\{\mathfrak{q}\}}(K)_{\Gamma_*}$ be the restriction mapping. For a sufficiently large n, we see that the kernel of $i_{0,n}$ is isomorphic to $p_0(X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}})$, where $X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}}$ is the maximal finite $\mathbb{Z}_p[\![\Gamma_*]\!]$-submodule of $X_{\{\mathfrak{q}\}}(K)$ (see the proof of [22, p. 218, Proposition]).

We shall consider the following exact sequence.

$$0 \to X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}} \to X_{\{\mathfrak{q}\}}(K) \to X_{\{\mathfrak{q}\}}(K)/X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}} \to 0.$$

By taking the Γ_*-invariant and the Γ_*-coinvariant of each term, we obtain the following exact sequence.

$$(X_{\{\mathfrak{q}\}}(K)/X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}})^{\Gamma_*} \to (X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}})_{\Gamma_*} \to X_{\{\mathfrak{q}\}}(K)_{\Gamma_*}.$$

Since $X_{\{\mathfrak{q}\}}(K)_{\Gamma_*}$ is finite, we can show that $(X_{\{\mathfrak{q}\}}(K)/X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}})^{\Gamma_*}$ is trivial, and then the right homomorphism is injective. This implies that $p_0(X_{\{\mathfrak{q}\}}(K)_{\mathrm{fin}})$ is not trivial. As a consequence, the kernel of $i_{0,n}$ is also not trivial for some n. □

Proof of Proposition 4.2. The following proof uses the ideas given in [8, p. 269]. Assume that $X_{\{\mathfrak{q}\}}(K)$ has a non-trivial finite submodule. Then, by Lemma 4.6, the kernel of $i_{0,n}$ is not trivial for some $n > 0$. We fix such n. Since the prime lying above p is totally ramified in K/k, we can see that $|B_{\{\mathfrak{q}\}}(K_n)| = |A_{\{\mathfrak{q}\}}(k)|$ (see also the proof of Corollary 3.5). We also remark that $|A_{\{\mathfrak{q}\}}(k)| > 1$ under the assumptions of this proposition, hence $B_{\{\mathfrak{q}\}}(K_n)$ is not trivial. As noted in Section 3, $D_{\{\mathfrak{q}\}}(K_n)$ can be identified with the subgroup of $A_{\{\mathfrak{q}\}}(K_n)$ generated by the ray class containing the prime ideal lying above p. By using Lemma 4.5, we see

$$|B_{\{\mathfrak{q}\}}(K_n)| = |B'_{\{\mathfrak{q}\}}(K_n)| = |i_{0,n}(A_{\{\mathfrak{q}\}}(k))\, D_{\{\mathfrak{q}\}}(K_n)|.$$

Since $|i_{0,n}(A_{\{\mathfrak{q}\}}(k))|$ is smaller than $|B_{\{\mathfrak{q}\}}(K_n)|$, we see that $D_{\{\mathfrak{q}\}}(K_n)$ is not trivial. □

We will show Theorem 1.4 (stated in Section 1).

Proof of Theorem 1.4. For a non-negative integer n, let $\mathbb{Q}_n^c$ be the nth layer of $\mathbb{Q}^c/\mathbb{Q}$. Take a prime $\mathfrak{q} \in S_1$, and denote by q the prime number lying below $\mathfrak{q}$. Then $\{q\}$ satisfies the condition (C1.1).

Let $D_{\{q\}}(\mathbb{Q}_n^c)$ be the decomposition subgroup of $X_{\{q\}}(\mathbb{Q}_n^c)$ for the unique prime lying above p. Note that $X_{\{q\}}(\mathbb{Q}^c)$ is non-trivial and finite by [12, Theorem 3.1]. Hence we can apply Proposition 4.2, and then we see that $D_{\{q\}}(\mathbb{Q}_n^c)$ is not trivial for a certain n.

Under the condition (C1.3), we see that $L_{\{q\}}(\mathbb{Q}_n^c)k$ is contained in $L_S(k_n^c)$, where k_n^c is the nth layer of k^c/k. Hence the non-triviality of $D_{\{q\}}(\mathbb{Q}_n^c)$ implies the non-triviality of the decomposition subgroup $D_S(k_n^c)$ of $X_S(k_n^c)$ for the unique prime lying above p. Then, by using Lemma 4.1 (ii), we can obtain the assertion. (We remark that this proof also works for the case that $k = \mathbb{Q}(\sqrt{-3})$ and $p = 3$, because we use Proposition 4.2 only for $\mathbb{Q}^c/\mathbb{Q}$.) □

For Question 1.2, the remaining case is when $S_1 = \emptyset$. For this case, we can obtain a result which is similar to Theorem 3.6. (The proof is more complicated because we consider the initial layer of k^a/k. See also [13, Remark 4.7].)

Theorem 4.7. *Suppose that k and p satisfy (C4.1). Assume that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$. Let k^a/k be the anti-cyclotomic $\mathbb{Z}_p$-extension. Assume that k^a/k is totally ramified at the unique prime lying above p. Then there exist infinitely many rational primes q satisfying all of the following conditions.*

1. *$q \equiv -1 \pmod{p}$, and q is inert in k,*
2. *$X_{\{\mathfrak{q}\}}(\widetilde{k})$ contains a non-trivial pseudo-null submodule, where $\mathfrak{q}$ is the unique prime of k lying above q.*

Proof. We use some notations given in the proof of Theorem 3.6. For a non-negative integer n, let k_n^a be the nth layer of k^a/k. Suppose that $k \neq \mathbb{Q}(\sqrt{-p})$ or $p \equiv 1 \pmod{4}$. It follows that k_1^a and $\mathbb{Q}(\zeta_p)$ are linearly disjoint. It is known that $\mathrm{Gal}(k_1^a/\mathbb{Q})$ is a dihedral group of order $2p$. Then we choose $\sigma \in \mathrm{Gal}(k_1^a(\zeta_p)/\mathbb{Q})$ so that $\sigma|_{k_1^a}$ has order 2, and that $\sigma|_{\mathbb{Q}(\zeta_p)}$ is the complex conjugation. Suppose that $k = \mathbb{Q}(\sqrt{-p})$ and $p \equiv 3 \pmod{4}$. It follows that $k_1^a \cap \mathbb{Q}(\zeta_p) = k$. Then we choose $\sigma \in \mathrm{Gal}(k_1^a(\zeta_p)/\mathbb{Q})$ so that σ has order 2, and that $\sigma|_{\mathbb{Q}(\zeta_p)}$ is the complex conjugation. It follows that $\sigma|_{k_1^a}$ also has order 2.

Let E_n be the group of units of k_n^a, and $E_1/E_1^p = (E_1/E_1^p)^+ \oplus (E_1/E_1^p)^-$ the decomposition of E_1/E_1^p with respect to the action of σ. Since k_1^a is not a CM-field, we see that $(E_1/E_1^p)^-$ is not trivial. Pick a unit $\varepsilon \in E_1 \backslash E_1^p$ such that $\varepsilon^\sigma \bmod E_1^p = \varepsilon^{-1} \bmod E_1^p$. Similar to the proof of Theorem 3.6, we have an isomorphism

$$\mathrm{Gal}(k_1^a(\zeta_p, \sqrt[p]{\varepsilon})/k_1^a(\zeta)) \cong \mathrm{Hom}(\langle \varepsilon \bmod E_1^p \rangle, \langle \zeta_p \rangle)$$

as $\langle \sigma \rangle$-modules. Let F be the fixed field of $\langle \sigma \rangle$. By the choice of σ, we see that $k_1^a(\zeta_p, \sqrt[p]{\varepsilon})/F$ is abelian, and hence is a cyclic extension of degree $2p$.

Let $\widetilde{\sigma}$ be a generator of $\mathrm{Gal}(k_1^a(\zeta_p, \sqrt[p]{\varepsilon})/F)$. By the Čebotarev density theorem, there exist infinitely many prime ideals $\mathfrak{Q}$ of $k_1^a(\zeta_p, \sqrt[p]{\varepsilon})$ such that

$$\widetilde{\sigma} = \left[\frac{k_1^a(\zeta_p, \sqrt[p]{\varepsilon})/F}{\mathfrak{Q}}\right].$$

Let q be the prime number lying below $\mathfrak{Q}$. We also may assume that q splits completely in F. By the choice of σ, it follows that q is inert in k and that $q \equiv -1 \pmod{p}$. Let $\mathfrak{Q}_0$ be the prime of k_1^a lying below $\mathfrak{Q}$. It follows that $\varepsilon \bmod \mathfrak{Q}_0 \notin ((O_{k_1^a}/\mathfrak{Q}_0)^\times)^p$. Let $\mathfrak{q}$ be the prime ideal of k generated by q. To see the assertion, we claim that $X_{\{\mathfrak{q}\}}(\widetilde{k})$ contains a non-trivial pseudo-null submodule.

First, we assume that the unramified Iwasawa module $X_\emptyset(k^a)$ contains a non-trivial finite submodule. Then, similar to Proposition 4.2, we can show that $D_\emptyset(k_n^a)$ (the decomposition subgroup of $X_\emptyset(k_n^a)$ for the unique prime lying above p) is not trivial for some n. (Note that this fact essentially comes from the arguments given in the proofs of [8, Theorem 1] and Lemma 4.6. We briefly explain this here. Define $A_\emptyset(k)$, $A_\emptyset(k_n^a)$, $B_\emptyset(k_n^a)$, and $B'_\emptyset(k_n^a)$ similarly (for the ideal class group). Since the order of the group of units in k is prime to p, we see that $|B_\emptyset(k_n^a)| = |B'_\emptyset(k_n^a)|$. Let $i_{0,n}(A_\emptyset(k))$ be the image of the mapping induced by the extension of ideals to $A_\emptyset(k_n^a)$. Then,

$$|A_\emptyset(k)| = |B_\emptyset(k_n^a)| = |B'_\emptyset(k_n^a)| = |i_{0,n}(A_\emptyset(k))\, D_\emptyset(k_n^a)|.$$

We note that $A_\emptyset(k)$ is not trivial in this case (this follows from Iwasawa's result given in [14]). Moreover, we see that $|i_{0,n}(A_\emptyset(k))|$ is smaller than $|A_\emptyset(k)|$ for some n by using the argument given in the proof of Lemma 4.6.) Hence, we also obtain the fact that $D_{\{\mathfrak{q}\}}(k_n^a)$ is not trivial. Then the claim follows from Lemma 4.1. The assertion of this theorem has been shown for this case.

In the following, we assume that $X_\emptyset(k^a)$ does not contain a non-trivial finite submodule. Let I (resp. I_n) be the kernel of the restriction $X_{\{\mathfrak{q}\}}(k^a) \to X_\emptyset(k^a)$ (resp. $X_{\{\mathfrak{q}\}}(k_n^a) \to X_\emptyset(k_n^a)$). We put $\Gamma_n = \mathrm{Gal}(k^a/k_n)$. Note that in our situation, $X_\emptyset(k^a)_{\Gamma_n} \cong X_\emptyset(k_n^a)$ and $X_{\{\mathfrak{q}\}}(k^a)_{\Gamma_n} \cong X_{\{\mathfrak{q}\}}(k_n^a)$. By the assumption, we see that $X_\emptyset(k^a)^{\Gamma_n}$ is trivial because it is a finite submodule of $X_\emptyset(k^a)$.

From these facts, we obtain the following exact sequence

$$0 \to I_{\Gamma_n} \to X_{\{\mathfrak{q}\}}(k_n^a) \to X_\emptyset(k_n^a) \to 0.$$

Hence we see that $I_{\Gamma_n} \cong I_n$.

Let R_n be the Sylow p-subgroup of $(O_{k_n^a}/\mathfrak{q})^\times$. We put $R = \varprojlim R_n$, where the inverse limit is taken with respect to the norm mapping. Since q is inert in k, $\mathfrak{q}$ splits completely in k^a/k. We put $\Lambda_a = \mathbb{Z}_p[\![\Gamma_0]\!]$. Then, as a Λ_a-module, R is isomorphic to $\mathcal{R} = \Lambda_a/(p^c)$, where $c = \nu_p(q^2-1) \geq 1$. By class field theory, there is a surjective Λ_a-module homomorphism $R \to I$, and let J be its kernel. Under the isomorphism $R \cong \mathcal{R}$, J corresponds to a submodule $\mathcal{J}$ of $\mathcal{R}$.

We claim that $\mathcal{J}$ is not contained in $p\mathcal{R}$. By taking the Γ_1-coinvariant of the following exact sequence

$$0 \to J \to R \to I \to 0$$

and using the fact that $I_{\Gamma_1} \cong I_1$, we obtain the exact sequence

$$J_{\Gamma_1} \to R_1 \to I_1 \to 0.$$

Assume that $\mathcal{J}$ is contained in $p\mathcal{R}$. Then we can see that the image of J_{Γ_1} is contained in R_1^p. This implies that

$$I_1 \otimes \mathbb{F}_p \cong R_1 \otimes \mathbb{F}_p \cong \mathbb{F}_p^{\oplus p},$$

as $\mathbb{F}_p$-vector spaces. On the other hand, since ε (which is taken in the second paragraph of this proof) is not a pth power in R_1, the $\mathbb{F}_p$-dimension of $I_1 \otimes \mathbb{F}_p$ is at most $p-1$. It is a contradiction. The claim follows.

The above claim implies that $\mathcal{R}/\mathcal{J}$ is finite. Hence we see that I is finite. Note that I is not trivial because $I_0 \cong \mathrm{Gal}(L_{\{\mathfrak{q}\}}(k)/L_{\emptyset}(k))$ is not trivial. Hence $X_{\{\mathfrak{q}\}}(k^a)$ contains a non-trivial finite submodule. By Proposition 4.2, we can show that $D_{\{\mathfrak{q}\}}(k_n^a)$ is not trivial for some n. Consequently, by using Lemma 4.1, we see that $X_{\{\mathfrak{q}\}}(\widetilde{k})$ contains a non-trivial pseudo-null submodule. The theorem completely follows. □

Remark 4.8. Let k be an imaginary quadratic field, and assume that p does not split in k. One can show that if $X_{\emptyset}(\widetilde{k})$ is non-trivial and pseudo-null, then $X_S(\widetilde{k})$ contains a non-trivial pseudo-null submodule for every finite set S of finite places of k. We shall give an outline of the proof. Under the assumption, by using [24, Theorem 2 (ii)], we see that there is a $\mathbb{Z}_p$-extension K/k such that $X_{\emptyset}(K)$ is finite and the unique prime of k lying above p is totally ramified. If $X_{\emptyset}(K)$ is trivial (this implies the triviality of $X_{\emptyset}(k)$), then $X_{\emptyset}(\widetilde{k})$ is also trivial (this can be shown by using Iwasawa's result given in [14]), and hence this contradicts our assumption. Thus, $X_{\emptyset}(K)$ is not trivial. Let K_n be the nth layer of K/k. In this situation, it can be shown that $D_{\emptyset}(K_n)$ is non-trivial for some n. (See the third paragraph of the proof of Theorem 4.7. Note that we may assume that $k \neq \mathbb{Q}(\sqrt{-3})$ when $p = 3$.) Since $L_{\emptyset}(K_n)$ is an intermediate field of $L_S(K_n)/K_n$, we see that $D_S(K_n)$ is also non-trivial. Then the assertion follows from Lemma 4.1 (2).

Remark 4.9. We mention about the computational results given in [13, Section 5]. (Some of those results are related to Question 1.2 via Lemma 4.1.) After that paper was published, a problem was found in the computer programs. However, the values stated in the tables of [13, Section 5] seem correct (it has not been completely confirmed yet). The details will be reported elsewhere.

5. Application to the structure of the Galois group of the maximal pro-p extension unramified outside S

There is an application of GGC to "non-abelian Iwasawa theory". M. Ozaki obtained the following result: if p splits in an imaginary quadratic field k and GGC holds for k and p, then the Galois group of the maximal unramified pro-p extension over k^c cannot be a non-abelian free pro-p group. (This is mentioned in [25, p. 34] without proof. After that, the first author [3] gave a more general result including Ozaki's one.) In this section, we shall consider its S-ramified analog.

Firstly, let S be a finite set of finite primes of $\mathbb{Q}$, and assume that S does not contain p. Let $\mathcal{L}_S(\mathbb{Q}^c)$ be the maximal pro-p extension over $\mathbb{Q}^c$ unramified outside S. We put $\mathcal{X}_S(\mathbb{Q}^c) = \mathrm{Gal}(\mathcal{L}_S(\mathbb{Q}^c)/\mathbb{Q}^c)$. Then $X_S(\mathbb{Q}^c)$ is the maximal pro-p abelian quotient of $\mathcal{X}_S(\mathbb{Q}^c)$. Note also that $\mathcal{X}_S(\mathbb{Q}^c)$ is a finitely generated pro-p group because $X_S(\mathbb{Q}^c)$ is finitely generated as a $\mathbb{Z}_p$-module. From Theorem 1.1, we can see the following:

Corollary 5.1. *Assume that S satisfies the condition* (C1.1)*. Then $\mathcal{X}_S(\mathbb{Q}^c)$ is not a free pro-p group.*

Next, let k be an imaginary quadratic field. (We do not add any assumption on the splitting of p.) Let S be a finite set of finite primes of k, and assume that S does not contain any prime lying above p. We define $\mathcal{X}_S(k^c)$ similar to the above. It also can be shown that $\mathcal{X}_S(k^c)$ is a finitely generated pro-p group.

Corollary 5.2. *Assume that S satisfies both* (C1.2) *and* (C1.3)*. (Note that the condition* (C1.3) *is unrelated to the splitting of p.) If $S_1 \neq \emptyset$, then $\mathcal{X}_S(k^c)$ is not a free pro-p group.*

Proof. Under the assumptions, $\mathrm{Gal}(k^c/\mathbb{Q}^c)$ acts on $X_S(k^c)$, and we decompose

$$X_S(k^c) \cong X_S(k^c)^+ \oplus X_S(k^c)^-$$

with respect to its action. We can see that $X_S(k^c)^+ \cong X_{S_1^\dagger}(\mathbb{Q}^c)$, where $S_1^\dagger$ is the set of rational primes lying below S_1. Note that $S_1^\dagger$ satisfies (C1.1). Assume that $S_1 \neq \emptyset$. Then $S_1^\dagger$ is also not empty, and we see that $X_{S_1^\dagger}(\mathbb{Q}^c)$ contains a non-trivial finite Λ_1-submodule by Theorem 1.1. Hence $X_S(k^c)$ also contains a non-trivial element of finite order. Then the assertion follows. □

When p splits in k, we can obtain one more result. The following is an S-ramified version of a result given in [3].

Proposition 5.3. *Assume that p splits in k, and S satisfies* (C1.2). *If $X_S(\widetilde{k})$ contains a non-trivial pseudo-null Λ_2-submodule, then $\mathcal{X}_S(k^c)$ is not a free pro-p group.*

Proof. This can be shown by using the arguments given in the proof of [3, Proposition 2.1]. Hence we omit to state the details. □

6. Appendix: On the structure of $\mathfrak{X}_{S,\mathfrak{p}}(k^c)$

Let the notations be as in Section 3. We will consider the assertion (a) in the proof of Theorem 1.3. We give a result on the structure of $\mathfrak{X}_{S,\mathfrak{p}}(k^c)$ for general S.

Proposition 6.1. *Assume that k and p satisfy* (C3.1), *and S satisfies* (C1.2). *Let s_∞ be the number of primes in k^c lying above S (it is finite), and λ the $\mathbb{Z}_p$-rank of $X_\emptyset(k^c)$ (that is, λ is the Iwasawa λ-invariant of k^c/k). Then, as a $\mathbb{Z}_p$-module, $\mathfrak{X}_{S,\mathfrak{p}}(k^c) \cong \mathbb{Z}_p^{\oplus s_\infty+\lambda}$.*

Proof. Our proof uses the idea written in some earlier literatures (see, e.g., [6, 12]), and is inspired by the idea given in [27]. When $S = \emptyset$, the assertion is already shown ([4, Lemma 2]). Hence we may assume that S is not empty, and we write $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$. For an integer $n \geq 0$, we denote by k_n^c the nth layer of k^c/k. We shall define some notations as follows.

- $R_n(\mathfrak{q}_i)$: the Sylow p-subgroup of $(\mathcal{O}_{k_n^c}/\mathfrak{q}_i)^\times$ for $i = 1, \ldots, m$,
- $R_n = \oplus_{i=1}^m R_n(\mathfrak{q}_i)$,
- $\mathfrak{p}_n$: the prime of k_n^c lying above $\mathfrak{p}$,
- $k_{n,\mathfrak{p}}^c$: the completion of k_n^c at $\mathfrak{p}_n$,
- $\mathcal{U}_n^1$: the group of principal units of $k_{n,\mathfrak{p}}^c$,
- $E_n^1 = \{\varepsilon \,|\, \varepsilon \text{ is a global unit of } k_n^c \text{ satisfying } \varepsilon \equiv 1 \pmod{\mathfrak{p}_n}\}$,
- $E_n^1(S) = \{\varepsilon \in E_n^1 \,|\, \text{the order of } \varepsilon \text{ in } \bigoplus_{i=1}^m (\mathcal{O}_{k_n^c}/\mathfrak{q}_i)^\times \text{ is a power of } p\}$,
- $\mathcal{E}_n$: the closure of the image of $E_n^1 \to \mathcal{U}_n^1$,
- $\mathcal{E}_n(S)$: the closure of the diagonal image of $E_n^1(S) \to \mathcal{U}_n^1 \oplus R_n$.

By using class field theory (see, e.g., [6, III, §1]), we see that the kernel of the restriction

$$\mathfrak{X}_{S,\mathfrak{p}}(k_n^c) \to \mathfrak{X}_{\emptyset,\mathfrak{p}}(k_n^c)$$

is isomorphic to the kernel of

$$f : (\mathcal{U}_n^1 \oplus R_n)/\mathcal{E}_n(S) \to \mathcal{U}_n^1/\mathcal{E}_n, \quad (u, \boldsymbol{x})\mathcal{E}_n(S) \mapsto u\mathcal{E}_n.$$

(Note that f is surjective.) We mention the fact that $E_n^1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{E}_n$. (That is, a variation of Leopoldt conjecture holds. See, e.g., [9, p. 94].) We also note that the index $(E_n^1 : E_n^1(S))$ is finite and prime to p. From these facts, we can see that the homomorphism

$$g : R_n \to (\mathcal{U}_n^1 \oplus R_n)/\mathcal{E}_n(S), \quad \boldsymbol{x} \mapsto (1, \boldsymbol{x})\mathcal{E}_n(S)$$

is injective, and the image of g coincides with the kernel of f. Then, we obtain the following exact sequence

$$0 \to R_n \to \mathfrak{X}_{S,\mathfrak{p}}(k_n^c) \to \mathfrak{X}_{\emptyset,\mathfrak{p}}(k_n^c) \to 0.$$

Since each term of the above is profinite, taking the inverse limits (with respect to the norm for the left term, with respect to the restriction for the remaining terms), we obtain the following exact sequence

$$0 \to \varprojlim R_n \to \mathfrak{X}_{S,\mathfrak{p}}(k^c) \to \mathfrak{X}_{\emptyset,\mathfrak{p}}(k^c) \to 0. \tag{6.1}$$

We see that $\varprojlim R_n \cong \mathbb{Z}_p^{s_\infty}$ as a $\mathbb{Z}_p$-module. As noted in the first paragraph of this proof, we see that $\mathfrak{X}_{\emptyset,\mathfrak{p}}(k^c) = X_\emptyset(k^c)$, and hence it is isomorphic to $\mathbb{Z}_p^\lambda$ as a $\mathbb{Z}_p$-module (see, e.g. [28]). Thus, the exact sequence (6.1) splits (as $\mathbb{Z}_p$-modules), and we obtain the assertion. □

We shall give a counterexample of the assertion (a) in the proof of Theorem 1.3 when $S_1 \neq \emptyset$. Assume that S satisfies both conditions (C1.2), and (C1.3). Assume also that $S_1 \neq \emptyset$. By Proposition 6.1, we see that the $\mathbb{Z}_p$-rank of $\mathfrak{X}_{S,\mathfrak{p}}(k^c)$ is $s_\infty + \lambda$. We can compute the $\mathbb{Z}_p$-rank of $X_S(k^c)$ by using [12, Theorem 1.4]. (Since S satisfies (C1.3), we can apply this theorem). In fact, by using the value $P'_{\max}$ which is defined in [12], the $\mathbb{Z}_p$-rank of $X_S(k^c)$ is expressed as

$$\lambda + s_\infty - P'_{\max}.$$

(Recall that s_∞ is the number of primes in k^c lying above S. See also [12, p. 1496].) We can see that if $S_1 \neq \emptyset$, then $P'_{\max} > 0$. This implies that the $\mathbb{Z}_p$-rank of $X_S(k^c)$ is exactly smaller than $s_\infty + \lambda$. Hence, under these conditions, we see that $M_{S,\mathfrak{p}}(k^c) \neq L_S(k^c)$.

Remark 6.2. Assume that k, p, and S satisfy the assumption of Proposition 6.1, and $S_1 = \emptyset$. Then, by using Proposition 6.1 and the fact that $M_{S,\mathfrak{p}}(k^c) = L_S(k^c)$, we see that $X_S(k^c)$ has no non-trivial finite $\mathbb{Z}_p[\![\mathrm{Gal}(k^c/k)]\!]$-submodule (this also can be shown by using the argument given in [12]). Hence, an analog of Theorem 1.1 for the cyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field does not hold in general.

7. Additional remarks

Let k be an imaginary quadratic field. T. Kataoka obtained a result [16] which is closely related to our result. That is, he determined the characteristic ideal of $X_S(\widetilde{k})$ as a $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{k}/k)]\!]$-module under some conditions. From this result, we can find an example of $X_S(\widetilde{k})$ which is not pseudo-null.

Recall that our second proof of Theorem 1.1 uses the characteristic ideal. It seems that one can obtain another type criterion for the existence of a non-trivial pseudo-null submodule of $X_S(\widetilde{k})$ (under certain situations) from Kataoka's result.

Note added in proof. Concerning Remark 4.9, the values of the tables in [13] had been confirmed to be correct.

References

[1] L. J. Federer, “Noetherian $\mathbf{Z}_p[[T]]$-modules, adjoints, and Iwasawa theory”, *Ill. J. Math.* **30** (1986), no. 4, p. 636-652.

[2] S. Fujii, “Pseudo-null submodules of the unramified Iwasawa module for $\mathbb{Z}_p^2$-extensions”, *Interdiscip. Inf. Sci.* **16** (2010), no. 1, p. 55-66.

[3] ———, “On the depth of the relations of the maximal unramified pro-p Galois group over the cyclotomic $\mathbb{Z}_p$-extension”, *Acta Arith.* **149** (2011), no. 2, p. 101-110.

[4] ———, “On restricted ramifications and pseudo-null submodules of Iwasawa modules for $\mathbb{Z}_p^2$-extensions”, *J. Ramanujan Math. Soc.* **29** (2014), no. 3, p. 295-305.

[5] T. Fukuda & K. Komatsu, “Noncyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields”, *Exp. Math.* **11** (2002), no. 4, p. 469-475.

[6] G. Gras, *Class field theory, From theory to practice*, Springer Monographs in Mathematics, Springer, 2003, xiii+491 pages.

[7] R. Greenberg, “The Iwasawa invariants of Γ-extensions of a fixed number field”, *Am. J. Math.* **95** (1973), no. 1, p. 204-214.

[8] ———, “On the Iwasawa invariants of totally real number fields”, *Am. J. Math.* **98** (1976), no. 1, p. 263-284.

[9] ———, “On the structure of certain Galois groups”, *Invent. Math.* **47** (1978), no. 1, p. 85-99.

[10] ———, “Iwasawa theory – past and present”, in *Class field theory – its centenary and prospect*, Advanced Studies in Pure Mathematics, vol. 30, Mathematical Society of Japan, 2001, p. 335-385.

[11] ———, “On the structure of certain Galois cohomology groups”, *Doc. Math.* (2006), p. 335-391.

[12] T. Itoh, Y. Mizusawa & M. Ozaki, “On the $\mathbb{Z}_p$-ranks of tamely ramified Iwasawa modules”, *Int. J. Number Theory* **9** (2013), no. 6, p. 1491-1503.

[13] T. Itoh & Y. Takakura, “On tamely ramified Iwasawa modules for $\mathbb{Z}_p$-extensions of imaginary quadratic fields”, *Tokyo J. Math.* **37** (2014), no. 2, p. 405-431.

[14] K. Iwasawa, “A note on class numbers of algebraic number fields”, *Abh. Math. Semin. Univ. Hamb.* **20** (1956), no. 3-4, p. 257-258.

[15] J.-F. Jaulent, C. Maire & G. Perbet, “Sur les formules asymptotiques le long des $\mathbb{Z}_\ell$-extensions”, *Ann. Math. Qué* **37** (2013), no. 1, p. 63-78.

[16] T. Kataoka, “On pseudo-isomorphism classes of tamely ramified Iwasawa modules over imaginary quadratic fields”, *Acta Arith.* **180** (2017), no. 2, p. 171-182.

[17] J. Minardi, “Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields”, PhD Thesis, University of Washington (USA), 1986.

[18] Y. Mizusawa, “Tame pro-2 Galois groups and the basic $\mathbb{Z}_2$-extension”, *Trans. Am. Math. Soc.* **370** (2018), no. 4, p. 2423-2461.

[19] Y. Mizusawa & M. Ozaki, “On tame pro-p Galois groups over basic $\mathbb{Z}_p$-extensions”, *Math. Z.* **273** (2013), no. 3-4, p. 1161-1173.

[20] J. Nekovář, *Selmer complexes*, Astérisque, vol. 310, Société Mathématique de France, 2006, viii+559 pages.

[21] T. Nguyen Quang Do, “Formations de classes et modules d’Iwasawa”, in *Number theory (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics, vol. 1068, Springer, 1983, p. 167-185.

[22] M. Ozaki, “A note on the capitulation in $\boldsymbol{Z}_p$-extensions”, *Proc. Japan Acad., Ser. A* **71** (1995), no. 9, p. 218-219.

[23] ———, “The class group of $\boldsymbol{Z}_p$-extensions over totally real number fields”, *Tôhoku Math. J.* **49** (1997), no. 3, p. 431-435.

[24] ———, “Iwasawa invariants of $\mathbb{Z}_p$-extensions over an imaginary quadratic field”, in *Class field theory – its centenary and prospect*, Advanced Studies in Pure Mathematics, vol. 30, Mathematical Society of Japan, 2001, p. 387-399.

[25] ———, "Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions", in *Young Philosophers in Number Theory*, vol. 1256, Sūrikaisekikenkyūsho Kōkyūroku, 2002, p. 25-37.

[26] ———, "Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions", *J. Reine Angew. Math.* **602** (2007), p. 59-94.

[27] B. Perrin-Riou, "Arithmétique des courbes elliptiques et théorie d'Iwasawa", *Mém. Soc. Math. Fr., Nouv. Sér.* **17** (1984), p. 1-130.

[28] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer, 1997, xiv+487 pages.

[29] K. Wingberg, "Free pro-p extensions of number fields", preprint.

Satoshi Fujii
Faculty of Education,
Shimane University,
1060 Nishikawatsucho, Matsue, Shimane, 690-8504, Japan
E-mail: fujiisatoshi@edu.shimane-u.ac.jp

Tsuyoshi Itoh
Division of Mathematics, Education Center,
Faculty of Social Systems Science,
Chiba Institute of Technology,
2-1-1 Shibazono, Narashino, Chiba, 275-0023, Japan
E-mail: tsuyoshi.itoh@it-chiba.ac.jp