Tsuyoshi ITOH

Tamely ramified Iwasawa modules having no non-trivial pseudo-null submodules


<http://jtnb.cedram.org/item?id=JTNB_2018__30_3_859_0>
Tamely ramified Iwasawa modules having no non-trivial pseudo-null submodules

par Tsuyoshi ITOH

Résumé. Ce travail fait suite à l’article [4] de Satoshi Fujii et l’auteur. Soient \( k \) un corps de nombres, \( p \) un nombre premier, et \( k^c/k \) la \( \mathbb{Z}_p \)-extension cyclotomique. Pour un ensemble fini \( S \) de nombres premiers qui ne contient pas \( p \), le module d’Iwasawa (par rapport à la pro-\( p \) extension abélienne maximale non ramifiée en dehors de \( S \)) a été étudié dans plusieurs articles. Nous donnons des exemples non-triviaux où \( X_S(k^c) \) a un sous-module fini non-nul avec \( k \) totalement réel. Nous donnons également un exemple similaire dans le cas de la \( \mathbb{Z}_p^{\oplus 2} \)-extension d’un corps quadratique imaginaire. De plus, nous discutons en appendice des analogues faibles de la conjecture de Greenberg pour \( X_S(k^c) \).

Abstract. The present paper is a sequel to the previous paper [4] (by Satoshi Fujii and the author). Let \( k \) be an algebraic number field, \( p \) a prime number, and \( k^c/k \) the cyclotomic \( \mathbb{Z}_p \)-extension. For a finite set \( S \) of prime numbers which does not contain \( p \), the Iwasawa module \( X_S(k^c) \) (with respect to the maximal pro-\( p \) abelian extension unramified outside \( S \)) has been studied in several papers. We will give some non-trivial examples such that \( X_S(k^c) \) has no non-trivial finite submodules even when \( k \) is totally real. We also give a similar example for the case of the \( \mathbb{Z}_p^{\oplus 2} \)-extension of an imaginary quadratic field. Moreover, weak analogs of Greenberg’s conjecture for \( X_S(k^c) \) are also discussed in the appendix.

1. Introduction and results

Let \( p \) be a prime number, \( S \) a finite set of prime numbers which does not contain \( p \). For an algebraic extension \( \mathcal{K}/\mathbb{Q} \), let \( L_S(\mathcal{K})/\mathcal{K} \) be the maximal abelian (pro-)\( p \)-extension unramified outside \( S \). We put \( X_S(\mathcal{K}) = \text{Gal}(L_S(\mathcal{K})/\mathcal{K}) \). When \( \mathcal{K} \) is an algebraic number field (i.e., \( \mathcal{K}/\mathbb{Q} \) is finite), \( L_S(\mathcal{K})/\mathcal{K} \) is finite because all ramified primes are tamely ramified.
Let $k$ be an algebraic number field, and $K/k$ a $\mathbb{Z}_p$-extension. We put $\Lambda_{K/k} = \mathbb{Z}_p[[\text{Gal}(K/k)]]$. Then, we can show that $X_S(K)$ is a finitely generated torsion module over $\Lambda_{K/k}$ (this is often called a tamely ramified Iwasawa module). We will consider the existence of a non-trivial pseudo-null $\Lambda_{K/k}$-submodule of $X_S(K)$. (For the definition of pseudo-nullity, see, e.g., [18]. In this case, a pseudo-null $\Lambda_{K/k}$-module is just a finite $\Lambda_{K/k}$-module.) We denote by $k^c/k$ the cyclotomic $\mathbb{Z}_p$-extension.

In [4], it was shown that if $p$ is odd and $X_S(\mathbb{Q}^c) \neq 0$, then $X_S(\mathbb{Q}^c)$ always contains a non-trivial finite submodule. On the other hand, when $p = 2$, Mizusawa’s result [16, Theorem 7.3] implies the existence of the case that $X_S(\mathbb{Q}^c) \cong \mathbb{Z}_2$ as a $\mathbb{Z}_2$-module. Hence, the case when $p = 2$ is more complicated. Our first result is a determination of the set $S$ of odd prime numbers such that $X_S(\mathbb{Q}^c)$ does not contain a non-trivial finite submodule for $p = 2$ (the proof will be given in Section 3).

**Theorem 1.1.** Assume that $p = 2$. Let $S$ be a non-empty finite set of odd prime numbers. For an odd prime number $q$, we denote by $P(q)$ the number of primes in $\mathbb{Q}^c$ lying above $q$. (Note that $q$ is finitely decomposed in $\mathbb{Q}^c$.) Then $X_S(\mathbb{Q}^c)$ does not have a non-trivial finite $\Lambda_{\mathbb{Q}^c/\mathbb{Q}}$-submodule if and only if $S = \{q_1, \ldots, q_r\}$ satisfies $q_1 \equiv \cdots \equiv q_r \equiv 3 \pmod{4}$ and $P(q_1) = \cdots = P(q_r)$ (where $q_1, \ldots, q_r$ are distinct prime numbers).

When $p$ is an odd prime number, we can also find an example of a totally real number field $k$ such that $X_S(k^c)$ does not contain a non-trivial finite submodule. Our second result is a simple criterion whether $X_S(k^c)$ has no non-trivial finite submodules for a real quadratic field $k$ and certain $p$ and $S$. We denote by $|A|$ the number of elements of a finite set $A$.

**Theorem 1.2.** Let $p$ be an odd prime number, and $k$ a real quadratic field. Assume that $p$ is inert in $k$ and $p$ does not divide the class number of $k$. Take distinct prime numbers $q_1, \ldots, q_r$ such that $q_i \equiv -1 \pmod{p}$ and $q_i$ is inert in $k$ for $i = 1, \ldots, r$. We put $S = \{q_1, \ldots, q_r\}$. We denote by $P(q_i)$ the number of primes of $\mathbb{Q}^c$ lying above $q_i$, and by $P'$ the largest number of $P(q_i)$ for $i = 1, \ldots, r$. Then $X_S(k^c)$ does not have a non-trivial finite $\Lambda_{k^c/k}$-submodule if and only if

$$|X_S(k)| = p^{r-1} \cdot \left( \prod_{i=1}^{r} P(q_i) \right) / P'.$$

(Note that $p^{r-1} \cdot \left( \prod_{i=1}^{r} P(q_i) \right) / P' \leq |X_S(k)| \leq p^r \cdot \prod_{i=1}^{r} P(q_i)$ in this case. We also see that $X_S(k^c)$ is infinite if $|S| \geq 2$.)

This theorem will be shown in Section 4. As a consequence, one can find an explicit example such that $X_S(k^c)$ does not have a non-trivial finite submodule (see Remark 4.3). We note that when $p$ splits in a real quadratic
field \( k \), the same type result does not hold (see Appendix A). We also give another (non-trivial) example of a totally real field \( k \) such that \( X_S(k^c) \) does not have a non-trivial finite submodule (Proposition 4.5).

Next, we will consider the case of the \( \mathbb{Z}_p^{\oplus 2} \)-extension of an imaginary quadratic field \( k \). Concerning this paragraph, see also [4] for the details. Let \( \bar{k}/k \) be the unique \( \mathbb{Z}_p^{\oplus 2} \)-extension. We put \( \Lambda_{\bar{k}/k} = \mathbb{Z}_p[[\text{Gal}(\bar{k}/k)]] \). Then \( X_S(\bar{k}) \) is a finitely generated torsion \( \Lambda_{\bar{k}/k} \)-submodule. In [4], some sufficient conditions such that \( X_S(\bar{k}) \) has a non-trivial pseudo-null \( \Lambda_{\bar{k}/k} \)-submodule were given. However, there is a non-trivial example such that \( X_S(\bar{k}) \) does not contain a non-trivial pseudo-null submodule. In Section 5, we will prove the following:

**Theorem 1.3.** We put \( k = \mathbb{Q}(\sqrt{-3}) \) and \( p = 3 \). Let \( \bar{k}/k \) be the unique \( \mathbb{Z}_3^{\oplus 2} \)-extension. Take a set \( S = \{q_1, q_2\} \) of distinct prime numbers which satisfy \( q_i \equiv 2 \pmod{3} \) and \( q_i \) is not decomposed in \( \mathbb{Q}^c \) for \( i = 1, 2 \). Then \( X_S(\bar{k}) \) is not pseudo-null, and it does not contain a non-trivial pseudo-null submodule.

In Appendix A, we consider analogs of weak forms of Greenberg’s conjecture in the sense of Nguyen Quang Do.

2. Preliminaries

We shall define some notations. Let \( |\cdot|_p \) be the multiplicative \( p \)-adic absolute value normalized as \( |p|_p = p^{-1} \). In the following of this section, \( k \) denotes an arbitrary algebraic number field. We denote by \( \mathcal{O}_k \) the ring of integers of \( k \), and by \( E(k) \) the group of units of \( k \). For a non-zero integral ideal \( m \) of \( k \), we put \( R(k,m) = (\mathcal{O}_k/m)^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p \). We consider every algebraic extension field over \( \mathbb{Q} \) as a subfield of \( \mathbb{C} \), and put \( \zeta_n = e^{2\pi i/n} \) for a positive integer \( n \).

Let \( K/k \) be a \( \mathbb{Z}_p \)-extension. Put \( \Gamma = \text{Gal}(K/k) \), and \( \Lambda_{K/k} = \mathbb{Z}_p[\Gamma] \). We also note that \( \Lambda_{K/k} \) is isomorphic to the power series ring \( \mathbb{Z}_p[T] \) (and we fix an isomorphism). Let \( S \) be a finite set of prime numbers not containing \( p \). In this case, there is a pseudo-isomorphism

\[
X_S(K) \rightarrow \bigoplus_{i=1}^m \mathbb{Z}_p[T]/p^{c_i} \mathbb{Z}_p[T] \oplus \bigoplus_{j=1}^n \mathbb{Z}_p[T]/g_j^{d_j} \mathbb{Z}_p[T],
\]

where \( c_i, d_j \) are positive integers and \( g_j \) is an irreducible distinguished polynomial for each \( i, j \) (see, e.g., [18], [26]). We put

\[
\mu_{K/k,S} = \sum_{i=1}^m c_i \quad \text{and} \quad F_{K/k,S}(T) = \prod_{j=1}^n g_j^{d_j}.
\]
$F_{K/k,S}(T)$ is called the characteristic polynomial of $X_S(K)$ (in the sense of [18, (5.3.9) Definition]). Note that $\mu_{K/k,S} = 0$ if and only if $X_S(K)$ is finitely generated as a $\mathbb{Z}_p$-module. In particular, if $k/\mathbb{Q}$ is an abelian extension and $K = k^c$ (the cyclotomic $\mathbb{Z}_p$-extension), then $\mu_{k^c/k,S} = 0$ (see, e.g., [10, p. 1494]). Note also that $X_S(K)$ is finitely generated as a $\mathbb{Z}_p$-module if and only if $X_S(K)\Gamma$ is finitely generated as a $\mathbb{Z}_p$-module. In particular, if $k/\mathbb{Q}$ is an abelian extension and $K = k^c$ (the cyclotomic $\mathbb{Z}_p$-extension), then $\mu_{k^c/k,S} = 0$ (see, e.g., [10, p. 1494]). Note also that if $X_S(K)$ is finite, then $\mu_{K/k,S} = 0$ and $F_{K/k,S}(T) = 1$. Moreover, we denote by $X_S(K)\Gamma$ the $\Gamma$-invariant submodule of $X_S(K)$, and by $X_S(K)/\Gamma$ the $\Gamma$-coinvariant quotient of $X_S(K)$ (similar notations will be used in Section 5 under a slightly different setting).

The following is our main criterion. (This type result seems well known, however, we will give a brief proof.)

**Proposition 2.1.** Assume that there is only one prime $p$ of $k$ lying above $p$, and $p$ is totally ramified in $K/k$. Then $X_S(K)$ does not have a non-trivial finite $\Lambda_{K/k}$-submodule if and only if

$$\left|X_S(k)\right| \cdot \left|F_{K/k,S}(0)\right|_p = p^{\mu_{K/k,S}}.$$

**Proof.** By our assumptions, we can show that $X_S(K)\Gamma \cong X_S(k)$ (see also, e.g., [13, Proposition 2.2.2] for a more general result), and hence $X_S(K)\Gamma$ is finite. This implies that $X_S(K)\Gamma$ is also finite, and $F_{K/k,S}(0) \neq 0$ (see, e.g., [18, p. 300, Exercise 3]). We can show that $X_S(K)$ does not have a non-trivial finite $\Lambda_{K/k}$-submodule if and only if $X_S(K)\Gamma$ is trivial (see, e.g., [18, (5.3.19) Proposition] or the argument given in the proof of [22, Proposition 2]). It is known that

$$\left|X_S(K)\Gamma\right| \cdot \left|F_{K/k,S}(0)\right|_p = \left|X_S(K)\Gamma\right| \cdot p^{\mu_{K/k,S}}$$

(see, e.g., [18, p. 300, Exercise 3]). The assertion follows from this. \qed

As a corollary, we can obtain the following simpler criterion. (This type result also seems well known. See, e.g., the proof of [23, Theorem 2].)

**Corollary 2.2.** Let the assumptions be as in Proposition 2.1. If $\left|X_S(k)\right| = p$ and $X_S(K)$ is infinite, then $X_S(K)$ does not have a non-trivial finite $\Lambda_{K/k}$-submodule.

We will prove Theorems 1.1 and 1.2 by using Proposition 2.1 directly. (Note that a similar idea is already used in [4] to show the existence of a non-trivial finite submodule of $X_S(\mathbb{Q}^c)$ when $p$ is odd.)

### 3. Proof of Theorem 1.1

In this section, we will only treat the case of $\mathbb{Q}^c/\mathbb{Q}$ when $p = 2$. Let $S$ be a non-empty finite set of odd prime numbers. In this section, we write $F(T) = F_{\mathbb{Q}^c/\mathbb{Q},S}(T)$ for simplicity (note that $\mu_{\mathbb{Q}^c/\mathbb{Q},S} = 0$). We can compute $F(T)$ from the results given in [10]. To state this, we need some preparations.
We define a topological generator of $\text{Gal}(\mathbb{Q}^c/\mathbb{Q})$ similar to [10]. That is, let $\gamma$ be the topological generator of $\text{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}(\zeta_4))$ satisfying $\zeta_2^2 = \zeta_2^3$, and let $\gamma_1$ be the restriction of $\gamma$ to $\mathbb{Q}^c$. Then $\gamma_1$ is a topological generator of $\text{Gal}(\mathbb{Q}^c/\mathbb{Q})$. We fix an isomorphism $\Lambda_{\mathbb{Q}^c/\mathbb{Q}} \to \mathbb{Z}_2[T]$ satisfying $\gamma_1 \mapsto 1 + T$.

We define the subsets $S^o$ and $S^•$ of $S$ by

$$S^o = \{ q \in S \mid q \equiv 1 \pmod{4} \}, \quad S^• = \{ q \in S \mid q \equiv 3 \pmod{4} \}.$$ 

For $q \in S$, we put $P(q)$ the number of primes of $\mathbb{Q}^c$ lying above $q$. Let $P^o$ be the largest number of $P(q)$ for $q \in S^o$ (if $S^o$ is empty, we put $P^o = 0$). Moreover, let $P^•$ be the set of (distinct) numbers $P(q)$ for $q \in S^•$, and put $P^{••} = \{ P \in P^• \mid P \geq P^o \}$ (if $S^•$ is empty, then both $P^•$ and $P^{••}$ are also empty). We define the following polynomials

$$F^o(T) = \begin{cases} \left( \prod_{q \in S^o} ((1 + T)^{P(q)} - 5^{P(q)}) \right) / \left( (1 + T)^{P^o} - 5^{P^o} \right) & \text{if } S^o \neq \emptyset, \\ 1 & \text{if } S^o = \emptyset, \end{cases}$$

$$F^•(T) = \begin{cases} \left( \prod_{q \in S^•} ((1 + T)^{P(q)} + 5^{P(q)}) \right) / \left( \prod_{P \in P^{••}} ((1 + T)^P + 5^P) \right) & \text{if } S^• \neq \emptyset, \\ 1 & \text{if } S^• = \emptyset. \end{cases}$$

Then, from the arguments and results given in [10] (especially, see the proof of Lemma 2.3 of [10]), we see that

$$F(T) = F^o(T) \cdot F^•(T).$$

By using this formula, the value $|F(0)|_2$ can be obtained. (Note that $|1 - 5^{2^a}|_2 = 2^{-(a+2)}$ and $|1 + 5^{2^a}|_2 = 2^{-1}$.) We can also compute $|X_S(\mathbb{Q})|$ from the following exact sequence

$$0 \to E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \bigoplus_{q \in S} R(\mathbb{Q}, q\mathbb{Z}) \to X_S(\mathbb{Q}) \to 0$$

and the fact that $E(\mathbb{Q}) = \{ \pm 1 \}$.

At first, we assume that $S^o = \emptyset$. In this case, we see that

$$F(T) = \left( \prod_{q \in S^•} ((1 + T)^{P(q)} + 5^{P(q)}) \right) / \left( \prod_{P \in P^•} ((1 + T)^P + 5^P) \right).$$

From this,

$$|F(0)|_2 = 2^{|P^•| - |S|}.$$ 

We also see that $|X_S(\mathbb{Q})| = 2^{|S| - 1}$, and hence

$$|X_S(\mathbb{Q})| \cdot |F(0)|_2 = 2^{|P^•| - 1}.$$
This implies that $|X_S(\mathbb{Q})| \cdot |F(0)|_2 = 1$ if and only if $|\mathcal{P}^*| = 1$. When $S = \{q_1, \ldots, q_r\}$, $|\mathcal{P}^*| = 1$ if and only if $P(q_1) = \cdots = P(q_r)$. Hence, by using Proposition 2.1, the assertion of Theorem 1.1 has been shown for this case.

We shall show the remaining case. It is sufficient to show that $X_S(\mathbb{Q}^c)$ has a non-trivial finite submodule when $S^o \neq \emptyset$. In this case, we see that

$$|F^o(0)|_2 = 2^2 \cdot P^o \prod_{q \in S^o} (2^{-2}P(q)^{-1}), \quad |F^*(0)|_2 = 2^{|\mathcal{P}^*| - |S^o|}.$$

On the other hand, we can show that

$$|X_S(\mathbb{Q})| = \left(2^{|S^o|} \cdot \prod_{q \in S^o} (2^2P(q))\right)/2.$$

Hence

$$|X_S(\mathbb{Q})| \cdot |F(0)|_2 = 2^{|\mathcal{P}^*| + 1} \cdot P^o > 1.$$

By using Proposition 2.1, we see that $X_S(\mathbb{Q}^c)$ has a non-trivial finite submodule in this case. Thus we have completed the proof of Theorem 1.1. \(\square\)

4. Totally real fields

We shall show Theorem 1.2, however, we will give a simple remark before this.

**Remark 4.1.** Let $k$ be a real quadratic field, and $p$ an odd prime number. Let $S$ be a non-empty finite set of prime numbers not containing $p$. For the structure of $X_S(\mathbb{Q}^c)$, it is sufficient to consider the case that every $q \in S$ satisfies either

(a) $q \equiv 1 \pmod{p}$, or

(b) $q \equiv -1 \pmod{p}$ and $q$ is inert in $k$

(see [8]). We put

$$S_1 = \{q \in S \mid q \equiv 1 \pmod{p}\}.$$ We note that if $S_1 \neq \emptyset$, then $X_S(\mathbb{Q}^c)$ always contains a non-trivial finite $\Lambda_{k^c/k}$-submodule. Indeed, since $\text{Gal}(k^c/\mathbb{Q}^c)$ acts on $X_S(\mathbb{Q}^c)$, the plus and minus parts

$$X_S(\mathbb{Q}^c)^\pm = \{x \in X_S(\mathbb{Q}^c) \mid \sigma(x) = \pm x \text{ for the generator } \sigma \text{ of } \text{Gal}(k^c/\mathbb{Q}^c)\}$$

can be defined, and we see that $X_S(\mathbb{Q}^c) \cong X_S(\mathbb{Q}^c)^+ \oplus X_S(\mathbb{Q}^c)^-$. We can show that $X_S(\mathbb{Q}^c)^+$ is isomorphic to $X_{S_1}(\mathbb{Q}^c)$, and this is not trivial because $S_1 \neq \emptyset$ (see also [10]). Hence, the assertion follows from the fact (which is shown in [4]) that $X_{S_1}(\mathbb{Q}^c)$ contains a non-trivial finite submodule. (The same type result for imaginary quadratic fields is given in [4].)
Proof of Theorem 1.2. Let \( k \) be a real quadratic field. Assume that \( p \) is inert in \( k \), and \( p > 2 \) does not divide the class number of \( k \). Let \( k_n^c \) be the \( n \)th layer of \( k^c/k \). Take a topological generator \( \gamma \) of \( \text{Gal}(k(\zeta_p^c)/k(\zeta_p)) \) which satisfies \( \zeta_{p^n}^c = \zeta_{p^n}^{1+p} \) for all \( n \). Let \( \gamma_1 \) be the restriction of \( \gamma \) to \( k^c \), then \( \gamma_1 \) is a topological generator of \( \text{Gal}(k^c/k) \). We fix an isomorphism from \( \Lambda_{k^c/k} \) to \( \mathbb{Z}_p[T] \) satisfying \( \gamma_1 \mapsto 1 + T \).

Let \( q_1, \ldots, q_r \) be distinct prime numbers satisfying the assumption of this theorem. For each \( i \), we see that \( R(k, q_iO_k) \) is a cyclic group of order \( p \cdot P(q_i) \). Since \( X_0(k) = 0 \), we obtain the following exact sequence

\[
E(k) \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow \bigoplus_{i=1}^r R(k, q_iO_k) \rightarrow X_S(k) \rightarrow 0.
\]

We note that \( E(k) \otimes_{\mathbb{Z}} \mathbb{Z}_p \) is a cyclic \( \mathbb{Z}_p \)-module. Hence, we have the inequalities

\[
p^{r-1} \cdot \left( \prod_{i=1}^r P(q_i) \right) / P' \leq |X_S(k)| \leq p^r \cdot \prod_{i=1}^r P(q_i).
\]

We will compute the characteristic polynomial of \( X_S(k^c) \). The following argument is essentially given in [8, Section 6], however, we shall reconstruct it for our situation. We denote by \( k_n^c \) the \( n \)th layer of \( k^c/k \). We put \( R_i = \lim_{\leftarrow n} R(k_n^c, q_iO_{k_n^c}) \) (for each \( i \)) and \( \mathcal{E} = \lim_{\leftarrow n} E(k_n^c) \otimes_{\mathbb{Z}} \mathbb{Z}_p \), where the projective limits are taken with respect to the norm mappings. By using class field theory, we obtain the following exact sequence

\[
\mathcal{E} \rightarrow \bigoplus_{i=1}^r R_i \rightarrow X_S(k^c) \rightarrow 0
\]

of \( \mathbb{Z}_p[\text{Gal}(k^c/Q)] \)-modules (note that \( X_0(k^c) = 0 \) by Iwasawa’s result [11]). For each term of the above exact sequence, we can consider its plus and minus parts with respect to the action of \( \text{Gal}(k^c/Q^c) \). We note that \( X_S(k^c)^+ \cong X_S(Q^c) = 0 \) because \( q_i \equiv -1 \pmod{p} \) for all \( i \) (see also Remark 4.1).

Hence we will consider the structure of \( X_S(k^c)^-(\cong X_S(k^c)) \) as a module over \( \Lambda_{k^c/k} \cong \mathbb{Z}_p[T] \). We can show that

\[
R_i^c \cong R_i \cong \mathbb{Z}_p[T]/((1 + T)^{P(q_i)} - (1 + p)^{P(q_i)})
\]
as \( \mathbb{Z}_p[T] \)-modules for each \( i \) (see, e.g., the argument given in the proof of [10, Lemma 2.1]). Note also that \( \mathcal{E}^c \cong \mathbb{Z}_p[T] \) as a \( \mathbb{Z}_p[T] \)-module. (For example, by using [18, (11.3.11) Theorem (iii)], we see that

\[
\mathcal{E} \cong \mathbb{Z}_p[\text{Gal}(k^c/Q)] \cong \mathbb{Z}_p[\text{Gal}(k/Q)][T],
\]

and hence the fact follows.) From [8, Theorem 1.1], we see that \( X_{\{q_i\}}(k^c) \) is finite for each \( i \). Hence, by using the same type argument given in [10],
we obtain the following exact sequence

\[ 0 \to \mathcal{E}^- / ((1 + T)^{P'} - (1 + p)^{P'}) \to \bigoplus_{i=1}^{r} R_i \to X_S(k^c) \to 0 \]

as \( \mathbb{Z}_p[T] \)-modules. From the above results, we can see that

\[ F_{k^c/k,S}(T) = \left( \prod_{i=1}^{r} ((1 + T)^{P(q_i)} - (1 + p)^{P(q_i)}) \right) / ((1 + T)^{P'} - (1 + p)^{P'}) \]

(and \( \mu_{k^c/k,S} = 0 \)). Then, we can obtain the formula

\[ |F_{k^c/k,S}(0)|_p = p^{1-r} \cdot P' / \left( \prod_{i=1}^{r} P(q_i) \right). \]

Consequently, we see that \( |X_S(k)| \cdot |F_{k^c/k,S}(0)|_p = 1 \) if and only if

\[ |X_S(k)| = p^{r-1} \cdot \left( \prod_{i=1}^{r} P(q_i) \right) / P'. \]

The assertion follows from Proposition 2.1.

As a special case of Theorem 1.2, we obtain the following:

**Corollary 4.2.** Let the assumptions be as in Theorem 1.2, and suppose also that \( P(q_i) = 1 \) for \( i = 1, \ldots, r \). Then, \( X_S(k^c) \) does not have a non-trivial finite submodule if and only if \( |X_S(k)| = p^{r-1} \).

**Remark 4.3.** Let the assumptions be as in the above corollary (that is, \( P(q_i) = 1 \) for all \( i \)). In this case, we can show that if \( |X_{\{q_i\}}(k)| = 1 \) for some \( q_i \), then \( |X_S(k)| = p^{r-1} \), and hence \( X_S(k^c) \) does not have a non-trivial finite submodule. We will give an example. In the case when \( k = \mathbb{Q}(\sqrt{2}) \) and \( p = 3 \), it can be shown that \( |X_{\{q\}}(k)| = 1 \) for \( q = 5, 11, 83 \). (The author used PARI/GP [25] (versions 2.9.1 and 2.9.3) to check these examples.) As a consequence, at least for \( k = \mathbb{Q}(\sqrt{2}) \) and \( p = 3 \), we can take a set \( S \) such that \( X_S(k^c) \cong \mathbb{Z}_3^{|c|} \) (as a \( \mathbb{Z}_3 \)-module) for any given positive integer \( c \) (e.g., \( X_{\{5,11,29\}}(k^c) \cong \mathbb{Z}_3^{|5| \cdot |11| \cdot |29|} \)).

**Remark 4.4.** Let the assumptions be as in Theorem 1.2, however, we remove the assumption that \( p \) does not divide the class number of \( k \). We also assume that \( X_{\emptyset}(k^c) \) is non-trivial and finite. Under these assumptions, we can see that the characteristic polynomial \( F_{k^c/k,S}(T) \) of \( X_S(k^c) \) is the same as in the proof of Theorem 1.2. In this case, we see that

\[ |X_S(k)| \cdot |F_{k^c/k,S}(0)|_p \geq |X_{\emptyset}(k)| > 1 \]

(recall also that \( \mu_{k^c/k,S} = 0 \)), and hence \( X_S(k^c) \) contains a non-trivial finite submodule.
We will give another example. The method of construction is different from Theorem 1.2.

**Proposition 4.5.** Let \( p \) be an odd prime number. There is a finite set \( S \) of prime numbers (not containing \( p \)), and a finite \( p \)-extension \( k \) of \( \mathbb{Q} \) such that \( X_S(k^c) \cong \mathbb{Z}_p \) as a \( \mathbb{Z}_p \)-module.

**Proof.** We use the result given in [17] (see also [9]). Let \( S = \{q_1, q_2\} \) be a set of distinct prime numbers satisfying the condition of [17, Theorem 1]. (We will not use this condition directly in this proof. For the existence of such a set \( S \), see also [17, Remark 1, Remark 2].) Let \( L_S(\mathbb{Q}^c) / \mathbb{Q}^c \) be the maximal pro-\( p \) extension unramified outside \( S \). From [17, Theorem 1], we see that \( \text{Gal}(L_S(\mathbb{Q}^c) / \mathbb{Q}^c) \) is isomorphic to an infinite metacyclic pro-\( p \) group \( G \) topologically generated by \( a, b \) which satisfy

\[
a^b^2 = 1, \quad b^{-1}ab = a^{1+p}.
\]

(In the following, we will identify \( \text{Gal}(L_S(\mathbb{Q}^c) / \mathbb{Q}^c) \) with \( G \).) For a positive integer \( n \), let \( H_n \) be the open subgroup of \( G \) which is topologically generated by \( b^n \). Then, we can take \( n \) such that the fixed field \( L \) of \( L_S(\mathbb{Q}^c) \) by \( H_n \) is a Galois extension over \( \mathbb{Q} \). Since \( L / \mathbb{Q}^c \) is finite, there is a finite \( p \)-extension \( k / \mathbb{Q} \) such that \( L = k^c \). We also note that \( k \) is totally real.

By the above results, \( \text{Gal}(L_S(\mathbb{Q}^c) / k^c) \cong \mathbb{Z}_p \). Note that \( L_S(\mathbb{Q}^c) \) is also the maximal pro-\( p \) extension of \( k^c \) unramified outside \( S \). This implies that \( X_S(k^c) \cong \text{Gal}(L_S(\mathbb{Q}^c) / k^c) \). The assertion follows. \( \square \)

### 5. Proof of Theorem 1.3

In this section, we put \( k = \mathbb{Q}(\sqrt{-3}) \) and \( p = 3 \). Note that there is only one prime \( p \) of \( k \) lying above 3. Suppose that \( q_1, q_2 \) satisfy the assumptions of Theorem 1.3, and put \( S = \{q_1, q_2\} \). We see that \( q_i \) is inert in \( k \) and \( |R(k, q_iO_k)| = 3 \) for \( i = 1, 2 \). Note also that \( |X_S(k)| = 3 \) because the image of \( \zeta_3 \) in \( R(k, q_1O_k) \oplus R(k, q_2O_k) \) is not trivial.

First, we will show that \( X_S(k) \) is not pseudo-null. To see this, we need some preparations. Let \( k^a / k \) be the anti-cyclotomic \( \mathbb{Z}_3 \)-extension, and \( k_m^a \) its \( m \)th layer.

**Lemma 5.1.** Let the assumptions be as in Theorem 1.3. We put \( F = k_m^a \). Then \( \dim_{\mathbb{Q}_3} X_S(F^c) \otimes_{\mathbb{Z}_3} \mathbb{Q}_3 \geq 3^m - 1 \).

**Proof.** Our proof of this lemma uses a method given in [8], [10], [17], etc.

Take a topological generator \( \gamma \) of \( \text{Gal}(F^c / F) \) satisfying \( \zeta_{3^n} \mapsto \zeta_{3^n}^4 \) for all \( n \), and fix an isomorphism from \( \Lambda_{F^c / F} \) to \( \mathbb{Z}_p[[T]] \) satisfying \( \gamma \mapsto 1 + T \).

We remark that the prime of \( k \) lying above \( q_i \) splits completely in \( F \) (see, e.g., [12]), and hence there are \( 3^m \) primes in \( F \) lying above \( q_i \) (for \( i = 1, 2 \)). Put \( r = 3^m \). We denote by \( q_{1,1}, \ldots, q_{r,1} \) (resp. \( q_{1,2}, \ldots, q_{r,2} \)) the primes of \( F \) lying above \( q_1 \) (resp. \( q_2 \)). Note that each \( q_{i,j} \) is not decomposed in \( F^c / F \).
by the assumptions. Let $F^c_n$ be the $n$th layer of $F^c/F$. We denote by $i_n(q_{i,j})$ the extension of $q_{i,j}$ in $F^c_n$. Note that we can see that
\[
\lim_n R(F^c_n, i_n(q_{i,j})) \cong \mathbb{Z}_3[[T]]/(T - 3)
\]
as a $\mathbb{Z}_3[[T]]$-module (see also the proof of Theorem 1.2 in Section 4).

Note that 3 does not divide the class number of $k$, and only $p$ is ramified in $F^c_n/k$. Hence $X_0(F^c)$ is trivial (by Iwasawa’s result [11]). We put $E = \lim_n E(F^c_n) \otimes \mathbb{Z}_3[\mathbb{T}]$ where the projective limit is taken with respect to the norm mappings. We can also regard $E$ as a $\mathbb{Z}_3[[T]]$-module. By using class field theory, we obtain the following exact sequence
\[
E/(T - 3) \to \lim_n \bigoplus_{j=1}^2 \bigoplus_{i=1}^{2^r} R(F^c_n, i_n(q_{i,j})) \to X_S(F^c) \to 0
\]
(cf. e.g., [17], [10]). Note that the second term is isomorphic to $(\mathbb{Z}_3[[T]]/(T - 3))^{\oplus 2r}$, and hence it is free of rank $2r$ as a $\mathbb{Z}_3$-module.

By using [18, (11.3.11) Theorem (iii)] ($F^c/F$ satisfies the assumption of this theorem), we see that
\[
E \cong \mathbb{Z}_3[[T]]^{\oplus r} \oplus \mathbb{Z}_3(1),
\]
here $\mathbb{Z}_3(1)$ is the first Tate twist of $\mathbb{Z}_3$. Hence $\dim_{\mathbb{Q}_3} E/(T - 3) \otimes \mathbb{Z}_3 \mathbb{Q}_3 = r + 1$.

The assertion follows from these facts.

\[\square\]

**Lemma 5.2.** Under the assumptions of Theorem 1.3, $X_S(\tilde{k})$ is not pseudo-null as a $\Lambda_{\tilde{k}/k}$-module.

**Proof.** Let the notations be as in Lemma 5.1. Note that $F^c$ is an intermediate field of $\tilde{k}/k^c$, and $F^c/\tilde{k}/k^c$ is a cyclic extension of degree $3^r$. Since $p$ is totally ramified in $\tilde{k}/k$, we see that the Gal($\tilde{k}/F^c)$-coinvariant quotient $X_S(\tilde{k})_{\text{Gal}(\tilde{k}/F^c)}$ is isomorphic to $X_S(F^c)$. We can also show that $X_S(\tilde{k})$ is a finitely generated $\mathbb{Z}_3[[\text{Gal}(\tilde{k}/k^c)]]$-module because $X_S(\tilde{k})_{\text{Gal}(\tilde{k}/k^c)} \cong X_S(k^c)$ is finitely generated over $\mathbb{Z}_3$ (see, e.g., [10]). However, Lemma 5.1 implies that $X_S(\tilde{k})$ is not a torsion $\mathbb{Z}_3[[\text{Gal}(\tilde{k}/k^c)]]$-module. From this, we can deduce that $X_S(\tilde{k})$ is not pseudo-null as a $\Lambda_{\tilde{k}/k}$-module (see Greenberg [7], or Lemma 2.3 of Fujii [3]).

\[\square\]

**Remark 5.3.** Concerning the non-pseudo-nullity of $X_S(\tilde{k})$ (for a general imaginary quadratic field $k$), see also Kataoka [14]. However, Kataoka’s result does not cover our case ($p = 3$ and $k = \mathbb{Q}(\sqrt{-3})$).

**Lemma 5.4.** Under the assumptions of Theorem 1.3, $X_S(K)$ does not have a non-trivial finite $\Lambda_K/k$-submodule for every $\mathbb{Z}_3$-extension $K/k$. 
**Proof.** Let $K/k$ be an arbitrary $\mathbb{Z}_3$-extension, and put $H = \text{Gal}(\bar{k}/K)$. We recall that $p$ is totally ramified in $K/k$, and $|X_S(k)| = 3$. Hence, by Corollary 2.2, it is sufficient to show that $X_S(K)$ is infinite. Assume that $X_S(K)$ is finite. In our situation, the $H$-coinvariant quotient $X_S(\bar{k})_H$ is isomorphic to $X_S(K)$, and hence $X_S(\bar{k})_H$ is also finite. Then we can see that $X_S(\bar{k})$ is pseudo-null by using Perrin-Riou’s result [24, Lemme 4] (see also Minardi [15]). However, this contradicts to Lemma 5.2. □

The remaining part of our proof of Theorem 1.3 is heavily relied on Greenberg’s results given in [6]. Assume that the maximal pseudo-null submodule $Z$ of $X_S(\bar{k})$ is not trivial. Let $I$ be the augmentation ideal of $\mathbb{Z}_3[\text{Gal}(\bar{k}/k)]$. We claim that $Z/I$ is finite. To show this, we use a similar argument which is given in the paragraph before Lemma 5 of [6]. Let $K/k$ be a $\mathbb{Z}_3$-extension. We put $H = \text{Gal}(\bar{k}/K)$ and $\Gamma = \text{Gal}(K/k)$. Recall that $p$ is totally ramified in $\bar{k}/k$. Then $X_S(\bar{k})_H \cong X_S(K)$, and it is a finitely generated torsion $\mathbb{Z}_3[\text{Gal}(K/k)]$-module. From this, we can see that $(X_S(\bar{k})/Z)^H$ is trivial, and hence the natural $\mathbb{Z}_3[\text{Gal}(K/k)]$-module homomorphism $Z^H \to X_S(\bar{k})_H (\cong X_S(K))$ is injective. Moreover, since $X_S(K)_\Gamma \cong X_S(k)$, we can show that $(Z^H)_\Gamma$ is finite. Then the claim follows. From this, we can apply [6, Lemma 5]. In this case, there must be a $\mathbb{Z}_3$-extension $K^\dagger/k$ such that $Z_{\text{Gal}(K^\dagger/k)}$ has a non-trivial finite submodule, and then $X_S(K^\dagger)$ has a non-trivial finite submodule from the above argument. This contradicts Lemma 5.4. Hence, Theorem 1.3 completely follows. □

**Remark 5.5.** There is another method to deduce Theorem 1.3 from the lemmas. We shall state this briefly. We take the isomorphism $\mathbb{Z}_3[[\text{Gal}(k^c/k)]] \cong \mathbb{Z}_3[T]$ given in the proof of Lemma 5.1, then we see that $\mu_{k^c/k,S} = 0$ and $F_{k^c/k,S}(T) = T - 3$ (see, e.g., [10]). Moreover, by Lemma 5.4, we see that $X_S(k^c) \cong \mathbb{Z}_3$ as a $\mathbb{Z}_3$-module. Recall also that $X_S(k)_{\text{Gal}(\bar{k}/k^c)} \cong X_S(k^c)$. Moreover, it can be shown that $X_S(\bar{k})$ is a cyclic $\mathbb{Z}_3[[\text{Gal}(\bar{k}/k^c)]]$-module. Hence, $X_S(\bar{k}) \cong \mathbb{Z}_3[[\text{Gal}(\bar{k}/k^c)]]/\mathfrak{A}$, where $\mathfrak{A}$ is the annihilator ideal of $\mathbb{Z}_3[[\text{Gal}(\bar{k}/k^c)]]$ for $X_S(\bar{k})$. By Lemma 5.2, $X_S(\bar{k})$ is not pseudo-null. By a similar argument given in the proof of [2, Proposition 3.1] (or [15, Section 3.D]), we can show that $\mathfrak{A}$ is a principal ideal generated by an irreducible element. (The fact that $F_{k^c/k,S}(T) = T - 3$ is crucial.) Hence, $X_S(\bar{k})$ does not contain a non-trivial pseudo-null submodule.

**Appendix A. Weak analogs of Greenberg’s conjecture**

Let $k$ be a totally real field and $p$ an odd prime number. We denote by $S$ a finite set of prime numbers which does not contain $p$. To consider
the structure of $X_S(k^c)$, it is sufficient to treat $S$ satisfying the following condition (see also, e.g., [10]):

(R) For each $q \in S$, there is a prime $q^\prime$ of $k$ lying above $q$ such that $R(k, q^\prime)$ is not trivial.

When $k$ is a real quadratic field, the condition (R) is equivalent to the condition that every $q \in S$ satisfies (a) or (b) in Remark 4.1.

Let $M_{S,p}(k^c)$ be the maximal abelian pro-$p$ extension of $k^c$ unramified outside $S \cup \{p\}$. In this case, we see that $\text{Gal}(M_{S,p}(k^c)/k^c)$ is a finitely generated torsion $\Lambda_{k^c/k}$-module. We also see that $\text{Gal}(M_{S,p}(k^c)/k^c)$ does not contain a non-trivial finite $\Lambda_{k^c/k}$-submodule. (For these results, see, e.g., [6], [18].)

First, we consider the case when $S = \emptyset$. It is conjectured that $X_\emptyset(k^c)$ is finite (Greenberg’s conjecture [5]). Moreover, some weak forms of this conjecture are also proposed (see Nguyen Quang Do [19], [20]).

(Conj1) $X_\emptyset(k^c)$ is trivial or contains a non-trivial finite $\Lambda_{k^c/k}$-submodule. 

(Conj2) $\text{Gal}(M_\emptyset, p(k^c)/k^c)$ is trivial or $\text{Gal}(M_\emptyset, p(k^c)/L_\emptyset(k^c))$ is not trivial.

**Remark A.1.** Note that (Conj1) implies (Conj2). If $p$ splits completely in $k$ and Leopoldt’s conjecture holds for $k$ and $p$, then (Conj1) and (Conj2) are equivalent (see [19], [22]). In [19] and [20], Nguyen Quang Do considered these conjectures for the case when $k$ is a real abelian field and $p$ splits completely in $k$ (see also [21]).

Next, we shall consider the “$S$-ramified” version of these assertions:

(Conj1S) $X_S(k^c)$ is trivial or contains a non-trivial finite $\Lambda_{k^c/k}$-submodule.

(Conj2S) $\text{Gal}(M_{S,p}(k^c)/k^c)$ is trivial or $\text{Gal}(M_{S,p}(k^c)/L_S(k^c))$ is not trivial.

However, the results given in Section 4 imply that the assertion (Conj1S) does not hold in general. For the assertion (Conj2S), we can obtain the following:

**Theorem A.2.** Let $k$ be a totally real field, $p$ an odd prime number, and $S$ a non-empty finite set of prime numbers which does not contain $p$. Assume that $S$ satisfies (R). If $\text{Gal}(L_{\{q\}}(k^c)/L_\emptyset(k^c))$ is finite for some $q \in S$, then $\text{Gal}(M_{S,p}(k^c)/L_S(k^c))$ is not trivial.

**Proof.** When $k = \mathbb{Q}$, this assertion is already mentioned in [4] (and the proof of our case is almost similar). Take a prime number $q \in S$ such that $\text{Gal}(L_{\{q\}}(k^c)/L_\emptyset(k^c))$ is finite. Since $S$ satisfies (R), we see that $\text{Gal}(M_{\{q\}, p}(k^c)/M_\emptyset, p(k^c))$ is infinite (see, e.g., [18, (11.3.5) Theorem and (11.3.6) Corollary]). Hence $\text{Gal}(M_{\{q\}, p}(k^c)/L_\emptyset(k^c))$ is also infinite. Thus, we conclude that $\text{Gal}(M_{\{q\}, p}(k^c)/L_{\{q\}}(k^c))$ is infinite. Since $L_S(k^c) \subseteq M_{\{q\}, p}(k^c)L_S(k^c) \subseteq M_{S,p}(k^c)$, we can show that $\text{Gal}(M_{S,p}(k^c)/L_S(k^c))$ is not trivial. (Note that we do not need the validity of Leopoldt’s conjecture in this proof.)
Moreover, we can also see the following:

**Proposition A.3.** Let $k$ be a totally real field, $p$ an odd prime number, and $S$ a non-empty finite set of prime numbers which does not contain $p$. Assume that Leopoldt’s conjecture holds for $k$ and $p$. Assume also that $p$ splits completely in $k$. Then $X_S(k^c)$ contains a non-trivial finite $\Lambda_{k^c/k}$-submodule if and only if $\text{Gal}(M_{S,p}(k^c)/L_S(k^c))$ is not trivial.

**Proof.** The proof is quite similar to the case when $S = \emptyset$. See [22] or [19] (see also [4] for the case when $k = \mathbb{Q}$ and $S \neq \emptyset$). Note that we need the finiteness of $\text{Gal}(M_{S,p}(k^c)/k^c)$ (where $\Gamma = \text{Gal}(k^c/k)$) to show the triviality of $\text{Gal}(M_{S,p}(k^c)/k^c)^\Gamma$, however, this follows from class field theory and the validity of Leopoldt’s conjecture for $k$ and $p$ (see, e.g., [18]). □

Hence we obtained the following:

**Corollary A.4.** Let $k$ be a totally real field, $p$ an odd prime number, and $S$ a non-empty finite set of prime numbers which does not contain $p$. Assume that $S$ satisfies (R). Assume also that $p$ splits completely in $k$, and Leopoldt’s conjecture holds for $k$ and $p$. If $\text{Gal}(L_{\{q\}}(k^c)/L_\emptyset(k^c))$ is finite for some $q \in S$, then $X_S(k^c)$ contains a non-trivial finite submodule.

When $k$ is a real abelian field and $p$ is an odd prime, it was shown that $\text{Gal}(L_{\{q\}}(k^c)/L_\emptyset(k^c))$ is finite for every prime number $q (\neq p)$ (see [8, Theorem 1.1]). Hence, by combining the validity of Leopoldt’s conjecture (see [1]), we can also obtain the following:

**Corollary A.5.** Let $k$ be a real abelian field, $p$ an odd prime number, and $S$ a non-empty finite set of prime numbers which does not contain $p$. Assume that $S$ satisfies (R). Then the following statements hold.

1. $\text{Gal}(M_{S,p}(k^c)/L_S(k^c))$ is not trivial.
2. Moreover, if $p$ splits completely in $k$, then $X_S(k^c)$ contains a non-trivial finite submodule.

Note that the assertions of the above corollary were already shown in [4] for the case when $k = \mathbb{Q}$.

**References**

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