J. Ramanujan Math. Soc. **29**, No.3 (2014) 295–305

On restricted ramifications and pseudo-null submodules of Iwasawa modules for $\mathbb{Z}_p^2$-extensions

Satoshi Fujii
Kanazawa Institute of Technology, 7-1 Ohgigaoka, Nonoichi, Ishikawa 921-8501 Japan
e-mail: fujiisatoshi@neptune.kanazawa-it.ac.jp

Communicated by: *R. Sujatha*

Received: November 14, 2013

Abstract. Ozaki studied the non-triviality and the existence of non-trivial finite submodules of the Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension over totally real fields. In this article, we show analogous results for the $\mathbb{Z}_p^2$-extension over imaginary quadratic fields.

2010 *Mathematics Subject Classification.* 11R23.

1. Introduction

Let p be an odd prime number and $k/\mathbb{Q}$ a finite extension. Let $\mathbb{Z}_p$ be the ring of p-adic integers. Let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension and k_n a unique intermediate field of k_∞/k such that $[k_n : k] = p^n$ for each non-negative integer n. Let $L(k_\infty)/k_\infty$ be the maximal unramified abelian pro-p extension. By class field theory, the Galois group $\mathrm{Gal}(L(k_\infty)/k_\infty)$ is identified with the projective limit of the p-part of the ideal class groups of k_n for all integers $n \geq 0$ with respect to the norm maps. The Galois group $\mathrm{Gal}(k_\infty/k)$ acts on $\mathrm{Gal}(L(k_\infty)/k_\infty)$ via the inner automorphism, and then the complete group ring

$$\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]] := \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(k_n/k)]$$

acts on $\mathrm{Gal}(L(k_\infty)/k_\infty)$. Here the projective limit is taken with respect to the restriction maps $\mathrm{Gal}(k_{n+1}/k) \to \mathrm{Gal}(k_n/k)$ of Galois groups for each non-negative integers n. A subject of the theory of $\mathbb{Z}_p$-extensions is studying the $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$-module structure of $\mathrm{Gal}(L(k_\infty)/k_\infty)$.

This research was supported by Grant-in-Aid for JSPS Fellows (22–5731) from Japan Society for the Promotion of Science. The work of this article was done when the author was a Research Fellow of the Japan Society for the Promotion of Science.

Ozaki showed a totally real analogue of Kummer's criterion (see for example section 5 of [13]) of the divisibility of the class number of the p-th cyclotomic field.

Theorem A (Ozaki [11]). *Suppose that k is totally real and that p splits completely in $k/\mathbb{Q}$. Then the following conditions are equivalent:*

(1) $\mathrm{Gal}(L(k_\infty)/k_\infty) \neq 0$.
(2) $p\zeta_p(0, k) \equiv 0 \bmod p$.

Here we denote by $\zeta_p(s, k)$ the p-adic zeta function of k.

As an application of the proof of Theorem A, Ozaki also showed the following result. We shall introduce a slightly modified statement.

Theorem B (Ozaki [11]). *Suppose that k is totally real and p splits completely in $k/\mathbb{Q}$. Suppose further that Leopoldt's conjecture holds for p and k. Then the following two conditions are equivalent:*

(1) $\mathrm{Gal}(L(k_\infty)/k_\infty)$ *has a non-trivial finite* $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$*-submodule.*
(2) $M(k_\infty) \neq L(k_\infty)$.

Here we denote by $M(k_\infty)$ the maximal abelian pro-p extension of k_∞ unramified outside p.

Note that a $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$-module is finite if and only if its annihilator ideal contains two elements which are relatively prime (see section 13 of [13]). For totally real fields k, it is conjectured by Greenberg that $\mathrm{Gal}(L(k_\infty)/k_\infty)$ is finite (see [4]), and no counter examples of totally real fields have been found yet. It is not known even whether $\mathrm{Gal}(L(k_\infty)/k_\infty)$ always has a non-trivial finite submodule or not when $\mathrm{Gal}(L(k_\infty)/k_\infty) \neq 0$. So Theorem B seems interesting because the existence of non-trivial finite submodules is characterized by non-trivial ramifications of primes lying above p.

In the present article, we will show results analogous to Theorem A and Theorem B for $\mathbb{Z}_p^2$-extensions of imaginary quadratic fields. Greenberg's conjecture is also studied for imaginary quadratic fields, furthermore, for all number fields (see Greenberg [6]).

2. Results for $\mathbb{Z}_p^2$-extensions over imaginary quadratic fields

From here, let p be an odd prime number and k an imaginary quadratic field in which p splits, write $(p) = \mathfrak{p}\mathfrak{p}'$ in k with $\mathfrak{p} \neq \mathfrak{p}'$. By class field theory, there is a unique $\mathbb{Z}_p^2$-extension $\widetilde{k}/k$. Let $L(\widetilde{k})/\widetilde{k}$ be the maximal unramified pro-p abelian extension. Let χ be the Dirichlet character associated to k and ω the Teichmüller character of mod p. Let $L_p(s, \omega\chi^{-1})$ be the p-adic

Dirichlet L-function associated to the even character $\omega\chi^{-1}$. It is known that $L_p(s, \omega\chi^{-1})$ is an analytic function in $s \in \mathbb{Z}_p$, and hence we can consider the derivative $L'_p(s, \omega\chi^{-1})$ of $L_p(s, \omega\chi^{-1})$. At first, we give a result analogous to Theorem A.

Theorem 1. *The following two conditions are equivalent.*

(1) $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k}) \neq 0$.

(2) $\dfrac{L'_p(0, \omega\chi^{-1})}{p} \equiv 0 \bmod p$.

We must mention here that a very similar result had been obtained by Byeon (see Proposition 2.3 of [1].)

Let $M_{\mathfrak{p}}(\widetilde{k})/\widetilde{k}$ be the maximal pro-p abelian extension unramified outside all primes lying above $\mathfrak{p}$. Then the complete group ring

$$\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]] = \varprojlim_{k'} \mathbb{Z}_p[\mathrm{Gal}(k'/k)] \quad (k \subseteq k' \subseteq \widetilde{k},\ [k' : k] < \infty)$$

acts on $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k})$ and on $\mathrm{Gal}(M_{\mathfrak{p}}(\widetilde{k})/\widetilde{k})$, and it is known that these modules are finitely generated and torsion (for this, we shall see below for our special cases). A finitely generated, torsion $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$-module is called pseudo-null if the annihilator ideal contains two elements which are relatively prime. The second result of this article is an analogue of Theorem B.

Theorem 2. *The following two conditions are equivalent.*

(1) $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k})$ *has a non-trivial pseudo-null* $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$*-submodule.*

(2) $M_{\mathfrak{p}}(\widetilde{k}) \neq L(\widetilde{k})$.

It is conjectured by Greenberg [6] that $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k})$ is a pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$-module, and no counter examples have been found yet. It is also not known whether $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k})$ always has a non-trivial pseudo-null $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$-submodule or not when $\mathrm{Gal}(L(\widetilde{k})/\widetilde{k}) \neq 0$. The author expects that Theorem A, Theorem B, Theorem 1 and Theorem 2 will play crucial roles in the study of Greenberg's conjecture.

At first, we give the proof of Theorem 2, and then we prove Theorem 1.

3. Proof of Theorem 2

Let p be an odd prime number and k an imaginary quadratic field in which p splits, that is, $p = \mathfrak{p}\mathfrak{p}'$ with $\mathfrak{p} \neq \mathfrak{p}'$ in k. Recall the cyclotomic $\mathbb{Z}_p$-extension k_∞/k, and let K/k be a $\mathbb{Z}_p$-extension such that $K \cap k_\infty = k$. Then we have $\widetilde{k} = k_\infty K$. Let τ and σ be topological generators of $\mathrm{Gal}(\widetilde{k}/k_\infty)$ and $\mathrm{Gal}(\widetilde{k}/K)$ respectively. By putting $T = \tau - 1$ and $S = \sigma - 1$, we have that

$\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]] = \mathbb{Z}_p[[S, T]]$, here denote by $\mathbb{Z}_p[[S, T]]$ the formal power series ring in two variables with coefficients in $\mathbb{Z}_p$. For an intermediate field F of $\widetilde{k}/k$ (not necessary finite), let $M_{\mathfrak{p}}(F)/F$ and $L(F)/F$ be the maximal pro-p abelian extension unramified outside all primes lying above $\mathfrak{p}$ and the maximal unramified abelian pro-p extension respectively. Put $\mathfrak{X}_{\mathfrak{p}} = \mathrm{Gal}(M_{\mathfrak{p}}(\widetilde{k})/\widetilde{k})$ and $X = \mathrm{Gal}(L(\widetilde{k})/\widetilde{k})$. Then Λ acts on $\mathfrak{X}_{\mathfrak{p}}$ and on X. For a Λ-module M and an element $f \in \Lambda$, let $M[f]$ be the maximal submodule of M which is annihilated by f, namely, $M[f] = \{m \in M \mid fm = 0\}$.

Lemma 1. *The extension $\widetilde{k}/k_\infty$ is unramified at all primes.*

Proof. Let $\mathfrak{I}$ be the inertia group of a prime lying above p in the extension $\widetilde{k}/k$. Since p splits in k, there is a surjective morphism $\mathbb{Z}_p^\times \to \mathfrak{I}$ by class field theory. It follows from $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p$ that $\mathfrak{I} \simeq \mathbb{Z}_p$. Because k_∞/k is totally ramified at all primes lying above p, one sees that $\mathfrak{I} \cap \mathrm{Gal}(\widetilde{k}/k_\infty) = 1$, and hence $\widetilde{k}/k_\infty$ is unramified at all primes lying above p. Since $\widetilde{k}/k$ is unramified outside primes lying above p (see Proposition 13.2 of [13]), we can conclude that $\widetilde{k}/k_\infty$ is unramified at all primes. □

Lemma 2. $M_{\mathfrak{p}}(k_\infty) = L(k_\infty)$.

Proof. The inclusion $L(k_\infty) \subseteq M_{\mathfrak{p}}(k_\infty)$ follows from the definitions of $L(k_\infty)$ and $M_{\mathfrak{p}}(k_\infty)$. Let $M(k_\infty)/k_\infty$ be the maximal pro-p abelian extension unramified outside all primes lying above p. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}$. By the maximality of $M(k_\infty)$, $M(k_\infty)/\mathbb{Q}_\infty$ is a Galois extension, and hence $\mathrm{Gal}(k_\infty/\mathbb{Q}_\infty) = \langle J \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(M(k_\infty)/k_\infty)$ via the inner automorphism.

Here we show that $\mathbb{Q}_\infty$ has no non-trivial abelian p-extensions unramified outside all primes lying above p. Suppose that there is a non-trivial abelian p-extension $M_0/\mathbb{Q}_\infty$ unramified outside all primes lying above p. By taking the Galois closure of $M_0/\mathbb{Q}$, we may assume that $M_0/\mathbb{Q}$ is a Galois extension. Let M_1 be the maximal subfield of M_0 such that $M_1/\mathbb{Q}$ is abelian. Note that $\mathbb{Q}_\infty \subseteq M_1$. By the topological version of Nakayama's lemma, $M_1/\mathbb{Q}_\infty$ is a non-trivial extension. By Kronecker–Weber's theorem, M_1 is contained in the algebraic extension $\mathbb{Q}(\mu_{p^\infty})$ of $\mathbb{Q}$ obtained by adjoining all p-power-th roots of unity. Hence the existence of M_1 contradicts to the fact that $[\mathbb{Q}(\mu_{p^\infty}) : \mathbb{Q}_\infty] = p - 1$. Therefore $\mathbb{Q}_\infty$ has no non-trivial abelian p-extensions unramified outside all primes lying above p.

The above fact shows that J acts on $\mathrm{Gal}(M(k_\infty)/k_\infty)$ as inverse, and hence each submodule of $\mathrm{Gal}(M(k_\infty)/k_\infty)$ is a J-submodule. This implies that each subextension of $M(k_\infty)/k_\infty$ is a Galois extension over $\mathbb{Q}_\infty$. In particular, $M_{\mathfrak{p}}(k_\infty)/\mathbb{Q}_\infty$ is a Galois extension. Since the prime lying above p splits in $k_\infty/\mathbb{Q}_\infty$, and since $M_\mathfrak{p}(k_\infty)/k_\infty$ is unramified at all primes lying above $\mathfrak{p}'$, $M_\mathfrak{p}(k_\infty)/\mathbb{Q}_\infty$ is unramified at all primes lying above $\mathfrak{p}'$. Because of $M_\mathfrak{p}(k_\infty)/\mathbb{Q}_\infty$ is a Galois extension, all primes lying above $\mathfrak{p}$ is also unramified in $M_\mathfrak{p}(k_\infty)/\mathbb{Q}_\infty$. Thus $M_\mathfrak{p}(k_\infty)/k_\infty$ is unramified, and hence $M_\mathfrak{p}(k_\infty) \subseteq L(k_\infty)$. □

Lemma 3.

(1) *The* Λ*-modules* $\mathfrak{X}_\mathfrak{p}$ *and* X *are finitely generated and torsion.*
(2) *The* T*-torsion submodule* $X[T]$ *of* X *is a pseudo-null submodule.*

Proof. (1) The fixed field L by $(\tau - 1)X = TX$ of $L(\widetilde{k})$ is the maximal abelian subfield of $L(\widetilde{k})/k_\infty$. By lemma 2 of [11], we know that $L = L(k_\infty)$, and further we have the following exact sequence

$$0 \longrightarrow X/TX \longrightarrow \mathrm{Gal}(L(k_\infty)/k_\infty) \longrightarrow \mathrm{Gal}(\widetilde{k}/k_\infty) \longrightarrow 0$$

of $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$-modules. By lemma 1 and lemma 2, we also have the following exact sequence

$$0 \longrightarrow \mathfrak{X}_\mathfrak{p}/T\mathfrak{X}_\mathfrak{p} \longrightarrow \mathrm{Gal}(L(k_\infty)/k_\infty) \longrightarrow \mathrm{Gal}(\widetilde{k}/k_\infty) \longrightarrow 0$$

of $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$-modules. It follows from Ferrero–Washington's Theorem [2] and Corollary 13.28 of [13] that $\mathrm{Gal}(L(k_\infty)/k_\infty)$ is a finitely generated free $\mathbb{Z}_p$-module of rank $\lambda_p(k)$, which is the Iwasawa λ-invariant of $k_\infty = k$. Put $r = \lambda_p(k) - 1$. From the above exact sequences, we have

$$X/TX \simeq \mathfrak{X}_\mathfrak{p}/T\mathfrak{X}_\mathfrak{p} \simeq \mathbb{Z}_p^r$$

as $\mathbb{Z}_p$-modules. By the topological version of Nakayama's lemma, X and $\mathfrak{X}_\mathfrak{p}$ are generated by r elements over $\mathbb{Z}_p[[T]]$, write

$$X = \sum_{i=1}^{r} \mathbb{Z}_p[[T]]x_i$$

and

$$\mathfrak{X}_\mathfrak{p} = \sum_{i=1}^{r} \mathbb{Z}_p[[T]]y_i$$

for some elements $x_1, \ldots, x_r \in X$ and $y_1, \ldots, y_r \in \mathfrak{X}_\mathfrak{p}$. In particular X and $\mathfrak{X}_\mathfrak{p}$ are finitely generated over Λ. It follows that there are (r,r)-matrices A and B with entries in $\mathbb{Z}_p[[T]]$ such that

$$S\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = A\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}, S\begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = B\begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix}.$$

Hence $\det(S - A)$ and $\det(S - B)$ annihilate X and $\mathfrak{X}_{\mathfrak{p}}$ respectively, and therefore X and $\mathfrak{X}_{\mathfrak{p}}$ are torsion over Λ.
(2) First, suppose that $r = 0$. Then X/TX is trivial. By the topological version of Nakayama's lemma, X is also trivial, in particular is pseudo-null. Next, suppose that $r > 0$. Then $\det(S - A)$ is a non-constant monic polynomial of variable S with coefficients in $\mathbb{Z}_p[[T]]$ of degree r. Since T does not divide $\det(S - A)$ and since T is a prime element of Λ, $X[T]$ is a pseudo-null submodule of X. □

The following proposition is a key stone of the proof of Theorem 2.

Proposition 1. *$\mathfrak{X}_{\mathfrak{p}}$ has no non-trivial pseudo-null Λ-submodule.*

Proof. Proposition 1 is obtained by Perrin–Riou [12]. However, in our case, the proof is not difficult, so we prefer to give a proof here.

Let $\mathfrak{D}'$ be the decomposition group in $\widetilde{k}/k$ of a prime lying above $\mathfrak{p}'$.

Lemma 4. $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}'] < \infty$.

Proof. This fact is stated in Minardi's thesis [9]. We prefer to prove it here. Let J_k be the idéle group of k. Let $M(k)/k$ be the maximal pro-p abelian extension unramified outside all primes lying above p. For primes $\mathfrak{p}$ and $\mathfrak{p}'$, let $U_{\mathfrak{p}}^{(1)}$ and $U_{\mathfrak{p}'}^{(1)}$ be the local principal unit groups with respect to $\mathfrak{p}$ and $\mathfrak{p}'$. By class field theory, there is a closed subgroup H which contains $k^\times$ and local unit groups at all primes not above p, and an isomorphism

$$J_k/H \simeq \mathrm{Gal}(M(k)/k),$$

via Artin's map. Also, we have an exact sequence

$$0 \longrightarrow U_{\mathfrak{p}}^{(1)} \times U_{\mathfrak{p}'}^{(1)} \longrightarrow J_k/H \longrightarrow Cl_k \otimes \mathbb{Z}_p \longrightarrow 0$$

of profinite abelian groups. Let $\pi' \in k^\times$ be a prime element of $\mathfrak{p}'$. Put

$$\alpha_{\mathfrak{q}} = \begin{cases} \pi'^{p-1} & \text{if } \mathfrak{q} = \mathfrak{p}' \\ 1 & \text{otherwise} \end{cases},$$

and

$$\beta_{\mathfrak{q}} = \begin{cases} \pi'^{-p+1} & \text{if } \mathfrak{q} = \mathfrak{p} \\ 1 & \text{otherwise} \end{cases}.$$

Then $(\alpha_{\mathfrak{q}})_{\mathfrak{q}}$ and $(\beta_{\mathfrak{q}})_{\mathfrak{q}}$ are in J_k, and

$$(\alpha_{\mathfrak{q}})_{\mathfrak{q}} \equiv (\beta_{\mathfrak{q}})_{\mathfrak{q}} \bmod H.$$

From the facts that $\pi'^{p-1} \in U_{\mathfrak{p}}^{(1)}$ and $\overline{\langle \pi'^{p-1} \rangle} \times U_{\mathfrak{p}'}^{(1)}$ has finite index in $U_{\mathfrak{p}}^{(1)} \times U_{\mathfrak{p}'}^{(1)}$, we conclude that the decomposition group of $\mathfrak{p}'$ in $M(k)/k$ has finite index. Therefore, $[\mathrm{Gal}(\widetilde{k}/k) : \mathfrak{D}'] < \infty$. □

Let k' be the fixed field of $\widetilde{k}$ by $\mathfrak{D}'$. By Lemma 4, k'/k is finite. Let $\mathfrak{X}_p$ be the Galois group of the maximal pro-p abelian extension $M(\widetilde{k})/\widetilde{k}$ unramified outside all primes lying above p, and $\mathfrak{I}_{\mathfrak{P}'}$ be the inertia subgroup of $\mathfrak{X}_p$ of a prime $\mathfrak{P}'$ of $\widetilde{k}$ lying above $\mathfrak{p}'$. Then we have the following exact sequence

$$\bigoplus_{\mathfrak{P}'|\mathfrak{p}'} \mathfrak{I}_{\mathfrak{P}'} \longrightarrow \mathfrak{X}_p \longrightarrow \mathfrak{X}_{\mathfrak{p}} \longrightarrow 0$$

of Λ-modules. Note that there are $[k' : k]$ primes of $\widetilde{k}$ lying above $\mathfrak{p}'$. Here we determine the Λ-module structure of $\bigoplus_{\mathfrak{P}'|\mathfrak{p}'} \mathfrak{I}_{\mathfrak{P}'}$. Let $\mathfrak{p}'_{k'}$ be a prime of k' lying above $\mathfrak{p}'$. Since $\mathfrak{p}'_{k'}$ is unramified in $k'/\mathbb{Q}$ and has degree 1, the completion of k' at $\mathfrak{p}'_{k'}$ is isomorphic to $\mathbb{Q}_p$, the p-adic number field. By local class field theory, there is a unique $\mathbb{Z}_p^2$-extension $\widetilde{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. Let $\mathfrak{P}'$ be the unique prime of $\widetilde{k}$ lying above $\mathfrak{p}'_{k'}$. It follows that the localization of $\widetilde{k}$ at $\mathfrak{P}'$ is isomorphic to $\widetilde{\mathbb{Q}_p}$. We need the following.

Theorem D (From the Theorem of Wintenberger [14]). *There is a surjective morphism*

$$\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k')]](\simeq \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{\mathbb{Q}_p}/\mathbb{Q}_p)]]) \longrightarrow \mathfrak{I}_{\mathfrak{P}'}$$

of $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k')]]$*-modules.*

Remark.

(1) Wintenberger dealt with more general situations for $\mathbb{Z}_p^d$-extensions of local fields.
(2) We can also show Theorem D by using the fact that the Galois group of the maximal pro-p extension of $\mathbb{Q}_p$ is a free pro-p group of rank 2.

By Theorem D, there is a surjective morphism from $\bigoplus_{\mathfrak{P}'|\mathfrak{p}'} \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k')]]$ to $\bigoplus_{\mathfrak{P}'|\mathfrak{p}'} I_{\mathfrak{P}'}$. On the other hand, $\bigoplus_{\mathfrak{P}'|\mathfrak{p}'} \mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k')]]$ is isomorphic to Λ as Λ-modules. Hence we have the following exact sequence

$$\Lambda \longrightarrow \mathfrak{X}_p \longrightarrow \mathfrak{X}_{\mathfrak{p}} \longrightarrow 0$$

of Λ-modules. By Greenberg's result [5], we know that $\mathfrak{X}_p$ has Λ-rank 1. Also, the Λ-rank of $\mathfrak{X}_{\mathfrak{p}}$ is 0 by Lemma 3 (1). This implies that the morphism $\Lambda \to \mathfrak{X}_p$ must be injective.

Let B be a pseudo-null submodule of $\mathfrak{X}_{\mathfrak{p}}$, and let C be the inverse image of B with respect to the morphism $\mathfrak{X}_p \to \mathfrak{X}_{\mathfrak{p}}$. Then $0 \to \Lambda \to C \to B \to 0$ is exact. Now we claim that the Λ-torsion submodule of C is trivial. Indeed, let $\mathrm{Tor}_\Lambda C$ be the submodule of C which consists of all Λ-torsion elements. Then $\mathrm{Tor}_\Lambda C + \Lambda/\Lambda$ maps to B injectively. Since

$$\mathrm{Tor}_\Lambda C + \Lambda/\Lambda \simeq \mathrm{Tor}_\Lambda C/\mathrm{Tor}_\Lambda C \cap \Lambda \simeq \mathrm{Tor}_\Lambda C,$$

we find that $\mathrm{Tor}_{\Lambda} C$ is a pseudo-null submodule of $\mathfrak{X}_p$. However, Greenberg [5] also showed that $\mathfrak{X}_p$ has no non-trivial pseudo-null submodule. Therefore, $\mathrm{Tor}_{\Lambda} C = 0$.

Since B is pseudo-null, there are two annihilators f and g of B such that f and g are relatively prime. Observe the following diagram,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & C & \longrightarrow & B & \longrightarrow & 0 \\ & & {\scriptstyle g\times}\downarrow & & {\scriptstyle g\times}\downarrow & & {\scriptstyle g\times}\downarrow & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & C & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

By the Snake lemma, we have an exact sequence

$$C[g] \longrightarrow B[g] \longrightarrow \Lambda/(g)$$

of Λ-modules. From the above claim, we have $C[g] = 0$, and by the choice of g we have $B[g] = B$. Observe the following commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \longrightarrow & \Lambda/(g) \\ & & {\scriptstyle f\times}\downarrow & & {\scriptstyle f\times}\downarrow \\ 0 & \longrightarrow & B & \longrightarrow & \Lambda/(g) \end{array}$$

of Λ-modules. Since Λ is a UFD and since f and g are relatively prime, the right vertical morphism is injective. However, since f annihilates B, the above morphism on B is trivial, and hence B must be trivial. This completes the proof of Proposition 1. □

We finish the proof of Theorem 2. First, suppose that $M_{\mathrm{p}}(\widetilde{k}) = L(\widetilde{k})$. Then $\mathfrak{X}_{\mathrm{p}} = X$. By Proposition 1, $X = \mathfrak{X}_{\mathrm{p}}$ has no non-trivial pseudo-null submodules. Next suppose that $M_{\mathrm{p}}(\widetilde{k}) \neq L(\widetilde{k})$. Put $Y = \mathrm{Gal}(M_{\mathrm{p}}(\widetilde{k})/L(\widetilde{k}))$. By the Snake lemma to the following exact–commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y & \longrightarrow & \mathfrak{X}_{\mathrm{p}} & \longrightarrow & X & \longrightarrow & 0 \\ & & {\scriptstyle T\times}\downarrow & & {\scriptstyle T\times}\downarrow & & {\scriptstyle T\times}\downarrow & & \\ 0 & \longrightarrow & Y & \longrightarrow & \mathfrak{X}_{\mathrm{p}} & \longrightarrow & X & \longrightarrow & 0 \end{array}$$

of Λ-modules, we have the following exact sequence

$$X[T] \longrightarrow Y/TY \longrightarrow \mathfrak{X}_{\mathrm{p}}/T\mathfrak{X}_{\mathrm{p}} \longrightarrow X/TX \longrightarrow 0.$$

By Lemma 2, we find that $\mathfrak{X}_{\mathrm{p}}/T\mathfrak{X}_{\mathrm{p}} \simeq X/TX$. Hence $X[T] \to Y/TY$ is surjective. By the topological version of Nakayama's lemma, Y/TY is not trivial. Thus $X[T]$ is also not trivial. Furthermore, from Lemma 3, $X[T]$ is a non-trivial pseudo-null submodule of X. This completes the proof of Theorem 2. □

Remark. Let $M_{\mathfrak{p}'}(\widetilde{k})/\widetilde{k}$ be the maximal pro-p abelian extension unramified outside all primes lying above $\mathfrak{p}'$. Since $M_{\mathfrak{p}}(\widetilde{k})$ and $M_{\mathfrak{p}'}(\widetilde{k})$ are conjugate over k, $M_{\mathfrak{p}}(\widetilde{k}) \neq L(\widetilde{k})$ if and only if $M_{\mathfrak{p}'}(\widetilde{k}) \neq L(\widetilde{k})$.

4. Proof of Theorem 1

The notations of this section are the same as before. Let p be an odd prime number and k an imaginary quadratic field in which p splits as $p = \mathfrak{p}\mathfrak{p}'$. Let χ be Dirichlet character associated to k, ω the Teichmüller character of mod p and $L_p(s, \omega\chi^{-1})$ be the p-adic L-function associated to the even character $\omega\chi^{-1}$. Denote by $\lambda_p(k)$ the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k. We introduce some facts.

Lemma 5 (cf. Theorem 5.11 of [13]). *For each positive integer n, it holds that*

$$L_p(1-n, \omega\chi^{-1}) = -(1 - \omega^{1-n}\chi^{-1}(p)p^{n-1})\frac{B_{n,\omega^{1-n}\chi^{-1}}}{n}.$$

Here, denote by $B_{n,\omega^{1-n}\chi^{-1}}$ the generalized Bernoulli number associated to n and $\omega^{1-n}\chi^{-1}$. □

Lemma 6 (Iwasawa [7]). *There exists a power series $G(S) \in \mathbb{Z}_p[[S]]$ such that $L_p(s, \omega\chi^{-1}) = G((1+p)^s - 1)$ for all $s \in \mathbb{Z}_p$.* □

By the Weierstrass preparation theorem and Ferrero–Washington's theorem [2], there are a distinguished polynomial $g(S)$ in $\mathbb{Z}_p[S]$, a monic polynomial of the form $g(S) = S^{\deg g} + \cdots + a_1 S + a_0$ with $a_i \in p\mathbb{Z}_p$ for $0 \le i \le \deg g - 1$, and a unit power series $U(S) \in \mathbb{Z}_p[[S]]$ such that $G(S) = g(S)U(S)$. Since p splits in k, it follows that $\chi^{-1}(p) = \chi(p) = 1$. Then by Lemma 5, one sees that $L_p(0, \omega\chi^{-1}) = 0$. This implies that $a_0 = 0$. Put $f(S) = g(S)/S$. By the analytic class number formula (cf. Theorem 7.14 of [13]), it follows that $\deg g = \lambda_p(k)$. Recall that $\mathrm{Gal}(L(k_\infty)/k_\infty)$ is a free $\mathbb{Z}_p$-module of rank $\lambda_p(k)$. Hence $X/TX \simeq \mathbb{Z}_p^{\deg f}$ as $\mathbb{Z}_p$-modules. It follows from the topological version of Nakayama's lemma that $X \neq 0$ if and only if $X/TX \neq 0$. Also, $X/TX \neq 0$ if and only if $\deg f > 0$, which is equivalent to $f(0) \equiv 0 \bmod p$. Now we consider the derivative of $L_p(s, \omega\chi^{-1})$ at $s = 0$. We then have

$$L_p'(0, \omega\chi^{-1}) = \log_p(1+p) \cdot f(0)U(0).$$

Since the normalized p-adic additive valuation of $\log_p(1+p)$ is 1, $f(0) \equiv 0 \bmod p$ if and only if

$$\frac{L_p'(0, \omega\chi^{-1})}{p} \equiv 0 \bmod p.$$

This completes the proof of Theorem 1.

5. Discussion

If $\lambda_p(k) = 2$, it is known that X has a non-trivial pseudo-null Λ-submodule if and only if X is itself a pseudo-null Λ-module (see for example [3]). So we can obtain the following.

Theorem 3. *Suppose $\lambda_p(k) = 2$. Then the following two statements are equivalent.*

(1) *X is a pseudo-null Λ-module.*
(2) $M_{\mathfrak{p}}(\widetilde{k}) \neq L(\widetilde{k})$.

To find relationships between arithmetic objects and analytic objects is an important theme in number theory. When one looks at the results stated in this article, the following questions arise naturally.

Question. Let p be an odd prime number.

(1) Let k be a totally real field in which p splits completely. Does

$$p\zeta_p(0, k) \equiv 0 \bmod p$$

imply $M(k_\infty) \neq L(k_\infty)$?

(2) Let k be an imaginary quadratic field in which p splits. Does

$$\frac{L'_p(0, \omega\chi^{-1})}{p} \equiv 0 \bmod p$$

imply $M_{\mathfrak{p}}(\widetilde{k}) \neq L(\widetilde{k})$?

Acknowledgement

The author would like to express his thanks to the referee for reading this article carefully and for finding many misprints.

References

[1] D. Byeon, Imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1, *Acta Arith*, **120** (2005) 145–152.

[2] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.*, **109** (1979) 377–395.

[3] S. Fujii, Pseudo-null submodule of the unramified Iwasawa modules for $\mathbb{Z}_p^2$-extensions, *Interdisciplinary Information Sciences*, **16** (2010) 55–66.

[4] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. of Math.*, **98** (1976) 263–284.

[5] R. Greenberg, On the structure of certain Galois groups, *Invent. Math.*, **47** (1978) 85–99.

[6] R. Greenberg, Iwasawa theory–past and present, *Adv. Stud. Pure Math.*, **30**, *Math. Soc.*, Japan, Tokyo (2001) 335–385.
[7] K. Iwasawa, Lectures on p-adic L-functions, Annals of Mathematics Studies, No. 74. Princeton University Press (1972).
[8] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, *Ann. Math.*, **98** (1973) 246–326.
[9] J. Minardi, Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields, Thesis, University of Washington (1986).
[10] M. Ozaki, A note on the capitulation in $\mathbb{Z}_p$-extensions, Proc. of the Japan Academy, Series A, *Math. Sciences*, **71** (1995) 218–219.
[11] M. Ozaki, The class group of $\mathbb{Z}_p$-extensions over totally real number fields, *Tôhoku Math. J.*, **49** (1997) 431–435.
[12] B. Perrin–Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa, Mémoires de la Société Mathématique de France, *Sér., 2*, **7** (1984) 1–130
[13] L. C. Washington, Introduction to cyclotomic fields, 2-nd edition, GTM **87**, Springer.
[14] J.-P., Wintenberger, Structure galoisienne de limites projectives d'unités locales, *Comp. Math.*, **42** (1980) 89–104.