New York Journal of Mathematics

New York J. Math. **28** (2022) 523–533.

On families of imaginary abelian fields with pseudo-null unramified Iwasawa modules

Satoshi Fujii

ABSTRACT. Let p be a prime number. We show that, there exists an infinite family of imaginary abelian fields such that, the Iwasawa module of the maximal multiple $\mathbb{Z}_p$-extension is non trivial and pseudo-null for each field in the family. We also discuss on an application to non-abelian Iwasawa theory in the sense of Ozaki.

CONTENTS

1. Introduction

All algebraic extensions of the field of rational numbers $\mathbb{Q}$ are assumed to be contained in a fixed algebraic closure of $\mathbb{Q}$. Let $k/\mathbb{Q}$ be a finite extension. For a prime number p, let $\mathbb{Z}_p$ be the ring of p-adic integers. Let $\tilde{k}$ be the composite field of all $\mathbb{Z}_p$-extensions of k. Then, by theorem 3 of [Iwa73] (see also theorem 13.4 of [Was97]), there exists a non negative integer δ such that $\mathrm{Gal}(\tilde{k}/k)$ is isomorphic to $\mathbb{Z}_p^{r_2+1+\delta}$ as a topological group, here r_2 denotes the number of complex primes of k. We should remark that if Leopoldt's conjecture for p and k holds then $\delta = 0$. It is known from Brumer's result [Bru67] that if k is contained in an abelian extension of an imaginary quadratic field then Leopoldt's conjecture for p and k holds, and hence $\tilde{k}/k$ is a $\mathbb{Z}_p^{r_2+1}$-extension.

Let $L_{\tilde{k}}/\tilde{k}$ be the maximal unramified abelian pro-p extension and put $X_{\tilde{k}} = \mathrm{Gal}(L_{\tilde{k}}/\tilde{k})$, which is often called the unramified Iwasawa module of $\tilde{k}$. The

Received July 12, 2021.
2010 *Mathematics Subject Classification.* 11R23.
Key words and phrases. Unramified Iwasawa modules, Greenberg's generalized conjecture.
This research was partly supported by JSPS KAKENHI Grant Numbers JP18K03259, JP19H01783.

ISSN 1076-9803/2022

Galois group $\mathrm{Gal}(\tilde{k}/k)$ acts on $X_{\tilde{k}}$ via the inner automorphism, and then, the complete group ring

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

of $\mathrm{Gal}(\tilde{k}/k)$ with coefficients in $\mathbb{Z}_p$ acts on $X_{\tilde{k}}$, the projective limit is taken with respect to restriction maps of Galois groups. It is shown that $X_{\tilde{k}}$ is a finitely generated torsion Λ-module, see theorem 1 of [Gre73]. A finitely generated torsion Λ-module M is called pseudo-null if the annihilator ideal of M over Λ is not contained in any height one prime ideals of Λ, and write $M \sim 0$ for pseudo-null Λ-modules M. For example, $M = 0$ is a pseudo-null module since the annihilator ideal of 0 is Λ. In [Gre01], Greenberg proposed the following conjecture.

Conjecture (Greenberg's generalized conjecture, [Gre01])**.** For each prime number p and each number field k, it holds that $X_{\tilde{k}} \sim 0$.

In [Gre76], Greenberg originally proposed so called Greenberg's conjecture (GC for short), which asserts the finiteness of the unramified Iwasawa module of the cyclotomic $\mathbb{Z}_p$-extension of totally real fields. Thereafter, Greenberg proposed the above conjecture. For $\mathbb{Z}_p$-extensions, on the unramified Iwasawa module, it is well known that the finiteness is equivalent to the pseudo-nullity. If Leopoldt's conjecture holds for a totally real field k and a prime number p, then the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of k. Hence, Greenberg's generalized conjecture (GGC for short) is in fact a generalization of GC in this sense. No counterexamples of GC and GGC have been found yet.

In this article, we will discuss on families of prime numbers p and number fields k such that $X_{\tilde{k}} \sim 0$. As we will see in section 2, it has been shown that, for each prime number p, there exist infinitely many imaginary quadratic fields k such that $X_{\tilde{k}} = 0$. The main result of this article is as follows.

Main Theorem (Theorem 2.7 of Section 2). *Let p be a prime number. Then there exist infinitely many imaginary abelian fields k such that $X_{\tilde{k}} \neq 0$ and $X_{\tilde{k}} \sim 0$.*

From theorem 1 of [Oza04], for each prime number p, there exist infinitely many cyclotomic $\mathbb{Z}_p$-extensions k_∞ of totally real fields k such that the Iwasawa module of k_∞/k is non trivial and finite, namely pseudo-null. In fact Ozaki has obtained a much stronger conclusion about the structure of Iwasawa modules. Although we cannot mention on the structure of $X_{\tilde{k}}$ here, we will prove that at least there is an infinite family of imaginary abelian fields with non trivial pseudo-null Iwasawa modules.

2. Examples of prime numbers and number fields

In this section, first, we introduce some results (propositions 2.2, 2.5, and 2.6, and corollary 2.3), which can be deduced directly from combining known

results. Second we present our main result (theorem 2.7). Let h_k be the class number of a number field k. Let P be a prime number or a finite prime of a number field. When P divides an integer b we write $P \mid b$, if not, we write $P \nmid b$.

Lemma 2.1 (See [Iwa56])**.** *Let p be a prime number. Let L/K be a finite p-extension of a finite extension $K/\mathbb{Q}$. Suppose that L/K is ramified at only one prime of K and is totally ramified. If $p \nmid h_K$ then $p \nmid h_L$.*

Let p be a prime number. It is known that $X_{\tilde{k}}$ is also defined to be the projective limit with respect to the norm maps of the p-Sylow subgroups of the ideal class groups of intermediate fields k' of $\tilde{k}/k$ which are finite over k. Hence if $p \nmid h_{k'}$ for each k' then $X_{\tilde{k}} = 0$. Assume that the prime number p does not split in $k/\mathbb{Q}$ and $p \nmid h_k$. Then, $\tilde{k}/k$ is totally ramified at the unique prime of k lying above p. By lemma 2.1 and $p \nmid h_k$, we have $p \nmid h_{k'}$. Hence we have the following.

Proposition 2.2. *Let p be a prime number and $k/\mathbb{Q}$ a finite extension. If p does not split in $k/\mathbb{Q}$ and if $p \nmid h_k$, then $X_{\tilde{k}} = 0$. In particular, $X_{\tilde{k}} \sim 0$.*

Let $k/\mathbb{Q}$ be a finite cyclic extension. There exist infinitely many prime numbers p such that, p does not divide the discriminant of k, $p \nmid h_k$, and that the Frobenius of p in $k/\mathbb{Q}$ generates $\mathrm{Gal}(k/\mathbb{Q})$. For such prime numbers p, it holds that $X_{\tilde{k}} = 0$ by proposition 2.2. Thus we have the following.

Corollary 2.3. *Let $k/\mathbb{Q}$ be a finite cyclic extension. Then there exist infinitely many prime numbers p such that $X_{\tilde{k}} = 0$.*

In the rest of Section 2, we discuss on the existence of families of number fields with pseudo-null Iwasawa modules for each prime number. Minardi proved the following result.

Proposition 2.4 (Minardi [Min86])**.** *Let p be a prime number and k an imaginary quadratic field. If $p \nmid h_k$, then $X_{\tilde{k}} \sim 0$.*

In particular, if k is an imaginary quadratic field of class number 1, then $X_{\tilde{k}} \sim 0$ for all prime numbers p.

Let $p = 2$. By Dirichlet's theorem, there exist infinitely many prime numbers q such that $q \equiv 7 \bmod 8$. Put $k = \mathbb{Q}(\sqrt{-q})$. Then, the prime 2 splits in k, and by genus theory we have $2 \nmid h_k$. Let $p = 3$. By Nakagawa–Horie's theorem [NH88], there exist infinitely many imaginary quadratic fields k such that the prime 3 splits in k and that $3 \nmid h_k$. Let $p \geq 5$. By Horie–Ônishi's theorem [HO88], there exist infinitely many imaginary quadratic fields k such that the prime p splits in k and that $p \nmid h_k$. Therefore, for each prime number p, there exist infinitely many of imaginary quadratic fields k in which p splits such that $p \nmid h_k$. We then have the following by proposition 2.4.

Proposition 2.5. *Let p be a prime number. Then, there exist infinitely many imaginary quadratic fields k such that p splits in k and that $X_{\tilde{k}} \sim 0$.*

By the way, in general, to understand whether $X_{\tilde{k}} = 0$ or not is difficult. For each prime number p, we can find an infinite family of imaginary quadratic fields k in which p splits such that $X_{\tilde{k}} = 0$. Let $\lambda_p(k)$ be the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of k. When $p = 2$, let q be a prime number with $q \equiv 7 \bmod 16$ and let $k = \mathbb{Q}(\sqrt{-q})$. As explained in the above, the prime number 2 splits in k, and it holds that $2 \nmid h_k$. By the result proved by Ferrero [Fer80] and by Kida [Kid79] independently, it holds that $\lambda_2(k) = 1$. For odd prime numbers p, thanks to works of Jochnowitz [Joc94], Byeon [Bye05] and Ito [Ito15], we can see that there exist infinitely many imaginary quadratic fields k in which p splits such that $\lambda_p(k) = 1$. It is known that, if a prime number p splits in an imaginary quadratic field k and if $\lambda_p(k) = 1$, then $X_{\tilde{k}} = 0$. Thus, we have the following.

Proposition 2.6. *Let p be a prime number. Then there exist infinitely many imaginary quadratic fields k in which p splits such that $X_{\tilde{k}} = 0$.*

We are then interested in finding families of number fields k such that $X_{\tilde{k}} \neq 0$ and $X_{\tilde{k}} \sim 0$. In this article, we show the following.

Theorem 2.7. *Let p be a prime number. Then there exist infinitely many imaginary abelian fields k such that $X_{\tilde{k}} \neq 0$ and $X_{\tilde{k}} \sim 0$.*

Some results on sufficient conditions of the pseudo-nullity of $X_{\tilde{k}}$ for abelian fields or CM-fields k under elementary situations have been obtained, see [Min86], [Itoh11] and [Fuj17]. However, as stated in the above, even if we know the pseudo-nullity of $X_{\tilde{k}}$, further to know whether $X_{\tilde{k}} = 0$ or not is basically difficult. Hence, the author thinks that what the existence of families of imaginary abelian fields of theorem 2.7 are guaranteed is important in the study of GGC. As we will see in the proof of theorem 2.7, we choose k as imaginary quadratic fields if $p = 2$, and as imaginary cyclic fields of degree $2p$ if $p > 2$. For each odd prime number p, to find an infinite family of imaginary quadratic fields k such that $X_{\tilde{k}} \neq 0$ and $X_{\tilde{k}} \sim 0$ is an interesting problem.

In section 3, we will give the proof of theorem 2.7. In section 4, we will give an application to non-abelian Iwasawa theory in the sense of Ozaki [Oza07].

3. Proof of theorem 2.7

In this section, we prove theorem 2.7. For a number field K and a prime number p, let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension and $\lambda_p(K)$ the Iwasawa λ-invariant of K_∞/K. We need the following well known lemma.

Lemma 3.1. *Let p be a prime number and $K/\mathbb{Q}$ a finite extension. Suppose that p splits completely in $K/\mathbb{Q}$. Then $\tilde{K}/K_\infty$ is an unramified abelian pro-p extension.*

Proof. Let $\mathfrak{p}$ be a prime of K lying above p and I the inertia subgroup of $\mathfrak{p}$ in $\tilde{K}/K$. Then $\mathfrak{p}$ is unramified in $K/\mathbb{Q}$ and has degree 1. This implies that $I \simeq \mathbb{Z}_p$. Since $K_\infty = K\mathbb{Q}_\infty$ and $\mathbb{Q}_\infty/\mathbb{Q}$ is totally ramified at p, K_∞/K is ramified at $\mathfrak{p}$. Thus the restriction map $I \to \mathrm{Gal}(K_\infty/K)$ is injective, and hence $\tilde{K}/K_\infty$ is

unramified at all primes lying above $\mathfrak{p}$. Since $\tilde{K}/K$ is unramified outside primes lying above p, we can conclude that $\tilde{K}/K_\infty$ is unramified at all primes. □

First, suppose that $p = 2$. Let q be a prime number such that $q \equiv 15 \bmod 16$ and put $k = \mathbb{Q}(\sqrt{-q})$. Then, the prime 2 splits in k, and by genus theory, we have $2 \nmid h_k$. Thus $X_{\tilde{k}}$ is a pseudo-null Λ-module by proposition 2.4. Furthermore, by the result of Ferrero [Fer80] and Kida [Kid79], it holds that $\lambda_2(k) \geq 3$. Since $\tilde{k}/k_\infty$ is an unramified $\mathbb{Z}_2$-extension by lemma 3.1, there is a surjective morphism $X_{\tilde{k}} \to \mathbb{Z}_2^2$. Therefore it holds that $X_{\tilde{k}} \neq 0$.

Next, suppose that $p \geq 3$. We show the following.

Theorem 3.2. *Let p be an odd prime number. Then there exist infinitely many imaginary cyclic fields k of degree $2p$ in which p splits completely such that $X_{\tilde{k}} \neq 0$ and $X_{\tilde{k}} \sim 0$.*

In principle, for each odd prime number p, we can find an imaginary abelian field k which satisfies the conditions of theorem 3.2.

From here, we begin the proof of theorem 3.2. Let p be an odd prime number. We need the following.

Proposition 3.3 (Theorem 1 of [Fuj17])**.** *Let p be an odd prime number, k a CM-field of degree greater than 2 and k^+ the maximal totally real subfield of k. Suppose that, the prime number p splits completely in $k/\mathbb{Q}$, $p \nmid h_k$, and all of the Iwasawa λ-, μ- and ν-invariants of the cyclotomic $\mathbb{Z}_p$-extension k_∞^+ of k^+ are 0. Then $X_{\tilde{k}} \sim 0$.*

Remark 3.4. (1) In [Itoh11], Itoh showed a result for quartic imaginary abelian fields precisely analogous to proposition 2.4. Proposition 3.3 is a generalization of Itoh's result.
(2) In theorem 1 of [Fuj17], the author put the assumption that Leopoldt's conjecture holds for p and k^+. The author must remark here that, if an odd prime number p splits completely in $k^+/\mathbb{Q}$, Leopoldt's conjecture for p and k^+ is implied by the vanishing of Iwasawa invariants λ and μ of k_∞^+/k^+, that is, GC for p and k holds. For this, see proposition 1 of [Oza97]. Hence, in theorem 1 of [Fuj17], the assumption on Leopoldt's conjecture is not needed.

By proposition 3.3, to prove theorem 3.2, it suffices to find infinitely many imaginary abelian fields k of degree $2p$ which satisfy the conditions of proposition 3.3 and $X_{\tilde{k}} \neq 0$.

When $p = 3$, put $F = \mathbb{Q}(\sqrt{-47})$. It is known that $h_F = 5$ (the author checked by using Pari/gp [Par18]). When $p \geq 5$, By Horie-Ônishi's result [HO88], there is an imaginary quadratic field F such that the prime p splits in $F/\mathbb{Q}$ and that $p \nmid h_F$. Alternatively, Ito [Ito15] showed that the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{1-p})$ and $\mathbb{Q}(\sqrt{4-p})$ are not divisible by p, see lemma 2.4 of [Ito15], hence we can choose F as $\mathbb{Q}(\sqrt{1-p})$ or $\mathbb{Q}(\sqrt{4-p})$. We fix once such an imaginary quadratic field F for each odd prime number p.

For a positive integer n, let μ_n be the group of n-th roots of unity. For each non-negative integer n and a number field K, let K_n be the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K.

Lemma 3.5. *Restrictions of Galois groups induce the following isomorphism*

$$\mathrm{Gal}(F\mathbb{Q}_1\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}) \simeq \mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}),$$

where $\mathbb{Q}_1$ denotes the 1-st layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Proof. Since $[F : \mathbb{Q}] = 2$ and $[\mathbb{Q}_1 : \mathbb{Q}] = p > 2$, it holds that $F \cap \mathbb{Q}_1 = \mathbb{Q}$. Note that $\mathbb{Q}(\mu_p)/\mathbb{Q}$ is abelian and $\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}$ is non-abelian. This implies that

$$(F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p, \sqrt[p]{p}) = (F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p).$$

Since $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p - 1$, it holds that $\mathbb{Q}_1 \nsubseteq (F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p)$. By the choice of F, if $F \subseteq (F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p)$, then F is a subfield of $\mathbb{Q}(\mu_p)$ decomposed at p. This is a contradiction because $\mathbb{Q}(\mu_p)/\mathbb{Q}$ is totally ramified at p. Hence $F \nsubseteq (F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p)$. Therefore, it holds that

$$(F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p, \sqrt[p]{p}) = (F\mathbb{Q}_1) \cap \mathbb{Q}(\mu_p) = \mathbb{Q}.$$

This completes the proof. □

By the Chebotarev density theorem and lemma 3.5, there exist infinitely many prime numbers ℓ such that all of the following three conditions are satisfied:

(1) ℓ is inert in $F/\mathbb{Q}$,
(2) ℓ is inert in $\mathbb{Q}_1/\mathbb{Q}$,
(3) ℓ splits completely in $\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}$.

We fix once such a prime number ℓ. For a finite prime $\mathfrak{q}$ of a number field, we identify finite primes and prime numbers when a number field is $\mathbb{Q}$, let $\mathbb{F}_\mathfrak{q}$ be the residue class field at $\mathfrak{q}$.

Lemma 3.6. *A prime number ℓ splits completely in $\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}$ if and only if the following two conditions are satisfied.*

- $\ell \equiv 1 \bmod p$.
- $p \bmod \ell \in (\mathbb{F}_\ell^\times)^p$.

Proof. Let $\mathfrak{L}$ be a prime of $\mathbb{Q}(\mu_p)$ lying above ℓ. The prime number ℓ splits completely in $\mathbb{Q}(\mu_p)$ if and only if $\ell \equiv 1 \bmod p$. The prime $\mathfrak{L}$ splits completely in $\mathbb{Q}(\mu_p, \sqrt[p]{p})$ if and only if the equation $X^p - p \equiv 0 \bmod \mathfrak{L}$ has a root in $\mathbb{F}_\mathfrak{L}$ since $\mathbb{Q}(\mu_p, \sqrt[p]{p})/\mathbb{Q}(\mu_p)$ is unramified at $\mathfrak{L}$. This assertion is equivalent to that $p \bmod \mathfrak{L} \in (\mathbb{F}_\mathfrak{L}^\times)^p$. Since $\mathfrak{L}$ has degree 1, we have $\mathbb{F}_\ell \simeq \mathbb{F}_\mathfrak{L}$. Hence $p \bmod \mathfrak{L} \in (\mathbb{F}_\mathfrak{L}^\times)^p$ if and only if $p \bmod \ell \in (\mathbb{F}_\ell^\times)^p$. □

By the condition (3) and lemma 3.6, there is the unique subfield k^+ of $\mathbb{Q}(\mu_\ell)$ such that $[k^+ : \mathbb{Q}] = p$ in which p splits completely. Since $k^+/\mathbb{Q}$ is unramified outside ℓ, it holds that $p \nmid h_{k^+}$ by lemma 2.1.

Let $n \geq 0$ be an integer. It is well known that $p \nmid h_{\mathbb{Q}_n}$ by lemma 2.1. By the condition (2), the prime ℓ remains a prime of $\mathbb{Q}_n$ for each n. Since $k_n^+/\mathbb{Q}_n$ is ramified at only the unique prime of $\mathbb{Q}_n$ lying above ℓ, it holds that $p \nmid h_{k_n^+}$ by lemma 2.1 for all n. This implies that all of Iwasawa invariants λ, μ and ν of k_∞^+/k^+ are 0.

Put $k = Fk^+$. From the choices of F and k^+, p splits completely in $k/\mathbb{Q}$. From the condition (1), the prime ℓ is inert in $F/\mathbb{Q}$. Since k/F is ramified at only the unique prime of F lying above ℓ and since $p \nmid h_F$, it holds that $p \nmid h_k$ by lemma 2.1. By combining all of the above arguments, we have seen that the imaginary cyclic field k of degree $2p$ satisfies all of the assumptions of proposition 3.3.

Finally, we show that $X_{\tilde{k}} \neq 0$. Since p splits completely in $k/\mathbb{Q}$, Leopoldt's conjecture holds for k and p, and since $[k : \mathbb{Q}] = 2p$, by lemma 3.1, it holds that $\tilde{k}/k_\infty$ is an unramified $\mathbb{Z}_p^p$-extension. Suppose that $p = 3$. By using Mizusawa's software [MizWeb], we find that $\lambda_3(F) = \lambda_3(\mathbb{Q}(\sqrt{-47})) = 2$. By Kida's formula [Kid80], one sees that $\lambda_3(k) = 6$. As stated in the above, it holds that $\tilde{k}/k_\infty$ is an unramified $\mathbb{Z}_3^3$-extension, and therefore, there is a surjective morphism $X_{\tilde{k}} \to \mathbb{Z}_3^3$. In particular, we have $X_{\tilde{k}} \neq 0$.

Suppose that $p > 3$. For an algebraic extension $K/\mathbb{Q}$ and a prime number p, let X_K be the Galois group of the maximal unramified abelian pro-p extension of K. When $K/\mathbb{Q}$ is finite, let γ be a topological generator of $\mathrm{Gal}(K_\infty/K)$, and put $R = \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$. We need the following two lemmas.

Lemma 3.7. *Let p be a prime number and let $K/\mathbb{Q}$ be a finite extension. Let r_1 and r_2 be the number of real primes and the number of complex primes of K respectively. For each non negative integer n, let E_n be the unit group of K_n. Let $E = \varprojlim_n E_n \otimes \mathbb{Z}_p$ be the projective limit of modules $E_n \otimes \mathbb{Z}_p$ with respect to the norm maps. Suppose that K_∞/K is totally ramified at all primes of K lying above p. Then the $\mathbb{Z}_p$-rank of $E/(\gamma - 1)E$ is $r_1 + r_2$.*

Remark 3.8. Lemma 3.7 can be deduced from theorem 10.3.25 and theorem 11.3.11 of [NSW08]. Because we need only to know the $\mathbb{Z}_p$-rank of $E/(\gamma - 1)E$ here, we prefer to prove lemma 3.7 briefly.

Proof. For a R-module M, let $M^{\mathrm{Gal}(K_\infty/K)}$ be the maximal submodule of M on which $\mathrm{Gal}(K_\infty/K)$ acts trivially. For each non negative integer n, let $U_{\mathfrak{p}_n}$ be the principal local unit group at a prime $\mathfrak{p}_n$ of K_n lying above p, and let $U = \varprojlim_n \oplus_{\mathfrak{p}_n|p} U_{\mathfrak{p}_n}$ be the projective limit of modules $\oplus_{\mathfrak{p}_n|p} U_{\mathfrak{p}_n}$ with respect to the norm maps. By theorem 25 of [Iwa73], we can see that U is a finitely generated R-module of rank $[K : \mathbb{Q}] = r_1 + 2r_2$, and $U^{\mathrm{Gal}(K_\infty/K)} = 0$. Let $\mathfrak{X}$ be the Galois group of the maximal abelian pro-p extension over K_∞ unramified outside all primes lying above p. By class field theory and by remark 2 of theorem 4.2 of [Kuz73], there is the following exact sequence

$$0 \to E \to U \to \mathfrak{X} \to X_{K_\infty} \to 0$$

of R-modules. It is well known that the R-rank of $\mathfrak{X}$ is r_2, see theorem 17 of [Iwa73] (see also theorem 13.31 of [Was97]). Combining the above, since X_{K_∞} is a torsion R-module, we find that E is a finitely generated R-module of rank $r_1 + r_2$, and that $E^{\mathrm{Gal}(K_\infty/K)} = 0$. In particular, E has no non trivial finite R-submodules.

Let $T_R E$ be the R-submodule of E which consists of all R-torsion elements of E. By the structure theorem of R-modules, we have an injective morphism $E \to R^{r_1+r_2} \oplus T_R E$ with a finite cokernel. Then we have an exact sequence

$$(\text{finite}) \to E/(\gamma-1)E \to \mathbb{Z}_p^{r_1+r_2} \oplus T_R E/(\gamma-1)T_R E \to (\text{finite})$$

of $\mathbb{Z}_p$-modules. Since $E^{\mathrm{Gal}(K_\infty/K)} = 0$, we find that $T_R E/(\gamma-1)T_R E$ is finite. Therefore the $\mathbb{Z}_p$-rank of $E/(\gamma-1)E$ is $r_1 + r_2$. □

Lemma 3.9. *Let p be a prime number and $K/\mathbb{Q}$ a totally imaginary finite extension in which the prime number p splits completely. Assume that Leopoldt's conjecture for p and K holds. Then we have $[K : \mathbb{Q}] \leq 6$ if $X_{\tilde{K}} = 0$.*

Proof. For an algebraic extension $L/\mathbb{Q}$, not necessary finite, let $\mathcal{G}_L$ be the Galois group of the maximal unramified pro-p extension of L. It holds that $[K : \mathbb{Q}] = 2r_2$. By lemma 3.1, $\mathcal{G}_{\tilde{K}}$ is a closed normal subgroup of $\mathcal{G}_{K_\infty}$, and it holds that

$$\mathcal{G}_{K_\infty}/\mathcal{G}_{\tilde{K}} \simeq \mathrm{Gal}(\tilde{K}/K_\infty).$$

Assume that $X_{\tilde{K}} = 0$. By pro-p version of Burnside's basis theorem, if $X_{\tilde{K}} = 0$ then $\mathcal{G}_{\tilde{K}} = 1$. By lemma 3.1, it holds that

$$\mathcal{G}_{K_\infty} = X_{K_\infty} = \mathrm{Gal}(\tilde{K}/K_\infty) \simeq \mathbb{Z}_p^{r_2},$$

since Leopoldt's conjecture for p and K holds. Note that $\mathrm{Gal}(K_\infty/K)$ acts on X_{K_∞} trivially since $\tilde{K}/K$ is abelian.

By theorem C of [Oza07] for $i = 2$, since $\mathcal{G}_{K_\infty} = X_{K_\infty}$, we have a surjective morphism

$$E \to H_2(X_{K_\infty}, \mathbb{Z}_p) \simeq X_{K_\infty} \wedge X_{K_\infty},$$

of R-modules, where the exterior product $\wedge$ is taken over $\mathbb{Z}_p$. The action of γ on $x \wedge y \in X_{K_\infty} \wedge X_{K_\infty}$ is given by

$$\gamma(x \wedge y) = (\gamma x) \wedge (\gamma y).$$

Since $\mathrm{Gal}(K_\infty/K)$ acts on X_{K_∞} trivially, the above morphism factors through $E/(\gamma-1)E$. Thus, since

$$X_{K_\infty} \wedge X_{K_\infty} \simeq \mathbb{Z}_p^{\frac{r_2(r_2-1)}{2}},$$

we also have a surjective morphism

$$E/(\gamma-1)E \to \mathbb{Z}_p^{\frac{r_2(r_2-1)}{2}}.$$

By the assumption that K is totally imaginary and by lemma 3.7, the $\mathbb{Z}_p$-rank of $E/(\gamma-1)E$ is equal to r_2. This implies that

$$\frac{r_2(r_2-1)}{2} \leq r_2.$$

Therefore we have $[K:\mathbb{Q}] = 2r_2 \leq 6$. □

We finish the proof of theorem 3.2. By our assumption that $p > 3$, it holds that $[k:\mathbb{Q}] = 2p > 6$. By lemma 3.9, we have $X_{\tilde{k}} \neq 0$. Since there are infinitely many prime numbers such as ℓ, this completes the proof of theorem 3.2. □

Remark. Okano [Oka12] has obtained a result stricter than lemma 3.9 for certain imaginary abelian fields. In fact, the non-triviality of $X_{\tilde{k}}$ is also deduced from theorem 1.2 of [Oka12] when $p > 3$.

4. Non-freeness conjecture

We give an application to non-abelian Iwasawa theory in the sense of Ozaki [Oza07]. Let p be a prime number and k_∞/k the cyclotomic $\mathbb{Z}_p$-extension of a number field k. Recall we have denoted by $\mathcal{G}_{k_\infty}$ the Galois group of the maximal unramified pro-p extension over k_∞ in the proof of lemma 3.9. In his lecture [OzaSem], Ozaki proposed the following conjecture.

Conjecture (Non-freeness Conjecture [OzaSem])**.** For each prime number p and each finite extension $k/\mathbb{Q}$, the group $\mathcal{G}_{k_\infty}$ never be a non-abelian free pro-p group.

Each abelian free pro-p group is isomorphic to $\mathbb{Z}_p$. We have checked that there exist infinitely many imaginary quadratic fields k in which p splits such that $X_{k_\infty} \simeq \mathbb{Z}_p$ for each prime number p, and hence $\mathcal{G}_{k_\infty} \simeq \mathbb{Z}_p$, see proposition 2.6.

In [Fuj11], the author showed following.

Lemma 4.1 ([Fuj11])**.** *Let p be a prime number and $k/\mathbb{Q}$ a finite extension. If a prime number p splits completely in k and $X_{\tilde{k}} \sim 0$, then $\mathcal{G}_{k_\infty}$ is not a non-abelian free pro-p group.*

As a consequence of lemma 4.1, the proof of theorem 2.7 and results given by several authors, we have the following.

Corollary 4.2. *Let p be a prime number. Then there exist infinitely many imaginary abelian fields k satisfying the following three conditions.*
(1) *The prime number p splits completely in $k/\mathbb{Q}$.*
(2) *$\mathcal{G}_{k_\infty}$ is a non-abelian pro-p group.*
(3) *$\mathcal{G}_{k_\infty}$ is not a free pro-p group.*

Proof. Let $p = 2$ and q be a prime number with $q \equiv 31 \bmod 32$. Put $k = \mathbb{Q}(\sqrt{-q})$. Then, by proposition 2.4, $X_{\tilde{k}}$ is a pseudo-null Λ-module. Hence, by lemma 4.1, $\mathcal{G}_{k_\infty}$ is not a non-abelian free pro-2 group. Further, by theorem 2 of [MO10], $\mathcal{G}_{k_\infty}$ is not abelian.

Let $p \geq 3$. We have checked that $X_{\tilde{k}}$ is a pseudo-null Λ-module. By lemma 4.1, $\mathcal{G}_{k_\infty}$ is not a non-abelian free pro-p group. By theorem 1.2 of [Oka12], $\mathcal{G}_{k_\infty}$ is not abelian, since $\lambda_3(F) = 2$ when $p = 3$. □

Acknowledgments

The author would like to express his thanks to Takuya Yamauchi, the study of this article was motivated by questions from Yamauchi to the author.

References

[Bru67] BRUMER, ARMAND. On the units of algebraic number fields. *Mathematika*. **14** (1967), 121–124. MR0220694, Zbl 0171.01105, doi: 10.1112/S0025579300003703. 523

[Bye05] BYEON, DONGHO. Imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1. *Acta Arith.* **120** (2005), no. 2, 145–152. MR2187784, Zbl 1165.11339, doi: 10.4064/aa120-2-2. 526

[Fer80] FERRERO, BRUCE. The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields. *Amer. J. Math.* **102** (1980), no. 3, 447–459. MR0573095, Zbl 0463.12002, doi: 10.2307/2374108. 526, 527

[Fuj11] FUJII, SATOSHI. 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, 101–110. MR2805623, Zbl 1250.11094, doi: 10.4064/aa149-2-1. 531

[Fuj17] FUJII, SATOSHI. On Greenberg's generalized conjecture for CM-fields. *J. Reine Angew. Math.* **731** (2017), 259–278. MR3709067, Zbl 1400.11140, doi: 10.1515/crelle-2014-0148. 526, 527

[Gre73] GREENBERG, RALPH. The Iwasawa invariants of Γ-extensions of a fixed number field. *Amer. J. Math.* **95** (1973), 204–214. MR0332712, Zbl 0268.12005, doi: 10.2307/2373652. 524

[Gre76] GREENBERG, RALPH. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.* **98** (1976), no. 1, 263–284. MR0401702, Zbl 0334.12013, doi: 10.2307/2373625. 524

[Gre01] GREENBERG, RALPH. Iwasawa theory–past and present. *Class field theory–its centenary and prospect* (Tokyo, 1998), 335–385, Adv. Stud. Pure Math., 30. *Math. Soc. Japan, Tokyo*, 2001. MR1846466, Zbl 0998.11054. 524

[HO88] HORIE, KUNIAKI; ÔNISHI, YOSHIHIRO. The existence of certain infinite families of imaginary quadratic fields. *J. Reine Angew. Math.* **390** (1988), 97–113. MR0953679, Zbl 0638.12001. 525, 527

[Ito15] ITO, AKIKO. On certain infinite families of imaginary quadratic fields whose Iwasawa λ-invariant is equal to 1. *Acta Arith.* **168** (2015), no. 4, 301–340. MR3352436, Zbl 1390.11124, arXiv:1212.1392, doi: 10.4064/aa168-4-1. 526, 527

[Itoh11] ITOH, TSUYOSHI. On multiple $\mathbb{Z}_p$-extensions of imaginary abelian quartic fields. *J. Number Theory* **131** (2011), no. 1, 59–66. MR2729209, Zbl 1211.11119, doi: 10.1016/j.jnt.2010.08.001. 526, 527

[Iwa56] IWASAWA, KENKICHI. A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258. MR0083013, Zbl 0074.03002, doi: 10.1007/BF03374563. 525

[Iwa73] IWASAWA, KENKICHI. On $\mathbb{Z}_\ell$-extensions of algebraic number fields. *Ann. Math.* (2) **98** (1973), 246–326. MR0349627, Zbl 0285.12008, doi: 10.2307/1970784. 523, 529, 530

[Joc94] JOCHNOWITZ, NAOMI. A p-adic conjecture about derivatives of L-series attached to modular forms. *p-adic monodromy and the Birch and Swinnerton–Dyer conjecture.* (Boston, MA, 1991), 239–263. *Contemp. Math.*, 165. *Amer. Math. Soc., Providence, RI*, 1994. MR1279612, Zbl 0869.11040. 526

[Kid79] KIDA, YÛJI. On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields. *Tohoku Math. J.* (2) **31** (1979), no. 1, 91–96. MR0526512, Zbl 0408.12006, doi: 10.2748/tmj/1178229880. 526, 527

[Kid80] KIDA, YÛJI. l-extensions of CM-fields and cyclotomic invariants. *J. Number Theory* **12** (1980), no. 4, 519–528. MR0599821, Zbl 0455.12007, doi: 10.1016/0022-314X(80)90042-6. 529

[Kuz73] KUZ'MIN, LEONID V. The Tate module for algebraic number fields. *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 267 –327; translation in *Math. USSR, Izv.* **6** (1972), 263-321. MR0304353, Zbl 0257.12003, doi: 10.1070/IM1972v006n02ABEH001875. 529

[Min86] MINARDI, JOHN VICTOR. Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields. Thesis (Ph.D.)-University of Washington. 1986. 77 pp. MR2635492. 525, 526

[MizWeb] MIZUSAWA, YASUSHI. Computing Iwasawa polynomials by PARI/GP. Preprint, available at http://mizusawa.web.nitech.ac.jp/Iwapoly/index.html. 529

[MO10] MIZUSAWA, YASUSHI; OZAKI, MANABU. Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields. *Math. Ann.* **347** (2010), no. 2, 437–453. MR2606944, Zbl 1239.11121, doi: 10.1007/s00208-009-0431-8. 531

[NH88] NAKAGAWA, JIN; HORIE, KUNIAKI. Elliptic curves with no rational points. *Proc. Amer. Math. Soc.* **104** (1988), no. 1, 20–24. MR0958035, Zbl 0663.14023, doi: 10.2307/2047452. 525

[NSW08] NEUKIRCH, JÜRGEN; SCHMIDT, ALEXANDER; WINGBERG, KAY. Cohomology of number fields. 2nd ed. Grundlehren der Mathematischen Wissenschaften, 323. *Springer-Verlag, Berlin*, 2008. xvi+825 pp. ISBN: 978-3-540-37888-4. MR2392026, Zbl 1136.11001 529

[Oka12] OKANO, KEIJI. The commutativity of the Galois groups of the maximal unramified pro-p-extensions over the cyclotomic $\mathbb{Z}_p$-extensions. *J. Number Theory* **132** (2012), no. 4, 806–819. MR2887619, Zbl 1287.11125, doi: 10.1016/j.jnt.2011.08.006. 531, 532

[Oza97] OZAKI, MANABU. The class group of $\mathbb{Z}_p$-extensions over totally real number fields. *Tohoku Math. J.* (2) **49** (1997), no. 3, 431–435. MR1464188, Zbl 0896.11044, doi: 10.2748/tmj/1178225114. 527

[Oza04] OZAKI, MANABU. Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa modules. *J. Math. Soc. Japan* **56** (2004), no. 3, 787–801. MR2071673, Zbl 1142.11368, doi: 10.2969/jmsj/1191334086. 524

[Oza07] OZAKI, MANABU. Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions. *J. Reine Angew. Math.* **602** (2007), 59–94. MR2300452, Zbl 1123.11034, doi: 10.1515/CRELLE.2007.003. 526, 530, 531

[OzaSem] OZAKI, MANABU. On the maximal unramified p-extension over $\mathbb{Z}_p$-extensions. A lecture given in Waseda Number Theory Seminar. 5th October 2018. 531

[Par18] THE PARI GROUP. PARI/GP version `2.9.4`, Univ. Bordeaux, 2018. http://pari.math.u-bordeaux.fr. 527

[Was97] WASHINGTON, LAWRENCE C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1997. xiv+487 pp. ISBN: 0-387-94762-0. MR1421575, Zbl 0966.11047. 523, 530

(Satoshi Fujii) FACULTY OF EDUCATION, SHIMANE UNIVERSITY, 1060 NISHIKAWATSUCHO, MATSUE, SHIMANE, 690–8504, JAPAN
fujiisatoshi@edu.shimane-u.ac.jp
mophism@gmail.com

This paper is available via http://nyjm.albany.edu/j/2022/28-20.html.