ON THE STRUCTURE OF THE GALOIS GROUP OF THE MAXIMAL PRO-$p$ EXTENSION WITH RESTRICTED RAMIFICATION OVER THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSION

TSUYOSHI ITOH

Abstract. Let $k_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of an algebraic number field $k$. We denote by $S$ a finite set of prime numbers which does not contain $p$, and $S(k_\infty)$ the set of primes of $k_\infty$ lying above $S$. In the present paper, we will study the structure of the Galois group $\mathcal{X}_S(k_\infty)$ of the maximal pro-$p$ extension unramified outside $S(k_\infty)$ over $k_\infty$. We mainly consider the question whether $\mathcal{X}_S(k_\infty)$ is a non-abelian free pro-$p$ group or not. In the former part, we treat the case when $k$ is an imaginary quadratic field and $S = \emptyset$ (here $p$ is an odd prime number which does not split in $k$). In the latter part, we treat the case when $k$ is a totally real field and $S \neq \emptyset$.

1. Introduction

1.1. Maximal unramified pro-$p$ extension over the cyclotomic $\mathbb{Z}_p$-extension. Let $p$ be an arbitrary prime number, and $k_\infty/k$ the cyclotomic $\mathbb{Z}_p$-extension of an algebraic number field. We denote by $\mathcal{L}(k_\infty)/k_\infty$ the maximal unramified pro-$p$ extension, and put $\mathcal{X}(k_\infty) = \text{Gal}(\mathcal{L}(k_\infty)/k_\infty)$. For the structure of $\mathcal{X}(k_\infty)$, there are many studies ([37], [39], [40], [32], [34], [7], etc.). Concerning this, the following conjecture is considered (see, e.g., [45], p.298, [7], p.101).

Conjecture A. Let the notation be as above. Then $\mathcal{X}(k_\infty)$ is not a “non-abelian free pro-$p$ group”.

At this time, there seems to be no counter-examples for Conjecture A (see also [44], p.32, Remark). In particular, when $p$ splits completely in $k$, “Greenberg’s generalized conjecture” ([12], Conjecture (3.5)) for $k$ and $p$ implies Conjecture A for $k$ and $p$ (see [7], Main Theorem 1.2).

Let $L(k_\infty)/k_\infty$ be the maximal unramified abelian pro-$p$ extension. Then, $X(k_\infty) = \text{Gal}(L(k_\infty)/k_\infty)$ is a fundamental research object in Iwasawa theory. This is also the maximal abelian pro-$p$ quotient of $\mathcal{X}(k_\infty)$, and is an important object to study Conjecture A. Especially, Conjecture A holds when $\mathcal{X}(k_\infty)$ has a non-trivial $\mathbb{Z}_p$-torsion element (see also [7], p.104).

When $p = 2$, M. Ozaki announced that Conjecture A holds for most imaginary quadratic fields. Inspired by his study, the author conducted the study of the present paper. (Several ideas in the present paper were learned from Ozaki’s talk.)

1.2. Criteria for imaginary quadratic fields. Let $k$ be an imaginary quadratic field and $p$ an odd prime number. Assume that $k$ and $p$ satisfy both of the following conditions:

(C1) $p$ does not split in $k$,
(C2) the class number $h(k)$ of $k$ is divisible by $p$.

2010 Mathematical Subject Classification. 11R23.
Date: December 18, 2018.
We recall some properties of $X(k_\infty)$ in this case. Denote by $\lambda(k)$ the Iwasawa $\lambda$-invariant of $k_\infty/k$. Since $p$ is odd, it is well known that $X(k_\infty)$ is isomorphic to $\mathbb{Z}_p^{\oplus \lambda(k)}$ as a $\mathbb{Z}_p$-module (see, e.g., [39, p.82], [47]). Thus, to verify Conjecture A, we need more information. Since $k$ satisfies (C2), we see that $\lambda(k) \geq 1$. (We note that $X(k_\infty)$ is an abelian free pro-$p$ group when $\lambda(k)$ is 0 or 1.)

Let $K/k$ be an unramified cyclic extension of degree $p$. By considering the action of $\text{Gal}(K/Q)$ on the Sylow $p$-subgroup of the ideal class group of $k$, we can show that $K$ is a Galois extension over $Q$, and $\text{Gal}(K/Q)$ is isomorphic to the dihedral group of order $2p$. Let $F$ be an intermediate field of $K/Q$ of degree $p$. We denote by $\lambda(F)$ the Iwasawa $\lambda$-invariant of the cyclotomic $\mathbb{Z}_p$-extension $F_\infty/F$. We can obtain the following criterion for Conjecture A (the proof will be given in Section 2.2).

**Theorem 1.2.1.** Let $k$ be an imaginary quadratic field and $p$ an odd prime number. Assume that $k$ and $p$ satisfy (C1) and (C2). Let $K/k$ be an unramified cyclic extension of degree $p$, and $F$ an intermediate field of $K/Q$ of degree $p$. Assume also that $\lambda(k) \geq 2$. If

$$\lambda(F) \leq \frac{(p-1)\lambda(k)-p}{2},$$

then $X(k_\infty)$ is not a free pro-$p$ group.

When $p = 3$, we can also obtain another criterion for Conjecture A. Assume that $k$ and $3(=p)$ satisfy (C1) and (C2). Then, the above $F$ is a cubic (non-Galois) extension over $Q$. We note that the unique prime of $k$ lying above 3 splits completely in $K$. From this, we see that there are exactly two primes lying above 3 in $F$, and they are totally ramified in $F_\infty$. For an integer $n \geq 0$, let $F_n$ be the $n$th layer of $F_\infty/F$ (note that $F_0 = F$). We denote by $p_n$, $p_n'$ the primes of $F_n$ lying above 3. Let $A(F_n)$ be the Sylow 3-subgroup of the ideal class group of $F_n$. We put

$$D(F_n) = \langle c(p_n), c(p_n') \rangle \cap A(F_n),$$

where $c(p_n)$ (resp. $c(p_n')$) is the ideal class containing $p_n$ (resp. $p_n'$). The second criterion is the following:

**Theorem 1.2.2.** Assume that $p = 3$. Let $k$ be an imaginary quadratic field satisfying (C1) and (C2), $K/k$ an unramified cyclic cubic extension, and $F$ an intermediate field of $K/Q$ of degree 3. If $D(F_n)$ is not trivial for some $n \geq 0$, then $X(k_\infty)$ is not a free pro-3 group.

The above theorem seems close to Ozaki’s result [39, Proposition 5]. Note that our proof of the above theorem uses different tools from Ozaki’s. (See also Section 3.3) This theorem will be shown in Section 2.3.

1.3. Several results around Conjecture A. In Sections 2.4 and 2.5, we will give results obtained from the study of Conjecture A.

Let $k$ be an imaginary quadratic field and $p$ an odd prime number which satisfies (C1) and (C2), and take $K$, $F$ similarly as above. Separately from the validity of Conjecture A, we are also concerned with the structure of $X(F_\infty)$ itself. We will give a result which relates $X(F_\infty)$ to $\lambda(k)$. Before stating this, we shall introduce the following additional condition:

(C3) the Sylow $p$-subgroup $A(k)$ of the ideal class group of $k$ is cyclic.
We will show the following theorem in Section 2.4. This theorem can be shown by using Lemmermeyer’s results given in [30].

**Theorem 1.3.1.** Let \( k \) be an imaginary quadratic field and \( p \) an odd prime number. Assume that \( k \) and \( p \) satisfy (C1), (C2), and (C3). We denote by \( K/k \) the unique unramified cyclic extension of degree \( p \), and \( F \) an intermediate field of \( K/\mathbb{Q} \) of degree \( p \). Then, \( \lambda(k) = 1 \) if and only if \( X(F_\infty) \) is trivial.

The above theorem slightly relates to our criteria for Conjecture A (Theorems 1.2.1 and 1.2.2). See the last paragraph of Section 3.2.

When \( p = 3 \), Theorem 1.3.1 can be reformulated as the following. In this case, \( F \) is a cubic field (and it is not totally real). Let \( E(F) \) be the group of units in \( F \). Since the free rank of \( E(F) \) is 1, we can take a unit \( \varepsilon_F \) which satisfies \( E(F) = \langle -1, \varepsilon_F \rangle \). As noted before, there are two primes lying above 3 in \( F \). We also see that one of such a prime \( p \) satisfies \( F_p = \mathbb{Q}_3 \) (i.e., the local degree at \( p \) is 1). Then we can obtain the following corollary by using Hachimori’s result given in [13] (for the details, see Section 2.4).

**Corollary 1.3.2.** Let the assumptions be as in Theorem 1.3.1. Moreover, assume that \( p = 3 \). Then, \( \lambda(k) = 1 \) if and only if \( \varepsilon_F^2 \not\equiv 1 \pmod{p^2} \).

This corollary says that a property of a certain unit of \( F \) determines whether \( \lambda(k) = 1 \) or \( \lambda(k) > 1 \) (when \( p = 3 \)). (Note that there is another criterion. See [28, Theorem 1]. See also [14].)

In Section 2.5, we consider a question whether \( X(k_\infty) \) is a Demuškin group or not. For this question, we will give a result similar to Theorem 1.2.1.

In Section 3, we shall give some computational results.

1.4. \( S \)-ramified analog of Conjecture A. We shall return to the general case. That is, \( p \) is an arbitrary prime number, and \( k_\infty/k \) the cyclotomic \( \mathbb{Z}_p \)-extension of an algebraic number field. Let \( S \) be a finite set of prime numbers, and \( k(k) \) (resp. \( S(k_\infty) \)) the set of primes of \( k \) (resp. \( k_\infty \)) lying above the prime numbers in \( S \). Assume that \( S \) does not contain \( p \). Let \( L_S(k_\infty)/k_\infty \) be the maximal pro-\( p \) extension unramified outside \( S(k_\infty) \). (We mention that \( L_S(k_\infty)/k_\infty \) is unramified at archimedean primes.) Put \( X_S(k_\infty) = \text{Gal}(L_S(k_\infty)/k_\infty) \). In this situation, we will consider a question similar to Conjecture A (see also [8, Section 5]).

**Question B.** Let the notation and the assumption be as above (in particular, \( p \not\in S \)). Can \( X_S(k_\infty) \) be a non-abelian free pro-\( p \) group?

Let \( \mathbb{B}_\infty \) be the cyclotomic \( \mathbb{Z}_p \)-extension \( \mathbb{Q} \). When \( p \) is odd, it is known that if \( X_S(\mathbb{B}_\infty) \) is not trivial, then it is not a free pro-\( p \) group ([8, Corollary 5.1]). This result follows from the fact that the maximal abelian pro-\( p \) quotient of \( X_S(\mathbb{B}_\infty) \) has a non-trivial \( \mathbb{Z}_p \)-torsion element when it is not trivial ([8, Theorem 1.1]). Note also that some partial results for imaginary quadratic fields are given in [8]. Moreover, [14] also gave results concerning Question B. (For the structure of \( X_S(k_\infty) \) and related topics, see also [41], [42], [33], [17], [33], etc.)

In the present paper, we shall consider Question B when \( k' \) is a totally real field. (We use the symbol \( k' \) for a totally real field because \( k \) is used as an imaginary quadratic field in Sections 2 and 3.) First, we will relate the above question to Greenberg’s conjecture (see [13]) which states that \( X(k'_\infty) \) is finite if \( k' \) is totally real. In Section 4, we shall show the following result.
Theorem 1.4.1. Let \( p \) be an (arbitrary) prime number, \( k' \) a totally real number field, and \( S \) a finite set of prime numbers which does not contain \( p \). Assume that there is an infinite Galois extension \( \mathbb{L}/k'_\infty \) unramified outside \( S(k'_\infty) \) such that \( G = \text{Gal}(\mathbb{L}/k'_\infty) \) is a finitely generated pro-\( p \) group and satisfies either of the following conditions:

(F) \( G \) is a free pro-\( p \) group with \( d(G) \geq 2 \), or
(D) \( G \) is a Demuškin group with \( d(G) \geq 3 \).

(Here, \( d(G) \) denotes the generator rank of \( G \).) Then, there is a totally real number field \( k'' \) such that \( X(k''_\infty) \) is not finite (i.e., a counter-example for Greenberg’s conjecture exists).

In particular, if \( \mathcal{X}_S(k'_\infty) \) is a finitely generated “non-abelian” free pro-\( p \) group for some totally real field \( k' \), then Greenberg’s conjecture fails. Hence it seems significant to determine whether \( \mathcal{X}_S(k'_\infty) \) is a free pro-\( p \) group or not. (Note that if \( \mathcal{X}_S(k'_\infty) \) is not finitely generated, then \( X(k'_\infty) \) is not finitely generated as a \( \mathbb{Z}_p \)-module. See, e.g., [18, p.1494].)

In Section 5 we shall consider Question B in the case of real quadratic fields (with odd \( p \)). Let \( k' \) be a real quadratic field, and \( k'_\infty/k' \) the cyclotomic \( \mathbb{Z}_p \)-extension. We put \( X_S(k'_\infty) = \text{Gal}(L_S(k'_\infty)/k'_\infty) \) (resp. \( X_S(k') = \text{Gal}(L_S(k')/k') \)), where \( L_S(k'_\infty)/k'_\infty \) (resp. \( L_S(k')/k' \)) is the maximal abelian pro-\( p \) extension unramified outside \( S(k'_\infty) \) (resp. \( S(k') \)).

When \( X_S(k'_\infty) \) is trivial or \( X_S(k'_\infty) \) contains a non-trivial \( \mathbb{Z}_p \)-torsion element, then \( \mathcal{X}_S(k'_\infty) \) is a non-abelian free pro-\( p \) group. Unfortunately, there is a case that \( \mathcal{X}_S(k'_\infty) \) is not trivial and has no non-trivial \( \mathbb{Z}_p \)-torsion elements. (For this topic, see [16].) We will consider the above question for such a case. In the present paper, we show the following:

Theorem 1.4.2. Let \( k' \) be a real quadratic field and \( p \) an odd prime number. Assume that \( p \) is inert in \( k' \), and \( p \) does not divide the class number of \( k' \). Let \( r \) be a positive integer satisfying \( r \geq 3 \), and \( S = \{q_1, q_2, q_3, \ldots, q_r\} \) a set of \( r \) distinct prime numbers. Suppose that

\[ q_i \text{ is inert in } k', \quad q_i \equiv -1 \pmod{p}, \quad \text{and} \quad q_i^2 \not\equiv 1 \pmod{p^2} \]

for \( i = 1, 2, 3, \ldots, r \). Suppose also that both \( X_{\{q_1\}}(k') \) and \( X_{\{q_2\}}(k') \) are trivial. Then \( \mathcal{X}_S(k'_\infty) \) is not a free pro-\( p \) group.

Under the assumptions of the above theorem, we see that \( X_S(k'_\infty) \cong \mathbb{Z}_p^r \) as a \( \mathbb{Z}_p \)-module (see Lemma 5.1.1).

1.5. Notation. Let \( p \) be an arbitrary prime number. In this subsection, \( \mathcal{K} \) is an algebraic extension of \( \mathbb{Q} \), and \( S \) is a finite set of prime numbers not containing \( p \). (We assume that all algebraic extensions of \( \mathbb{Q} \) are embedded in \( \mathbb{C} \) under a fixed embedding.) Let \( S(\mathcal{K}) \) be the set of primes of \( \mathcal{K} \) lying above \( S \). We will use the following notation:

- \( \mathcal{L}_S(\mathcal{K})/\mathcal{K} \): the maximal pro-\( p \) extension unramified outside \( S(\mathcal{K}) \),
- \( \mathcal{X}_S(\mathcal{K}) = \text{Gal}(\mathcal{L}_S(\mathcal{K})/\mathcal{K}) \),
- \( L_S(\mathcal{K})/\mathcal{K} \): the maximal abelian pro-\( p \) extension unramified outside \( S(\mathcal{K}) \), and
- \( X_S(\mathcal{K}) = \text{Gal}(L_S(\mathcal{K})/\mathcal{K}) \).

For simplicity, we shall write \( \mathcal{L}(\mathcal{K}), \mathcal{X}(\mathcal{K}), L(\mathcal{K}), X(\mathcal{K}) \) instead of \( \mathcal{L}_0(\mathcal{K}), \mathcal{X}_0(\mathcal{K}), L_0(\mathcal{K}), X_0(\mathcal{K}) \), respectively.

We denote by \( \mathbb{B}_\infty \) the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \). When \( \mathcal{K} \) is a finite extension of \( \mathbb{Q} \), we will define the following notation:

- \( h(\mathcal{K}) \): the class number of \( \mathcal{K} \),
- \( A(\mathcal{K}) \): the Sylow \( p \)-subgroup of the ideal class group of \( \mathcal{K} \) (\( A(\mathcal{K}) \cong X(\mathcal{K}) \) by class field theory),
• $E(K)$: the group of units in $K$,
• $K_p$: the completion of $K$ at a prime $p$ of $K$,
• $K_{\infty} = KB_{\infty}$ (the cyclotomic $Z_p$-extension of $K$),
• $K_n$: the $n$th layer of $K_{\infty}/K$ ($K_n/K$ is a cyclic extension of degree $p^n$),
• $\lambda(K)$: the Iwasawa $\lambda$-invariant of $K_{\infty}/K$, and
• $\mu(K)$: the Iwasawa $\mu$-invariant of $K_{\infty}/K$.

For a finite group $G_1$, we denote by $|G_1|$ its order. For a finite abelian $p$-group $G_2$, we put $r_p(G_2) = \dim_{Z_p} G_2/pG_2$ (the $p$-rank of $G_2$). For a $Z_p$-module $M_1$, we put $\text{rank}_{Z_p} M_1 = \dim_{Q_p} M_1 \otimes_{Z_p} Q_p$ (the $Z_p$-rank of $M_1$). For a cyclic $p$-group (resp. an infinite pro-cyclic pro-$p$ group) $G_3$ and a $Z_p[G_3]$-module (resp. $Z_p[[G_3]]$-module) $M_2$, let $(M_2)^{G_3}$ be the $G_3$-invariant submodule of $M_2$ and $(M_2)_{G_3}$ the $G_3$-coinvariant quotient of $M_2$.

1.6. Free pro-$p$ groups and Demuškin groups. In this subsection, we recall some properties of free pro-$p$ groups and Demuškin groups. (See, e.g., [13, 26, 36].)

Let $p$ be an arbitrary prime number. For a pro-$p$ group $G$, we denote by $d(G) = \dim_{Z_p} H^1(G, F_p)$ its generator rank and $G^{ab}$ its maximal abelian pro-$p$ quotient.

Lemma 1.6.1. Let $G$ be a finitely generated pro-$p$ group.

(i) If $G$ is a free pro-$p$ group satisfying $d(G) \geq 1$, then
• $G^{ab}$ is a free $Z_p$-module of rank $d(G)$, and
• for every open subgroup $U$ of $G$, $U$ is also a free pro-$p$ group and
  $$d(U) - 1 = (G:U)(d(G) - 1).$$

(ii) If $G$ is a Demuškin group satisfying $d(G) \geq 2$, then
• $\text{rank}_{Z_p} G^{ab}$ is $d(G)$ or $d(G) - 1$, and
• for every open subgroup $U$ of $G$, $U$ is also a Demuškin group and
  $$d(U) - 2 = (G:U)(d(G) - 2).$$

Proof. These assertions are well known. See, e.g., [13, 26, 36].

2. Results for imaginary quadratic fields

2.1. Preliminaries ($p \geq 3$). Let $k$ be an imaginary quadratic field and $p$ an odd prime number satisfying (C1) and (C2). Take an unramified cyclic extension $K/k$ of degree $p$, and let $F$ be an intermediate field of $K/Q$ of degree $p$. We fix elements $\sigma$, $\tau$ of $\text{Gal}(K/Q)$ such that $\sigma$ generates $\text{Gal}(K/k)$ and $\tau$ generates $\text{Gal}(K/F)$. (Then, $\tau\sigma = \sigma^{-1}\tau$.)

We will give some remarks on $K_{\infty}/K$ and $X(K_{\infty})$. Since $K \cap B_{\infty} = Q$, we shall identify $\text{Gal}(K_{\infty}/B_{\infty})$ with $\text{Gal}(K/Q)$. We put $\Gamma = \text{Gal}(K_{\infty}/K)$, and we also identify $\text{Gal}(F_{\infty}/F)$, $\text{Gal}(k_{\infty}/k)$ with $\Gamma$. It is well known that $X(K_{\infty})$ is finitely generated torsion $Z_p[[\Gamma]]$-module. We see that $\mu(k) = 0$ by Ferrero-Washington’s theorem [6], and we also see that $\mu(K) = 0$ because $K_{\infty}/k_{\infty}$ is a cyclic extension of degree $p$ (see [21] Theorem 3). Hence, $X(K_{\infty})$ is finitely generated as a $Z_p$-module (the same assertion also holds for $X(F_{\infty})$). We also note that all primes of $K$ lying above $p$ are totally ramified in $K_{\infty}$.

We put $X(K_{\infty})^+ = (1 + \tau)X(K_{\infty})$. Then $X(K_{\infty}) \cong X(K_{\infty})^+ \oplus X(K_{\infty})^-$, and $X(K_{\infty})^+ \cong X(F_{\infty})$. We shall define a homomorphism (as $Z_p$-modules) from $X(K_{\infty})^-$ to $X(K_{\infty})^+$ inspired by the idea given in Konomi’s paper (see [27] Proposition 1.5 (4)).
Lemma 2.1.2. Let the notation be as above. Then the image of $G$ is certainly contained in $X(K)\uparrow$, and the kernel $\ker \phi$ of $\phi$ is
\[ \{ x \in X(K) \mid \sigma x = x \}. \]

Proof. This lemma follows from direct computations. \qed

2.2. First criterion $(p \geq 3)$.

Proof of Theorem 1.2.1 Assume that $\mathcal{X}(k)$ is a free pro-$p$ group and
\[ \lambda(F) \leq \frac{(p - 1)\lambda(k) - p}{2}. \]

Put $\mathcal{G} = \mathcal{X}(k)$ and $U = \mathcal{X}(K)$. From the fact that $K/k$ is unramified, we see that $L(K) = L(k)$, and hence $U$ is an open subgroup of $\mathcal{G}$ of index $p$. We shall apply Lemma 1.6.1(i) for $\mathcal{G}$ and $U$. Since $X(k) = \mathbb{Z}^\lambda$, the generator rank of $\mathcal{G}$ is $\lambda(k)$. We see that $U$ is also a free pro-$p$ group, and
\[ d(U) - 1 = p(\lambda(k) - 1). \]

Consequently,
\[ \lambda(K) = \text{rank}_{\mathbb{Z}_p} U^{ab} = d(U) = p\lambda(k) - p + 1. \]

Let $\phi$ be the homomorphism given in Definition 2.1.1. We put
\[ \lambda^+(K) = \text{rank}_{\mathbb{Z}_p} X(K)\uparrow(= \lambda(F)) \quad \text{and} \quad \lambda^-(K) = \text{rank}_{\mathbb{Z}_p} X(K)\downarrow. \]

Consider the following exact sequence
\[ 0 \to X(K)\uparrow(\sigma) \to X(K)\uparrow(\sigma-1) \to X(K)\to X(K)\downarrow(\sigma) \to 0. \]

From this, we see that $\text{rank}_{\mathbb{Z}_p} X(K)\uparrow(\sigma) = \text{rank}_{\mathbb{Z}_p} X(K)\downarrow(\sigma)$. We note that $\ker \phi$ is a $\mathbb{Z}_p$-submodule of $X(K)\downarrow(\sigma)$. Note also that the intermediate field $L'$ of $L(K)/K$ corresponding to $(\sigma - 1)X(K)$ is an abelian (unramified) pro-$p$ extension over $k$ (that is, $L'$ is an intermediate field of $L(k)/k$). By combining these facts, we obtain the following inequalities
\[ \text{rank}_{\mathbb{Z}_p}(\ker \phi) \leq \text{rank}_{\mathbb{Z}_p} X(K)\downarrow(\sigma) = \text{rank}_{\mathbb{Z}_p} X(K)\downarrow(\sigma) \leq \lambda(k). \]

Hence, by using Lemma 2.1.2, we see that
\[ \lambda^-(K) \leq \text{rank}_{\mathbb{Z}_p}(\ker \phi) + \lambda^+(K) \leq \lambda(k) + \lambda(F). \]

Moreover, we see the following:
\[ \lambda(K) = \lambda^+(K) + \lambda^-(K) \leq \lambda(k) + 2\lambda(F). \]

Since $2\lambda(F) \leq (p - 1)\lambda(k) - p$, we see
\[ \lambda(K) \leq p\lambda(k) - p. \]

This contradicts the equality (1). \qed
2.3. Second criterion \((p = 3)\). In this subsection, we assume that \(p = 3\). Recall that \(F\) is a cubic field which is not totally real, and there are only two primes lying above 3 in \(F\).

**Definition 2.3.1.** Let \(\mathfrak{p}\) be the prime of \(F\) which is lying above 3 and satisfies \(F_{\mathfrak{p}} = \mathbb{Q}_3\). We also take a unit \(\varepsilon_F\) such that \(E(F) = \langle -1, \varepsilon_F \rangle\). We define a positive integer \(e(F)\) which satisfies

\[
\varepsilon_F^2 \equiv 1 \pmod{p^{e(F)}} \quad \text{and} \quad \varepsilon_F^2 \not\equiv 1 \pmod{p^{e(F)+1}}.
\]

Note that \(e(F)\) does not depend on the choice of \(\varepsilon_F\).

**Proof of Theorem 1.2.2.** By using Lemma 1.6.1 (i), we see that if \(X\) is a non-trivial \(\mathbb{Z}_3\)-torsion element, then \(X\) is a finitely generated free \(\mathbb{Z}_3\)-module (recall the first paragraph of the proof of Theorem 1.2.1). Hence, \(X\) is not a non-trivial \(\mathbb{Z}_3\)-torsion element.

Recall the facts that \(X(K_{\infty}) \cong X(K_{\infty})^+ \oplus X(K_{\infty})^-\) and \(X(K_{\infty})^+ \cong X(F)\). Hence, to see the assertion of this theorem, it is sufficient to show that \(X(K_{\infty})\) has a non-trivial \(\mathbb{Z}_3\)-torsion element (cf. \([8, 16]\)). The outline of the following proof is similar to \([8, \text{ Corollary 3.5 (i)}]\).

Let \(\mathfrak{p}\) and \(e(F)\) be as in Definition 2.3.1. We put \(\Gamma_n = \text{Gal}(F_n/F)\) for \(n \geq 0\). First of all, we shall show the following inequality:

\[
|A(F_n)^{\Gamma_n}| \leq |A(F)| \cdot 3^{e(F)-1}.
\]

We will use the idea given in \([13]\). For \(n \geq 0\), let \(M_{(p)}(F_n)\) be the maximal abelian pro-3 extension of \(F_n\) unramified outside \(\mathfrak{p}\), and put \(X_{(p)}(F_n) = \text{Gal}(M_{(p)}(F_n)/F_n)\). Since there are only two primes in \(F\) lying above 3 and they are totally ramified in \(F_{\infty}/F\), we can see that \(X_{(p)}(F_n)_{\Gamma_n} \cong X_{(p)}(F)\). Let \(U_1^p(F)\) be the group of principal units of \(F_p\), that is,

\[
U_1^p(F) = \{u \mid u \text{ is a unit of } F_p \text{ satisfying } u \equiv 1 \pmod{p}\}
\]

(we also use the symbol \(p\) for the maximal ideal of the ring of integers of \(F_p\), and denote by \(\mathcal{E}\) the subgroup of \(U_1^p(F)\) topologically generated by \(\varepsilon_F^2\). From the exact sequence

\[
0 \to U_1^p(F)/\mathcal{E} \to X_{(p)}(F) \to A(F) \to 0
\]

and the fact that \(|U_1^p(F)/\mathcal{E}| = 3^{e(F)-1}\), we see that \(|X_{(p)}(F)| = |A(F)| \cdot 3^{e(F)-1}\). We also note that \(A(F_n)\) can be seen as a quotient of \(X_{(p)}(F_n)\), then \(|X_{(p)}(F_n)_{\Gamma_n}| \geq |A(F_n)_{\Gamma_n}|\).

From these facts, we see that

\[
|A(F_n)^{\Gamma_n}| = |A(F_n)_{\Gamma_n}| \leq |X_{(p)}(F_n)_{\Gamma_n}| = |X_{(p)}(F)| = |A(F)| \cdot 3^{e(F)-1}.
\]

The inequality \((2)\) has been shown.

Assume that an ideal class \(c\) of \(D(F_{m'})\) is not trivial for some \(n'\). Next, we claim that \(c\) becomes trivial in \(A(F_m)\) for a sufficiently large \(m > n'\). Since \(D(F_n)\) is a subgroup of \(A(F_n)^{\Gamma_n}\), the boundedness of \(|A(F_n)^{\Gamma_n}|\) also implies the boundedness of \(|D(F_n)|\). Then the claim follows from the argument given in the proof of \([11, \text{ p.267, Corollary}]\) (with a slight modification).

Finally, by using \([38, \text{ p.218, Corollary}]\), we see that the maximal finite \(\mathbb{Z}_3[[\Gamma]]\)-submodule of \(X(F)\) is not trivial. Then the theorem follows. \(\square\)
2.4. Proof of Theorem 1.3.1 \((p \geq 3)\). In this subsection, \(p\) denotes an odd prime number.

**Proposition C** (see Lemmermeyer [30]). Let \(k\) be an imaginary quadratic field and \(p\) an odd prime number satisfying (C1), (C2), and (C3). Let \(K/k\) be the unique unramified cyclic extension of degree \(p\), and \(F\) an intermediate field of \(K/Q\) of degree \(p\). For a non-negative integer \(n\), if \(r_p(X(k_n)) = 1\) then \(X(F_n)\) is trivial. (In particular, \(X(F)\) is always trivial because \(k\) and \(p\) satisfy (C3).)

**Proof.** This is a special case of [30, Proposition 8.4]. (Apply this proposition for \(K_n/B_n\). Note that the class number of \(B_n\) is prime to \(p\), and \(K_n/k_n\) is an unramified extension.) \(\square\)

**Proof of Theorem 1.3.1** First, we shall show the only if part. We note that \(X(F)\) is trivial by Proposition C. Assume that \(\lambda(k) = 1\). Since \(X(k_\infty) \cong \mathbb{Z}_p\) as a \(\mathbb{Z}_p\)-module, we see that \(r_p(X(k_1)) = 1\). Then, by using Proposition C for \(n = 1\), we see that \(X(F_1)\) is trivial. Since both \(X(F)\) and \(X(F_1)\) are trivial, we conclude that \(X(F_\infty)\) is trivial. (See [9, Theorem 1 (1)]. Note that every prime lying above \(p\) is totally ramified in \(F_\infty/F\).

Next, we will show the if part. Assume that \(X(F_\infty)\) is trivial. Then \(X(F_1)\) must be trivial. To see the assertion, we will show that \(r_p(X(k_1)) = 1\) and then apply [9, Theorem 1 (2)].

For a finite extension \(K'/K\) of algebraic number fields, we denote by \(N_{K'/K}\) the norm mapping from \(K'\) to \(K\) (elements or ideals). We use the following result. This is a special case of [30, Theorem 2.1].

**Theorem D** (see Lemmermeyer [30]). Let the assumptions be as in Theorem 1.3.1. If \(X(F_1)\) is trivial and \(N_{F_1/B_1}E(F_1) = E(B_1)\), then \(r_p(X(k_1)) = 1\).

Hence it is sufficient to show that \(N_{F_1/B_1}E(F_1) = E(B_1)\) under the assumption that \(X(F_1)\) is trivial. In the remaining part, we shall show this.

Recall that \(p\) does not split in \(k\), and the unique prime of \(k\) lying above \(p\) splits completely in \(K\). Then we can take a prime \(p_F\) of \(F\) which satisfies \(\bar{F}_{p_F} = \mathbb{Q}_p\). Let \(p_{F_1}\) be the unique prime of \(F_1\) lying above \(p_F\) (note that \(p_F\) is totally ramified in \(F_1/F\)). From our assumption, \(h(F_1)\) (the class number of \(F_1\)) is not divisible by \(p\). Hence there is a positive integer \(h\) (which is prime to \(p\)) such that \(p_{F_1}^h\) is a principal ideal generated by an algebraic integer \(\eta_{F_1}\) of \(F_1\).

Fix a generator \(\gamma\) of \(\text{Gal}(F_1/F)\) \((\cong \text{Gal}(B_1/Q))\). Then \(u := \eta_{F_1}^{-1}\) is a unit of \(F_1\), and hence \(u' := N_{F_1/B_1}u\) is a unit of \(B_1\). Note that \(N_{F_1/B_1}u^\gamma = (u')^\gamma\).

We claim that \(u'E(B_1)^p\) generates \(E(B_1)/E(B_1)^p\) as a \(\mathbb{F}_p[\text{Gal}(B_1/Q)]\)-module. Recall that the unique prime \(p_{B_1}\) of \(B_1\) lying above \(p\) is a principal ideal generated by \(\eta_{B_1} := N_Q(\zeta_p^2)/B_1(1 - \zeta_p^2)\), where \(\zeta_p^2 = e^{2\pi i/p}\). Since \(N_{F_1/B_1}p_{F_1} = p_{B_1}\), we can write \(N_{F_1/B_1}p_{F_1} = p_{B_1}\), we can write \(N_{F_1/B_1}\eta_{F_1} = \eta_{B_1}^h\eta_{B_1}^e\) with an unit \(\varepsilon\) of \(B_1\). It is known that \(u := \eta_{B_1}^{-1}\) generates \(E(B_1)/E(B_1)^p\) as a \(\mathbb{F}_p[\text{Gal}(B_1/Q)]\)-module (see [46, 17, and 29, pp.204–205]). Since \(u' = u'^h\varepsilon^{\gamma^{-1}}\) (and \(h\) is prime to \(p\)), we see that \(u'E(B_1)^p\) generates \(E(B_1)/E(B_1)^p\) modulo \((E(B_1)/E(B_1)^p)^{\gamma^{-1}}\). Then, by using Nakayama’s lemma, the claim can be shown.

Since \(N_{F_1/B_1}E(F_1)\) contains \(E(B_1)^p\), the above facts yield that \(N_{F_1/B_1}E(F_1) = E(B_1)\). Then, by using Theorem D, we see that \(r_p(X(k_1)) = 1\) (and that \(\lambda(k) = 1\). \(\square\)
Proof of Corollary 2.3. Throughout this proof, we assume that $p = 3$. We use the notation given in Section 2.3. (Especially, $p$ is the unique prime of $F$ lying above 3 which satisfies $F_p = \mathbb{Q}_3$.) In this situation, we can apply [13, Theorem 8.1] for $F$ and $p = 3$. We note that $X(F)$ is trivial by Proposition C. Thus we see that $X(F_{\infty})$ is trivial if and only if $U_p^1(F)/\mathcal{E}$ is trivial. We also see that $U_p^1(F)/\mathcal{E}$ is trivial if and only if $\varepsilon_F^2 \not\equiv 1 \pmod{p}$ (cf. [13, Example 8.3]). The assertion follows. □

2.5. When is $\mathcal{X}(k_{\infty})$ a Demuˇskin group? ($p \geq 3$). Let $k$ be an imaginary quadratic field and $p$ an odd prime number. In this subsection, we consider the question whether $\mathcal{X}(k_{\infty})$ is a Demuˇskin group.

We assume that $\lambda(k) = 2$ in this paragraph. Then $\mathcal{X}(k_{\infty})^{ab} \cong \mathbb{Z}_p^{\oplus 2}$. It can be seen that if a Demuˇskin group $\mathcal{G}$ satisfies $d(\mathcal{G}) = 2$ and $\mathcal{G}^{ab} \cong \mathbb{Z}_p^{\oplus 2}$, then $\mathcal{G}$ must be isomorphic to $\mathbb{Z}_p^{\oplus 2}$. (This follows from a well known property of Demuˇskin groups. See e.g., [36, (3.9.1)Theorem].) Hence, this implies that $\mathcal{X}(k_{\infty})$ is a Demuˇskin group if and only if $\mathcal{X}(k_{\infty})^{ab} = \mathcal{X}(k_{\infty})^{\oplus 2}$. Okano [37] gave a criterion whether $\mathcal{X}(k_{\infty})$ is abelian or not. In particular, by using [37, Theorem 1.1], if $p$ does not split in $k$ and $\lambda(k) = 2$, then $\mathcal{X}(k_{\infty})$ is not a Demuˇskin group. (On the other hand, when $p$ splits in $k$, there is a pair $k, p$ such that $\mathcal{X}(k_{\infty}) \cong \mathbb{Z}_p^{\oplus 2}$, which is an abelian Demuˇskin group.)

We will consider the case when $\lambda(k) \geq 3$.

Remark 2.5.1. Since $p$ is odd, the generator rank of a Demuˇskin group must be even (see, e.g., [36, (3.9.16)Proposition]). Hence, if $\lambda(k)$ is odd, then $\mathcal{X}(k_{\infty})$ cannot be a Demuˇskin group.

When $p$ does not split in $k$, we can obtain the following criterion.

Theorem 2.5.2. Let $k$, $K$, and $F$ be as in Theorem 1.2.1. Assume that $\lambda(k) \geq 4$ and $\lambda(k)$ is even. If

$$\lambda(F) \leq \frac{(p - 1)\lambda(k) - 2p}{2},$$

then $\mathcal{X}(k_{\infty})$ is not a Demuˇskin group. (It is also not a free pro-$p$ group by Theorem 1.2.1.)

Proof. Suppose that $\mathcal{X}(k_{\infty})$ is a Demuˇskin group. We note that $U = \mathcal{X}(K_{\infty})$ is an open subgroup of $\mathcal{X}(k_{\infty})$. Then by Lemma 1.6.1(ii), we see that $U$ is also a Demuˇskin group and

$$d(U) = p\lambda(k) - 2p + 2$$

(recall that $d(\mathcal{X}(k_{\infty})) = \lambda(k)$). We note that $d(U) \geq 2$ because $\lambda(k) \geq 4$. By applying the first assertion of Lemma 1.6.1(ii) for $U$, we see that $\lambda(K) = \text{rank}_{\mathbb{Z}_p} U^{ab} \geq d(U) - 1$. Hence,

$$\lambda(K) \geq p\lambda(k) - 2p + 1.$$ 

On the other hand, if $2\lambda(F) \leq (p - 1)\lambda(k) - 2p$, then we obtain the following inequality

$$\lambda(K) \leq \lambda(k) + 2\lambda(F) \leq p\lambda(k) - 2p$$

by using the same argument given in the proof of Theorem 1.2.1. It is a contradiction. □

3. Computations for Imaginary Quadratic Fields

Let $k$ be an imaginary quadratic field, and put $p = 3$. Assume that $k$ and $p$ satisfy (C1) and (C2) in Section 1. We will give computational results for Conjecture A.
3.1. Remarks on computations. The computations were done by using Magma \[2\] and PARI/GP \[10\]. For several computations, the author used both Magma and PARI/GP independently and checked that these results are the same. However, for example, the author used PARI/GP only for the computation of the Iwasawa $\lambda$-invariant of imaginary quadratic fields (because it was due to the function $\text{Iwapoly}$ made by Y. Mizusawa \[31\]). For the Magma computations, the author referenced the source codes written by the co-author of \[19\]. The author used PARI/GP version 2.9.4 at the time that the first manuscript of the present paper was written, however, he re-computed the examples by using PARI/GP version 2.11.0 at the time of revising.

Note that the ideal class groups were computed without assuming GRH (except for the computations given in Remark \[3.3.2\]). That is, the author used the command $\text{ClassGroup}$ with \texttt{Proof:="Full"} for Magma computations, and used $\text{bnf certify}$ for PARI/GP computations.

3.2. Computations for Conjecture A ($p = 3$). We assume that $p = 3$. Let $K/k$ be an unramified cubic cyclic extension, and $F$ an intermediate field of $K/\mathbb{Q}$ of degree 3. The author used $\text{AbelianpExtension}$ (Magma), $\text{rnfkummer}$ (PARI/GP) to construct $K$.

Before stating examples, we shall give some remarks on the structure of $X(F_\infty)$. We can show that $\mu(F) = 0$ (see Section \[2.1\]). However, it seems a mysterious question whether $\lambda(F) = 0$ or not. Since $F$ is not totally real, this question lies outside of Greenberg’s conjecture. On the other hand, $p$ does not split completely in $F$, and hence the result given in \[11\] p.266 is not applicable (i.e., it cannot be said that $\lambda(F) > 0$ always holds). However, we can determine that $\lambda(F) = 0$ for some cases by using an analog of known criteria (cf., e.g., \[11\], \[10\]).

**Proposition 3.2.1.** Assume that $p = 3$. Let $k$ and $F$ be as in Theorem \[1.2.2\], $D(F_n)$ as in the paragraph before Theorem \[1.2.2\], and $e(F)$ as in Definition \[2.3.1\]. If $|D(F_n)| = |A(F)| \cdot 3^{e(F)-1}$ for some $n \geq 0$, then $\lambda(F) = 0$.

**Proof.** Under the assumptions, we see that $|A(F_m)^{\Gamma_m}| = |D(F_m)| = |A(F)| \cdot 3^{e(F)-1}$ for all $m \geq n$ by using the inequality \[2\] given in the proof of Theorem \[1.2.2\] and the fact that the mapping $D(F_m) \to D(F_n)$ (induced from the norm) is surjective. Hence by using the argument given in the proof of \[11\] Theorem 2, we can conclude that $\lambda(F) = 0$. \hfill $\square$

**Example 3.2.2.** Put $k = \mathbb{Q}(\sqrt{-21})$ and $p = 3$. Then $k$ and $3$ satisfy (C1) and (C2). We see that $|A(k)| = 3$ and $\lambda(k) = 2$. Then $K$ is the unique unramified cyclic cubic extension over $k$. In this case, we found that $|A(F_1)| = |D(F_1)| = 3$ (note that the degree of $F_1/\mathbb{Q}$ is 9). Then, by Theorem \[1.2.2\], we see that Conjecture A holds for this case. (Alternatively, we see that $|A(F)| = 1$ and $e(F) = 2$, then $\lambda(F) = 0$ by Proposition \[3.2.1\]. Hence we can also apply Theorem \[1.2.1\].)

**Example 3.2.3.** Put $k = \mathbb{Q}(\sqrt{-274})$ and $p = 3$. This pair satisfy (C1) and (C2). We see that $|A(k)| = 3$ and $\lambda(k) = 4$. Take $K$ and $F$ similarly ($K$ is uniquely determined). We found that $|A(F_1)| = |D(F_1)| = 3$. Hence Conjecture A follows from Theorem \[1.2.2\]. Moreover, we see that $|A(F)| = 1$ and $e(F) = 2$, and then $\lambda(F) = 0$ by Proposition \[3.2.1\].

From this, by using Theorem \[2.5.2\] we also see that $X(k_\infty)$ is not a Demushkin group.

At this time, Theorem \[1.2.2\] seems more useful than Theorem \[1.2.1\] (when $p = 3$). If there were an example of trivial $X(F_\infty)$ (with $\lambda(k) \geq 2$), it could be an example such that Theorem \[1.2.1\] is applicable but Theorem \[1.2.2\] is not applicable. Unfortunately, there are
no such examples (Theorem 1.3.1). Note also that [9 Theorem 1 (2)] is applicable to find an upper bound of \( \lambda(F) \), even when \( D(F_n) \) is trivial. (That is, if \( r_p(A(F_n)) = r_p(A(F_{n+1})) \) for some \( n \), then \( \lambda(F) \leq r_p(A(F)) \).) However, we need the information of \( A(F_n) \) for a sufficiently large \( n \) (in particular, when \( |A(F)| = 1 \) and \( |A(F)| > 1 \), we must compute \( A(F_n) \) for \( n \geq 2 \).

3.3. Comparison of Theorem 1.2.2 and Ozaki’s criterion. We shall recall Ozaki’s result [39 Proposition 5]. In this paragraph, let \( p \) be an odd prime number which does not split in \( k \) (imaginary quadratic field). Let \( L^{(2)}(k_n) \) be the maximal unramified abelian \( p \)-extension over \( L(k_n) \) such that

1. \( L^{(2)}(k_n) \) is a Galois extension over \( k_n \), and
2. \( \text{Gal}(L^{(2)}(k_n)/L(k_n)) \) is contained in the center of \( \text{Gal}(L^{(2)}(k_n)/k_n) \).

We put \( X^{(2)}(k_n) = \text{Gal}(L^{(2)}(k_n)/L(k_n)) \). Then \( X^{(2)}(k_n) \) is the same as \( X^{(2)}_n \) defined in [39 p.62]. We also denote by \( D^{(2)}(k_n) \) the subgroup of \( X^{(2)}(k_n) \) which is generated by the decomposition subgroups for the primes lying above \( p \). Then, Ozaki’s result says that \( X(k_{\infty}) \) is not a free pro-\( p \) group if both of the following conditions are satisfied:

1. \( D^{(2)}(k_n) \) is not trivial for some \( n \), and
2. a certain condition on the \( p \)-adic \( L \)-function.

Actually, [39 Proposition 5] gives a more precise result for the structure of \( X(k_{\infty}) \).

As remarked before, the above criterion seems close to our Theorem 1.2.2. Note that Theorem 1.2.2 does not need the condition on the \( p \)-adic \( L \)-function (but only works for the case when \( p = 3 \)). We also mention that the non-triviality of \( D(F_n) \) does not imply the non-triviality of \( D^{(2)}(k_n) \) (for a fixed \( n \)). In the following, we shall give an example.

**Example 3.3.1.** Put \( k = \mathbb{Q}(\sqrt{-9934}) \) and \( p = 3 \). We note that \( A(k) \cong (\mathbb{Z}/3\mathbb{Z})^{\oplus 2} \). Let \( K \) be the splitting field of the polynomial

\[
x^3 - x^2 - 39x - 109
\]

over \( \mathbb{Q} \) (the user used PARI/GP to obtain this polynomial). Then \( K/k \) is an unramified cyclic cubic extension. Let \( F \) be a cubic extension of \( \mathbb{Q} \) which is contained in \( K \). Then, \( |A(F)| = 9 \) and \( |D(F)| = 3 \) (it was checked by both PARI/GP and Magma).

On the other hand, we can see that \( L^{(2)}(k)/L(k) \) is a cyclic cubic extension from the fact that \( A(k) \wedge A(k) \cong \mathbb{Z}/3\mathbb{Z} \) (see [39]). Let \( L^{sp}(K)/K \) be the maximal unramified abelian 3-extension in which every prime lying above 3 splits completely. By using Magma, it was checked that

\[
\text{Gal}(L^{sp}(K)/K) \cong \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.
\]

\text{Gal}(L^{sp}(K)/L(k)) \) is non-trivial. We note that \( L^{sp}(K) \) is a Galois extension over \( k \). Then the quotient of \( \text{Gal}(L^{sp}(K)/L(k)) \) such that \( \text{Gal}(L(k)/k) \) acts trivially is not trivial. Since \( |\text{Gal}(L^{(2)}(k)/L(k))| = 3 \), we can conclude that \( L^{(2)}(k) \) is an intermediate field of \( L^{sp}(K)/L(k) \). Recall that every prime lying above 3 splits completely in \( L^{sp}(K)/L(k) \). Thus we see that \( D^{(2)}(k) \) is trivial.

From the fact that \( |D(F)| = 3 \), we see that \( X(k_{\infty}) \) is not a free pro-3 group by using Theorem 1.2.2. However, since \( D^{(2)}(k) \) is trivial, Ozaki’s criterion is not applicable at least for \( n = 0 \).

**Remark 3.3.2.** For the case when \( p = 3 \) and \( k = \mathbb{Q}(\sqrt{-211}) \) or \( k = \mathbb{Q}(\sqrt{-274}) \) (recall Examples 3.2.2 and 3.2.3), the author computed the ideal class group of \( K_1 \) by using...
Magma assuming GRH. (That is, the command \texttt{ClassGroup} was used with \texttt{Proof} :="GRH". Note that the degree of $K_1/Q$ is $18$.) We define $L^{sp}(K_1)/K_1$ similarly to the above. For both cases, we found that $L^{sp}(K_1) = L(k_1)$ and $L(K_1) \neq L^{sp}(K_1)$. From these facts, we can deduce that $D^{(2)}(k_1)$ is not trivial (under GRH).

See also the computational results given in \cite{39} pp.83–85] (our computations given in Example 3.3.1 and Remark 3.3.2 were done based on Ozaki’s computation).

4. Proof of Theorem 1.4.1 ($p \geq 2$)

In this section, $p$ denotes an arbitrary prime number. (In particular, we allow the case when $p = 2$.) Let the notation $(k', S, L, G)$ be as in Theorem 1.4.1. First, we will show Theorem 1.4.1 when $G$ satisfies the condition (D) (i.e., $G$ is a Demuškin group with $d(G) \geq 3$).

4.1. When $G$ satisfies (D). Assume that $G = \text{Gal}(L/k_\infty)$ satisfies (D). We need some preparations to state our proof. Denote by $M/k_\infty$ a finite extension contained in $L$. Let $L_M/k_\infty$ be the maximal abelian pro-$p$ extension contained in $L$. We recall that $S(M)$ is the set of primes of $M$ lying above $S$. (Note that $S(M)$ is a finite set.) For $v \in S(M)$, let $I(M, v)$ be the inertia subgroup of $\text{Gal}(L_M/k_\infty)$ for $v$. Since $v$ is not lying above $p$, we see that $I(M, v)$ is finite or isomorphic to $\mathbb{Z}_p$ (see, e.g., \cite{36}). We remark that if $I(M, v) \cong \mathbb{Z}_p$, then $I(M', v') \cong \mathbb{Z}_p$ for every finite extension $M'/M$ contained in $L$ and every prime $v' \in S(M')$ lying above $v$.

We denote by $S_1(k_\infty')$ the maximal subset of $S(k_\infty')$ which satisfies the following property:

(I) for every $v \in S_1(k_\infty')$ there exists a finite extension $M/k_\infty'$ contained in $L$ and a prime $v' \in S(M)$ lying above $v$ such that $I(M, v') \cong \mathbb{Z}_p$.

We also put $S_2(k_\infty') = S(k_\infty') \setminus S_1(k_\infty')$. That is,

(II) if $v \in S_2(k_\infty')$, then $I(M, v')$ is finite for any finite extension $M/k_\infty'$ contained in $L$ and any prime $v' \in S(M)$ lying above $v$.

For a finite extension $M/k_\infty'$ contained in $L$, we denote by $S_1(M)$ (resp. $S_2(M)$) the set of primes of $M$ lying above $S_1(k_\infty')$ (resp. $S_2(k_\infty')$). Of course, $S(M) = S_1(M) \cup S_2(M)$ and $S_1(M) \cap S_2(M) = \emptyset$.

Lemma 4.1.1. Let the notation be as in Theorem 1.4.1. We also assume that $G$ satisfies (D) of Theorem 1.4.1. Then, there is a finite extension $K^{(0)}/k_\infty'$ contained in $L$ satisfying the following properties:

- $I(K^{(0)}, v') \cong \mathbb{Z}_p$ for every $v' \in S_1(K^{(0)})$, and
- $I(K^{(0)}, v')$ is finite for every $v' \in S_2(K^{(0)})$.

Proof. Take $v \in S_1(k_\infty')$ and $M$ which satisfy $I(M, v') \cong \mathbb{Z}_p$ for a prime $v'$ of $M$ lying above $v$. Then the Galois closure $M(v)$ of $M$ over $k_\infty'$ is a finite extension of $k_\infty'$ contained in $L$, and satisfies the following property: $I(M(v), v'') \cong \mathbb{Z}_p$ for every $v'' \in S(M(v))$ lying above $v$.

We put $K^{(0)} = \bigcup_{v \in S_1(k_\infty')} M(v)$, then $K^{(0)}$ satisfies the desired properties. \hfill $\square$

Let $K^{(0)}$ be as in Lemma 4.1.1. Put $U^{(0)} = \text{Gal}(L/K^{(0)})$. By Lemma 1.6.1 (ii), $U^{(0)}$ is also a Demuškin group, and satisfies

$$d(U^{(0)}) - 2 = (G : U^{(0)})(d(G) - 2).$$
Since $d(\mathcal{G}) \geq 3$, we also see that $d(U^{(0)}) \geq 3$. We note that for every finite extension $M'/K^{(0)}$ contained in $L$, $I(M', v') \cong \mathbb{Z}_p$ (resp. $I(M', v')$ is finite) for every $v' \in S_1(M')$ (resp. $v' \in S_2(M')$).

**Lemma 4.1.2.** Let the notation be as in Theorem 4.1.1. Assume that $\mathcal{G}$ satisfies (D) of Theorem 4.1.1, and take $K^{(0)}$ as in Lemma 4.1.1. Then, there is an infinite Galois extension $K^{(\infty)}/K^{(0)}$ contained in $L$ such that

- $\text{Gal}(K^{(\infty)}/K^{(0)}) \cong \mathbb{Z}_p$, and
- for every $v' \in S_1(K^{(0)})$, the inertia subgroup of $\text{Gal}(K^{(\infty)}/K^{(0)})$ for $v'$ has finite index.

**Proof.** Recall that $L_{K^{(0)}}^{ab}/K^{(0)}$ is the maximal abelian pro-$p$ extension contained in $L$. We also note that $\text{Gal}(L_{K^{(0)}}^{ab}/K^{(0)})$ is finitely generated as a $\mathbb{Z}_p$-module. Let $\tilde{K}$ be the intermediate field of $L_{K^{(0)}}^{ab}/K^{(0)}$ corresponding to the maximal $\mathbb{Z}_p$-torsion subgroup of $\text{Gal}(L_{K^{(0)}}^{ab}/K^{(0)})$. Then $\text{Gal}(\tilde{K}/K^{(0)})$ is isomorphic to $\mathbb{Z}_p^{\geq m}$ (where $m$ is equal to $d(U^{(0)})$ or $d(U^{(0)}) - 1$, and then $m \geq 2$). Since $L_{K^{(0)}}^{ab}/\tilde{K}$ is finite, the inertia subgroup of $\text{Gal}(\tilde{K}/K^{(0)})$ for every $v' \in S_1(K^{(0)})$ is isomorphic to $\mathbb{Z}_p$.

Then the assertion follows by using Kataoka’s result [23 Lemma 3.3] (by setting $M$ as $\text{Gal}(\tilde{K}/K^{(0)})$ and $L_j$ as the inertia subgroups). Actually, we only need a much weaker result than Kataoka’s, because it is sufficient to find one extension $K^{(\infty)}/K^{(0)}$. $\square$

**Proof of Theorem 4.1.1 when $\mathcal{G}$ satisfies (D).** Take $K^{(0)}$ and $K^{(\infty)}$ be as in above lemmas. Then there is a sequence of extensions

$$K^{(0)} \subset K^{(1)} \subset K^{(2)} \subset \cdots \subset K^{(n)} \subset \cdots \subset K^{(\infty)}$$

such that

- $\text{Gal}(K^{(n)}/K^{(0)}) \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n$, and
- if $n$ is sufficiently large, then every $v' \in S_1(K^{(0)})$ actually ramifies in $K^{(n)}/K^{(0)}$.

Let $s_n$ be the cardinality of $S_1(K^{(n)})$. The above facts imply that $s_n$ is bounded as $n \to \infty$. Fix a positive integer $C$ satisfying $s_n < C$ for all $n$.

We put $U^{(n)} = \text{Gal}(L/K^{(n)})$, and $L^{(n),ab} = L_{K^{(0)}}^{ab}(n)$ (the maximal abelian pro-$p$ extension of $K^{(n)}$ contained in $L$). By using Lemma 1.6.1 (ii), we see that $U^{(n)}$ is also a Demuškin group and $d(U^{(n)}) - 2 = p^n(d(U^{(0)}) - 2)$.

Recall that $d(U^{(0)}) \geq 3$, and then an inequality $d(U^{(n)}) \geq p^n + 2$ holds. Since $\text{Gal}(L^{(n)},ab/K^{(n)}) \cong (U^{(n)})^{ab}$, the $\mathbb{Z}_p$-rank of $\text{Gal}(L^{(n)},ab/K^{(n)})$ is greater than $p^n$.

Let $\mathcal{T}^{(n)}$ be the $\mathbb{Z}_p$-submodule of $\text{Gal}(L^{(n),ab}/K^{(n)})$ generated by $I(K^{(n)}, v)$ for all $v \in S(K^{(n)})$. Since $L^{(n),ab}/K^{(n)}$ is unramified outside $S(K^{(n)})$, the fixed field $L^{(n),ab}_{\text{unr}}$ of $\mathcal{T}^{(n)}$ is an unramified abelian pro-$p$ extension over $K^{(n)}$. By using the fact which is noted before, we see that $I(K^{(n)}, v) \cong \mathbb{Z}_p$ (resp. $I(K^{(n)}, v)$ is finite) for every $v' \in S_1(K^{(n)})$ (resp. $v' \in S_2(K^{(n)})$). Hence the $\mathbb{Z}_p$-rank of $\mathcal{T}^{(n)}$ is smaller than $C$.

Take $n$ such that $p^n > C$. By combining the above facts, we see that the $\mathbb{Z}_p$-rank of $\text{Gal}(L^{(n),ab}_{\text{unr}}/K^{(n)})$ is positive. This implies that $X(K^{(n)})$ is infinite. We recall that $K^{(n)}/k'$ is a finite extension. As noted in [22] (without proof), there exists a finite extension $k''$ of $\mathbb{Q}$ such that $K^{(n)}$ is the cyclotomic $\mathbb{Z}_p$-extension of $k''$. Since any archimedean prime
does not ramify in \( K^{(n)}/k'_\infty \), we see that this \( k'' \) is totally real. Then the theorem (when \( G \) satisfies (D)) follows. \( \square \)

### 4.2. When \( G \) satisfies (F)

Next, we will show the remaining case.

**Proof of Theorem 1.4.1 when \( G \) satisfies (F).** In fact, we can also see the assertion for this case quite similarly (by using Theorem 1.6.1 (i) instead of Theorem 1.6.1 (ii)).

As an alternative proof, we can see that the existence of the objects satisfying (F) implies the existence of the objects satisfying (D). That is, if there is a triple \( k', S, L \) satisfying (F), then we can take intermediate fields \( M \) and \( L' \) of \( L/k'_\infty \) such that \( M/k'_\infty \) is a finite extension and \( \text{Gal}(L'/M) \) is a Demuškin group with \( d(\text{Gal}(L'/M)) \geq 3 \). (Note that \( M \) is the cyclotomic \( \mathbb{Z}_p \)-extension of a certain totally real field.) \( \square \)

### 5. Proof of Theorem 1.4.2 (\( p \geq 3 \))

Let \( k' \) and \( S \) be as in Theorem 1.4.2. We assume that \( p \) is an odd prime number such that \( p \) is inert in \( k' \) and does not divide \( h(k') \). (Hence \( X(k'_\infty) \) is trivial by Iwasawa’s theorem \([20]\).) Moreover, we assume that \( X_{\{q_1\}}(k') \) and \( X_{\{q_2\}}(k') \) are trivial.

#### 5.1. Several preliminary facts.

**Lemma 5.1.1.** Let the assumptions be as in Theorem 1.4.2. Then

\[
X_{\{q_1,q_2\}}(k') \cong \mathbb{Z}/p\mathbb{Z}, \ X_S(k') \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus r-1}, \ X_{\{q_1,q_2\}}(k'_\infty) \cong \mathbb{Z}_p, \ \text{and} \ X_S(k'_\infty) \cong \mathbb{Z}_p^{\oplus r-1}
\]

as \( \mathbb{Z}_p \)-modules.

**Proof.** Put \( R_k'(q_i) = (O_{k'}/q_iO_{k'})^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \) for \( i = 1, \ldots, r \) (where \( O_{k'} \) is the ring of integers of \( k' \)). We note that \( R_k'(q_i) \) is a cyclic group of order \( p \). Then, by class field theory, we obtain the exact sequence

\[
E(k') \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{f} R_{k'}(q_1) \oplus R_{k'}(q_2) \rightarrow X_{\{q_1,q_2\}}(k') \rightarrow 0
\]

(recall that \( X(k') \) is trivial). By the assumption that \( X_{\{q_1\}}(k') \) is trivial, we see that the natural mapping \( E(k') \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow R_{k'}(q_1) \) is surjective. From this, we see that the cokernel of \( f \) is a cyclic group of order \( p \) (note that the image of \( f \) is cyclic). The assertion that \( X_{\{q_1,q_2\}}(k') = \mathbb{Z}/p\mathbb{Z} \) follows. The assertion that \( X_S(k') \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus r-1} \) can be shown similarly. (See also Remark 4.3 of \([10]\).)

The remaining two assertions can be shown by using \([16]\) Corollary 4.2. Note that the \( \mathbb{Z}_p \)-rank can be computed by using the formula given in \([15]\) Example 6.6] (see also the proof of \([16]\) Theorem 1.2). \( \square \)

We note that \( L_{\{q_1,q_2\}}(k') \) is a Galois extension over \( \mathbb{Q} \) of degree \( 2p \). We can see that \( \text{Gal}(L_{\{q_1,q_2\}}(k')/\mathbb{Q}) \) is isomorphic to the dihedral group of order \( 2p \). (If it is a cyclic group, then there exists a cyclic extension of degree \( p \) over \( \mathbb{Q} \) unramified outside \( \{q_1,q_2\} \). However, since \( q_1 \equiv q_2 \equiv -1 \pmod{p} \), such an extension does not exist.)

**Definition 5.1.2.** Let the notation be as in Theorem 1.4.2 For an integer \( n \geq 1 \), we put \( \zeta_p^n = e^{2\pi i n/p} \). We also put

\[
K' = L_{\{q_1,q_2\}}(k'), \quad H = K'(\zeta_p), \quad \text{and} \quad H^+ = K'(\zeta_p + \zeta_p^{-1}).
\]

Since \( K' \) is totally real, \( H \) is a CM-field and \( H^+ \) is the maximal real subfield of \( H \).
From the facts that $p$ is inert in $k'$ and $\text{Gal}(K'/\mathbb{Q})$ is isomorphic to the dihedral group of order $2p$, we see that the unique prime of $k'$ lying above $p$ splits completely in $K'$.

Similarly, since $q_j$ ($j = 3, \ldots, r$) is also inert in $k'$, then the unique prime of $k'$ lying above $q_j$ splits completely in $K'$. On the other hand, since $X_{\{q_1\}}(k')$ (resp. $X_{\{q_2\}}(k')$) is trivial, the unique prime of $k'$ lying above $q_1$ (resp. $q_2$) must ramify in $K'$.

We also remark that every prime of $K'$ lying above $p$ is totally ramified in $K'_\infty/K'$, and every prime of $K'$ lying above $q_i$ ($i = 1, \ldots, r$) does not split in $K'_\infty/K'$. (Recall the assumptions that $q_i \equiv -1 \pmod{p}$ and $q_i^2 \not\equiv 1 \pmod{p^2}$). From these, $q_i$ does not split in $\mathbb{B}_\infty/\mathbb{Q}$.)

**Lemma 5.1.3.** Let the assumptions be as in Theorem 1.4.2 and $K'$ as in Definition 5.1.2. Then $X(K'_\infty)$ is trivial.

**Proof.** We note that $K'_\infty$ is the unique intermediate field of $L_{\{q_1,q_2\}}(k'_\infty)/k'_\infty$ of degree $p$ over $k'_\infty$ (recall that $X_{\{q_1,q_2\}}(k'_\infty) \cong \mathbb{Z}_p$ by Lemma 5.1.1). Moreover, we also see that $L_{\{q_1,q_2\}}(k'_\infty) = L_{\{q_1,q_2\}}(k'_\infty)$. Note that the prime of $k'_\infty$ lying above $q_1$ is totally ramified in $L_{\{q_1,q_2\}}(k'_\infty)$ (this follows from the fact that the prime of $k'$ lying above $q_1$ ramifies in $K'$ but does not ramify in $k'_\infty$). Hence, if $X(K'_\infty)$ is not trivial, then there is a non-trivial unramified abelian $p$-extension of $L'/K'_\infty$ such that $L' \cap L_{\{q_1,q_2\}}(k') = K'_\infty$. However, this contradicts the fact that $L_{\{q_1,q_2\}}(k'_\infty) = L_{\{q_1,q_2\}}(k'_\infty)$. Hence $X(K'_\infty)$ is trivial, and then the assertion follows. \qed

To show the assertion of Theorem 1.4.2 it is sufficient to show that the $\mathbb{Z}_p$-rank of $X_S(K'_\infty)$ is not so large.

**Proposition 5.1.4.** Let the assumptions be as in Theorem 1.4.2 and $K'$ as in Definition 5.1.2. If

$$\text{rank}_{\mathbb{Z}_p} X_S(K'_\infty) \leq p(r - 2)$$

then $X_S(k'_\infty)$ is not a free pro-$p$ group.

**Proof.** Put $G = X_S(k'_\infty)$ and $U = X_S(K'_\infty)$. From the fact that $K'/k'$ is unramified outside $S(k')$, we see that $L_S(K'_\infty) = L_S(k'_\infty)$, and hence $U$ is an open subgroup of $G$ of index $p$.

Assume that $G$ is a free pro-$p$ group. Since $X_S(k'_\infty) \cong \mathbb{Z}_p^{\oplus r - 1}$, we see that $d(G) = r - 1$. Hence, by using Lemma 1.6.1 (i), we see that

$$\text{rank}_{\mathbb{Z}_p} X(K'_\infty) = d(U) = p(r - 2) + 1.$$

The assertion follows from this. \qed

5.2. **Proof of Theorem 1.4.2.** The following proposition is a key result to prove Theorem 1.4.2.

**Proposition 5.2.1.** Let the assumptions be as in Theorem 1.4.2 and $H^+$ as in Definition 5.1.2. Then, $\text{Gal}(L_{\{q_3\}}(H'_\infty)/L(H'_\infty))$ is finite.

**Proof.** Our proof of this proposition is almost same as that of a special case of [15, Theorem 1.1] (see also the proof of [18, Theorem 3.1]). Hence, for the most part of this proof, we will state the outline only.

However, since $H^+$ is not an abelian extension over $\mathbb{Q}$, we must be careful in some places. In the proof of [15, Theorem 1.1], the following are major places in which the assumption that the base field is a real abelian field is used.
• Calculation of the $\mathbb{Z}_p$-rank of the subgroup generated by the inertia subgroups of the Galois group of a certain Kummer extension (see [15, Proposition 3.3]).

• Estimation of (a part of) the characteristic ideal of the “$p$-ramified Iwasawa module” (see [15, pp.521–522]).

However, for our case, we can also handle these places.

Let $H$ be as in Definition 5.1.2. Take a topological generator $\gamma$ of $\text{Gal}(H_\infty/H)$ which satisfies $\zeta_{p^n}^\gamma = \zeta_{p^{n+1}}$ for all $n$. (We will use the same symbol $\gamma$ for the restriction of $\gamma$ to $H_\infty^+$. We also fix an isomorphism from $\mathbb{Z}_p[[\text{Gal}(H_\infty/H)]]$ to $\Lambda = \mathbb{Z}_p[[T]]$ satisfying $\gamma \mapsto 1 + T$, and we regard $\mathbb{Z}_p[[\text{Gal}(H_\infty/H)]]$-modules (or $\mathbb{Z}_p[[\text{Gal}(H_\infty^+ / H^+)]]$-modules) as $\Lambda$-modules via this isomorphism. For a finitely generated torsion $\Lambda$-module $Y$, we denote by $\text{char}_\Lambda Y$ its characteristic ideal.

We put $m = p(p-1)/2$ (= the degree of $H^+/k'$). Hence the degree of $H/k'$ is $2m$. From the assumptions on $q_3$, we see that the unique prime of $k'$ lying above $q_3$ splits completely in $H$. (Moreover, every prime lying above $q_3$ does not split in $H_\infty/H$.) We also note that there are $p$ primes of $H$ lying above $p$, and denote by $\mathfrak{P}_1, \ldots, \mathfrak{P}_p$ these primes. For $i = 1, \ldots, p$, let $\mathcal{U}_{1,i}(H)$ be the group of principal units of $H_{\mathfrak{P}_i}$ (see also the proof Theorem 1.2.2 given in Section 2.3). We put $\mathcal{U}^1 = \prod_{i=1}^p \mathcal{U}_{1,i}(H)$. Then the $\mathbb{Z}_p$-rank of $\mathcal{U}^1$ is $2p(p-1) = 4m$.

Fix a prime $\mathfrak{P}$ of $H$ which is lying above $q_3$. We can take a positive integer $h$ such that $\mathfrak{P}^h$ is a principal ideal generated by $\alpha$ (where $\alpha$ is an algebraic integer of $H$), and $\alpha \equiv 1 \pmod{\mathfrak{P}_i}$ for all $\mathfrak{P}_i$ ($i = 1, \ldots, p$). Let $\iota$ be the complex conjugation. Take elements $\sigma_1, \ldots, \sigma_m$ of $\text{Gal}(H/k')$ which represents $\text{Gal}(H/k')$ modulo $\langle \iota \rangle$. We define a subgroup $A$ of the multiplicative group $H^\times$ generated by $\alpha^{\sigma_1}, \alpha^{\sigma_1 \iota}, \ldots, \alpha^{\sigma_m}, \alpha^{\sigma_m \iota}$.

We see that $A$ is free of rank $2m$ as a $\mathbb{Z}$-module, because the unique prime of $k'$ lying above $q_3$ splits completely in $H$.

We put $\beta_i = \alpha^{\sigma_i}/\alpha^{\sigma_i \iota}$ and

$$N = \bigcup_{n \geq 1} H_\infty(\sqrt[n]{\beta_1}, \ldots, \sqrt[n]{\beta_m}).$$

Then $N$ is a Galois extension over $H^+$, and an abelian extension over $H_\infty^+$. Let $\mathcal{I}$ be the subgroup of $\text{Gal}(N/H_\infty)$ which is generated by the inertia subgroups for the primes lying above $p$. We would like to show that $\text{rank}_{\mathbb{Z}_p} \mathcal{I} = m$ by using [24, Lemma 2.5] (see also [18]). To see this, it is sufficient to show that the $\mathbb{Z}_p$-rank of $\mathcal{A}$ is $2m$, where $\mathcal{A}$ is the closure of the image of the diagonal embedding $A \rightarrow \mathcal{U}^1$. In [15], the assumption that the base field is abelian over $\mathbb{Q}$ is used to prove a similar result (see also [15]). However, in our case, we only consider the $\text{Gal}(H/k')$-conjugates of $\alpha$, and $H/k'$ is an abelian extension. Thanks to these facts, we can imitate the argument (using Baker-Brumer’s theorem [4]) given in [18, p.1498], [15, pp.519–520]. (Note that we consider the matrix $(\log_p(\alpha^{\sigma \tau^{-1}}))_{\sigma, \tau \in \text{Gal}(H/k')}$. In our case, see also [47, §5.6].) Thus we see that $\text{rank}_{\mathbb{Z}_p} \mathcal{A} = 2m$, and hence

$$(3) \quad \text{rank}_{\mathbb{Z}_p} \mathcal{I} = m.$$

Let $N^+$ be the unique intermediate field of $N/H_\infty$ such that $\text{Gal}(N^+/H_\infty^+) \cong \mathbb{Z}_p^{2m}$. From the above facts, $N^+/H_\infty^+$ is unramified outside the primes lying above $p$ or $q_3$, and $\gamma$ acts on $x \in \text{Gal}(N^+/H_\infty^+)$ as $x^\gamma = x^{1+p}$. 

16
Let \( M_{(p,q_3)}(H_\infty^+)/H_\infty^+ \) (resp. \( M_{(p)}(H_\infty^+)/H_\infty^+ \)) be the maximal abelian pro-\( p \) extension which is unramified outside the primes lying above \( p \) or \( q_3 \) (resp. \( p \)). Put
\[
\mathcal{X}_{(p,q_3)}(H_\infty^+) = \text{Gal}(M_{(p,q_3)}(H_\infty^+)/H_\infty^+) \quad \text{and} \quad \mathcal{X}_{(p)}(H_\infty^+) = \text{Gal}(M_{(p)}(H_\infty^+)/H_\infty^+).
\]
Since \( H^+ \) is totally real, both \( \mathcal{X}_{(p,q_3)}(H_\infty^+) \) and \( \mathcal{X}_{(p)}(H_\infty^+) \) are finitely generated torsion \( \Lambda \)-modules (see, e.g., [36 (11.3.2)Theorem (iv)]).

We shall consider \( \text{char}_\Lambda \mathcal{X}_{(p,q_3)}(H_\infty^+) \) (in [15], the assumption that the base field is a real abelian field is used in this process). Before this, we consider \( \text{X}(H_\infty^+)^{-} = (i - 1)\text{X}(H_\infty^+) \) (the usual minus part of the unramified Iwasawa module for a CM field). Note that \( k'(\zeta_p) \) is an abelian extension over \( \mathbb{Q} \), and \( H \) is a cyclic extension of degree \( p \) over \( k'(\zeta_p) \). Then, by using Ferrero-Washington’s theorem [5] and Iwasawa’s theorem [21 Theorem 3] (see also Section 2.1), we see that \( \mu(H) = 0 \). Take \( g(T) \in \Lambda \) which generates \( \text{char}_\Lambda \text{X}(H_\infty^+) \).

We note the important fact that there is no prime lying above \( p \) which splits in \( H_\infty^+/H_\infty^+ \) (because \( p \) does not ramify in \( K'/\mathbb{Q} \)). This implies that \( g(T) \) is relatively prime to \( T \). (We remark that \( H \) is not abelian over \( \mathbb{Q} \), however, this assertion holds. See, e.g., [3].)

Put \( h(T) = g(\text{1}_{T} + \text{1}_{T} - 1) \in \Lambda \). Then, by Kummer duality, we see that \( h(T) \) generates \( \text{char}_\Lambda \mathcal{X}_{(p)}(H_\infty^+) \). (Note that we can see that
\[
\mathcal{X}_{(p)}(H_\infty^+) \cong \text{Hom}_{\mathbb{Z}_p}(A(H_\infty^-), W_{p^{\infty}}),
\]
where \( A(H_\infty^-) \) is the minus part of \( \text{lim} \ A(H_n) \) and \( W_{p^{\infty}} \) is the group of all \( p \)-power roots of unity. Moreover, from a well known argument using the adjoint, we can obtain this fact. See, e.g., [47 Chapters 13, 15].) Hence we see that \( \mathcal{X}_{(p)}(H_\infty^+) \) is finitely generated as a \( \mathbb{Z}_p \)-module, and \( h(T) \) is relatively prime to \( T - p \). By using [36 (11.3.5)Theorem] (see also its proof), we can see that
\[
(T - p)^m h(T) \quad \text{generates} \quad \text{char}_\Lambda \mathcal{X}_{(p,q_3)}(H_\infty^+).
\]
(Note that there are \( m \) primes in \( H^+ \) lying above \( q_3 \), and they does not split in \( H_\infty^+ \). Actually, we can know the structure of \( \mathcal{X}_{(p,q_3)}(H_\infty^+) \) more precisely.)

The remaining part of the proof is similar to that given in [15 pp.522–525] (for “Case NS”). Let \( M' \) be the intermediate field of \( M_{(p,q_3)}(H_\infty^+)/(L(H_\infty^+)) \) corresponding to
\[
(T - p) \text{Gal}(M_{(p,q_3)}(H_\infty^+))/(L(H_\infty^+)).
\]
We see that both \( L_{(q_3)}(H_\infty^+) \) and \( L(H_\infty^+) \) are intermediate fields of \( M'/L(H_\infty^+) \). By using [4], we can show that \( \text{rank}_{\mathbb{Z}_p} \text{Gal}(M'/L(H_\infty^+)) = m \). Let \( I' \) be the subgroup of \( \text{Gal}(M'/H_\infty^+) \) generated by the inertia subgroups for the primes lying above \( p \). Then we can see \( \text{rank}_{\mathbb{Z}_p} I' = m \) by using [3]. Hence \( L_{(q_3)}(H_\infty^+)/L(H_\infty^+) \) is a finite extension. □

Corollary 5.2.2. Let the assumptions be as in Theorem 1.4.2 and \( K' \) as in Definition 5.1.2. Then, \( \mathcal{X}_{(q_3)}(K'_\infty) \) is finite.

Proof. Let \( H^+ \) be as in Definition 5.1.2. We see that \( \text{Gal}(L_{(q_3)}(H_\infty^+)/L(H_\infty^+)) \) is finite by Proposition 5.2.1. Then we can show that \( \text{Gal}(L_{(q_3)}(K'_{\infty})/L(K'_{\infty})) \) is also finite (see, e.g., [15 Lemma 2.1]). By Lemma 5.1.2 we see that \( \text{Gal}(L(K'_n)/K'_n) \) is trivial. Thus the assertion follows. □

Remark 5.2.3. In the last line of the proof of [15 Lemma 2.1], “\( \text{Gal}(M_q(k'_n)/L(k'_n)) \)” should be read “\( \text{Gal}(M_q(k_n)/L(k_n)) \)”.

Now we shall finish the proof of Theorem 1.4.2
Proof of Theorem 1.4.2. Let $K'$ be as in Definition 5.1.2. We shall give an upper bound of \( \text{rank}_{\mathbb{Z}_p} X_S(K'_\infty) \) by using (a rough version of) the known method (see, e.g., [35], [18]).

For \( q \in S(K') \), we put \( R_n(q) = (O_{K'_q} / q_n)^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \), where \( q_n \) is the extension of \( q \) in \( K'_n \). We also put \( R_\infty(q) = \lim_{n \to \infty} R_n(q) \). Since \( |(O_{K'/q})^\times| \) is divisible by \( p \) and \( q \) is not decomposed in \( K'_\infty \), we see that \( R_\infty(q) \cong \mathbb{Z}_p \) (as a \( \mathbb{Z}_p \)-module) for every \( q \in S(K') \).

Recall that there is only one prime of \( K' \) lying above \( q_i \) (for \( i = 1, 2 \)), and there are \( p \) primes of \( K' \) lying above \( q_j \) (for \( j = 3, \ldots, r \)). We put

\[
R_\infty(S) = \bigoplus_{q \in S(K')} R_\infty(q) \quad \text{and} \quad R_\infty(q_3) = \bigoplus_{q \in S(K'), q \in q_3} R_\infty(q).
\]

By using class field theory (and Lemma 5.1.3), we obtain the following exact sequences

\[
\lim_{\to}(E(K'_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p) \xrightarrow{f_1} R_\infty(S) \to X_S(K'_\infty) \to 0,
\]

\[
\lim_{\to}(E(K'_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p) \xrightarrow{f_2} R_\infty(q_3) \to X_{(q_3)}(K'_\infty) \to 0.
\]

By Corollary 5.2.2, \( X_{(q_3)}(K'_\infty) \) is finite. This implies that the \( \mathbb{Z}_p \)-rank of the image of \( f_2 \) is \( p \) (recall that \( \text{rank}_{\mathbb{Z}_p} R_\infty(q_3) = p \)). Then, we see that the \( \mathbb{Z}_p \)-rank of the image of \( f_1 \) is greater than or equal to \( p \). Since

\[
\text{rank}_{\mathbb{Z}_p} R_\infty(S) = p(r - 2) + 2,
\]

we have obtained the inequality

\[
\text{rank}_{\mathbb{Z}_p} X_S(K'_\infty) \leq p(r - 2) + 2 - p.
\]

Then Theorem 1.4.2 follows from Proposition 5.1.4. \qed

Acknowledgements. The author would express his thanks to Manabu Ozaki for giving motivation and advice. The author also express thanks to Yutaka Konomi for giving information around his paper [27]. This work was partly supported by JSPS KAKENHI Grant Number JP15K04791.

Note on the computational results given in [19]. As mentioned in [8], there is a problem in the programs used in the computations of [19, Section 5]. We explain the details. The Magma command \texttt{RayClassGroup} returns a “guaranteed” result only when the ideal class group was computed in advance. See [2, Chapter 40]. However, the process of computing the ideal class group in advance was omitted in the programs used in the research of [19] (as was confirmed by the author himself). Hence, it has to be said that the computational results given [19, Section 5] were “not guaranteed by Magma” at the time when that paper was published.

Thus, the author re-computed the ray class groups by using a method to obtain results guaranteed by Magma. (The author used the same defining polynomials of number fields which were used in the original programs. Hence, the defining polynomials given in [25], [8] were also used in this re-computation.) Consequently, it was checked that the values given in the tables of [19] coincide with the values obtained by this re-computation. (Hence we do not need a correction of the values.)

Thanks to Shun’ichi Yokoyama and the Magma staff (especially Nicole Sutherland) for answering questions and giving advice. The author wrote this note with the consent of the co-author of [19].
References

[1] J. Blondeau, P. Lebacque, and C. Maire: On the cohomological dimension of some pro-$p$-extensions above the cyclotomic $\mathbb{Z}_p$-extension of a number field, Mosc. Math. J. 13 (2013), 601–619.

[2] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.): Handbook of Magma functions, Edition 2.23 (2017), 5914 pages.

[3] D. Brink: Prime decomposition in the anti-cyclotomic extension, Math. Comp. 76 (2007), 2127–2138.

[4] A. Brumer: On the units of algebraic number fields, Mathematika 14 (1967), 121–124.

[5] L. J. Federer and B. H. Gross (with an appendix by W. Sinnott): Regulators and Iwasawa modules, Invent. Math. 62 (1981), 443–457.

[6] B. Ferrero and L. C. Washington: The Iwasawa invariant $\mu_p$ vanishes for abelian number fields, Ann. of Math. (2) 109 (1979), 377–395.

[7] S. Fujii: 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), 101–110.

[8] S. Fujii and T. Itoh: Some remarks on pseudo-null submodules of tamely ramified Iwasawa modules, J. Théor. Nombres Bordeaux 30 (2018), 533–555.

[9] T. Fukuda: Remarks on $\mathbb{Z}_p$-extensions of number fields, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), 264–266.

[10] T. Fukuda and K. Komatsu: On the $\lambda$ invariants of $\mathbb{Z}_p$-extensions of real quadratic fields, J. Number Theory 23 (1986), 238–242.

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

[12] R. Greenberg: Iwasawa theory—past and present, Class field theory—its centenary and prospect, 335–385, Adv. Stud. Pure. Math. 30, Math. Soc. Japan, Tokyo, 2001.

[13] Y. Hachimori: Iwasawa theory for extensions with restricted $p$-ramification, Tokyo J. Math. 26 (2003), 179–198.

[14] D. Hubbard and L. C. Washington: Kummer generators and lambda invariants, J. Number Theory 130 (2010), 61–81.

[15] T. Itoh: On tamely ramified Iwasawa modules for the cyclotomic $\mathbb{Z}_p$-extension of abelian fields, Osaka J. Math. 51 (2014), 513–536.

[16] T. Itoh: Tamely ramified Iwasawa modules having no non-trivial pseudo-null submodules, accepted in J. Théor. Nombres Bordeaux.

[17] T. Itoh and Y. Mizusawa: On tamely ramified pro-$p$-extensions over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, Math. Proc. Cambridge Philos. Soc. 156 (2014), 281–294.

[18] T. Itoh, Y. Mizusawa, and M. Ozaki: On the $\mathbb{Z}_p$-ranks of tamely ramified Iwasawa modules, Int. J. Number Theory 9 (2013), 1491–1503.

[19] T. Itoh and Y. Takakura: On tamely ramified Iwasawa modules for $\mathbb{Z}_p$-extensions of imaginary quadratic fields, Tokyo J. Math. 37 (2014), 405–431.

[20] K. Iwasawa: A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[21] K. Iwasawa: On the $\mu$-invariants of $\mathbb{Z}_l$-extensions, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, 1–11, Kinokuniya, Tokyo, 1973.

[22] K. Iwasawa: Riemann-Hurwitz formula and $p$-adic Galois representations for number fields, Tôhoku Math. J. (2) 33 (1981), 263–288.

[23] T. Kataoka: A consequence of Greenberg’s generalized conjecture on Iwasawa invariants of $\mathbb{Z}_p$-extensions, J. Number Theory 172 (2017), 200–233.

[24] C. Khare and J.-P. Wintenberger: Ramification in Iwasawa theory and splitting conjectures, Int. Math. Res. Not. IMRN 2014 (2014), 194–223.

[25] J. M. Kim and J. Oh: Defining polynomial of the first layer of anti-cyclotomic $\mathbb{Z}_5$-extension of imaginary quadratic fields of class number 1, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), 18–19.

[26] H. Koch: Galois theory of $p$-extensions, Springer Monographs in Mathematics. Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[27] Y. Konno: The ideal class groups of dihedral extensions over imaginary quadratic fields and the special values of the Artin $L$-function, J. Number Theory 131 (2011), 1062–1069.
[28] J. S. Kraft and L. C. Washington: Heuristics for class numbers and lambda invariants, Math. Comp. 76 (2007), 1005–1023.
[29] M. Kurihara: Remarks on the $\lambda_p$-invariants of cyclic fields of degree $p$, Acta Arith. 116 (2005), 199–216.
[30] F. Lemmermeyer: Class groups of dihedral extensions, Math. Nachr. 278 (2005), 679–691.
[31] Y. Mizusawa: Iwapoly.gp (PARI/GP function), available from http://mizusawa.web.nitech.ac.jp/Iwapoly/index.html.
[32] Y. Mizusawa: On the maximal unramified pro-$2$-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field, J. Théor. Nombres Bordeaux 22 (2010), 115–138.
[33] Y. Mizusawa: Tame pro-$2$ Galois groups and the basic $\mathbb{Z}_2$-extension, Trans. Amer. Math. Soc. 370 (2018), 2423–2461.
[34] Y. Mizusawa and M. Ozaki: Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, Math. Ann. 347 (2010), 437–453.
[35] Y. Mizusawa and M. Ozaki: On tame pro-$p$ Galois groups over basic $\mathbb{Z}_p$-extensions, Math. Z. 273 (2013), 1161–1173.
[36] J. Neukirch, A. Schmidt, and K. Wingberg: Cohomology of number fields, Second edition, Grundlehren Math. Wiss., 323, Springer-Verlag, Berlin, Heiderberg, 2008.
[37] K. Okano: Abelian $p$-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields, Acta Arith. 125 (2006), 363–381.
[38] M. Ozaki: A note on the capitulation in $\mathbb{Z}_p$-extensions, Proc. Japan Acad. Ser. A Math. Sci. 71 (1995), 218–219.
[39] M. Ozaki: Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions, J. Reine Angew. Math. 602 (2007), 59–94.
[40] The PARI-Group: PARI/GP version 2.11.0, Univ. Bordeaux, 2018, http://pari.math.u-bordeaux.fr/.
[41] L. Salle: Sur les pro-$p$-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d’un corps de nombres, J. Théor. Nombres Bordeaux 20 (2008), 485–523.
[42] L. Salle: On maximal tamely ramified pro-$2$-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field, Osaka J. Math. 47 (2010), 921–942.
[43] J.-P. Serre: Galois cohomology, Springer Monographs in Mathematics. Springer-Verlag, Berlin, Heidelberg, 1997, 2002 (second printing).
[44] R. T. Sharifi: Massey products and ideal class groups, J. Reine Angew. Math. 603 (2007), 1–33.
[45] R. T. Sharifi: On Galois groups of unramified pro-$p$ extensions, Math. Ann. 342 (2008), 297–308.
[46] W. Sinnott: On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980), 181–234.
[47] L. C. Washington: Introduction to cyclotomic fields, Second edition, Graduate Texts in Math. 83, Springer-Verlag, New York, Berlin, Heidelberg, 1997.

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