A REMARK ON GREENBERG’S GENERALIZED CONJECTURE FOR IMAGINARY $S_3$-EXTENSIONS OF $\mathbb{Q}$

TSUYOSHI ITOH

Abstract. Let $K/\mathbb{Q}$ be an imaginary $S_3$-extension, and $p$ a prime number which splits into exactly three primes in $K$. We give a sufficient condition for the validity of Greenberg's generalized conjecture for $K$ and $p$.

1. Introduction

Let $p$ be a prime number. We recall the statement of Greenberg’s generalized conjecture (GGC) for an algebraic number field $K_0$ and $p$. We denote by $\tilde{K}_0$ the composite of all $\mathbb{Z}_p$-extensions of $K_0$. Then, the Galois group $\text{Gal}(\tilde{K}_0/K_0)$ is topologically isomorphic to $\mathbb{Z}^{d_p}$ with some positive integer $d$. Let $L(\tilde{K}_0)/\tilde{K}_0$ be the maximal unramified abelian pro-$p$ extension. We put $X(\tilde{K}_0) = \text{Gal}(L(\tilde{K}_0)/\tilde{K}_0)$. We denote by $\Lambda_{\text{Gal}(\tilde{K}_0/K_0)}$ the completed group ring $\mathbb{Z}_p[[\text{Gal}(\tilde{K}_0/K_0)]]$. It is well known that $X(\tilde{K}_0)$ is a finitely generated torsion module over $\Lambda_{\text{Gal}(\tilde{K}_0/K_0)}$ (see [5, Theorem 1]).

Greenberg’s generalized conjecture ([6 Conjecture (3.5)]). $X(\tilde{K}_0)$ is a pseudo-null $\Lambda_{\text{Gal}(\tilde{K}_0/K_0)}$-module. That is, there are two relatively prime elements of $\Lambda_{\text{Gal}(\tilde{K}_0/K_0)}$ such that both annihilate $X(\tilde{K}_0)$.

Minardi [14] studied GGC, mainly for imaginary quadratic fields. After that, many authors gave sufficient conditions for the validity of GGC in various situations. For example, see the author [8], Fujii [3], Kleine [12], Kataoka [11], Takahashi [18]. In [18, Remark 1.3], several known results are stated in detail. See also Assim-Boughadi [1] and the results referred there. We also mention Murakami [15] as a recent result.

In the present paper, we consider GGC for the following $K$ and $p$. Let $K/\mathbb{Q}$ be an imaginary Galois extension whose Galois group is isomorphic to the symmetric group $S_3$ of degree 3. We assume that $p$ splits into three primes $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ in $K/\mathbb{Q}$.

There is a unique imaginary quadratic field $k$ contained in $K$. In our situation, $p$ is not decomposed in $k$, and the unique prime of $k$ lying above $p$ is completely decomposed in $K$. For each $i \in \{1, 2, 3\}$, let $K_{\mathfrak{p}_i}$ be the completion of $K$ at $\mathfrak{p}_i$. Then $[K_{\mathfrak{p}_i} : \mathbb{Q}_p] = 2$ for every $i$.

The decomposition field $F$ of $K/\mathbb{Q}$ for $\mathfrak{p}_1$ is a complex cubic field. We denote by $\mathfrak{p}$ the prime of $F$ lying below $\mathfrak{p}_1$. There is just one more prime $\mathfrak{p}^*$ of $F$ lying above $p$, which splits into two primes $\mathfrak{p}_2$, $\mathfrak{p}_3$ in $K/F$. We note that $[F_\mathfrak{p} : \mathbb{Q}_p] = 1$ and $[F_{\mathfrak{p}^*} : \mathbb{Q}_p] = 2$, where $F_\mathfrak{p}$ (resp. $F_{\mathfrak{p}^*}$) is the completion of $F$ at $\mathfrak{p}$ (resp. $\mathfrak{p}^*$). It is known that there exists a unique $\mathbb{Z}_p$-extension $N^*/F$ unramified outside $\mathfrak{p}^*$ (see [11 Lemma 3.4 (2)]).

Our main result is the following:

2020 Mathematics Subject Classification. 11R23
Key Words : Greenberg’s generalized conjecture, $\mathbb{Z}_p^{\otimes d}$-extensions.
**Theorem 1.1.** Let the notation be as above. Moreover, let $M_{\mathfrak{P}_3}(K)/K$ be the maximal abelian pro-$p$ extension unramified outside $\mathfrak{P}_3$. Assume that all of the following conditions are satisfied:

(C1) $p$ is finitely decomposed in $N^*$,

(C2) $p^*$ is not decomposed in $N^*$, and

(C3) $\mathfrak{P}_2$ is not decomposed in $M_{\mathfrak{P}_3}(K)$.

Then, GGC for $K$ and $p$ holds.

**Remark 1.2.** $M_{\mathfrak{P}_3}(K)/K$ is known to be a finite extension (see Section 2). The condition (C1) is equivalent to [11] Assumption 3.1 (when the complex cubic field has two primes dividing $p$). It seems unknown whether (C1) always holds or not (see also [11] Remark 3.2 (2)], [7] Sections 7.2 and 7.3). However, (C1) was confirmed to be satisfied for many cases (see Remark 1.3).

**Remark 1.3.** Kataoka [11] gave sufficient conditions for the validity of GGC for complex cubic fields (he treated all cases of decomposition on $p$). Compare our Theorem 1.1 with [11] Theorem 3.3 (1), (2)]. In particular, by using [11] Theorem 3.3 (2)], we see that GGC for (our) $F$ and $p$ also holds under the assumptions (C1), (C2), (C3). To show [11] Theorem 3.3 (2)], Kataoka used $N^*/F$ as the first step of his proof ([11] Proposition 3.5 (2)]). We use $N^*/K$ as the first step. However, $\widetilde{F}$ is not used in our proof.

**Remark 1.4.** Assume that $p = 3$. When $K$ is contained in $\tilde{k}$, the validity of GGC for $k$ and $p$ implies the validity of GGC for $K$ and $p$. See [14] p.43, Remarks (ii)]. However, in our case, if $K$ is contained in $\tilde{k}$, then $K/k$ is an unramified extension, hence the validity of GGC for $k$ and $p$ seems non-trivial (see, e.g., [14] Section 3.D]). Incidentally, for the case where $p = 2$, we see that $K$ is never contained in $\tilde{F}$ because the real archimedean prime of $F$ ramifies in $K$. For a somewhat related result, see also [12] Corollary 4.4.

We give several preparations in Sections 2. We shall show Theorem 1.1 in Section 3. We will give examples in Section 4.

## 2. Preliminaries

First, we define several notation and recall well known facts. We denote by $|A|$ the cardinality of a set $A$. We also denote by $\text{rank}_{\mathbb{Z}_p}B$ the $\mathbb{Z}_p$-rank of a finitely generated $\mathbb{Z}_p$-module $B$. For a pro-$p$ group $G$ which is topologically isomorphic to $\mathbb{Z}_p^d$ with some positive integer $d$, let $\Lambda_G$ be the the completed group ring $\mathbb{Z}_p[[G]]$. We use the notation defined in Section 1.

In this paragraph, we denote by $K$ an algebraic extension of $K$. Let $L(K)/K$ be the maximal unramified abelian pro-$p$ extension, and put $X(K) = \text{Gal}(L(K)/K)$. We denote by $S_p$ the set $\{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$. For a non-empty subset $S$ of $S_p$, let $M_S(K)/K$ be the maximal abelian pro-$p$ extension unramified outside $S$, and put $\mathfrak{x}_S(K) = \text{Gal}(M_S(K)/K)$. For the case where $S = \{\mathfrak{P}_i\}$, we shall write them $M_{\mathfrak{P}_i}(K)$, $\mathfrak{x}_{\mathfrak{P}_i}(K)$ in short.

For $i \in \{1, 2, 3\}$, let $U_i$ be the group of principal units in $K_{\mathfrak{P}_i}$, and put $U = \bigoplus_{i=1}^3 U_i$. Let $E_K$ be the group of units in $K$, and put

$$E'_K = \{\varepsilon \in E_K \mid \varepsilon \equiv 1 \pmod{\mathfrak{P}_i} \text{ for every } i \in \{1, 2, 3\}\}.$$  

We denote by $E'$ the image of the mapping $E'_K \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \rightarrow U$ induced from the diagonal embedding

$$E'_K \rightarrow U = U_1 \oplus U_2 \oplus U_3, \quad \varepsilon \mapsto (\varepsilon, \varepsilon, \varepsilon).$$
(see, e.g., [9, Appendix]). By class field theory, $U/\mathcal{E}$ is isomorphic to $\text{Gal}(M_{S_p}(K)/L(K))$. It is known that Leopoldt’s conjecture holds for $K$ and $p$ since $K$ is an abelian extension of an imaginary quadratic field (see [2]). Then, $\text{rank}_{\mathbb{Z}} U$ is 2, which is equal to the free rank of $E_K$. Since $\text{rank}_{\mathbb{Z}} U$ is 6, we see that $\text{rank}_{\mathbb{Z}} \text{Gal}(M_{S_p}(K)/L(K))$ is 4. Hence, $\tilde{K}/K$ is a $\mathbb{Z}_p^{\oplus 4}$-extension.

Next, we shall state several results which will be used in the proof of Theorem 1.1. Recall that $N^* F$ is the $\mathbb{Z}_p$-extension unramified outside $p^*$. We put $N^{(1)} = N^* K$, which is a $\mathbb{Z}_p$-extension of $K$. The following result is crucial to prove Theorem 1.1.

**Theorem A** (Maire [13]). For a non-negative integer $n$, let $N^{(1)}_n$ be the $n$th layer of $N^{(1)}/K$. Then for every $n$, $\mathfrak{X}_{\mathfrak{P}} (N^{(1)}_n)$ is finite. In particular, $\mathfrak{X}_{\mathfrak{P}} (K)$ is finite.

**Proof.** We recall the following facts: $N^{(1)}_n/F$ is an abelian extension, $\mathfrak{P}_1$ is the unique prime of $K$ lying above $p$, $[F_p : \mathbb{Q}_p] = 1$, and $[F : \mathbb{Q}] = 3$. Then we can apply [13, Theorem 25], and the assertion follows.

We can also see that both $\mathfrak{X}_{\mathfrak{P}_1} (K)$ and $\mathfrak{X}_{\mathfrak{P}_2} (K)$ are finite.

We note that Hachimori [7] treated similar situation to ours. In particular, it seems that he essentially showed a result similar to Theorem A for the cyclotomic $\mathbb{Z}_p$-extension of $K$ (see the proofs of [7, Theorems 6.2 and 7.3]).

**Corollary 2.1.** We put $S = \{\mathfrak{P}_i, \mathfrak{P}_j\}$ with $1 \leq i < j \leq 3$. Then $\text{rank}_{\mathbb{Z}} \mathfrak{X}_S (K)$ is 2.

**Proof.** Since $K/\mathbb{Q}$ is a Galois extension, it is sufficient to show only for the case where $S = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. This corollary follows from the basic result on abelian pro-$p$ extensions with restricted ramification (see, e.g., [13, Theorem 5], [7, Proposition 3.1]). Theorem A (for $K$) asserts that the image of $E'_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow \mathcal{U}_1$ has $\mathbb{Z}_p$-rank 2. Then the image of the mapping $E'_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrow \mathcal{U}_1 \oplus \mathcal{U}_2$ induced from the diagonal embedding also has $\mathbb{Z}_p$-rank 2. Since $\text{rank}_{\mathbb{Z}} (\mathcal{U}_1 \oplus \mathcal{U}_2)$ is 4, the assertion has been shown.

**Definition 2.2.** Let $\mathcal{K}/K$ be an abelian (finite or infinite) extension, and $\mathcal{K}'$ an intermediate field of $\mathcal{K}/K$. For $i \in \{1, 2, 3\}$, we define the following symbols.

- $D_i(\mathcal{K}/\mathcal{K}')$ : the decomposition subgroup of $\text{Gal}(\mathcal{K}/\mathcal{K}')$ for a prime lying above $\mathfrak{P}_i$.
- $I_i(\mathcal{K}/\mathcal{K}')$ : the inertia subgroup of $\text{Gal}(\mathcal{K}/\mathcal{K}')$ for a prime lying above $\mathfrak{P}_i$.

Since $\mathcal{K}/K$ is abelian, these groups are uniquely determined independent on the choice of a prime lying above $\mathfrak{P}_i$.

**Lemma 2.3.** Assume that the condition (C1) in Theorem 1.1 is satisfied. Then, $\text{rank}_{\mathbb{Z}} I_i(\tilde{K}/K) = 2$ and $\text{rank}_{\mathbb{Z}} D_i(\tilde{K}/K) = 3$ for every $i \in \{1, 2, 3\}$.

**Proof.** Since $\text{rank}_{\mathbb{Z}} \mathcal{U}_i$ is 2, we see that $\text{rank}_{\mathbb{Z}} I_i(\tilde{K}/K)$ is at most 2, and $\text{rank}_{\mathbb{Z}} D_i(\tilde{K}/K)$ is at most 3. We shall construct a $\mathbb{Z}_p^{\oplus 3}$-extension such that the inertia and decomposition subgroups have the maximal $\mathbb{Z}_p$-rank.

It is sufficient to show the assertion for $i = 1$. By Corollary 2.1 there is a unique $\mathbb{Z}_p^{\oplus 2}$-extension $N^*/K$ unramified outside $\{\mathfrak{P}_1, \mathfrak{P}_2\}$. By Theorem A, we see that $\text{rank}_{\mathbb{Z}} I_1(N^*/K)$ must be 2. From this fact, we also see that $N^{(1)} \cap N^*/K$ is a finite extension (note that
$N^{(1)}/K$ is unramified at $\Psi_1$). Then, $N^{(1)}N^2/K$ is a $\mathbb{Z}_p^{\oplus 3}$-extension. We assumed that (C1) is satisfied, that is, $\Psi_1$ is finitely decomposed in $N^{(1)}/K$. Combining these facts, we see that
\[
\text{rank}_{\mathbb{Z}_p} I_1(N^{(1)}N^2/K) = 2 \quad \text{and} \quad \text{rank}_{\mathbb{Z}_p} D_1(N^{(1)}N^2/K) = 3.
\]

The assertion of this lemma follows from the facts stated in the previous paragraph. □

**Remark 2.4.** We do not need the satisfaction of (C1) to show $\text{rank}_{\mathbb{Z}_p} I_1(\tilde{K}/K) = 2$. (There is another approach to show this fact by using $\tilde{k}/k$. See [14, Section 3].) One can show that the infiniteness of $D_1(\tilde{K}/K)/I_1(\tilde{K}/K)$ is equivalent to the satisfaction of (C1). Note that Minardi also considered the infiniteness of $D_1(\tilde{K}/K)/I_1(\tilde{K}/K)$ for certain $S_3$-extensions $K/\mathbb{Q}$ (see [14, Sections 3, 6]). In it, he mentioned the equivalence of the infiniteness of $D_1(\tilde{K}/K)/I_1(\tilde{K}/K)$ and the validity of the conjecture called “Jaulent’s conjecture” (a conjecture which seems to be derived from [10, p.155, Conjecture]) there.

**Proposition 2.5.** (i) Assume that the condition (C1) in Theorem 1.1 is satisfied. Then, $\text{rank}_{\mathbb{Z}_p} (D_2(\tilde{K}/K) \cap D_3(\tilde{K}/K))$ is 2.

(ii) $I_1(\tilde{K}/K) \cap D_2(\tilde{K}/K) \cap D_3(\tilde{K}/K)$ is trivial.

**Proof.** We shall show (i). Let $K^{\Psi_2}$ (resp. $K^{\Psi_3}$) be the decomposition field of $\tilde{K}/K$ for $\Psi_2$ (resp. $\Psi_3$). As a consequence of Lemma 2.3, we see that both $\text{rank}_{\mathbb{Z}_p} \text{Gal}(K^{\Psi_2}/K)$ and $\text{rank}_{\mathbb{Z}_p} \text{Gal}(K^{\Psi_3}/K)$ are 1. By using Theorem A, we can see that $K^{\Psi_2} \cap K^{\Psi_3}/K$ is a finite extension. Hence, the $\mathbb{Z}_p$-rank of $\text{Gal}(K^{\Psi_2}K^{\Psi_3}/K)$ is 2. Since $K^{\Psi_2}K^{\Psi_3}$ corresponds to $D_2(\tilde{K}/K) \cap D_3(\tilde{K}/K)$, we obtain (i).

To show (ii), we first give several preparations. Let $\sigma, \tau_1$ be elements of $\text{Gal}(K/\mathbb{Q})$ such that $\sigma$ generates $\text{Gal}(K/k)$ and $\tau_1$ generates $\text{Gal}(K/F)$. Assume that $\sigma(\Psi_1) = \Psi_2$ and $\sigma^2(\Psi_1) = \Psi_3$. Then $\sigma \tau_1 \sigma^{-1} \text{fixes } \Psi_2$ and $\sigma^2 \tau_1 \sigma^{-2} \text{fixes } \Psi_3$.

We can take $\varepsilon_1 \in E^*_K$ satisfying the following conditions: $\tau_1(\varepsilon_1) = \varepsilon_1, \varepsilon_1 \sigma(\varepsilon_1) \sigma^2(\varepsilon_1) = 1$, and $\varepsilon_1, \sigma(\varepsilon_1)$ are multiplicative independent. We put $\varepsilon_2 = \sigma(\varepsilon_1)$ and $\varepsilon_3 = \sigma^2(\varepsilon_1)$. Since Leopoldt’s conjecture holds for $K$ and $p$, we see that the image of
\[
\langle \varepsilon_1, \varepsilon_2 \rangle \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathcal{U}
\]
has $\mathbb{Z}_p$-rank 2.

We can also take a $\Psi_1$-unit $\pi_1$ of $K$ satisfying the following conditions: $\pi_1$ generates a positive power of $\Psi_1$, $\tau_1(\pi_1) = \pi_1$, and $\pi_1 \equiv 1 \pmod{\Psi_1}$ for every $i \in \{2, 3\}$. We put $\pi_2 = \sigma(\pi_1)$ and $\pi_3 = \sigma^2(\pi_1)$. Then $\pi_2$ (resp. $\pi_3$) is a $\Psi_2$-unit (resp. $\Psi_3$-unit). We shall define the subgroups $D_2, D_3$ of $\mathcal{U} = U_1 \oplus U_2 \oplus U_3$ as the following:
\[
D_2 = \{ (\pi_2^x, u_2, \pi_3^y) \mid x \in \mathbb{Z}_p, u_2 \in U_2 \}, \quad D_3 = \{ (\pi_3^x, \pi_3^y, u_3) \mid y \in \mathbb{Z}_p, u_3 \in U_3 \}.
\]

By class field theory, the image of $D_2 \to \mathcal{U}/\mathcal{E}$ (resp. $D_3 \to \mathcal{U}/\mathcal{E}$) corresponds to a finite index subgroup of $D_{\Psi_2}(M_{\mathbb{Q}_p}(K)/K)$ (resp. $D_{\Psi_3}(M_{\mathbb{Q}_p}(K)/K)$) (cf. [14, pp.24–25]). We also note that the image of
\[
\{ (u_1, 1, 1) \mid u_1 \in U_1 \} \to \mathcal{U}/\mathcal{E}
\]
corresponds to $I_{\Psi_1}(M_{\mathbb{Q}_p}(K)/K)$.

We claim that
\[
I_{\Psi_1}(M_{\mathbb{Q}_p}(K)/K) \cap D_{\Psi_2}(M_{\mathbb{Q}_p}(K)/K) \cap D_{\Psi_3}(M_{\mathbb{Q}_p}(K)/K)
\]
is finite. Since $M_{S_p}(K)/\tilde{K}$ is a finite extension and $\text{Gal}(\tilde{K}/K)$ is $\mathbb{Z}_p$-torsion free, the assertion of (ii) follows from this claim.

In the remaining part, we shall give a proof of the above claim. We take an element $u_1 \in U_1$ such that the class $(u_1, 1, 1)$ corresponds to the element of $X_{S_p}(K)$ contained in $D_{p_1}(M_{S_p}(K)/K) \cap D_{p_2}(M_{S_p}(K)/K)$. Then, there exists a non-zero integer $n$ such that $(u_1^n, 1, 1)$ is contained in both the image of $D_2 \to U/E$ and the image of $D_3 \to U/E$. That is, there exist

$$\varepsilon, \varepsilon' \in E_{K}^r \otimes_{\mathbb{Z}} \mathbb{Z}_p, \ x, y \in \mathbb{Z}_p, \ u_2 \in U_2, \ u_3 \in U_3$$

such that

$$(u_1^n \varepsilon, \varepsilon, \varepsilon) = (\pi_x^n, u_2, \pi_2^x) \ \text{and} \ (u_1^n \varepsilon', \varepsilon', \varepsilon') = (\pi_3^n, \pi_3, u_3) \ \text{in} \ U.$$

By retaking $n$ if necessary, we may assume that $\varepsilon, \varepsilon'$ are the elements of $E_{K}^r \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Hence we write $\varepsilon = \varepsilon_1^a \varepsilon_2^a$ and $\varepsilon' = \varepsilon_1^b \varepsilon_2^b$ with $a_1, a_2, b_1, b_2 \in \mathbb{Z}_p$. By summarizing them, we see that

$$(1) \quad u_1^n \varepsilon_1^a \varepsilon_2^a = \pi_x^n, \ u_1^n \varepsilon_1^b \varepsilon_2^b = \pi_3^n \ \text{in} \ U_1,$$

$$(2) \quad \varepsilon_1^a \varepsilon_2^a = u_2, \ \varepsilon_1^b \varepsilon_2^b = \pi_3^x \ \text{in} \ U_2,$$

$$(3) \quad \varepsilon_1^a \varepsilon_2^a = \pi_x^n, \ \varepsilon_1^b \varepsilon_2^b = u_3 \ \text{in} \ U_3.$$

The second equation of (2) can be rewritten as the following:

$$(4) \quad \varepsilon_1^b \varepsilon_2^b = \pi_3^n \ \text{in} \ U_1.$$

The first equation of (3) can be rewritten as the following:

$$(5) \quad \varepsilon_3^a \varepsilon_2^a \ (= \varepsilon_1^a \varepsilon_2^{-a_1+a_2}) = \pi_x^n \ \text{in} \ U_1.$$

Then, combining (4), (5) with (1), we obtain the following equations:

$$u_1^n \varepsilon_1^a \varepsilon_2^a = \varepsilon_1^{-a_1} \varepsilon_2^{-a_1+a_2}, \ u_1^n \varepsilon_1^b \varepsilon_2^b = \varepsilon_1^b \varepsilon_2^b \ \text{in} \ U_1.$$ 

Hence

$$\varepsilon_1^{-a_1} \varepsilon_2^{-a_1} = \varepsilon_1^{b_1-b_1} \varepsilon_2^{b_1-b_2} \ \text{in} \ U_1$$

We note that the image of $E_{K}^r \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $U_1$ has $\mathbb{Z}_p$-rank 2 by Theorem A. This implies that

$$-2a_1 = b_2 - b_1, \ -a_1 = b_1 - b_2$$

and then $a_1 = 0$. Therefore, we see that $u_1^n = 1$. Our claim follows from this. \hfill $\Box$

At the end of this section, we introduce the following result, which is a specialized version of [14, Proposition 4.B].

**Proposition B** (Minardi [14]). Let $K/K$ be a $\mathbb{Z}_p^{\oplus d}$-extension ($d$ is 3 or 4). Assume that there exists an intermediate $\mathbb{Z}_p^{\oplus d-1}$-extension $\mathcal{K}/K$ of $K/K$ satisfying the following property: for every $i \in \{1, 2, 3\}$ such that $I_i(K/K')$ is not trivial, rank$_{\mathbb{Z}_p} D_i(K'/K) \geq 2$. Under this assumption, the pseudo-nullity of $X(K')$ as a $\Lambda_{\text{Gal}(K'/K)}$-module implies the pseudo-nullity of $X(K)$ as a $\Lambda_{\text{Gal}(K/K')}$-module.
3. Proof of Theorem 1.1

We use the well known method, which was used in Minardi [14] and several other authors. That is, we take a sequence of $\mathbb{Z}_p^{\oplus d}$-extensions $N^{(1)} \subset N^{(2)} \subset N^{(3)} \subset \overline{K}$, and show the pseudo-nullity inductively.

Let the notation be as in the previous sections. In the following, we assume that all of the conditions (C1), (C2), (C3) of Theorem 1.1 are satisfied.

Recall that $N^*/F$ is the $\mathbb{Z}_p$-extension unramified outside $p^\infty$, and $N^{(1)} = N^*/K$. $\mathcal{P}_1$ is unramified and finitely decomposed in $N^{(1)}$ by the assumption on (C1). Both $\mathcal{P}_2$ and $\mathcal{P}_3$ are ramified in $N^{(1)}/K$. Moreover, both $\mathcal{P}_2$ and $\mathcal{P}_3$ are not decomposed in $N^{(1)}$ by the assumption on (C2). (This is satisfied even when $p = 2$, because $p^\infty$ is decomposed in $K$.)

**Proposition 3.1.** $X(N^{(1)})$ is finite.

**Proof.** Note that our situation is quite similar to that of [11, Proposition 3.5 (1)], and the following proof is also essentially the same.

In this proof, we abbreviate $M_{\mathcal{P}_3}(K)$ to $M_3$. By the assumption on (C3) and the fact stated in the paragraph after Theorem A, we see that $M_3/K$ is a finite cyclic $p$-extension. Hence $\mathfrak{x}_{\mathcal{P}_3}(M_3)$ is trivial.

The unique prime of $M_3$ lying above $\mathcal{P}_2$ is totally ramified in the $\mathbb{Z}_p$-extension $N^{(1)}M_3/M_3$. By using the argument given in the proof of [7, Proposition 4.2], we see that the coinvariant quotient $\mathfrak{x}_{\mathcal{P}_3}(N^{(1)}M_3)_{\text{Gal}(N^{(1)}M_3/M_3)}$ is isomorphic to $\mathfrak{x}_{\mathcal{P}_3}(M_3)$ (see also the proof of [8, Proposition 3.2]). Hence, $\mathfrak{x}_{\mathcal{P}_3}(N^{(1)}M_3)_{\text{Gal}(N^{(1)}M_3/M_3)}$ is trivial, and it can be shown that $\mathfrak{x}_{\mathcal{P}_3}(N^{(1)}M_3)$ is also trivial by using topological Nakayama’s lemma. Since $N^{(1)}M_3/N^{(1)}$ is a finite extension and unramified outside $\mathcal{P}_3$, we see that $\mathfrak{x}_{\mathcal{P}_3}(N^{(1)})$ is finite.

Note that $X(N^{(1)})$ is a quotient of $\mathfrak{x}_{\mathcal{P}_3}(N^{(1)})$. Hence $X(N^{(1)})$ is also finite. □

We shall take the $\mathbb{Z}_p^{\oplus 2}$-extension $N^{(2)}/K$ as the following. Recall Lemma 2.3 and its proof. Let $N^2/K$ be the unique $\mathbb{Z}_p^{\oplus 2}$-extension unramified outside $\{\mathcal{P}_1, \mathcal{P}_2\}$. Since $\text{rank}_{\mathbb{Z}_p}I_1(N^2/K)$ is 2, we see that $N^2 \cap N^{(1)}/K$ is a finite extension. Hence $N^2N^{(1)}/K$ is a $\mathbb{Z}_p^{\oplus 3}$-extension. Since $\mathcal{P}_2$ is ramified in $N^{(1)}/K$, we can see that $\text{rank}_{\mathbb{Z}_p}I_2(N^2N^{(1)}/N^{(1)})$ is 1. Then, there is a (unique) intermediate field $N^{(2)}$ of $N^2N^{(1)}/N^{(1)}$ such that $N^{(2)}/K$ is a $\mathbb{Z}_p^{\oplus 2}$-extension and the prime of $N^{(1)}$ lying above $\mathcal{P}_2$ is unramified in $N^{(2)}$. Hence, $N^{(2)}/N^{(1)}$ is unramified outside $\mathcal{P}_1$. We note that $N^{(2)}/N^{(1)}$ is ramified at every prime lying above $\mathcal{P}_1$.

**Proposition 3.2.** $X(N^{(2)})$ is pseudo-null as a $\Lambda_{\text{Gal}(N^{(2)}/K)}$-module.

**Proof.** We follow the argument given in the proof of Minardi [14, Proposition 3.2]. There are several similar results which are shown based on the same idea ([8, Proposition 4.1], [8, Section 3, Step 2], [11, Proposition 3.6], [18, Section 5]). Hence, we only give an outline for the well known part.

We denote by $\mathcal{X}$ the coinvariant quotient $X(N^{(2)})_{\text{Gal}(N^{(2)}/N^{(1)})}$. We shall show that $\mathcal{X}$ is finite. Put $\Gamma_m = D(N^{(1)}/K)$, and let $N^{(1)}_m$ be the fixed field of $\Gamma_m$. Since we assumed that (C1) is satisfied, we see that $N^{(1)}_m/K$ is a finite extension.

Let $L'$ be the intermediate field of $L(N^{(2)})/N^{(2)}$ corresponding to $\mathcal{X}$, then $L'$ is an abelian extension over $N^{(1)}$. We note that $\text{Gal}(L'/N^{(1)})$ can be considered as a $\Lambda_{\Gamma_m}$-module. Note that $L(N^{(1)})$ is an intermediate field of $L'/N^{(1)}$. Let $\mathcal{I}$ be the kernel of the
natural surjection \(\text{Gal}(L'/N^{(1)}) \to X(N^{(1)})\). We denote by \(S\) the set of primes of \(N^{(1)}\) lying above \(\mathfrak{P}_1\). For \(P \in S\), we also denote by \(I_P\) the inertia subgroup of \(\text{Gal}(L'/N^{(1)})\) for \(P\). Note that \(\Gamma_m\) acts trivially on \(I_P\). Since \(I\) is (topologically) generated by \(I_P\) with \(P \in S\), it is a \(\Lambda_{\Gamma_m}\)-submodule of \(X\) with trivial \(\Gamma_m\)-action. We note that \(I\) is finitely generated as a \(\mathbb{Z}_p\)-module, and hence \(\text{Gal}(L'/N^{(1)})\) is also.

Let \(L''\) be the intermediate field of \(L'/N^{(1)}\) corresponding to the maximal finite \(\Lambda_{\Gamma_m}\)-submodule of \(\text{Gal}(L'/N^{(1)})\). Then \(L''\) contains \(N^{(2)}\). By using the finiteness of \(X(N^{(1)})\), we can see that \(\Gamma_m\) acts trivially on \(\text{Gal}(L''/N^{(1)})\). Hence \(L''\) is an abelian extension over \(N^{(1)}\).

Let \(I_2\) (resp. \(I_3\)) be the inertia subgroup of \(\text{Gal}(L''/N^{(1)})\) for the unique prime lying above \(\mathfrak{P}_2\) (resp. \(\mathfrak{P}_3\)), and \(I'\) the subgroup of \(\text{Gal}(L''/N^{(1)})\) (topologically) generated by \(I_2\) and \(I_3\). Since both \(I_2\) and \(I_3\) have \(\mathbb{Z}_p\)-rank 1, we see that \(\text{rank}_{\mathbb{Z}_p} I'\) is at most 2. The fixed field of \(L''\) by \(I'\) is an abelian pro-\(p\) extension of \(N^{(1)}\) unramified outside \(\mathfrak{P}_1\). By Theorem A, it must be a finite extension. Then, we conclude that \(\text{rank}_{\mathbb{Z}_p} \text{Gal}(L''/N^{(1)})\) is 2.

From the above facts, we see that \(X = \text{Gal}(L'/N^{(2)})\) is finite. By applying \cite[p.12, Lemme 4]{17}, we obtain the pseudo-nullity of \(X(N^{(2)})\).

We recall that \(N^{(2)}/N^{(1)}\) is unramified at every prime lying above \(\mathfrak{P}_2\) or \(\mathfrak{P}_3\). We shall use Proposition B in the next step. To apply this proposition, we need the information on the decomposition of these primes. However, for our purpose, it is sufficient to show the following result (we do not determine \(\text{rank}_{\mathbb{Z}_p} D_2(N^{(2)}/K), \text{rank}_{\mathbb{Z}_p} D_3(N^{(2)}/K)\) exactly).

**Lemma 3.3.** The case where \(\text{rank}_{\mathbb{Z}_p} D_2(N^{(2)}/K) = \text{rank}_{\mathbb{Z}_p} D_3(N^{(2)}/K) = 1\) does not occur. (Note that both \(D_2(N^{(2)}/K)\) and \(D_3(N^{(2)}/K)\) have \(\mathbb{Z}_p\)-rank at least 1.)

**Proof.** Let \(N^{\mathfrak{P}_2}/K\) (resp. \(N^{\mathfrak{P}_3}/K\)) be the unique \(\mathbb{Z}_p\)-extension such that \(\mathfrak{P}_2\) (resp. \(\mathfrak{P}_3\)) splits completely (the uniqueness follows from Proposition 2.3(i)).

Assume that \(\text{rank}_{\mathbb{Z}_p} D_2(N^{(2)}/K) = \text{rank}_{\mathbb{Z}_p} D_3(N^{(2)}/K) = 1\). Then both \(N^{\mathfrak{P}_2}/K\) and \(N^{\mathfrak{P}_3}/K\) are intermediate fields of \(N^{(2)}/K\). Since \(N^{\mathfrak{P}_2} \cap N^{\mathfrak{P}_3}/K\) is a finite extension (see the proof of Proposition 2.3(i)), we see that \(N^{(2)} = N^{\mathfrak{P}_2} N^{\mathfrak{P}_3}\).

We note that \(N^{\mathfrak{P}_2} N^{\mathfrak{P}_3}/K\) is contained in the fixed field of \(D_2(\tilde{K}/K) \cap D_3(\tilde{K}/K)\). Then, by using Lemma 2.3 and Proposition 2.3 (i), (ii), we see that the image of the natural mapping

\[I_1(\tilde{K}/K) \to \text{Gal}(\tilde{K}/K)/(D_2(\tilde{K}/K) \cap D_3(\tilde{K}/K))\]

has \(\mathbb{Z}_p\)-rank 2. This implies that \(\text{rank}_{\mathbb{Z}_p} I_1(N^{\mathfrak{P}_2} N^{\mathfrak{P}_3}/K) = 2\).

On the other hand, \(N^{(1)}\) is an intermediate field of \(N^{(2)} = N^{\mathfrak{P}_2} N^{\mathfrak{P}_3}\) over \(K\), and the \(\mathbb{Z}_p\)-extension \(N^{(1)}/K\) is unramified at \(\mathfrak{P}_1\). This is a contradiction. Then the assertion follows.

We choose the \(\mathbb{Z}_p^{\otimes 3}\)-extension \(N^{(3)}/N\) depending on the following cases.

(a) The prime of \(N^{(1)}\) lying above \(\mathfrak{P}_2\) is finitely decomposed in \(N^{(2)}\).

(b) The prime of \(N^{(1)}\) lying above \(\mathfrak{P}_2\) is completely decomposed in \(N^{(2)}\).

For the case (a), we see that

\[\text{rank}_{\mathbb{Z}_p} D_1(N^{(2)}/K) = \text{rank}_{\mathbb{Z}_p} D_2(N^{(2)}/K) = 2.\]
By Lemma 2.3, we see that $\text{rank}_{\mathbb{Z}_p} I_3(\tilde{K}/N^{(2)}) = 1$. Hence we can take a $\mathbb{Z}_p^\oplus 3$-extension $N^{(3)}/N$ such that $N^{(3)}/N^{(2)}$ is unramified outside $\{\mathfrak{P}_1, \mathfrak{P}_2\}$.

For the case (b), we see that the prime of $N^{(1)}$ lying above $\mathfrak{P}_3$ is finitely decomposed in $N^{(2)}$ by Lemma 3.3. Hence

$$\text{rank}_{\mathbb{Z}_p} D_1(N^{(2)}/K) = \text{rank}_{\mathbb{Z}_p} D_3(N^{(2)}/K) = 2.$$ 

Similar to the case (a), we can take a $\mathbb{Z}_p^\oplus 3$-extension $N^{(3)}/N$ such that $N^{(3)}/N^{(2)}$ is unramified outside $\{\mathfrak{P}_1, \mathfrak{P}_3\}$.

**Proposition 3.4.** For the $\mathbb{Z}_p^\oplus 3$-extension $N^{(3)}/N$ chosen above, $X(N^{(3)})$ is pseudo-null as a $\Lambda_{\text{Gal}(N^{(3)}/K)}$-module.

**Proof.** For either case (a) and (b), we can apply Proposition B for $N^{(3)}/N^{(2)}$. □

Now we shall finish the proof of Theorem 1.1.

**Proof of Theorem 1.1.** By Lemma 2.3 we see that all of $D_1(N^{(3)}/K)$, $D_3(N^{(3)}/K)$, $D_3(N^{(3)}/K)$ have $\mathbb{Z}_p$-rank at least 2 (this holds for either choice of $N^{(3)}$). Then we can also apply Proposition B for $\tilde{K}/N^{(3)}$. □

4. Examples

We shall give examples which satisfy the conditions of Theorem 1.1.

**Example 4.1.** We put $p = 3$. Let $K$ be the minimal splitting field of $X^3 - 10$. We can confirm that (C1) is satisfied. The class number of $F$ is 1, hence (C2) is satisfied. We can also check that $\mathfrak{X}_{\mathfrak{P}_3}(K)$ is trivial. Thus (C3) is also satisfied. Then, GGC for $K$ and $p$ holds by Theorem 1.1.

**Example 4.2.** We put $p = 3$. Let $K$ be the minimal splitting field of $X^3 - 17$. We can confirm that (C1) and (C2) are satisfied (note that the class number of $F$ is 1). In this case, the order of $\mathfrak{X}_{\mathfrak{P}_3}(K)$ is 3. However, we can also see that $\mathfrak{P}_2$ is not decomposed in $M_{\mathfrak{P}_3}(K)$, hence (C3) is satisfied. Consequently, GGC for $K$ and $p$ also holds for this case by Theorem 1.1.

**Remark 4.3.** Let $M'_p(F)/F$ be the maximal abelian pro-$p$ extension unramified outside $p^*$ and split completely at $p$. To confirm (C1), it is sufficient to show that $M'_p(F)/F$ is a finite extension. Hachimori checked that $[M'_p(F) : F] = 9$ for $F = \mathbb{Q}(\sqrt[3]{10})$. (See [7, Section 7.3]. He also gave partial results for other pure cubic fields.) Kataoka also checked [11] Assumption 3.1 for many cases (see [11] p.630]). His result includes confirming (C1) for the above examples (recall Remark 1.2). Note that for the examples given in the present paper, all conditions are checked separately by using PARI/GP [10]. (In this computation, the author also referred to the data and an idea of computation stated in Gras [4] Appendix A.)

**References**

[1] J. Assim and Z. Boughadi : *On Greenberg’s generalized conjecture*, J. Number Theory 242 (2023), 576–602.
[2] A. Brumer : *On the units of algebraic number fields*, Mathematika 14 (1967), 121–124.
[3] S. Fujii : *On Greenberg’s generalized conjecture for CM-fields*, J.reine angew. Math. 731 (2017), 259–278.
[4] G. Gras : *Note on some p-invariants of $\mathbb{Q}(\sqrt[p]{N})$ using reflection theorem*, preprint (arXiv:1910.00332).
[5] R. Greenberg : *The Iwasawa invariants of $\Gamma$-extensions of a fixed number field*, Amer. J. Math. 95 (1973), 204–214.
[6] 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.
[7] Y. Hachimori : *Iwasawa theory for extensions with restricted p-ramification*, Tokyo J. Math. 26 (2003), 179–198.
[8] T. Itoh : *On multiple $\mathbb{Z}_p$-extensions of imaginary abelian quartic fields*, J. Number Theory 131 (2011), 59–66.
[9] K. Iwasawa : *A simple remark on Leopoldt’s conjecture* (unpublished article), Kenkichi Iwasawa collected papers. vol.II, 862–870, Springer-Verlag, Tokyo, 2001.
[10] J.-F. Jaulent : *Sur l’indépendence l-adique de nombres algébriques*, J. Number Theory 20 (1985), 149–158.
[11] T. Kataoka : *On Greenberg’s generalized conjecture for complex cubic fields*, Int. J. Number Theory 13 (2017), 619–631.
[12] S. Kleine : *Relative extensions of number fields and Greenberg’s generalized conjecture*, Acta Arith. 174 (2016), 367–392.
[13] C. Maire : *On the $\mathbb{Z}_l$-rank of abelian extensions with restricted ramification*, J. Number Theory 92 (2002), 376–404.
[14] J. V. Minardi : *Iwasawa modules for $\mathbb{Z}_p^d$-extension of algebraic number fields*, Thesis, University of Washington, 1986.
[15] K. Murakami : *A weak form of Greenberg’s generalized conjecture for imaginary quadratic fields*, J. Number Theory 244 (2023), 308–338.
[16] The PARI Group : PARI/GP version 2.15.0, Univ. Bordeaux, 2022, http://pari.math.u-bordeaux.fr/.
[17] B. Perrin-Riou : *Arithmétique des courbes elliptiques et théorie d’Iwasawa*, Mém. Soc. Math. France 17 (1984), 1–130.
[18] N. Takahashi : *On Greenberg’s generalized conjecture for imaginary quartic fields*, Int. J. Number Theory 17 (2021), 1163–1173.

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