arXiv:2406.01892v1 [math.NT] 4 Jun 2024

On the triviality of the unramified Iwasawa modules of the maximal multiple $\mathbb{Z}_p$-extensions

Keiji OKANO [*]

Abstract

For a number field k and an odd prime number p, we consider the maximal multiple $\mathbb{Z}_p$-extension $\widetilde{k}$ of k and the unramified Iwasawa module $X(\widetilde{k})$, which is the Galois group of the maximal unramified abelian p-extension over $\widetilde{k}$. In the present article, we classify CM-fields k which are decomposed completely at p such that $X(\widetilde{k}) = 0$.

1 Introduction

Let p be an odd prime number and k a finite algebraic number field. A $\mathbb{Z}_p$-extension k_∞ of k is defined by a Galois extension of k such that the Galois group $\mathrm{Gal}(k_\infty/k)$ is isomorphic to the p-adic additive group $\mathbb{Z}_p$. The maximal unramified abelian p-extension of k_∞ is one of the most important objects in classical Iwasawa theory. As one of its generalizations, we consider the maximal multiple $\mathbb{Z}_p$-extension $\widetilde{k}$ of k and the Galois group $X(\widetilde{k})$ of the maximal unramified abelian extension of $\widetilde{k}$. We call $X(\widetilde{k})$ the unramified Iwasawa module of $\widetilde{k}$. It is known that $X(\widetilde{k})$ is a finitely generated torsion $\mathbb{Z}_p\llbracket\mathrm{Gal}(\widetilde{k}/k)\rrbracket$-module, where $\mathbb{Z}_p\llbracket\mathrm{Gal}(\widetilde{k}/k)\rrbracket$ is the complete group ring. In [11], Greenberg conjectured that $X(\widetilde{k})$ is a pseudo-null $\mathbb{Z}_p\llbracket\mathrm{Gal}(\widetilde{k}/k)\rrbracket$-module. In other words, $X(\widetilde{k})$ is conjectured such that any prime ideal with height less than 2 annihilates $X(\widetilde{k})$. This conjecture is usually called the Generalized Greenberg's Conjecture (GGC, for short). Roughly speaking, it means that $X(\widetilde{k})$ is small. In fact, if we specialize k to totally real fields which satisfy Leopoldt's conjecture for p, then $\widetilde{k}$ coincides with the cyclotomic $\mathbb{Z}_p$-extension k_{cyc} of k, and therefore the conjecture means that the unramified Iwasawa module of k_{cyc} should be finite (this is the original Greenberg's conjecture proposed in [10]).

There are many results which satisfy the original and generalized Greenberg's conjecture and significant results which follow from these conjectures. Here, we introduce some results about GGC. Minardi [18], Itoh [12], and Fujii [7] gave conditions under which $X(\widetilde{k})$ will be pseudo-null for CM-fields k that are decomposed completely at p (their ideas will be used in this paper). Moreover, as its application, Fujii [8] constructed an infinite family of k which holds GGC and $X(\widetilde{k}) \neq 0$. A weak version of the GGC has also been proposed in Nguyen Quang Do [23], [24] and Wingberg [31]. It states that $X(\widetilde{k})$ has a non-trivial

[*] Department of Teacher Education, Tsuru University, 3-8-1 Tahara, Tsuru-shi, Yamanashi 402-0054, Japan. email: okano@tsuru.ac.jp

2010 *Mathematics Subject Classification.* 11R23, 11R37.

Key Words: multiple $\mathbb{Z}_p$-extensions, Iwasawa modules.

pseudo-null submodule if $X(\widetilde{k}) \neq 0$. Fujii [5] and Kleine [16] gave a relation between weak GGC and GGC. Also [5], Shinkawa [27] and Murakami [21] gave many examples which satisfy weak GGC and GGC. On the other hand, Kurihara (unpublished) and Kataoka [15] proved that if k is an imaginary quadratic field which is decomposed completely at p, then $X(\widetilde{k})$ has no non-trivial finite submodule. So it seems that the unramified Iwasawa modules $X(\widetilde{k})$ may be not so small.

From these studies about the size of the unramified Iwasawa modules, the question naturally arises: when does $X(\widetilde{k})$ become trivial? In the case where k is totally real, which satisfies Leopoldt's conjecture for p (so $\widetilde{k} = k_{\mathrm{cyc}}$), there are some known conditions under which the unramified Iwasawa modules are trivial. For example, the Iwasawa's criterion [13] (or Washington [30, Theorem 10.1]) gives a necessary and sufficient condition for $X(k_{\mathrm{cyc}}) = 0$ under some assumptions, and Fukuda's criterion [9] also gives a sufficient condition for $X(k_{\mathrm{cyc}}) = 0$. Yamamoto [32] determined all absolutely abelian p-extensions k for which $X(k_{\mathrm{cyc}}) = 0$. Moreover, there are some results about the density of real quadratic fields k for which $X(k_{\mathrm{cyc}}) = 0$ (see Taya and Yamamoto [29] and its references). We remark that in the case where $p = 2$, Mouhib and Movahhedi [20] listed real quadratic fields k for which $X(k_{\mathrm{cyc}})$ vanishes, respectively, is cyclic. Also, Taya and Yamamoto [28] determined all real abelian 2-extensions k for which $X(k_{\mathrm{cyc}}) = 0$.

Contrary to the totally real case as above, there are few results in the case where k is a CM-field. Indeed, in this case, the known results may be the only ones that can be easily obtained. For example, in the case where k is an imaginary quadratic field, see Theorem 1.1.1(I) below and [19, Theorem 1.6]. We remark that, in each case where k is a totally real field and a CM-field that are decomposed completely at p, Jaulent [14] gave necessary conditions such that $X(\widetilde{k})$ is trivial. So, we attempt to determine CM-fields k such that $X(\widetilde{k}) = 0$. In this paper, we completely classify CM-fields k that are decomposed completely at p such that $X(\widetilde{k}) = 0$. We remark that, for such CM-fields k, the triviality of $X(\widetilde{k})$ implies that the maximal unramified p-extension of k_{cyc} is abelian. Finally, we remark that our result in this paper does not require the assumption that GGC holds; rather our result provides a new example that satisfies GGC.

1.1 Main theorem

Let p be an odd prime number and k a CM-field that is decomposed completely at p. We suppose that Leopoldt's conjecture for k and p holds. Let us denote by $A(k)$ and $D(k)$ the p-Sylow subgroup of the ideal class group of k and the subgroup of $A(k)$ consisting of classes containing of a power of a prime ideal above p, respectively. Let k_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of k and $\widetilde{k}$ the maximal multiple $\mathbb{Z}_p$-extension of k. We will denote by $X(k_{\mathrm{cyc}})$ and $X(\widetilde{k})$ the Galois group of the maximal unramified abelian p-extension of k_{cyc} and $\widetilde{k}$, respectively. For a prime ideal $\mathfrak{P}$ in k above p, we write the complex conjugate of $\mathfrak{P}$ as $\overline{\mathfrak{P}}$. Moreover, to describe the main theorem, we define the sets S, T of the prime ideals in k above p as follows:

- In the case $[k:\mathbb{Q}]=4$: according to the prime decomposition $(p)=\mathfrak{p}\mathfrak{q}\overline{\mathfrak{p}}\overline{\mathfrak{q}}$ of p in k, define $T=\{\mathfrak{p},\overline{\mathfrak{p}}\}$, $S=\{\mathfrak{q},\overline{\mathfrak{q}}\}$.
- In the case $[k:\mathbb{Q}]=6$: according to the prime decomposition $(p)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\overline{\mathfrak{p}_1}\ \overline{\mathfrak{p}_2}\ \overline{\mathfrak{p}_3}$ of p in k, define $T=\{\mathfrak{p}_1,\mathfrak{p}_2\}$, $S=\{\mathfrak{p}_3,\overline{\mathfrak{p}_1},\overline{\mathfrak{p}_2},\overline{\mathfrak{p}_3}\}$.

Then the main theorem is described as follows.

Theorem 1.1.1. *Let p be an odd prime number and k a CM-field that is decomposed completely at p and holds Leopoldt's conjecture for k and p. If $X(\widetilde{k})=0$, then $[k:\mathbb{Q}]\leq 6$. Furthermore, according to the degree of k, the following holds:*

(I) *In the case $[k:\mathbb{Q}]=2$: $X(\widetilde{k})=0$ if and only if $X(k_{\mathrm{cyc}})\simeq\mathbb{Z}_p$.*

(II) *In the case $[k:\mathbb{Q}]=4$ or 6: $X(\widetilde{k})=0$ if and only if all of the following conditions* (i)(ii)(iii)(iv) *hold:*

(i) *$A(k)=0$ or $A(k)$ is cyclic.*

(ii) *$A(k)=D(k)$.*

(iii) *$X(k_{\mathrm{cyc}})\simeq\mathbb{Z}_p^{\oplus[k:\mathbb{Q}]/2}$ as $\mathbb{Z}_p[\![\mathrm{Gal}(k_{\mathrm{cyc}}/k)]\!]$-modules.*

(iv) *There is no non-trivial p-extension of k that is unramified outside S and completely decomposes at every prime ideal in T. Here, S and T are defined according to the degree $[k:\mathbb{Q}]$ as above.*

In fact, in the case where $[k:\mathbb{Q}]=4$ and $A(k)$ is cyclic, if (i)(ii)(iii) *hold then* (iv) *also does. Therefore, in this case, we can remove* (iv).

Remark 1.1.2. The case (I) is known. In addition, Jaulent [14] gives a method for finding the case $X(k_{\mathrm{cyc}})\simeq\mathbb{Z}_p$. On the other hand, using central class field theory and Kida's formula in Iwasawa theory, the special case of Theorem 1.1.1, where $p=3$ and k is a totally imaginary abelian extension with degree 6, is shown by [26]. Moreover, in the case where $p=3$, $[k:\mathbb{Q}]=6$ and $A(k)$ is cyclic, if (i)(ii)(iii) hold then (iv) also does. Therefore, similar to the case where $[k:\mathbb{Q}]=4$ and $A(k)$ is cyclic, we can remove (iv) in this case. (see Remark 4.3.2).

1.2 Organization of this paper

§§2.1 presents the notations and basic facts that are frequently used in this article. In §§2.2, we introduce central class field theory. If we restrict our target to only the case of degree 4, we can prove our main theorem without central class field theory. In §§2.3, we give a tool for proving the necessary condition of Theorem 1.1.1. In §§2.4, we narrowing-down the number of targets we should consider. In §3 and §4, we prove the main results in the case of degrees 4 and 6, respectively. Although the results in the case of degree 4 are not used in the case of degree 6, the basic idea provided in §3 is also used in §4.

2 Preliminaries

2.1 Notation

We start from the notation of groups and modules. For elements $x, y, \ldots$ in a $\mathbb{Z}_p$-modules M, we use the notation $\langle x, y, \ldots \rangle$ as the $\mathbb{Z}_p$-submodule of M generated by $x, y, \ldots$. The same notation is used for the $\mathbb{Z}_p$-submodule that is generated by some submodules. For example, for an element $x \in M$ and a submodule N of M, $\langle x, N \rangle$ means the $\mathbb{Z}_p$-submodule generated by x and elements in N. For an abelian group G and a G-module M, let M^G and M_G denote the maximal submodule that G acts on trivially and the maximal quotient that G acts on trivially, respectively. In particular, if G is a group generated by the complex conjugation, then put $M^+ := M^G$ and $M^- := M/M^+$. If p is an odd prime number and M is a $\mathbb{Z}_p$-module, M^- is isomorphic to the maximal submodule of M that G acts on as -1.

In the remainder of this paper, let p be an odd prime number. As in §1.1, for any finite extension F over $\mathbb{Q}$, let us denote by F_{cyc} and $\widetilde{F}$ the cyclotomic $\mathbb{Z}_p$-extension of F and the maximal multiple $\mathbb{Z}_p$-extension of F, respectively. Note that any prime ideal in F above p ramifies at F_{cyc} (Neukirch, Schmidt and Wingberg [22, Proposition 11.1.1(ii)]). Also, as in §1.1, let denote by $A(F)$ and $D(F)$ the p-Sylow subgroup of the ideal class group of F and the subgroup of $A(F)$ consisting of classes containing a power of a prime ideal above p, respectively. Let $L(F)$ be the maximal unramified abelian p-extension of F, and we write $X(F) := \mathrm{Gal}(L(F)/F)$. We use the same notations $L(F)$ and $X(F)$ if F is an infinite extension over $\mathbb{Q}$.

Fix a topological generator $\overline{\gamma} \in \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Then $\mathrm{Gal}(F_{\mathrm{cyc}}/F)$ acts on $X(F_{\mathrm{cyc}})$ as follows. Choose an extension $\gamma \in \mathrm{Gal}(L(F_{\mathrm{cyc}})/F)$ of $\overline{\gamma}$. Then $\overline{\gamma}(x) := \gamma x \gamma^{-1}$ for $x \in X(F_{\mathrm{cyc}})$. This action is independent of the choice of γ. It is known that $X(F_{\mathrm{cyc}})$ is a finitely generated torsion module over the complete group ring $\mathbb{Z}_p[\![\mathrm{Gal}(F_{\mathrm{cyc}}/F)]\!]$ ([22, Proposition 11.1.4] or [30, Lemma 13.18]). For more properties of $X(F_{\mathrm{cyc}})$, see [22, Chapter XI] or [30, §13]. Moreover, for a $\mathbb{Z}_p$-extension F_∞, we define the p-split Iwasawa module $X'(F_\infty)$ of F_∞ by the Galois group of the maximal abelian p-extension of F_∞ where every prime above p splits completely.

Let $r_1(F)$ and $r_2(F)$ be the numbers of real primes and pairs of complex primes of F, respectively. By class field theory,

$$\mathrm{Gal}(\widetilde{F}/F) \simeq \mathbb{Z}_p^{\oplus r_2(F)+1},$$

if Leopoldt's conjecture for F and p holds ([22, Theorem 11.1.2] or [30, Theorem 13.4]). For convenience, we use the following notation.

Definition 2.1.1. *For a closed subgroup H in $\mathrm{Gal}(\widetilde{F}/F)$ and an intermediate field M of $\widetilde{F}/F$, we write $M \leftrightarrow H$ if M is the fixed field by H.*

Now, we introduce the following lemmas which are often used in this article. The first lemma is well known.

Lemma 2.1.2. *Let G be a pro-p group with a normal and abelian subgroup H. Then G/H acts on H via inner automorphism. In addition, suppose that G/H is $\mathbb{Z}_p$-cyclic. Then G is abelian if and only if the action is trivial.*

Lemma 2.1.3. *Assume that p splits completely at F. Let F_∞ be a $\mathbb{Z}_p$-extension of F such that any prime ideal in F above p ramifies. Then $\widetilde{F}/F_\infty$ is an unramified abelian p-extension. In other words, $\widetilde{F}$ is a subfield in $L(F_\infty)$.*

Proof. This follows from class field theory and the assumption. For more details, see [14, Lemme 4] or the beginning of §2 in Fujii [6] for example. □

Corollary 2.1.4. *With the notation and assumption in Lemma* 2.1.3*, there exists a surjection $X(F_\infty) \twoheadrightarrow \mathbb{Z}_p^{\oplus r_2(F)}$ as $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/F)]\!]$-modules.*

Proof. By Lemma 2.1.3, there exists a natural surjection $X(F_\infty) \twoheadrightarrow \mathrm{Gal}(\widetilde{F}/F_\infty)$. And, by Lemma 2.1.2, $\mathrm{Gal}(F_\infty/F)$ acts on $\mathrm{Gal}(\widetilde{F}/F_\infty)$ trivially. By $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(\widetilde{F}/F_\infty) \geq r_2(F)$, this completes the proof. □

Lemma 2.1.5. *Let K/F be a Galois extension possibly of infinite degree and H the normal subgroup of* $\mathrm{Gal}(K/F)$. (*Then* $\mathrm{Gal}(K/F)$ *acts on $X(K)$ via inner automorphism by Lemma* 2.1.2.) *Denote by L the subfield in $L(K)/K$ which satisfies* $\mathrm{Gal}(L/K) \simeq X(K)_H$. *Then, L/F is a Galois extension.*

Proof. Since K/F is a Galois extension and $L(K)$ is the maximal abelian extension of K unramified at all primes, $L(K)/F$ is also a Galois extension. Therefore, it is sufficient to show that $\mathrm{Gal}(L(K)/L)$ is normal in $\mathrm{Gal}(L(K)/F)$. By the definition,

$$\mathrm{Gal}(L(K)/L) = \left[X(K), \mathrm{Gal}(L(K)/K^H)\right].$$

Here, for subgroups H_1, H_2 of a pro-p group, we use the notation $[H_1, H_2]$ as the closed normal subgroup generated by elements with the form $[h_1, h_2] := h_1 h_2 h_1^{-1} h_2^{-1}$ ($h_i \in H_i$). Note that $\mathrm{Gal}(L(K)/K^H)$ is a normal subgroup in $\mathrm{Gal}(L(K)/F)$ since K^H/F is Galois. For any elements $x \in X(K)$, $\sigma \in \mathrm{Gal}(L(K)/K^H)$, and $\tau \in \mathrm{Gal}(L(K)/F)$, we have $\tau[x,\sigma]\tau^{-1} = [\tau x \tau^{-1}, \tau\sigma\tau^{-1}]$. Since $\tau x \tau^{-1} \in X(K)$ and $\tau\sigma\tau^{-1} \in \mathrm{Gal}(L(K)/K^H)$, this completes the proof. □

2.2 Theorems in central class field theory

Let p be an odd prime number, F a finite algebraic number field, and K/F a finite abelian p-extension. Set $G := \mathrm{Gal}(L(K)/F)$. Then G acts on $X(L(K))$ via inner automorphism since $X(L(K))$ is abelian. We define the central p-class field $\mathcal{C}_{L(K)/F}$ associated with $L(K)/F$ as the subfield in $L(L(K))/L(K)$ such that

$$\mathrm{Gal}(\mathcal{C}_{L(K)/F}/L(K)) \simeq X(L(K))_G. \tag{2.1}$$

In other words, $\mathcal{C}_{L(K)/F}$ is the subfield of $L(L(K))$ fixed by $[X(L(K)), \mathrm{Gal}(L(L(K))/F)]$. Note that $X(L(K)) = 0$ if and only if $X(L(K))_G = 0$ by Nakayama's lemma. For a prime ideal $\mathfrak{l}$ in F which is ramified in K/F, we fix a prime ideal above $\mathfrak{l}$ in $L(K)$ and denote its decomposition group in G by $D_{\mathfrak{l}}$. Then we have the following proposition by central class field theory (see Fröhlich [4, Proposition 3.6, (3.24), Theorem 3.11]).

Proposition 2.2.1. *With the notation above, put*

$$\mathcal{K}(G) := \mathrm{Coker}\left(\prod_{\mathfrak{l}} H_2(D_{\mathfrak{l}}, \mathbb{Z}_p) \to H_2(G, \mathbb{Z}_p)\right),$$

which is induced by the canonical map $D_{\mathfrak{l}} \to G$, where the product is taken over all ramified primes in F. Then we have the exact sequence

$$(E(F) \cap N_{L(K)/F}\mathbb{A}_{L(K)}^{\times}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathcal{K}(G) \to X(L(K))_G \to 0, \tag{2.2}$$

where $\mathbb{A}_{L(K)}^{\times}$ is the idèle group of $L(K)$ and $N_{L(K)/F}$ is the norm map.

Remark 2.2.2. Since we assume that K/F is abelian, the genus field associated with $L(K)/F$, which is defined in [4, §2 page 13], coincides with $L(K)$.

If K or F is an infinite extension, by taking the projective limit with respect to its finite subextensions, we have an exact sequence similar to (2.2). On the other hand, suppose that $K = F$. Then we obtain $E(F) \cap N_{L(F)/F}\mathbb{A}_{L(F)}^{\times} = E(F)$ and $H_2(X(F), \mathbb{Z}_p) \simeq A(F) \wedge_{\mathbb{Z}_p} A(F)$. Hence if $L(L(F)) = L(F)$, i.e., $X(L(F)) = 0$, then the induced map $E(F) \to A(F) \wedge_{\mathbb{Z}_p} A(F)$ is surjective. We therefore obtain the following.

Corollary 2.2.3. *If $X(L(F)) = 0$, then*

$$\dim_{\mathbb{F}_p} A(F)/p \leq \frac{1 + \sqrt{1 + 8(r_1(F) + r_2(F) + \nu - 1)}}{2},$$

where $\nu = 1$ or 0 according to whether a primitive pth root of unity is in F or not.

If $\mathcal{K}(G) = 0$ then we have $X(L(K))_G = 0$, so $X(L(K)) = 0$ by Nakayama's lemma. The module $\mathcal{K}(G)$ can be calculated as follows. We consider the commutative diagram of the minimal presentations

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{R} \arrow[r] & \mathcal{F} \arrow[r] & G \arrow[r] & 1 \\
1 \arrow[r] & \mathcal{R}_{\mathfrak{l}} \arrow[r] \arrow[u] & \mathcal{F}_{\mathfrak{l}} \arrow[r] \arrow[u] & D_{\mathfrak{l}} \arrow[r] \arrow[u] & 1
\end{tikzcd}$$

of G and the decomposition groups $D_{\mathfrak{l}}$ by free pro-p-groups $\mathcal{F}$ and $\mathcal{F}_{\mathfrak{l}}$, respectively. Since the Hochschild-Serre spectral sequence yields the isomorphisms

$$H_2(G,\mathbb{Z}_p) \simeq \mathcal{R} \cap [F,F]/[R,F], \quad H_2(D_{\mathfrak{l}},\mathbb{Z}_p) \simeq \mathcal{R}_{\mathfrak{l}} \cap [\mathcal{F}_{\mathfrak{l}},\mathcal{F}_{\mathfrak{l}}]/[\mathcal{R}_{\mathfrak{l}},\mathcal{F}_{\mathfrak{l}}], \tag{2.3}$$

we see that $\mathcal{K}(G) = 0$ if and only if

$$\Phi \colon \prod_{\mathfrak{l}} \mathcal{R}_{\mathfrak{l}} \cap [\mathcal{F}_{\mathfrak{l}},\mathcal{F}_{\mathfrak{l}}]/[\mathcal{R}_{\mathfrak{l}},\mathcal{F}_{\mathfrak{l}}] \longrightarrow R \cap [F,F]/[R,F] \tag{2.4}$$

is surjective.

2.3 $\mathbb{Z}_p$-extension with action of the complex conjugation

Hereinafter we will suppose that k is a CM-field. We denote by k^+ the maximal totally real subfield of k.

Lemma 2.3.1. *Let p be an odd prime number, k a CM-field which does not contain all primitive pth roots of unity, and k_∞ a $\mathbb{Z}_p$-extension of k. Denote the p^nth intermediate field of k_∞/k by k_n and put $\Gamma := \mathrm{Gal}(k_\infty/k)$, $\Gamma_n := \mathrm{Gal}(k_n/k)$. Suppose that $\mathrm{Gal}(k/k^+)$ acts on Γ via inner automorphism and any prime ideal in k above p does not split in k_∞/k. Then the induced action of $\mathrm{Gal}(k/k^+)$ on the cokernel*

$$\mathrm{Coker}\left(\varprojlim_{\text{norm}} D(k_n) \hookrightarrow X(k_\infty)^\Gamma \right)$$

is trivial.

Proof. The proof is almost the same as in [25, Lemma 4.1]. Note that Γ acts on $D(k_n)$ trivially, since any prime ideal in k above p does not split in k_∞/k. Also note that k_∞/k^+ is a Galois extension by the assumption and that $\mathrm{Gal}(k/k^+)$ acts on $X(k_\infty)^\Gamma$ via inner automorphism. Denote the unit group, the principal ideal group, and the group of fractional ideals of k_n by $E(k_n)$, $P(k_n)$, and $I(k_n)$, respectively. Consider the two exact sequences of Γ_n-modules

$$0 \to E(k_n) \to k_n^\times \to P(k_n) \to 0, \quad 0 \to P(k_n) \to I(k_n) \to I(k_n)/P(k_n) \to 0.$$

Taking the cohomological long exact sequence of these two exact sequences, we obtain the exact sequence

$$0 \to i_n(A(k))D(k_n) \to A(k_n)^\Gamma \to E(k) \cap N_{\Gamma_n} k_n^\times / N_{\Gamma_n} E(k_n) \to 0, \tag{2.5}$$

where $i_n \colon A(k) \to A(k_n)$ is the lifting map and N_{Γ_n} is the norm operator. Since we assume that k does not contain all primitive pth roots of unity, the group index $[E(k) : E(k^+)]$ is coprime to odd prime number p (see [30, Theorem 4.12]). Therefore, $\mathrm{Gal}(k/k^+)$ acts on the right term in (2.5) trivially. Moreover, since the norm from k_n to k_{n-1} of each term in (2.5) maps every element to its pth power, we see that the norm commutes with the action of $\mathrm{Gal}(k/k^+)$. Note that $\varprojlim i_n(A(k)) = 0$. Therefore, taking the projective limit with respect to the norm maps of (2.5), we have an injective morphism $\varprojlim D(k_n) \hookrightarrow X(k_\infty)^\Gamma$ of $\mathrm{Gal}(k/k^+)$-modules whose cokernel has a trivial $\mathrm{Gal}(k/k^+)$-action. □

Corollary 2.3.2. *With the notation and assumption in Lemma* 2.3.1*, put* $k_\infty = k_{\mathrm{cyc}}$ *and* $\Gamma = \mathrm{Gal}(k_{\mathrm{cyc}}/k)$*. Then, for the* p*-split Iwasawa module* $X'(k_{\mathrm{cyc}})$ *of* k_{cyc}*, we have*

$$X'(k_{\mathrm{cyc}})^- \simeq \left(X(k_{\mathrm{cyc}})/X(k_{\mathrm{cyc}})^\Gamma\right)^- .$$

Proof. We have $X'(k_{\mathrm{cyc}}) \simeq \varprojlim_{\mathrm{norm}}(A(k_n)/D(k_n))$. Note that $\mathrm{Gal}(k/k^+)$ acts on $X(k_{\mathrm{cyc}})$ since $\mathrm{Gal}(k_{\mathrm{cyc}}/k^+) \simeq \Gamma \times \mathrm{Gal}(k/k^+)$. By Lemma 2.3.1, we obtain $\left(\varprojlim D(k_n)\right)^- \simeq \left(X(k_{\mathrm{cyc}})^\Gamma\right)^-$. Hence we have

$$X'(k_{\mathrm{cyc}})^- \simeq \left(\varprojlim A(k_n)\right)^- / \left(\varprojlim D(k_n)\right)^- \simeq X(k_{\mathrm{cyc}})^- / \left(X(k_{\mathrm{cyc}})^\Gamma\right)^- .$$

This yields the claim. □

For CM-fields k such that p splits completely, [14] used the same result as in Corollary 2.3.2 to give a sufficient condition for $X(\widetilde{k}) \neq 0$. On the other hand, we will use the following corollary to show $X(\widetilde{k}) \neq 0$.

Corollary 2.3.3. *With the notation and assumption in Lemma* 2.3.1*, suppose that the following conditions* (i)(ii) *hold.*

(i) *In* k*,* p *splits completely.*
(ii) *Any prime ideal in* k *above* p *is non-split and ramifies in* k_∞/k*.*

If $X(\widetilde{k}) = 0$*, then an action of* $\mathrm{Gal}(k/k^+)$ *on* $X'(k_\infty)$ *is induced from the action on* $X(k_\infty)^\Gamma$ *and it is trivial.*

Proof. The conditions (i)(ii) imply that $k_\infty \subset \widetilde{k} \subset L(k_\infty)$ by Lemma 2.1.3. Moreover, by the assumption that $X(\widetilde{k}) = 0$, we obtain $\widetilde{k} = L(k_\infty)$. Therefore $X(k_\infty) = X(k_\infty)^\Gamma$, so we have the exact sequence

$$0 \to \varprojlim D(k_n) \to X(k_\infty)^\Gamma \to X'(k_\infty) \to 0.$$

From this, the action of $\mathrm{Gal}(k/k^+)$ on $X'(k_\infty)$ is naturally induced. By Lemma 2.3.1, the action is trivial. □

2.4 Narrowing-down the number of targets

In this subsection, we introduce the following proposition which follows from known results.

Proposition 2.4.1. *Let p be an odd prime number and k a CM-field that satisfies Leopoldt's conjecture. Moreover, suppose that p splits in k completely. If $X(\widetilde{k}) = 0$, then the following conditions hold*:

(i) $[k : \mathbb{Q}] \leq 6$.
(ii) $\dim_{\mathbb{F}_p} A(k)/pA(k) \leq 2$.
(iii) $A(k) = D(k)$.
(iv) $X(k_{\mathrm{cyc}}) \simeq \mathbb{Z}_p^{\oplus [k:\mathbb{Q}]/2}$ *as* $\mathbb{Z}_p[\![\mathrm{Gal}(k_{\mathrm{cyc}}/k)]\!]$*-modules, in other words,* $L(k_{\mathrm{cyc}}) = \widetilde{k}$.

Proof. As in the proof of Corollary 2.3.3, we obtain (iv) by Lemma 2.1.3 and $X(\widetilde{k}) = 0$. The condition (iii) is the same as [25, Proposition 4.3]. The condition (i) is the same as in [8, Lemma 3.9] or [14, Théorème 10(i)]. Finally, we show that the condition (ii) holds. Since $X(\widetilde{k}) = 0$, we have $X(L(k)) = 0$. Indeed, if it does not hold, then $L(L(k))$ is not contained in $\widetilde{k}$ since it is not abelian over k. Hence $L(L(k))\widetilde{k}/\widetilde{k}$ is a non-trivial unramified p-extension. This contradicts the assumption that $X(\widetilde{k}) = 0$. Thus, we obtain the inequality

$$\dim_{\mathbb{F}_p} A(k)/pA(k) \leq \frac{1 + \sqrt{4[k : \mathbb{Q}] - 7}}{2} < 3$$

by Corollary 2.2.3 and (i). □

It is known that in the case where k is an imaginary quadratic field, $X(\widetilde{k}) = 0$ if and only if $X(k_{\mathrm{cyc}}) \simeq \mathbb{Z}_p$. Indeed, if $X(k_{\mathrm{cyc}}) \simeq \mathbb{Z}_p$, then we have $L(k_{\mathrm{cyc}}) = \widetilde{k}$ and $H_2(X(k_{\mathrm{cyc}}), \mathbb{Z}_p) \simeq X(k_{\mathrm{cyc}}) \wedge_{\mathbb{Z}_p} X(k_{\mathrm{cyc}}) = 0$. So, $\mathcal{K}(X(k_{\mathrm{cyc}}))$ in Proposition 2.2.1 is trivial, which implies $X(\widetilde{k}) = 0$ by Proposition 2.2.1 and Nakayama's lemma. Conversely, if $X(\widetilde{k}) = 0$, then $L(k_{\mathrm{cyc}}) = \widetilde{k}$, which implies $X(k_{\mathrm{cyc}}) \simeq \mathbb{Z}_p$. Therefore, it is sufficient to consider a CM-field k of degree 4 or 6 which satisfies the following conditions:

(I) Leopoldt's conjecture for k and p holds.
(II) In k, p splits completely.
(III) The conditions (ii)(iii)(iv) in Proposition 2.4.1 hold.

In particular, in this case, it is automatically assumed that "$\mu(k_{\mathrm{cyc}}/k) = 0$" (this means that $X(k_{\mathrm{cyc}}/k)$ is finitely generated as a $\mathbb{Z}_p$-module) and that $X(k_{\mathrm{cyc}}^+) = 0$. Indeed, (iv) in Proposition 2.4.1 implies that $\mu(k_{\mathrm{cyc}}/k) = 0$. Also, since we assume that Leopoldt's conjecture holds, k_{cyc}^+ is the unique $\mathbb{Z}_p$-extension of k^+. Therefore the complex conjugation acts on $X(k_{\mathrm{cyc}}) = \mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})$ as -1, so $X(k_{\mathrm{cyc}}^+) \simeq X(k_{\mathrm{cyc}})^+ = 0$.

Hereinafter we will write the operator of $\mathrm{Gal}(\widetilde{k}/k)$ multiplicatively.

3 In the case of degree 4

3.1 The non-Galois or cyclic case

3.1.1 Setting and preparation

Let k be a non-Galois CM-field of degree 4 or a totally imaginary cyclic extension over $\mathbb{Q}$ of degree 4. Suppose that k satisfies the conditions (I)(II)(III) in the last expression of §2.4. Let $F/\mathbb{Q}$ be the Galois closure of $k/\mathbb{Q}$ with Galois group $\Delta := \mathrm{Gal}(F/\mathbb{Q})$. Then it is known that

$$\Delta \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} = \{\sigma \mid \sigma^4 = 1\} & \text{if } k \text{ is cyclic,} \\ D_8 := \{\sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1}\} & \text{if } k \text{ is non-Galois.} \end{cases}$$

We identify Δ as each group appearing above. The center of Δ is $\langle \sigma^2 \rangle$. By [17, Corollary 1.5], $F/\mathbb{Q}$ is also a CM-field. From this, it follows that $F^+/\mathbb{Q}$ is Galois and therefore σ^2 is the complex conjugation: $\mathrm{Gal}(F/F^+) = \langle \sigma^2 \rangle$. Fix a prime ideal $\mathfrak{P}$ in F above p. Since p splits completely in $k/\mathbb{Q}$, it does so in $F/\mathbb{Q}$. Therefore, we can write the prime decomposition of p in F as $(p) = \prod_{g \in \Delta} g(\mathfrak{P})$. Put $\mathfrak{Q} := \sigma(\mathfrak{P})$, $\overline{\mathfrak{P}} := \sigma^2(\mathfrak{P})$, and $\overline{\mathfrak{Q}} := \sigma^3(\mathfrak{P})$. Then each $\overline{\mathfrak{P}}$ and $\overline{\mathfrak{Q}}$ is the complex conjugate of $\mathfrak{P}$ and $\mathfrak{Q}$, respectively. We define

$$\mathfrak{p} := N_{F/k}\mathfrak{P}, \quad \mathfrak{q} := N_{F/k}\mathfrak{Q}, \quad \overline{\mathfrak{p}} := N_{F/k}\overline{\mathfrak{P}}, \quad \overline{\mathfrak{q}} := N_{F/k}\overline{\mathfrak{Q}}.$$

Lemma 3.1.1. *The four prime ideals $\mathfrak{p}$, $\mathfrak{q}$, $\overline{\mathfrak{p}}$, and $\overline{\mathfrak{q}}$ are distinct.*

Proof. In the case where $\Delta = \mathbb{Z}/4\mathbb{Z}$, there is nothing to prove. So, we assume that $\Delta = D_8$. We only prove that $\mathfrak{p}$ is different from other prime ideals. If $\mathfrak{p} = \overline{\mathfrak{p}}$, then $N_{\mathrm{Gal}(F/k)}(\mathfrak{P}) = N_{\mathrm{Gal}(F/k)} \circ \sigma^2(\mathfrak{P})$. By the uniqueness of the prime ideal factorization of $N_{\mathrm{Gal}(F/k)}(\mathfrak{P})$, we have $\sigma^2 \in \mathrm{Gal}(F/k)$, which implies k is totally real. This is a contradiction. Assume that $\mathfrak{p}$ coincides with another prime ideal except $\overline{\mathfrak{p}}$. Then, in the same way, σ or σ^3 is contained in $\mathrm{Gal}(F/k)$. This implies that $\mathrm{Gal}(F/k)$ has an element of order 4. However, the order of $\mathrm{Gal}(F/k)$ is 2. Hence, this is a contradiction. □

We denote by $D_{\mathfrak{p}}$, $D_{\mathfrak{q}}$, $D_{\overline{\mathfrak{p}}}$, and $D_{\overline{\mathfrak{p}}}$ the decomposition groups of $\mathfrak{p}$, $\mathfrak{q}$, $\overline{\mathfrak{p}}$, and $\overline{\mathfrak{q}}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Similarly, let us denote by $I_{\mathfrak{p}}$, $I_{\mathfrak{q}}$, $I_{\overline{\mathfrak{p}}}$, and $I_{\overline{\mathfrak{p}}}$ the inertia groups of $\mathfrak{p}$, $\mathfrak{q}$, $\overline{\mathfrak{p}}$, and $\overline{\mathfrak{q}}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Note that these inertia groups are isomorphic to $\mathbb{Z}_p$ since p splits completely.

Lemma 3.1.2. *With the notation and assumption in the above, the restriction $\sigma|_k \in \mathrm{Hom}(k, F)$ of σ to k acts on $\mathrm{Gal}(\widetilde{k}/k)$ and $X(\widetilde{k})$ via inner automorphism. Moreover,*

$$\sigma|_k(D_{\mathfrak{p}}) = D_{\mathfrak{q}}, \quad \sigma|_k(D_{\mathfrak{q}}) = D_{\overline{\mathfrak{p}}}, \quad \sigma|_k(D_{\overline{\mathfrak{p}}}) = D_{\overline{\mathfrak{q}}}.$$

Proof. Note that $\mathrm{Gal}(\widetilde{F}/F)$ is equipped with the action of σ. Let $D_{\mathfrak{P}}$, $D_{\mathfrak{Q}}$, $D_{\overline{\mathfrak{P}}}$, and $D_{\overline{\mathfrak{Q}}}$ be the decomposition groups in $\mathrm{Gal}(\widetilde{F}/F)$ of $\mathfrak{P}$, $\mathfrak{Q}$, $\overline{\mathfrak{P}}$, and $\overline{\mathfrak{Q}}$, respectively. Then, by the definition of these prime ideals, we have $\sigma(D_{\mathfrak{P}}) = D_{\mathfrak{Q}}$, $\sigma(D_{\mathfrak{Q}}) = D_{\overline{\mathfrak{P}}}$, and $\sigma(D_{\overline{\mathfrak{P}}}) = D_{\overline{\mathfrak{Q}}}$. Since p splits completely in $F/\mathbb{Q}$, the canonical projection $\pi_{\mathfrak{P}} \colon D_{\mathfrak{P}} \to D_{\mathfrak{p}}$ is the isomorphism. From this, we see that

$$\sigma|_k(D_{\mathfrak{p}}) = D_{\mathfrak{q}}$$

is induced. Indeed, using another isomorphism, $\pi_{\mathfrak{Q}} \colon D_{\mathfrak{Q}} \to D_{\mathfrak{q}}$, the map $\sigma|_k \colon D_{\mathfrak{p}} \to D_{\mathfrak{q}}$ is actually written as $\sigma|_k = \pi_{\mathfrak{Q}} \circ \sigma \circ \pi_{\mathfrak{P}}^{-1}$. In the same way, $\sigma|_k(D_{\mathfrak{q}}) = D_{\overline{\mathfrak{p}}}$ and $\sigma|_k(D_{\overline{\mathfrak{p}}}) = D_{\overline{\mathfrak{q}}}$ are induced. We remark that any two of these maps are the same on the intersection of each domain of definition. Since $\mathrm{Gal}(\widetilde{k}/k) = \langle D_{\mathfrak{p}}, D_{\mathfrak{q}}, D_{\overline{\mathfrak{p}}}, D_{\overline{\mathfrak{q}}} \rangle$ by the condition $A(k) = D(k)$, σ acts on $\mathrm{Gal}(\widetilde{k}/k)$. Via the canonical isomorphism $\mathrm{Gal}(F_{\mathrm{cyc}}/F) \simeq \mathrm{Gal}(k_{\mathrm{cyc}}/k)$, we see that $\sigma|_k$ acts on $\mathrm{Gal}(k_{\mathrm{cyc}}/k)$ and the action is trivial. Hence $\sigma|_k$ also acts on $X(k_{\mathrm{cyc}}) = \mathrm{Ker}(\mathrm{Gal}(\widetilde{k}/k) \to \mathrm{Gal}(k_{\mathrm{cyc}}/k))$. This completes the proof. □

Now, we show that the decomposition groups and inertia groups are represented by some parameters as in the following lemma. This fact is a key stone in the proof of our theorem.

Lemma 3.1.3. *Let $\gamma \in \mathrm{Gal}(\widetilde{k}/k)$ be a topological generator of $I_{\mathfrak{p}}$. Then there are some $x, y \in X(k_{\mathrm{cyc}})$ and $a, b \in \mathbb{Z}_p$ such that*

$$\begin{cases} \mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y \rangle, & X(k_{\mathrm{cyc}}) = \langle x, y \rangle, \\ D_{\mathfrak{p}} = \langle \gamma \rangle \times \langle x \rangle, & D_{\mathfrak{q}} = \langle \gamma x^a y^b \rangle \times \langle y \rangle, \\ D_{\overline{\mathfrak{p}}} = \langle \gamma x^{a-b} y^{a+b} \rangle \times \langle x^{-1} \rangle, & D_{\overline{\mathfrak{q}}} = \langle \gamma x^{-b} y^a \rangle \times \langle y^{-1} \rangle. \end{cases}$$

Here, the left side of each direct product is the inertia group of the corresponding prime ideal.

Proof. Take $\sigma|_k$ as in Lemma 3.1.2. We also take $x \in X(k_{\mathrm{cyc}})$ which satisfies $D_{\mathfrak{p}} = \langle \gamma \rangle \times \langle x \rangle$ and put $y := \sigma|_k(x)$. Note that $y \in X(k_{\mathrm{cyc}})$ by Lemma 3.1.2 and that $(\sigma|_k)^2$ is the complex conjugation, so that $(\sigma|_k)^2$ acts on $X(k_{\mathrm{cyc}}) = X(k_{\mathrm{cyc}})^-$ as -1. Applying $\sigma|_k$ on each $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ repeatedly, we obtain

$$D_{\mathfrak{q}} = \langle \sigma|_k(\gamma) \rangle \times \langle y \rangle, \quad D_{\overline{\mathfrak{p}}} = \langle (\sigma|_k)^2(\gamma) \rangle \times \langle x^{-1} \rangle, \quad D_{\overline{\mathfrak{q}}} = \langle (\sigma|_k)^3(\gamma) \rangle \times \langle y^{-1} \rangle \tag{3.1}$$

again by Lemma 3.1.2. Here, the left side of each direct product is the inertia group of the corresponding prime ideal. By the assumption, $X(k_{\mathrm{cyc}})^+$ is trivial and so is $X'(k_{\mathrm{cyc}})^+$. Therefore, by Corollary 2.3.2, we have $X'(k_{\mathrm{cyc}}) \simeq \left(X(k_{\mathrm{cyc}})/X(k_{\mathrm{cyc}})^{\mathrm{Gal}(k_{\mathrm{cyc}}/k)}\right)^-$. Combining this with the assumption that $X(k_{\mathrm{cyc}})$ satisfies the condition (iv) in Proposition 2.4.1, we obtain the triviality of $X'(k_{\mathrm{cyc}})$. This means that the maximal abelian p-extension of k_{cyc} where every prime above p splits completely coincides with k_{cyc}. So we have

$$X(k_{\mathrm{cyc}}) = \langle D_{\mathfrak{p}} \cap X(k_{\mathrm{cyc}}),\ D_{\mathfrak{q}} \cap X(k_{\mathrm{cyc}}),\ D_{\overline{\mathfrak{p}}} \cap X(k_{\mathrm{cyc}}),\ D_{\overline{\mathfrak{q}}} \cap X(k_{\mathrm{cyc}})\rangle = \langle x, y\rangle.$$

Since we know that $\sigma|_k$ acts on $\mathrm{Gal}(k_{\mathrm{cyc}}/k)$ trivially, we get $\sigma|_k(\gamma) \equiv \gamma \bmod X(k_{\mathrm{cyc}})$. So there are some $a, b \in \mathbb{Z}_p$ such that

$$\sigma|_k(\gamma) = \gamma x^a y^b.$$

Combining (3.1) with this, we obtain the representation of the decomposition groups. Finally, since $A(k) = D(k)$, $\mathrm{Gal}(\widetilde{k}/k)$ is generated by the four decomposition groups. This yields $\mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y\rangle$. □

Remark 3.1.4. (i) For the remainder of §3.1, we do not use the Galois action of $\mathrm{Gal}(k/\mathbb{Q})$ except for the complex conjugation $J \in \mathrm{Gal}(k/k^+)$.
(ii) We see that

$$a \neq 0,\ b \neq 0,\ a + b \neq 0.$$

In fact, assume that $a = 0$. Then, $D_{\mathfrak{q}} = \langle \gamma, y\rangle \supset I_{\mathfrak{p}}, I_{\mathfrak{q}}$. This means that the fixed field by $D_{\mathfrak{q}}$ is a $\mathbb{Z}_p$-extension of k which is unramified outside $\{\overline{\mathfrak{p}}, \overline{\mathfrak{q}}\}$ and infinitely decomposed at $\mathfrak{q}$. This contradicts [7, Lemma 3]. In the same way, we get $b \neq 0$. The rest, $a + b \neq 0$, also follows in the same way: if $a + b = 0$, then the fixed field by $D_{\mathfrak{p}} = D_{\overline{\mathfrak{p}}} = \langle \gamma, x\rangle$ is a $\mathbb{Z}_p$-extension of k which is unramified outside $\{\mathfrak{q}, \overline{\mathfrak{q}}\}$ and infinitely decomposed at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. This is again contradicted by the same lemma in [7].

Corollary 3.1.5. *According to the number of generators of $A(k)$, a and b satisfy the following.*

(i) $A(k) = 0 \iff a^2 + b^2 \not\equiv 0 \bmod p$.
(ii) $A(k)$ *is cyclic* $\iff a \not\equiv 0,\ b \not\equiv 0,\ a^2 + b^2 \equiv 0 \bmod p$.
(iii) $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2 \iff a \equiv b \equiv 0 \bmod p$.

Proof. By Lemma 3.1.3, we have $A(k) \simeq \langle \gamma, x, y\rangle / \langle I_{\mathfrak{p}}, I_{\mathfrak{q}}, I_{\overline{\mathfrak{p}}}, I_{\overline{\mathfrak{p}}}\rangle = \langle \gamma, x, y\rangle / \langle \gamma, x^a y^b, x^{-b} y^a\rangle$. Hence, we have a presentation of $A(k)$ whose presentation matrix is given by

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{bmatrix}.$$

In other words, there is a linear map $\langle \gamma, x, y\rangle \to \langle \gamma, x, y\rangle$ whose cokernel is $A(k)$ and whose representation matrix is A. So, it is sufficient to consider the rank of $\overline{A} := A \bmod p$:

$$\begin{cases} A(k) = 0 & \iff \operatorname{rank} \overline{A} = 3 \\ A(k) \text{ is cyclic} & \iff \operatorname{rank} \overline{A} = 2 \\ \dim_{\mathbb{F}_p} A(k)/pA(k) = 2 & \iff \operatorname{rank} \overline{A} = 1. \end{cases}$$

The lemma directly follows from this. □

We put $G := \mathrm{Gal}(L(k_{\mathrm{cyc}})/k)$ and compute $\mathcal{K}(G)$. We remark that the following is used in §3.1.2 but not in §3.1.3.

Lemma 3.1.6. *Set $G := \mathrm{Gal}(L(k_{\mathrm{cyc}})/k)$ and let $\mathcal{K}(G)$ be the module defined in Proposition* 2.2.1. *Then $\mathcal{K}(G) = 0$ if and only if $a + b \not\equiv 0 \bmod p$.*

Proof. Let F be a free pro-p group generated by γ, x, and y and R be the closed normal subgroup of F generated by $[\gamma, x]$, $[\gamma, y]$, $[x, y]$ and their conjugates. Then we have a minimal representation $1 \to R \to F \to \mathrm{Gal}(L(k_{\mathrm{cyc}})/k) \to 1$ of $\mathrm{Gal}(L(k_{\mathrm{cyc}})/k)$ by Lemma 3.1.3 and

$$H_2(\mathrm{Gal}(L(k_{\mathrm{cyc}})/k), \mathbb{Z}_p) \simeq R \cap [F, F]/[R, F] = \langle [\gamma, x], [\gamma, y], [x, y] \rangle [R, F]/[R, F]$$

by (2.3). In the same way, we see that each image of $H_2(D_{\mathfrak{p}}, \mathbb{Z}_p)$, $H_2(D_{\mathfrak{q}}, \mathbb{Z}_p)$, $H_2(D_{\overline{\mathfrak{p}}}, \mathbb{Z}_p)$, and $H_2(D_{\overline{\mathfrak{q}}}, \mathbb{Z}_p)$ by the map (2.4) is generated by

$$[\gamma, x], \quad [\gamma x^a y^b, y], \quad [\gamma x^{a-b} y^{a+b}, x^{-1}], \quad [\gamma x^{-b} y^a, y^{-1}],$$

respectively. In modulo $[R, F]$, we have

$$\begin{aligned}
&[\gamma x^a y^b, y] \equiv [\gamma, y][x^a, y][y^b, y] \equiv [\gamma, y][x, y]^a, \\
&[\gamma x^{a-b} y^{a+b}, x^{-1}] \equiv [\gamma, x]^{-1}[x, y]^{a+b}, \\
&[\gamma x^{-b} y^a, y^{-1}] \equiv [\gamma, y]^{-1}[x, y]^b.
\end{aligned}$$

Fixing the basis $\{[\gamma, x], [\gamma, y], [x, y]\}$ of $\mathbb{Z}_p$-module $R \cap [F, F]/[R, F]$, we obtain a presentation of $\mathcal{K}(G)$ whose presentation matrix is given by

$$K := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ -1 & 0 & a+b \\ 0 & -1 & b \end{bmatrix}.$$

So, $\mathcal{K}(G) = 0$ if and only if the rank of K mod p is equal to 3, which is equivalent to $a + b \not\equiv 0 \bmod p$. □

3.1.2 Proof

To prove the main theorem in this case, we only need to show the following.

Proposition 3.1.7. *Let k be a non-Galois CM-field or a totally imaginary cyclic extension of degree* 4. *Suppose that k satisfies the conditions* (I)(II)(III) *in the last expression of* §2.4. *Then $X(\widetilde{k})$ is trivial if and only if $a + b \not\equiv 0 \bmod p$.*

Here, we explain that the main theorem in this case follows from the above proposition. Since $\langle D_{\mathfrak{p}}, D_{\overline{\mathfrak{p}}}\rangle = \langle \gamma, x, y^{a+b}\rangle$ by Lemma 3.1.3, the condition $a+b \not\equiv 0 \bmod p$ holds if and only if there is no non-trivial p-extension of k which is completely decomposed at any prime ideal in $\{\mathfrak{p}, \overline{\mathfrak{p}}\}$ and unramified outside $\{\mathfrak{q}, \overline{\mathfrak{q}}\}$. Therefore, in the case where $A(k) = 0$, the proposition is a paraphrase of the main theorem using different words. If $A(k)$ is cyclic, then we can easily check $a+b \not\equiv 0 \bmod p$ by Corollary 3.1.5, so the proposition yields that $X(\widetilde{k})$ is trivial. Similarly, in the case where $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2$, we know that $a+b \equiv 0 \bmod p$, so we obtain that $X(\widetilde{k})$ is not trivial.

To prove Proposition 3.1.7, we need the following.

Lemma 3.1.8. *Define k_∞ by $k_\infty \leftrightarrow \langle \gamma x^a, xy^{-1}\rangle$ (for the notation $\leftrightarrow$, see Definition 2.1.1). Then k_∞/k is a $\mathbb{Z}_p$-extension such that p is non-split and ramifies. Moreover, the complex conjugation $J \in \mathrm{Gal}(k/k^+)$ acts on $\mathrm{Gal}(k_\infty/k)$ as -1.*

Proof. Note that

$$J(\gamma x^a) = \gamma x^a \cdot x^{-a-b}y^{a+b} \in \langle \gamma x^a, xy^{-1}\rangle.$$

Since $\mathrm{Gal}(k_\infty/k) = \langle \gamma, x, y\rangle / \langle \gamma x^a, xy^{-1}\rangle = \langle x, \gamma x^a, xy^{-1}\rangle / \langle \gamma x^a, xy^{-1}\rangle \simeq \mathbb{Z}_p$, we see that k_∞/k is a $\mathbb{Z}_p$-extension and that J acts on $\mathrm{Gal}(k_\infty/k)$ as -1. On the other hand, by Lemma 3.1.3 and Remark 3.1.4(ii), we see that

$$\begin{cases} \langle \gamma x^a, xy^{-1}, I_{\mathfrak{p}}\rangle = \langle \gamma x^a, xy^{-1}, I_{\overline{\mathfrak{p}}}\rangle = \langle \gamma, x^a, xy^{-1}\rangle \neq \langle \gamma x^a, xy^{-1}\rangle \\ \langle \gamma x^a, xy^{-1}, I_{\mathfrak{q}}\rangle = \langle \gamma x^a, xy^{-1}, I_{\overline{\mathfrak{q}}}\rangle = \langle \gamma x^a, y^b, xy^{-1}\rangle \neq \langle \gamma x^a, xy^{-1}\rangle. \end{cases}$$

Similarly, we see that all four of the groups $\langle \gamma x^a, xy^{-1}, D_{\mathfrak{p}}\rangle$, $\langle \gamma x^a, xy^{-1}, D_{\overline{\mathfrak{p}}}\rangle$, $\langle \gamma x^a, xy^{-1}, D_{\mathfrak{q}}\rangle$, and $\langle \gamma x^a, xy^{-1}, D_{\overline{\mathfrak{q}}}\rangle$ coincide with $\langle \gamma, x, y\rangle$. These facts imply that any prime ideal above p is non-split and ramifies in k_∞/k. □

Now, we show Proposition 3.1.7. If $a+b \not\equiv 0 \bmod p$, then $X(\widetilde{k})$ is trivial by Lemma 3.1.6 and Proposition 2.2.1 (for an alternative proof, see §3.1.3). To prove the converse by contradiction, assume that $a+b \equiv 0 \bmod p$ and $X(\widetilde{k})$ is trivial. Set $n := \mathrm{ord}_p(a+b)$. Note that $n < \infty$ by Remark 3.1.4(ii) and that if $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2$ then $n > 0$ by Corollary 3.1.5. Define P_∞, Q_∞, P_n, Q_n by

$$\begin{cases} P_\infty \leftrightarrow D_{\mathfrak{p}} = \langle \gamma, x\rangle, & Q_\infty \leftrightarrow D_{\mathfrak{q}} = \langle \gamma x^a, y\rangle, \\ P_n \leftrightarrow \langle D_{\mathfrak{p}}, D_{\overline{\mathfrak{p}}}\rangle = \langle \gamma, x, y^{a+b}\rangle, & Q_n \leftrightarrow \langle D_{\mathfrak{q}}, D_{\overline{\mathfrak{q}}}\rangle = \langle \gamma x^a, x^{a+b}, y\rangle. \end{cases}$$

Then we see that both P_∞ and Q_∞ are $\mathbb{Z}_p$-extensions of k and that each P_n and Q_n is contained in P_∞ and Q_∞, respectively. Let k_∞ be the field defined in Lemma 3.1.8. Then $k_\infty \subset P_\infty Q_\infty$ since $P_\infty Q_\infty \leftrightarrow \langle \gamma x^a\rangle$. Also, $P_\infty Q_\infty / k_\infty$ is a $\mathbb{Z}_p$-extension, and especially cyclic (Figure 1).

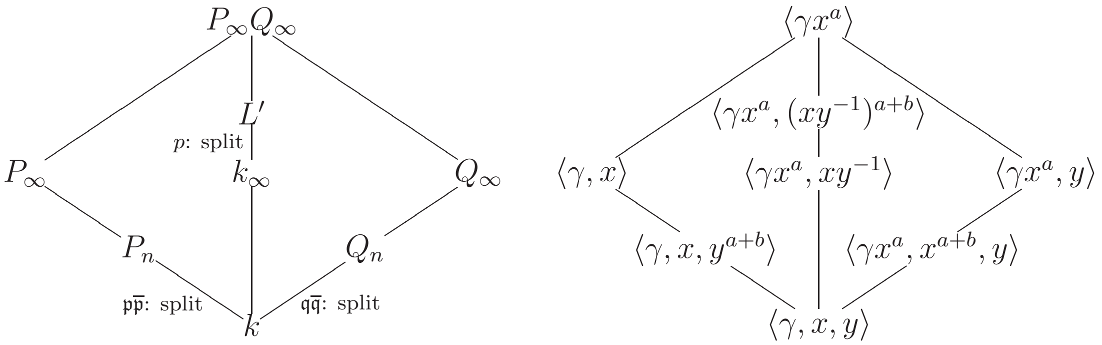

$P_\infty Q_\infty$
L'
p: split
P_∞
k_∞
Q_∞
P_n
Q_n
$\mathfrak{p}\overline{\mathfrak{p}}$: split
$\mathfrak{q}\overline{\mathfrak{q}}$: split
k
$\langle \gamma x^a \rangle$
$\langle \gamma x^a, (xy^{-1})^{a+b} \rangle$
$\langle \gamma, x \rangle$
$\langle \gamma x^a, xy^{-1} \rangle$
$\langle \gamma x^a, y \rangle$
$\langle \gamma, x, y^{a+b} \rangle$
$\langle \gamma x^a, x^{a+b}, y \rangle$
$\langle \gamma, x, y \rangle$

Figure 1:

Note that p does not split in k_∞/k by Lemma 3.1.8. Since $\mathfrak{p}$, $\overline{\mathfrak{p}}$ and $\mathfrak{q}$, $\overline{\mathfrak{q}}$ split completely in P_n/k and Q_n/k, respectively, there exists a cyclic extension L' of k_∞ with degree p^n such that p splits completely in L'/k_∞. Moreover, L'/k_∞ is unramified by Lemma 3.1.8 again. Therefore there is a natural projection

$$X'(k_\infty) \twoheadrightarrow \mathrm{Gal}(L'/k_\infty) = \langle \gamma x^a, xy^{-1} \rangle / \langle \gamma x^a, (xy^{-1})^{a+b} \rangle.$$

Thus, by Corollary 2.3.3, the induced action of the complex conjugation J on $\mathrm{Gal}(L'/\widetilde{k})$ is trivial. However, we can check that J actually acts on $\mathrm{Gal}(L'/\widetilde{k}) = \langle xy^{-1}, \gamma x^a \rangle / \langle (xy^{-1})^{a+b}, \gamma x^a \rangle$ as -1. This is a contradiction. So we conclude that if $X(\widetilde{k})$ is trivial, then $a+b \not\equiv 0 \bmod p$.

3.1.3 Another proof

We give another proof of the sufficient condition in Proposition 3.1.7 since the idea, which is based on Minardi [18], Itoh [12], and Fujii [7], is used in §4.2. In other words, we prove that if $a+b \not\equiv 0 \bmod p$, then $X(\widetilde{k})$ is trivial without using Proposition 2.2.1.

Suppose that $a+b \not\equiv 0 \bmod p$. Then $\dim_{\mathbb{F}_p} A(k)/pA(k) \le 1$ by Corollary 3.1.5. Define $k^{(1)}$, $k^{(2)}$, $N_\mathfrak{p}$ and their conjugate $\overline{k^{(1)}}$, $\overline{k^{(2)}}$, $N_{\overline{\mathfrak{p}}}$ by

$$\begin{cases} k^{(1)} \leftrightarrow \langle I_\mathfrak{p}, I_\mathfrak{q} \rangle = \langle \gamma, x^a y^b \rangle, & k^{(2)} \leftrightarrow I_\mathfrak{p} = \langle \gamma \rangle, \qquad N_\mathfrak{p} \leftrightarrow D_\mathfrak{p} = \langle \gamma, x \rangle, \\ \overline{k^{(1)}} \leftrightarrow \langle I_{\overline{\mathfrak{p}}}, I_{\overline{\mathfrak{q}}} \rangle = \langle \gamma x^{a-b} y^{a+b}, x^a y^b \rangle, & \overline{k^{(2)}} \leftrightarrow I_{\overline{\mathfrak{p}}} = \langle \gamma x^{a-b} y^{a+b} \rangle, \quad N_{\overline{\mathfrak{p}}} \leftrightarrow D_{\overline{\mathfrak{p}}} = \langle \gamma y^{a+b}, x \rangle. \end{cases}$$

We may assume that $a \not\equiv 0 \bmod p$ in the following argument. Otherwise (this occurs in the case where $A(k) = 0$, and then $b \not\equiv 0 \bmod p$), replacing the role of $\mathfrak{q}$ with $\overline{\mathfrak{q}}$, for example $k^{(1)} \leftrightarrow \langle I_\mathfrak{p}, I_{\overline{\mathfrak{q}}} \rangle = \langle \gamma, x^{-b} y^a \rangle$, we have the same conclusion.

Lemma 3.1.9. *The module $X(k^{(1)})$ is trivial.*

Proof. We remark that, in the case where $A(k) = 0$, the claim follows directly from [12, Corollary 3.3]. However, we do not need this fact. Let L_0 be the maximal subfield in $L(k^{(1)})$ which is abelian over k. Then $\mathrm{Gal}(L_0/k^{(1)})$ is isomorphic to $X(k^{(1)})_{\mathrm{Gal}(k^{(1)}/k)}$, since $\mathrm{Gal}(k^{(1)}/k) \simeq \mathbb{Z}_p$. Since L_0/k is an abelian p-extension that is unramified outside $\{\mathfrak{q}, \overline{\mathfrak{p}}, \overline{\mathfrak{q}}\}$, we obtain $L_0 \subset k^{(2)} \cap L(k^{(1)})$. On the other hand, by the definition of $k^{(2)}$, all primes in $k^{(1)}$ above $\mathfrak{q}$ are totally ramified in $k^{(2)} \cap L(k^{(1)})/k^{(1)}$. Therefore $k^{(2)} \cap L(k^{(1)}) = k^{(1)}$, which yields $L_0 = k^{(1)}$. From this, it follows that $X(k^{(1)})_{\mathrm{Gal}(k^{(1)}/k)}$ is trivial, and so is $X(k^{(1)})$ by Nakayama's lemma. □

Lemma 3.1.10. *The module $X(k^{(2)})$ is trivial.*

Proof. From the assumption $a \not\equiv 0 \bmod p$, we obtain $\langle I_{\mathfrak{p}}, D_{\mathfrak{q}} \rangle = \langle \gamma, x^a, y \rangle = \langle \gamma, x, y \rangle$, which implies that $\mathfrak{q}$ is totally inert in $k^{(1)}/k$. So, there is only one prime in $k^{(1)}$ above $\mathfrak{q}$. Therefore, in $k^{(2)}/k^{(1)}$, exactly one prime is ramified and it is totally ramified. Combining Lemma 3.1.9 with this, it follows that $X(k^{(2)})$ is trivial. □

Let L_2 be the maximal subfield in $L(\widetilde{k})$ which is abelian over $k^{(2)}$. Then $\mathrm{Gal}(L_2/k^{(2)})$ is isomorphic to $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k^{(2)})}$ since $\mathrm{Gal}(\widetilde{k}/k^{(2)}) \simeq \mathbb{Z}_p$.

Lemma 3.1.11. *With the notation above, $L_2/N_{\mathfrak{p}}$ is abelian.*

Proof. Our proof is similar to the proofs of [18], [12], and [7]. For a prime $\mathfrak{P}^{(2)}$ of $k^{(2)}$ above $\mathfrak{p}$, denote by $I_{\mathfrak{P}^{(2)}}$ the inertia subgroup in $\mathrm{Gal}(L_2/k^{(2)})$. Any prime in $N_{\mathfrak{p}}$ above $\mathfrak{p}$ is totally inert in $k^{(2)}/N_{\mathfrak{p}}$ by the definitions of $k^{(2)}$ and $N_{\mathfrak{p}}$. This shows that $I_{\mathfrak{P}^{(2)}}$ is a $\mathbb{Z}_p[\![\mathrm{Gal}(k^{(2)}/N_{\mathfrak{p}})]\!]$-module for each prime $\mathfrak{P}^{(2)}$ of $k^{(2)}$ above $\mathfrak{p}$. Since $X(k^{(2)})$ is trivial by Lemma 3.1.10 and $L_2/k^{(2)}$ is unramified outside $\mathfrak{p}$, we have the isomorphism

$$\mathrm{Gal}(L_2/k^{(2)}) = \sum_{\mathfrak{P}^{(2)}|\mathfrak{p}} I_{\mathfrak{P}^{(2)}} \tag{3.2}$$

as $\mathbb{Z}_p[\![\mathrm{Gal}(k^{(2)}/N_{\mathfrak{p}})]\!]$-modules. Now we claim that $\mathrm{Gal}(k^{(2)}/N_{\mathfrak{p}})$ acts on $I_{\mathfrak{P}^{(2)}}$ trivially. Since $L_2/\widetilde{k}$ is unramified, we have $I_{\mathfrak{P}^{(2)}} \cap \mathrm{Gal}(L_2/\widetilde{k}) = 1$. This shows that the restriction map $I_{\mathfrak{P}^{(2)}} \to \mathrm{Gal}(\widetilde{k}/k^{(2)})$ is injective. Since $\widetilde{k}/N_{\mathfrak{p}}$ is abelian, the action of $\mathrm{Gal}(k^{(2)}/N_{\mathfrak{p}})$ on $\mathrm{Gal}(\widetilde{k}/k^{(2)})$ is trivial by Lemma 2.1.2, and therefore its action on $I_{\mathfrak{P}^{(2)}}$ is also trivial. By (3.2), $\mathrm{Gal}(k^{(2)}/N_{\mathfrak{p}})$ acts on $\mathrm{Gal}(L_2/k^{(2)})$ trivially, so by Lemma 2.1.2 again, $L_2/N_{\mathfrak{p}}$ is abelian. □

Replacing the role of $\mathfrak{p}$ and $\mathfrak{q}$ with $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{q}}$, respectively, in the above argument, we see that $\overline{L_2}/N_{\overline{\mathfrak{p}}}$ is abelian, where $\overline{L_2}$ is the maximal subfield in $L(\widetilde{k})$ which is abelian over $\overline{k^{(2)}}$. To prove the triviality of $X(\widetilde{k})$, we show that $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ is trivial. Let $\mathcal{C}_{\widetilde{k}/k}$ be the subfield in $L(\widetilde{k})/\widetilde{k}$ such that $\mathrm{Gal}(\mathcal{C}_{\widetilde{k}/k}/\widetilde{k}) \simeq X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$. Note that $k = N_{\mathfrak{p}} \cap N_{\overline{\mathfrak{p}}}$, since

$N_{\mathfrak{p}} \cap N_{\overline{\mathfrak{p}}} \leftrightarrow \langle D_{\mathfrak{p}}, D_{\overline{\mathfrak{p}}} \rangle = \langle \gamma, x, y^{a+b} \rangle$, and $a + b \not\equiv 0 \bmod p$. Combining the correspondence $N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}} \leftrightarrow \langle x \rangle$ with this, we have the following (see Figure 2):

$$k = N_{\mathfrak{p}} \cap N_{\overline{\mathfrak{p}}} \subset k_{\mathrm{cyc}} \subset N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}. \tag{3.3}$$

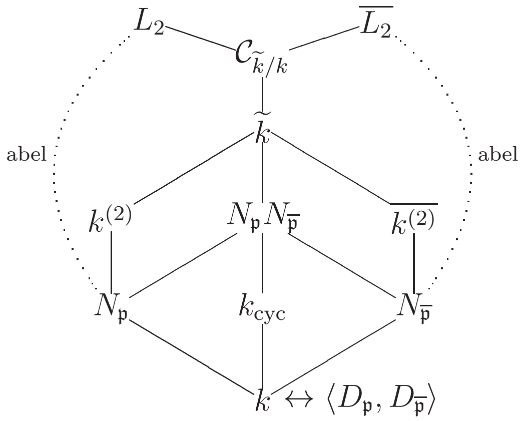

L_2
$\overline{L_2}$
$\mathcal{C}_{\widetilde{k}/k}$
$\widetilde{k}$
abel
abel
$k^{(2)}$
$N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}$
$\overline{k^{(2)}}$
$N_{\mathfrak{p}}$
k_{cyc}
$N_{\overline{\mathfrak{p}}}$
$k \leftrightarrow \langle D_{\mathfrak{p}}, D_{\overline{\mathfrak{p}}} \rangle$

Figure 2:

On the other hand, by the natural surjections $\mathrm{Gal}(L_2/\widetilde{k}) \simeq X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k^{(2)})} \twoheadrightarrow X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ and $\mathrm{Gal}(\overline{L_2}/\widetilde{k}) \simeq X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/\overline{k^{(2)}})} \twoheadrightarrow X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$, we have

$$\widetilde{k} \subset \mathcal{C}_{\widetilde{k}/k} \subset L_2 \cap \overline{L_2}.$$

Since $\widetilde{k}/k_{\mathrm{cyc}}$ is unramified and $\widetilde{k} \subset \mathcal{C}_{\widetilde{k}/k} \subset L(\widetilde{k})$, we see that the (possibly non-abelian) p-extension $\mathcal{C}_{\widetilde{k}/k}/k_{\mathrm{cyc}}$ is also unramified. Now we claim that $\mathcal{C}_{\widetilde{k}/k}/k_{\mathrm{cyc}}$ is abelian. Indeed, since $\mathcal{C}_{\widetilde{k}/k}/N_{\mathfrak{p}}$ is abelian by Lemma 3.1.11, $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/N_{\mathfrak{p}})$, which is isomorphic to $\mathbb{Z}_p$, acts on $\mathrm{Gal}(\mathcal{C}_{\widetilde{k}/k}/N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}})$ trivially by Lemma 2.1.2. In the same way, $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/N_{\overline{\mathfrak{p}}})$ also acts on $\mathrm{Gal}(\mathcal{C}_{\widetilde{k}/k}/N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}})$ trivially. Since any element in $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/k_{\mathrm{cyc}})$ is represented by the product of elements in $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/N_{\mathfrak{p}})$ and $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/N_{\overline{\mathfrak{p}}})$ by (3.3), we see that $\mathrm{Gal}(N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}}/k_{\mathrm{cyc}}) \simeq \mathbb{Z}_p$ also acts on $\mathrm{Gal}(\mathcal{C}_{\widetilde{k}/k}/N_{\mathfrak{p}} N_{\overline{\mathfrak{p}}})$ trivially. So, by Lemma 2.1.2 again, $\mathcal{C}_{\widetilde{k}/k}/k_{\mathrm{cyc}}$ is abelian (and unramified). Since we know $\widetilde{k} = L(k_{\mathrm{cyc}})$, this implies that $\mathcal{C}_{\widetilde{k}/k} = \widetilde{k}$. By the definition of $\mathcal{C}_{\widetilde{k}/k}$, we obtain that $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ is trivial and so is $X(\widetilde{k})$ by Nakayama's lemma. This completes the proof.

3.2 The case of totally imaginary $(2, 2)$-extensions

In this subsection, let k be a totally imaginary $(2, 2)$-extension over $\mathbb{Q}$. Suppose that k satisfies the conditions (I)(II)(III) in the last expression of §2.4. We chose two generators σ, τ of $\mathrm{Gal}(k/\mathbb{Q})$ as $J := \sigma\tau$ is the complex conjugation. Then $\sigma\tau$ acts on $X(k_{\mathrm{cyc}}) =$

$X(k_{\mathrm{cyc}})^-$ as -1. Fix one of the prime ideals $\mathfrak{p}$ of k above p and define the other prime ideals $\overline{\mathfrak{p}}$, $\mathfrak{q}$, and $\overline{\mathfrak{q}}$ of k above p as follows:

$$\overline{\mathfrak{p}} := \sigma\tau(\mathfrak{p}), \quad \mathfrak{q} := \sigma(\mathfrak{p}), \quad \overline{\mathfrak{q}} := \tau(\mathfrak{p}). \tag{3.4}$$

Then the notation $\overline{\,\cdot\,}$ means the complex conjugate. We denote by $D_{\mathfrak{p}}$, $D_{\mathfrak{q}}$, $D_{\overline{\mathfrak{p}}}$, and $D_{\overline{\mathfrak{p}}}$ the decomposition group of $\mathfrak{p}$, $\mathfrak{q}$, $\overline{\mathfrak{p}}$, and $\overline{\mathfrak{q}}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Similarly, we denote by $I_{\mathfrak{p}}$, $I_{\mathfrak{q}}$, $I_{\overline{\mathfrak{p}}}$, and $I_{\overline{\mathfrak{p}}}$ the inertia group of $\mathfrak{p}$, $\mathfrak{q}$, $\overline{\mathfrak{p}}$, and $\overline{\mathfrak{q}}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Now, we obtain a result similar to Lemma 3.1.3:

Lemma 3.2.1. *Let $\gamma \in \mathrm{Gal}(\widetilde{k}/k)$ be a topological generator of $I_{\mathfrak{p}}$. Then there are some $x, y \in X(k_{\mathrm{cyc}})$ and $a, b \in \mathbb{Z}_p$ such that*

$$\begin{cases} \mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y \rangle, & X(k_{\mathrm{cyc}}) = \langle x, y \rangle, \\ D_{\mathfrak{p}} = \langle \gamma \rangle \times \langle x \rangle, & D_{\mathfrak{q}} = \langle \gamma x^a y^{-a} \rangle \times \langle y \rangle, \\ D_{\overline{\mathfrak{p}}} = \langle \gamma x^{a+b} y^{b-a} \rangle \times \langle x^{-1} \rangle, & D_{\overline{\mathfrak{q}}} = \langle \gamma x^b y^b \rangle \times \langle y^{-1} \rangle. \end{cases}$$

Here, the left side of each direct product is the inertia group of the corresponding prime ideal.

Proof. We take $x \in X(k_{\mathrm{cyc}})$ which satisfies $D_{\mathfrak{p}} = \langle \gamma \rangle \times \langle x \rangle$ and put $y := \sigma(x)$. Note that $\tau(x) = y^{-1}$ since $\sigma(\tau(x)) = x^{-1}$. Apply σ, $\sigma\tau$, and τ on each $I_{\mathfrak{p}}$ and $D_{\mathfrak{p}}$; then we obtain

$$D_{\mathfrak{q}} = \langle \sigma(\gamma) \rangle \times \langle y \rangle, \quad D_{\overline{\mathfrak{p}}} = \langle \sigma\tau(\gamma) \rangle \times \langle x^{-1} \rangle, \quad D_{\overline{\mathfrak{q}}} = \langle \tau(\gamma) \rangle \times \langle y^{-1} \rangle \tag{3.5}$$

by (3.4). Here, the left side of each direct product is the inertia group of the corresponding prime ideal. In the same way as in the proof of Lemma 3.1.3, we obtain

$$X(k_{\mathrm{cyc}}) = \langle D_{\mathfrak{p}} \cap X(k_{\mathrm{cyc}}),\ D_{\mathfrak{q}} \cap X(k_{\mathrm{cyc}}),\ D_{\overline{\mathfrak{p}}} \cap X(k_{\mathrm{cyc}}),\ D_{\overline{\mathfrak{q}}} \cap X(k_{\mathrm{cyc}}) \rangle = \langle x, y \rangle,$$

and $\sigma(\gamma) \equiv \gamma \bmod X(k_{\mathrm{cyc}})$. So there are some $a, b, c, d \in \mathbb{Z}_p$ such that $\sigma(\gamma) = \gamma x^a y^c$, $\tau(\gamma) = \gamma x^b y^d$. Since both σ^2 and τ^2 are the identity map, we have $\gamma = \sigma^2(\gamma) = \gamma x^{a+c} y^{a+c}$ and $\gamma = \tau^2(\gamma) = \gamma x^{b-d} y^{d-b}$, which yield $c = -a$ and $d = b$. Therefore

$$\sigma(\gamma) = \gamma x^a y^{-a}, \quad \tau(\gamma) = \gamma x^b y^b.$$

Combining (3.5) with these equations, we obtain the representation of the decomposition groups. Finally, again in the same manner as in the proof of Lemma 3.1.3, we have $\mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y \rangle$. □

Remark 3.2.2. For the same reason as in Remark 3.1.4, we have $a \neq 0,\ b \neq 0,\ a - b \neq 0$.

In a similar way as in §3.1, we can prove the main theorem in this case. Here, we only write each object down in Table 1 (the modulus in the table is p).

	§3.1	§3.2
$A(k) = 0 \quad \Longleftrightarrow$	$a^2 + b^2 \not\equiv 0$	$a \not\equiv 0,\ b \not\equiv 0$
$A(k)$: cyclic $\quad \Longleftrightarrow$	$a, b \not\equiv 0,\ a^2 + b^2 \equiv 0$	$ab \equiv 0$ and $a - b \not\equiv 0$
$\dim_{\mathbb{F}_p} A(k)/pA(k) = 2 \quad \Longleftrightarrow$	$a \equiv b \equiv 0$	$a \equiv b \equiv 0$
$\mathcal{K}(G) = 0 \quad \Longleftrightarrow$	$n := \mathrm{ord}_p(a+b)$ is 0	$n := \mathrm{ord}_p(a-b)$ is 0
k_∞	$\langle \gamma x^a, xy^{-1} \rangle$	$\langle \gamma x^a, xy \rangle$
P_∞	$D_\mathfrak{p} = \langle \gamma, x \rangle$	$D_\mathfrak{p} = \langle \gamma, x \rangle$
Q_∞	$D_\mathfrak{q} = \langle \gamma x^a, y \rangle$	$D_\mathfrak{q} = \langle \gamma x^a, y \rangle$
P_n	$\langle D_\mathfrak{p}, D_{\overline{\mathfrak{p}}} \rangle = \langle \gamma, x, y^{a+b} \rangle$	$\langle D_\mathfrak{p}, D_{\overline{\mathfrak{p}}} \rangle = \langle \gamma, x, y^{a-b} \rangle$
Q_n	$\langle D_\mathfrak{q}, D_{\overline{\mathfrak{q}}} \rangle = \langle \gamma, x^{a+b}, y \rangle$	$\langle D_\mathfrak{q}, D_{\overline{\mathfrak{q}}} \rangle = \langle \gamma, x^{a-b}, y \rangle$
L'	$\langle \gamma x^a, (xy^{-1})^{a+b} \rangle$	$\langle \gamma x^a, (xy)^{a-b} \rangle$
$k^{(1)}$	$\langle I_\mathfrak{p}, I_\mathfrak{q} \rangle = \langle \gamma, x^a y^b \rangle$	$\langle I_\mathfrak{p}, I_\mathfrak{q} \rangle = \langle \gamma, x^a y^{-a} \rangle$
$k^{(2)}$ and $N_\mathfrak{p}$	$I_\mathfrak{p} = \langle \gamma \rangle$ and $D_\mathfrak{p} = \langle \gamma, x \rangle$	$I_\mathfrak{p} = \langle \gamma \rangle$ and $D_\mathfrak{p} = \langle \gamma, x \rangle$
The goal: $X(\widetilde{k}) = 0 \quad \Longleftrightarrow$	$a + b \not\equiv 0$	$a - b \not\equiv 0$

Table 1:

4 In the case of degree 6

4.1 Setting and preparation

Suppose that k is a CM-field of degree 6 which satisfies the conditions (I)(II)(III) in the last expression of §2.4. Let $F/\mathbb{Q}$ be the Galois closure of $k/\mathbb{Q}$ with the Galois group $\Delta := \mathrm{Gal}(F/\mathbb{Q})$. For the group structure of Δ, the following is known (see, for example, Dodson [2, Theorem in §5.1.2] or Bouw et al. [1, Proposition 2.1]).

Lemma 4.1.1. *Let k be a CM-field of degree 6 and let Δ be the Galois group of the Galois closure of $k/\mathbb{Q}$. Then Δ is isomorphic to one of the following groups:*

(i) $\mathbb{Z}/6\mathbb{Z} = \{\sigma \mid \sigma^6 = 1\}$,

(ii) $D_{12} = \{\sigma, \tau \mid \sigma^6 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1}\}$,

(iii) $$(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z} = \left\{ a, b, c, x \;\middle|\; \begin{array}{l} a^2 = b^2 = c^2 = x^3 = 1,\ ab = ba,\ bc = cb,\ ca = ac, \\ ax = xc,\ bx = xa,\ cx = xb \end{array} \right\},$$

(iv) $$(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathcal{S}_3 = \left\{ a, b, c, x, y \;\middle|\; \begin{array}{l} a^2 = b^2 = c^2 = x^3 = y^2 = 1,\ ab = ba,\ bc = cb,\ ca = ac, \\ ax = xc,\ bx = xa,\ cx = xb,\ ya = by,\ yb = ay,\ yc = cy, \\ yx = x^2 y \end{array} \right\}.$$

Here, $\mathcal{S}_3$ is the symmetric group of degree 3. *And* $\rtimes$ *denotes the semi-direct product of groups, so* $\mathbb{Z}/3\mathbb{Z}$ *in* (iii) *and* $\mathcal{S}_3$ *in* (iv) *are acting by permutations on the three copies of* $\mathbb{Z}/2\mathbb{Z}$. *In particular, if* $k/\mathbb{Q}$ *is Galois, then the Galois group* Δ *is cyclic of order* 6.

We identify Δ as each group appearing in Lemma 4.1.1. In the cases (iii) and (iv), set

$$\sigma := abcx.$$

Then, in every case of (i), ..., (iv), we can check that σ is of order 6 and $\langle\sigma^3\rangle$ is the center of $\mathrm{Gal}(F/\mathbb{Q})$. By [17, Corollary 1.5], $F/\mathbb{Q}$ is also CM-field. This yields that $F^+/\mathbb{Q}$ is Galois and therefore $\mathrm{Gal}(F/F^+) = \langle\sigma^3\rangle$, in other words, σ^3 is the complex conjugation. Fix a prime ideal $\mathfrak{P}_1$ in F above p. Since p splits completely in $k/\mathbb{Q}$, it does so in $F/\mathbb{Q}$. Therefore, each prime ideal $g(\mathfrak{P}_1)$ $(g \in \Delta)$ is distinct. Put

$$\begin{aligned} &\overline{\mathfrak{P}_2} := \sigma(\mathfrak{P}_1), \quad \mathfrak{P}_3 := \sigma^2(\mathfrak{P}_1), \\ \overline{\mathfrak{P}_1} := \sigma^3(\mathfrak{P}_1), \quad &\mathfrak{P}_2 := \sigma^4(\mathfrak{P}_1), \quad \overline{\mathfrak{P}_3} := \sigma^5(\mathfrak{P}_1). \end{aligned} \tag{4.1}$$

Then $\overline{\mathfrak{P}_i}$ is the complex conjugate of $\mathfrak{P}_i$ $(i = 1, 2, 3)$. We define

$$\mathfrak{p}_i := N_{F/k}\mathfrak{P}_i, \quad \overline{\mathfrak{p}_i} := N_{F/k}\overline{\mathfrak{P}_i} \quad (i = 1, 2, 3).$$

Lemma 4.1.2. *The six prime ideals* $\mathfrak{p}_1$, $\overline{\mathfrak{p}_i}$ $(i = 1, 2, 3)$ *in* k *are distinct.*

Proof. The proof is similar to that of Lemma 3.1.1. In the case where $\Delta = \mathbb{Z}/6\mathbb{Z}$, there is nothing to prove. So, we consider other cases. We only prove $\mathfrak{p}_1$ is different from other prime ideals. If $\mathfrak{p}_1 = \overline{\mathfrak{p}_1}$, then $N_{\mathrm{Gal}(F/k)}(\mathfrak{P}_1) = N_{\mathrm{Gal}(F/k)} \circ \sigma^3(\mathfrak{P}_1)$. By the uniqueness of the prime ideal factorization of $N_{\mathrm{Gal}(F/k)}(\mathfrak{P}_1)$, we have $\sigma^3 \in \mathrm{Gal}(F/k)$, which implies k is totally real. This is a contradiction. Assume that $\mathfrak{p}_1$ coincides with another prime ideal except $\overline{\mathfrak{p}_1}$. Then, in the same way, there is some $1 \le j \le 5$ $(j \neq 3)$ such that $\sigma^j \in \mathrm{Gal}(F/k)$. This implies that $\mathrm{Gal}(F/k)$ has an element ρ of order 3. Therefore, the fixed field by $\langle\rho\rangle$ contains k and has a degree of power of 2 over $\mathbb{Q}$. This is a contradiction. □

For each $i = 1, 2, 3$, we denote by D_i and $D_{\overline{i}}$ the decomposition group of $\mathfrak{p}_i$ and $\overline{\mathfrak{p}_i}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Similarly, let us denote by I_i and $I_{\overline{i}}$ the inertia group of $\mathfrak{p}_i$ and $\overline{\mathfrak{p}_i}$ in $\mathrm{Gal}(\widetilde{k}/k)$, respectively. Then we have a lemma similar to Lemma 3.1.2:

Lemma 4.1.3. *With the notation and assumption in the above, the restriction* $\sigma|_k \in \mathrm{Hom}(k, F)$ *of* σ *to* k *acts on* $\mathrm{Gal}(\widetilde{k}/k)$ *and* $X(\widetilde{k})$ *via inner automorphism. Moreover,*

$$\begin{aligned} &\sigma|_k(D_1) = D_{\overline{2}}, \quad (\sigma|_k)^2(D_1) = D_3, \\ (\sigma|_k)^3(D_1) = D_{\overline{1}}, \quad &(\sigma|_k)^4(D_1) = D_2, \quad (\sigma|_k)^5(D_1) = D_{\overline{3}}. \end{aligned}$$

Proof. Note that $\mathrm{Gal}(\widetilde{F}/F)$ is equipped with the action of σ. Let $D_{\mathfrak{P}_i}$, $D_{\overline{\mathfrak{P}_i}}$ be the decomposition groups in $\mathrm{Gal}(\widetilde{F}/F)$ of $\mathfrak{P}_i$, $\overline{\mathfrak{P}_i}$, respectively ($i = 1, 2, 3$). Then, by the definition of these prime ideals (4.1), we have

$$\sigma(D_{\mathfrak{P}_1}) = D_{\overline{\mathfrak{P}_2}}, \quad \sigma^2(D_{\mathfrak{P}_1}) = D_{\mathfrak{P}_3},$$
$$\sigma^3(D_{\mathfrak{P}_1}) = D_{\overline{\mathfrak{P}_1}}, \quad \sigma^4(D_{\mathfrak{P}_1}) = D_{\mathfrak{P}_2}, \quad \sigma^5(D_{\mathfrak{P}_1}) = D_{\overline{\mathfrak{P}_3}}.$$

Since p splits completely in $F/\mathbb{Q}$, all of the canonical projections $\pi_{\mathfrak{P}_i} \colon D_{\mathfrak{P}_i} \to D_i$, $\pi_{\overline{\mathfrak{P}_i}} \colon D_{\overline{\mathfrak{P}_i}} \to D_{\overline{i}}$ ($i = 1, 2, 3$) are the isomorphisms. So,

$$\sigma|_k(D_1) = D_{\overline{2}},$$

etc. are induced. Indeed, for example, the map $\sigma|_k \colon D_1 \to D_{\overline{2}}$ is actually written as $\sigma|_k = \pi_{\overline{\mathfrak{P}_2}} \circ \sigma \circ \pi_{\mathfrak{P}_1}$. We remark that any two of these maps are the same on the intersection of each domain of definition. So, since $\mathrm{Gal}(\widetilde{k}/k) = \langle D_1, D_2, D_3, D_{\overline{1}}, D_{\overline{2}}, D_{\overline{3}} \rangle$ by the condition $A(k) = D(k)$, σ acts on $\mathrm{Gal}(\widetilde{k}/k)$. Via the canonical isomorphism $\mathrm{Gal}(F_{\mathrm{cyc}}/F) \simeq \mathrm{Gal}(k_{\mathrm{cyc}}/k)$, we see that $\sigma|_k$ acts on $\mathrm{Gal}(k_{\mathrm{cyc}}/k)$ and the action is trivial. Hence $\sigma|_k$ also acts on $X(k_{\mathrm{cyc}}) = \mathrm{Ker}(\mathrm{Gal}(\widetilde{k}/k) \to \mathrm{Gal}(k_{\mathrm{cyc}}/k))$. This completes the proof. □

Now, we obtain a similar result as Lemmas 3.1.3 and 3.2.1:

Lemma 4.1.4. *Let $\gamma \in \mathrm{Gal}(\widetilde{k}/k)$ be a topological generator of I_1. Then there are some $x, y, z \in X(k_{\mathrm{cyc}})$ and $a, b, c \in \mathbb{Z}_p$ such that*

$$\begin{cases} \mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y, z \rangle, & X(k_{\mathrm{cyc}}) = \langle x, y, z \rangle, \\ D_1 = \langle \gamma \rangle \times \langle x \rangle, & D_{\overline{1}} = \langle \gamma x^{a-b-c} y^{a+b-c} z^{a+b+c} \rangle \times \langle x^{-1} \rangle, \\ D_2 = \langle \gamma x^{-b-c} y^{a-c} z^{a+b} \rangle \times \langle y^{-1} \rangle, & D_{\overline{2}} = \langle \gamma x^a y^b z^c \rangle \times \langle y \rangle, \\ D_3 = \langle \gamma x^{a-c} y^{a+b} z^{b+c} \rangle \times \langle z \rangle, & D_{\overline{3}} = \langle \gamma x^{-b} y^{-c} z^a \rangle \times \langle z^{-1} \rangle, \end{cases}$$

Here, the left side of each direct product is the inertia group of the corresponding prime ideal.

Proof. The lemma follows in the same way as in the proof of Lemma 3.1.3. Take $\sigma|_k$ as in Lemma 4.1.3. We also take $x \in X(k_{\mathrm{cyc}})$ which satisfies $D_1 = \langle \gamma \rangle \times \langle x \rangle$ and put $y := \sigma|_k(x)$, $z := (\sigma|_k)^2(x)$. Note that $y, z \in X(k_{\mathrm{cyc}})$ by Lemma 4.1.3 and that $(\sigma|_k)^3$ is the complex conjugation, so that $(\sigma|_k)^3$ acts on $X(k_{\mathrm{cyc}}) = X(k_{\mathrm{cyc}})^-$ as -1. Applying $\sigma|_k$ on each D_1 and I_1 repeatedly, we obtain

$$D_{\overline{2}} = \langle \sigma|_k(\gamma) \rangle \times \langle y \rangle, \qquad D_3 = \langle (\sigma|_k)^2(\gamma) \rangle \times \langle z \rangle,$$
$$D_{\overline{1}} = \langle (\sigma|_k)^3(\gamma) \rangle \times \langle x^{-1} \rangle, \quad D_2 = \langle (\sigma|_k)^4(\gamma) \rangle \times \langle y^{-1} \rangle, \quad D_{\overline{3}} = \langle (\sigma|_k)^5(\gamma) \rangle \times \langle z^{-1} \rangle,$$

again by Lemma 4.1.3. Here, the left side of each direct product is the inertia group of the corresponding prime ideal. By the assumption that $X(k_{\mathrm{cyc}})^+$ is trivial, so is $X'(k_{\mathrm{cyc}})^+$. Therefore, by Corollary 2.3.2, we have $X'(k_{\mathrm{cyc}}) \simeq \left(X(k_{\mathrm{cyc}})/X(k_{\mathrm{cyc}})^{\mathrm{Gal}(k_{\mathrm{cyc}}/k)}\right)^-$. Combining this with the assumption that $X(k_{\mathrm{cyc}})$ satisfies the condition (iv) in Proposition 2.4.1, we obtain the triviality of $X'(k_{\mathrm{cyc}})$. This means that

$$X(k_{\mathrm{cyc}}) = \langle D_1 \cap X(k_{\mathrm{cyc}}),\ \ldots,\ D_{\overline{3}} \cap X(k_{\mathrm{cyc}})\rangle = \langle x, y, z\rangle.$$

Since we know that $\sigma|_k$ acts on $\mathrm{Gal}(k_{\mathrm{cyc}}/k)$ trivially, we get $\sigma|_k(\gamma) \equiv \gamma \bmod X(k_{\mathrm{cyc}})$. So there are some $a, b, c \in \mathbb{Z}_p$ such that

$$\sigma|_k(\gamma) = \gamma x^a y^b z^c.$$

Combining (4.1) with this, we obtain the representation of the decomposition groups. Finally, since $A(k) = D(k)$, $\mathrm{Gal}(\widetilde{k}/k)$ is generated by the six decomposition groups. This yields $\mathrm{Gal}(\widetilde{k}/k) = \langle \gamma, x, y, z\rangle$. □

The following is a paraphrase of (iv) in the main theorem using slightly different language, which follows directly from $\langle D_1, D_2\rangle = \langle \gamma, x, y, z^{a+b}\rangle$.

Corollary 4.1.5. *There is no non-trivial p-extension of k which is completely decomposed at any prime ideal in $\{\mathfrak{p}_1, \mathfrak{p}_2\}$ and unramified outside $\{\mathfrak{p}_3, \overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}, \overline{\mathfrak{p}_3}\}$ if and only if the condition $a + b \not\equiv 0$ mod p holds.*

Now, for matrices A and B, we denote $A \sim B$ if A and B are similar. We give some properties of a, b, c:

Corollary 4.1.6. *Define*

$$|A| := (a - b + c)\left((a^2 + bc) + (b^2 - ac) + (c^2 + ab)\right).$$

($|A|$ is actually the determinant of a certain matrix.) According to the number of generators of $A(k)$, the parameters a, b and c satisfy the following congruences modulo p:

(i) $A(k) = 0 \iff |A| \not\equiv 0.$

(ii) $A(k)$ *is cyclic* $\iff |A| \equiv 0$ *and* $\begin{cases} a^2 + bc \not\equiv 0 \ \textit{or} \\ b^2 - ac \not\equiv 0 \ \textit{or} \\ c^2 + ab \not\equiv 0. \end{cases}$

(iii) $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2 \iff \begin{cases} a^2 + bc \equiv b^2 - ac \equiv c^2 + ab \equiv 0 \ \textit{and} \\ \textit{one of } a, b, c \textit{ is not congruent to } 0. \end{cases}$

Proof. By Lemma 4.1.4, we have

$$A(k) \simeq \langle \gamma, x, y, z\rangle / \langle I_1, \dots, I_{\overline{3}}\rangle = \langle \gamma, x, y, z\rangle / \langle \gamma, x^a y^b z^c, x^{-c} y^a z^b, x^{-b} y^{-c} z^a\rangle.$$

Hence, we have a presentation of $A(k)$ whose presentation matrix is given by

$$A' := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & c \\ 0 & -c & a & b \\ 0 & -b & -c & a \end{bmatrix}.$$

In other words, there is a linear map $\langle \gamma, x, y, z\rangle \to \langle \gamma, x, y, z\rangle$ whose cokernel is $A(k)$ and whose representation matrix is A'. So, it suffices to consider the rank of $\overline{A'} := A'$ mod p:

$$\left\{ \begin{array}{ccc} A(k) = 0 & \iff & \text{rank } \overline{A'} = 3 \\ A(k) \text{ is cyclic} & \iff & \text{rank } \overline{A'} = 2 \\ \dim_{\mathbb{F}_p} A(k)/pA(k) = 2 & \iff & \text{rank } \overline{A'} = 1. \end{array} \right.$$

Put $A := \begin{bmatrix} a & b & c \\ -c & a & b \\ -b & -c & a \end{bmatrix}$. Then the determinant of A coincides with $|A|$. The lemma follows from this. □

Lemma 4.1.7. $(a^2 + bc) + (c^2 + ab) \neq 0$ *and* $(b^2 - ac) + (c^2 + ab) \neq 0$.

Proof. Define $K \leftrightarrow \langle I_1, I_{\overline{1}}, I_2, I_{\overline{2}}\rangle$. Then K/k is an abelian p-extension unramified outside $\{\mathfrak{p}_3, \overline{\mathfrak{p}_3}\}$. By [7, Lemmas 2(2) and 3], we see that $\text{rank}_{\mathbb{Z}_p}\text{Gal}(K/k) = 1$ and that $\overline{\mathfrak{p}_2}$ splits finitely in K/k. Hence $\langle I_1, I_{\overline{1}}, I_2, D_{\overline{2}}\rangle = \langle \gamma, y, x^a z^c, x^{-b-c} z^{a+b}\rangle$ is a subgroup of $\langle \gamma, x, y, z\rangle$ with finite index. This means that

$$\det \begin{bmatrix} a & c \\ -b-c & a+b \end{bmatrix} = (a^2 + bc) + (c^2 + ab) \neq 0.$$

In the same way, considering $\langle I_1, D_{\overline{1}}, I_2, I_{\overline{2}}\rangle = \langle \gamma, x, y^b z^c, y^{a-c} z^{a+b}\rangle$, we obtain $(b^2 - ac) + (c^2 + ab) \neq 0$. □

We put $G := \text{Gal}(L(k_{\text{cyc}})/k)$ and compute $\mathcal{K}(G)$.

Lemma 4.1.8. *Define*

$$|K| := (a + b + c)^3 + (a + b - c)^3 = 2(a + b)\left((a + b)^2 + 3c^2\right).$$

($|K|$ is actually the determinant of a certain matrix.) Set $G := \text{Gal}(L(k_{\text{cyc}})/k)$ *and let* $\mathcal{K}(G)$ *be the module defined in Proposition* 2.2.1. *Then* $\mathcal{K}(G) = 0$ *if and only if* $|K| \not\equiv 0$ mod p.

Proof. Let F be a free pro-p group generated by γ, x, y, and z, and R be the closed normal subgroup of F generated by $[\gamma, x]$, $[\gamma, y]$, $[\gamma, z]$, $[x, y]$, $[y, z]$, $[z, x]$ and their conjugates. Then we have a minimal representation $1 \to R \to F \to \mathrm{Gal}(L(k_{\mathrm{cyc}})/k) \to 1$ of $\mathrm{Gal}(L(k_{\mathrm{cyc}})/k)$ by Lemma 4.1.4 and

$$\begin{aligned} H_2(\mathrm{Gal}(L(k_{\mathrm{cyc}})/k), \mathbb{Z}_p) &\simeq R \cap [F, F]/[R, F] \\ &= \langle [\gamma, x], [\gamma, y], [\gamma, z], [x, y], [y, z], [z, x] \rangle [R, F]/[R, F] \end{aligned}$$

by (2.3). In the same way, we see that each image of $H_2(D_i, \mathbb{Z}_p)$, $H_2(D_{\bar{i}}, \mathbb{Z}_p)$ $(i = 1, 2, 3)$ by the map (2.4) is generated by

$$\begin{array}{lll} [\gamma, x], & [\gamma x^{-b-c} z^{a+b}, y^{-1}], & [\gamma x^{a-c} y^{a+b}, z], \\ {[\gamma y^{a+b-c} z^{a+b+c}, x^{-1}]}, & [\gamma x^{a} z^{c}, y], & [\gamma x^{-b} y^{-c}, z^{-1}], \end{array}$$

respectively. In modulo $[R, F]$, we have

$$\begin{aligned} &[\gamma x^{-b-c} z^{a+b}, y^{-1}] \equiv [\gamma, y]^{-1} [x, y]^{b+c} [y, z]^{a+b}, \\ &[\gamma x^{a-c} y^{a+b}, z] \equiv [\gamma, z] [y, z]^{a+b} [z, x]^{c-a}, \\ &[\gamma y^{a+b-c} z^{a+b+c}, x^{-1}] \equiv [\gamma, x]^{-1} [x, y]^{a+b-c} [z, x]^{-a-b-c}, \\ &[\gamma x^{a} z^{c}, y] \equiv [\gamma, y] [x, y]^{a} [y, z]^{-c}, \\ &[\gamma x^{-b} y^{-c}, z^{-1}] \equiv [\gamma, z]^{-1} [y, z]^{c} [z, x]^{-b}. \end{aligned}$$

Fixing the basis $\{[\gamma, x], [\gamma, y], [\gamma, z], [x, y], [y, z], [z, x]\}$ of $\mathbb{Z}_p$-module $R \cap [F, F]/[R, F]$, we obtain a presentation of $\mathcal{K}(G)$ whose presentation matrix is given by

$$\begin{aligned} K' &:= \left[\begin{array}{ccc|ccc} 1 & & & 0 & 0 & 0 \\ & 1 & & a & -c & 0 \\ & & 1 & 0 & a+b & c-a \\ \hline -1 & & & a+b-c & 0 & -a-b-c \\ & -1 & & b+c & a+b & 0 \\ & & -1 & 0 & c & -b \end{array} \right] \\ &\sim \left[\begin{array}{ccc|ccc} 1 & & & 0 & 0 & 0 \\ & 1 & & a & -c & 0 \\ & & 1 & 0 & a+b & c-a \\ \hline & & & a+b-c & 0 & -a-b-c \\ & & & a+b+c & a+b-c & 0 \\ & & & 0 & a+b+c & -a-b+c \end{array} \right], \end{aligned}$$

where blank entries are all zeros. So, $\mathcal{K}(G) = 0$ if and only if

$$-\det \begin{bmatrix} a+b-c & 0 & -a-b-c \\ a+b+c & a+b-c & 0 \\ 0 & a+b+c & -a-b+c \end{bmatrix} = (a+b+c)^3 + (a+b-c)^3 \not\equiv 0 \mod p.$$

This completes the proof. □

Remark 4.1.9. The correspondence with [26]: The special case of this article — where $p = 3$ and k is a totally imaginary extension of degree 6 — is treated in [26]. Here, we give the correspondence of notations in Table 2.

[26]	this article
δ, ε, ε^{δ}, ε^{δ^2}	σ^2, x, z, y^{-1}
j_1 and j_2	$a+b+c$ and $-a-b+c$
$J(\delta)$	$(a-b-c)+(a+b+c)\delta+(-a-b+c)\delta^2$
$A(\delta)$	$(a-c)+(b+c)\sigma^2+(-a-b)(\sigma^2)^2$
$\alpha = j_1 - j_2$ and $\alpha \equiv 0 \bmod 3$	$2(a+b)$ and $a+b \equiv 0 \bmod 3$

Table 2:

Hereinafter, the notation $\equiv$ is used for a congruence modulo p.

4.2 Proof in the case $\dim_{\mathbb{F}_p} A(k)/pA(k) \le 1$ and $a+b \not\equiv 0$

Suppose that $\dim_{\mathbb{F}_p} A(k)/pA(k) \le 1$ and $a+b \not\equiv 0$. Recall Corollary 4.1.5. In this subsection, we show the following proposition. The idea is based on Minardi [18], Itoh [12], and Fujii [7].

Proposition 4.2.1. *Let k be a CM-field of degree 6. Suppose that k satisfies the conditions* (I)(II)(III) *in the last expression of* §2.4. *If $\dim_{\mathbb{F}_p} A(k)/pA(k) \le 1$ and $a+b \not\equiv 0 \bmod p$, then $X(\widetilde{k})$ is trivial.*

Put

$$e := \operatorname{ord}_p(a-b+c), \quad f := \operatorname{ord}_p\left((a^2+bc)+(b^2-ac)+(c^2+ab)\right).$$

Then the order of $A(k)$ is p^{e+f} by the proof of Lemma 4.1.6. In particular, $A(k)=0$ if and only if $e=f=0$. In the following two cases, we easily obtain the triviality of $X(\widetilde{k})$ by central class field theory (Proposition 2.2.1):

Lemma 4.2.2.

(i) *If $e \neq 0$ then $X(\widetilde{k})$ is trivial.*

(ii) *Suppose that $e = 0$. If $(a^2+bc)+(c^2+ab) \equiv (b^2-ac)+(c^2+ab) \equiv 0$, then $X(\widetilde{k})$ is trivial.*

Proof. (i) By Proposition 2.2.1 and Lemma 4.1.8, we only need to show that $|K| = 2(a+b)\left((a+b)^2+3c^2\right) \not\equiv 0$. Substituting $c \equiv b-a$ in $|K|$, we obtain $|K| \equiv 8(a+b)(a-ab+b^2)$. On the other hand, all of a^2+bc, b^2-ac and c^2+ab are congruent to $a-ab+b^2$ mod p.

Hence $a - ab + b^2 \not\equiv 0$ by Lemma 4.1.6, so $|K| \not\equiv 0$.
(ii) Similar to (i), we only need to show $|K| \not\equiv 0$. If $c \equiv 0$, then $|K| \equiv 2(a+b)^3 \not\equiv 0$, since $a+b \not\equiv 0$. Suppose that $c \not\equiv 0$, then substituting $a^2 \equiv -bc-(c^2+ab)$ and $b^2 \equiv ac-(c^2+ab)$ in $|K|$, we obtain $|K| \equiv 2(a+b)c(a-b+c)$. Since $a-b+c \not\equiv 0$ and $a+b \not\equiv 0$, we obtain $|K| \not\equiv 0$ in the case $c \equiv 0$. This completes the proof. □

By the above lemma, we may assume that

$$\begin{cases} e = 0 \ \text{ i.e., } \ a - b + c \not\equiv 0, \\ (a^2+bc)+(c^2+ab) \not\equiv 0 \ \text{ or } \ (b^2-ac)+(c^2+ab) \not\equiv 0. \end{cases} \tag{4.2}$$

Define $k^{(i)}$ $(i = 1, 2, 3)$ by

$$\begin{cases} k^{(1)} \leftrightarrow \langle \gamma, xy, xz^{-1} \rangle, \\ k^{(2)} \leftrightarrow \langle I_2, I_3 \rangle = \langle \gamma x^{a-c} y^{a+b} z^{b+c}, x^{a+b} y^{b+c} z^{c-a} \rangle, \\ k^{(3)} \leftrightarrow I_3 \text{ or } I_2, \text{ which will be defined in §4.2.2.} \end{cases}$$

Let us denote the complex conjugate of $k^{(1)}$ and $k^{(2)}$ by $\overline{k^{(1)}}$ and $\overline{k^{(2)}}$, respectively. In fact, if $A(k) = 0$ i.e., if $e = f = 0$, then $k^{(1)} \leftrightarrow \langle I_1, I_2, I_3 \rangle$ (see Lemma 4.2.3(i) below). Our plan is to show successively the triviality of $X(k^{(2)})$, $X(k^{(3)})$, and $X(\widetilde{k})$.

4.2.1 The triviality of $X(k^{(2)})$

Define

$$L_0 \leftrightarrow \langle I_1, I_2, I_3 \rangle = \langle \gamma, x^{-b-c} y^{a-c} z^{a+b}, x^{a-c} y^{a+b} z^{b+c} \rangle,$$

and we begin to give some properties of $k^{(1)}$ and L_0.

Lemma 4.2.3.

(i) $k^{(1)} \subset L_0$ *and* $[L_0 : k^{(1)}] = p^f$.
(ii) *In* $k^{(1)}/k$, $\mathfrak{p}_i$ $(i = 1, 2, 3)$ *are totally inert and* $\overline{\mathfrak{p}_i}$ $(i = 1, 2, 3)$ *are totally ramified.*
(iii) $L_0 = L(k^{(1)}) \cap k^{(2)}$. *Moreover,* L_0 *is the maximal abelian subextension in* $L(k^{(1)})/k$.

Proof. (i) We have

$$x^{-b-c} y^{a-c} z^{a+b} = (xy)^{a-c} (xz^{-1})^{-a-b} \quad \text{and} \quad x^{a-c} y^{a+b} z^{b+c} = (xy)^{a+b} (xz^{-1})^{-b-c}.$$

This implies that $\langle I_1, I_2, I_3 \rangle \subset \langle \gamma, xy, xz^{-1} \rangle$. Also, its quotient is generated by the class of xy, since we see $xz^{-1} \in \langle I_1, I_2, I_3 \rangle$ by $(xz^{-1})^{a+b} = (xy)^{a-c} (x^{-b-c} y^{a-c} z^{a+b})^{-1}$ and $a + b \in \mathbb{Z}_p^\times$. The equation

$$(x^{a-c} y^{a+b} z^{b+c})^{a+b} = (xy)^{(a^2+bc)+(b^2-ac)+(c^2+ab)} (x^{-b-c} y^{a-c} z^{a+b})^{b+c}$$

yields that the index is p^f.
(ii) The claim follows from

$$\langle \gamma, xy, xz^{-1}, D_i \rangle = \langle \gamma, xy, xz^{-1}, D_{\bar{i}} \rangle = \langle \gamma, x, y, z \rangle,$$
$$\langle \gamma, xy, xz^{-1}, I_{\bar{i}} \rangle = \langle \gamma, x^{a-b+c}, xy, xz^{-1} \rangle$$

for $i = 1, 2, 3$ since we assume $a - b + c \in \mathbb{Z}_p^{\times}$.
(iii) Since $\widetilde{k}$ coincides with the maximal abelian p-extension of k unramified outside p, L_0 is the maximal abelian p-extension of k unramified outside $\{\overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}, \overline{\mathfrak{p}_3}\}$. Combining (ii) with this, $L_0/k^{(1)}$ is unramified abelian, so $L_0 \subset L(k^{(1)})$. Also, by the Galois correspondence, we have $L_0 \subset k^{(2)}$. Therefore we obtain

$$k^{(1)} \subset L_0 \subset L(k^{(1)}) \cap k^{(2)} \subset k^{(2)}.$$

By the definitions of $k^{(2)}$ and L_0, $\mathfrak{p}_1$ is totally ramified in $k^{(2)}/L_0$, which implies that $L_0 = L(k^{(1)}) \cap k^{(2)}$. On the other hand, let L_0' be the maximal abelian subextension in $L(k^{(1)})/k$. Then L_0' is unramified over $k^{(1)}$ and unramified outside $\{\mathfrak{p}_3, \overline{\mathfrak{p}_1}, \overline{\mathfrak{p}_2}, \overline{\mathfrak{p}_3}\}$ over k, so we have $L_0' \subset L(k^{(1)}) \cap k^{(2)}$. Conversely, L_0 is unramified over $k^{(1)}$ and abelian over k, so $L_0 \subset L_0'$. This completes the proof. □

Remark 4.2.4. At this point, we obtain the triviality of $X(k^{(2)})$ if $A(k) = 0$, although we do not need this fact. Indeed, since $k^{(1)} \leftrightarrow \langle I_1, I_2, I_3 \rangle$ in this case, we can apply the argument of Step 1 in [7], which implies that $X(k^{(1)})$ is trivial. By Lemma 4.2.3(ii), the prime in $k^{(1)}$ above $\mathfrak{p}_1$ is only one and it is totally ramified in $k^{(2)}/k^{(1)}$. Other primes, $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\overline{\mathfrak{p}_i}$ ($i = 1, 2, 3$), are unramified in $k^{(2)}/k^{(1)}$. Therefore $X(k^{(2)})$ is trivial.

In a similar way as in §3.1.3, we show the following.

Lemma 4.2.5. *$L_0 = L(k^{(1)})$, i.e., $L(k^{(1)})$ is abelian over k.*

Proof. We show that $\mathrm{Gal}(L(k^{(1)})/L_0)$ is trivial (then by Lemma 4.2.3(iii), $L(k^{(1)})$ is abelian over k). Note that $L(k^{(1)})/L_0$ is unramified and that each of $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ is totally ramified in $k^{(2)}/L_0$, $k^{(3)}/k^{(2)}$, and $\widetilde{k}/k^{(3)}$, respectively. From this, we obtain an unramified extension $L(k^{(1)})\widetilde{k}/\widetilde{k}$ and

$$\mathrm{Gal}(L(k^{(1)})/L_0) \simeq Y := \mathrm{Gal}\left(L(k^{(1)})\widetilde{k}/\widetilde{k}\right). \tag{4.3}$$

We have that $L(k^{(1)})\widetilde{k}/k^{(1)}$ is abelian. Also, we see that $L(k^{(1)})\widetilde{k}/k$ is Galois, since both $L(k^{(1)})/k$ and $\widetilde{k}/k$ are Galois. Therefore $\mathrm{Gal}(\widetilde{k}/k)$, and so $\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})$, act on Y (see Lemma 2.1.2). Then, we define an unramified abelian p-extension M_1 in $L(k^{(1)})\widetilde{k}/\widetilde{k}$ by $\mathrm{Gal}(M_1/\widetilde{k}) \simeq Y_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$. In the same way, we also define an unramified abelian p-extension $\overline{M_1}$ in $L(\overline{k^{(1)}})\widetilde{k}/\widetilde{k}$ by $\mathrm{Gal}(\overline{M_1}/\widetilde{k}) \simeq \mathrm{Gal}\left(L(\overline{k^{(1)}})\widetilde{k}/\widetilde{k}\right)_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$. Note that $\overline{M_1}$ is the complex conjugate of M_1. Moreover, in a similar way as in the above, we see that $L(\overline{k^{(1)}})$ is abelian over k (Figure 3).

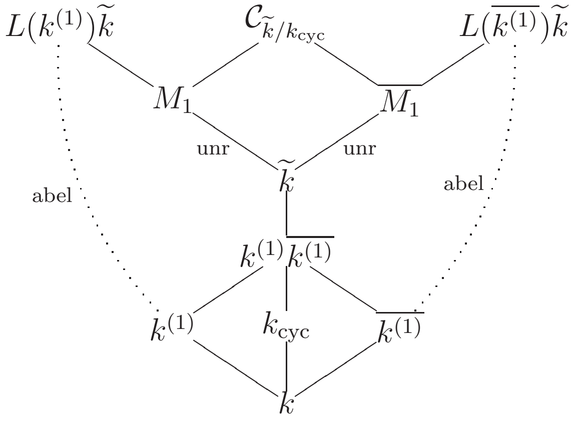

$L(k^{(1)})\widetilde{k}$
$\mathcal{C}_{\widetilde{k}/k_{\mathrm{cyc}}}$
$L(\overline{k^{(1)}})\widetilde{k}$
M_1
$\overline{M_1}$
unr
unr
$\widetilde{k}$
abel
abel
$k^{(1)}\overline{k^{(1)}}$
$k^{(1)}$
k_{cyc}
$\overline{k^{(1)}}$
k

Figure 3:

Let us denote by $\mathcal{C}_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$ the subfield in $L(\widetilde{k})/\widetilde{k}$ such that $\mathrm{Gal}(\mathcal{C}_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}/\widetilde{k}) \simeq X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$. Apply Lemma 2.1.5 as $F = k^+$, $K = \widetilde{k}$, $H = \mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})$ (so $L = \mathcal{C}_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$). We see that $\mathcal{C}_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$ is a Galois extension of k^+. Hence, in particular, complex conjugation $J \in \mathrm{Gal}(k/k^+) \simeq \mathrm{Gal}(k_{\mathrm{cyc}}/k^+_{\mathrm{cyc}})$ naturally acts on $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$.

Consider the exact sequence

$$1 \to X(\widetilde{k}) \to \mathrm{Gal}(L(\widetilde{k})/k_{\mathrm{cyc}}) \to \mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}}) \to 1.$$

Taking its Hochschild-Serre spectral sequence, we obtain the following exact sequence of $\mathrm{Gal}(k/k^+)$-modules:

$$H_2(\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}}), \mathbb{Z}_p) \to X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})} \to \mathrm{Gal}(L(\widetilde{k})/k_{\mathrm{cyc}})^{\mathrm{ab}} \to \mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}}) \to 0,$$

where $\mathrm{Gal}(L(\widetilde{k})/k_{\mathrm{cyc}})^{\mathrm{ab}}$ is the maximal abelian quotient of $\mathrm{Gal}(L(\widetilde{k})/k_{\mathrm{cyc}})$. In our condition, the maximal abelian subextension in $L(\widetilde{k})/k_{\mathrm{cyc}}$ is $L(k_{\mathrm{cyc}}) = \widetilde{k}$, so we have the isomorphism $\mathrm{Gal}(L(\widetilde{k})/k_{\mathrm{cyc}})^{\mathrm{ab}} \simeq X(k_{\mathrm{cyc}}) = \mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})$. Also, there is an isomorphism $H_2(\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}}), \mathbb{Z}_p) \simeq X(k_{\mathrm{cyc}}) \wedge_{\mathbb{Z}_p} X(k_{\mathrm{cyc}})$ of $\mathrm{Gal}(k/k^+)$-modules, where $\mathrm{Gal}(k/k^+)$ acts on $X(k_{\mathrm{cyc}}) \wedge_{\mathbb{Z}_p} X(k_{\mathrm{cyc}})$ diagonally. Combining these two isomorphisms with the above exact sequence, we have the surjection

$$X(k_{\mathrm{cyc}}) \wedge_{\mathbb{Z}_p} X(k_{\mathrm{cyc}}) \twoheadrightarrow X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$$

of $\mathrm{Gal}(k/k^+)$-modules. Since $X(k_{\mathrm{cyc}}) = X(k_{\mathrm{cyc}})^-$, $\mathrm{Gal}(k/k^+)$ acts on the left hand side, and hence on the right hand side, trivially. Therefore, $\mathrm{Gal}(k/k^+)$ also acts trivially on the quotient $\mathrm{Gal}(M_1/\widetilde{k})$ of $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$. This yields that

$$M_1 = \overline{M_1}.$$

Since $M_1/k^{(1)}$ is abelian, $\mathrm{Gal}(k^{(1)}\overline{k^{(1)}}/k^{(1)})$ acts on $\mathrm{Gal}(M_1/k^{(1)}\overline{k^{(1)}})$ trivially by Lemma 2.1.2. Similarly, $\mathrm{Gal}(k^{(1)}\overline{k^{(1)}}/\overline{k^{(1)}})$ acts on $\mathrm{Gal}(\overline{M_1}/k^{(1)}\overline{k^{(1)}})$ trivially. Consequently, combining these facts with $M_1 = \overline{M_1}$, we see that $\mathrm{Gal}(k^{(1)}\overline{k^{(1)}}/k^{(1)}\cap\overline{k^{(1)}})$ acts on $\mathrm{Gal}(M_1/k^{(1)}\overline{k^{(1)}})$ trivially. Now, we use the assumption that $a - b + c \not\equiv 0$, and then we can check $k^{(1)} \cap \overline{k^{(1)}} = k$. Therefore, we obtain that $k \subset k_{\mathrm{cyc}} \subset k^{(1)}\overline{k^{(1)}}$ and that $\mathrm{Gal}(k^{(1)}\overline{k^{(1)}}/k_{\mathrm{cyc}})$ acts on $\mathrm{Gal}(M_1/k^{(1)}\overline{k^{(1)}})$ trivially. Again by Lemma 2.1.2, this implies that M_1/k_{cyc} is abelian. Since M_1/k_{cyc} is unramified, M_1 must be contained in $L(k_{\mathrm{cyc}}) = \widetilde{k}$, which yields that $Y_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$ is trivial. By Nakayama's lemma, Y is also trivial and so is $\mathrm{Gal}(L(k^{(1)})/L_0)$ by (4.3). This completes the proof. □

Corollary 4.2.6. *The module $X(k^{(2)})$ is trivial.*

Proof. Let L_1 denote the maximal abelian subextension in $L(k^{(2)})/k^{(1)}$. There is only one prime in $k^{(1)}$ above $\mathfrak{p}_3$ by Lemma 4.2.3(ii). Hence

$$X(k^{(2)})_{\mathrm{Gal}(k^{(2)}/k^{(1)})} \simeq \mathrm{Gal}(L_1/k^{(1)}) \simeq \mathrm{Gal}(L(k^{(1)})/L(k^{(1)}) \cap k^{(2)}).$$

By Lemmas 4.2.3(iii) and 4.2.5, we get $L(k^{(1)}) \cap k^{(2)} = L_0 = L(k^{(1)})$. This means that $X(k^{(2)})_{\mathrm{Gal}(k^{(2)}/k^{(1)})}$ is trivial, and so is $X(k^{(2)})$ by Nakayama's lemma. □

4.2.2 The triviality of $X(k^{(3)})$

Now, according to (4.2), we define a $\mathbb{Z}_p$-extension $N^{(1)}$ of k and its complex conjugate $\overline{N^{(1)}}$ as follows. If $(b^2 - ac) + (c^2 + ab) \not\equiv 0$, then

$$\begin{cases} N^{(1)} \leftrightarrow \langle D_2, I_3 \rangle = \langle \gamma x^{a-c} z^{b+c}, y, x^{a+b} z^{c-a} \rangle, \\ \overline{N^{(1)}} \leftrightarrow \langle D_{\overline{2}}, I_{\overline{3}} \rangle = \langle \gamma x^{a} z^{c}, y, x^{a+b} z^{c-a} \rangle. \end{cases}$$

In this case, we see that $N^{(1)} \cap \overline{N^{(1)}} \leftrightarrow \langle \gamma x^a z^c, y, x^{-c} z^b, x^{a+b} z^{c-a} \rangle = \langle \gamma, x, y, z \rangle$. On the other hand, if $(b^2 - ac) + (c^2 + ab) \equiv 0$, which implies $(a^2 + bc) + (c^2 + ab) \not\equiv 0$, then

$$\begin{cases} N^{(1)} \leftrightarrow \langle I_2, D_3 \rangle = \langle \gamma x^{a-c} y^{a+b}, z, x^{a+b} y^{b+c} \rangle, \\ \overline{N^{(1)}} \leftrightarrow \langle I_{\overline{2}}, D_{\overline{3}} \rangle = \langle \gamma x^{a} y^{b}, z, x^{a+b} y^{b+c} \rangle. \end{cases}$$

In this case, we also obtain that $N^{(1)} \cap \overline{N^{(1)}} \leftrightarrow \langle \gamma x^a y^b, z, x^{-c} y^a, x^{a+b} y^{b+c} \rangle = \langle \gamma, x, y, z \rangle$. We may assume that the former condition holds (otherwise, replacing the role of $\mathfrak{p}_2$ and p_3 with each other, we have the same conclusion as in the following by the the latter condition). We have

$$N^{(1)}\overline{N^{(1)}} \leftrightarrow \langle y, x^{a+b} z^{c-a} \rangle, \quad N^{(1)} \cap \overline{N^{(1)}} = k, \tag{4.4}$$

and define

$$k^{(3)} \leftrightarrow I_3, \quad \overline{k^{(3)}} \leftrightarrow I_{\overline{3}}.$$

Let L_2 be the maximal subfield in $L(k^{(3)})$ that is abelian over $k^{(2)}$. Then $\mathrm{Gal}(L_2/k^{(2)})$ is isomorphic to $X(k^{(3)})_{\mathrm{Gal}(k^{(3)}/k^{(2)})}$ since $\mathrm{Gal}(k^{(3)}/k^{(2)}) \simeq \mathbb{Z}_p$. We know that $X(k^{(2)})$ is trivial and that $\mathfrak{p}_2$ is totally inert in $k^{(2)}/N^{(1)}$. Therefore, by Lemma 4.2.6, in the same way as in the proof of Lemma 3.1.11, we have the following lemma for which we omit the proof.

Lemma 4.2.7. *With the notation above, $L_2/N^{(1)}$ is abelian.*

Using a similar technique as in the proof of Lemma 4.2.5, we show the following:

Lemma 4.2.8. *The module $X(k^{(3)})$ is trivial.*

Proof. We show that $\mathrm{Gal}(L_2/k^{(3)})$ is trivial. To do this, it is sufficient to show that $L_2\widetilde{k} = \widetilde{k}$, since $\mathfrak{p}_3$ is totally ramified in $\widetilde{k}/k^{(3)}$ which implies $\mathrm{Gal}(L_2/k^{(3)}) \simeq \mathrm{Gal}(L_2\widetilde{k}/\widetilde{k})$. By Lemma 4.2.7, $L_2\widetilde{k}/N^{(1)}$ is abelian. Let $\overline{L_2}$ denote the maximal subfield in $L(\overline{k^{(3)}})$ that is abelian over $\overline{k^{(2)}}$. Then, in the same way as in Lemma 4.2.7, we see that $\overline{L_2}\widetilde{k}/\overline{N^{(1)}}$ is also abelian (Figure 4).

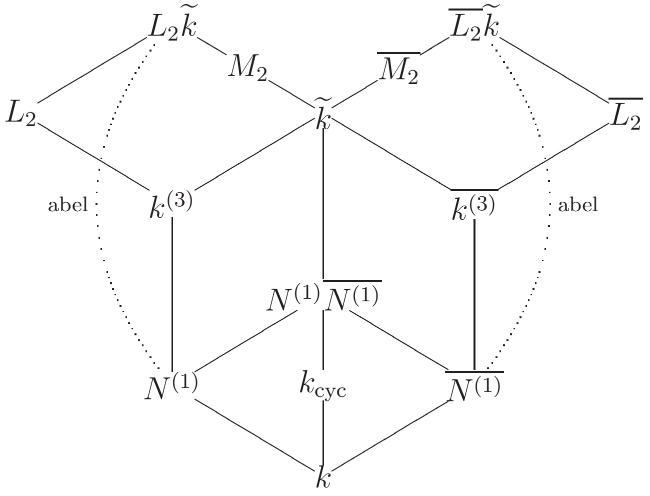


Figure 4:

Here, we use the assumption $a + b \not\equiv 0$ to obtain that

$$k \subset k_{\mathrm{cyc}} \subset N^{(1)}\overline{N^{(1)}}$$

by (4.4) and $k_{\mathrm{cyc}} \leftrightarrow \langle x, y, z \rangle$. We apply Lemma 2.1.5 as $F = k$, $K = k^{(3)}$, $H = \mathrm{Gal}(k^{(3)}/k^{(2)})$ (so $L = \mathrm{Gal}(L_2/k^{(3)})$), and then we have that L_2/k is Galois, and so is $L_2\widetilde{k}/k$. By Lemma 2.1.2, it follows that $\mathrm{Gal}(\widetilde{k}/k)$ acts on $\mathrm{Gal}(L_2\widetilde{k}/\widetilde{k})$. So, let us denote by M_2 the subfield in $L_2\widetilde{k}/\widetilde{k}$ such that $\mathrm{Gal}(M_2/\widetilde{k}) \simeq \mathrm{Gal}(L_2\widetilde{k}/\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$. The natural projection $X(\widetilde{k}) \twoheadrightarrow \mathrm{Gal}(L_2\widetilde{k}/\widetilde{k})$ induces the surjection $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})} \twoheadrightarrow \mathrm{Gal}(M_2/\widetilde{k})$. From the proof of Lemma 4.2.5, we know that $\mathrm{Gal}(k/k^+)$ acts on $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k_{\mathrm{cyc}})}$ trivially, and hence also does on $\mathrm{Gal}(M_2/\widetilde{k})$ trivially. Therefore, we obtain

$$M_2 = \overline{M_2}.$$

Since $M_2/N^{(1)}$ is abelian, $\mathrm{Gal}(N^{(1)}\overline{N^{(1)}}/N^{(1)})$ acts on $\mathrm{Gal}(M_2/N^{(1)}\overline{N^{(1)}})$ trivially by Lemma 2.1.2. Similarly, $\mathrm{Gal}(N^{(1)}\overline{N^{(1)}}/\overline{N^{(1)}})$ acts on $\mathrm{Gal}(\overline{M_2}/N^{(1)}\overline{N^{(1)}})$ trivially. In a similar way as in the proof of Lemma 4.2.5, combining these facts with $M_2 = \overline{M_2}$, we see that $\mathrm{Gal}(N^{(1)}\overline{N^{(1)}}/k_{\mathrm{cyc}})$ acts on $\mathrm{Gal}(M_2/N^{(1)}\overline{N^{(1)}})$ trivially. Again by Lemma 2.1.2, this implies that M_2/k_{cyc} is abelian. Since M_2/k_{cyc} is unramified, M_2 must be contained in $L(k_{\mathrm{cyc}}) = \widetilde{k}$, which yields that $M_2 = \widetilde{k}$. Therefore, by Nakayama's lemma, $\mathrm{Gal}(L_2\widetilde{k}/\widetilde{k})$ is trivial, and so is $\mathrm{Gal}(L_2/k^{(3)})$. Again by Nakayama's lemma, we have that $X(k^{(3)})$ is trivial, which completes the proof. □

4.2.3 The triviality of $X(\widetilde{k})$

Let $\mathcal{C} = \mathcal{C}_{\widetilde{k}/k}$ be the subfield in $L(\widetilde{k})/\widetilde{k}$ such that $\mathrm{Gal}(\mathcal{C}/\widetilde{k}) \simeq X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$. To obtain the triviality of $X(\widetilde{k})$, it is sufficient to show that of $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$. Denote by L_3 and $\overline{L_3}$ the maximal abelian subextension of $L(\widetilde{k}/k^{(3)})$ and $L(\widetilde{k}/\overline{k^{(3)}})$, respectively. Define three $\mathbb{Z}_p^2$-extensions $N^{(2)}$, $\overline{N^{(2)}}$, and N by

$$N^{(2)} \leftrightarrow D_3, \quad \overline{N^{(2)}} \leftrightarrow D_{\overline{3}}, \quad N \leftrightarrow \langle x^{a+b-c}y^{a+b+c}, z\rangle.$$

Here, note that $a+b-c \not\equiv 0$ or $a+b+c \not\equiv 0$ holds by $a+b \not\equiv 0$ and that $k_{\mathrm{cyc}} \subset N$. By Lemma 4.2.8, in the same way as in the proof of Lemma 3.1.11, we have the following lemma, for which we omit the proof.

Lemma 4.2.9. *With the notation above, $L_3/N^{(2)}$ and $\overline{L_3}/\overline{N^{(2)}}$ are abelian.*

By the above lemma we see that $\mathcal{C}/N^{(2)}$ and $\mathcal{C}/\overline{N^{(2)}}$ are also abelian and so is $\mathcal{C}/N$ by Lemma 2.1.2 (Figure 5).

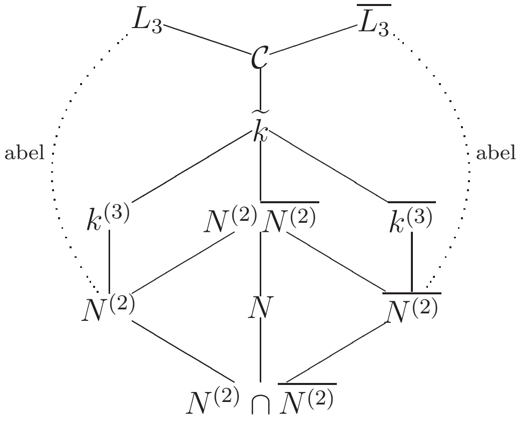


Figure 5:

Now, assume that $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ is not trivial, i.e., $\mathcal{C} \neq \widetilde{k}$. Since $\mathcal{C}/k$ is Galois, so is $\mathcal{C}/k_{\mathrm{cyc}}$. Hence, since $\mathcal{C}/N$ is abelian, we can regard $\mathrm{Gal}(\mathcal{C}/N)$ as a $\mathrm{Gal}(N/k_{\mathrm{cyc}})$-module by Lemma 2.1.2, and we can regard $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ as its $\mathrm{Gal}(N/k_{\mathrm{cyc}})$-submodule with trivial action. Since the free $\mathbb{Z}_p$-module $\mathrm{Gal}(\widetilde{k}/N) \simeq \mathbb{Z}_p^{\oplus 2}$ is projective, $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ is non-trivial and a direct summand of $\mathrm{Gal}(\mathcal{C}/N)$ as a $\mathbb{Z}_p$-module. Therefore, we can take a $\mathbb{Z}_p$-basis $\{g_1, \dots, g_m\}$ of $\mathrm{Gal}(\mathcal{C}/N)$ such that $\{g_1, \dots, g_{m-2}\}$ becomes a $\mathbb{Z}_p$-basis of $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$. Pick a topological generator of $\mathrm{Gal}(N/k_{\mathrm{cyc}})$; then the representation matrix of its action with respect to the basis is written as

$$\left[\begin{array}{ccc|cc} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ \hline * & * & * & * & * \\ * & * & * & * & * \end{array}\right],$$

where blank entries are all zeros. This implies that, by adding some liner form of $g_1, \dots, g_{m-2}$ to g_{m-1} and g_m, we can take a $\mathrm{Gal}(N/k_{\mathrm{cyc}})$-subgroup H in $\mathrm{Gal}(\mathcal{C}/N)$ such that $\mathrm{Gal}(\mathcal{C}/N) \simeq H \times X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ as a $\mathrm{Gal}(N/k_{\mathrm{cyc}})$-module. Then $\mathrm{Gal}(\mathcal{C}^H/N)$ is isomorphic to $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ as $\mathrm{Gal}(N/k_{\mathrm{cyc}})$-modules, where $\mathcal{C}^H$ is the fixed field by H. Now, let us denote by F the maximal abelian subextension in $\mathcal{C}^H/k_{\mathrm{cyc}}$. Then, since N/k_{cyc} is a $\mathbb{Z}_p$-extension, we see that $\mathrm{Gal}(F/N) \simeq \mathrm{Gal}(\mathcal{C}^H/N)_{\mathrm{Gal}(N/k_{\mathrm{cyc}})}$, which is non-trivial. This means that F is an unramified abelian p-extension which is not contained in $\widetilde{k}$. However, this contradicts our assumption that $L(k_{\mathrm{cyc}}) = \widetilde{k}$. Therefore, $X(\widetilde{k})_{\mathrm{Gal}(\widetilde{k}/k)}$ is trivial, and so is $X(\widetilde{k})$. This completes the proof of Proposition 4.2.1.

4.3 Proof in the case $\dim_{\mathbb{F}_p} A(k)/pA(k) \leq 1$ and $a + b \equiv 0$

Suppose that $\dim_{\mathbb{F}_p} A(k)/pA(k) \leq 1$ and $a + b \equiv 0$. Recall Corollary 4.1.5. In this subsection, we show the following proposition. The outline of the proof is similar to §3.1.2, although it is a little complicated.

Proposition 4.3.1. *Let k be a CM-field of degree 6. Suppose that k satisfies the conditions* (I)(II)(III) *in the last expression of* §2.4. *If $\dim_{\mathbb{F}_p} A(k)/pA(k) \leq 1$ and $a + b \equiv 0 \bmod p$, then $X(\widetilde{k})$ is not trivial.*

Remark 4.3.2. If $p = 3$ and $A(k)$ is cyclic, then the case in this subsection does not occur. Indeed, assume that $p = 3$, $A(k)$ is cyclic and $a + b \equiv 0$. Then, by Corollary 4.1.6(ii), we have

$$0 \equiv |A| \equiv (c - a)^3 \equiv c - a.$$

From this, we obtain $a^2 + bc \equiv b^2 - ac \equiv c^2 + ab \equiv 0$. This contradicts Corollary 4.1.6(ii).

First, we set $m := \mathrm{ord}_p(a+b) > 0$ and denote by $J \in \mathrm{Gal}(k/k^+)$ the complex conjugation. We remark that

$$a - c \not\equiv 0, \quad b + c \not\equiv 0.$$

Indeed, since $a+b \equiv 0$, we have $a^2+bc \equiv a(a-c)$, $b^2-ac \equiv a(a-c)$, $c^2+ab \equiv (c+a)(c-a)$. By Corollary 4.1.6(ii), we obtain $a-c \not\equiv 0$, so $b+c \not\equiv 0$. Next, to obtain the desired $\mathbb{Z}_p$-extension k_∞/k satisfying Corollary 2.3.3, we construct three cyclic p-extensions $R_m^{(i)}$ $(i = 1, 2, 3)$ of degree p^m. Define

$$P_m^{(1)} \leftrightarrow \langle D_1, D_2 \rangle = \langle \gamma, x, y, z^{a+b} \rangle, \quad Q_m^{(1)} \leftrightarrow \langle D_1, D_3 \rangle = \langle \gamma, x, y^{a+b}, z \rangle.$$

Then $P_m^{(1)} Q_m^{(1)} \leftrightarrow \langle D_1, D_2 \rangle \cap \langle D_1, D_3 \rangle = \langle \gamma, x, y^{a+b}, z^{a+b} \rangle$ and $P_m^{(1)} \cap Q_m^{(1)} = k$. Therefore $P_m^{(1)} Q_m^{(1)}/k$ is a (p^m, p^m)-extension unramified outside p.

Lemma 4.3.3. *Define $R_m^{(1)} \subset P_m^{(1)} Q_m^{(1)}$ by $R_m^{(1)} \leftrightarrow \langle \gamma, x, yz^{-1}, z^{a+b} \rangle$. Then*

(i) *$R_m^{(1)}/k$ is a cyclic p-extension of degree p^m and J acts on $\mathrm{Gal}(R_m^{(1)}/k)$ as -1.*
(ii) *In $R_m^{(1)}/k$, $\mathfrak{p}_2$, $\overline{\mathfrak{p}_2}$, $\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$ are totally ramified and $\mathfrak{p}_1$, $\overline{\mathfrak{p}_1}$ split completely.*

Proof. (i) We can easily check that $\mathrm{Gal}(R_m^{(1)}/k) = \langle \gamma, x, y, z \rangle / \langle \gamma, x, yz^{-1}, z^{a+b} \rangle \simeq \mathbb{Z}/p^m\mathbb{Z}$. We see that

$$J(\gamma) = \gamma x^{a-b-c} y^{a+b-c} z^{a+b+c} = \gamma \cdot x^{a-b-c} \cdot (yz^{-1})^{a+b-c} \cdot z^{2(a+b)} \in \langle \gamma, x, yz^{-1}, z^{a+b} \rangle.$$

From this, it follows that J acts on $\langle \gamma, x, yz^{-1}, z^{a+b} \rangle$. Since the class of z generates $\mathrm{Gal}(R_m^{(1)}/k)$, J acts on $\mathrm{Gal}(R_m^{(1)}/k)$ as -1.
(ii) Since $D_1 \subset \langle D_1, D_2 \rangle \cap \langle D_1, D_3 \rangle$, $\mathfrak{p}_1$ splits completely in $P_m^{(1)} Q_m^{(1)}/k$, especially in $R_m^{(1)}/k$. On the other hand, since we obtain $\langle \gamma, x, yz^{-1}, z^{a+b}, I_2 \rangle = \langle \gamma, x, y, z \rangle$ by $a - c \in \mathbb{Z}_p^\times$, $\mathfrak{p}_2$ is totally ramified in $R_m^{(1)}/k$. In the same way, we see that the same is true for $\mathfrak{p}_3$. Consequently, by (i), we see that $\overline{\mathfrak{p}_2}$ and $\overline{\mathfrak{p}_3}$ are totally ramified and $\overline{\mathfrak{p}_1}$ splits completely in $R_m^{(1)}/k$. □

In a similar way, we can construct cyclic p-extensions $R_m^{(2)}$, $R_m^{(3)}$ of degree p^m, and also we have their properties from $P_m^{(2)} \leftrightarrow \langle D_2, D_1 \rangle$, $Q_m^{(2)} \leftrightarrow \langle D_2, D_3 \rangle$ and $P_m^{(3)} \leftrightarrow \langle D_3, D_1 \rangle$, $Q_m^{(2)} \leftrightarrow \langle D_3, D_2 \rangle$, respectively:

$$R_m^{(2)} \leftrightarrow \langle \gamma x^{a-c}, y, xz, x^{a+b} \rangle \quad : \quad \text{In } R_m^{(2)}/k, \begin{cases} \mathfrak{p}_1, \overline{\mathfrak{p}_1}, \mathfrak{p}_3, \overline{\mathfrak{p}_3} \text{ are totally ramified,} \\ \mathfrak{p}_2, \overline{\mathfrak{p}_2} \text{ split completely,} \end{cases}$$

$$R_m^{(3)} \leftrightarrow \langle \gamma x^{a-c}, xy^{-1}, z, y^{a+b} \rangle \quad : \quad \text{In } R_m^{(3)}/k, \begin{cases} \mathfrak{p}_1, \overline{\mathfrak{p}_1}, \mathfrak{p}_2, \overline{\mathfrak{p}_2} \text{ are totally ramified,} \\ \mathfrak{p}_3, \overline{\mathfrak{p}_3} \text{ split completely.} \end{cases}$$

Now, we prove Proposition 4.3.1. Define

$$L'_m := R_m^{(2)} R_m^{(3)} \leftrightarrow \langle \gamma x^{a-c}, xy^{-1}z, x^{a+b}, y^{a+b}, z^{a+b} \rangle.$$

Then we have $R_m^{(1)} \subset L'_m$ (see Figure 6).

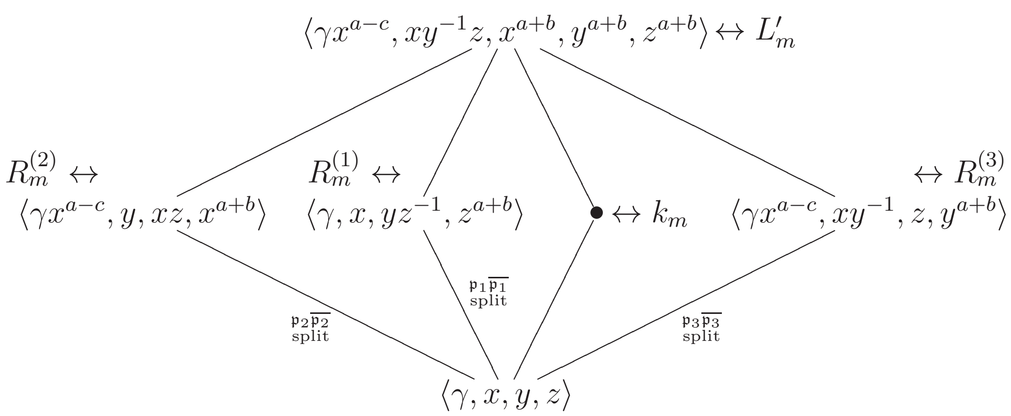

$\langle \gamma x^{a-c}, xy^{-1}z, x^{a+b}, y^{a+b}, z^{a+b} \rangle \leftrightarrow L'_m$
$R_m^{(2)} \leftrightarrow$
$\langle \gamma x^{a-c}, y, xz, x^{a+b} \rangle$
$R_m^{(1)} \leftrightarrow$
$\langle \gamma, x, yz^{-1}, z^{a+b} \rangle$
$\bullet \leftrightarrow k_m$
$\leftrightarrow R_m^{(3)}$
$\langle \gamma x^{a-c}, xy^{-1}, z, y^{a+b} \rangle$
$\mathfrak{p}_1\overline{\mathfrak{p}_1}$ split
$\mathfrak{p}_2\overline{\mathfrak{p}_2}$ split
$\mathfrak{p}_3\overline{\mathfrak{p}_3}$ split
$\langle \gamma, x, y, z \rangle$

Figure 6:

Therefore, the decomposition field of each prime ideal above p has degree p^m in L'_m/k. In $\mathrm{Gal}(L'_m/k)$, the inertia groups of $\mathfrak{p}_i$ and $\overline{\mathfrak{p}_i}$ are $\mathrm{Gal}(L'_m/R_m^{(i)})$ $(i = 1, 2, 3)$. Note that J acts on $\mathrm{Gal}(L'_m/k)$ as -1. Define the intermediate field k_m of L'_m/k by

$$k_m \leftrightarrow \langle \gamma x^{a-c}, xy^{-1}z, xy, x^{a+b}, y^{a+b}, z^{a+b} \rangle.$$

Then we see that k_m/k is a cyclic extension of degree p^m and that p is totally ramified in k_m/k. From this, it follows that L'_m/k_m is an unramified cyclic extension which p splits completely. Finally, define

$$k_\infty \leftrightarrow \langle \gamma x^{a-c}, xy^{-1}z, xy \rangle = \langle J(\gamma)\gamma, xy^{-1}z, xy \rangle. \tag{4.5}$$

Then J acts on $\mathrm{Gal}(k_\infty/k)$ as -1 and $k_m \subset k_\infty$. In addition, p is totally ramified in the $\mathbb{Z}_p$-extension k_∞/k, since p is totally ramified in k_m/k. So, put $L' := L'_m k_\infty$; then we have projection $X'(k_\infty) \twoheadrightarrow \mathrm{Gal}(L'/k_\infty)$. Now, assume that $X(\widetilde{k})$ is trivial. Then by Corollary 2.3.3, J acts on $\mathrm{Gal}(L'/k_\infty)$ trivially. However, J indeed acts on it as -1 since J acts on $\mathrm{Gal}(L'_m/k)$ as -1. This is a contradiction. So, $X(\widetilde{k})$ is not trivial. This completes the proof of Proposition 4.3.1.

4.4 Proof in the case $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2$

Suppose that $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2$. In this subsection, we show the following proposition. The outline of the proof is similar to §3.1.2, although the computation is a little complicated.

Proposition 4.4.1. *Let k be a CM-field of degree 6. Suppose that k satisfies the conditions* (I)(II)(III) *in the last of* §2.4. *If* $\dim_{\mathbb{F}_p} A(k)/pA(k) = 2$ *then* $X(\widetilde{k})$ *is not trivial.*

By Corollary 4.1.6, one of a, b, c is not congruent to 0 and

$$a^2 + bc \equiv b^2 - ac \equiv c^2 + ab \equiv 0.$$

(Recall that the notation $\equiv$ is used for a congruence modulo p.) In addition, we have the following.

Lemma 4.4.2. *In modulo p,*

(i) *All of a, b, c are not congruent to* 0.
(ii) $a + b + c \not\equiv 0$, $a + b - c \not\equiv 0$.

Proof. (i) If $a \equiv 0$, then we obtain $b \equiv c \equiv 0$ since $b^2 - ac \equiv c^2 + ab \equiv 0$. This is a contradiction, so $a \not\equiv 0$. In the same way, we have $b \not\equiv 0$, $c \not\equiv 0$.
(ii) Assume that $a + b + c \equiv 0$, i.e., $c \equiv -a - b$. This yields that

$$0 \equiv c^2 + ab \equiv a^2 + 3ab + b^2 \quad \text{and} \quad 0 \equiv a^2 + bc \equiv a^2 - ab - b^2.$$

Then we have $2a(a + b) \equiv 0$, so $a + b \equiv 0$ by (i). Then $0 \equiv a + b + c \equiv c \not\equiv 0$, which is a contradiction. Therefore, $a + b + c \not\equiv 0$. Next, assume that $a + b - c \equiv 0$, i.e., $c \equiv a + b$. Then

$$0 \equiv c^2 + ab \equiv a^2 + 3ab + b^2 \quad \text{and} \quad 0 \equiv a^2 + bc \equiv a^2 + ab + b^2.$$

Then we have $2ab \equiv 0$, which contradicts (i). Thus, we obtain $a + b - c \not\equiv 0$. □

Define P_∞, Q_∞ by

$$\begin{cases} P_\infty \leftrightarrow \langle D_1, D_{\overline{1}} \rangle = \langle \gamma, x, y^{a+b-c} z^{a+b+c} \rangle, \\ Q_\infty \leftrightarrow \langle D_2, D_{\overline{2}} \rangle = \langle \gamma x^a z^c, y, x^{-a-b-c} z^{a+b-c} \rangle. \end{cases} \tag{4.6}$$

By Lemma 4.4.2(ii), both P_∞ and Q_∞ are $\mathbb{Z}_p$-extensions of k. Put $Z := \langle D_1, D_{\overline{1}} \rangle \cap \langle D_2, D_{\overline{2}} \rangle$ for convenience.

Lemma 4.4.3.

(i) $Z = \left\langle \gamma^{a+b+c} x^{a(a+b+c)} y^{c(a+b-c)} z^{c(a+b+c)},\ x^{(a+b+c)^2} y^{-(a+b-c)^2} z^{-(a+b-c)(a+b+c)} \right\rangle.$
(ii) *The complex conjugation $J \in \mathrm{Gal}(k/k^+)$ acts on $\langle \gamma, x, y, z \rangle / Z$ as -1.*

Proof. (i) Denote by Z' the right hand side of the equation in the lemma. By Lemma 4.4.2(i), we have

$$\langle D_1, D_{\overline{1}}, D_2, D_{\overline{2}} \rangle = \langle \gamma, x, y, z^c \rangle = \langle \gamma, x, y, z \rangle \tag{4.7}$$

and $\langle \gamma, x, y, z\rangle / \langle D_i, D_{\bar{i}}\rangle \simeq \mathbb{Z}_p$ $(i = 1, 2)$. Hence we obtain

$$\langle D_1, D_{\bar{1}}, D_2, D_{\bar{2}}\rangle / Z \simeq \mathbb{Z}_p^{\oplus 2}. \tag{4.8}$$

On the other hand, by (4.6), we can easily check

$$\begin{cases} \gamma^{a+b+c}x^{a(a+b+c)}y^{c(a+b-c)}z^{c(a+b+c)} = \gamma^{a+b+c} \cdot x^{a(a+b+c)} \cdot (y^{a+b-c}z^{a+b-c})^{c} \in \langle D_1, D_{\bar{1}}\rangle, \\ x^{(a+b+c)^2}y^{-(a+b-c)^2}z^{-(a+b-c)(a+b+c)} = x^{(a+b+c)^2}(y^{a+b-c}z^{a+b+c})^{-(a+b+c)} \in \langle D_1, D_{\bar{1}}\rangle \end{cases}$$

and

$$\begin{cases} \gamma^{a+b+c}x^{a(a+b+c)}y^{c(a+b-c)}z^{c(a+b+c)} = (\gamma x^a z^c)^{a+b+c} \cdot y^{c(a+b-c)} \in \langle D_2, D_{\bar{2}}\rangle, \\ x^{(a+b+c)^2}y^{-(a+b-c)^2}z^{-(a+b-c)(a+b+c)} = y^{-(a+b-c)^2} \cdot (x^{a+b+c}z^{-(a+b-c)})^{a+b+c} \in \langle D_2, D_{\bar{2}}\rangle. \end{cases}$$

Hence $Z' \subset Z$. Moreover, we can check

$$\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \end{bmatrix} \sim \begin{bmatrix} 1 & a & * & * \\ 0 & 1 & * & * \end{bmatrix}$$

since $a+b+c \in \mathbb{Z}_p^{\times}$. This implies that $\langle \gamma, x, y, z\rangle / Z' \simeq \mathbb{Z}_p^{\oplus 2}$. Combining (4.8) with this, we obtain $Z = Z'$.

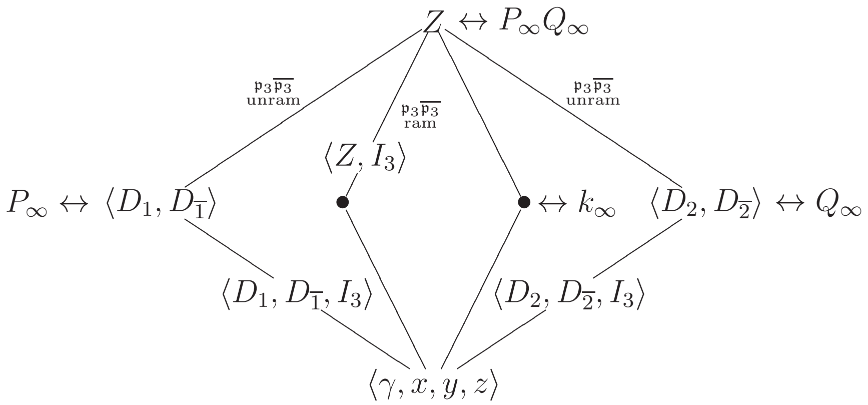
(ii) It suffices to show $J(\gamma)\gamma \in Z$, which is equivalent to $\langle Z, J(\gamma)\gamma\rangle = Z$. Since $J(\gamma) = \gamma x^{a-b-c}y^{a+b-c}z^{a+b+c}$ and $a+b+c \in \mathbb{Z}_p^{\times}$, we know that

$$\langle Z, J(\gamma)\gamma\rangle = \langle Z, (\gamma^2 x^{a-b-c}y^{a+b-c}z^{a+b+c})^{a+b+c}\rangle.$$

So, by direct computation, we have

$$\begin{aligned} &\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 2(a+b+c) & (a-b-c)(a+b+c) & (a+b-c)(a+b+c) & (a+b+c)^2 \end{bmatrix} \\ &\sim \begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & -(a+b+c)^2 & (a+b-c)^2 & (a+b-c)(a+b+c) \end{bmatrix} \\ &\qquad \text{(add } (-2)\times\text{(the first row) to the third row)} \\ &\sim \begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

This implies $\langle Z, J(\gamma)\gamma\rangle = Z$, which completes the proof. □



$Z \leftrightarrow P_\infty Q_\infty$
$\mathfrak{p}_3\overline{\mathfrak{p}_3}$ unram
$\mathfrak{p}_3\overline{\mathfrak{p}_3}$ ram
$\mathfrak{p}_3\overline{\mathfrak{p}_3}$ unram
$\langle Z, I_3\rangle$
$P_\infty \leftrightarrow \langle D_1, D_{\overline{1}}\rangle$
$\leftrightarrow k_\infty$
$\langle D_2, D_{\overline{2}}\rangle \leftrightarrow Q_\infty$
$\langle D_1, D_{\overline{1}}, I_3\rangle$
$\langle D_2, D_{\overline{2}}, I_3\rangle$
$\langle \gamma, x, y, z\rangle$

Figure 7:

To obtain the desired $\mathbb{Z}_p$-extension k_∞/k satisfying Corollary 2.3.3, we consider the inertia groups of $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$ in $\mathrm{Gal}(P_\infty Q_\infty/k)$ (Figure 7). Note that $k \leftrightarrow \langle D_1, D_{\overline{1}}, D_2, D_{\overline{2}}\rangle$ by (4.7). Since $(a^2+bc)+(c^2+ab) \neq 0$ by Lemma 4.1.7, we see that $\langle D_1, D_{\overline{1}}, I_3\rangle = \langle D_1, D_{\overline{1}}, I_{\overline{3}}\rangle = \langle \gamma, x, y^{-c}z^a, y^{a+b}z^{b+c}\rangle$ is a subgroup of $\langle \gamma, x, y, z\rangle$ with a finite index. This implies that $P_\infty Q_\infty/P_\infty$ is unramified at $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. In the same way, since $(b^2-ac)+(c^2+ab)\neq 0$, we obtain that $P_\infty Q_\infty/Q_\infty$ is unramified at $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. On the other hand, we can easily check $\langle Z, x\rangle = \langle D_1, D_{\overline{1}}\rangle$ and $\langle Z, y\rangle = \langle D_2, D_{\overline{2}}\rangle$ by Lemmas 4.4.2(ii), 4.4.3(i) and (4.6). Hence, there are some $\alpha, \beta \in \mathbb{Z}_p$ such that

$$\langle Z, I_3\rangle = \langle Z, I_{\overline{3}}\rangle = \langle Z, x^\alpha y^\beta\rangle \ \ (\alpha, \beta \neq 0).$$

Now, we define an integer d as follows. If $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$, then set $d := 0$; otherwise, i.e., if $\beta/\alpha \in \mathbb{Z}_p^\times$, then d is an integer satisfying $\pm 1 + pd \neq \beta/\alpha$. Then, we define

$$k_\infty \leftrightarrow \begin{cases} \langle Z, xy^{1+pd}\rangle & \text{if } a+b \equiv 0, \\ \langle Z, xy^{-1+pd}\rangle & \text{if } a+b \not\equiv 0. \end{cases}$$

Then k_∞ is different from $P_\infty(\leftrightarrow \langle Z, x\rangle)$ and $Q_\infty(\leftrightarrow \langle Z, y\rangle)$. Moreover, k_∞ has the following properties.

Lemma 4.4.4.

(i) *k_∞/k is a $\mathbb{Z}_p$-extension, and $P_\infty Q_\infty/k_\infty$ is a $\mathbb{Z}_p$-extension unratified at $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$.*

(ii) *The complex conjugation acts on* $\mathrm{Gal}(k_\infty/k)$ *as* -1.

(iii) *In k_∞/k, p is non-split and ramified.*

Proof. (i) Considering the representation matrix of $\mathrm{Gal}(k_\infty/k)$, we have

$$\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & 1 & \pm 1 + pd & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & * & 0 \\ 0 & 0 & * & 1 \\ 0 & 1 & * & 0 \end{bmatrix}$$

by Lemma 4.4.2. This implies that each k_∞ and $P_\infty Q_\infty$ is a $\mathbb{Z}_p$-extension over k and k_∞, respectively. Assume that $\mathfrak{p}_3$ ramifies in $P_\infty Q_\infty/k_\infty$. Then k_∞ is contained in the fixed field by $\langle Z, I_3\rangle$, so $\langle Z, I_3, xy^{\pm 1+pd}\rangle \simeq \mathbb{Z}_p^{\oplus 3}$. However, by the definition of d, we see that the rank of

$$\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & 1 & \pm 1+pd & 0 \\ 0 & \alpha & \beta & 0 \end{bmatrix}$$

is 4, which is a contradiction. Therefore, $\mathfrak{p}_3$ is unramified in $P_\infty Q_\infty/k_\infty$, and so is $\overline{\mathfrak{p}_3}$.
(ii) The claim follows directly from Lemma 4.4.3(ii).
(iii) We first show that p is non-split in k_∞/k. By Lemmas 4.4.2 and 4.4.3(i), we obtain

$$\langle Z, xy^{\pm 1+pd}, D_1\rangle = \langle \gamma, x, y, z^{-(a+b-c)(a+b+c)}\rangle = \langle \gamma, x, y, z\rangle.$$

This implies $\mathfrak{p}_1$ is non-split in k_∞/k. In the same way, we obtain the same results for $\mathfrak{p}_2$, $\overline{\mathfrak{p}_1}$ and $\overline{\mathfrak{p}_2}$. We proceed to consider $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$. In the case where $a+b \equiv 0$, considering the representation matrix of $\langle Z, xy^{1+pd}, D_3\rangle$ mod p, we have

$$\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & 1 & +1+pd & 0 \\ 1 & a-c & a+b & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\equiv \begin{bmatrix} c & ac & -c^2 & c^2 \\ 0 & c^2 & -c^2 & c^2 \\ 0 & 1 & 1 & 0 \\ 1 & a-c & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & a & -c & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & a-c & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & a & -c & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -c & c & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The last matrix has rank 4. This implies $\mathfrak{p}_3$ (and so $\overline{\mathfrak{p}_3}$ by 4.4.3(ii)) is non-split in k_∞/k. Similarly, in the case where $a+b \not\equiv 0$, the representation matrix of $\langle Z, xy^{-1+pd}, D_3\rangle$ mod p is

$$\begin{bmatrix} a+b+c & a(a+b+c) & c(a+b-c) & c(a+b+c) \\ 0 & (a+b+c)^2 & -(a+b-c)^2 & -(a+b-c)(a+b+c) \\ 0 & 1 & -1 & 0 \\ 1 & a-c & a+b & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Add $-(a+b+c)\times$(the fourth row) to the first row and add $-(a+b+c)^2\times$(the third row) to the second row, then we see that the matrix is similar to

$$\begin{bmatrix} 0 & c(a+b+c) & -(a+b)^2-c^2 & c(a+b+c) \\ 0 & 0 & 4(a+b)c & -(a+b-c)(a+b+c) \\ 0 & 1 & -1 & 0 \\ 1 & a-c & a+b & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

This matrix has rank 4 since $4(a+b)c \in \mathbb{Z}_p^\times$. So, we obtain that $\mathfrak{p}_3$ (and so $\overline{\mathfrak{p}_3}$) is non-split in k_∞/k.

Next, we show that p is unramified in k_∞/k. Recall that $P_\infty Q_\infty/k$ is a $\mathbb{Z}_p^2$-extension that is especially bicyclic, and that k_∞/k is a $\mathbb{Z}_p$-extension. Assume that $\mathfrak{p}_2$ is unramified in P_∞/k. Then, by Lemma 4.4.3(ii), $\overline{\mathfrak{p}_2}$ is also unramified in P_∞/k. This implies that P_∞/k is a $\mathbb{Z}_p$-extension unramified outside $\{\mathfrak{p}_3, \overline{\mathfrak{p}_3}\}$ in which $\mathfrak{p}_1$ splits completely. This is a contradiction by [7, Lemma 3]. Thus, $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ are ramified in P_∞/k. In the same way, $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$ are also ramified in P_∞/k. Similarly, $\mathfrak{p}_1$, $\overline{\mathfrak{p}_1}$, $\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$ are ramified in Q_∞/k. Consequently, we see that $\mathfrak{p}_1$ and $\overline{\mathfrak{p}_1}$ are ramified in $P_\infty Q_\infty/P_\infty$ and that $\mathfrak{p}_2$ and $\overline{\mathfrak{p}_2}$ are ramified in $P_\infty Q_\infty/Q_\infty$. Therefore, these primes are unramified in $P_\infty Q_\infty/k_\infty$. By (i), $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_3}$ are unramified in $P_\infty Q_\infty/k_\infty$. So, $P_\infty Q_\infty/k_\infty$ is an unramified extension, which implies that p is ramified in k_∞/k. This completes the proof. □

Now, we prove Proposition 4.4.1. Recall that the complex conjugation acts on $\mathrm{Gal}(k_\infty/k)$ (as -1) by Lemma 4.4.4(ii). Since $\mathfrak{p}_1$, $\overline{\mathfrak{p}_1}$, $\mathfrak{p}_2$, and $\overline{\mathfrak{p}_2}$ infinitely split in $P_\infty Q_\infty/k$ and are non-split in k_∞/k by Lemma 4.4.4(iii), these four primes split completely in $P_\infty Q_\infty/k_\infty$. Assume that $\mathfrak{p}_3$ does not split in the $\mathbb{Z}_p$-extension $P_\infty Q_\infty/k_\infty$. Then, again by Lemma 4.4.4(iii), this implies that $\mathfrak{p}_3$ does not split in $P_\infty Q_\infty/k$, and especially in $P_\infty Q_\infty/P_\infty$. Using $(a^2+bc)+(c^2+ab)\equiv 0$, we have

$$\langle D_1, D_{\overline{1}}, I_3\rangle = \langle \gamma, x, y^{-c}z^a, y^{a+b}z^{b+c}\rangle \neq \langle D_1, D_{\overline{1}}, D_3\rangle = \langle \gamma, x, y^{a+b-c}, z\rangle = \langle \gamma, x, y, z\rangle.$$

This implies that $\mathfrak{p}_3$ must be inert in P_∞/k, and therefore $\mathfrak{p}_3$ cannot be totally inert in $P_\infty Q_\infty/P_\infty$. In other words, $\mathfrak{p}_3$ splits in $P_\infty Q_\infty/P_\infty$. However, since $\mathfrak{p}_3$ does not split in $P_\infty Q_\infty/k$, this is a contradction. Therefore, $\mathfrak{p}_3$ splits in $P_\infty Q_\infty/k_\infty$. The same is true for $\overline{\mathfrak{p}_3}$ in place of $\mathfrak{p}_3$ by Lemma 4.4.3(ii). Hence, there is an unramified subextension L'/k_∞ in $P_\infty Q_\infty$ which p splits completely. Now, assume that $X(\widetilde{k})$ is trivial. Then by Corollary 2.3.3, the complex conjugation J acts on $\mathrm{Gal}(L'/k_\infty)$ trivially. However, J indeed acts on it as -1 by Lemma 4.4.3(ii). This is a contradiction. So, $X(\widetilde{k})$ is not trivial.

Question. Under the conditions that $[k:\mathbb{Q}] > 2$ and $X(\widetilde{k}) \neq 0$, is $X(\widetilde{k})$ finitely generated as a $\mathbb{Z}_p$-module? No such examples have been found; nor have any examples been found that do not. If there should exist a CM-field k with $[k:\mathbb{Q}] \geq 4$ which satisfies the following, then $X(\widetilde{k})$ is $\mathrm{Gal}(L(k_{\mathrm{cyc}})/\widetilde{k})$, which is finitely generated as a $\mathbb{Z}_p$-module:

(i) p splits completely in k and Leopoldt's conjecture holds for k and p.

(ii) $\mu(k_{\mathrm{cyc}}/k) = 0$ (this holds if k is abelian over $\mathbb{Q}$ by Ferrero and Washington [3]).

(ii) $X(\widetilde{k}) \neq 0$ and k_{cyc} has an abelian p-class field tower; i.e., the maximal unramified p-extension of k_{cyc} is abelian.

Acknowledgement. The author would like to express his thanks to Professor Satoshi Fujii, Professor Tsuyoshi Itoh and Doctor John Minardi for their earlier studies [7], [12], and [18]. Many parts of the proof in this paper are supported by their brilliant ideas. The author would also like to express his gratitude to Professor Satoshi Fujii for pointing out the author's mistakes and providing valuable comments, and to Professor Tsuyoshi Itoh for helpful input. Thanks also go to Takashi Fukuda for providing his program to find examples.

References

[1] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, and E. Ozman, *Bad reduction of genus three curves with complex multiplication,* Women in numbers Europe, 109–151. Assoc. Women Math. Ser., **2** Springer, Cham, (2015).

[2] B. Dodson, *The structure of Galois groups of CM-fields,* Trans. Amer. Math. Soc. **283** (1984) 1–32.

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

[4] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields,* Contemporary Mathematics, 24. American Mathematical Society, Providence, RI, 1983.

[5] S. Fujii, *Pseudo-null submodules of the unramified Iwasawa module for $\mathbb{Z}_p^2$-extensions,* Interdiscip. Inf. Sci. **16** (2010) 55–66.

[6] 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.

[7] S. Fujii, *On Greenberg's generalized conjecture for CM-fields,* J. Reine Angew. Math. **731** (2017) 259–278.

[8] S. Fujii, *On families of imaginary abelian fields with pseudo-null unramified Iwasawa modules,* New York J. Math. **28** (2022) 523–533.

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

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

[11] R. Greenberg, *Iwasawa theory-past and present,* in: Class field theory - its centenary and prospect (Tokyo 1998), Adv. Stud. Pure Math. **30**, Mathematical Society of Japan, Tokyo (2001) 335–385.

[12] T. Itoh, *On multiple $\mathbb{Z}_p$-extensions of imaginary abelian quartic fields,* J. Number Theory **131** (2011) 59–66.

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

[14] J.-F. Jaulent, *Sur la trivialité de certains modules d'Iwasawa,* Funct. Approx. Comment. Math. **70** (2024) 29–39.

[15] T. Kataoka, *Finite submodules of Iwasawa modules for multi-variable extensions,* J. Number Theory. **239** (2022) 228–250.

[16] S. Kleine *On pseudo-null Iwasawa modules,* J. Théor. Nombres Bordeaux **34** (2022) 583–618.

[17] J.S. Milne, *C*omplex multiplication, (2006). Available at
`https://www.jmilne.org/math/`

[18] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields,* Thesis (Ph.D.) University of Washington. 1986.

[19] T. Miura, K. Murakami, K. Okano and R. Otsuki, *Galois coinvariants of the unramified Iwasawa modules of multiple $\mathbb{Z}_p$-extensions,* Ann. Math. Qué. **45** (2021) 407–431.

[20] A. Mouhib and A. Movahhedi, *Cyclicity of the unramified Iwasawa module,* Manuscripta Math. **135** (2011) 91–106.

[21] K. Murakami, *A weak form of Greenberg's generalized conjecture for imaginary quadratic fields,* J. Number Theory **244** (2023) 308–338.

[22] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields,* Second edition. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2008.

[23] T. Nguyen Quang Do, *Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé,* Int. J. Number Theory **2** (2006) 49–64.

[24] T. Nguyen Quang Do, *Sur une forme faible de la conjecture de Greenberg II,* Int. J. Number Theory **13** (2017) 1061–1070.

[25] K. Okano, *Abelian p-class Field Towers over the Cyclotomic $\mathbb{Z}_p$-extensions of Imaginary Quadratic Fields,* Acta Arith. **125** (2006) 363–381.

[26] K. Okano, *The commutativity of the Galois groups of the maximal unramified pro-p-extensions over the cyclotomic $\mathbb{Z}_p$-extensions,* J. Number Theory **132** (2012) 806–819.

[27] T. Shirakawa, *Generalized Greenberg conjecture for imaginary quadratic fields,* Master's thesis, Keio University, 2012 (in Japanese).

[28] H. Taya and G. Yamamoto, *Notes on certain real abelian 2-extension fields with $\lambda_2 = \mu_2 = \nu_2 = 0$,* Trends in Mathematics, Information Center for Mathematical Sciences **9** (2006) 81–89.

[29] H. Taya and G. Yamamoto, *On the density of real quadratic fields with $\lambda_2 = \mu_2 = \nu_2 = 0$,* Interdiscip. Inform. Sci. **16** (2010) 87–92.

[30] L. C. Washington, *Introduction to Cyclotomic Fields,* Second edition. Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1997.

[31] K. Wingberg, *Free pro-p extensions of number fields,* preprint.

[32] G. Yamamoto, *On the vanishing of Iwasawa invariants of absolutely abelian p-extensions,* Acta Arith. **94** (2000) 365–371.