Okano, K.
Osaka J. Math.
49 (2012), 271–295

THE COMMUTATIVITY OF GALOIS GROUPS OF THE MAXIMAL UNRAMIFIED PRO-p-EXTENSIONS OVER THE CYCLOTOMIC $\mathbb{Z}_p$-EXTENSIONS II

KEIJI OKANO

(Received October 13, 2009, revised October 22, 2010)

Abstract

Let p be an odd prime number and K_∞ the cyclotomic $\mathbb{Z}_p$-extension of a Galois p-extension K over an imaginary quadratic field. We consider the Galois group $\tilde{X}(K_\infty)$ of the maximal unramified pro-p-extension of K_∞. In this paper, under certain assumptions, we give certain K such that $\tilde{X}(K_\infty)$ is abelian. Also, we give an example such that a special value of the characteristic polynomial of the Iwasawa module of K_∞ determines whether $\tilde{X}(K_\infty)$ is abelian or not.

1. Introduction

Let p be an odd prime number, F a finite extension over the field $\mathbb{Q}$ of rational numbers and F_∞ the cyclotomic $\mathbb{Z}_p$-extension of F. In other words, F_∞ is defined by the following. The extension over F which is obtained by adjoining to F all roots of unity of p-power order has the unique subfield whose Galois group over F is isomorphic to the additive group of the ring $\mathbb{Z}_p$ of p-adic integers. We define F_∞ by the subfield. Denote by $\tilde{X}(F)$ (resp. $\tilde{X}(F_\infty)$) the Galois group of the maximal unramified pro-p-extension $\tilde{L}(F)$ of F (resp. $\tilde{L}(F_\infty)$ of F_∞). The extensions $\tilde{L}(F)/F$, $\tilde{L}(F_\infty)/F_\infty$ are called the p-class field towers, and their Galois groups $\tilde{X}(F)$, $\tilde{X}(F_\infty)$ are very interesting objects in number theory. Though $\tilde{X}(F)$ can be infinite, we have quite a few known criterions for assuring that $\tilde{X}(F)$ is finite: in addition, we do not have efficient methods for describing the structure of $\tilde{X}(F)$. However, we mention that Ozaki [17] recently showed that there exists F such that $\tilde{X}(F)$ is isomorphic to any given *finite* p-group.

We apply Iwasawa theory to the study of p-class field towers, such as in Mizusawa [11], [12] and Ozaki [16]. We consider to *classify the finite algebraic number fields F such that each $\tilde{X}(F_\infty)$ is abelian*; in other words, the maximal unramified pro-p-extension of each F_∞ remains abelian extension. It is equivalent that $\tilde{X}(F_\infty)$ is abelian and that all sufficiently large subfields in F_∞/F have the p-class field towers whose Galois groups are abelian. Also if $\tilde{X}(F)$ is abelian for a finite algebraic number field

2000 Mathematics Subject Classification. Primary 11R23; Secondary 11R37.

F, then $\tilde{X}(F)$ is finite and isomorphic to the p-Sylow subgroup of the ideal class group of F.

In [14], the author determined the all imaginary quadratic fields F such that $\tilde{X}(F_\infty)$ is abelian for an odd prime number p: for $p = 2$, the same result was shown by Mizusawa–Ozaki [13]. After [13] and [14], one of further problems for the above classifying is to treat the case where F is an abelian number field. However, this problem seems very difficult. Since, for instance, there is Greenberg's conjecture which says that the maximal unramified abelian pro-p-extension of F_∞ is finite if F is totally real. In [15], the author studied necessary conditions for $\tilde{X}(F_\infty)$ to be abelian. And also the case where each F is totally imaginary abelian p-extensions over imaginary quadratic fields with certain assumptions is treated. On the other hand, Sharifi [18] computed the structure of $\tilde{X}(F_\infty)$ in the case where F is the cyclotomic p-th extension.

In this paper, we treat totally imaginary abelian p-extensions over imaginary quadratic fields with certain assumptions which are different from [15]. Simultaneously, we consider the following question.

We note the fact in [13] that, if $p = 2$, there is a case where the special value modulo 2^2 at -1 of the characteristic polynomial of Iwasawa module contributes to the condition for $\tilde{X}(F_\infty)$ to be abelian. This fact is interesting since the characteristic polynomials of Iwasawa modules are connected to the p-adic L-function by Mazur–Wiles [10]. So that the next question arises. Is there a similar case if p is odd?

We use the notation $A(F)$ for the p-Sylow subgroup of the ideal class group of F. Then we obtain followings:

Theorem 1.1. *Let p, l be odd prime numbers such that $p \mid l-1$, k an imaginary quadratic field with the property that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$, and K^+ an abelian p-extension of $\mathbb{Q}$ with conductor l. Put $K := kK^+$ and let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K. Assume that p does not split in K and l does not split in k. Then the Galois group $\tilde{X}(K_\infty)$ of the maximal unramified pro-p-extension over K_∞ is abelian if and only if $A(k) = 0$ moreover we have then $\tilde{X}(K_\infty) = 1$.*

Theorem 1.2. *Let l be an odd prime number such that $3 \parallel l-1$, k an imaginary quadratic field with the property that $k \neq \mathbb{Q}(\sqrt{-3})$, and K^+ the unique abelian 3-extension of $\mathbb{Q}$ with conductor l. Put $K := kK^+$ and let $P_K(T) \in \mathbb{Z}_3[T]$ be the characteristic polynomial of the Iwasawa module of the cyclotomic $\mathbb{Z}_3$-extension K_∞/K. Suppose that 3 does not split in K but l splits in k. Moreover, assume that $A(k) = 0$ and $\dim_{\mathbb{F}_3} A(K) \otimes_{\mathbb{Z}} \mathbb{F}_3 = 1$. Then $\tilde{X}(K_\infty)$ is abelian if and only if $P_K(-1) \not\equiv 1 \bmod 3^2$.*

2. Preliminaries

From now on, for any CM-field F, we use the notation F^+ and F_n for the maximal totally real subfield of F and the unique subfield with degree p^n of the cyclotomic $\mathbb{Z}_p$-extension F_∞ over F, respectively. Denote the maximal unramified abelian

p-extension of F by $L(F)$ and its Galois group $\tilde{X}(F)^{\mathrm{ab}}$ by $X(F)$. Similarly, denote the maximal unramified abelian pro-p-extension of F_∞ by $L(F_\infty)$ and its Galois group by $X(F_\infty)$. For any module A on which $\mathrm{Gal}(F/F^+)$ acts, put $A^+ := A^{\mathrm{Gal}(F/F^+)}$, $A^- := A/A^+$.

Fix a topological generator $\bar{\gamma}$ of $\mathrm{Gal}(F_\infty/F)$. And we write its restriction on $\mathrm{Gal}(F_n/F)$ as the same notation for each $n \geq 0$. Choose an extension $\gamma \in \mathrm{Gal}(L(F_\infty)/F)$ of $\bar{\gamma}$. Then $\mathrm{Gal}(F_n/F)$ acts on $X(F_n)$ as the inner automorphisms defined by $x^{\bar{\gamma}} = \gamma x \gamma^{-1}$ for any $x \in X(F_n)$. Note that this action is independent of the choice of an extension γ and commutes with the Artin maps $X(F_n) \simeq A(F_n)$. We identify $X(F_n)$ with $A(F_n)$ by these isomorphisms. Since $X(F_\infty) \simeq \varprojlim X(F_n)$, the complete group ring $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$ acts on $X(F_\infty)$ continuously, where each inverse limit is taken over Galois restrictions. Hence the formal power series ring $\Lambda := \mathbb{Z}_p[[T]]$ acts on $X(F_\infty)$ via the non-canonical isomorphism $\Lambda \simeq \varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/F)]$ which is obtained by sending $1+T$ to the fixed topological generator $\bar{\gamma}$ of $\mathrm{Gal}(F_\infty/F)$. Therefore $X(F_\infty)$ is a Λ-module, so that we write the action of Λ additionally; $x^{\bar{\gamma}} = (1+T)x$.

The module Λ is a noetherian local ring with the maximal ideal (p, T). We define a distinguished polynomial $P(T) \in \mathbb{Z}_p[T]$ by monic polynomial such that $P(T) \equiv T^{\deg P(T)} \bmod p$. Then, by the p-adic Weierstraß preparation theorem [19, Theorem 7.3], any non-zero element $f(T) \in \Lambda$ can be uniquely written

$$f(T) = p^{\mu} P(T) U(T)$$

with an integer $\mu \geq 0$, a distinguished polynomial $P(T)$ and $U(T) \in \Lambda^\times$. Then $\deg P(T)$ is called the residue degree of $f(T)$. Also, there is a division theorem [19, Proposition 7.2] for distinguished polynomials: if $f(T) \in \Lambda$ is non-zero and $P(T)$ is distinguished, then there uniquely exist $q(T) \in \Lambda$ and $r(T) \in \mathbb{Z}_p[T]$ such that

$$f(T) = q(T)P(T) + r(T), \quad \deg r(T) < \deg P(T).$$

Therefore Λ is a UFD, whose irreducible elements are p and irreducible distinguished polynomials.

It turns out that $X(F_\infty)$ is a finitely generated torsion module over Λ. Therefore we can define the Iwasawa λ-invariant λ_F of F_∞/F by the dimension of $X(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ over the p-adic field $\mathbb{Q}_p$. There is a Λ-homomorphism

$$X(F_\infty)^- \to \bigoplus_{i=1}^{s} \Lambda/(P_i)^{m_i}$$

such that its kernel and cokernel are finite, where the principal ideals (P_i) in Λ are prime ideals of height 1, the ideals (P_i) and the integers m_i, s are uniquely determined by $X(F_\infty)^-$ ([19, Theorem 13.12]). In fact, the map is injective since $X(F_\infty)^-$ has no non-trivial finite Λ-submodules by [19, Theorem 13.28]. We say that the Iwasawa

μ-invariant μ_F of F_∞/F is zero if $X(F_\infty)$ is also finitely generated over $\mathbb{Z}_p$: For example, if $F/\mathbb{Q}$ is an abelian extension, then $\mu_F = 0$ by Ferrero–Washington [2]. In particular, if $\mu_F = 0$, then $X(F_\infty)^-$ is a free $\mathbb{Z}_p$-module, and so that we may take each P_i as an irreducible distinguished polynomial. Then the polynomial $P_F(T) := \prod_{i=1}^{s} P_i^{m_i}$ is called the characteristic polynomial of $X(F_\infty)^-$ and we have $\lambda_F^- := \lambda_F - \lambda_{F^+} = \deg P_F(T)$. It turns out that, if the extension F_∞/F is totally ramified at all primes lying above p, then there is an isomorphism

$$X(F_n) \simeq X(F_\infty) \Big/ \frac{\omega_n(T)}{T} Y \tag{1}$$

for any $n \geq 0$, where $Y := \mathrm{Gal}(L(F_\infty)/L(F)F_\infty)$, $\omega_n(T) := (T+1)^{p^n} - 1$.

Now, let k be a CM-field such that k is a finite extension over $\mathbb{Q}$ with $\mu_k = 0$ and K^+ a cyclic extension of k^+ with degree p such that $k_\infty^+ \cap K^+ = k^+$. Put $K := kK^+$ and $\Delta := \mathrm{Gal}(K/k)$. First of all, we compare $P_K(T)$ with $P_k(T)$ (Proposition 2.1). We identify $\Gamma := \mathrm{Gal}(k_\infty/k)$ with $\mathrm{Gal}(K_\infty/K)$ and Δ with $\mathrm{Gal}(K_\infty/k_\infty)$ by the canonical isomorphisms. Note that Δ acts on $X(K_\infty)$ and $X(K_\infty)^-$ as the inner automorphisms similar to the action of Γ. The actions of Γ and Δ are commutative since $X(K_\infty)$, $X(K_\infty)^-$ and $\mathrm{Gal}(K_\infty/k)$ are abelian. Therefore $X(K_\infty)$, $X(K_\infty)^-$ are $\Lambda[\Delta]$-modules. By Iwasawa [7] and Kida's formula [8], $\mu_K = 0$ and

$$\lambda_K^- = p\lambda_k^- + (p-1)(s-\nu), \tag{2}$$

where s is the number of primes in K_∞^+ not lying above p which split in K_∞/K_∞^+ and ramify in K_∞^+/k_∞^+, and $\nu = 1$ or 0 according as a primitive p-th root of unity is in k or not. In addition, suppose that $X(K_\infty)^-$ is cyclic over Λ. Then we have a surjection

$$\Lambda/(P_K(T)) \twoheadrightarrow X(K_\infty)^-,$$

since $X(K_\infty)^-$ has no non-trivial finite Λ-submodules and is annihilated by $P_K(T)$. Comparing the $\mathbb{Z}_p$-ranks, we have $X(K_\infty)^- \simeq \Lambda/(P_K(T))$. Fix a generator $\varepsilon \in X(K_\infty)^-$ over Λ and a generator $\delta \in \Delta$. We described the action of Δ as x^δ. Then we have

$$\varepsilon^\delta = (Q(T)+1)\varepsilon$$

for some $Q(T) \in \Lambda$. Then polynomial $Q(T) \in \Lambda$ is uniquely defined up to the modulus $P_K(T)$ and independent of the choice of ε. We may assume that $Q(T)$ is a polynomial by the division theorem. Put

$$N(T) := Q(T)^{p-1} + \binom{p}{p-1} Q(T)^{p-2} + \cdots + \binom{p}{1} = \frac{(Q(T)+1)^p - 1}{Q(T)}, \tag{3}$$

where $\binom{p}{k}$ is a binomial coefficient. Then we have the following proposition:

Proposition 2.1. *Let K/k and Δ be as above. Assume that $X(K_\infty)^-$ is non-trivial and cyclic over Λ. Then the followings hold*:
(i) *If $\lambda_k^- = 1$, $s = 0$ and $\nu = 1$, where s and ν are defined above, then $X(K_\infty)^- \simeq \mathbb{Z}_p$ as $\mathbb{Z}_p[\Delta]$-modules and $P_K(T) = P_k(T)$. And then, $Q(T) = 0$.*
(ii) *If $\lambda_k^- \neq 1$ or $s \neq 0$ or $\nu \neq 1$, then $s - \mu \geq 0$,*

$$P_K(T) = (\Lambda\text{-unit})P_k(T)N(T) \quad \textit{i.e.,} \quad P_k(T)N(T)/P_K(T) \in \Lambda^\times,$$
$$X(K_\infty)^- \simeq \mathbb{Z}_p[\Delta]^{\oplus \lambda_k^-} \oplus I_\Delta^{\oplus(s-\nu)} \quad \textit{as } \mathbb{Z}_p[\Delta]\textit{-modules}$$

and the residue degree of $Q(T)$ is $\lambda_k^- + s - \nu$, where I_Δ is the augmentation ideal in $\mathbb{Z}_p[\Delta]$.

Proof. We treat $X(K_\infty)^-$ as the inverse limit of ideal class groups via the identification $X(K_\infty)^- = \varprojlim A(K_n)^-$. We consider the norm map $N_{K_\infty/k_\infty}\colon X(K_\infty)^- \to X(k_\infty)^-$ which is induced by the norm maps $N_{K_n/k_n}\colon X(K_n)^- \to X(k_n)^-$ and the norm operator $N_\Delta\colon X(K_\infty)^- \to X(K_\infty)^-$ ($N_\Delta(x) := x + x^\delta + \cdots + x^{\delta^{p-1}}$). If K_∞/k_∞ is not unramified, in other words, $K_\infty \cap L(k_\infty) = k_\infty$, then N_{K_∞/k_∞} is surjective by the class field theory. Similarly, N_{K_∞/k_∞} is surjective if K_∞/k_∞ is unramified. Indeed, by taking the minus-part of the exact sequence of Galois groups

$$1 \to \mathrm{Gal}(L(k_\infty)/K_\infty) \to X(k_\infty) \to \Delta \to 1,$$

we have $X(k_\infty)^- = \mathrm{Gal}(L(k_\infty)/K_\infty)^-$. The right hand side is isomorphic to the image of $X(K_\infty)^-$ by N_{K_∞/k_∞}, and so that N_{K_∞/k_∞} is surjective. Hence $X(k_\infty)^-$ is a cyclic Λ-module generated by $N_{K_\infty/k_\infty}\varepsilon$ and is isomorphic to $\Lambda/(P_k(T))$.

The norm operator N_Δ coincides with the endomorphism by multiplicating $N(T)$ since

$$\begin{aligned} N_\Delta(x) &= x + x^\delta + \cdots + x^{\delta^{p-1}} \\ &= (1 + (1 + Q(T)) + \cdots + (1 + Q(T))^{p-1})x \\ &= N(T)x. \end{aligned}$$

Therefore we have the following commutative diagram:

$$\begin{array}{ccccc} \Lambda/(P_K(T)) \simeq X(K_\infty)^- & \xrightarrow{N_\Delta} & X(K_\infty)^- \simeq \Lambda/(P_K(T)) \\ \text{id.}\downarrow \qquad\quad \downarrow N_{K_\infty/k_\infty} & & \uparrow\text{lift.} \qquad\quad \uparrow N(T) \\ \Lambda/(P_k(T)) \simeq X(k_\infty)^- & = & X(k_\infty)^- \simeq \Lambda/(P_k(T)). \end{array}$$

Here the each map id. and lift. is the map induced by the identity map $\Lambda \to \Lambda$ and the lifting maps on the ideal class groups $\iota_n\colon A(k_n)^- \to A(K_n)^-$, respectively, and the commutativity of the center square follows from $N_\Delta = \iota_n \circ N_{K_n/k_n}$. It follows from this that

$$P_k(T) \mid P_K(T) \mid P_k(T)N(T), \tag{4}$$

where we use the notation $f(T) \mid g(T)$ if $f(T), g(T) \in \Lambda$ satisfy $g(T)/f(T) \in \Lambda$ (recall that Λ is a UFD). Now, we see that $Q(T)N(T)$ belongs to the ideal $(P_K(T))$ of Λ since $\varepsilon = \varepsilon^{\delta^p}$, so that there is some $F(T) \in \Lambda$ such that $Q(T)N(T) = P_K(T)F(T)$. This equation and (3) follow $Q(0) \in p\mathbb{Z}_p$ since $P_K(0) \notin \mathbb{Z}_p^\times$ by the assumption $X(K_\infty)^- \neq 0$. Moreover, we see that $p \parallel N(0)$ by (3) (note that $p \geq 3$). Therefore, by the p-adic Weierstraß preparation theorem,

$$N(T) = pU(T) \quad \text{or} \quad N(T) = \bar{N}(T)U(T)$$

with some $U(T) \in \Lambda^\times$ and some irreducible distinguished polynomial $\bar{N}(T) \in \mathbb{Z}_p[T]$. Combining (4) with $p \nmid P_K(T)$, we have

$$P_K(T) = P_k(T) \quad \text{or} \quad P_K(T) = P_k(T)\bar{N}(T).$$

First, we suppose $P_K(T) = P_k(T)$. Then $1 \leq \lambda_k^- = \lambda_K^- = \nu - s$ by (2) and we have

$$P_K(T) = P_k(T) \iff \lambda_k^- = 1,\ s = 0,\ \nu = 1.$$

Then we may assume that $\deg Q(T) < \deg P_K(T) = 1$ by the division theorem. If $Q(T) \neq 0$, then $Q(T)$ is a constant, and so is $P_K(T)F(T) = Q(T)N(T)$, which is a contradiction. Therefore $Q(T) = 0$, which implies that δ acts on $X(K_\infty)^-$ trivially.

Next, we suppose that $P_K(T) = P_k(T)\bar{N}(T)$ to show the rest of (ii). Then, note that $Q(T), N(T) \notin p\Lambda$ since $P_K(T) \notin p\Lambda$. Let $\bar{Q}(T) \in \mathbb{Z}_p[T]$ be a distinguished polynomial such that $Q(T)/\bar{Q}(T) \in \Lambda^\times$; $\bar{Q}(T)$ depends on the choice of $Q(T)$. Then we know

$$\deg \bar{N}(T) = (p-1)\deg \bar{Q}(T) = (p-1)(\lambda_k^- + s - \nu) \tag{5}$$

by $N(T) \equiv T^{(p-1)\deg \bar{Q}(T)}(Q(T)/\bar{Q}(T))^{p-1} \bmod p$ and (2). Hence $\deg \bar{Q}(T) = \lambda_k^- + s - \nu$. In particular, $\deg \bar{Q}(T)$ does not depend on the choice of $Q(T)$. Note that $P_k(T) \mid Q(T)$ by $Q(T)N(T) = P_K(T)F(T)$ and $P_K(T) = P_k(T)\bar{N}(T)$. This implies that $s - \nu = \deg \bar{Q}(T) - \deg P_k(T) \geq 0$ and also that $P_k(T)$ and $\bar{N}(T)$ are relatively prime by (3). Finally, since Δ is a cyclic group with order p and $X(K_\infty)^-$ is a free $\mathbb{Z}_p$-module, we have a representation

$$X(K_\infty)^- \simeq \mathbb{Z}_p[\Delta]^{\oplus \lambda_k^-} \oplus I_\Delta^{\oplus(s-\nu)}$$

as $\mathbb{Z}_p[\Delta]$-modules by Gold–Madan [5]. This completes the proof. $\square$

Corollary 2.2. *Let K/k and Δ be as above. Suppose that only one prime of K_∞ lies above p and that this prime is totally ramified in K_∞/K. Assume that $A(K)^-$ is non-trivial and cyclic, then*

$$\#A(K)^- = \begin{cases} \#A(k)^- & (\textit{if the assumption of } \text{Proposition 2.1 (i)} \textit{ holds}), \\ p \cdot \#A(k)^- & (\textit{if the assumption of } \text{Proposition 2.1 (ii)} \textit{ holds}), \end{cases}$$

where we denote the order of a set M by $\#M$.

Proof. By the assumption and [19, Theorem 13.22], we obtain

$$A(K) \simeq X(K_\infty)/TX(K_\infty).$$

By Nakayama's lemma, $X(K_\infty)^-$ is non-trivial and cyclic over Λ since $A(K)^-$ is non-trivial and cyclic. Therefore, the claim follows from $A(K)^- \simeq \Lambda/(P_K(T), T) \simeq \mathbb{Z}_p/P_K(0)\mathbb{Z}_p$. $\square$

To prove the main theorems, we use the central p-class field theory as follows. For the central p-class field theory, see [3] and also [14, §2]. Let F be a finite abelian p-extension of an imaginary quadratic field k. For a prime $\mathfrak{q}$ in k which is ramified in F/k, we fix a prime lying above $\mathfrak{q}$ in $L(F)$ and denote its decomposition group in $\mathrm{Gal}(L(F)/k)$ by $Z_\mathfrak{q}$. Then we have the following proposition by the central p-class field theory and the judgment whether $\tilde{L}(F) = L(F)$ or not is reduced to the computation of the map Φ:

Proposition 2.3. *With the notation above, assume that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$. Consider the map*

$$\Phi\colon \prod_{\mathfrak{q}} H_2(Z_\mathfrak{q}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \to H_2(\mathrm{Gal}(L(F)/k), \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$$

which is induced by the canonical map $Z_\mathfrak{q} \to \mathrm{Gal}(L(F)/k)$, where the product is taken over all primes in k which are ramified in F/k. Then $\tilde{L}(F) = L(F)$ if and only if Φ is surjective.

3. Proof of Theorem 1.1

3.1. Arithmetic part. Let p, l be odd prime numbers such that $p \mid l-1$. We define an integer e by $p^{e+1} \parallel l-1$. Let k be an imaginary quadratic field with the condition that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$, and K^+ an abelian p-extension of $\mathbb{Q}$ with conductor l. Put $K := kK^+$. We identify $\Gamma := \mathrm{Gal}(k_\infty/k)$ with $\mathrm{Gal}(K_\infty/K)$ and $\Delta := \mathrm{Gal}(K/k)$ with $\mathrm{Gal}(K_\infty/k_\infty)$. Assume that neither p nor l splits in K. Note that $X(\mathbb{Q}_\infty) = 0$ and

$X(K_\infty^+) = 0$ by Iwasawa [6]. If $A(k) = 0$, then $\tilde{X}(K_\infty) = 1$ again by [6]. Therefore we have only to show that $\tilde{L}(K_\infty) \neq L(K_\infty)$ under the assumption that

$$A(k) \neq 0 \quad \text{and} \quad [K^+ : \mathbb{Q}] = p$$

for proving Theorem 1.1. Moreover, if $\lambda_k \geq 2$, then $\tilde{X}(k_\infty)$ is not abelian by [14], and neither $\tilde{X}(K_\infty)$ is. Therefore we may assume that

$$\lambda_k = \lambda_k^- = 1 \quad \text{and} \quad \lambda_K = \lambda_K^- = p.$$

Since $\lambda_k = 1$, we know $X(k_\infty) \simeq \mathbb{Z}_p$. Moreover, since the only one prime of k_∞ lying above p is totally ramified in k_∞/k, $A(k)$ is a non-trivial cyclic group. Now, we apply Proposition 2.3 to the extension $L(K)/k$:

Lemma 3.1. *With the notation above,* $\tilde{L}(K) = L(K)$ *if and only if* $\dim_{\mathbb{F}_p} A(K) \otimes_{\mathbb{Z}} \mathbb{F}_p \leq 1$.

Proof. Since l does not split in K/K^+, the only one prime lying above l in K splits completely in $L(K)/K$ by the class field theory. Hence the decomposition group in $\mathrm{Gal}(L(K)/k)$ of a prime lying above l in $L(K)$ is cyclic, and so that its Schur multiplier is trivial. Therefore, $\tilde{L}(K) = L(K)$ holds if and only if $H_2(\mathrm{Gal}(L(K)/k), \mathbb{Z}_p) = 0$ by Proposition 2.3. By Evens [1], we have

$$H_2(\mathrm{Gal}(L(K)/k), \mathbb{Z}_p) \simeq H_2(\Delta, \mathbb{Z}_p) \oplus H_1(\Delta, X(K)) \oplus H_2(X(K), \mathbb{Z}_p)_\Delta,$$

since $\mathrm{Gal}(L(K)/k) \simeq X(K) \rtimes \Delta$. If $\dim_{\mathbb{F}_p} A(K) \otimes_{\mathbb{Z}} \mathbb{F}_p \geq 2$, then $H_2(X(K), \mathbb{Z}_p)_\Delta \simeq (A(K) \wedge_{\mathbb{Z}_p} A(K))_\Delta \neq 0$. This implies that $\tilde{L}(K) \neq L(K)$. On the other hand, the sufficiency of the assertion is clear. □

By Lemma 3.1 and the above argument, for proving Theorem 1.1, it is sufficient to show the following proposition:

Proposition 3.2. *Suppose that the following conditions hold*:
(i) *Neither p nor l splits in $K/\mathbb{Q}$,*
(ii) $\lambda_k = 1$ (*hence* $A(k) \neq 0$ *and* $\lambda_K = p$),
(iii) $\dim_{\mathbb{F}_p} A(K) \otimes_{\mathbb{Z}} \mathbb{F}_p = 1$.
Then $\tilde{L}(K_n) \neq L(K_n)$ *for any* $n \geq 1$.

In the rest of this section, for a fixed non-negative integer n, we show Proposition 3.2. Suppose that p, l, k and K satisfy the condition of Proposition 3.2. Our first aim is to describe $G_n := \mathrm{Gal}(L(K_n)/k)$ and some decomposition subgroups. Put $\Gamma_n := \Gamma/\Gamma^{p^n}$ for simplicity. Let $\bar{\gamma}$ a fixed generator of Γ. Identify $\Lambda = \mathbb{Z}_p[[T]]$ with

$\varprojlim \mathbb{Z}_p[\Gamma_n]$ by sending $1+T$ to $\bar{\gamma}$. Since the only one prime lying above p in K is totally ramified in K_∞/K and $A(K)$ is a non-trivial cyclic group, $X(K_\infty)$ is cyclic over Λ. Let ε be a fixed generator of $X(K_\infty)$ over Λ and $\bar{\delta}$ a fixed generator of Δ. Then, since $X(K_\infty^+)=0$, we can apply Proposition 2.1 (ii) to obtain

$$\begin{cases} X(K_\infty)=\Lambda\varepsilon \simeq \Lambda/(P_K(T)) \quad \text{as } \Lambda\text{-modules},\\ X(K_\infty)\simeq \mathbb{Z}_p[\Delta] \quad \text{as } \mathbb{Z}_p[\Delta]\text{-modules},\\ Q(T)/P_k(T)\in\Lambda^\times \quad (\text{since the residue degree of } Q(T) \text{ is } \lambda_k \text{ and } P_k(T)\mid Q(T)),\\ P_k(T)N(T)/P_K(T)\in\Lambda^\times. \end{cases}$$

Here $Q(T)$ is defined by $\varepsilon^{\bar{\delta}}=(Q(T)+1)\varepsilon$ and $N(T)$ is defined as in (3). Let M_n be the maximal abelian subextension in $L(K_n)/k$. We denote by ε_n, $\bar{\varepsilon}_n$ the projection of $\varepsilon\in X(K_\infty)$ to G_n, $G_n^{\mathrm{ab}}:=\mathrm{Gal}(M_n/k)$, respectively. Let $\tilde{\mathfrak{p}}_n$ (resp. $\tilde{\mathfrak{l}}_n$) be a prime in $L(K_n)$ lying above p (resp. l), and $\gamma_n\in G_n$ (resp. δ_n) a generator of the inertia group $I_p\simeq\Gamma_n$ of $\tilde{\mathfrak{p}}_n$ (resp. the inertia group $I_l\simeq\Delta$ of $\tilde{\mathfrak{l}}_n$). Put $\bar{\gamma}_n:=\gamma_n \bmod [G_n,G_n]$, $\bar{\delta}_n:=\delta_n \bmod [G_n,G_n]$. Here $[G,G]$ stands for the topological commutator subgroup of a topological group G, which is generated by $[g,h]:=ghg^{-1}h^{-1}$ for all $g,h\in G$. We may assume that γ_n (resp. δ_n) is an extension of $\bar{\gamma} \bmod \Gamma^{p^n}$ (resp. $\bar{\delta}\in\Delta$). Then $\mathrm{Gal}(K_n/k)$ acts on $X(K_n)=\Lambda\varepsilon_n\simeq\Lambda/(P_K(T),\omega_n(T))$ by

$$\varepsilon_n^{\bar{\gamma}}=\gamma_n\varepsilon_n\gamma_n^{-1}=(1+T)\varepsilon_n,\quad \varepsilon_n^{\bar{\delta}}=\delta_n\varepsilon_n\delta_n^{-1}=(1+Q(T))\varepsilon_n.$$

Lemma 3.3. *As Λ-modules, $[G_n,G_n]\simeq(T,p^m)/(P_K(T),\omega_n(T))$. Also we have*

$$G_n^{\mathrm{ab}}=\langle\bar{\gamma}_n\rangle\oplus\langle\bar{\delta}_n\rangle\oplus\langle\bar{\varepsilon}_n\rangle\simeq\mathbb{Z}/p^n\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^m\mathbb{Z},$$

where m is defined by $\#A(k)=p^m$.

Proof. Note that the maximal abelian subextension in $L(K_n)/K$ is the fixed field by the Galois subgroup corresponding to

$$(T,P_K(T))/(P_K(T),\omega_n(T))=(T,P_K(0))/(P_K(T),\omega_n(T)).$$

Clearly, M_n is contained in the field and also contains K_n. Hence there is some $p^t\le P_K(0)$ such that $[G_n,G_n]\simeq(T,p^t)/(P_K(T),\omega_n(T))$. We show that $t=m$, in other words, $\mathrm{Gal}(M_n/K_n)\simeq\mathbb{Z}/p^m\mathbb{Z}$ for any $n\ge0$. If $n=0$, then M_0 has degree p^m over K by the genus formula [9, Chapter 13 Lemma 4.1]. Denote by M_n' the maximal abelian subextension in M_n/k which is unramified outside l. Clearly $M_0\subset M_n'$. Moreover, we have $M_n'=M_0$ since M_n'/K is unramified and abelian. Since M_n' is the fixed field in M_n by the inertia group of a prime lying above p, $M_n/M_n'K_n$ is totally ramified at the prime. On the other hand, since $M_n'\cap K_n=K$, $M_n/M_n'K_n$ is unramified at every prime. Therefore $M_0K_n = M'_nK_n = M_n$, and $\langle\bar{\varepsilon}_n\rangle = \mathrm{Gal}(M_n/K_n) \simeq \mathbb{Z}/p^m\mathbb{Z}$. Hence we find

$$[G_n, G_n] \simeq (T, p^m)/(P_K(T), \omega_n(T)).$$

Also, by the definitions of $\bar{\gamma}_n$, $\bar{\delta}_n$, $\bar{\varepsilon}_n$, we obtain $\langle\bar{\gamma}_n\rangle \oplus \langle\bar{\delta}_n\rangle \oplus \langle\bar{\varepsilon}_n\rangle \subset G_n^{\mathrm{ab}}$. Comparing each order, we obtain the assertion. □

In fact, γ_n and δ_n are commutative and hence $G_n \simeq X(K_n) \rtimes (\Gamma_n \times \Delta)$. This fact follows from the next lemma. Recall that $p^{e+1} \parallel l-1$. From now on throughout this section, we regard $X(K_n)$ as a subset of G_n and write the operator of $X(K_n)$ multiplicatively.

Lemma 3.4. *Let the subgroups Z_p, Z_l of G_n be the decomposition groups of $\tilde{\mathfrak{p}}_n$, $\tilde{\mathfrak{l}}_n$, respectively. Then, changing $\tilde{\mathfrak{l}}_n$ if necessary, there is some $D(T) \in \Lambda$ defined uniquely up to the modulus $P_K(T)$ such that*

$$Z_p = \langle\gamma_n\rangle \oplus \langle\delta_n\rangle,$$
$$Z_l = \begin{cases} \langle\delta_n\rangle & (\text{if } n \le e),\\ \langle\gamma_n^{p^e}\varepsilon_n^{D(T)N(T)}\rangle \oplus \langle\delta_n\rangle & (\text{if } n > e).\end{cases}$$

Proof. The image of Z_p in G_n^{ab} is generated by $\bar{\gamma}_n$ and $\bar{\delta}_n$. Therefore, Z_p is generated by the generator γ_n of I_p and a pre-image ρ_n of a generator of Z_p/I_p. Moreover, every prime lying above p splits completely in $L(K_n)/K_n$. Hence $Z_p \cap [G_n, G_n] = 1$. This implies that $[\gamma_n, \delta_n] = 1$, and so that Z_p is abelian. Comparing the orders, we see that the natural surjection $Z_p = \langle\gamma_n\rangle \oplus \langle\rho_n\rangle \twoheadrightarrow \langle\bar{\gamma}_n\rangle \oplus \langle\bar{\delta}_n\rangle$ is isomorphic. We can take ρ_n which satisfies $\rho_n \equiv \delta_n \bmod [G_n, G_n]$. It follows from this that there is some $B(T) \in (T, p^m)$ defined up to the modulus $P_K(T)$ such that $\rho_n = \delta_n\varepsilon_n^{B(T)}$. Since

$$1 = \rho_n^p = \varepsilon_n^{N(T)B(T)},$$

we obtain $P_K(T) \mid N(T)B(T)$. Hence $Q(T) \mid B(T)$. On the other hand, let $x := \varepsilon_n^{-(1+Q(T))B(T)/Q(T)}$ (note that $1 + Q(T) \in \Lambda^\times$ since $\varepsilon_n^{1+Q(T)} = \varepsilon_n^{\bar{\delta}_n}$), then

$$x\delta_n x^{-1} = \delta_n\delta_n^{-1}x\delta_n x^{-1} = \delta_n x^{(1+Q(T))^{-1}-1} = \delta_n\varepsilon_n^{B(T)} = \rho_n.$$

Hence δ_n and ρ_n are conjugate each other in G_n, so that we may assume that $\delta_n = \rho_n$, changing $\tilde{\mathfrak{l}}_n$ if necessary. This implies that $B(T) = 0$ and also γ_n and δ_n are commutative.

On the other hand, we deal with Z_l. Suppose that $n \le e$. Then every prime lying above l splits completely in $L(K_n)/K$, so that $Z_l = I_l$. Suppose that $e < n$. Then the image of Z_l in G_n^{ab} is generated by $\bar{\gamma}_n^{p^e}$ and $\bar{\delta}_n$. In the same way as in the above, we see that there is some $C(T) \in (T, p^m)$ defined up to the modulus $P_K(T)$ such that

$$Z_l = \langle \gamma_n^{p^e} \varepsilon_n^{C(T)} \rangle \oplus \langle \delta_n \rangle$$

Since

$$1 = \gamma_n^{p^e} \varepsilon_n^{C(T)} \delta_n \varepsilon_n^{-C(T)} \gamma_n^{-p^e} \delta_n^{-1} = \varepsilon_n^{-(1+T)^{p^e} Q(T)C(T)},$$

we obtain $P_K(T) \mid Q(T)C(T)$ and so that, $D(T) := C(T)/N(T)$ is in Λ. This completes the proof. □

Lemma 3.5. *For any* $n \geq 1$, $\dim_{\mathbb{F}_p} H_2(G_n, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \geq 2$. *If* $e > 0$, *then* $\tilde{L}(K_n) \neq L(K_n)$ *for any* $n \geq 1$.

Proof. Combining the splitting exact sequence

$$1 \to X(K_n) \to G_n \to \Gamma_n \times \Delta \to 1$$

with the result in [1], we obtain

$$H_2(G_n, \mathbb{Z}_p) \simeq H_2(\Gamma_n \times \Delta, \mathbb{Z}_p) \oplus H_1(\Gamma_n \times \Delta, X(K_n)) \oplus H_2(X(K_n), \mathbb{Z}_p)_{\Gamma_n \times \Delta}.$$

We find that $H_2(\Gamma_n \times \Delta, \mathbb{Z}_p) \simeq \mathbb{Z}/p\mathbb{Z}$ again by [1]. On the other hand, we know that $H_1(\Gamma_n, X(K_n)) \simeq \hat{H}^0(\Gamma_n, A(K_n)) = 0$ which follows from the genus formula [9, Chapter 13 Lemma 4.1] and the injection $A(K) \to A(K_n)$ (see [19, Proposition 13.26]). Also, we get

$$H_1(\Delta, X(K_n)_{\Gamma_n}) \cong \hat{H}^0(\Delta, X(K_n)_{\Gamma_n}) \cong (T, P_K(T))/(T, P_K(T)) = 0$$

from $p^m \mid Q(0)$. Therefore the Hochschild–Serre exact sequence

$$H_1(\Gamma_n, X(K_n))_\Delta \to H_1(\Gamma_n \times \Delta, X(K_n)) \to H_1(\Delta, X(K_n)_{\Gamma_n}) \to 0$$

yields the result $H_1(\Gamma_n \times \Delta, X(K_n)) = 0$. We have $H_2(X(K_n), \mathbb{Z}_p)_{\Gamma_n \times \Delta} \neq 0$. Indeed, $X(K_n)$ is not cyclic by $\lambda_K = p$ and Fukuda [4], so that $H_2(X(K_n), \mathbb{Z}_p) \neq 0$ and $H_2(X(K_n), \mathbb{Z}_p)_{\Gamma_n \times \Delta} \neq 0$. This shows the first claim.

We are in the position of proving the second claim. Assume that $e > 0$. Take an integer $n \geq 1$ such that $n \leq e$. Then, for such an n, we have $H_2(Z_l, \mathbb{Z}_p) = 0$ and $H_2(Z_p, \mathbb{Z}_p) \simeq \mathbb{F}_p$. The combination of Proposition 2.3 and the first claim implies that $\tilde{X}(K_n)$ is not abelian and that neither every $\tilde{X}(K_n)$ is $(n \geq 1)$. □

3.2. Group theorical part. We deal with the remaining case where $e = 0$. Assume that $e = 0$. Our next aim is to obtain minimal presentations of G_n, Z_p, Z_l and their Schur multipliers by free pro-p-groups. Let $F := \langle \gamma, \delta, \varepsilon \rangle$ be a free pro-p-group of rank 3. We define the action of a polynomial $f(\gamma) = a_k\gamma^k + \cdots + a_1\gamma + a_0$ ($a_i \in \mathbb{Z}_p$) on F by the product of inner products such as

$$x^{f(\gamma)} := x^{a_k\gamma^k} \cdots x^{a_1\gamma} x^{a_0}.$$

Put

$$R := \langle \gamma^{p^n}, \delta^p, \varepsilon^{P_K(\gamma-1)}, [\delta, \gamma], [\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1}, [\varepsilon, \varepsilon^{\gamma}], [\varepsilon, \varepsilon^{\gamma^2}], \dots, [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}] \rangle_F,$$

where $\langle x, y, \dots \rangle_F$ stands for the closed normal subgroup generated by $x, y, \dots$ and their conjugates. Note that there are equations

$$\begin{aligned} &[x, y]^z = [x^z, y^z],\\ &[x, yz] = [x, y][x, z]^y,\\ &[x, y^k] = [x, y][x, y]^y \cdots [x, y]^{y^{k-1}} \end{aligned}$$

for any $x, y, z \in F$ and any integer $k \geq 1$. We have the following lemma in the same way as in the proof of [14, Lemma 5.3]:

Lemma 3.6. *For arbitrary $z_1, z_2 \in \mathbb{Z}_p$, $i, j \in \mathbb{Z}$,*
(i) $[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}]$ *is congruent with some product of* $[\varepsilon, \varepsilon^{\gamma}], \dots, [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}]$ mod $[R, F]$. *In particular,* $[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}] \in R$.
(ii) $[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^p}] \equiv [\varepsilon, \varepsilon^{\gamma^i}]^{-z_1z_2}$ mod $[R, F](R \cap [F, F])^p$.

Proof. (i) First, we prove the case where $z_1 = z_2 = 1$. We have only to prove the claim that $[\varepsilon^{\gamma^{-k}}, \varepsilon]$ is congruent with some product of $[\varepsilon, \varepsilon^{\gamma}], \dots, [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}]$ mod $[R, F]$ for any non-negative integer k. If $k = 0, \pm 1, \dots, \pm(p-1)/2$, this claim is clear. Fix an integer $k \geq (p-1)/2$ and assume that the claim holds for any non-negative integer i such that $0 \leq i \leq k$. If we put $P_K(\gamma - 1) = \gamma^p + c_{p-1}\gamma^{p-1} + \cdots + c_0$, then we have

$$\begin{aligned} 1 &\equiv [\varepsilon^{\gamma^{-k+(p-1)}}, (\varepsilon^{-P_K(\gamma-1)})^{-1}] = [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_0}\varepsilon^{c_1\gamma} \cdots \varepsilon^{\gamma^p}]\\ &= [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_0}][\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_1\gamma} \cdots \varepsilon^{\gamma^p}]^{\varepsilon^{c_0}}\\ &\equiv [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon]^{c_0}[\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_1\gamma} \cdots \varepsilon^{\gamma^p}]^{\varepsilon^{c_0}} \quad \text{mod } [R, F], \end{aligned}$$

since $-(p-1)/2 \leq k - (p-1) < k$. Hence $[\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_1\gamma} \cdots \varepsilon^{\gamma^p}] \in R$ and so that, in the same way, we obtain

$$\begin{aligned} 1 &\equiv [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon]^{c_0}[\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon^{c_1\gamma} \cdots \varepsilon^{\gamma^p}]\\ &= [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon]^{c_0}[\varepsilon^{\gamma^{-k+(p-2)}}, \varepsilon^{c_1} \cdots \varepsilon^{\gamma^{p-1}}]^{\gamma}\\ &\cdots \end{aligned}$$

$$\begin{aligned}
&\equiv [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon]^{c_0}[\varepsilon^{\gamma^{-k+(p-2)}}, \varepsilon]^{c_1\gamma} \cdots [\varepsilon^{\gamma^{-k}}, \varepsilon]^{c_{p-1}\gamma^{p-1}}[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon]^{\gamma^p} \\
&\equiv [\varepsilon^{\gamma^{-k+(p-1)}}, \varepsilon]^{c_0}[\varepsilon^{\gamma^{-k+(p-2)}}, \varepsilon]^{c_1} \cdots [\varepsilon^{\gamma^{-k}}, \varepsilon]^{c_{p-1}}[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon]^{\gamma^p} \mod [R, F].
\end{aligned}$$

Therefore we obtain $[\varepsilon^{\gamma^{-(k+1)}},\varepsilon]^{\gamma^p} \in R$ and so that $[\varepsilon^{\gamma^{-(k+1)}},\varepsilon]^{\gamma^p} \equiv [\varepsilon^{\gamma^{-(k+1)}},\varepsilon] \bmod [R,F]$. This implies that the claim holds. The general case where any $z_1, z_2 \in \mathbb{Z}_p$ follows from this, since, taking the limit later if necessary, we may assume that $1 \le z_1, z_2 \in \mathbb{Z}$.

(ii) We have only to prove the case where $z_1 = z_2 = 1$, since the general case follows from this immediately. For a polynomial

$$\begin{aligned}
f(\gamma - 1) &= a_k\gamma^k + \cdots + a_1\gamma + a_0 \\
&= b_k(\gamma - 1)^k + \cdots + b_1(\gamma - 1) + b_0 \quad (a_i, b_i \in \mathbb{Z}_p),
\end{aligned}$$

we obtain that

$$a_i = \sum_{j=0}^{k} \binom{j}{i} (-1)^{j-i} b_j,$$

where we define $\binom{j}{i} = 0$ if $j < i$. And, in the same way as in the proof of (i), we obtain that

$$\begin{aligned}
[\varepsilon^{\gamma^i}, \varepsilon^{f(\gamma-1)}] &= [\varepsilon^{\gamma^i}, \varepsilon^{a_k\gamma^k+\cdots+a_1\gamma+c_0}] \\
&\equiv [\varepsilon^{\gamma^i}, \varepsilon^{\gamma^k}]^{a_k} \cdots [\varepsilon^{\gamma^i}, \varepsilon^{\gamma}]^{a_1}[\varepsilon^{\gamma^i}, \varepsilon]^{a_0} \mod [R, F],
\end{aligned}$$

since $[\varepsilon^{\gamma^i}, \varepsilon^{\gamma^j}] \in R$. Now, if $f(\gamma - 1) = P_K(\gamma - 1)$, then $b_p = 1$ and $b_{p-1} \equiv \cdots \equiv b_0 \equiv 0 \bmod p$, so that we obtain

$$a_i \equiv \begin{cases} -1 \bmod p & (\text{if } i = 0), \\ 1 \bmod p & (\text{if } i = p), \\ 0 \bmod p & (\text{otherwise}). \end{cases}$$

Therefore we have $1 \equiv [\varepsilon^{\gamma^i}, \varepsilon^{P_K(\gamma-1)}] \equiv [\varepsilon^{\gamma^i}, \varepsilon^{\gamma^p}][\varepsilon^{\gamma^i}, \varepsilon]^{-1} \bmod [R,F](R \cap [F,F])^p$. $\square$

Lemma 3.7. *Let $x \in F$. Then, for any polynomial $f(T) \in \mathbb{Z}_p[T]$ and any non-negative integer k, we have*

$$[x, (\varepsilon^{f(\gamma-1)})^{\delta^k}] \equiv [x, \varepsilon^{f(\gamma-1)(Q(\gamma-1)+1)^k}] \mod [R, F],$$

where the action of a product of polynomials $f(\gamma)$, $g(\gamma)$ is defined as

$$x^{f(\gamma)g(\gamma)} := x^{a_k\gamma^k} \cdots x^{a_1\gamma} x^{a_0} \quad \textit{if} \ \ f(\gamma)g(\gamma) = a_k\gamma^k + \cdots + a_1\gamma + a_0.$$

Proof. If $k = 0$, then the congruence holds. Suppose that the congruence holds for some k. Note that, by $[\delta, \gamma] \in R$ and Lemma 3.6 (i), the congruences $[x, (\varepsilon^{\gamma^i})^{\delta}] \equiv$

$[x, (\varepsilon^{\delta})^{\gamma^i}]$ and $[x, \varepsilon^{\gamma^i}\varepsilon^{\gamma^j}] = [x, [\varepsilon^{\gamma^i}, \varepsilon^{\gamma^j}]\varepsilon^{\gamma^j}\varepsilon^{\gamma^i}] \equiv [x, \varepsilon^{\gamma^j}\varepsilon^{\gamma^i}] \bmod [R, F]$ hold for arbitrary $i, j \in \mathbb{Z}$. Hence we have

$$
\begin{aligned}
[x, (\varepsilon^{f(\gamma-1)})^{\delta^{k+1}}] &\equiv [x, ((\varepsilon^{\delta})^{f(\gamma-1)})^{\delta^k}] \\
&\equiv [x, ((\varepsilon^{Q(\gamma-1)+1})^{f(\gamma-1)})^{\delta^k}] \quad (\text{by } [\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1} \in R), \\
&\equiv [x, (\varepsilon^{f(\gamma-1)(Q(\gamma-1)+1)})^{\delta^k}] \\
&\equiv [x, \varepsilon^{f(\gamma-1)(Q(\gamma-1)+1)^{k+1}}] \mod [R, F] \text{ (by the assumption).}
\end{aligned}
$$

Therefore the congruence holds for any k by induction. □

Lemma 3.8. *For $n \geq 1$, the sequence of pro-p-groups $1 \to R \to F \xrightarrow{\phi} G_n \to 1$ is exact, where the map $\phi\colon F \to G_n$ is given by $\gamma \mapsto \gamma_n$, $\delta \mapsto \delta_n$, $\varepsilon \mapsto \varepsilon_n$.*

Proof. It is clear that $R \subset \operatorname{Ker}\phi$ and ϕ is surjective, so that we have the surjective maps

$$F/[F, F]R = (F/R)^{\mathrm{ab}} \twoheadrightarrow G_n^{\mathrm{ab}}, \quad [F, F]R/R = [F/R, F/R] \twoheadrightarrow [G_n, G_n].$$

We prove that these two maps are isomorphisms. We know that $[F, F]$ is generated by $[\delta, \gamma]$, $[\gamma, \varepsilon] = \varepsilon^{\gamma-1}$, $[\delta, \varepsilon]$ and their conjugates. Hence, using $[\delta, \varepsilon] \equiv \varepsilon^{Q(\gamma-1)} \bmod R$ and Lemma 3.6 (i), we see that $[F, F]R/R$ is generated by $\varepsilon^{\gamma-1}$ and $\varepsilon^{Q(0)} \bmod R$ and their conjugates. But, by the congruences

$$(\varepsilon^{\gamma-1})^{\varepsilon} \equiv \varepsilon^{\gamma-1}, \quad (\varepsilon^{Q(0)})^{\delta} \equiv (\varepsilon^{Q(0)})^{Q(\gamma-1)+1}, \quad (\varepsilon^{\gamma-1})^{\delta} \equiv (\varepsilon^{\gamma-1})^{Q(\gamma-1)+1} \mod R$$

and $\varepsilon^{\omega_n(\gamma-1)} \equiv 1 \bmod R$ which follows from $T \mid \omega_n(T)$, we obtain

$$
\begin{aligned}
[F, F]R/R &= \langle (\varepsilon^{\gamma-1})^{F(\gamma-1)}, (\varepsilon^{p^m})^{F(\gamma-1)} \mid F(T) \in \Lambda \rangle R/R \\
&= \langle \varepsilon^{F(\gamma-1)} \mid F(T) \in (T, p^m) \rangle R/R.
\end{aligned}
$$

Then the surjective map

$$[G_n, G_n] \simeq (T, p^m)/(P_K(T), \omega_n(T)) \twoheadrightarrow [F, F]R/R$$

is induced and hence $[F, F]R/R \simeq [G_n, G_n]$. Finally $F/[F, F]R$ is generated by the classes of $\gamma, \delta, \varepsilon$ which are annihilated by p^n, p, p^m, respectively. Therefore we have $\#(F/[F, F]R) \leq \#G_n^{\mathrm{ab}}$ and so that $F/[F, F]R \simeq G_n^{\mathrm{ab}}$. □

Lemma 3.9.

$$R/[R, F] = \langle \gamma^{p^n}, \delta^p, [\delta, \gamma], [\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1}, [\varepsilon, \varepsilon^{\gamma}], \ldots, [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}] \rangle [R, F]/[R, F].$$

Proof. Throughout the proof, the notation $\equiv$ is used for a congruence modulo the right hand side of the above equation. It is sufficient to show that $\varepsilon^{P_K(\gamma-1)} \equiv 1$. By Lemmas 3.6 and 3.7, we have

$$\begin{aligned}[\delta, \varepsilon]^{\delta^k} &= [\delta, \varepsilon^{\delta^k}] \equiv [\delta, \varepsilon^{(Q(\gamma-1)+1)^k}] \\ &\equiv (\varepsilon^{\delta})^{(Q(\gamma-1)+1)^k}(\varepsilon^{-1})^{(Q(\gamma-1)+1)^k} \\ &\equiv (\varepsilon^{(Q(\gamma-1)+1)})^{(Q(\gamma-1)+1)^k}(\varepsilon^{-1})^{(Q(\gamma-1)+1)^k} \\ &\equiv \varepsilon^{Q(\gamma-1)(Q(\gamma-1)+1)^k}.\end{aligned}$$

Therefore $1 \equiv [\delta^p, \varepsilon] = [\delta, \varepsilon]^{\delta^{p-1}} \cdots [\delta, \varepsilon]^{\delta}[\delta, \varepsilon] \equiv \varepsilon^{Q(\gamma-1)N(\gamma-1)}$. Since $Q(T)N(T) = P_K(T)F(T)$ with some polynomial $F(T) \in \Lambda^{\times}$, we have $1 \equiv \varepsilon^{P_K(\gamma-1)F(\gamma-1)} \equiv (\varepsilon^{P_K(\gamma-1)})^{F(0)}$. Hence $\varepsilon^{P_K(\gamma-1)} \equiv 1$. $\square$

Recall that $D(T) \in \Lambda$ is defined in Lemma 3.4. The closed subgroups $F_p := \langle \gamma, \delta \rangle$, $F_l := \langle \gamma(\varepsilon^{\delta^{p-1}+\cdots+\delta+1})^{D(\gamma-1)}, \delta \rangle$ of F and their closed normal subgroups

$$\begin{aligned}R_p &:= \langle \gamma^{p^n}, \delta^p, [\delta, \gamma] \rangle_{F_p}, \\ R_l &:= \langle (\gamma(\varepsilon^{\delta^{p-1}+\cdots+1})^{D(\gamma-1)})^{p^n}, \delta^p, [\delta, \gamma(\varepsilon^{\delta^{p-1}+\cdots+1})^{D(\gamma-1)}] \rangle_{F_l}\end{aligned}$$

give minimal presentations $1 \to R_p \to F_p \to Z_p \to 1$ of Z_p and $1 \to R_l \to F_l \to Z_l \to 1$ of Z_l. The Hochschild–Serre exact sequence with respect to the minimal presentation of G_n induces the isomorphism $H_2(G_n, \mathbb{Z}_p) \simeq R \cap [F, F]/[R, F]$. Therefore $H_2(G_n, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \simeq (R_p \cap [F_p, F_p])/([R_p, F_p](R_p \cap [F_p, F_p])^p)$. Hence, for completing the proof of Proposition 3.2, it is sufficient to show the map

$$\Phi\colon \frac{R_p \cap [F_p, F_p]}{[R_p, F_p](R_p \cap [F_p, F_p])^p} \times \frac{R_l \cap [F_l, F_l]}{[R_l, F_l](R_l \cap [F_l, F_l])^p} \to \frac{R \cap [F, F]}{[R, F](R \cap [F, F])^p}$$

is not surjective by Proposition 2.3.

Lemma 3.10. *The followings hold*:
(i) $R \cap [F, F]/[R, F] = \langle [\delta, \gamma], [\varepsilon, \varepsilon^{\gamma}], \dots, [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}] \rangle [R, F]/[R, F]$,
(ii) $R_p \cap [F_p, F_p]/[R_p, F_p] = \langle [\delta, \gamma] \rangle [R_p, F_p]/[R_p, F_p]$,
(iii) $R_l \cap [F_l, F_l]/[R_l, F_l] = \langle [\delta, \gamma(\varepsilon^{\delta^{p-1}+\cdots+1})^{D(\gamma-1)}] \rangle [R_l, F_l]/[R_l, F_l]$.

Proof. We show only (i) because the remainder are shown in the same way. For any $x \in R \cap [F, F] \subset R$, there exist $z_1, \dots, z_{4+(p-1)/2} \in \mathbb{Z}_p$ such that

$$x \equiv (\gamma^{p^n})^{z_1}(\delta^p)^{z_2}[\delta, \gamma]^{z_3}([\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1})^{z_4}[\varepsilon, \varepsilon^{\gamma}]^{z_5} \cdots [\varepsilon, \varepsilon^{\gamma^{(p-1)/2}}]^{z_{4+(p-1)/2}} \mod [R, F]$$

by Lemma 3.9. Hence we obtain $1 \equiv \gamma^{p^n z_1}\delta^{p z_2}\varepsilon^{-Q(0)z_4} \mod [F, F]$, and so that $z_1 = z_2 = z_4 = 0$. This shows (i). $\square$

We now conclude our proof. Put $d := \varepsilon^{Q(\gamma-1)}$ for convenience. By Lemma 3.10, it is sufficient to show that $[\delta, \gamma]$ and $[\delta, (\varepsilon^{\delta^{p-1}+\cdots+\delta+1})^{D(\gamma-1)}]$ do not generate $(R \cap [F, F])/([R, F](R \cap [F, F])^p)$. By induction, we have

$$\varepsilon^{\delta^k} \equiv ([\delta, \varepsilon]d^{-1})^k d^{\delta^{k-1}+\cdots+\delta+1}\varepsilon \mod [R, F] \ (k \geq 1).$$

Indeed, by the assumption of the induction,

$$\begin{aligned}(\varepsilon^{\delta^{k-1}})^\delta &\equiv ([\delta, \varepsilon]d^{-1})^{k-1} d^{\delta^{k-1}+\cdots+\delta}\varepsilon^\delta \\ &\equiv ([\delta, \varepsilon]d^{-1})^{k-1} d^{\delta^{k-1}+\cdots+\delta}([\delta, \varepsilon]d^{-1})d\varepsilon \\ &\equiv ([\delta, \varepsilon]d^{-1})^k d^{\delta^{k-1}+\cdots+\delta+1}\varepsilon \mod [R, F].\end{aligned}$$

Using $([\delta, \varepsilon]d^{-1})^k \in R$ and this congruence, we obtain

$$\begin{aligned}&[\delta, \varepsilon^{\delta^{p-1}+\cdots+\delta+1}] \\ &= \delta(\varepsilon^{\delta^{p-1}} \cdots \varepsilon^\delta\varepsilon)\delta^{-1} \times (\varepsilon^{-1}\varepsilon^{-\delta}\varepsilon^{-\delta^2} \cdots \varepsilon^{-\delta^{p-1}}) \\ &= \varepsilon^{\delta^p}\varepsilon^{\delta^{p-1}} \cdots \varepsilon^{\delta^2}\varepsilon^\delta \times \varepsilon^{-1}\varepsilon^{-\delta}\varepsilon^{-\delta^2} \cdots \varepsilon^{-\delta^{p-1}} \\ &\equiv \varepsilon(d^{\delta^{p-2}+\cdots+1}\varepsilon) \cdots (d^{\delta+1}\varepsilon)(d\varepsilon) \times \varepsilon^{-1}(d\varepsilon)^{-1}(d^{\delta+1}\varepsilon)^{-1} \cdots (d^{\delta^{p-2}+\cdots+1}\varepsilon)^{-1} \\ &= [\varepsilon, (d^{\delta^{p-2}+\cdots+1}\varepsilon) \cdots (d^{\delta+1}\varepsilon)d] \\ &\equiv [\varepsilon, d^{\delta^{p-2}}][\varepsilon, d^{\delta^{p-3}}]^2 \cdots [\varepsilon, d^\delta]^{p-2}[\varepsilon, d]^{p-1} \mod [R, F],\end{aligned}$$

where the last congruence is obtained from $[\varepsilon, d^{\delta^k}] = [\varepsilon, (\varepsilon^{Q(\gamma-1)})^{\delta^k}] \in R$ by Lemmas 3.6 (i) and 3.7. Moreover, using

$$\sum_{k=0}^{p-2}(p-1-k)Q(T)(Q(T)+1)^k = N(T) - p$$

and again Lemma 3.7, we have

$$\begin{aligned}[\delta, \varepsilon^{\delta^{p-1}+\cdots+\delta+1}] &\equiv \prod_{k=0}^{p-2}[\varepsilon, \varepsilon^{Q(\gamma-1)(Q(\gamma-1)+1)^k}]^{p-1-k} \\ &\equiv [\varepsilon, \varepsilon^{N(\gamma-1)}] \mod [R, F].\end{aligned}$$

Now, dividing $N(T)$ by the distinguished polynomial $P_K(T)$, we write

$$\begin{aligned}N(\gamma-1) &= a_{p-1}\gamma^{p-1} + \cdots + a_0 + P_K(\gamma-1)f(\gamma-1) \\ &= b_{p-1}(\gamma-1)^{p-1} + \cdots + b_0 + P_K(\gamma-1)f(\gamma-1) \quad (a_i, b_i \in \mathbb{Z}_p).\end{aligned}$$

Then $b_0 \equiv \cdots \equiv b_{p-2} \equiv 0 \bmod p$ since the residue degree of $N(T)$ is $p-1$ by (5). Therefore, in the same way as in the proof of Lemma 3.7, we get

$$[\varepsilon, \varepsilon^{N(\gamma-1)}] \equiv [\varepsilon, \varepsilon^{\gamma^{p-1}}]^{a_{p-1}} \cdots [\varepsilon, \varepsilon^{\gamma}]^{a_1}[\varepsilon, \varepsilon]^{a_0} \mod [R, F]$$

and $a_i = \sum_{j=0}^{p-1} \binom{j}{i}(-1)^{j-i} b_j \equiv (-1)^i \binom{p-1}{i} b_{p-1} \bmod p$. Finally, for $1 \le i \le (p-1)/2$,

$$[\varepsilon, \varepsilon^{\gamma^i}]^{a_i} \equiv [\varepsilon^{\gamma^p}, \varepsilon^{\gamma^i}]^{a_i} \equiv [\varepsilon, \varepsilon^{\gamma^{p-i}}]^{-a_i} \mod [R, F](R \cap [F, F])^p$$

by Lemma 3.6 (ii) and $a_{p-i} - a_i \equiv \binom{p}{i}(-1)^{i+1} b_{p-1} \equiv 0 \bmod p$. Therefore we obtain

$$\begin{aligned}[\delta, \varepsilon^{\delta^{p-1}+\cdots+\delta+1}] &\equiv \prod_{i=1}^{p-1}[\varepsilon, \varepsilon^{\gamma^{p-i}}]^{a_{p-i}} = \prod_{i=1}^{(p-1)/2} [\varepsilon, \varepsilon^{\gamma^{p-i}}]^{a_{p-i}}[\varepsilon, \varepsilon^{\gamma^i}]^{a_i} \\ &\equiv 1 \mod [R, F](R \cap [F, F])^p.\end{aligned}$$

By Lemma 3.5, this implies that Φ is not surjective, which completes the proof of Proposition 3.2.

EXAMPLE. Let $p = 3$, $k = \mathbb{Q}(\sqrt{-31})$ and K^+ an abelian p-extension of $\mathbb{Q}$ with conductor $l = 43$. Then $A(k) \simeq \mathbb{Z}/3\mathbb{Z}$, $\lambda_k = 1$, $A(K) \simeq \mathbb{Z}/9\mathbb{Z}$ and $\lambda_K = 3$. They satisfy the condition of Proposition 3.2. Therefore $\tilde{X}(K_n)$ is not abelian for any $n \ge 1$.

4. Proof of Theorem 1.2

Since the strategy of the proof of Theorem 1.2 is similar to the proof of Theorem 1.1, we explain briefly. Let p, l be odd prime numbers such that $p \parallel l - 1$ (later, we assume that $p = 3$), k an imaginary quadratic field with the property that $k \neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$, and K^+ the unique abelian p-extension of $\mathbb{Q}$ with conductor l. Put $K := kK^+$. Assume that p does not split in K, but l splits in k and $\dim_{\mathbb{F}_p} A(K) \otimes_{\mathbb{Z}} \mathbb{F}_p = 1$. We may assume that $\lambda_k = \lambda_k^- \le 1$ similarly as in §3 by [14]. Then $\lambda_K = \lambda_K^- = p\lambda_k + p - 1$, $X(K_\infty)$ is cyclic over Λ and $\#A(K) = p^{m+1}$. Here m is defined by $\#A(k) = p^m$ by Corollary 2.2. Let $\tilde{\mathfrak{p}}_n$ (resp. $\tilde{\mathfrak{l}}_n$) be a prime in $L(K_n)$ lying above p (resp. l). We define $J \in \mathrm{Gal}(L(K_n)/K_n^+)$ as an element of order 2 in the decomposition subgroup of $\tilde{\mathfrak{p}}_n$ in $\mathrm{Gal}(L(K_n)/K_n^+)$. Then a prime $\tilde{\mathfrak{l}}_n^J$ in $L(K_n)$ is a conjugate of $\tilde{\mathfrak{l}}_n$ and the principal ideal (l) in k splits as $(l) = \mathfrak{l}\mathfrak{l}^J$, where $\mathfrak{l} := \tilde{\mathfrak{l}}_n \cap k$. We use the notation as in §3; namely, $\Gamma = \langle \bar{\gamma} \rangle$, Γ_n, $\Delta = \langle \bar{\delta} \rangle$, G_n, γ_n, $\bar{\gamma}_n$, δ_n, $\bar{\delta}_n$, ε_n, $\bar{\varepsilon}_n$.

Lemma 4.1. *The primes $\mathfrak{l}$ and $\mathfrak{l}^J$ do not split in $L(K)/K$.*

Proof. By the genus formula [9, Chapter 13 Lemma 4.1], the maximal abelian subextension in $L(K)/k$ has degree p^{m+1} over K. Therefore it coincides with $L(K)$

and so that $G_0 \simeq A(K) \oplus \Delta$. Let F be a free pro-p-group of rank 2 generated by the symbols δ, ε and $R := \langle \delta^p, \varepsilon^{p^{m+1}}, [\delta, \varepsilon] \rangle_F$. Then $G_0 \simeq F/R$, and so that $H_2(G_0, \mathbb{Z}_p) \simeq \langle [\delta, \varepsilon] \rangle [R, F]/[R, F]$. On the other hand, the decomposition group of $\tilde{\mathfrak{l}}_0$ (resp. $\tilde{\mathfrak{l}}_0^J$) in G_0 is $\langle \delta_0 \rangle \oplus \langle \varepsilon_0^v \rangle$ (resp. $\langle \delta_0 \varepsilon_0^u \rangle \oplus \langle \varepsilon_0^v \rangle$ since $\tilde{\mathfrak{l}}_0^J$ is ramified in K/k) for some $u, v \in \mathbb{Z}_p$. Since $\tilde{L}(K) = L(K)$ by the cyclicity of $A(K)$, applying Proposition 2.3, we have $v \in \mathbb{Z}_p^\times$. This implies that the decomposition groups equal to G_0. Hence $\mathfrak{l}$ and $\mathfrak{l}^J$ do not split in $L(K)/K$. Also, note that the p-adic order of u is equal to m, since the fixed field of $\langle \delta_0, \varepsilon_0^u \rangle$ is the maximal subextension $L(k)$ which is unramified at $\tilde{\mathfrak{l}}_0$, $\tilde{\mathfrak{l}}_0^J$. □

We use the notation $Q(T)$, $N(T)$ as in §3. Fix $n \geq 1$. Since the next lemma is shown in the way similar to Lemmas 3.3, we omit the proofs.

Lemma 4.2. *As Λ-modules, $[G_n, G_n] \simeq (T, p^{m+1})/(P_K(T), \omega_n(T))$. Moreover $G_n^{\mathrm{ab}} = \langle \bar{\gamma}_n \rangle \oplus \langle \bar{\delta}_n \rangle \oplus \langle \bar{\varepsilon}_n \rangle \simeq \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^{m+1}\mathbb{Z}$.*

We define $A(T) \in \Lambda$ by $[\delta_n, \gamma_n] = \varepsilon_n^{A(T)}$. Note that $A(T)$ is defined uniquely up to the modulus $P_K(T)$.

Lemma 4.3. (i) *Let the subgroup Z_p of G_n be the decomposition group of $\tilde{\mathfrak{p}}_n$. Then there is an element $B(T) \in (p^m, T)$ defined uniquely up to the modulus $P_K(T)$ such that*

$$Z_p = \langle \gamma_n \rangle \oplus \langle \delta_n \varepsilon_n^{B(T)} \rangle, \quad P_K(T) \mid -A(T) + T(1 + Q(T))B(T).$$

Therefore the exact sequence $1 \to X(K_n) \to G_n \to \Gamma_n \times \Delta \to 1$ splits.
(ii) *Let $Z_{\mathfrak{l}}$, $Z_{\mathfrak{l}}^J$ be the decomposition groups of $\tilde{\mathfrak{l}}_n$ and $\tilde{\mathfrak{l}}_n^J$, respectively. Then, changing ε_n, if necessary, there is an element $J(T) \in (p^m, T)$ defined uniquely up to the modulus $P_K(T)$ such that*

$$Z_{\mathfrak{l}} = \langle \gamma_n \varepsilon_n^{-1/(1+T)} \rangle \oplus \langle \delta_n \rangle, \quad P_K(T) \mid A(T) - Q(T),$$
$$Z_{\mathfrak{l}}^J = \langle \gamma_n \varepsilon_n^{1/(1+T)} \rangle \oplus \langle \delta_n \varepsilon_n^{J(T)} \rangle, \quad P_K(T) \mid -A(T) - Q(T) + T(1 + Q(T))J(T)$$

for any $n \geq m+1$ and $J(0) \equiv u \bmod p^{m+1}$. Here u is defined in the proof of Lemma 4.1.

Proof. The image of Z_p in G_n^{ab} is generated by $\bar{\gamma}_n$ and $\bar{\delta}_n \bar{\varepsilon}_n^w$ for some $w \in p^m\mathbb{Z}_p$ (In fact, $w \not\equiv 0$, $w \not\equiv v \bmod p^{m+1}$, since the image $\langle \bar{\delta}_0 \bar{\varepsilon}_0^w \rangle$ under a projection of Z_p in G_0^{ab} coincide neither the inertia groups of $\tilde{\mathfrak{l}}_0$ nor of $\tilde{\mathfrak{l}}_0^J$). Since every primes lying above p split completely in $L(K_n)/K_n$, in the same way as in the proof of Lemma 3.4, there is some $B(T) \in (p^m, T)$ defined up to the modulus $P_K(T)$ such that $B(0) \equiv w \bmod p^{m+1}$ and

$$Z_p = \langle \gamma_n \rangle \oplus \langle \delta_n \varepsilon_n^{B(T)} \rangle \simeq \langle \bar{\gamma}_n \rangle \oplus \langle \bar{\delta}_n \bar{\varepsilon}_n^w \rangle.$$

Hence, we obtain $P_K(T) \mid -A(T) + T(1 + Q(T))B(T)$ since

$$1 = \gamma_n \delta_n \varepsilon_n^{B(T)} \gamma_n^{-1} \varepsilon_n^{-B(T)} \delta_n^{-1} = \varepsilon_n^{-A(T)+T(1+Q(T))B(T)}.$$

(ii) Put $n \geq m + 1$. Since $\mathfrak{l}$ does not split in K_∞/K, $\mathfrak{l}$ splits in $L(K_n)^{[G_n,G_n]}/K_n$ completely by Lemmas 4.1 and 4.2. There the image of Z_l in G_n^{ab} is generated by $\bar{\delta}_n$ and $\bar{\gamma}_n \bar{\varepsilon}_n^v$, where $v \in \mathbb{Z}_p^\times$ is defined in the proof of Lemma 4.1. Hence Z_l is generated by δ_n and $\gamma_n \varepsilon_n^{v+C(T)}$ for some $C(T) \in (p^{m+1}, T)$. Moreover, since $\langle \delta_n \rangle \lhd Z_l$ and $[G_n, G_n] \cap \langle \delta_n \rangle = 1$, we find

$$Z_{\mathfrak{l}} = \langle \gamma_n \varepsilon_n^{v+C(T)} \rangle \oplus \langle \delta_n \rangle, \quad P_K(T) \mid A(T) + Q(T)(1+T)(v + C(T)).$$

The decomposition group of $\tilde{\mathfrak{l}}_n^J$ is given by $Z_{\mathfrak{l}}^J = \langle J(\gamma_n \varepsilon_n^{v+C(T)}) J^{-1} \rangle \oplus \langle J \delta_n J \rangle$. We find $JxJ^{-1} + x = 0$ for any $x \in X(K_n)$ since $A(K_n^+) = 0$. Also we find $J\gamma_n J^{-1} = \gamma_n$ since the natural projection from the decomposition group of $\tilde{\mathfrak{p}}_n$ in $\mathrm{Gal}(L(K_n)/K^+)$ to the abelian group $\mathrm{Gal}(K_n/K^+)$ is an isomorphism. On the other hand, $\langle J\delta_n J \rangle$ is the inertia group of $\tilde{\mathfrak{l}}_n^J$, so that we may assume, changing u if necessary, that the image of a projection of $J\delta_n J$ in G_n^{ab} is $\bar{\delta}_n \bar{\varepsilon}_n^u$. Hence $J\delta_n J$ can be written as $\delta_n \varepsilon_n^{u+j(T)}$ with some element $j(T) \in (p^{m+1}, T)$. Therefore we have

$$\begin{aligned} &Z_{\mathfrak{l}}^J = \langle \gamma_n \varepsilon_n^{-(v+C(T))} \rangle \oplus \langle \delta_n \varepsilon_n^{J(T)} \rangle, \\ &P_K(T) \mid -A(T) + Q(T)(1+T)(v + C(T)) + T(1 + Q(T))J(T), \end{aligned}$$

where $J(T) := u + j(T)$. Since $v \in \mathbb{Z}_p^\times$, changing ε_n, if necessary, we may assume that $v + C(T) = -1/(1+T)$, which completes the proof. □

By Lemmas 4.3, we may assume that $A(T) = Q(T)$ and $J(T) \equiv 2B(T) \bmod P_K(T)$ since $T \nmid P_K(T)$. Now, we fix $Q(T)$ to simplify the proof. Since the residue degree of $Q(T)$ is $\lambda_k + 1 > \deg P_k(T)$ and $P_k(T) \mid Q(T)$, we obtain $p^{m+1} \mid Q(0)$. Therefore, changing the representation of $Q(T) \bmod P_K(T)$ for vanishing the constant term if necessary, we may assume that

$$T \mid Q(T), \quad \deg Q(T) \leq \lambda_K,$$

since $p^{m+1} \parallel P_K(0)$. Also, dividing by the distinguished polynomial $P_K(T)$, we may assume that $\deg J(T) = \deg B(T) \leq \lambda_K - 1$. Note that the differentials $Q'(T)$, $J'(T)$ modulo the ideal (p, T) of $Q(T)$, $J(T)$ are independent of the choices of $Q(T)$ and $J(T)$. By Lemma 4.3, there is an element $F(T) \in \Lambda$ such that

$$J(T)(1 + Q(T)) - 2\frac{Q(T)}{T} = P_K(T)F(T).$$

Put $T = 0$, and on the other hand, differentiate at $T = 0$. Then we have

$$u \equiv 2Q'(0) \bmod p, \quad J'(0) \equiv -2Q'(0)^2 + Q''(0) \bmod p. \tag{6}$$

In the following, we suppose that $p = 3$ and $A(k) = 0$; in other words, suppose that the assumption in Theorem 1.2 holds. Then $m = 0$, $\lambda_K = 2$ and $u \in \mathbb{Z}_3^\times$.

Lemma 4.4. $\dim_{\mathbb{F}_3} H_2(G_n, \mathbb{Z}_3) \otimes_{\mathbb{Z}_3} \mathbb{F}_3 = 3$ *for* $n \geq 1$.

Proof. Since $G_n \simeq X(K_n) \rtimes (\Gamma_n \times \Delta)$ by Lemma 4.3, in the same way as in the proof of Lemma 3.5, we obtain this lemma. Note that $H_2(X(K_\infty), \mathbb{Z}_3) \simeq I_\Delta \wedge_{\mathbb{Z}_3} I_\Delta \simeq \mathbb{Z}_3$ since $p = 3$ and $X(K_\infty) \simeq I_\Delta$ by Proposition 2.1. $\square$

We write

$$Q(T) = T(q_1 T + q_1 + q_0) \quad (q_1, q_0 \in \mathbb{Z}_3).$$

Then $Q(\gamma - 1) = (\gamma - 1)(q_1\gamma + q_0) = q_1\gamma^2 + (q_0 - q_1)\gamma - q_0$. Note that $q_1 + q_0 \in \mathbb{Z}_3^\times$ since the residue degree of $Q(T)$ is equal to 1. Let $F := \langle \gamma, \delta, \varepsilon \rangle$ be a free pro-p-group of rank 3. Put

$$R := \langle \gamma^{3^n}, \delta^3, \varepsilon^{P_K(\gamma-1)}, [\delta, \gamma](\varepsilon^{Q(\gamma-1)})^{-1}, [\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1}, [\varepsilon, \varepsilon^\gamma] \rangle_F$$

and $C := [\delta, \gamma](\varepsilon^{Q(\gamma-1)})^{-1}$, $D := [\delta, \varepsilon](\varepsilon^{Q(\gamma-1)})^{-1}$. Then, since $\lambda_K \leq 3$, we obtain the same result as in [14, Lemma 5.3 (ii)] which is stronger than Lemma 3.6:

$$[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}] \equiv [\varepsilon, \varepsilon^\gamma]^{z_1 z_2 (j-i)} \mod (R \cap [F, F])^3[R, F]. \tag{7}$$

In the following, *the notation* $\equiv$ *is used for a congruence modulo* $(R \cap [F, F])^3[R, F]$.

Lemma 4.5. (i) *For* $n \geq 1$, *the sequence of pro-*p*-groups* $1 \to R \to F \xrightarrow{\phi} G_n \to 1$ *is exact, where the map* $\phi\colon F \to G_n$ *is given by* $\gamma \mapsto \gamma_n$, $\delta \mapsto \delta_n$, $\varepsilon \mapsto \varepsilon_n$.
(ii) $R \cap [F, F]/[R, F] = \langle [\varepsilon, \varepsilon^\gamma], C, D \rangle [R, F]/[R, F]$.

Proof. Using (7), we find $C, D \in R \cap [F, F]$ since $T \mid Q(T)$. Then, in the same way as in the proofs of Lemmas 3.8 and 3.10, we obtain the lemma. $\square$

Lemma 4.6. *For any polynomial* $f(\gamma - 1)$ *with degree* 1, *put*

$$W_f := \varepsilon^{(Q(\gamma-1)+1)f(\gamma-1)}, \quad E := \varepsilon^{q_1\gamma + q_0},$$

where the action of a factorized polynomial is defined in the same way as Lemma 3.7. *Then*

$$[\varepsilon^{f(\gamma-1)}, \gamma]^\delta \equiv ((W_f E^{-1})^{\gamma-1})^{-1}(\varepsilon^{Q(\gamma-1)})^{-1}[\varepsilon, \varepsilon^\gamma]^{q_1^2 + q_1 q_0 + q_0^2}.$$

Proof. Describe $f(\gamma-1)$ as $f(\gamma-1)=f_1\gamma+f_0$ ($f_1, f_0\in\mathbb{Z}_3$). Since $C\in R$ and $[(\varepsilon^{f(\gamma-1)})^\delta, C]\in[R,F]$,

$$\begin{aligned}[\varepsilon^{f(\gamma-1)},\gamma]^\delta &= [(\varepsilon^{f(\gamma-1)})^\delta,\gamma^\delta]\\ &= [(\varepsilon^{f(\gamma-1)})^\delta, C\varepsilon^{Q(\gamma-1)}\gamma]\\ &= [(\varepsilon^{f(\gamma-1)})^\delta, C]C[(\varepsilon^{f(\gamma-1)})^\delta,\varepsilon^{Q(\gamma-1)}\gamma]C^{-1}\\ &\equiv [(\varepsilon^{f(\gamma-1)})^\delta,\varepsilon^{Q(\gamma-1)}\gamma]=[((\varepsilon^\gamma)^\delta)^{f_1}(\varepsilon^{f_0})^\delta,\varepsilon^{Q(\gamma-1)}\gamma].\end{aligned}$$

We find

$$\begin{aligned}(\varepsilon^{f_0})^\delta &= (\varepsilon^\delta)^{f_0}=(D\varepsilon^{Q(\gamma-1)+1})^{f_0}\\ &\equiv D^{f_0}(\varepsilon^{Q(\gamma-1)+1})^{f_0},\\ (\varepsilon^{f_1\gamma})^\delta &= ((\varepsilon^\gamma)^\delta)^{f_1}=([\delta,\gamma](\varepsilon^\delta)^\gamma[\delta,\gamma]^{-1})^{f_1}\\ &\equiv (C\varepsilon^{Q(\gamma-1)}(D\varepsilon^{Q(\gamma-1)+1})^\gamma(\varepsilon^{Q(\gamma-1)})^{-1}C^{-1})^{f_1}\\ &\equiv r(\varepsilon^{Q(\gamma-1)+1})^{f_1\gamma}\end{aligned}$$

for some $r\in R$ by (7). Therefore we obtain

$$\begin{aligned}[\varepsilon^{f(\gamma-1)},\gamma]^\delta &\equiv [(\varepsilon^{Q(\gamma-1)+1})^{f_1\gamma}\cdot(\varepsilon^{Q(\gamma-1)+1})^{f_0},\varepsilon^{Q(\gamma-1)}\gamma]\\ &\equiv [r'\varepsilon^{(Q(\gamma-1)+1)(f_1\gamma+f_0)},\varepsilon^{Q(\gamma-1)}\gamma]\quad(\text{for some } r'\in R \text{ by } (7))\\ &\equiv [W_f,\varepsilon^{Q(\gamma-1)}\gamma]\\ &= W_f\varepsilon^{Q(\gamma-1)}W_f^{-\gamma}(\varepsilon^{Q(\gamma-1)})^{-1}.\end{aligned}$$

On the other hand, $E^{\gamma-1}\equiv\varepsilon^{Q(\gamma-1)}[\varepsilon,\varepsilon^\gamma]^{q_1q_0}$ by (7). Therefore, again by (7),

$$\begin{aligned}\varepsilon^{Q(\gamma-1)} &\equiv [E^\gamma,E^{-1}]E^{-1}E^\gamma[\varepsilon,\varepsilon^\gamma]^{-q_1q_0}\\ &\equiv E^{-1}E^\gamma[\varepsilon,\varepsilon^\gamma]^{q_1^2+q_1q_0+q_0^2}.\end{aligned}$$

Combining this with the above, we obtain the lemma. □

Lemma 4.7. (i) $[\delta\varepsilon^{B(\gamma-1)},\gamma]\equiv C[\varepsilon,\varepsilon^\gamma]^{q_1^2+q_1q_0+q_0^2}$,
(ii) $[\delta,\gamma\varepsilon^{-\gamma^{-1}}]\equiv CD^{-1}$,
(iii) $[\delta\varepsilon^{J(\gamma-1)},\gamma\varepsilon^{\gamma^{-1}}]\equiv CD[\varepsilon,\varepsilon^\gamma]^{q_1^2+q_0^2-q_1-q_0-J'(0)}$.

Proof. By Lemma 4.5 (i), the relation $P_K(T)\mid -Q(T)/T+(1+T)B(T)$ in Lemma 4.3 implies that $W_BE^{-1}\in R$. Hence, by Lemma 4.6, we get

$$\begin{aligned}[\delta\varepsilon^{B(\gamma-1)},\gamma] &= [\varepsilon^{B(\gamma-1)},\gamma]^\delta[\delta,\gamma]\\ &\equiv ((W_BE^{-1})^{\gamma-1})^{-1})(\varepsilon^{Q(\gamma-1)})^{-1}[\varepsilon,\varepsilon^\gamma]^{q_1^2+q_1q_0+q_0^2}[\delta,\gamma]\\ &\equiv C[\varepsilon,\varepsilon^\gamma]^{q_1^2+q_1q_0+q_0^2}.\end{aligned}$$

In the same way,

$$\begin{aligned}[\delta, \gamma\varepsilon^{-\gamma^{-1}}] &= [\delta, \varepsilon^{-1}\gamma] = [\delta, \varepsilon^{-1}][\delta, \gamma]^{\varepsilon^{-1}} = \varepsilon^{-1}[\delta, \varepsilon]^{-1}\varepsilon[\delta, \gamma]^{\varepsilon^{-1}} \\ &\equiv \varepsilon^{-1}(\varepsilon^{Q(\gamma-1)})^{-1}D^{-1}\varepsilon\varepsilon^{-1}C\varepsilon^{Q(\gamma-1)}\varepsilon \\ &\equiv CD^{-1}.\end{aligned}$$

Finally, we compute $[\delta\varepsilon^{J(\gamma-1)}, \gamma\varepsilon^{\gamma^{-1}}] = [\delta\varepsilon^{J(\gamma-1)}, \varepsilon][\delta\varepsilon^{J(\gamma-1)}, \gamma]^{\varepsilon}$. Note that the relation $P_K(T) \mid J(T)(1+Q(T)) - 2Q(T)/T$ implies that $W_J E^{-2} \in R$. Since $J(T) = J'(0)T + J(0)$, it turns out that

$$\begin{aligned}[\delta\varepsilon^{J(\gamma-1)}, \varepsilon] &= [\varepsilon^{J(\gamma-1)}, \varepsilon]^{\delta}[\delta, \varepsilon] \equiv [\varepsilon, \varepsilon^{\gamma}]^{-J'(0)}D\varepsilon^{Q(\gamma-1)}, \\ [\delta\varepsilon^{J(\gamma-1)}, \gamma] &= [\varepsilon^{J(\gamma-1)}, \gamma]^{\delta}[\delta, \gamma] \\ &\equiv ((W_J E^{-1})^{\gamma-1})^{-1}(\varepsilon^{Q(\gamma-1)})^{-1}[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_1q_0+q_0^2}C\varepsilon^{Q(\gamma-1)} \\ &\equiv ((W_J E^{-1})^{\gamma-1})^{-1}C[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_1q_0+q_0^2} \\ &\equiv (\varepsilon^{Q(\gamma-1)})^{-1}C[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_0^2}.\end{aligned}$$

In fact, the last congruence follows from the congruences

$$(W_J E^{-1})^{\gamma-1} = [\gamma, W_J E^{-2}E] \equiv E^{\gamma-1} \equiv \varepsilon^{Q(\gamma-1)}[\varepsilon, \varepsilon^{\gamma}]^{q_1q_0}.$$

Therefore

$$\begin{aligned}[\delta\varepsilon^{J(\gamma-1)}, \gamma\varepsilon^{\gamma^{-1}}] &\equiv [\varepsilon, \varepsilon^{\gamma}]^{-J'(0)}D\varepsilon^{Q(\gamma-1)} \cdot \varepsilon(\varepsilon^{Q(\gamma-1)})^{-1}C[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_0^2}\varepsilon^{-1} \\ &\equiv [\varepsilon, \varepsilon^{\gamma}]^{-J'(0)}D[\varepsilon, (\varepsilon^{Q(\gamma-1)})^{-1}]C[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_0^2} \\ &\equiv CD[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_0^2-q_1-q_0-J'(0)}.\end{aligned}$$

This completes the proof. □

We apply Proposition 2.3 to the extension $L(K_n)/k$. By Lemmas 4.3, 4.5 and 4.7, we obtain $\tilde{L}(K_n) = L(K_n)$ if and only if the three elements $C[\varepsilon, \varepsilon^{\gamma}]^{q_1^2+q_1q_0+q_0^2}$, CD^{-1}, $CD^{q_1^2+q_0^2-q_1-q_0-J'(0)}$ generate the group $\langle[\varepsilon, \varepsilon^{\gamma}], C, D\rangle[R, F]/(R \cap [F, F])^3[R, F]$. Since $J'(0) \equiv -2(q_1+q_0)^2 + 2q_1 \equiv 1 - q_1 \bmod 3$ by (6), we see that this is equivalent to $(q_1+q_0)^2 + q_1 + q_0 + J'(0) \equiv q_0 - 1 \not\equiv 0 \bmod 3$. To complete the proof of Theorem 1.2, we show the following:

Lemma 4.8. *Put* $P_K(T) = T^2 + c_1T + c_0$ $(c_1, c_0 \in 3\mathbb{Z}_3)$, *then* $c_0 \equiv 3 \bmod 3^2$ *and*

$$q_0 \not\equiv 1 \bmod 3 \iff c_1 \not\equiv 3 \bmod 3^2.$$

Therefore $\tilde{L}(K_n) = L(K_n)$ *if and only if* $P_K(-1) \equiv 4 - c_1 \not\equiv 1 \bmod 3^2$.

Proof. Dividing by $P_K(T) = T^2 + c_1T + c_0$, $Q(T)$ has the form $Q(T) = q_1P_K(T) + rT - c_0q_1$, where $r := q_1 + q_0 - c_1q_1 \in \mathbb{Z}_3^\times$. Then, by Proposition 2.1, $P_K(T)$ has the form

$$\begin{aligned} P_K(T) &= (\Lambda\text{-unit})(Q(T)^2 + 3Q(T) + 3) \\ &\equiv (\Lambda\text{-unit})((rT - c_0q_1)^2 + 3(rT - c_0q_1) + 3) \mod P_K(T). \end{aligned}$$

Hence $P_K(T) \mid (rT - c_0q_1)^2 + 3(rT - c_0q_1) + 3$. Therefore we get

$$\begin{aligned} P_K(T) &= (\Lambda\text{-unit})((rT - c_0q_1)^2 + 3(rT - c_0q_1) + 3) \\ &= T^2 + r^{-1}(3 - 2c_0q_1)T + r^{-2}(c_0^2q_1^2 - 3c_0q_1 + 3), \end{aligned}$$

where note that the leading coefficient of the last polynomial is 1 since the characteristic polynomial $P_K(T)$ is distinguished. Therefore we obtain $c_1r = 3 - 2c_0q_1$, $c_0r^2 = c_0^2q_1^2 - 3c_0q_1 + 3$. Put $c_i = 3\bar{c}_i$ $(i = 1, 0)$, then

$$\bar{c}_0 \equiv 1 \mod 3, \quad \bar{c}_1 \equiv r^{-1}(1 + q_1) \equiv (q_1 + q_0)(1 + q_1) \mod 3,$$

since $r^2 \equiv 1 \mod 3$. We can easily check that the lemma follows from these congruences and $q_1 + q_0 \not\equiv 0 \mod 3$. □

Finally, we give some examples:

Proposition 4.9. $P_K(-1) \not\equiv 1 \mod 3^2$ *if and only if* $A(K_1)$ *has no element with order* 3^3 *i.e.,* $A(K_1) \simeq (\mathbb{Z}/3^2\mathbb{Z})^{\oplus 2}$.

Proof. We know

$$\begin{aligned} A(K_1) &\simeq \Lambda/(P_K(T), T^3 + 3T^2 + 3T) \\ &\simeq \Lambda/(P_K(T), (3 - c_0 - 3c_1 + c_1^2)T - c_0(3 - c_1)) \end{aligned}$$

by (1). Then we can easily check $3^2 \mid (3 - c_0 - 3c_1 + c_1^2)T - c_0(3 - c_1)$, since $c_0 \equiv 3 \mod 3^2$. If $P_K(-1) \not\equiv 1 \mod 3^2$ i.e., $c_1 \not\equiv 3 \mod 3^2$, then

$$A(K_1) \simeq \Lambda/(P_K(T), 3^2) \simeq (\mathbb{Z}/3^2\mathbb{Z})^{\oplus 2}.$$

On the other hand, if $c_1 \equiv 3 \mod 3^2$, then

$$A(K_1) \simeq \Lambda/(P_K(T), 3^2(s_1T + 3s_0))$$

for some $s_1, s_0 \in \mathbb{Z}_3$. Consider the exact sequence

$$0 \to \frac{(P_K(T), 3^2)}{(P_K(T), 3^2(s_1T + 3s_0))} \to \frac{\Lambda}{(P_K(T), 3^2(s_1T + 3s_0))} \to \frac{\Lambda}{(P_K(T), 3^2)} \to 0.$$

Assume that $A(K_1)$ has no element with order 3^3. Then $3^2 \in (P_K(T), 3^2(s_1T + 3s_0))$, and so that there exist some $f(T), g(T) \in \Lambda$ such that $3^2 = P_K(T)f(T) + 3^2(s_1T + 3s_0)g(T)$. This induces $3^2 \mid f(T)$. However, then $3^2 \equiv P_K(0)f(0) \equiv 0 \mod 3^3$. This is a contradiction. Since $\dim_{\mathbb{F}_3} A(K_1) \otimes_{\mathbb{Z}} \mathbb{F}_3 = 2$, we complete the proof. $\square$

EXAMPLE. Let $k = \mathbb{Q}(\sqrt{-m})$ and K^+ an abelian 3-extension of conductor $l = 43$. If $m = 7, 30, 37$, then $A(K_1) \simeq (\mathbb{Z}/3^2\mathbb{Z})^{\oplus 2}$ and so that $\tilde{L}(K_n) = L(K_n)$ for any $n \geq 0$. On the other hand, if $m = 46$, then $A(K_1) \simeq \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/3^3\mathbb{Z}$ and so that $\tilde{L}(K_n) \neq L(K_n)$ for any $n \geq 1$.

REMARKS. If we discard the assumption $p = 3$ in Theorem 1.2, the author cannot compute $\dim_{\mathbb{F}_p} H_2(G_n, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ as in the same way similar to Lemma 4.4 since it seems to depend on the form of $Q(T)$.

Let p, l be odd prime numbers such that $p \mid l - 1$. Take k, K^+, and K as in the beginning of this section. Assume that p does not split in K. If we assume, on the contrary to the assumption in Theorem 1.1, that l splits in k, we do not succeed in classifying the field K such that $\tilde{L}(K_\infty) = L(K_\infty)$. Applying [15, Theorem 1.1], we have the following:

$$\tilde{L}(K_\infty) = L(K_\infty) \Rightarrow \begin{cases} \text{(a)} \quad p \parallel l - 1,\ \lambda_k = 1,\ \dim_{\mathbb{F}_p} A(K) = 1 \quad \text{or} \\ \text{(b)} \quad p \parallel l - 1,\ \lambda_k = 0. \end{cases}$$

Theorem 1.2 is a special case of (b). In the case (a), we can prove the fact that $\dim_{\mathbb{F}_p} H_2(G_n, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{F}_p = 3$. However, the author cannot find any relations like (7).

References

[1] L. Evens: *The Schur multiplier of a semi-direct product*, Illinois J. Math. **16** (1972), 166–181.

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

[3] A. Fröhlich: Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, Contemporary Mathematics **24**, Amer. Math. Soc., Providence, RI, 1983.

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

[5] R. Gold and M. Madan: *Galois representations of Iwasawa modules*, Acta Arith. **46** (1986), 243–255.

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

[7] K. Iwasawa: *On the μ-invariants of Z_1-extensions*; in Number Theory, Algebraic Geometry and Commutative Algebra, in Honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1–11, 1973.

[8] Y. Kida: *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory **12** (1980), 519–528.

[9] S. Lang: Cyclotomic Fields I and II, combined second edition, Graduate Texts in Mathematics **121**, Springer, New York, 1990.

[10] B. Mazur and A. Wiles: *Class fields of abelian extensions of* $\boldsymbol{Q}$, Invent. Math. **76** (1984), 179–330.

[11] Y. Mizusawa: *On the maximal unramified pro*-2-*extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields*, J. Number Theory **105** (2004), 203–211.

[12] Y. Mizusawa: *On the maximal unramified pro*-2-*extension of* $\mathbb{Z}_2$*-extensions of certain real quadratic fields* II, Acta Arith. **119** (2005), 93–107.

[13] Y. Mizusawa and M. Ozaki: *Abelian* 2*-class field towers over the cyclotomic* $\mathbb{Z}_2$*-extensions of imaginary quadratic fields*, Math. Ann. **347** (2010), 437–453.

[14] K. Okano: *Abelian* p*-class field towers over the cyclotomic* $\mathbb{Z}_p$*-extensions of imaginary quadratic fields*, Acta Arith. **125** (2006), 363–381.

[15] K. Okano: *The commutativity of the Galois groups of the maximal unramified pro-*p*-extensions over the cyclotomic* $\mathbb{Z}_p$*-extensions*, to appear in J. Number Theory.

[16] M. Ozaki: *Non-abelian Iwasawa theory of* $\mathbb{Z}_p$*-extensions*, J. Reine Angew. Math. **602** (2007), 59–94.

[17] M. Ozaki: *Construction of maximal unramified* p*-extensions with prescribed Galois groups*, preprint.

[18] R.T. Sharifi: *On Galois groups of unramified pro-*p *extensions*, Math. Ann. **342** (2008), 297–308.

[19] L.C. Washington: Introduction to Cyclotomic Fields, second edition, Graduate Texts in Mathematics **83**, Springer, New York, 1997.

Department of Mathematics
Faculty of Science and Technology
Tokyo University of Science
2641 Yamazaki, Noda, Chiba, 278-8510
Japan
e-mail: okano_keiji@ma.noda.tus.ac.jp