<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>The commutativity of galois groups of the maximal unramified pro-p-extensions over the cyclotomic Zp-extensions II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Okano, Keiji</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 49(2) P.271–P.295</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>2012-06</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/12486">https://doi.org/10.18910/12486</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/12486</td>
</tr>
</tbody>
</table>

_Osaka University Knowledge Archive : OUKA_

https://ir.library.osaka-u.ac.jp/repo/ouka/all/

Osaka University
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 $K_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of a Galois $p$-extension $K$ over an imaginary quadratic field. We consider the Galois group $\hat{X}(K_\infty)$ of the maximal unramified pro-$p$-extension of $K_\infty$. In this paper, under certain assumptions, we give certain $K$ such that $\hat{X}(K_\infty)$ is abelian. Also, we give an example such that a special value of the characteristic polynomial of the Iwasawa module of $K_\infty$ determines whether $\hat{X}(K_\infty)$ 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 $F_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $F$. In other words, $F_\infty$ 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 $F_\infty$ by the subfield. Denote by $\hat{X}(F)$ (resp. $\hat{X}(F_\infty)$) the Galois group of the maximal unramified pro-$p$-extension $\tilde{L}(F)$ of $F$ (resp. $\tilde{L}(F_\infty)$ of $F_\infty$). The extensions $\tilde{L}(F)/F$, $\tilde{L}(F_\infty)/F_\infty$ are called the $p$-class field towers, and their Galois groups $\hat{X}(F)$, $\hat{X}(F_\infty)$ are very interesting objects in number theory. Though $\hat{X}(F)$ can be infinite, we have quite a few known criterions for assuring that $\hat{X}(F)$ is finite: in addition, we do not have efficient methods for describing the structure of $\hat{X}(F)$. However, we mention that Ozaki [17] recently showed that there exists $F$ such that $\hat{X}(F)$ 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 $\hat{X}(F_\infty)$ is abelian; in other words, the maximal unramified pro-$p$-extension of each $F_\infty$ remains abelian extension. It is equivalent that $\hat{X}(F_\infty)$ is abelian and that all sufficiently large subfields in $F_\infty/F$ have the $p$-class field towers whose Galois groups are abelian. Also if $\hat{X}(F)$ is abelian for a finite algebraic number field.
$F$, 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 $F_{\infty}$ 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 $2^2$ 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 $K_\infty$ 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 $K_\infty$ 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 $3 \mid l - 1$, $k$ 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 $K_{\infty}/K$. Suppose that 3 does not split in $K$ but $l$ splits in $k$. Moreover, assume that $A(k) = 0$ and $\text{dim}_{\mathbb{F}_3}A(K) \otimes \mathbb{Z}_3\mathbb{F}_3 = 1$. Then $\tilde{X}(K_\infty)$ is abelian if and only if $P_K(-1) \not\equiv 1$ mod $3^2$.

2. Preliminaries

From now on, for any CM-field $F$, we use the notation $F^\pm$ 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 $F_{\infty}$ over $F$, respectively. Denote the maximal unramified abelian
\( p \)-extension of \( F \) by \( L(F) \) and its Galois group \( \tilde{X}(F)^{ab} \) by \( X(F) \). Similarly, denote the maximal unramified abelian pro-\( p \)-extension of \( F_\infty \) by \( L(F_\infty) \) and its Galois group by \( X(F_\infty) \). For any module \( A \) on which \( \text{Gal}(F/F^+) \) acts, put \( A^+ := A^{\text{Gal}(F/F^+)} \), \( A^- := A/A^+ \).

Fix a topological generator \( \tilde{\gamma} \) of \( \text{Gal}(F_\infty/F) \). And we write its restriction on \( \text{Gal}(F_n/F) \) as the same notation for each \( n \geq 0 \). Choose an extension \( \gamma \in \text{Gal}(L(F_\infty)/F) \) of \( \tilde{\gamma} \). Then \( \text{Gal}(F_n/F) \) acts on \( X(F_n) \) as the inner automorphisms defined by \( x^\gamma = \gamma x \gamma^{-1} \) for any \( x \in X(F_n) \). Note that this action is independent of the choice of an extension \( \gamma \) 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 \( \lim Z_p[\text{Gal}(F_n/F)] \) acts on \( X(F_\infty) \) continuously, where each inverse limit is taken over Galois restrictions. Hence the formal power series ring \( \Lambda := Z_p[[T]] \) acts on \( X(F_\infty) \) via the non-canonical isomorphism \( \Lambda \simeq \varprojlim Z_p[\text{Gal}(F_n/F)] \) which is obtained by sending \( 1 + T \) to the fixed topological generator \( \tilde{\gamma} \) of \( \text{Gal}(F_\infty/F) \). Therefore \( X(F_\infty) \) is a \( \Lambda \)-module, so that we write the action of \( \Lambda \) additionally; \( x^\gamma = (1 + T)x \).

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

\[
 f(T) = p^n P(T) U(T)
\]

with an integer \( n \geq 0 \), 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 \( r(T) \in Z_p[T] \) such that

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

Therefore \( \Lambda \) 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 \( \Lambda \). Therefore we can define the Iwasawa \( \lambda \)-invariant \( \lambda_F \) of \( F_\infty/F \) by the dimension of \( X(F_\infty) \otimes_{Z_p} \mathbb{Q}_p \) over the \( p \)-adic field \( \mathbb{Q}_p \). There is a \( \Lambda \)-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 \( \Lambda \) 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 \( \Lambda \)-submodules by [19, Theorem 13.28]. We say that the Iwasawa
\( \mu_{inv} \mu_F \) of \( F_\infty/F \) is zero if \( X(F_\infty) \) is also finitely generated over \( \mathbb{Z}_p \); For example, if \( F/Q \) 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 \( P_F(T) := \prod_{i=1}^{n} P_i^{m_i} \) 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 \( F_\infty/F \) is totally ramified at all primes lying above \( p \), then there is an isomorphism

\[
(1) \quad X(F_n) \simeq X(F_\infty) / \frac{\omega_n(T)}{T} Y
\]

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

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 \( \Delta := \text{Gal}(K/k) \). First of all, we compare \( P_K(T) \) with \( P_k(T) \) (Proposition 2.1). We identify \( \Gamma := \text{Gal}(k_\infty/k) \) with \( \text{Gal}(K_\infty/K) \) and \( \Delta \) with \( \text{Gal}(K_\infty/k_\infty) \) by the canonical isomorphisms. Note that \( \Delta \) acts on \( X(K_\infty) \) and \( X(K_\infty)^- \) as the inner automorphisms similar to the action of \( \Gamma \). The actions of \( \Gamma \) and \( \Delta \) are commutative since \( X(K_\infty) \), \( X(K_\infty)^- \) and \( \text{Gal}(K_\infty/k) \) 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

\[
(2) \quad \lambda_k^- = p \lambda_k^- + (p - 1)(s - v),
\]

where \( s \) is the number of primes in \( K_\infty^+ \) not lying above \( p \) which split in \( K_\infty/K_\infty^+ \) and ramify in \( K_\infty^+ /k_\infty^+ \), and \( v = 1 \) 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 \( \Lambda \). Then we have a surjection

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

since \( X(K_\infty)^- \) has no non-trivial finite \( \Lambda \)-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 \( \Lambda \) and a generator \( \delta \in \Delta \). We described the action of \( \Delta \) as \( \varepsilon^\delta \). 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 \( \varepsilon \). We may assume that \( Q(T) \) is a polynomial by the division theorem. Put

\[
(3) \quad N(T) := Q(T)^{p-1} + \left( \frac{p}{p-1} \right) Q(T)^{p-2} + \cdots + \left( \frac{p}{1} \right) = \frac{(Q(T) + 1)^p - 1}{Q(T)},
\]

where \( \left( \frac{p}{r} \right) \) is a binomial coefficient. Then we have the following proposition:
Proposition 2.1. Let $K/k$ and $\Delta$ be as above. Assume that $X(K_{\infty})^{-}$ is non-trivial and cyclic over $\Lambda$. Then the followings hold:

(i) If $\lambda_{k}^{-} = 1$, $s = 0$ and $\nu = 1$, where $s$ and $\nu$ 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 $s - \mu \geq 0$,

$$P_{K}(T) = (\Lambda\text{-unit})P_{k}(T)N(T) \quad \text{i.e.,} \quad P_{k}(T)N(T)/P_{K}(T) \in \Lambda_{\times},$$

$$X(K_{\infty})^{-} \simeq \mathbb{Z}_{p}[\Delta]^{\oplus \lambda_{k}^{-}} \oplus I_{\Delta}^{\oplus (s - \nu)} \quad \text{as} \quad \mathbb{Z}_{p}[\Delta]\text{-modules}$$

and the residue degree of $Q(T)$ is $\lambda_{k}^{-} + s - \nu$, where $I_{\Delta}$ 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 $X(K_{\infty})^{-} = \lim_{\leftarrow} \Lambda(K_{n})^{-}$. We consider the norm map $N_{K_{n}/K_{\infty}} : X(K_{\infty})^{-} \to X(k_{\infty})^{-}$ which is induced by the norm maps $N_{K_{n}/K_{\infty}} : X(K_{n})^{-} \to X(k_{n})^{-}$ and the norm operator $N_{\Delta} : X(K_{\infty})^{-} \to X(K_{\infty})^{-}$ ($N_{\Delta}(x) := x + x^{\frac{\mu}{p-1}} + \cdots + x^{p^{n} - 1}$). If $K_{\infty}/k_{\infty}$ is not unramified, in other words, $K_{\infty} \cap L(k_{\infty}) = k_{\infty}$, then $N_{K_{n}/k_{\infty}}$ is surjective by the class field theory. Similarly, $N_{K_{n}/k_{\infty}}$ is surjective if $K_{\infty}/k_{\infty}$ is unramified. Indeed, by taking the minus-part of the exact sequence of Galois groups

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

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

The norm operator $N_{\Delta}$ coincides with the endomorphism by multiplying $N(T)$ since

$$N_{\Delta}(x) = x + x^{\frac{\mu}{p-1}} + \cdots + x^{p^{n} - 1}$$

$$= (1 + (1 + Q(T)) + \cdots + (1 + Q(T))^{p-1})x$$

$$= N(T)x.$$

Therefore we have the following commutative diagram:

$$
\begin{array}{ccc}
\Lambda/(P_{k}(T)) & \simeq & X(K_{\infty})^{-} \quad \xrightarrow{N_{\Delta}} \\
\Lambda/(P_{k}(T)) & \simeq & X(k_{\infty})^{-} \quad \xrightarrow{\text{lift.}} \\
\Lambda/(P_{k}(T)) & \simeq & X(k_{\infty})^{-} \quad \xrightarrow{\text{lift.}} \\
\end{array}
$$

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

\[(4) \quad P_\epsilon(T) \mid P_K(T) \mid P_p(T) N(T),\]

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 $\Lambda$ is a UFD). Now, we see that $Q(T) N(T)$ belongs to the ideal $(P_K(T))$ of $\Lambda$ since $\epsilon = e^{s \rho_p}$, 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 $P_K(0) \not\in \mathbb{Z}_p^\times$ by the assumption $X(K_{\infty})^\tau \neq 0$. Moreover, we see that $p \mid N(0)$ by (3) (note that $p \geq 3$). Therefore, by the $p$-adic Weierstraß preparation theorem,

\[N(T) = p U(T) \quad \text{or} \quad N(T) = \tilde{N}(T) U(T)\]

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

\[P_K(T) = P_p(T) \quad \text{or} \quad P_K(T) = P_p(T) \tilde{N}(T).\]

First, we suppose $P_K(T) = P_p(T)$. Then $1 \leq \lambda_{\tilde{N}} = \lambda_\epsilon = v - s$ by (2) and we have

\[P_K(T) = P_p(T) \iff \lambda_{\tilde{N}} = 1, \quad s = 0, \quad v = 1.\]

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 $\delta$ acts on $X(K_{\infty})^\tau$ trivially.

Next, we suppose that $P_K(T) = P_p(T) \tilde{N}(T)$ to show the rest of (ii). Then, note that $Q(T), N(T) \notin p \Lambda$ since $P_K(T) \not\in p \Lambda$. Let $\tilde{Q}(T) \in \mathbb{Z}_p[T]$ be a distinguished polynomial such that $Q(T)/\tilde{Q}(T) \in \Lambda^\times$: $\tilde{Q}(T)$ depends on the choice of $Q(T)$. Then we know

\[(5) \quad \deg \tilde{N}(T) = (p - 1) \deg \tilde{Q}(T) = (p - 1)(\lambda_{\tilde{N}} + s - v)\]

by $N(T) \equiv T^{(p - 1) \deg \tilde{Q}(T)(Q(T)/\tilde{Q}(T))} \pmod{p}$ and (2). Hence $\deg \tilde{Q}(T) = \lambda_{\tilde{N}} + s - v$. In particular, $\deg \tilde{Q}(T)$ 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 $P_K(T) = P_p(T) \tilde{N}(T)$.

This implies that $s - v = \deg \tilde{Q}(T) - \deg P_p(T) \geq 0$ and also that $P_p(T)$ and $\tilde{N}(T)$ are relatively prime by (3). Finally, since $\Delta$ is a cyclic group with order $p$ and $X(K_{\infty})^\tau$ is a free $\mathbb{Z}_p$-module, we have a representation

\[X(K_{\infty})^\tau \simeq \mathbb{Z}_p[\Delta]^{\oplus \lambda_{\tilde{N}}} \oplus I_\Delta^{p(s-\lambda_{\tilde{N}})}\]

as $\mathbb{Z}_p[\Delta]$-modules by Gold–Madan [5]. This completes the proof.
Corollary 2.2. Let $K/k$ and $\Delta$ be as above. Suppose that only one prime of $K_\infty$ lies above $p$ and that this prime is totally ramified in $K_\infty/K$. Assume that $A(K)^-\simeq \Lambda/(P_k(T), T) \simeq \mathbf{Z}_p/P_K(0)\mathbf{Z}_p$. Assume that $A(K)^-$ is non-trivial and cyclic, then

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

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

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

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

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

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 $q$ in $k$ which is ramified in $F/k$, we fix a prime lying above $q$ in $L(F)$ and denote its decomposition group in $\text{Gal}(L(F)/k)$ by $Z_q$. 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 $\Phi$:

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

$$\Phi: \prod_q H_2(Z_q, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{F}_p \to H_2(\text{Gal}(L(F)/k), \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{F}_p$$

which is induced by the canonical map $Z_q \to \text{Gal}(L(F)/k)$, 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 $\Phi$ 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 $k \neq \mathbf{Q}(\sqrt{-3})$ if $p = 3$, and $K^+$ an abelian $p$-extension of $\mathbf{Q}$ with conductor $l$. Put $K := kK^+$. We identify $\Gamma := \text{Gal}(k_\infty/k)$ with $\text{Gal}(K_\infty/K)$ and $\Delta := \text{Gal}(K/k)$ with $\text{Gal}(K_\infty/k_\infty)$. Assume that neither $p$ nor $l$ splits in $K$. Note that $X(\mathbf{Q}_\infty) = 0$ 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 $X(k_{\infty})$ 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 $k_{\infty}$ lying above $p$ is totally ramified in $k_{\infty}/k$, $A(k)$ 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 $\text{Gal}(L(K)/k)$ 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 $H_2(\text{Gal}(L(K)/k), \mathbb{Z}_p) = 0$ by Proposition 2.3. By Evens [1], we have

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

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

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 $G_n := \text{Gal}(L(K_n)/k)$ and some decomposition subgroups. Put $\Gamma_n := \Gamma/\Gamma^p$ for simplicity. Let $\tilde{\gamma}$ a fixed generator of $\Gamma$. Identify $\Lambda = \mathbb{Z}_p[[T]]$ with
\[
\lim \mathbb{Z}_p[\Gamma_n] \text{ by sending } 1 + T \text{ to } \bar{\gamma}. \quad \text{Since the only one prime lying above } p \text{ in } K \text{ is totally ramified in } K^\infty/K \text{ and } A(K) \text{ is a non-trivial cyclic group, } X(K^\infty) \text{ is cyclic over } \Lambda. \text{ Let } \varepsilon \text{ be a fixed generator of } X(K^\infty) \text{ over } \Lambda \text{ and } \delta \text{ a fixed generator of } \Delta. \text{ Then, since } X(K^\infty) = 0, \text{ we can apply Proposition 2.1 (ii) to obtain}
\]

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

Here \(Q(T)\) is defined by \(\varepsilon^\delta = (Q(T) + 1)\varepsilon\) and \(N(T)\) is defined as in (3). Let \(M_n\) be the maximal abelian subextension in \(L(K_n)/k\). We denote by \(\varepsilon_n, \bar{\varepsilon}_n\) the projection of \(\varepsilon \in X(K^\infty)\) to \(G_n, G_n^ab := \text{Gal}(M_n/k)\), respectively. Let \(\bar{p}_n\) (resp. \(\bar{\gamma}_n\)) be a prime in \(L(K_n)\) lying above \(p\) (resp. \(l\)), and \(\gamma_n \in G_n\) (resp. \(\delta_n\)) a generator of the inertia group \(I_p \simeq \Gamma_n\) of \(\bar{p}_n\) (resp. the inertia group \(I_l \simeq \Gamma_n\)). Put \(\bar{\gamma}_n := \gamma_n \mod [G_n, G_n], \bar{\delta}_n := \delta_n \mod [G_n, G_n]\). 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 \(\gamma_n\) (resp. \(\delta_n\)) is an extension of \(\gamma \mod \Gamma p^m\) (resp. \(\delta \mod \Delta\)). Then \(\text{Gal}(K_n/k)\) acts on \(X(K_n) = \Lambda \varepsilon_n \simeq \Lambda/(P_k(T), \omega_n(T))\) by

\[
\varepsilon^\delta_n = \gamma_n \varepsilon_n \gamma_n^{-1} = (1 + T)\varepsilon_n, \quad \varepsilon^\delta = \delta_n \varepsilon_n \delta_n^{-1} = (1 + Q(T))\varepsilon_n.
\]

**Lemma 3.3.** As \(\Lambda\text{-modules}, [G_n, G_n] \simeq (T, p^m)/(P_k(T), \omega_n(T)).\) Also we have

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

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 \(p^i \leq P_k(0)\) such that \([G_n, G_n] \simeq (T, p^i)/(P_k(T), \omega_n(T))\). We show that \(t = m\), in other words, \(\text{Gal}(M_n/K_n) \simeq \mathbb{Z}/p^m\mathbb{Z}\) for any \(n \geq 0\). 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 \( \langle \tilde{e}_n \rangle = \Gal(M_n/K_n) \cong \mathbb{Z}/p^m\mathbb{Z} \). Hence we find \[ [G_n, G_n] \cong (T, p^m)/(\Gal(T), \omega_n(T)). \]

Also, by the definitions of \( \tilde{y}_n, \tilde{h}_n, \tilde{e}_n \), we obtain \( \langle \tilde{y}_n \rangle \oplus \langle \tilde{h}_n \rangle \oplus \langle \tilde{e}_n \rangle \subset G^{ab}_n \). Comparing each order, we obtain the assertion.

In fact, \( \gamma_n \) and \( \delta_n \) are commutative and hence \( G_n \cong X(K_n) \rtimes (\Gamma_n \times \Delta) \). This fact follows from the next lemma. Recall that \( p^{e+1} \mid l - 1 \). 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 \( \tilde{p}_n, \tilde{l}_n \), respectively. Then, changing \( \tilde{l}_n \) if necessary, there is some \( D(T) \in \Lambda \) defined uniquely up to the modulus \( P_k(T) \) such that

\[
Z_p = \langle \gamma_n \rangle \oplus \langle \delta_n \rangle,
\]

\[
Z_l = \begin{cases}
\langle \delta_n \rangle & \text{if } n \leq e, \\
\langle \gamma_n \rangle \oplus \langle \delta_n \rangle & \text{if } n > e.
\end{cases}
\]

**Proof.** The image of \( Z_p \) in \( G^{ab}_n \) is generated by \( \tilde{y}_n \) and \( \tilde{h}_n \). Therefore, \( Z_p \) is generated by the generator \( \gamma_n \) of \( I_p \) and a pre-image \( \rho_n \) 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 \( Z_p = \langle \gamma_n \rangle \oplus \langle \rho_n \rangle \twoheadrightarrow \langle \tilde{y}_n \rangle \oplus \langle \tilde{h}_n \rangle \) is isomorphic. We can take \( \rho_n \) which satisfies \( \rho_n \equiv \delta_n \mod [G_n, G_n] \). It follows from this that there is some \( B(T) \in (T, p^m) \) defined up to the modulus \( P_k(T) \) such that \( \rho_n = \delta_n e_nB(T) \). Since \( 1 = \rho_n^p = e_n^{N(T)B(T)} \), we obtain \( P_k(T) \mid N(T)B(T) \). Hence \( Q(T) \mid B(T) \). On the other hand, let \( x := e_n^{-(1+Q(T))/B(T)/Q(T)} \) (note that \( 1 + Q(T) \in \Lambda^\times \) since \( e_n^{1+Q(T)} = e_n^1 \)), then

\[
x \delta_n x^{-1} = \delta_n \delta_n^{-1} x \delta_n x^{-1} = \delta_n x^{(1+Q(T))^{-1}-1} = \delta_n e_n^{B(T)} = \rho_n.
\]

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

On the other hand, we deal with \( Z_l \). Suppose that \( n \leq e \). Then every prime lying above \( l \) splits completely in \( L(K_n)/K_n \), so that \( Z_l = I_l \). Suppose that \( e < n \). Then the image of \( Z_l \) in \( G^{ab}_n \) is generated by \( \tilde{y}_n^{\rho_n} \) and \( \tilde{h}_n \). 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

$$Z_T = \langle y_n^{p'} e_n^{C(T)} \rangle \oplus \langle \delta_n \rangle$$

Since

$$1 = y_n^{p'} e_n^{C(T)} \delta_n^{-1} = e_n^{-(1+T)p^r Q(T) C(T)}$$

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

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

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

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

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 $(n \geq 1)$.

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

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

Put

$$R := \langle \gamma^p, \delta^p, e^{P_k(y-1)}, [\delta, \gamma], [\delta, e, \gamma^r], [\delta, e, y^r], \ldots, [\delta, e, y^{(p-1)/2}] \rangle_F,$$

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

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

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) $[\varepsilon^{z_1} y^i, \varepsilon^{z_2} y^i]$ is congruent with some product of $[\varepsilon, \varepsilon^y], \ldots, [\varepsilon, \varepsilon^{y^{(p-1)/2}}]$ mod $[R, F]$. In particular, $[\varepsilon^{z_1} y^i, \varepsilon^{z_2} y^i] \in R$.

(ii) $[\varepsilon^{z_1} y^i, \varepsilon^{z_2} y^i] \equiv [\varepsilon, \varepsilon^y]^{-z_1 z_2}$ 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 $[\varepsilon y^k, \varepsilon]$ is congruent with some product of $[\varepsilon, \varepsilon^y], \ldots, [\varepsilon, \varepsilon^{y^{(p-1)/2}}]$ mod $[R, F]$ for any non-negative integer $k$. If $k = 0, \pm 1, \ldots, \pm (p-1)/2$, 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 $0 \leq i < k$. If we put $P_k(y-1) = y^p + c_{p-1} y^{p-1} + \cdots + c_0$, then we have

$$1 \equiv \varepsilon y^{-i+(p-1)}, \ (\varepsilon^{-i} P_k(y-1))^{-1} = \varepsilon^{y^{-i} + (p-1)}, \varepsilon^{c_1}, \varepsilon^{c_2} \ldots \varepsilon^{c_0} \varepsilon^y \ldots \varepsilon^{y^p} \equiv [\varepsilon y^{-i+(p-1)}, \varepsilon^{c_1} \varepsilon^{c_2} \ldots \varepsilon^{c_0} \varepsilon^y \ldots \varepsilon^{y^p}] \mod [R, F],$$

since $-(p-1)/2 \leq k - (p-1) < k$. Hence $[\varepsilon y^{-i+(p-1)}, \varepsilon^{c_1} \varepsilon^{c_2} \ldots \varepsilon^{c_0} \varepsilon^y \ldots \varepsilon^{y^p}] \in R$ and so that, in the same way, we obtain

$$1 \equiv \varepsilon y^{-i+(p-1)}, \varepsilon^{c_1} \varepsilon^{c_2} \ldots \varepsilon^{c_0} \varepsilon^y \ldots \varepsilon^{y^p} \equiv [\varepsilon y^{-i+(p-1)}, \varepsilon^{c_1} \varepsilon^{c_2} \ldots \varepsilon^{c_0} \varepsilon^y \ldots \varepsilon^{y^p}] \frac{1}{y} \ldots \frac{1}{y^k} \mod [R, F] .$$
\[
\begin{align*}
&= [e^{y_{n+1}(n+1)}], \varepsilon]^{0} [e^{y_{n+1}(n+1)}], \varepsilon]^{e_{1} y} \cdots [e^{y_{k}], \varepsilon]^{e_{l_{-1}} y_{l_{-1}} [e^{y_{k}], \varepsilon}]^{y_{l_{-1}}} \\
&= [e^{y_{n+1}(n+1)}], \varepsilon]^{0} [e^{y_{n+1}(n+1)}], \varepsilon]^{e_{1} y} \cdots [e^{y_{k}], \varepsilon]^{e_{l_{-1}} y_{l_{-1}} [e^{y_{k}], \varepsilon}]^{y_{l_{-1}}} \mod [R, F].
\end{align*}
\]

Therefore we obtain \([e^{y_{n+1}(n+1)}, \varepsilon]^{y_{l_{-1}} \in R}\) and so that \([e^{y_{n+1}(n+1)}, \varepsilon]^{y_{l_{-1}}} = [e^{y_{n+1}(n+1)}, \varepsilon] \mod [R, F].\)

This implies that the claim holds. The general case where any \(z_{1}, z_{2} \in \mathbb{Z}\) follows from this, since, taking the limit later if necessary, we may assume that \(1 \leq z_{1}, z_{2} \in \mathbb{Z}\).

(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

\[
f(y - 1) = a_{k} y^{k} + \cdots + a_{1} y + a_{0}
= b_{k}(y - 1)^{k} + \cdots + b_{1}(y - 1) + b_{0} \quad (a_{i}, b_{i} \in \mathbb{Z}),
\]

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

\[
[e^{y'}, e^{f(y - 1)}] = [e^{y'}, e^{a_{1} y^{1} + \cdots + a_{1} y + c_{0}}]
= [e^{y'}, e^{y^{k}}]^{b_{1}} \cdots [e^{y'}, e^{y^{l_{-1}}}]^{b_{l_{-1}}} \mod [R, F],
\]

since \([e^{y'}, e^{y^{k}}] \in R\). Now, if \(f(y - 1) = P_{K}(y - 1)\), then \(b_{p} = 1\) and \(b_{p-1} \equiv \cdots \equiv b_{0} \equiv 0 \mod p\), so that we obtain

\[
a_{i} \equiv \begin{cases} -1 \mod p & \text{(if } i = 0), \\ 1 \mod p & \text{(if } i = p), \\ 0 \mod p & \text{(otherwise).}
\end{cases}
\]

Therefore we have \(1 \equiv [e^{y'}, e^{P_{K}(y - 1)}] \equiv [e^{y'}, e^{P_{0}(y - 1)}] \mod [R, F](R \cap [F, F])^{p}. \)

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

\[
[x, (e^{f(y - 1)}^{k})^{\delta}] \equiv [x, e^{f(y - 1)(y - 1)\delta}] \mod [R, F],
\]

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

\[
x^{f(y)g(y)} := x^{a_{1} y^{k} \cdots x^{a_{1} y^{l_{-1}}}} \quad \text{if } f(y)g(y) = a_{k} y^{k} + \cdots + a_{1} y + a_{0}.
\]

**Proof.** If \(k = 0\), then the congruence holds. Suppose that the congruence holds for some \(k\). Note that, by \([\delta, y] \in R\) and Lemma 3.6 (i), the congruences \([x, (e^{y^{l_{-1}}})^{\delta}] \equiv
Therefore the congruence holds for any $k$, $i$, $j \in \mathbb{Z}$. Hence we have
\[
[x, (e^{f(y-1)})^j] \equiv [x, ((e^{Q(y-1)+1})^j e^{f(y-1)})^j] \equiv [x, e^{f(y-1)(Q(y-1)+1)^j}] \mod [R, F] \text{ (by the assumption)}.
\]

Therefore the congruence holds for any $k$ by induction. \hfill \Box

**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 $\phi: F \to G_n$ is given by $\gamma \mapsto \gamma_n$, $\delta \mapsto \delta_n$, $\varepsilon \mapsto \varepsilon_n$.

**Proof.** It is clear that $R \subset \text{Ker} \phi$ and $\phi$ is surjective, so that we have the surjective maps
\[
F/[F, F]R = (F/R)^{ab} \to G_n^{ab}, \quad [F, F]R/R = [F/R, F/R] \to [G_n, G_n].
\]
We prove that these two maps are isomorphisms. We know that $[F, F]$ is generated by $[\delta, \gamma]$, $[\gamma, \varepsilon] = e^{y-1}$, $[\delta, \varepsilon]$ and their conjugates. Hence, using $[\delta, \varepsilon] = e^{Q(y-1)} \mod R$ and Lemma 3.6 (i), we see that $[F, F]R/R$ is generated by $e^{y-1}$ and $e^{Q(0)} \mod R$ and their conjugates. But, by the congruences
\[
(e^{y-1})^{\varepsilon} \equiv e^{y-1}, \quad (e^{Q(0)})^{\delta} \equiv (e^{Q(0)})^{Q(y-1)+1}, \quad (e^{y-1})^{\delta} \equiv (e^{y-1})^{Q(y-1)+1} \mod R
\]
and $e^{\omega_n(y-1)} \equiv 1 \mod R$ which follows from $T \mid \omega_n(T)$, we obtain
\[
[F, F]R/R = \langle (e^{y-1})^{F(y-1)}, (e^{p^n})^{F(y-1)} \mid F(T) \in \Lambda \rangle R/R = \langle e^{F(y-1)} \mid F(T) \in (T, p^m) \rangle R/R.
\]
Then the surjective map
\[
[G_n, G_n] \simeq (T, p^m)/(P_K(T), \omega_n(T)) \to [F, F]R/R
\]
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 $\#(F/[F, F]R) \leq \#G_n^{ab}$ and so that $F/[F, F]R \simeq G_n^{ab}$. \hfill \Box

**Lemma 3.9.**
\[
R/[R, F] = \langle \gamma^{p^n}, \delta^n, [\delta, \gamma], [\delta, \varepsilon](e^{Q(y-1)})^{-1}, [\varepsilon, e^y], \ldots, [\varepsilon, e^{Q(y-1)/2}] \rangle [R, F]/[R, F].
\]
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 \( \epsilon^{p^k(y-1)} \equiv 1 \). By Lemmas 3.6 and 3.7, we have

\[
[\delta, \epsilon]^\delta = [\delta, \epsilon^Q(y-1)+1]^\delta
\]

\[
\equiv (\epsilon^Q(y-1)+1)^{Q(y-1)+1}(\epsilon^{-1})^Q(y-1)+1)
\]

\[
\equiv (\epsilon^{Q(y-1)+1})^Q(y-1)+1)^{Q(y-1)+1}(\epsilon^{-1})^Q(y-1)+1)
\]

\[
\equiv \epsilon^{Q(y-1)+Q(y-1)+1)}
\]

Therefore \( 1 \equiv [\delta^p, \epsilon] = [\delta, \epsilon]^\delta \equiv [\delta, \epsilon^{Q(y-1)+1}] \). Since \( Q(T)N(T) = P_k(T)F(T) \) with some polynomial \( F(T) \in \Lambda^* \), we have \( 1 \equiv \epsilon^{p^k(y-1)+Q(y-1)} = (\epsilon^{p^k(y-1)})^F(0) \). Hence \( \epsilon^{p^k(y-1)} \equiv 1 \). \( \Box \)

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

\[
R_p := \langle \gamma, \gamma, \delta^p, [\gamma, \gamma] \rangle_{F_p},
\]

\[
R_l := \langle (\gamma^{(\epsilon^{Q^{p^i-1}+\cdots+\delta^i+1})^{D(y-1)}}, \delta^p, [\gamma, \gamma^{(\epsilon^{Q^{p^i-1}+\cdots+\delta^i+1})^{D(y-1)}}]_F \rangle
\]

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

\[
\Phi: \frac{R_p \cap [F_p, F_p]}{[R_p, F_p]/[R_p, F_p]} \times \frac{R_l \cap [F_l, F_l]}{[R_l, F_l]/[R_l, F_l]} \rightarrow \frac{R \cap [F, F]}{[R, F]/[R \cap [F, F]]}^p
\]

is not surjective by Proposition 2.3.

**Lemma 3.10.** The followings hold:

(i) \( R \cap [F, F]/[R, F] = \langle [\delta, \gamma], [\epsilon, \epsilon^{y}] \rangle, \ldots, [\epsilon, \epsilon^{y^{(p^i-1)/2}}]\rangle / [R, F] / [R, F] \),

(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) \( R_l \cap [F_l, F_l]/[R_l, F_l] = \langle [\delta, \gamma^{(\epsilon^{Q^{p^i-1}+\cdots+\delta^i+1})^{D(y-1)}}] \rangle / [R_l, F_l] / [R_l, F_l] \).

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 \( z_1, \ldots, z_{4+(p-1)/2} \in \mathbb{Z}_p \) such that

\[
x \equiv (\gamma^{p^i z_i})^{z_i} \delta^{p^{i/2} z_i} [\gamma, \gamma]^{z_i} ([\delta, \epsilon] \epsilon^{Q(y-1)-1})^{z_i} [\epsilon, \epsilon^{y^{(p^i-1)/2}}]^{z_i} \mod [R, F]
\]

by Lemma 3.9. Hence we obtain \( 1 \equiv \gamma^{p^i z_i} \delta^{p^{i/2} z_i} \epsilon^{Q(y-1)-1} \mod [F, F] \), and so that \( z_1 = z_2 = z_4 = 0 \). This shows (i). \( \Box \)
We now conclude our proof. Put \( d := \varepsilon^{Q(y-1)} \) for convenience. By Lemma 3.10, it is sufficient to show that \([\delta, \gamma]\) and \([\delta, (e^{[\gamma-1] \odot \ldots \odot \gamma + 1})] \) do not generate \((R \cap \{F, F\})/(R \cap \{F, F\})^{\pmod{}}\). By induction, we have

\[
e^{\delta} \equiv ([\delta, \varepsilon])d^{-1} \; d^{\beta^1 + \ldots + \beta^i + 1} \; \varepsilon \mod [R, F] \; (k \geq 1).
\]

Indeed, by the assumption of the induction,

\[
(e^{\delta^{k-1}})^{\delta} \equiv ([\delta, \varepsilon])d^{-1} \; d^{\beta^1 + \ldots + \beta^i} \; e^{\delta}
\]

\[
= ([\delta, \varepsilon])d^{-1} \; d^{\beta^1 + \ldots + \beta^i} ([\delta, \varepsilon])d^{-1}d^{\varepsilon}
\]

\[
= ([\delta, \varepsilon])d^{-1} \; d^{\beta^1 + \ldots + \beta^i + 1} \; \varepsilon \mod [R, F].
\]

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

\[
\delta(e^{\beta^1} \cdots e^{\beta^i} \varepsilon)\delta^{-1} \times (\varepsilon^{-1} e^{-\delta} e^{-\delta} \cdots e^{-\beta^1})
\]

\[
e^{\beta^1} e^{\beta^1} \cdots e^{\beta^i} \varepsilon \times \varepsilon^{-1} e^{-\delta} e^{-\delta} \cdots e^{-\beta^1}
\]

\[
e(\varepsilon d^{\beta^2 + \ldots + 1} \varepsilon) \cdots (\varepsilon^{\beta^1 + 1} \varepsilon)(\varepsilon^{-1} d \varepsilon)^{-1}(d^{\beta^1 + 1} \varepsilon)^{-1} \cdots (d^{\beta^2 + \ldots + 1} \varepsilon)^{-1}
\]

\[
= [\varepsilon, (d^{\beta^2 + \ldots + 1} \varepsilon) \cdots (d^{\beta^1 + 1} \varepsilon)]d
\]

\[
= [\varepsilon, d^{\beta^1}] [\varepsilon, d^{\beta^2}]^2 \cdots [\varepsilon, d^{\beta^i}]^{p-2} [\varepsilon, d]^{p-1} \mod [R, F],
\]

where the last congruence is obtained from \([\varepsilon, d^{\beta^i}] = [\varepsilon, (e^{Q(y-1)})^{\beta^i}] \in R\) 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

\[
[\delta, e^{\delta^{k-1} + \ldots + \delta} + 1] \equiv \prod_{k=0}^{p-2} [\varepsilon, e^{Q(y-1)(Q(y-1) + 1)^k}]_{p-1-k}
\]

\[
= [\varepsilon, e^{N(y-1)}] \mod [R, F].
\]

Now, dividing \(N(T)\) by the distinguished polynomial \(P_k(T)\), we write

\[
N(\gamma - 1) = a_p(\gamma - 1)^{p-1} + \cdots + a_0 + P_k(\gamma - 1) f(\gamma - 1)
\]

\[
= b_p(\gamma - 1)^{p-1} + \cdots + b_0 + P_k(\gamma - 1) f(\gamma - 1) \; (a_i, b_i \in \mathbb{Z}_p).
\]
Then $b_0 \equiv \cdots \equiv b_{p-2} \equiv 0 \pmod{p}$ 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

$$[\varepsilon, e^{N^*(p-1)}] \equiv [\varepsilon, e^{\gamma_{p-1}}] \equiv \cdots [\varepsilon, e^\gamma]^{a_p} \mod [R, F]$$

and $a_i = \sum_{j=0}^{p-1} (\begin{bmatrix} i \end{bmatrix})(-1)^{j-i} b_j \equiv (-1)^i (p-1) b_{p-1} \pmod{p}$. Finally, for $1 \leq i \leq (p-1)/2$,

$$[\varepsilon, e^\gamma]^{a_i} \equiv [\varepsilon, e^{\gamma_{p-1}}]^{a_i} \equiv [\varepsilon, e^{\gamma_{p-1}}]^{a_{p-1}} \mod [R, F](R \cap [F, F])^p$$

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

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

By Lemma 3.5, this implies that $\Phi$ 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 $X(K_n)$ is not abelian for any $n \geq 1$.

### 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 $p \mid l - 1$ (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 $\lambda_k = \lambda_K \leq 1$ similarly as in §3 by [14]. Then $\lambda_K = \lambda_K' = p\lambda_k + p - 1$, $X(K_{\infty})$ is cyclic over $\Lambda$ and $\#A(K) = p^{m+1}$. Here $m$ is defined by $\#A(k) = p^m$ by Corollary 2.2. Let $\tilde{p}_n$ (resp. $\tilde{l}_n$) be a prime in $L(K_n)$ lying above $p$ (resp. $l$). We define $J \in \text{Gal}(L(K_n)/K_n^+)$ as an element of order 2 in the decomposition subgroup of $\tilde{p}_n$ in $\text{Gal}(L(K_n)/K_n^+)$. Then a prime $\tilde{l}_n^i$ in $L(K_n)$ is a conjugate of $\tilde{l}_n$ and the principal ideal $(l)$ in $k$ splits as $(l) = \mathfrak{l}_n^l$, where $\mathfrak{l}_n := \tilde{l}_n \cap k$. We use the notation as in §3; namely, $\Gamma = \langle \tilde{\gamma} \rangle$, $\Gamma_n$, $\Delta = \langle \tilde{\delta} \rangle$, $G_n$, $\gamma_n$, $\tilde{\gamma}_n$, $\delta_n$, $\tilde{\delta}_n$, $\epsilon_n$, $\tilde{\epsilon}_n$.

**Lemma 4.1.** The primes $l$ and $l^i$ 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 $\delta, \epsilon$ and $R := \langle \delta^p, \epsilon^{p^{m+1}}, [\delta, \epsilon] \rangle_F$. Then $G_0 \simeq F / R$, and so that $H_2(G_0, \mathbb{Z}_p) \simeq \langle [\delta, \epsilon] \rangle [R, F] / [R, F]$. On the other hand, the decomposition group of $\bar{1}_0$ (resp. $\bar{1}_0'$) in $G_0$ is $\langle \delta_0 \rangle \oplus \langle \epsilon_0'' \rangle$ (resp. $\langle \delta_0 \epsilon_0'' \rangle \oplus \langle \epsilon_0'' \rangle$) since $\bar{1}_0'$ is ramified in $K / k$ for some $u, v \in \mathbb{Z}_p$. Since $\bar{L}(K) = L(K)$ by the cyclicity of $A(K)$, applying Proposition 2.3, we have $v \in \mathbb{Z}_p$. This implies that the decomposition groups equal to $G_0$. Hence $l$ and $l'$ 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 $\langle \delta_0, \epsilon_0'' \rangle$ is the maximal subextension $L(k)$ which is unramified at $\bar{1}_0, \bar{1}_0'$. 

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 $\Lambda$-modules, $[G_n, G_n] \simeq (T, p^{m+1})/(P_K(T), \omega_h(T))$. Moreover $G_n^{ab} = \langle \gamma_n \rangle \oplus \langle \delta_n \rangle \oplus \langle \delta_n \rangle \simeq \mathbb{Z} / p^n \mathbb{Z} \oplus \mathbb{Z} / p \mathbb{Z} \oplus \mathbb{Z} / p^{m+1} \mathbb{Z}$.

We define $A(T) \in \Lambda$ by $[\delta_n, \gamma_n] = \epsilon_n^{A(T)}$. 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 $\bar{\gamma}_n$. Then there is an element $B(T) \in (p^n, T)$ defined uniquely up to the modulus $P_K(T)$ such that

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

Therefore the exact sequence $1 \to X(K_n) \to G_n \to \Gamma_n \times \Delta \to 1$ splits.

(ii) Let $Z_1, Z_1'$ be the decomposition groups of $\bar{1}_n$ and $\bar{1}_n'$, respectively. Then, changing $\epsilon_n$, if necessary, there is an element $J(T) \in (p^n, T)$ defined uniquely up to the modulus $P_K(T)$ such that

$$Z_1 = \langle \gamma_n \epsilon_n^{-1/(1 + T)} \rangle \oplus \langle \delta_n \rangle, \quad P_K(T) \mid A(T) - Q(T).$$

$$Z_1' = \langle \gamma_n \epsilon_n^{1/(1 + T)} \rangle \oplus \langle \delta_n \epsilon_n^{J(T)} \rangle, \quad P_K(T) \mid -A(T) - Q(T) + T(1 + Q(T))J(T)$$

for any $n \geq m + 1$ and $J(0) \equiv u \mod p^{m+1}$. 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 $\bar{\delta}_n \bar{\epsilon}_n^w$ for some $w \in p^n \mathbb{Z}_p$ (In fact, $w \neq 0, w \neq v \mod p^{m+1}$, since the image $\langle \bar{\delta}_0 \bar{\epsilon}_0^w \rangle$ under a projection of $Z_p$ in $G_0^{ab}$ coincide neither the inertia groups of $\bar{1}_n$ nor of $\bar{1}_n'$). 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 $B(T) \in (p^n, T)$ defined up to the modulus $P_K(T)$ such that $B(0) \equiv w \mod p^{m+1}$ and

$$Z_p = \langle \gamma_n \rangle \oplus \langle \delta_n \epsilon_n^{B(T)} \rangle \simeq \langle \bar{\gamma}_n \rangle \oplus \langle \bar{\delta}_n \bar{\epsilon}_n^w \rangle.$$
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 $1$ does not split in $K_\infty/K$, $1$ 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 $G_n$ is generated by $\tilde{\delta}_n$ and $\tilde{\gamma}_n \varepsilon_n^{\delta_n}$, where $v \in \mathbb{Z}^\times$ is defined in the proof of Lemma 4.1. Hence $Z_l$ is generated by $\delta_n$ and $\gamma_n \varepsilon_n^{u + C(T)}$ for some $C(T) \in (p^{m+1}, T)$. Moreover, since $\langle \delta_n \rangle \triangleleft Z_l$ and $[G_n, G_n] \cap \langle \delta_n \rangle = 1$, we find

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

The decomposition group of $\tilde{u}_l$ is given by $Z_l^{\tilde{u}} = \langle J(\gamma_n \varepsilon_n^{u + C(T)})^{-1} \rangle \oplus \langle J \delta_n J \rangle$. We find $JxJ^{-1} + x = 0$ for any $x \in X(K_n)$ since $A(K_n^\times) = 0$. Also we find $J \gamma_n J^{-1} = \gamma_n$ since the natural projection from the decomposition group of $\tilde{\gamma}_n$ in $\text{Gal}(L(K_n)/K^\times)$ to the abelian group $\text{Gal}(K_n/K^\times)$ is an isomorphism. On the other hand, $\langle J \delta_n J \rangle$ is the inertia group of $\tilde{u}_l$, so that we may assume, changing $u$ if necessary, that the image of a projection of $J \delta_n J$ in $G_n$ is $\tilde{\delta}_n \varepsilon_n^{\delta_n}$. 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

$$Z_l = \langle \gamma_n \varepsilon_n^{u + C(T)} \rangle \oplus \langle \delta_n \varepsilon_n^{j(T)} \rangle,$$

$$P_K(T) \mid -A(T) + Q(T)(1 + T)(u + C(T)) + T(1 + Q(T))J(T),$$

where $J(T) := u + j(T)$. Since $v \in \mathbb{Z}^\times_p$, changing $\varepsilon_n$, 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 $J(T) \equiv 2B(T) \mod P_K(T)$ 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 $Q(T)$ mod $P_K(T)$ for vanishing the constant term if necessary, we may assume that

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

since $p^{m+1} \mid P_K(0)$. 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

$$u \equiv 2Q'(0) \mod p, \quad J'(0) \equiv -2Q'(0)^2 + Q''(0) \mod p.$$
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 \( G_n \simeq X(K_n) \times (\Gamma_n \times \Delta) \) 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.

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

\[ R := \langle \gamma^3, \delta^3, \varepsilon^p \gamma^{(\gamma - 1)}, [\delta, \gamma](\varepsilon Q(\gamma - 1))^{-1}, [\delta, \varepsilon](\varepsilon Q(\gamma - 1))^{-1}, [\varepsilon, \gamma^2] \rangle_F \]

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:

\[ [\varepsilon^2 \gamma^2, \varepsilon^2 \gamma^2] \equiv [\varepsilon, \varepsilon \gamma^2]^1_{i=1} \mod (R \cap [F, F])^3/R, F]. \]

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 \( 1 \rightarrow R \rightarrow F \rightarrow G_n \rightarrow 1 \) is exact, where the map \( \phi: F \rightarrow G_n \) is given by \( \gamma \mapsto \gamma_n, \delta \mapsto \delta_n, \varepsilon \mapsto \varepsilon_n \).

(ii) \( R \cap [F, F]/[F, F] = \langle [\varepsilon, \varepsilon \gamma^2], C, D \rangle[R, F]/[R, F] \).

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.

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

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

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

\[ [\varepsilon^{f(\gamma - 1)}, \gamma]^0 \equiv ((W_f E^{-1})^{(\gamma - 1)})^{-1}(\varepsilon^{Q(\gamma - 1)})^{-1}[\varepsilon, \varepsilon \gamma^2 ]_{i=1}^{q_1 \gamma + q_0 + q_0^2} \].
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 $[(\varepsilon f(\gamma - 1))\delta, C] \in [R, F]$,

$$[\varepsilon f(\gamma - 1), \gamma]^\delta = [(\varepsilon f(\gamma - 1))\delta, \gamma^\delta]$$

$$= [(\varepsilon f(\gamma - 1))\delta, C \varepsilon^{Q(\gamma - 1)} \gamma]$$

$$= [(\varepsilon f(\gamma - 1))\delta, C][(\varepsilon f(\gamma - 1))\delta, \varepsilon^{Q(\gamma - 1)} \gamma]C^{-1}$$

$$= [(\varepsilon f(\gamma - 1))\delta, \varepsilon^{Q(\gamma - 1)} \gamma] = [[(\varepsilon^\delta)^\delta f_1(\varepsilon f_0)^\delta, \varepsilon^{Q(\gamma - 1)} \gamma].$$

We find

$$(\varepsilon f_0)^\delta = (\varepsilon f_0) = (D_{\varepsilon}^{Q(\gamma - 1) + 1} f_0)$$

$$= D_{\varepsilon}^{f_0} (D_{\varepsilon}^{Q(\gamma - 1) + 1} f_0),$$

$$(\varepsilon f_1 \gamma)^\delta = ((\varepsilon^\delta)^\delta f_1 = (\{\delta, \gamma\} (\varepsilon^\delta)^\delta [\delta, \gamma]^{-1}) f_1$$

$$= (C \varepsilon^{Q(\gamma - 1)} (D_{\varepsilon}^{Q(\gamma - 1) + 1} \gamma (\varepsilon^{Q(\gamma - 1) - 1} C^{-1} f_1)$$

$$= r(\varepsilon^{Q(\gamma - 1) + 1} f_1 \gamma$$

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

$$[\varepsilon f(\gamma - 1), \gamma]^\delta = [[(\varepsilon^{Q(\gamma - 1) + 1} f_1 \gamma (\varepsilon^{Q(\gamma - 1)} f_0) \varepsilon^{Q(\gamma - 1)} \gamma]$$

$$= [r' \varepsilon^{Q(\gamma - 1) + 1} (f_1 \gamma f_0) \varepsilon^{Q(\gamma - 1)} \gamma]$$

(for some $r' \in R$ by (7))

$$= [W f, \varepsilon^{Q(\gamma - 1)} \gamma]$$

$$= W_f \varepsilon^{Q(\gamma - 1)} W_f^{-\gamma} (\varepsilon^{Q(\gamma - 1) - 1}.$$

On the other hand, $E^{\gamma - 1} = \varepsilon^{Q(\gamma - 1)} [\varepsilon, \varepsilon^\gamma]^{q_1 q_0}$ by (7). Therefore, again by (7),

$$\varepsilon^{Q(\gamma - 1)} = [E^\gamma, E^{-1}] E^{-1} E^{\gamma} [\varepsilon, \varepsilon^\gamma]^{q_1 q_0}$$

$$= E^{-1} E^{\gamma} [\varepsilon, \varepsilon^\gamma]^{q_1 q_0 + q_1 q_0 + q_0^2}. $$

Combining this with the above, we obtain the lemma. 

Lemma 4.7. (i) $[\delta \varepsilon^{B(\gamma - 1)}, \gamma] \equiv C[\varepsilon, \varepsilon^\gamma]^{q_1^2 + q_1 q_0 + q_0^2}$,

(ii) $[\delta, \gamma \varepsilon^{-\gamma}] \equiv C D^{-1}$,

(iii) $[\delta \varepsilon^{J(\gamma - 1)}, \gamma \varepsilon^{-\gamma}] \equiv C D[\varepsilon, \varepsilon^\gamma]^{q_1^2 + q_0^2 - q_1 - q_0 - J(0)}.$

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

$$[\delta \varepsilon^{B(\gamma - 1)}, \gamma] = [\varepsilon^{B(\gamma - 1)}, \gamma]^\delta [\delta, \gamma]$$

$$= ((W_B E^{-1})^{-1} (\varepsilon^{Q(\gamma - 1)) - 1} [\varepsilon, \varepsilon^\gamma]^{q_1^2 + q_1 q_0 + q_0^2} [\delta, \gamma]$$

$$= C[\varepsilon, \varepsilon^\gamma]^{q_1^2 + q_1 q_0 + q_0^2}. $$
In the same way,
\[
[\delta, \gamma e^{-\gamma^{-1}}] = [\delta, e^{-1}\gamma] = [\delta, e^{-1}][\delta, \gamma]e^{-1} = e^{-1}[\delta, \gamma]e^{-1} = e^{-1}(e^Q)^{-1}D^{-1}e^{-1}C e^Q e^{-1}e
\]
\[
\equiv CD^{-1}.
\]

Finally, we compute \([\delta e^{J(\gamma^{-1})}, \gamma e^{\gamma^{-1}}] = [\delta e^{J(\gamma^{-1})}, e][\delta e^{J(\gamma^{-1})}, \gamma]^e\). Note that the relation \(P_k(T) | J(T)(1 + Q(T)) - 2Q(T)/T\) implies that \(W_j E^{-2} \in R\). Since \(J(T) = J(0)T + J(0)\), it turns out that
\[
\begin{align*}
[\delta e^{J(\gamma^{-1})}, e] = [e^{J(\gamma^{-1})}, e]^e[\delta, e] &\equiv [\delta, e^\gamma]^{-J(0)}D e^Q e^{-1},

[\delta e^{J(\gamma^{-1})}, \gamma] = [e^{J(\gamma^{-1})}, \gamma]^e[\delta, \gamma] &\equiv ((W_j E^{-1})^{\gamma^{-1}}) e^Q e^{-1} C[e, e^\gamma]^{q_1 + q_0 + q_0^2} e
\end{align*}
\]
\[
\equiv (W_j E^{-1})^{\gamma^{-1}}C[e, e^\gamma]^{q_1 + q_0^2}.
\]

In fact, the last congruence follows from the congruences
\[
(W_j E^{-1})^{\gamma^{-1}} = [\gamma, W_j E^{-2} E] \equiv E^{\gamma^{-1}} \equiv e^Q e^{-1} e^{q_1 + q_0}.
\]

Therefore
\[
[\delta e^{J(\gamma^{-1})}, \gamma e^{\gamma^{-1}}] \equiv [e, e^\gamma]^{-J(0)}D e^Q e^{-1} e^{e^Q e^{-1} C[e, e^\gamma]^{q_1 + q_0^2} e^{-1}}
\]
\[
\equiv [e, e^\gamma]^{-J(0)}D[e, e^Q e^{-1}] C[e, e^\gamma]^{q_1 + q_0^2}
\]
\[
\equiv CD[e, e^\gamma]^{q_1 + q_0^2} = J(0).
\]

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 \(\bar{L}(K_n) = L(K_n)\) if and only if the three elements \(C[e, e^\gamma]^{q_1 + q_0 + q_0^2}, CD^{-1}, CD^{q_1 + q_0 - q_0 - J(0)}\) generate the group \([e, e^\gamma], C, D][R, F]/(R \cap [F, F])^3[R, F]\). Since \(J(0) \equiv -2(q_1 + q_0)^2 + 2q_1 \equiv 1 - q_1 \mod 3\) by (6), we see that this is equivalent to \((q_1 + q_0)^2 + q_1 + q_0 + J(0) \equiv q_0 - 1 \equiv 0 \mod 3\). To complete the proof of Theorem 1.2, we show the following:

**Lemma 4.8.** Put \(P_k(T) = T^2 + c_1 T + c_0 \ (c_1, c_0 \in 3\mathbb{Z}_3)\), then \(c_0 \equiv 3 \mod 3^2\) and \(q_0 \not\equiv 1 \mod 3\) if and only if \(P_k(-1) \equiv 4 - c_1 \not\equiv 1 \mod 3^2\).
Proof. Dividing by $P_K(T) = T^2 + c_1 T + c_0$, $Q(T)$ has the form $Q(T) = q_1 P_K(T) + r T - c_0 q_1$, where $r := q_1 + q_0 - c_1 q_1 \in \mathbb{Z}_3^*$. Then, by Proposition 2.1, $P_K(T)$ has the form

$$P_K(T) = (\Lambda \text{-unit})(Q(T)^2 + 3Q(T) + 3) \equiv (\Lambda \text{-unit})(r T^2 - c_0 q_1)^2 + 3(r T - c_0 q_1) + 3) \mod P_K(T).$$

Hence $P_K(T) | (r T - c_0 q_1)^2 + 3(r T - c_0 q_1) + 3$. Therefore we get

$$P_K(T) = (\Lambda \text{-unit})(r T^2 - c_0 q_1)^2 + 3(r T - c_0 q_1) + 3) = T^2 + r^{-1}(3 - 2c_0 q_1)T + r^{-2}(c_0 q_1^2 - 3c_0 q_1 + 3),$$

where note that the leading coefficient of the last polynomial is 1 since the characteristic polynomial $P_K(T)$ is distinguished. Therefore we obtain $c_1 r = 3 - 2c_0 q_1$, $c_0 r^2 = c_0^2 q_1^2 - 3c_0 q_1 + 3$. Put $c_i = 3\tilde{c}_i$ ($i = 1, 0$), then

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

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

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., $A(K_1) \simeq (\mathbb{Z}/3^2\mathbb{Z})^6$.

**Proof.** We know

$$A(K_1) \simeq \Lambda/(P_K(T), T^3 + 3T^2 + 3T) \simeq \Lambda/(P_K(T), (3 - c_0 - 3c_1 + c_1^2)T - c_0(3 - c_1))$$

by (1). Then we can easily check $3^2 | (3 - c_0 - 3c_1 + c_1^2)T - c_0(3 - c_1)$, 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

$$A(K_1) \simeq \Lambda/(P_K(T), 3^2) \simeq (\mathbb{Z}/3^2\mathbb{Z})^{18}.$$

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

$$A(K_1) \simeq \Lambda/(P_K(T), 3^2(s_1 T + 3s_0))$$

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

$$0 \rightarrow (P_K(T), 3^2) \rightarrow (P_K(T), 3^2(s_1 T + 3s_0)) \rightarrow \Lambda \rightarrow (P_K(T), 3^2) \rightarrow 0.$$
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. \hfill \Box

**Example.** Let $k = \mathbb{Q}(\sqrt{-m})$ and $K^+$ an abelian 3-extension of conductor $l = 43$. If $m = 7, 30, 37$, then $A(K_1) \simeq (\mathbb{Z}/3^2\mathbb{Z})^2$ 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:

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

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**


THE COMMUTATIVITY OF THE GALOIS GROUPS II


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