Fujii, S.
Osaka J. Math.
45 (2008), 41–60

ON THE MAXIMAL PRO-p EXTENSION UNRAMIFIED OUTSIDE p OF AN IMAGINARY QUADRATIC FIELD

SATOSHI FUJII

(Received January 10, 2006, revised December 19, 2006)

Abstract

In this article, we study the group structure of the Galois group of the maximal pro-p extension unramified outside p of imaginary quadratic fields by using Iwasawa theory.

1. Results

Let k be a number field. Throughout this article, denote by p an *odd* prime number. Let M_k/k be the maximal pro-p extension unramified outside all primes lying above p and $G_k(p) = \mathrm{Gal}(M_k/k)$ its Galois group. In the case k is a finite extension of $\mathbb{Q}$, many deep investigations on extensions with restricted ramification have been made under several motivation, which was originated in Shafarevich's work [17].

The most basic invariants of $G_k(p)$ are the minimal number of topological generators (the generator rank) and the minimal number of defining relations (the relation rank), of $G_k(p)$. These invariants can be expressed by the dimensions of cohomology groups as follows;

$\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p)$ = the minimal number of topological generators of $G_k(p)$,

$\dim_{\mathbb{F}_p} \mathrm{H}^2(G_k(p), \mathbb{Z}/p)$ = the minimal number of defining relations of $G_k(p)$.

Here $\mathbb{F}$ stands for the field of p-elements. It is also well known that the p-cohomological dimension of $G_k(p)$ is less than 3, the Euler-Poincaré characteristic satisfies the equation

$$\sum_{i=0}^{2}(-1)^i \dim_{\mathbb{F}_p} \mathrm{H}^i(G_k(p), \mathbb{Z}/p) = -r_2(k), \tag{1}$$

where $r_2(k)$ is the number of complex primes of k, and Leopoldt's conjecture for k and p implies that $\mathrm{H}^2(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p) = 0$, and so on, see Section 8 and 10 of [14] for reference.

It is known that the generator rank and the relation rank of $G_k(p)$ can be expressed by arithmetic invariants of k (see Section 8.7 of [14]). Also, there are two types of relation,the first one is "local relation", which comes from the relation of Galois groups

2000 Mathematics Subject Classification. 11R23.

of local fields. The second one is called "unknown relation", which is suggested by Koch [8]. We shall explain the definition of unknown relation for the extension M_k/k. Let $\mathfrak{p}$ be a prime of a number field k lying above p, $k_\mathfrak{p}$ the completion of k at $\mathfrak{p}$ and $G_{k_\mathfrak{p}}(p)$ the Galois group of the maximal pro-p extension $M_{k_\mathfrak{p}}/k_\mathfrak{p}$. By the natural mapping $G_{k_\mathfrak{p}}(p) \to G_k(p)$ induced from an inclusion $k \hookrightarrow k_\mathfrak{p}$, we can get a mapping of cohomology groups $\mathrm{H}^i(G_k(p), \mathbb{Z}/p) \to \mathrm{H}^i(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p)$. If the kernel of the product of the above maps $\mathrm{H}^2(G_k(p), \mathbb{Z}/p) \to \prod_{\mathfrak{p}|p} \mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p)$ is non-trivial, then we call $G_k(p)$ has an unknown relation.

When the relation rank of $G_k(p)$ is greater than 0, there is no general theory to describe forms of relations. The results of Fröhlich [1] and Koch [8], [9] (Chapter 11) are the case where all relations are local relation. Also, Komatsu [10] found a real quadratic field such that $G_k(p)$ has an unknown relation. Looking at these results, one will have a question, that is, what happens when k is an imaginary quadratic field? In this article, we will study $G_k(p)$ when $\dim_{\mathbb{F}_p} \mathrm{H}^2(G_k(p), \mathbb{Z}/p)$ is at most one. Our results in this article are as follows:

- (Theorem 4.1) Giving a characterization in terms of the ideal class groups such that $G_k(p)$ is a free pro-p group.
- (Theorem 5.1) Describing a form of relations of $G_k(p)$ modulo a closed normal subgroup of infinite index of a free pro-p group of rank 3 in two cases where $\dim_{\mathbb{F}_p} \mathrm{H}^2(G_k(p), \mathbb{Z}/p) = 1$. In particular, we will give the explicit structure of the maximal pro-p class 2 quotient of $G_k(p)$ in these cases. Besides, we will discuss that $G_k(p)$ has an unknown relation or not.

For the first result, we must recall here that a characterization of the relation rank of $G_k(p)$ had already been obtained in terms of arithmetic invariants of k. However, for small prime numbers p, the author thinks that our characterization is convenient even though we have to treat the ideal class groups of other fields. For the second result, our method is based on the Kummer theory over the cyclotomic $\mathbb{Z}_p$-extension which was studied by Iwasawa [7]. Komatsu [10] had studied $G_k(p)$ by using the cyclotomic $\mathbb{Z}_p$-extension to obtain a form of relations of $G_k(p)$ modulo $[G_k(p), [G_k(p), G_k(p)]]$, and more general result on totally real fields is obtained by Nguyen Quang Do [15].

The contents of this article are as follows. In Section 2 we determine the Galois module structure of the p-unit group of the cyclotomic $\mathbb{Z}_p$-extension of certain abelian fields. This argument is a keystone of Kummer theory over cyclotomic $\mathbb{Z}_p$-extensions. In Section 3 we give a brief guide of Iwasawa's work [7] on the Kummer pairing over the cyclotomic $\mathbb{Z}_p$-extension. In Section 4 we prove Theorem 4.1. In Section 5 we show Theorem 5.1 by using an idea from pro-p Γ-operator groups. Besides, we will discuss that when $G_k(p)$ has an unkown relation. In Section 6 we will give examples of Theorem 5.1.

2. The Galois module structure of the p-unit group

Throughout this article, we shall denote by k_∞ and k_n the cyclotomic $\mathbb{Z}_p$-extension and the n-th layer of k_∞/k, namely, unique subextension of k_∞/k with $[k_n : k] = p^n$, of a number field k.

Let K be an abelian field such that K contains the group of p-th roots of unity μ_p and that the exponent of the Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ is $p-1$, for example, $K = \mathbb{Q}(\mu_p)$ or $K = \mathbb{Q}(\sqrt{m}, \mu_p)$ for some integer m. Let D_p be the decomposition group in Δ at p. Let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K. In this case K_∞ is the field $K(\mu_{p^\infty})$ obtained by adjoining all p-power-th roots of unity μ_{p^∞}. Put $\bar{\Gamma}_n = \mathrm{Gal}(K_n/K)$ for $n \geq 0$. From the condition on K, we have the canonical decomposition

$$\mathrm{Gal}(K_n/\mathbb{Q}) = \Delta \times \bar{\Gamma}_n$$

of $\mathrm{Gal}(K_n/\mathbb{Q})$. Let E'_{K_n} be the p-unit group of K_n. In this section, we describe the structure of $E'_{K_n} \otimes \mathbb{Q}$ as a $\mathbb{Q}[\Delta \times \bar{\Gamma}_n]$-module in terms of Δ, D_p and $\bar{\Gamma}_n$. Let $\bar{\Delta} = \Delta/\langle J \rangle$, where J is the complex conjugation. For a finite group H, let $N_H = \sum_{h \in H} h \in \mathbb{Z}[H]$ be the norm operator of H.

Proposition 2.1. *There is an isomorphism*

$$E'_{K_n} \otimes \mathbb{Q} \simeq \mathbb{Q}[\bar{\Gamma}_n]/(N_{\bar{\Gamma}_n}) \oplus \mathbb{Q}[\bar{\Gamma}_n \times \bar{\Delta}]/(N_{\bar{\Delta}}) \oplus \mathbb{Q}[\Delta/D_p]$$

of $\mathbb{Q}[\Delta \times \bar{\Gamma}_n]$*-modules.*

Proof. Let $v_\mathfrak{p}$ be the normalized $\mathfrak{p}$-adic valuation of a finite prime $\mathfrak{p}$. Also, let

$$\mathcal{V}_p \colon E'_{K_n} \to \prod_{\mathfrak{p}|p} \mathbb{Z}, \quad x \mapsto (v_\mathfrak{p}(x))_\mathfrak{p}$$

be the product of the valuation maps of the primes lying above p. Note that $\prod_{\mathfrak{p}|p} \mathbb{Z}$ is a $\mathbb{Z}[\Delta \times \bar{\Gamma}_n]$-module with the $\Delta \times \bar{\Gamma}_n$-action defined by $g \cdot (x_\mathfrak{p})_\mathfrak{p} = (x_{g^{-1}\mathfrak{p}})_\mathfrak{p}$ for $g \in G \times \bar{\Gamma}_n$ and $(x_\mathfrak{p})_\mathfrak{p} \in \prod_{\mathfrak{p}|p} \mathbb{Z}$, and the above mapping is a $\mathbb{Z}[\Delta \times \bar{\Gamma}_n]$-homomorphism. Furthermore, $\prod_{\mathfrak{p}|p} \mathbb{Z}$ is isomorphic to $\mathbb{Z}[\Delta/D_p]$ as $\mathbb{Z}[\Delta \times \bar{\Gamma}_n]$-modules since the decomposition group at p is $D_p \times \bar{\Gamma}_n$. Let $h_\mathfrak{p}$ be a positive integer such that $\mathfrak{p}^{h_\mathfrak{p}} = (\alpha_\mathfrak{p})$ for each prime $\mathfrak{p}$ dividing p and an integer $\alpha_\mathfrak{p}$ of K_n. By the choice of $h_\mathfrak{p}$, we find that

$$\prod_{\mathfrak{p}|p} h_\mathfrak{p}\mathbb{Z} \subseteq \mathrm{Image}(\mathcal{V}_p) \subseteq \prod_{\mathfrak{p}|p} \mathbb{Z},$$

whence $\#\mathrm{Coker}\, \mathcal{V}_p$ is finite. Therefore $\mathcal{V}_p$ induces a surjective mapping

$$\mathcal{V}_p \otimes 1 \colon E'_{K_n} \otimes \mathbb{Q} \to \mathbb{Q}[\Delta/D_p]$$

of $\mathbb{Q}[\Delta \times \bar{\Gamma}_n]$-modules. Note that the kernel of $\mathcal{V}_p$ is the unit group E_{K_n} of K_n. The existence of Minkowski units implies that there is an isomorphism

$$E_{K_n} \otimes \mathbb{Q} \simeq \mathbb{Q}[\bar{\Delta} \times \bar{\Gamma}_n]/(N_{\bar{\Delta} \times \bar{\Gamma}_n})$$

of $\mathbb{Q}[\Delta \times \bar{\Gamma}_n]$-modules.

Lemma 2.1. *Let G_1 and G_2 be finite groups. Then*

$$\begin{aligned}\mathbb{Q}[G_1 \times G_2]/(N_{G_1 \times G_2}) &\simeq \mathbb{Q}[G_1]/(N_{G_1}) \oplus \mathbb{Q}[G_1 \times G_2]/(N_{G_2}) \\ &\simeq \mathbb{Q}[G_2]/(N_{G_2}) \oplus \mathbb{Q}[G_1 \times G_2]/(N_{G_1})\end{aligned}$$

as $\mathbb{Q}[G_1 \times G_2]$-modules.

Proof. The second isomorphism follows if we show the first one. Let $\psi\colon \mathbb{Q}[G_1 \times G_2] \to \mathbb{Q}[G_1]/(N_{G_1})$ be a mapping defined by

$$\sum_{g_1 g_2 \in G_1 \times G_2} a(g_1, g_2) g_1 g_2 \mapsto \sum_{g_1 g_2 \in G_1 \times G_2} a(g_1, g_2) g_1 \mod (N_{G_1}).$$

Then we have a natural mapping

$$\phi\colon \mathbb{Q}[G_1 \times G_2] \to \mathbb{Q}[G_1]/(N_{G_1}) \oplus \mathbb{Q}[G_1 \times G_2]/(N_{G_2}), \quad \phi(x) = (\psi(x), x \bmod (N_{G_2}))$$

of $\mathbb{Q}[G_1 \times G_2]$-modules. Suppose that $x = \sum_{g_1 g_2 \in G_1 \times G_2} x(g_1, g_2) g_1 g_2$ is in $\operatorname{Ker} \phi$. Then $x = N_{G_2} y$ for some $y \in \mathbb{Q}[G_1 \times G_2]$. Put $y = \sum_{g_1 g_2 \in G_1 \times G_2} y(g_1, g_2) g_1 g_2$. Thus $x = N_{G_2} y = N_{G_2} \sum_{g_1 g_2 \in G_1 \times G_2} y(g_1, g_2) g_1$. On the other hand, we have

$$\sum_{g_1 g_2 \in G_1 \times G_2} x(g_1, g_2) g_1 = \#G_2 \sum_{g_1 g_2 \in G_1 \times G_2} y(g_1, g_2) g_1 = N_{G_1} z$$

for some $z \in \mathbb{Q}$. Hence

$$\sum_{g_1 g_2 \in G_1 \times G_2} y(g_1, g_2) g_1 = \frac{z}{\#G_2} N_{G_1}.$$

Therefore we obtain

$$x = N_{G_2} \sum_{g_1 g_2 \in G_1 \times G_2} y(g_1, g_2) g_1 = \frac{z}{\#G_2} N_{G_1} N_{G_2} = \frac{z}{\#G_2} N_{G_1 \times G_2},$$

so that $\mathrm{Ker}\phi \subseteq (N_{G_1\times G_2})$. The converse inclusion is clear. Hence we obtain an injective mapping

$$\bar{\phi}\colon \mathbb{Q}[G_1\times G_2]/(N_{G_1\times G_2}) \hookrightarrow \mathbb{Q}[G_1]/(N_{G_1})\oplus \mathbb{Q}[G_1\times G_2]/(N_{G_2}).$$

Since

$$\begin{aligned}\dim_{\mathbb{Q}} \mathbb{Q}[G_1\times G_2]/(N_{G_1\times G_2}) &= \#G_1\#G_2 - 1,\\ \dim_{\mathbb{Q}} \mathbb{Q}[G_1]/(N_{G_1}) &= \#G_1 - 1,\\ \dim_{\mathbb{Q}} \mathbb{Q}[G_1\times G_2]/(N_{G_2}) &= (\#G_2 - 1)\#G_1,\end{aligned}$$

we have $\#G_1\#G_2 - 1 = \#G_1\#G_2 - \#G_1 + \#G_1 - 1 = \#G_1(\#G_2 - 1) + \#G_1 - 1$, and hence the mapping $\bar{\phi}$ must be an isomorphism. □

By Lemma 2.1, we obtain an isomorphism

$$E_{K_n}\otimes\mathbb{Q} \simeq \mathbb{Q}[\bar{\Delta}\times\bar{\Gamma}_n]/(N_{\bar{\Delta}\times\bar{\Gamma}_n}) \simeq \mathbb{Q}[\bar{\Gamma}_n]/(N_{\bar{\Gamma}_n})\oplus\mathbb{Q}[\bar{\Delta}\times\bar{\Gamma}_n]/(N_{\bar{\Delta}})$$

of $\mathbb{Q}[\Delta\times\bar{\Gamma}_n]$-modules. Since $E_{K_n}\otimes\mathbb{Q}$ is the kernel of $\mathcal{V}_p$, we have

$$E'_{K_n}\otimes\mathbb{Q} \simeq \mathbb{Q}[\bar{\Gamma}_n]/(N_{\bar{\Gamma}_n})\oplus\mathbb{Q}[\bar{\Delta}\times\bar{\Gamma}_n]/(N_{\bar{\Delta}})\oplus\mathbb{Q}[\Delta/D_p]$$

as $\mathbb{Q}[\Delta\times\bar{\Gamma}_n]$-modules. □

3. Iwasawa's theorem on the Kummer pairing for abelian fields

In this section, we shall give a brief guide to the Kummer pairing over cyclotomic $\mathbb{Z}_p$-extensions, which was obtained by Iwasawa (see Sections 6, 7 and 8 of [7]). For reference, see also Chapter 11 of [14].

Let Γ be the Galois group of the cyclotomic $\mathbb{Z}_p$-extension of a number field. Fix an isomorphism $\mathbb{Z}_p[[\Gamma]] := \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}] \simeq \Lambda = \mathbb{Z}_p[[T]]$, the ring of formal power series of one variable with coefficients in $\mathbb{Z}_p$, by sending a fixed topological generator γ_0 of Γ to $1+T$ (see Section 7 of [18]). Since a pro-p Γ-module M is a $\mathbb{Z}_p[[\Gamma]]$-module, we regard M a Λ-module via $\gamma_0 m = (1+T)m$ for $m\in M$. For Λ-modules M and N, the Γ-action on $\mathrm{Hom}_{\mathbb{Z}_p}(M,N)$ is given by $(\gamma_0 f)(m) = \gamma_0 f(\gamma_0^{-1}m)$ for $m\in M$. Let $\kappa\colon \Gamma\to\mathbb{Z}_p^\times$ be the cyclotomic character. Let $T(1) = \varprojlim \mu_{p^n}$ be the Tate module and let $T(-1) = \mathrm{Hom}_{\mathbb{Z}_p}(T(1),\mathbb{Z}_p)$. Then $T(1)$ and $T(-1)$ are Γ-modules with the Γ-actions $\gamma_0 t_1 = \kappa(\gamma_0)t_1$ and $\gamma_0 t_{-1} = \kappa(\gamma_0)^{-1}t_{-1}$ for $t_1\in T(1)$ and $t_{-1}\in T(-1)$. For a Λ-module M, we then define the Tate twists $M(1)$ and $M(-1)$ of M by $M(\pm1) = M\otimes_{\mathbb{Z}_p} T(\pm1)$, so that $M(1)$ and $M(-1)$ are Λ-modules by the diagonal actions. One sees that $M(\pm1)\simeq M$ as abelian groups, but that $M(\pm1)$ are equipped with the Γ-action different from M. Also, let M° be the Λ-module with the new Γ-action $\gamma_0\circ m = \gamma_0^{-1}m$

for $m \in M^\circ$. Then we define the Iwasawa involution $M^\bullet$ of a Λ-module M by $M^\bullet = M(-1)^\circ = M^\circ(1)$. Note that the operator $*^\bullet$ works as an involution on Λ-modules, nemely, $(M^\bullet)^\bullet = (M^\circ(1))(-1)^\circ = (M^\circ)^\circ = M$. Finally, remark that if $f\colon M_1 \to M_2$ is a Λ-homomorphism, then the mapping $f^\bullet\colon M_1^\bullet \to M_2^\bullet$, which is induced by f, is also a Λ-homomorphism.

Let C be a compact Λ-module, D a discrete Λ-module and let

$$(\ ,\ )\colon C \times D \to \mu_{p^\infty},$$

be a non-degenerate pairing with the property $\gamma_0(c, d) = (\gamma_0 c, \gamma_0 d)$ for $c \in C$ and $d \in D$. Then we have an isomorphism

$$C \simeq \mathrm{Hom}_{\mathbb{Z}_p}(D, \mu_{p^\infty})$$

of Λ-modules. Then we also have a non-degenerate pairing

$$\langle\ ,\ \rangle\colon C(-1) \times D \to \mathbb{Q}_p/\mathbb{Z}_p$$

with $\langle \gamma_0 c, d\rangle = \langle c, \gamma_0^{-1} d\rangle$. In particular, the pairing $\langle\ ,\ \rangle$ induces an isomorphism $C(-1) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(D, \mathbb{Q}_p/\mathbb{Z}_p)$ of Λ-modules. Note that the pairing $\langle\ ,\ \rangle$ induces the pairing

$$\langle\ ,\ \rangle\colon C^\bullet \times D \to \mathbb{Q}_p/\mathbb{Z}_p$$

with the property $\langle \gamma_0 c, d\rangle = \langle c, \gamma_0 d\rangle$ (see Section 8.1 of [7]).

Here, we shall set the notations. Denote by $\mathfrak{X}_k$ the Galois group of the maximal pro-p abelian extension M_k^{ab}/k of a number field k which is unramified outside all primes lying above p. The Galois group $\mathfrak{X}_k$ is also defined to be the maximal pro-p abelian quotient $\mathfrak{X}_k = G_k(p)^{\mathrm{ab}}$ of $G_k(p)$. Let K be an abelian field of Section 2. Recall the definitions of K_∞ and K_n (see introduction of Section 2). Put $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ and recall $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. For a $\mathbb{Z}_p[\Delta]$-module M and a $\mathbb{Z}_p$-valued character χ of Δ, we have the χ-eigen-submodule M^χ of M as $M^\chi = \{x \in M \mid \delta m = \chi(\delta)m \text{ for all } \delta \in \Delta\}$. Further, we get a decomposition of M such that $M = \bigoplus_\chi M^\chi$. We then know that $\mathrm{Gal}(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$ acts on $\mathfrak{X}_{K_\infty}$ via $\sigma(x) = \bar{\sigma} x \bar{\sigma}^{-1}$ for $x \in \mathfrak{X}_{K_\infty}$ since $M_{K_\infty}^{\mathrm{ab}}/\mathbb{Q}$ is a Galois extension, where $\bar{\sigma} \in \mathrm{Gal}(M_{K_\infty}^{\mathrm{ab}}/\mathbb{Q})$ denotes a lift of σ. In particular, we get a decomposition $\mathfrak{X}_{K_\infty} = \bigoplus_\chi \mathfrak{X}_{K_\infty}^\chi$ of $\mathfrak{X}_{K_\infty}$ as a $\Lambda[\Delta]$-module. Let $\omega\colon \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) (\simeq (\mathbb{Z}/p\mathbb{Z})^\times) \to \mu_{p-1}\ (\subseteq \mathbb{Z}_p^\times)$ be the Teichmüller character of modulo p, namely, it satisfies the congruence $\omega(a) \equiv a \bmod p$. We will use these notations also in later sections.

By Kummer's duality, there is a subgroup $S \subseteq K_\infty^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and a non-degenerate pairing

$$\mathfrak{X}_{K_\infty} \times S \to \mu_{p^\infty}, \quad (x, s \otimes (1/p^n)) = x(\sqrt[p^n]{s})/\sqrt[p^n]{s}.$$

Note that this pairing satisfies the property $\sigma(x, s\otimes(1/p^n)) = (\sigma(x), \sigma(s)\otimes(1/p^n))$ for any $\sigma \in \mathrm{Gal}(K_\infty/\mathbb{Q})$. For a $\mathbb{Z}_p$-valued character χ of Δ, we then also have a non-degenerate pairing

$$\mathfrak{X}_{K_\infty}^{\chi} \times S^{\omega\chi^{-1}} \to \mu_{p^\infty}. \tag{2}$$

Let $E'_{K_\infty} = \bigcup_{n\geq 0} E'_{K_n}$. Let $N = K_\infty\left(\sqrt[p^\infty]{E'_{K_\infty}}\right)$ be the algebraic extension of K_∞ obtained by adjoining all p-power-th roots of p-units E'_{K_∞} of K_∞ and $\mathcal{X} = \mathrm{Gal}(N/K_\infty)$ its Galois group. Put $\mathcal{E} = E'_{K_\infty}\otimes\mathbb{Q}_p/\mathbb{Z}_p$. Then we have a non-degenerate pairing

$$\mathcal{X}^{\chi} \times \mathcal{E}^{\omega\chi^{-1}} \to \mu_{p^\infty}, \tag{3}$$

whence $\mathcal{X}^{\chi} \simeq \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{E}^{\omega\chi^{-1}}, \mu_{p^\infty})$ as Λ-modules. We shall analyze this pairing. Put $\mathcal{E}_n = E'_{K_n}\otimes\mathbb{Q}_p/\mathbb{Z}_p$. Let A'_{K_n} be the p-primary part of the p-ideal class group of K_n and put $A'_{K_\infty} = \varinjlim A'_{K_n}$, where the inductive limit is taken with respect to the lift maps of ideals. Let $X'_{K_\infty} = \varprojlim A'_{K_n}$, the projective limit is taken with respect to the norm maps. Let X'_f be the maximal finite Λ-submodule of X'_{K_∞}; Remark that X'_f is determined as the kernel of a pseudo-isomorphism from X'_{K_∞} to an elementary Λ-module. By Theorem 12 and the arguments in p.270 of [7], we know the following properties on $\mathcal{E}$ and $\mathcal{E}_n$:

- For all pairs of non-negative integers m, n with $m \geq n$, the natural mapping $\mathcal{E}_n \to \mathcal{E}_m$ is injective. In particular, the injectivity is also true on $\mathcal{E}_n \to \mathcal{E}$ for all $n \geq 0$.
- There are isomorphisms

$$\mathcal{E}^{\Gamma_n}/\mathcal{E}_n \simeq \mathrm{H}^1\left(\Gamma_n, E'_{K_\infty}\right) \simeq \mathrm{Ker}\left(A'_{K_n} \to A'_{K_\infty}\right) \simeq X'_f \tag{4}$$

of Λ-modules for all sufficiently large n.

Recall the Kummer pairing (3)

$$\mathcal{X}^{\chi} \times \mathcal{E}^{\omega\chi^{-1}} \to \mu_{p^\infty}.$$

Then we have a non-degenerate pairing

$$\langle\ ,\ \rangle\colon \mathcal{X}^{\chi}(-1) \times \mathcal{E}^{\omega\chi^{-1}} \to \mathbb{Q}_p/\mathbb{Z}_p,$$

from which the pairing $\mathcal{X}^{\chi\bullet} \times \mathcal{E}^{\omega\chi^{-1}} \to \mathbb{Q}_p/\mathbb{Z}_p$ is induced. Put $\omega_n = (1+T)^{p^n} - 1 \in \Lambda$. Let $\mathcal{X}_n^{\chi\bullet}$ be the annihilator of $\mathcal{E}_n^{\omega\chi^{-1}}$. Note that $\omega_n\mathcal{X}^{\chi\bullet}$ is the annihilator of $(\mathcal{E}^{\omega\chi^{-1}})^{\Gamma_n}$. Thus

$$\mathcal{X}_n^{\chi\bullet}/\omega_n\mathcal{X}^{\chi\bullet} \simeq \mathrm{Hom}_{\mathbb{Z}_p}\left(X_f'^{\omega\chi^{-1}}, \mathbb{Q}_p/\mathbb{Z}_p\right)^{\circ} \tag{5}$$

by isomorphism (4) for all sufficiently large n. Since $\mathcal{E}_n^{\omega\chi^{-1}}$ is a p-divisible group of finite $\mathbb{Z}_p$-corank, $\mathcal{X}^{\chi\bullet}/\mathcal{X}_n^{\chi\bullet}$ is a finitely generated free $\mathbb{Z}_p$-module of the same rank. We want to know its $\mathbb{Z}_p$-rank.

Lemma 3.1. *Let $d_\chi = 0$ or 1 according as χ is even or not and*

$$\rho_\chi = \begin{cases} 1 & \text{if } \omega\chi^{-1}(D_p) = 1,\ \chi \neq \omega, \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\operatorname{rank}_{\mathbb{Z}_p} \mathcal{X}^{\chi\bullet}/\mathcal{X}_n^{\chi\bullet} = d_\chi p^n + \rho_\chi$$

for all $n \geq 0$.

Proof. It follows from Proposition 2.1 that

$$\begin{aligned} \dim_{\mathbb{Q}_p}(E'_{K_n} \otimes \mathbb{Q}_p)^{\omega\chi^{-1}} &= \dim_{\mathbb{Q}_p}(\mathbb{Q}_p[\bar{\Gamma}_n]/(N_{\bar{\Gamma}_n}))^{\omega\chi^{-1}} \\ &\quad + \dim_{\mathbb{Q}_p}(\mathbb{Q}_p[\bar{\Delta} \times \bar{\Gamma}_n]/(N_{\bar{\Delta}}))^{\omega\chi^{-1}} \\ &\quad + \dim_{\mathbb{Q}_p} \mathbb{Q}_p[\Delta/D_p]^{\omega\chi^{-1}}. \end{aligned}$$

Since

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p[\bar{\Gamma}_n]/(N_{\bar{\Gamma}_n}))^{\omega\chi^{-1}} = \begin{cases} p^n - 1 & \text{if } \chi = \omega, \\ 0 & \text{otherwise,} \end{cases}$$

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p[\bar{\Delta} \times \bar{\Gamma}_n]/(N_{\bar{\Delta}}))^{\omega\chi^{-1}} = \begin{cases} p^n & \text{if } \chi \text{ is odd, } \chi \neq \omega \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\dim_{\mathbb{Q}_p} \mathbb{Q}_p[\Delta/D_p]^{\omega\chi^{-1}} = \begin{cases} 1 & \text{if } \omega\chi^{-1}(D_p) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

the assertion follows. □

It follows from the isomorphism $\mathcal{X}^\chi(-1) \simeq \operatorname{Hom}_{\mathbb{Z}_p}(\mathcal{E}^{\omega\chi^{-1}}, \mathbb{Q}_p/\mathbb{Z}_p)$ that $\mathcal{X}^{\chi\bullet}$ has no $\mathbb{Z}_p$-torsion element. Further, since $\mathcal{X}^{\chi\bullet}/\omega_n\mathcal{X}^{\chi\bullet}$ is a finitely generated $\mathbb{Z}_p$-module by (5) and Lemma 3.1, $\mathcal{X}^{\chi\bullet}$ is a finitely generated Λ-module by Nakayama's lemma. By the structure theorem of Λ-modules, there are a finite Λ-module M_χ and the exact sequence

$$0 \to \mathcal{X}^{\chi\bullet} \to E \to M_\chi \to 0$$

of Λ-modules, where $E = \Lambda^{\oplus e_\chi} \oplus \bigoplus_{i=1}^{s_\chi} \Lambda/(f_i^\chi)$ is an elementary Λ-module and f_i^χ a power of an irreducible distinguished polynomial.

Proposition 3.1 (corresponding to Theorem 15 of [7]). *We have* $e_\chi = d_\chi$, $s_\chi = \rho_\chi$ *and* $f_i^\chi = T$, *namely, the following sequence*

$$0 \to \mathcal{X}^{\chi\bullet} \to \Lambda^{d_\chi} \oplus (\Lambda/(T))^{\rho_\chi} \to M_\chi \to 0$$

is exact as Λ*-modules. In particular,* $\mathrm{Tor}_\Lambda \mathcal{X}^{\chi\bullet}$ *is isomorphic to* $(\Lambda/(T))^{\rho_\chi}$ *as* Λ*-modules.*

Proof. This follows from isomorphism (5) and Lemma 3.1. Since $\mathrm{Tor}_\Lambda \mathcal{X}^{\chi\bullet}$ is imbedded into $(\Lambda/(T))^{\rho_\chi}$ with finite index, the second assertion follows. □

Remark that there is an exact sequence

$$0 \to \mathcal{E} \to S \to A'_{K_\infty} \to 0.$$

(See Lemma 10 of [7]) Since $\mathrm{Gal}\left(M^{\mathrm{ab}}_{K_\infty}/N\right)$ ($\simeq \mathrm{Hom}_{\mathbb{Z}_p}(A'_{K_\infty}, \mu_{p^\infty})$) is a Λ-torsion Λ-module (see Theorem 16 of [7]), we see that $\mathfrak{X}_{K_\infty}/\mathrm{Tor}_\Lambda \mathfrak{X}_{K_\infty} \simeq \mathcal{X}/\mathrm{Tor}_\Lambda \mathcal{X}$.

Proposition 3.2 (corresponding to Lemma 12 of [7]). *We have the exact sequence*

$$0 \to \mathrm{Tor}_\Lambda \mathfrak{X}^\chi_{K_\infty} \to \mathfrak{X}^\chi_{K_\infty} \to \Lambda^{d_\chi} \to \mathrm{Hom}_{\mathbb{Z}_p}\left(X_f^{\prime\omega\chi^{-1}}, \mu_{p^\infty}\right) \to 0$$

of Λ*-modules. The sequence*

$$0 \to \mathrm{Hom}_{\mathbb{Z}_p}\left(A_{K_\infty}^{\prime\omega\chi^{-1}}, \mu_{p^\infty}\right) \to \mathrm{Tor}_\Lambda \mathfrak{X}^\chi_{K_\infty} \to \mathrm{Tor}_\Lambda \mathcal{X}^\chi \to 0$$

is also exact.

Proof. For the proof of first assertion, see Lemma 12 of Iwasawa [7]. The second assertion is trivial since $\mathrm{Hom}_{\mathbb{Z}_p}\left(A_{K_\infty}^{\prime\omega\chi^{-1}}, \mu_{p^\infty}\right)$ is a torsion Λ-module. □

4. Characterization of imaginary quadratic fields k with $G_k(p)$ being a free pro-p group

In this section, we shall prove the following.

Theorem 4.1. *Let* $k = \mathbb{Q}(\sqrt{-m})$ *be an imaginary quadratic field with a square-free positive integer* m *and put* $K = k(\mu_p)$. *Let* χ *be the Dirichlet character corresponding to* k. *Then,* $G_k(p)$ *is a free pro-*p *group of rank* 2 *if and only if one of the following three conditions holds*:

(1) $p = 3$ *and* $m = 3$.

(2) $p = 3$, $m \not\equiv 3 \bmod 9$ *and* $A'_{\mathbb{Q}(\sqrt{3m})} = 0$.

(3) $p \geq 5$ *and* $A_K^{\prime\omega\chi} = 0$.

Proof. For an abelian group A, put $A[p] = \{a \in A \mid pa = 0\}$ and $A/p = A/pA$. As we deompose $\mathfrak{X}_K$ by the action of Δ, we then have $\mathfrak{X}_k \simeq (\mathfrak{X}_K)_{\mathrm{Gal}(K/k)} = \mathfrak{X}_K^{\chi} \oplus \mathfrak{X}_{\mathbb{Q}}$. Also, since $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$, we have $\mathfrak{X}_{\mathbb{Q}} \simeq \mathbb{Z}_p$. Since k is an imaginary quadratic field, by the Euler-Poincaré characteristic (1), we find that $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = \dim_{\mathbb{F}_p} \mathrm{H}^2(G_k(p), \mathbb{Z}/p) + 2$. Note that

$$\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) - 1 = \dim_{\mathbb{F}_p} \mathrm{Hom}(\mathfrak{X}_K^{\chi}, \mu_p)$$

since $\mathfrak{X}_k = \mathfrak{X}_K^{\chi} \oplus \mathfrak{X}_{\mathbb{Q}}$ and $\mathfrak{X}_{\mathbb{Q}} \simeq \mathbb{Z}_p$. Hence $G_k(p)$ is a free pro-p group if and only if $\dim_{\mathbb{F}_p} \mathrm{Hom}(\mathfrak{X}_K^{\chi}, \mu_p) = 1$.

By Kummer's theory, there is a subgroup T of $K^\times/(K^\times)^p$ with the non-degenerate pairing

$$\mathfrak{X}_K/p \times T \to \mu_p.$$

Thus $\dim_{\mathbb{F}_p} \mathrm{Hom}(\mathfrak{X}_K^{\chi}, \mu_p) = \dim_{\mathbb{F}_p} T^{\omega\chi}$ $(\chi^{-1} = \chi)$. Also, since there is an exact sequence

$$0 \to E_K'/p \to T \to A_K'[p] \to 0,$$

we have $\dim_{\mathbb{F}_p} \mathrm{Hom}(\mathfrak{X}_K^{\chi}, \mu_p) = \dim_{\mathbb{F}_p}(E_K'/p)^{\omega\chi} + \dim_{\mathbb{F}_p} A_K'[p]^{\omega\chi}$. It follows from Proposition 2.1 that $\dim_{\mathbb{F}_p}(E_K'/p)^{\omega\chi} = 1 + \rho_\chi$. It is also easy to see that $\rho_\chi = 1$ if and only if $p = 3$ and $3 \neq m \equiv 3 \bmod 9$, and that $A_K'^{\omega\chi} = A'_{\mathbb{Q}(\sqrt{3m})}$ if $p = 3$. Since $\dim_{\mathbb{F}_p} A_K'[p]^{\omega\chi} = \dim_{\mathbb{F}_p} A_K'^{\omega\chi}/p$, combining the above, we have

$$\text{(6)} \quad \dim_{\mathbb{F}_p} \mathrm{Hom}(\mathfrak{X}_K^{\chi}, \mu_p) = \begin{cases} 2 + \dim_{\mathbb{F}_3} A'_{\mathbb{Q}(\sqrt{3m})}/3 & \text{if } p = 3,\ 3 \neq m \equiv 3 \bmod 9, \\ 1 + \dim_{\mathbb{F}_p} A_K'^{\omega\chi}/p & \text{otherwise.} \end{cases}$$

This implies Theorem 4.1. □

Let L_k/k be the maximal unramified abelian p-extension. Assume that $m \not\equiv 3 \bmod 9$ when $p = 3$. Let $\tilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k. Then Minardi [13] (Section A, Proposition 6.B and its Corollary of Chapter 6) showed that $L_k \subseteq \tilde{k}$ if and only if $A_K'^{\omega\chi} = 0$ by the same method. Under the assumption on m, one can easily check that $L_k \subseteq \tilde{k}$ if and only if $G_k(p)$ is a free pro-p group. Hence we must mention here that Theorem 4.1 had been essentially obtained by Minardi.

5. The explicit structure of $G_k(p)/[G_{k_\infty}(p), [G_{k_\infty}(p), G_{k_\infty}(p)]]$

Let $k = \mathbb{Q}(\sqrt{-m})$ and K be fields of the previous section and Γ the Galois group of the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k. Let $1 \to R \to F \to G_k(p) \to 1$ be a minimal presentation of $G_k(p)$ by a free pro-p group F and H the kernel of the composition

of the maps $F \to G_k(p) \to \Gamma$. Then the following diagram

$$\begin{array}{ccccccccc} & & & & R & \longrightarrow & R & & \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & F & \longrightarrow & \Gamma & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & G_{k_\infty}(p) & \longrightarrow & G_k(p) & \longrightarrow & \Gamma & \longrightarrow & 1 \end{array} \tag{7}$$

is exact-commutative. In this section, we will analyze the following exact sequence:

$$1 \to R \to H \to G_{k_\infty}(p) \to 1. \tag{8}$$

We shall discuss the properties of the group H here. Let γ ($\in F$) be an inverse image of a topological generator γ_0 of Γ. Then Γ acts on H via $\gamma_0(h) = \gamma h \gamma^{-1}$ for $h \in H$. Remark that this action is non-canonical. If we let γ_1 ($\in G_k(p)$) the image of γ, then Γ also acts on $G_{k_\infty}(p)$ via $\gamma_0(g) = \gamma_1 g \gamma_1^{-1}$ for $g \in G_{k_\infty}(p)$. This asserts that the groups H and $G_{k_\infty}(p)$ can be considered as pro-p Γ-operator groups, and the sequence (8) is exact as pro-p Γ-operator groups (see Section I of [19]). Since the topological commutator group $[\mathfrak{G}, \mathfrak{G}]$ of a pro-p Γ-operator group $\mathfrak{G}$ is a characteristic subgroup, Γ also acts on $\mathfrak{G}^{\mathrm{ab}}$, so that $\mathfrak{G}^{\mathrm{ab}}$ becomes a Λ-module.

Proposition 5.1. *Let* $d = \dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p)$. *Then* $H^{\mathrm{ab}} \simeq \Lambda^{\oplus d-1}$.

Proof. Since $F \to G_k(p)$ is a minimal presentation, we see that $\dim_{\mathbb{F}_p} \mathrm{H}^1(F, \mathbb{Z}/p) = d$. By the (dual of the) five term sequence, the sequence

$$0 \to (H^{\mathrm{ab}}/p)_\Gamma \to F^{\mathrm{ab}}/p \ (\simeq (\mathbb{Z}/p)^{\oplus d}) \to \Gamma/p \ (\simeq \mathbb{Z}/p) \to 0$$

is exact since Γ is a free pro-p group. By the topological version of Nakayama's lemma, H^{ab} is generated by $d-1$ elements over Λ. Let

$$0 \to Z \to \Lambda^{\oplus d-1} \to H^{\mathrm{ab}} \to 0$$

be a minimal presentation of H^{ab}. Since H ($\subseteq F$) is a free pro-p group, H^{ab} is $\mathbb{Z}_p$-torsion-free, whence the sequence

$$0 \to Z/p \to (\Lambda/p)^{\oplus d-1} \to H^{\mathrm{ab}}/p \to 0$$

is also exact. By taking the homology sequence, one obtains the following exact sequence;

$$0 \to \mathrm{H}_1(\Gamma, H^{\mathrm{ab}}/p) \to (Z/p)_\Gamma \to (\mathbb{Z}/p)^{\oplus d-1} \xrightarrow{\sim} (H^{\mathrm{ab}}/p)_\Gamma \to 0.$$

Note that $\mathrm{H}_1(\Gamma, H^{\mathrm{ab}}/p)$ is the dual of $\mathrm{H}^1(\Gamma, \mathrm{H}^1(H, \mathbb{Z}/p))$. From the Hochschild-Serre spectral sequence, there is an exact sequence $\mathrm{H}^2(F, \mathbb{Z}/p) \to \mathrm{H}^1(\Gamma, \mathrm{H}^1(H, \mathbb{Z}/p)) \to \mathrm{H}^2(\Gamma, \mathrm{H}^0(H, \mathbb{Z}/p))$ (see Section 2.1 and Exercise 5 of Section 2.1 in [14]). Hence $\mathrm{H}^1(\Gamma, \mathrm{H}^1(H, \mathbb{Z}/p)) = 0$ since $\mathrm{H}^2(F, \mathbb{Z}/p) = \mathrm{H}^2(\Gamma, \mathrm{H}^0(H, \mathbb{Z}/p)) = 0$. This shows that $(Z/p)_\Gamma = 0$, and therefore $Z = 0$ by Nakayama's lemma. Finally, we remark that H is a free pro-p Γ-operator group, see Proposition 1.7 of [19]. □

By the exact sequence (8), Theorem 10.3.22 or Theorem 10.3.25 of [14], there is an exact sequence

$$0 \to R/[R, H] \to H^{\mathrm{ab}} \ (\simeq \Lambda^{\oplus d-1}) \to \mathfrak{X}_{k_\infty} \to 0 \tag{9}$$

of Λ-modules. As the same to the proof of $H_\Gamma^{\mathrm{ab}}/p \simeq (\mathbb{Z}/p)^{\oplus d-1}$, we have $\dim_{\mathbb{F}_p}(\mathfrak{X}_{k_\infty})_\Gamma/p = d-1$. Therefore (9) is a minimal presentation of $\mathfrak{X}_{k_\infty}$ as a Λ-module by Proposition 5.1, and $R/[R, H]$ is generated by the relations of $G_k(p)$ over Λ since $(R/[R, H])_\Gamma = R/[R, F]$. By using (9), we show the following.

Theorem 5.1. *Let $F = \langle \gamma, x_1, x_2 \rangle$ be a free pro-p group of rank 3 and $H = (x_1, x_2)_F$ the closed normal subgroup of F enerated by x_1 and x_2. In general, denote by $(a_1, \ldots, a_s)_F$ the closed normal subgroup of F generated by $a_1, \ldots, a_s$. For a pro-p group $\mathfrak{G}$, denote by $C_i(\mathfrak{G})$ the i-th lower central series of $\mathfrak{G}$, e.g. $C_1(\mathfrak{G}) = \mathfrak{G}$, $C_2(\mathfrak{G}) = [\mathfrak{G}, \mathfrak{G}]$ and $C_3(\mathfrak{G}) = [\mathfrak{G}, C_2(\mathfrak{G})]$. Suppose that one of the following two statements holds*:
(I) $p = 3$, $3 \neq m \equiv 3 \bmod 9$ *and* $A'_{\mathbb{Q}(\sqrt{3m})_1} = 0$.
(II) $0 \neq X'^{\omega\chi}_{K_\infty} \simeq \mathbb{Z}/p^c$. *When $p = 3$ we further assume $m \not\equiv 3 \bmod 9$.*
Then $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = 3$ *and*

$$G_k(p)/C_3(G_{k_\infty}(p)) \simeq \begin{cases} F/(\gamma x_1 \gamma^{-1} x_1^{-8} \gamma x_1 \gamma^{-1})_F C_3(H) & \text{(I)}, \\ F\Big/\big(x_1^{p^c} \gamma x_2 \gamma^{-1} x_2^{-2(a+1)} \gamma x_2 \gamma^{-1} x_1^{p^c}\big)_F C_3(H) \ (\exists a \in p\mathbb{Z}) & \text{(II)} \end{cases}$$

as pro-p groups.

It is conjectured that $X^{\omega\chi}_{K_\infty}$ is always finite [3], and no counter examples have been found yet. There are many examples of real quadratic fields where this conjecture holds when $p = 3$, see Ichimura-Sumida [5], [6] and Kraft-Schoof [11]. The integer a is determined by the action of Γ on $X'^{\omega\chi}_{K_\infty}$.

Proof. By the natural isomorphism $\mathrm{Gal}(K_\infty/K) \simeq \mathrm{Gal}(k_\infty/k) = \Gamma$, we identify these groups. Let $\gamma_0 \in \Gamma$ be the topological generator such that $\gamma_0(\zeta) = \zeta^{1+p}$ for all $\zeta \in \mu_{p^\infty}$. We shall give two remarks here. Since $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$, one sees that $\mathfrak{X}_{\mathbb{Q}_\infty} = 0$. It follows from the fact that $\mathfrak{X}_{k_\infty}$ is isomorphic to $\mathfrak{X}^\chi_{K_\infty} \oplus \mathfrak{X}_{\mathbb{Q}_\infty}$ by seeing the action of Δ on $\mathfrak{X}_{K_\infty}$ that $\mathfrak{X}^\chi_{K_\infty} = \mathfrak{X}_{k_\infty}$. Also, recall that if $p = 3$, then the fixed field

of $\mathrm{Ker}\,\omega\chi$ is $\mathbb{Q}(\sqrt{3m})$, which is the totally real subfield of $K = k(\mu_3)$. First, we show that $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = 3$ in both cases (I) and (II).

Suppose that $p = 3$, $3 \neq m \equiv 3 \bmod 9$ and $A'_{\mathbb{Q}(\sqrt{3m})_1} = 0$. Since $\mathbb{Q}(\sqrt{3m})_1/\mathbb{Q}(\sqrt{3m})$ is totally ramified at all primes lying above 3, the norm map $A'_{\mathbb{Q}(\sqrt{3m})_1} \to A'_{\mathbb{Q}(\sqrt{3m})}$ is surjective by class field theory. Hence $A'_{\mathbb{Q}(\sqrt{3m})_1} = 0$ implies that $A'_{\mathbb{Q}(\sqrt{3m})} = 0$. By the equation (6), we obtain that $\dim_{\mathbb{F}_3} \mathrm{H}^1(G_k(3), \mathbb{Z}/3) = 3$.

Suppose that $0 \neq X'^{\omega\chi}_{K_\infty} \simeq \mathbb{Z}/p^c$ as abelian groups, and further assume that $m \not\equiv 3 \bmod 9$ if $p = 3$. We then have $\rho_\chi = 0$. Applying the dual of the five term sequence to $1 \to G_{k_\infty}(p) \to G_k(p) \to \Gamma \to 1$, we obtain $0 \to (\mathfrak{X}_{k_\infty}/p)_\Gamma \to \mathfrak{X}_k/p \to \Gamma/p \to 0$. Hence

$$\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = \dim_{\mathbb{F}_p} \mathfrak{X}_k/p = 1 + \dim_{\mathbb{F}_p}(\mathfrak{X}_{k_\infty}/p)_\Gamma.$$

We shall show that $\dim_{\mathbb{F}_p}(\mathfrak{X}_{k_\infty}/p)_\Gamma = 2$. Since $X'^{\omega\chi}_{K_\infty}$ is finite, one sees that $A'^{\omega\chi}_{K_\infty} = 0$ by (4). It follows from Proposition 3.1, Proposition 3.2 and $\rho_\chi = 0$ that $\mathrm{Tor}_\Lambda \mathfrak{X}_{k_\infty} = 0$ and that $0 \to \mathfrak{X}_{k_\infty} \to \Lambda \to \mathrm{Hom}_{\mathbb{Z}_p}(X'^{\omega\chi}_f, \mu_{p^\infty}) \to 0$ is exact. Since Γ is cyclic, we have the following exact sequence;

$$0 \to \mathrm{Hom}_{\mathbb{Z}_p}(X'^{\omega\chi}_f, \mu_{p^\infty})^\Gamma \to (\mathfrak{X}_{k_\infty})_\Gamma \to \mathbb{Z}_p \to \mathrm{Hom}_{\mathbb{Z}_p}(X'^{\omega\chi}_f, \mu_{p^\infty})_\Gamma \to 0. \tag{10}$$

Hence $(\mathfrak{X}_{k_\infty})_\Gamma \simeq \mathbb{Z}_p \oplus \mathrm{Hom}_{\mathbb{Z}_p}(X'^{\omega\chi}_f, \mu_{p^\infty})^\Gamma$ as $\mathbb{Z}_p$-modules. Since $X'^{\omega\chi}_f = X'^{\omega\chi}_{K_\infty} \simeq \mathbb{Z}/p^c$ by our assumption, we then have obtained $\dim_{\mathbb{F}_p}(\mathfrak{X}_{k_\infty}/p)_\Gamma = 2$, so that $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = 3$.

Next, we will determine the explicit structure of $\mathfrak{X}_{k_\infty}$ as a Λ-module. Suppose the condition of (I). Since $\mathbb{Q}(\sqrt{3m})_\infty/\mathbb{Q}(\sqrt{3m})$ is totally ramified at all primes lying above 3, the condition $A'_{\mathbb{Q}(\sqrt{3m})_1} = 0$ implies that $X'_{\mathbb{Q}(\sqrt{3m})_\infty} = X'^{\omega\chi}_{K_\infty} = 0$ by [2]. It follows from Proposition 3.2 that the sequence

$$0 \to \mathrm{Tor}_\Lambda \mathfrak{X}_{k_\infty} \to \mathfrak{X}_{k_\infty} \to \Lambda \to \mathrm{Hom}_{\mathbb{Z}_3}(X'^{\omega\chi}_f, \mu_{3^\infty}) \ (= 0),$$

is exact, so that $\mathfrak{X}_{k_\infty} \simeq \mathrm{Tor}_\Lambda \mathfrak{X}_{k_\infty} \oplus \Lambda$ as Λ-modules. Also, $X'^{\omega\chi}_{K_\infty} = 0$ implies that $A'^{\omega\chi}_{K_\infty} = 0$, whence we have $\mathrm{Tor}_\Lambda \mathfrak{X}_{k_\infty} \simeq \mathrm{Tor}_\Lambda \mathcal{X}^\chi$ by Proposition 3.2. Since $\mathrm{Tor}_\Lambda \mathcal{X}^{\chi\bullet} \simeq \Lambda/(T)$ by Proposition 3.1, we see that $\mathrm{Tor}_\Lambda \mathcal{X}^\chi \simeq \Lambda/((1+3)(1+T)^{-1} - 1) = \Lambda/(T-3)$ as Λ-modules. Therefore, there is an isomorphism

$$\mathfrak{X}_{k_\infty} \simeq \Lambda/(T-3) \oplus \Lambda \tag{11}$$

of Λ-modules.

Suppose the condition of (II). Recall that $\rho_\chi = 0$, $X'^{\omega\chi}_f = X'^{\omega\chi}_{K_\infty} \simeq \mathbb{Z}/p^c$ and $A'^{\omega\chi}_{K_\infty} = 0$. By Proposition 3.2, we have the exact sequence

$$0 \to \mathfrak{X}_{k_\infty} \to \Lambda \to \mathrm{Hom}_{\mathbb{Z}_p}(X'^{\omega\chi}_f, \mu_\infty) \to 0 \tag{12}$$

of Λ-modules. Note that $\mathbb{Z}/p^c \simeq X_f'^{\omega\chi} \simeq \mathrm{Hom}_{\mathbb{Z}_p}(X_f'^{\omega\chi}, \mu_{p^\infty})$ as abelian groups.

Lemma 5.1. *Let M be a Λ-module such that $M \simeq \mathbb{Z}/p^c$ as abelian groups. Then there is an integer $a \in p\mathbb{Z}$ such that $M \simeq \Lambda/(p^c, T-a)$ as Λ-modules.*

Proof. Let m be a generator of M, so that $M = \Lambda m$. Put $I = \mathrm{Ker}(\Lambda \to M)$. Then there is $a \in p\mathbb{Z}$ such that $(1+T)m = (1+a)m$. This shows that $T-a \in I$. Since $\Lambda/(T-a) \simeq \mathbb{Z}_p$ as abelian groups, it follows that $I = (T-a, p^c)$. This completes the proof of Lemma 5.1. □

By the above lemma, there is an integer $a \in p\mathbb{Z}$ such that $\mathrm{Hom}_{\mathbb{Z}_p}(X_f'^{\omega\chi}, \mu_{p^\infty}) \simeq \Lambda/(T-a, p^c)$ as Λ-modules. It follows from the exact sequence (12) that $\mathfrak{X}_{k_\infty} \simeq (T-a, p^c)$ as Λ-modules.

Let $\Lambda^{\oplus 2} \to \mathfrak{X}_{k_\infty} \simeq (T-a, p^c)$ be a minimal presentation of $\mathfrak{X}_{k_\infty}$ with the correspondence $(1,0) \mapsto T-a$, $(0,1) \mapsto -p^c$, so that $(f(T), g(T))$ maps to $(T-a)f(T) - p^c g(T)$. Let L be the kernel of $\Lambda^{\oplus 2} \to (T-a, p^c)$. Doing the same as (10), we have an exact sequence

$$0 \to L/TL \to \mathbb{Z}_p^{\oplus 2} \to (T-a, p^c)/(T(T-a), p^c T) \to 0.$$

(Remark that $1+T$ acts as γ_0.) Since $p^c \bmod (T(T-a), p^c T)$ is $\mathbb{Z}_p$-free, L/TL has $\mathbb{Z}_p$-rank at most one. Hence L is a cyclic Λ-module by Nakayama's lemma, say $L = \Lambda(r(T), s(T))$. Now we show that $L = \Lambda(p^c, T-a)$. It follows from $(T-a)r(T) - p^c s(T) = 0$ that p^c divides $r(T)$ and that $T-a$ divides $s(T)$ since Λ is an UFD. Let $r'(T)$ and $s'(T)$ be elements of Λ with $r(T) = p^c r'(T)$ and $s(T) = (T-a)s'(T)$. Since $(p^c, T-a) \in L$, there is a power series $f(T)$ in Λ such that $p^c = f(T)r(T) = p^c f(T)r'(T)$ and $T-a = f(T)s(T) = (T-a)f(T)s'(T)$. It follows that $f(T)$ is an unit power series and that $f(T) = r'(T)^{-1} = s'(T)^{-1}$. Thus

$$\begin{aligned} L &= \Lambda(r(T), s(T)) \\ &= \Lambda(f(T)^{-1}(p^c),\ f(T)^{-1}(T-a)) \\ &= \Lambda(p^c, T-a). \end{aligned}$$

Therefore

$$\mathfrak{X}_{k_\infty} \simeq \Lambda^{\oplus 2}/\Lambda(p^c, T-a) \tag{13}$$

as Λ-modules.

Now, we discuss actions of $\langle J \rangle = \mathrm{Gal}(k/\mathbb{Q}) \simeq \mathbb{Z}/2$ on $G_k(p)$ and $G_{k_\infty}(p)$. Since the p-cohomological dimensions of $\mathrm{Gal}(k/\mathbb{Q})$ and $\mathrm{Gal}(k_\infty/\mathbb{Q})$ are 0 and 1, we can consider (non-canonical) actions of J and $\mathrm{Gal}(k_\infty/\mathbb{Q})$ on $G_k(p)$ and $G_{k_\infty}(p)$, respectively (see Section 3.5 of [14]).

Proposition 5.2. *There exist topological generators γ_1, w_1, w_2 of $G_k(p)$ such that $J(\gamma_1) = \gamma_1$ and $J(w_i) = w_i^{-1}$ for $i = 1, 2$.*

Proof. Let $\mathfrak{X}_k/p = (\mathfrak{X}_k/p)^+ \oplus (\mathfrak{X}_k/p)^-$ be the decomposition with respect to the action of J. Let M be the fixed field of $(\mathfrak{X}_k/p)^-$. Then $M/\mathbb{Q}$ is an abelian extension. Further, $M^{\langle J\rangle}/\mathbb{Q}$ is an abelian p-extension of $\mathbb{Q}$ unramified outside p, and hence $M^{\langle J\rangle} = \mathbb{Q}_1$. This shows that $(\mathfrak{X}_k/p)^+ \simeq \mathbb{Z}/p$. Therefore, $(\mathfrak{X}_k/p)^- \simeq (\mathbb{Z}/p)^{\oplus 2}$. It follows from Theorem 2.3 of [4] and $\dim_{\mathbb{F}_p} \mathrm{H}^1(G_k(p), \mathbb{Z}/p) = 3$ that there exist topological generators γ_1, w_1, w_2 of $G_k(p)$ such that $J(\gamma_1) = \gamma_1$ and $J(w_i) = w_i^{-1}$ for $i = 1, 2$. □

Let $\{\gamma_1, w_1, w_2\}$ be a system of topological generators of $G_k(p)$ with the property of Proposition 5.2. Let $\mathcal{G} = (w_1, w_2)_{G_k(p)}$ be the normal closed subgroup of $G_k(p)$ generated by w_1 and w_2. Here we prove that $\mathcal{G} = G_{k_\infty}(p)$. Let $\mathcal{K}$ be the fixed field of $\mathcal{G}$. Since J acts on $\langle \gamma_1 \mathcal{G}\rangle$ trivially, we see that $\mathcal{K} = k_\infty$ or k_n for some $n \geq 0$. If $\mathcal{K} = k_n$, then $\mathcal{G} = \mathrm{Gal}(M_{k_n}/k_n)$. But since J acts on $\mathcal{G}^{\mathrm{ab}}$ as the inverse, this contradicts the fact that k_n has the cyclotomic $\mathbb{Z}_p$-extension k_∞. Hence $\mathcal{K} = k_\infty$ and $\mathcal{G} = G_{k_\infty}(p)$. From this reason, we adopt a lift $\gamma_1 \in G_k(p)$ of γ_0 with $\gamma_0(\zeta) = \zeta^{1+p}$ for all $\zeta \in \mu_{p^\infty}$. Let y_1 and y_2 be elements of $G_{k_\infty}(p)$ such that $\mathfrak{X}_{k_\infty}$ is generated by $y_1 C_2(G_{k_\infty}(p)), y_2 C_2(G_{k_\infty}(p))$ over Λ, namely, $\mathfrak{X}_{k_\infty} = \sum_{i=1}^2 \Lambda y_i C_2(G_{k_\infty}(p))$. By the exact sequence $0 \to (\mathfrak{X}_{k_\infty}/p)_\Gamma \to \mathfrak{X}_k/p \to \Gamma/p \to 0$ (the dual of the five term sequence with coefficients in $\mathbb{Z}/p$), we see that $G_k(p) = \langle \gamma_1, y_1, y_2\rangle$ by Burnside's basis theorem. If it is necessary we may assume that $J(y_i) = y_i^{-1}$ for $i = 1, 2$ by replacing y_i with $y_i^{1/2} J(y_i)^{-1/2}$ since $y_i \equiv y_i^{1/2} J(y_i)^{-1/2} \mod C_2(G_{k_\infty}(p))$ and $J\left(y_i^{1/2} J(y_i)^{-1/2}\right) = J(y_i)^{1/2} y_i^{-1/2} = \left(y_i^{1/2} J(y_i)^{-1/2}\right)^{-1}$. Hence these topological generators γ_1, y_1, y_2 satisfy the condition of Proposition 5.2, so that w_i's are also obtained from this way.

We choose special elements of $G_{k_\infty}(p)$. Fix an isomorphism

$$\mathfrak{X}_{k_\infty} \simeq \begin{cases} \Lambda/(T-3) \oplus \Lambda & \text{in the case (I),} \\ (T-a,\ p^c) & \text{in the case (II)} \end{cases} \tag{14}$$

of Λ-modules. Let $z_1, z_2 \in G_{k_\infty}(p)$ be elements such that

$$\begin{cases} \Lambda z_1 C_2(G_{k_\infty}(3)) \simeq \Lambda/(T-3), \quad \Lambda z_2 C_2(G_{k_\infty}(3)) \simeq \Lambda & \text{in the case (I),} \\ z_1 C_2(G_{k_\infty}(p)) \mapsto T-a, \quad z_2 C_2(G_{k_\infty}(p)) \mapsto p^c & \text{in the case (II).} \end{cases} \tag{15}$$

If it is necessary, we may suppose $J(z_i) = z_i^{-1}$ for $i = 1$ and 2. Recall that $F = \langle \gamma, x_1, x_2\rangle$ is a free pro-p group of rank 3 and $H = (x_1, x_2)_F$. Then we can define the action of J on F via $J(\gamma) = \gamma$ and $J(x_i) = x_i^{-1}$ for $i = 1$ and 2. Let $1 \to R \to F \to G_k(p) \to 1$ be a minimal presentation of $G_k(p)$ by sending $\gamma \to \gamma_1$ and $x_i \to z_i$ for $i = 1$ and 2, so that $F \to G_k(p)$ is compatible to the action of J. Further, we adopt a lift γ of γ_0. Then the morphism $H \to G_{k_\infty}(p)$ is also compatible to the actions of J and Γ.

From the exact sequence (9), the isomorphism (14) and the choice of the generators z_1, z_2 (15), there exists $r \in H$ such that

$$r \equiv \begin{cases} [\gamma, x_1]x_1^{-3} \mod C_2(H) & \text{in the case (I),} \\ x_1^{p^c}[\gamma, x_2]x_2^{-a} \mod C_2(H) & \text{in the case (II),} \end{cases}$$

and that $G_{k_\infty}(p) \simeq H/(r)_F$ as pro-p Γ-operator groups. Here we let $[x, y] = xyx^{-1}y^{-1}$ for $x, y \in F$. Remark that $(H^{\mathrm{ab}})^- = H^{\mathrm{ab}}$.

Lemma 5.2. *Let N be a pro-p group with the action of J. If $(N^{\mathrm{ab}})^- = N^{\mathrm{ab}}$, then J acts on $C_2(N)/C_3(N)$ trivially.*

Proof. Consider the pairing

$$[\ ,\ ] : N^{\mathrm{ab}} \times N^{\mathrm{ab}} \to C_2(N)/C_3(N).$$

Let $x, y \in N$. Since $J([x, y]) = [J(x), J(y)] = [x^{-1}, y^{-1}] = [x, y]$, J acts on $C_2(N)/C_3(N)$ trivially. □

Since $r^{1-J} = rJ(r)^{-1}$ is also a generator of R as a closed subgroup of F, we may assume that the following congruence holds true;

$$r \equiv \begin{cases} ([\gamma, x_1]x_1^{-3})^{1-J} \mod C_2(H) & \text{in the case (I),} \\ \left(x_1^{p^c}[\gamma, x_2]x_2^{-a}\right)^{1-J} \mod C_2(H) & \text{in the case (II).} \end{cases}$$

Let $r' \in H$ be the element of right-hand-side in the above congruence. By Lemma 5.2, one sees that

$$\begin{aligned} rr'^{-1} &\equiv J\left(rr'^{-1}\right) \\ &= J(r)J(r')^{-1} \\ &= r^{-1}r' \mod C_3(H), \end{aligned}$$

Thus $r \equiv r' \bmod C_3(H)$. Then the above congruence may be replaced by

$$r \equiv \begin{cases} ([\gamma, x_1]x_1^{-3})^{1-J} \mod C_3(H) & \text{in the case (I),} \\ \left(x_1^{p^c}[\gamma, x_2]x_2^{-a}\right)^{1-J} \mod C_3(H) & \text{in the case (II).} \end{cases} \tag{16}$$

The form of relation r of (16) shows that

$$G_k(p)/C_3(G_{k_\infty}(p)) \simeq \begin{cases} F/(\gamma x_1\gamma^{-1}x_1^{-8}\gamma x_1\gamma^{-1})_F C_3(H) & \text{in the case (I),} \\ F\Big/\left(x_1^{p^c}\gamma x_2\gamma^{-1}x_2^{-2(a+1)}\gamma x_2\gamma^{-1}x_1^{p^c}\right)_F C_3(H) & \text{in the case (II)} \end{cases}$$

as pro-p groups. This completes the proof of Theorem 5.1. □

At the end of this section, we shall discuss whether the relation r is an unknown relation or not.

Proposition 5.3. *Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a square-free positive integer m and p an odd prime number. Then $G_k(p)$ does not have an unknown relation, namely, the product of restriction maps*

$$\varphi_p : \mathrm{H}^2(G_k(p), \mathbb{Z}/p) \to \prod_{\mathfrak{p}|p} \mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p)$$

is injective, if and only if $G_k(p)$ is free, or $p = 3$, $3 \neq m \equiv 3 \bmod 9$ and $A'_{\mathbb{Q}(\sqrt{3m})} = 0$.

Proof. We need the following.

Lemma 5.3 (Proposition 7.3.10 and Theorem 7.5.8 of [14]). *Let $\mathcal{F}/\mathbb{Q}_p$ be a finite extension.*
(1) *If $\mathcal{F}$ does not contain μ_p, then $G_\mathcal{F}(p)$ is a free pro-p group of rank $[\mathcal{F} : \mathbb{Q}_p] + 1$. Otherwise, $G_\mathcal{F}(p)$ is a Demuskin group of rank $[\mathcal{F} : \mathbb{Q}_p] + 2$.*
(2) $\mathrm{H}^2(G_\mathcal{F}(p), \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Let $U_\mathfrak{p}$ be the principal unit group of $k_\mathfrak{p}$ with $\mathfrak{p} \mid p$. Note that $\#E_k$ is finite since k is an imaginary quadratic field. By class field theory, we have the following exact sequence

$$0 \to E_k \otimes \mathbb{Z}_p \to \prod_{\mathfrak{p}|p} U_\mathfrak{p} \to \mathfrak{X}_k.$$

(See Section 13.1 of [18].) Hence $\prod_{\mathfrak{p}|p} U_\mathfrak{p}[p] \to \mathfrak{X}_k[p]$ is injective unless $p = 3$ and $m = 3$. It follows that $U_\mathfrak{p}[p] \simeq (k_\mathfrak{p}^\times \otimes \mathbb{Z}_p)[p] \simeq G_{k_\mathfrak{p}}(p)^{\mathrm{ab}}[p]$ by class field theory and that $G_{k_\mathfrak{p}}(p)^{\mathrm{ab}}[p]$ is the dual of $\mathrm{H}^1(G_{k_\mathfrak{p}}(p), \mathbb{Q}_p/\mathbb{Z}_p)/p$. This implies that the restriction map

$$\mathrm{H}^1(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p)/p \to \prod_{\mathfrak{p}|p} \mathrm{H}^1(G_{k_\mathfrak{p}}(p), \mathbb{Q}_p/\mathbb{Z}_p)/p$$

is surjective unless $p = 3$ and $m = 3$. Applying the long exact sequence of cohomology groups to the exact sequence $0 \to \mathbb{Z}/p \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \to 0$, it follows that

$$\mathrm{H}^1(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p)/p \simeq \mathrm{H}^2(G_k(p), \mathbb{Z}/p), \quad \mathrm{H}^1(G_{k_\mathfrak{p}}(p), \mathbb{Q}_p/\mathbb{Z}_p)/p \simeq \mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p)$$

since $\mathrm{H}^2(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ by Lemma 5.3. Therefore, we ob-

tain the following commutative diagram;

$$\begin{array}{ccc} \mathrm{H}^1(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p)/p & \xrightarrow{\sim} & \mathrm{H}^2(G_k(p), \mathbb{Z}/p) \\ \downarrow & & \downarrow{\scriptstyle \varphi_p} \\ \prod_{\mathfrak{p}|p} \mathrm{H}^1(G_{k_\mathfrak{p}}(p), \mathbb{Q}_p/\mathbb{Z}_p)/p & \xrightarrow{\sim} & \prod_{\mathfrak{p}|p} \mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p), \end{array}$$

where the vertical maps are the restriction maps. Thus φ_p is surjective unless $p = 3$ and $m = 3$.

Suppose that $p \geq 5$. Then $k_\mathfrak{p}$ does not contain μ_p, whence $G_{k_\mathfrak{p}}(p)$ is a free pro-p group by Lemma 5.3. This implies that $\mathrm{H}^2(G_{k_\mathfrak{p}}(p), \mathbb{Z}/p) = 0$, so that φ_p is injective if and only if $\mathrm{H}^2(G_k(p), \mathbb{Z}/p) = 0$, which is equivalent to the freeness of $G_k(p)$.

Suppose that $p = 3$. One can easily see that the completion $k_\mathfrak{p}$ of $k = \mathbb{Q}(\sqrt{-m})$ at a prime $\mathfrak{p}$ of k above 3 contains μ_3 if and only if $m \equiv 3 \bmod 9$. If $m \not\equiv 3 \bmod 9$, then $k_\mathfrak{p}$ does not contain μ_3 and hence $G_{k_\mathfrak{p}}(3)$ is a free pro-3 group. This implies that φ_3 is injective if and only if $\mathrm{H}^2(G_k(3), \mathbb{Z}/3) = 0$ when $m \not\equiv 3 \bmod 9$.

Suppose that $p = 3$ and $m \equiv 3 \bmod 9$. If $k = \mathbb{Q}(\mu_3)$, then $G_k(3)$ is a free pro-3 group by Theorem 4.1. If $m \neq 3$, then we see that k has only one prime $\mathfrak{p}$ above 3, $k_\mathfrak{p}$ contains μ_3 and that φ_3 is surjective. By Lemma 5.3, $G_{k_\mathfrak{p}}(3)$ is a Demuskin group, so that $\mathrm{H}^2(G_{k_\mathfrak{p}}(3), \mathbb{Z}/3) \simeq \mathbb{Z}/3$. Hence φ_3 is injective if and only if $\mathrm{H}^2(G_k(3), \mathbb{Z}/3) \simeq \mathbb{Z}/3$, which is equivalent to $A'_{\mathbb{Q}(\sqrt{3m})} = 0$ by (6). □

By Proposition 5.3, the relation of the case (I) of Theorem 5.1 comes from the relation of Demuskin groups. Actually, the form of relation (16) seems like the relation of a Demuskin group. On the other hand, the relation of the case (II) does not come from the relations of the Galois groups of local fields, whence it is a global object.

6. Examples

Here we give examples of Theorem 5.1 for $p = 3$. Let $m = 21$ or 129. Then $3 \neq m \equiv 3 \bmod 9$ and $A'_{\mathbb{Q}(\sqrt{3m})_1} = 0$. Thus the fields $k = \mathbb{Q}(\sqrt{-m})$ with $m = 21$ or 129 satisfy the assumption of Theorem 5.1 (1). A difference of these fields is whether the prime 3 divides the class number h_k of k or not. If $m = 21$, then $3 \nmid h_k$, and if $m = 129$, then $3 \mid h_k$.

Next, we give examples of Theorem 5.1 (2). Let $m = 107$, then $m \equiv 8 \not\equiv 3 \bmod 9$. One can show that $A_{\mathbb{Q}(\sqrt{3m})}$, $A_{\mathbb{Q}(\sqrt{3m})_1} \simeq \mathbb{Z}/3$, and this implies that $X_{K_\infty}^{\prime\omega\chi} \simeq \mathbb{Z}/3$ by [2]. Hence $c = 1$ and $a = 0$. Here we give an example with $a \neq 0$, which is obtained by Kraft and Schoof [11]. Let $m = 1583$. Then we have $\mathrm{Hom}_{\mathbb{Z}_3}(X_{K_\infty}^{\prime\omega\chi}, \mathbb{Q}_3/\mathbb{Z}_3) \simeq \Lambda/(T - 3, 27) \simeq \mathbb{Z}/27$. Thus $\mathrm{Hom}_{\mathbb{Z}_3}(X_{K_\infty}^{\prime\omega\chi}, \mu_{3^\infty}) \simeq \mathrm{Hom}_{\mathbb{Z}_3}(X_{K_\infty}^{\prime\omega\chi}, \mathbb{Q}_3/\mathbb{Z}_3)(1) \simeq (\Lambda/(T-3, 27))(1)$. Since $\gamma_0((1 \bmod (T-3, 27)) \otimes t_1) = (1+T \bmod (T-3, 27)) \otimes \gamma_0 t_1) = (4 \bmod (T-3, 27)) \otimes 4t_1 = 16(1 \bmod (T - 3, 27)) \otimes t_1$, we have $\mathrm{Hom}_{\mathbb{Z}_3}(X_{K_\infty}^{\prime\omega\chi}, \mu_{3^\infty}) \simeq (\Lambda/(T - 3, 27))(1) \simeq \Lambda/(T - 15, 27)$. Therefore, $c = 3$ and $a = 15$.

ACKNOWLEDGMENT. I would like to express my thanks to Professor Keiichi Komatsu for many valuable suggestions and advice. I would also like to express my thanks to the referee for making great attention to read this article and giving the author many valuable comments. This research is partially supported by the Waseda University Grant for Special Research Projects: 2004B-895.

References

[1] A. Fröhlich: *On fields of class two*, Proc. London Math. Soc. (3) **4** (1954), 235–256.
[2] T. Fukuda: *Remarks on $\mathbf{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 264–266.
[3] R. Greenberg: *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
[4] W.N. Herfort and L. Ribes: *On automorphisms of free pro-p-groups*, I, Proc. Amer. Math. Soc. **108** (1990), 287–295.
[5] H. Ichimura and H. Sumida: *On the Iwasawa λ-invariant of the real p-cyclotomic field*, J. Math. Sci. Univ. Tokyo **3** (1996), 457–470.
[6] H. Ichimura and H. Sumida: *On the Iwasawa invariants of certain real abelian fields*. II, Internat. J. Math. **7** (1996), 721–744.
[7] K. Iwasawa: *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.
[8] H. Koch: *Fields of class two and Galois cohomology*; in Algebraic Number Fields: L-Functions and Galois Properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, 609–624.
[9] H. Koch: Galois Theory of p-Extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.
[10] K. Komatsu: *On the maximal p-extensions of real quadratic fields unramified outside p*, J. Algebra **123** (1989), 240–247.
[11] J.S. Kraft and R. Schoof: *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155, Erratum: Compositio Math. **103** (1996), 241.
[12] B. Mazur and A. Wiles: *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), 179–330.
[13] J. Minardi: *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Washington University, Thesis (1986).
[14] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of Number Fields, Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2000.
[15] T. Nguyen Quang Do: *Sur la p-ramification non abélienne de corps de nombres totalement réels*; in Théorie des Nombres, Années 1989/90–1990/91, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1991, 14.
[16] M. Ozaki: *A note on the capitulation in $\mathbf{Z}_p$-extensions*, Proc. Japan Acad. Ser. A Math. Sci. **71** (1995), 218–219.
[17] I.R. Shafarevich: *Extensions with prescribed ramification points*, Inst. Hautes Études Sci. Publ. Math. **18** (1963), 71–95.
[18] L.C. Washington: Introduction to Cyclotomic Fields, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.
[19] K. Wingberg: *On the maximal unramified p-extension of an algebraic number field*, J. Reine Angew. Math. **440** (1993), 129–156.

Department of Mathematical Sciences
School of Science and Engineering
Waseda University
Okubo, Shinjuku-ku, Tokyo, 169–8555
Japan

Current address:
School of Science and Engineering
Keio University
Yokohama, Kohoku-ku, 223–8522
Japan
e-mail: fujii@ruri.waseda.jp