TOKYO J. MATH.
VOL. 30, NO. 1, 2007

Some Problems on p-class Field Towers

Satoshi FUJII† and Keiji OKANO

Waseda University

(Communicated by Y. Yamada)

1. Introduction

Let p be a prime number, k a finite extension of the field of rational numbers $\mathbf{Q}$ and $L(k)$ the maximal unramified abelian p-extension of k. Let $\tilde{L}(k)$ be the maximal unramified pro-p extension of k, which is called the p-class field tower of k, and denote its Galois group $\mathrm{Gal}(\tilde{L}(k)/k)$ over k by $\tilde{G}_k$. Then $\mathrm{Gal}(L(k)/k) = \tilde{G}_k^{\mathrm{ab}} \simeq A_k$, the p-primary part of the ideal class group of k, by the class field theory. For a number field k which can be an infinite extension of $\mathbf{Q}$, we use the same notation, e.g. $\tilde{L}(k)$ and $\tilde{G}_k$, as in a finite extension. Let k_∞ be the cyclotomic $\mathbf{Z}_p$-extension over a number field k; in other words, k_∞ is the unique infinite Galois subextension of the field obtained by adjoining to k all roots of unity of p-power order, whose Galois group is isomorphic to the additive group of the ring $\mathbf{Z}_p$ of p-adic integers. Denote by k_n the unique subextension of k_∞ over k of degree p^n.

Iwasawa theory of $\mathbf{Z}_p$-extensions deals with Galois groups of various abelian p-extensions over k_n and k_∞, in particular, of the maximal unramified abelian pro-p extensions over k_n and k_∞. Recently, a number of mathematicians have been engaged in the study of non-abelian extensions of k_∞ and k_n using Iwasawa theory, especially the study of maximal pro-p extensions with restricted ramification. For example, Ozaki [18] studied the maximal unramified pro-p extension of k_n for all n, and proved a non-abelian analogy of the Iwasawa class number formula. And from the point of view of the analogy between the theory of $\mathbf{Z}_p$-extensions of algebraic number fields and the theory of the Jacobian variety of algebraic curves, A. Schmidt and K. Wingberg study the Galois group of "the maximal positively ramified extensions over algebraic number fields", which is the analogy of the fundamental group of compact Riemann surfaces.

In such studies, the question which asks what kind of groups can appear as the Galois group $\tilde{G}_{k_\infty}$ of the maximal *unramified* pro-p extension $\tilde{L}(k_\infty)$ of k_∞, and what kind of properties characterize $\tilde{G}_{k_\infty}$ is an interesting problem for reasons of being concerned with the

Received October 4, 2005; revised April 13, 2006
2000 *Mathematics Subject Classification.* 11R23.
†This research is partially supported by the Waseda University Grant for Special Research Projects: 2004B-895

theory of class field towers. Although a lot of investigations into this problem have been done, quite a few groups are known which appear as $\tilde{G}_{k_\infty}$. For example, in the case of infinite non-abelian groups, we know almost nothing, while in the case of finite non-abelian groups, they are dihedral groups or generalized quaternion groups (Mizusawa [14], [15]). More precisely, in the case of infinite non-abelian groups, we do not know more than that there is an example of a non-free pro-p group $\tilde{G}_{k_\infty}$ for an odd prime p and some CM-field k. While there are no known effective sufficient conditions for $\tilde{G}_{k_\infty}$ to be a free pro-p group, we will give some conditions, though ineffective, in the last section of this article. It seems that one of the reasons of the difficulty in determining the structure of $\tilde{G}_{k_\infty}$ is the existence of archimedean primes of algebraic number fields.

In this paper under the condition that $\tilde{G}_{k_\infty}$ is a non-abelian free pro-p group for some kind of k we answer the following two questions which are concerned with the theory of class field towers. We must here mention that we have no examples of such $\tilde{G}_{k_\infty}$ up to now.

(a) For an odd prime p, to find an example of a number field k with the infinite p-class field tower whose p-primary part of the ideal class group A_k satisfies the condition that $\dim_{\mathbf{Z}/p\mathbf{Z}} A_k/A_k^p = 2$.

(b) For the cyclotomic $\mathbf{Z}_p$-extension k_∞/k, in case that $\tilde{G}_{k_n}$ is infinite, to know whether $\tilde{G}_{k_n}$ has no torsion elements, in particular, whether its cohomological dimension is finite.

The question (a) arises from the fact that, for any odd prime p and any imaginary quadratic field k, the p-class field tower is infinite if $\dim_{\mathbf{Z}/p\mathbf{Z}} A_k/A_k^p \geq 3$ ([9], [11]). We remark that Hajir [4] showed $k = \mathbf{Q}(\sqrt{-5 \cdot 11 \cdot 461})$, whose 2-primary part of the ideal class group is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, has the infinite 2-class field tower. On the other hand Hajir [5] also connected the question (b) with the Fontaine-Mazur conjecture. Unfortunately we have no examples of the non-abelian free pro-p Galois group $\tilde{G}_{k_\infty}$, as mentioned above. Therefore, the question whether there exist such Galois groups seems a most interesting problem.

The main results in this article are the following.

THEOREM 1.1. *Let p be an odd prime number, k a CM-field with the maximal totally real field k^+, k_∞ the cyclotomic $\mathbf{Z}_p$-extension of k and k_n its n-th layer. Suppose that*

(1) *$\tilde{G}_{k_\infty}$ is a free pro-p group with rank $\lambda \geq 2$,*

(2) *the prime p does not split in $k_\infty/\mathbf{Q}$,*

(3) *the class number of k^+ is prime to p.*

If $p \geq 5$ and $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_0}/A_{k_0}^p = 2$, or $p = 3$ and $A_{k_0} \simeq \mathbf{Z}/3^a\mathbf{Z} \oplus \mathbf{Z}/3^b\mathbf{Z}$ with $a, b \geq 2$, then $\tilde{L}(k_1)/k_1$ is an infinite extension.

It is known that if $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_0}/A_{k_0}^p \geq 3$, then $\tilde{L}(k_0)/k_0$ is an infinite extension by [9].

THEOREM 1.2. *Let p be an odd prime number, k a CM-field, ζ_p a primitive p-th root of unity, k^+ the maximal totally real subfield of k and k_∞/k the cyclotomic $\mathbf{Z}_p$-extension. Suppose that*

(1) $\tilde{G}_{k_\infty^+} \simeq \mathbf{Z}/p\mathbf{Z}$, *and* $\tilde{G}_{k_\infty L(k_\infty^+)}$ *is a free pro-p group,*
(2) k_∞/k *is totally ramified at any prime lying above p,*
(3) $\lambda(k_\infty/k) \geq 1+2\sqrt{1+\delta+s}$; *where $\lambda(k_\infty/k)$ is the Iwasawa λ-invariant of k_∞/k, s the number of primes of k_∞ lying above p, and $\delta = 1$ or 0 according as $\zeta_p \in k$ or not.*

For all n sufficiently large, more precisely if $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_n}/A_{k_n}^p = \dim_{\mathbf{Z}/p\mathbf{Z}} \tilde{G}_{k_\infty}^{\mathrm{ab}}/(\tilde{G}_{k_\infty}^{\mathrm{ab}})^p$, *then* $\#\tilde{G}_{k_n} = \infty$ *and* $\tilde{G}_{k_n}$ *has an element of order p.*

Theorem 1.2 follows from the next theorem.

THEOREM 1.3. *Let p be an odd prime number, K/k an unramified Galois extension of degree p of CM-fields and denote by K^+ and k^+ the maximal totally real field of K and k respectively. Let K_∞, k_∞ the cyclotomic $\mathbf{Z}_p$-extension of K and k respectively. Assume that $\tilde{G}_{K_\infty}$ is a free pro-p group and $\tilde{G}_{K_\infty^+}$ is trivial. Then $\tilde{G}_{k_\infty}$ is expressed as*

$$\tilde{G}_{k_\infty} \simeq \begin{cases} (\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p) \coprod F_{\lambda(k_\infty/k)-1} & (\textit{if} \ \ \zeta_p \in k) \\ \mathbf{Z}/p\mathbf{Z} \coprod F_{\lambda(k_\infty/k)} & (\textit{if} \ \ \zeta_p \notin k)\,, \end{cases}$$

where ζ_p is a primitive p-th root of unity, F_d is a free pro-p group of rank d, $\lambda(k_\infty/k)$ is the Iwasawa λ-invariant of k_∞/k, and the symbol $\coprod$ stands for the free pro-p product.

Though in each proof of Theorem 1.1 and Theorem 1.3, the assumption that the Galois groups $\tilde{G}_{k_\infty}$ and $\tilde{G}_{K_\infty}$ are free plays a crucial role, it is very difficult to check whether these Galois groups are free.

We remark that Theorem 1.1 may be an answer of the above question (a) because if $\lambda = 2$ and $n \geq 0$ then $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_n}/A_{k_n}^p = 2$ under the condition of the theorem. It is known under some similar situations that $\#\tilde{G}_{k_n} = \infty$ for all sufficiently large n. In Theorem 1.3, we remark that the assumption $\tilde{G}_{K_\infty^+} = 0$ is equivalent to the statement $\tilde{G}_{k_\infty^+} \simeq \mathbf{Z}/p\mathbf{Z}$, and that the Iwasawa μ-invariants of K_∞/K and k_∞/k are zero, since $\tilde{G}_{K_\infty}$ is a free pro-p group.

2. Preliminaries

In the following, for any finite number field k, we use the notation k_∞, $\lambda(k_\infty/k)$, $\mu(k_\infty/k)$ for the cyclotomic $\mathbf{Z}_p$-extension of k and the Iwasawa λ, μ-invariants of k_∞/k respectively. For any odd prime p and any CM-field k, we also use the notation k^+ for the maximal totally real subfield of k, and put $\lambda(k_\infty/k)^- = \lambda(k_\infty/k) - \lambda(k_\infty^+/k^+)$, $\mu(k_\infty/k)^- = \mu(k_\infty/k) - \mu(k_\infty^+/k^+)$.

To prove our results, we will use some lemmas in this section. First, we introduce pro-p group theoretical lemmas. The first one is a criterion for the infiniteness of a finitely generated pro-p group. The second one is a pro-p analogue of the theorem of Dyer and Scott in [1]. It has been proved in [20] by Scheiderer in the case where a given group is finitely generated, and extended by Herfort, Ribes and Zalesskii in [6] to the general case (but we need only the finitely generated case).

LEMMA 2.1 (Theorem 7.21 of [10]). *Let p be a prime number and G a finitely generated pro-p group, i.e., G is generated by finite elements of G topologically. Put $d := \dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^1(G, \mathbf{Z}/p\mathbf{Z})$ and $r := \dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z})$. Let $1 \to R \to F \to G \to 1$ be a minimal presentation of G by a free pro-p group F. Let $I \subseteq \mathbf{Z}/p\mathbf{Z}[[F]]$ be the argumentation ideal of the complete group ring $\mathbf{Z}/p\mathbf{Z}[[F]]$ of F with coefficients in $\mathbf{Z}/p\mathbf{Z}$, and put $F(n) := \{a \in F | a - 1 \in I^n\}$ (The set $\{F(n) | n \geq 1\}$ is called the Zassenhaus filtration.)*

(1) *If $a \in F$ and $b \in F(n)$, then $[a, b] = aba^{-1}b^{-1} \in F(n+1)$ and $b^p \in F(pn)$.*

(2) *If G is finite and $R \subseteq F(n)$, then $r > (d^n(n-1)^{n-1})/n^n$.*

LEMMA 2.2. (Scheiderer [20], Herfort-Ribes-Zalesskii [6]) *Let p be a prime number and let G be a pro-p group that contains an open free pro-p subgroup H of index p. Then G is written as a free pro-p product*:

$$G \simeq \left(\coprod_{x \in X} (\mathbf{Z}/p\mathbf{Z} \times F^{(x)}) \right) \coprod F ,$$

where F is a free pro-p group and $F^{(x)}$'s are free pro-p groups indexed by a profinite space X (the profinite space X is a quotient of the space of conjugacy classes of elements of order p in G).

The following two lemmas are basic facts in the theory of $\mathbf{Z}_p$-extensions. Lemma 2.3 describes the relation rank of $\tilde{G}_{k_n}$ by using $\tilde{G}_{k_\infty}$. Note that $\mathrm{Gal}(k_\infty/k)(\simeq \mathbf{Z}_p)$ acts on $\tilde{G}_{k_\infty}$ non-canonically via the inner automorphism (this action is defined modulo $\mathrm{Inn}\tilde{G}_{k_\infty}$), since the p-cohomological dimension of $\mathrm{Gal}(k_\infty/k)$ is 1. Lemma 2.4, called Kida's formula, is an analogue of the formula of Riemann-Hurwitz.

LEMMA 2.3. *Let k be a finite extension of $\mathbf{Q}$ and k_∞/k the cyclotomic $\mathbf{Z}_p$-extension which is totally ramified at all primes lying above p. Then we may assume that an extension $\tilde{\gamma} \in \mathrm{Gal}(\tilde{L}(k_\infty)/k)$ of a topological generator $\gamma \in \Gamma = \mathrm{Gal}(k_\infty/k)$ generates the inertia subgroup of a prime lying above p. We define the action of Γ on $\tilde{G}_{k_\infty}$ by $\gamma(g) := \tilde{\gamma} g \tilde{\gamma}^{-1}$. Let R_n be the kernel of the natural mapping from $\tilde{G}_{k_\infty}$ to $\tilde{G}_{k_n}$ and s the number of primes of k_∞ lying above p. Then there are elements $g_2, \ldots, g_s \in \tilde{G}_{k_\infty}$ such that R_n is generated by $[\Gamma^{p^n}, \tilde{G}_{k_\infty}] = \langle \sigma(g)g^{-1} | \sigma \in \Gamma^{p^n}, g \in \tilde{G}_{k_\infty} \rangle$ and $\nu_n(g_i) = g_i \gamma(g_i) \cdots \gamma^{p^n-1}(g_i)$ $(2 \leq i \leq s)$ as a closed normal subgroup of $\tilde{G}_{k_\infty}$.*

PROOF. For a proof, see [18] or Lemma 13.15 of [21]. □

LEMMA 2.4. (Kida [8]) *Let p be an odd prime, and let k and K be CM-fields such that K/k is a Galois p-extension. Let K_∞ (resp. k_∞) be the cyclotomic $\mathbf{Z}_p$-extension of K (resp. k). Assume $\mu(k_\infty/k)^- = 0$. Then $\mu(K_\infty/K)^- = 0$ and*

$$\lambda(K_\infty/K)^- = [K_\infty : k_\infty](\lambda(k_\infty/k)^- - \delta) + \sum_{w_+}(e(w^+) - 1) + \delta\,,$$

where the sum on the right side is taken over all finite non-p-primes w^+ on K_∞^+, split in the extension K_∞/K_∞^+, $e(w^+)$ is the ramification index in K_∞^+/k_∞^+ of w^+, and $\delta = 1$ or 0 according as $\zeta_p \in k$ or not.

As a corollary to Lemmas 2.1 and 2.3, we obtain an upper bound of the relation ranks of $\tilde{G}_{k_n}$ and a sufficient condition for the p-class field tower to be infinite.

COROLLARY 2.1. *Let k be a finite extension of $\mathbf{Q}$ and k_∞/k the cyclotomic $\mathbf{Z}_p$-extension which is totally ramified at any prime lying above p. Put $h_n^i = \dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^i(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z})$ and $h^i = \dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^i(\tilde{G}_{k_\infty}, \mathbf{Z}/p\mathbf{Z})$. Suppose that $h^2 < \infty$. Then $h_n^1 \le h_n^2 \le h_n^1 + h^2 + s - 1$. In particular, if $h_n^1 \ge 2 + 2\sqrt{h^2 + s}$, then $\#\tilde{G}_{k_n} = \infty$.*

PROOF. Applying the five term sequence to the sequence $1 \to R_n \to \tilde{G}_{k_\infty} \to \tilde{G}_{k_n} \to 1$, we obtain an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^1(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z}) &\longrightarrow \mathrm{H}^1(\tilde{G}_{k_\infty}, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^1(R_n, \mathbf{Z}/p\mathbf{Z})^{\tilde{G}_{k_n}} \\ \longrightarrow \mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z}) &\longrightarrow \mathrm{H}^2(\tilde{G}_{k_\infty}, \mathbf{Z}/p\mathbf{Z}). \end{aligned}$$

It follows from Lemma 2.3 that $\dim_{\mathbf{Z}/p\mathbf{Z}} \mathrm{H}^1(R_n, \mathbf{Z}/p\mathbf{Z})^{\tilde{G}_{k_n}} \le h^1 + s - 1$. Thus $h_n^2 \le h_n^1 + h^2 + s - 1$. The inequality $h_n^1 \le h_n^2$ is always valid since $\tilde{G}_{k_n}^{\mathrm{ab}} \simeq A_k$ is finite. If $1 \to R \to F \to \tilde{G}_{k_n} \to 1$ is a minimal presentation of $\tilde{G}_{k_n}$ by a free pro-p group F, then $R \subseteq F^p[F, F] \subseteq F(2)$. By Lemma 2.1, if $h_n^2 \le h_n^1 + h^2 + s - 1 \le (h_n^1)^2/4$, then $\#\tilde{G}_{k_n} = \infty$, so that the second assertion follows. □

3. Proof of Theorem 1.1

First of all, we remark that our assumptions and Corollary 2.1 imply that $h_n^1 = h_n^2$ for each $n \ge 0$. This implies $\mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Q}_p/\mathbf{Z}_p) = 0$ for all $n \ge 0$. By the natural isomorphisms of the Galois groups $\langle J \rangle = \mathrm{Gal}(k/k^+) \simeq \mathrm{Gal}(k_n/k_n^+) \simeq \mathrm{Gal}(k_\infty/k_\infty^+)$ for all $n \ge 0$, we identify these groups. The involution J also acts on $\tilde{G}_{k_\infty}$ and $\tilde{G}_{k_n}$ via the inner automorphism which is defined modulo $\mathrm{Inn}\tilde{G}_{k_\infty}$ and modulo $\mathrm{Inn}\tilde{G}_{k_n}$. We define this action as following: Let $Z \subset \mathrm{Gal}(\tilde{L}(k_\infty)/k^+)$ be the decomposition group of a prime lying above p. We may assume $\tilde{\gamma} \in Z$. Then there is the natural isomorphism $Z \simeq \Gamma \times \langle J \rangle$ since $\tilde{\gamma}$ generates the inertia group by our assumptions, so that we can chose an extension of J such that it commutes to $\tilde{\gamma}$.

So we define the action of J by inner automorphism by this extension. Note that the action of J on $\tilde{G}_{k_\infty}$-, $\tilde{G}_{k_n}$-cohomology groups is independent on the choice of the extension of J.

Suppose that $h_1^1 \geq 3$. Since the class number of k_n^+ is prime to p for all $n \geq 0$ and $\mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z}) \simeq \mathrm{H}^1(\tilde{G}_{k_n}, \mathbf{Q}_p/\mathbf{Z}_p)/p$ from $\mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Q}_p/\mathbf{Z}_p) = 0$, one sees that $\mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z}) = \mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z})^-$, the minus part of $\mathrm{H}^2(\tilde{G}_{k_n}, \mathbf{Z}/p\mathbf{Z})$ with respect to the action of J. Hence $\#\tilde{G}_{k_1} = \infty$ by [9].

Let λ be the Iwasawa λ-invariant of k_∞/k. By the assumption (1), $\tilde{G}_{k_\infty}$ is a free pro-p group of rank λ. Let $\{x_1, \dots, x_\lambda\}$ be a system of generators of $\tilde{G}_{k_\infty}$. We may assume $J(x_i) = x_i^{-1}$ for each i with $1 \leq i \leq \lambda$. Since the class number of k^+ is prime to p, k_∞/k is totally ramified at the prime lying above p. To go to the rest of the proof, we need the description of R_n which is defined by the exact sequence $1 \to R_n \to \tilde{G}_{k_\infty} \to \tilde{G}_{k_n} \to 1$. Since p does not split in $k_\infty/\mathbf{Q}$, R_n is a closed normal subgroup of $\tilde{G}_{k_\infty}$ generated by the elements $\gamma^{p^n}(x_i)x_i^{-1}$ $(1 \leq i \leq \lambda)$ by Lemma 2.3. If $\lambda \geq 3$, then $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_1}/A_{k_1}^p \geq 3$ by Theorem 1 of Fukuda [3], and hence $\tilde{L}(k_1)/k_1$ is infinite by the above arguments. Suppose that $p \geq 5$ and $\lambda = 2$. Since $\tilde{G}_{k_\infty}$ is a free pro-p group of rank 2 and $\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_n}/A_{k_n}^p = 2$, the exact sequence

$$1 \longrightarrow R_n \longrightarrow \tilde{G}_{k_\infty} \longrightarrow \tilde{G}_{k_n} \longrightarrow 1$$

is a minimal presentation of $\tilde{G}_{k_n}$ for every $n \geq 0$. This implies that $R_n \subseteq \tilde{G}_{k_\infty}^p C_2(\tilde{G}_{k_\infty})$, where $C_i(\tilde{G}_{k_\infty})$ stands for the i-th lower central series of $\tilde{G}_{k_\infty}$ and $\tilde{G}_{k_\infty}^p$ is the closed normal subgroup topologically generated by the p-th powers of elements of $\tilde{G}_{k_\infty}$. So that especially $\gamma(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}^p C_2(\tilde{G}_{k_\infty})$ for $i = 1$ and 2. Now we consider the filtration

$$\tilde{G}_{k_\infty} \supseteq \tilde{G}_{k_\infty}^p C_2(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^p C_4(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^p C_5(\tilde{G}_{k_\infty})$$

of $\tilde{G}_{k_\infty}$. Since the map $C_2(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty}) \to \tilde{G}_{k_\infty}^p C_2(\tilde{G}_{k_\infty})/\tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})$ is surjective and since J acts on $C_2(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})$ trivially because of the fact $\tilde{G}_{k_\infty}^{ab} = (\tilde{G}_{k_\infty}^{ab})^-$, we see that $\gamma(x_i)x_i^{-1} \equiv J(\gamma(x_i)x_i^{-1}) = \gamma(x_i)^{-1}x_i \bmod \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})$. From the fact that abelian pro-p groups are uniquely divisible by n such that $p \nmid n$, we obtain $\gamma(x_i) \equiv x_i \bmod \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})$, i.e. $\gamma(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})$. Next we consider the surjective map

$$C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^p C_4(\tilde{G}_{k_\infty}) \to \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})/\tilde{G}_{k_\infty}^p C_4(\tilde{G}_{k_\infty})\,.$$

Note that $C_3(\tilde{G}_{k_\infty})/C_4(\tilde{G}_{k_\infty})$ is generated over $\mathbf{Z}_p$ by the elements $[x_1, [x_1, x_2]]C_4(\tilde{G}_{k_\infty})$ and $[x_2, [x_1, x_2]]C_4(\tilde{G}_{k_\infty})$. Then we see that

$$C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^p C_4(\tilde{G}_{k_\infty}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$$

and that $C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^p C_4(\tilde{G}_{k_\infty})$ is a $\mathbf{Z}/p\mathbf{Z}[[\Gamma]]$-module. Recall that $\mathbf{Z}/p\mathbf{Z}[[\Gamma]]$ is a complete discrete valuation ring with the maximal ideal $(\gamma - 1)$. These facts show that $C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^p C_4(\tilde{G}_{k_\infty})$ is killed by $(\gamma - 1)^{p-1}$ because $p \geq 3$. Since $(\gamma - 1)^{p-1} \equiv \gamma^{p-1} + \cdots + \gamma + 1 \bmod p$, we obtain

$$1 \equiv (\gamma^{p-1} + \cdots + \gamma + 1)(\gamma(x_i)x_i^{-1}) \equiv \gamma^p(x_i)x_i^{-1} \bmod \tilde{G}_{k_\infty}^p C_4(\tilde{G}_{k_\infty})$$

by the above surjective map $C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^p C_4(\tilde{G}_{k_\infty}) \to \tilde{G}_{k_\infty}^p C_3(\tilde{G}_{k_\infty})/\tilde{G}_{k_\infty}^p C_4(\tilde{G}_{k_\infty})$. In the same way as the above, we can show that $\gamma^p(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}^p C_5(\tilde{G}_{k_\infty})$. By the properties of the Zassenhaus filtration, we obtain $\tilde{G}_{k_\infty}^p, C_5(\tilde{G}_{k_\infty}) \subseteq \tilde{G}_{k_\infty}(5)$ (here $\tilde{G}_{k_\infty}(n)$ stands for the n-th Zassenhaus filtration of $\tilde{G}_{k_\infty}$), hence $\gamma^p(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}(5)$. We mentioned in the above that both the generator rank and the relation rank of $\tilde{G}_{k_n}$ are equal to 2. By Lemma 2.3, $R_1 \subseteq \tilde{G}_{k_\infty}(5)$ and hence

$$r = 2 < \frac{2^5}{5^5}4^4 = \frac{8192}{3125}\,.$$

This implies that $\tilde{L}(k_1)/k_1$ is infinite.

Suppose that $p = 3$, $\lambda = 2$ and $A_k \simeq \mathbf{Z}/3^a\mathbf{Z} \oplus \mathbf{Z}/3^b\mathbf{Z}$ with $a, b \geq 2$. Then we have $\gamma(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}^9 C_2(\tilde{G}_{k_\infty})$. We consider the filtration

$$\tilde{G}_{k_\infty} \supseteq \tilde{G}_{k_\infty}^9 C_2(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})^3 C_4(\tilde{G}_{k_\infty}) \supseteq \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})^3 C_5(\tilde{G}_{k_\infty})$$

of $\tilde{G}_{k_\infty}$. By using the action of J, we see that $\gamma(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})$. >From the above arguments, the surjective maps

$$C_3(\tilde{G}_{k_\infty})/C_3(\tilde{G}_{k_\infty})^3 C_4(\tilde{G}_{k_\infty}) \longrightarrow \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})/\tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})^3 C_4(\tilde{G}_{k_\infty})$$

and

$$C_4(\tilde{G}_{k_\infty})/C_5(\tilde{G}_{k_\infty}) \longrightarrow \tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})^3 C_4(\tilde{G}_{k_\infty})/\tilde{G}_{k_\infty}^9 C_3(\tilde{G}_{k_\infty})^3 C_5(\tilde{G}_{k_\infty})\,,$$

yields that $\gamma^3(x_i)x_i^{-1} \in \tilde{G}_{k_\infty}(5)$ since $\tilde{G}_{k_\infty}^9, C_3(\tilde{G}_{k_\infty})^3 \subseteq \tilde{G}_{k_\infty}(9)$ and $C_5(\tilde{G}_{k_\infty}) \subseteq \tilde{G}_{k_\infty}(5)$. Hence $\tilde{L}(k_1)/k_1$ is infinite.

4. Proof of Theorem 1.2 and Theorem 1.3

First, we prove Theorem 1.3. Suppose that p, k and K satisfy the assumption of Theorem 1.3. Regard $\tilde{G}_{K_\infty} \subseteq \tilde{G}_{k_\infty}$. Put $G = \tilde{G}_{k_\infty} \supseteq H = \tilde{G}_{K_\infty}$, $\lambda = \lambda(k_\infty/k) = \lambda(k_\infty/k)^-$ and $\lambda' = \lambda(K_\infty/K) = \lambda(K_\infty/K)^-$. Then we have $H^{\mathrm{ab}} = (H^{\mathrm{ab}})^- \simeq \mathbf{Z}_p^{\oplus\lambda'}$, $G^{\mathrm{ab}} \simeq (G^{\mathrm{ab}})^+ \oplus (G^{\mathrm{ab}})^- \simeq \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}_p^{\oplus\lambda}$ as $\mathbf{Z}_p$-modules, since $(H^{\mathrm{ab}})^-$ and $(G^{\mathrm{ab}})^-$, which are defined as the minus part of H^{ab} and G^{ab} with respect to the action of $\mathrm{Gal}(k_\infty/k_\infty^+) \simeq \mathrm{Gal}(K_\infty/K_\infty^+)$, have no torsion and $\mu(k_\infty/k) = 0$. It follows that H is a free pro-p group with rank λ' and that

$$\mathrm{H}^1(G, \mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus(\lambda+1)}$$

(i.e. the generator rank of G is $\lambda + 1$). The key to the proof is the next proposition that Ozaki had also obtained.

PROPOSITION 4.1. *The cohomology group* $\mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z})$ *is isomorphic to* $(\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$ *or* $\mathbf{Z}/p\mathbf{Z}$ (*i.e. the relation rank of* G *is* 2 *or* 1) *according as* $\zeta_p \in k$ *or not.*

PROOF. Since H^{ab} is a $\mathbf{Z}_p$-torsion free $\mathbf{Z}_p[G/H]$-module and G/H is a cyclic group of order p, H^{ab} can be described as follows (see Reiner [19]):

$$H^{\mathrm{ab}} \simeq \mathbf{Z}_p[G/H]^{\oplus a_p} \oplus I(G/H)^{\oplus a_{p-1}} \oplus \mathbf{Z}_p^{\oplus a_1} \quad (a_p, a_{p-1}, a_1 \geq 0)\,,$$

where $I(G/H)$ is the augmentation ideal of the group ring $\mathbf{Z}_p[G/H]$. Therefore the coinvariant $(H^{\mathrm{ab}})_{G/H}$ is described as $(H^{\mathrm{ab}})_{G/H} \simeq (I(G/H)/I^2(G/H))^{\oplus a_{p-1}} \oplus \mathbf{Z}_p^{\oplus(a_p+a_1)}$. From the facts that $\mathbf{Z}_p^{\oplus\lambda} = (G^{\mathrm{ab}})^-$ is equal to $(H^{\mathrm{ab}})_{G/H}$ and $I(G/H)/I^2(G/H) \simeq \mathbf{Z}/p\mathbf{Z}$, we obtain $a_{p-1} = 0$ and $a_p + a_1 = \lambda$. Hence we have

$$\mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{Z}/p\mathbf{Z}[G/H]^{\oplus a_p} \oplus (\mathbf{Z}/p\mathbf{Z})^{\oplus a_1}$$

as $\mathbf{Z}/p\mathbf{Z}[G/H]$-modules, and $p\,a_p + a_1 = \lambda'$. On the other hand, by Theorem 2.4, $\lambda' = p(\lambda - \delta) + \delta$, where δ is the same as in Theorem 2.4. Hence $a_1 = \delta$. Thus we obtain

$$\mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{Z}/p\mathbf{Z}[G/H]^{\oplus(\lambda-\delta)} \oplus (\mathbf{Z}/p\mathbf{Z})^{\oplus\delta}\,.$$

Therefore $\mathrm{H}^0(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus\lambda}$ and $\mathrm{H}^1(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus\delta}$. Next, we determine the relation rank of G. Since $H^q(H, \mathbf{Z}/p\mathbf{Z}) = 0$ for all $q \geq 2$, the Serre-Hochschild spectral sequence induces a long exact sequence

$$\begin{aligned} 0 &\longrightarrow \mathrm{H}^1(G/H, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^1(G, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^0(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \\ &\longrightarrow \mathrm{H}^2(G/H, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathrm{H}^1(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \\ &\xrightarrow{d_2^{1,1}} \mathrm{H}^3(G/H, \mathbf{Z}/p\mathbf{Z}) \longrightarrow \cdots \end{aligned}$$

Computing the dimension over $\mathbf{Z}/p\mathbf{Z}$ of each term in the above exact sequence, we see that the sequence

$$0 \to \mathrm{H}^2(G/H, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z}) \to \mathrm{H}^1(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \xrightarrow{d_2^{1,1}} \mathrm{H}^3(G/H, \mathbf{Z}/p\mathbf{Z})$$

is exact. If $\zeta_p \notin k$, then we know $\mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z}) \simeq \mathrm{H}^2(G/H, \mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{Z}/p\mathbf{Z}$. In order to determine the relation rank of G in the case $\zeta_p \in k$, we investigate the map

$$d_2^{1,1} : \mathrm{H}^1(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \to \mathrm{H}^3(G/H, \mathbf{Z}/p\mathbf{Z})\,.$$

If $d_2^{1,1} = 0$, then we obtain $\mathrm{H}^2(G, \mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$ by the above exact sequence. So that it is sufficient to show $d_2^{1,1} = 0$. The group extension

$$1 \longrightarrow H^{\mathrm{ab}} \longrightarrow G/[H, H] \longrightarrow G/H \longrightarrow 1$$

defines a cohomology class $u \in \mathrm{H}^2(G/H, H^{\mathrm{ab}})$, where $[H, H]$ is the topological commutator subgroup of H. Using $\mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z}) = \mathrm{Hom}(H^{\mathrm{ab}}, \mathbf{Z}/p\mathbf{Z})$, we obtain a canonical pairing $H^{\mathrm{ab}} \times \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z}) \to \mathbf{Z}/p\mathbf{Z}$ which induces a cup-product

$$\cup : \mathrm{H}^2(G/H, H^{\mathrm{ab}}) \times \mathrm{H}^1(G/H, \mathrm{H}^1(H, \mathbf{Z}/p\mathbf{Z})) \to \mathrm{H}^3(G/H, \mathbf{Z}/p\mathbf{Z})\,.$$

Let $u\cup$ be the map $x \mapsto u \cup x$. Then the maps $d_2^{1,1}$ and $u\cup$ are the same up to sign, i.e. $d_2^{1,1} = \pm u\cup$ (see Neukirch, Schmidt and Wingberg [17, Theorem 2.1.8]). Assume that G contains no element of order p. Then G must be free, according to Lemma 2.2. However, this contradicts the fact that G^{ab} has a subgroup isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Therefore there is some element x in G such that $x^p = 1$. Since H is free, x is not contained in H. Hence G/H is generated by the image of x, and hence the above group extension splits. It follows $u = 0$, and $d_2^{1,1}$ is a zero map. This completes the proof of Proposition 4.1. □

By Lemma 2.2, we have

$$G \simeq \left(\coprod_{i=1}^{r} (\mathbf{Z}/p\mathbf{Z} \times F_{d_i})\right) \coprod F_d$$

for some d_i, d, and r (note that G is finitely generated). Hence

$$G^{\mathrm{ab}} \simeq \bigoplus_{i=1}^{r} (\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}_p^{\oplus d_i}) \oplus \mathbf{Z}_p^{\oplus d}\,.$$

Since $G^{\mathrm{ab}} \simeq \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}_p^{\oplus \lambda}$, we have $r = 1$. Thus, by Proposition 4.1 and Künneth formula (see [7]), G must be isomorphic to $(\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p) \coprod F_{\lambda-1}$ or $\mathbf{Z}/p\mathbf{Z} \coprod F_\lambda$ according as $\zeta_p \in k$ or not. This completes the proof of Theorem 1.3.

We prove Theorem 1.2. Let k be a CM-field satisfying the condition in Theorem 1.2. Then, by Theorem 1.3 and the assumption in Theorem 1.2, the Galois group $\tilde{G}_{k_\infty} = \mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ has the form $\tilde{G}_{k_\infty} \simeq (\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}_p) \coprod F_{\lambda(k_\infty/k)-1}$ or $\mathbf{Z}/p\mathbf{Z} \coprod F_{\lambda(k_\infty/k)}$. Since

$$\dim_{\mathbf{Z}/p\mathbf{Z}} A_{k_n}/A_{k_n}^p = \dim_{\mathbf{Z}/p\mathbf{Z}} \tilde{G}_{k_\infty}^{\mathrm{ab}}/(\tilde{G}_{k_\infty}^{\mathrm{ab}})^p = \lambda(k_\infty/k) + 1 \geq 2 + 2\sqrt{1+\delta+s}\,,$$

we have $\#\tilde{G}_{k_n} = \infty$ by Corollary 2.1. Next, let

$$1 \longrightarrow R \longrightarrow F \longrightarrow \tilde{G}_{k_\infty} \longrightarrow 1$$

be a minimal presentation of $\tilde{G}_{k_\infty}$ by a free pro-p group F of rank $\lambda(k_\infty/k)+1$ and let N_n be the kernel of the composite of the map $F \to \tilde{G}_{k_\infty}$ and the surjective restriction $\tilde{G}_{k_\infty} \to \tilde{G}_{k_n}$.

Denote a generator of $\tilde{G}_{k_\infty}$ with order p by α and the pre-image by $a \in F$. Since $1 \to N_n \to F \to \tilde{G}_{k_n} \to 1$ is a minimal presentation of $\tilde{G}_{k_n}$, the image of a in $\tilde{G}_{k_n}$ must be a generator with order p. This completes the proof.

5. On the Freeness of $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$

In this section, we give a sufficient condition for $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ to be free for an imaginary quadratic field k. But, up to now, we cannot find an example of such a k.

PROPOSITION 5.1. *Let k be an imaginary quadratic field and p an odd prime number. Let M_k/k be the maximal pro-p extension unramified outside p. Suppose that p does not split in $k/\mathbf{Q}$. Let $\mathfrak{p}$ be the prime of k lying above p. Let $k_\mathfrak{p}$ be the completion of k with respect to the prime $\mathfrak{p}$ and $\overline{k_\mathfrak{p}}/k_\mathfrak{p}$ the maximal pro-p extension. If $\mathrm{Gal}(M_k/k)$ is a free pro-p group and the natural mapping $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p}) \to \mathrm{Gal}(M_k/k)$ is not injective, then $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ is a free pro-p group.*

An equivalent condition of the freeness of $\mathrm{Gal}(M_k/k)$ was essentially given by Minardi [13] (see also [2]). Note that if $\mathrm{Gal}(M_k/k)$ is a free pro-p group, then it is a pro-p group of rank 2.

PROOF. If $p = 3$ and $k = \mathbf{Q}(\sqrt{-3})$, then the claim is trivial because $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty) = 1$. So we may remove this case. Let H be the image of the mapping $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p}) \to \mathrm{Gal}(M_k/k)$. Then H is the decomposition group of a prime of M_k lying above p. Then H is a free pro-p group since $\mathrm{Gal}(M_k/k)$ is a free pro-p group. Note that we see $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p})$ is a free pro-p group of rank 3 by the injection from the principal local unit group of $k_\mathfrak{p}$ to the $\mathbf{Z}_p$-torsion free module $\mathrm{Gal}(M_k/k)^{\mathrm{ab}}$. By our assumption that the mapping $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p}) \to \mathrm{Gal}(M_k/k)$ is not injective, one sees that the generator rank of H is less than 3, so that it is equal to 2. Let $\tilde{L}'(k_\infty)/k_\infty$ be the maximal unramified pro-p extension which is completely decomposed at all primes of k_∞ above p, and put $\tilde{H} = H \cap \mathrm{Gal}(M_k/k_\infty)$. Let $\mathcal{H} = \langle g\tilde{H}g^{-1} | g \in \mathrm{Gal}(M_k/k_\infty)\rangle$ be the minimal closed normal subgroup of $\mathrm{Gal}(M_k/k_\infty)$ which contains $\tilde{H}$. Then we have the exact sequence

$$1 \longrightarrow \mathcal{H} \longrightarrow \mathrm{Gal}(M_k/k_\infty) \longrightarrow \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty) \longrightarrow 1$$

of pro-p groups. Since $\mathrm{Gal}(M_k/k)$ is a free pro-p group of rank 2, $\mathrm{Gal}(M_k/k_\infty)$ is a free pro-p Γ-operator group of rank 1. By the Hochschild-Serre spectral sequence, we have the following exact sequence

$$0 \to \mathrm{H}_2(\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty), \mathbf{Z}_p) \to \mathcal{H}/[\mathcal{H}, \mathrm{Gal}(M_k/k_\infty)] \to \Lambda \to \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}} \to 0\,.$$

Also, since $\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}}$ is a free $\mathbf{Z}_p$-module, there is a distinguished polynomial $f(T) \in \mathbf{Z}_p[T]$ such that $\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}} \simeq \Lambda/(f(T))$ as Λ-modules. This shows that

$$\mathcal{H}/[\mathcal{H}, \mathrm{Gal}(M_k/k_\infty)] \simeq \Lambda \oplus \mathrm{H}_2(\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty), \mathbf{Z}_p)$$

as Λ-modules.

Since H is the decomposition group of a prime lying above p and H is a free pro-p group of rank 2, $\tilde{H}$ is a free pro-p Γ-operator group of rank 1. Hence there is a surjective mapping

$$\tilde{H}^{\mathrm{ab}} \simeq \Lambda \twoheadrightarrow \mathcal{H}/[\mathcal{H}, \mathrm{Gal}(M_k/k_\infty)] \simeq \Lambda \oplus \mathrm{H}_2(\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty), \mathbf{Z}_p)\,.$$

Therefore $\mathrm{H}_2(\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty), \mathbf{Z}_p) = 0$. Since $\mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}}$ is $\mathbf{Z}_p$-torsion free, this shows that $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ is a free pro-p group. By the exact sequence

$$1 \longrightarrow D \longrightarrow \mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty) \longrightarrow \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty) \longrightarrow 1\,,$$

we have the exact sequence

$$0 \longrightarrow D/[D, \mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)] \longrightarrow \mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}} \longrightarrow 0\,.$$

Since $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)^{\mathrm{ab}} \simeq \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)^{\mathrm{ab}}$, we see that $D = 1$, we conclude that $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty) = \mathrm{Gal}(\tilde{L}'(k_\infty)/k_\infty)$ is a free pro-p group. □

Note that Proposition 5.1 is not contained in the theorems of Kuz'min [12] and Mukhamedov [16]. It is still an open problem whether $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p}) \to \mathrm{Gal}(M_k/k)$ is always injective or not. Also, by using the Iwasawa main conjecture, we have many examples of imaginary quadratic fields such that $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ is *not* a free pro-p group (see [18]).

REMARK. After the submission, the referee remarked that $\mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty) = 1$ under the assumption of Proposition 5.1 if the generalized Greenberg's conjecture is true for k and p.

ACKNOWLEDGEMENT. The authors would like to thank the referee for pointing out the above remark. Also, the authors would like to express their gratitude for a number of helpful suggestions to Doctor Yasushi Mizusawa.

References

[1] J. L. DYER and G. P. SCOTT, Periodic automorphisms of free groups, Comm. Algebra **3** (1975), 195–201.

[2] S. FUJII, On the maximal pro-p extension unramified outside p of an imaginary quadratic field, submitted.

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

[4] F. HAJIR, On a theorem of Koch, Pacific J. Math. **176** (1996), 15–18.

[5] F. HAJIR, On the growth of p-class groups in p-class field towers, J. Algebra **188** (1997), 256–271.

[6] W. N. HERFORT, L. RIBES and P. ZALESSKII, p-extensions of free pro-p groups, (English summary) Forum Math. **11** (1999), 49–61.

[7] U. JANNSEN, The splitting of the Hochschild-Serre spectral sequence for a product of groups, Canad. Math. Bull. **33** (1990), 181–183.

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

[9] H. KISILEVSKY and J. LABUTE, On a sufficient condition for the p-class tower of a CM-field to be infinite, In: Proceedings of the Int. Number Conf, Laval (1987), Berlin (1989).

[10] H. KOCH, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[11] H. KOCH and B. B. VENKOV, Über den p-Klassenkörperturm eines imaginärquadratischen Zahlkörpers, Soc. Math. France, Astérisque **24–25** (1975), 57–67.

[12] L. V. KUZ'MIN, Local extensions associated with l-extensions with restricted ramification, Izv. Akad. Nauk SSSR **39** (1975), no. 4 (English translation in Math. USSR Izv. 9 (1975), 693–726).

[13] J. MINARDI, Iwasawa modules for $\mathbf{Z}_p^d$-extensions of algebraic number fields, thesis, Harvard Univ., 1986.

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

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

[16] V. G. MUKHAMEDOV, Local extensions associated with the l-extensions of number fields with restricted ramification, Mat. Zametki **35** (1984), 481–490 (English translation in Math. Notes 35, 253–258).

[17] J. NEUKIRCH, A. SCHMIDT and K. WINGBERG, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

[18] M. OZAKI, Non-abelian Iwasawa theory of $\mathbf{Z}_p$-extensions, preprint.

[19] I. REINER, Integral representations of cyclic groups of prime order, Proc. Amer. Math. Soc. **8** (1957), 142–146.

[20] C. SCHEIDERER, The structure of some virtually free pro-p groups, Proc. Amer. Math. Soc. **127** (1999), 695–700.

[21] L. C. WASHINGTON, *Introduction to cyclotomic fields*, second edition, GTM 83, Springer-Verlag, 1997.

Present Addresses:
SATOSHI FUJII
KEIO UNIVERSITY,
HIYOSHI, KOHOKU-KU, YOKOHAMA, 223–8522 JAPAN.
e-mail: fujii@ruri.waseda.jp

KEIJI OKANO
DEPARTMENT OF MATHEMATICAL SCIENCES, SCHOOL OF SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
OKUBO, SHINJUKU-KU, TOKYO, 169–8555 JAPAN.
e-mail: okano@suou.waseda.jp