RIMS Kôkyûroku Bessatsu **4**
(2007), 223–233

On unramified pro-p Galois groups over cyclotomic $\mathbb{Z}_p$-extensions — A survey

By

Yasushi Mizusawa*

Abstract

For a fixed prime number p, we denote by k_∞ the cyclotomic $\mathbb{Z}_p$-extension of a given number field k. We expect that the Galois group $G(k_\infty)$ of the maximal unramified pro-p-extension over k_∞ would provide good information about the Galois groups of p-class field towers of number fields. In this paper, we will give an overview of some topics on $G(k_\infty)$ together with an announcement of some results in $p=2$ case.

§ 1. Introduction

Let p be a fixed prime number and $\mathbb{Z}_p$ the ring of p-adic integers. For a given finite extension k of the field $\mathbb{Q}$ of rational numbers, we denote by k_∞ the cyclotomic $\mathbb{Z}_p$-extension of the number field k. The Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$ is isomorphic to the additive group of $\mathbb{Z}_p$ and has a topological generator γ. The main object of this paper is the Galois group

$$G(k_\infty) = \mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$$

of the maximal unramified pro-p-extension $\widetilde{L}(k_\infty)$ of k_∞. By choosing a suitable section $\Gamma \hookrightarrow \mathrm{Gal}(\widetilde{L}(k_\infty)/k) : \gamma \mapsto \widetilde{\gamma}$ of the natural exact sequence

$$1 \to G(k_\infty) \to \mathrm{Gal}(\widetilde{L}(k_\infty)/k) \to \Gamma \to 1$$

(which splits since Γ is a free pro-p group) such that $\widetilde{\gamma}$ is an element of the inertia subgroup of a prime lying above p, we define an action of Γ on $G(k_\infty)$ via the left conjugations by $\widetilde{\gamma}$, i.e., we define a continuous homomorphism

$$\phi : \Gamma \to \mathrm{Aut}\, G(k_\infty)$$

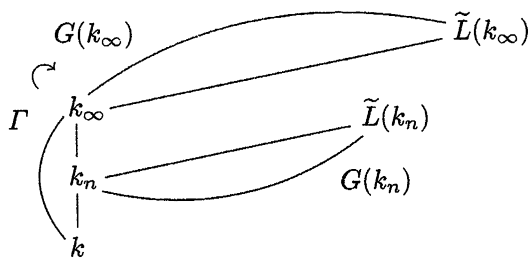
2000 Mathematics Subject Classification(s): 11R23.
The author was supported by JSPS Research Fellowships for Young Scientists.
*Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, 278-8510, Japan.

such that $\phi(\gamma)(g) = {}^{\gamma}g = \widetilde{\gamma}g\widetilde{\gamma}^{-1}$ for $g \in G(k_\infty)$. Then, the Galois group $G(k_\infty)$ is a pro-p-Γ operator group with ϕ (cf. [15] p.216, [23] I.1). To know the unramified pro-p Galois group $G(k_\infty)$ as a pro-p-Γ operator group is almost equivalent to knowing $\mathrm{Gal}(\widetilde{L}(k_\infty)/k) \simeq G(k_\infty) \rtimes \Gamma$ as a pro-p group.

For each integer $n \geq 0$, we denote by k_n the n-th layer of k_∞, i.e., the cyclic subextension of degree p^n over k. We are also interested in the Galois group $G(k_n) = \mathrm{Gal}(\widetilde{L}(k_n)/k_n)$ of the maximal unramified pro-p-extension $\widetilde{L}(k_n)$ of k_n. To borrow the words of Wingberg [23], the unramified pro-p Galois group is "one of the most mysterious objects in algebraic number theory". The sequence of unramified p-extensions associated to the commutator series of $G(k_n)$ is a classic object called p-class field tower of k_n. Especially, the abelianization of $G(k_n)$ is the Galois group of the Hilbert p-class field $L(k_n)$ over k_n, and the metabelian quotient of $G(k_n)$ is deeply related to the capitulation problem on the p-Sylow subgroup $A(k_n)$ ($\simeq \mathrm{Gal}(L(k_n)/k_n)$) of the ideal class group of k_n.

If n is sufficiently large, there is a surjective homomorphism $G(k_\infty) \twoheadrightarrow G(k_n)$ induced from the restriction mapping. Then, we can regard $G(k_n)$ as a quotient of $G(k_\infty)$, and the structure of $G(k_n)$ is reflected by the relations of pro-p group $G(k_\infty)$ and the action of Γ. By the induced projective system, we have an isomorphism $G(k_\infty) \simeq \varprojlim G(k_n)$.

In this paper, we investigate the Galois group $G(k_\infty)$ by expecting that its structure as a pro-p-Γ operator group would give good information about the Galois groups $G(k_n)$ of p-class field towers of k_n. As the grounds of the expectations, we shall see some topics on the Galois groups $G(k_\infty)$ and $G(k_n)$ in the next section. In the third section, we will see some examples of explicitly presented (abelian or metabelian) $G(k_\infty)$.



Acknowledgements. This paper is written as a report of the talk entitled "On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field" by the author. In the talk, the author announced some results written in subsection 3.2 with mentioning several topics in section 2. The author expresses his gratitude to Professor Ki-ichiro Hashimoto for giving him an opportunity of talking at the conference and submitting this article. The author also thanks to Doctor Satoshi

Fujii for giving him a lot of helpful advice and information.

§ 2. Related topics

2.1. From abelian Iwasawa theory. By the action of Γ induced from ϕ, the abelianization $X(k_\infty)$ of $G(k_\infty)$ is considered as an Iwasawa module, i.e., a module over the complete group ring $\mathbb{Z}_p[[\Gamma]]$. The module $X(k_\infty)$ is identified with the Galois group of the maximal unramified abelian pro-p-extension $L(k_\infty)$ of k_∞, and it is proven by Iwasawa that $X(k_\infty)$ is finitely generated and torsion as a $\mathbb{Z}_p[[\Gamma]]$-module. Then, we can define the Iwasawa invariants $\lambda = \lambda(X(k_\infty)) = \dim_{\mathbb{Q}_p}(X(k_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, $\mu = \mu(X(k_\infty))$ and the characteristic polynomial

$$P(T) = \det\big((1+T)id - \gamma \,|\, X(k_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \big)$$

of the Iwasawa module $X(k_\infty)$, where $\mathbb{Q}_p$ denotes the field of p-adic numbers (not p-th layer of $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$!). Based on the analogy with Alexander polynomial of a knot, it is pointed out in [14] that the Iwasawa polynomial $P(T)$ is also obtained in the words of pro-p Fox differential calculus if we have a presentation of $\mathrm{Gal}(\widetilde{L}(k_\infty)/k)$ explicitly.

For the cyclotomic $\mathbb{Z}_p$-extensions of any finite extensions of $\mathbb{Q}$, the vanishing of μ-invariants is conjectured by Iwasawa. Since "$\mu = 0$" is equivalent to the finiteness of the rank of $X(k_\infty)$ as a $\mathbb{Z}_p$-module, we can put this claim in the words about $G(k_\infty)$ as follows:

"$\mu = 0$" conjecture. The Galois group $G(k_\infty)$ is finitely generated as a pro-p group, i.e., the generator rank $d(G(k_\infty)) = \dim_{\mathbb{F}_p} H^1(G(k_\infty), \mathbb{Z}/p\mathbb{Z}) < \infty$.

Ferrero and Washington [3] proved that this conjecture is true if k is an abelian extension over $\mathbb{Q}$. This is an advantage of treating cyclotomic $\mathbb{Z}_p$-extensions.

Further, if k is a certain CM-field, the Iwasawa polynomial $P(T)$ is deeply related to the p-adic L-functions by the theorems of Mazur and Wiles [10] [22], namely "Iwasawa's main conjecture". Especially, if k is an imaginary quadratic field with the associated Dirichlet character χ ($\neq \omega$ the Teichmüller character), we have a power series $f(T) \in \mathbb{Z}_p[[T]]$ constructed from Stickelberger elements such that $(f(T)) = (2P(T))$ as a principal ideal of $\mathbb{Z}_p[[T]]$ and the Kubota-Leopoldt's p-adic L-function $L_p(s, \omega\chi) = f(\kappa(\gamma)^s - 1)$, where $\kappa : \Gamma \to \mathbb{Z}_p^\times$ is the restricted cyclotomic character.

2.2. Nonabelian Iwasawa type formulae. We define the lower central series of $G(k_\bullet)$ by putting $C^{(1)}(k_\bullet) = G(k_\bullet)$ and $C^{(i+1)}(k_\bullet) = [C^{(i)}(k_\bullet), G(k_\bullet)]$ for $i \geq 1$ inductively. The bracket means a topologically closed commutator subgroup. We also put the quotients $X^{(i)}(k_\bullet) = C^{(i)}(k_\bullet)/C^{(i+1)}(k_\bullet)$ for $i \geq 1$.

In [18], Ozaki defined the i-th Iwasawa module as the quotient $X^{(i)}(k_\infty)$ with the action of Γ induced from ϕ, and showed some basic properties. Especially, for each $i \geq 1$, $X^{(i)}(k_\infty) \simeq \varprojlim X^{(i)}(k_n)$ with respect to the restriction mappings. Note that $X^{(1)}(k_\infty) = X(k_\infty)$. If $\mu = 0$, the i-th Iwasawa module $X^{(i)}(k_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module with $\mu(X^{(i)}(k_\infty)) = 0$ for each $i \geq 1$. Then, the i-th Iwasawa λ-invariant is defined as $\lambda^{(i)} = \lambda(X^{(i)}(k_\infty)) = \dim_{\mathbb{Q}_p}(X^{(i)}(k_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$.

By considering the structure of $X^{(i)}(k_\infty)$ and putting $\widetilde{\lambda}^{(i)} = \sum_{j=1}^{i} \lambda^{(j)}$, Ozaki gave the following nonabelianization of Iwasawa's formula.

Theorem 2.1 (Ozaki [18]). *Assume that $\mu = 0$, and fix any $i \geq 1$. Then, there exists an integer $\widetilde{\nu}^{(i)}$ such that*

$$\#(G(k_n)/C^{(i+1)}(k_n)) = p^{\widetilde{\lambda}^{(i)}n + \widetilde{\nu}^{(i)}}$$

for all sufficiently large n.

Here, for each i, we denote by $n_0^{(i)}$ the minimal non-negative integer such that the above formula holds for all $n \geq n_0^{(i)}$.

The p-group $G(k_n)/C^{(i+1)}(k_n)$ is the maximal nilpotency-class-i quotient of $G(k_n)$. For $i = 1$, the formula above is well known as the Iwasawa's class number formula "$\#A(k_n) = p^{\lambda n + \mu p^n + \nu}$ $(n \gg 0)$" with $\mu = 0$ since $G(k_n)/C^{(2)}(k_n) \simeq A(k_n)$. In the case that $i = 2$, the asymptotic version "$\#(G(k_n)/C^{(3)}(k_n)) = p^{\widetilde{\lambda}^{(2)}n + o(1)}$ $(n \to \infty)$" has been proven by Fujii [5] under a certain condition.

The Ozaki's formula implies that the Galois groups $G(k_n)$ of p-class field towers also behave well Iwasawa-theoretically, i.e., the action of Γ on $G(k_\infty)$ controls the behavior of $G(k_n)$. Toward a nonabelianization of Iwasawa's main conjecture, Ozaki [17] asked that "What kind of p-adic functions relate to $X^{(i)}(k_\infty)$ and $G(k_\infty)$?". We are also interested in how p-adic L-functions relate to them.

2.3. Freeness and infinite p-class field towers. Based on the property that the Galois groups of p-class field towers are finitely presented, Golod and Shafarevich [7] gave a criterion for the infiniteness of p-class field towers. When the p-class field tower is infinite, we are interested in the cohomological dimension of the Galois group.

On the other hand, Ozaki [17] gave the following problem:

Problem 2.2. *Is the Galois group $G(k_\infty)$ always finitely presented as a pro-p group? Especially, the relation rank $r(G(k_\infty)) = \dim_{\mathbb{F}_p} H^2(G(k_\infty), \mathbb{Z}/p\mathbb{Z}) < \infty$?*

Though the general answer of this problem is not clear yet, Fujii and Okano [6] showed that $\#G(k_n) = \infty$ for sufficiently large n if $\infty > d(G(k_\infty))^2 \gg 4\,r(G(k_\infty))$, based on the idea of Wingberg [23]. Especially, they investigated the consequences under the assumption that $G(k_\infty)$ is a free pro-p group, i.e., $r(G(k_\infty)) = 0$.

Theorem 2.3 (Fujii-Okano [6]). *Let p be odd, and k a CM-field with the maximal totally real subfield k^+, and S the set of primes of k_∞ lying above p.*

(1) *Assume that $\#S = 1$, $\#A(k^+) = 1$ and $\dim_{\mathbb{F}_p}(3A(k)/3pA(k)) \geq 2$. If $G(k_\infty)$ is a free pro-p group, then $\#G(k_n) = \infty$ for all $n \geq 1$.*

(2) *Assume that $X(k_\infty^+) \simeq \mathbb{Z}/p\mathbb{Z}$, $\lambda \geq 1+2\sqrt{1+\delta+\#S}$ where $\delta = 1$ or 0 according to whether k contains a primitive p-th root ζ_p of unity or not. If $G(k'_\infty)$ is a free pro-p group for $k'_\infty = k_\infty L(k_\infty^+)$, then $\#G(k_n) = \infty$ for all sufficiently large n and $G(k_n)$ has an element of order p. (Especially, the cohomological dimension of $G(k_n)$ is infinite.)*

For each odd p, by using the result of [25], we can find infinitely many imaginary abelian extensions k of degree $2p$ satisfying the assumptions of (2) except for the freeness of $G(k'_\infty)$. In general, the freeness of $G(k_\infty)$ seems to be very delicate. Though the freeness for some CM-fields k (e.g., p-th cyclotomic field $k = \mathbb{Q}(\zeta_p)$) were treated in [23] (and [17] etc.), we have to pay attention to the pointing out (final Remark of [19]) and the results (announced in [20]) by Sharifi. Unfortunately, it seems that we have no concrete example of nonabelian free $G(k_\infty)$ yet.

If $G(k_\infty)$ is a nonabelian free pro-p group, we can see that $\lambda^{(i)}$ tends to infinity as $i \to \infty$. It is a considerable problem to find examples such that $\lambda^{(i)}$ (or $\widetilde{\lambda}^{(i)}$) are unbounded as $i \to \infty$.

2.4. p-adic analyticity and finite p-class field towers. For any finite dimensional vector space V_p over $\mathbb{Q}_p$ and any linear continuous representation $\rho : G(k_n) \to GL(V_p)$, it is conjectured (as a part of the conjecture by Fontaine and Mazur [4]) that the image of ρ is finite. In other words, this claim asserts that:

Fontaine-Mazur conjecture. The Galois group of p-class field tower has no infinite p-adic analytic quotient.

Since any finitely generated p-adic analytic pro-p group has an open powerful subgroup, we can replace the word "p-adic analytic" with "powerful" in the statement of this conjecture. As a weak version of this conjecture, we are also interested in the problem that whether the Galois group $G(k_n)$ itself can be infinite p-adic analytic (resp. powerful) or not. For this problem, Wingberg [24] proved the following by considering the Galois group $G(k_\infty)$.

Theorem 2.4 (Wingberg [24]). *Assume that p is odd and k is a CM-field containing ζ_p, and that $\mu = 0$ for k_∞. If n is sufficiently large and $G(k_n)$ is powerful, then $\#G(k_n) < \infty$.*

On the other hand, under the assumption that both "$\mu = 0$" conjecture and Fontaine-Mazur conjecture hold, we can easily show the following by the properties of p-adic analytic pro-p groups.

Proposition 2.5. *Assume that $\mu = 0$ for k_∞ and $G(k_\infty)$ is p-adic analytic. If Fontaine-Mazur conjecture (in the sense above) holds for $G(k_n)$, then $\#G(k_n) < \infty$.*

Proof. Put $H = \mathrm{Gal}(\widetilde{L}(k_n)/k_\infty \cap \widetilde{L}(k_n))$. Then H is an open subgroup of $G(k_n)$ and isomorphic to a quotient of $G(k_\infty)$. Since $G(k_\infty)$ has finite rank in the sense of [2] Definition 3.12 (cf. [2] Theorem 3.13, Corollary 8.33), H is also a pro-p group of finite rank (cf. [2] Exercise 3.1). Therefore, $G(k_n)$ is p-adic analytic. Since $G(k_n)$ has no infinite p-adic analytic quotient, $G(k_n)$ must be finite. □

The border between finite cases and infinite cases is one of the main theme in the study of p-class field towers. While the freeness of $G(k_\infty)$ provides criteria for infiniteness of $G(k_n)$ (Theorem 2.3, etc.), Proposition 2.5 implies that the p-adic analyticity of $G(k_\infty)$ provides criteria for finiteness of $G(k_n)$. Then, for $G(k_\infty)$, what is the border area between nearly free cases and p-adic analytic cases? It seems to be interesting problem to characterize number fields k with p-adic analytic $G(k_\infty)$ (including the cases that $G(k_\infty)$ becomes finite).

2.5. Greenberg's conjecture. For any totally real number field k, it is conjectured that $\#X(k_\infty) < \infty$ by Greenberg [8]. Since $X(k_\infty) = X^{(1)}(k_\infty) \simeq \varprojlim X^{(1)}(k_n)$, this claim is equivalent to that $\lambda = \mu = 0$, i.e., $X^{(1)}(k_\infty) \simeq X^{(1)}(k_n)$ for all $n \gg 0$. Since any finite unramified p-extension of k_∞ is also the cyclotomic $\mathbb{Z}_p$-extension of a certain totally real number field (which is actually a finite unramified p-extension of k_n for some n), we can extend this conjecture as follows:

Greenberg's conjecture (nonabelianized version). If k is a totally real number field, any open subgroup of $G(k_\infty)$ has finite abelianization (i.e., $G(k_\infty)$ satisfies "FIFA").

Let us call this property FIFA due to Boston [1]. The positive answers of this conjecture and Problem 2.2 imply that $G(k_\infty)$ is similar to the Galois groups of p-class field towers if k is totally real. From this point of view, Ozaki gave the following problem as a strong version of Greenberg's conjecture.

Problem 2.6. *If k is a totally real number field, $G(k_\infty) \simeq G(k_n)$ for $n \gg 0$?*

This claim is equivalent to that $\lambda = \mu = 0$ and $n_0^{(i)}$ is bounded as $i \to \infty$. If $G(k_\infty)$ is finite, this claim holds immediately. The finiteness of $G(k_\infty)$ is equivalent to the existence of a finite extension K over k such that $\#X(K_\infty) = 1$ (i.e., $\lambda = \mu = \nu = 0$ for K_∞). The abelian p-extensions K of $\mathbb{Q}$ with trivial $X(K_\infty)$ are completely characterized by Yamamoto ([25] etc.). It is also a considerable problem to characterize all finite (especially, p-)extensions K of $\mathbb{Q}$ with trivial $X(K_\infty)$.

If $G(k_\infty) \simeq G(k_n)$ for some $n \gg 0$, ϕ is not injective since $\phi(\gamma^{p^n}) = 1$. On the other hand, if ϕ is not injective, Γ^{p^n} acts on $G(k_\infty)$ trivially for all $n \gg 0$. Then, under the assumption that k is totally real and Leopoldt's conjecture holds for p and all subfields of $\widetilde{L}(k_\infty)$, we can show that $G(k_\infty)$ satisfies FIFA by using Proposition 1 of [8]. The injectivity of ϕ in the totally real case seems to be considerable as a problem between Greenberg's conjecture and Problem 2.6.

$$
\begin{array}{ccccc}
\boxed{\exists K/k \text{ finite};\, \#X(K_\infty) = 1} & \Leftrightarrow & \boxed{\#G(k_\infty) < \infty} & & \boxed{0 \neq r(G(k_\infty)) < \infty} \\
 & & \Downarrow & \nearrow\!\!\!\nearrow & \\
\boxed{\lambda = \mu = 0,\ \sup\{n_0^{(i)}\} < \infty} & \Leftrightarrow & \boxed{\forall n \gg 0;\, G(k_\infty) \simeq G(k_n)} & \Rightarrow & \\
 & & \Downarrow & & \boxed{G(k_\infty) \text{ satisfies FIFA}} \\
\boxed{\text{Leopoldt's conjecture}} & + & \boxed{\#\mathrm{Ker}\phi \neq 1} & \overset{*}{\Rightarrow} &
\end{array}
$$

For an imaginary quadratic field k in which p splits, the unique $\mathbb{Z}_p^{\oplus 2}$-extension $\widetilde{k}$ of k is unramified over k_∞. It is conjectured (as Greenberg's generalized conjecture) that the abelianization of $\mathrm{Gal}(\widetilde{L}(k_\infty)/\widetilde{k})$ is pseudo-null as a $\mathbb{Z}_p[[\mathrm{Gal}(\widetilde{k}/k)]]$-module. If this is true, $G(k_\infty)$ is not a nonabelian free pro-p group (cf. [17] etc.). On the other hand, we can find many examples for which $\widetilde{L}(k_\infty) = \widetilde{k}$, i.e., $G(k_\infty) \simeq \mathbb{Z}_p$ (not FIFA!) but $\#\mathrm{Im}\phi = 1$. (The arrow $\overset{*}{\Rightarrow}$ above depends on the totally reality of k.)

§ 3. Explicitly presented examples

3.1. Abelian examples. If $X(k_\infty)$ is a $\mathbb{Z}_p$-module of rank 1, then $G(k_\infty) \simeq X(k_\infty)$, i.e., $G(k_\infty)$ is also a cyclic pro-p group. In the case that $X(k_\infty)$ is not cyclic, it is not a trivial problem whether $G(k_\infty)$ is abelian or not. The abelianity of $G(k_\infty)$ is equivalent to the vanishing of second Iwasawa module $X^{(2)}(k_\infty)$. As an easiest case, we can show the following with nontrivial examples.

Proposition 3.1. *Let p be odd and k a CM-field containing ζ_p, and assume that $\mu = 0$. If $\lambda = 1$, then $G(k_\infty) \simeq \mathbb{Z}_p \oplus \mathbb{Z}/p^m\mathbb{Z}$ with some $m \geq 0$.*

Proof. Put $X^+ = X(k_\infty^+)$ for the maximal real subfield k^+ of k, and let X^- be the minus part of $X(k_\infty)$. Since p is odd, $X(k_\infty) \simeq X^+ \oplus X^-$. Since $\mu = 0$, X^- is a free $\mathbb{Z}_p$-module ([21] Corollary 13.29). By Leopoldt's Spiegelungssatz ([21] Theorem 10.11), we know that $\lambda(X^+) \leq \mathrm{rank} X^+ \leq \mathrm{rank} X^- = \lambda(X^-)$. Since $\lambda(X^+) + \lambda(X^-) = \lambda = 1$ by our assumption, we know that $G(k_\infty^+) \simeq X^+ \simeq \mathbb{Z}/p^m\mathbb{Z}$ with some $m \geq 0$ and $X^- \simeq \mathbb{Z}_p$. Then, $K_\infty^+ = \widetilde{L}(k_\infty^+)$ is an unramified finite cyclic p-extension of k_∞^+. Put

$K_\infty = k_\infty K_\infty^+$. Note that K_∞ is the cyclotomic $\mathbb{Z}_p$-extension of a certain CM-field K, and that $\# X(K_\infty^+) = 1$. By Kida's formula [9], we know that $\mu(X(K_\infty)) = 0$ and $\lambda(X(K_\infty)) = 1$. Since $G(K_\infty) \simeq X(K_\infty) \simeq \mathbb{Z}_p$, we can see that $\widetilde{L}(k_\infty) = \widetilde{L}(K_\infty) = L(k_\infty)$. Therefore, $G(k_\infty) \simeq X(k_\infty) \simeq \mathbb{Z}_p \oplus \mathbb{Z}/p^m\mathbb{Z}$. $\square$

By using the result of Yamamoto [25], Kida's formula [9] and Proposition 3.1, we can easily find infinitely many abelian sextic fields k containing $\mathbb{Q}(\sqrt{-3})$ such that $G(k_\infty) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}/3\mathbb{Z}$ in $p = 3$ case.

For odd p and $k = \mathbb{Q}(\zeta_p)$, it is announced by Sharifi [20] that $G(k_\infty)$ is abelian if $p < 1000$ (and there exists $p > 1000$ such that $G(k_\infty)$ is nonabelian!). Especially, $G(k_\infty) \simeq \mathbb{Z}_p^{\oplus 2}$ for $p = 157$, and $G(k_\infty) \simeq \mathbb{Z}_p^{\oplus 3}$ for $p = 461$. Further, for odd p, Okano [16] characterized an imaginary quadratic field k with noncyclic abelian $G(k_\infty)$ as follows:

Theorem 3.2 (Okano [16]). *For odd p and an imaginary quadratic field k, $G(k_\infty)$ is noncyclic abelian if and only if $\lambda = 2$ and $A(k)$ is generated by the ideal classes containing some power of a prime ideal above p. Then, $G(k_\infty) \simeq \mathbb{Z}_p^{\oplus 2}$.*

For odd p and imaginary quadratic fields k, the abelianity of $G(k_\infty)$ and the powerfulness of $G(k_\infty)$ are equivalent (cf. [24] Proposition 2.1). Also in $p = 2$ case, all imaginary quadratic fields k with abelian $G(k_\infty)$ are characterized by Ozaki and author [13]. Especially, the following case is related with the Iwasawa polynomial $P(T)$.

Theorem 3.3 ([13]). *For $p = 2$ and an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-q})$ with a prime number $q \equiv 15 \pmod{32}$, $G(k_\infty)$ is abelian if and only if $P(-1) \equiv 1 \pmod 4$. Then, $G(k_\infty) \simeq \mathbb{Z}_2^{\oplus 3}$.*

On the other hand, as a corollary of the results of Gen Yamamoto ($p = 2$ version of [25]), we can find infinitely many real quadratic fields k with $G(k_\infty) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (cf. e.g., [11]).

3.2. Metabelian examples in $p = 2$ case. Throughout this subsection, we put $p = 2$ and denote commutators by $[x, y] = x^{-1}y^{-1}xy$. For an imaginary quadratic field k with $\lambda = 1$, we can obtain an explicit presentation of $G(k_\infty)$ which is not necessarily abelian.

Theorem 3.4 ([12]). *Let $p = 2$ and $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with positive squarefree integer $m \equiv 1 \pmod 4$, and put a real quadratic field $K^+ = \mathbb{Q}(\sqrt{m})$. If $\lambda = 1$ for k_∞, then*

$$G(k_\infty) = \left\langle\, a,\, b \;\middle|\; [a, b] = a^{-2},\ a^{2^{N+1}} = 1 \,\right\rangle^{\text{pro-}2}$$

where 2^N is the order of $G(K_\infty^+)$ which is finite cyclic.

Corollary 3.5. *$X^{(i)}(k_\infty) \simeq \mathbb{Z}/2\mathbb{Z}$ for $2 \leq i \leq N+1$, and $\#X^{(i)}(k_\infty) = 1$ for $N+2 \leq i$. Especially, $\widetilde{\lambda}^{(i)} = 1$, $\lambda^{(i)} = 0$ for all $i \geq 2$ and $\sup\{n_0^{(i)}\} < \infty$.*

In Theorem 3.4, the metacyclic $G(k_\infty)$ is nonabelian if and only if $N \geq 1$, and such cases exist. For example, $N = 1$ if $m = 13 \cdot 29$.

Further, we have the following as an example of nonmetacyclic metabelian $G(k_\infty)$.

Theorem 3.6 ([12]). *Let $p = 2$ and $k = \mathbb{Q}(\sqrt{-q_1q_2})$ an imaginary quadratic field with prime numbers $q_1 \equiv 3 \pmod 8$, $q_2 \equiv 7 \pmod{16}$. Then, we have a presentation*

$$G(k_\infty) = \left\langle a,\, b,\, c \;\middle|\; [a,b] = a^{-2},\ [b,c] = a^2,\ [a,c] = 1 \right\rangle^{\text{pro-}2}$$

such that ${}^{\gamma}a = a$, ${}^{\gamma}b = bc$, ${}^{\gamma}c = a^{C_1}b^{-C_0}c^{1-C_1}$, where C_1, $C_0 \in \mathbb{Z}_2$ are the coefficients of the Iwasawa polynomial $P(T) = T^2 + C_1T + C_0$.

Corollary 3.7. *$X^{(i)}(k_\infty) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $i \geq 2$. Especially, $\widetilde{\lambda}^{(i)} = 2$, $\lambda^{(i)} = 0$ for all $i \geq 2$ and $\sup\{n_0^{(i)}\} = \infty$.*

The Galois group $G(k_\infty)$ in Theorem 3.6 is 2-adic analytic, especially a Poincaré pro-2 group of dimension 3. According to Proposition 2.5 and Fontaine-Mazur conjecture, the Galois groups $G(k_n)$ of 2-class field towers should be finite. In fact, $G(k_n)$ are finite since $G(k_\infty)$ is metabelian. Further, by using the explicit action of γ on $G(k_\infty)$, we can calculate the presentations of $G(k_n)$ for $n \geq 1$ under some assumptions as follows. (It is well known that $G(k)$ is abelian.)

Corollary 3.8 ([12]). *If $(q_1/q_2) = -1$, i.e., q_1 is not quadratic residue modulo q_2, then*

$$G(k_1) = \left\langle a,\, b,\, c \;\middle|\; [a,b] = a^{-2},\ [b,c] = a^2 = b^2 = c^2,\ [a,c] = a^4 = 1 \right\rangle.$$

Further, if $(q_1/q_2) = -1$ and $C_1 \equiv 0 \pmod 4$,

$$G(k_n) = \left\langle a,\, b,\, c \;\middle|\; [a,b] = a^{-2},\ [b,c] = a^2,\ [a,c] = a^{2^{n+1}} = b^{2^{n+1}} = c^{2^n} = 1 \right\rangle$$

for all $n \geq 2$.

For all pairs (q_1, q_2) with $q_1q_2 < 5000$, one can see that $P(T) \equiv T^2 + (1 + (q_1/q_2))T + (1 - (q_1/q_2)) \pmod 4$ by the numerical computation of Stickelberger elements. Then, one can expect that always $C_1 \equiv 0 \pmod 4$ if $(q_1/q_2) = -1$, but it is not clear yet.

Under the stronger assumptions that $(q_1/q_2) = -1$ and $C_1 \equiv 0 \pmod 4$, there is another proof of the metabelianity of $G(k_\infty)$ of Theorem 3.6. It is parallel to the proof (of if-part) of Theorem 3.3, which is based on the calculation of "$\mathrm{Gal}(L(k_n)/\mathbb{Q})$" and the decomposition subgroups of some primes. By putting $K = k(\sqrt{-1}, \sqrt{-q_1})$ and

$F = \mathbb{Q}(\sqrt{-1}, \sqrt{-q_1})$, one can see that $\mathrm{Gal}(L(K_n)/F)$ has a presentation which is very similar to the presentation of "$\mathrm{Gal}(L(k_n)/\mathbb{Q})$" in the proof of Theorem 3.3.

Finally, concerning Greenberg's conjecture, we remark that there are infinitely many real quadratic fields k with finite dihedral $G(k_\infty)$ in $p = 2$ case (cf. [11]).

References

[1] Boston, N., Galois p-groups unramified at p – A survey, *Contemp. Math.*, **416**, Primes and Knots, Amer. Math. Soc., Providence, RI, 2006., pp. 31–40

[2] Dixon, J. D., du Sautoy, M. P. F., Mann, A. and Segal, D., Analytic pro-p groups, Second edition, *Cambridge Studies in Advanced Mathematics* **61**, Cambridge University Press, Cambridge, 1999.

[3] Ferrero, B. and Washington, L. C., The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.*, **109** (1979), no. 2, 377–395.

[4] Fontaine, J. M. and Mazur, B., Geometric Galois representations, *Elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[5] Fujii, S., On a higher class number formula of $\mathbb{Z}_p$-extensions, *Tokyo J. Math.*, **28** (2005), no. 1, 55–61.

[6] Fujii, S. and Okano, K., Some problems on p-class field towers, *Tokyo J. Math.*, **30** (2007), no. 1, 211–222.

[7] Golod, E. S. and Shafarevich, I. R., On the class field tower, *Izv. Akad. Nauk SSSR Ser. Mat.*, **28** (1964), 261–272.

[8] Greenberg, R., On the Iwasawa invariants of totally real number fields, *Amer. J. Math.*, **98** (1976), no. 1, 263–284.

[9] Kida, Y., l-extensions of CM-fields and cyclotomic invariants, *J. Number Theory*, **12** (1980), no. 4, 519–528.

[10] Mazur, B. and Wiles, A., Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.*, **76** (1984), no. 2, 179–330.

[11] Mizusawa, Y., On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields II, *Acta Arith.*, **119** (2005), no. 1, 93–107.

[12] Mizusawa, Y., On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field, *preprint.*

[13] Mizusawa, Y. and Ozaki, M., Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, *preprint.*

[14] Morishita, M., Analogies between prime numbers and knots, (Japanese) *Sūgaku*, **58** (2006), no. 1, 40–63, (English) to appear in Sugaku Expositions, AMS.

[15] Neukirch, J., Schmidt, A. and Winberg, K., Cohomology of Number Fields, *Grundlehren der Mathematischen Wissenschaften*, **323**, Springer-Verlag, Berlin, 2000.

[16] Okano, K., Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields, *Acta Arith.*, **125** (2006), no. 4, 363–381.

[17] Ozaki, M., Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions, (Japanese) *Young philosophers in number theory* (Kyoto, 2001), RIMS Kôkyûroku, **1256** (2002), 25–37.

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

[19] Sharifi, R. T., Massey products and ideal class groups, *J. Reine Angew. Math.*, **603** (2007), 1–33.

[20] Sharifi, R. T., Galois groups of unramified pro-p extensions, *Pro-p Extensions of Global Fields and pro-p Groups*, Oberwolfach Reports, vol. **3** (2006), issue 2, 1473–1475.

[21] Washington, L. C., Introduction to Cyclotomic Fields, second edition, *Graduate Texts in Math.*, vol. **83**, Springer, 1997.

[22] Wiles, A., The Iwasawa conjecture for totally real fields, *Ann. of Math. (2)*, **131** (1990), no. 3, 493–540.

[23] Wingberg, K., On the maximal unramified p-extension of an algebraic number field, *J. Reine Angew. Math.*, **440** (1993), 129–156.

[24] Wingberg, K., On the Fontaine-Mazur conjecture for CM-fields, *Compositio Math.*, **131** (2002), no. 3, 341–354.

[25] Yamamoto, G., On the vanishing of Iwasawa invariants of absolutely abelian p-extensions, *Acta Arith.*, **94** (2000), no. 4, 365–371.