JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Yasushi MIZUSAWA

On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field

Tome 22, n° 1 (2010), p. 115-138.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_115_0>

Journal de Théorie des Nombres
de Bordeaux **22** (2010), 115-138

On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field

par Yasushi MIZUSAWA

Résumé. Pour k quadratique imaginaire, nous étudions le groupe de Galois $G(k_\infty)$ de la pro-2-extension non ramifiée maximale au-dessus de la $\mathbb{Z}_2$-extension cyclotomique k_∞ de k. Nous déterminons des familles de tels corps imaginaires k pour lesquels $G(k_\infty)$ est un pro-2-groupe métabélien et en donnons une présentation explicite ; nous précisons de même des familles pour lesquelles $G(k_\infty)$ est un pro-2-groupe métacyclique non abélien. Nous calculons enfin en termes de Théorie d'Iwasawa les groupes de Galois de 2-tours de corps de classes de certaines 2-extensions cyclotomiques.

Abstract. For the cyclotomic $\mathbb{Z}_2$-extension k_∞ of an imaginary quadratic field k, we consider the Galois group $G(k_\infty)$ of the maximal unramified pro-2-extension over k_∞. In this paper, we give some families of k for which $G(k_\infty)$ is a metabelian pro-2-group with the explicit presentation, and determine the case that $G(k_\infty)$ becomes a nonabelian metacyclic pro-2-group. We also calculate Iwasawa theoretically the Galois groups of 2-class field towers of certain cyclotomic 2-extensions.

1. Introduction

Let p be a fixed prime number. For an algebraic number field k, we denote by $G(k)$ the Galois group of the maximal unramified pro-p-extension $L^\infty(k)$ over k. The sequence of the fixed fields corresponding to the commutator series of $G(k)$ is a classic object called p-class field tower when k is a finite extension of the field $\mathbb{Q}$ of rational numbers. In this case, the group $G(k)$ can be infinite by the criteria originated from Golod-Shafarevich [13], while various finite p-groups also appear as $G(k)$, especially when $p = 2$ and k is an imaginary quadratic field ([3] [4] [6] etc.).

The main object of this paper is the Galois group $G(k_\infty)$ for the cyclotomic $\mathbb{Z}_p$-extension k_∞ of a finite extension k of $\mathbb{Q}$, where $\mathbb{Z}_p$ denotes (the additive group of) the ring of p-adic integers. From the nonabelian Iwasawa theoretical view seen in Ozaki [30], Sharifi [33], Wingberg [36] and [10] [11]

Manuscrit reçu le 21 février 2008.

[12] etc., it is expected that the Galois group $G(k_\infty)$ would give good information on the structure of $G(k_\bullet)$ (e.g., either finite or not) for finite extensions $k_\bullet$ of k contained in k_∞. However, it is still rather difficult to obtain the explicit presentation of nonabelian $G(k_\infty)$ in general, while the imaginary quadratic fields k with abelian $G(k_\infty)$ are classified (cf. [27] [28]).

Here, we note that $G(k_\infty)$ is allowed to have infinite p-adic analytic quotient while it is conjectured that $G(k)$ has no such quotient for finite extensions k of $\mathbb{Q}$ as a part of Fontaine-Mazur conjecture (cf. [5] [36] etc.). Then a question arises: *When does the Galois group $G(k_\infty)$ itself become a p-adic analytic pro-p-group, and what kind of such groups appear?* In this paper, we treat the case that $p = 2$, and give some families of imaginary quadratic fields k for which $G(k_\infty)$ becomes a metabelian 2-adic analytic pro-2-group with the explicit presentation.

Let us recall some knowledge on the Galois groups $G(k)$ and $G(k_\infty)$, and define some notations. For a finite extension k of $\mathbb{Q}$, it is well known that $G(k)$ is a finitely presented pro-p-group satisfying the property called FAb that any subgroup of finite index has finite abelianization (cf. [5] etc.). The abelianization of $G(k)$, which is regarded as the Galois group of the maximal unramified abelian p-extension $L(k)$ (called Hilbert p-class field) over k, is isomorphic to the p-Sylow subgroup $A(k)$ of the ideal class group of k via Artin map.

For the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k, the abelianization of $G(k_\infty)$ is also identified with the Galois group $X(k_\infty)$ of the maximal unramified abelian pro-p-extension $L(k_\infty)$ over k_∞, which we call Iwasawa module of k_∞. The Iwasawa module $X(k_\infty)$ is isomorphic via Artin map to the projective limit $\varprojlim A(k_\bullet)$ with respect to the norm mappings. It is conjectured that $G(k_\infty)$ is finitely generated as a pro-p-group, and it is true when k is an abelian extension of $\mathbb{Q}$ by the theorem of Ferrero-Washington [9]. Further, as a consequence of Greenberg's conjecture [14], it is conjectured that $G(k_\infty)$ is a FAb pro-p-group if k is a totally real number field (cf., e.g., [26]).

Notations. Throughout the following sections, always $p = 2$, and the above notations are used. For each integer $n \geq 0$, we define algebraic integers $\pi_{n+1} = 2 + \sqrt{\pi_n}$ with $\pi_0 = 2$, inductively. For any finite extension k of $\mathbb{Q}$, we write $k_n = k(\pi_n)$. The cyclotomic $\mathbb{Z}_2$-extension k_∞ of k is obtained by adding all π_n to the field k. Let $D(k)$ be the subgroup of $A(k)$ generated by ideal classes represented by some odd power of prime ideals of k lying above 2, and $E(k)$ the unit group of the ring of algebraic integers in k.

For closed subgroups G, H of a pro-2-group, we denote by $[G, H]$ the closed subgroup generated by the commutators $[g, h] = g^{-1}h^{-1}gh$ of $g \in G$ and $h \in H$, and G^2 denotes the closed subgroup generated by square elements g^2 of $g \in G$. The lower central series of G is defined by $G_1 = G$ and $G_i = [G_{i-1}, G]$ for $i \geq 2$ inductively, and the order of G is denoted by

$|G|$. For a G-module A, we denote by A^G the submodule generated by all G-invariant elements.

2. Main results

Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a positive square-free integer m, and Γ the Galois group of the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k. Note that $\pi_n = 2 + 2\cos(2\pi/2^{n+2})$ generates the principal prime ideal (π_n) of $\mathbb{Q}_n = \mathbb{Q}(\pi_n)$ above 2. Then the field $k_n = k(\cos(2\pi/2^{n+2}))$ is a cyclic extension of degree 2^n over k, which is contained in k_∞. Since $k_1 = k(\sqrt{2})$, we may assume that m is *odd* in our purpose.

Let γ be the topological generator of Γ which sends $\cos(2\pi/2^{n+2})$ to $\cos(5\cdot 2\pi/2^{n+2})$ for all $n \geq 0$, and take an extension $\widetilde{\gamma} \in \mathrm{Gal}(L^\infty(k_\infty)/L(k))$ of γ, which is a generator of the inertia subgroup of some place above 2 in $\mathrm{Gal}(L^\infty(k_\infty)/k)$. By using this, we define the action of Γ on $G(k_\infty) = \mathrm{Gal}(L^\infty(k_\infty)/k_\infty)$ by the left conjugation ${}^\gamma g = \widetilde{\gamma} g \widetilde{\gamma}^{-1}$ for $g \in G(k_\infty)$. Then the Galois group $G(k_\infty)$ becomes a pro-2-Γ operator group. The action of Γ on the Iwasawa module $X(k_\infty)$ is induced from this action.

The complete group ring $\mathbb{Z}_2[[\Gamma]]$ can be identified with the ring $\Lambda = \mathbb{Z}_2[[T]]$ of formal power series via $\gamma \leftrightarrow 1 + T$. Then the Iwasawa module $X(k_\infty)$ becomes a finitely generated torsion Λ-module isomorphic to $\varprojlim A(k_n)$ as Λ-modules. The characteristic polynomial

$$P(T) = \det\big(\,(1+t)id - \gamma \,\big|\, X(k_\infty) \otimes_{\mathbb{Z}_2} \overline{\mathbb{Q}}_2\,\big)\big|_{t=T}$$

which we call Iwasawa polynomial associated to $X(k_\infty)$, is defined as a distinguished polynomial in Λ, where $\overline{\mathbb{Q}}_2$ is the algebraic closure of the field of 2-adic numbers. The degree $\lambda(k_\infty/k)$ of $P(T)$, which is the $\mathbb{Z}_2$-rank of $X(k_\infty)$, coincides with the λ-invariant which appears in Iwasawa's formula for $|A(k_n)|$. In the present case, the structure of $X(k_\infty)$ as a $\mathbb{Z}_2$-module, including $\lambda(k_\infty/k)$, can be completely calculated from m by the results of Ferrero [8] and Kida [19].

Studying the Galois group $G(k_\infty)$ with the action of Γ is equivalent to consider the special quotient $\mathrm{Gal}(L^\infty(k_\infty)/k)$ of the Galois group $G_S(k)$ of the maximal pro-2-extension of k unramified outside 2. The Galois group $G_S(k)$ has been well studied, while the quotient $\mathrm{Gal}(L^\infty(k_\infty)/k)$ and the subquotient $G(k_\infty)$ are still rather uncertain. The main results of this paper, which determine the structure of $G(k_\infty)$ in some special cases, are the following two theorems.

The first one treats the case that $G(k_\infty)$ becomes a metacyclic pro-2-group.

Theorem 2.1. *Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-m})$ with a positive squarefree odd integer m. If $m \equiv 1 \pmod 4$ and the Iwasawa λ-invariant $\lambda(k_\infty/k) = 1$, the Galois group $G(k_\infty)$ of the maximal unramified pro-2-extension of k_∞ has a presentation*

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

as a pro-2-group, where $X(\mathbb{Q}_\infty(\sqrt{m}))$ is the Iwasawa module of the cyclotomic $\mathbb{Z}_2$-extension of the real quadratic field $\mathbb{Q}(\sqrt{m})$, which is a finite cyclic 2-group.

Remark. The Galois group $G(k_\infty)$ of Theorem 2.1 has an infinite open normal cyclic subgroup which is generated by b^2. Then $G(k_\infty)$ is a 2-adic analytic pro-2-group of dimension 1 (cf. [7] Corollary 8.34 etc.). The finiteness of $X(\mathbb{Q}_\infty(\sqrt{m}))$ is known as a result of Ozaki-Taya [31], and the presentation of $G(k)$ is described by Lemmermeyer [23]. Further, the generators a and b can be chosen such that ${}^{\gamma}a = a$ and ${}^{\gamma}b = a^{2^{\bullet}} b^{1-P(0)}$, where $2^{\bullet}$ is an uncertain power of 2 which can be determined in a certain special case. In §3, we will prove Theorem 2.1, and determine all m for which $G(k_\infty)$ is nonabelian metacyclic.

The second result gives the case that $G(k_\infty)$ becomes a certain nonmetacyclic metabelian pro-2-group.

Theorem 2.2. *Let $k = \mathbb{Q}(\sqrt{-q_1 q_2})$ be an imaginary quadratic field with prime numbers $q_1 \equiv 3 \pmod 8$ and $q_2 \equiv 7 \pmod{16}$, and k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of k with the Galois group Γ. Then the Galois group $G(k_\infty)$ of the maximal unramified pro-2-extension of k_∞ has a presentation*

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

with the action of the topological generator γ of Γ (defined above):

$${}^{\gamma}a = a\,, \quad {}^{\gamma}b = bc\,, \quad {}^{\gamma}c = a^{C_1} b^{-C_0} c^{1-C_1}\,,$$

where the 2-adic integers C_1 and C_0 are the coefficients of the Iwasawa polynomial

$$P(T) = T^2 + C_1 T + C_0$$

associated to the Iwasawa module of k_∞.

Remark. The Galois group $G(k_\infty)$ of Theorem 2.2 has an abelian maximal subgroup generated by a, b^2, c, which is a free $\mathbb{Z}_2$-module of rank 3. Then $G(k_\infty)$ is a 2-adic analytic pro-2-group of dimension 3 (cf. [7] Corollary 8.34 etc.). Especially, $G(k_\infty)$ is a Poincaré pro-2-group which has cohomological dimension $cd_2(G(k_\infty)) = 3$ and Euler characteristic $\chi(G(k_\infty)) = 0$ (cf. [22] [32]). It is known that $G(k)$ is an abelian 2-group of type $(2, 2^{\bullet})$ by [23]. We will prove Theorem 2.2 in §4, and consider the Galois groups $G(k_n)$ of the 2-class field towers of k_n.

By Iwasawa Main Conjecture (Theorem of Mazur-Wiles [25], Wiles [35]) and Iwasawa's construction of p-adic L-functions (cf., e.g., [34] § 7.2), there exists a power series $\Phi(T) \in \Lambda$ constructed from Stickelberger elements, such that $\Phi(T)$ and $P(T)$ generate the same principal ideal of Λ and $L_2(s,\psi) = 2\,\Phi(5^s - 1)$ is the 2-adic L-function for the even Dirichlet character ψ associated to the real quadratic field $\mathbb{Q}(\sqrt{m})$ ($m = q_1q_2$ in Theorem 2.2). Then the coefficients of Iwasawa polynomial $P(T)$ are approximately computable in our cases. For the method of computation, we refer to [16] etc.

3. On metacyclic cases

3.1. Preliminaries. Let $k = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field with a positive squarefree *odd* integer m. By Theorem 1 of [19], the $\mathbb{Z}_2$-torsion submodule $\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty)$ of the Iwasawa module $X(k_\infty)$ is nontrivial if and only if $1 \neq m \equiv 1 \pmod 4$. In this case, Theorem 5 of [8] says that

$$\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty) \simeq \varprojlim D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$$

via Artin map, and $\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty)$ coincides with the decomposition subgroup of any place above 2 in $X(k_\infty)$. The $\mathbb{Z}_2$-rank $\lambda(k_\infty/k)$ can be also calculated by [8] and [19] from the prime factors of m.

Especially, the following three conditions • are equivalent:

- $m \equiv 1 \pmod 4$ and $\lambda(k_\infty/k) = 1$.
- $X(k_\infty) \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}_2$ as $\mathbb{Z}_2$-modules.
- m satisfies one of the following:
    - $m = \ell$ with a prime number $\ell \equiv 9 \pmod{16}$
    - $m = p_1p_2$ with two distinct prime numbers; $p_1 \equiv p_2 \equiv 5 \pmod 8$
    - $m = q_1q_2$ with two distinct prime numbers; $q_1 \equiv q_2 \equiv 3 \pmod 8$

If one of them is satisfied, $A(k_n)$ is an abelian group of type $(2, 2^\bullet)$ for each sufficiently large n, and Theorem 2.1 says that $G(k_n)$ is a metacyclic 2-group. On the other hand, various types of pro-2-groups appear as $G(k)$ for imaginary quadratic fields k with $A(k) \simeq (2, 2^\bullet)$ (e.g., infinite [15], metabelian [1] [3] [23], of derived length 3 [6], etc.).

In order to prove Theorem 2.1, we need the following which is essentially the same as Proposition 7 of [2].

Lemma 3.1. *Let G a pro-2-group of rank 2, and H a maximal subgroup of G. Then G is abelian if and only if $G_2 = H_2$.*

Proof. We can choose the generators a, b of G such that H is generated by a, b^2 and G_2. Since

$$[a, b^2] = [a, b]^2[[a, b], b] \equiv 1 \bmod (G_2)^2G_3\,,$$

$H/(G_2)^2G_3$ is an abelian group. If G is not abelian, G_2/G_3 is a nontrivial cyclic 2-group generated by $[a,b]G_3$, especially, $G_2/(G_2)^2G_3$ has order 2. Then $G_2 \neq (G_2)^2G_3 \supset H_2$. Since the "only if" part is obvious, this completes the proof. □

3.2. Proof of Theorem 2.1. By the assumption, the shape of m is one of the above "∘". In each case, the field $K = k(\sqrt{-1})$ is an unramified quadratic extension of k in which the prime ideal of k above 2 splits. The maximal real subfield of the CM-field K is the real quadratic field $K^+ = \mathbb{Q}(\sqrt{m})$. Note that K_∞ is also unramified quadratic extension of k_∞.

Let $G = \mathrm{Gal}(L^2(k_\infty)/k_\infty)$ be the Galois group of the maximal unramified metabelian pro-2-extension $L^2(k_\infty)$ over k_∞, and $H = \mathrm{Gal}(L^2(k_\infty)/K_\infty)$ be the maximal subgroup of G associated to K_∞. The pro-2-group G is generated by two elements a, b such that $a^2 \in G_2$. Let N be the normal closed subgroup of G generated by a and G_2 with the fixed field $L'(k_\infty)$. Then $G/N \simeq \mathbb{Z}_2$ is generated by bN, and $N/G_2 \simeq \varprojlim D(k_n)$. Since any place of k_∞ above 2 splits in K_∞, i.e. $K_\infty \subset L'(k_\infty)$, the maximal subgroup H/G_2 of $X(k_\infty)$ contains N/G_2. Then H is generated by a, b^2 and G_2.

Lemma 3.2. *H is a pro-2-group of rank 2.*

Proof. Let $\Delta = \mathrm{Gal}(K_\infty/\mathbb{Q}_\infty(\sqrt{-1}))$, and put

$$\mathfrak{E}_n = E(\mathbb{Q}_n(\sqrt{-1}))/(E(\mathbb{Q}_n(\sqrt{-1})) \cap N_\Delta K_n^\times)$$

for each $n \geq 0$, where N_Δ is the norm mapping from K_n to $\mathbb{Q}_n(\sqrt{-1})$. Note that the number of prime ideals of $\mathbb{Q}_n(\sqrt{-1})$ which divide m is at most 4, and that K_n is a quadratic extension of $\mathbb{Q}_n(\sqrt{-1})$ unramified outside m. Since $A(\mathbb{Q}_n(\sqrt{-1}))$ is trivial, and the norm mappings $\mathfrak{E}_n \to \mathfrak{E}_1$ for each $n \geq 1$ and $\mathfrak{E}_1 \to \mathfrak{E}_0$ are surjective, the genus formula (e.g. [8] Lemma 1) for K_n over $\mathbb{Q}_n(\sqrt{-1})$ implies that

$$|A(K_n)/2A(K_n)| = |A(K_n)^\Delta| \leq \frac{2^3}{|\mathfrak{E}_n|} \leq \frac{2^3}{|\mathfrak{E}_1|} \leq \frac{2^3}{|\mathfrak{E}_0|}.$$

Assume that $m = \ell$, and $|\mathfrak{E}_1| = 1$. Then there exist some x, $y \in \mathbb{Q}_1(\sqrt{-1})^\times$ such that $\sqrt[4]{-1} = x^2 - y^2\ell$. Since ℓ splits in $\mathbb{Q}_1(\sqrt{-1})$ completely, we may regard x and y as ℓ-adic numbers. By considering the ℓ-adic values, we know that $x \in \mathbb{Z}_\ell^\times$ and $y \in \mathbb{Z}_\ell$. This implies that $-1 \equiv x^8 \pmod{\ell}$, i.e. $\ell \equiv 1 \pmod{16}$, which is a contradiction. Therefore $|\mathfrak{E}_1| \geq 2$ if $m = \ell$.

In the case that $m = p_1p_2$, if we assume that $|\mathfrak{E}_0| = 1$, then $\sqrt{-1} \equiv x^2 \pmod{p_1}$ with some p_1-adic unit $x \in \mathbb{Q}(\sqrt{-1})^\times$, i.e. $p_1 \equiv 1 \pmod{8}$, similarly. This contradiction implies that $|\mathfrak{E}_0| \geq 2$ if $m = p_1p_2$.

Assume that $|\mathfrak{E}_1| = 1$ in the remained case that $m = q_1q_2$, then $1+\sqrt{2} \in N_\Delta K_1^\times$. By taking the norm from $K_1^\times$ to $\mathbb{Q}(\sqrt{-2}, \sqrt{q_1q_2})^\times$, we obtain some x, $y \in \mathbb{Q}(\sqrt{-2})^\times$ satisfying $-1 = x^2 - y^2q_1q_2$. Since q_1 splits in $\mathbb{Q}(\sqrt{-2})$, those can be regarded as $x \in \mathbb{Z}_{q_1}^\times$ and $y \in \mathbb{Z}_{q_1}$, then $-1 \equiv x^2 \pmod{q_1}$. This implies a contradiction $q_1 \equiv 1 \pmod 4$. Therefore $|\mathfrak{E}_1| \geq 2$ when $m = q_1 q_2$.

By the above, it is known that $A(K_n)$ has rank at most 2 for all n in any cases. Since $H/H_2 \simeq \varprojlim A(K_n)$ and $H/G_2 \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}_2$, the rank of H/H_2 must be 2, i.e. H is a pro-2-group of rank 2. $\square$

Note that the bracket operation $[\ ,\ ] : G_i/G_{i+1} \times G/G_2 \to G_{i+1}/G_{i+2}$ is a bilinear surjective morphism over $\mathbb{Z}_2$. Since G_2/G_3 is generated by $[a,b]G_3$, and

$$[a,b^2] = [a,b]^2[[a,b],b] \equiv [a,b]^2 \equiv [a,b]^2[[a,b],a] = [a^2,b] \equiv 1 \bmod G_3\,,$$

H/G_3 is an abelian group generated by aG_3, b^2G_3 and $[a,b]G_3$. By Lemma 3.2, the torsion subgroup of H/G_3 which is generated by aG_3 and $[a,b]G_3$ must be cyclic, so that

$$a^2 \equiv [a,b] \bmod G_3\,.$$

Then

$$\begin{aligned}&[[a,b],a] \equiv [a^2,a] = 1 \bmod G_4\,,\\ &[[a,b],b] \equiv [a^2,b] = [a,b]^2[[a,b],a] \equiv [a,b]^2 \bmod G_4\,.\end{aligned}$$

This implies that $G_3 \subset G_4(G_2)^2$.

Let $\overline{G} = G/(G_2)^2$, which is also a finitely generated pro-2-group. Then the lower central series $\overline{G}_i = G_i(G_2)^2/(G_2)^2$ makes a fundamental system of closed neighborhoods of $1 \in \overline{G}$. Since $\overline{G}_3 = \overline{G}_4$, it becomes that $\overline{G}_3 = \{1\}$, i.e. $G_3 \subset (G_2)^2$. By the induced surjective morphism $G_2/G_3 \to G_2/(G_2)^2$, we know that the abelian group G_2 is a cyclic pro-2-group generated by $[a,b]$.

Further, we know that $G_3 = (G_2)^2$ and $a^2 = [a,b]^u$ with some $u \in \mathbb{Z}_2^\times$, so that G_2 is a cyclic pro-2-group generated by a^2. Since N/G_2 is generated by aG_2 and is the decomposition subgroup of G/G_2 for any place lying above 2, then N becomes a cyclic pro-2-group generated by a which is the decomposition subgroup of G for any place of $L^2(k_\infty)$ lying above 2. From the exact sequence

$$1 \to N \to G \to G/N \to 1$$

which has the cyclic terms N (generated by a) and $G/N \simeq \mathbb{Z}_2$ (generated by bN), we know that $G \simeq N \rtimes (G/N)$ is a metacyclic pro-2-group.

Lemma 3.3. *For each $n \geq 0$, $A(K_n^+) = D(K_n^+)$ is a cyclic 2-group.*

Proof. Note that the number of prime ideals of $\mathbb{Q}_n$ which ramify in K_n^+ is at most 2. By the genus formula for the quadratic extension K_n^+ over $\mathbb{Q}_n$, we know that $A(K_n^+)$ is a cyclic 2-group. If $A(K_n^+)$ is trivial, there is nothing we have to show. Assume that $A(K_n^+)$ is nontrivial.

Let $F^+ = F_n^+$ be the unique unramified quadratic extension of K_n^+, which is a $(2,2)$-extension of $\mathbb{Q}_n$, and put $F = F^+(\sqrt{-1})$. Note that any prime ideal of K_n^+ above 2 is totally ramified in K_∞. The field F_∞ is an unramified $(2,2)$-extension of k_∞, i.e. the fixed field of G^2G_2. Since G^2G_2 does not contain N, any prime ideal of K_∞ above 2 does not split in F_∞. Then any prime ideal of K_n^+ above 2 does not split in F_n^+, i.e. in $L(K_n^+)$. This implies that $A(K_n^+) = D(K_n^+)$. □

The Galois group $\Gamma = \mathrm{Gal}(k_\infty/k)$ can be identified with $\mathrm{Gal}(K_\infty/K)$ and $\mathrm{Gal}(K_\infty^+/K^+)$. By Proposition 1 of [14] and Lemma 3.3, we know that $X(K_\infty^+) \simeq A(K_n^+)$ for all sufficiently large n.

For each $n \geq 0$, the principal prime ideal (π_n) of $\mathbb{Q}_n$ does not ramify in K_n^+, so that the map $\iota_n : A(K_n^+) \to A(K_n)$ induced from the lifting of ideals is injective by Theorem 1 of [24]. Note that $\varprojlim D(K_n) \simeq N/H_2$ via Artin map. Then $D(K_n)$ is a cyclic 2-group for all $n \geq 0$. Since the prime ideals of K_n^+ above 2 ramify in K_n, the image of ι_n is a subgroup of $D(K_n)$ of index 2. By taking the projective limit, the sequence

$$0 \to X(K_\infty^+) \overset{\iota_\infty}{\to} \varprojlim D(K_n) \to \mathbb{Z}/2\mathbb{Z} \to 0$$

is exact, where $\iota_\infty = \varprojlim \iota_n$.

Assume that $X(K_\infty^+)$ is trivial. In this case, since $|N/G_2| = 2$, the natural map $N/H_2 \to N/G_2$ is an isomorphism, i.e. $G_2 = H_2$. By Lemma 3.1, we know that G is abelian. This implies the claim of Theorem 2.1 in the case that $|X(K_\infty^+)| = 1$.

On the other hand, we assume that $X(K_\infty^+)$ is nontrivial. Then there exists a totally real number field F^+ such that F_n^+ is an unramified quadratic extension of K_n^+ for all sufficiently large n. (In fact, $F^+ = F_n^+$ for some n.) By Lemma 3.3, it becomes that $A(F_n^+) = D(F_n^+)$ and $|A(K_n^+)| = 2|A(F_n^+)|$.

For the *CM*-field $F = F^+(\sqrt{-1})$, the field F_∞ is an unramified quadratic extension of K_∞, which is the fixed field of G^2G_2. One can see that $\varprojlim D(F_n) \simeq N^2/(G^2G_2)_2$ via Artin map, then $D(F_n)$ is a cyclic 2-group for all $n \gg 0$. Assume that n is sufficiently large. Since (π_n) is not a square of an ideal in F_n^+ and the prime ideals of F_n^+ above 2 ramify in F_n, the injective morphism $A(F_n^+) \to D(F_n)$ with cokernel of order 2 is induced from the lifting of ideals by Theorem 1 of [24] similarly. By taking the projective limit, we have the exact sequence:

$$0 \to X(F_\infty^+) \to \varprojlim D(F_n) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Here, we note that $|X(K_\infty^+)| = 2|X(F_\infty^+)|$ is finite. By the above,

$$|N/(G^2G_2)_2| = 2|N^2/(G^2G_2)_2| = 4|X(F_\infty^+)| = 2|X(K_\infty^+)| = |N/H_2|.$$

Then the natural isomorphism $N/(G^2G_2)_2 \to N/H_2$ induces that $H_2 = (G^2G_2)_2$. By Lemma 3.1 and 3.2, H is abelian, i.e. $L^2(k_\infty) = L(K_\infty)$.

Whether $|X(K_\infty^+)| = 1$ or not, $N \simeq \varprojlim D(K_n)$ via Artin map and which is a finite cyclic 2-group of order $2|X(K_\infty^+)|$ generated by a. Therefore G has a relation $a^{2|X(K_\infty^+)|} = 1$, and Γ acts on a trivially.

For each $n \geq 0$, choose a prime ideal $\mathfrak{P}_n$ of K_n which is lying above 2. Then the unique prime ideal of k_n lying above 2 splits into $\mathfrak{P}_n$ and $\mathfrak{P}_n^b$ in K_n. On the other hand, a prime ideal of $\mathbb{Q}_n(\sqrt{-1})$ lying above 2 is also unique and principal, and also splits into $\mathfrak{P}_n$ and $\mathfrak{P}_n^b$ in K_n. Therefore $\mathfrak{P}_n\mathfrak{P}_n^b$ is a principal ideal of K_n for all $n \geq 0$. This implies that b acts on $N \simeq \varprojlim D(K_n)$ as inverse, i.e. $b^{-1}ab = a^{-1}$. Then G has another relation $[a, b] = a^{-2}$.

Let F be a free pro-2-group generated by two letters a, b, and R the closed normal subgroup generated by the conjugates of $\mathsf{a}^{2|X(K_\infty^+)|}$, $\mathsf{a}^2[\mathsf{a}, \mathsf{b}]$. By the above, the natural morphism $\mathsf{F} \to G : \mathsf{a} \mapsto a$, $\mathsf{b} \mapsto b$ induces a surjective morphism $\mathsf{F}/\mathsf{R} \to G$. Since the isomorphisms $(\mathsf{F}/\mathsf{R})_2 = \mathsf{F}_2\mathsf{R}/\mathsf{R} \simeq G_2$ and $\mathsf{F}/\mathsf{F}_2\mathsf{R} \simeq G/G_2$ are induced, we know that $\mathsf{F}/\mathsf{R} \simeq G$ which gives a presentation of G.

Since $G_2 \simeq G(k_\infty)_2/(G(k_\infty)_2)_2$ is a cyclic 2-group, the pro-2-group $G(k_\infty)_2$ is also cyclic. Then $L^2(k_\infty) = L^\infty(k_\infty)$, i.e. $G = G(k_\infty)$. This completes the proof of Theorem 2.1.

3.3. Remark on *Γ*-actions. Now, we shall see the action of Γ on $G = G(k_\infty)$. Since $G/N \simeq X(k_\infty)/\mathrm{Tor}_{\mathbb{Z}_2}X(k_\infty) \simeq \Lambda/(P(T))$ and is generated by bN, we have

$$1 \equiv {}^{P(T)}b \equiv {}^{\gamma}b \cdot b^{-1+P(0)} \bmod N\,.$$

Then there exist some $2^\bullet u \in \mathbb{Z}_2$ with $1 \leq 2^\bullet \in 2^{\mathbb{Z}}$ and $u \in \mathbb{Z}_2^\times$ such that ${}^{\gamma}b = (a^u)^{2^\bullet} b^{1-P(0)}$. By replacing a with a^u, we may assume that the generators a, b in the presentation of $G(k_\infty)$ of Theorem 2.1 are given with the Γ-action:

$${}^{\gamma}a = a\,, \quad {}^{\gamma}b = a^{2^\bullet} b^{1-P(0)}\,.$$

Let Γ be identified with the cyclic closed subgroup of $\mathrm{Gal}(L^\infty(k_\infty)/k)$ generated by $\widetilde{\gamma}$. Then $G/[\Gamma, G]G_2 \simeq (G/G_2)/T(G/G_2) \simeq A(k)$ and

$$a^{2^\bullet} \equiv b^{P(0)} \bmod [\Gamma, G]G_2\,.$$

On the other hand, $G/[\Gamma, G]N \simeq (G/N)/T(G/N) \simeq A(k)/D(k) \simeq \mathbb{Z}_2/P(0)\mathbb{Z}_2$ and $[\Gamma, G]N/[\Gamma, G]G_2 \simeq D(k) \simeq \mathbb{Z}/2\mathbb{Z}$. Therefore the above congruence implies that $2^\bullet = 1$ if $A(k)$ is a cyclic 2-group, especially if $m = \ell$. In the other cases, we know that $2^\bullet \equiv 0 \pmod 2$. However, in the case that $m = p_1p_2$, the value $2^\bullet$ seems to depend on the structure of $G(k)$ and $X(K_\infty^+) \simeq \varprojlim A(K_n^+)$ concerning with Theorem 4, 5 and 6 of [23].

3.4. Determination of nonabelian metacyclic cases. As a corollary of Theorem 2.1, all imaginary quadratic fields k with nonabelian metacyclic $G(k_\infty)$ can be determined. Here, we remark that all imaginary quadratic fields k with abelian $G(k_\infty)$ are classified in [27].

Corollary 3.4. *For an imaginary quadratic field* $k=\mathbb{Q}(\sqrt{-m})$ *with a positive squarefree odd integer* m*, the Galois group* $G(k_\infty)$ *becomes nonabelian metacyclic if and only if* m *is one of the following:*

- $\circ$ $m=\ell$ *with a prime number* $\ell\equiv 9 \pmod{16}$ *such that* $2^{(\ell-1)/4}\equiv -1 \pmod{\ell}$
- $\circ$ $m=p_1p_2$ *with distinct two prime numbers;* $p_1\equiv p_2\equiv 5 \pmod 8$

Proof. Assume that $G=G(k_\infty)$ is nonabelian metacyclic. In particular, G/G_2 is not cyclic. Then there exists some cyclic closed normal subgroup N of G such that G/N is also a cyclic pro-2-group. Since $\{1\}\neq G_2\subsetneq N$, N/G_2 is a nontrivial finite cyclic 2-group. By the exact sequence

$$1\to N/G_2\to G/G_2\to G/N\to 1,$$

the rank of $X(k_\infty)\simeq G/G_2$ must be 2, and $X(k_\infty)$ has $\mathbb{Z}_2$-rank $\lambda(k_\infty/k)\le 1$ with nontrivial $\mathrm{Tor}_{\mathbb{Z}_2}X(k_\infty)$. Therefore, as seen in §3.1, $X(k_\infty)\simeq(\mathbb{Z}/2\mathbb{Z})\oplus\mathbb{Z}_2$, i.e. m is one of “$\circ$” in §3.1. Further, m satisfies that $|X(\mathbb{Q}_\infty(\sqrt{m}))|\neq 1$ by the present assumption and Theorem 2.1. By Theorem (1) (2) of [31], $|X(\mathbb{Q}_\infty(\sqrt{m}))|=1$ for the cases that $m=\ell$ with $2^{(\ell-1)/4}\not\equiv -1 \pmod{\ell}$ or $m=q_1q_2$. This completes the “only if” part.

Assume that $m=\ell$ with $2^{(\ell-1)/4}\equiv -1 \pmod{\ell}$ or $m=p_1p_2$, conversely. Note that $\mathbb{Q}_1(\sqrt{\ell})$ is an unramified quadratic extension of $\mathbb{Q}(\sqrt{2\ell})$. Then $|A(\mathbb{Q}_1(\sqrt{\ell}))|=2$ by the known facts that $|A(\mathbb{Q}(\sqrt{2\ell}))|=4$ (cf., e.g. [37] Theorem 3.4 (c)). Since there is a surjective morphism $X(\mathbb{Q}_\infty(\sqrt{\ell}))\to A(\mathbb{Q}_1(\sqrt{\ell}))$, the left hand side is also nontrivial. On the other hand, $X(\mathbb{Q}_\infty(\sqrt{p_1p_2}))$ is finite but nontrivial by Theorem (5) of [31]. As a result, $|X(\mathbb{Q}_\infty(\sqrt{m}))|\neq 1$ for each m above. Therefore G becomes nonabelian metacyclic by Theorem 2.1. □

4. On nonmetacyclic metabelian case

4.1. Preliminaries. For a *CM*-field k with the maximal real subfield k^+, we denote by $Q(k)=|E(k)/W(k)E(k^+)|\le 2$ Hasse's unit index, where $W(k)$ is the group of the roots of unity contained in k. Let $\delta(k)=1$ if $\sqrt{-1}\in k$, and 0 otherwise.

For the cyclotomic $\mathbb{Z}_2$-extension k_∞ of a *CM*-field k, we denote by $\Pi(k_\infty)$ the number of places of k_∞ above 2 which ramify over k_∞^+. For each sufficiently large n, there exists a *CM*-field $k_n^\vee$ such that $(k_n^\vee)^+=k_n^+$ and $k_n\neq k_n^\vee\subset k_{n+1}$. If $k_n=k_n^+(\sqrt{\alpha})$ with some $\alpha\in k_n^+$, the field $k_n^\vee=k_n^+(\sqrt{\alpha\pi_n})$.

According to the method of Ferrero [8], we obtain the following criterion for the freeness of the Iwasawa module $X(k_\infty)$ as a $\mathbb{Z}_2$-module.

Proposition 4.1. *For a CM-field k with the maximal real subfield k^+, the Iwasawa module $X(k_\infty)$ of the cyclotomic $\mathbb{Z}_2$-extension k_∞ is a free $\mathbb{Z}_2$-module if $X(k_\infty^+)$ is trivial and*

$$Q(k_n^\vee) \leq 1 + \delta(k) - \Pi(k_\infty)$$

for all sufficiently large n.

Proof. Assume that n is sufficiently large, and note that k_∞ (resp. k_∞^+) is unramified outside 2 and totally ramified at all places above 2 over k_n (resp. k_n^+). Then the extension k_{n+1} over $k_n^\vee$ is unramified outside 2 in which $\Pi(k_\infty)$ prime ideals ramify. For all $n \gg 0$, we have

$$|W(k_{n+1})| = 2^{\delta(k)-1}|W(k_n^\vee)||W(k_n)| = 2^{\delta(k)}|W(k_n)|.$$

Further, $Q(k_n) \geq Q(k_{n+1})$ if $\delta(k) = 1$, and $Q(k_n) \leq Q(k_{n+1})$ otherwise by [24] Proposition 1 (d) (e). Therefore $Q(k_n) = Q(k_{n+1})$ for all $n \gg 0$.

Let γ_n be the generator of $\mathrm{Gal}(k_{n+1}/k_n)$, and J a complex conjugation identified with the generator of $\mathrm{Gal}(k_{n+1}/k_{n+1}^+)$. Then $\sigma_n = J\gamma_n$ is a generator of $\Delta_n = \mathrm{Gal}(k_{n+1}/k_n^\vee)$. Since $|A(k_{n+1}^+)| = 1$ by our assumption, $1 + J$ annihilates $A(k_{n+1})$, i.e. J acts on $A(k_{n+1})$ as -1. Therefore $1 - \sigma_n$ acts on $A(k_{n+1})$ as $1 + \gamma_n$. Then we have the exact sequence:

$$0 \to A(k_{n+1})^{\Delta_n} \to A(k_{n+1}) \xrightarrow{1-\sigma_n} (1 + \gamma_n)A(k_{n+1}) \to 0.$$

The genus formula for k_{n+1} over $k_n^\vee$ yields that

$$\frac{|A(k_{n+1})|}{|(1 + \gamma_n)A(k_{n+1})|} = |A(k_{n+1})^{\Delta_n}| \leq 2^{\Pi(k_\infty)-1}|A(k_n^\vee)|.$$

On the other hand, by Proposition 2 of [24] and our assumption,

$$\begin{aligned} |A(k_{n+1})| &= \frac{Q(k_{n+1})}{Q(k_n^\vee)Q(k_n)} \frac{|W(k_{n+1})|}{|W(k_n^\vee)||W(k_n)|}|A(k_n)||A(k_n^\vee)| \\ &\geq 2^{\Pi(k_\infty)-1}|A(k_n)||A(k_n^\vee)| \end{aligned}$$

where we use the fact that $Q(K) = 2^{Q(K)-1}$ for any *CM*-field K. Since $(1+\gamma_n)A(k_{n+1})$ coincides with the image of the morphism $A(k_n) \to A(k_{n+1})$ induced from lifting of ideals, we have that

$$|\mathrm{Ker}(A(k_n) \to A(k_{n+1}))| = \frac{|A(k_n)|}{|(1 + \gamma_n)A(k_{n+1})|} \leq 1.$$

by combining the above inequalities. This implies that the morphisms $A(k_n) \to \varinjlim A(k_\bullet)$ induced from the lifting of ideals are injective for all $n \gg 0$. Since the $\mathbb{Z}_2$-torsion submodule of $X(k_\infty)$ is characterized by the well known isomorphism:

$$\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty) \simeq \varprojlim \mathrm{Ker}(A(k_n) \to \varinjlim A(k_\bullet))$$

(obtained from Theorem 7 and 10 of [18]), we know the freeness of $X(k_\infty)$. □

4.2. Proof of Theorem 2.2. For an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-q_1q_2})$ with prime numbers $q_1 \equiv 3 \pmod 8$ and $q_2 \equiv 7 \pmod{16}$, we know that $\lambda(k_\infty/k) = 2$ and $X(k_\infty) \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}_2^{\oplus 2}$ as $\mathbb{Z}_2$-modules by [8] and [19] (recall §3.1).

The genus field $K = k(\sqrt{q_1}, \sqrt{q_2})$ of k is a *CM*-field with the maximal real subfield $K^+ = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2})$, which contains three unramified quadratic extensions $k(\sqrt{q_1})$, $k(\sqrt{q_2})$, $k(\sqrt{-1})$ of k. For the cyclotomic $\mathbb{Z}_2$-extensions of these fields, the $\mathbb{Z}_2$-module structure of the Iwasawa modules are as follows.

Lemma 4.2. *$X(K_\infty)$ and $X(k_\infty(\sqrt{q_1}))$ are free $\mathbb{Z}_2$-modules of rank 3, and $X(k_\infty(\sqrt{q_2}))$, $X(k_\infty(\sqrt{-1}))$ are free $\mathbb{Z}_2$-modules of rank 2.*

Proof. $X(\mathbb{Q}_\infty(\sqrt{q_1}))$, $X(\mathbb{Q}_\infty(\sqrt{q_2}))$ and $X(\mathbb{Q}_\infty(\sqrt{q_1q_2}))$ are trivial, as mentioned in [31]. The genus formula for K_n^+ over $\mathbb{Q}_n(\sqrt{q_1q_2})$ implies that $|A(K_n^+)| = 1$ for all $n \geq 0$, i.e. $X(K_\infty^+)$ is also trivial. By Proposition 4.1, $X(K_\infty)$ is a free $\mathbb{Z}_2$-module since $\delta(K) = 1$ and $\Pi(K_\infty) = 0$.

On the other hand, $\delta(k(\sqrt{q_1})) = 0$ and $\Pi(k_\infty(\sqrt{q_1})) = 0$. The extension $k_n(\sqrt{q_1})^\vee = \mathbb{Q}_n(\sqrt{q_1}, \sqrt{-q_2\pi_n})$ over $\mathbb{Q}_n(\sqrt{q_1})$ is *essentially ramified* (cf. [24] p.349) since the integral ideal $(-q_2\pi_n)$ of $\mathbb{Q}_n(\sqrt{q_1})$ has nontrivial squarefree factor (q_2). Then $Q(k_n(\sqrt{q_1})^\vee) = 1$ for all n by [24] Theorem 1 (i)-1. This yields the freeness of $X(k_\infty(\sqrt{q_1}))$ by Proposition 4.1. The freeness of $X(k_\infty(\sqrt{q_2}))$ is also obtained similarly.

For the remained case, $\delta(k(\sqrt{-1})) = 1$ and $\Pi(k_\infty(\sqrt{-1})) = 1$. Since the ideal (π_n) remains prime in $\mathbb{Q}_n(\sqrt{q_1q_2})$, the extension $k_n(\sqrt{-1})^\vee = \mathbb{Q}_n(\sqrt{q_1q_2}, \sqrt{-\pi_n})$ is also essentially ramified. Then $Q(k_n(\sqrt{-1})^\vee) = 1$ for all n by [24] Theorem 1 (i)-1. By Proposition 4.1, we know the freeness of $X(k_\infty(\sqrt{-1}))$.

Note that K_∞^+ has 2 (resp. 4) places above q_1 (resp. q_2), which are not inert over $\mathbb{Q}_\infty$. By using Kida's formula [20], we know the $\mathbb{Z}_2$-rank of the Iwasawa modules. □

Let $G = \mathrm{Gal}(L^2(k_\infty)/k_\infty)$ be the Galois group of the maximal unramified metabelian pro-2-extension $L^2(k_\infty)$ over k_∞, and denote by N, N', N'' and H the open normal subgroups of G with the fixed fields $k_\infty(\sqrt{q_1})$, $k_\infty(\sqrt{q_2})$, $k_\infty(\sqrt{-1})$ and K_∞, respectively.

Since $G/G_2 \simeq X(k_\infty)$, G/G_2 has an element aG_2 of order 2 with some $a \in G$, and the Galois group G is a pro-2-group of rank 3. As seen in §3.1, aG_2 generates the decomposition subgroup of the place above 2 in $X(k_\infty)$. Then $aG_2 \in N/G_2$, i.e. $a \in N$ since the place of k_∞ above 2 splits in $k_\infty(\sqrt{q_1})$, and aH generates N/H. Further, we can take some $b \in N'$ such that bH generates N'/H. By taking some $c \in H$, we obtain a generator system a, b, c of G. Then the generating sets of the subgroups of G are as follows: (Note that $a^2 \in G_2$.)

$$\begin{array}{lll} G & = \mathrm{Gal}(L^2(k_\infty)/k_\infty) & = \langle\, a, b, c \,\rangle \\ N & = \mathrm{Gal}(L^2(k_\infty)/k_\infty(\sqrt{q_1})) & = \langle\, a, b^2, c, G_2 \,\rangle \\ N' & = \mathrm{Gal}(L^2(k_\infty)/k_\infty(\sqrt{q_2})) & = \langle\, b, c, G_2 \,\rangle \\ N'' & = \mathrm{Gal}(L^2(k_\infty)/k_\infty(\sqrt{-1})) & = \langle\, ab, c, G_2 \,\rangle \\ H & = \mathrm{Gal}(L^2(k_\infty)/K_\infty) & = \langle\, b^2, c, G_2 \,\rangle \end{array}$$

Note that G_2/G_3 is generated by $[a,b]G_3$, $[b,c]G_3$ and $[a,c]G_3$ as a $\mathbb{Z}_2$-module, and the closed subgroup $[b,c]^{\mathbb{Z}_2}G_3$ generated by $[b,c]$ and G_3 is a normal subgroup of G. Then

$$N'/[b,c]^{\mathbb{Z}_2}G_3 = \langle\, b, c, [a,b], [a,c], G_3 \,\rangle/[b,c]^{\mathbb{Z}_2}G_3$$

is an abelian group, in which b and c makes a free $\mathbb{Z}_2$-submodule of rank 2 since they are linearly independent over $\mathbb{Z}_2$ in G/G_2. On the other hand,

$$[a,b]^2 \equiv [a^2,b] \equiv 1, \quad [a,c]^2 \equiv [a^2,c] \equiv 1 \mod G_3,$$

i.e. $[a,b]$ and $[a,c]$ makes the torsion submodule of $N'/[b,c]^{\mathbb{Z}_2}G_3$. By Lemma 4.2 and the surjective morphism

$$X(k_\infty(\sqrt{q_2})) \simeq N'/N'_2 \to N'/[b,c]^{\mathbb{Z}_2}G_3,$$

$[a,b]$ and $[a,c]$ must be contained in $[b,c]^{\mathbb{Z}_2}G_3$, i.e. there exist some z_1, $z_2 \in \mathbb{Z}_2$ such that

$$[a,b] \equiv [b,c]^{z_1}, \quad [a,c] \equiv [b,c]^{z_2} \mod G_3.$$

Then G_2/G_3 is a cyclic $\mathbb{Z}_2$-module generated by $[b,c]G_3$. Especially, there exists some $z \in \mathbb{Z}_2$ such that

$$a^2 \equiv [b,c]^z \mod G_3.$$

If $[b,c] \in (G_2)^2G_3$, then $G_2 = G_3$, i.e. G is an abelian pro-2-group. However, the natural morphism $X(K_\infty) \to X(k_\infty)$ can not be injective by Lemma 4.2. Therefore

$$[b,c] \not\equiv 1 \mod (G_2)^2G_3.$$

Assume that $z_2 \in \mathbb{Z}_2^\times$. Then

$$[ab,c] \equiv [a,c][b,c] \equiv [a,c]^{1+z_2^{-1}} \equiv 1, \quad [b,c]^2 \equiv [a,c]^{2z_2^{-1}} \equiv 1 \mod G_3.$$

This yields that

$$N''/G_3 = \langle\, ab, c, [b,c], G_3 \,\rangle/G_3$$

is an abelian group in which $[b,c]G_3$ is a torsion element. Since abG_3 and cG_3 makes a free $\mathbb{Z}_2$-submodule of rank 2 and there is a surjective morphism

$$X(k_\infty(\sqrt{-1})) \simeq N''/N''_2 \to N''/G_3,$$

it becomes that $[b,c] \in G_3$ by Lemma 4.2. This contradiction yields that $z_2 \in 2\mathbb{Z}_2$.

By the above, we have that

$$[a,b^2] \equiv [a,b]^2 \equiv 1,\ [b^2,c] \equiv [b,c]^2 \equiv 1,\ [a,c] \equiv 1 \mod (G_2)^2G_3.$$

Then

$$N/(G_2)^2G_3 = \langle\, a, b^2, c, [b,c], G_3 \,\rangle/(G_2)^2G_3$$

is an abelian group. Since b^2G_2 and cG_2 are linearly independent in G/G_2 and $a^4 \equiv [b,c]^{2z} \equiv 1 \mod (G_2)^2G_3$, the free rank of the $\mathbb{Z}_2$-module $N/(G_2)^2G_3$ is 2 and the torsion submodule is

$$\mathrm{Tor}_{\mathbb{Z}_2}(N/(G_2)^2G_3) = \langle\, a, [b,c], G_3 \,\rangle/(G_2)^2G_3.$$

By Lemma 4.2 and the surjective morphism

$$X(k_\infty(\sqrt{q_1})) \simeq N/N_2 \to N/(G_2)^2G_3,$$

we know that $\mathrm{Tor}_{\mathbb{Z}_2}(N/(G_2)^2G_3)$ is a cyclic 2-group.

If $z \in 2\mathbb{Z}_2$, then $a^2 \equiv [b,c]^2 \equiv 1 \mod (G_2)^2G_3$. In this case, one of a, $[b,c]$, $a[b,c]$ is contained in $(G_2)^2G_3$. However, this induces a contradiction that either $a \in G_2$ or $[b,c] \in (G_2)^2G_3$. Then we know that $z \in \mathbb{Z}_2^\times$.

By the bracket operation $[-,-] : G_2/G_3 \times G/G_2 \to G_3/G_4$ which is a bilinear surjective morphism over $\mathbb{Z}_2$, we have that

$$G_3/G_4 = \langle\, [[b,c],a],\ [[b,c],b],\ [[b,c],c],\ G_4 \,\rangle/G_4.$$

and that

$$\begin{aligned}
[[b,c],a] &\equiv [a^{2z^{-1}},a] = 1 \mod G_4,\\
[[b,c],b] &\equiv [a^{2z^{-1}},b] = [a^{z^{-1}},b]^2[[a^{z^{-1}},b],a^{z^{-1}}] \equiv [[a,b]^{z^{-1}},a^{z^{-1}}]\\
&\equiv [a^{2z_1z^{-2}},a^{z^{-1}}] = 1 \mod (G_2)^2G_4,\\
[[b,c],c] &\equiv \cdots \equiv [a^{2z_2z^{-2}},a^{z^{-1}}] = 1 \mod (G_2)^2G_4.
\end{aligned}$$

These yield that $G_3 \subseteq (G_2)^2G_4$.

Then $\overline{G}_3 = \overline{G}_4$ for the lower central series $\overline{G}_i = G_i(G_2)^2/(G_2)^2$ of $\overline{G} = G/(G_2)^2$. Since the subgroups $\overline{G}_i$ make a fundamental system of closed neighborhoods of $1 \in \overline{G}$, it becomes that $\overline{G}_3 = \{1\}$, i.e. $G_3 \subseteq (G_2)^2$. By the induced surjective morphism

$$G_2/G_3 = \langle\, [b,c]G_3 \,\rangle \to G_2/(G_2)^2,$$

we know that G_2 is a cyclic pro-2-group generated by $[b,c]$. Then the Galois group $G(k_\infty)_2 = \mathrm{Gal}(L^\infty(k_\infty)/L(k_\infty))$ with the cyclic abelianization G_2 is also cyclic. This yields that $L^2(k_\infty) = L^\infty(k_\infty)$ and $G = G(k_\infty)$.

Since $(G_2)^2$ is generated by $[b,c]^2$, we may assume that

$$[a,b] = [b,c]^{z_1},\quad [a,c] = [b,c]^{z_2},\quad [b,c]^z = a^2$$

by replacing $z_1 \in \mathbb{Z}_2$, $z_2 \in 2\mathbb{Z}_2$ and $z \in \mathbb{Z}_2^\times$ suitably. Then G_2 is generated by a^2, and N is generated by a, b^2, c. Since N/N_2 is a free $\mathbb{Z}_2$-module of rank 3 by Lemma 4.2, a^2N_2 can not be a torsion element of N/N_2, i.e. $G_2/N_2 \simeq \mathbb{Z}_2$. This implies that

$$G_2 = \langle\, [b,c]\,\rangle = \langle\, a^2\,\rangle \simeq \mathbb{Z}_2$$

and $N_2 = \{1\}$, i.e. N is an abelian pro-2-group. Then H is also abelian, and $L^2(k_\infty) = L(K_\infty) = L(k_\infty(\sqrt{q_1}))$. Further,

$$\begin{aligned} 1 &= [b^2,c] = [b,c]^2[[b,c],b] = a^{4z^{-1}}[a^{2z^{-1}},b] = a^{2z^{-1}}(b^{-1}ab)^{2z^{-1}} \\ &= a^{2z^{-1}}(a[a,b])^{2z^{-1}} = a^{2z^{-1}}(a^{1+2z_1z^{-1}})^{2z^{-1}} = a^{4(z_1+z)z^{-2}}, \\ 1 &= [a,b^2] = \cdots = a^{4z_1(z_1+z)z^{-2}}, \\ 1 &= [a,c] = a^{2z_2z^{-1}}. \end{aligned}$$

Since a is not a torsion element of G, we have that $z_1 = -z$ and $z_2 = 0$, i.e.

$$[a,b] = a^{-2}, \quad [b,c] = a^{2z^{-1}}, \quad [a,c] = 1.$$

Let Γ be identified with the Galois group $\mathrm{Gal}(k_\infty(\sqrt{q_1})/k(\sqrt{q_1}))$. Since

$$\langle\, a\,\rangle/G_2 = \langle\, aG_2\,\rangle \simeq \mathrm{Tor}_{\mathbb{Z}_2}X(k_\infty) \simeq \varprojlim D(k_n)$$

(recall §3.1), the cyclic closed subgroup $\langle\, a\,\rangle$ generated by a is the decomposition subgroup of G for any place lying above 2. Especially, $\langle\, a\,\rangle$ is a normal subgroup of G and a Λ-submodule of $N = X(k_\infty(\sqrt{q_1})) \simeq \varprojlim A(k_n(\sqrt{q_1}))$. Further, since any place of $k_\infty(\sqrt{q_1})$ lying above 2 is totally ramified over $k(\sqrt{q_1})$, we have an isomorphism

$$\langle\, a\,\rangle \simeq \varprojlim D(k_n(\sqrt{q_1})) \simeq \Lambda/T\Lambda$$

as Λ-modules, i.e. Γ acts on $\langle\, a\,\rangle$ trivially. Since

$$G/\langle\, a\,\rangle \simeq X(k_\infty)/\mathrm{Tor}_{\mathbb{Z}_2}X(k_\infty)$$

as Λ-modules, we can take some x_0, x_1, x_2 and y_0, y_1, $y_2 \in \mathbb{Z}_2$ such that

$${}^{\gamma}a = a, \quad {}^{\gamma}b = a^{x_0}b^{x_1}c^{x_2}, \quad {}^{\gamma}c = a^{y_0}b^{y_1}c^{y_2}.$$

By using these 2-adic integers, the Iwasawa polynomial $P(T)$ associated to $X(k_\infty)$ is written as

$$P(T) = \det\left((1+T)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}\right).$$

Especially, the coefficients are

$$C_1 = 2 - x_1 - y_2, \quad C_0 = (1-x_1)(1-y_2) - x_2y_1 \ \in 2\mathbb{Z}_2.$$

Note that $H = X(K_\infty) = \langle a^2, b^2, c \rangle$ is a free $\mathbb{Z}_2$-module of rank 3 by Lemma 4.2. Since H is a Λ-module, ${}^\gamma c = a^{y_0} b^{y_1} c^{y_2}$ is contained in H. Further, since $\mathrm{Gal}(K_\infty/k_\infty) \simeq G/H = \langle aH, bH \rangle$ on which Γ acts trivially,

$$b^{-1}{}^\gamma b = (b^{-1}ab)^{x_0} b^{x_1-1} c^{x_2} = a^{-x_0} b^{x_1-1} c^{x_2}$$

is also contained in H. These yield that

$$x_0,\ y_0,\ y_1 \in 2\mathbb{Z}_2, \quad x_1,\ y_2 \in \mathbb{Z}_2^\times.$$

Assume that $x_2 \in 2\mathbb{Z}_2$. Then $b^{-1}{}^\gamma b \in G^2$. Since $a^{-1}{}^\gamma a$, $c^{-1}{}^\gamma c \in G^2$ and $G_2 \subset G^2$ by the above,

$$X(k_\infty)/2X(k_\infty) \simeq G/G^2 = \langle aG^2, bG^2, cG^2 \rangle$$

becomes an abelian group of type $(2,2,2)$ on which Γ acts trivially, i.e. $TX(k_\infty)$ is contained in $2X(k_\infty)$. By the well known isomorphism

$$A(k) \simeq X(k_\infty)/TX(k_\infty)$$

(cf. [34] Lemma 13.15), we have a contradiction:

$$\mathrm{Gal}(K/k) \simeq A(k)/2A(k) \simeq X(k_\infty)/2X(k_\infty) \simeq G/G^2.$$

This yields that $x_2 \in \mathbb{Z}_2^\times$.

Now, we take the other generator system a', b', c' of G as follows:

$$\begin{aligned}
a' &= a^{(x_2-x_0z)z^{-1}} && \equiv a \bmod G^2,\\
b' &= b^{(x_2-x_0z)x_2^{-1}} && \equiv b \bmod G^2,\\
c' &= b^{(x_1-1)(x_2-x_0z)x_2^{-1}} c^{x_2-x_0z} && \equiv c \bmod G^2.
\end{aligned}$$

Throughout the following calculations, we use the facts that $N = \langle a, b^2, c \rangle$ is an abelian group and a', b'^2, $c' \in N$. Then

$$\begin{aligned}
[a', b'] &= [a', b(b^2)^{-(x_0/2)zx_2^{-1}}] = [a', b] = a'^{-1}(b^{-1}ab)^{(x_2-x_0z)z^{-1}} = a'^{-2},\\
[b', c'] &= [b(b^2)^{-(x_0/2)zx_2^{-1}}, c'] = [b, c'] = [b, c^{x_2-x_0z}]\\
&= (b^{-1}cb)^{-(x_2-x_0z)} c^{x_2-x_0z} = (ca^{-2z^{-1}})^{-(x_2-x_0z)} c^{x_2-x_0z}\\
&= a^{2(x_2-x_0z)z^{-1}} = a'^2,\\
[a', c'] &= 1.
\end{aligned}$$

Further,

$$
\begin{aligned}
{}^{\gamma}a' &= a', \\
{}^{\gamma}b' &= {}^{\gamma}b \cdot ({}^{\gamma}b^2)^{-(x_0/2)zx_2^{-1}} \\
&= {}^{\gamma}b \cdot (a^{x_0}b^{x_1+1}(b^{-1}cb)^{x_2}(b^{-1}ab)^{x_0}b^{x_1-1}c^{x_2})^{-(x_0/2)zx_2^{-1}} \\
&= {}^{\gamma}b \cdot (a^{x_0}(b^2)^{(x_1+1)/2}(ca^{-2z^{-1}})^{x_2}(a^{-1})^{x_0}(b^2)^{(x_1-1)/2}c^{x_2})^{-(x_0/2)zx_2^{-1}} \\
&= {}^{\gamma}b \cdot (a^{-2z^{-1}x_2}b^{2x_1}c^{2x_2})^{-(x_0/2)zx_2^{-1}} \\
&= a^{x_0}b^{x_1}c^{x_2} \cdot a^{x_0}b^{-2x_1(x_0/2)zx_2^{-1}}c^{-x_0z} \\
&= b(b^{-1}ab)^{x_0} \cdot (b^2)^{(x_1-1)/2}c^{x_2}a^{x_0}(b^2)^{-x_1(x_0/2)zx_2^{-1}}c^{-x_0z} \\
&= ba^{-x_0} \cdot a^{x_0}b^{(x_1-1)-x_1x_0zx_2^{-1}}c^{x_2-x_0z} \\
&= b^{1-x_0zx_2^{-1}} \cdot b^{(x_1-1)(1-x_0zx_2^{-1})}c^{x_2-x_0z} \\
&= b'c', \\
{}^{\gamma}c' &= ({}^{\gamma}b^2)^{((x_1-1)/2)(x_2-x_0z)x_2^{-1}}({}^{\gamma}c)^{x_2-x_0z} \\
&= (a^{-2z^{-1}x_2}b^{2x_1}c^{2x_2})^{((x_1-1)/2)(x_2-x_0z)x_2^{-1}}(a^{y_0}(b^2)^{y_1/2}c^{y_2})^{x_2-x_0z} \\
&= a^{(x_2-x_0z)z^{-1}(-(x_1-1)+zy_0)}b^{(x_2-x_0z)x_2^{-1}(x_1(x_1-1)+y_1x_2)}c^{(x_2-x_0z)((x_1-1)+y_2)} \\
&= a'^{-(x_1-1)+zy_0}(b'^2)^{(x_1(x_1-1)+y_1x_2)/2}((b'^2)^{-(x_1-1)/2}c')^{(x_1-1)+y_2} \\
&= a'^{-(x_1-1)+zy_0}b'^{-(1-x_1)(1-y_2)+x_2y_1}c'^{1-(2-x_1-y_2)} \\
&= a'^{-(x_1-1)+zy_0}b'^{-C_0}c'^{1-C_1}.
\end{aligned}
$$

By using them and the facts that ${}^{\gamma}c' \in {}^{\gamma}cG^2 \subset N$ and $G_2 = \langle a' \rangle$,

$$
\begin{aligned}
a'^2 &= {}^{\gamma}(a'^2) = [{}^{\gamma}b', {}^{\gamma}c'] = [b'c', {}^{\gamma}c'] = c'^{-1}[b', {}^{\gamma}c']c'[c', {}^{\gamma}c'] = [b', {}^{\gamma}c'] \\
&= b'^{-1}(c'^{-1+C_1}b'^{C_0}a'^{(x_1-1)-zy_0})b'(a'^{-(x_1-1)+zy_0}b'^{-C_0}c'^{1-C_1}) \\
&= (b'^{-1}c'b')^{-1+C_1}b'^{C_0}(b'^{-1}a'b')^{(x_1-1)-zy_0}(a'^{-(x_1-1)+zy_0}b'^{-C_0}c'^{1-C_1}) \\
&= (c'a'^{-2})^{-1+C_1}(b'^2)^{C_0/2}a'^{-(x_1-1)+zy_0}(a'^{-(x_1-1)+zy_0}(b'^2)^{-C_0/2}c'^{1-C_1}) \\
&= (a'^2)^{-(x_1-1)+zy_0+1-C_1}.
\end{aligned}
$$

Since a' is not a torsion element, this implies that $C_1 = -(x_1-1) + zy_0$, i.e. ${}^{\gamma}c' = a'^{C_1}b'^{-C_0}c'^{1-C_1}$.

Let F be a free pro-2-group generated by three letters a, b, c, and R the closed normal subgroup generated by the conjugates of $\mathsf{a}^2[\mathsf{a},\mathsf{b}]$, $\mathsf{a}^{-2}[\mathsf{b},\mathsf{c}]$ and $[\mathsf{a},\mathsf{c}]$. Then there exists a surjective morphism $\mathsf{F}/\mathsf{R} \to G$: $\mathsf{aR} \mapsto a'$, $\mathsf{bR} \mapsto b'$, $\mathsf{cR} \mapsto c'$. Since this morphism induces $(\mathsf{F}/\mathsf{R})_2 = \mathsf{F}_2\mathsf{R}/\mathsf{R} \simeq G_2$ and $\mathsf{F}/\mathsf{F}_2\mathsf{R} \simeq G/G_2$, we know that $\mathsf{F}/\mathsf{R} \simeq G$ which gives a presentation of G. By replacing the notations a', b', c' by a, b, c, the proof of Theorem 2.2 is completed.

4.3. On metabelian 2-class field towers. As a corollary of Theorem 2.2, we calculate the Galois groups $G(k_n)$ of the 2-class field towers of k_n under some conditions as follows.

Proposition 4.3. *In addition to the statement of Theorem* 2.2, *if* $(q_1/q_2) = -1$ *(i.e. q_1 is not a quadratic residue modulo q_2), then $G(k)$ is an abelian group of type* $(2,2)$, *and $G(k_1)$ has a presentation*

$$G(k_1) = \langle\, \overline{a},\, \overline{b},\, \overline{c} \mid [\overline{b}, \overline{a}] = [\overline{b}, \overline{c}] = \overline{a}^2 = \overline{b}^2 = \overline{c}^2,\ [\overline{a}, \overline{c}] = \overline{a}^4 = 1 \,\rangle.$$

Further, if $C_1 \equiv 0 \pmod 4$, *$G(k_n)$ has a presentation*

$$G(k_n) = \langle\, \overline{a},\, \overline{b},\, \overline{c} \mid [\overline{b}, \overline{a}] = [\overline{b}, \overline{c}] = \overline{a}^2,\ [\overline{a}, \overline{c}] = \overline{a}^{2^{n+1}} = \overline{b}^{2^{n+1}} = \overline{c}^{2^n} = 1 \,\rangle$$

with the order $|G(k_n)| = 2^{3n+2}$ *for each* $n \geq 2$.

Proof. Since $(q_1/q_2) = -1$, $G(k) \simeq (2,2)$ by [21] § 2 (ii), i.e. $K = L^\infty(k)$ and $|A(K)| = 1$ for the genus field $K = k(\sqrt{q_1}, \sqrt{q_2})$ of k. Then, by [34] Lemma 13.15, $X(K_\infty)/\nu_n X(K_\infty) \simeq A(K_n)$ as Λ-modules for all $n \geq 0$, where

$$\nu_n = \nu_n(T) = ((1+T)^{2^n} - 1)/T \in \Lambda.$$

By applying the genus formula for K_1 over K, we know that $A(K_1) \simeq X(K_\infty)/\nu_1 X(K_\infty)$ is cyclic. Nakayama's lemma yields that $X(K_\infty)$ is a cyclic Λ-module.

Recall that $H = X(K_\infty)$ is an abelian subgroup of $G = G(k_\infty)$ which is generated by a^2, b^2, c. Since $\langle\, a^2 \,\rangle \simeq \Lambda/T\Lambda$, we have an exact sequence

$$0 \to \Lambda/T\Lambda \to X(K_\infty) \to X(k_\infty)/\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty) \to \mathbb{Z}/2\mathbb{Z} \to 0$$

of Λ-modules. Then the characteristic polynomial of the Λ-module $X(K_\infty)$ is $TP(T)$, and $H = X(K_\infty) \simeq \Lambda/TP(T)\Lambda$ as a Λ-module.

Lemma 4.4. $C_0 \equiv 2 \pmod 4$.

Proof. Since $\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty) \simeq D(k) \simeq \mathbb{Z}/2\mathbb{Z}$ (cf. [8] Lemma 10) under the surjective morphism $X(k_\infty) \to A(k) \simeq (2,2)$ with the kernel $TX(k_\infty)$ (cf. [34] Lemma 13.15), we know that

$$X(k_\infty)/(TX(k_\infty) + \mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty)) \simeq A(k)/D(k) \simeq \mathbb{Z}/2\mathbb{Z},$$

and that $X(k_\infty)/\mathrm{Tor}_{\mathbb{Z}_2} X(k_\infty) \simeq \Lambda/P(T)\Lambda$ by Nakayama's lemma. By combining these isomorphism, we have $\Lambda/(T, P(T)) \simeq \mathbb{Z}/2\mathbb{Z}$, i.e. $C_0 \equiv 2 \pmod 4$. □

Note that any polynomial in Λ acts on H by identifying T with $\gamma - 1$ (i.e. ${}^T h = {}^\gamma h \cdot h^{-1}$ for any $h \in H$). Let

$$F(T) = (C_1/C_0)P(T) - T - C_1$$

which is a polynomial in Λ by Lemma 4.4. Then

$$\begin{aligned}
{}^{P(T)}c &= {}^{\gamma^2}c \cdot ({}^{\gamma}c)^{C_1-2} c^{C_0-C_1+1} \\
&= ({}^{\gamma}a)^{C_1}({}^{\gamma}b)^{-C_0}({}^{\gamma}c)^{1-C_1} \cdot (a^{C_1}b^{-C_0}c^{1-C_1})^{C_1-2}c^{C_0-C_1+1} \\
&= a^{C_1}(b^2c[c,b]c)^{-C_0/2}(a^{C_1}b^{-C_0}c^{1-C_1})^{1-C_1} \cdot a^{C_1(C_1-2)}b^{-C_0(C_1-2)}c^{-(1-C_1)^2+C_0} \\
&= a^{C_1}(a^{-2}b^2c^2)^{-C_0/2}a^{-C_1}b^{C_0}c^{C_0} \\
&= a^{C_0}, \\
{}^{F(T)}c &= ({}^{P(T)}c)^{C_1/C_0}({}^{\gamma}c)^{-1}c^{1-C_1} = (a^{C_0})^{C_1/C_0}(a^{C_1}b^{-C_0}c^{1-C_1})^{-1}c^{1-C_1} \\
&= b^{C_0}.
\end{aligned}$$

By Lemma 4.4, we can choose an isomorphism $H \simeq \Lambda/TP(T)\Lambda$ such that

$$a^2 \mapsto (2/C_0)P(T)\ , \quad b^2 \mapsto (2/C_0)F(T)\ , \quad c \mapsto 1\ .$$

Note that a^2, b^2, c make a basis of the free $\mathbb{Z}_2$-module H and that $\nu_n(0) = 2^n$, $P(0) = C_0$ and $F(0) = 0$. For each $n \geq 0$, there exists uniquely a pair x_n, $\mathsf{y}_n \in \mathbb{Z}_2$ such that

$$\nu_n(T) \equiv \mathsf{x}_n\,(2/C_0)P(T) + \mathsf{y}_n\,(2/C_0)F(T) + (2^n - 2\mathsf{x}_n) \mod TP(T).$$

Especially, $\mathsf{x}_0 = \mathsf{y}_0 = 0$. By using these 2-adic integers, we have

$$\begin{aligned}
&\nu_n(T)\,(2/C_0)P(T) \equiv 2^n(2/C_0)P(T), \\
&\nu_n(T)\,(2/C_0)F(T) \equiv \\
&(2/C_0)\mathsf{y}_n(2/C_0)P(T) + (2^n - 2\mathsf{x}_n - C_1(2/C_0)\mathsf{y}_n)(2/C_0)F(T) - 2(2/C_0)\mathsf{y}_n \\
&\hfill \mod TP(T).
\end{aligned}$$

Then the endomorphism $\nu_n : H \to H$ is described by

$$\nu_n \begin{bmatrix} a^2 \\ b^2 \\ c \end{bmatrix} = \begin{bmatrix} 2^n & 0 & 0 \\ (2/C_0)\mathsf{y}_n & 2^n - 2\mathsf{x}_n - C_1(2/C_0)\mathsf{y}_n & -2(2/C_0)\mathsf{y}_n \\ \mathsf{x}_n & \mathsf{y}_n & 2^n - 2\mathsf{x}_n \end{bmatrix} \begin{bmatrix} a^2 \\ b^2 \\ c \end{bmatrix}$$

additively. In the following, we denote by A_n the 3×3 matrix in right hand side.

Since $H = G(K_\infty)$ is abelian and K_∞ is totally ramified over K_n, then $G(K_n)$ is an abelian subgroup of $G(k_n)$ which is isomorphic to $A(K_n)$ via Artin map. Further, since $\nu_n H$ is a normal subgroup of G and $H/\nu_n H \simeq G(K_n)$ via the restriction map, we know that

$$G/\nu_n H \simeq G(k_n)$$

for all $n \geq 0$. For each n fixed, we denote by $\overline{a}$, $\overline{b}$, $\overline{c}$ the images of a, b, c in right hand side.

Now, we consider the case that $n = 1$. Since $\nu_1 = T + 2$, then $\mathsf{x}_1 = C_1/2$, $\mathsf{y}_1 = -C_0/2$, and there exists some $\mathsf{U}_1 \in GL_3(\mathbb{Z}_2)$ such that

$$\mathsf{A}_1 = \begin{bmatrix} 2 & 0 & 0 \\ -1 & 2 & 2 \\ C_1/2 & -C_0/2 & 2 - C_1 \end{bmatrix} = \mathsf{U}_1 \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 2 \end{bmatrix}.$$

Therefore $\nu_1 H$ is generated by a^4, $a^{-2}b^2$ and $a^{-2}c^2$, and we obtain the presentation of $G(k_1) \simeq G/\langle a^4, a^{-2}b^2, a^{-2}c^2 \rangle$.

Lemma 4.5. $\mathsf{x}_n \equiv 2^{n-2}C_1$, $\mathsf{y}_n \equiv 0 \pmod{2^n}$ *for all* $n \geq 2$.

Proof. Since $\nu_{n+1}(T) = \nu_n(T)(T\nu_n(T) + 2)$ for all $n \geq 0$, we have

$$\begin{aligned} \mathsf{x}_{n+1} &= 2^n + (2^n - 2\mathsf{x}_n)(-(1 + 2\mathsf{y}_n) + (C_1/2)(2^n - 2\mathsf{x}_n)) \\ \mathsf{y}_{n+1} &= -(C_0/2)(2^n - 2\mathsf{x}_n)^2 + 2\mathsf{y}_n(1 + \mathsf{y}_n). \end{aligned}$$

Especially, $\mathsf{x}_2 \equiv C_1$, $\mathsf{y}_2 \equiv 0 \pmod 4$ by Lemma 4.4. Then we know that $\mathsf{x}_n \equiv 2^{n-2}C_1$, $\mathsf{y}_n \equiv 0 \pmod{2^n}$ for all $n \geq 2$ inductively. □

Assume that $C_1 \equiv 0 \pmod 4$ and $n \geq 2$. Lemma 4.5 yields that $\mathsf{x}_n \equiv \mathsf{y}_n \equiv 0 \pmod{2^n}$. Further, $\det(\mathsf{A}_n) \in 2^{3n}\mathbb{Z}_2^\times$ and $\mathsf{A}_n \equiv \mathsf{O} \pmod{2^n}$. Then we can find some $\mathsf{U}_n \in GL_3(\mathbb{Z}_2)$ such that

$$\mathsf{A}_n = \mathsf{U}_n \begin{bmatrix} 2^n & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 2^n \end{bmatrix} \equiv \begin{bmatrix} 2^n & 0 & 0 \\ \mathsf{y}_n & 2^n & 0 \\ \mathsf{x}_n & \mathsf{y}_n & 2^n \end{bmatrix} \bmod 2^{n+1}$$

by noting the congruence of right hand side. This implies that $\nu_n H$ is generated by $a^{2^{n+1}}$, $b^{2^{n+1}}$ and c^{2^n}, and that $A(K_n) \simeq (\mathbb{Z}/2^n\mathbb{Z})^{\oplus 3}$ as a $\mathbb{Z}_2$-module. Then we have the presentation of $G(k_n) \simeq G/\langle a^{2^{n+1}}, b^{2^{n+1}}, c^{2^n} \rangle$ for $n \geq 2$, and know that $|G(k_n)| = 2^{3n+2}$. □

Example. There are 48 (resp. 53) pairs of prime numbers $q_1 \equiv 3 \pmod 8$, $q_2 \equiv 7 \pmod{16}$ such that $q_1 q_2 < 5000$ and $(q_1/q_2) = -1$ (resp. $(q_1/q_2) = 1$). For all of them, we can see that $P(T) \equiv T^2 + 2 \pmod 4$, i.e. $C_1 \equiv 0 \pmod 4$ (resp. that $P(T) \equiv T^2 + 2T \pmod 4$) by the computation with the use of Stickelberger elements. Especially, if $q_1 = 3$ and $q_2 = 7$, i.e. $k = \mathbb{Q}(\sqrt{-21})$, then $P(T) \equiv T^2 + 15604T + 26266 \pmod{2^{15}}$.

5. On some relating problems

5.1. Let k be an imaginary quadratic field in which the prime number 2 splits. Then the unique $\mathbb{Z}_2^{\oplus 2}$-extension $\widetilde{k}$ of k is unramified over k_∞, i.e. $G(\widetilde{k})$ is a closed normal subgroup of $G(k_\infty)$ such that $G(k_\infty)/G(\widetilde{k}) \simeq \mathbb{Z}_2$. In this case, Greenberg's generalized conjecture is considered as a problem relating to the structure of $G(k_\infty)$, which asserts that $X(\widetilde{k}) = G(\widetilde{k})/G(\widetilde{k})_2$ is pseudo-null as a finitely generated torsion $\mathbb{Z}_2[[\mathrm{Gal}(\widetilde{k}/k)]]$-module. In [11] and [29], it is shown that $G(k_\infty)$ is not a nonabelian free pro-2-group if $X(\widetilde{k})$ is pseudo-null. Further, some criteria for the pseudo-nullity of $X(\widetilde{k})$ are established (cf., e.g., [17]), though the explicit structure of $X(\widetilde{k})$ is uncertain in general. Here, we obtain the following by the analogous arguments to the proof of Theorem 2.2.

Proposition 5.1. *Let $k = \mathbb{Q}(\sqrt{-q_1q_2q_3})$ be an imaginary quadratic field with prime numbers $q_1 \equiv q_2 \equiv 3$, $q_3 \equiv 7 \pmod 8$ such that $(q_1q_2/q_3) = -1$, and $\widetilde{k}$ the $\mathbb{Z}_2^{\oplus 2}$-extension of k. Then $\widetilde{k}$ is an unramified $\mathbb{Z}_2$-extension over the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k satisfying that $L(\widetilde{k}) = L(k_\infty)$, i.e. there is an exact sequence*

$$0 \to X(\widetilde{k}) \to X(k_\infty) \to \mathrm{Gal}(\widetilde{k}/k_\infty) \to 0.$$

Especially, $X(\widetilde{k})$ is pseudo-null as a $\mathbb{Z}_2[[\mathrm{Gal}(\widetilde{k}/k)]]$-module.

Proof. Let $\mathfrak{p}$ be a prime ideal of k above 2, and $k(\mathfrak{p}^3)$ the ray 2-class field of k modulo $\mathfrak{p}^3$, which is a quadratic extension of $L(k)$. Let k'_∞ be the $\mathbb{Z}_2$-extension of k unramified outside $\mathfrak{p}$. Note that the genus field of k is $K = k(\sqrt{-q_1}, \sqrt{-q_2})$, and that $k'_\infty \cap k(\mathfrak{p}^3)$ is a quadratic extension of $k'_\infty \cap L(k)$. Since $(q_3/q_1) = -(q_3/q_2)$ and $q_1 \equiv q_2 \equiv 3 \pmod 8$, a prime ideal of k above either q_1 or q_2 has the decomposition subgroup of order 4 in $\mathrm{Gal}(k(\mathfrak{p}^3)/k)$, and hence the rank of $\mathrm{Gal}(k(\mathfrak{p}^3)/k)$ is 2. Therefore $k \subsetneq k'_\infty \cap L(k)$. Since $(q_1q_2/q_3) = -1$ and $q_3 \equiv 7 \pmod 8$, the prime ideal of k above q_3 is inert in $k(\sqrt{-q_3})$, and the prime ideal of $k(\sqrt{-q_3})$ above q_3 splits completely in $k(\mathfrak{p}^3)$. If $k(\sqrt{-q_3}) \subset k'_\infty \cap L(k)$, the prime ideal of k above q_3 does not split in $k'_\infty \cap k(\mathfrak{p}^3)$. This is a contradiction. Therefore $k(\sqrt{-q_3}) \not\subset k'_\infty \cap L(k)$. By replacing q_1 and q_2 suitably, we may assume that $k(\sqrt{-q_1}) \subset k'_\infty \cap L(k) \subset \widetilde{k}$.

Let $G = \mathrm{Gal}(L^2(k_\infty)/k_\infty)$ be the Galois group of the maximal unramified metabelian pro-2-extension of k_∞. Since $G/G_2 \simeq X(k_\infty)$ is a free $\mathbb{Z}_2$-module of rank $\lambda = 1 + 2^{v-2}$ by [8], where 2^v is the largest 2-power dividing $q_3 + 1$, then we can choose the generator system $a, b_1, \cdots, b_{\lambda-1}$ of G such that

$$H = \mathrm{Gal}(L^2(k_\infty)/\widetilde{k}) = \langle\, b_1, \cdots, b_{\lambda-1}, G_2 \,\rangle$$

and $N = \mathrm{Gal}(L^2(k_\infty)/k_\infty(\sqrt{-q_1})) = \langle\, a^2 \,\rangle H$. Further, by the similar arguments to the proof of Lemma 4.2 with the use of Proposition 4.1 and Kida's formula [20], we can show that $X(k_\infty(\sqrt{-q_1}))$ is also a free $\mathbb{Z}_2$-module of rank λ.

Now, we put $B = \langle\, [b_i, b_j] \mid 1 \leq i < j \leq \lambda - 1 \,\rangle (G_2)^2 G_3$. Since $[a^2, b_i] \in (G_2)^2 G_3$, N/B is abelian. Then, by considering the surjective morphism $X(k_\infty(\sqrt{-q_1})) \to N/B$, we can see that all $[a, b_i]$ are contained in B. This yields that $G_2 = B$, i.e. G_2/G_3 is generated by all $[b_i, b_j]G_3$. Since $[b_i, b_j] \in H_2$ and H_2 is a normal subgroup of G, we know that $G_2 \subseteq H_2$. Therefore $G_2 = H_2$, i.e. $L(\widetilde{k}) = L(k_\infty)$.

Note that $\mathrm{Gal}(\widetilde{k}/k)$ is generated by the restricted elements of a and $\widetilde{\gamma}$. Since a acts on $X(\widetilde{k}) \simeq H/G_2$ trivially and $P(\widetilde{\gamma} - 1)$ annihilates $X(\widetilde{k})$, we know that $X(\widetilde{k})$ is a pseudo-null $\mathbb{Z}_2[[\mathrm{Gal}(\widetilde{k}/k)]]$-module. □

Remark. For the imaginary quadratic fields k of Proposition 5.1, the pseudo-nullity of $X(\widetilde{k})$ can be shown as a consequence of the criteria by Itoh [17].

5.2. For the imaginary quadratic fields k treated in Theorem 2.1 and Theorem 2.2, we have seen that $L(K_\infty) = L^2(k_\infty)$ for the genus fields K of k. For several other families of k with the genus fields $K \neq k$, if $X(K_\infty^+)$ is trivial, one can also calculate the structure of the quotient $\mathrm{Gal}(L(K_\infty)/k_\infty)$ of $G(k_\infty)$ by the similar arguments. However, it is still difficult problem to determine the structure of $G(k_\infty)$ itself and even the metabelian quotient $\mathrm{Gal}(L^2(k_\infty)/k_\infty)$ in general situation. One of the difficulties is the structure of $G(K_\infty^+)$ relating with Greenberg's conjecture [14]. If $G(K_\infty^+)$ is infinite, one can easily find the open subgroups of $G(k_\infty)$ with arbitrary large generator rank by using Kida's formula [20].

As a step to the above problem, the following seems to be one of the considerable problems: *Characterize the imaginary quadratic fields k with $L^2(k_\infty) = L(K_\infty) \neq L(k_\infty)$*. This can be regarded as an analogy of Problem 2 in [38] Appendix 2.

Acknowledgements

The author expresses his gratitude to Professor Ken Yamamura for giving valuable information on number fields with 2-class group of type $(2, 2^\bullet)$. The author also thanks to the referee for helpful comments and suggestions for improvement of this paper. The author was supported by JSPS Research Fellowships for Young Scientists.

References

[1] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$. J. Number Theory **67** (1997), no. 2, 229–245.

[2] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower*. J. Number Theory **73** (1998), no. 2, 182–194.

[3] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with* $\mathrm{Cl}_2(k) \simeq (2, 2^m)$ *and rank* $\mathrm{Cl}_2(k^1) = 2$. Pacific J. Math. **198** (2001), no. 1, 15–31.

[4] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields with* $\mathrm{Cl}_2(k) \simeq (2, 2, 2)$. J. Number Theory **103** (2003), no. 1, 38–70.

[5] N. Boston, *Galois groups of tamely ramified p-extensions*. J. Théor. Nombres Bordeaux **19** (2007), no. 1, 59–70.

[6] M. R. Bush, *Computation of Galois groups associated to the 2-class towers of some quadratic fields*. J. Number Theory **100** (2003), no. 2, 313–325.

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

[8] B. Ferrero, *The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields*. Amer. J. Math. **102** (1980), no. 3, 447–459.

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

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

[11] S. Fujii, *Non-abelian Iwasawa theory of cyclotomic $\mathbb{Z}_p$-extensions*. The COE Seminar on Mathematical Sciences 2007, 85–97, Sem. Math. Sci. **37**, Keio Univ., Yokohama, 2008.

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

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

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

[15] F. Hajir, *On a theorem of Koch*. Pacific J. Math. **176** (1996), no. 1, 15–18. Correction: **196** (2000), no. 2, 507–508.

[16] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*. Inter. J. Math. **7** (1996), no. 6, 721–744.

[17] T. Itoh, *Pseudo-null Iwasawa modules for $\mathbb{Z}_2^2$-extensions*. Tokyo J. Math. **30** (2007), no. 1, 199–209.

[18] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*. Ann. of Math. (2) **98** (1973), 246–326.

[19] Y. Kida, *On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*. Tohoku Math. J. (2) **31** (1979), no. 1, 91–96.

[20] Y. Kida, *Cyclotomic $\mathbb{Z}_2$-extensions of J-fields*. J. Number Theory **14** (1982), no. 3, 340–352.

[21] H. Kisilevsky, *Number fields with class number congruent to* 4 *mod* 8 *and Hilbert's theorem 94*. J. Number Theory **8** (1976), no. 3, 271–279.

[22] M. Lazard, *Groupes analytiques p-adiques*. Inst. Hautes Études Sci. Publ. Math. **26** (1965), 389–603.

[23] F. Lemmermeyer, *On* 2*-class field towers of imaginary quadratic number fields*. J. Théor. Nombres Bordeaux **6** (1994), no. 2, 261–272.

[24] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields I*. Acta Arith. **72** (1995), no. 4, 347–359.

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

[26] Y. Mizusawa, *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.

[27] Y. Mizusawa and M. Ozaki, *Abelian* 2*-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*. Math. Ann. **347** (2010, no. 2, 437–453.

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

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

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

[31] M. Ozaki and H. Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*. Manuscripta Math. **94** (1997), no. 4, 437–444.

[32] J.-P. Serre, *Galois cohomology*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

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

[34] L. C. Washington, *Introduction to Cyclotomic Fields (2nd edition)*. Graduate Texts in Math. vol. **83**, Springer, 1997.

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

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

[37] Y. Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*. Osaka J. Math. **21** (1984), no. 1, 1–22.

[38] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*. J. Théor. Nombres Bordeaux **9** (1997), no. 2, 405–448.

Yasushi Mizusawa
Department of Mathematics
Nagoya Institute of Technology
Gokiso, Showa, Nagoya, Aichi 466-8555, JAPAN
E-mail: mizusawa.yasushi@nitech.ac.jp