ON UNRAMIFIED GALOIS 2-GROUPS OVER $\mathbb{Z}_2$ -EXTENSIONS OF REAL QUADRATIC FIELDS

YASUSHI MIZUSAWA

(Communicated by Ken Ono)

ABSTRACT. We prove that the Galois groups of the maximal unramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$ -extensions of certain real quadratic fields are metacyclic pro-2 groups, and we give some criteria for the finiteness and examples relating to Greenberg's conjecture.

1. INTRODUCTION

Let ℓ be a prime number and k a number field of finite degree. We denote by k_∞ the cyclotomic $\mathbb{Z}_\ell$ -extension of k . For each integer $n \geq 0$, k_∞ contains a unique cyclic extension k_n/k of degree ℓ^n . Let $A(k_n)$ be the Sylow ℓ -subgroup of the ideal class group of k_n , and let $X(k_\infty) = \varprojlim A(k_n)$ be the projective limit with respect to the norm mappings. For all sufficiently large n , the order $|A(k_n)|$ is described as

$$|A(k_n)| = \ell^{\lambda_\ell(k)n + \mu_\ell(k)\ell^n + \nu_\ell(k)}$$

by the Iwasawa invariants $\lambda_\ell(k)$, $\mu_\ell(k)$ and $\nu_\ell(k)$. The Iwasawa module $X(k_\infty)$ is finite if and only if $\lambda_\ell(k) = \mu_\ell(k) = 0$. Greenberg [10] conjectured that $\lambda_\ell(k) = \mu_\ell(k) = 0$ if k is a totally real number field. Ferrero and Washington [7] proved that $\mu_\ell(k) = 0$ if k is an abelian extension of the rational number field $\mathbb{Q}$.

Let $G(k_\infty)$ (resp. $G(k_n)$) be the Galois group of the maximal unramified pro- ℓ -extension k_∞^{ur}/k_∞ (resp. k_n^{ur}/k_n). The commutator series of $G(k_n)$ corresponds to the ℓ -class field tower of k_n . Then $G(k_\infty) \simeq \varprojlim G(k_n)$ with respect to the restriction mappings, and the maximal abelian quotient of $G(k_\infty)$ (resp. $G(k_n)$) is isomorphic to $X(k_\infty)$ (resp. $A(k_n)$). The triviality of $G(k_\infty)$ is equivalent to the vanishing of the Iwasawa invariants $\lambda_\ell(k) = \mu_\ell(k) = \nu_\ell(k) = 0$. Concerning a restatement of Greenberg's conjecture, we have the following proposition.

Proposition 1. (i) $G(k_\infty)$ is a *Fab* pro- ℓ group (i.e., the maximal abelian quotient of any open subgroup is finite) if and only if $\lambda_\ell(F) = \mu_\ell(F) = 0$ for any finite subextension F/k of k_∞^{ur}/k .

(ii) $G(k_\infty)$ is a finite ℓ -group if and only if there exists a finite extension F/k satisfying $\lambda_\ell(F) = \mu_\ell(F) = \nu_\ell(F) = 0$.

Received by the editors June 19, 2009 and, in revised form, November 29, 2009.

2010 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R20.

This work was supported by KAKENHI (20840022), Grant-in-Aid for Young Scientists (Start-up).

©2010 American Mathematical Society
 Reverts to public domain 28 years from publication

Proof. (i) The fixed field F_∞ of any open subgroup of $G(k_\infty)$ is the cyclotomic $\mathbb{Z}_\ell$ -extension of some finite extension F of k . Conversely, for any finite subextension F/k of k_∞^{ur}/k , $G(F_\infty)$ is an open subgroup of $G(k_\infty)$. These yield the claim.

(ii) If $G(k_\infty)$ is finite, $k_n^{ur}k_\infty = k_\infty^{ur}$ for some n . Then $G(F_\infty)$ is trivial for a finite extension $F = k_n^{ur}$ of k . Conversely, if such an extension F/k exists, $G(k_\infty)$ is finite since $k_\infty^{ur} \subset F_\infty$. This completes the proof. $\square$

Greenberg's conjecture asserts that $G(k_\infty)$ is Fab if k is a totally real number field. As a step to this problem, we consider the finiteness of $G(k_\infty)$ when $\ell = 2$ and k is a real quadratic field. Some criteria and examples with $X(k_\infty) \simeq (2, 2) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ have been established by Mouhib and Movahhedi [12]. The purpose of this paper is to obtain further examples of finite metacyclic $G(k_\infty)$, including the case $X(k_\infty) \not\simeq (2, 2)$, by showing the following theorem.

Theorem 2. *Let k_∞ be the cyclotomic $\mathbb{Z}_2$ -extension of a real quadratic field $k = \mathbb{Q}(\sqrt{pq})$ with prime numbers $p \equiv 9 \pmod{16}$, $q \equiv 3 \pmod{4}$. Then the Galois group $G(k_\infty)$ of the maximal unramified pro-2-extension over k_∞ is a metacyclic pro-2 group of which the commutator subgroup is finite. Especially, $G(k_\infty)$ is a finite 2-group if the Iwasawa λ -invariant $\lambda_2(k)$ is zero.*

Remark. A pro- ℓ group G is called *metacyclic* if there exists a closed normal subgroup H such that both H and G/H are cyclic as pro- ℓ groups.

After proving Theorem 2, we see some criteria for the finiteness and examples.

2. PRELIMINARIES

2.1. For an additive ℓ -group A , we denote by $\text{rank } A$ the dimension of $A/\ell A$ as a $\mathbb{Z}/\ell\mathbb{Z}$ -vector space. For a finite extension $k/\mathbb{Q}$, we denote by $L(k)$ the Hilbert ℓ -class field of k and by $L'(k)$ the maximal unramified abelian ℓ -extension of k in which any prime ideal of k lying over ℓ splits completely. Let $D(k)$ be the subgroup of $A(k)$ consisting of ideal classes which contain an ideal all of whose prime factors lie over ℓ . Then $A(k) \simeq \text{Gal}(L(k)/k)$ and $A'(k) = A(k)/D(k) \simeq \text{Gal}(L'(k)/k)$.

We assume that the cyclotomic $\mathbb{Z}_\ell$ -extension k_∞/k is totally ramified at any prime ideal lying over ℓ . Fix a topological generator γ of $\Gamma = \text{Gal}(k_\infty/k)$ and identify the complete group ring $\mathbb{Z}_2[[\Gamma]]$ with the ring $\Lambda = \mathbb{Z}_2[[T]]$ of formal power series via $\gamma = 1 + T$. Then $X = X(k_\infty)$ and $X' = \varprojlim A'(k_n)$ are finitely generated Λ -modules, and there exist submodules Y and Y' such that $A(k_n) \simeq X/(\omega_n/T)Y$ and $A'(k_n) \simeq X'/(\omega_n/T)Y'$ for all $n \geq 0$, where $\omega_n = (1 + T)^{\ell^n} - 1$ (cf. [11], [16]). As a version of Fukuda's theorems [8], we obtain the following proposition.

Proposition 3. *Assume that the cyclotomic $\mathbb{Z}_\ell$ -extension k_∞/k is totally ramified at any prime ideal lying over ℓ . Then:*

- (1) *If $|A'(k_1)| = |A'(k)|$, then $A'(k_n) \simeq A'(k)$ for all $n \geq 0$.*
- (2) *If $\text{rank } A'(k_1) = \text{rank } A'(k)$, then $\text{rank } A'(k_n) = \text{rank } A'(k)$ for all $n \geq 0$.*
- (3) *Assume that only one prime ideal of k lies over ℓ . If the lifting mapping $A'(k) \rightarrow A'(k_m)$ is a zero mapping for some m , then $A'(k_n) \simeq A'(k_m)$ for all $n \geq m$.*

Proof. (1) If $|A'(k_1)| = |A'(k)|$, then $|X'/(\omega_1/T)Y'| = |X'/Y'|$ and hence $Y' = (\omega_1/T)Y' \subset (\ell, T)Y'$. Since Y' is a finitely generated Λ -module, we have $Y' = 0$ by Nakayama's lemma. Therefore $A'(k_n) \simeq X' \simeq A'(k)$ for all $n \geq 0$.

(2) If $\text{rank } A'(k_1) = \text{rank } A'(k)$, then $|X'/((\omega_1/T)Y' + \ell X')| = |A'(k_1)/\ell A'(k_1)| = |A'(k)/\ell A'(k)| = |X'/(Y' + \ell X')|$ and hence $Y' + \ell X' = (\omega_1/T)Y' + \ell X' \subset (\ell, T)Y' + \ell X'$. By applying Nakayama's lemma to $(Y' + \ell X')/\ell X'$, we have $Y' \subset \ell X'$. Therefore $A'(k_n)/\ell A'(k_n) \simeq X'/\ell X' \simeq A'(k)/\ell A'(k)$ and hence $\text{rank } A'(k_n) = \text{rank } A'(k)$ for all $n \geq 0$.

(3) Since $A'(k) \simeq \text{Gal}(L'(k)k_\infty/k_\infty) \simeq X'/TX'$ by the assumption, we have $Y' = TX'$ and $A'(k_n) \simeq X'/\omega_n X'$ for all $n \geq 0$. If the lifting mapping $A'(k) \rightarrow A'(k_m)$ is a zero mapping, the homomorphism $X'/TX' \rightarrow X'/\omega_m X' : x' \bmod TX' \mapsto (\omega_m/T)x' \bmod \omega_m X'$ is also a zero mapping by Theorem 8 of [11]. Then $(\omega_m/T)X' \subset \omega_m X' = T(\omega_m/T)X'$. By Nakayama's lemma, we have $(\omega_m/T)X' = 0$, and hence $\omega_n X' = 0$ for all $n \geq m$. Therefore $A'(k_n) \simeq X' \simeq A'(k_m)$ for all $n \geq m$. $\square$

2.2. Let us recall a part of genus theory (cf. e.g. [17]). For a finite extension $F/\mathbb{Q}$, we denote by $E(F)$ the unit group of F . Let k/F be a cyclic ℓ -extension with the Galois group $G = \text{Gal}(k/F) = \langle g \rangle$. Let $B(k)$ be the subgroup of $A(k)$ consisting of G -invariant ideal classes, and let $B'(k)$ be the subgroup of $B(k)$ consisting of ideal classes represented by G -invariant ideals. $B(k)$ and $B'(k)$ are usually called the subgroup of ambiguous ideal classes and the subgroup generated by ambiguous ideals. Then we obtain the genus formulae

$$|B(k)| = \frac{|A(F)| \prod_v e_v}{|G| |E(F)/E(F) \cap N_{k/F} k^\times|}, \quad |B'(k)| = \frac{|A(F)| \prod_v e_v}{|G| |E(F)/N_{k/F} E(k)|},$$

where v runs over all places of F , e_v is the ramification index in k/F , and $N_{k/F} : k^\times \rightarrow F^\times$ is the norm mapping. Then $|B(k)| = |A(k)/(g-1)A(k)| = |\text{Gal}(K/k)|$, where K is the genus ℓ -class field of k/F , i.e., the maximal unramified ℓ -extension of k which is abelian over F . If $\ell = |G| = 2$ and $A(F) = 0$, then $B(k) \simeq A(k)/2A(k)$ and K is the maximal unramified elementary abelian 2-extension of k . If $F = \mathbb{Q}$ and k is a real quadratic field with discriminant $d_1 d_2 \cdots d_r$, which is a product of prime discriminants $d_i \equiv 0, 1 \pmod{4}$, then the genus field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \dots, \sqrt{d_r}) \cap \mathbb{R}$.

2.3. In order to prove Theorem 2, we refer to some results from group theory. For a finite ℓ -group G and its subgroup H , we denote by $[G, H]$ the subgroup of G generated by commutators $[g, h] = g^{-1}h^{-1}gh$ ($g \in G, h \in H$). Put $G' = G_2 = [G, G]$, $G'' = [G', G']$ and $G_3 = [G, G_2]$. By referring to Theorem 1 of [4] and Theorem 2.3 of [5], we have the following proposition.

Proposition 4. (i) If $G'/G'' \simeq \mathbb{Z}/\ell^e \mathbb{Z} \oplus \mathbb{Z}/\ell^d \mathbb{Z}$ with $e \geq d \geq 0$, then $|G''|^2 \leq \ell^d$.
(ii) G is metacyclic if and only if $G/(G_2)^\ell G_3$ is metacyclic.

In the following sections, we put $\ell = 2$.

3. PROOF OF THEOREM 2

About the $\mathbb{Z}_2$ -extension $\mathbb{Q}_\infty/\mathbb{Q}$, we note that $A(\mathbb{Q}_n) = 0$ for all n and that the narrow class number of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ is 1. Then there exists a prime element $\pi_1 = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ ($x, y \in \mathbb{Z}$) lying over p which is totally positive, and the principal ideal $(\sqrt{2})$ is the unique prime ideal of $\mathbb{Q}_1$ lying over 2. Since $p = (x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2 \equiv 9 \pmod{16}$, a simple calculation shows that $\pi_1 \equiv \pm 3, \pm(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$. Note that $3 + 2\sqrt{2} = (1 + \sqrt{2})^2$ and that $z^2 \equiv 1, 3 + 2\sqrt{2} \pmod{4\sqrt{2}}$ for any $z \in \mathbb{Z}[\sqrt{2}]$ which is prime to 2. We denote by

$(\frac{2}{p})_4 = \pm 1 \equiv 2^{\frac{p-1}{4}} \pmod{p}$ the quartic residue symbol modulo p . By referring to Lemma 3.8 of [9] and Lemma 1 (2) of [13], we obtain the following lemmas.

Lemma 5. *Let z be an element of $\mathbb{Z}[\sqrt{2}]$ which is prime to 2. Then we have:*

- (i) $\mathbb{Q}_1(\sqrt{z})/\mathbb{Q}_1$ is unramified at $(\sqrt{2})$ if and only if $z \equiv 1, 3 + 2\sqrt{2} \pmod{4}$.
- (ii) $(\sqrt{2})$ splits in $\mathbb{Q}_1(\sqrt{z})/\mathbb{Q}_1$ if and only if $z \equiv 1, 3 + 2\sqrt{2} \pmod{4\sqrt{2}}$.

Lemma 6. *There exists a quadratic extension of $\mathbb{Q}_1$ unramified outside π_1 if and only if $(\frac{2}{p})_4 \neq 1$.*

By the genus theory, the genus field of $k/\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, and hence $\text{rank } A(k) = 1$. Since $K \subset L'(k)$, we have $\text{rank } A'(k) = 1$. Note that $K_n = K\mathbb{Q}_n$ is an unramified quadratic extension of k_n for all n . For $k_1 = k(\sqrt{2})$, $\text{rank } A(k_1) = 2$ by Théorème 1 of [1]. Since the norm mapping $N_{k_n/k_1} : A(k_n) \rightarrow A(k_1)$ is surjective, we have $\text{rank } A(k_n) \geq 2$ for all $n \geq 1$.

Lemma 7. *If $q \equiv 3 \pmod{8}$, then $\text{rank } A(k_n) = 2$ for all $n \geq 1$.*

Proof. By the genus formula for $\mathbb{Q}_n/\mathbb{Q}_1$, we have $|E(\mathbb{Q}_1)/N_{\mathbb{Q}_n/\mathbb{Q}_1}E(\mathbb{Q}_n)| = 1$. Since $q \equiv 3 \pmod{8}$, the number of ramified primes in $k_n/\mathbb{Q}_n$ is 4 for all $n \geq 1$. Put $\mathfrak{E}_n = E(\mathbb{Q}_n)/E(\mathbb{Q}_n) \cap N_{k_n/\mathbb{Q}_n}k_n^\times$. Since $N_{\mathbb{Q}_n/\mathbb{Q}_1} : \mathfrak{E}_n \rightarrow \mathfrak{E}_1$ is surjective, we have

$$|A(k_n)/2A(k_n)| = \frac{2^3}{|\mathfrak{E}_n|} \leq \frac{2^3}{|\mathfrak{E}_1|} = |A(k_1)/2A(k_1)| = 2^2$$

by the genus formulae for $k_n/\mathbb{Q}_n$. Therefore $\text{rank } A(k_n) = 2$ for all $n \geq 1$. $\square$

Lemma 8. *If $(\frac{2}{p})_4 \neq 1$ or $q \equiv 7 \pmod{8}$, then $\text{rank } A'(k_n) = 1$, $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ and $A(k_n) \simeq A'(k_n) \oplus D(k_n)$ as abelian groups for all $n \geq 1$.*

Proof. First, we assume that $(\frac{2}{p})_4 \neq 1$. By Lemma 6, there exists a quadratic extension $\mathbb{Q}_1(\sqrt{z})/\mathbb{Q}_1$ unramified outside π_1 , where $z \in (-1)^{\mathbb{Z}}(1 + \sqrt{2})^{\mathbb{Z}}\pi_1^{\mathbb{Z}}$. Since $\mathbb{Q}_1(\sqrt{z})$ is totally real, we have $z \in \pi_1(\mathbb{Q}_1^\times)^2$. Then $\mathbb{Q}_1(\sqrt{z}) = \mathbb{Q}_1(\sqrt{\pi_1})$. Since $\mathbb{Q}_1(\sqrt{\pi_1})/\mathbb{Q}_1$ is unramified at $(\sqrt{2})$, we have $\pi_1 \equiv 1, 3 + 2\sqrt{2} \pmod{4}$ by Lemma 5 (i), and hence $\pi_1 \equiv -3, -(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$. By Lemma 5 (ii), $(\sqrt{2})$ is inert in $\mathbb{Q}_1(\sqrt{\pi_1})/\mathbb{Q}_1$. Then $K_1(\sqrt{\pi_1})/k_1$ is an unramified $(2, 2)$ -extension which is not contained in $L'(k_1)$. Since $\text{rank } A(k_1) = 2$, we have $\text{rank } A'(k_1) = 1$ and $D(k_1) \neq 0$. By Proposition 3 (2), we have $\text{rank } A'(k_n) = 1$ for all n . Since $k_n/\mathbb{Q}_n$ is ramified at the unique prime ideal lying over 2 and $N_{k_n/k_1} : D(k_n) \rightarrow D(k_1)$ is surjective, we have $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$. Therefore $\text{rank } A(k_n) = 2$ and $A(k_n) \simeq A'(k_n) \oplus D(k_n)$ as abelian groups for all $n \geq 1$.

Second, we assume that $(\frac{2}{p})_4 = 1$ and $q \equiv 7 \pmod{8}$. By Lemma 6, $\mathbb{Q}_1(\sqrt{\pi_1})/\mathbb{Q}_1$ is ramified at $(\sqrt{2})$. Since $\pi_1 \not\equiv 1, 3 + 2\sqrt{2} \pmod{4}$ by Lemma 5 (i), $\pi_1 \equiv 3, 1 + 2\sqrt{2} \pmod{4\sqrt{2}}$. Then $\pi_1 q \equiv 1, 3 + 2\sqrt{2} \pmod{4}$ and $\pi_1 q \not\equiv 1, 3 + 2\sqrt{2} \pmod{4\sqrt{2}}$. By Lemma 5 (ii), $(\sqrt{2})$ is inert in $\mathbb{Q}_1(\sqrt{\pi_1 q})/\mathbb{Q}_1$. Then $K_1(\sqrt{\pi_1 q})/k_1$ is an unramified $(2, 2)$ -extension which is not contained in $L'(k_1)$. This implies that $\text{rank } A'(k_1) = 1$ and $D(k_1) \neq 0$. By Proposition 3 (2), $\text{rank } A'(k_n) = 1$. Further, $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$. Therefore $A(k_n) \simeq A'(k_n) \oplus D(k_n)$ for all $n \geq 1$. $\square$

Lemma 9. *If $(\frac{2}{p})_4 = 1$, then $G(k_\infty)$ is an abelian metacyclic pro-2 group.*

Proof. Let σ, τ be the generator of $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{p}))$, $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{q}))$ respectively. Then $\text{Gal}(K_n/k_n) = \langle \sigma\tau \rangle$. Since $A(\mathbb{Q}_n(\sqrt{q})) = 0$ (cf. [14]), τ acts on $A(K_n)$ as -1 . Since $(\frac{2}{p})_4 = 1$, $A(\mathbb{Q}_n(\sqrt{p})) = 0$ by Theorem (1) of [14]. Then σ also acts on $A(K_n)$ as -1 , and hence $\sigma\tau$ acts on $A(K_n)$ trivially. This yields that $L(K_n) = L(k_n)$. Since $\text{rank } A(k_n) = 2$ by Lemma 7 and Lemma 8, $G(k_n)$ is abelian by Proposition 7 of [3]. Therefore $G(k_\infty) \simeq X(k_\infty)$, which is an abelian metacyclic pro-2 group. $\square$

By Lemma 9, it suffices to consider the case that $(\frac{2}{p})_4 \neq 1$ in the following. Now we assume that $(\frac{2}{p})_4 \neq 1$ and $n \geq 1$. By Lemma 8, $\text{rank } A'(k_n) = 1$, $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ and $A(k_n) \simeq A'(k_n) \oplus D(k_n)$. Let $L^2(k_n) = L(L(k_n))$ be the maximal unramified metabelian 2-extension of k_n . Put $G = \text{Gal}(L^2(k_n)/k_n)$, $H = \text{Gal}(L^2(k_n)/K_n)$ and $G_2 = [G, G]$, $G_3 = [G, G_2]$. Then G is the maximal metabelian quotient of $G(k_n)$. Since $G/G_2 = \text{Gal}(L(k_n)/k_n) \simeq A(k_n)$ and $K_n \subset L'(k_n)$, G has the generators a, b such that $\langle bH \rangle = G/H$ and $\langle aG_2 \rangle = \text{Gal}(L(k_n)/L'(k_n)) \simeq D(k_n)$. Then we have

$$[a, b^2] \equiv [a, b]^2 \equiv [a^2, b] \equiv 1 \pmod{G_3}.$$

This implies that $G_2/G_3 = \langle [a, b]G_3 \rangle$ has the order at most 2 and that H/G_3 is an abelian quotient of $H = \langle a, b^2, [a, b], G_3 \rangle$. Since $\text{rank } A'(k_n) = 1$ and $K_n \subset L'(k_n)$, we have $L'(K_n) = L'(k_n)$. Hence the surjective homomorphism $A(K_n) \rightarrow H/G_3$ induces a surjective homomorphism $D(K_n) \rightarrow \langle a, G_2 \rangle/G_3$. Then $D(K_n) \neq 0$ and there is an exact sequence

$$D(K_n) \rightarrow G/G_3 \rightarrow A'(k_n) \rightarrow 1.$$

Since $A(\mathbb{Q}_n(\sqrt{q})) = 0$ (cf. [14]) and the unique prime ideal of $\mathbb{Q}_n(\sqrt{q})$ lying over 2 splits in $K_n/\mathbb{Q}_n(\sqrt{q})$, $D(K_n)$ is a cyclic group. Therefore G/G_3 is a metacyclic 2-group and hence G is a metacyclic 2-group by Proposition 4 (ii). Since $G_2 = \text{Gal}(L^2(k_n)/L(k_n))$ is cyclic, then $\text{Gal}(k_n^{ur}/L(k_n))$ is also cyclic. Thus $k_n^{ur} = L^2(k_n)$ and $G = G(k_n)$. Since $G(k_n)$ is metacyclic for all $n \geq 1$, $G(k_\infty)$ is a metacyclic pro-2 group (cf. [6], Chapter 3, Exercise 10).

$$\begin{array}{ccccccccccccccc} \mathbb{Q} & \longrightarrow & k_n & \longrightarrow & K_n & \longrightarrow & L'(K_n) & \longrightarrow & L(k_n) & \longrightarrow & \cdot & \longrightarrow & L(K_n) & \longrightarrow & L^2(k_n) = k_n^{ur} \\ & & & & & & & & & & & & & & \\ & & & & & & A(K_n) & \longrightarrow & D(K_n) & \longrightarrow & \cdot & \longrightarrow & \cdot & \longrightarrow & 0 \\ \mathfrak{G} & \longrightarrow & G & \longrightarrow & H = \mathfrak{G}' & \longrightarrow & \langle a, G_2 \rangle & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & \mathfrak{G}'' & \longrightarrow & 1 \end{array}$$

FIGURE 1

Since $H = G(K_n)$ is also metacyclic for all $n \geq 1$, $A(K_n) \simeq \mathbb{Z}/2^{e_n}\mathbb{Z} \oplus \mathbb{Z}/2^{d_n}\mathbb{Z}$ with some $e_n \geq d_n \geq 0$. Since Leopoldt's conjecture holds for the abelian extension $K/\mathbb{Q}$, $\varprojlim D(K_n)$ is finite by Proposition 1 of [10]. Put $2^d = |\varprojlim D(K_n)|$. Since $L'(K_n) = L'(k_n)$, $\text{rank } A'(K_n) \leq 1$. We now assume that d_n is unbounded as $n \rightarrow \infty$. Then, since $|A'(K_n)|$ is unbounded as $n \rightarrow \infty$, we have $\varprojlim A'(K_n) \simeq \mathbb{Z}_2$ as a $\mathbb{Z}_2$ -module and $\text{Tor}_{\mathbb{Z}_2} X(K_\infty) = \varprojlim D(K_n)$. Since $2^d X(K_\infty) \simeq \mathbb{Z}_2$, $2^d A(K_n)$ is cyclic for all n . This is a contradiction. Therefore d_n is bounded as $n \rightarrow \infty$.

Lemma 10. K_n is the maximal subfield of k_n^{ur} which is abelian over $\mathbb{Q}$.

Proof. Let F_n be the maximal subfield of k_n^{ur} which is abelian over $\mathbb{Q}$. Then $K_n \subset F_n \subset L(k_n)$ and F_n/k is abelian. Let F be the inertia subfield of the unique prime ideal of k lying over 2 in F_n/k . Then $F_n = Fk_n$, and F is an unramified 2-extension of k which is abelian over $\mathbb{Q}$. Thus $F \subset K$, and hence $F_n = Fk_n \subset Kk_n = K_n$. Therefore $F_n = K_n$. $\square$

Now we consider the finite 2-group $\mathfrak{G} = \text{Gal}(k_n^{ur}/\mathbb{Q})$ for $n \geq 1$. Put $\mathfrak{G}' = [\mathfrak{G}, \mathfrak{G}]$ and $\mathfrak{G}'' = [\mathfrak{G}', \mathfrak{G}']$. Since $\mathfrak{G}' = \text{Gal}(k_n^{ur}/K_n)$ by Lemma 10, we have $\mathfrak{G}'/\mathfrak{G}'' \simeq A(K_n)$ and $G_2/\mathfrak{G}'' = \text{Gal}(L(K_n)/L(k_n))$. By Proposition 4 (i), $|\mathfrak{G}''|^2 \leq 2^{d_n}$. The exact sequence

$$1 \rightarrow \mathfrak{G}'' \rightarrow G_2 \rightarrow D(K_n)$$

yields that the order of the commutator subgroup G_2 of $G(k_n)$ is bounded as $n \rightarrow \infty$. Therefore the commutator subgroup of $G(k_\infty)$ is finite. This completes the proof of Theorem 2.

4. CRITERIA

In this section we give some criteria for the finiteness and the structure of $G(k_\infty)$. We denote by $\left(\frac{p}{q}\right)$ the quadratic residue symbol and put $k^\vee = \mathbb{Q}(\sqrt{2pq})$.

Proposition 11. *The following hold under the assumption of Theorem 2:*

- (i) *If $\left(\frac{p}{q}\right) = 1$, then $X(k_\infty) \not\simeq (2, 2)$.*
- (ii) *Assume that $\left(\frac{p}{p}\right)_4 \neq 1$ and $n \geq 1$. Then $G(k_n)$ is abelian if and only if $|A(\mathbb{Q}_n(\sqrt{p}))| = 2$ and the lifting mapping $A(\mathbb{Q}_n(\sqrt{p})) \rightarrow A(K_n)$ is a zero mapping.*
- (iii) *Assume that $\left(\frac{p}{p}\right)_4 \neq 1$ or $q \equiv 7 \pmod{8}$. If $\left(\frac{p}{q}\right) = -1$, then $G(k_\infty)$ is a finite 2-group with $X(k_\infty) \simeq (2, 2)$.*
- (iv) *Assume that $\left(\frac{p}{p}\right)_4 \neq 1$ or $q \equiv 7 \pmod{8}$. If $D(k) = 0$ or $D(k^\vee) = 0$, then $G(k_\infty)$ is finite.*

Proof. (i) By Théorème 2 of [2], $A(k_1) \simeq (2, 2)$ if and only if $\left(\frac{p}{q}\right) = -1$. By Théorème 1 of [1], $\text{rank } A(k_1) = 2$. Since the natural mapping $X(k_\infty) \rightarrow A(k_1)$ is surjective, we have the claim.

(ii) In the proof of Lemma 8, we have seen that $(\sqrt{2})$ is inert in $\mathbb{Q}_1(\sqrt{\pi_1})/\mathbb{Q}_1$. Then $\mathbb{Q}_n(\sqrt{p}, \sqrt{\pi_1})/\mathbb{Q}_n(\sqrt{p})$ is an unramified extension which is not contained in $L'(\mathbb{Q}_n(\sqrt{p}))$. Therefore $D(\mathbb{Q}_n(\sqrt{p})) \not\subset 2A(\mathbb{Q}_n(\sqrt{p}))$. The genus formula for $\mathbb{Q}_n(\sqrt{p})/\mathbb{Q}_n$ yields that

$$|A(\mathbb{Q}_n(\sqrt{p}))/2A(\mathbb{Q}_n(\sqrt{p}))| = \frac{2}{|E(\mathbb{Q}_n)/E(\mathbb{Q}_n) \cap N_{\mathbb{Q}_n(\sqrt{p})/\mathbb{Q}_n} \mathbb{Q}_n(\sqrt{p})^\times|} \leq 2.$$

Then $\text{rank } A(\mathbb{Q}_n(\sqrt{p})) = 1$ and hence $A(\mathbb{Q}_n(\sqrt{p})) = D(\mathbb{Q}_n(\sqrt{p})) \neq 0$. On the other hand, in the proof of Theorem 2 we have seen that $L'(K_n) = L'(k_n)$ and $|D(k_n)| = 2$. By Proposition 7 of [3], $G(k_n)$ is abelian if and only if $|D(K_n)| = 2$. Since $K_n/\mathbb{Q}_n(\sqrt{p})$ is ramified at a prime ideal lying over 2, we have $2 \leq |D(\mathbb{Q}_n(\sqrt{p}))| \leq |D(K_n)| \leq 2|D(\mathbb{Q}_n(\sqrt{p}))|$. The equality $|D(K_n)| = 2|D(\mathbb{Q}_n(\sqrt{p}))|$ holds if and only if the lifting mapping $D(\mathbb{Q}_n(\sqrt{p})) \rightarrow D(K_n)$ is injective. If $G(k_n)$ is abelian, $|D(K_n)| = |D(\mathbb{Q}_n(\sqrt{p}))| = 2$, and hence the mapping $D(\mathbb{Q}_n(\sqrt{p})) \rightarrow D(K_n)$ is a zero mapping. Conversely, if $|D(\mathbb{Q}_n(\sqrt{p}))| = 2$ and the mapping $D(\mathbb{Q}_n(\sqrt{p})) \rightarrow D(K_n)$ is a zero mapping (i.e., not injective), we have $|D(K_n)| = |D(\mathbb{Q}_n(\sqrt{p}))|$, and hence $|D(K_n)| = 2$. Then $G(k_n)$ is abelian.

(iii) By Lemma 8, $A(k_n) \simeq A'(k_n) \oplus D(k_n)$ and $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$. If $(\frac{p}{q}) = -1$, then $A(k_1) \simeq (2, 2)$ by Théorème 2 of [2], and hence $A'(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$. Since $N_{k_1/k} : A'(k_1) \rightarrow A'(k)$ is surjective and $\text{rank } A'(k) = 1$, then $A'(k) \simeq \mathbb{Z}/2\mathbb{Z}$. By Proposition 3 (1), we have $A'(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$. Therefore $A(k_n) \simeq (2, 2)$ for all $n \geq 1$. This yields that $X(k_\infty) \simeq (2, 2)$.

(iv) Since k_∞/k is ramified at only one prime ideal of k which is totally ramified, we have $A(k) \simeq X/TX$, i.e., $Y = TX$. Therefore $A(k_n) \simeq X/\omega_n X$ for all n . Assume that $G(k_\infty)$ is infinite. By Lemma 8, $D = \varprojlim D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ and $X' \simeq X/D \simeq \Lambda/(T - \alpha)$ with some $\alpha \in 2\mathbb{Z}_2$. Since $A(k_n)$ is finite, $T - \alpha$ is prime to ω_n for all $n \geq 0$. Let $a_0 \in \text{Ker } \iota_n$ be an arbitrary element of the kernel of the lifting mapping $\iota_n : A(k) \rightarrow A(k_n)$ for $n \geq 1$, and let $x_0 \bmod TX$ be the corresponding element of X/TX . By Theorem 7 of [11], $(\omega_n/T)x_0 \in \omega_n X$, i.e., $\omega_n(x_0 - Tx'_0) = 0$ with some $x'_0 \in X$. Then $x_0 - Tx'_0 \in D$, and hence $x_0 \bmod TX \in (D + TX)/TX$. This implies that $a_0 \in D(k)$. Since $\iota_1(D(k)) = 0$, we have $D(k) = \text{Ker } \iota_n$. Now, we choose n such that $2^{n-1} \geq |A(k)|$. If $D(k_n) \subset \iota_n(A(k))$, we have $D(k_1) = N_{k_n/k_1} D(k_n) \subset N_{k_n/k_1} \iota_n(A(k)) = \iota_1(2^{n-1} A(k)) = 0$. This is a contradiction. Therefore $D(k_n) \not\subset \iota_n(A(k))$. Then the genus formula for k_n/k yields that

$$2|A'(k)| = |\iota_n(A(k))D(k_n)| \leq \frac{|A(k)|}{|E(k)/N_{k_n/k}E(k_n)|} \leq |A(k)|.$$

This implies that $D(k) \neq 0$. By the same arguments for the $\mathbb{Z}_2$ -extension $k_\infty/k^\vee$, we have that $D(k^\vee) \neq 0$ if $G(k_\infty)$ is infinite. This completes the proof. $\square$

Remarks. (1) The finiteness of $X(k_\infty)$ in case (iii) has been proved in [9] and [13].

(2) If $(\frac{p}{q}) = -1$, then $G(k_1) \simeq (2, 2)$ by Théorème 6 of [2]. (See (ii) in *Preuve*.)

5. EXAMPLES

By using `bnfinit`(,1,[0.3,12,4]) (and `bnfcertify`, `bnfisprincipal`, etc.) on a PARI/GP calculator ver.2.3.4 [15], we have the following examples. The notation $[\dots]$ means an abelian group of such type as the output of the calculator.

First, we put $p = 41$, which satisfies $(\frac{2}{p})_4 \neq 1$ and $A(\mathbb{Q}_2(\sqrt{p})) \simeq [4]$. By Proposition 11 (ii), $G(k_n)$ is not abelian for all $n \geq 2$.

(a1) For $q = 23$ which satisfies $(\frac{p}{q}) = 1$, we have $A(k^\vee) \simeq [4]$ and $D(k^\vee) \simeq [] = 0$. Then $G(k_\infty)$ is finite by Proposition 11 (iv). Further we have $A(k_1) \simeq [4, 2]$, and therefore $A'(k^\vee) \simeq A'(k_1) \simeq \mathbb{Z}/4\mathbb{Z}$ by Lemma 8. By applying Proposition 3 (1) to the $\mathbb{Z}_2$ -extension $k_\infty/k^\vee$ we have $A'(k_n) \simeq \mathbb{Z}/4\mathbb{Z}$ for all $n \geq 1$, and hence $G(k_\infty)$ is a finite nonabelian metacyclic 2-group with $X(k_\infty) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(a2) If $q = 43$, we cannot apply Proposition 11 (iv) since $D(k) \simeq D(k^\vee) \simeq [2]$. However, we have $A(k_1) \simeq A(k_2) \simeq [8, 2]$. Therefore $G(k_\infty)$ is a finite nonabelian metacyclic 2-group with $X(k_\infty) \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ by applying Proposition 3 (1) to the $\mathbb{Z}_2$ -extension k_∞/k_1 .

We now prepare the following lemma for the convenience of the calculation.

Lemma 12. *Let $[\mathfrak{p}_1]$ (resp. $[\mathfrak{q}_1]$) $\in A(k_1)$ be the ideal class of a prime ideal $\mathfrak{p}_1$ (resp. $\mathfrak{q}_1$) of k_1 lying over p (resp. q). If $(\frac{2}{p})_4 = 1$, $(\frac{p}{q}) = -1$ and $q \equiv 3 \pmod{8}$, then $A(k_1) = \langle [\mathfrak{p}_1], [\mathfrak{q}_1] \rangle \simeq (2, 2)$ and $D(k_1) = 0$.*

Proof. Since $\text{Gal}(L(k_1)/k_1) \simeq A(k_1) \simeq (2, 2)$ by Théorème 2 of [2], $\text{Gal}(L(k_1)/k)$ is the dihedral group of order 8. Since $(\frac{p}{q}) = -1$, $\mathfrak{p}_1$ is inert in K_1/k_1 , and any prime

ideal of $k(\sqrt{2p})$ lying over q is inert in $K_1/k(\sqrt{2p})$. Since $\text{Gal}(L(k_1)/K) \simeq (2, 2)$, $L(k_1)/k(\sqrt{2p})$ is an unramified cyclic extension of degree 4 in which any prime ideal lying over q does not split. Then any prime ideal of K_1 lying over q is inert in $L(k_1)/K_1$, and hence K_1 is the decomposition subfield of $\mathfrak{q}_1$ in $L(k_1)/k_1$. Therefore $A(k_1) = \langle [\mathfrak{p}_1], [\mathfrak{q}_1] \rangle$. Since $\mathbb{Q}_1(\sqrt{\pi_1})/\mathbb{Q}_1$ is ramified at $(\sqrt{2})$ by Lemma 6, we have $\pi_1 \equiv 3, 1 + 2\sqrt{2} \pmod{4\sqrt{2}}$ by Lemma 5 (i). Since $\pi_1 q \equiv 1, 3 + 2\sqrt{2} \pmod{4\sqrt{2}}$, $(\sqrt{2})$ splits in $\mathbb{Q}_1(\sqrt{\pi_1 q})/\mathbb{Q}_1$ by Lemma 5 (ii). Then $K_1(\sqrt{\pi_1 q})/k_1$ is an unramified $(2, 2)$ -extension in which the prime ideal lying over 2 splits completely. This yields that $L(k_1) = K_1(\sqrt{\pi_1 q}) = L'(k_1)$ and $A'(k_1) \simeq A(k_1)$. $\square$

Second, we put $p = 73$, which satisfies $(\frac{2}{p})_4 = 1$. Then $G(k_\infty)$ is abelian by Lemma 9.

(b1) For $q = 223 \equiv 7 \pmod{8}$, we have $A(k^\vee) \simeq [8]$ and $D(k^\vee) \simeq []$. Then $G(k_\infty)$ is finite by Proposition 11 (iv). Further we have $A(k_1) \simeq [8, 2]$, and hence $A'(k_n) \simeq \mathbb{Z}/8\mathbb{Z}$ for all $n \geq 1$ similarly to (a1). Therefore $G(k_\infty) \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(b2) For $q = 11 \equiv 3 \pmod{8}$ which satisfies $(\frac{2}{q}) = -1$, we have $A(k_2) \simeq [4, 2]$ and $D(k_2) \simeq [2]$. By this results and Lemma 12, $A'(k_1) \simeq A'(k_2) \simeq (2, 2)$ and $D(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 2$. By applying Proposition 3 (1) to the $\mathbb{Z}_2$ -extension k_∞/k_1 , we have $A'(k_n) \simeq (2, 2)$ for all $n \geq 1$, and hence $G(k_\infty) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

(b3) For $q = 43 \equiv 3 \pmod{8}$ which satisfies $(\frac{2}{q}) = -1$, we have $A(k_2) \simeq [4, 4]$ and $\text{Im}(A(k_1) = \langle [\mathfrak{p}_1], [\mathfrak{q}_1] \rangle \rightarrow A(k_2)) = D(k_2) \simeq [2]$, i.e., $\text{Im}(A'(k_1) \rightarrow A'(k_2)) \simeq []$. Then $A'(k_n) \simeq A'(k_2)$ for all $n \geq 2$ by applying Proposition 3 (3) for k_∞/k_1 . This implies that $A(k_n) \simeq A(k_2)$ for all $n \geq 2$, and hence $G(k_\infty) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Finally, we put $(p, q) = (89, 139)$, which satisfies $(\frac{2}{p})_4 = 1$, $(\frac{2}{q}) = 1$ and $q \equiv 3 \pmod{8}$. Then $A(k_1) \simeq A(k_2) \simeq [8, 4]$. By Theorem 1 (1) of [8], we have $G(k_\infty) \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

TABLE 1. Examples

	p $(\frac{2}{p})_4$	q $\pmod{8}$	$A(k)$ $D(k)$	$A(k^\vee)$ $D(k^\vee)$	$A(k_1)$ $D(k_1)$	$A(k_2)$ $D(k_2)$	$X(k_\infty)$ $G(k_\infty)$
(a1)	41 -1	23 $\equiv 7$	- 1	[4] []	[4, 2] $\mathbb{Z}/2\mathbb{Z}$	- $\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ nonabelian
(a2)	41 -1	43 $\equiv 3$	[4] [2]	[8] [2]	[8, 2] $\mathbb{Z}/2\mathbb{Z}$	[8, 2] $\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ nonabelian
(b1)	73 1	223 $\equiv 7$	- 1	[8] []	[8, 2] $\mathbb{Z}/2\mathbb{Z}$	- $\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ abelian
(b2)	73 1	11 $\equiv 3$	- -1	- -	(2, 2) 0	[4, 2] [2]	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ abelian
(b3)	73 1	43 $\equiv 3$	- -1	- -	(2, 2) 0	[4, 4] [2]	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ abelian
	89 1	139 $\equiv 3$	- 1	- -	[8, 4] -	[8, 4] -	$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ abelian

ACKNOWLEDGEMENT

The author thanks the referee for valuable comments and suggestions for the improvement of this paper.

REFERENCES

1. A. Azizi and A. Mouhib, *Sur le rang du 2-groupe de classes de $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou un premier $p \equiv 1 \pmod{4}$* , Trans. Amer. Math. Soc. **353** (2001), no. 7, 2741–2752. MR1828471 (2002b:11152)
2. A. Azizi and A. Mouhib, *Capitulation des 2-classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{d})$ où d est un entier naturel sans facteurs carrés*, Acta Arith. **109** (2003), no. 1, 27–63. MR1980850 (2004f:11121)
3. 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. MR1658015 (2000c:11179)
4. N. Blackburn, *On prime-power groups in which the derived group has two generators*, Proc. Cambridge Philos. Soc. **53** (1957), 19–27. MR0081904 (18:464f)
5. N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. **54** (1958), 327–337. MR0102557 (21:1348)
6. 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. MR1720368 (2000m:20039)
7. 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. MR528968 (81a:12005)
8. T. Fukuda, *Remarks on $\mathbb{Z}_p$ -extensions of number fields*, Proc. Japan Acad. Ser. A **70** (1994), 264–266. MR1303577 (96e:11135)
9. T. Fukuda and K. Komatsu, *On the Iwasawa λ -invariant of the cyclotomic $\mathbb{Z}_2$ -extension of a real quadratic field*, Tokyo J. Math. **28** (2005), no. 1, 259–264. MR2149635 (2006b:11134)
10. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284. MR0401702 (53:5529)
11. K. Iwasawa, *On $\mathbb{Z}_l$ -extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326. MR0349627 (50:2120)
12. A. Mouhib and A. Movahhedi, *On the p -class tower of a $\mathbb{Z}_p$ -extension*, Tokyo J. Math. **31** (2008), no. 2, 321–332. MR2477874
13. Y. Nishino, *On the Iwasawa invariants of the cyclotomic $\mathbb{Z}_2$ -extensions of certain real quadratic fields*, Tokyo J. Math. **29** (2006), no. 1, 239–245. MR2258282 (2007g:11141)
14. 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. MR1484637 (99a:11122)
15. The Pari Group, *PARI/GP*, Bordeaux, 2008, <http://pari.math.u-bordeaux.fr/>.
16. L. C. Washington, *Introduction to Cyclotomic Fields (2nd Edition)*, Graduate Texts in Math. **83**, Springer, 1997. MR1421575 (97h:11130)
17. H. Yokoi, *On the class number of a relatively cyclic number field*, Nagoya Math. J. **29** (1967), 31–44. MR0207681 (34:7496)

DEPARTMENT OF MATHEMATICS, NAGOYA INSTITUTE OF TECHNOLOGY, GOKISO, SHOWA, NAGOYA, AICHI, 466-8555 JAPAN

E-mail address: mizusawa.yasushi@nitech.ac.jp