ACTA ARITHMETICA
119.1 (2005)

On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields II

by

YASUSHI MIZUSAWA (Tokyo)

1. Introduction. Let k be a number field, and denote by $\mathcal{L}(k)$ the maximal unramified pro-2-extension of k. The fixed field $L(k)$ of the commutator subgroup of the Galois group $\mathrm{Gal}(\mathcal{L}(k)/k)$ is the maximal unramified abelian pro-2-extension of k. In particular, if k is a finite extension of the field $\mathbb{Q}$ of rational numbers, then $L(k)$ is the Hilbert 2-class field of k and the Galois group $\mathrm{Gal}(L(k)/k)$ is isomorphic to $A(k)$, the 2-Sylow subgroup of the ideal class group of k. For a finite extension k of $\mathbb{Q}$, the Hilbert 2-class field tower of k is the sequence of the fixed fields associated to the derived series of $\mathrm{Gal}(\mathcal{L}(k)/k)$. Concerning the capitulation theorem etc., the structure of the Galois group $\mathrm{Gal}(\mathcal{L}(k)/k)$ has more information on ideals. By the theorems of Golod–Shafarevich type, the group $\mathrm{Gal}(\mathcal{L}(k)/k)$ can be infinite. On the other hand, various finite 2-groups appear as the Galois groups $\mathrm{Gal}(\mathcal{L}(k)/k)$ for quadratic fields k (cf. [3], [4], [5], [10], etc.).

Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of a finite extension k of $\mathbb{Q}$. For each positive integer n, there is a unique cyclic extension k_n/k of degree 2^n contained in k_∞, which is called the nth *layer* of k_∞/k. We shall consider the Galois group

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

of the maximal unramified pro-2-extension of k_∞. The maximal abelian quotient group $G^{\mathrm{ab}} \simeq \mathrm{Gal}(L(k_\infty)/k_\infty)$ is isomorphic to the Iwasawa module $X = \varprojlim A(k_n)$, the inverse limit with respect to the norm mappings. Let $\lambda(k)$, $\mu(k)$, $\nu(k)$ be the Iwasawa invariants satisfying Iwasawa's formula

$$\#A(k_n) = 2^{\lambda(k)n+\mu(k)2^n+\nu(k)}$$

for all sufficiently large n. Greenberg's conjecture [8] asserts that $\lambda(k) = \mu(k) = 0$, i.e., the Iwasawa module $X \simeq G^{\mathrm{ab}}$ is finite for any totally real

2000 *Mathematics Subject Classification*: Primary 11R23.
Key words and phrases: $\mathbb{Z}_2$-extension, class field tower, real quadratic field.
The author was supported by JSPS Research Fellowships for Young Scientists.

number field k. This implies that if k is totally real, then $\lambda(K)=\mu(K)=0$ for any subfield K of $\mathcal{L}(k_\infty)$, i.e., the maximal abelian quotient of any open subgroup of G is finite. Then, under the assumption that Greenberg's conjecture holds, the derived series of the Galois group G for a totally real number field k also has finite factors. Further, we can also see that the Galois group G becomes finite if and only if there is a finite extension K of k with $\lambda(K)=\mu(K)=\nu(K)=0$ (cf. [14]).

In a previous paper [14], we constructed an infinite family of k such that the Galois group G is a finite non-abelian 2-group with the maximal abelian quotient of type $(2,2)$, and gave a few examples. In this paper, we shall consider more precisely the structure of the Galois groups G and $\mathrm{Gal}(\mathcal{L}(k_n)/k_n)$ for such real quadratic fields k.

2. Main results. Our first result is a refinement of the main theorem of [14].

Theorem 1. *Let p_1, p_2, q be prime numbers such that*

$$p_1 \equiv p_2 \equiv 5 \pmod 8, \qquad q \equiv 3 \pmod 4, \qquad \left(\frac{p_1p_2}{q}\right) = -1,$$

where $\left(\frac{*}{*}\right)$ is Legendre's symbol. Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of the real quadratic field $k=\mathbb{Q}(\sqrt{p_1p_2q})$. Then the Galois group $G=\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$ of the maximal unramified pro-2-extension of k_∞ is isomorphic to a dihedral group D_{2^m} with finite order $2^m \geq 8$ or a generalized quaternion group Q_{2^m} with finite order $2^m \geq 16$. Furthermore, if $\left(\frac{p_2}{p_1}\right)=1$ and the absolute norm of the fundamental unit of $\mathbb{Q}(\sqrt{p_1p_2})$ is positive, then G is isomorphic to the Galois group $\mathrm{Gal}(\mathcal{L}(k)/k)$ of the 2-class field tower of k, which is isomorphic to a dihedral group D_{2^m} of order $2^m \geq 8$ such that 2^{m-2} is the 2-part of the class number of $\mathbb{Q}(\sqrt{p_1p_2})$.

For the real quadratic fields $k=\mathbb{Q}(\sqrt{p_1p_2q})$ satisfying the assumption of the latter half of Theorem 1, we also know the order of the Galois group G by computing the class number of $\mathbb{Q}(\sqrt{p_1p_2})$. For example, $G \simeq D_8$, D_{16}, D_{32}, D_{512} for the triples $(p_1,p_2,q)=(5,61,3)$, $(5,181,3)$, $(29,181,3)$, $(1061,3821,7)$, respectively. However, we have no example of $k=\mathbb{Q}(\sqrt{p_1p_2q})$ in Theorem 1 such that $G \simeq Q_{2^m}$. It is not even known whether G in Theorem 1 can be isomorphic to Q_{2^m} or not. On the other hand, by dealing with other real quadratic fields, we have the following theorem.

Theorem 2. *Let p_1, p_2 be prime numbers such that*

$$p_1 \equiv 1,\ p_2 \equiv 5 \pmod 8, \qquad \left(\frac{p_2}{p_1}\right) = -1, \qquad \left(\frac{2}{p_1}\right)_4 = (-1)^{(p_1-1)/8},$$

where $\left(\frac{*}{*}\right)$ is Legendre's symbol and $\left(\frac{*}{*}\right)_4$ is the 4th power residue symbol. Let k_∞/k be the cyclotomic $\mathbb{Z}_2$-extension of the real quadratic field $k=$

$\mathbb{Q}(\sqrt{p_1p_2})$, *and* k_n *its nth layer. Assume that the following conditions are satisfied*:

(C1) *The* (*unique*) *prime ideal of* $\mathbb{Q}(\sqrt{2p_1}, \sqrt{p_2})$ *above* 2 *is not principal.*
(C2) *The class number of* $k_2 = k(\cos(2\pi/16))$ *is not divisible by* 8.

Then the Galois group $G = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$ *of the maximal unramified pro-2-extension* $\mathcal{L}(k_\infty)/k_\infty$ *is isomorphic to a generalized quaternion group* Q_{2^m} *of order* $2^m \geq 8$ *such that* 2^m *is the* 2*-part of the class number of* $\mathbb{Q}(\sqrt{2p_1}, \sqrt{p_2})$.

For some pairs (p_1, p_2) satisfying the first assumption of Theorem 2, we can calculate whether conditions (C1) and (C2) hold or not, and find $\#A(\mathbb{Q}(\sqrt{2p_1}, \sqrt{p_2}))$ by using the computer software "PARI/GP calculator ver. 2.1.3". It turns out that several pairs do not satisfy either (C1) or (C2). But, assuming the GRH (Generalized Riemann Hypothesis) for k_2, we can see that $G \simeq Q_{16}$, Q_8, Q_{32} for the pairs $(p_1, p_2) = (113, 5)$, $(409, 13)$, $(4513, 5)$, respectively. Further, for the first pair $(113, 5)$, the result holds without assuming GRH.

3. Preliminaries

3.1. We consider some finite 2-groups with two generators x, y:

$$\begin{aligned}
Q_{2^m} &= \langle x, y \mid x^{2^{m-2}} = y^2,\ y^4 = 1,\ y^{-1}xy = x^{-1} \rangle \quad \text{with } m \geq 3,\\
D_{2^m} &= \langle x, y \mid x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{-1} \rangle \quad \text{with } m \geq 3,\\
SD_{2^m} &= \langle x, y \mid x^{2^{m-1}} = y^2 = 1,\ y^{-1}xy = x^{2^{m-2}-1} \rangle \quad \text{with } m \geq 4,\\
(2,2) &= \langle x, y \mid x^2 = y^2 = 1,\ y^{-1}xy = x \rangle,
\end{aligned}$$

where the 2-groups Q_{2^m}, D_{2^m}, SD_{2^m} are the *generalized quaternion*, *dihedral*, *semidihedral* groups of order 2^m respectively, and $(2,2)$ is the *Klein four group*. These 2-groups are characterized by the following proposition.

Proposition 3 (cf. [10], [5], etc.). *Let G be a finite 2-group. Then the maximal abelian quotient group G^{ab} of G is isomorphic to $(2,2)$ if and only if G is isomorphic to Q_{2^m}, D_{2^m}, $SD_{2^{m+1}}$ for some $m \geq 3$, or $(2,2)$.*

Let G be one of the above 2-groups. Then the commutator subgroup $[G, G]$ is $\langle x^2 \rangle$, and G has three maximal subgroups: $H_1 = \langle x \rangle$, $H_2 = \langle x^2, y \rangle$, $H_3 = \langle x^2, xy \rangle$. In Table 1, the structure of these subgroups is determined in each type of G.

Table 1. The structure of maximal subgroups ($m \geq 4$)

G	D_8	D_{2^m}	Q_8	Q_{2^m}	SD_{2^m}	$(2,2)$
H_1	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2^{m-1}\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2^{m-1}\mathbb{Z}$	$\mathbb{Z}/2^{m-1}\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
H_2	$(2,2)$	$D_{2^{m-1}}$	$\mathbb{Z}/4\mathbb{Z}$	$Q_{2^{m-1}}$	$D_{2^{m-1}}$	$\mathbb{Z}/2\mathbb{Z}$
H_3	$(2,2)$	$D_{2^{m-1}}$	$\mathbb{Z}/4\mathbb{Z}$	$Q_{2^{m-1}}$	$Q_{2^{m-1}}$	$\mathbb{Z}/2\mathbb{Z}$

Let k be a finite extension of $\mathbb{Q}$ with 2-class group $A(k) \simeq (2,2)$. The Galois group $G = \mathrm{Gal}(\mathcal{L}(k)/k)$ has the maximal abelian quotient isomorphic to $(2,2)$, so it is isomorphic to Q_{2^m}, D_{2^m}, SD_{2^m} or $(2,2)$, by Proposition 3. Let F_1, F_2, F_3 be the fixed fields of the maximal subgroups H_1, H_2, H_3 of G (in the above notation), respectively. For $i = 1,2,3$, the field F_i is an unramified quadratic extensions of k with 2-class group $A(F_i) \simeq H_i^{\mathrm{ab}}$. If $G \simeq Q_8$ or $(2,2)$, then $A(F_i)$ is cyclic for each i. If $G \simeq Q_{2^{m+1}}, D_{2^m}$, or $SD_{2^{m+1}}$ for some $m \geq 3$, then $A(F_1)$ is cyclic and $A(F_2) \simeq A(F_3) \simeq (2,2)$.

For each field $F = F_i$ $(i = 1,2,3)$, we denote by $j : A(k) \to A(F)$ the homomorphism induced from the lifting of ideals. Now, we set the following two conditions which are often called the *Taussky conditions* (TC):

$$\text{(A)} \quad \#(\ker j \cap N_{F/k}A(F)) > 1,$$

$$\text{(B)} \quad \#(\ker j \cap N_{F/k}A(F)) = 1,$$

where $N_{F/k}$ is the norm mapping. By the theorem of H. Kisilevsky [10], we can characterize the structure of the Galois group $G = \mathrm{Gal}(\mathcal{L}(k)/k)$ by the order of the kernel of j and the Taussky conditions as in Table 2.

Table 2 (by the theorem in [10], $m \geq 3$)

	F_1		F_2		F_3	
G	$\#\ker j$	TC	$\#\ker j$	TC	$\#\ker j$	TC
D_{2^m}	4	(A)	2	(B)	2	(B)
Q_8	2	(A)	2	(A)	2	(A)
$Q_{2^{m+1}}$	2	(A)	2	(B)	2	(B)
$SD_{2^{m+1}}$	2	(B)	2	(B)	2	(B)
$(2,2)$	4	(A)	4	(A)	4	(A)

3.2. Let K be a real biquadratic bicyclic extension of $\mathbb{Q}$. The field K contains three real quadratic fields F_1, F_2, F_3. For each $i = 1, 2, 3$, we denote by ε_i the fundamental unit of F_i, and define the group index $Q(K) = [E(K) : \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle]$. By Satz 11 in [12], we know that $Q(K) = 1$, 2, or 4, and a system of fundamental units of K is of one of the following types:

1) $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$,
2) $\{\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3\}$ $(N\varepsilon_1 = 1)$,
3) $\{\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3\}$ or $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \varepsilon_3\}$ $(N\varepsilon_1 = N\varepsilon_2 = 1)$,
4) $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_3}, \varepsilon_2\}$ or $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_2\varepsilon_3}, \sqrt{\varepsilon_3\varepsilon_1}\}$ $(N\varepsilon_1 = N\varepsilon_2 = N\varepsilon_3 = 1)$,
5) $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ $(N\varepsilon_1 = N\varepsilon_2 = N\varepsilon_3 = \pm 1)$,

where $N\varepsilon_i$ is the absolute norm of ε_i for each i. Furthermore, by Satz 5 in [11], we have the following formula:

$$\#A(K) = 2^{-2} \cdot Q(K) \cdot \#A(F_1) \cdot \#A(F_2) \cdot \#A(F_3),$$

which is often called *Kuroda's class number formula*, extended by T. Kubota (cf. [13]).

3.3. We mention some results on the rank of 2-class groups. Let k be a finite extension of $\mathbb{Q}$, and K a quadratic extension of k. Let t be the number of places of k which are ramified in K. We denote by $A(K)^G$ the subgroup of $A(K)$ generated by the ideal classes fixed by the action of $\mathrm{Gal}(K/k)$, and by $B(K)^G$ the subgroup of $A(K)$ generated by the classes containing ideals fixed by the action of $\mathrm{Gal}(K/k)$. The following formulae are well known.

PROPOSITION 4 (genus formulae). *In the above setting, we have*

$$\#A(K)^G = \frac{\#A(k)\cdot 2^t}{2\cdot[E(k):E(k)\cap N_{K/k}K^\times]},$$
$$\#B(K)^G = \frac{\#A(k)\cdot 2^t}{2\cdot[E(k):N_{K/k}E(K)]}.$$

If the image of the lifting mapping $j : A(k) \to A(K)$ is trivial, a non-trivial element of $\mathrm{Gal}(K/k)$ acts on $A(K)$ as -1. Thus, $A(K)^G$ is the subgroup of $A(K)$ generated by all elements of order 2, and $\#A(K)^G = \#(A(K)/2A(K))$.

Let k be a real quadratic field, and $A^+(k)$ be the 2-Sylow subgroup of the narrow ideal class group of k. We denote by $D = 2^e p_1^* \cdots p_t^*$ the discriminant of k, where $e = 0$, 2, or 3, and $p_i^* = \pm p_i \equiv 1 \pmod 4$ are the prime discriminants for odd prime numbers p_i. The narrow genus field k_G^+ of k is specified as follows: $k \subseteq k_G^+ = \mathbb{Q}(\sqrt{\delta}, \sqrt{p_1^*}, \dots, \sqrt{p_t^*})$, where $\delta = \pm 1$, ± 2, and δ must be 1 if $e = 0$. The genus field k_G of k is the maximal abelian extension of $\mathbb{Q}$ which is contained in the Hilbert 2-class field $L(k)$. We can see that the field k_G is the maximal totally real subfield of k_G^+, and $\mathrm{Gal}(k_G/k) \simeq A(k)/2A(k)$, $\mathrm{Gal}(k_G^+/k) \simeq A^+(k)/2A^+(k)$.

Let $S_1(k)$ be the set of pairs (D_1, D_2) of integers such that $D = D_1 D_2$, $|D_1| < |D_2|$ and $D_i \equiv 0$ or $1 \pmod 4$ for $i = 1, 2$. Let $S_2(k)$ be the set of pairs $(D_1, D_2) \in S_1(k)$ such that $\chi_{D_1}(p) = 1$ for all prime factors p of D_2 and $\chi_{D_2}(p) = 1$ for all prime factors p of D_1, where $\chi_{D_i}(p)$ is Kronecker's symbol, i.e., $\chi_{D_i}(p) = \left(\frac{D_i}{p}\right)$ when $p \neq 2$, and $\chi_{D_i}(2) = 1$ or -1 when $D_i \equiv 1$ or $5 \pmod 8$, respectively. Now, we have the following proposition.

PROPOSITION 5 (Rédei–Reichardt [16]). *In the above setting,*

$$\#S_1(k) = \#(A^+(k)/2A^+(k)), \qquad \#S_2(k) = \#(2A^+(k)/4A^+(k)).$$

For the first layer k_1 of the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k, we can determine the rank of $A(k_1)$ by the following proposition, which is a part of the theorems in [1].

PROPOSITION 6 (Azizi–Mouhib [1]). *Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field with a positive square-free odd integer m. Denote by t_1 the number of prime ideals of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ which are ramified in $k_1 = \mathbb{Q}(\sqrt{2}, \sqrt{m})$, and by r_1 the rank of $A(k_1)$.*

(i) *If m has a prime factor $\equiv 3 \pmod 4$, then $r_1 = t_1 - 2$ or $t_1 - 3$. In this case, $r_1 = t_1 - 2$ if and only if m has no prime factor $\equiv 7 \pmod 8$.*
(ii) *If m has no prime factor $\equiv 3 \pmod 4$, then $r_1 = t_1 - 1$ or $t_1 - 2$. In this case, $r_1 = t_1 - 1$ if and only if m has no prime factor p such that $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right)_4 \neq (-1)^{(p-1)/8}$.*

4. Real quadratic fields with $X \simeq (2,2)$. Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field with a positive square-free integer m. The first layer k_1 of the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k is the field $\mathbb{Q}(\sqrt{2}, \sqrt{m})$. If $m \neq 2$, then k_1 has just three real quadratic subfields $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$, $k = \mathbb{Q}(\sqrt{m})$, $k' = \mathbb{Q}(\sqrt{2m})$, and we have $k'_\infty = k_\infty$. By genus theory, m is an even integer if k_1/k is unramified. Our purpose is to consider the cyclotomic $\mathbb{Z}_2$-extensions of real quadratic fields, and the case $m = 2$ is well known; so we may assume that m is odd, i.e., any prime ideal of k above 2 is totally ramified in k_∞. By these assumptions and the results in [7], if the Iwasawa module X is isomorphic to the Klein four group $(2,2)$, one of the following conditions holds:

- $A(k_n) \simeq (2,2)$ for all $n \geq 0$,
- $\#A(k) = 2$ and $A(k_n) \simeq (2,2)$ for all $n \geq 1$,
- $\#A(k) = 1$, $\#A(k_1) = 2$ and $A(k_n) \simeq (2,2)$ for all $n \geq 2$.

As we shall see later, a real quadratic field k treated in Theorem 2 satisfies the second condition. The following proposition characterizes the real quadratic fields k satisfying the first condition.

PROPOSITION 7. *Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field with a positive square-free odd integer m, and $A(k_n)$ the 2-class group of the nth layer k_n of the cyclotomic $\mathbb{Z}_2$-extension k_∞/k. Then $A(k_n) \simeq (2,2)$ for all $n \geq 0$ if and only if m is of one of the following types.*

(i) *$m = p_1p_2q$ with prime numbers p_1, p_2, q satisfying*

$$p_1 \equiv p_2 \equiv 5 \pmod 8, \qquad q \equiv 3 \pmod 4, \qquad \left(\frac{p_1p_2}{q}\right) = -1,$$

(ii) *$m = q_1q_2q_3$ with prime numbers q_1, q_2, q_3 satisfying*

$$q_1 \equiv q_2 \equiv 3, \ q_3 \equiv 7 \pmod 8, \qquad \left(\frac{q_1q_2}{q_3}\right) = -1.$$

Proof. We put $k' = \mathbb{Q}(\sqrt{2m})$ and denote by k_G the genus field of k. If $m = p_1p_2q$, $q_1q_2q_3$ satisfy (i), (ii), we have $\lambda(k) = \mu(k) = 0$ and $\nu(k) = 2$, respectively, by [15]. The rank of $A(k)$ is 2 by genus theory, and k_∞/k is totally ramified, so $A(k_n)$ must be isomorphic to $(2,2)$ for all $n \geq 0$. This completes the "if" part.

Now, we assume that $A(k_n) \simeq (2,2)$ for all $n \geq 0$. Since the rank of $A(k)$ is 2, the number of prime numbers which ramify in $k/\mathbb{Q}$ must be 3 or 4 by genus theory. Thus, the positive square-free odd integer m is of one of the following types: $m = pq_1q_2$, pq, $p_1p_2p_3p_4$, $p_1p_2p_3$, $p_1p_2q_1q_2$, $q_1q_2q_3q_4$, p_1p_2q, $q_1q_2q_3$, where p and p_i are prime numbers $\equiv 1 \pmod 4$, and q and q_i are prime numbers $\equiv 3 \pmod 4$.

For $m = pq_1q_2$, pq, we have $k_G = k(\sqrt{p})$, i.e., $A(k)$ is cyclic. For $m = p_1p_2p_3p_4$, $k_G = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$, i.e., the rank of $A(k)$ is 3. For $m = p_1p_2p_3$, $p_1p_2q_1q_2$, $q_1q_2q_3q_4$, we can see that the rank of $A(k)$ is 2 but the rank of $A(k')$ is 3 by similar arguments. By the formula in 3.2, we have $\#A(k_1) \geq 8$, i.e., $A(k_1) \not\simeq (2,2)$. Therefore, these cases do not occur.

In the remaining cases $m = p_1p_2q$, $q_1q_2q_3$, the extensions k_1/k and k_1/k' are not unramified, and both $A(k)$ and $A(k')$ have rank 2. By our assumption, $A(k_1) \simeq A(k) \simeq (2,2)$ and $A(k') \simeq (2,2)$.

Let t_1 be the number of prime ideals of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ which ramify in k_1. For $m = p_1p_2q$, we have $t_1 = 4$ when $q \equiv 3 \pmod 8$, and $t_1 = 5$ when $q \equiv 7 \pmod 8$ by Proposition 6. In each case, p_1 and p_2 do not split in $\mathbb{Q}_1/\mathbb{Q}$, so $p_1 \equiv p_2 \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$. Furthermore, by Proposition 5, we can see that $\left(\frac{p_1p_2}{q}\right) = -1$.

We consider the case $m = q_1q_2q_3$. First, suppose that $q_i \equiv 3 \pmod 8$ for all i. Since $A(k) \simeq (2,2)$, the Hilbert 2-class field $L(k)$ of k is equal to $k_G = \mathbb{Q}(\sqrt{q_1}, \sqrt{q_2}, \sqrt{q_3})$. Let $\mathfrak{l}$ be the prime ideal of k above 2. Since $\mathfrak{l}^2 = (2)$, the ideal class of $\mathfrak{l}$ is an element of $A(k)$. We can see that $\mathfrak{l}$ splits in $k(\sqrt{q_i})/k$ for all i, i.e., $\mathfrak{l}$ splits completely in $L(k)/k$. Therefore, $\mathfrak{l}$ is principal, i.e., $(\alpha)^2 = (2)$ as principal ideals of k for some $\alpha \in k^\times$. By genus theory, we have $N\varepsilon = 1$, where $N\varepsilon$ is the absolute norm of the fundamental unit ε of k. Thus $2 = \varepsilon^z\alpha^2$ for some integer z. Since $\sqrt{2} \notin k$, the integer z must be odd. Therefore $2 = \varepsilon\beta^2$ for some $\beta \in k^\times$, and $\sqrt{2} = \pm\sqrt{\varepsilon}\,\beta$, so that $\sqrt{\varepsilon} \in k_1$. By the formula in 3.2, we have $\#A(k_1) \geq 8$, i.e., $A(k_1) \not\simeq (2,2)$. This contradicts our assumption. Thus, $q_i \equiv 7 \pmod 8$ for some i. In this situation, $t_1 = 5$ by Proposition 6, so $q_1 \equiv q_2 \equiv 3$, $q_3 \equiv 7 \pmod 8$, without loss of generality. Furthermore, by Proposition 5, we can see that $\left(\frac{q_1q_2}{q_3}\right) = -1$.

By the above, m satisfies condition (i) or (ii), and the "only if" part is completed. ∎

The real quadratic fields $k = \mathbb{Q}(\sqrt{m})$ satisfying condition (i) in Proposition 7 are treated in Theorem 1. On the other hand, for the real quadratic fields k satisfying (ii), we already know the following theorem as a corollary to the results of G. Yamamoto [17].

THEOREM 8. *Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of a real quadratic field $k=\mathbb{Q}(\sqrt{m})$ satisfying condition* (ii) *in Proposition* 7. *Then the Galois group $G=\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$ of the maximal unramified pro-2-extension of k_∞ is isomorphic to the Klein four group* $(2,2)$.

Proof. Consider the field $K=\mathbb{Q}(\sqrt{q_1},\sqrt{q_2},\sqrt{q_3})$ and its cyclotomic $\mathbb{Z}_2$-extension K_∞/K. As in the proof of Proposition 7, we know that $L(k_n)=K_n$ for all $n\geq 0$. In [17], it has been proved that $\lambda(K)=\mu(K)=\nu(K)=0$, i.e., $L(K_\infty)=K_\infty$. (As in [17], we can see that $\#A(K_1)=1$ by Theorem 5.6 of [6]. By using Theorem 1 of [7], we get $\lambda(K)=\mu(K)=\nu(K)=0$.) Thus, $\mathcal{L}(k_\infty)=K_\infty$, i.e., $G=\mathrm{Gal}(K_\infty/k_\infty)\simeq X\simeq(2,2)$. ∎

5. Proof of Theorem 1. Let p_1, p_2, q be prime numbers as in the statement of Theorem 1. Without loss of generality, we may assume that

$$(\dagger)\qquad p_1\equiv p_2\equiv 5 \pmod 8,\quad q\equiv 3 \pmod 4,\quad \left(\frac{p_1}{q}\right)=1,\quad \left(\frac{p_2}{q}\right)=-1.$$

By Proposition 7, we already know that $A(k_n)\simeq(2,2)$ for any nth layer $k_n=\mathbb{Q}_n(\sqrt{p_1p_2q})$ of the cyclotomic $\mathbb{Z}_2$-extension k_∞/k, and so the Iwasawa module $X\simeq G^{\mathrm{ab}}\simeq(2,2)$. Since the Hilbert 2-class field $L(k)$ of k is equal to the genus field $k_G=\mathbb{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{q})$, we know that $L(k_n)=\mathbb{Q}_n(\sqrt{p_1},\sqrt{p_2},\sqrt{q})$ for all $n\geq 0$ and $L(k_\infty)=\mathbb{Q}_\infty(\sqrt{p_1},\sqrt{p_2},\sqrt{q})$. Therefore, $L(k_n)/k_n$ has just three quadratic subextensions $k_n(\sqrt{p_1})/k_n$, $k_n(\sqrt{p_2})/k_n$, $k_n(\sqrt{q})/k_n$. By Proposition 3, for each $n\geq 0$, the Galois group $\mathrm{Gal}(\mathcal{L}(k_n)/k_n)$ of the maximal unramified pro-2-extension $\mathcal{L}(k_n)/k_n$ is isomorphic to Q_{2^m}, D_{2^m}, $SD_{2^{m+1}}$, or $(2,2)$ for some $m\geq 3$.

LEMMA 9. *Under the above assumptions, if $\left(\frac{p_2}{p_1}\right)=1$, then $\mathrm{Gal}(\mathcal{L}(k)/k)\simeq D_{2^m}$ and $A(k(\sqrt{q}))\simeq\mathrm{Gal}(\mathcal{L}(k)/k(\sqrt{q}))\simeq\mathbb{Z}/2^{m-1}\mathbb{Z}$ for some $m\geq 3$. On the other hand, if $\left(\frac{p_2}{p_1}\right)=-1$, then $\mathrm{Gal}(\mathcal{L}(k)/k)\simeq(2,2)$, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1)\simeq D_8$, and $A(k_1(\sqrt{q}))\simeq\mathrm{Gal}(\mathcal{L}(k_1)/k_1(\sqrt{q}))\simeq\mathbb{Z}/4\mathbb{Z}$.*

Proof. For $\left(\frac{p_2}{p_1}\right)=1$, we can argue as in the proof of Lemma 1 in [14]. Therefore, we shall consider only the second case.

Assume that $\left(\frac{p_2}{p_1}\right)=-1$ in addition to $(\dagger)$. Let ε, $\varepsilon_{p_1p_2}$, ε_q be the fundamental units of the real quadratic fields k, $\mathbb{Q}(\sqrt{p_1p_2})$, $\mathbb{Q}(\sqrt{q})$, respectively. By Proposition 5, we can see that $A(\mathbb{Q}(\sqrt{p_1p_2}))\simeq A^+(\mathbb{Q}(\sqrt{p_1p_2}))\simeq\mathbb{Z}/2\mathbb{Z}$. Therefore, $N\varepsilon_{p_1p_2}=-1$. By the arguments in Proof (II) of Lemma in [15], we know that $k_1(\sqrt{p_1})=k_1(\sqrt{\varepsilon})$ and $\sqrt{\varepsilon}\notin k(\sqrt{q})$. Since $\#A(\mathbb{Q}(\sqrt{q}))=1$ and the prime 2 ramifies in $\mathbb{Q}(\sqrt{q})$, the prime ideal of $\mathbb{Q}(\sqrt{q})$ above 2 is a principal ideal. Therefore, there is an element α of $\mathbb{Q}(\sqrt{q})$ such that $\sqrt{2}=\pm\alpha\sqrt{\varepsilon_q}$. Then $\mathbb{Q}_1(\sqrt{q})=\mathbb{Q}(\sqrt{q},\sqrt{\varepsilon_q})$, and $\sqrt{\varepsilon_q}\notin k(\sqrt{q})$. If $\sqrt{\varepsilon\varepsilon_q}\in k(\sqrt{q})$, we have $k_1(\sqrt{q})=k_1(\sqrt{q},\sqrt{\varepsilon_q})=k_1(\sqrt{q},\sqrt{\varepsilon})=k_1(\sqrt{q},\sqrt{p_1})$, which is a contradiction. Thus $\sqrt{\varepsilon}, \sqrt{\varepsilon_q}, \sqrt{\varepsilon\varepsilon_q} \notin k(\sqrt{q})$. Note that $N\varepsilon = N\varepsilon_q = 1$ and $N\varepsilon_{p_1p_2} = -1$. By 3.2, we have $Q(k(\sqrt{q})) = 1$ and $\#A(k(\sqrt{q})) = 2$. By Table 1 in 3.1, we know that $\mathrm{Gal}(\mathcal{L}(k)/k) \simeq (2,2)$.

Now, we consider the field $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$ and its cyclotomic $\mathbb{Z}_2$-extension K_∞/K. We know that $K = k_G = L(k) = \mathcal{L}(k)$, and $K_n = L(k_n)$, $\#A(K) = 1$. If $\#A(K_1) = 1$, we have $\lambda(K) = \mu(K) = \nu(K) = 0$ by Theorem 1 in [7]. However, this contradicts the determination of the abelian 2-extensions $K/\mathbb{Q}$ with $\lambda(K) = \mu(K) = \nu(K) = 0$ in Yamamoto's thesis [17]. Hence $\#A(K_1) \neq 1$ and $\mathrm{Gal}(\mathcal{L}(k_1)/k_1) \not\simeq (2,2)$. (As in [17], we can also see that the class number of $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{q})$ is even, i.e., $\#A(K_1) \neq 1$ by applying Theorem 5.6 in [6].) Therefore, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1) \simeq D_{2^m}$, Q_{2^m}, or $SD_{2^{m+1}}$ for some $m \geq 3$.

Now, suppose that $A(k_1(\sqrt{q}))$ is not cyclic. Then $A(k_1(\sqrt{q})) \simeq (2,2)$ and $\mathrm{Gal}(\mathcal{L}(k_1)/k_1) \not\simeq Q_8$ by the arguments in 3.1. By applying Proposition 4 for $\mathbb{Q}_1(\sqrt{p_1p_2})/\mathbb{Q}_1$ and the fact that $\#A(\mathbb{Q}_1) = 1$, and condition (†), we find that $A(\mathbb{Q}_1(\sqrt{p_1p_2}))$ is cyclic. The norm map $A(k_1(\sqrt{q})) \to A(\mathbb{Q}_1(\sqrt{p_1p_2}))$ is surjective, so $A(\mathbb{Q}_1(\sqrt{p_1p_2})) \simeq \mathbb{Z}/2\mathbb{Z}$ and $L(\mathbb{Q}_1(\sqrt{p_1p_2})) = \mathbb{Q}_1(\sqrt{p_1}, \sqrt{p_2})$. Let $\mathfrak{l}_1$ be a prime ideal of $\mathbb{Q}_1(\sqrt{p_1p_2})$ above the prime number 2, and h_1 the non-2-part of the class number of $k_1(\sqrt{q})$. We note that the non-2-part of the class number of $\mathbb{Q}_1(\sqrt{p_1p_2})$ divides h_1. By (†), the prime $\mathfrak{l}_1$ is inert in $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p_2})$. Then the ideal $\mathfrak{a}_1 = \mathfrak{l}_1^{h_1}$ is not principal in $\mathbb{Q}_1(\sqrt{p_1p_2})$, and the ideal class containing $\mathfrak{a}_1$ is a generator of $A(\mathbb{Q}_1(\sqrt{p_1p_2}))$. Let $\mathfrak{L}_1$ be a prime ideal of $k_1(\sqrt{q})$ above the prime $\mathfrak{l}_1$ and consider the ideal $\mathfrak{A}_1 = \mathfrak{L}_1^{h_1}$. The prime $\mathfrak{l}_1$ is ramified in $k_1(\sqrt{q})/\mathbb{Q}_1(\sqrt{p_1p_2})$, i.e., $\mathfrak{l}_1 = \mathfrak{L}_1^2$. The ideal class containing $\mathfrak{A}_1$ is a non-trivial element of $A_1(k(\sqrt{q}))$, and $\mathfrak{A}_1^2$ is principal. Since $\mathfrak{a}_1 = \mathfrak{A}_1^2$ is principal in $k_1(\sqrt{q})$, the lifting map $A(\mathbb{Q}_1(\sqrt{p_1p_2})) \to A(k_1(\sqrt{q}))$ is the zero map. Then so is the endomorphism $\sigma + 1 : A(k_1(\sqrt{q})) \to A(k_1(\sqrt{q}))$, where σ is a generator of $\mathrm{Gal}(k_1(\sqrt{q})/\mathbb{Q}_1(\sqrt{p_1p_2}))$. The action of σ on $A(k_1(\sqrt{q}))$ is trivial. Let τ be a generator of $\mathrm{Gal}(k_1(\sqrt{q})/\mathbb{Q}_1(\sqrt{q}))$. Since $\#A(\mathbb{Q}_1(\sqrt{q})) = 1$ (use Theorem in [9]), the action of τ on $A(k_1(\sqrt{q}))$ is also trivial. Then the group $\mathrm{Gal}(k_1(\sqrt{q})/k_1) = \langle\sigma\tau\rangle$ acts on $A(k_1(\sqrt{q}))$ trivially, so that $L(k_1(\sqrt{q}))/k_1$ is an unramified abelian 2-extension, but $L(k_1(\sqrt{q})) \neq L(k_1)$. This is a contradiction. It follows that $A(k_1(\sqrt{q}))$ is cyclic and isomorphic to $\mathrm{Gal}(\mathcal{L}(k_1)/k_1(\sqrt{q}))$.

Let $\mathfrak{L}$, $\mathfrak{L}_1$ be the prime ideals above 2 of the fields $k(\sqrt{q})$, $k_1(\sqrt{q})$ such that $\mathfrak{L} = \mathfrak{L}_1^2$. We denote by h_1 the non-2-part of the class number of $k_1(\sqrt{q})$. By (†), $\mathfrak{L}$ and $\mathfrak{L}_1$ are inert in $L(k)$ and $L(k_1)$, respectively. Hence $\mathfrak{L}$ and $\mathfrak{L}_1$ are not decomposed in $L(k_1(\sqrt{q})) = \mathcal{L}(k_1)$. Therefore, the ideal classes containing $\mathfrak{A} = \mathfrak{L}^{h_1}$, $\mathfrak{A}_1 = \mathfrak{L}_1^{h_1}$ generate $A(k(\sqrt{q}))$, $A(k_1(\sqrt{q}))$, respectively. Since $\mathfrak{A}_1^4 = \mathfrak{A}_1^2$ is principal and $\#A(K_1) \neq 1$, we have $A(k_1(\sqrt{q})) \simeq \mathbb{Z}/4\mathbb{Z}$ and $\#\,\mathrm{Gal}(\mathcal{L}(k_1)/k_1) = 8$. Thus, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1) \simeq D_8$ or Q_8.

Set $F = k(\sqrt{p_1}, \sqrt{2q})$. The $(2,2)$-extension $L(k_1)/k(\sqrt{p_1})$ has three non-trivial subextensions $L(k)$, F, $k_1(\sqrt{p_1})$. The extension $\mathcal{L}(k_1)/k(\sqrt{p_1})$ is unramified outside 2, and no prime ideal above 2 ramifies in $L(k_1)/F$, so $\mathcal{L}(k_1)/F$ is an unramified extension of degree 4.

Now, suppose $H = \mathrm{Gal}(\mathcal{L}(k_1)/k(\sqrt{p_1}))$ is abelian. Let $\mathfrak{L}'$ be a prime ideal of $k(\sqrt{p_1})$ above 2. By (†), $\mathfrak{L}'$ is a unique prime ideal of $k(\sqrt{p_1})$ ramified in $\mathcal{L}(k_1)/k(\sqrt{p_1})$, and its ramification index is 2. Then $k_T/k(\sqrt{p_1})$ is an unramified abelian extension of degree 4, where k_T is the inertia subfield of $\mathcal{L}(k_1)/k(\sqrt{p_1})$. This contradicts $\#A(k(\sqrt{p_1})) = 2$. Therefore, $H = \mathrm{Gal}(\mathcal{L}(k_1)/k(\sqrt{p_1}))$ is a non-abelian 2-group of degree 8, and has the maximal abelian quotient $H^{\mathrm{ab}} = \mathrm{Gal}(L(k_1)/k(\sqrt{p_1})) \simeq (2,2)$. By Proposition 3, $H \simeq D_8$ or Q_8. Further, the prime ideal above 2 is ramified in $L(k_1)/L(k)$ and unramified in $\mathcal{L}(k_1)/L(k_1)$, so $\mathcal{L}(k_1)/L(k)$ cannot be cyclic. It follows that $H = \mathrm{Gal}(\mathcal{L}(k_1)/k(\sqrt{p_1})) \simeq D_8$ and $\mathrm{Gal}(\mathcal{L}(k_1)/L(k)) \simeq (2,2)$.

We shall consider the extension $F/\mathbb{Q}(\sqrt{p_1})$. Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Q}(\sqrt{p_1})$ above q. By (†), the prime $\mathfrak{q}$ is ramified in $\mathbb{Q}(\sqrt{p_1}, \sqrt{2q})$ and $k(\sqrt{p_1})$. Let $\mathfrak{q}$, $\mathfrak{q}_0$ be the prime ideals above $\mathfrak{q}$ of $k(\sqrt{p_1})$, $\mathbb{Q}(\sqrt{p_1}, \sqrt{2q})$ respectively. By (†), $\mathfrak{q}$ and $\mathfrak{q}_0$ split in F, so that $\mathfrak{q} = \mathfrak{q}_0$ as ideals of F. Let h be the non-2-part of the class number of F, and put $\mathfrak{a} = \mathfrak{q}^h$. By (†), $\mathfrak{q}$ is inert in $L(k) = L(k(\sqrt{p_1}))$, therefore the ideal class containing $\mathfrak{a}$ is a generator of $A(k(\sqrt{p_1})) \simeq \mathbb{Z}/2\mathbb{Z}$. On the other hand, the ideal class containing $\mathfrak{a}_0 = \mathfrak{q}_0^h$ is an element of $A(\mathbb{Q}(\sqrt{p_1}, \sqrt{2q}))$ and $\mathfrak{a} = \mathfrak{a}_0$ as ideals of F. We can check that $\mathbb{Q}(\sqrt{p_1}, \sqrt{2q})$ is the genus field of the real quadratic field $\mathbb{Q}(\sqrt{2p_1q})$, and that $A^+(\mathbb{Q}(\sqrt{2p_1q})) \simeq A(\mathbb{Q}(\sqrt{2p_1q})) \simeq \mathbb{Z}/2\mathbb{Z}$ by Proposition 5 and (†). Therefore $\#A(\mathbb{Q}(\sqrt{p_1}, \sqrt{2q})) = 1$ and $\mathfrak{a}_0$ is a principal ideal of $\mathbb{Q}(\sqrt{p_1}, \sqrt{2q})$, i.e., $\mathfrak{a} = \mathfrak{a}_0$ is principal in F. We know that the lifting map $A(k(\sqrt{p_1})) \to A(F)$ is the zero map. By (†), the unique prime ideal of $k(\sqrt{p_1})$ above 2 is the only prime ideal ramified in F. By Proposition 4, we can infer that $A(F)$ is cyclic. The maximal subgroups of $H \simeq D_8$ are $\mathrm{Gal}(\mathcal{L}(k_1)/L(k)) \simeq (2,2)$ and $\mathrm{Gal}(\mathcal{L}(k_1)/k_1(\sqrt{p_1})) \simeq A(k_1(\sqrt{p_1}))$, $\mathrm{Gal}(\mathcal{L}(k_1)/F) \simeq A(F)$. By the above results, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1(\sqrt{p_1})) \simeq A(k_1(\sqrt{p_1})) \simeq (2,2)$. Therefore, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1)$ cannot be isomorphic to Q_8, i.e., $\mathrm{Gal}(\mathcal{L}(k_1)/k_1) \simeq D_8$. This completes the proof of Lemma 9. ∎

By Lemma 9 and the arguments in 3.1, for each $n \geq 1$, we have $\mathrm{Gal}(\mathcal{L}(k_n)/k_n) \simeq Q_{2^{m+1}}$, D_{2^m}, or $SD_{2^{m+1}}$ for some $m \geq 3$, and the Galois group $\mathrm{Gal}(\mathcal{L}(k_n)/k_n(\sqrt{q})) \simeq A(k_n(\sqrt{q}))$ is cyclic.

Let $\mathfrak{L}_0$ be a prime ideal of $k(\sqrt{q})$ above 2, and $\mathfrak{L}_n$ a prime ideal of $k_n(\sqrt{q})$ above $\mathfrak{L}_0$. Let h_n be the non-2-part of the class number of $k_n(\sqrt{q})$, and consider the ideal $\mathfrak{A}_n = \mathfrak{L}_n^{h_n}$. By (†), we can see that $\mathfrak{L}_n$ is inert in the unramified quadratic extension $L(k_n)/k_n(\sqrt{q})$ for all $n \geq 0$. Then the ideal class of $\mathfrak{A}_n$ is a generator of $A(k_n(\sqrt{p}))$ for each $n \geq 0$. The prime $\mathfrak{L}_0$ is totally ramified in the cyclotomic $\mathbb{Z}_2$-extension $k_\infty(\sqrt{q})/k(\sqrt{q})$, i.e., $\mathfrak{L}_0 = \mathfrak{L}_n^{2^n}$ for all $n \geq 0$. Then the Galois group $\Gamma = \mathrm{Gal}(k_\infty(\sqrt{q})/k(\sqrt{q})) \simeq \mathbb{Z}_2$ acts on $A(k_n(\sqrt{p}))$ trivially. By applying Proposition 1 of [8] to $k_\infty(\sqrt{q})/k(\sqrt{q})$, we deduce that $\#A(k_n(\sqrt{q}))$ is bounded as $n \to \infty$. Then $\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty(\sqrt{q}))$, which is the Iwasawa module associated to $k_\infty(\sqrt{q})/k(\sqrt{q})$, is a finite cyclic group.

Let $\mathfrak{l}_n$ and $\mathfrak{l}_n'$ be the prime ideals of k_n and $\mathbb{Q}_n(\sqrt{q})$ above 2, respectively. Define the ideals $\mathfrak{a}_n = (\mathfrak{l}_n)^{h_n}$ and $\mathfrak{a}_n' = (\mathfrak{l}_n')^{h_n}$. By Theorem in [9], we have $\#A(\mathbb{Q}_n(\sqrt{q})) = 1$ and $\mathfrak{a}_n'$ is principal. By (†), both prime ideals $\mathfrak{l}_n$ and $\mathfrak{l}_n'$ split in $k_n(\sqrt{q})$, so $\mathfrak{a}_n = \mathfrak{a}_n'$ as principal ideals of $k_n(\sqrt{q})$. Since $\mathfrak{a}_n = N_{k_n(\sqrt{q})/k_n}\mathfrak{A}_n$, we have $\#(\ker j_n \cap N_{k_n(\sqrt{q})/k_n} A(k_n(\sqrt{q}))) > 1$, where $j_n : A(k_n) \to A(k_n(\sqrt{q}))$ is the lifting map. By Table 2 in 3.1, we know that $\mathrm{Gal}(\mathcal{L}(k_n)/k_n) \simeq D_{2^m}$ or $Q_{2^{m+1}}$ for some $m \geq 3$. Since $\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty) \simeq \mathrm{Gal}(\mathcal{L}(k_n)/k_n)$ for all sufficiently large $n \geq 0$, we have $G = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty) \simeq D_{2^m}$ or $Q_{2^{m+1}}$ for some $m \geq 3$. This is the first half of the statement of Theorem 1.

Now, we prove the other half. In the following, we denote by ε_d the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. In particular, we write $\varepsilon = \varepsilon_{p_1p_2q}$ for the fundamental unit of k, and note that $\varepsilon_2 = 1 + \sqrt{2}$ is the fundamental unit of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$. Assume that $\left(\frac{p_2}{p_1}\right) = 1$ and $N\varepsilon_{p_1p_2} = +1$.

Since the genus field of $\mathbb{Q}(\sqrt{p_1p_2})$ is $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, $A(\mathbb{Q}(\sqrt{p_1p_2}))$ is cyclic. Thus, $\#A(\mathbb{Q}(\sqrt{p_1p_2})) = 2\#A(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}))$. By Kuroda's class number formula in 3.2, and since $\#A(\mathbb{Q}(\sqrt{p_1})) = \#A(\mathbb{Q}(\sqrt{p_2})) = 1$, we have

$$\#A(\mathbb{Q}(\sqrt{p_1p_2})) = 2\#A(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})) = 2^{-1}Q(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}))\#A(\mathbb{Q}(\sqrt{p_1p_2})).$$

So $Q(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}))$ must be 2. By the results in 3.2, and since $N\varepsilon_{p_1} = N\varepsilon_{p_2} = -1$, the unit $\sqrt{\varepsilon_{p_1p_2}}$ is contained in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$.

We already know that $A(k_1(\sqrt{q}))$ is cyclic, hence so is $A(\mathbb{Q}_1(\sqrt{p_1p_2}))$. Let l_0 be a prime ideal of $\mathbb{Q}(\sqrt{p_1p_2})$ above 2, and l_1 the prime ideal of $\mathbb{Q}_1(\sqrt{p_1p_2})$ above l_0. We denote by h the non-2-part of the class number of $k_1(\sqrt{q})$. Then the ideal classes containing $a_0 = l_0^h$, $a_1 = l_1^h$ are contained in $A(\mathbb{Q}(\sqrt{p_1p_2}))$, $A(\mathbb{Q}_1(\sqrt{p_1p_2}))$ respectively. Since l_0, l_1 are inert in the unramified extensions $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p_2})$, the ideal classes containing a_0, a_1 are generators of $A(\mathbb{Q}(\sqrt{p_1p_2}))$, $A(\mathbb{Q}_1(\sqrt{p_1p_2}))$ respectively. Since $l_0 = l_1^2$, i.e., $a_0 = a_1^2$, we have $\#A(\mathbb{Q}_1(\sqrt{p_1p_2})) = e \cdot \#A(\mathbb{Q}(\sqrt{p_1p_2}))$ with $e = 1$ or 2.

By Proposition 5, $A^+(\mathbb{Q}(\sqrt{2p_1p_2})) \simeq A(\mathbb{Q}(\sqrt{2p_1p_2})) \simeq (2, 2)$ and $N\varepsilon_{2p_1p_2} = -1$. By applying the formula in 3.2 to $\mathbb{Q}_1(\sqrt{p_1p_2}) = \mathbb{Q}(\sqrt{2}, \sqrt{p_1p_2})$, we have

$$e \cdot \#A(\mathbb{Q}(\sqrt{p_1p_2})) = \#A(\mathbb{Q}_1(\sqrt{p_1p_2})) = Q(\mathbb{Q}_1(\sqrt{p_1p_2}))\#A(\mathbb{Q}(\sqrt{p_1p_2})),$$

and $Q(\mathbb{Q}_1(\sqrt{p_1p_2})) = e = 1$ or 2. If $e = 2$, then $\sqrt{\varepsilon_{p_1p_2}} \in \mathbb{Q}_1(\sqrt{p_1p_2})$ since

$N\varepsilon_2 = N\varepsilon_{2p_1p_2} = -1$, $N\varepsilon_{p_1p_2} = +1$. However, $\sqrt{\varepsilon_{p_1p_2}} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$, so $Q(\mathbb{Q}_1(\sqrt{p_1p_2})) = e$ must be 1. In particular, we have

$$\#A(\mathbb{Q}(\sqrt{p_1p_2})) = \#A(\mathbb{Q}_1(\sqrt{p_1p_2})).$$

Let $\mathfrak{l}_0$ be the prime ideal of $k(\sqrt{q})$ above l_0, and set $\mathfrak{a}_0 = \mathfrak{l}_0^h$. Then $a_0 = \mathfrak{a}_0^2$ since l_0 is ramified in $k(\sqrt{q})/\mathbb{Q}(\sqrt{p_1p_2})$. Furthermore, $\mathfrak{l}_0$ is inert in $L(k)/k(\sqrt{q})$ since l_0 is inert in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}(\sqrt{p_1p_2})$. Since $A(k(\sqrt{q}))$ is cyclic by Lemma 9, the ideal class containing $\mathfrak{a}_0$ is a generator of $A(k(\sqrt{q}))$. By the above, $\#A(k(\sqrt{q})) = e'\cdot \#A(\mathbb{Q}(\sqrt{p_1p_2}))$ with $e' = 1$ or 2. By applying Kuroda's class number formula to $k(\sqrt{q}) = \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q})$, we obtain

$$e'\cdot \#A(\mathbb{Q}(\sqrt{p_1p_2})) = \#A(k(\sqrt{q})) = Q(k(\sqrt{q}))\#A(\mathbb{Q}(\sqrt{p_1p_2})),$$

so that $Q(k(\sqrt{q})) = e'$. Now, suppose that $Q(k(\sqrt{q})) = e' = 1$. Since $N\varepsilon_q = N\varepsilon_{p_1p_2} = 1$, we have $N_{k(\sqrt{q})/k}(\varepsilon) = \varepsilon^2$ and $N_{k(\sqrt{q})/k}(\varepsilon_q) = N_{k(\sqrt{q})/k}(\varepsilon_{p_1p_2}) = 1$, and hence $N_{k(\sqrt{q})/k}E(k(\sqrt{q})) = E(k)^2$. By applying Proposition 4 to the unramified extension $k(\sqrt{q})/k$, we reach a contradiction:

$$1 \le \#B(k(\sqrt{q}))^G = \frac{\#A(k)}{2\cdot [E(k) : E(k)^2]} = 2^{-1}.$$

Therefore, $Q(k(\sqrt{q})) = e'$ must be 2. In particular,

$$\#A(k(\sqrt{q})) = 2\#A(\mathbb{Q}(\sqrt{p_1p_2})).$$

Let $\mathfrak{l}_1$ be the prime ideal of $k_1(\sqrt{q})$ above l_1, and put $\mathfrak{a}_1 = \mathfrak{l}_1^h$. Then $a_1 = \mathfrak{a}_1^2$ since l_1 is ramified in $k_1(\sqrt{q})/\mathbb{Q}_1(\sqrt{p_1p_2})$. Furthermore, $\mathfrak{l}_1$ is inert in $L(k_1)/k_1(\sqrt{q})$ since l_1 is inert in $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}_1(\sqrt{p_1p_2})$. Since $A(k_1(\sqrt{q}))$ is cyclic by Lemma 9, the ideal class containing $\mathfrak{a}_1$ is a generator of $A(k_1(\sqrt{q}))$. By the above, we have

$$\#A(k_1(\sqrt{q})) \le 2\#A(\mathbb{Q}_1(\sqrt{p_1p_2})).$$

By the above results,

$$\begin{aligned} 2\#A(\mathbb{Q}_1(\sqrt{p_1p_2})) \ge \#A(k_1(\sqrt{q})) \ge \#A(k(\sqrt{q})) &= 2\#A(\mathbb{Q}(\sqrt{p_1p_2})) \\ &= 2\#A(\mathbb{Q}_1(\sqrt{p_1p_2})), \end{aligned}$$

so $\#A(k(\sqrt{q})) = \#A(k_1(\sqrt{q}))$. By applying Theorem 1 of [7] to the cyclotomic $\mathbb{Z}_2$-extension $k_\infty(\sqrt{q})/k(\sqrt{q})$, we find that $A(k(\sqrt{q})) \simeq A(k_n(\sqrt{q}))$ for all $n \ge 0$. By Lemma 9, $\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty(\sqrt{q})) \simeq \mathrm{Gal}(\mathcal{L}(k)/k(\sqrt{q}))$ and $\mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty) \simeq \mathrm{Gal}(\mathcal{L}(k)/k) \simeq D_{2^m}$ for some $m \ge 3$. Furthermore, $2^m = \#\,\mathrm{Gal}(\mathcal{L}(k)/k) = 2\#A(k(\sqrt{q})) = 4\#A(\mathbb{Q}(\sqrt{p_1p_2}))$. Now, the latter half of Theorem 1 is proved. This completes the proof of Theorem 1. ∎

6. Proof of Theorem 2. Let p_1, p_2 be as in the statement of Theorem 2. By applying Proposition 5 to $k = \mathbb{Q}(\sqrt{p_1p_2})$ and $k' = \mathbb{Q}(\sqrt{2p_1p_2})$, we deduce that $A^+(k) \simeq A(k) \simeq \mathbb{Z}/2\mathbb{Z}$ and $A^+(k') \simeq A(k') \simeq (2,2)$. Then the

Hilbert 2-class fields are $L(k)=\mathbb{Q}(\sqrt{p_1},\sqrt{p_2})$ and $L(k')=\mathbb{Q}(\sqrt{2},\sqrt{p_1},\sqrt{p_2})$. Furthermore, $\mathrm{Gal}(\mathcal{L}(k')/k')\simeq Q_{2^m}$, D_{2^m}, $SD_{2^{m+1}}$ for some $m\geq 3$ or $(2,2)$ by Proposition 3.

Let $\mathfrak{l}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ be the prime ideals of k' above 2, p_1, p_2, respectively. Then the decomposition subfields of the extension $L(k')/k'$ associated to $\mathfrak{l}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ are $k'(\sqrt{p_1})$, $k'(\sqrt{2})$, $k'(\sqrt{p_2})$, respectively. Then the ideal classes containing $\mathfrak{l}$, $\mathfrak{p}_1$, $\mathfrak{p}_2$ are distinct non-trivial elements of $A(k')\simeq(2,2)$.

Since the number of prime ideals ramified in $k_1/\mathbb{Q}_1$ is 3, we can see that the rank of $A(k_1)$ is 2 by Proposition 6. The first layer $k_1=k'(\sqrt{2})$ is unramified over k', so $\mathcal{L}(k')=\mathcal{L}(k_1)$. Therefore, $\mathrm{Gal}(\mathcal{L}(k_1)/k_1)$ is the maximal subgroup of $\mathrm{Gal}(\mathcal{L}(k')/k')$ with non-cyclic abelian quotient $\mathrm{Gal}(L(k_1)/k_1)\simeq A(k_1)$. By the arguments in 3.1, $\mathrm{Gal}(\mathcal{L}(k')/k')$ is not isomorphic to Q_8 nor $(2,2)$, and $\mathrm{Gal}(L(k_1)/k_1)\simeq A(k_1)\simeq(2,2)$.

By applying Proposition 4 to $k'(\sqrt{p_2})/\mathbb{Q}(\sqrt{p_2})$, and since $\#A(\mathbb{Q}(\sqrt{p_2}))=1$, we find that $A(k'(\sqrt{p_2}))$ is cyclic. Then $\mathrm{Gal}(\mathcal{L}(k')/k'(\sqrt{p_2}))\simeq A(k'(\sqrt{p_2}))$ is the unique maximal subgroup of $\mathrm{Gal}(\mathcal{L}(k')/k')$ which is cyclic. Let $\mathfrak{p}_2'=(\sqrt{p_2})$ be the prime ideal of $\mathbb{Q}(\sqrt{p_2})$ above p_2. Since both prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ split in $k'(\sqrt{p_2})$, it follows that $\mathfrak{p}_2=\mathfrak{p}_2'$ as principal ideals of $k'(\sqrt{p_2})$, and the ideal class containing $\mathfrak{p}_2$ is an element of $N_{k'(\sqrt{p_2})/k'}A(k'(\sqrt{p_2}))$. Hence $\#(\ker j\cap N_{k'(\sqrt{p_2})/k'}A(k'(\sqrt{p_2})))>1$, where $j:A(k')\to A(k'(\sqrt{p_2}))$ is the lifting map. Here, we note that $\mathfrak{l}$ is inert in $k'(\sqrt{p_2})=\mathbb{Q}(\sqrt{2p_1},\sqrt{p_2})$, and the lifted $\mathfrak{l}$ is the unique prime ideal of $\mathbb{Q}(\sqrt{2p_1},\sqrt{p_2})$ above 2. By assumption (C1), we have $\#\ker j=2$. By the arguments in 3.1 and Table 2, $\mathrm{Gal}(\mathcal{L}(k')/k')\simeq Q_{2^{m+1}}$ with $2^m=\#A(\mathbb{Q}(\sqrt{2p_1},\sqrt{p_2}))\geq 8$. Furthermore, we also know that $\mathrm{Gal}(\mathcal{L}(k_1)/k_1)\simeq Q_{2^m}$.

The $\mathbb{Z}_2$-extension k_∞/k_1 is totally ramified, so the norm mapping $A(k_2)\to A(k_1)$ is surjective. By assumption (C2), $A(k_2)\simeq A(k_1)\simeq(2,2)$. Furthermore, by applying Theorem 1 in [7] to k_∞/k_1, we have $A(k_n)\simeq(2,2)$ for all $n\geq 1$. Since the restriction map $\mathrm{Gal}(\mathcal{L}(k_n)/k_n)\to\mathrm{Gal}(\mathcal{L}(k_1)/k_1)$ is surjective for each $n\geq 1$, we have $\mathrm{Gal}(\mathcal{L}(k_n)/k_n)\simeq G_n=Q_{2^{\mathbf{m}}}$, $D_{2^{\mathbf{m}}}$, or $SD_{2^{\mathbf{m}}}$ for some $\mathbf{m}\geq m$ by Proposition 3. Let $\{x,y\}$ be a generator system of the group G_n satisfying the relations as in 3.1, i.e.,

$$\begin{aligned} Q_{2^{\mathbf{m}}}&=\langle x,y\mid x^{2^{\mathbf{m}-2}}=y^2,\, y^4=1,\, y^{-1}xy=x^{-1}\rangle, && \mathbf{m}\geq 3,\\ D_{2^{\mathbf{m}}}&=\langle x,y\mid x^{2^{\mathbf{m}-1}}=y^2=1,\, y^{-1}xy=x^{-1}\rangle, && \mathbf{m}\geq 3,\\ SD_{2^{\mathbf{m}}}&=\langle x,y\mid x^{2^{\mathbf{m}-1}}=y^2=1,\, y^{-1}xy=x^{2^{\mathbf{m}-2}-1}\rangle, && \mathbf{m}\geq 4. \end{aligned}$$

Let N be the kernel of the surjective homomorphism $G_n\to Q_{2^m}$ induced by the restriction map $\mathrm{Gal}(\mathcal{L}(k_n)/k_n)\to\mathrm{Gal}(\mathcal{L}(k_1)/k_1)$. Then N is contained in the commutator subgroup $\langle x^2\rangle\simeq\mathbb{Z}/2^{\mathbf{m}-2}\mathbb{Z}$. We have $N=\langle x^{2^{m-1}}\rangle\simeq\mathbb{Z}/2^{\mathbf{m}-m}\mathbb{Z}$, and $x^{2^{m-1}}\in N$ but $x^{2^{m-2}}\notin N$. If $G_n=D_{2^{\mathbf{m}}}$, we can see that $G_n/N\simeq D_{2^m}$, which is a contradiction. If $G_n=SD_{2^{\mathbf{m}}}$, we may assume that

$\mathbf{m} \geq m+1$ and $\#N \neq 1$. Then $\mathbf{m}-2 \geq m-1$, we have $x^{2^{\mathbf{m}-2}} \in N$, and

$$y^{-1}xy = x^{2^{\mathbf{m}-2}-1} \equiv x^{-1} \pmod N.$$

Therefore, we infer that $G_n/N \simeq D_{2^m}$, a contradiction. Hence $G_n = Q_{2^{\mathbf{m}}}$ for some $\mathbf{m} \geq m$. Assume that $\mathbf{m} > m$, i.e., $\#N \neq 1$. Then $\mathbf{m}-2 \geq m-1$ and

$$y^2 = x^{2^{\mathbf{m}-2}} \equiv 1 \pmod N.$$

Hence $G_n/N \simeq D_{2^m}$, a contradiction. Thus, we have $\mathbf{m} = m$, i.e., $\#N = 1$ and $G_n = Q_{2^m}$ for each $n \geq 1$. Therefore, $\mathrm{Gal}(\mathcal{L}(k_n)/k_n) \simeq \mathrm{Gal}(\mathcal{L}(k_1)/k_1) \simeq Q_{2^m}$ for all $n \geq 1$, and

$$G = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty) \simeq Q_{2^m}.$$

Recall that $2^m = \#A(\mathbb{Q}(\sqrt{2p_1}, \sqrt{p_2}))$. This completes the proof of Theorem 2. ∎

7. A question. As mentioned in the Introduction, under the assumption that Greenberg's conjecture holds, it seems that the Galois group $G = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$ for totally real k_∞ has similar properties to the Galois group of a 2-class field tower of a finite extension of $\mathbb{Q}$. By the results of Kisilevsky [10] and Benjamin–Snyder [5], all the types Q_{2^m}, D_{2^m}, SD_{2^m}, $(2,2)$ appear as the Galois groups of 2-class field towers of quadratic fields. From this point of view, we have the following question.

QUESTION 10. *For the cyclotomic $\mathbb{Z}_2$-extensions k_∞ of real quadratic fields k, does each of the types Q_{2^m}, D_{2^m}, SD_{2^m}, $(2,2)$ appear as the Galois group $G = \mathrm{Gal}(\mathcal{L}(k_\infty)/k_\infty)$?*

For the types D_{2^m}, $(2,2)$, we have infinite families by Theorems 1 and 8. For the type Q_{2^m}, we have some computational examples in Theorem 2, but we have not obtained any infinite families. For the remaining type SD_{2^m}, we have no example even for the general totally real number field k. To obtain a real quadratic field with $G \simeq SD_{2^m}$, we have to deal with other real quadratic fields which are not treated in Proposition 7 and Theorem 2. At present, the above question is still an open problem.

REMARK. Part of results (Proposition 7, Theorem 8, Lemma 9, etc.) can be proven as a consequence of the theorems of A. Azizi and A. Mouhib [2] (cf. Théorème 5, Théorème 15, etc.).

References

[1] A. Azizi et 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), 2741–2752.

[2] A. Azizi et 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), 27–63.
[3] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$, J. Number Theory 67 (1997), 229–245.
[4] —, —, —, *Real quadratic fields with abelian 2-class field tower*, ibid. 73 (1998), 182–194.
[5] E. Benjamin and C. Snyder, *Real quadratic number fields with 2-class group of type* $(2,2)$, Math. Scand. 76 (1995), 161–178.
[6] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., Providence, RI, 1983.
[7] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A 70 (1994), 264–266.
[8] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.
[9] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.
[10] H. Kisilevsky, *Number fields with class number congruent to 4 mod 8 and Hilbert's theorem* 94, J. Number Theory 8 (1976), 271–279.
[11] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. 10 (1956), 65–85.
[12] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I 4 (1943), 383–406.
[13] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. 66 (1994), 245–260.
[14] Y. Mizusawa, *On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields*, J. Number Theory 105 (2004), 203–211.
[15] —, *On the Iwasawa invariants of $\mathbb{Z}_2$-extensions of certain real quadratic fields*, Tokyo J. Math. 27 (2004), 255–261.
[16] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.
[17] G. Yamamoto, *Iwasawa invariants of abelian p-extension fields*, thesis, Waseda Univ., 2000.

Department of Mathematical Sciences
School of Science and Engineering
Waseda University
3-4-1, Okubo, Shinjuku-ku
Tokyo, 169-8555 Japan
E-mail: mizusawa@akane.waseda.jp

Current address:
Department of Mathematics
Sophia University
7-1, Kioi-cho Chiyoda-ku
Tokyo, 102-8554 Japan
E-mail: mizusawa@mm.sophia.ac.jp

Received on 21.12.2004 (4915)