Mizusawa, Y.
Osaka J. Math.
53 (2016), 1063–1088

ON CERTAIN 2-EXTENSIONS OF $\mathbb{Q}$ UNRAMIFIED AT 2 AND ∞

YASUSHI MIZUSAWA

(Received March 3, 2015, revised October 20, 2015)

Abstract

Based on the method of Boston and Leedham-Green et al. for computing the Galois groups of tamely ramified p-extensions of number fields, this paper gives a large family of triples of odd prime numbers such that the maximal totally real 2-extension of the rationals unramified outside the three prime numbers has the Galois group of order 512 and derived length 3. This family is characterized arithmetically, and the explicit presentation of the Galois group by generators and relations is also determined completely.

1. Introduction

Let p be a prime number. For a number field k and a finite set S of primes of k none of which lies over p, we denote by k_S the maximal pro-p-extension over k unramified outside S. Then the Galois group $\mathrm{Gal}(k_S/k)$ is a *fab* pro-p group, i.e., the maximal abelian quotient of any open subgroup is finite. In particular when $S = \emptyset$, the derived series of $\mathrm{Gal}(k_\emptyset/k)$ corresponds to the p-class field tower of k, which is a classical object in algebraic number theory. By the theorems of Golod–Shafarevich type, $\mathrm{Gal}(k_S/k)$ can be infinite. While any finite p-groups appear as $\mathrm{Gal}(k_\emptyset/k)$ for suitable k (cf. [20]), it is still a considerable problem to determine the structure (finite or not, the isomorphism class, etc.) of $\mathrm{Gal}(k_S/k)$ for given k and S. Since the characterization of metabelian $\mathrm{Gal}(k_S/k)$ has been developed relatively well (cf. [1], [3], [6] etc.), we focus on the cases where $\mathrm{Gal}(k_S/k)$ has the derived length at least 3.

For this problem, Boston and Leedham-Green [4] introduced a powerful method to compute $\mathrm{Gal}(k_S/k)$ approximately with respect to the profinite topology, which is based on the p-group generation algorithm [19]. In particular, they showed for $p = 2$ and $S = \{\infty, 5, 19\}$ that $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ is isomorphic to one of certain two finite 2-groups of order 2^{19} and derived length 4 (cf. [4, Theorem 2]). Eick and Koch [9] have extended this result to a large family of S characterized by power residue symbols and class numbers with the ingenious use of the complex conjugation in $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. On the other hand, applying this method to the case where $p = 2$ and $S = \emptyset$, Bush [7] showed for an imaginary quadratic field $k = \mathbb{Q}(\sqrt{-445})$ that $\mathrm{Gal}(k_\emptyset/k)$ is isomorphic to one of certain two finite 2-groups of order 2^8 and derived length 3 (cf. [7, Proposition 2]).

2010 Mathematics Subject Classification. Primary 11R37; Secondary 11R11, 11R32, 20D15.

As in these results (and [5], [8], [18], [22] etc.), this method often provides a few finite p-groups similar to each other (more precisely, having the common large quotients) as the candidates of the isomorphism class of $\mathrm{Gal}(k_S/k)$. Then it is a natural question that which candidate is isomorphic to $\mathrm{Gal}(k_S/k)$. In particular, we are interested in how the arithmetical conditions determine the isomorphism class. Toward this question, we need to find and compute a suitable subgroup of $\mathrm{Gal}(k_S/k)$ such that the Galois closure of the fixed field is large enough. Hence answering to this question seems still difficult if the order of $\mathrm{Gal}(k_S/k)$ is big or $S = \emptyset$ as in the cases above. Mayer [16] determined the isomorphism classes of 3-groups $\mathrm{Gal}(k_\emptyset/k)$ for some quadratic fields k individually via computing the capitulation of ideals, while it is also difficult to extend such examples to a family characterized arithmetically.

In this paper, avoiding these difficulties, we obtain the following theorem which gives a large family of S characterized by arithmetical conditions, such that the Galois 2-group $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ has the derived length 3 and the isomorphism class is completely determined. We put $p = 2$ throughout the following, and denote by $[2^{e_1}, 2^{e_2}, \dots, 2^{e_n}]$ the abelian group $\bigoplus_{i=1}^{n} \mathbb{Z}/2^{e_i}\mathbb{Z}$.

Theorem 1.1. *Let l, q and r be distinct prime numbers such that $l \equiv 5 \pmod 8$, $q \equiv r \equiv 3 \pmod 4$, $(qr)^{(l-1)/4} \equiv 1 \pmod l$ and the class number of $\mathbb{Q}(\sqrt{lqr})$ is congruent to 4 modulo 8. Let $\mathbb{Q}_S$ be the maximal (totally real) pro-2-extension of $\mathbb{Q}$ unramified outside $S = \{l,q,r\}$. Then the Galois group $G = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ is a finite 2-group of order 2^9 which has a presentation as an abstract group with two generators a, b and two relations*

$$a^{-4}[b^2, a], \quad b^{-2}[[b, a], a]a^4$$

where $[x, y] = x^{-1}y^{-1}xy$. In particular, G has the derived series $G \supset G' \supset G'' \supset \{1\}$ of length 3 such that $G/G' \simeq [2, 4]$, $G'/G'' \simeq [2, 2, 4]$ and $G'' \simeq [2, 2]$.

EXAMPLE 1.1. Using PARI/GP [24] etc., one can find 18 triples (l, q, r) satisfying the assumptions of Theorem 1.1 in the range $\max\{l, q, r\} < 100$, e.g., (5, 11, 71), (5, 19, 79), (13, 23, 43), (29, 83, 7), (37, 47, 7), (53, 7, 59), (61, 19, 3).

The proof of Theorem 1.1 is based on the methods of Boston and Leedham-Green [4] and Eick and Koch [9]. However, since $\infty \notin S$ in our case, we can not use the complex conjugation, and we have to treat more units of algebraic integers. In the next section, we calculate the abelianizations of some open subgroups of $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ as the 2-parts of ray class groups of the fixed fields. Then we prove Theorem 1.1 in the third section, using the p-group generation algorithm on GAP [23]. In the first half of the proof of Theorem 1.1, we also reach two candidates of the isomorphism class. Since 2^9 is not so big and $S \neq \emptyset$ in our case, we can identify the fixed fields of suitable subgroups by the ramification condition. Hence we can determine the isomorphism class of $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

REMARK 1.1. Under the assumptions of Theorem 1.1, the (narrow) ideal class group of $\mathbb{Q}(\sqrt{lqr})$ has the 4-rank 1. Hence the theorem of Rédei and Reichardt [21] yields that $\left(\frac{q}{l}\right) = \left(\frac{r}{l}\right) = 1$ (cf. also [2, Proposition 1]), where $\left(-\right)$ denotes the quadratic residue symbol. Then, since the number of primes dividing lqr of $\mathbb{Q}(\sqrt{d})$ is 5, where $d = -q$ or $-r$ according to $\left(\frac{r}{q}\right) = 1$ or -1, $\mathrm{Gal}(\mathbb{Q}_{S\cup\{\infty\}}/\mathbb{Q}(\sqrt{d}))$ is infinite (cf. [17, (10.10.1) Theorem]). Hence $\mathrm{Gal}(\mathbb{Q}_{S\cup\{\infty\}}/\mathbb{Q})$ is also infinite.

2. Ray class groups

2.1. Preliminaries. Let k be a number field, and S a set of ideals of k which are prime to 2. Let $S(k) = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\}$ be the ordered set of all prime ideals of k dividing $\prod_{\mathfrak{a}\in S}\mathfrak{a}$. Then k_S denotes the maximal pro-2-extension of k unramified outside $S(k)$. We denote by $A_S(k)$ the Sylow 2-subgroup of the ray class group of k modulo $\prod_{i=1}^{n}\mathfrak{p}_i$. Then $A_S(k) \simeq \mathrm{Gal}(k_S^{ab}/k)$, where k_S^{ab} denotes the maximal abelian 2-extension of k unramified outside $S(k)$. Burnside's basis theorem yields that if $A_S(k)$ is cyclic then $\mathrm{Gal}(k_S/k)$ is also cyclic, in particular $k_S = k_S^{ab}$. The definition of the ray class groups induces an exact sequence

$$\begin{array}{ccccccc}
E(k) & \xrightarrow{\varphi} & \bigoplus_{i=1}^{n}((O_k/\mathfrak{p}_i)^\times \otimes \mathbb{Z}_2) & \longrightarrow & A_S(k) & \longrightarrow & A_\emptyset(k) \longrightarrow 0, \\
\Downarrow & & \Downarrow & & & & \\
\varepsilon & \longmapsto & ((\varepsilon \bmod \mathfrak{p}_i) \otimes 1)_i & & & &
\end{array}$$

where O_k is the ring of integers in k, $E(k) = O_k^\times$ is the unit group of k, and $\mathbb{Z}_2$ denotes the ring of 2-adic integers. For each $1 \le i \le n$, we choose a primitive element $g_i \in O_k$ of the finite field $O_k/\mathfrak{p}_i$, i.e., $(O_k/\mathfrak{p}_i)^\times = \langle g_i \bmod \mathfrak{p}_i\rangle$. Let 2^{e_i} be the order of cyclic 2-group $(O_k/\mathfrak{p}_i)^\times \otimes \mathbb{Z}_2$. Then $\mathbb{Z}/2^{e_i}\mathbb{Z} \simeq (O_k/\mathfrak{p}_i)^\times \otimes \mathbb{Z}_2\colon a \bmod 2^{e_i} \mapsto (g_i^a \bmod \mathfrak{p}_i) \otimes 1$. Depending on the order in $S(k)$ and the choice of g_i $(1 \le i \le n)$, the above sequence induces the exact sequence

$$\begin{array}{ccccccc}
E(k) & \xrightarrow{\varphi_{k,S}} & [2^{e_1}, 2^{e_2}, \ldots, 2^{e_n}] & \longrightarrow & A_S(k) & \longrightarrow & A_\emptyset(k) \longrightarrow 0, \\
\Downarrow & & \Downarrow & & & & \\
\varepsilon & \longmapsto & (a_1, a_2, \ldots, a_n) & & & &
\end{array}$$

where a_i is the abbreviation of $a_i \bmod 2^{e_i}$ satisfying $\varepsilon \equiv g_i^{a_i} \bmod \mathfrak{p}_i$. Let $\{\varepsilon_j\}_{1\le j\le d} \subset E(k)$ be a system (not necessarily minimum) such that $\{\varphi_{k,S}(\varepsilon_j)\}_{1\le j\le d}$ generates $\varphi_{k,S}(E(k))$ as a $\mathbb{Z}_2$-module. Then we put a column vector

$$v_{k,S} = \begin{pmatrix} \varphi_{k,S}(\varepsilon_1) \\ \varphi_{k,S}(\varepsilon_2) \\ \vdots \\ \varphi_{k,S}(\varepsilon_d) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1d} & a_{2d} & \cdots & a_{nd} \end{pmatrix} = (a_{ij})_{1\le j\le d,\, 1\le i\le n}.$$

For any $A \in GL_d(\mathbb{Z}_2)$, the components of a vector $Av_{k,S}$ generate $\operatorname{Im}\varphi_{k,S}$. By finding suitable A such that $Av_{k,S}$ has a simple form, one can calculate $\operatorname{Coker}\varphi_{k,S}$.

REMARK 2.1. For a set Σ of ideals of k such that $\Sigma(k) = \{\mathfrak{p}_{i_1}, \mathfrak{p}_{i_2}, \dots, \mathfrak{p}_{i_m}\} \subset S(k)$ $(1 \leq i_1 < i_2 < \cdots < i_m \leq n)$, we choose the same g_{i_μ} $(1 \leq \mu \leq m)$. Then we have the exact sequence

$$E(k) \xrightarrow{\varphi_{k,\Sigma}} [2^{e_{i_1}}, 2^{e_{i_2}}, \dots, 2^{e_{i_m}}] \to A_\Sigma(k) \to A_\emptyset(k) \to 0$$

with a vector $v_{k,\Sigma} = (\varphi_{k,\Sigma}(\varepsilon_j))_{1\leq j\leq d} = (a_{i_\mu j})_{1\leq j\leq d,\, 1\leq\mu\leq m}$. If $Av_{k,S} = (b_{ij})_{1\leq j\leq d,\, 1\leq i\leq n}$ for $A \in GL_d(\mathbb{Z}_2)$, then $Av_{k,\Sigma} = (b_{i_\mu j})_{1\leq j\leq d,\, 1\leq\mu\leq m}$. Hence one can also calculate $\operatorname{Coker}\varphi_{k,\Sigma}$ simultaneously.

We use the following formula (cf. [25]) which is also often called genus formula. For a quadratic extension K/k with the Galois group $\operatorname{Gal}(K/k) = \langle\sigma\rangle$, we have

$$|\{[\mathfrak{A}] \in A_\emptyset(K) \mid \mathfrak{A}^\sigma = \mathfrak{A}\}| = \frac{|A_\emptyset(k)|2^r}{2|E(k)/E(K)^{1+\sigma}|}, \tag{2.1}$$

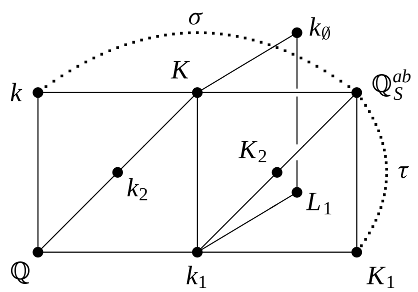
where r denotes the number of primes of k ramifying in K/k. Here we note that an ideal $\mathfrak{A}$ of K satisfies $\mathfrak{A}^\sigma = \mathfrak{A}$ if and only if $\mathfrak{A} = \mathfrak{B}(\mathfrak{a}O_K)$ for some ideal $\mathfrak{a}$ of k and a product $\mathfrak{B}$ of primes of K ramified in K/k.

2.2. Settings. In the following, we suppose that the prime numbers l, q, r satisfy the assumptions of Theorem 1.1. Put $S = \{l, q, r\}$, and put $k = \mathbb{Q}(\sqrt{lqr})$. Then $\operatorname{Gal}(\mathbb{Q}_S^{ab}/\mathbb{Q}) \simeq [2, 4]$ and $A_\emptyset(k) \simeq \mathbb{Z}/4\mathbb{Z}$. Since $A_\emptyset(k)$ has the positive 4-rank, we have $\left(\frac{q}{l}\right) = \left(\frac{r}{l}\right) = 1$ (cf. [21] or [2, Proposition 1]). Hence $q^{(l-1)/4} \equiv r^{(l-1)/4} \equiv \pm 1 \pmod{l}$. By replacing q and r suitably, we may assume that

$$q^{(l-1)/4} \equiv r^{(l-1)/4} \equiv \left(\frac{r}{q}\right) \pmod{l}. \tag{2.2}$$

Put $k_1 = \mathbb{Q}(\sqrt{l})$, $k_2 = \mathbb{Q}(\sqrt{qr})$, $K = \mathbb{Q}(\sqrt{l}, \sqrt{qr})$, $K_1 = \mathbb{Q}_{\{l,q\}}^{ab}$, $K_2 = \mathbb{Q}_{\{l,r\}}^{ab}$. Then $\operatorname{Gal}(K_1/\mathbb{Q}) \simeq \operatorname{Gal}(K_2/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, and hence $K_1 = \mathbb{Q}_{\{l,q\}}$, $K_2 = \mathbb{Q}_{\{l,r\}}$. Moreover, since $A_\emptyset(k)$ is cyclic, we have $k_\emptyset = k_\emptyset^{ab} = K_\emptyset$. Then $k_\emptyset/\mathbb{Q}$ is a dihedral extension of degree 8, and $k_\emptyset/k_1$ is a [2, 2]-extension. Let L_1, L_1' be distinct quadratic extensions of k_1 contained in $k_\emptyset$ and different from K. Then the quartic field L_1 is not a Galois extension of $\mathbb{Q}$, and the conjugate of L_1 is L_1'. We denote by σ (resp. τ) a generator of $\operatorname{Gal}(\mathbb{Q}_S^{ab}/k) \simeq \mathbb{Z}/4\mathbb{Z}$ (resp. $\operatorname{Gal}(\mathbb{Q}_S^{ab}/K_1) \simeq \mathbb{Z}/2\mathbb{Z}$). A prime ideal of a subfield of $\mathbb{Q}_S^{ab}$ dividing lqr will be denoted as in Fig. 1.

As a preparation for proof of Theorem 1.1, we obtain the following theorem.



The primes ramify (resp. are inert) in the lined (resp. dotted) extensions below.

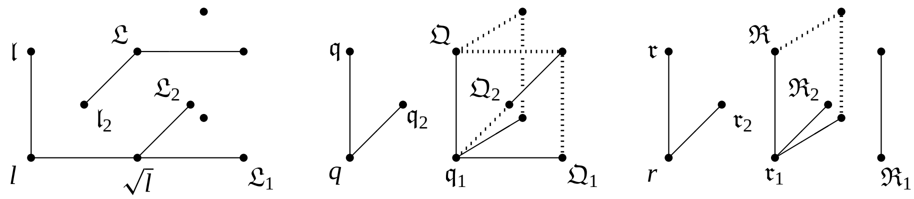


Fig. 1. Ramification in $\mathbb{Q}_S^{ab}/\mathbb{Q}$ and $k_\emptyset/\mathbb{Q}$.

Theorem 2.1. *Under the assumptions and notations above, we have*

$$A_S(k) \simeq [2, 8], \quad A_S(k_1) \simeq [2, 2, 2], \quad A_S(k_2) \simeq [4, 4],$$
$$A_S(K) \simeq [2, 2, 4], \quad A_S(K_1) \simeq [2, 2, 2, 2], \quad A_S(K_2) \simeq [4, 4].$$

2.3. Proof of Theorem 2.1. Let z_l (resp. z_q, z_r) $\in \mathbb{Z}$ be a primitive root of l (resp. q, r). We denote by $\mathfrak{l}$ (resp. $\mathfrak{q}$, $\mathfrak{r}$) the prime ideal of $k = \mathbb{Q}(\sqrt{lqr})$ lying over l (resp. q, r). Then z_l (resp. z_q, z_r) is also a primitive element of $O_k/\mathfrak{l} \simeq \mathbb{F}_l$ (resp. $O_k/\mathfrak{q} \simeq \mathbb{F}_q$, $O_k/\mathfrak{r} \simeq \mathbb{F}_r$). Since $l \equiv 5 \pmod 8$ and $q \equiv r \equiv 3 \pmod 4$, we have $|\mathbb{F}_l^\times \otimes \mathbb{Z}_2| = 4$ and $|\mathbb{F}_q^\times \otimes \mathbb{Z}_2| = |\mathbb{F}_r^\times \otimes \mathbb{Z}_2| = 2$. Let $\varepsilon > 1$ be the fundamental unit of k. For the ordered set $S(k) = \{\mathfrak{l}, \mathfrak{q}, \mathfrak{r}\}$ and these primitive elements, we have the sequence

$$E(k) \xrightarrow{\varphi_{k,S}} [4, 2, 2] \to A_S(k) \to \mathbb{Z}/4\mathbb{Z} \to 0$$

and

$$v_{k,S} = \begin{pmatrix} \varphi_{k,S}(-1) \\ \varphi_{k,S}(\varepsilon) \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ a & a_1 & a_2 \end{pmatrix}, \tag{2.3}$$

where we recall that $\varepsilon \equiv z_l^a \pmod{\mathfrak{l}}$, $\varepsilon \equiv z_q^{a_1} \pmod{\mathfrak{q}}$ and $\varepsilon \equiv z_r^{a_2} \pmod{\mathfrak{r}}$. The exponent of $A_S(k)$ and (a, a_1, a_2) are determined via the calculations on $A_S(K)$ (cf. (2.13), Lemmas 2.3 and 2.4), where some results on $A_\Sigma(k_1)$ and $A_\Sigma(k_2)$ are needed. Hence we will calculate $A_S(k)$ and $A_S(K)$ simultaneously, after proving the statements for $A_S(k_1)$ and $A_S(k_2)$.

We denote by $\mathfrak{q}_1$ (resp. $\mathfrak{r}_1$) a prime ideal of $k_1 = \mathbb{Q}(\sqrt{l})$ lying over q (resp. r). By replacing L_1 and L_1' suitably, we may assume that L_1 is the inertia field of $\mathfrak{q}_1^\sigma$ in the [2, 2]-extension $K_\emptyset/k_1$ unramified outside $\{\mathfrak{q}_1, \mathfrak{q}_1^\sigma, \mathfrak{r}_1, \mathfrak{r}_1^\sigma\}$. Since $L_1 \not\subset K_1$ and $L_1 \not\subset K_2$, L_1/k_1 is ramified at $\mathfrak{q}_1$, and ramified at $\mathfrak{r}_1$ or $\mathfrak{r}_1^\sigma$. In particular, L_1' is the inertia field of $\mathfrak{q}_1$ in $K_\emptyset/k_1$. Since $L_1' \not\subset K_1$, L_1/k_1 is unramified at $\mathfrak{r}_1$ or $\mathfrak{r}_1^\sigma$. Therefore, by replacing $\mathfrak{r}_1$ and $\mathfrak{r}_1^\sigma$ suitably, we may assume that L_1/k_1 is unramified outside $\{\mathfrak{q}_1, \mathfrak{r}_1\}$, and ramified at both $\mathfrak{q}_1$ and $\mathfrak{r}_1$. Then L_1'/k_1 is unramified outside $\{\mathfrak{q}_1^\sigma, \mathfrak{r}_1^\sigma\}$, and ramified at both $\mathfrak{q}_1^\sigma$ and $\mathfrak{r}_1^\sigma$. We also choose z_l (resp. z_q, z_r) as a primitive element of $O_{k_1}/(\sqrt{l}) \simeq \mathbb{F}_l$ (resp. $O_{k_1}/\mathfrak{q}_1 \simeq O_{k_1}/\mathfrak{q}_1^\sigma \simeq \mathbb{F}_q$, $O_{k_1}/\mathfrak{r}_1 \simeq O_{k_1}/\mathfrak{r}_1^\sigma \simeq \mathbb{F}_r$). Since $k_1 = \mathbb{Q}_{\{l\}}$, we have $A_{\{l\}}(k_1) \simeq 0$, in particular $A_\emptyset(k_1) \simeq 0$. Let $\varepsilon_1 > 1$ be the fundamental unit of k_1. For the ordered set $S(k_1) = \{(\sqrt{l}), \mathfrak{q}_1, \mathfrak{q}_1^\sigma, \mathfrak{r}_1, \mathfrak{r}_1^\sigma\}$ and these primitive elements, we have the sequence

$$E(k_1) \xrightarrow{\varphi_{k_1,S}} [4, 2, 2, 2, 2] \to A_S(k_1) \to 0$$

and

$$v_{k_1,S} = \begin{pmatrix} \varphi_{k_1,S}(-1) \\ \varphi_{k_1,S}(\varepsilon_1) \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ b & b_1 & b_1' & b_2 & b_2' \end{pmatrix}. \tag{2.4}$$

Since $\varphi_{k_1,S}(\varepsilon_1^\sigma) = (b, b_1', b_1, b_2', b_2)$ and $\varepsilon_1^{1+\sigma} = -1$, we have $2b \equiv 2 \pmod 4$ and $b_1 + b_1' \equiv b_2 + b_2' \equiv 1 \pmod 2$. If $b_1 + b_2 \equiv 1 \pmod 2$, then $\varphi_{k_1,\{\mathfrak{q}_1,\mathfrak{r}_1\}}$ is surjective, i.e., $A_{\{\mathfrak{q}_1,\mathfrak{r}_1\}}(k_1) \simeq 0$ (cf. Remark 2.1). This contradicts to the existence of quadratic extension L_1/k_1 unramified outside $\{\mathfrak{q}_1, \mathfrak{r}_1\}$. Therefore

$$b \equiv 1 \pmod 2, \quad b_1 \equiv b_2 \not\equiv b_1' \equiv b_2' \pmod 2. \tag{2.5}$$

Since

$$\begin{pmatrix} b_1 & (1+2b_1)b^{-1} \\ 1 & 2b^{-1} \end{pmatrix} v_{k_1,S} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \tag{2.6}$$

we have

$$A_S(k_1) \simeq [2, 2, 2]. \tag{2.7}$$

Moreover, we have $A_{\{l,\mathfrak{q}_1,\mathfrak{r}_1\}}(k_1) \simeq A_{\{\mathfrak{q}_1,\mathfrak{r}_1\}}(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$ (cf. Remark 2.1) and hence

$$L_1 = (k_1)_{\{\mathfrak{q}_1,\mathfrak{r}_1\}} = (k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1\}}. \tag{2.8}$$

Here, using this field L_1, we prepare the following lemma on the decomposition of primes in $k_\emptyset = K_\emptyset$.

Lemma 2.1. *$[\mathfrak{l}] = 1$ and $[\mathfrak{q}] = [\mathfrak{r}] \neq 1$ in $A_\emptyset(k)$, where $[\mathfrak{a}]$ denotes the ideal class of an ideal $\mathfrak{a}$.*

Proof. Recall that L_1 is a quadratic extension of k_1 unramified outside $\{\mathfrak{q}_1, \mathfrak{r}_1\}$. Then there is a totally positive $\alpha \in O_{k_1}$ such that $L_1 = k_1(\sqrt{\alpha})$ and $\alpha O_{k_1} = \mathfrak{q}_1\mathfrak{r}_1\mathfrak{b}^2$ with some ideal $\mathfrak{b} \subset O_{k_1}$. Note that the class number h_{k_1} of k_1 is odd. Since $\varepsilon_1^{1+\sigma} = -1$, $\mathfrak{b}^{h_{k_1}} = \beta O_{k_1}$ with some totally positive $\beta \in O_{k_1}$. Then $\alpha^{h_{k_1}} O_{k_1} = (\mathfrak{q}_1\mathfrak{r}_1)^{h_{k_1}}\beta^2$. Put $\gamma = \alpha^{h_{k_1}}\beta^{-2} \in k_1$. Since $\gamma O_{k_1} = (\mathfrak{q}_1\mathfrak{r}_1)^{h_{k_1}}$, we have $\gamma \in O_{k_1}$ and $L_1 = k_1(\sqrt{\gamma})$. There is some $x \in \mathbb{Z}$ such that $\gamma \equiv z_l^x \pmod{\sqrt{l}}$. Since γ is totally positive, $(qr)^{h_{k_1}} = \gamma^{1+\sigma} \equiv z_l^{2x} \pmod{l}$. By the assumption, $z_l^{(l-1)x/2} \equiv (qr)^{(l-1)h_{k_1}/4} \equiv 1 \pmod{l}$, and hence x is even. Hensel's lemma yields that $(\sqrt{l})$ splits in L_1/k_1. Then the prime ideals of K lying over l also split in $k_\emptyset/K$ and hence $[\mathfrak{l}] = 1$. Since $[\mathfrak{l}][\mathfrak{q}][\mathfrak{r}] = [(\sqrt{lqr})] = 1$ and $[\mathfrak{q}]^2 = [\mathfrak{r}]^2 = 1$, we have $[\mathfrak{q}] = [\mathfrak{r}]$. By the genus formula (2.1) for $k/\mathbb{Q}$, we have

$$|\langle[\mathfrak{l}], [\mathfrak{q}], [\mathfrak{r}]\rangle| = \frac{2^3}{2|E(\mathbb{Q})/E(k)^{1+\sigma}|} = 2,$$

and hence $[\mathfrak{q}] = [\mathfrak{r}] \neq 1$. Thus the proof of Lemma 2.1 is completed. $\square$

Now we calculate $A_S(k_2)$. Let $\mathfrak{l}_2$ (resp. $\mathfrak{q}_2$, $\mathfrak{r}_2$) a prime ideal of $k_2 = \mathbb{Q}(\sqrt{qr})$ lying over l (resp. q, r). Then z_l (resp. z_q, z_r) is also a primitive element of $O_{k_2}/\mathfrak{l}_2 \simeq O_{k_2}/\mathfrak{l}_2^\sigma \simeq \mathbb{F}_l$ (resp. $O_{k_2}/\mathfrak{q}_2 \simeq \mathbb{F}_q$, $O_{k_2}/\mathfrak{r}_2 \simeq \mathbb{F}_r$). Since $k_2 = \mathbb{Q}_{\{q,r\}}$, we have $A_{\{q,r\}}(k_2) \simeq 0$, in particular $A_\emptyset(k_2) \simeq 0$. Let $\varepsilon_2 > 1$ be the fundamental unit of k_2. For the ordered set $S(k_2) = \{\mathfrak{l}_2, \mathfrak{l}_2^\sigma, \mathfrak{q}_2, \mathfrak{r}_2\}$ and these primitive elements, we have the sequence

$$E(k_2) \xrightarrow{\varphi_{k_2,S}} [4, 4, 2, 2] \to A_S(k_2) \to 0$$

and

$$v_{k_2,S} = \begin{pmatrix} \varphi_{k_2,S}(-1) \\ \varphi_{k_2,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 \\ c & c' & c_1 & c_2 \end{pmatrix}. \tag{2.9}$$

Since $\varphi_{k_2,S}(\varepsilon_2^\sigma) = (c', c, c_1, c_2)$ and $\varepsilon_2^{1+\sigma} = 1$, we have $c + c' \equiv 0 \pmod 4$. Since the [2, 2]-extension $K_\emptyset/k_2$ is unramified outside $\{l\}$, $A_{\{l\}}(k_2) \simeq \operatorname{Coker}\varphi_{k_2,\{l\}} = [4, 4]/\langle(2, 2), (c, c')\rangle$ is not cyclic, and hence c and c' are even. Since $\operatorname{Coker}\varphi_{k_2,\{q,r\}} \simeq A_{\{q,r\}}(k_2) \simeq 0$, we have $c_1 + c_2 \equiv 1 \pmod 2$. Therefore

$$c \equiv c' \equiv 0 \pmod 2, \quad c \equiv c' \pmod 4, \quad c_1 \not\equiv c_2 \pmod 2. \tag{2.10}$$

Since

$$\begin{pmatrix} 1 + \dfrac{c}{2} & -1 \\ -\dfrac{c}{2} & 1 \end{pmatrix} v_{k_2,S} = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

we have

$$A_S(k_2) \simeq [4, 4].$$

Moreover, for $\Sigma = \{l, q\}$ or $\{l, r\}$, we have

$$\begin{pmatrix} 1+\dfrac{c}{2} & -1 \\ -\dfrac{c}{2} & 1 \end{pmatrix} v_{k_2,\Sigma} = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore

$$A_{\{l,q\}}(k_2) \simeq [4, 4] \quad \text{or} \quad A_{\{l,r\}}(k_2) \simeq [4, 4]. \tag{2.11}$$

Using the results above, $A_S(k)$ and $A_S(K)$ are calculated simultaneously as follows. Let $\mathfrak{L}$ (resp. $\mathfrak{Q}$, $\mathfrak{R}$) be a prime ideal of $K = \mathbb{Q}(\sqrt{l}, \sqrt{qr})$ lying over $\mathfrak{l}_2$ (resp. $\mathfrak{q}_1$, $\mathfrak{r}_1$). Then z_l (resp. z_q, z_r) is also a primitive element of $O_K/\mathfrak{L} \simeq O_K/\mathfrak{L}^\sigma \simeq \mathbb{F}_l$ (resp. $O_K/\mathfrak{Q} \simeq O_K/\mathfrak{Q}^\sigma \simeq \mathbb{F}_q$, $O_K/\mathfrak{R} \simeq O_K/\mathfrak{R}^\sigma \simeq \mathbb{F}_r$). For the ordered set $S(K) = \{\mathfrak{L}, \mathfrak{L}^\sigma, \mathfrak{Q}, \mathfrak{Q}^\sigma, \mathfrak{R}, \mathfrak{R}^\sigma\}$ and these primitive elements, we have the exact sequence

$$E(K) \xrightarrow{\varphi_{K,S}} [4, 4, 2, 2, 2, 2] \to A_S(K) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Lemma 2.2. $E(K) = \langle -1, \sqrt{\varepsilon}, \varepsilon_1, \varepsilon_2 \rangle$.

Proof. Kuroda's class number formula (cf. [15])

$$|A_\emptyset(K)| = \frac{1}{4}|E(K)/\langle -1, \varepsilon, \varepsilon_1, \varepsilon_2\rangle| \cdot |A_\emptyset(k)| \cdot |A_\emptyset(k_1)| \cdot |A_\emptyset(k_2)|$$

for $K/\mathbb{Q}$ yields that $|E(K)/\langle -1, \varepsilon, \varepsilon_1, \varepsilon_2\rangle| = 2$. Recall that $\mathrm{Gal}(K/k_2) = \langle \tau\sigma|_K \rangle$. Since $\varepsilon^{1+\tau} = \varepsilon_2^{1+\sigma} = 1$ and $\varepsilon_1^{1+\sigma} = -1$, one of $\sqrt{\varepsilon}$, $\sqrt{\varepsilon_2}$, $\sqrt{\varepsilon\varepsilon_2}$ is contained in $E(K)$. Since $\mathfrak{l}_2$ ramifies in K/k_2, we have $\sqrt{\varepsilon_2} \notin E(K)$. Since $(\varepsilon\varepsilon_2)^{1+\tau\sigma} = \varepsilon_2^2$, we have $(\sqrt{\varepsilon\varepsilon_2})^{1+\tau\sigma} = \pm\varepsilon_2$. By Lemma 2.1, both $\mathfrak{L}$ and $\mathfrak{L}^\sigma$ split in $K_\emptyset/K$. The genus formula (cf. (2.1))

$$1 = |\langle [\mathfrak{L}], [\mathfrak{L}^\sigma] \rangle \cap A_\emptyset(K)| = \frac{|A_\emptyset(k_2)| 2^2}{2|E(k_2)/E(K)^{1+\tau\sigma}|}$$

for K/k_2 yields that $|E(k_2)/E(K)^{1+\tau\sigma}| = 2$. Since $-1 = \varepsilon_1^{1+\sigma} = \varepsilon_1^{1+\tau\sigma} \in E(K)^{1+\tau\sigma}$, we have $\sqrt{\varepsilon\varepsilon_2} \notin E(K)$. Therefore $\sqrt{\varepsilon} \in E(K)$ and hence $E(K) = \langle -1, \sqrt{\varepsilon}, \varepsilon_1, \varepsilon_2 \rangle$. The proof of Lemma 2.2 is completed. □

By Lemma 2.2 and (2.4), (2.9), we have

$$v_{K,S} = \begin{pmatrix} \varphi_{K,S}(-1) \\ \varphi_{K,S}(\sqrt{\varepsilon}) \\ \varphi_{K,S}(\varepsilon_1) \\ \varphi_{K,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 & 1 & 1 \\ d & d' & d_1 & d_1' & d_2 & d_2' \\ b & b & b_1 & b_1' & b_2 & b_2' \\ c & c' & c_1 & c_1 & c_2 & c_2 \end{pmatrix}. \tag{2.12}$$

Since $\varphi_{K,S}(\varepsilon) = (a, a, a_1, a_1, a_2, a_2) \in \varphi_{K,S}(E(K)^2) \subset 2[4, 4, 2, 2, 2, 2]$ (cf. (2.3)), we have

$$a \equiv a_1 \equiv a_2 \equiv 0 \pmod 2. \tag{2.13}$$

Then $\varphi_{K,S}(\sqrt{\varepsilon}) = (d, d', d_1, d_1', d_2, d_2')$ satisfies $2d \equiv 2d' \equiv a \pmod 4$. Since $\varphi_{K,S}(-\sqrt{\varepsilon}) = \varphi_{K,S}((\sqrt{\varepsilon})^\sigma) = (d', d, d_1', d_1, d_2', d_2)$, we have

$$d' \equiv 2 + d \pmod 4, \quad d_1' \not\equiv d_1 \pmod 2, \quad d_2' \not\equiv d_2 \pmod 2. \tag{2.14}$$

The following lemma and (2.13) determine $\varphi_{k,S}(\varepsilon) = (a, a_1, a_2)$.

Lemma 2.3. $2d \equiv 2d' \equiv a \equiv 2 \pmod 4$.

Proof. Put $\Sigma = \{l, q\}$ or $\{l, r\}$ such that $A_\Sigma(k_2) \simeq [4, 4]$ (cf. (2.11)). We consider the exact sequence

$$E(k) \xrightarrow{\varphi_{k,\Sigma}} [4, 2] \to A_\Sigma(k) \to \mathbb{Z}/4\mathbb{Z} \to 0.$$

Since there is a $[2, 4]$-extension $k_\emptyset \mathbb{Q}_S^{ab}/k$ unramified outside $\{l\} \subset \Sigma$, $A_\Sigma(k)$ is not cyclic. Assume that $a \equiv 0 \pmod 4$, i.e., $d \equiv d' \equiv 0 \pmod 2$. Then, since

$$v_{k,\Sigma} = \begin{pmatrix} \varphi_{k,\Sigma}(-1) \\ \varphi_{k,\Sigma}(\varepsilon) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$$

(cf. (2.3) and (2.13)), we have $\operatorname{Coker} \varphi_{k,\Sigma} \simeq \mathbb{Z}/4\mathbb{Z}$, and hence $A_\Sigma(k) \simeq [2, 8]$ or $[4, 4]$. On the other hand, we have the sequence

$$E(K) \xrightarrow{\varphi_{K,\Sigma}} [4, 4, 2, 2] \to A_\Sigma(K) \to \mathbb{Z}/2\mathbb{Z} \to 0$$

and

$$v_{K,\Sigma} = \begin{pmatrix} \varphi_{K,\Sigma}(-1) \\ \varphi_{K,\Sigma}(\sqrt{\varepsilon}) \\ \varphi_{K,\Sigma}(\varepsilon_1) \\ \varphi_{K,\Sigma}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 \\ d & d' & d_i & d_i' \\ b & b & b_i & b_i' \\ c & c' & c_i & c_i \end{pmatrix}$$

where $i = 1$ if $\Sigma = \{l, q\}$, and $i = 2$ if $\Sigma = \{l, r\}$ (cf. (2.12)). Since

$$\begin{pmatrix} 1 & 0 & -2b^{-1} & 0 \\ -d_i & 1 & (2d_i - d)b^{-1} & 0 \\ -b_i & 0 & (2b_i + 1)b^{-1} & 0 \\ -c_i & 0 & (2c_i - c)b^{-1} & 1 \end{pmatrix} v_{K,\Sigma} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(cf. (2.5), (2.10) and (2.14)), we have $\operatorname{Coker} \varphi_{K,\Sigma} \simeq \mathbb{Z}/4\mathbb{Z}$. In particular, $2|A_\Sigma(K)| = |A_\Sigma(k)| = 16$. By the same argument to the proof of [2, Proposition 7], we have

$k_\Sigma^{ab} = k_\Sigma$. Since K/k_2 is unramified outside $\{l\}$, $(k_2)_\Sigma = k_\Sigma$ and hence $A_\Sigma(k_2) \simeq [4,4]$ is a quotient of the group $\mathrm{Gal}(k_\Sigma/k_2)$ of order 16. Therefore $(k_2)_\Sigma^{ab} = k_\Sigma$ and $\mathrm{Gal}(k_\Sigma/k_2) \simeq [4,4]$. Then both $\mathrm{Gal}(K/k) = \langle \sigma|_K \rangle$ and $\mathrm{Gal}(K/k_2) = \langle \tau\sigma|_K \rangle$ act on $A_\Sigma(K) \simeq \mathrm{Gal}(k_\Sigma/K)$ trivially, $\mathrm{Gal}(K/k_1) = \langle \tau|_K \rangle$ also acts on $\mathrm{Gal}(k_\Sigma/K)$ trivially, i.e., k_Σ/k_1 is an abelian extension of degree 16 unramified outside S. However, we have seen that $|A_S(k_1)| = 8$ (cf. (2.7)). This contradiction implies that $a \equiv 2 \pmod 4$. Thus the proof of Lemma 2.3 is completed. □

In order to determine the exponent of $A_S(k)$, we consider a quotient $A_{\{q,r\}}(k)$. The exact sequence

$$E(k) \xrightarrow{\varphi_{k,\{q,r\}}} [2,2] \to A_{\{q,r\}}(k) \to \mathbb{Z}/4\mathbb{Z} \to 0$$

with

$$v_{k,\{q,r\}} = \begin{pmatrix} \varphi_{k,\{q,r\}}(-1) \\ \varphi_{k,\{q,r\}}(\varepsilon) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

(cf. (2.3) and (2.13)) yields that $A_{\{q,r\}}(k) \simeq [2,4]$ or $\mathbb{Z}/8\mathbb{Z}$.

Lemma 2.4. $A_{\{q,r\}}(k) \simeq \mathbb{Z}/8\mathbb{Z}$.

Proof. If $A_{\{q,r\}}(k) \simeq [2,4]$, there is uniquely a $[2,2]$-extension F/k unramified outside $\{\mathfrak{q}, \mathfrak{r}\}$. Then $F/\mathbb{Q}$ is a 2-extension unramified outside S, and $\mathrm{Gal}(F/\mathbb{Q})$ is a 2-group of order 8 with two generators (i.e., a dihedral group, a quaternion group, or $[2,4]$). Hence $\mathrm{Gal}(F/\mathbb{Q})$ has a cyclic maximal subgroup. The maximal subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are $\mathrm{Gal}(F/k) \simeq [2,2]$, $\mathrm{Gal}(F/k_1)$ and $\mathrm{Gal}(F/k_2)$. Since $A_S(k_1) \simeq [2,2,2]$ (cf. (2.7)), we have $\mathrm{Gal}(F/k_1) \not\simeq \mathbb{Z}/4\mathbb{Z}$. Since $\mathfrak{l}_2$ ramifies in K/k_2 and $\mathfrak{L}$ does not ramify in F/K, $\mathrm{Gal}(F/k_2)$ can not be cyclic. This is a contradiction. Therefore $A_{\{q,r\}}(k)$ is cyclic, i.e., $A_{\{q,r\}}(k) \simeq \mathbb{Z}/8\mathbb{Z}$. The proof of Lemma 2.4 is completed. □

Lemma 2.3 and (2.13) yield that $\varphi_{k,S}(\varepsilon) = (2,0,0)$, i.e., $\mathrm{Coker}\,\varphi_{k,S} \simeq [2,2]$ (cf. (2.3)). Since $A_S(k)$ has a quotient $A_{\{q,r\}}(k) \simeq \mathbb{Z}/8\mathbb{Z}$ (cf. Lemma 2.4), we have

$$A_S(k) \simeq [2,8].$$

On the other hand, by (2.5), (2.10), (2.12), (2.13), (2.14) and Lemma 2.3,

$$Av_{K,S} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{2.15}$$

for

$$A = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & d_1 - d_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 - d_1 & 1 & 0 & 0 \\ -b_1 & 0 & 1 & 0 \\ -c_1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2b^{-1} & 0 \\ 0 & 1 & -db^{-1} & 0 \\ 0 & 0 & b^{-1} & 0 \\ 0 & 0 & -cb^{-1} & 1 \end{pmatrix}.$$

Hence $\operatorname{Coker} \varphi_{K,S} \simeq [2, 2, 2]$. Since $A_S(K)$ has a quotient $A_{\{q,r\}}(K) \simeq \mathbb{Z}/4\mathbb{Z}$ (cf. Lemma 2.4), we have

$$A_S(K) \simeq [2, 2, 4].$$

Here we prepare the following lemma which we need for the calculations of $A_S(K_1)$ and $A_S(K_2)$.

Lemma 2.5. $A_{\{l,q\}}(K) \simeq [2, 2, 2]$.

Proof. Since

$$Av_{K,\{l,q\}} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$Av_{K,\{l,r\}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

we have the exact sequences

$$0 \to [2, 2] \to A_\Sigma(K) \to \mathbb{Z}/2\mathbb{Z} \to 0$$

for $\Sigma = \{l, q\}$ and $\Sigma = \{l, r\}$. Then $\mathrm{Gal}(K_\Sigma^{ab}/K_\emptyset) \simeq [2, 2]$, and $A_\Sigma(K) \simeq [2, 2, 2]$ or $[2, 4]$.

First, we show that $A_{\{l,r\}}(K) \simeq [2, 4]$. Since $K_2 = \mathbb{Q}_{\{l,r\}} = (k_1)_{\{l,r\}}$, we have $A_{\{l,r\}}(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$. Put $\mathfrak{A} = \mathfrak{Q}^{(h_K/2)((l-1)/4)((r-1)/2)}$ and put $\mathfrak{a}_1 = \mathfrak{q}_1^{(h_K/2)((l-1)/4)((r-1)/2)}$ where h_K is the class number of K. Then $\mathfrak{a}_1 O_K = \mathfrak{A}^2$, $[\mathfrak{A}] \in A_{\{l,r\}}(K)$ and $[\mathfrak{a}_1] \in A_{\{l,r\}}(k_1)$. Since $\mathfrak{q}_1$ is inert in K_2/k_1 by the assumption (2.2), we have $A_{\{l,r\}}(k_1) = \langle [\mathfrak{a}_1] \rangle$. Now we suppose that $A_{\{l,r\}}(K) \simeq [2, 2, 2]$. Since $[\mathfrak{A}]^2 = 1$, the mapping $A_{\{l,r\}}(k_1) \to A_{\{l,r\}}(K)$: $[\mathfrak{a}] \mapsto [\mathfrak{a} O_K]$ is zero mapping. Then $A_{\{l,r\}}(K)^{\tau-1} = A_{\{l,r\}}(K)^{1+\tau} \simeq 0$, where we note that $\mathrm{Gal}(K/k_1) = \langle \tau|_K \rangle$. This implies that $K_{\{l,r\}}^{ab}/k_1$ is an abelian extension of degree 16. However, we have seen that $|A_S(k_1)| = 8$ (cf. (2.7)). This is a contradiction. Therefore $A_{\{l,r\}}(K) \simeq [2, 4]$.

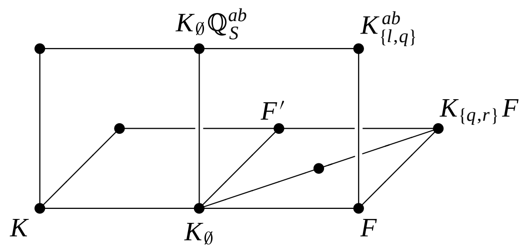


Fig. 2. Proof of Lemma 2.5.

Suppose that $A_{\{l,q\}}(K) \simeq [2, 4]$. Then $K_{\emptyset}\mathbb{Q}_S^{ab}$ is the unique [2, 2]-extension of K contained in $K_{\{l,q\}}^{ab}$. Let F be the inertia field of $\mathfrak{L}^{\sigma}$ in $K_{\{l,q\}}^{ab}/K$. Since the inertia group $\mathrm{Gal}(K_{\{l,q\}}^{ab}/F)$ is cyclic and $K_{\emptyset} \subset F \subset K_{\{l,q\}}^{ab}$, F/K is a quartic extension. Since $K_{\emptyset}\mathbb{Q}_S^{ab}/K$ is not unramified at $\mathfrak{L}^{\sigma}$, $F \neq K_{\emptyset}\mathbb{Q}_S^{ab}$ and hence F/K is a cyclic extension of degree 4 unramified outside $\{\mathfrak{L}, \mathfrak{Q}, \mathfrak{Q}^{\sigma}\}$. Since

$$Av_{K,\{\mathfrak{L},\mathfrak{Q}\}} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad Av_{K,\{\mathfrak{L},\mathfrak{Q}^{\sigma}\}} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$$

and

$$Av_{K,\{q\}} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix},$$

we have $K_{\{\mathfrak{L},\mathfrak{Q}\}} = K_{\{\mathfrak{L},\mathfrak{Q}^{\sigma}\}} = K_{\{q\}} = K_{\emptyset}$. This implies that $F/K_{\emptyset}$ is ramified at any primes dividing $\mathfrak{L}q$. Recall that $\mathrm{Gal}(K_{\{q,r\}}/K) \simeq A_{\{q,r\}}(K) \simeq \mathbb{Z}/4\mathbb{Z}$ by Lemma 2.4. Then $K_{\{q,r\}}F/K$ is a $[2,4]$-extension such that $\mathrm{Gal}(K_{\{q,r\}}F/K_{\emptyset}) \simeq [2,2]$. Since $K_{\{q,r\}} = k_{\{q,r\}}$ and

$$v_{k,\{q\}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad v_{k,\{r\}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$K_{\{q,r\}}/K_{\emptyset}$ is ramified at any primes dividing qr. Let F' be the unique $[2,2]$-extension of K contained in $K_{\{q,r\}}F$. Since $F/K_{\emptyset}$ and $K_{\{q,r\}}/K_{\emptyset}$ are ramified at any primes dividing q, F' is the inertia field of any primes dividing q in the [2, 2]-extension $K_{\{q,r\}}F/K_{\emptyset}$, i.e., $F'/K_{\emptyset}$ is unramified at any primes dividing q. Hence F'/K is a [2, 2]-extension unramified outside $\{\mathfrak{L}, r\}$. Since $\mathbb{Q}_S^{ab}/K$ is ramified at $\mathfrak{L}^{\sigma}$, we have $\mathbb{Q}_S^{ab} \cap F' = K$. Thus we obtain a [2, 2, 2]-extension $F'\mathbb{Q}_S^{ab}/K$ unramified outside $\{l, r\}$. However, we have seen that $A_{\{l,r\}}(K) \simeq [2, 4]$. This contradiction yields that $A_{\{l,q\}}(K) \simeq [2, 2, 2]$. Thus the proof of Lemma 2.5 is completed. $\square$

We calculate $A_S(K_2)$ as follows. Let $\mathfrak{L}_2$ (resp. $\mathfrak{Q}_2$, $\mathfrak{R}_2$) be a prime ideal of K_2 lying over $(\sqrt{l})$ (resp. $\mathfrak{q}_1$, $\mathfrak{r}_1$). By the assumption (2.2), the prime $\mathfrak{q}_1$ is inert in K_2/k_1, i.e., $\mathfrak{Q}_2 = \mathfrak{q}_1 O_{K_2}$.

Lemma 2.6. *$A_{\{\mathfrak{Q}_2\}}(K_2) \simeq \mathbb{Z}/2\mathbb{Z}$, the 4-rank of $A_{\{q\}}(K_2)$ is 1, and $|A_{\{q,r\}}(K_1)| \geq 8$.*

Proof. Since $A_\emptyset(K_2) \simeq 0$, the exact sequence

$$E(K_2) \to (O_{K_2}/\mathfrak{Q}_2)^\times \otimes \mathbb{Z}_2 \to A_{\{\mathfrak{Q}_2\}}(K_2) \to 0$$

and the cyclicity of $(O_{K_2}/\mathfrak{Q}_2)^\times$ imply that $A_{\{\mathfrak{Q}_2\}}(K_2)$ is cyclic. Recall that there is a quadratic extension L_1/k_1 unramified outside $\{\mathfrak{q}_1, \mathfrak{r}_1\}$ and ramified at both $\mathfrak{q}_1$ and $\mathfrak{r}_1$. Then K_2L_1/K_2 is a quadratic extension unramified outside $\{\mathfrak{Q}_2\}$ and ramified at $\mathfrak{Q}_2$. In particular, $|A_{\{\mathfrak{Q}_2\}}(K_2)| \neq 1$.

Suppose that $|A_{\{\mathfrak{Q}_2\}}(K_2)| \geq 4$. Then there exists uniquely a cyclic quartic extension F/K_2 unramified outside $\{\mathfrak{Q}_2\}$, and $K_2 \subset K_2L_1 \subset F$. Since $\mathfrak{Q}_2 = \mathfrak{q}_1 O_{K_2}$, F is a Galois extension of k_1. Since K_2L_1/k_1 is a $[2,2]$-extension unramified outside $\{l, \mathfrak{q}_1, r\}$, K_2L_1/L_1 is unramified outside $\{l, \mathfrak{r}_1^\sigma\}$. Then F/L_1 is a $[2,2]$-extension unramified outside $\{l, \mathfrak{q}_1, \mathfrak{r}_1^\sigma\}$. Recall that $k_1 \subset L_1 \subset K_\emptyset$ and $\mathrm{Gal}(K_\emptyset/k_1) \simeq [2,2]$. Since $\mathfrak{R}^\sigma$ is inert in $K_\emptyset/K$ by Lemma 2.1, $\mathfrak{r}_1^\sigma$ is also inert in L_1/k_1, i.e., $\mathfrak{r}_1^\sigma O_{L_1}$ is a prime of L_1 which ramifies in K_2L_1/L_1. Hence the inertia field of $\mathfrak{r}_1^\sigma O_{L_1}$ in F/L_1 is a quadratic extension of L_1 unramified outside $\{l, \mathfrak{q}_1\}$. However, we have seen that $L_1 = (k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1\}}$ (cf. (2.8)), which implies that $A_{\{l,\mathfrak{q}_1\}}(L_1) \simeq 0$. This is a contradiction. Therefore $A_{\{\mathfrak{Q}_2\}}(K_2) \simeq \mathbb{Z}/2\mathbb{Z}$.

The kernel of the surjective restriction mapping

$$\mathrm{Gal}((K_2)^{ab}_{\{q\}}/K_2) \to \mathrm{Gal}((K_2)^{ab}_{\{\mathfrak{Q}_2\}}/K_2) \simeq A_{\{\mathfrak{Q}_2\}}(K_2) \simeq \mathbb{Z}/2\mathbb{Z}$$

is the inertia group of $\mathfrak{Q}_2^\sigma$, which is cyclic. Hence the 2-rank of $A_{\{q\}}(K_2)$ is at most 2, and the 4-rank of $A_{\{q\}}(K_2)$ is at most 1. By Lemma 2.5, $K^{ab}_{\{l,q\}}/K$ is a $[2,2,2]$-extension, which is Galois over k_1. Then $K^{ab}_{\{l,q\}}/\mathbb{Q}^{ab}_S$ is a $[2,2]$-extension unramified outside $\{q\}$, and $\mathrm{Gal}(\mathbb{Q}^{ab}_S/K) = \langle \sigma^2 \rangle$ acts on $\mathrm{Gal}(K^{ab}_{\{l,q\}}/\mathbb{Q}^{ab}_S)$ trivially. Since $A_{\{q\}}(K_1) \simeq 0$, we have $A_{\{q\}}(\mathbb{Q}^{ab}_S)^{1+\tau} \simeq 0$. Hence $(A_{\{q\}}(\mathbb{Q}^{ab}_S)/2)^{\tau-1} = (A_{\{q\}}(\mathbb{Q}^{ab}_S)/2)^{1+\tau} \simeq 0$. This implies that $\mathrm{Gal}(\mathbb{Q}^{ab}_S/K_1) = \langle \tau \rangle$ acts on $\mathrm{Gal}(K^{ab}_{\{l,q\}}/\mathbb{Q}^{ab}_S)$ trivially, i.e., $K^{ab}_{\{l,q\}}/K_1$ is an abelian extension of degree 8 unramified outside $\{q,r\}$. Therefore $|A_{\{q,r\}}(K_1)| \geq 8$. Since $\mathrm{Gal}(\mathbb{Q}^{ab}_S/K_2) = \langle \sigma^2\tau \rangle$ also acts on $\mathrm{Gal}(K^{ab}_{\{l,q\}}/\mathbb{Q}^{ab}_S)$ trivially, $K^{ab}_{\{l,q\}}/K_2$ is an abelian extension of degree 8 unramified outside $\{q\}$. Then $|A_{\{q\}}(K_2)| \geq 8$. Since the 2-rank of $A_{\{q\}}(K_2)$ is at most 2, the 4-rank of $A_{\{q\}}(K_2)$ is 1. Thus the proof of Lemma 2.6 is completed. □

Let $g_q \in O_{K_2}$ be a primitive element of $O_{K_2}/\mathfrak{Q}_2 \simeq \mathbb{F}_{q^2}$ such that $g_q^{1+q} \equiv z_q \pmod{\mathfrak{Q}_2}$. Then g_q^σ is a primitive element of $O_{K_2}/\mathfrak{Q}_2^\sigma \simeq \mathbb{F}_{q^2}$ satisfying $(g_q^\sigma)^{1+q} \equiv z_q \pmod{\mathfrak{Q}_2^\sigma}$, and

z_l (resp. z_r) is also a primitive element of $O_{K_2}/\mathfrak{L}_2 \simeq \mathbb{F}_l$ (resp. $O_{K_2}/\mathfrak{R}_2 \simeq \mathbb{F}_r$). Recall that $\varepsilon_1 \equiv z_q^{b_1} \pmod{\mathfrak{q}_1}$ and $\varepsilon_1 \equiv z_q^{b_1'} \pmod{\mathfrak{q}_1^\sigma}$ (cf. (2.4)). Then $\varepsilon_1 \equiv g_q^{(1+q)b_1} \pmod{\mathfrak{Q}_2}$ and $\varepsilon_1 \equiv (g_q^\sigma)^{(1+q)b_1'} \pmod{\mathfrak{Q}_2^\sigma}$. Since the genus formula (cf. (2.1))

$$1 = \frac{2^3}{2|E(k_1)/E(K_2)^{1+\sigma^2}|}$$

for K_2/k_1 yields that $\pm\varepsilon_1 \notin E(K_2)^{1+\sigma^2} = E(k_1)^2$, we have $E(K_2) = \langle -1, \varepsilon_1, \xi_2, \xi_2^\sigma \rangle$ where ξ_2 is a relative fundamental unit of K_2 satisfying $\xi_2^{1+\sigma^2} = \pm 1$ (cf. [12], [13] or [26]). Since $\xi_2^{1+\sigma^2} \in E(K_2)^{1+\sigma^2} = E(k_1)^2$, we have $\xi_2^{1+\sigma^2} = 1$. If $\xi_2 \equiv g_q^{f_1} \pmod{\mathfrak{Q}_2}$ and $\xi_2 \equiv (g_q^\sigma)^{f_1'} \pmod{\mathfrak{Q}_2^\sigma}$, then $\xi_2^\sigma \equiv (g_q^\sigma)^{f_1} \pmod{\mathfrak{Q}_2^\sigma}$ and $\xi_2^\sigma \equiv (g_q^{\sigma^2})^{f_1'} \equiv g_q^{qf_1'}$ $\pmod{\mathfrak{Q}_2}$, where we note that σ^2 acts on $O_{K_2}/\mathfrak{Q}_2$ as the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$. Put

$$2^m = |\mathbb{F}_{q^2}^\times \otimes \mathbb{Z}_2| = |\mathbb{Z}_2/(q^2-1)\mathbb{Z}_2|.$$

Then $m \geq 3$. For the ordered set $S(K_2) = \{\mathfrak{L}_2, \mathfrak{Q}_2, \mathfrak{Q}_2^\sigma, \mathfrak{R}_2, \mathfrak{R}_2^\sigma\}$, we have the sequence

$$E(K_2) \xrightarrow{\varphi_{K_2,S}} [4, 2^m, 2^m, 2, 2] \to A_S(K_2) \to 0$$

and

$$v_{K_2,S} = \begin{pmatrix} \varphi_{K_2,S}(-1) \\ \varphi_{K_2,S}(\varepsilon_1) \\ \varphi_{K_2,S}(\xi_2) \\ \varphi_{K_2,S}(\xi_2^\sigma) \end{pmatrix} = \begin{pmatrix} 2 & 2^{m-1} & 2^{m-1} & 1 & 1 \\ b & 2^{m-1}b_1 & 2^{m-1}b_1' & b_2 & b_2' \\ f & f_1 & f_1' & f_2 & f_2' \\ f & qf_1' & f_1 & f_2' & f_2 \end{pmatrix}$$

(cf. (2.4)), where we note that $1 + q \equiv 2^{m-1} \pmod{2^m}$. Since

$$v_{K_2,\{\mathfrak{Q}_2\}} = \begin{pmatrix} 2^{m-1} \\ 2^{m-1}b_1 \\ f_1 \\ qf_1' \end{pmatrix}$$

and $A_{\{\mathfrak{Q}_2\}}(K_2) \simeq \mathbb{Z}/2\mathbb{Z}$ by Lemma 2.6, we have $f_1 \equiv f_1' \equiv 0 \pmod 2$, and either $f_1 \equiv 2 \pmod 4$ or $f_1' \equiv 2 \pmod 4$ are satisfied. In particular, $qf_1' \equiv -f_1' \pmod{2^m}$. Recalling (2.5), we have

$$A_2 v_{K_2,S} = \begin{pmatrix} 1 & 2^{m-1} & 0 & 1 & 0 \\ 1 & 0 & 2^{m-1} & 0 & 1 \\ 0 & 2h_1 & 2h_2 & f + f_2 + f_2' & 0 \\ 0 & -2h_2 & 2h_1 & 0 & f + f_2 + f_2' \end{pmatrix}$$

for

$$A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -(f+f_2') & 0 & 1 & 0 \\ -f_2' & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ fb_1 & -f & 1 & 0 \\ fb_1 & -f & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2b^{-1} & 0 & 0 \\ 0 & b^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where h_1 and h_2 are integers such that $2h_1 = f_1 - 2^{m-1}(f+f_2')$ and $2h_2 = f_1' + 2^{m-1} f_2'$. Then $h_1 \equiv 1 \pmod 2$ or $h_2 \equiv 1 \pmod 2$.

Lemma 2.7. $h_1 \equiv h_2 \equiv 1 \pmod 2$.

Proof. Suppose that $h_1 \equiv h_2 + 1 \equiv 0 \pmod 2$ or $h_1 + 1 \equiv h_2 \equiv 0 \pmod 2$. Then $h_1^2 + h_2^2 \in \mathbb{Z}_2^\times$, and hence the equation

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \dfrac{h_1}{h_1^2+h_2^2} & \dfrac{-h_2}{h_1^2+h_2^2} \\ 0 & 0 & \dfrac{h_2}{h_1^2+h_2^2} & \dfrac{h_1}{h_1^2+h_2^2} \end{pmatrix} A_2 v_{K_2,\{q\}} = \begin{pmatrix} 2^{m-1} & 0 \\ 0 & 2^{m-1} \\ 2 & 0 \\ 0 & 2 \end{pmatrix}$$

yields that $A_{\{q\}}(K_2) \simeq [2, 2]$. However, the 4-rank of $A_{\{q\}}(K_2)$ is 1 by Lemma 2.6. This is a contradiction. Therefore $h_1 \equiv h_2 \equiv 1 \pmod 2$. The proof of Lemma 2.7 is completed. $\square$

Since

$$A_2 v_{K_2,\{l,r\}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & f+f_2+f_2' & 0 \\ 0 & 0 & f+f_2+f_2' \end{pmatrix}$$

and $A_{\{l,r\}}(K_2) \simeq 0$, we have $f + f_2 + f_2' \equiv 1 \pmod 2$. By Lemma 2.7, $h_1^2 + h_2^2 \equiv 2 \pmod 4$. Then

$$A_2' A_2 v_{K_2,S} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & 0 & 4 & 0 & 0 \end{pmatrix}$$

for

$$A_2' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2^{m-3} \\ 0 & 0 & 1 & \dfrac{h_1 - h_2}{2h_1} \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2^{m-2} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 2^{m-2} & \dfrac{2h_1}{h_1^2 + h_2^2} \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \dfrac{1}{h_1} & 0 \\ 0 & 0 & \dfrac{h_2}{h_1} & 1 \end{pmatrix},$$

and hence

$$A_S(K_2) \simeq [4, 4].$$

Now we calculate $A_S(K_1)$. Let $\mathfrak{L}_1$ (resp. $\mathfrak{Q}_1$, $\mathfrak{R}_1$) be a prime ideal of K_1 lying over $(\sqrt{l})$ (resp. $\mathfrak{q}_1$, $\mathfrak{r}_1$). By the assumption (2.2), r splits completely in $K_1/\mathbb{Q}$. In particular $\mathfrak{r}_1 O_{K_1} = \mathfrak{R}_1^{1+\sigma^2}$. Then z_l (resp. z_q, z_r) is also a primitive element of $O_{K_1}/\mathfrak{L}_1 \simeq \mathbb{F}_l$ (resp. $O_{K_1}/\mathfrak{Q}_1 \simeq O_{K_1}/\mathfrak{Q}_1^{\sigma} \simeq \mathbb{F}_q$, $O_{K_1}/\mathfrak{R}_1^{\sigma^j} \simeq \mathbb{F}_r$ for any $j \in \mathbb{Z}$). Since the genus formula (cf. (2.1))

$$1 = \frac{2^3}{2|E(k_1)/E(K_1)^{1+\sigma^2}|}$$

for K_1/k_1 yields that $E(K_1)^{1+\sigma^2} = E(k_1)^2$, we have $E(K_1) = \langle -1, \varepsilon_1, \xi_1, \xi_1^{\sigma} \rangle$ with a relative fundamental unit ξ_1 of K_1 satisfying $\xi_1^{1+\sigma^2} = 1$ (cf. [12], [13] or [26]). For the ordered set $S(K_1) = \{\mathfrak{L}_1, \mathfrak{Q}_1, \mathfrak{Q}_1^{\sigma}, \mathfrak{R}_1, \mathfrak{R}_1^{\sigma^2}, \mathfrak{R}_1^{\sigma}, \mathfrak{R}_1^{\sigma^3}\}$ and the primitive elements z_l, z_q and z_r, we have the sequence

$$E(K_1) \xrightarrow{\varphi_{K_1,S}} [4, 2, 2, 2, 2, 2, 2] \to A_S(K_1) \to 0.$$

If $\varphi_{K_1,S}(\xi_1) = (s, s_1, s_1', s_2, s_2'', s_2', s_2''')$, then

$$(0, 0, 0, 0, 0, 0, 0) = \varphi_{K_1,S}(\xi_1^{1+\sigma^2}) = (2s, 0, 0, s_2 + s_2'', s_2 + s_2'', s_2' + s_2''', s_2' + s_2'''),$$

i.e., $s \equiv 0 \pmod 2$, $s_2'' \equiv s_2 \pmod 2$ and $s_2''' \equiv s_2' \pmod 2$. Thus we obtain a vector

$$v_{K_1,S} = \begin{pmatrix} \varphi_{K_1,S}(-1) \\ \varphi_{K_1,S}(\varepsilon_1) \\ \varphi_{K_1,S}(\xi_1) \\ \varphi_{K_1,S}(\xi_1^{\sigma}) \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ b & b_1 & b_1' & b_2 & b_2 & b_2' & b_2' \\ s & s_1 & s_1' & s_2 & s_2 & s_2' & s_2' \\ s & s_1' & s_1 & s_2' & s_2' & s_2 & s_2 \end{pmatrix}$$

(cf. (2.4)). Then, recalling (2.5), we have

$$A_1 v_{K_1,S} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & s_1+s_1' & 0 & s_2+s_1' & s_2+s_1' & s_2'+s_1' & s_2'+s_1' \\ 0 & s_1+s_1' & s_1+s_1' & s_2+s_2' & s_2+s_2' & s_2+s_2' & s_2+s_2' \end{pmatrix} \tag{2.16}$$

for

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ b_1 & 1 & 0 & 0 \\ s_1' & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2b^{-1} & 0 & 0 \\ 0 & b^{-1} & 0 & 0 \\ 0 & -sb^{-1} & 1 & 0 \\ 0 & -sb^{-1} & 0 & 1 \end{pmatrix}.$$

Lemma 2.8. $s_1 + s_1' \equiv s_2 + s_2' \equiv 1 \pmod 2$.

Proof. Since $\operatorname{Coker} \varphi_{K_1,\{l,q\}} \simeq A_{\{l,q\}}(K_1) \simeq 0$, we have $s_1 + s_1' \equiv 1 \pmod 2$ by (2.16). If $s_2 + s_2' \equiv 0 \pmod 2$, we have

$$\begin{pmatrix} s_2+s_1' & 0 & 1 & s_2+s_1'+1 \\ s_2+s_1' & 1 & 1 & s_2+s_1'+1 \\ s_2+s_1' & 0 & 1 & s_2+s_1' \\ 1 & 0 & 0 & 1 \end{pmatrix} A_1 v_{K_1,\{q,r\}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and $A_{\{q,r\}}(K_1) \simeq \operatorname{Coker} \varphi_{K_1,\{q,r\}} \simeq [2, 2]$. However, $|A_{\{q,r\}}(K_1)| \geq 8$ by Lemma 2.6. This contradiction yields that $s_2 + s_2' \equiv 1 \pmod 2$. Thus the proof of Lemma 2.8 is completed. □

By (2.16) and Lemma 2.8, we have

$$A_S(K_1) \simeq [2, 2, 2, 2].$$

Thus the proof of Theorem 2.1 is completed.

3. Computation of the Galois group

3.1. Preliminaries. For a pro-2 group G and the closed subgroup H, we denote by $[G, H]$ (resp. H^2) the closed subgroup of G generated by $[g, h] = g^{-1}h^{-1}gh$ (resp. h^2) ($g \in G$, $h \in H$). In particular, we put $G' = [G, G]$ and $G^{ab} = G/G'$. For a pro-2 group G, put $P_0(G) = G$ and put $P_{n+1}(G) = P_n(G)^2[G, P_n(G)]$ for $n \geq 0$ recursively. In particular, $P_1(G) = \Phi(G) = G^2[G, G]$ is the Frattini subgroup of G. Then we obtain the lower 2-central series

$$G = P_0(G) \supset P_1(G) \supset P_2(G) \supset \cdots \supset P_n(G) \supset \cdots$$

of G. The 2-class of a finite 2-group H is the smallest n such that $P_n(H) \simeq 1$. For a finite 2-group H of 2-class n, a finite 2-groups G such that $G/P_n(G) \simeq H$ is called a descendant of H. Then, if a descendant G has the 2-class $n+1$, G is called an immediate descendant of H. The p-group generation algorithm [19] allows us to find all immediate descendants of a given finite 2-group H. For instance, the ANUPQ package [11] of GAP [23] provides a function to use this algorithm.

Suppose that G is a finite 2-group of 2-class $n \geq 2$, and let $F/R \simeq G$ be a minimal presentation of G as a pro-2 group, where F is a free pro-2 group such that $F/P_1(F) \simeq G/P_1(G)$. Let $\mu(G)$ be the 2-multiplicator rank of G, i.e., the 2-rank of the 2-multiplicator $H_2(G, \mathbb{Z}/2\mathbb{Z}) \simeq R/[F, R]R^2$. Let $\nu(G)$ be the nuclear rank of G, i.e., the 2-rank of the nucleus $P_n(F)[F, R]R^2/[F, R]R^2$. Since $P_n(F) \subset R$, we have $\mu(G) \geq \nu(G)$.

3.2. Proof of Theorem 1.1. Put $G = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, and let $\mathbb{Q}_S^{(n)}$ be the maximal 2-extension of $\mathbb{Q}$ unramified outside S of which Galois group has 2-class at most n. Then $G/P_1(G) \simeq [2, 2]$ and $G/P_n(G) \simeq \mathrm{Gal}(\mathbb{Q}_S^{(n)}/\mathbb{Q})$. For a finite 2-group H, we set a condition $C(H)$ consisting of the following four statements:

1. $H^{ab} \simeq [2, 4]$.
2. For the six normal subgroups N_i $(1 \leq i \leq 6)$ of H such that

$$N_1/H' \simeq N_2/H' \simeq H/N_4 \simeq H/N_5 \simeq \mathbb{Z}/4\mathbb{Z}, \quad N_3/H' \simeq H/N_6 \simeq [2, 2],$$

there are surjective homomorphisms

$$[2, 8] \to N_{i_1}^{ab}, \quad [4, 4] \to N_{i_2}^{ab}, \quad [2, 2, 2] \to N_3^{ab},$$
$$[2, 2, 2, 2] \to N_{i_4}^{ab}, \quad [4, 4] \to N_{i_5}^{ab}, \quad [2, 2, 4] \to N_6^{ab},$$

where $(i_1, i_2) = (1, 2)$ or $(2, 1)$, and $(i_4, i_5) = (4, 5)$ or $(5, 4)$.

3. There exists some $a \in H$ such that $a^2 \notin H'$ and $b^{-1}ab = a^5$ for some $b \in H$.
4. $\mu(H/P_m(H)) - \nu(H/P_m(H)) \leq 2$ for all $m \geq 2$.

We obtain the following proposition including a translation of Theorem 2.1.

Proposition 3.1. *If $H \simeq G/P_n(G)$ for some $n \geq 2$, then H satisfies the condition $C(H)$.*

Proof. Suppose that $n \geq 2$, and put $H = \mathrm{Gal}(\mathbb{Q}_S^{(n)}/\mathbb{Q}) \simeq G/P_n(G)$. It suffices to prove that this H satisfies the condition $C(H)$. Since the quotient $\mathrm{Gal}(\mathbb{Q}_S^{ab}/\mathbb{Q}) \simeq [2, 4]$ of G is a finite 2-group of 2-class 2, we have $\mathbb{Q}_S^{ab} \subset \mathbb{Q}_S^{(2)} \subset \mathbb{Q}_S^{(n)}$. Hence there is a surjective homomorphism $H \to [2, 4]$. On the other hand, there is also a surjective homomorphism $[2, 4] \simeq G^{ab} \to H^{ab}$. Therefore $H^{ab} \simeq [2, 4]$. By the settings of the subfields of $\mathbb{Q}_S^{ab}$ in the previous section, we have

$$(\mathrm{Gal}(\mathbb{Q}_S^{(n)}/k), \mathrm{Gal}(\mathbb{Q}_S^{(n)}/k_2)) = (N_1, N_2) \quad \text{or} \quad (N_2, N_1), \quad \mathrm{Gal}(\mathbb{Q}_S^{(n)}/k_1) = N_3,$$
$$(\mathrm{Gal}(\mathbb{Q}_S^{(n)}/K_1), \mathrm{Gal}(\mathbb{Q}_S^{(n)}/K_2)) = (N_4, N_5) \quad \text{or} \quad (N_5, N_4), \quad \mathrm{Gal}(\mathbb{Q}_S^{(n)}/K) = N_6.$$

The maximal abelian quotients of these Galois groups are quotients of the corresponding ray class 2-groups. Hence the second statement of $C(H)$ holds by Theorem 2.1.

Let τ_l (resp. τ_q) be a generator of the inertia subgroup of G for a prime lying over l (resp. q). Let σ_l (resp. σ_q) be the corresponding Frobenius element, i.e., the decomposition group of the prime is generated by τ_l and σ_l (resp. τ_q and σ_q). Then the pro-2 group G has a minimal presentation with 2 generators corresponding to τ_l, τ_q and 2 relations represented by $\sigma_l\tau_l\sigma_l^{-1} = \tau_l^l$, $\sigma_q\tau_q\sigma_q^{-1} = \tau_q^q$ in G (cf. [14, Theorem 11.10 and Example 11.12]). In particular, we have $\mathrm{Gal}(\mathbb{Q}_S^{ab}/k_2) = \langle \tau_l|_{\mathbb{Q}_S^{ab}} \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, and G has trivial Schur multiplicator. Put $b = \sigma_l^{-u}|_{\mathbb{Q}_S^{(n)}} \in H$, where $u = \log_2 5/\log_2 l \in \mathbb{Z}_2$ and $\log_2$ denotes the 2-adic logarithm. Then $a = \tau_l|_{\mathbb{Q}_S^{(n)}} \in H$ satisfies $b^{-1}ab = a^5$. Since $\mathbb{Q}_S^{ab} \subset \mathbb{Q}_S^{(n)}$, we have $a^2 \notin H'$. On the other hand, $H/P_m(H) \simeq G/P_m(G)$ for all $m \leq n$, and $H/P_m(H) \simeq H/P_n(H) \simeq H$ for all $m \geq n$. Therefore the last statement of $C(H)$ also holds by [4, Lemma]. Thus the proof of Proposition 3.1 is completed. $\square$

Suppose that a finite 2-group H of 2-class $n+1 \geq 3$ satisfies the condition $C(H)$ with the six subgroups N_i. Since the 2-class of $H^{ab} \simeq [2, 4]$ is 2, we have $P_n(H) \subset P_2(H) \subset [H, H] \subset N_i$. Then $\overline{H} = H/P_n(H)$ also satisfies the condition $C(\overline{H})$ with the six subgroups $\overline{N}_i = N_i/P_n(H)$ for the second statement of $C(\overline{H})$. Thus we can define a rooted tree T such that the root is the isomorphism class of $[2, 2]$, the other vertices are the isomorphism classes of finite 2-groups H satisfying the condition $C(H)$, and the edges have the extremities H and $\overline{H}$ such that H is an immediate descendant of $\overline{H}$. Proposition 3.1 yields that $G/P_n(G)$ is isomorphic to one of the vertices of this tree T. For each $n \geq 2$, all vertices of T of 2-class at most n are computable with the repeated use of the p-group generation algorithm. To compute them, we use GAP [23] and ANUPQ package [11] here. A program as in Fig. 3 returns a result which indicates that T has no vertex of 2-class greater than 6 and the diagram of T is of the form as in Fig. 4. In particular, T is finite. Therefore G is a finite 2-group of 2-class at most 6, and G is isomorphic to one of the vertices of T.

Recall that $H^2(G, \mathbb{Z}/2\mathbb{Z}) \simeq [2, 2]$ (cf. [14, Theorem 11.10 and Example 11.12] or [17, (10.7.15) Theorem]). A function on GAP which computes $H^2(H, \mathbb{Z}/2\mathbb{Z})$ for a given finite 2-group H is provided by HAP package [10]. Applying this function to all vertices H of T, which have been computed by a program as in Fig. 3, we find only two vertices H such that $H^2(H, \mathbb{Z}/2\mathbb{Z}) \simeq [2, 2]$. These two vertices $G_1 =$ `G[1][1]` and $G_2 =$ `G[2][1]` are identified by codes in GAP as in Fig. 5. Then G is isomorphic to G_1 or G_2, which are finite 2-groups of order 512 and 2-class 6 such that $G_1/P_5(G_1) \simeq G_2/P_5(G_2)$.

```
f := function(G, A) # checks the existence of a surjective homomorphism A --> G/[G, G].
return (AbelianInvariants(G) in Set(AllSubgroups(AbelianGroup(A)), x->AbelianInvariants(x)));
end;;

h := function(H) local D, N, r, a; # checks the condition C(H) except for 4th statement.
if AbelianInvariants(H) = [2, 4] then
D := DerivedSubgroup(H); N := IntermediateSubgroups(H, D).subgroups;
SortParallel(List(N, x->[Index(H, x), RankPGroup(FactorGroup(x, D)), RankPGroup(FactorGroup(H, x))]), N);
  if ((f(N[1], [2, 8]) and f(N[2], [4, 4])) or (f(N[2], [2, 8]) and f(N[1], [4, 4]))) and f(N[3], [2, 2, 2])
  and ((f(N[4], [2, 2, 2, 2]) and f(N[5], [4, 4])) or (f(N[5], [2, 2, 2, 2]) and f(N[4], [4, 4]))) and f(N[6], [2, 2, 4])
  then r := 0; for a in H do if (not (a^2 in D)) and (a^5 in ConjugacyClass(H, a)) then r := 1; break; fi; od;
  return r; else return 0; fi;
else return 0; fi;
end;;

LoadPackage("ANUPQ");;
T := [];; T[1] := [[AbelianGroup([2, 2]), []]];;
for n in [2..7] do T[n] := []; for k in [1..Size(T[n-1])] do
  procid := PqStart(T[n-1][k][1]); D := PqDescendants(procid:ClassBound := n); PqQuit(procid); t := 1;
  for i in [1..Size(D)] do if h(D[i]) = 1 and MultiplicatorRank(D[i])-NuclearRank(D[i])<3 then
      Add(T[n], [D[i], Concatenation(T[n-1][k][2], [t])]); t := t+1;
  fi; od;
od; od;
```

Fig. 3. Computing T.

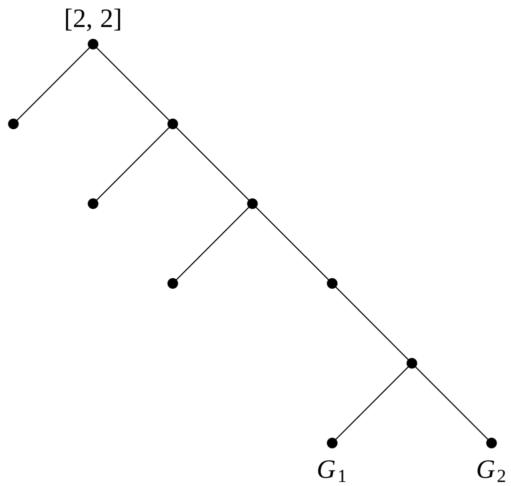


Fig. 4. T.

```
LoadPackage("HAP");;
G := [];; for n in [1..6] do for k in [1..Size(T[n])] do
if Size(GroupCohomology(T[n][k][1], 2, 2)) = 2 then Add(G, T[n][k]); fi;
od; od;

g := function(G) local N, M, U; # computes the abelianizations of M_3 and U_i (i = 1, 2, 3, 4).
N := List(MaximalSubgroups(G)); SortParallel(List(N, x->-Exponent(CommutatorFactorGroup(x))), N);
M := IntermediateSubgroups(N[3], FrattiniSubgroup(N[1])).subgroups; SortParallel(List(M, x->IsNormal(G, x)), M);
U := List(MaximalSubgroups(M[3])); SortParallel(List(U, x->IsSubgroup(x, FrattiniSubgroup(N[3]))<>true), U);
return [ AbelianInvariants(M[3]), List([U[1], U[2], U[3], U[4]], x->AbelianInvariants(x)) ];
end;;

gap> List(G, x->x[1]);
[ <pc group of size 512 with 9 generators>, <pc group of size 512 with 9 generators> ]
gap> CodePcGroup(G[1][1]); CodePcGroup(G[2][1]);
13830505503288171864898804013533563491412215720741354747545296882850687
13830505503288171864898804013533563491412215720741354756552496137591679
gap> g(G[1][1]); g(G[2][1]); # [ M_3^ab, [ U_1^ab, U_2^ab, U_3^ab, U_4^ab ] ]
[ [ 2, 2, 4 ], [ [ 2, 2, 4 ], [ 2, 2, 4 ], [ 2, 2, 4 ], [ 2, 2, 4 ] ] ]
[ [ 2, 2, 4 ], [ [ 4, 4 ], [ 4, 4 ], [ 4, 4 ], [ 4, 4 ] ] ]
gap> F := FreeGroup( "a", "b" );; a := F.1;; b := F.2;;
gap> G1 := F/[ a^-4*Comm(b^2, a), b^-2*Comm(Comm(b, a), a)*a^4 ];;
gap> (IsomorphismGroups(G[1][1], G1)<>fail);
true
gap> List(DerivedSeries(G[1][1]), x->AbelianInvariants(x));
[ [ 2, 4 ], [ 2, 2, 4 ], [ 2, 2 ], [ ] ]
```

Fig. 5. Two candidates G_1 and G_2.

We also use the same notations as in the previous section. Put $N_3 = \mathrm{Gal}(\mathbb{Q}_S/k_1)$ and $N_1 = \mathrm{Gal}(\mathbb{Q}_S/k)$. By Theorem 2.1, N_3 (resp. N_1) is the unique maximal subgroup of G such that $N_3^{ab} \simeq [2,2,2]$ (resp. $N_1^{ab} \simeq [2,8]$). Since $k_\emptyset\mathbb{Q}_S^{ab}/k$ is a $[2,4]$-extension and $A_S(k) \simeq [2{,}8]$, we have $k_S^{\mathrm{elem}} \subset k_\emptyset\mathbb{Q}_S^{ab}$, where k_S^{elem} denotes the maximal elementary abelian 2-extension of k unramified outside S. Then

$$N_3' = \Phi(N_3) = \mathrm{Gal}(\mathbb{Q}_S/k_\emptyset\mathbb{Q}_S^{ab}) \subset \Phi(N_1) = \mathrm{Gal}(\mathbb{Q}_S/k_S^{\mathrm{elem}}) \subset N_3.$$

Moreover, $G/\Phi(N_1) \simeq \mathrm{Gal}(k_S^{\mathrm{elem}}/\mathbb{Q})$ is a dihedral group of order 8. Since there is a surjective homomorphism $[2{,}2{,}2] \simeq N_3^{ab} \to N_3/\Phi(N_1)$, the maximal subgroup $N_3/\Phi(N_1)$ of $G/\Phi(N_1)$ is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$, i.e., $N_3/\Phi(N_1) \simeq \mathrm{Gal}(k_S^{\mathrm{elem}}/k_1) \simeq [2{,}2]$. Hence N_3 has two maximal subgroups containing $\Phi(N_1)$ and not normal in G. Note that these two maximal subgroups are isomorphic. Let M_3 be one of them. Then $M_3/\Phi(N_3) \simeq [2,2]$. Since $G \simeq G_1$ or $G \simeq G_2$, GAP tells us that $M_3^{ab} \simeq [2,2,4]$ (cf. Fig. 5). Then M_3 has four maximal subgroups U_i $(1 \le i \le 4)$ not containing $\Phi(N_3)$. GAP also tells us that

$$U_i^{ab} \simeq \begin{cases} [2,2,4] & \text{if } G \simeq G_1, \\ [4,4] & \text{if } G \simeq G_2 \end{cases}$$

for all i (cf. Fig. 5).

Recall the assumption (2.2) and that L_1/k_1 is unramified outside $\{\mathfrak{q}_1, \mathfrak{r}_1\}$. Then we can characterize the fixed field of M_3 as follows.

Lemma 3.1. *$M_3 \simeq \mathrm{Gal}(\mathbb{Q}_S/(k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1^\sigma\}})$, and $(k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1^\sigma\}}/k_1$ is ramified at any primes dividing $l\mathfrak{q}_1\mathfrak{r}_1^\sigma$.*

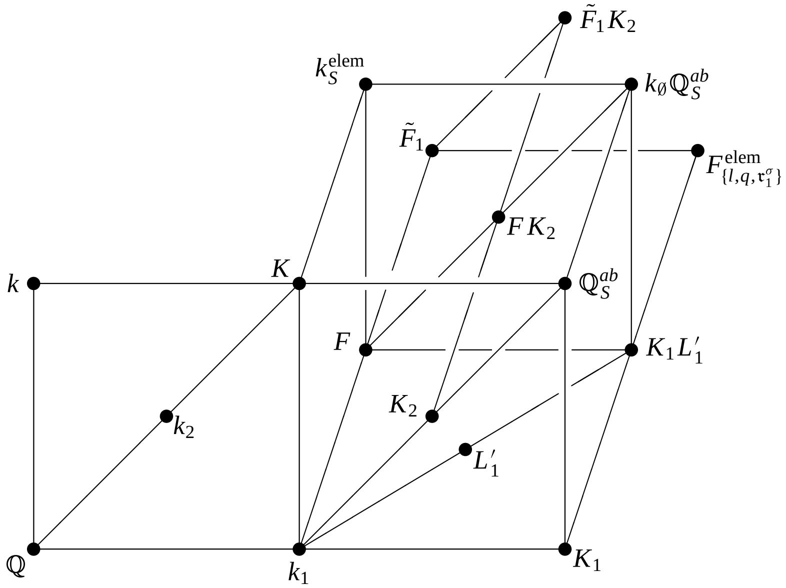


Fig. 6. Some subfields of $\mathbb{Q}_S$.

Proof. Recall that $\mathrm{Gal}(k_S^{\mathrm{elem}}/\mathbb{Q})$ is a dihedral group of which cyclic maximal subgroup is $\mathrm{Gal}(k_S^{\mathrm{elem}}/k_2) \simeq \mathbb{Z}/4\mathbb{Z}$. Then k_S^{elem}/k_2 is totally ramified at any primes lying over l. In particular, k_S^{elem}/K is ramified at any primes lying over l. Then the inertia field of $(\sqrt{l})$ in the [2, 2]-extension k_S^{elem}/k_1 is K, and K/k_1 is ramified at all primes dividing qr. Let F be the inertia field of $\mathfrak{q}_1^\sigma$ in k_S^{elem}/k_1. Then F/k_1 is unramified outside $\{l, \mathfrak{q}_1, r\}$. Since $F \neq K$, $F/\mathbb{Q}$ is not a Galois extension, and hence $M_3 \simeq \mathrm{Gal}(\mathbb{Q}_S/F)$. Moreover, F/k_1 is ramified at $(\sqrt{l})$. Since $(k_1)_{\{l,r\}} = \mathbb{Q}_{\{l,r\}} = K_2$, F/k_1 is ramified at $\mathfrak{q}_1$. If F/k_1 is ramified at both $\mathfrak{r}_1$ and $\mathfrak{r}_1^\sigma$, the conjugate F' of F is the inertia field of $\mathfrak{r}_1$ and $\mathfrak{r}_1^\sigma$ in k_S^{elem}/k_1, and F'/k_1 is unramified outside $\{l, \mathfrak{q}_1^\sigma\}$. Since $(k_1)_{\{l,q\}} = \mathbb{Q}_{\{l,q\}} = K_1$ contains neither F nor F', F/k_1 is ramified at one of $\mathfrak{r}_1$ and $\mathfrak{r}_1^\sigma$ and unramified at another one. Since $F \neq (k_1)_{\{\mathfrak{q}_1,\mathfrak{r}_1\}} = L_1 = (k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1\}}$ (cf. (2.8)) and $A_{\{l,\mathfrak{q}_1,\mathfrak{r}_1^\sigma\}}(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$ by (2.6), we have $F = (k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1^\sigma\}}$ and F/k_1 is ramified at $\mathfrak{r}_1^\sigma$. Thus the proof of Lemma 3.1 is completed. □

Put $F = (k_1)_{\{l,\mathfrak{q}_1,\mathfrak{r}_1^\sigma\}}$, and let $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}$ be the maximal elementary abelian extension of F unramified outside $\{l, q, \mathfrak{r}_1^\sigma\}$ (cf. Fig. 6). Then $A_{\{l,q,\mathfrak{r}_1^\sigma\}}(F)/2 \simeq \mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F)$ and $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1$ is a Galois extension. Recall that L_1'/k_1 is a quadratic extension unramified outside $\{\mathfrak{q}_1^\sigma, \mathfrak{r}_1^\sigma\}$. Then K_1L_1'/k_1 is a $[2,2]$-extension unramified outside $\{l, q, \mathfrak{r}_1^\sigma\}$. By (2.6), we have $A_{\{l,q,\mathfrak{r}_1^\sigma\}}(k_1) \simeq [2,2]$, and hence $F \subset (k_1)^{ab}_{\{l,q,\mathfrak{r}_1^\sigma\}} = K_1L_1' \subset F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}$. In particular, $\mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1)^{ab} \simeq A_{\{l,q,\mathfrak{r}_1^\sigma\}}(k_1) \simeq [2,2]$. Since $\mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1)$ has an elementary abelian maximal subgroup $\mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F)$, $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1$ is a $[2,2]$-extension or a dihedral extension of degree 8. Recall that $k_\emptyset$ is a $[2,2]$-extension of k_1 which contains K, L_1 and L_1'. Since $\mathfrak{r}_1$ ramifies in K/k_1 and $\mathfrak{R}_1$ is inert in $k_\emptyset/K$ by Lemma 2.1, $\mathfrak{r}_1$ is also inert in L_1'/k_1. Since $\mathfrak{r}_1$ splits in K_1/k_1, i.e., the decomposition field of $\mathfrak{r}_1$ in the $[2,2]$-extension K_1L_1'/k_1 is K_1, we know that $\mathfrak{r}_1$ is inert in F/k_1. Then the kernel of the surjective homomorphism

$$\mathrm{Gal}(F_S^{ab}/F) \simeq A_S(F) \to A_{\{l,q,\mathfrak{r}_1^\sigma\}}(F)$$

is isomorphic to the inertia group of the unique prime of F lying over $\mathfrak{r}_1$ which is cyclic. Since $\mathrm{Gal}(F_S^{ab}/F) \simeq M_3^{ab} \simeq [2,2,4]$, $A_{\{l,q,\mathfrak{r}_1^\sigma\}}(F)$ has the 2-rank at least 2, i.e., $\mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F) \simeq [2,2]$. Therefore $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1$ is a dihedral extension of degree 8.

We shall see the ramification of primes in $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/k_1$. Since $\mathrm{Gal}((K_1)_S^{ab}/K_1)$ is elementary abelian by Theorem 2.1, $\mathrm{Gal}(F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/K_1)$ is also elementary abelian. Hence $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/K_1$ is a $[2,2]$-extension and $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/L_1'$ is a cyclic quartic extension. Since both $\mathfrak{R}_1^\sigma$ and $\mathfrak{R}_1^{\sigma^3}$ ramify in K_1L_1'/K_1 and the $[2,2]$-extension $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/K_1$ is not totally ramified at any tamely ramified primes, $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/K_1L_1'$ is unramified at any primes lying over $\mathfrak{r}_1^\sigma$. Since any primes dividing $l\mathfrak{q}_1\mathfrak{r}_1^\sigma$ ramify in F/k_1 by Lemma 3.1 and do not totally ramify in the $[2,2]$-extension K_1L_1'/k_1, K_1L_1'/F is unramified outside $\{\mathfrak{q}_1^\sigma\}$ and ramified at any primes dividing $\mathfrak{q}_1^\sigma$. Hence $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F$ is unramified outside $\{l,q\}$. On the other hand, since any primes dividing $l\mathfrak{q}_1$ ramify in K_1L_1'/L_1', the cyclic quartic extension $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/L_1'$ is totally ramified at any primes dividing $l\mathfrak{q}_1$. Therefore $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F$ is ramified at any primes dividing lq.

Recall that $M_3 \supset \Phi(N_1)$, i.e., $F \subset k_S^{\mathrm{elem}}$. Then F is the inertia field of $\mathfrak{q}_1^\sigma$ in the $[2,2]$-extension k_S^{elem}/k_1. By Lemma 2.1, $\mathfrak{Q}^\sigma$ is inert in $k_\emptyset$. Since $\mathfrak{Q}^\sigma$ is also inert in $\mathbb{Q}_S^{ab}$, the decomposition field of $\mathfrak{Q}^\sigma$ in the $[2,2]$-extension $k_\emptyset\mathbb{Q}_S^{ab}/K$ is k_S^{elem}, i.e., $\mathfrak{Q}^\sigma$ splits in k_S^{elem}/K. Therefore $\mathfrak{q}_1^\sigma$ splits in F/k_1. Let $\overline{\mathfrak{q}_1^\sigma}$ and $\overline{\mathfrak{q}_1^\sigma}'$ be the distinct primes of F lying over $\mathfrak{q}_1^\sigma$. Let $\tilde{F}_1$ be the inertia field of $\overline{\mathfrak{q}_1^\sigma}'$ in the $[2,2]$-extension $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F$. Then $\tilde{F}_1$ is the unique quadratic extension of F unramified outside $\{l,\mathfrak{q}_1,\overline{\mathfrak{q}_1^\sigma}\}$. Since $\tilde{F}_1 \neq K_1L_1'$ and K_1L_1' is the inertia field of the unique prime of F lying over l in $F^{\mathrm{elem}}_{\{l,q,\mathfrak{r}_1^\sigma\}}/F$, $\tilde{F}_1/F$ is ramified at the prime lying over l. Recall that $k_\emptyset\mathbb{Q}_S^{ab} = (k_1)_S^{ab}$ is a $[2,2,2]$-extension of k_1. Then the ramification indices of any primes in $k_\emptyset\mathbb{Q}_S^{ab}/k_1$ are at most 2. By Lemma 3.1, $k_\emptyset\mathbb{Q}_S^{ab}/F$ is a $[2,2]$-extension unramified outside $\{\mathfrak{q}_1^\sigma,\mathfrak{r}_1\}$. Therefore $\tilde{F}_1 \cap k_\emptyset\mathbb{Q}_S^{ab} = F$. By Lemma 3.1, FK_2/F is a quadratic extension unramified outside $\{\mathfrak{r}_1\}$. Since $\mathfrak{q}_1^\sigma$ is inert in K_2/k_1, $\overline{\mathfrak{q}_1^\sigma}'$ is also inert in FK_2/F. The $[2,2]$-extension $\tilde{F}_1K_2$ of F contains a quadratic extension $\tilde{F}_2$ of F different from $\tilde{F}_1$ and FK_2. Then $\tilde{F}_2$ also satisfies $\tilde{F}_2 \cap k_\emptyset\mathbb{Q}_S^{ab} = F$. Put

$$\tilde{F} = \begin{cases} \tilde{F}_1 & \text{if } \overline{\mathfrak{q}_1^\sigma}' \text{ splits in } \tilde{F}_1/F, \\ \tilde{F}_2 & \text{if } \overline{\mathfrak{q}_1^\sigma}' \text{ is inert in } \tilde{F}_1/F. \end{cases} \tag{3.1}$$

Then $\overline{\mathfrak{q}_1^\sigma}'$ splits in $\tilde{F}/F$ and $\tilde{F}\cap k_\emptyset\mathbb{Q}_S^{ab}=F$, i.e., $\mathrm{Gal}(\mathbb{Q}_S/\tilde{F})\simeq U_i$ for some i. Moreover, since K_1L_1'/F is ramified at $\overline{\mathfrak{q}_1^\sigma}'$, $\tilde{F}K_1L_1'/\tilde{F}$ is a quadratic extension ramified at any primes lying over $\overline{\mathfrak{q}_1^\sigma}'$. Let $\tilde{\mathfrak{Q}}$ be a prime of $\tilde{F}$ lying over $\overline{\mathfrak{q}_1^\sigma}'$.

Now we assume that $G\simeq G_2$. Then $U_i^{ab}\simeq[4,4]$, and hence there is a cyclic quartic extension of $\tilde{F}$ unramified outside S which contains $\tilde{F}K_1L_1'$. Since the cyclic quartic extension is totally ramified at $\tilde{\mathfrak{Q}}$, the ramification index of $\tilde{\mathfrak{Q}}$ in $\tilde{F}_S^{ab}/\tilde{F}$ is 4, i.e., the inertia group $I_{\tilde{\mathfrak{Q}}}=\mathrm{Ker}(\mathrm{Gal}(\tilde{F}_S^{ab}/\tilde{F}_\emptyset^{ab})\to\mathrm{Gal}(\tilde{F}_\Sigma^{ab}/\tilde{F}_\emptyset^{ab}))$ has order 4, where $\Sigma=S(\tilde{F})\setminus\{\tilde{\mathfrak{Q}}\}$. On the other hand, applying the snake lemma for the commutative diagram

$$\begin{array}{ccccccc}
 & & E(\tilde{F}) & \longrightarrow & \bigoplus_{\mathfrak{p}\in S(\tilde{F})}(O_{\tilde{F}}/\mathfrak{p})^\times\otimes\mathbb{Z}_2) & \longrightarrow & \mathrm{Gal}(\tilde{F}_S^{ab}/\tilde{F}_\emptyset^{ab}) \longrightarrow 0\\
 & & \downarrow & & \downarrow & & \downarrow\\
0 & \longrightarrow & E(\tilde{F})/\mathrm{Ker}\,\varphi_{\tilde{F},\Sigma} & \longrightarrow & \bigoplus_{\mathfrak{p}\in\Sigma}((O_{\tilde{F}}/\mathfrak{p})^\times\otimes\mathbb{Z}_2) & \longrightarrow & \mathrm{Gal}(\tilde{F}_\Sigma^{ab}/\tilde{F}_\emptyset^{ab}) \longrightarrow 0
\end{array}$$

with exact rows, we obtain a surjective homomorphism $(O_{\tilde{F}}/\tilde{\mathfrak{Q}})^\times\otimes\mathbb{Z}_2\to I_{\tilde{\mathfrak{Q}}}$. Since $\tilde{\mathfrak{Q}}$ is a prime of degree 1, i.e., $(O_{\tilde{F}}/\tilde{\mathfrak{Q}})^\times\otimes\mathbb{Z}_2\simeq\mathbb{F}_q^\times\otimes\mathbb{Z}_2\simeq\mathbb{Z}/2\mathbb{Z}$, we have $|I_{\tilde{\mathfrak{Q}}}|\le 2$. This is a contradiction. Therefore $G\simeq G_1$. Using GAP again (cf. Fig. 5), one can see that

$$G\simeq G_1\simeq\langle a,b\mid a^{-4}[b^2,a],\ b^{-2}[[b,a],a]a^4\rangle$$

as an abstract group and that $G/G'\simeq[2,4]$, $G'/G''\simeq[2,2,4]$ and $G''\simeq[2,2]$. Thus the proof of Theorem 1.1 is completed.

REMARK 3.1. GAP tells us that a finite 2-group G satisfies $G/G'\simeq[2,4]$, $G'/G''\simeq[2,2,4]$, $G''\simeq[2,2]$ and $H^2(G,\mathbb{Z}/2\mathbb{Z})\simeq[2,2]$ if and only if $G\simeq G_1$ or G_2.

REMARK 3.2. Both of two cases of (3.1) can occur. Put $(l,q,r)=(5,11,71)$. Choosing $\mathfrak{q}_1$ and $\mathfrak{r}_1$ suitably, we can see by PARI/GP [24] that $F=k_1(\sqrt{\alpha})$ for $\alpha=\left(\frac{5-\sqrt{5}}{2}\right)(4+\sqrt{5})\left(\frac{17+\sqrt{5}}{2}\right)\in\sqrt{l}\mathfrak{q}_1\mathfrak{r}_1^\sigma$ satisfying $\alpha^2-130\alpha+3905=0$. Choosing a prime as $\overline{\mathfrak{q}_1^\sigma}$, some functions (`bnrinit`, `rnfkummer` etc.) on PARI/GP tell us that $A_{\{l,\mathfrak{q}_1,\overline{\mathfrak{q}_1^\sigma}\}}(F)\simeq\mathbb{Z}/2\mathbb{Z}$, $\tilde{F}_1=F^{ab}_{\{l,\mathfrak{q}_1,\overline{\mathfrak{q}_1^\sigma}\}}\simeq\mathbb{Q}[x]/(x^8-50x^6+715x^4-3190x^2+605)$ and that $\overline{\mathfrak{q}_1^\sigma}'$ is inert in $\tilde{F}_1/F$. On the other hand, if we put $(l,q,r)=(5,19,79)$ and choose primes suitably, we have $F=k_1(\sqrt{\alpha})$ with $\alpha^2-175\alpha+7505=0$ and $\tilde{F}_1=F^{ab}_{\{l,\mathfrak{q}_1,\overline{\mathfrak{q}_1^\sigma}\}}\simeq\mathbb{Q}[x]/(x^8-590x^6+88255x^4-361570x^2+1805)$. Then $\overline{\mathfrak{q}_1^\sigma}'$ splits in $\tilde{F}_1/F$. It seems still difficult to write σ_l, σ_q explicitly as the (pro-2) words of letters τ_l, τ_q.

ACKNOWLEDGEMENTS. The author thanks the referee for valuable suggestions for the improvement of this paper. This work was supported by JSPS KAKENHI Grant Number 26800010, Grant-in-Aid for Young Scientists (B).

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), 229–245.

[2] E. Benjamin, F. Lemmermeyer and C. Snyder: *Real quadratic fields with abelian* 2*-class field tower*, J. Number Theory **73** (1998), 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), 15–31.

[4] N. Boston and C. Leedham-Green: *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), 402–413.

[5] N. Boston and H. Nover: *Computing pro-p Galois groups*; in Algorithmic Number Theory, Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 1–10, 2002.

[6] N. Boston and D. Perry: *Maximal* 2*-extensions with restricted ramification*, J. Algebra **232** (2000), 664–672.

[7] M.R. Bush: *Computation of Galois groups associated to the* 2*-class towers of some quadratic fields*, J. Number Theory **100** (2003), 313–325.

[8] M.R. Bush and D.C. Mayer: 3*-class field towers of exact length* 3, J. Number Theory **147** (2015), 766–777.

[9] B. Eick and H. Koch: *On maximal* 2*-extensions of* $\mathbb{Q}$ *with given ramification*; in Proceedings of the St. Petersburg Mathematical Society **12**, Amer. Math. Soc. Transl. Ser. 2, **219**, Amer. Math. Soc., Providence, RI, 87–102, 2006.

[10] G. Ellis: *HAP—Homological algebra programming, a GAP package*, ver. 1.10.12, (2013), `http://hamilton.nuigalway.ie/Hap/www`.

[11] G. Gamble, W. Nickel and E.A. O'Brien: *ANUPQ—ANU p-Quotient, a GAP package*, ver. 3.0, (2006), `http://gap-system.github.io/anupq/`.

[12] M.-N. Gras: *Classes et unités des extensions cycliques réelles de degré* 4 *de* $\mathbf{Q}$, Ann. Inst. Fourier (Grenoble) **29** (1979), 107–124.

[13] H. Hasse: *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsch. Akad. Wiss. Berlin. Math.-Nat. Kl. (1948).

[14] H. Koch: Galois Theory of p-Extensions, Springer Monographs in Mathematics, Springer, Berlin, 2002.

[15] F. Lemmermeyer: *Kuroda's class number formula*, Acta Arith. **66** (1994), 245–260.

[16] D.C. Mayer: *Index-p abelianization data of p-class tower groups*, Advances in Pure Mathematics **5** (2015), 286–313.

[17] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of Number Fields, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2008.

[18] H. Nover: *Computation of Galois groups associated to the* 2*-class towers of some imaginary quadratic fields with* 2*-class group* $C_2 \times C_2 \times C_2$, J. Number Theory **129** (2009), 231–245.

[19] E.A. O'Brien: *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), 677–698.

[20] M. Ozaki: *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math. **183** (2011), 649–680.

[21] L. Rédei and H. Reichardt: *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1934), 69–74.

[22] A. Steurer: *On the Galois groups of the* 2*-class towers of some imaginary quadratic fields*, J. Number Theory **125** (2007), 235–246.

[23] The GAP Group: *GAP—Groups, algorithms, and programming*, ver. 4.6.5 (2013), `http://www.gap-system.org`.

[24] The PARI Group: *PARI/GP* version 2.5.5, Bordeaux, (2013), `http://pari.math.u-bordeaux.fr/`.

[25] H. Yokoi: *On the class number of a relatively cyclic number field*, Nagoya Math. J. **29** (1967), 31–44.

[26] K. Yoshino: *On Hasse's algorithm to calculate fundamental units of real cyclic biquadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), 182–186.

Department of Mathematics
Nagoya Institute of Technology
Gokiso, Showa, Nagoya 466-8555
Japan
e-mail: mizusawa.yasushi@nitech.ac.jp