TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 4, April 2018, Pages 2423–2461
http://dx.doi.org/10.1090/tran/7023
Article electronically published on October 31, 2017

TAME PRO-2 GALOIS GROUPS AND THE BASIC $\mathbb{Z}_2$-EXTENSION

YASUSHI MIZUSAWA

Abstract. For a number field, we consider the Galois group of the maximal tamely ramified pro-2-extension with restricted ramification. Providing a general criterion for the metacyclicity of such Galois groups in terms of 2-ranks and 4-ranks of ray class groups, we classify all finite sets of odd prime numbers such that the maximal pro-2-extension unramified outside the set has prometacyclic Galois group over the $\mathbb{Z}_2$-extension of the rationals. The list of such sets yields new affirmative examples of Greenberg's conjecture.

1. Introduction

Let p be a prime number. For an algebraic extension k of the rational number field $\mathbb{Q}$ and a finite set S of primes of (a subfield of) k, we consider the Galois group $G_S(k) = \mathrm{Gal}(k_S/k)$ of the maximal pro-p-extension k_S of k unramified outside (primes dividing an element of) S. When the degree $[k : \mathbb{Q}]$ is finite, the pro-p group $G_S(k)$ is finitely presented by generators and relations. While arithmetical symbols describe the relations approximately (cf. e.g. [14]), it is in general difficult to know the structure explicitly. If k_S contains a $\mathbb{Z}_p$-extension k_∞ of k, where $\mathbb{Z}_p$ denotes (the additive group of) the ring of p-adic integers, then $G_S(k)$ and its closed subgroup $G_S(k_\infty)$ are relatively well studied also in Iwasawa theory (cf. e.g. [18]).

On the other hand, we focus on the case where S contains no primes lying over p. Then $G_S(k)$ is a 'fab' pro-p group with derived series corresponding to the ray p-class field tower of k. Such Galois groups are also studied in nonabelian Iwasawa theory [22] as the closed subgroup $G_S(k_\infty) \simeq \varprojlim G_S(k_n)$ of the finitely presented pro-p group $\mathrm{Gal}((k_\infty)_S/k)$ for the cyclotomic $\mathbb{Z}_p$-extension $k_\infty = k\mathbb{Q}_{\{p\}}$ (cf. also [4], [26], etc.), where the projective limit is taken on the restriction mappings and the subfields $k \subset k_n \subset k_\infty$. While there are several explicit examples of finitely presented $G_S(k_\infty)$ ([27], etc.), it is not known whether $G_S(k_\infty)$ is always finitely presented or not. Moreover, one of the difficulties is Greenberg's conjecture [8] which states the finiteness of the Galois group $G_\emptyset(K_\infty)^{\mathrm{ab}}$ of the maximal unramified abelian pro-p-extension over the cyclotomic $\mathbb{Z}_p$-extension K_∞ of an arbitrary totally real number field K. Then it is a supplemental strategy to consider $G_\emptyset(K_\infty)^{\mathrm{ab}}$ as a subquotient of $G_S(k_\infty)$ for a p-extension K_∞/k_∞ unramified outside S. We consider these subjects in the case where $p = 2$ and $k = \mathbb{Q}$. The main theorem (Theorem 1.1) below gives a classification of all S with prometacyclic $G_S(\mathbb{Q}_\infty)$ and new examples of finite $G_\emptyset(K_\infty)^{\mathrm{ab}}$ as a subquotient of $G_S(\mathbb{Q}_\infty)$.

Received by the editors April 30, 2016, and, in revised form, July 14, 2016.
2010 *Mathematics Subject Classification.* Primary 11R23; Secondary 11R18, 11R20, 11R32.
This work was supported by JSPS KAKENHI Grant Number JP26800010, Grant-in-Aid for Young Scientists (B).

A prometacyclic (resp. procyclic) pro-p group is a projective limit of metacyclic (resp. cyclic) p-groups. A pro-p group is prometacyclic if and only if it has a procyclic closed normal subgroup with procyclic quotient (cf. [5, Exercise 3.10]), and hence a prometacyclic pro-p group is finitely presented.

In this paper, ℓ and q denote prime numbers such that $\ell \equiv -q \equiv 1 \pmod 4$, and ∞ as an element of S denotes the archimedean prime of $\mathbb{Q}$. Also $\left(\frac{\cdot}{\cdot}\right)$ denotes the quadratic residue symbol, and $\left(\frac{\cdot}{\cdot}\right)_4$ denotes the biquadratic residue symbol defined as follows: $\left(\frac{z}{\ell}\right)_4 = \pm 1 \equiv z^{\frac{\ell-1}{4}} \pmod{\ell}$ for $z \in \mathbb{Z}_\ell$ such that $\left(\frac{z}{\ell}\right) = 1$, and $\left(\frac{a}{2}\right)_4 = (-1)^{\frac{a-1}{8}}$ for an integer $a \equiv 1 \pmod 8$.

Theorem 1.1. *Let S be a finite set of primes of $\mathbb{Q}$ not containing 2, and let $\mathbb{Q}_\infty$ be the $\mathbb{Z}_2$-extension of $\mathbb{Q}$. The Galois group $G_S(\mathbb{Q}_\infty) = \mathrm{Gal}((\mathbb{Q}_\infty)_S/\mathbb{Q}_\infty)$ of the maximal pro-2-extension $(\mathbb{Q}_\infty)_S$ of $\mathbb{Q}_\infty$ unramified outside S is prometacyclic if and only if S satisfies one of the following:*

(1) *$S \subset \{\infty\}$ or $S = \{q\}$ and $q \equiv 3 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is trivial.*
(2) *$S = \{\ell\}$, $\ell \equiv 5 \pmod 8$ or $\ell \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell}\right)_4\left(\frac{\ell}{2}\right)_4 = -1$. Then $G_S(\mathbb{Q}_\infty)$ is procyclic.*
(3) *$S = \{q, r\}$, $q \equiv 3 \pmod 4$ and $\left(\frac{2}{r}\right) = -1$. Then $G_S(\mathbb{Q}_\infty)$ is procyclic.*
(4) *$S = \{r, \infty\}$ and $\left(\frac{2}{r}\right) = -1$. Then $G_S(\mathbb{Q}_\infty)$ is procyclic.*
(5) *$S = \{\ell\}$, $\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$ and $\left(\frac{1+\sqrt{2}}{\ell}\right)_4 = (-1)^{1+\frac{1}{2}h_\ell}$ for the class number h_ℓ of $\mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{\ell})$. Then $G_S(\mathbb{Q}_\infty)$ is not procyclic.*
(6) *$S = \{r_1, r_2\}$ and one of the following is satisfied:*
   - $r_1 \equiv 5 \pmod 8$, $r_2 \equiv 5 \pmod 8$, $\left(\frac{r_1}{r_2}\right) = \left(\frac{r_1}{r_2}\right)_4\left(\frac{r_2}{r_1}\right)_4 = 1$.
   - $r_1 \equiv 5 \pmod 8$, $r_2 \equiv 5 \pmod 8$, $\left(\frac{r_1}{r_2}\right) = \left(\frac{2r_1}{r_2}\right)_4\left(\frac{2r_2}{r_1}\right)_4\left(\frac{r_1 r_2}{2}\right)_4 = -1$.
   - $r_1 \equiv 1 \pmod 8$, $r_2 \equiv 5 \pmod 8$, $\left(\frac{r_1}{r_2}\right) = \left(\frac{2}{r_1}\right)_4\left(\frac{r_1}{2}\right)_4 = -1$.
   - $r_1 \equiv 1 \pmod 8$, $r_2 \equiv 3 \pmod 4$, $\left(\frac{r_2}{r_1}\right) = \left(\frac{r_1}{2}\right)_4 = -\left(\frac{2}{r_1}\right)_4 = -\left(\frac{2}{r_2}\right)$.
   - $r_1 \equiv 7 \pmod{16}$, $r_2 \equiv 15 \pmod{16}$.

   Then $G_S(\mathbb{Q}_\infty)$ is not procyclic.
(7) *$S = \{q_1, q_2, r\}$, $q_1 \equiv 3 \pmod 8$ and one of the following is satisfied:*
   - $q_2 \equiv 7 \pmod 8$, $r \equiv 5 \pmod 8$, $\left(\frac{q_2}{r}\right) = -1$.
   - $q_2 \equiv 3 \pmod 8$, $r \equiv 5 \pmod 8$, $\left(\frac{q_1 q_2}{r}\right) = -1$.
   - $q_2 \equiv 3 \pmod 8$, $r \equiv 7 \pmod 8$, $\left(\frac{q_1 q_2}{r}\right) = -1$.

   Then $G_S(\mathbb{Q}_\infty)$ is not procyclic.
(8) *$S = \{q, \infty\}$ and $q \equiv 7 \pmod{16}$. Then $G_S(\mathbb{Q}_\infty)$ is not procyclic.*

Moreover, if $\infty \notin S$ and $G_S(\mathbb{Q}_\infty)$ is prometacyclic, and if $K/\mathbb{Q}$ is a finite extension contained in $(\mathbb{Q}_\infty)_S$, then the cyclotomic $\mathbb{Z}_2$-extension K_∞ of K has no infinite unramified abelian pro-2-extension (i.e., $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is finite).

Remark 1.2. If $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$, then h_ℓ is even (cf. e.g. [20]). Moreover, one can see that $\left(\frac{1+\sqrt{2}}{\ell}\right) = 1$ from the decomposition of ℓ in $\mathbb{Q}(\sqrt[4]{2}, \sqrt{1+\sqrt{2}})$. Since $(1+\sqrt{2})(1-\sqrt{2}) = -1$ and $\left(\frac{-1}{\ell}\right)_4 = 1$, the symbol $\left(\frac{1+\sqrt{2}}{\ell}\right)_4$ does not depend on the choice of an embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{Z}_\ell$.

In the proof of Theorem 1.1, we see that $G_S(\mathbb{Q}_\infty)$ is infinite procyclic if and only if S satisfies the condition 3 and $q \equiv r \pmod 8$. By [9, Theorem 1.1], one can also see that (the maximal abelian pro-2 quotient of) $G_S(\mathbb{Q}_\infty)$ is infinite if S

satisfies the condition (6) and $r_2 \not\equiv 7 \pmod 8$ or the condition (7) and $q_2 \equiv 3 \pmod 8$. The finiteness of $G_\emptyset(K_\infty)^{\mathrm{ab}}$ in Theorem 1.1 for abelian $K/\mathbb{Q}$ is already known essentially (cf. [20], [23], [28], etc.) and is used in the proof of Theorem 1.1. Theorem 1.1 yields new examples of finite $G_\emptyset(K_\infty)^{\mathrm{ab}}$ when $K/\mathbb{Q}$ is nonabelian. Similar statements for $p \neq 2$ (and for a special case of $p = 2$) have been obtained in [10] and [19], while the influences of $G_\emptyset(K_\infty)^{\mathrm{ab}}$ on the prometacyclicity of $G_S(\mathbb{Q}_\infty)$ are different according to the parity of p (cf. assumptions of [19, Theorems 1 and 2]). As a clarification of this difference and as a key tool for the proof of Theorem 1.1, we provide a general criterion (Theorem 3.1 in Section 3) for the metacyclicity of tame pro-2 Galois groups $G_S(k)$ in terms of 2-ranks and 4-ranks of ray class groups. After recalling some basic facts on pro-p groups and ray class groups and cyclotomic $\mathbb{Z}_2$-extensions (in Sections 2 and 4), we prove the first half of Theorem 1.1, dividing the statements according to $(r \bmod 4)_{r\in S}$ (from Sections 5 to 9). Also, we see the structure of $G_S(\mathbb{Q}_\infty)$ more explicitly in some special cases. The proof of Theorem 1.1 will be completed in the final section (Section 10).

Example 1.3. Since $\left(\frac{29}{5}\right)_4 = \left(\frac{5}{29}\right)_4 = -1$, the set $S = \{5, 29\}$ satisfies the condition (6). Then $K = \mathbb{Q}_S$ is a nonabelian metacyclic 2-extension of $\mathbb{Q}$ (cf. Remark 2.2 below). Moreover, $G_S(\mathbb{Q}_\infty)$ is a pro-2 group with two generators a, b and two relations a^{16}, $a^{-3}b^{-1}ab$ (cf. [19, Example 2]). Put $\ell = 137$ or $\ell = 409$. Then $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$. Since $31^2 \equiv 2 \pmod{137}$ and $97^2 \equiv 2 \pmod{409}$, we have $\left(\frac{1+\sqrt{2}}{137}\right)_4 = \left(\frac{32}{137}\right)_4 = -1$ and $\left(\frac{1+\sqrt{2}}{409}\right)_4 = \left(\frac{98}{409}\right)_4 = 1$. Moreover, $h_{137} \equiv 0 \pmod 4$ and $h_{409} \equiv 2 \pmod 4$ by [24]. Hence $S = \{\ell\}$ satisfies the condition (5).

2. Preliminaries

2.1. **Pro-p groups.** We denote by $|S|$ the cardinality of a set S and by $\mathbb{F}_{p^n}$ the finite field of cardinality p^n. An abelian pro-p group A is often regarded as a $\mathbb{Z}_p$-module. For an integer $e \geq 1$, we put $A/p^e = A/A^{p^e}$ and denote by $\mathrm{r}_{p^e}(A) = \dim_{\mathbb{F}_p}(A^{p^{e-1}}/A^{p^e})$ the p^e-rank. In particular, $\mathrm{r}_2(A)$ and $\mathrm{r}_4(A)$ denote the 2-rank and the 4-rank of an abelian pro-2 group A respectively.

Let G be a pro-p group (not necessarily finitely generated) and H a closed subgroup of G. Then $[G, H]$ (resp. H^p) denotes the minimal closed subgroup of G containing all of $[g, h] = g^{-1}h^{-1}gh$ (resp. h^p) ($g \in G, h \in H$). If H is a normal subgroup of G, the left action of G on H is defined as ${}^g h = ghg^{-1}$. Let $\{G_i\}_i$ be the lower central series of G, which is defined as $G_1 = G$ and $G_i = [G, G_{i-1}]$ for $i \geq 2$ recursively. In particular, $G_2 = [G, G]$ is the closed commutator subgroup of G, and $G^{\mathrm{ab}} = G/G_2$ is the maximal abelian pro-p quotient of G. Burnside's basis theorem yields that G is finitely generated if and only if $\mathrm{r}_p(G^{\mathrm{ab}})$ is finite. Then $\mathrm{r}_p(G^{\mathrm{ab}})$ is the (minimal) number of generators of G. In particular, G is nontrivial procyclic (resp. trivial) if and only if $\mathrm{r}_p(G^{\mathrm{ab}}) = 1$ (resp. 0). If G is a prometacyclic pro-p group, then its pro-p quotients and H are also prometacyclic, in particular $\mathrm{r}_p(H^{\mathrm{ab}}) \leq 2$. A finite p-group G is metacyclic if and only if $G/(G_2)^pG_3$ is metacyclic (cf. [3, Theorem 2.3]).

A group-theoretical part of the proof of Theorem 1.1 is based on the following proposition, which does not depend on the parity of p.

Proposition 2.1. *Let G be a pro-p group such that $\mathrm{r}_p(G^{\mathrm{ab}}) = 2$. If G has a maximal subgroup H such that $\mathrm{r}_p(H/G_2) = \mathrm{r}_p(H^{\mathrm{ab}})$, then G is a prometacyclic pro-p group.*

Proof. First, we prove the statement for a finite p-group G with $\mathrm{r}_p(G^{\mathrm{ab}}) = 2$. If G is abelian, G is metacyclic. Also, if $\mathrm{r}_p(H^{\mathrm{ab}}) = 1$, then G is metacyclic. Assume that G is nonabelian and $\mathrm{r}_p(H/G_2) = \mathrm{r}_p(H^{\mathrm{ab}}) = 2$. There are generators a, b of G such that $\langle aG_2\rangle \cap \langle bG_2\rangle = \{1\}$. Then H is either $\langle a, b^p\rangle G_2$, $\langle a^p, b\rangle G_2$ or $\langle ab^i, b^p\rangle G_2 = \langle ab^i, a^p\rangle G_2$ with $1 \le i < p$. Replacing

$$(a,b) \text{ by } \begin{cases} (b,a) & \text{if } H = \langle a^p, b\rangle G_2, \\ (ab^i, a) & \text{if } H = \langle ab^i, b^p\rangle G_2 \text{ and } |\langle aG_2\rangle| \le |\langle bG_2\rangle|, \\ (ab^i, b) & \text{if } H = \langle ab^i, b^p\rangle G_2 \text{ and } |\langle aG_2\rangle| > |\langle bG_2\rangle|, \end{cases}$$

we may assume that $H = \langle a, b^p\rangle G_2$ and $\langle aG_2\rangle \cap \langle bG_2\rangle = \{1\}$. (For example, if $(ab^iG_2)^x \in \langle aG_2\rangle$, we have $b^{ix}G_2 \in \langle aG_2\rangle \cap \langle bG_2\rangle = \{1\}$, i.e., $x \equiv 0 \pmod{|\langle bG_2\rangle|}$. Then $(ab^iG_2)^x = 1$ if $|\langle aG_2\rangle| \le |\langle bG_2\rangle|$.) Note that $G_2/G_3 = \langle [a,b]G_3\rangle \not\simeq 1$. Since $[a, b^p] \equiv [a,b]^p \pmod{G_3}$, there is a surjective homomorphism $H^{\mathrm{ab}} \to H/(G_2)^pG_3 = \langle a(G_2)^pG_3, b^p(G_2)^pG_3, [a,b](G_2)^pG_3\rangle$. Since $\mathrm{r}_p(H^{\mathrm{ab}}) = 2$, we have $a^x(b^p)^y[a,b]^z \equiv 1 \pmod{(G_2)^pG_3}$ for some $(x,y,z) \not\equiv (0,0,0) \pmod p$. In particular, $a^x(b^p)^y \equiv 1 \pmod{G_2}$. Then $x = p^m x'$ and $y = p^{n-1}y'$ with some x', $y' \in \mathbb{Z}$, where $p^m = |\langle aG_2\rangle|$ and $p^n = |\langle bG_2\rangle|$. Since $\mathrm{r}_p(H/G_2) = 2$, we have $n \ge 2$, and hence $x \equiv y \equiv 0 \pmod p$. Therefore $z \in \mathbb{Z}_p^\times$. Note that $a^{p^m} \equiv [a,b]^u \pmod{G_3}$ and $b^{p^n} \equiv [a,b]^v \pmod{G_3}$ with some $u, v \in \mathbb{Z}$. Then $[a,b]^{-z} \equiv a^x b^{py} \equiv [a,b]^{ux'+vy'} \pmod{(G_2)^pG_3}$. This implies that $(u,v) \not\equiv (0,0) \pmod p$. Put $N = \langle a\rangle G_2$ or $N = \langle b\rangle G_2$ according to $u \in \mathbb{Z}_p^\times$ or $v \in \mathbb{Z}_p^\times$. Then both $N/(G_2)^pG_3$ and G/N are cyclic, and hence $G/(G_2)^pG_3$ is metacyclic. Therefore G is metacyclic by [3, Theorem 2.3].

Suppose that G is not necessarily finite. Let $\{U_i\}_i$ be the lower p-central series of G, which is defined as $U_1 = G$ and $U_i = U_{i-1}^p[G, U_{i-1}]$ for $i \ge 2$ recursively. We put $\overline{G} = G/U_i$ and $\overline{H} = H/U_i$ for arbitrary $i \ge 2$. Since $\{U_i\}_i$ forms a fundamental system of open neighbourhoods of 1, $\mathrm{r}_p(\overline{G}^{\mathrm{ab}}) = 2$ and $\mathrm{r}_p(\overline{H}/\overline{G}_2) = \mathrm{r}_p(\overline{H}^{\mathrm{ab}})$ if i is sufficiently large. Then $\overline{G}$ is metacyclic. Therefore $G \simeq \varprojlim G/U_i$ is prometacyclic. $\square$

For a nonabelian pro-2 group G, it is well known that $G^{\mathrm{ab}} \simeq [2,2]$ if and only if G is either (pro)dihedral, quaternion, generalized quaternion or semidihedral (cf. e.g. [13]). Such pro-2 groups G are prometacyclic.

Remark 2.2. Shafarevich's formula (cf. e.g. [14, (11.12)]) yields that the tame pro-p Galois group $G = G_S(\mathbb{Q})$ has deficiency zero; i.e., the cohomology with $\mathbb{Z}/p\mathbb{Z}$-coefficients satisfies $\mathrm{r}_p(H^1(G)) = \mathrm{r}_p(H^2(G))$ (cf. [21, (10.7.15)]). Since any finite noncyclic abelian p-group has nontrivial Schur multiplier, $G_S(\mathbb{Q})$ (and $G_S(\mathbb{Q}_\infty)$) cannot be abelian if $p \notin S$ and $G_S(\mathbb{Q})$ is not cyclic. We often use this fact.

2.2. **Ray class groups.** Let $k/\mathbb{Q}$ be an algebraic extension and S a finite set of integral divisors of (a subfield of) k which are prime to 2. Let S_k be the set of all primes of k dividing $\prod_{\mathfrak{a}\in S}\mathfrak{a}$. We denote by k_S (resp. k_S^{ab}, k_S^{elem}) the maximal (resp. maximal abelian, maximal elementary abelian) pro-2-extension of k unramified outside S_k, and put $G = G_S(k) = \mathrm{Gal}(k_S/k)$. Suppose that $[k : \mathbb{Q}]$ is finite and $S_k = \{\mathfrak{l}_1, \mathfrak{l}_2, \cdots, \mathfrak{l}_n\}$. Let k' be a subfield of k (possibly $k = k'$) such that k/k' is a 2-extension and $\mathrm{Gal}(k/k')$ acts on S_k. Then $\mathrm{Gal}(k/k')$ acts on G^{ab} via the left action of $\mathrm{Gal}(k_S^{\mathrm{ab}}/k')$ on $\mathrm{Gal}(k_S^{\mathrm{ab}}/k)$. We denote by $A_S(k)$ the Sylow 2-subgroup of the ray class group of k modulo $\prod_{i=1}^n \mathfrak{l}_i$. Then $A_S(k) \simeq \mathrm{Gal}(k_S^{\mathrm{ab}}/k) \simeq G^{\mathrm{ab}}$

and $A_S(k)/2 \simeq \mathrm{Gal}(k_S^{\mathrm{elem}}/k) \simeq G/G^2G_2$ as $\mathrm{Gal}(k/k')$-modules via the Artin map. Suppose that S_k contains no archimedean prime. The definition of the ray class groups induces an exact sequence

$$E(k) \xrightarrow{\Phi_{k,S}} (O_k/\textstyle\prod_{i=1}^n \mathfrak{l}_i)^\times \otimes \mathbb{Z}_2 \to A_S(k) \to A_\emptyset(k) \to 0$$

of $\mathrm{Gal}(k/k')$-modules, where O_k is the ring of integers in k, $E(k) = O_k^\times$ is the unit group of k. For each $1 \le i \le n$, we choose a primitive element $g_{\mathfrak{l}_i} \in O_k$ of the finite field $O_k/\mathfrak{l}_i$. Let 2^{e_i} be the order of the cyclic 2-group $(O_k/\mathfrak{l}_i)^\times \otimes \mathbb{Z}_2$. Then $\mathbb{Z}/2^{e_i}\mathbb{Z} \simeq (O_k/\mathfrak{l}_i)^\times \otimes \mathbb{Z}_2 : a \bmod 2^{e_i} \mapsto (g_{\mathfrak{l}_i}^a \bmod \mathfrak{l}_i) \otimes 1$. Depending on the choice of $g_{\mathfrak{l}_i}$ $(1 \le i \le n)$, the above sequence induces the exact sequence

$$\begin{array}{ccccc} E(k) & \xrightarrow{\varphi_{k,S}} & [2^{e_1}_{\mathfrak{l}_1}, 2^{e_2}_{\mathfrak{l}_2}, \cdots, 2^{e_n}_{\mathfrak{l}_n}] & \to A_S(k) \to A_\emptyset(k) \to 0, \\ \cup & & \cup & \\ \epsilon & \longmapsto & (a_1, a_2, \cdots, a_n), & \end{array}$$

where the second term denotes an abelian group $[2^{e_1}, 2^{e_2}, \cdots, 2^{e_n}] = \bigoplus_{i=1}^n (\mathbb{Z}/2^{e_i}\mathbb{Z})$, and a_i is the abbreviation of $a_i \bmod 2^{e_i}$ satisfying $\epsilon \equiv g_{\mathfrak{l}_i}^{a_i} \bmod \mathfrak{l}_i$. Let $\{\epsilon_j\}_{1 \le j \le d} \subset E(k)$ be a system (not necessarily minimum) such that $\{\varphi_{k,S}(\epsilon_j)\}_{1 \le j \le d}$ generates $\varphi_{k,S}(E(k))$ as a $\mathbb{Z}_2$-module. Then we put a column vector

$$v_{k,S} = \begin{pmatrix} \varphi_{k,S}(\epsilon_1) \\ \varphi_{k,S}(\epsilon_2) \\ \vdots \\ \varphi_{k,S}(\epsilon_d) \end{pmatrix} = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & & \vdots \\ a_{1d} & a_{2d} & \cdots & a_{nd} \end{pmatrix} = (a_{ij})_{1 \le j \le d,\, 1 \le i \le n}.$$

For any $A \in GL_d(\mathbb{Z}_2)$, the components of a vector $Av_{k,S}$ also generate $\mathrm{Im}\,\varphi_{k,S}$. By finding suitable A such that $Av_{k,S}$ has a simple form, one can calculate $\mathrm{Coker}\,\varphi_{k,S}$. For a set Σ of ideals of k such that $\Sigma_k = \{\mathfrak{l}_{i_1}, \mathfrak{l}_{i_2}, \cdots, \mathfrak{l}_{i_m}\} \subset S_k$, we choose the same $g_{\mathfrak{l}_{i_\mu}}$ $(1 \le \mu \le m)$. Then we have the exact sequence

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

with a vector

$$v_{k,\Sigma} = (\varphi_{k,\Sigma}(\epsilon_j))_{1 \le j \le d} = (a_{i_\mu j})_{1 \le j \le d,\, 1 \le \mu \le m}.$$

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

2.3. **Class number formulas.** We denote by $N_{K/k}$ (a map induced from) the norm mapping of a 2-extension K/k. For a cyclic 2-extension K/k with Galois group $\mathrm{Gal}(K/k) = \langle \sigma \rangle$, we have a genus formula

$$|\{[\mathfrak{A}] \in A_\emptyset(K) \,|\, \mathfrak{A}^\sigma = \mathfrak{A}\}| = \frac{|A_\emptyset(k)| \prod_{\mathfrak{r}} e(\mathfrak{r})}{[K:k]\, |E(k)/N_{K/k}E(K)|}, \tag{2.1}$$

which is well known as Chevalley's ambiguous class number formula (cf. also [17, Proposition 1], [31, Proof of Lemma 4], etc.), where $\mathfrak{r}$ varies among all primes of k and $e(\mathfrak{r})$ is the ramification index of $\mathfrak{r}$ in K/k. In particular for a quadratic extension K/k, 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.

On the other hand, we suppose that K/k is a $[2,2]$-extension with three quadratic subextensions F, F', F''. Then we have Kuroda's formula (cf. [16])

$$|A_\emptyset(K)| = \frac{2^{d-1-v}}{|E(k)/E(k)^2|} Q(K/k)|A_\emptyset(F)||A_\emptyset(F')||A_\emptyset(F'')||A_\emptyset(k)|^{-2} \tag{2.2}$$

where $Q(K/k) = |E(K)/E(F)E(F')E(F'')|$, d is the number of archimedean primes of k ramifying in K/k, and $v = 1$ or 0 according to whether $K = k(\sqrt{\epsilon}, \sqrt{\epsilon'})$ with some ϵ, $\epsilon' \in E(k)$ or not. In particular, if $k = \mathbb{Q}$ and K is real, then

$$|A_\emptyset(K)| = 4^{-1}Q(K/\mathbb{Q})|A_\emptyset(F)||A_\emptyset(F')||A_\emptyset(F'')| \tag{2.3}$$

and $Q(K/\mathbb{Q}) \in \{1, 2, 4\}$ (cf. [15]). Let ε, ε', ε'' be the fundamental units of the real quadratic fields F, F', F'' respectively. Then $N_{F/\mathbb{Q}}(\varepsilon) = 1$ if $\sqrt{\varepsilon} \in E(K)$. Moreover, $N_{F/\mathbb{Q}}(\varepsilon) = N_{F'/\mathbb{Q}}(\varepsilon') = 1$ if $\sqrt{\varepsilon\varepsilon'} \in E(K)$, and $N_{F/\mathbb{Q}}(\varepsilon) = N_{F'/\mathbb{Q}}(\varepsilon') = N_{F''/\mathbb{Q}}(\varepsilon'')$ if $\sqrt{\varepsilon\varepsilon'\varepsilon''} \in E(K)$.

3. Criteria

If $A_S(k) \simeq [2,2]$, then $G_S(k)$ is metacyclic. When $A_S(k) \not\simeq [2,2]$ and $A_\emptyset(k) \simeq 0$ (and S contains no archimedean primes), we obtain the following criterion for the metacyclicity of $G_S(k)$.

Theorem 3.1. *Let k be a finite extension of $\mathbb{Q}$ with odd class number. Assume that a triple $(K/k, S, \Sigma)$ is given, where S is a finite set of prime ideals of k none of which lies over 2, Σ is a subset of S such that $A_\Sigma(k) \simeq 0$, and K/k is a quadratic extension unramified outside S and ramified at all $\mathfrak{l} \in S \setminus \Sigma$. Then we have*

$$\mathrm{r}_2(A_S(k)) = 1 + \mathrm{r}_2(A_\Sigma(K)). \tag{3.1}$$

Moreover, if $\mathrm{r}_2(A_S(k)) = 2$ (i.e., $\mathrm{r}_2(A_\Sigma(K)) = 1$), then the following four statements hold true:

1. *For any $\mathfrak{l} \in S \setminus \Sigma$, we have $\mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(k)) = 1$; i.e., $k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}\}}/k$ is a quadratic extension. Then, moreover, $A_\Sigma(k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}\}}) \simeq 0$.*
2. *Assume that there is $\mathfrak{l} \in S\setminus\Sigma$ such that $k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}\}}$ is contained in a cyclic quartic extension of k unramified outside S, i.e., $\mathrm{r}_4(A_S(k)) = 2$ or $\mathrm{r}_4(A_S(k)) = \mathrm{r}_2(\mathrm{Gal}(k^{\mathrm{ab}}_S/K)) = 1$. Then $G_S(k)$ is metacyclic if and only if $|A_\Sigma(K)| = 2$.*
3. *If $\mathrm{r}_4(A_S(k)) = 1$, $\mathrm{r}_2(\mathrm{Gal}(k^{\mathrm{ab}}_S/K)) = 2$ and $|A_\Sigma(K)| \geq 4$, then $G_S(k)$ is metacyclic.*
4. *If $\mathrm{r}_4(A_S(k)) = 1$, $\mathrm{r}_2(\mathrm{Gal}(k^{\mathrm{ab}}_S/K)) = 2$, $|A_\Sigma(K)| = 2$ and the following three conditions are satisfied, then $G_S(k)$ is not metacyclic.*
   - (a) *$G_S(k)$ is nonabelian.*
   - (b) *$|O_k/\mathfrak{l}| \not\equiv 1 \pmod{|A_S(k)|}$ for any $\mathfrak{l} \in S \setminus \Sigma$.*
   - (c) *There exists $\mathfrak{l}_0 \in S \setminus \Sigma$ such that no $\mathfrak{l} \in S \setminus \Sigma$ is inert in $k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}_0\}}/k$.*

Proof. Since $A_\Sigma(k) \simeq 0$, i.e., $k^{\mathrm{ab}}_\Sigma = k$, the existence of K/k implies that $S \neq \Sigma$. Let σ be a generator of $\mathrm{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$. Since $1 + \sigma : A_\Sigma(K) \stackrel{\text{norm}}{\longrightarrow} A_\Sigma(k) \stackrel{\text{lift}}{\to} A_\Sigma(K)$ is zero mapping, $(A_\Sigma(K)/2)^{1+\sigma} \simeq 0$; i.e., σ acts on $A_\Sigma(K)/2$ trivially. Hence $K^{\mathrm{elem}}_\Sigma \subset k^{\mathrm{ab}}_S$, and the ramification index of any $\mathfrak{l} \in S \setminus \Sigma$ in $K^{\mathrm{elem}}_\Sigma/k$ is 2. If $\mathrm{r}_4(\mathrm{Gal}(K^{\mathrm{elem}}_\Sigma/k)) \geq 1$, K^{elem}_Σ contains a cyclic quartic extension of k. Then, since

$A_\Sigma(k) \simeq 0$, the cyclic quartic extension is totally ramified at some $\mathfrak{l} \in S \setminus \Sigma$; i.e., the ramification index of such $\mathfrak{l}$ in $K_\Sigma^{\mathrm{elem}}/k$ is at least 4. This is a contradiction. Therefore $K_\Sigma^{\mathrm{elem}} \subset k_S^{\mathrm{elem}}$, and hence $1 + \mathrm{r}_2(A_\Sigma(K)) \leq \mathrm{r}_2(A_S(k))$. On the other hand, since all $\mathfrak{l} \in S \setminus \Sigma$ ramify in K, k_S^{elem}/K is unramified outside Σ. Therefore $\mathrm{r}_2(A_S(k)) - 1 = \mathrm{r}_2(\mathrm{Gal}(k_S^{\mathrm{elem}}/K)) \leq \mathrm{r}_2(A_\Sigma(K))$, and hence we obtain the equality (3.1). In particular, we have $K_\Sigma^{\mathrm{elem}} = k_S^{\mathrm{elem}}$.

In the following, we assume that $\mathrm{r}_2(A_S(k)) = 2$. Let K' be the inertia field of $\mathfrak{l} \in S \setminus \Sigma$ in the $[2,2]$-extension k_S^{elem}/k. Since $k \subset K \subset k_S^{\mathrm{elem}}$ and $\mathfrak{l}$ ramifies in K/k, K' is a quadratic extension of k unramified outside $S \setminus \{\mathfrak{l}\}$. In particular, we have $\mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(k)) \geq 1$. Moreover, since $K' \not\subset k_\Sigma^{\mathrm{ab}} = k$, we have $S \setminus \{\mathfrak{l}\} \neq \Sigma$, i.e., $|S \setminus \Sigma| \geq 2$. On the other hand, since k_S^{elem}/k is not unramified outside $S \setminus \{\mathfrak{l}\}$, we have $\mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(k)) < \mathrm{r}_2(A_S(k)) = 2$, i.e., $\mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(k)) = 1$. Hence $K' = k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$. Moreover, $k_{S\setminus\{\mathfrak{l}\}}/k$ is cyclic. By the assumption that $A_\Sigma(k) \simeq 0$, $k_{S\setminus\{\mathfrak{l}\}}/k$ is totally ramified at some $\mathfrak{l}' \in S \setminus (\Sigma \cup \{\mathfrak{l}\})$. Since $k \subset K' \subset (K')_\Sigma^{\mathrm{ab}} \subset k_{S\setminus\{\mathfrak{l}\}}$, we have $K' = (K')_\Sigma^{\mathrm{ab}}$, i.e., $A_\Sigma(K') \simeq 0$. Hence statement (1) holds.

We show statement (2). Let F/k be a cyclic quartic extension unramified outside S, which contains $K' = k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ for some $\mathfrak{l} \in S \setminus \Sigma$. Let $\Sigma' \subset S \setminus \Sigma$ be the set of all primes in $S \setminus \Sigma$ which ramify in K'. Since $A_\Sigma(k) \simeq 0$, we have $\Sigma' \neq \emptyset$. Then $\mathfrak{l} \notin \Sigma' \cup \Sigma$ and $K' = k_{\Sigma\cup\Sigma'}^{\mathrm{elem}}$. Put a sequence $S \setminus \Sigma' = \Sigma_0 \subset \Sigma_1 \subset \cdots \subset \Sigma_n = S$ such that $\Sigma_i \setminus \Sigma_{i-1} = \{\mathfrak{l}_i\}$ $(1 \leq i \leq n)$. Then $\Sigma' = \{\mathfrak{l}_1, \cdots, \mathfrak{l}_n\}$. Since K/k and K'/k are ramified at any $\mathfrak{l}_i \in \Sigma'$, all $\mathfrak{l}_i$ have the common inertia field $K'' = k_{S\setminus\{\mathfrak{l}_i\}}^{\mathrm{elem}} = k_{\Sigma_0}^{\mathrm{elem}}$ in the $[2,2]$-extension k_S^{elem}/k. Moreover, we have $k_S^{\mathrm{elem}} \subset (K')_{\Sigma_0}^{\mathrm{elem}}$. Since the inertia group $I_{\mathfrak{l}_i} \subset G_{\Sigma_i}(K')^{\mathrm{ab}}$ of the unique prime of K' lying over $\mathfrak{l}_i$ is cyclic and $G_{\Sigma_i}(K')^{\mathrm{ab}}/I_{\mathfrak{l}_i} \simeq A_{\Sigma_{i-1}}(K')$, we have $\mathrm{r}_2(A_{\Sigma_i}(K')) \leq 2$ if $\mathrm{r}_2(A_{\Sigma_{i-1}}(K')) = 1$.

$$\begin{tikzcd}
K \arrow[rr, dash] \arrow[dd, dash] & & k_S^{\mathrm{elem}} \arrow[r, dotted, dash] \arrow[dd, dash] & (K')_{\Sigma_i}^{\mathrm{elem}} \\
 & K'' \arrow[ur, dash] & & \\
k \arrow[ur, dash] \arrow[rr, dash] & & K' \arrow[r, dash] & F
\end{tikzcd}$$

Now we assume that $|A_\Sigma(K)| = 2$. Since k_S^{elem}/K' is ramified at any prime lying over a prime in $\Sigma_0 \setminus \Sigma$, $(K')_{\Sigma_0}^{\mathrm{elem}}/k_S^{\mathrm{elem}}$ is unramified outside Σ. Recall that $k_S^{\mathrm{elem}} = K_\Sigma^{\mathrm{elem}}$. The assumption $|A_\Sigma(K)| = 2$ implies that $k_S^{\mathrm{elem}} = K_\Sigma$, i.e., $A_\Sigma(k_S^{\mathrm{elem}}) \simeq 0$. Hence $k_S^{\mathrm{elem}} = (K')_{\Sigma_0}^{\mathrm{elem}}$ and $\mathrm{r}_2(A_{\Sigma_0}(K')) = 1$. We can show that $\mathrm{r}_2(A_{\Sigma_i}(K')) = 1$ if $\mathrm{r}_2(A_{\Sigma_{i-1}}(K')) = 1$ and $i < n$ as follows. Suppose that $\mathrm{r}_2(A_{\Sigma_{i-1}}(K')) = 1$ and $\mathrm{r}_2(A_{\Sigma_i}(K')) = 2$ for $i < n$. Then $(K')_{\Sigma_i}^{\mathrm{elem}}/k$ is a Galois extension of degree 8, and $k_S^{\mathrm{elem}} = (K')_{\Sigma_{i-1}}^{\mathrm{elem}}$. Since $(K')_{\Sigma_i}^{\mathrm{elem}} \neq (K')_{\Sigma_{i-1}}^{\mathrm{elem}}$, $(K')_{\Sigma_i}^{\mathrm{elem}}/K''$ is totally ramified at a prime lying over $\mathfrak{l}_i$. Then $(K')_{\Sigma_i}^{\mathrm{elem}}/K''$ is a cyclic quartic extension. However, k_S^{elem}/K'' is ramified at any prime lying over $\mathfrak{l}_n \notin \Sigma_0$, and $(K')_{\Sigma_i}^{\mathrm{elem}}/k_S^{\mathrm{elem}}$ is unramified at any prime lying over $\mathfrak{l}_n \notin \Sigma_i$. This is a contradiction. Therefore $\mathrm{r}_2(A_{\Sigma_i}(K')) = 1$ if $\mathrm{r}_2(A_{\Sigma_{i-1}}(K')) = 1$ and $i < n$. Since $\mathrm{r}_2(A_{\Sigma_0}(K')) = 1$, we have $\mathrm{r}_2(A_{\Sigma_{n-1}}(K')) = 1$ by induction, and hence $\mathrm{r}_2(A_S(K')) \leq 2$. Put $G = G_S(k)$ and $H = G_S(K')$. Since FK/K' is a $[2,2]$-extension and $FK \subset k_S^{\mathrm{ab}}$, we have $\mathrm{r}_2(H/G_2) = \mathrm{r}_2(H^{\mathrm{ab}}) = \mathrm{r}_2(A_S(K')) = 2$. Then G is metacyclic by Proposition 2.1. Thus we obtain the if-part of statement (2).

Conversely, we assume that $|A_\Sigma(K)| \geq 4$. Then there exists a unique cyclic quartic extension L/K unramified outside Σ. Then $k_S^{\mathrm{elem}} = K_\Sigma^{\mathrm{elem}} \subset L$, and L/k is a Galois extension of degree 8. Since k_S^{elem}/K' is ramified at the primes lying over $\mathfrak{l}$, L/K' is not cyclic.

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & k_S^{\mathrm{elem}} \arrow[r, dash] \arrow[d, dash] & L \\
k \arrow[r, dash] & K' \arrow[r, dash] & F
\end{tikzcd}$$

Since K'/k is ramified at $\mathfrak{l}_1 \in \Sigma'$, k_S^{elem}/K' is unramified at any prime lying over $\mathfrak{l}_1$. Hence L/K' is a $[2,2]$-extension unramified outside $S \setminus \{\mathfrak{l}_1\}$. Since F/k is totally ramified at $\mathfrak{l}_1$, F/K' is a quadratic extension ramified at the prime lying over $\mathfrak{l}_1$. Therefore FL/K' is a $[2,2,2]$-extension unramified outside S. Then $G_S(k)$ is not metacyclic. Thus we obtain statement (2).

We show statement (3). Assume that $\mathrm{r}_4(A_S(k)) = 1$, $\mathrm{r}_2(\mathrm{Gal}(k_S^{\mathrm{ab}}/K)) = 2$ and $|A_\Sigma(K)| \geq 4$. Take $\mathfrak{l} \in S \setminus \Sigma$ arbitrarily. Since $A_\Sigma(k) \simeq 0$, the quadratic extension $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}/k$ is ramified at some $\mathfrak{l}' \in S \setminus \Sigma$. Then $k_S^{\mathrm{elem}} = k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}} k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{elem}}$ and $k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{elem}}/k$ is a quadratic extension ramified at $\mathfrak{l}$. Since $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}} \cap k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{elem}} = k$, we have $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{ab}} \cap k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{ab}} = k$. Note that both $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{ab}}$ and $k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{ab}}$ are cyclic extensions of k. Since $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{ab}} k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{ab}} \subset k_S^{\mathrm{ab}}$, the assumption $\mathrm{r}_4(A_S(k)) = 1$ implies that either $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{ab}}/k$ or $k_{S\setminus\{\mathfrak{l}'\}}^{\mathrm{ab}}/k$ is a quadratic extension. Replacing $\mathfrak{l}$ and $\mathfrak{l}'$ if necessary, we may assume that $|A_{S\setminus\{\mathfrak{l}\}}(k)| = 2$, i.e., $k_{S\setminus\{\mathfrak{l}\}} = k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{ab}} = k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$. Put $r = \mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(K)) \geq \mathrm{r}_2(A_\Sigma(K)) = 1$. We can also show that $r = 1$ as follows. Suppose that $r \geq 2$. Note that $k_S^{\mathrm{elem}} = K_\Sigma^{\mathrm{elem}} \subset K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$. Then $K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}/k$ is a Galois extension of degree 2^{r+1}, and hence $K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ is a Galois extension of degree 2^r. Let $M = (k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}})_S^{\mathrm{ab}} \cap K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ be the maximal abelian extension of $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ contained in $K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ (cf. a diagram below). Since $|\mathrm{Gal}(K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}})| = 2^r \neq 2$, we have $|\mathrm{Gal}(K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}})^{\mathrm{ab}}| > 2$, i.e., $M \neq k_S^{\mathrm{elem}}$. Then $M/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ is an abelian extension of degree at least 4. On the other hand, since $\mathrm{r}_2(A_\Sigma(K)) = 1$ and $|A_\Sigma(K)| \geq 4$, there exists a unique cyclic quartic extension L/K unramified outside Σ. Then L/k is a Galois extension of degree 8, and hence $L/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ is also an abelian quartic extension. Since M/K is an elementary abelian 2-extension, we have $L \cap M = k_S^{\mathrm{elem}}$. Therefore $LM/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ is an abelian extension of degree at least 8.

$$\begin{tikzcd}
 & L \arrow[rr, dash] \arrow[d, dash] & & LM \arrow[d, dash] & \\
k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}} \arrow[r, dash] \arrow[d, dash] & k_S^{\mathrm{elem}} \arrow[rr, dash] \arrow[d, dash] & & M \arrow[r, dotted, dash] & K_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}} \\
k \arrow[r, dash] & K & & &
\end{tikzcd}$$

Let I be the subgroup of $\mathrm{Gal}(LM/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}})$ generated by the inertia groups of the prime ideals $\mathfrak{L}$ of $k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ lying over $\mathfrak{l}$. Since LM/k_S^{elem} is unramified outside $S \setminus \{\mathfrak{l}\}$, the ramification indices of $\mathfrak{L}$ in $LM/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}}$ are at most 2. Since the number of $\mathfrak{L}$ is at most 2, we have $|I| \leq 4$. Then $|\mathrm{Gal}(LM/k_{S\setminus\{\mathfrak{l}\}}^{\mathrm{elem}})/I| \geq 8/4 = 2$, and hence the fixed field of I is a nontrivial abelian 2-extension of $k_{S\setminus\{\mathfrak{l}\}} = k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}\}}$ unramified outside $S \setminus \{\mathfrak{l}\}$. This is a contradiction. Therefore $\mathrm{r}_2(A_{S\setminus\{\mathfrak{l}\}}(K)) = r = 1$. Put $G = G_S(k)$ and $H = G_S(K)$. Since the inertia group $I_{\mathfrak{l}} \subset H^{\mathrm{ab}}$ of the unique prime of K lying over $\mathfrak{l}$ is cyclic and $H^{\mathrm{ab}}/I_{\mathfrak{l}} \simeq A_{S\setminus\{\mathfrak{l}\}}(K)$, we have $\mathrm{r}_2(H^{\mathrm{ab}}) \le 2$. The assumption $\mathrm{r}_2(H/G_2) = \mathrm{r}_2(\mathrm{Gal}(k_S^{\mathrm{ab}}/K)) = 2$ yields that $\mathrm{r}_2(H^{\mathrm{ab}}) = 2$. Then G is metacyclic by Proposition 2.1. Thus we obtain statement (3).

We show statement (4). Put $K' = k^{\mathrm{elem}}_{S\setminus\{\mathfrak{l}_0\}}$, and put $G = G_S(k)$, $H = G_S(K)$ and $H' = G_S(K')$. Since $G^{\mathrm{ab}} \simeq A_S(k) \simeq [2, 2^m]$ with some $m \ge 2$, G has two generators a, b such that $a^2 \equiv b^{2^m} \equiv 1 \pmod{G_2}$. Since $H/G_2 \simeq \mathrm{Gal}(k_S^{\mathrm{ab}}/K)$ and $\mathrm{r}_2(\mathrm{Gal}(k_S^{\mathrm{ab}}/K)) = 2$, we have $\mathrm{r}_2(A_S(K)) \ge 2$ and $H'/G_2 \simeq \mathbb{Z}/2^m\mathbb{Z}$. Replacing b by ab if necessary, we may assume that $H' = \langle b, G_2\rangle$. Then $H = \langle a, b^2, G_2\rangle = \langle a, b^2, [a,b], (G_2)^2G_3\rangle$, and $H/(G_2)^2G_3$ is abelian (cf. the proof of Proposition 2.1). The condition (4a) yields that $[a,b] \notin (G_2)^2G_3$. Suppose that $\mathrm{r}_2(A_S(K)) = 2$. Then, since there are surjective homomorphisms $A_S(K) \to H/(G_2)^2G_3 \to H/G_2$, we have $\mathrm{r}_2(H/(G_2)^2G_3) = 2$. Since $\langle a, b^{2^{m-1}}G_2\rangle/G_2 \simeq [2,2]$ and $G_2/(G_2)^2G_3 = \langle [a,b](G_2)^2G_3\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, we have $\langle a, b^{2^{m-1}}G_2\rangle/(G_2)^2G_3 \simeq [2,4]$. Hence $a^2 \notin (G_2)^2G_3$ or $b^{2^m} \notin (G_2)^2G_3$. Note that $A_\Sigma(K') \simeq A_\emptyset(K') \simeq 0$ by statement (1). By the snake lemma for the commutative diagram

$$\begin{array}{ccccccc}
 & & E(K')\otimes\mathbb{Z}_2 & \xrightarrow{\Phi_{K',S}} & (O_{K'}/\prod_{\mathfrak{L}\in S_{K'}}\mathfrak{L})^\times\otimes\mathbb{Z}_2 & \longrightarrow & A_S(K') \longrightarrow 0 \\
 & & \downarrow & & \downarrow{\scriptstyle\Psi} & & \downarrow \\
0 & \longrightarrow & \mathrm{Im}\,\Phi_{K',\Sigma} & \longrightarrow & (O_{K'}/\prod_{\mathfrak{Q}\in\Sigma_{K'}}\mathfrak{Q})^\times\otimes\mathbb{Z}_2 & \longrightarrow & A_\Sigma(K')
\end{array}$$

with exact rows, we obtain a surjective homomorphism $(O_{K'}/\prod_{\mathfrak{L}\in S_{K'}\setminus\Sigma_{K'}}\mathfrak{L})^\times \otimes \mathbb{Z}_2 \simeq \mathrm{Ker}\,\Psi \to A_S(K')$. The condition (4c) yields that $O_{K'}/\mathfrak{L} \simeq O_k/\mathfrak{l}$ for any $\mathfrak{L} \in S_{K'}\setminus\Sigma_{K'}$ and $\mathfrak{l} = \mathfrak{L}\cap K' \in S\setminus\Sigma$. Hence the condition (4b) implies that the exponent of $A_S(K') \simeq (H')^{\mathrm{ab}}$ is at most 2^m. In particular, $b^{2^m} \in (H')_2$. Since $H'/(G_2)^2G_3 = \langle b(G_2)^2G_3, [a,b](G_2)^2G_3\rangle$ is also abelian, i.e., $(H')_2 \subset (G_2)^2G_3$, we have $b^{2^m} \in (G_2)^2G_3$. Therefore $a^2 \notin (G_2)^2G_3$, and hence $a^2 \equiv [a,b] \pmod{(G_2)^2G_3}$. Since

$$a^{-1}b^2a \equiv b^2[b^2,a] \equiv b^2[b,a]^2 \equiv b^2 \pmod{(G_2)^2G_3},$$

the fixed field k_S^N of $N = \langle b^2, (G_2)^2G_3\rangle$ is a Galois extension of k. Note that $b^{2^{m-1}} \notin G_2 \supset (G_2)^2G_3$. Since

$$[k_S^N : k] = \frac{|G/G_2||G_2/(G_2)^2G_3|}{|N/(G_2)^2G_3|} = \frac{2^{m+1}\cdot 2}{2^{m-1}} = 8,$$

we have $\mathrm{Gal}(k_S^N/K') \simeq H'/N = \langle bN, [a,b]N\rangle \simeq [2,2]$ and $\mathrm{Gal}(k_S^N/K) \simeq H/N = \langle aN\rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Put $H'' = \langle ab, G_2\rangle$, and let $K'' = k_S^{H''}$ be the fixed field of H''. Since

$$(ab)^2 = abab \equiv ab^{-1}ab = a^2[a,b] \equiv [a,b]^2 \equiv 1 \pmod{N},$$

we have $\mathrm{Gal}(k_S^N/K'') \simeq H''/N \simeq \langle abN, [a,b]N\rangle \simeq [2,2]$. (In fact, k_S^N/k is a dihedral extension of degree 8.)

$$\begin{tikzcd}
k_S^{\langle b,(G_2)^2G_3\rangle} \arrow[rr, dash] \arrow[d, dash] & & k_S^N \arrow[r, dash] \arrow[d, dash] & k_S^{(G_2)^2G_3} \arrow[d, dash] \\
K' \arrow[rr, dash] \arrow[dd, dash] & & k_S^{\mathrm{elem}} \arrow[r, dash] \arrow[dd, dash] & k_S^{\mathrm{ab}} \arrow[dd, dash] \\
& K'' \arrow[ur, dash] \arrow[dl, dash] & & \\
k \arrow[rr, dash] & & K \arrow[r, dash] & k_S^{\langle a,G_2\rangle}
\end{tikzcd}$$

For any $\mathfrak{l} \in S \setminus \Sigma$, the inertia field of $\mathfrak{l}$ in the $[2,2]$-extension k_S^{elem}/k is either K' or K''; i.e., either k_S^{elem}/K' or k_S^{elem}/K'' is ramified at any prime lying over $\mathfrak{l}$. Since k_S^N/K' and k_S^N/K'' are $[2,2]$-extensions, $k_S^N/k_S^{\mathrm{elem}}$ is unramified outside Σ. Since $k_S^{\mathrm{elem}} = K_\Sigma^{\mathrm{elem}}$, k_S^N/K is a cyclic quartic extension unramified outside Σ. However, $|A_\Sigma(K)| = 2$ by the assumption of statement (4). This is a contradiction. Therefore we have $\mathrm{r}_2(A_S(K)) \geq 3$, and hence $G_S(k)$ is not metacyclic. Thus the proof of Theorem 3.1 is completed. $\square$

We see various examples of Theorem 3.1 in the proof of Theorem 1.1 (from Sections 5 to 8).

4. Cyclotomic $\mathbb{Z}_2$-extensions

We recall some basic facts on cyclotomic $\mathbb{Z}_2$-extensions. Put $\zeta_{2^{n+2}} = \exp \frac{2\pi\sqrt{-1}}{2^{n+2}} \in \mathbb{C}$ and $\mathbb{Q}_n = \mathbb{Q}(\cos \frac{2\pi}{2^{n+2}}) \subset \mathbb{Q}(\zeta_{2^{n+2}})$ for each $n \geq 0$. The Galois group $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ of the basic $\mathbb{Z}_2$-extension $\mathbb{Q}_\infty = \bigcup_{n\geq 0} \mathbb{Q}_n = \mathbb{Q}_{\{2\}}$ is isomorphic to the additive group of $\mathbb{Z}_2$ (i.e., an infinite procyclic pro-2 group). For a finite extension $k/\mathbb{Q}$, we put $k_n = k\mathbb{Q}_n$. Then the field $k_\infty = k\mathbb{Q}_\infty = \bigcup_{n\geq 0} k_n$ is the cyclotomic $\mathbb{Z}_2$-extension of k with the Galois group $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$. In particular, $\mathbb{Q}(\zeta_{2^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{2^{n+2}})$ is the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{-1})$. The following proposition provides a description of the cases with trivial $G_S(\mathbb{Q}_\infty)$.

Proposition 4.1. *Let $k/\mathbb{Q}$ be a finite extension and S a finite set of primes of k none of which lies over 2. If the prime of k lying over 2 is unique and $G_S(k)^{\mathrm{ab}} \simeq 0$, then $G_S(k_\infty)$ is trivial for the cyclotomic $\mathbb{Z}_2$-extension k_∞/k.*

Proof. Since $G_S(k)^{\mathrm{ab}} \simeq 0$, we have $A_\emptyset(k) \simeq 0$, and hence k_∞/k is totally ramified at the unique prime $\mathfrak{p}$ of k lying over 2. Suppose that $G_S(k_\infty)$ is nontrivial. Since k_∞/k is totally ramified at $\mathfrak{p}$ and $(k_\infty)_S^{\mathrm{ab}}/k_\infty$ is a nontrivial pro-2-extension unramified at the prime lying over $\mathfrak{p}$, $G = \mathrm{Gal}((k_\infty)_S^{\mathrm{ab}}/k)$ is not procyclic. Hence the fixed field L of G_2 is a nontrivial pro-2-extension of k_∞ unramified outside S. Since the abelian pro-2-extension L/k is not totally ramified at $\mathfrak{p}$, the inertia field of $\mathfrak{p}$ is a nontrivial abelian 2-extension of k unramified outside S. Then $G_S(k)^{\mathrm{ab}} \not\simeq 0$. This is a contradiction. Therefore $G_S(k_\infty)$ is trivial. Thus the proof of Proposition 4.1 is completed. $\square$

The following corollary for $S = \emptyset$ is a theorem of Weber.

Corollary 4.2. *Let S be a finite set of primes of $\mathbb{Q}$ not containing 2. Then $G_S(\mathbb{Q}_\infty)$ is trivial if and only if $S \subset \{\infty\}$ or $S = \{q\}$ and $q \equiv 3 \pmod 4$. In particular, we have $A_{\{q\}}(\mathbb{Q}_n) \simeq 0$ for all $n \geq 0$ if $q \equiv 3 \pmod 4$.*

Proof. By Proposition 4.1, $G_S(\mathbb{Q}_\infty)$ is trivial if and only if $G_S(\mathbb{Q})^{\mathrm{ab}} \simeq 0$. Hence we obtain the claim. $\square$

Depending on the choice of a topological generator γ of $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$, a module over the complete group ring $\mathbb{Z}_2[[\mathrm{Gal}(k_\infty/k)]]$ is regarded as a module over the ring $\Lambda = \mathbb{Z}_2[[T]]$ of formal power series via the isomorphism $\mathbb{Z}_2[[\mathrm{Gal}(k_\infty/k)]] \simeq \Lambda : \gamma \mapsto 1+T$. Let S be a finite set of primes of k none of which lies over 2. For fixed $\widetilde{\gamma} \in \mathrm{Gal}((k_\infty)_S/k)$ such that $\widetilde{\gamma}|_{\mathbb{Q}_\infty} = \gamma$, the left action of Γ on $G_S(k_\infty)$ is defined by ${}^\gamma g = \widetilde{\gamma} g \widetilde{\gamma}^{-1}$ ($g \in G_S(k_\infty)$). Recall that $G_S(k_\infty) \simeq \varprojlim G_S(k_n)$. Then we obtain an isomorphism $G_S(k_\infty)^{\mathrm{ab}} \simeq \varprojlim A_S(k_n)$ as Λ-modules, where the projective limit is taken on N_{k_n/k_m}. Suppose that k_∞/k is totally ramified at any prime lying over 2. For any $n \geq m$, since $k_n \cap (k_m)_S = k_m$, the restriction mapping $G_S(k_n) \to G_S(k_m)$ is surjective. Hence $N_{k_n/k_m} : A_S(k_n) \to A_S(k_m)$ is also surjective. The following theorem (Fukuda's theorem [7] for $p = 2$) is frequently used in the following sections. We give a proof for convenience.

Theorem 4.3 (Fukuda)**.** *Let k_∞ be the cyclotomic $\mathbb{Z}_2$-extension of a finite extension k of $\mathbb{Q}$ and S a finite set of prime ideals of k none of which lies over* 2*. Assume that k_∞/k is totally ramified at any prime lying over* 2*. Then the following two statements hold true for $m \geq 0$:*

(1) *If $|A_S(k_{m+1})| = |A_S(k_m)|$, then $A_S(k_n) \simeq A_S(k_m)$ for all $n \geq m$.*
(2) *Suppose that $e \geq 1$. If $|A_S(k_{m+1})/2^e| = |A_S(k_m)/2^e|$, then $A_S(k_n)/2^e \simeq A_S(k_m)/2^e$ for all $n \geq m$.*

Proof. Since k_∞ is also the cyclotomic $\mathbb{Z}_2$-extension of k_m and $A_S(k_n) = A_{S_{k_m}}(k_n)$ for all $n \geq m$, it suffices to prove the statements for $m = 0$. Put $X = G_S(k_\infty)^{\mathrm{ab}} \simeq \varprojlim A_S(k_n)$. By the same argument as in [29, §13.3], X is a finitely generated Λ-module, and $A_S(k_n) \simeq X/\nu_n Y$ for all $n \geq 0$, where $Y = \mathrm{Gal}((k_\infty)_S^{\mathrm{ab}}/k_\infty k_S^{\mathrm{ab}})$ and $\nu_n = ((1+T)^{2^n} - 1)/T$. Note that $\nu_0 = 1$ and $\nu_1 = 2+T \in (2, T)$, where $(2, T)$ is the maximal ideal of Λ. If $|A_S(k_1)| = |A_S(k)|$, we have $|X/\nu_1 Y| = |X/Y|$, which implies that $Y = \nu_1 Y \subset (2, T)Y$. Then Nakayama's lemma for Y yields that $Y \simeq 0$, i.e., $A_S(k_n) \simeq X \simeq A_S(k)$ for all $n \geq 0$. Suppose that $|A_S(k_1)/2^e| = |A_S(k)/2^e|$. Then $|X/(\nu_1 Y + 2^e X)| = |X/(Y + 2^e X)|$, and hence $Y + 2^e X = \nu_1 Y + 2^e X \subset (2, T)Y + 2^e X$. Nakayama's lemma for $(Y + 2^e X)/2^e X$ yields that $Y \subset 2^e X$. In particular, $\nu_n Y \subset 2^e X$ for all $n \geq 0$. Therefore $A_S(k_n)/2^e \simeq X/(\nu_n Y + 2^e X) \simeq X/2^e$ for all $n \geq 0$. Thus the proof of Theorem 4.3 is completed. $\square$

As an example of the usage of Theorem 4.3, we obtain the following.

Corollary 4.4. *Under the same assumptions of Theorem* 4.3*, the following hold true:*

(1) *If $A_S(k) \simeq 0$ and $|A_S(k_2)| = 2$, then $|A_S(k_n)| = 2$ for all $n \geq 1$.*
(2) *If $\mathrm{r}_2(A_S(k_2)) = 1 + \mathrm{r}_2(A_S(k))$, then $\mathrm{r}_2(A_S(k_n)) = 1 + \mathrm{r}_2(A_S(k))$ for all $n \geq 1$.*

Proof. Put $A_n = A_S(k_n)$ or $A_n = A_S(k_n)/2$ according to the statements. If $|A_1| = |A_0|$, then $|A_n| = |A_0|$ for all $n \geq 0$ by Theorem 4.3 for $m = 0$. Therefore $|A_1| \neq |A_0|$ if $|A_2| \neq |A_0|$. If $|A_2| = 2|A_0|$, the surjectivity of N_{k_n/k_m} yields that $2|A_0| = |A_2| \geq |A_1| > |A_0|$, i.e., $|A_2| = |A_1|$. Then $|A_n| = |A_1| = 2|A_0|$ for all $n \geq 1$ by Theorem 4.3 for $m = 1$. Thus we obtain the statements. $\square$

For the basic $\mathbb{Z}_2$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, we choose a canonical generator $\gamma = \overline{\gamma}|_{\mathbb{Q}_\infty}$ of $\mathit{\Gamma}$ with a generator $\overline{\gamma}$ of $\overline{\mathit{\Gamma}} = \mathrm{Gal}(\mathbb{Q}(\zeta_{2^\infty})/\mathbb{Q}(\zeta_4)) \simeq \mathbb{Z}_2$ such that $\overline{\gamma}(\zeta_{2^{n+2}}) = \zeta_{2^{n+2}}^5$ for all $n \geq 0$. Moreover, we can choose $\widetilde{\gamma}$ such that $\widetilde{\gamma} \in \mathrm{Gal}((\mathbb{Q}_\infty)_S/\mathbb{Q}_S)$. Fukuda's theorem (Theorem 4.3) above and Theorem 3.1 imply that it suffices to consider mainly the metacyclicity of $G_S(\mathbb{Q}_2)$ (or $G_S(\mathbb{Q}_1)$) in the proof of Theorem 1.1. Then we often use the cyclotomic unit

$$\xi = \zeta_{16}^{-2} \frac{1-\zeta_{16}^5}{1-\zeta_{16}} \in E(\mathbb{Q}_2)$$

to calculate $A_S(\mathbb{Q}_2)$. Since $\zeta_{16}^{\gamma^2} = \zeta_{16}^9 = -\zeta_{16}$, we have $N_{\mathbb{Q}_2/\mathbb{Q}_1}(\xi) = \xi^{1+\gamma^2} = \zeta_8^{-2}\frac{1-\zeta_8^5}{1-\zeta_8} = \varepsilon_2$, where $\varepsilon_2 = 1+\sqrt{2} \in E(\mathbb{Q}_1)$ is the fundamental unit of $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$. Note that the class number of $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is 1. Since $A_\emptyset(\mathbb{Q}_n) \simeq 0$ for all $n \geq 0$ (by Corollary 4.2), the genus formula (2.1) for $\mathbb{Q}_n/\mathbb{Q}$ yields that $N_{\mathbb{Q}_n/\mathbb{Q}} = \sum_{i=0}^{2^n-1} \gamma^i : E(\mathbb{Q}_n) \to E(\mathbb{Q})$ is surjective. Hence $E(\mathbb{Q}_n) \otimes \mathbb{Z}_2$ is a cyclic $\mathit{\Lambda}$-module for all $n \geq 0$, and $E(\mathbb{Q}_2) = \langle \xi, \xi^\gamma, \xi^{\gamma^2}, \xi^{\gamma^3} \rangle$ (cf. [29, Theorem 8.2, Proposition 8.11 and Remark]). In the following sections, we denote by ε_d the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{d})$. For $z \in \mathbb{Z}$, $v_2(z)$ denotes the normalized additive 2-adic valuation, i.e., $|\mathbb{Z}_2/z\mathbb{Z}_2| = 2^{v_2(z)}$.

5. The case $S = \{\ell\}$

This section treats the case where $S = \{\ell\}$ consists of one prime $\ell \equiv 1 \pmod 4$. First, we determine the sets S with procyclic $G_S(\mathbb{Q}_\infty)$.

Proposition 5.1. *Put $S = \{\ell\}$ with a prime number $\ell \equiv 1 \pmod 4$. Then the following four conditions are equivalent:*

1. *$G_S(\mathbb{Q}_\infty)$ is procyclic.*
2. *$G_S(\mathbb{Q}_\infty)$ is finite cyclic.*
3. *$G_\emptyset(\mathbb{Q}_\infty(\sqrt{\ell}))$ is trivial.*
4. *ℓ satisfies $\ell \equiv 5 \pmod 8$ or $\ell \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell}\right)_4 \left(\frac{\ell}{2}\right)_4 = -1$.*

Moreover, we have $G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}/2\mathbb{Z}$ if $\ell \equiv 5 \pmod 8$.

Proof. Since $G_S(\mathbb{Q}_\infty)^{\mathrm{ab}}$ is finite by [9, Theorem 3.1], the conditions (1) and (2) are equivalent. Put $k = \mathbb{Q}(\sqrt{\ell})$. By (3.1) for the triple $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$, we have $\mathrm{r}_2(G_S(\mathbb{Q}_n)^{\mathrm{ab}}) = 1 + \mathrm{r}_2(G_\emptyset(k_n)^{\mathrm{ab}})$ for all $n \geq 0$, and hence the conditions (1) and (3) are equivalent. The conditions (3) and (4) are also equivalent by [20, Corollary 3.4] (and [23]). Suppose that $\ell \equiv 5 \pmod 8$. Then $k = \mathbb{Q}_S$. Since 2 is inert in k and $A_S(k) \simeq 0$, $G_S(k_\infty)$ is trivial by Proposition 4.1. This implies that $k_\infty = (\mathbb{Q}_\infty)_S$, and hence $G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}/2\mathbb{Z}$. □

We prove the following theorem which characterizes $S = \{\ell\}$ such that $G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic.

Theorem 5.2. *Put $S = \{\ell\}$ with a prime number $\ell \equiv 1 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic if and only if one of the following two conditions holds:*

1. *$\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$, $\left(\frac{\varepsilon_2}{\ell}\right)_4 = 1$, and $|A_\emptyset(\mathbb{Q}_2(\sqrt{\ell}))| = 2$.*
2. *$\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$, $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$, and $|A_\emptyset(\mathbb{Q}_2(\sqrt{\ell}))| \geq 4$.*

Proof. By Proposition 5.1, it suffices to consider the case where $\ell \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell}\right)_4 = (-1)^{\frac{\ell-1}{8}}$. Put $k = \mathbb{Q}(\sqrt{\ell})$ and $k' = \mathbb{Q}(\sqrt{2\ell})$. Let $\mathfrak{l}$ be a prime ideal of $\mathbb{Q}_1$ lying over ℓ. In the following, $z_\ell \in \mathbb{Z}$ denotes a primitive element modulo ℓ.

Lemma 5.3. *If* $\ell \equiv 1 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = 1$ *and* $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$, *then* $|A_\emptyset(k_2)| \geq 4$ *and* $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 2$.

Proof. Proposition 5.1 and Theorem 4.3 imply that $A_\emptyset(k_1) \not\simeq 0$. Since $k' \subset k_1 \subset (k')^{\mathrm{ab}}_\emptyset$ and $\mathrm{r}_2(A_\emptyset(k')) = 1$ (cf. e.g. [30]), we have $(k')^{\mathrm{ab}}_\emptyset = (k_1)^{\mathrm{ab}}_\emptyset$ and hence $\mathrm{r}_2(A_\emptyset(k_1)) = 1$. Then (3.1) for the triple $(k_1/\mathbb{Q}_1, \{\mathfrak{l}, \mathfrak{l}^\gamma\}, \emptyset)$ yields that $\mathrm{r}_2(A_S(\mathbb{Q}_1)) = 2$. Moreover, $(\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}/\mathbb{Q}_1$ is a quadratic extension by Theorem 3.1(1). Note that $A_{\{\mathfrak{l}\}}(\mathbb{Q}_1)/2 \simeq \mathrm{Gal}((\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}/\mathbb{Q}_1)$ via the Artin map. Since $O_{\mathbb{Q}_1}/\mathfrak{l} \simeq \mathbb{Z}/\ell\mathbb{Z}$, $\sqrt{2} \equiv z_\ell^x \pmod{\mathfrak{l}}$ with some $x \in \mathbb{Z}$. Then $2 \equiv z_\ell^{2x} \pmod{\ell}$. The assumption $\left(\frac{2}{\ell}\right)_4 = 1$ yields that x is even. Therefore $[(\sqrt{2}^{\frac{\ell-1}{2^m}})] = [(z_\ell^{\frac{\ell-1}{2^m}})]^x \in 2A_{\{\mathfrak{l}\}}(\mathbb{Q}_1)$ as the ideal classes, where $m = v_2(\ell-1) \geq 4$. This implies that the prime $(\sqrt{2})$ of $\mathbb{Q}_1$ splits in $(\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}$. Then the prime of $\mathbb{Q}_n$ lying over 2 splits completely in the $[2,2]$-extension $(\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}k_n/\mathbb{Q}_n$, and hence a prime $\mathfrak{p}_n$ of k_n lying over 2 also splits in the unramified quadratic extension $(\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}k_n/k_n$ for all $n \geq 1$. Suppose that $|A_\emptyset(k_2)| = 2$. Then $A_\emptyset(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$ by Theorem 4.3, and $A_\emptyset(k_n) = A_\emptyset(k_n)^\Gamma = \langle [\mathfrak{p}_n^{h_n/2}] \rangle$ by [8, Theorem 2], where h_n is the class number of k_n. This implies that $\mathfrak{p}_n$ is inert in $(k_n)^{\mathrm{ab}}_\emptyset = (\mathbb{Q}_1)^{\mathrm{elem}}_{\{\mathfrak{l}\}}k_n$. This is a contradiction. Therefore $|A_\emptyset(k_2)| \geq 4$.

Let $\mathfrak{L}$ be a prime ideal of $\mathbb{Q}_2$ lying over $\mathfrak{l}$. By the assumption $\ell \equiv 1 \pmod{16}$, ℓ splits completely in $\mathbb{Q}_2$, and hence $O_{\mathbb{Q}_2}/\mathfrak{L}^{\gamma^i} \simeq O_{\mathbb{Q}_1}/\mathfrak{l}^{\gamma^i} \simeq \mathbb{Z}/\ell\mathbb{Z}$. We choose $g_{\mathfrak{L}^{\gamma^i}} = g_{\mathfrak{l}^{\gamma^i}} = z_\ell$ for any i. Recall that $m = v_2(\ell-1) \geq 4$. Then we obtain the commutative diagram

$$\begin{array}{ccccccc}
E(\mathbb{Q}_2) & \xrightarrow{\varphi_{\mathbb{Q}_2,S}} & [2^m_{\mathfrak{L}}, 2^m_{\mathfrak{L}^\gamma}, 2^m_{\mathfrak{L}^{\gamma^2}}, 2^m_{\mathfrak{L}^{\gamma^3}}] & \longrightarrow & A_S(\mathbb{Q}_2) & \longrightarrow & 0 \\
\uparrow\cup & & \uparrow\psi & & & & \\
E(\mathbb{Q}_1) & \xrightarrow{\varphi_{\mathbb{Q}_1,S}} & [2^m_{\mathfrak{l}}, 2^m_{\mathfrak{l}^\gamma}] & \longrightarrow & A_S(\mathbb{Q}_1) & \longrightarrow & 0
\end{array}$$

with exact rows, where $\psi(x_0, x_1) = (x_0, x_1, x_0, x_1)$. Moreover, since $\varepsilon_2 = \xi^{1+\gamma^2}$, we have

$$v_{\mathbb{Q}_2,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_2,S}(\xi) \\ \varphi_{\mathbb{Q}_2,S}(\xi^\gamma) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^2}) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^3}) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_0 \end{pmatrix}$$

and

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2^{m-1} & 2^{m-1} \\ a_0 + a_2 & a_1 + a_3 \end{pmatrix}$$

with some a_j $(0 \leq j \leq 3)$, where we note that $-1 \equiv z_\ell^{\frac{\ell-1}{2}} \pmod{\ell}$ and $\frac{\ell-1}{2} \equiv 2^{m-1} \pmod{2^m}$. By the assumption that $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$, at least one of a_j is odd. Since $\xi^{1+\gamma+\gamma^2+\gamma^3} = -1$, we have $a_0 + a_1 + a_2 + a_3 \equiv 2^{m-1} \pmod{2^m}$. Since $\mathrm{r}_2(A_S(\mathbb{Q}_1)) = 2$, we have $\mathrm{Im}\,\varphi_{\mathbb{Q}_1,S} \subset 2[2^m, 2^m]$, i.e., $a_0 + a_2 \equiv a_1 + a_3 \equiv 0 \pmod 2$. Then, in particular, $a_0 + a_2 \equiv a_1 + a_3 \pmod 4$. If $a_0 + a_2 \equiv a_1 + a_3 \equiv 0 \pmod 4$, we have $\mathrm{Im}\,\varphi_{\mathbb{Q}_1,S} \subset 4[2^m, 2^m]$ and hence $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = \mathrm{r}_4(A_S(\mathbb{Q}_1)) = 2$. Suppose that $a_0 + a_2 \equiv a_1 + a_3 \equiv 2 \pmod 4$. If all of a_j is odd, then $v_{\mathbb{Q}_2,S} \equiv (1)_{0 \leq i \leq 3, 0 \leq j \leq 3} \pmod 2$, which implies that $A_S(\mathbb{Q}_2)/2 \simeq \mathrm{Coker}(\varphi_{\mathbb{Q}_2,S} \bmod 2) \simeq [2,2,2]$. Hence, by the assumption that $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$, at least one of a_j is even. Then $a_{j_0} \equiv 0 \pmod 4$ for some j_0. Recall that there are also odd a_j. Replacing the pair $(\mathfrak{l}, \mathfrak{L})$ by $(\mathfrak{l}^{\gamma^{j_0}}, \mathfrak{L}^{\gamma^{j_0}})$ if $j_0 \neq 0$, we may assume that $(a_0, a_1, a_2, a_3) \equiv (0, 1, 2, 1) \pmod 4$. Since

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} v_{\mathbb{Q}_2,S} \equiv \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \pmod 4,$$

we have $A_S(\mathbb{Q}_2)/4 \simeq \mathrm{Coker}(\varphi_{\mathbb{Q}_2,S} \bmod 4) \simeq [4, 4]$. Thus the proof of Lemma 5.3 is completed. $\square$

Lemma 5.4. *Assume that* $\ell \equiv 9 \pmod{16}$ *and* $\left(\frac{2}{\ell}\right)_4 = -1$. *Then*

$$\begin{aligned} &A_S(\mathbb{Q}_1) \simeq A_S(\mathbb{Q}_2) \simeq [4, 4] && \text{if } \left(\tfrac{\varepsilon_2}{\ell}\right)_4 = 1, \\ &A_S(\mathbb{Q}_1) \simeq [8, 2] \text{ and } A_S(\mathbb{Q}_2) \simeq [16, 2] && \text{if } \left(\tfrac{\varepsilon_2}{\ell}\right)_4 \neq 1. \end{aligned}$$

Proof. Since $\ell \equiv 9 \pmod{16}$, $O_{\mathbb{Q}_2}/\mathfrak{l} \simeq O_{\mathbb{Q}_2}/\mathfrak{l}^{\gamma} \simeq \mathbb{F}_{\ell^2}$ on which γ^2 acts as the Frobenius automorphism $x \mapsto x^{\ell}$ $(x \in \mathbb{F}_{\ell^2})$. We choose $g_{\mathfrak{l}O_{\mathbb{Q}_2}}$ and z_ℓ such that $z_\ell \equiv g_{\mathfrak{l}O_{\mathbb{Q}_2}}^{1+\ell} \pmod{\mathfrak{l}}$. Put $g_{\mathfrak{l}^{\gamma}O_{\mathbb{Q}_2}} = g_{\mathfrak{l}O_{\mathbb{Q}_2}}^{\gamma}$. Then $z_\ell \equiv g_{\mathfrak{l}^{\gamma}O_{\mathbb{Q}_2}}^{1+\ell} \pmod{\mathfrak{l}^{\gamma}}$, and we obtain the commutative diagram

$$\begin{array}{ccccccc} E(\mathbb{Q}_2) & \xrightarrow{\varphi_{\mathbb{Q}_2,S}} & [16_{\mathfrak{l}O_{\mathbb{Q}_2}}, 16_{\mathfrak{l}^{\gamma}O_{\mathbb{Q}_2}}] & \longrightarrow & A_S(\mathbb{Q}_2) & \longrightarrow & 0 \\ \uparrow\cup & & \uparrow\psi & & & & \\ E(\mathbb{Q}_1) & \xrightarrow{\varphi_{\mathbb{Q}_1,S}} & [8_{\mathfrak{l}}, 8_{\mathfrak{l}^{\gamma}}] & \longrightarrow & A_S(\mathbb{Q}_1) & \longrightarrow & 0 \end{array}$$

with exact rows, where $\psi(x_0, x_1) = ((\ell+1)x_0, (\ell+1)x_1) = (10x_0, 10x_1)$. In particular, $\mathrm{r}_2(A_S(\mathbb{Q}_1)) \leq \mathrm{r}_2(A_S(\mathbb{Q}_2)) \leq 2$. Since $\mathrm{r}_2(A_S(\mathbb{Q})) = 1$ and $G_S(\mathbb{Q}_\infty)$ is not cyclic by Proposition 5.1, we have $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$ by Theorem 4.3. Since $-1 \equiv z_\ell^{\frac{\ell-1}{2}} \pmod{\ell}$ and $\frac{\ell-1}{2} \equiv 4 \pmod 8$, we have $\varphi_{\mathbb{Q}_1,S}(-1) = (4, 4)$. Since $\mathrm{r}_2(A_S(\mathbb{Q}_1)) = 2$, $\mathrm{Im}\,\varphi_{\mathbb{Q}_1,S} \subset 2[8, 8]$ and hence $\varphi_{\mathbb{Q}_1,S}(\varepsilon_2) = (a_0, a_1)$ with some $a_0, a_1 \in 2\mathbb{Z}$. Then $\varphi_{\mathbb{Q}_1,S}(\varepsilon_2^{\gamma}) = (a_1, a_0)$. Since $\varepsilon_2^{1+\gamma} = -1$, we have $a_0 + a_1 \equiv 4 \pmod 8$. Note that $a_0 \equiv a_1 \equiv 0 \pmod 4$ if and only if $\left(\frac{\varepsilon_2}{\ell}\right)_4 = 1$. Then

$$\mathrm{Im}\,\varphi_{\mathbb{Q}_1,S} = \begin{cases} \langle\, (4, 0), (0, 4) \,\rangle & \text{if } \left(\frac{\varepsilon_2}{\ell}\right)_4 = 1, \\ \langle\, (2, 2) \,\rangle & \text{if } \left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1. \end{cases}$$

Thus we obtain the claim for $A_S(\mathbb{Q}_1)$. Since $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$ and $2\ell \equiv 2 \pmod{16}$, we have

$$v_{\mathbb{Q}_2,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_2,S}(\xi) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma}) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^2}) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^3}) \end{pmatrix} = \begin{pmatrix} b_0 & b_1 \\ b_1\ell & b_0 \\ b_0\ell & b_1\ell \\ b_1\ell^2 & b_0\ell \end{pmatrix} = \begin{pmatrix} b_0 & b_1 \\ b_1 & b_0 \\ b_0 & b_1 \\ b_1 & b_0 \end{pmatrix}$$

with some $b_0, b_1 \in 2\mathbb{Z}$. Since $\varepsilon_2 = \xi^{1+\gamma^2}$ and $\varphi_{\mathbb{Q}_2,S}|_{E(\mathbb{Q}_1)} = \psi \circ \varphi_{\mathbb{Q}_1,S}$, we have $(2b_0, 2b_1) = (10a_0, 10a_1) = (2a_0, 2a_1) \in [16, 16]$, i.e., $(b_0, b_1) \equiv (a_0, a_1) \pmod{8[16, 16]}$. Recall that $a_0 \equiv 0 \pmod 4$ if and only if $\left(\frac{\varepsilon_2}{\ell}\right)_4 = 1$. Since $b_0 + b_1 \equiv a_0 + a_1 \equiv \pm 4 \pmod{16}$, we have

$$\mathrm{Im}\,\varphi_{\mathbb{Q}_2,S} = \langle\, (b_0, b_1), (4, 4) \,\rangle = \begin{cases} \langle\, (4, 0), (0, 4) \,\rangle & \text{if } \left(\frac{\varepsilon_2}{\ell}\right)_4 = 1, \\ \langle\, (2, 2) \,\rangle \text{ or } \langle\, (2, 10) \,\rangle & \text{if } \left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1. \end{cases}$$

This implies the claim for $A_S(\mathbb{Q}_2)$. Thus the proof of Lemma 5.4 is completed. $\square$

Lemma 5.5. *If* $\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$, $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$, *then* $G_S(\mathbb{Q}_1)$ *is nonabelian metacyclic.*

Proof. Since $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$, we have $A_\emptyset(k') \simeq \mathbb{Z}/4\mathbb{Z}$ and $N_{k'/\mathbb{Q}}(\varepsilon_{2\ell}) = -1$ by [30, Proposition 3.4(b)]. Then $A_\emptyset(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$. Applying Kuroda's formula (2.3) for $k_1/\mathbb{Q}$, we have

$$2 = |A_\emptyset(k_1)| = 4^{-1}Q(k_1/\mathbb{Q})|A_\emptyset(\mathbb{Q}_1)||A_\emptyset(k')||A_\emptyset(k)| = Q(k_1/\mathbb{Q}),$$

i.e., $|E(k_1)/\langle -1, \varepsilon_2, \varepsilon_\ell, \varepsilon_{2\ell} \rangle| = 2$. Let $\mathfrak{L}$ be the prime ideal of k_1 lying over $\mathfrak{l}$. Choosing $g_{\mathfrak{L}^{\gamma^i}} = g_{\mathfrak{l}^{\gamma^i}} = g_{\sqrt{\ell}O_k} = g_{\mathfrak{L}\cap k'} = z_\ell$, we obtain the commutative diagram

$$\begin{tikzcd}
E(\mathbb{Q}_1) \arrow[r, "\varphi_{\mathbb{Q}_1,S}"] \arrow[d, hook, "\cap"] & {[8_{\mathfrak{l}}, 8_{\mathfrak{l}^\gamma}]} \arrow[r] \arrow[d, equal] & A_S(\mathbb{Q}_1) \arrow[r] & 0 & \\
E(k_1) \arrow[r, "\varphi_{k_1,S}"] & {[8_{\mathfrak{L}}, 8_{\mathfrak{L}^\gamma}]} \arrow[r] & A_S(k_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
E(k) \arrow[r, "\varphi_{k,S}"] \arrow[u, hook, "\cup"'] & \mathbb{Z}/8\mathbb{Z} \arrow[r] \arrow[u, "\psi"] & A_S(k) \arrow[r] & 0 & \\
E(k') \arrow[r, "\varphi_{k',S}"] \arrow[uu, bend left, hook, "\cup"] & \mathbb{Z}/8\mathbb{Z} \arrow[r] \arrow[uu, bend right, "\psi"'] & A_S(k') \arrow[r] & \mathbb{Z}/4\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\psi(x) = (x, x)$. In the proof of Lemma 5.4, we have seen that $\varphi_{k_1,S}(E(\mathbb{Q}_1)) = \operatorname{Im}\varphi_{\mathbb{Q}_1,S} = \langle (2,2) \rangle$ when $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$. Since $A_S(\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}_S^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, we have $A_S(k) \simeq \mathbb{Z}/2\mathbb{Z}$ and hence $\varphi_{k_1,S}(E(k)) = \psi(\operatorname{Im}\varphi_{k,S})$ $= \psi(2\mathbb{Z}/8\mathbb{Z}) = \langle (2,2) \rangle$. Since $k' \subset (\mathbb{Q}_S^{\mathrm{ab}})_1 \subset (k')_S^{\mathrm{ab}}$ and $(\mathbb{Q}_S^{\mathrm{ab}})_1/k'$ is not unramified, we have $A_S(k') \not\simeq A_\emptyset(k')$; i.e., $\varphi_{k',S}$ is not surjective. Hence $\varphi_{k_1,S}(E(k')) \subset \psi(2\mathbb{Z}/8\mathbb{Z}) = \langle (2,2) \rangle$. Then $\varphi_{k_1,S}$ induces the surjective homomorphism

$$\mathbb{Z}/2\mathbb{Z} \simeq E(k_1)/\langle -1, \varepsilon_2, \varepsilon_\ell, \varepsilon_{2\ell} \rangle \to \operatorname{Im}\varphi_{k_1,S}/\langle (2,2) \rangle.$$

This implies that $|\operatorname{Im}\varphi_{k_1,S}| \leq 8$, i.e., $|\operatorname{Coker}\varphi_{k_1,S}| \geq 8$. Since $A_S(\mathbb{Q}_1) \simeq [8,2]$ by Lemma 5.4, we have $|A_S(k_1)| = 2|\operatorname{Coker}\varphi_{k_1,S}| \geq 16 = |A_S(\mathbb{Q}_1)|$. This implies that $G_S(\mathbb{Q}_1)$ is nonabelian. Put $G = G_S(\mathbb{Q}_1)$ and $H = G_S(K)$, where $K = (\mathbb{Q}_1)_{\{\mathfrak{l}\}}$. Since $\operatorname{Im}\varphi_{\mathbb{Q}_1,\{\mathfrak{l}\}} = 2\mathbb{Z}/8\mathbb{Z}$, we have $|A_{\{\mathfrak{l}\}}(\mathbb{Q}_1)| = 2$ and hence $K/\mathbb{Q}_1$ is a quadratic extension such that $A_{\{\mathfrak{l}\}}(K) \simeq 0$. Recall that $A_\emptyset(k') \simeq \mathbb{Z}/4\mathbb{Z}$ and $N_{k'/\mathbb{Q}}(\varepsilon_{2\ell}) = -1$. Then $1 \neq [\mathfrak{L} \cap k'] \in A_\emptyset(k') \simeq A_{\{\infty\}}(k')$ and $[\mathfrak{L} \cap k']^2 = 1$. Hence $1 \neq [\mathfrak{L}^\gamma] \in A_\emptyset(k_1)$; i.e., $\mathfrak{L}^\gamma$ is inert in $(k_1)_\emptyset = k_1K$. This implies that $\mathfrak{l}^\gamma$ is inert in $K/\mathbb{Q}_1$. Since $A_{\{\mathfrak{l}\}}(K) \simeq 0$, K_S^{ab}/K is totally ramified at $\mathfrak{l}^\gamma O_K$. Therefore $\mathrm{r}_2(H^{\mathrm{ab}}) = \mathrm{r}_2(A_S(K)) = 1$; i.e., G has a cyclic maximal subgroup H. Hence G is metacyclic. Thus the proof of Lemma 5.5 is completed. $\square$

Now we complete the proof of Theorem 5.2. If $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$, we have $S_{\mathbb{Q}_n} = \{\mathfrak{l}O_{\mathbb{Q}_n}, \mathfrak{l}^\gamma O_{\mathbb{Q}_n}\}$ and $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for any $n \geq 1$ by Lemma 5.4 and Theorem 4.3. Then, since $(\mathbb{Q}_n)_{\{\mathfrak{l}\}}^{\mathrm{elem}}/\mathbb{Q}_n$ is a quadratic extension by Theorem 3.1(1) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$, $\mathbb{Q}_S^{\mathrm{ab}}(\mathbb{Q}_n)_{\{\mathfrak{l}\}}^{\mathrm{elem}}/k_n$ is a $[2,2]$-extension. This implies that $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_n)_S^{\mathrm{ab}}/k_n)) = 2$ for any $n \geq 1$. Now we assume one of the two conditions of Theorem 5.2. Suppose $n \geq 2$. Then

$$\begin{aligned}
&A_S(\mathbb{Q}_n) \simeq [4,4] \text{ and } |A_\emptyset(k_n)| = 2 && \text{if } \left(\tfrac{\varepsilon_2}{\ell}\right)_4 = 1 \text{ and } |A_\emptyset(k_2)| = 2,\\
&A_S(\mathbb{Q}_n)/4 \simeq [2,4] \text{ and } |A_\emptyset(k_n)| \geq 4 && \text{if } \left(\tfrac{\varepsilon_2}{\ell}\right)_4 \neq 1 \text{ and } |A_\emptyset(k_2)| \geq 4
\end{aligned}$$

by Lemma 5.4 and Theorem 4.3. Hence $G_S(\mathbb{Q}_n)$ is metacyclic by Theorem 3.1(2), (3) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$. Therefore $G_S(\mathbb{Q}_\infty) \simeq \varprojlim G_S(\mathbb{Q}_n)$ is prometacyclic. Thus the if-part is completed.

Conversely, we assume that $G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic. Then $\ell \equiv 1 \pmod 8$, $\left(\frac{2}{\ell}\right)_4 = (-1)^{\frac{\ell-1}{8}}$ and $G_\emptyset(k_\infty)^{\mathrm{ab}} \not\simeq 0$ by Proposition 5.1. Theorem 4.3 implies that $|A_\emptyset(k_n)| \geq 2$ and $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$. We apply Theorem 3.1 for $(k_2/\mathbb{Q}_2, S_{\mathbb{Q}_2}, \emptyset)$. Then $\mathrm{r}_2(A_\emptyset(k_2)) = 1$ by (3.1). Since $G_S(\mathbb{Q}_2)$ is metacyclic, $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 1$ or $|A_\emptyset(k_2)| = 2$ by Theorem 3.1(2). Hence $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$ by Lemma 5.3. Then we have seen that $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_2)_S^{\mathrm{ab}}/k_2)) = 2$. Since $(\mathbb{Q}_2)_{\{\mathfrak{l}\}}^{\mathrm{elem}}/\mathbb{Q}_1$ is a $[2,2]$-extension and $\mathfrak{l}^\gamma$ is inert in $\mathbb{Q}_2/\mathbb{Q}_1$, $\mathfrak{l}^\gamma O_{\mathbb{Q}_2}$ splits in $(\mathbb{Q}_2)_{\{\mathfrak{l}\}}^{\mathrm{elem}}/\mathbb{Q}_2$; i.e., the condition (4c) of Theorem 3.1 is satisfied. Note that $|O_{\mathbb{Q}_2}/\mathfrak{l}| = |O_{\mathbb{Q}_2}/\mathfrak{l}^\gamma| = \ell^2 \not\equiv 1 \pmod{32}$. If $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 1$, we have $A_S(\mathbb{Q}_2) \simeq [2,16]$ and $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$ by Lemma 5.4, and $G_S(\mathbb{Q}_2)$ is nonabelian by Lemma 5.5. Then the conditions (4a) and (4b) are also satisfied. Moreover if $|A_\emptyset(k_2)| = 2$ is also satisfied, $G_S(\mathbb{Q}_2)$ is not metacyclic by Theorem 3.1(4). This is a contradiction. Therefore $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 1$ and $|A_\emptyset(k_2)| = 2$ do not occur simultaneously; i.e., we have either $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 1$ and $|A_\emptyset(k_2)| \geq 4$ or $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 2$ and $|A_\emptyset(k_2)| = 2$. Then Lemma 5.4 completes the only-if part. Thus the proof of Theorem 5.2 is completed. □

Remark 5.6. Assume that $\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$ and $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$. Then $A_S(\mathbb{Q}_1) \simeq [2,8]$ by Lemma 5.4, and $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_1)_S^{\mathrm{ab}}/k_1)) = 2$. Moreover, $|A_\emptyset(k_1)| = 2$ (cf. the proof of Lemma 5.5). Since $|O_{\mathbb{Q}_1}/\mathfrak{l}| = |O_{\mathbb{Q}_1}/\mathfrak{l}^\gamma| = \ell \not\equiv 1 \pmod{16}$ and $G_S(\mathbb{Q}_1)$ is nonabelian metacyclic by Lemma 5.5, the triple $(k_1/\mathbb{Q}_1, S_{\mathbb{Q}_1}, \emptyset)$ satisfies the assumptions of Theorem 3.1(4) except (4c).

6. The case $S = \{\ell, q\}$

This section treats the case where $S = \{\ell, q\}$ consists of two primes $\ell \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. First, we prepare the following lemma.

Lemma 6.1. *Put $S = \{\ell, q\}$ with prime numbers $\ell \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Assume that $\left(\frac{2}{\ell}\right)_4\left(\frac{\ell}{2}\right)_4 = -1$ if $\ell \equiv 1 \pmod 8$. Put $v = v_2(\frac{\ell-1}{4}) \geq 0$ and $w = v_2(\frac{q+1}{4}) \geq 0$. Then $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = \min\{2^v, 2^w + 1\}$ for all $n \geq \max\{v, w\}$.*

Proof. The decomposition field of ℓ (resp. q) in $\mathbb{Q}_\infty/\mathbb{Q}$ is $\mathbb{Q}_v$ (resp. $\mathbb{Q}_w$). By Proposition 5.1, $A_{\{\ell\}}(\mathbb{Q}_n)$ is cyclic for all n. Suppose that $n \geq \max\{v, w\}$. Since $(O_{\mathbb{Q}_n}/\ell)^\times \otimes \mathbb{Z}_2$ and $(O_{\mathbb{Q}_n}/q)^\times \otimes \mathbb{Z}_2$ are cyclic Λ-modules, we have $(O_{\mathbb{Q}_n}/\ell)^\times \otimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2[[T]]/T^{2^v}$ and $(O_{\mathbb{Q}_n}/q)^\times \otimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{F}_2[[T]]/T^{2^w}$ as $\mathbb{F}_2[[T]]$-modules. Hence we obtain the commutative diagram

$$\begin{tikzcd}
E(\mathbb{Q}_n) \otimes \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, equal] & \mathbb{F}_2[[T]]/T^{2^v} \arrow[r] & A_{\{\ell\}}(\mathbb{Q}_n)/2 \arrow[r] & 0 \\
E(\mathbb{Q}_n) \otimes \mathbb{Z}/2\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, equal] & \mathbb{F}_2[[T]]/T^{2^v} \oplus \mathbb{F}_2[[T]]/T^{2^w} \arrow[r] \arrow[u, "(a,b)\mapsto a"'] \arrow[d, "(a,b)\mapsto b"] & A_S(\mathbb{Q}_n)/2 \arrow[r] & 0 \\
E(\mathbb{Q}_n) \otimes \mathbb{Z}/2\mathbb{Z} \arrow[r] & \mathbb{F}_2[[T]]/T^{2^w} \arrow[r] & A_{\{q\}}(\mathbb{Q}_n)/2 \arrow[r] & 0
\end{tikzcd}$$

of $\mathbb{F}_2[[T]]$-modules with exact rows. Since $E(\mathbb{Q}_n) \otimes \mathbb{Z}_2$ is a cyclic Λ-module, $\mathrm{Im}\,\varphi = \mathbb{F}_2[[T]](f \bmod T^{2^v}, g \bmod T^{2^w})$ with some $f, g \in \mathbb{F}_2[[T]]$. Since $\mathbb{F}_2[[T]]/(f, T^{2^v}) \simeq A_{\{\ell\}}(\mathbb{Q}_n)/2 \simeq \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{F}_2[[T]]/(g, T^{2^w}) \simeq A_{\{q\}}(\mathbb{Q}_n)/2 \simeq 0$ (cf. Corollary 4.2), we have $f \equiv T \pmod{T^2}$ and $g \equiv 1 \pmod{T}$. Hence $\operatorname{Im}\varphi \simeq \mathbb{F}_2[[T]]/T^{\max\{2^v-1,2^w\}}$ as $\mathbb{F}_2[[T]]$-modules. Therefore $A_S(\mathbb{Q}_n)/2 \simeq \operatorname{Coker}\varphi \simeq \mathbb{F}_2^{\min\{2^v,2^w+1\}}$ as $\mathbb{F}_2$-vector spaces. Thus the proof of Lemma 6.1 is completed. □

The following proposition determines the case where $G_{\{\ell,q\}}(\mathbb{Q}_\infty)$ is procyclic.

Proposition 6.2. *Put $S = \{\ell, q\}$ with prime numbers $\ell \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Then the following three conditions are equivalent:*

(1) *$G_S(\mathbb{Q}_\infty)$ is procyclic.*
(2) *$G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}/4\mathbb{Z}$.*
(3) *$\ell \equiv 5 \pmod 8$.*

Proof. Suppose that $G_S(\mathbb{Q}_\infty)$ is procyclic. Then $G_{\{\ell\}}(\mathbb{Q}_\infty)$ is also procyclic, and hence $\ell \equiv 5 \pmod 8$ or $\ell \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell}\right)_4\left(\frac{\ell}{2}\right)_4 = -1$ by Proposition 5.1. Since $\mathrm{r}_2(A_S(\mathbb{Q}_n)) \geq 2$ in the latter case by Lemma 6.1, we have $\ell \equiv 5 \pmod 8$. Therefore (1) implies (3). Suppose that $\ell \equiv 5 \pmod 8$. Then $k = \mathbb{Q}_S^{\mathrm{ab}}$ is a cyclic quartic extension of $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{\ell}) \subset k$. Since 2 is inert in $k = \mathbb{Q}_S$ and $A_S(k) \simeq 0$, $G_S(k_\infty)$ is trivial by Proposition 4.1. This implies that $k_\infty = (\mathbb{Q}_\infty)_S$, and hence $G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}/4\mathbb{Z}$. Thus the proof of Proposition 6.2 is completed. □

We prove the following theorem which determines the case where $G_{\{\ell,q\}}(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic.

Theorem 6.3. *Put $S = \{\ell, q\}$ with prime numbers $\ell \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is (nonprocyclic) prometacyclic if and only if one of the following two conditions holds:*

(1) *$\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = 1$, $q \equiv 7 \pmod 8$ and $\left(\frac{q}{\ell}\right) = -1$.*
(2) *$\ell \equiv 1 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$, $q \equiv 3 \pmod 8$ and $\left(\frac{q}{\ell}\right) = 1$.*

Proof. Put $k = \mathbb{Q}_S^{\mathrm{elem}} = \mathbb{Q}(\sqrt{\ell})$ and $k' = \mathbb{Q}(\sqrt{2\ell})$. Let $\mathfrak{l}$ be a prime of $\mathbb{Q}_1$ lying over ℓ. In the following, z_ℓ (resp. z_q) denotes a primitive element modulo ℓ (resp. q). First, we consider the case where $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$.

Lemma 6.4. *If $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$, then $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = \mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$, and $|A_{\{q\}}(k_2)| \geq 4$.*

Proof. Suppose that $n \geq 1$. We have $\mathrm{r}_2(A_S(\mathbb{Q}_n)) \geq \mathrm{r}_2(A_{\{\ell\}}(\mathbb{Q}_1)) = 2$ by Lemma 5.4. Let $I_{\mathfrak{l}}$ (resp. $I_{\mathfrak{l}^\gamma}$) be the inertia group of the prime $\mathfrak{l}O_{\mathbb{Q}_n}$ (resp. $\mathfrak{l}^\gamma O_{\mathbb{Q}_n}$) of $\mathbb{Q}_n$ in $G_S(\mathbb{Q}_n)^{\mathrm{ab}}$. Since $I_{\mathfrak{l}}$ and $I_{\mathfrak{l}^\gamma}$ are cyclic and $G_S(\mathbb{Q}_n)^{\mathrm{ab}}/I_{\mathfrak{l}}I_{\mathfrak{l}^\gamma} \simeq A_{\{q\}}(\mathbb{Q}_n) \simeq 0$ (cf. Corollary 4.2), we have $\mathrm{r}_4(A_S(\mathbb{Q}_n)) \leq \mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$. Since $\mathrm{r}_4(A_S(\mathbb{Q}_n)) \geq \mathrm{r}_4(A_{\{\ell\}}(\mathbb{Q}_1))$, Lemma 5.4 yields that $\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$ if $\left(\frac{\varepsilon_2}{\ell}\right)_4 = 1$. Suppose that $\left(\frac{\varepsilon_2}{\ell}\right)_4 \neq 1$. We choose $g_{\mathfrak{l}} = g_{\mathfrak{l}^\gamma} = z_\ell$. If $q \equiv 3 \pmod 8$, then $S_{\mathbb{Q}_1} = \{\mathfrak{l}, \mathfrak{l}^\gamma, qO_{\mathbb{Q}_1}\}$, and we fix $g_{qO_{\mathbb{Q}_1}}$. If $q \equiv 7 \pmod 8$, then $S_{\mathbb{Q}_1} = \{\mathfrak{l}, \mathfrak{l}^\gamma, \mathfrak{q}, \mathfrak{q}^\gamma\}$, and we choose $g_{\mathfrak{q}} = g_{\mathfrak{q}^\gamma} = z_q$, where $\mathfrak{q}$ is a prime of $\mathbb{Q}_1$ lying over q. Then we have an exact sequence

$$E(\mathbb{Q}_1) \xrightarrow{\varphi_{\mathbb{Q}_1,S}} [8_{\mathfrak{l}}, 8_{\mathfrak{l}^\gamma}, 8_{qO_{\mathbb{Q}_1}}] \to A_S(\mathbb{Q}_1) \to 0 \quad \text{if } q \equiv 3 \pmod 8,$$

$$E(\mathbb{Q}_1) \xrightarrow{\varphi_{\mathbb{Q}_1,S}} [8_{\mathfrak{l}}, 8_{\mathfrak{l}^\gamma}, 2_{\mathfrak{q}}, 2_{\mathfrak{q}^\gamma}] \to A_S(\mathbb{Q}_1) \to 0 \quad \text{if } q \equiv 7 \pmod 8.$$

Since $\varphi_{\mathbb{Q}_1,\{\ell\}}(\varepsilon_2) = (2,2)$ or $(6,6) \in [8,8]$ (cf. the proof of Lemma 5.4), we have

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2^{\pm 1}) \end{pmatrix} = \begin{pmatrix} 4 & 4 & 4 \\ 2 & 2 & a \end{pmatrix} \text{ or } \begin{pmatrix} 4 & 4 & 1 & 1 \\ 2 & 2 & a_0 & a_1 \end{pmatrix}$$

with some $a, a_0, a_1 \in \mathbb{Z}$ according to $q \equiv 3$ or $7 \pmod 8$. Since $A_{\{q\}}(\mathbb{Q}_1) \simeq 0$, $\varphi_{\mathbb{Q}_1,\{q\}}$ is surjective. Hence a is odd when $q \equiv 3 \pmod 8$, and $(a_0, a_1) = (1, 0)$ or $(0, 1)$ when $q \equiv 7 \pmod 8$. By an easy calculation, we have $A_S(\mathbb{Q}_1) \simeq [8, 4]$. Then $\mathrm{r}_4(A_S(\mathbb{Q}_n)) \geq \mathrm{r}_4(A_S(\mathbb{Q}_1)) = 2$, and hence $\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$. Therefore $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = \mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$.

Put $\Sigma = \{q\}$. We prove the inequality $|A_\Sigma(k_2)| \geq 4$. By Proposition 5.1 and Theorem 4.3, $A_\emptyset(k_n) \not\simeq 0$ for all $n \geq 1$. If $|A_\emptyset(k_2)| \geq 4$, then $|A_\Sigma(k_2)| \geq |A_\emptyset(k_2)| \geq 4$. In the following, we assume that $A_\emptyset(k_2) \simeq \mathbb{Z}/2\mathbb{Z}$. Then $A_\emptyset(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$ and hence $A_\emptyset(k_n) \simeq \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$ by Theorem 4.3. Let M be a cyclic quartic extension of $\mathbb{Q}$ contained in k_2 different from $\mathbb{Q}_2$, and let $\mathfrak{L}$ be the unique prime of k_2 lying over $\mathfrak{l}$. Then $M/\mathbb{Q}_1$ is a quadratic extension ramified at $\mathfrak{l}$ and $\mathfrak{l}^\gamma$, and $\mathfrak{L} \cap M$ and $\mathfrak{L}^\gamma \cap M$ are inert in the unramified quadratic extension k_2/M. By [20, Proposition 3.6], we have $A_\emptyset(M) \simeq [2, 2]$. Then $M_\emptyset^{\mathrm{ab}} = (k_2)_\emptyset^{\mathrm{ab}}$ is a $[2, 2]$-extension of M, and hence both $\mathfrak{L}$ and $\mathfrak{L}^\gamma$ split in $(k_2)_\emptyset^{\mathrm{ab}}/k_2$; i.e., $[\mathfrak{L}] = [\mathfrak{L}^\gamma] = 1$ in $A_\emptyset(k_2)$. Moreover, Kuroda's formula (2.2)

$$2 = |A_\emptyset(k_2)| = 2^{-3} Q(k_2/\mathbb{Q}_1)|A_\emptyset(\mathbb{Q}_2)||A_\emptyset(M)||A_\emptyset(k_1)||A_\emptyset(\mathbb{Q}_1)|^{-2} = Q(k_2/\mathbb{Q}_1)$$

for $k_2/\mathbb{Q}_1$ yields that

$$E(k_2)/E(\mathbb{Q}_2)E(M)E(k_1) = \langle \eta E(\mathbb{Q}_2)E(M)E(k_1)\rangle \simeq \mathbb{Z}/2\mathbb{Z}$$

with some $\eta \in E(k_2)$. Let σ be a generator of $\mathrm{Gal}(k_2/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z}$. We regard γ as a generator of $\mathrm{Gal}(k_2/k) \simeq \mathbb{Z}/4\mathbb{Z}$. Note that $\varepsilon_2^{1+\gamma} = -1$ and $\varepsilon_\ell^{1+\sigma} = -1$. Moreover, we have $|A_\emptyset(k')| = 4$ and $\varepsilon_{2\ell}^{1+\gamma} = \varepsilon_{2\ell}^{1+\sigma} = -1$ by [30, Proposition 3.4 (b)]. Then Kuroda's formula (2.3)

$$2 = |A_\emptyset(k_1)| = 4^{-1} Q(k_1/\mathbb{Q})|A_\emptyset(\mathbb{Q}_1)||A_\emptyset(k)||A_\emptyset(k')| = Q(k_1/\mathbb{Q})$$

for $k_1/\mathbb{Q}$ yields that $E(k_1) = \langle -1, \varepsilon_2, \varepsilon_\ell, \sqrt{\varepsilon_2\varepsilon_\ell\varepsilon_{2\ell}}\rangle$. Since $(\varepsilon_2\varepsilon_\ell\varepsilon_{2\ell})^{1+\sigma} = \varepsilon_2^2$ and $\varepsilon_\ell^{1+\sigma} = -1$, we have $E(k_1)^{1+\sigma} = E(\mathbb{Q}_1)$. By the genus formula (2.1)

$$1 = |\langle [\mathfrak{L}], [\mathfrak{L}^\gamma]\rangle| = \frac{|A_\emptyset(\mathbb{Q}_2)|2^2}{2|E(\mathbb{Q}_2)/E(k_2)^{1+\sigma}|}$$

for $k_2/\mathbb{Q}_2$, we have $E(\mathbb{Q}_2)/E(k_2)^{1+\sigma} \simeq \mathbb{Z}/2\mathbb{Z}$. Since

$$E(\mathbb{Q}_2)/E(\mathbb{Q}_2)^2E(\mathbb{Q}_1) = \langle \xi E(\mathbb{Q}_2)^2E(\mathbb{Q}_1), \xi^\gamma E(\mathbb{Q}_2)^2E(\mathbb{Q}_1)\rangle \simeq [2, 2],$$

we obtain the exact sequence

$$0 \to E(k_2)/E(\mathbb{Q}_2)E(M)E(k_1) \xrightarrow{1+\sigma} E(\mathbb{Q}_2)/E(\mathbb{Q}_2)^2E(\mathbb{Q}_1) \to \mathbb{Z}/2\mathbb{Z} \to 0$$

of Galois modules. Note that $(E(\mathbb{Q}_2)/E(\mathbb{Q}_2)^2E(\mathbb{Q}_1))^\Gamma = \langle \xi^{1+\gamma}E(\mathbb{Q}_2)^2E(\mathbb{Q}_1)\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Since $\eta^\gamma \equiv \eta \pmod{E(\mathbb{Q}_2)E(M)E(k_1)}$, we have $(\eta^{1+\sigma})^\gamma \equiv \eta^{1+\sigma} \pmod{E(\mathbb{Q}_2)^2E(\mathbb{Q}_1)}$. Hence

$$\eta^{1+\sigma} \equiv \xi^{1+\gamma} \mod E(\mathbb{Q}_2)^2E(\mathbb{Q}_1). \tag{6.1}$$

Let $\mathfrak{Q}$ be a prime of k_2 lying over q.

Suppose that $q \equiv 3 \pmod 8$. Then $O_{\mathbb{Q}_2}/q \simeq \mathbb{F}_{q^4}$, and the prime $qO_{\mathbb{Q}_1}$ splits in $k_1/\mathbb{Q}_1$. We choose $g_{qO_{\mathbb{Q}_2}} = g_\mathfrak{Q} = g_{\mathfrak{Q}^\sigma}$ and $g_{qO_{\mathbb{Q}_1}} = g_{\mathfrak{Q}\cap k_1} = g_{\mathfrak{Q}^\sigma \cap k_1}$ such that $g_{qO_{\mathbb{Q}_2}}^{1+q^2} \equiv g_{qO_{\mathbb{Q}_1}} \pmod q$. Since $O_M/q \simeq O_{k_2}/\mathfrak{Q} \simeq O_{k_2}/\mathfrak{Q}^\sigma$, we can choose g_{qO_M} such that $g_{qO_M} \equiv g_\mathfrak{Q} \pmod{\mathfrak{Q}}$. Since $\sigma|_M$ acts on O_M/q as the generator of

$\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$, $g_{qO_M}^{\sigma} \equiv g_{qO_M}^{q^2} \pmod{q}$ and hence $g_{qO_M} \equiv g_{\mathfrak{Q}^{\sigma}}^{q^2} \pmod{\mathfrak{Q}^{\sigma}}$. Then we obtain the commutative diagram

$$\begin{tikzcd}
E(M) \arrow[r, "\varphi_{M,\Sigma}"] \arrow[dd, bend right=60, "\cap"'] & \mathbb{Z}/16\mathbb{Z} \arrow[r] \arrow[dd, bend left=60, "\psi_M"] & A_{\Sigma}(M) \arrow[r] & A_{\emptyset}(M) \arrow[r] & 0 \\
E(\mathbb{Q}_2) \arrow[r, "\varphi_{\mathbb{Q}_2,\Sigma}"] \arrow[d, "\cap"] & \mathbb{Z}/16\mathbb{Z} \arrow[r] \arrow[d, "\psi_{\mathbb{Q}_2}"] & 0 & & \\
E(k_2) \arrow[r, "\varphi_{k_2,\Sigma}"] & {[16_{\mathfrak{Q}}, 16_{\mathfrak{Q}^{\sigma}}]} \arrow[r] & A_{\Sigma}(k_2) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
E(k_1) \arrow[r, "\varphi_{k_1,\Sigma}"] \arrow[u, "\cup"] & {[8_{\mathfrak{Q}\cap k_1}, 8_{\mathfrak{Q}^{\sigma}\cap k_1}]} \arrow[r] \arrow[u, "\psi_{k_1}"] & A_{\Sigma}(k_1) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\psi_{\mathbb{Q}_2}(x) = (x, x) \in \langle(1,1)\rangle$, $\psi_{k_1}(x_0, x_1) = (x_0(1+q^2), x_1(1+q^2)) \in 2[16,16]$ and $\psi_M(y) = (y, q^2 y) \in \langle(2,0),(1,1)\rangle$. Since $\varphi_{\mathbb{Q}_2,\Sigma}$ is surjective, $\varphi_{\mathbb{Q}_2,\Sigma}(\xi) = (u)$ with some odd u. Since γ acts on $O_{\mathbb{Q}_2}/q$ as a generator of $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_q)$, we have $\xi^{\gamma} \equiv \xi^{q^i} \pmod{q}$ where $i \in \{1,3\}$. Since $\varepsilon_2 = \xi^{1+\gamma^2}$, we have $\varphi_{\mathbb{Q}_2,\Sigma}(\varepsilon_2) = (u(1+q^{2i})) \in 2\mathbb{Z}/16\mathbb{Z}$. In particular, $\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)^2 E(\mathbb{Q}_1)) \subset \langle(2,2)\rangle$. Put $(a_0, a_1) = \varphi_{k_2,\Sigma}(\eta)$. Then $\varphi_{k_2,\Sigma}(\eta^{\sigma}) = (a_1, a_0)$. The congruence (6.1) yields that

$$\begin{aligned}
(a_0 + a_1, a_0 + a_1) = \varphi_{k_2,\Sigma}(\eta^{1+\sigma}) &\equiv \varphi_{k_2,\Sigma}(\xi^{1+\gamma}) = (u(1+q^i), u(1+q^i)) \\
&\equiv (0,0) \mod \langle(2,2)\rangle.
\end{aligned}$$

Hence $a_0 \equiv a_1 \pmod{2}$, i.e., $(a_0, a_1) \in \langle(2,0),(1,1)\rangle$. Since $E(k_2)$ is generated by η and $E(\mathbb{Q}_2)E(M)E(k_1)$, we have $\mathrm{Im}\,\varphi_{k_2,\Sigma} \subset \langle(2,0),(1,1)\rangle$; i.e., $\varphi_{k_2,\Sigma}$ is not surjective. Therefore $|A_{\Sigma}(k_2)| \geq 4$ if $q \equiv 3 \pmod{8}$.

Suppose that $q \equiv 7 \pmod{8}$, and assume that $q \not\equiv 15 \pmod{16}$ or $\left(\frac{\ell}{q}\right) = -1$. Then q splits in $\mathbb{Q}_1$, and none of the primes lying over q splits completely in $k_2/\mathbb{Q}_1$. Let F be the decomposition field of q in $k_2/\mathbb{Q}$, and let F', F'' be the quadratic extensions of $\mathbb{Q}_1$ contained in k_2 and different from F. ($\{F, F', F''\} = \{\mathbb{Q}_2, M, k_1\}$ as a set.) Then $O_{F'}/(\mathfrak{Q} \cap F') \simeq O_{k_2}/\mathfrak{Q} \simeq O_{F''}/(\mathfrak{Q} \cap F'') \simeq \mathbb{F}_{q^2}$. Let τ be the generator of $\mathrm{Gal}(k_2/F')$. We choose $g_{\mathfrak{Q}\cap F'} = g_{\mathfrak{Q}} = g_{\mathfrak{Q}^{\tau}}$ and z_q such that $z_q \equiv g_{\mathfrak{Q}\cap F'}^{1+q} \pmod{\mathfrak{Q}^{1+\tau}}$. Then $g_{\mathfrak{Q}^{\gamma}\cap F'} = g_{\mathfrak{Q}^{\gamma}} = g_{\mathfrak{Q}^{\gamma\tau}} := g_{\mathfrak{Q}\cap F'}^{\gamma}$ satisfies $z_q \equiv g_{\mathfrak{Q}^{\gamma}\cap F'}^{1+q} \pmod{\mathfrak{Q}^{\gamma(1+\tau)}}$. On the other hand, we choose $g_{\mathfrak{Q}\cap F''}$ such that $g_{\mathfrak{Q}\cap F''} \equiv g_{\mathfrak{Q}} \pmod{\mathfrak{Q}}$. Then $g_{\mathfrak{Q}\cap F''}^{\tau} \equiv g_{\mathfrak{Q}^{\tau}} \pmod{\mathfrak{Q}^{\tau}}$. Moreover, $g_{\mathfrak{Q}^{\gamma}\cap F''} := g_{\mathfrak{Q}\cap F''}^{\gamma}$ satisfies $g_{\mathfrak{Q}^{\gamma}\cap F''} \equiv g_{\mathfrak{Q}^{\gamma}} \pmod{\mathfrak{Q}^{\gamma}}$. Since $\mathfrak{Q} \cap F'' = \mathfrak{Q}^{\tau} \cap F''$, τ acts on $O_{F''}/(\mathfrak{Q} \cap F'')$ as the Frobenius automorphism. Then $g_{\mathfrak{Q}\cap F''}^{\tau} \equiv g_{\mathfrak{Q}\cap F''}^{q} \pmod{\mathfrak{Q}^{1+\tau}}$, and hence $g_{\mathfrak{Q}\cap F''} \equiv g_{\mathfrak{Q}\cap F''}^{q^2} \equiv g_{\mathfrak{Q}\cap F''}^{\tau q} \equiv g_{\mathfrak{Q}^{\tau}}^{q} \pmod{\mathfrak{Q}^{\tau}}$. Then $g_{\mathfrak{Q}^{\gamma}\cap F''} \equiv g_{\mathfrak{Q}^{\gamma\tau}}^{q} \pmod{\mathfrak{Q}^{\gamma\tau}}$. Choosing z_q as the primitive elements of the residue fields $\mathbb{F}_q$ of O_F, we obtain the commutative diagram

$$\begin{tikzcd}
E(F'') \arrow[r, "\varphi_{F'',\Sigma}"] \arrow[dd, bend right=60, "\cap"'] & {[2^m_{\mathfrak{Q}\cap F''}, 2^m_{\mathfrak{Q}^{\gamma}\cap F''}]} \arrow[r] \arrow[dd, bend left=60, "\psi_2"] & A_{\Sigma}(F'') \arrow[r] & A_{\emptyset}(F'') \arrow[r] & 0 \\
E(F') \arrow[r, "\varphi_{F',\Sigma}"] \arrow[d, "\cap"] & {[2^m_{\mathfrak{Q}\cap F'}, 2^m_{\mathfrak{Q}^{\gamma}\cap F'}]} \arrow[r] \arrow[d, "\psi_1"] & A_{\Sigma}(F') \arrow[r] & A_{\emptyset}(F') \arrow[r] & 0 \\
E(k_2) \arrow[r, "\varphi_{k_2,\Sigma}"] & {[2^m_{\mathfrak{Q}}, 2^m_{\mathfrak{Q}^{\tau}}, 2^m_{\mathfrak{Q}^{\gamma}}, 2^m_{\mathfrak{Q}^{\gamma\tau}}]} \arrow[r] & A_{\Sigma}(k_2) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
E(F) \arrow[r, "\varphi_{F,\Sigma}"] \arrow[u, "\cup"] & {[2_{\mathfrak{Q}\cap F}, 2_{\mathfrak{Q}^{\tau}\cap F}, 2_{\mathfrak{Q}^{\gamma}\cap F}, 2_{\mathfrak{Q}^{\gamma\tau}\cap F}]} \arrow[r] \arrow[u, "\psi_0"] & A_{\Sigma}(F) \arrow[r] & A_{\emptyset}(F) \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $m = v_2(q^2-1) \geq 4$,

$$\psi_0(x_0, x_1, x_2, x_3) = (2^{m-1}x_0, 2^{m-1}x_1, 2^{m-1}x_2, 2^{m-1}x_3),$$

$\psi_1(x_0, x_1) = (x_0, x_0, x_1, x_1)$ and $\psi_2(x_0, x_1) = (x_0, qx_0, x_1, qx_1)$. Then $\sum_{i=0}^{2} \operatorname{Im}\psi_i$ is generated by $2^{m-1}[2^m, 2^m, 2^m, 2^m]$ and $(1,1,0,0), (0,0,1,1), (1,q,0,0), (0,0,1,q)$. Hence $[2^m, 2^m, 2^m, 2^m]/\sum_{i=0}^{2}\operatorname{Im}\psi_i \simeq [2,2]$. Since $\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) \subset \sum_{i=0}^{2}\operatorname{Im}\psi_i$ and $E(k_2)/E(\mathbb{Q}_2)E(M)E(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$, $\varphi_{k_2,\Sigma}$ is not surjective. Therefore $|A_\Sigma(k_2)| \geq 4$ if $q \not\equiv 15 \pmod{16}$ or $\left(\frac{\ell}{q}\right) = -1$.

Suppose that $q \equiv 15 \pmod{16}$ and $\left(\frac{\ell}{q}\right) = 1$. Then q splits completely in k_2. Choosing z_q as the primitive elements of the residue fields $\mathbb{F}_q$, we obtain a commutative diagram

$$\begin{array}{ccccccc}
E(k_2) & \xrightarrow{\varphi_{k_2,\Sigma}} & [2_{\mathfrak{Q}}, 2_{\mathfrak{Q}^\gamma}, 2_{\mathfrak{Q}^{\gamma^2}}, 2_{\mathfrak{Q}^{\gamma^3}}, 2_{\mathfrak{Q}^\sigma}, 2_{\mathfrak{Q}^{\gamma\sigma}}, 2_{\mathfrak{Q}^{\gamma^2\sigma}}, 2_{\mathfrak{Q}^{\gamma^3\sigma}}] & \longrightarrow & A_\Sigma(k_2) & \twoheadrightarrow & \mathbb{Z}/2\mathbb{Z} \\
\uparrow \cup & & \uparrow \psi_F & & & & \\
E(F) & \xrightarrow{\varphi_{F,\Sigma}} & [2_{\mathfrak{Q}\cap F}, 2_{\mathfrak{Q}^\gamma\cap F}, 2_{\mathfrak{Q}^\tau\cap F}, 2_{\mathfrak{Q}^{\gamma\tau}\cap F}] & \longrightarrow & A_\Sigma(F) & \twoheadrightarrow & A_\emptyset(F)
\end{array}$$

with exact rows, where

$$\psi_F(x_0, x_1, x_2, x_3) = \begin{cases} (x_0, x_1, x_0, x_1, x_2, x_3, x_2, x_3) \text{ and } \tau = \sigma & \text{if } F = k_1, \\ (x_0, x_1, x_2, x_3, x_0, x_1, x_2, x_3) \text{ and } \tau = \gamma^2 & \text{if } F = \mathbb{Q}_2, \\ (x_0, x_1, x_2, x_3, x_2, x_3, x_0, x_1) \text{ and } \tau = \gamma^2 & \text{if } F = M. \end{cases}$$

An easy calculation shows that $[2,2,2,2,2,2,2,2]/\sum_{F\in\{\mathbb{Q}_2,M,k_1\}}\operatorname{Im}\psi_F \simeq [2,2]$. This implies that $|A_\Sigma(k_2)| \geq 4$. Thus the proof of Lemma 6.4 is completed. □

As we will see later, Lemma 6.4 implies that $G_S(\mathbb{Q}_\infty)$ is not prometacyclic if $\left(\frac{2}{\ell}\right)_4 = (-1)^{\frac{\ell-1}{8}}$. In the following, we consider the case where $\left(\frac{2}{\ell}\right)_4 \neq (-1)^{\frac{\ell-1}{8}}$. If $G_S(\mathbb{Q}_\infty)$ is prometacyclic, then $\mathrm{r}_2(A_S(\mathbb{Q}_n)) \leq 2$ for all n. Hence, by Lemma 6.1, it suffices to consider the case where $v = 1$ or $w = 0$, i.e., $\ell \equiv 9 \pmod{16}$ or $q \equiv 3 \pmod 8$.

Lemma 6.5. *Assume that $\ell \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell}\right)_4 \neq (-1)^{\frac{\ell-1}{8}}$. If $q \equiv 3 \pmod 8$, then $\mathrm{r}_4(A_S(\mathbb{Q}_1)) = 2$ and*

$$\begin{array}{ll} |A_{\{q\}}(k_2)| = 2 & \text{if } \ell \equiv 1 \pmod{16} \text{ and } \left(\frac{q}{\ell}\right) = 1, \\ |A_{\{q\}}(k_2)| \geq 4 & \text{if } \ell \equiv 9 \pmod{16} \text{ or } \left(\frac{q}{\ell}\right) = -1. \end{array}$$

If $\ell \equiv 9 \pmod{16}$ and $q \equiv 7 \pmod 8$, then $A_S(\mathbb{Q}_2) \simeq [2,16]$ and

$$\begin{array}{ll} |A_{\{q\}}(k_2)| = 2 & \text{if } \left(\frac{q}{\ell}\right) = 1, \\ |A_{\{q\}}(k_2)| \geq 4 & \text{if } \left(\frac{q}{\ell}\right) = -1. \end{array}$$

Proof. First, we prepare some properties of units. By the assumption, $A_\emptyset(k_n) \simeq 0$ for all $n \geq 0$ (cf. Proposition 5.1). Let σ be a generator of $\operatorname{Gal}(k_2/\mathbb{Q}_2)$. We regard γ as a generator of $\operatorname{Gal}(k_2/k)$. Recall that $\varepsilon_2^{\gamma+1} = \varepsilon_\ell^{\sigma+1} = -1$. Since k_1/k' is unramified and $A_\emptyset(k_1) \simeq 0$, we have $k_1 = (k')_\emptyset^{\mathrm{ab}}$ and $A_\emptyset(k') \simeq \mathbb{Z}/2\mathbb{Z}$. Since $|A_{\{\infty\}}(k')| \geq 4$ (cf. [30]), we have $\varepsilon_{2\ell}^{\sigma+1} = 1$. Kuroda's formula (2.3)

$$1 = |A_\emptyset(k_1)| = 4^{-1}Q(k_1/\mathbb{Q})|A_\emptyset(\mathbb{Q}_1)||A_\emptyset(k)||A_\emptyset(k')| = 2^{-1}Q(k_1/\mathbb{Q})$$

for $k_1/\mathbb{Q}$ yields that $E(k_1) = \langle -1, \varepsilon_2, \varepsilon_\ell, \sqrt{\varepsilon_{2\ell}}\rangle$. An easy calculation shows that $\sqrt{\varepsilon_{2\ell}} = x\sqrt{2} + y\sqrt{\ell} \in O_{k_1}$ with some $x, y \in \mathbb{Q}$. Then $2x^2 - \ell y^2 = \sqrt{\varepsilon_{2\ell}}^{1+\sigma} = \pm 1$. If $2x^2 - \ell y^2 = 1$, then $2|x| + |y|\sqrt{2\ell} \in O_{k'}$ is totally positive and $(2|x| + |y|\sqrt{2\ell})O_{k'}$ is the prime lying over 2. If $2x^2-\ell y^2=-1$, then $\ell|y|+|x|\sqrt{2\ell}\in O_{k'}$ is totally positive and $(\ell|y|+|x|\sqrt{2\ell})O_{k'}$ is the prime lying over ℓ. By [30, Proposition 3.4(a)], we have

$$-\sqrt{\varepsilon_{2\ell}}^{1+\gamma}=\sqrt{\varepsilon_{2\ell}}^{1+\sigma}=(-1)^{\frac{\ell-1}{8}}, \tag{6.2}$$

where we note that $\sqrt{\varepsilon_{2\ell}}^{\gamma\sigma}=-\sqrt{\varepsilon_{2\ell}}$. Let M be a cyclic quartic extension of $\mathbb{Q}$ contained in k_2 different from $\mathbb{Q}_2$. Then $k_2=M_{\emptyset}^{\mathrm{ab}}$. Kuroda's formula (2.2)

$$1=|A_{\emptyset}(k_2)|=2^{-3}Q(k_2/\mathbb{Q}_1)|A_{\emptyset}(\mathbb{Q}_2)||A_{\emptyset}(M)||A_{\emptyset}(k_1)||A_{\emptyset}(\mathbb{Q}_1)|^{-2}=2^{-2}Q(k_2/\mathbb{Q}_1)$$

for $k_2/\mathbb{Q}_1$ yields that $|E(k_2)/E(\mathbb{Q}_2)E(M)E(k_1)|=4$. The genus formula (2.1)

$$1=|A_{\emptyset}(k_2)|\geq\frac{|A_{\emptyset}(k_1)|2^2}{2|E(k_1)/E(k_2)^{1+\gamma^2}|}$$

for k_2/k_1 yields the existence of an exact sequence

$$E(k_2)/E(\mathbb{Q}_2)E(M)E(k_1)\xrightarrow{1+\gamma^2}E(k_1)/E(\mathbb{Q}_1)E(k_1)^2\to\mathbb{Z}/2\mathbb{Z}\to 0.$$

Note that $E(\mathbb{Q}_1)E(k_1)^2=\langle -1,\varepsilon_2,\varepsilon_\ell^2,\varepsilon_{2\ell}\rangle=(E(\mathbb{Q}_2)E(M)E(k_1))^{1+\gamma^2}$ and

$$E(k_1)/E(\mathbb{Q}_1)E(k_1)^2=\langle\varepsilon_\ell E(\mathbb{Q}_1)E(k_1)^2,\sqrt{\varepsilon_{2\ell}}E(\mathbb{Q}_1)E(k_1)^2\rangle\simeq[2,2].$$

The genus formula (2.1)

$$1=|A_{\emptyset}(k_2)|\geq\frac{|A_{\emptyset}(k)|4^2}{4|E(k)/E(k_2)^{(1+\gamma^2)(1+\gamma)}|}$$

for k_2/k yields that $E(k_2)^{(1+\gamma^2)(1+\gamma)}=\langle -1,\varepsilon_\ell^4\rangle$. Since $\varepsilon_\ell^{1+\gamma}=\varepsilon_\ell^2$ and $(\sqrt{\varepsilon_{2\ell}}\varepsilon_\ell)^{1+\gamma}$ $=\pm\varepsilon_\ell^2$, we have ε_ℓ, $\sqrt{\varepsilon_{2\ell}}\varepsilon_\ell\notin E(k_2)^{1+\gamma^2}$, and hence $\sqrt{\varepsilon_{2\ell}}\in E(k_2)^{1+\gamma^2}$. Therefore

$$E(k_2)=\langle\eta_1,\eta_2\rangle E(\mathbb{Q}_2)E(M)E(k_1)$$

with some η_1, $\eta_2\in E(k_2)$ such that

$$\eta_1^{1+\gamma^2}\equiv\sqrt{\varepsilon_{2\ell}},\quad \eta_2^{1+\gamma^2}\equiv 1\pmod{E(\mathbb{Q}_1)E(k_1)^2}. \tag{6.3}$$

Put $\Sigma=\{q\}$, and put $e=v_2(q+1)\geq 2$. Let $\mathfrak{Q}$ be a prime of k_2 lying over q. If $\ell\equiv 9\pmod{16}$ or $q\equiv 3\pmod 8$, we have $\mathrm{r}_2(A_S(\mathbb{Q}_n))=2$ for all $n\geq 1$ by Lemma 6.1. Then $\mathrm{r}_2(A_\Sigma(k_n))=1$ for all $n\geq 1$ by (3.1) for the triple $(k_n/\mathbb{Q}_n,S_{\mathbb{Q}_n},\Sigma_{\mathbb{Q}_n})$. Since $\mathbb{Q}_S^{\mathrm{ab}}/\mathbb{Q}$ is a cyclic extension totally ramified at ℓ, we have $A_\Sigma(k)\simeq 0$, and hence γ acts on $A_\Sigma(k_1)$ as -1. Since $A_\Sigma(\mathbb{Q}_1)\simeq 0$, σ also acts on $A_\Sigma(k_1)$ as -1. Therefore $\sigma\gamma$ acts on $A_\Sigma(k_1)$ trivially. This implies that $(k')_\Sigma^{\mathrm{ab}}=(k_1)_\Sigma^{\mathrm{ab}}$. In particular, $|A_\Sigma(k')|=2|A_\Sigma(k_1)|\geq 4$. Recall the exact sequence

$$E(k')\xrightarrow{\Phi_{k',\Sigma}}(O_{k'}/q)^\times\otimes\mathbb{Z}_2\to A_\Sigma(k')\to\mathbb{Z}/2\mathbb{Z}\to 0.$$

Since $\Phi_{k',\Sigma}(-1)$ is nontrivial, $\Phi_{k',\Sigma}$ is not zero mapping. If $\left(\frac{2\ell}{q}\right)=1$, then $(O_{k'}/q)^\times\otimes\mathbb{Z}_2\simeq[2,2]$, and hence $|A_\Sigma(k')|=4$. This implies that $\operatorname{Im}\Phi_{k',\Sigma}=\langle\Phi_{k',\Sigma}(-1)\rangle$ if $\left(\frac{2\ell}{q}\right)=1$. If $\left(\frac{2\ell}{q}\right)=-1$, we choose $g_{qO_{k'}}$ which is also a primitive element of $O_{k_1}/(\mathfrak{Q}\cap k_1)\simeq O_{k'}/q\simeq\mathbb{F}_{q^2}$. Then $(O_{k'}/q)^\times\otimes\mathbb{Z}_2=\langle g_{qO_{k'}}\otimes 1\rangle\simeq\mathbb{Z}/2^{e+1}\mathbb{Z}$ and $\sqrt{\varepsilon_{2\ell}}\equiv g_{qO_{k'}}^t\pmod{\mathfrak{Q}\cap k_1}$ with some $t\in\mathbb{Z}$. If $\left(\frac{2}{q}\right)=-1$ and $\left(\frac{q}{\ell}\right)=1$, then $g_{qO_{k'}}^{(1+q)t}\equiv\sqrt{\varepsilon_{2\ell}}^{1+\gamma}\pmod{\mathfrak{Q}\cap k_1=\mathfrak{Q}^\gamma\cap k_1}$. If $\left(\frac{2}{q}\right)=1$ and $\left(\frac{q}{\ell}\right)=-1$, then

$g_{qO_{k'}}^{(1+q)t} \equiv \sqrt{\varepsilon_{2\ell}}^{1+\sigma} \pmod{\mathfrak{Q} \cap k_1 = \mathfrak{Q}^\sigma \cap k_1}$. By (6.2), the parity of t is determined as

$$(-1)^t = \left(\tfrac{2}{q}\right)(-1)^{\frac{\ell-1}{8}}. \tag{6.4}$$

Since $\varepsilon_{2\ell} \equiv g_{qO_{k'}}^{2t} \pmod{q}$ and $|A_\Sigma(k_1)| = |\mathrm{Coker}\,\varPhi_{k',\Sigma}|$, we have

$$\begin{aligned} &|A_\Sigma(k_1)| = 2 \quad \text{if } \left(\tfrac{2\ell}{q}\right) = 1 \text{ or } (-1)^{\frac{\ell-1}{8}} \neq \left(\tfrac{2}{q}\right), \\ &|A_\Sigma(k_1)| \geq 4 \quad \text{if } \left(\tfrac{2\ell}{q}\right) = -1 \text{ and } (-1)^{\frac{\ell-1}{8}} = \left(\tfrac{2}{q}\right). \end{aligned} \tag{6.5}$$

Suppose that $q \equiv 3 \pmod 8$. For $g_{qO_{\mathbb{Q}_1}}$ and $g_{\mathfrak{l}} = g_{\mathfrak{l}^\gamma} = z_\ell$, we obtain the exact sequence

$$E(\mathbb{Q}_1) \xrightarrow{\varphi_{\mathbb{Q}_1,S}} [2_{\mathfrak{l}}^m, 2_{\mathfrak{l}^\gamma}^m, 8_{qO_{\mathbb{Q}_1}}] \to A_S(\mathbb{Q}_1) \to 0$$

and

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2^{m-1} & 2^{m-1} & 4 \\ a_0 & a_1 & b \end{pmatrix},$$

with some $a_0, a_1, b \in \mathbb{Z}$, where $m = v_2(\ell-1) \geq 3$. Since $G_{\{\ell\}}(\mathbb{Q}_\infty)$ is cyclic by Proposition 5.1, $(\mathbb{Q}_1)_{\{\ell\}}^{\mathrm{elem}} = k_1$, and hence $A_{\{\mathfrak{l}\}}(\mathbb{Q}_1) \simeq A_{\{\mathfrak{l}^\gamma\}}(\mathbb{Q}_1) \simeq 0$. Recall that $A_\Sigma(\mathbb{Q}_1) \simeq 0$ (cf. Corollary 4.2). These imply that $\varphi_{\mathbb{Q}_1,\{\mathfrak{l}\}}$, $\varphi_{\mathbb{Q}_1,\{\mathfrak{l}^\gamma\}}$ and $\varphi_{\mathbb{Q}_1,\Sigma}$ are surjective; i.e., a_0, a_1 and b are odd. An easy calculation shows that $A_S(\mathbb{Q}_1) \simeq [2^m, 4]$. In particular, $\mathrm{r}_4(A_S(\mathbb{Q}_1)) = 2$. If $\left(\frac{q}{\ell}\right) = 1$ and $\ell \equiv 9 \pmod{16}$, we have the claim $|A_\Sigma(k_2)| \geq |A_\Sigma(k_1)| \geq 4$ by (6.5). Suppose that $\left(\frac{q}{\ell}\right) = -1$ or $\ell \equiv 1 \pmod{16}$. Then $|A_\Sigma(k_1)| = 2$ by (6.5). Note that $O_{\mathbb{Q}_2}/q \simeq \mathbb{F}_{q^4} \simeq O_M/q$ and that $qO_{\mathbb{Q}_1}$ splits in $k_1/\mathbb{Q}_1$. We choose $g_{qO_{\mathbb{Q}_1}} = g_{\mathfrak{Q}\cap k_1} = g_{\mathfrak{Q}^\sigma \cap k_1}$ and $g_{qO_{\mathbb{Q}_2}} = g_{\mathfrak{Q}} = g_{\mathfrak{Q}^\sigma}$ such that $g_{qO_{\mathbb{Q}_1}} \equiv g_{qO_{\mathbb{Q}_2}}^{1+q^2} \pmod{q}$. We also choose g_{qO_M} such that $g_{qO_M} \equiv g_{\mathfrak{Q}} \pmod{\mathfrak{Q}}$. Since $\mathfrak{Q}^{\sigma\gamma^2} = \mathfrak{Q}^\sigma$ and γ^2 acts on $O_{k_2}/\mathfrak{Q}^\sigma$ as a generator of $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$, we have $g_{qO_M} \equiv g_{\mathfrak{Q}}^{\sigma\gamma^2} \equiv g_{\mathfrak{Q}^\sigma}^{q^2} \pmod{\mathfrak{Q}^\sigma}$. Then we obtain the commutative diagram

$$\begin{tikzcd}
E(M) \arrow[r, "\varphi_{M,\Sigma}"] \arrow[dd, bend right=60, "\cap"'] & \mathbb{Z}/16\mathbb{Z} \arrow[r] \arrow[dd, bend left=60, "\psi_M"] & A_\Sigma(M) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \\
E(\mathbb{Q}_2) \arrow[r, "\varphi_{\mathbb{Q}_2,\Sigma}"] \arrow[d, "\cap"] & \mathbb{Z}/16\mathbb{Z} \arrow[r] \arrow[d, "\psi_{\mathbb{Q}_2}"] & 0 & & \\
E(k_2) \arrow[r, "\varphi_{k_2,\Sigma}"] & {[16_{\mathfrak{Q}}, 16_{\mathfrak{Q}^\sigma}]} \arrow[r] & A_\Sigma(k_2) \arrow[r] & 0 & \\
E(k_1) \arrow[r, "\varphi_{k_1,\Sigma}"] \arrow[u, "\cup"] & {[8_{\mathfrak{Q}\cap k_1}, 8_{\mathfrak{Q}^\sigma \cap k_1}]} \arrow[r] \arrow[u, "\psi_{k_1}"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 & \\
E(k') \arrow[r, "\varPhi_{k',\Sigma}"] \arrow[u, "\cup"] & (O_{k'}/q)^\times \otimes \mathbb{Z}_2 \arrow[u, "\varPsi"] & & &
\end{tikzcd}$$

with exact rows, where $\psi_{k_1}(x_0, x_1) = ((1+q^2)x_0, (1+q^2)x_1) = (10x_0, 10x_1)$, $\psi_{\mathbb{Q}_2}(x) = (x, x)$ and $\psi_M(y) = (y, q^2 y) \in \langle (1,1), (4,0) \rangle$. If $(x_0, x_1) = \varphi_{k_1,\Sigma}(\varepsilon)$ with some $\varepsilon \in E(k_1)$, then $(x_1, x_0) = \varphi_{k_1,\Sigma}(\varepsilon^\sigma)$. This implies that $\mathrm{Im}\,\varphi_{k_1,\Sigma} = \langle (1,1), (2,0) \rangle$, i.e., $\varphi_{k_2,\Sigma}(E(k_1)) = \langle (2,2), (4,0) \rangle$. Therefore

$$\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) = \langle (1,1), (4,0) \rangle. \tag{6.6}$$

If $\left(\frac{q}{\ell}\right) = -1$, we have $\varphi_{k_2,\Sigma}(\varepsilon_{2\ell}) \in \psi_{k_1}(\varPsi(\mathrm{Im}\,\varPhi_{k',\Sigma})) = \psi_{k_1}(\varPsi(\langle \varPhi_{k',\Sigma}(-1) \rangle)) = \langle (8,8) \rangle$. On the other hand, if $\left(\frac{q}{\ell}\right) = 1$, $g_{qO_{k'}} \equiv g_{\mathfrak{Q}\cap k_1}^u \pmod{\mathfrak{Q} \cap k_1}$ with some odd $u \in \mathbb{Z}$. Then, since $\mathfrak{Q}^{\sigma\gamma} \cap k_1 = \mathfrak{Q}^\sigma \cap k_1$ and γ acts on $O_{k_1}/(\mathfrak{Q}^\sigma \cap k_1)$ as the Frobenius automorphism, we have $g_{qO_{k'}} \equiv g_{\mathfrak{Q}\cap k_1}^{u\sigma\gamma} \equiv g_{\mathfrak{Q}^\sigma \cap k_1}^{qu} \pmod{\mathfrak{Q}^\sigma \cap k_1}$. Since $\varepsilon_{2\ell} \equiv g_{qO_{k'}}^{2t}$

(mod q), we have $\varphi_{k_2,\Sigma}(\varepsilon_{2\ell}) = \psi_{k_1}(\varphi_{k_1,\Sigma}(\varepsilon_{2\ell})) = \psi_{k_1}((2tu, 2tuq)) = (4tu, -4tu)$ if $\left(\frac{q}{\ell}\right) = 1$. Therefore

$$\varphi_{k_2,\Sigma}(\sqrt{\varepsilon_{2\ell}}) \equiv \begin{cases} (0,0) \pmod{\langle (4,4),(8,0)\rangle} & \text{if } \left(\frac{q}{\ell}\right) = -1, \\ (2tu, -2tu) \pmod{8[16,16]} & \text{if } \left(\frac{q}{\ell}\right) = 1. \end{cases} \tag{6.7}$$

Recall that $(E(\mathbb{Q}_2)E(M)E(k_1))^{1+\gamma^2} = E(\mathbb{Q}_1)E(k_1)^2$. If $(y_0, y_1) = \varphi_{k_2,\Sigma}(\varepsilon)$ with some $\varepsilon \in E(k_2)$, then $(q^2y_0, q^2y_1) = \varphi_{k_2,\Sigma}(\varepsilon^{\gamma^2})$. Hence $\varphi_{k_2,\Sigma}(E(\mathbb{Q}_1)E(k_1)^2) = \langle (2,2),(8,0)\rangle \supset 8[16,16]$ by (6.6). Put $(c_0, c_1) = \varphi_{k_2,\Sigma}(\eta_1)$ and $(d_0, d_1) = \varphi_{k_2,\Sigma}(\eta_2)$. Since $(10c_0, 10c_1) = \varphi_{k_2,\Sigma}(\eta_1^{1+\gamma^2}) \equiv \varphi_{k_2,\Sigma}(\sqrt{\varepsilon_{2\ell}}) \pmod{\langle (2,2),(8,0)\rangle}$ and $(10d_0, 10d_1) = \varphi_{k_2,\Sigma}(\eta_2^{1+\gamma^2}) \in \langle (2,2),(8,0)\rangle$ by (6.3), we have

$$(5c_0, 5c_1) \equiv \begin{cases} (0,0) \pmod{\langle (1,1),(4,0)\rangle} & \text{if } \left(\frac{q}{\ell}\right) = -1, \\ (tu, -tu) \pmod{\langle (1,1),(4,0)\rangle} & \text{if } \left(\frac{q}{\ell}\right) = 1 \end{cases}$$

and $(5d_0, 5d_1) \in \langle (1,1),(4,0)\rangle$ by (6.7). Then $\operatorname{Im}\varphi_{k_2,\Sigma} = \langle (5c_0, 5c_1), (1,1), (4,0)\rangle$. If $\left(\frac{q}{\ell}\right) = -1$, we have $|A_\Sigma(k_2)| = 4$. If $\left(\frac{q}{\ell}\right) = 1$ and $\ell \equiv 1 \pmod{16}$, then t is odd by (6.4), and hence $|A_\Sigma(k_2)| = 2$. Thus we obtain the statement for the case where $q \equiv 3 \pmod 8$.

Suppose that $\ell \equiv 9 \pmod{16}$. Recall that $\mathrm{r}_2(A_\Sigma(k_n)) = 1$ for all $n \geq 1$. Then $(k_2)_\Sigma^{\mathrm{elem}} = (k_1)_\Sigma^{\mathrm{elem}} k_2$ is a $[2,2]$-extension of k_1. Let $\mathfrak{L}$ be a prime of k_2 lying over $\mathfrak{l}$. Since $\mathfrak{L} \cap k_1$ is inert in k_2/k_1, $\mathfrak{L}$ splits in $(k_2)_\Sigma^{\mathrm{elem}}/k_2$. Since $\mathfrak{L} \cap M$ is also inert in k_2/M, the quartic extension $(k_2)_\Sigma^{\mathrm{elem}}/M$ is a $[2,2]$-extension unramified outside Σ. Since $M_\Sigma = (k_2)_\Sigma^{\mathrm{ab}}$, $\mathrm{r}_4(A_\Sigma(M)) \leq 1$ and $\mathrm{r}_2(A_\Sigma(M)) = 2$. Let M' and M'' be the distinct quadratic extensions of M contained in $(k_2)_\Sigma^{\mathrm{elem}}$ different from k_2. Since $(k_2)_\Sigma^{\mathrm{elem}}/\mathbb{Q}$ is not abelian, $M'/\mathbb{Q}$ is not a Galois extension, and M'' is the conjugate of M'. Then $G_\Sigma(M)^{\mathrm{ab}} \simeq A_\Sigma(M)$ has a cyclic maximal subgroup $\mathrm{Gal}(M_\Sigma^{\mathrm{ab}}/k_2)$, and two other maximal subgroups $\mathrm{Gal}(M_\Sigma^{\mathrm{ab}}/M')$, $\mathrm{Gal}(M_\Sigma^{\mathrm{ab}}/M'')$ are isomorphic to each other. This implies that $\mathrm{r}_4(A_\Sigma(M)) = 0$, i.e., $A_\Sigma(M) \simeq [2,2]$.

Suppose that $\ell \equiv 9 \pmod{16}$ and $q \equiv 7 \pmod{16}$. Then $O_{\mathbb{Q}_2}/\mathfrak{l} \simeq \mathbb{F}_{\ell^2}$ and $O_{\mathbb{Q}_2}/(\mathfrak{Q} \cap \mathbb{Q}_2) \simeq \mathbb{F}_{q^2}$. We choose $g_{\mathfrak{l}O_{\mathbb{Q}_2}}$, $g_{\mathfrak{Q}\cap\mathbb{Q}_2}$, and put $g_{\mathfrak{l}^\gamma O_{\mathbb{Q}_2}} = g_{\mathfrak{l}O_{\mathbb{Q}_2}}^\gamma$, $g_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2} = g_{\mathfrak{Q}\cap\mathbb{Q}_2}^\gamma$. If $\varepsilon \equiv g_{\mathfrak{l}^\gamma O_{\mathbb{Q}_2}}^a \pmod{\mathfrak{l}^\gamma}$ and $\varepsilon \equiv g_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2}^b \pmod{\mathfrak{Q}^\gamma \cap \mathbb{Q}_2}$ for some $\varepsilon \in E(\mathbb{Q}_2)$ and a, $b \in \mathbb{Z}$, then $\varepsilon^\gamma \equiv g_{\mathfrak{l}O_{\mathbb{Q}_2}}^{\gamma^2 a} \equiv g_{\mathfrak{l}O_{\mathbb{Q}_2}}^{\ell a} \pmod{\mathfrak{l}}$ and $\varepsilon^\gamma \equiv g_{\mathfrak{Q}\cap\mathbb{Q}_2}^{\gamma^2 b} \equiv g_{\mathfrak{Q}\cap\mathbb{Q}_2}^{qb}$ $\pmod{\mathfrak{Q} \cap \mathbb{Q}_2}$. Hence we obtain the exact sequence

$$E(\mathbb{Q}_2) \xrightarrow{\varphi_{\mathbb{Q}_2,S}} [16_{\mathfrak{l}O_{\mathbb{Q}_2}}, 16_{\mathfrak{l}^\gamma O_{\mathbb{Q}_2}}, 16_{\mathfrak{Q}\cap\mathbb{Q}_2}, 16_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2}] \to A_S(\mathbb{Q}_2) \to 0$$

and

$$v_{\mathbb{Q}_2,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_2,S}(\xi) \\ \varphi_{\mathbb{Q}_2,S}(\xi^\gamma) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^2}) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^3}) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & b_0 & b_1 \\ \ell a_1 & a_0 & qb_1 & b_0 \\ \ell a_0 & \ell a_1 & qb_0 & qb_1 \\ \ell^2 a_1 & \ell a_0 & q^2 b_1 & qb_0 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & b_0 & b_1 \\ 9a_1 & a_0 & 7b_1 & b_0 \\ 9a_0 & 9a_1 & 7b_0 & 7b_1 \\ a_1 & 9a_0 & b_1 & 7b_0 \end{pmatrix}.$$

Since $\varphi_{\mathbb{Q}_2,S}(\xi^{1+\gamma+\gamma^2+\gamma^3}) = \varphi_{\mathbb{Q}_2,S}(-1) = (8,8,8,8)$, we have $a_0 + a_1 \equiv 4 \pmod 8$ and $b_0 + b_1 \equiv 1 \pmod 2$. In particular, $a_0 + a_1 \equiv \pm 4 \pmod{16}$. Replacing $\mathfrak{Q}$ by $\mathfrak{Q}^\gamma$ if necessary, we may assume that $b_0 \in \mathbb{Z}_2^\times$. Since $A_{\{\ell\}}(\mathbb{Q}_2)$ is cyclic by Proposition 5.1, $\operatorname{Im}\varphi_{\mathbb{Q}_2,\{\ell\}} \notin 2[16,16]$, i.e., $a_0 \equiv a_1 \equiv 1 \pmod 2$. Then $a_1^2 \equiv 8 + a_0^2 \pmod{16}$.

Since

$$\begin{pmatrix} 1 & -1 & \frac{a_0-9a_1}{2a_0} & 0 \\ 0 & 1 & \frac{9a_1-1}{2a_0} & 0 \\ 0 & -2 & \frac{-9a_1}{a_0} & 0 \\ 0 & 0 & 4 & 1 \end{pmatrix} \begin{pmatrix} \frac{9-7b_0}{2b_0} & 0 & \frac{b_0-1}{2b_0} & 0 \\ \frac{b_1}{2b_0} & 1 & \frac{7b_1}{2b_0} & 0 \\ 7 & 0 & -1 & 0 \\ \frac{b_0-4}{b_0} & 1 & \frac{b_0+4}{b_0} & 1 \end{pmatrix} v_{\mathbb{Q}_2,S} = \begin{pmatrix} 0 & 0 & 1 & \frac{b_1-b_0^2-b_1^2}{b_0} \\ 1 & \frac{a_1}{a_0} & 0 & \frac{b_0^2+b_1^2}{b_0} \\ 0 & 0 & 0 & -2\frac{b_0^2+b_1^2}{b_0} \\ 0 & 0 & 0 & 8 \end{pmatrix},$$

one can see that $A_S(\mathbb{Q}_2) \simeq [2,16]$. Since $O_{\mathbb{Q}_2}/(\mathfrak{Q} \cap \mathbb{Q}_2) \simeq O_{k_2}/\mathfrak{Q} \simeq O_{k_2}/\mathfrak{Q}^\sigma$, we can put $g_{\mathfrak{Q}} = g_{\mathfrak{Q}^\sigma} := g_{\mathfrak{Q}\cap\mathbb{Q}_2}$ and $g_{\mathfrak{Q}^\gamma} = g_{\mathfrak{Q}^{\sigma\gamma}} := g_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2}$. Put $(F, F') = (k_1, M)$ or (M, k_1) according to $\left(\frac{q}{\ell}\right) = 1$ or -1. Then F is the decomposition field of q in $k_2/\mathbb{Q}$, and $\mathfrak{Q} \cap F' = \mathfrak{Q}^\sigma \cap F'$. We choose z_q satisfying $g_{\mathfrak{Q}}^{1+q} \equiv z_q \pmod{\mathfrak{Q}}$ as the primitive elements of residue fields $\mathbb{F}_q$, and $g_{\mathfrak{Q}\cap F'}$ such that $g_{\mathfrak{Q}\cap F'} \equiv g_{\mathfrak{Q}} \pmod{\mathfrak{Q}}$. Since σ acts on $O_{F'}/(\mathfrak{Q} \cap F')$ as the Frobenius automorphism, $g_{\mathfrak{Q}\cap F'} \equiv g_{\mathfrak{Q}\cap F'}^{q\sigma} \equiv g_{\mathfrak{Q}^\sigma}^{q}$ $\pmod{\mathfrak{Q}^\sigma}$, and $g_{\mathfrak{Q}^\gamma\cap F'} := g_{\mathfrak{Q}\cap F'}^{\gamma}$ satisfies $g_{\mathfrak{Q}^\gamma\cap F'} \equiv g_{\mathfrak{Q}^\gamma} \pmod{\mathfrak{Q}^\gamma}$ and $g_{\mathfrak{Q}^\gamma\cap F'} \equiv g_{\mathfrak{Q}^{\sigma\gamma}}^{q} \pmod{\mathfrak{Q}^{\sigma\gamma}}$. Then we obtain the commutative diagram

$$\begin{tikzcd}
E(F') \arrow[r, "\varphi_{F',\Sigma}"] \arrow[dd, bend right, "\cap"'] & {[16_{\mathfrak{Q}\cap F'}, 16_{\mathfrak{Q}^\gamma\cap F'}]} \arrow[r] \arrow[dd, bend left, "\psi'"] & A_\Sigma(F') \arrow[r] & A_\emptyset(F') \arrow[r] & 0 \\
E(\mathbb{Q}_2) \arrow[r, "\varphi_{\mathbb{Q}_2,\Sigma}"] \arrow[d, "\cap"] & {[16_{\mathfrak{Q}\cap\mathbb{Q}_2}, 16_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2}]} \arrow[r] \arrow[d, "\psi_{\mathbb{Q}_2}"'] & 0 & & \\
E(k_2) \arrow[r, "\varphi_{k_2,\Sigma}"] & {[16_{\mathfrak{Q}}, 16_{\mathfrak{Q}^\sigma}, 16_{\mathfrak{Q}^\gamma}, 16_{\mathfrak{Q}^{\sigma\gamma}}]} \arrow[r] & A_\Sigma(k_2) \arrow[r] & 0 & \\
E(F) \arrow[r, "\varphi_{F,\Sigma}"] \arrow[u, "\cup"'] & {[2_{\mathfrak{Q}\cap F}, 2_{\mathfrak{Q}^\sigma\cap F}, 2_{\mathfrak{Q}^\gamma\cap F}, 2_{\mathfrak{Q}^{\sigma\gamma}\cap F}]} \arrow[r] \arrow[u, "\psi"] & A_\Sigma(F) \arrow[r] \arrow[u, "\iota"] & A_\emptyset(F) \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\psi_{\mathbb{Q}_2}(x_0, x_1) = (x_0, x_0, x_1, x_1)$, $\psi'(y_0, y_1) = (y_0, qy_0, y_1, qy_1)$ and $\psi(x_0, x_1, x_2, x_3) = (8x_0, 8x_1, 8x_2, 8x_3)$. Recall that $A_\Sigma(M) \simeq [2, 2]$, $A_\emptyset(M) \simeq \mathbb{Z}/2\mathbb{Z}$ and $A_\emptyset(k_1) \simeq 0$. By (6.5), we have $A_\Sigma(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$. These yield that $|\operatorname{Coker} \varphi_{F,\Sigma}| = |\operatorname{Coker} \varphi_{F',\Sigma}| = 2$. Note that $g_{\mathfrak{Q}^\gamma\cap F'}^{\gamma} = g_{\mathfrak{Q}\cap F'}^{\gamma^2} \equiv g_{\mathfrak{Q}\cap F'}^{q}$ or $g_{\mathfrak{Q}\cap F'}$ $\pmod{\mathfrak{Q} \cap F'}$ according to $\left(\frac{q}{\ell}\right) = 1$ or -1. If $\varphi_{F',\Sigma}(\varepsilon) = (1, 0)$ (resp. $(0, 1)$) for some ε, then $\varphi_{F',\Sigma}(\varepsilon^\gamma) = (0, 1)$ (resp. $(q, 0)$ or $(1, 0)$). Since $\varphi_{F',\Sigma}$ is not surjective, $\{(1, 0), (0, 1)\} \cap \operatorname{Im} \varphi_{F',\Sigma} = \emptyset$, and hence $\operatorname{Im} \varphi_{F',\Sigma} = \langle (1, 1), (2, 0) \rangle$. Then

$$\begin{aligned} \varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(F')) &= \langle (1, 1, 0, 0), (0, 0, 1, 1), (1, q, 1, q), (2, 2q, 0, 0) \rangle \\ &= \langle (1, 1, 0, 0), (0, 0, 1, 1), (0, 2, 0, 2), (0, 4, 0, 0) \rangle \end{aligned}$$

and $\varphi_{k_2,\Sigma}(E(F)) \subset \operatorname{Im} \psi = 8[16, 16, 16, 16] \subset \varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(F'))$. In particular,

$$\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) = \langle (1, 1, 0, 0), (0, 0, 1, 1), (0, 2, 0, 2), (0, 4, 0, 0) \rangle.$$

Since $A_\Sigma(\mathbb{Q}_2) \simeq 0$, σ acts on $A_\Sigma(k_2)$ as -1. If $\left(\frac{q}{\ell}\right) = 1$, the inclusion $\operatorname{Im} \psi \subset \operatorname{Im} \varphi_{k_2,\Sigma}$ implies that $\iota : A_\Sigma(k_1) \to A_\Sigma(k_2)$ is zero mapping; i.e., γ^2 also acts on $A_\Sigma(k_2)$ as -1. Then, since $\sigma\gamma^2$ acts on $A_\Sigma(k_2)$ trivially, $(k_2)_\Sigma^{\mathrm{ab}}/M$ is abelian, i.e., $(k_2)_\Sigma^{\mathrm{ab}} = M_\Sigma^{\mathrm{ab}}$. Therefore $|A_\Sigma(k_2)| = \frac{1}{2}|A_\Sigma(M)| = 2$ if $\left(\frac{q}{\ell}\right) = 1$. Suppose that $\left(\frac{q}{\ell}\right) = -1$. Then $(F, F') = (M, k_1)$ and $\mathfrak{Q}^\sigma = \mathfrak{Q}^{\gamma^2}$. Recall that $(E(\mathbb{Q}_2)E(M)E(k_1))^{1+\gamma^2} = E(\mathbb{Q}_1)E(k_1)^2$. If $(y_0, y_1, y_2, y_3) = \varphi_{k_2,\Sigma}(\varepsilon)$ with some $\varepsilon \in E(k_2)$, then $(qy_1, qy_0, qy_3, qy_2) = \varphi_{k_2,\Sigma}(\varepsilon^{\gamma^2})$. Hence

$$\varphi_{k_2,\Sigma}(E(\mathbb{Q}_1)E(k_1)^2) = \langle (-2, 2, -2, 2), (-4, 4, 0, 0) \rangle.$$

Put $(d_0, d_1, d_2, d_3) = \varphi_{k_2,\Sigma}(\eta_2)$. By (6.3), we have

$$(d_0 + qd_1, d_1 + qd_0, d_2 + qd_3, d_3 + qd_2) \in \langle(-2, 2, -2, 2), (-4, 4, 0, 0)\rangle.$$

In particular, $d_0 - d_1 \equiv d_2 - d_3 \pmod 4$ and $d_2 - d_3 \equiv 0 \pmod 2$. Then

$$\begin{aligned}&\varphi_{k_2,\Sigma}(\eta_2)\\ &= d_0(1,1,0,0) + d_2(0,0,1,1) - \tfrac{d_2-d_3}{2}(0,2,0,2) + \tfrac{(d_2-d_3)-(d_0-d_1)}{4}(0,4,0,0)\\ &\in \varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)).\end{aligned}$$

Hence $|\mathrm{Im}\,\varphi_{k_2,\Sigma}/\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1))| \le 2$. Since

$$[16, 16, 16, 16]/\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) \simeq [2, 4],$$

we have $|A_\Sigma(k_2)| \ge 4$ if $\left(\frac{q}{\ell}\right) = -1$.

Suppose that $\ell \equiv 9 \pmod{16}$ and $q \equiv 15 \pmod{16}$. We choose $g_{\mathfrak{l}O_{\mathbb{Q}_2}}$ and put $g_{\mathfrak{l}^\gamma O_{\mathbb{Q}_2}} = g^\gamma_{\mathfrak{l}O_{\mathbb{Q}_2}}$. Choosing z_q as the primitive elements of residue fields $\mathbb{F}_q$, we obtain the exact sequence

$$E(\mathbb{Q}_2) \xrightarrow{\varphi_{\mathbb{Q}_2,S}} [16_{\mathfrak{l}O_{\mathbb{Q}_2}}, 16_{\mathfrak{l}^\gamma O_{\mathbb{Q}_2}}, 2_{\mathfrak{Q}\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^{\gamma^2}\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^{\gamma^3}\cap\mathbb{Q}_2}] \to A_S(\mathbb{Q}_2) \to 0$$

and

$$v_{\mathbb{Q}_2,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_2,S}(\xi) \\ \varphi_{\mathbb{Q}_2,S}(\xi^\gamma) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^2}) \\ \varphi_{\mathbb{Q}_2,S}(\xi^{\gamma^3}) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & b_0 & b_2 & b_1 & b_3 \\ 9a_1 & a_0 & b_3 & b_1 & b_0 & b_2 \\ 9a_0 & 9a_1 & b_2 & b_0 & b_3 & b_1 \\ a_1 & 9a_0 & b_1 & b_3 & b_2 & b_0 \end{pmatrix}.$$

Since $\xi^{1+\gamma+\gamma^2+\gamma^3} = -1$, we have $a_0 + a_1 \equiv \pm 4 \pmod{16}$ and $\sum_{i=0}^3 b_i \equiv 1 \pmod 2$. Replacing $\mathfrak{Q}$ by $\mathfrak{Q}^{\gamma^i}$ if necessary, we may assume that $b_0 \equiv 1$, $b_2 \equiv 0 \pmod 2$. Then $b_1 \equiv b_3 \pmod 2$. Since $A_{\{\ell\}}(\mathbb{Q}_2)$ is cyclic by Proposition 5.1, $\mathrm{Im}\,\varphi_{\mathbb{Q}_2,\{\ell\}} \notin 2[16, 16]$, i.e., $a_0 \equiv a_1 \equiv 1 \pmod 2$. Then

$$\begin{pmatrix} 1 & 0 & 0 & b_1 \\ 0 & 1 & b_1 & b_1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 8 - \frac{a_1}{a_0} & 1 & 0 & 0 \\ -9 & 0 & 1 & 0 \\ 10 & 3 & 2 & 1 \end{pmatrix} v_{\mathbb{Q}_2,S} = \begin{pmatrix} a_0 & a_1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Hence we have $A_S(\mathbb{Q}_2) \simeq [2, 16]$. Recall that $\mathrm{r}_2(A_\Sigma(k_2)) = 1$. If $\left(\frac{q}{\ell}\right) = 1$, q splits completely in $k_2/\mathbb{Q}$. Then the exact sequence

$$E(k_2) \xrightarrow{\varphi_{k_2,\Sigma}} [2_{\mathfrak{Q}}, 2_{\mathfrak{Q}^{\gamma^2}}, 2_{\mathfrak{Q}^\gamma}, 2_{\mathfrak{Q}^{\gamma^3}}, 2_{\mathfrak{Q}^\sigma}, 2_{\mathfrak{Q}^{\sigma\gamma^2}}, 2_{\mathfrak{Q}^{\sigma\gamma}}, 2_{\mathfrak{Q}^{\sigma\gamma^3}}] \to A_\Sigma(k_2) \to 0$$

yields that $|A_\Sigma(k_2)| = 2$. Suppose that $\left(\frac{q}{\ell}\right) = -1$. We choose $g_{qO_k} = g_{\mathfrak{Q}^{\gamma^i}\cap k_1} = g_{\mathfrak{Q}^{\gamma^i}}$ commonly for all i. Then $z_q \equiv g_{qO_k}^{u(1+q)} \pmod q$ with some odd u. We choose $g_{\mathfrak{Q}\cap M}$ such that $g_{\mathfrak{Q}\cap M} \equiv g_{qO_k} \pmod{\mathfrak{Q}}$. Then $g_{\mathfrak{Q}\cap M} \equiv g_{\mathfrak{Q}\cap M}^{q\gamma^2} \equiv g_{qO_k}^{q}$ $(\mathrm{mod}\ \mathfrak{Q}^{\gamma^2})$, and $g_{\mathfrak{Q}^\gamma\cap M} = g_{\mathfrak{Q}\cap M}^{\gamma}$ satisfies $g_{\mathfrak{Q}^\gamma\cap M} \equiv g_{qO_k} \pmod{\mathfrak{Q}^\gamma}$ and $g_{\mathfrak{Q}^\gamma\cap M} \equiv g_{qO_k}^{q} \pmod{\mathfrak{Q}^{\gamma^3}}$. Then we obtain a commutative diagram

$$\begin{tikzcd}
E(\mathbb{Q}_2) \arrow[r, "\varphi_{\mathbb{Q}_2,\Sigma}"] \arrow[d, "\cap"] & {[2_{\mathfrak{Q}\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^{\gamma^2}\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^{\gamma}\cap\mathbb{Q}_2}, 2_{\mathfrak{Q}^{\gamma^3}\cap\mathbb{Q}_2}]} \arrow[r] \arrow[d, "\psi_{\mathbb{Q}_2}"] & 0 & \\
E(k_2) \arrow[r, "\varphi_{k_2,\Sigma}"] & {[2^{e+1}_{\mathfrak{Q}}, 2^{e+1}_{\mathfrak{Q}^{\gamma^2}}, 2^{e+1}_{\mathfrak{Q}^{\gamma}}, 2^{e+1}_{\mathfrak{Q}^{\gamma^3}}]} \arrow[r] & A_\Sigma(k_2) \arrow[r] & 0 \\
E(k_1) \arrow[r, "\varphi_{k_1,\Sigma}"] \arrow[u, "\cup"] & {[2^{e+1}_{\mathfrak{Q}\cap k_1}, 2^{e+1}_{\mathfrak{Q}^{\gamma}\cap k_1}]} \arrow[r] \arrow[u, "\psi_{k_1}"] & A_\Sigma(k_1) \arrow[r] & 0 \\
E(M) \arrow[r, "\varphi_{M,\Sigma}"] \arrow[uu, bend left, "\cup"] & {[2^{e+1}_{\mathfrak{Q}\cap M}, 2^{e+1}_{\mathfrak{Q}^{\gamma}\cap M}]} \arrow[r] \arrow[uu, bend right, "\psi_M"'] & A_\Sigma(M) \arrow[r, two heads] & A_\emptyset(M)
\end{tikzcd}$$

with exact rows, where $e = v_2(q+1) \geq 4$, $\psi_{k_1}(x_0, x_1) = (x_0, x_0, x_1, x_1)$, $\psi_M(x_0, x_1) = (x_0, qx_0, x_1, qx_1)$ and $\psi_{\mathbb{Q}_2}(y_0, y_2, y_1, y_3) = (2^e y_0, 2^e y_2, 2^e y_1, 2^e y_3)$. By (6.5), $A_\Sigma(k_1) \simeq \mathbb{Z}/2\mathbb{Z}$. Recall that $A_\Sigma(M) \simeq [2,2]$ and $A_\emptyset(M) \simeq \mathbb{Z}/2\mathbb{Z}$. Note that $\varphi_{k_1,\Sigma}(\varepsilon^\gamma) = (x_1, x_0)$ if $\varphi_{k_1,\Sigma}(\varepsilon) = (x_0, x_1)$ and that $\varphi_{M,\Sigma}(\varepsilon^\gamma) = (qx_1, x_0)$ if $\varphi_{M,\Sigma}(\varepsilon) = (x_0, x_1)$. Therefore $\operatorname{Im}\varphi_{k_1,\Sigma} = \langle (1,1), (2,0)\rangle$ and $\operatorname{Im}\varphi_{M,\Sigma} = \langle (1,1), (2,0)\rangle$. Then

$$\varphi_{k_2,\Sigma}(E(M)E(k_1)) = \langle (1,1,1,1), (2,2,0,0), (1,q,1,q), (2,2q,0,0)\rangle$$

and $\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)) = 2^e[2^{e+1}, 2^{e+1}, 2^{e+1}, 2^{e+1}] \subset \varphi_{k_2,\Sigma}(E(M)E(k_1))$. Thus we have

$$\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) = \langle (1,1,1,1), (2,2,0,0), (2,0,2,0), (4,0,0,0)\rangle.$$

Since $|\operatorname{Im}\varphi_{k_2,\Sigma}/\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1))| \leq 4$ and

$$[2^{e+1}, 2^{e+1}, 2^{e+1}, 2^{e+1}]/\varphi_{k_2,\Sigma}(E(\mathbb{Q}_2)E(M)E(k_1)) \simeq [2,2,4],$$

we have $|A_\Sigma(k_2)| \geq 4$. Thus the proof of Lemma 6.5 is completed. $\square$

Lemma 6.6. *If* $\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = 1$, $q \equiv 7 \pmod 8$ *and* $\left(\frac{q}{\ell}\right) = 1$, *then* $G_S(\mathbb{Q}_1)$ *is nonabelian.*

Proof. Recall that $E(k_1) = \langle -1, \varepsilon_2, \varepsilon_\ell, \sqrt{\varepsilon_{2\ell}}\rangle$ (cf. the proof of Lemma 6.5). Let σ (resp. γ) be a generator of $\mathrm{Gal}(k_1/\mathbb{Q}_1)$ (resp. $\mathrm{Gal}(k_1/k)$). Let $\mathfrak{L}$ (resp. $\mathfrak{Q}$) be a prime of k_1 lying over $\mathfrak{l}$ (resp. q). We choose z_ℓ (resp. z_q) as the primitive elements of residue fields $\mathbb{F}_\ell$ (resp. $\mathbb{F}_q$). Then we obtain the commutative diagram

$$\begin{tikzcd}
E(k) \arrow[r, "\varphi_{k,S}"] \arrow[d, "\cap"] & {[8_{\sqrt{\ell}O_k}, 2_{\mathfrak{Q}\cap k}, 2_{\mathfrak{Q}^\sigma\cap k}]} \arrow[r] \arrow[d, "\psi_k"] & A_S(k) \arrow[r] & 0 \\
E(k_1) \arrow[r, "\varphi_{k_1,S}"] & {[8_{\mathfrak{L}}, 8_{\mathfrak{L}^\gamma}, 2_{\mathfrak{Q}}, 2_{\mathfrak{Q}^\sigma}, 2_{\mathfrak{Q}^\gamma}, 2_{\mathfrak{Q}^{\sigma\gamma}}]} \arrow[r] & A_S(k_1) \arrow[r] & 0 \\
E(\mathbb{Q}_1) \arrow[r, "\varphi_{\mathbb{Q}_1,S}"] \arrow[u, "\cup"] & {[8_{\mathfrak{l}}, 8_{\mathfrak{l}^\gamma}, 2_{\mathfrak{Q}\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}^\gamma\cap\mathbb{Q}_1}]} \arrow[r] \arrow[u, "\psi_{\mathbb{Q}_1}"] & A_S(\mathbb{Q}_1) \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\psi_k(x, y_0, y_1) = (x, x, y_0, y_1, y_0, y_1)$ and $\psi_{\mathbb{Q}_1}(x_0, x_1, y_0, y_1) = (x_0, x_1, y_0, y_0, y_1, y_1)$. Recall that $\varepsilon_2^{1+\gamma} = -1$ and $A_{\{q\}}(\mathbb{Q}_1) \simeq 0$. Since $\mathrm{r}_2(A_{\{\ell\}}(\mathbb{Q}_1)) = 1$ by Proposition 5.1, we have

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 4 & 4 & 1 & 1 \\ u & 4-u & b & b+1 \end{pmatrix}$$

with some $u \equiv 1 \pmod 2$ and $b \in \{0,1\}$. Then one can easily see that $A_S(\mathbb{Q}_1) \simeq [2,8]$. Since $\varepsilon_\ell^{1+\sigma} = -1$, we have $\varphi_{k,S}(\varepsilon_\ell) = (a, d, d+1)$ with some $a \equiv 2 \pmod 4$ and $d \in \{0,1\}$. Since $\varepsilon_{2\ell} \in E(k_1)^2$ and $\varepsilon_{2\ell}^{1+\sigma} = 1$, we have $\varphi_{k_1,S}(\varepsilon_{2\ell}) = (c, c, 0, 0, 0, 0)$ with some $c \equiv 0 \pmod 4$. Put

$$w_{k_1,S} = \begin{pmatrix} \varphi_{k_1,S}(-1) \\ \varphi_{k_1,S}(\varepsilon_2) \\ \varphi_{k_1,S}(\varepsilon_\ell) \\ \varphi_{k_1,S}(\varepsilon_{2\ell}) \end{pmatrix} = \begin{pmatrix} 4 & 4 & 1 & 1 & 1 & 1 \\ u & 4-u & b & b & b+1 & b+1 \\ a & a & d & d+1 & d & d+1 \\ c & c & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then

$$\begin{pmatrix} -1 & 0 & 2 & 0 \\ -b & \frac{1}{u} & 2b & 0 \\ -d & 0 & \frac{2}{a}+2d & 0 \\ 0 & 0 & \frac{c}{2} & 1 \end{pmatrix} w_{k_1,S} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 3 & 0 & 0 & 1 & 1 \\ 2 & 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This yields that $[8,8,2,2,2,2]/\varphi_{k_1,S}(\langle -1, \varepsilon_2, \varepsilon_\ell, \varepsilon_{2\ell}\rangle) \simeq [8,2,2]$. Hence $|A_S(k_1)| = |\mathrm{Coker}\,\varphi_{k_1,S}| \geq \frac{1}{2}|[8,2,2]| = |A_S(\mathbb{Q}_1)|$. This implies that $G_S(\mathbb{Q}_1)$ is nonabelian. Thus the proof of Lemma 6.6 is completed. $\square$

Now we complete the proof of Theorem 6.3. Put $\Sigma = \{q\}$. Since $\ell \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 4$, $\mathbb{Q}_S^{\mathrm{ab}}/\mathbb{Q}$ is a cyclic extension of degree at least 8, which is totally ramified at ℓ. Hence $\mathrm{r}_4(A_S(\mathbb{Q}_n)) \geq 1$ for all $n \geq 0$. Moreover, $G_S(\mathbb{Q}_\infty)$ is not procyclic by Proposition 6.2, and hence $\mathrm{r}_2(A_S(\mathbb{Q}_n)) \geq 2$ for all $n \geq 1$ by Theorem 4.3. If $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$, Theorem 3.1(1) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \Sigma_{\mathbb{Q}_n})$ yields that $(\mathbb{Q}_n)^{\mathrm{elem}}_{S_{\mathbb{Q}_n}\setminus\{\mathfrak{L}\}} \neq \mathbb{Q}_n$ for $\mathfrak{L} \in S_{\mathbb{Q}_n} \setminus \Sigma_{\mathbb{Q}_n}$. Then $\mathbb{Q}_S^{\mathrm{ab}}(\mathbb{Q}_n)^{\mathrm{elem}}_{S_{\mathbb{Q}_n}\setminus\{\mathfrak{L}\}}/k_n$ is a noncyclic abelian extension. Therefore $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_n)_S^{\mathrm{ab}}/k_n)) = 2$ if $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$.

First, we prove the if-part. Assume one of the two conditions, and suppose $n \geq 1$. Then $\left(\frac{2}{\ell}\right)_4 \neq (-1)^{\frac{\ell-1}{8}}$. Since $\ell \equiv 9 \pmod{16}$ or $q \equiv 3 \pmod 8$, we have $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ by Lemma 6.1, and hence $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_n)_S^{\mathrm{ab}}/k_n)) = 2$. Recall that $\mathrm{r}_4(A_S(\mathbb{Q}_1)) \geq 1$. For any $n \geq 2$,

$$\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 1 \text{ and } |A_\Sigma(k_n)| \geq 4 \ \text{ if } \ell \equiv 9 \pmod{16},\ q \equiv 7 \pmod 8,\ \left(\tfrac{q}{\ell}\right) = -1,$$
$$\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2 \text{ and } |A_\Sigma(k_n)| = 2 \ \text{ if } \ell \equiv 1 \pmod{16},\ q \equiv 3 \pmod 8,\ \left(\tfrac{q}{\ell}\right) = 1$$

by Lemma 6.5 and Theorem 4.3. Hence $G_S(\mathbb{Q}_n)$ is metacyclic for all $n \geq 2$ by Theorem 3.1(2), (3) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \Sigma_{\mathbb{Q}_n})$. Therefore $G_S(\mathbb{Q}_\infty)$ is prometacyclic.

Conversely, we assume that $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Then $G_{\{\ell\}}(\mathbb{Q}_\infty)$ is also prometacyclic. Suppose that $\left(\frac{2}{\ell}\right)_4 = (-1)^{\frac{\ell-1}{8}}$. Then, since $\ell \equiv 9 \pmod{16}$ and $\left(\frac{2}{\ell}\right)_4 = -1$ by Theorem 5.2, we have $\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$ and $|A_\Sigma(k_n)| \geq 4$ for all $n \geq 2$ by Lemma 6.4. Theorem 3.1(2) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \Sigma_{\mathbb{Q}_n})$ implies that $G_S(\mathbb{Q}_n)$ is not metacyclic if $n \geq 2$. This is a contradiction. Therefore $\left(\frac{2}{\ell}\right)_4 \neq (-1)^{\frac{\ell-1}{8}}$. Since $G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic, we have $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$ by Theorem 4.3. In particular, $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$, and hence $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_2)_S^{\mathrm{ab}}/k_2)) = 2$. Also, $\ell \equiv 9 \pmod{16}$ or $q \equiv 3 \pmod 8$ by Lemma 6.1. We apply Theorem 3.1 for $(k_2/\mathbb{Q}_2, S_{\mathbb{Q}_2}, \Sigma_{\mathbb{Q}_2})$. Since $G_S(\mathbb{Q}_2)$ is metacyclic, $\mathrm{r}_4(A_S(\mathbb{Q}_1)) = 1$ or $|A_\Sigma(k_2)| = 2$ by Theorem 3.1(2). Hence, if $q \equiv 3 \pmod 8$, we have $\ell \equiv 1 \pmod{16}$ (i.e., $\left(\frac{2}{\ell}\right)_4 = -1$) and $\left(\frac{q}{\ell}\right) = 1$ by Lemma 6.5. This is one of the two conditions. On the other hand, we assume that $\ell \equiv 9 \pmod{16}$ (i.e., $\left(\frac{2}{\ell}\right)_4 = 1$). Then $q \equiv 7 \pmod 8$, and $S_{\mathbb{Q}_2} \setminus \Sigma_{\mathbb{Q}_2} = \{\mathfrak{l}O_{\mathbb{Q}_2}, \mathfrak{l}^\gamma O_{\mathbb{Q}_2}\}$. Lemma 6.5 yields that $A_S(\mathbb{Q}_2) \simeq [2,16]$. In particular, $\mathrm{r}_4(A_S(\mathbb{Q}_2)) = 1$ and $|O_{\mathbb{Q}_2}/\mathfrak{l}| = |O_{\mathbb{Q}_2}/\mathfrak{l}^\gamma| = \ell^2 \not\equiv 1 \pmod{|A_S(\mathbb{Q}_2)|}$.

Since $(\mathbb{Q}_2)^{\mathrm{elem}}_{\{\mathfrak{l},q\}}/\mathbb{Q}_1$ is a $[2,2]$-extension and $\mathfrak{l}^\gamma$ is inert in $\mathbb{Q}_2/\mathbb{Q}_1$, $\mathfrak{l}^\gamma O_{\mathbb{Q}_2}$ splits in the quadratic extension $(\mathbb{Q}_2)^{\mathrm{elem}}_{\{\mathfrak{l},q\}}/\mathbb{Q}_2$ ramified at $\mathfrak{l}O_{\mathbb{Q}_2}$. Hence the conditions (4b), (4c) of Theorem 3.1 are satisfied. If $\left(\frac{q}{\ell}\right)=1$, we have $|A_\Sigma(k_2)|=2$ by Lemma 6.5, and $G_S(\mathbb{Q}_2)$ is nonabelian (i.e., (4a) is also satisfied) by Lemma 6.6. Then Theorem 3.1(4) yields that $G_S(\mathbb{Q}_2)$ is not metacyclic. This is a contradiction. Therefore, $q\equiv 7 \pmod 8$ and $\left(\frac{q}{\ell}\right)=-1$ if $\ell\equiv 9 \pmod{16}$ (i.e., $\left(\frac{2}{\ell}\right)_4=1$). Thus the proof of Theorem 6.3 is completed. □

7. The case of other $S=\{r_1,r_2\}$

This section treats the cases where $S=\{r_1,r_2\}$ and $r_1\equiv r_2 \pmod 4$. First, we consider the case $S=\{\ell_1,\ell_2\}$. The following theorem is a partial refinement of [19, Theorem 2].

Theorem 7.1. *Put $S=\{\ell_1,\ell_2\}$ with two distinct prime numbers $\ell_1\equiv 1 \pmod 4$ and $\ell_2\equiv 1 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if one of the following two conditions holds:*

(1) $\ell_1\equiv\ell_2\equiv 5 \pmod 8$ *and* $|A_\emptyset(\mathbb{Q}_1(\sqrt{\ell_1\ell_2}))|\geq 4$.

(2) $\ell_i\equiv 1 \pmod 8$, $\left(\frac{2}{\ell_i}\right)_4\left(\frac{\ell_i}{2}\right)_4=-1$ *and* $\ell_j\equiv 5 \pmod 8$ *for* $(i,j)=(1,2)$ *or* $(2,1)$, *and* $|A_\emptyset(\mathbb{Q}_1(\sqrt{\ell_1\ell_2}))|=2$.

Proof. Since $\mathrm{r}_2(A_S(\mathbb{Q}))=2$, $G_S(\mathbb{Q}_n)$ is not cyclic for all $n\geq 0$. Put $k=\mathbb{Q}(\sqrt{\ell_1\ell_2})$. Then $2\leq \mathrm{r}_2(A_S(\mathbb{Q}_n))=1+\mathrm{r}_2(A_\emptyset(k_n))$ for all $n\geq 0$ by (3.1) for $(k_n/\mathbb{Q}_n,S_{\mathbb{Q}_n},\emptyset)$. Theorem 4.3 implies that $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is procyclic (i.e., $\mathrm{r}_2(A_\emptyset(k_n))=1$ for all $n\geq 0$) if and only if $\mathrm{r}_2(A_\emptyset(k_1))=1$. Since $\mathrm{r}_2(A_S(\mathbb{Q}_1))=2$ if $G_S(\mathbb{Q}_\infty)$ is prometacyclic, it suffices to consider only the case where $\mathrm{r}_2(A_\emptyset(k_1))=1$. If $\ell_1\equiv\ell_2\equiv 1 \pmod 8$, then $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is not procyclic (cf. e.g. [20, Theorem 3.8]). Hence, replacing (ℓ_1,ℓ_2) by (ℓ_2,ℓ_1) if necessary, we may assume that $\ell_2\equiv 5 \pmod 8$. Then $\mathrm{r}_2(A_\emptyset(k_1))=1$ if and only if $\ell_1\equiv 5 \pmod 8$ or $\ell_1\equiv 1 \pmod 8$ and $\left(\frac{2}{\ell_1}\right)_4\left(\frac{\ell_1}{2}\right)_4=-1$ (cf. [20, Theorem 3.8]).

Assume that $\ell_1\equiv\ell_2\equiv 5 \pmod 8$. Then $A_S(\mathbb{Q})\simeq[2,4]$. Note that γ acts on $O_{\mathbb{Q}_1}/\ell_i\simeq\mathbb{F}_{\ell_i^2}$ as the Frobenius automorphism for each i. Choosing $g_{\ell_1O_{\mathbb{Q}_1}}$ and $g_{\ell_2O_{\mathbb{Q}_1}}$, we obtain the exact sequence

$$E(\mathbb{Q}_1)\xrightarrow{\varphi_{\mathbb{Q}_1,S}}[8_{\ell_1O_{\mathbb{Q}_1}},8_{\ell_2O_{\mathbb{Q}_1}}]\to A_S(\mathbb{Q}_1)\to 0.$$

Since $\mathrm{r}_2(A_S(\mathbb{Q}_1))=2$, $\varphi_{\mathbb{Q}_1,S}(\varepsilon_2)=(a,b)$ with some a, $b\in 2\mathbb{Z}$. Since $(4,4)=\varphi_{\mathbb{Q}_1,S}(-1)=\varphi_{\mathbb{Q}_1,S}(\varepsilon_2^{1+\gamma})=((\ell_1+1)a,(\ell_2+1)b)$, we have $a\equiv b\equiv 2 \pmod 4$. Then $A_S(\mathbb{Q}_1)\simeq[2,8]$, and hence $A_S(\mathbb{Q}_n)/4\simeq[2,4]$ for all $n\geq 0$ by Theorem 4.3. Moreover, $|O_{\mathbb{Q}_1}/\ell_1|\equiv|O_{\mathbb{Q}_1}/\ell_2|\not\equiv 1 \pmod{|A_S(\mathbb{Q}_1)|}$. Since $G_S(\mathbb{Q})$ is nonabelian (cf. Remark 2.2), $G_S(\mathbb{Q}_1)$ is also nonabelian. Moreover, $\ell_2O_{\mathbb{Q}_1}$ splits in $\mathbb{Q}_1(\sqrt{\ell_1})=(\mathbb{Q}_1)^{\mathrm{elem}}_{\{\ell_1\}}$. Hence the conditions (4a), (4b) and (4c) of Theorem 3.1 for $(k_1/\mathbb{Q}_1,S_{\mathbb{Q}_1},\emptyset)$ are satisfied. Since $\mathbb{Q}_S^{\mathrm{ab}}/k$ is a $[2,2]$-extension, we have $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_n)_S^{\mathrm{ab}}/k_n))=2$ for any $n\geq 0$. Hence, if $|A_\emptyset(k_1)|=2$, then $G_S(\mathbb{Q}_1)$ is not metacyclic by Theorem 3.1(4) for $(k_1/\mathbb{Q}_1,S_{\mathbb{Q}_1},\emptyset)$. On the other hand, if $|A_\emptyset(k_1)|\geq 4$, then $|A_\emptyset(k_n)|\geq 4$ for all $n\geq 1$, and hence $G_S(\mathbb{Q}_n)$ is metacyclic for all $n\geq 1$ by Theorem 3.1(3) for $(k_n/\mathbb{Q}_n,S_{\mathbb{Q}_n},\emptyset)$. Therefore $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if $|A_\emptyset(k_1)|\geq 4$.

Assume that $\ell_1\equiv 1 \pmod 8$, $\left(\frac{2}{\ell_1}\right)_4\left(\frac{\ell_1}{2}\right)_4=-1$ and $\ell_2\equiv 5 \pmod 8$. Let $\mathfrak{l}$ be a prime of $\mathbb{Q}_1$ lying over ℓ_1. Choosing $g_{\mathfrak{l}}=g_{\mathfrak{l}^\gamma}=z_{\ell_1}$ and $g_{\ell_2O_{\mathbb{Q}_1}}$, we obtain the exact sequence

$$E(\mathbb{Q}_1) \xrightarrow{\varphi_{\mathbb{Q}_1,S}} [2^m_{\mathfrak{l}}, 2^m_{\mathfrak{l}^\gamma}, 8_{\ell_2 O_{\mathbb{Q}_1}}] \to A_S(\mathbb{Q}_1) \to 0$$

and

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 2^{m-1} & 2^{m-1} & 4 \\ a_0 & a_1 & b \end{pmatrix},$$

where $m = v_2(\ell_1 - 1) \geq 3$. Since $\varepsilon_2^{1+\gamma} = -1$ and $\mathrm{r}_2(A_S(\mathbb{Q}_1)) = 2$, we have $a_0 \equiv a_1 \equiv 1 \pmod 2$ and $b \equiv 2 \pmod 4$. Then $A_S(\mathbb{Q}_1) \simeq [2^m, 4]$, and hence $\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$. For any $n \geq 1$, Theorem 3.1(2) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$ yields that $G_S(\mathbb{Q}_n)$ is metacyclic if and only if $|A_\emptyset(k_n)| = 2$. Theorem 4.3 implies that $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if $|A_\emptyset(k_1)| = 2$. Thus the proof of Theorem 7.1 is completed. □

For a real quadratic field k, the 4-rank $\mathrm{r}_4(A_{\{\infty\}}(k))$ of the narrow class group of k can be calculated by the theorem of Rédei and Reichardt [25] (cf. [1, Proposition 1]), and whether $G_\emptyset(k)$ is abelian or not can be decided by the theorems of Benjamin, Lemmermeyer and Snyder [1]. Hence the two conditions of Theorem 7.1 can be written in the words of power residue symbols as follows.

Lemma 7.2. *Let ℓ_1 and ℓ_2 be distinct prime numbers such that $\ell_1 \equiv 1 \pmod 4$ and $\ell_2 \equiv 5 \pmod 8$. When $\ell_1 \equiv 5 \pmod 8$, we have $|A_\emptyset(\mathbb{Q}_1(\sqrt{\ell_1\ell_2}))| \geq 4$ if and only if $\left(\frac{\ell_1}{\ell_2}\right) = \left(\frac{\ell_1}{\ell_2}\right)_4\left(\frac{\ell_2}{\ell_1}\right)_4 = 1$ or $\left(\frac{\ell_1}{\ell_2}\right) = \left(\frac{2\ell_1}{\ell_2}\right)_4\left(\frac{2\ell_2}{\ell_1}\right)_4\left(\frac{\ell_1\ell_2}{2}\right)_4 = -1$. When $\ell_1 \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell_1}\right)_4\left(\frac{\ell_1}{2}\right)_4 = -1$, we have $|A_\emptyset(\mathbb{Q}_1(\sqrt{\ell_1\ell_2}))| = 2$ if and only if $\left(\frac{\ell_1}{\ell_2}\right) = -1$.*

Proof. Put $k = \mathbb{Q}(\sqrt{\ell_1\ell_2})$ and $k' = \mathbb{Q}(\sqrt{2\ell_1\ell_2})$. Then $\mathrm{r}_2(A_\emptyset(k')) = 2$. Since $(k')_\emptyset^{\mathrm{elem}} = k_1(\sqrt{\ell_1}) \subset (k_1)_\emptyset^{\mathrm{elem}}$, we have $|A_\emptyset(k_1)| = 2$ if and only if $G_\emptyset(k') \simeq [2, 2]$.

Suppose that $\ell_1 \equiv 5 \pmod 8$. Then, since $A_{\{\infty\}}(k') \simeq A_\emptyset(k') \simeq [2, 2]$ by [25] (cf. [1, Proposition 1]), $|A_\emptyset(k_1)| \geq 4$ if and only if $G_\emptyset(k')$ is nonabelian. Hence [1, Theorem 1] implies the claim for the case $\ell_1 \equiv 5 \pmod 8$.

Suppose that $\ell_1 \equiv 1 \pmod 8$ and $\left(\frac{2}{\ell_1}\right)_4\left(\frac{\ell_1}{2}\right)_4 = -1$. If $G_\emptyset(k')$ is abelian and $\left(\frac{\ell_1}{\ell_2}\right) = 1$, we have $N_{k'/\mathbb{Q}}(\varepsilon_{2\ell_1\ell_2}) = -1$ by [1, Theorem 1]. Then $A_\emptyset(k') \simeq A_{\{\infty\}}(k')$, and hence $\mathrm{r}_4(A_\emptyset(k')) \geq 1$ by [25] (cf. [1, Proposition 1]). Hence $\left(\frac{\ell_1}{\ell_2}\right) = -1$ if $G_\emptyset(k') \simeq [2, 2]$. Conversely, if $\left(\frac{\ell_1}{\ell_2}\right) = -1$, then $G_\emptyset(k')$ is abelian and $\mathrm{r}_4(A_\emptyset(k')) = 0$ by [1, Theorem 1] and [25] (cf. [1, Proposition 1]). Thus we obtain Lemma 7.2. □

The next theorem treats the case $S = \{q_1, q_2\}$.

Theorem 7.3. *Put $S = \{q_1, q_2\}$ with two distinct prime numbers $q_1 \equiv 3 \pmod 4$ and $q_2 \equiv 3 \pmod 4$. Then the following two statements hold true:*

(1) *$G_S(\mathbb{Q}_\infty)$ is procyclic if and only if $q_1 \equiv 3 \pmod 8$ or $q_2 \equiv 3 \pmod 8$. Then*

$$G_S(\mathbb{Q}_\infty) \simeq \begin{cases} \mathbb{Z}_2 & \text{if } q_1 \equiv q_2 \equiv 3 \pmod 8, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } q_1 \not\equiv q_2 \pmod 8. \end{cases}$$

(2) *$G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic if and only if $q_1 \equiv q_2 \equiv 7 \pmod 8$ and $q_1 \not\equiv q_2 \pmod{16}$. Then $G_S(\mathbb{Q}_\infty)^{\mathrm{ab}} \simeq [2, 2]$.*

Proof. Put $k = \mathbb{Q}(\sqrt{q_1q_2}) = \mathbb{Q}_S^{\mathrm{ab}}$. For each $n \geq 0$, $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 1 + \mathrm{r}_2(A_\emptyset(k_n))$ by (3.1) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$. Hence $G_S(\mathbb{Q}_\infty)$ is procyclic (i.e., $A_\emptyset(k_n) \simeq 0$ for all n) if and only if $q_1 \equiv 3 \pmod 8$ or $q_2 \equiv 3 \pmod 8$ by [20, Corollary 3.4] (and [23]). If $q_1 \equiv q_2 \equiv 3 \pmod 8$, then $G_S(\mathbb{Q}_\infty)^{\mathrm{ab}}$ is infinite, i.e., $G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}_2$ by

[9, Theorem 1.1]. If $q_1 \not\equiv q_2 \pmod 8$, 2 is inert in $k = \mathbb{Q}_S$. Then, since $A_S(k) \simeq 0$, $G_S(k_\infty)$ is trivial by Proposition 4.1. Therefore $G_S(\mathbb{Q}_\infty) \simeq G_S(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

On the other hand, $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$ (i.e., $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is nontrivial procyclic) if and only if $q_1 \equiv q_2 \equiv 7 \pmod 8$ and $q_i \equiv 7 \pmod{16}$ for $i = 1$ or 2 by [20, Theorem 3.8] and Theorem 4.3. If $G_S(\mathbb{Q}_\infty)$ is nonprocyclic prometacyclic, then $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 1$ by Theorem 4.3. Hence, replacing (q_1, q_2) by (q_2, q_1) if necessary, it suffices to consider only the case where $q_1 \equiv 7 \pmod{16}$ and $q_2 \equiv 7 \pmod 8$ for the second statement.

Lemma 7.4. *Assume* $q_1 \equiv 7 \pmod{16}$ *and* $q_2 \equiv 7 \pmod 8$. *Then* $A_S(\mathbb{Q}_1) \simeq [2,2]$. *Moreover, the primes of* k_1 *lying over* 2 *split in* $(\mathbb{Q}_1)_S^{\mathrm{elem}}$ *if and only if* $q_2 \equiv 7 \pmod{16}$.

Proof. We regard γ as a generator of $\mathrm{Gal}(k_1/k)$. Let $\mathfrak{Q}_i$ be a prime of k_1 lying over q_i. Choosing $z_{q_i} \in \mathbb{Z}$ as the primitive element of $\mathbb{F}_{q_i}$, we obtain the commutative diagram

$$\begin{array}{ccccccc}
E(\mathbb{Q}_1) & \xrightarrow{\varphi_{\mathbb{Q}_1,S}} & [2_{\mathfrak{Q}_1\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_1^\gamma\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_2\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_2^\gamma\cap\mathbb{Q}_1}] & \longrightarrow & A_S(\mathbb{Q}_1) & \longrightarrow & 0 \\
\downarrow\cap & & \| & & \downarrow & & \\
\mathbb{Z}[\frac{1}{\sqrt{2}}]^\times & \xrightarrow{\varphi'_{\mathbb{Q}_1,S}} & [2_{\mathfrak{Q}_1\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_1^\gamma\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_2\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_2^\gamma\cap\mathbb{Q}_1}] & \longrightarrow & A_S(\mathbb{Q}_1)/\langle[\sqrt{2}O_{\mathbb{Q}_1}]\rangle & \longrightarrow & 0
\end{array}$$

with exact rows, where $\varphi'_{\mathbb{Q}_1,S}|_{E(\mathbb{Q}_1)} = \varphi_{\mathbb{Q}_1,S}$ and $\varphi'_{\mathbb{Q}_1,S}(\sqrt{2}) = (a_1, b_1, a_2, b_2)$ with a_i, $b_i \in \mathbb{Z}$ such that $\sqrt{2} \equiv z_{q_i}^{a_i} \pmod{\mathfrak{Q}_i}$ and $\sqrt{2} \equiv z_{q_i}^{b_i} \pmod{\mathfrak{Q}_i^\gamma}$. Since $\varphi_{\mathbb{Q}_1,S}(-1) = (1,1,1,1)$ and $A_{\{q_i\}}(\mathbb{Q}_1) \simeq 0$ (i.e., $\varphi_{\mathbb{Q}_1,\{q_i\}}$ is surjective), we may assume that $\varphi_{\mathbb{Q}_1,S}(\varepsilon_2) = (1,0,1,0)$, replacing $\mathfrak{Q}_i$ by $\mathfrak{Q}_i^\gamma$ if necessary. In particular, we have $A_S(\mathbb{Q}_1) \simeq [2,2]$. Since $z_{q_i}^{a_i} \equiv \sqrt{2}^\gamma \equiv -z_{q_i}^{b_i} \pmod{\mathfrak{Q}_i^\gamma}$, we have $a_i \equiv 1 + b_i \pmod 2$, i.e., $\varphi'_{\mathbb{Q}_1,S}(\varepsilon_2\sqrt{2}) = (b_1, b_1, b_2, b_2)$. Note that $\mathfrak{Q}_i \cap \mathbb{Q}_1$ is inert in $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{\varepsilon_2\sqrt{2}})$ (i.e., $\sqrt{\varepsilon_2\sqrt{2}} \notin \mathbb{Z}_{q_i}$) if and only if $q_i \equiv 7 \pmod{16}$. Hence $b_i \equiv 1 \pmod 2$ if and only if $q_i \equiv 7 \pmod{16}$. Therefore $b_1 \equiv 1 \pmod 2$, and

$$\varphi'_{\mathbb{Q}_1,S}(\sqrt{2}) = \begin{cases} (0,1,0,1) \in \operatorname{Im}\varphi_{\mathbb{Q}_1,S} & \text{if } q_2 \equiv 7 \pmod{16}, \\ (0,1,1,0) \notin \operatorname{Im}\varphi_{\mathbb{Q}_1,S} & \text{if } q_2 \equiv 15 \pmod{16}. \end{cases}$$

This implies that the prime $\sqrt{2}O_{\mathbb{Q}_1}$ splits completely in the $[2,2]$-extension $(\mathbb{Q}_1)_S^{\mathrm{elem}}/\mathbb{Q}_1$ (i.e., $\langle[\sqrt{2}O_{\mathbb{Q}_1}]\rangle \simeq 0$) if and only if $q_2 \equiv 7 \pmod{16}$. Since $\sqrt{2}O_{\mathbb{Q}_1}$ splits in $k_1/\mathbb{Q}_1$, we obtain the claim. $\square$

Assume that $q_1 \equiv 7 \pmod{16}$ and $q_2 \equiv 15 \pmod{16}$. Since $A_{\{q_1\}}(\mathbb{Q}_2) \simeq 0$, the snake lemma for the commutative diagram

$$\begin{array}{ccccccc}
 & & E(\mathbb{Q}_2) \otimes \mathbb{Z}_2 & \xrightarrow{\Phi_{\mathbb{Q}_2,S}} & (O_{\mathbb{Q}_2}/q_1q_2)^\times \otimes \mathbb{Z}_2 & \longrightarrow & A_S(\mathbb{Q}_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow\Psi & & \downarrow & & \\
0 & \longrightarrow & \operatorname{Im}\Phi_{\mathbb{Q}_2,\{q_1\}} & \longrightarrow & (O_{\mathbb{Q}_2}/q_1)^\times \otimes \mathbb{Z}_2 & \longrightarrow & A_{\{q_1\}}(\mathbb{Q}_2) & &
\end{array}$$

with exact rows induces a surjective homomorphism $[2,2,2,2] \simeq (O_{\mathbb{Q}_2}/q_2)^\times \otimes \mathbb{Z}_2 \to A_S(\mathbb{Q}_2)$. Since $\mathrm{r}_2(A_S(\mathbb{Q}_2)) = 2$, this implies that $A_S(\mathbb{Q}_2) \simeq A_S(\mathbb{Q}_1) \simeq [2,2]$. Then $G_S(\mathbb{Q}_\infty)^{\mathrm{ab}} \simeq [2,2]$ by Theorem 4.3, and hence $G_S(\mathbb{Q}_\infty)$ is prometacyclic.

Assume that $q_1 \equiv q_2 \equiv 7 \pmod{16}$. Let $\mathfrak{p}_1$ be a prime of k_1 lying over 2. By Lemma 7.4, $\mathfrak{p}_1$ splits in $(\mathbb{Q}_1)_S^{\mathrm{elem}}$. On the other hand, we have $G_S(\mathbb{Q}_\infty)^{\mathrm{ab}} \simeq \mathbb{Z}_2^2$ by [9, Theorem 1.1]. Hence $G_S(\mathbb{Q}_\infty)$ is abelian if $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Recall that

$\mathrm{r}_2(A_\emptyset(k_n)) = 1$ for all $n \geq 1$. Since the generator of $\mathrm{Gal}(k_n/\mathbb{Q}_n)$ acts on $A_\emptyset(k_n)$ as -1, $\mathrm{Gal}((k_n)_\emptyset^{\mathrm{ab}}/\mathbb{Q}_n)$ is nonabelian if $|A_\emptyset(k_n)| \geq 4$. Suppose that $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Then $|A_\emptyset(k_n)| = 2$ for all $n \geq 1$. In particular, $A_\emptyset(k_n) = A_\emptyset(k_n)^\Gamma$ and $(\mathbb{Q}_1)_S^{\mathrm{elem}} = (k_1)_\emptyset^{\mathrm{ab}}$. Since $N_{k_n/k_1} : A_\emptyset(k_n) \to A_\emptyset(k_1)$ is surjective, we have $A_\emptyset(k_1) = \langle [\mathfrak{p}_1^{h_1/2}] \rangle$ by [8, Theorem 2], where h_1 is the class number of k_1. This implies that $\mathfrak{p}_1$ is inert in $(k_1)_\emptyset^{\mathrm{ab}} = (\mathbb{Q}_1)_S^{\mathrm{elem}}$. This is a contradiction. Therefore $G_S(\mathbb{Q}_\infty)$ is not prometacyclic if $q_1 \equiv q_2 \equiv 7 \pmod{16}$. Thus the proof of Theorem 7.3 is completed. □

Lemma 7.4 above induces the following corollary which we need in the proof of Theorem 1.1.

Corollary 7.5. *Put $k = \mathbb{Q}(\sqrt{q_1 q_2})$ with prime numbers $q_1 \equiv 7 \pmod{16}$ and $q_2 \equiv 15 \pmod{16}$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is finite cyclic.*

Proof. By [20, Theorem 3.8] and Theorem 4.3, we have $\mathrm{r}_2(A_\emptyset(k_n)) = 1$ for all $n \geq 1$. Let $\mathfrak{p}_0$ be a prime of k lying over 2 and $\mathfrak{p}_n$ the prime of k_n lying over $\mathfrak{p}_0$. Put $S = \{q_1, q_2\}$. By Lemma 7.4, $A_S(\mathbb{Q}_1) \simeq [2, 2]$, and $\mathfrak{p}_1$ is inert in $(\mathbb{Q}_1)_S^{\mathrm{elem}} = (k_1)_\emptyset^{\mathrm{elem}}$. Therefore, $\mathfrak{p}_n$ is also inert in $(k_n)_\emptyset^{\mathrm{elem}}$; i.e., $A_\emptyset(k_n) = \langle [\mathfrak{p}_n^{h'_n}] \rangle$ for any $n \geq 1$, where h'_n is the maximal odd factor of the class number of k_n. In particular, $A_\emptyset(k_n) = A_\emptyset(k_n)^\Gamma$ for all $n \geq 1$. Since k_∞ is the unique $\mathbb{Z}_2$-extension of k, $|A_\emptyset(k_n)^\Gamma|$ is bounded as $n \to \infty$ (cf. [8, Proposition 1]), and hence $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is finite cyclic. □

8. The case $S = \{r_1, r_2, r_3\}$

If $G_S(\mathbb{Q}_\infty)$ is prometacyclic for $S = \{r_1, r_2, r_3\}$ (and $\{2, \infty\} \cap S = \emptyset$), then $\mathrm{r}_2(A_S(\mathbb{Q})) \leq 2$, and hence S contains at least one prime $q \equiv 3 \pmod 4$.

Proposition 8.1. *If $S = \{\ell_1, \ell_2, q\}$ with three distinct prime numbers $\ell_1 \equiv 1 \pmod 4$, $\ell_2 \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, then $G_S(\mathbb{Q}_\infty)$ is not prometacyclic.*

Proof. Note that $\mathrm{r}_4(A_S(\mathbb{Q})) = \mathrm{r}_2(A_S(\mathbb{Q})) = 2$. Suppose that $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Then $\mathrm{r}_4(A_S(\mathbb{Q}_1)) = \mathrm{r}_2(A_S(\mathbb{Q}_1)) = 2$, and $(\mathbb{Q}_\infty)_S^{\mathrm{elem}}/\mathbb{Q}_\infty$ is a $[2, 2]$-extension. For each $i \in \{1, 2\}$, since $\mathbb{Q}_\infty(\sqrt{\ell_i}) \subset (\mathbb{Q}_\infty)_{\{\ell_i\}}^{\mathrm{elem}}$, we have $(\mathbb{Q}_\infty)_S^{\mathrm{elem}} \neq (\mathbb{Q}_\infty)_{S\setminus\{\ell_i\}}^{\mathrm{elem}}$, and hence $(\mathbb{Q}_\infty)_{S\setminus\{\ell_i\}}^{\mathrm{elem}}/\mathbb{Q}_\infty$ is a quadratic extension; i.e., $G_{S\setminus\{\ell_i\}}(\mathbb{Q}_\infty)$ is procyclic. Proposition 6.2 yields that $\ell_1 \equiv \ell_2 \equiv 5 \pmod 8$. Put $k = \mathbb{Q}(\sqrt{\ell_1 \ell_2})$ and $\Sigma = \{q\}$. Since $G_{\{\ell_1, \ell_2\}}(\mathbb{Q}_\infty)$ is also prometacyclic, we have $|A_\Sigma(k_1)| \geq |A_\emptyset(k_1)| \geq 4$ by Theorem 7.1. Then $G_S(\mathbb{Q}_1)$ is not metacyclic by Theorem 3.1(2) for $(k_1/\mathbb{Q}_1, S_{\mathbb{Q}_1}, \Sigma_{\mathbb{Q}_1})$. This is a contradiction. Thus we obtain the statement. □

Theorem 8.2. *Put $S = \{\ell, q_1, q_2\}$ with three distinct prime numbers $\ell \equiv 1 \pmod 4$, $q_1 \equiv 3 \pmod 4$ and $q_2 \equiv 3 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if one of the following two conditions holds true:*

(1) *$\ell \equiv 5 \pmod 8$, $q_1 \equiv q_2 \equiv 3 \pmod 8$, $\left(\frac{q_1 q_2}{\ell}\right) = -1$.*
(2) *$\ell \equiv 5 \pmod 8$, $q_i \equiv 3 \pmod 8$, $q_j \equiv 7 \pmod 8$, $\left(\frac{q_j}{\ell}\right) = -1$ for $(i, j) = (1, 2)$ or $(2, 1)$.*

Moreover, we have $G_\emptyset(\mathbb{Q}_\infty(\sqrt{\ell q_1 q_2})) \simeq \mathbb{Z}/2\mathbb{Z}$ under each of these conditions.

Proof. Put $k = \mathbb{Q}(\sqrt{\ell q_1 q_2})$. For each $n \geq 0$, $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 1 + \mathrm{r}_2(A_\emptyset(k_n)) \geq 2$ by (3.1) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$. Then $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 0$ (i.e., $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is procyclic) if and only if $\ell \equiv 5 \pmod 8$ and $q_i \equiv 3 \pmod 8$ for $i = 1$ or 2 by

[20, Theorem 3.8]. Since $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ for all $n \geq 0$ if $G_S(\mathbb{Q}_\infty)$ is prometacyclic, it suffices to consider only this case. Replacing (q_1, q_2) by (q_2, q_1) if necessary, we may assume that $\ell \equiv 5 \pmod 8$ and $q_1 \equiv 3 \pmod 8$. Then, since $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$, we have $(\mathbb{Q}_n)^{\mathrm{elem}}_{S_{\mathbb{Q}_n}\setminus\{\mathfrak{l}\}} = \mathbb{Q}_n(\sqrt{\ell})$ for $\mathfrak{l} = q_1 O_{\mathbb{Q}_n}$ by Theorem 3.1(1). Since $\mathbb{Q}^{\mathrm{ab}}_{\{\ell,q_1\}}\mathbb{Q}_n/\mathbb{Q}_n$ is a cyclic quartic extension which contains $\mathbb{Q}_n(\sqrt{\ell})$, Theorem 3.1(2) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \emptyset)$ yields that $G_S(\mathbb{Q}_n)$ is metacyclic if and only if $|A_\emptyset(k_n)| = 2$. Theorem 4.3 implies that $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if $|A_\emptyset(k_1)| = 2$. Put $k' = \mathbb{Q}(\sqrt{2\ell q_1 q_2})$. Since $(k')^{\mathrm{elem}}_\emptyset = k_1(\sqrt{\ell}) \subset (k_1)^{\mathrm{elem}}_\emptyset$, we have $|A_\emptyset(k_1)| = 2$ if and only if $G_\emptyset(k') \simeq [2,2]$. By the theorem of Rédei and Reichardt [25] (or [2, Proposition 1]), $A_\emptyset(k') \simeq [2,2]$ if and only if at least one of $\left(\frac{2}{q_2}\right)$, $\left(\frac{q_1}{\ell}\right)$, $\left(\frac{q_2}{\ell}\right)$ is 1. Then $G_\emptyset(k') \simeq [2,2]$ if and only if $\left(\frac{2}{q_2}\right) = \left(\frac{q_1 q_2}{\ell}\right) = -1$ or $\left(\frac{2}{q_2}\right) = -\left(\frac{q_2}{\ell}\right) = 1$ by [1, Theorem 2] (or [2, Theorem 2]). Thus the proof of Theorem 8.2 is completed. □

Theorem 8.3. *Put $S = \{q_1, q_2, q_3\}$ with three distinct prime numbers $q_1 \equiv 3 \pmod 4$, $q_2 \equiv 3 \pmod 4$ and $q_3 \equiv 3 \pmod 4$. Then $G_S(\mathbb{Q}_\infty)$ is prometacyclic if and only if $q_1 \equiv q_2 \equiv 3 \pmod 8$, $q_3 \equiv 7 \pmod 8$ and $\left(\frac{q_1 q_2}{q_3}\right) = -1$ after a suitable permutation of the indices.*

Proof. Since $(\mathbb{Q}_\infty)^{\mathrm{ab}}_{S\setminus\{q_i\}} \cap (\mathbb{Q}_\infty)^{\mathrm{ab}}_{S\setminus\{q_j\}} = \mathbb{Q}_\infty$ for any distinct i and j, $G_{S\setminus\{q_i\}}(\mathbb{Q}_\infty)^{\mathrm{ab}}$ is procyclic for any i if $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Theorem 7.3 implies that $G_{S\setminus\{q_i\}}(\mathbb{Q}_\infty)^{\mathrm{ab}}$ is procyclic for any i if and only if at least two $q \in S$ satisfy $q \equiv 3 \pmod 8$. If all of $q \in S$ satisfy $q \equiv 3 \pmod 8$, $G_S(\mathbb{Q}_\infty)$ has a quotient $G_{S\setminus\{q_1\}}(\mathbb{Q}_\infty) \times G_{S\setminus\{q_2\}}(\mathbb{Q}_\infty) \simeq \mathbb{Z}_2^2$ by Theorem 7.3. Then, since $G_S(\mathbb{Q})$ is nonabelian (cf. Remark 2.2), $G_S(\mathbb{Q}_\infty)$ is not prometacyclic. Hence, permuting the indices if necessary, it suffices to consider only the case where $q_1 \equiv q_2 \equiv 3 \pmod 8$ and $q_3 \equiv 7 \pmod 8$. Then, since the inertia group $I_{q_2} \subset G_S(\mathbb{Q}_n)^{\mathrm{ab}}$ of the prime $q_2 O_{\mathbb{Q}_n}$ is cyclic and $G_S(\mathbb{Q}_n)^{\mathrm{ab}}/I_{q_2} \simeq A_{\{q_1,q_3\}}(\mathbb{Q}_n) \simeq \mathbb{Z}/2\mathbb{Z}$ by Theorem 7.3, we have $\mathrm{r}_2(A_S(\mathbb{Q}_n)) = 2$ and $\mathrm{r}_4(A_S(\mathbb{Q}_n)) \leq 1$ for all $n \geq 0$.

Put $k = \mathbb{Q}(\sqrt{q_1 q_2})$ and $k' = \mathbb{Q}(\sqrt{2 q_1 q_2})$. Then $A_\emptyset(k_n) \simeq 0$ for all $n \geq 0$ by [23, Theorem]. We regard γ as the generator of $\mathrm{Gal}(k_1/k)$. Since $-1 = \varepsilon_2^{1+\gamma} \in E(k_1)^{1+\gamma}$, the genus formula (2.1)

$$1 = |A_\emptyset(k_1)| \geq \frac{2^2}{2|E(k)/E(k_1)^{1+\gamma}|}$$

for k_1/k yields that $\pm\varepsilon_{q_1 q_2} \notin E(k_1)^{1+\gamma}$. Hence Kuroda's formula (2.3)

$$1 = |A_\emptyset(k_1)| = 4^{-1} Q(k_1/\mathbb{Q}) |A_\emptyset(\mathbb{Q}_1)||A_\emptyset(k)||A_\emptyset(k')| = 2^{-1} Q(k_1/\mathbb{Q})$$

implies that $E(k_1) = \langle -1, \varepsilon_2, \varepsilon_{q_1 q_2}, \sqrt{\varepsilon_{2 q_1 q_2}} \rangle$. Let $\mathfrak{Q}_i$ be a prime of k_1 lying over q_i. Then $\mathfrak{Q}_i \cap \mathbb{Q}_1 = q_i O_{\mathbb{Q}_1}$ for $i \in \{1, 2\}$. Choosing $g_{q_1 O_{\mathbb{Q}_1}}$, $g_{q_2 O_{\mathbb{Q}_1}}$ and $g_{\mathfrak{Q}_3 \cap \mathbb{Q}_1} = g_{\mathfrak{Q}_3^\gamma \cap \mathbb{Q}_1} = z_{q_3} \in \mathbb{Z}$, we obtain the exact sequence

$$E(\mathbb{Q}_1) \xrightarrow{\varphi_{\mathbb{Q}_1,S}} [8_{q_1 O_{\mathbb{Q}_1}}, 8_{q_2 O_{\mathbb{Q}_1}}, 2_{\mathfrak{Q}_3 \cap \mathbb{Q}_1}, 2_{\mathfrak{Q}_3^\gamma \cap \mathbb{Q}_1}] \to A_S(\mathbb{Q}_1) \to 0.$$

Since $\mathrm{Coker}\, \varphi_{\mathbb{Q}_1,\{q_i\}} \simeq A_{\{q_i\}}(\mathbb{Q}_1) \simeq 0$ for all $i \in \{1,2,3\}$, replacing $\mathfrak{Q}_3$ by $\mathfrak{Q}_3^\gamma$ if necessary, we may assume that

$$v_{\mathbb{Q}_1,S} = \begin{pmatrix} \varphi_{\mathbb{Q}_1,S}(-1) \\ \varphi_{\mathbb{Q}_1,S}(\varepsilon_2) \end{pmatrix} = \begin{pmatrix} 4 & 4 & 1 & 1 \\ a_1 & a_2 & 0 & 1 \end{pmatrix}$$

with $a_1 \equiv a_2 \equiv 1 \pmod 2$. Hence an easy calculation shows that $A_S(\mathbb{Q}_1) \simeq [2, 8]$ and $A_{\{q_1,q_2\}}(\mathbb{Q}_1) \simeq \mathbb{Z}/8\mathbb{Z}$. This implies that $\mathrm{r}_2(\mathrm{Gal}((\mathbb{Q}_n)_S^{\mathrm{ab}}/k_n)) = 2$ for all $n \geq 1$. Moreover, we have $\mathrm{r}_4(A_S(\mathbb{Q}_n)) = 1$ for all $n \geq 1$. Put $\Sigma = \{q_3\}$. Then (3.1) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \Sigma_{\mathbb{Q}_n})$ yields that $\mathrm{r}_2(A_\Sigma(k_n)) = 1$ for all $n \geq 0$.

Assume that $\left(\frac{q_1q_2}{q_3}\right) = -1$. We choose $g_{\mathfrak{Q}_3} = g_{\mathfrak{Q}_3^\gamma} = g_{q_3O_k}$ and $g_{q_3O_{k'}}$ such that $g_{q_3O_{k'}} \equiv g_{\mathfrak{Q}_3} \pmod{\mathfrak{Q}_3}$. Then $g_{q_3O_k}^{(1+q_3)u} \equiv z_{q_3} \pmod{q_3}$ with some odd u. Moreover, since $g_{q_3O_{k'}}^\gamma \equiv g_{q_3O_{k'}}^{q_3} \pmod{q_3}$, we have $g_{q_3O_{k'}} \equiv g_{\mathfrak{Q}_3^\gamma}^{q_3} \pmod{\mathfrak{Q}_3^\gamma}$. Then we obtain the commutative diagram

$$\begin{tikzcd}
E(\mathbb{Q}_1) \arrow[r, "\varphi_{\mathbb{Q}_1,\Sigma}"] \arrow[d, "\cap"] & {[2_{\mathfrak{Q}_3\cap\mathbb{Q}_1}, 2_{\mathfrak{Q}_3^\gamma\cap\mathbb{Q}_1}]} \arrow[r] \arrow[d, "\psi_{\mathbb{Q}_1}"] & 0 & & \\
E(k_1) \arrow[r, "\varphi_{k_1,\Sigma}"] & {[2^m_{\mathfrak{Q}_3}, 2^m_{\mathfrak{Q}_3^\gamma}]} \arrow[r] & A_\Sigma(k_1) \arrow[r] & 0 & \\
E(k) \arrow[r, "\varphi_{k,\Sigma}"] \arrow[u, "\cup"] & \mathbb{Z}/2^m\mathbb{Z} \arrow[r] \arrow[u, "\psi_k"] & A_\Sigma(k) \arrow[r] & 0 & \\
E(k') \arrow[r, "\varphi_{k',\Sigma}"] \arrow[uu, bend left=60, "\cup"] & \mathbb{Z}/2^m\mathbb{Z} \arrow[r] \arrow[uu, bend right=60, "\psi_{k'}"'] & A_\Sigma(k') \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $m = v_2(q_3^2 - 1) \geq 4$, $\psi_{\mathbb{Q}_1}(x_0, x_1) = (2^{m-1}x_0, 2^{m-1}x_1)$, $\psi_k(x) = (x, x)$, and $\psi_{k'}(x) = (x, q_3x) = (x, (2^{m-1}-1)x)$. Since $k(\sqrt{q_1q_3}) \subset k_\Sigma^{\mathrm{ab}}$ and $k_1(\sqrt{q_1q_3}) \subset (k')_\Sigma^{\mathrm{ab}}$, we have $|A_\Sigma(k)| \geq 2$ and $|A_\Sigma(k')| \geq 4$. Hence $\varphi_{k,\Sigma}(\varepsilon_{q_1q_2}) = (2a)$ and $\varphi_{k',\Sigma}(\varepsilon_{2q_1q_2}) = (2b)$ with some a, $b \in \mathbb{Z}$. Then

$$v_{k_1,\Sigma} = \begin{pmatrix} \varphi_{k_1,\Sigma}(-1) \\ \varphi_{k_1,\Sigma}(\varepsilon_2) \\ \varphi_{k_1,\Sigma}(\varepsilon_{q_1q_2}) \\ \varphi_{k_1,\Sigma}(\sqrt{\varepsilon_{2q_1q_2}}) \end{pmatrix} = \begin{pmatrix} 2^{m-1} & 2^{m-1} \\ 0 & 2^{m-1} \\ 2a & 2a \\ b + 2^{m-1}e_0 & -b + 2^{m-1}e_1 \end{pmatrix}$$

with some e_0, $e_1 \in \{0, 1\}$. Since $\mathrm{r}_2(A_\Sigma(k_1)) = 1$, we have $b \equiv 1 \pmod 2$. Then

$$\begin{pmatrix} 1 & 0 & 0 & 2^{m-1} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2a \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{e_0}{b} & \frac{e_0+e_1}{b} & 0 & b^{-1} \end{pmatrix} v_{k_1,\Sigma} = \begin{pmatrix} 0 & 0 \\ 0 & 2^{m-1} \\ 0 & 4a \\ 1 & -1 \end{pmatrix},$$

and hence $|A_\Sigma(k_1)| \geq 4$. By Theorem 3.1(3) for $(k_n/\mathbb{Q}_n, S_{\mathbb{Q}_n}, \Sigma_{\mathbb{Q}_n})$, $G_S(\mathbb{Q}_n)$ is metacyclic for any $n \geq 1$. Therefore $G_S(\mathbb{Q}_\infty)$ is prometacyclic if $\left(\frac{q_1q_2}{q_3}\right) = -1$.

Assume that $\left(\frac{q_1q_2}{q_3}\right) = 1$. Then q_3 splits completely in $k_1/\mathbb{Q}$. Since there is a surjective homomorphism $[2_{\mathfrak{Q}_3}, 2_{\mathfrak{Q}_3^\sigma}, 2_{\mathfrak{Q}_3^\gamma}, 2_{\mathfrak{Q}_3^{\sigma\gamma}}] \to A_\Sigma(k_1)$, we have $|A_\Sigma(k_1)| = 2$. We apply Theorem 3.1 for $(k_1/\mathbb{Q}_1, S_{\mathbb{Q}_1}, \Sigma_{\mathbb{Q}_1})$. Since $G_S(\mathbb{Q})$ is nonabelian (cf. Remark 2.2), $G_S(\mathbb{Q}_1)$ is also nonabelian. For each $i \in \{1, 2\}$, $|O_{\mathbb{Q}_1}/q_i| = q_i^2 \not\equiv 1 \pmod{|A_S(\mathbb{Q}_1)|}$. By Theorem 3.1(1), $(\mathbb{Q}_1)^{\mathrm{elem}}_{S_{\mathbb{Q}_1}\setminus\{\mathfrak{l}_0\}} = \mathbb{Q}_1(\sqrt{q_1q_3})$ for $\mathfrak{l}_0 = q_2O_{\mathbb{Q}_1}$. Since $\mathbb{Q}_1(\sqrt{q_1q_3})/\mathbb{Q}$ is a $[2, 2]$-extension, the prime $q_2O_{\mathbb{Q}_1}$ splits in $\mathbb{Q}_1(\sqrt{q_1q_3})$. Hence no prime in $S_{\mathbb{Q}_1} \setminus \Sigma_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{q_1q_3})/\mathbb{Q}_1$. By Theorem 3.1(4), $G_S(\mathbb{Q}_1)$ is not metacyclic. Therefore $G_S(\mathbb{Q}_\infty)$ is not prometacyclic if $\left(\frac{q_1q_2}{q_3}\right) = 1$. Thus the proof of Theorem 8.3 is completed. □

9. The case $\infty \in S$

For a finite extension $k/\mathbb{Q}$, the Iwasawa λ-invariant $\lambda(k)$ is defined as the 2-rank of the maximal free abelian pro-2 quotient of $G_\emptyset(k_\infty)$. Then there is a surjective homomorphism $G_\emptyset(k_\infty)^{\mathrm{ab}} \to \mathbb{Z}_2^{\lambda(k)}$ with torsion kernel. First, we prepare the following lemma.

Lemma 9.1. *Let S be a finite set of primes of $\mathbb{Q}$ not containing 2 and $K/\mathbb{Q}$ a finite extension such that $K_\infty \subset (\mathbb{Q}_\infty)_S$. If $G_S(\mathbb{Q}_\infty)$ is prometacyclic, then $\lambda(K) \leq 1$.*

Proof. Assume that $\lambda(K) \geq 2$. Then there are surjective homomorphisms $G_S(K_\infty) \to G_\emptyset(K_\infty)^{\mathrm{ab}} \to \mathbb{Z}_2^2$. Suppose that $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Then there exists a procyclic extension $M/\mathbb{Q}_\infty$ such that $(\mathbb{Q}_\infty)_S/M$ is also a procyclic extension. Moreover, since $G_S(K_\infty)$ is also prometacyclic, we have $G_S(K_\infty) \simeq \mathbb{Z}_2^2$. Then $(\mathbb{Q}_\infty)_S = (K_\infty)_\emptyset^{\mathrm{ab}}$.

$$\begin{tikzcd}[arrows=dash]
 & & (\mathbb{Q}_\infty)_S \arrow[d] \\
 & K_\infty \arrow[r] \arrow[d] & K_\infty M \arrow[d] \\
\mathbb{Q}_\infty \arrow[r] & K_\infty \cap M \arrow[r] & M
\end{tikzcd}$$

Hence $K_\infty M/K_\infty$ is an unramified $\mathbb{Z}_2$-extension. Since $[K_\infty : K_\infty \cap M] \leq [K : \mathbb{Q}]$, any prime has finite ramification index in $K_\infty M/(K_\infty \cap M)$. On the other hand, since $G_{\{\infty\}}(\mathbb{Q}_\infty) \simeq 1$ (cf. Corollary 4.2) and $M/(K_\infty \cap M)$ is also a $\mathbb{Z}_2$-extension, $M/\mathbb{Q}_\infty$ is a $\mathbb{Z}_2$-extension totally ramified at some $v \in S_{\mathbb{Q}_\infty}$. Then the primes lying over v have infinite ramification indices in $K_\infty M/(K_\infty \cap M)$. This is a contradiction. Therefore $G_S(\mathbb{Q}_\infty)$ is not prometacyclic if $\lambda(K) \geq 2$. Thus the proof is completed. $\square$

We recall Kida's formulas [12] for the λ-invariants. Suppose that $k/\mathbb{Q}$ is an imaginary abelian extension unramified at 2. Then $k \cap \mathbb{Q}_\infty = \mathbb{Q}$, $\sqrt{-1} \notin k_\infty$ and the μ-invariant is zero (cf. [12, Remarks (i)] or [29, §7.5]). By [12, Theorem 1], we have

$$\lambda(k) = \lambda(k^+) + \mathrm{r}_2(A_{\{\infty\}}(k_n^+)) - 1 + s(k_n/k_n^+) \tag{9.1}$$

for all sufficiently large n, where $k^+ = k \cap \mathbb{R}$, and $s(k_n/k_n^+)$ denotes the number of prime ideals of k_n ramified over k_n^+. Moreover, $G_\emptyset(k_\infty)^{\mathrm{ab}} \simeq \mathbb{Z}_2^{\lambda(k)}$ if k is an imaginary quadratic field with odd discriminant (cf. [6] or [11, Theorem 1]). Let K be a CM-field such that K/k is a finite 2-extension. Suppose that $K_\infty/\mathbb{Q}_\infty$ is unramified at any prime lying over 2. Then $\sqrt{-1} \notin K_\infty$, and we have

$$\lambda(K) - \lambda(K^+) = [K_\infty : k_\infty](\lambda(k) - \lambda(k^+)) + \textstyle\sum_v (e_v - 1) - \sum_{v^+} (e_{v^+} - 1) \tag{9.2}$$

by [12, Theorem 3], where $K^+ = K \cap \mathbb{R}$, v (resp. v^+) runs over all nonarchimedean primes of K_∞ (resp. K_∞^+), and e_v (resp. e_{v^+}) is the ramification index of v in K_∞/k_∞ (resp. v^+ in K_∞^+/k_∞^+). Using these formulas, we obtain the following theorem.

Theorem 9.2. *Let Σ be a finite set of odd prime numbers, and put $S = \Sigma \cup \{\infty\}$. Then the following two statements hold true:*

(1) $G_S(\mathbb{Q}_\infty)$ *is nontrivial procyclic if and only if* $\Sigma = \{r\}$ *and* $\left(\frac{2}{r}\right) = -1$. *Then* $G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}_2/(r-1)\mathbb{Z}_2$.

(2) $G_S(\mathbb{Q}_\infty)$ *is nonprocyclic prometacyclic if and only if* $\Sigma = \{q\}$ *and* $q \equiv 7 \pmod{16}$. *Then* $G_S(\mathbb{Q}_\infty)$ *is isomorphic to a prodihedral pro-2 group* $\mathbb{Z}_2 \rtimes (\mathbb{Z}/2\mathbb{Z})$.

Proof. If $G_S(\mathbb{Q}_\infty)$ is nontrivial prometacyclic, then $|\Sigma| = \mathrm{r}_2(G_S(\mathbb{Q})^{\mathrm{ab}}) \leq 2$. Moreover, $\Sigma \neq \emptyset$ by Corollary 4.2. Hence it suffices to consider the case $1 \leq |\Sigma| \leq 2$.

Assume that $\Sigma = \{r\}$ and $\left(\frac{2}{r}\right) = -1$. Then 2 does not split in $k = \mathbb{Q}_S^{\mathrm{ab}}$. Since $k/\mathbb{Q}$ is cyclic, we have $k = \mathbb{Q}_S$. Since $G_S(k)^{\mathrm{ab}} \simeq 0$, $G_S(k_\infty)$ is trivial by Proposition 4.1. This implies that $(\mathbb{Q}_\infty)_S = k_\infty$. Hence $G_S(\mathbb{Q}_\infty) \simeq G_S(\mathbb{Q})^{\mathrm{ab}} \simeq \mathbb{Z}_2/(r-1)\mathbb{Z}_2$.

Assume that $\Sigma = \{\ell\}$ and $\ell \equiv 1 \pmod 8$. Put $k = \mathbb{Q}_S^{\mathrm{ab}}$. Then $k/\mathbb{Q}$ is a cyclic extension totally ramified at ℓ, and hence $s(k_1/k_1^+) = |\Sigma_{\mathbb{Q}_1}| = 2$. Since $|A_{\{\infty\}}(\mathbb{Q}(\sqrt{2\ell}))| \geq 4$ (cf. [30]), we have $|A_{\{\infty\}}(k_1^+)| \geq |A_{\{\infty\}}(\mathbb{Q}_1(\sqrt{\ell}))| \geq 2$. Then $\lambda(k) \geq \mathrm{r}_2(A_{\{\infty\}}(k_1^+)) - 1 + s(k_1/k_1^+) \geq 2$ by (9.1), and hence $G_S(\mathbb{Q}_\infty)$ is not prometacyclic by Lemma 9.1.

Assume that $\Sigma = \{q\}$ and $q \equiv 7 \pmod 8$. Put $k = \mathbb{Q}(\sqrt{-q})$. Since $A_\Sigma(\mathbb{Q}_n) \simeq 0$, the commutative diagram

$$\begin{array}{ccccccc}
E(k_n) & \xrightarrow{\Phi_{k_n,\Sigma}} & (O_{k_n}/\sqrt{-q})^\times \otimes \mathbb{Z}_2 & \longrightarrow & A_\Sigma(k_n) & \longrightarrow & A_\emptyset(k_n) \longrightarrow 0 \\
\| & & \simeq\uparrow & & & & \\
E(\mathbb{Q}_n) & \xrightarrow{\Phi_{\mathbb{Q}_n,\Sigma}} & (O_{\mathbb{Q}_n}/q)^\times \otimes \mathbb{Z}_2 & \longrightarrow & A_\Sigma(\mathbb{Q}_n) & \longrightarrow & 0
\end{array}$$

with exact rows yields that $G_S(k_n)^{\mathrm{ab}} \simeq A_\Sigma(k_n) \simeq A_\emptyset(k_n)$ for all $n \geq 0$. Hence $G_S(k_\infty)^{\mathrm{ab}} \simeq \varprojlim A_\emptyset(k_n) \simeq \mathbb{Z}_2^{\lambda(k)}$. If $q \equiv 15 \pmod{16}$, then $\lambda(k) \geq -1 + s(k_2/\mathbb{Q}_2) = 3$ by (9.1), and hence $G_S(\mathbb{Q}_\infty)$ is not prometacyclic by Lemma 9.1. Suppose that $q \equiv 7 \pmod{16}$. Then $\lambda(k) = 1$ by (9.1) (or [6, Theorem 7]). Since $A_\emptyset(\mathbb{Q}_n) \simeq 0$ for all $n \geq 0$, the generator of $\mathrm{Gal}(k_\infty/\mathbb{Q}_\infty)$ acts on $G_S(k_\infty) \simeq \varprojlim A_\emptyset(k_n) \simeq \mathbb{Z}_2$ as -1. Therefore $G_S(\mathbb{Q}_\infty)$ is prodihedral if $q \equiv 7 \pmod{16}$.

Assume that $\Sigma = \{\ell_1, \ell_2\}$ and $\ell_1 \equiv \ell_2 \equiv 1 \pmod 4$. If $\left(\frac{2}{\ell_1}\right) = 1$ or $\left(\frac{2}{\ell_2}\right) = 1$, then we have seen that $G_{\{\ell_i,\infty\}}(\mathbb{Q}_\infty)$ is not prometacyclic. Put $k = \mathbb{Q}(\sqrt{\ell_1\ell_2})$. If $\ell_1 \equiv \ell_2 \equiv 5 \pmod 8$ and $|A_\emptyset(k_2)| = 2$, then $G_\Sigma(\mathbb{Q}_\infty)$ is not prometacyclic by Theorem 7.1. Note that $\mathbb{Q}_S^{\mathrm{ab}} \cap k(\sqrt{\ell_1})_\emptyset^{\mathrm{ab}} = k(\sqrt{\ell_1}) = k_\emptyset^{\mathrm{elem}}$. If $\ell_1 \equiv \ell_2 \equiv 5 \pmod 8$ and $|A_\emptyset(k_2)| \geq 4$, then $\mathbb{Q}_S^{\mathrm{ab}}L/k_2(\sqrt{\ell_1})$ is a $[2,2,2]$-extension unramified outside S, where L is an unramified quartic extension of k_2. Therefore $G_S(\mathbb{Q}_\infty)$ is not prometacyclic.

Assume that $\Sigma = \{\ell, q\}$ and $\ell \not\equiv q \equiv 3 \pmod 4$. Put $k = \mathbb{Q}(\sqrt{-q})$ and $K = \mathbb{Q}_S^{\mathrm{ab}}$. Then K_∞/k_∞ and $K_\infty^+/\mathbb{Q}_\infty$ are cyclic extensions unramified outside ℓ and totally ramified at any prime lying over ℓ. Since any prime of $\mathbb{Q}_\infty$ lying over ℓ splits in k_∞, we have $\lambda(K) \geq \sum_{v^+|\ell}(e_{v^+} - 1) \geq \sum_{v^+|\ell} 3 \geq 3$ by (9.2). Hence $G_S(\mathbb{Q}_\infty)$ is not prometacyclic by Lemma 9.1.

Assume that $\Sigma = \{q_1, q_2\}$ and $q_1 \equiv q_2 \equiv 3 \pmod 4$. Since $(\mathbb{Q}_\infty)_{\{q_1,\infty\}} \cap (\mathbb{Q}_\infty)_{\{q_2,\infty\}} = \mathbb{Q}_\infty$, $G_{\{q_1,\infty\}}(\mathbb{Q}_\infty)$ and $G_{\{q_2,\infty\}}(\mathbb{Q}_\infty)$ are procyclic if $G_S(\mathbb{Q}_\infty)$ is prometacyclic. We have seen that $G_{\{q_i,\infty\}}(\mathbb{Q}_\infty)$ is not procyclic if $q_i \equiv 7 \pmod 8$. Hence $G_S(\mathbb{Q}_\infty)$ is not prometacyclic if $\left(\frac{2}{q_1}\right) = 1$ or $\left(\frac{2}{q_2}\right) = 1$. Suppose that $q_1 \equiv q_2 \equiv 3 \pmod 8$. Then q_1 and q_2 are primes in $\mathbb{Q}_\infty$. Since $G_\Sigma(\mathbb{Q}_\infty) \simeq \mathbb{Z}_2$

by Theorem 7.3, there is a 2-extension $K^+/\mathbb{Q}$ such that $\mathbb{Q}(\sqrt{q_1 q_2}) \subset K^+$ and K^+_∞ is the unique cyclic quartic extension of $\mathbb{Q}_\infty$ unramified outside Σ. Then $K^+_\infty/\mathbb{Q}_\infty$ is totally ramified at q_1 and q_2. Put $k = \mathbb{Q}(\sqrt{-q_2})$, $k' = \mathbb{Q}(\sqrt{-q_1})$ and $K = K^+k = K^+k'$. Note that q_1 (resp. q_2) splits in $k_\infty/\mathbb{Q}_\infty$ (resp. $k'_\infty/\mathbb{Q}_\infty$). Then $\lambda(K) \geq \sum_{v|q_1} 3 + \sum_{v|q_2} 1 - \sum_{v^+ \in \Sigma} 3 = 2$ by (9.2) for K/k, and hence $G_S(\mathbb{Q}_\infty)$ is not prometacyclic by Lemma 9.1. Thus the proof of Theorem 9.2 is completed. □

10. Proof of Theorem 1.1

By Corollary 4.2, $G_S(\mathbb{Q}_\infty)$ is trivial if and only if $S \subset \{\infty\}$ or $S = \{q\}$ and $q \equiv 3 \pmod 4$ (i.e., $G_S(\mathbb{Q})$ is trivial). Then $G_\emptyset(K_\infty)$ is trivial for such S and $K \subset (\mathbb{Q}_\infty)_S = \mathbb{Q}_\infty$. The statement for the case $\infty \in S$ has been obtained as Theorem 9.2. In the following, we assume that $\infty \notin S$ and $G_S(\mathbb{Q}_\infty)$ is nontrivial. If $G_S(\mathbb{Q}_\infty)$ is nontrivial prometacyclic, $G_S(\mathbb{Q})$ is also nontrivial metacyclic. Then $1 \leq \mathrm{r}_2(A_S(\mathbb{Q})) \leq 2$, and hence $S = \{\ell\}$, $\{r_1, r_2\}$ or $\{r_1, r_2, q\}$, where $\ell \equiv -q \equiv 1 \pmod 4$. Thus we obtain the list of all S with prometacyclic $G_S(\mathbb{Q}_\infty)$, combining the following:

- Proposition 5.1 and Theorem 5.2 for $S = \{\ell\}$.
- Proposition 6.2 and Theorem 6.3 for $S = \{r_1, r_2\}$ with $r_1 \not\equiv r_2 \pmod 4$.
- Theorem 7.1 (with Lemma 7.2) and Theorem 7.3 for $S = \{r_1, r_2\}$ with $r_1 \equiv r_2 \pmod 4$.
- Proposition 8.1, Theorem 8.2 and Theorem 8.3 for $S = \{r_1, r_2, q\}$.

Put $G = G_S(\mathbb{Q}_\infty)$. Recall that Γ has a generator $\gamma = \overline{\gamma}|_{\mathbb{Q}_\infty}$, where $\overline{\gamma}$ is a generator of $\overline{\Gamma}$ such that $\overline{\gamma}(\zeta_{2^{n+2}}) = \zeta_{2^{n+2}}^5$ for all $n \geq 0$. Put $n_r = v_2(\frac{r^2-1}{8}) \geq 0$ for $r \in S$. Then the decomposition field of r in $\mathbb{Q}_\infty/\mathbb{Q}$ is $\mathbb{Q}_{n_r}$. Let $\mathfrak{r}$ be a prime of $\mathbb{Q}_{n_r}$ lying over r. Suppose that $n > n_r$. Since $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}_{n_r}$ is not a cyclic extension and $\mathfrak{r}$ does not split in $\mathbb{Q}_n/\mathbb{Q}_{n_r}$, $\mathfrak{r}O_{\mathbb{Q}_n}$ splits in $\mathbb{Q}(\zeta_{2^{n+2}}) = \mathbb{Q}_n(\sqrt{-1})$. Let $\mathfrak{R}$ be a prime of $\mathbb{Q}(\zeta_{2^{n_r+3}})$ lying over $\mathfrak{r}$. Then $O_{\mathbb{Q}_n}/\mathfrak{r} \simeq \mathbb{Z}[\zeta_{2^{n+2}}]/\mathfrak{R} \simeq \mathbb{F}_{r^{2^{n-n_r}}}$. Note that $v_2(|\mathbb{F}^\times_{r^{2^{n-n_r}}}|) = v_2(r^{2^{n-n_r}} - 1) = 2^{n+2}$. Since

$$(O_{\mathbb{Q}_n}/\mathfrak{r})^\times \otimes \mathbb{Z}_2 \simeq (\mathbb{Z}[\zeta_{2^{n+2}}]/\mathfrak{R})^\times \otimes \mathbb{Z}_2 = \langle (\zeta_{2^{n+2}} \bmod \mathfrak{R}) \otimes 1 \rangle \simeq \langle \zeta_{2^{n+2}} \rangle$$

as $\overline{\Gamma}^{2^{n_r+1}}$-modules, $\gamma^{2^{n_r+1}}$ acts on $(O_{\mathbb{Q}_n}/r)^\times \otimes \mathbb{Z}_2 \simeq \bigoplus_{\mathfrak{r}|r}((O_{\mathbb{Q}_n}/\mathfrak{r})^\times \otimes \mathbb{Z}_2)$ as $5^{2^{n_r+1}}$ for any $n > n_r$. Put $\nu = \max\{n_r + 1 \,|\, r \in S\}$. Then, since there is a surjective Λ-homomorphism $\varprojlim((O_{\mathbb{Q}_n}/\prod_{r \in S} r)^\times \otimes \mathbb{Z}_2) \to \varprojlim A_S(\mathbb{Q}_n) \simeq G^{\mathrm{ab}}$, γ^{2^ν} acts on G^{ab} as 5^{2^ν}, i.e., ${}^{\gamma^{2^\nu}}g = \widetilde{\gamma}^{2^\nu} g \widetilde{\gamma}^{-2^\nu} \equiv g^{5^{2^\nu}} \pmod{G_2}$ for $g \in G$.

Let $K/\mathbb{Q}$ be a finite extension such that $K \subset (\mathbb{Q}_\infty)_S$. Then $\mathbb{Q}_\infty \subset K_\infty \subset (K_\infty)^{\mathrm{ab}}_\emptyset \subset (\mathbb{Q}_\infty)_S$. We show that $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is finite if G is prometacyclic. If G is finite, then $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is also finite. In the following, we assume that G is infinite prometacyclic. If $G_\emptyset(K'_\infty)^{\mathrm{ab}}$ is finite for some finite extension K'/K, then $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is also finite. Hence we may assume that $K/\mathbb{Q}$ is a finite Galois extension such that $(\mathbb{Q}_\infty)^{\mathrm{elem}}_S \subset K_\infty$. Let N be a procyclic closed normal subgroup of G such that G/N is also procyclic. If G is procyclic, we assume that N is trivial. Put $M = (\mathbb{Q}_\infty)^N_S$ the fixed field of N. Since $G_\emptyset(\mathbb{Q}_\infty)$ is trivial, $M/\mathbb{Q}_\infty$ is totally ramified at some prime v of $\mathbb{Q}_\infty$. If G is procyclic, then $(\mathbb{Q}_\infty)_S = M$, and hence $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is trivial. Suppose that N is finite. Then the subquotient $\mathrm{Gal}((K_\infty)^{\mathrm{ab}}_S/K_\infty M)$ of N is also finite. Since G is infinite, $M/\mathbb{Q}_\infty$ is a $\mathbb{Z}_2$-extension, and hence $K_\infty M$ is the unique $\mathbb{Z}_2$-extension of K_∞ unramified outside S. Since $M/\mathbb{Q}_\infty$ is totally ramified at v, $K_\infty M/K_\infty$ is not unramified. This implies that

K_∞ has no unramified $\mathbb{Z}_2$-extension. Therefore $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is finite if N is finite. In the following, we assume that N is infinite and G is not procyclic. Let a, b be the generators of G such that $N = \langle a \rangle \simeq \mathbb{Z}_2$ and $G/N = \langle bN \rangle$. Since $G_2 \subset N$, we have $[a, b] = a^z$ with some $z \in 2\mathbb{Z}_2$. Then $G_2 = \langle a^z \rangle$ and $b^{-1}ab = a^{1+z}$. Since γ^{2^ν} acts on G^{ab} as 5^{2^ν}, ${}^{\gamma^{2^\nu}}a = a^{5^{2^\nu}+xz}$ and ${}^{\gamma^{2^\nu}}b = b^{5^{2^\nu}}a^{yz}$ with some $x, y \in \mathbb{Z}_2$. Hence

$$1 = {}^{\gamma^{2^\nu}}1 = {}^{\gamma^{2^\nu}}(a^{-(1+z)}b^{-1}ab) = a^{(1+z)(5^{2^\nu}+xz)((1+z)^{5^{2^\nu}-1}-1)}.$$

This implies that $(1+z)^{5^{2^\nu}-1} = 1$, i.e., $z = 0$ or $z = -2$. If $z = 0$, then G is abelian, and $G/G^2 \simeq \mathbb{F}_2[[T]]/T^2$ or $(\mathbb{F}_2[[T]]/T)^2$ as $\mathbb{F}_2[[T]]$-modules. If $z = -2$, we have $b^{-1}ab = a^{-1}$ and $G_2 = \langle a^2 \rangle$. Then $[a, b^2] = 1$. Let H be an abelian maximal subgroup of G such that:

- $H/G^2 = T(G/G^2)$ if $z = 0$ and $G/G^2 \simeq \mathbb{F}_2[[T]]/T^2$,
- $H = \langle a, b^2 \rangle$ if $z = -2$.

(If $z = 0$ and $G/G^2 \simeq (\mathbb{F}_2[[T]]/T)^2$, then H is an arbitrary maximal subgroup of G.) If $z = 0$, then $T(H/G^2) \simeq 0$, i.e., ${}^\gamma h \equiv h \pmod{G^2}$ for any $h \in H$, and hence ${}^\gamma H = H$. If $z = -2$ and $b^2 \in N$, then G is prodihedral, and $H = N$ is the unique procyclic maximal subgroup. If $z = -2$ and $b^2 \notin N$, then $\mathrm{r}_4(G/G_2) = 1$, and H is the unique maximal subgroup such that $\mathrm{r}_2(H/G_2) = 2$. Therefore, by the uniqueness of such H, we have ${}^\gamma H = H$ even if $z = -2$. This implies that the fixed field $(\mathbb{Q}_\infty)_S^H$ of H is a Galois extension of $\mathbb{Q}$. Since γ acts on G/H trivially, $(\mathbb{Q}_\infty)_S^H/\mathbb{Q}$ is abelian. Hence the inertia field k of 2 in $(\mathbb{Q}_\infty)_S^H/\mathbb{Q}$ is a real quadratic field, and $(\mathbb{Q}_\infty)_S^H = k_\infty$. Recall that we are assuming $k_\infty \subset (\mathbb{Q}_\infty)_S^{\mathrm{elem}} \subset K_\infty$. Since H is abelian, $(K_\infty)_\emptyset^{\mathrm{ab}}/k_\infty$ is an abelian extension. Since any prime in the finite set S_{k_∞} has finite ramification index in $(K_\infty)_\emptyset^{\mathrm{ab}}/k_\infty$, $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is infinite if $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is infinite. Hence it suffices to show the finiteness of nontrivial $G_\emptyset(k_\infty)^{\mathrm{ab}}$. Since $(k_\infty)_\emptyset^{\mathrm{elem}}/\mathbb{Q}_\infty$ is an elementary abelian 2-extension, $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is procyclic. By the list of S with nonprocyclic prometacyclic G and [20, Corollary 3.4 and Theorem 3.8], the real quadratic field $k \subset \mathbb{Q}_S$ with nontrivial procyclic $G_\emptyset(k_\infty)^{\mathrm{ab}}$ satisfies one of the following:

- $k = \mathbb{Q}(\sqrt{\ell})$, $\ell \equiv 9 \pmod{16}$, $\left(\frac{2}{\ell}\right)_4 = -1$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is finite by [20, Theorem 4.1].
- $k = \mathbb{Q}(\sqrt{r_1 r_2})$, $r_1 \equiv r_2 \equiv 5 \pmod 8$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is finite by [23].
- $k = \mathbb{Q}(\sqrt{r_1 r_2})$, $r_1 \equiv 1 \pmod 8$, $r_2 \equiv 5 \pmod 8$, $\left(\frac{r_1}{r_2}\right) = -1$, $\left(\frac{2}{r_1}\right)_4\left(\frac{r_1}{2}\right)_4 = -1$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ by Theorem 4.3 and Lemma 7.2.
- $k = \mathbb{Q}(\sqrt{r_1 r_2})$, $r_1 \equiv 7 \pmod{16}$, $r_2 \equiv 15 \pmod{16}$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}}$ is finite by Corollary 7.5.
- $k = \mathbb{Q}(\sqrt{q_1 q_2 r})$, $q_1 \equiv 3 \pmod 8$, $q_2 \equiv 7 \pmod 8$, $r \equiv 5 \pmod 8$, $\left(\frac{q_2}{r}\right) = -1$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ by Theorem 8.2 (cf. also [20, Theorem 4.4]).
- $k = \mathbb{Q}(\sqrt{q_1 q_2 r})$, $q_1 \equiv q_2 \equiv 3 \pmod 8$, $r \equiv 5 \pmod 8$, $\left(\frac{q_1 q_2}{r}\right) = -1$. Then $G_\emptyset(k_\infty)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ by Theorem 8.2.

The finiteness of $G_\emptyset(k_\infty)^{\mathrm{ab}}$ has been known in each case. Therefore $G_\emptyset(K_\infty)^{\mathrm{ab}}$ is finite if $G_S(\mathbb{Q}_\infty)$ is prometacyclic. Thus the proof of Theorem 1.1 is completed.

Acknowledgment

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

References

[1] Elliot Benjamin, Franz Lemmermeyer, and C. Snyder, *Real quadratic fields with abelian* 2*-class field tower*, J. Number Theory **73** (1998), no. 2, 182–194, DOI 10.1006/jnth.1998.2291. MR1658015

[2] Elliot Benjamin and C. Snyder, *Real quadratic number fields with* 2*-class group of type* $(2,2)$, Math. Scand. **76** (1995), no. 2, 161–178, DOI 10.7146/math.scand.a-12532. MR1354574

[3] N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. **54** (1958), 327–337. MR0102557

[4] Julien Blondeau, Philippe Lebacque, and Christian Maire, *On the cohomological dimension of some pro-p-extensions above the cyclotomic* $\mathbb{Z}_p$*-extension of a number field* (English, with English and Russian summaries), Mosc. Math. J. **13** (2013), no. 4, 601–619, 736–737. MR3184074

[5] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999. MR1720368

[6] Bruce Ferrero, *The cyclotomic* $\mathbf{Z}_2$*-extension of imaginary quadratic fields*, Amer. J. Math. **102** (1980), no. 3, 447–459, DOI 10.2307/2374108. MR573095

[7] Takashi Fukuda, *Remarks on* $\mathbf{Z}_p$*-extensions of number fields*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 8, 264–266. MR1303577

[8] Ralph Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284, DOI 10.2307/2373625. MR0401702

[9] Tsuyoshi Itoh, Yasushi Mizusawa, and Manabu Ozaki, *On the* $\mathbb{Z}_p$*-ranks of tamely ramified Iwasawa modules*, Int. J. Number Theory **9** (2013), no. 6, 1491–1503, DOI 10.1142/S1793042113500395. MR3103900

[10] Tsuyoshi Itoh and Yasushi Mizusawa, *On tamely ramified pro-p-extensions over* $\mathbb{Z}_p$*-extensions of* $\mathbb{Q}$, Math. Proc. Cambridge Philos. Soc. **156** (2014), no. 2, 281–294, DOI 10.1017/S0305004113000637. MR3177870

[11] Yûji Kida, *On cyclotomic* $\mathbf{Z}_2$*-extensions of imaginary quadratic fields*, Tôhoku Math. J. (2) **31** (1979), no. 1, 91–96, DOI 10.2748/tmj/1178229880. MR526512

[12] Yûji Kida, *Cyclotomic* $\mathbf{Z}_2$*-extensions of J-fields*, J. Number Theory **14** (1982), no. 3, 340–352, DOI 10.1016/0022-314X(82)90069-5. MR660379

[13] H. Kisilevsky, *Number fields with class number congruent to* 4 mod 8 *and Hilbert's theorem* 94, J. Number Theory **8** (1976), no. 3, 271–279, DOI 10.1016/0022-314X(76)90004-4. MR0417128

[14] Helmut Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. MR1930372

[15] Tomio Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85. MR0083009

[16] Franz Lemmermeyer, *Kuroda's class number formula*, Acta Arith. **66** (1994), no. 3, 245–260. MR1276992

[17] Franz Lemmermeyer, *The ambiguous class number formula revisited*, J. Ramanujan Math. Soc. **28** (2013), no. 4, 415–421. MR3158989

[18] Christian Maire, *Sur la dimension cohomologique des pro-p-extensions des corps de nombres* (French, with English and French summaries), J. Théor. Nombres Bordeaux **17** (2005), no. 2, 575–606. MR2211309

[19] Yasushi Mizusawa and Manabu Ozaki, *On tame pro-p Galois groups over basic* $\mathbb{Z}_p$*-extensions*, Math. Z. **273** (2013), no. 3-4, 1161–1173, DOI 10.1007/s00209-012-1048-2. MR3030694

[20] Ali Mouhib and Abbas Movahhedi, *Cyclicity of the unramified Iwasawa module*, Manuscripta Math. **135** (2011), no. 1-2, 91–106, DOI 10.1007/s00229-010-0407-8. MR2783388

[21] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[22] Manabu Ozaki, *Non-abelian Iwasawa theory of* $\mathbb{Z}_p$*-extensions*, J. Reine Angew. Math. **602** (2007), 59–94, DOI 10.1515/CRELLE.2007.003. MR2300452

[23] Manabu Ozaki and Hisao Taya, *On the Iwasawa* λ_2*-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437–444, DOI 10.1007/BF02677865. MR1484637

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

[25] 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, DOI 10.1515/crll.1934.170.69. MR1581397

[26] Landry Salle, *Sur les pro-p-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres*, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 485–523. MR2477515

[27] Landry Salle, *On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field*, Osaka J. Math. **47** (2010), no. 4, 921–942. MR2791570

[28] H. Taya and G. Yamamoto, *Notes on certain real abelian 2-extension fields with $\lambda_2 = \mu_2 = \nu_2 = 0$*, Trends in Mathematics, Information Center for Mathematical Sciences **9** (2006), no. 1, 81–89. `http://mathnet.kaist.ac.kr/new_TM/`

[29] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575

[30] Yoshihiko Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. **21** (1984), no. 1, 1–22. MR736966

[31] Hideo Yokoi, *On the class number of a relatively cyclic number field*, Nagoya Math. J. **29** (1967), 31–44. MR0207681

Department of Mathematics, Nagoya Institute of Technology, Gokiso, Showa, Nagoya 466-8555, Japan

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