Maximal 2-Extensions with Restricted Ramification

Nigel Boston and David Perry

Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Communicated by George Glauberman

Received September 3, 1999

We compute the Galois groups of several 2-extensions of \( \mathbb{Q} \) ramified at finitely many odd primes. © 2000 Academic Press

INTRODUCTION

If \( K \) is a number field and \( S \) is a finite set of primes of \( K \), then the structure of the Galois group of the maximal \( p \)-extension of \( K \) unramified outside \( S \) is important in the study of \( p \)-adic Galois representations unramified outside \( S \). The case of \( S \) containing the primes above \( p \) is fairly well understood and widely applied. This is the kind of Galois representation arising from algebraic geometry.

On the other hand, there is very little known concerning the structure of the Galois group of the maximal \( p \)-extension of \( K \), unramified outside \( S \), if \( S \) contains no primes above \( p \). This includes, for instance, the case of Hilbert \( p \)-class towers (i.e., \( S = \emptyset \)), the Galois group of which is called one of the most mysterious objects in algebraic number theory in [10]. There are, however, conjectures regarding the structure of the Galois group, such as that it has no infinite quotient linear over the \( p \)-adic integers [3] and generalizations of this [1]. These have important consequences on the nonexistence of corresponding \( p \)-adic representations.

In this paper, we begin to fill this hole in our understanding by computing some of these Galois groups in the simplest case, namely for 2-extensions of \( \mathbb{Q} \). We observe an interesting phenomenon, namely that there appears to be a relatively small class of finite 2-groups to which these calculated Galois groups belong.

This phenomenon will be further examined in a subsequent paper by Charles Leedham-Green and the first author. They develop a new method...
that finds, given a particular $S$, a short list of possible $G_S$ (or, if infinite, large quotients of $G_S$), by an exhaustive computer search based on the $p$-group generation algorithm [9]. The methods of this paper are quite different, in that they are not computer-based and the results hold for whole families of sets $S$.

1. PRELIMINARIES

Let $S$ be a finite set of odd rational primes, $\mathbb{Q}_S$ the maximal 2-extension of $\mathbb{Q}$ unramified outside $S$ (we allow ramification at infinity), and $G_S = \text{Gal}(\mathbb{Q}_S/\mathbb{Q})$. We will study the pro-2 group $G_S$ for various $S$.

**Lemma 1.1.** (1) Every open subgroup of $G_S$ has finite abelianization.

(2) The generator and relator ranks of $G_S$, denoted $d(G_S)$ and $r(G_S)$, respectively, are both equal to $\#S$, and $G_S$ has trivial Schur multiplicator.

**Proof.** (1) is due to class field theory (the finiteness of certain ray class groups), and (2) is due to Shafarevich (see [4]).

**Remarks.** (1) implies that each subgroup of the derived series of $G_S$ is of finite index in $G_S$. In [4], Fröhlich also gives a presentation of the maximal nilpotency class 2 quotient of $G_S$. (2) implies that $G_S$ cannot be an Abelian group if $\#S > 1$, since noncyclic Abelian groups have nontrivial Schur multiplicator.

If $\#S = 1$, then $G_S$ is finite cyclic. If $S = \{p\}$, then $\mathbb{Q}_S \subseteq \mathbb{Q}(\zeta_p)$ and $G_S = \langle a \mid a^{p-1} \rangle$ (presented as a pro-2 group). If $\#S \geq 4$, then $G_S$ is infinite (as a consequence of the theorem of Golod and Shafarevich [5]). When $\#S = 3$, $G_S$ can be either finite or infinite. (Maire [8] showed that $G_S$ is infinite if $S = \{3, 13, 61\}$. Recent work of the first author and C. Leedham-Green shows that $G_S$ is finite if $S = \{3, 7, 11\}$.) It is unknown whether $G_S$ is finite or infinite in general when $\#S = 2$. In this paper we detail three cases where $G_S$ is finite and computable with $\#S = 2$.

Before we do so, we list results from group theory and class field theory which we will use in the next section.

**Lemma 1.2.** (Burnside’s basis theorem—profinite version). Let $H$ be a pro-$p$ group and let $\Phi(H)$ be its Frattini subgroup (i.e., the intersection of its maximal open subgroups). Any lifts to $H$ of generators of $H/\Phi(H)$ will (topologically) generate $H$. Hence, $d(H) = d(H/\Phi(H))$, and if $J$ is a closed subgroup of $H$ that maps onto $H/\Phi(H)$, then $J = H$.

The following lemma combines the relevant parts of [Go, Theorems 4.4 and 4.5].
LEMMA 1.3. Let $P$ be a non-Abelian 2-group of order $2^m$.

(1) If $P$ contains a cyclic subgroup of order $2^{m-1}$ and $m > 3$, then $P$ is dihedral, generalized quaternion, semidihedral, or the modular group $M_m(2)$.

(2) If $|P/P'| = 4$, then $P$ is dihedral, generalized quaternion, or semidihedral.

For the remainder of this paper we assume that $S = \{p, q\}$, where $p$ and $q$ are odd primes. Let $D_q$ and $I_q$ denote decomposition and inertia subgroups of $G_S$ at $q$, defined up to conjugacy. Note that $D_q$ is metacyclic (since there is no wild inertia). In fact $D_q$ is generated by elements $\tau$ and $y$ where $I_q = \langle \tau \rangle$ and $\tau^y = \tau^q$ (the tame relation). In the three cases detailed in the next section we establish that a decomposition subgroup is open in $G_S$, from which it follows (by Lemma 1.1 (1)) that $G_S$ is finite.

LEMMA 1.4. $G_S/G'_S \cong \mathbb{Z}_{2'} \times \mathbb{Z}_{2''}$, where $2'$ is the highest power of 2 dividing $p-1$ and $2''$ is the highest power of 2 dividing $q-1$.

Proof. Let $K$ be the maximal Abelian 2-extension of $\mathbb{Q}$ unramified outside $S$. Then $K = \text{Fix}(G'_S) \subseteq \mathbb{Q}(\zeta_n)$ for some $n$ by Kronecker–Weber. The restricted ramification implies that only $p$ and $q$ can divide $n$. Since $|\mathbb{Q}(\zeta_n) : \mathbb{Q}| = p^{k-1}(p-1)q^{l-1}(q-1)$ for some $k \geq 1$, $l \geq 1$, the result follows.

Note. $K$ is the compositum of the maximal Abelian 2-extensions of $\mathbb{Q}$ ramified only at $p$ and $q$, of degrees $2'$ and $2''$, respectively.

LEMMA 1.5. If $H$ is an open subgroup of $G_S$ and $H/H'$ is either cyclic or isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, then $G_S$ is finite.

Proof. $H/H'$ cyclic implies that $H$ is finite cyclic by Lemmas 1.1 (1) and 1.2. If $H/H' \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then $H'$ is open in $G_S$ and Lemma 1.3 (2) implies that $H'/H''$ is cyclic.

LEMMA 1.6. If $p \equiv 3 \pmod{4}$ or $q \equiv 3 \pmod{4}$, then there exists an involution $\sigma \in G_S$ such that $\sigma \notin \Phi(G_S)$, the Frattini subgroup of $G_S$.

Proof. Either $\mathbb{Q}(\sqrt{-p})$ or $\mathbb{Q}(\sqrt{-q})$ lies in $\text{Fix}(\Phi(G_S))$. Hence, the involution $\sigma = \text{complex conjugation} \in G_S$ does not lie in $\Phi(G_S)$.

LEMMA 1.7. If $p \equiv 3 \pmod{4}$, then the 2-part of the ray class group of $\mathbb{Q}(\sqrt{-p})$ of modulus $p \cdot q$ is

(i) $\mathbb{Z}_2$ if $(-p/q) = -1$, i.e., if $q$ is inert in $\mathbb{Q}(\sqrt{-p})$, where $2^k$ is the highest power of 2 dividing $|\langle F_q \rangle^\times| = q^2 - 1$, and

(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2$ if $(-p/q) = 1$, i.e., if $q$ splits in $\mathbb{Q}(\sqrt{-p})$, where $2^l$ is the highest power of 2 dividing $|\langle F_q \rangle^\times| = q - 1$. 
2. THREE EXPLICIT FAMILIES OF \( G_S \)

**Theorem 2.1.** Assume that \( p \equiv 3 \pmod{4} \), \( q \equiv 3 \pmod{4} \), and without loss of generality (by quadratic reciprocity) \( p \) is a quadratic residue of \( q \). If \( 2^k \) is the highest power of 2 dividing \( q^2 - 1 \), then

\[
G_S \cong \langle a, b \mid a^2 = b^{2^k} = 1, \ b^a = b^{-1+2^{k-1}} \rangle,
\]

the semidihedral group of order \( 2^{k+1} \). Further, we can take \( a \) to be complex conjugation and \( b \) to be the generator \( \sigma \) of any inertia subgroup \( I_q \) of \( G_S \).

**Proof.** \( G_S/G_S' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \) by Lemma 1.4 and so \( G_S \) is finite by Lemma 1.5. As \( G_S \) is non-Abelian, Lemma 1.3 implies that \( G_S \) is dihedral, generalized quaternion, or semidihedral. \( G_S \) cannot be dihedral, as such 2-groups have nontrivial Schur multiplicator (Lemma 1.1 (2)). \( G_S \) cannot be generalized quaternion, as such groups have a unique involution, which is in \( \Phi(G_S) \) (Lemma 1.6). Therefore, \( G_S \) is semidihedral.

\( q \) ramifies in \( \mathbb{Q}(\sqrt{-q}) \) and \( \mathbb{Q}(\sqrt{pq}) \) and remains inert in \( \mathbb{Q}(\sqrt{-p}) \). As these are the only quadratic extensions of \( \mathbb{Q} \) in \( \mathbb{Q}_S \), \( D_q \) maps onto \( G_S/\Phi(G_S) \). By Lemma 1.2, \( D_q = G_S \). Thus, \( G_S' \leq I_q \), and it follows from the above that \( \mathbb{Q}(\sqrt{-p}) = \text{Fix}(I_q) \). By Lemma 1.7, \( I_q \) has order \( 2^k \). As \( \sigma \) does not fix \( \mathbb{Q}(\sqrt{-p}) \), \( G_S = \langle \tau_q, \sigma \rangle \). The final claim of the theorem follows from the fact that a semidihedral group of order \( 2^{k+1} \) is generated by any element generating a cyclic subgroup of index 2 and any involution outside of that subgroup.

**Theorem 2.2.** Assume that \( p \equiv 3 \pmod{4} \), \( q \equiv 1 \pmod{4} \), and \( (p/q) = -1 \). If \( 2^k \) is the highest power of 2 dividing \( q-1 \), then

\[
G_S \cong M_{k+2}(2) = \langle a, b \mid a^2 = b^{2^k+1} = 1, \ b^a = b^{1+2^k} \rangle,
\]

the modular group of order \( 2^{k+2} \). Further, we can take \( a \) to be complex conjugation and \( b \) to be the generator of any inertia subgroup \( I_q \) of \( G_S \).

**Proof.** \( G_S/G_S' \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \) by Lemma 1.4, \( q \) ramifies in \( \mathbb{Q}(\sqrt{q}) \) and \( \mathbb{Q}(\sqrt{-pq}) \) and remains inert in \( \mathbb{Q}(\sqrt{-p}) \), so \( D_q = G_S \) as above (so \( G_S \) is finite), and \( \mathbb{Q}(\sqrt{-p}) = \text{Fix}(I_q) \). The index 4 subgroups of \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) lie in a unique index 2 subgroup, which necessarily corresponds to \( \mathbb{Q}(\sqrt{q}) \) (by the note following Lemma 1.4). Therefore, we have \( \mathbb{Q}(\sqrt{-p}) = \text{Fix}(I_q) \), and \( I_q \) has order \( 2^{k+1} \) by Lemma 1.7. By Lemma 1.3(1), \( G_S \) is dihedral, generalized
quaternion, semidihedral, or modular. As the first three families of groups have Abelianization of order 4, $G_S$ is modular of order $2^{k+2}$. The final claim of the theorem follows analogously to the proof of Theorem 2.1.

**Lemma 2.3.** (the critical quartic lemma). Assume $p \equiv 3 \pmod{4}$, $2^n \ (n \geq 2)$ exactly divides $q-1$, and either

1. $n = 2$ and $p \in (F_q)^4$, or
2. $n \geq 3$ and $p \in (F_q^*)^2 - (F_q^*)^4$.

Then $\text{Fix}(D_q) = \mathbb{Q}(\sqrt{-p})$, and $\mathbb{Q}_S$ is a finite extension of $\mathbb{Q}$.

**Proof.** This is given in Section 3.

**Theorem 2.4.** Assume the same hypotheses on $p$ and $q$ as in Lemma 2.3, so in particular $q \equiv 2^n + 1 \pmod{2^{n+1}}(n \geq 2)$. Then

$$G_S \cong P_n := \langle a, b \mid a^2 = b^{-1}abab^{-q-1}a = 1 \rangle$$

(presented as a pro-$2$ group), of order $2^{3n+1}$. Further, we can take $a$ to be complex conjugation and $b$ to be the generator of any inertia subgroup $I_q$ of $G_S$.

**Proof.** We know that $D_q$ is metacyclic generated, say, by $\tau$ and $y$ where $\langle \tau \rangle = I_q$ and $\tau^q = \tau^q$. By Lemma 2.3 $D_q$ is of index 2 in $G_S$ and complex conjugation $\sigma \in G_S - D_q$ (so $G_S$ is a split extension of $D_q$ by $\langle \sigma \rangle$). Since $\sigma$ permutes the two primes of $\mathbb{Q}(\sqrt{-p})$ above $q$, the corresponding inertia groups are generated by $\tau$ and $\tau^\sigma$, respectively. The proof of Lemma 2.3 shows that the images of these two elements in $D_q/\Phi(D_q)$ are distinct and nontrivial. Thus they generate $D_q/\Phi(D_q)$ and hence by Lemma 1.2 they generate $D_q$. It follows that $G_S = \langle \sigma, \tau, \tau^\sigma \rangle = \langle \sigma, \tau \rangle$.

As for relations, we have $\sigma^2 = 1$. Also, the image of $y$ in $D_q/\Phi(D_q)$ must be nontrivial and distinct from the images of $\tau$ and $\tau^\sigma$, since if, for instance, $y$ and $\tau$ were equal modulo $\Phi(D_q)$, then they would not generate $D_q$. Thus $y$ equals $\tau \tau^\sigma$ modulo $\Phi(D_q)$. The freedom in picking $y$ allows us to assume that $y = \tau \tau^\sigma$. Then the tame relation becomes $\tau \tau^\sigma = \tau^q$. Expanding this out gives (using $\sigma^2 = 1$) $\sigma \tau^{-1} \sigma \tau \sigma = \tau^q$.

Letting $H_q$ be the 2-group with presentation $\langle a, b \mid a^2 = b^{-1}abab^{-q}a = 1 \rangle$, we easily check that $H_q$ is isomorphic to $P_n$ of order $2^{3n+1}$. We have a surjection $\phi : H_q \to G_S$ given by $a \mapsto \sigma, b \mapsto \tau$. Since $\phi$ induces an isomorphism $H_q/\Phi(H_q) \to G_S/\Phi(G_S)$ and $G_S$ has trivial Schur multiplicator, it follows that $\phi$ is an isomorphism.

**Note.** For $n = 2$, $P_n$ is group #87 of order 128 in the standard databases of 2-groups of small order.
3. PROOF OF THE CRITICAL QUARTIC LEMMA

The proof of this lemma is technical and will be split into a series of claims.

**Claim 4.1.** \( \mathbb{Q}(\sqrt{-p}) \) has three quadratic extensions inside \( \mathbb{Q}_S \), One of them is \( \mathbb{Q}(\sqrt{-p}, \sqrt{q}) \) and the other two are nonnormal over \( \mathbb{Q} \).

*Proof.* Let \( H = \text{Gal}(\mathbb{Q}_S/\mathbb{Q}(\sqrt{-p})) \). By Lemma 1.7, \( H/\Phi(H) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \), establishing the first sentence of the claim. As in the proof of Theorem 2.2, any normal subextension of \( \mathbb{Q}_S \) of degree 4 over \( \mathbb{Q} \) necessarily contains \( \mathbb{Q}(\sqrt{q}) \).

**Claim 4.2.** There exists an integral solution to \( X^2 + pY^2 = 4q^i \) for some odd integer \( i \).

*Proof.* Let \( Q \) be one of the two prime ideals lying above \( q \) in \( \mathbb{Q}(\sqrt{-p}) \), which has odd class number by genus theory. Therefore, \( Q' \) is principal for some positive odd integer \( i \); let \( C + D(1 + \sqrt{-p})/2 \) \( (C, D \in \mathbb{Z}) \) denote a generator of that principal ideal. Then \( C^2 + CD + D^2(1 + p)/4 = \text{Norm}(C + D(1 + \sqrt{-p})/2) = q^i \), so \( (2C + D)^2 + pD^2 = 4q^i \), and we take \( X = 2C + D \) and \( Y = D \).

We construct one of the two quadratic extensions of \( \mathbb{Q}(\sqrt{-p}) \) in \( \mathbb{Q}_S \), non-normal over \( \mathbb{Q} \), by adjoining \( \sqrt{\theta} \), where \( \theta = A + B(1 + \sqrt{-p})/2 \in \mathbb{Q}(\sqrt{-p}) \) is chosen as follows:

Take \( m, n \in \mathbb{Z} \) such that \( m^2 + pn^2 = 4q^i \), where \( i \) is the smallest positive odd integer for which a solution exists. The minimality of \( i \) implies that \( q \nmid m, q \nmid n \), and \( (m, n) = 1 \) or 2. \( m \) and \( n \) have equal parity, and we set \( A = (m - n)/2 \) and \( B = n \). If \( \theta = A + B(1 + \sqrt{-p})/2 \), then \( \text{Norm}(\theta) = A^2 + AB + B^2(1 + p)/4 = q^i \). Noting that we are free to choose between \( m \) and \(-m\) and between \( n \) and \(-n\), we use the results in [7] to insure that only \( p \) and \( q \) ramify in \( L = \mathbb{Q}(\sqrt{\theta}) \).

Specifically, in [7, Theorem 1]:

1. If \( (m, n) = 1 \), we must take \( a = 2m, b = 2n, \) and \( c = -p \) in Theorem 1, choosing between \( m \) and \(-m\) so that \( a \equiv 6 \pmod{8} \) so that we fall in case C7, and \( L \) has discriminant \( p^2q \).

2. If \( (m, n) = 2 \), we must take \( a = m/2, b = n/2, \) and \( c = -p \) in Theorem 1, choosing between \( m \) and \(-m\) so that \( a + b \equiv 1 \pmod{4} \) so that we fall in case C2, and again \( L \) has discriminant \( p^2q \).

At worst, an injudicious choice results in ramification at 2 in \( L \) in addition to \( p \) and \( q \).

**Claim 4.3.** If \( m^2 + pn^2 = 4q^i \), \( q \nmid m \), and \( q \nmid n \), then \( (mn/q) = -1 \).
Proof. \( m^2 + pn^2 \equiv 0 \pmod{q} \), so \((m/n)^2 = -p \in \mathbb{F}_q^\times \). If \( n \) and \( m \) are simultaneously either residues or nonresidues modulo \( q \), then we have that \(-p\) is a fourth power modulo \( q \).

However, the hypotheses on \( p \) and \( q \) imply that exactly one of \(-1\) and \(-p\) is a fourth power modulo \( q \), so this is impossible. Hence, we must have \((mn/q) = -1\). \(\blacksquare\)

If \((m,n) = 2\), then set \(m = 2m'\) and \(n = 2n'\), so \((m',n') = 1\). Then \(m^2 + pn^2 = q'\), so \(m'\) and \(n'\) have opposite parity. By looking at this equation modulo 8, we find that necessarily \(m'\) is odd and \(n' = 2n''\) is even. Further, if \( q \equiv 5 \pmod{8} \), \(n''\) must be odd and if \( q \equiv 1 \pmod{8} \), \(n''\) must be even.

Claim 4.4. Assume \(m^2 + pn^2 = 4q'\) with \((m,n) = 1 \) or \(2 \), \(q \nmid m\), and \(q \nmid n\), with \(i \geq 1\) an odd integer, say, \(i = 2k + 1\). Then \((m/q) = -1\) and \((n/q) = 1\).

Proof. Here we must work in the Dedekind domain \(\mathcal{O}_{\mathbb{Q}((\sqrt{q})/\mathbb{Q})}\). Let \(\tau\) denote the nontrivial element of \(\text{Gal}(\mathbb{Q}((\sqrt{q})/\mathbb{Q}))\) which sends \(\sqrt{q}\) to \(-\sqrt{q}\).

First, assume that \(m\) and \(n\) are odd, with \((m,n) = 1\). We have \(pn^2 = (-m + 2q^k\sqrt{q})(m + 2q^k\sqrt{q})\). Let \(R = (-m + 2q^k\sqrt{q})\) be considered as a principal ideal in \(\mathcal{O}_{\mathbb{Q}((\sqrt{q})/\mathbb{Q})}\). As ideals,

\[
(p,t + \sqrt{q})(p,t - \sqrt{q}) \cdot (n^2) = R \cdot \tau(R),
\]

where \(t\) is a square root of \(q\) modulo \(p\).

Note that for any prime ideal \(Q\) lying above a prime \(p_i \mid n\), we cannot have \(Q \mid R\) and \(Q \mid \tau(R)\), or else \(R\), \(\tau(R) \subseteq Q\), implying \(2m = (m + 2q^k\sqrt{q}) - (-m + 2q^k\sqrt{q}) \in Q\) and \(n \in Q\), implying that \(1 \in Q\).

Let \(p_i \mid n\) be an odd prime. Assume that \((p_i/q) = -1\). Then \(P_i = (p_i)\) is a prime ideal, and \(\tau(P_i) = P_i\). As \(P_i \mid (n)\) as ideals, \(P_i \mid R\) or \(\tau(R)\). If \(P_i \mid R\), then \(P_i = \tau(P_i)\) or \(\tau(R)\), and vice versa. This is a contradiction, and so \((p_i/q) = 1\). As \(n\) is the product of quadratic residues modulo \(q\), \((n/q) = 1\).

By Claim 4.3, we also have \((m/q) = -1\).

Assume that \((m,n) = 2\), and let \(m', n', \) and \(n''\) be defined as above. \(m^2 + p \cdot n^2 = q^{2k+1}\), so \(p \cdot n^2 = (-m + q^k\sqrt{q})(m + q^k\sqrt{q})\). Let \(R = (-m + q^k\sqrt{q})\) be considered as a principal ideal in \(\mathcal{O}_{\mathbb{Q}((\sqrt{q})/\mathbb{Q})}\). Let \(l\) be such that \(n'' = 2^{l-1}n''\), where \(n''\) is odd. \(l = 1\) and \(n'' = n''\) if \(q \equiv 5 \pmod{8}\), and \(l > 1\), \(n'' = 2^{l-1}n''\) if \(q \equiv 1 \pmod{8}\). Note that \((2m',n'') = 1\). We have

\[
(p,t + \sqrt{q})(p,t - \sqrt{q}) \cdot (2)^{2l} \cdot (n'')^2 = R \cdot \tau(R)
\]

as ideals, and for any ideal \(Q\) lying above a prime \(p_i \mid n''\) we cannot have both \(Q \mid R\) and \(Q \mid \tau(R)\), lest \(1 \in Q\) as in the previous case. Proceeding as we did in the previous case, any odd prime \(p_i\) which divides \(n''\) must be a quadratic residue modulo \(q\). Therefore, \((n''/q) = 1\).
When \( q \equiv 5 \pmod{8} \), this implies that \( (n/q) = (2^{n}/q) = (4^{n''}/q) = (2^{n''}/q) = 1 \). When \( q \equiv 1 \pmod{8} \), this implies that \( (n/q) = (2^{n}/q) = (2^{n''}/q) = 1 \).

Recall that \( \theta = A + B(1 + \sqrt{-p})/2 \). Let \( \theta' = \sigma(\theta) = A + B(1 - \sqrt{-p})/2 \), so \( \theta + \theta' = 2A + B = m \). Also recall that \( N(\theta) = \theta \cdot \theta' = q' \). Let \( Q' = \sigma(Q) \), where \( Q \) is a prime ideal in \( \mathbb{Q}(\sqrt{-p}) \) lying above \( q \). As ideals, we have \( (\theta) \cdot (\theta') = Q' \cdot Q' \). We cannot have \( Q \mid (\theta) \) and \( Q \mid (\theta') \), lest \( m, q \in Q \), and hence \( 1 \in Q \). Therefore, \( (\theta) = Q' \) and \( (\theta') = Q'' \) (or vice versa, but without loss of generality we can assume the former).

Recall that \( L = K(\sqrt[3]{\theta}) \), where \( K = \mathbb{Q}(\sqrt{-p}) \). Hence, \( Q \) ramifies in \( L/K \).

**Claim 4.5.** \( Q' \) remains inert in \( L/K \).

**Proof.** We use the power residue symbol and relevant properties, found, for example, in [2, Exercise 1]. \( Q' \) is inert in \( L/K \) iff \( (\theta/Q') = -1 \). As \( (\bullet/(Q')\bullet) \) is periodic in \( (Q')\bullet \) and \( i \) is odd,

\[
\left( \frac{\theta}{Q} \right) = \left( \frac{\theta}{Q'} \right) = \left( \frac{\theta + \theta'}{Q'} \right) \equiv \left( \frac{m}{Q} \right) = \left( \frac{m}{q} \right) = -1
\]

by Claim 4.4.

We are now ready to prove the lemma. Let \( H = \text{Gal}(\mathbb{Q}_5/\mathbb{Q}(\sqrt{-p})) \). As \( q \) splits in \( \mathbb{Q}(\sqrt{-p}) \), \( H \leq D_q \). As \( q \) ramifies in \( \mathbb{Q}(\sqrt{-p}) \), we have each prime in \( \mathbb{Q}(\sqrt{-p}) \) lying above \( q \) ramifying in \( \mathbb{Q}(\sqrt{-p}, \sqrt{\ell}) \). Further, each prime in \( \mathbb{Q}(\sqrt{-p}) \) lying above \( q \) ramifies in either \( L \) or \( \sigma(L) \). Therefore, \( D_q \) maps onto \( H/\Phi(H) \), so by Lemma 1.2 we have \( D_q = H \), and hence \( G_S \) is finite.

### 4. Future Directions

The simplest cases not covered by the above theorems are those where \( p \equiv 3 \pmod{4}, \ q \equiv 5 \pmod{8} \), and \( p \) is a square but not a fourth power modulo \( q \). In recent joint work with C. Leedham-Green the first author has modified the \( p \)-group generation algorithm [9] so as to produce by computer ever larger quotients of \( G_S \) in these cases and many others not covered in the current paper. The number-theoretical information typically allows the determination, given \( S \), of a small finite set of groups to which \( G_S \) belongs. These computed groups do not have metacyclic subgroups of small index. This indicates that the methods of this paper will not extend to other families of sets \( S \).

For instance, the group \( G_{5,19} \) turns out to be of order \( 2^{19} \) and nilpotency class 11. Its largest metacyclic subgroup is of index \( 2^{10} \). This appears to be the first in a family of groups of order \( 2^{5k+4} \) and nilpotency class \( 3 \) \( (k = 3, 4, 5, \ldots) \).
If $G_S$ is infinite, the computational method yields quotients against which we can test the conjecture of Fontaine–Mazur and its generalizations. Hajir has shown that $G_S$ is infinite when $S = \{17, 101\}$.

ACKNOWLEDGMENTS

This work was partially supported by NSF Grant DMS96-22590. The authors acknowledge the kind suggestions of Stephen Ullom used to shorten the proof in Section 3.

REFERENCES