Brandon ALBERTS

**Cohen–Lenstra Moments for Some Nonabelian Groups**

Tome 32, n° 3 (2020), p. 631-664.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_3_631_0>
Cohen–Lenstra Moments for Some Nonabelian Groups

par Brandon ALBERTS

Abstract. Cohen and Lenstra gave a heuristic for the distribution of odd \(p\)-class groups for imaginary (respectively real) quadratic fields. One such formulation of this distribution is that the expected number of surjections from the class group of an imaginary quadratic field \(k\) to a fixed abelian group of odd order is 1. Class field theory tells us that the class group of \(k\) is also the Galois group of the Hilbert class field, the maximal unramified abelian extension of \(k\), so we could equivalently say that for a fixed abelian group \(G\) of odd order the expected number of unramified \(G\)-extensions of \(k\) is \(1/\#\text{Aut}(G)\). We generalize this to asking for the expected number of unramified \(G\)-extensions of \(k\), Galois over \(\mathbb{Q}\), for a fixed finite group \(G\), with no restrictions placed on \(G\). We review cases where the answer is known or conjectured by Bhargava, Boston–Bush–Hajir, and Boston–Wood, and then...
answer this question in several new cases. In particular, we consider when the expected number is zero and give a nontrivial family of groups realizing this. Additionally, we prove the expected number for the quaternion group $Q_8$ and dihedral group $D_4$ of order 8 is infinite. Lastly, we give evidence for the special case of groups generated by elements of order 2 for which Malle’s conjecture predicts an infinite expected number.

1. Introduction

The purpose of this paper is to find Cohen–Lenstra moments for non-abelian groups. For each odd prime $p$, there is a probability distribution on finite abelian $p$-groups assigning to each finite abelian $p$-group $A_p$ a probability $\text{Prob}(A_p)$ proportional to $1/\#\text{Aut}(A_p)$, called the Cohen–Lenstra measure. Cohen and Lenstra presented evidence in [5] for the heuristic that unramified $A_p$-extensions of imaginary quadratic fields ordered by absolute discriminant are distributed in the same way, which predicts how often the $p$-part of the class group of a quadratic field is isomorphic to a finite abelian $p$-group $A_p$. Namely, they predicted that for each odd prime $p$ and finite abelian $p$-group $A_p$,

$$\lim_{X \to \infty} \frac{\# \{ k/Q \text{ imaginary quadratic} : |\text{disc}(k)| < X, \text{Cl}(k)_p \cong A_p \} }{\# \{ k/Q \text{ imaginary quadratic} : |\text{disc}(k)| < X \} } = \frac{c_p}{\#\text{Aut}(A_p)},$$

where $c_p$ is independent of the $p$-group $A_p$. Cohen and Lenstra also provide similar evidence for a probability proportional to $1/(\#A_p \#\text{Aut}(A_p))$ for unramified $A_p$-extensions of real quadratic fields.

At the time of this writing, this limit has not been verified in any cases. The Cohen–Lenstra heuristics are equivalent to the so-called “moments version” of Cohen–Lenstra. Define $D_X^\pm = \{ k \text{ quadratic field} : 0 \leq \pm d_k \leq X \}$ to be the set of real/imaginary quadratic fields with discriminant $\text{disc}(k) = d_k$ bounded by $X$. For any odd order finite abelian group $A$, the Cohen–Lenstra moment can be defined by

$$\tilde{E}^\pm(A) := \lim_{X \to \infty} \frac{\sum_{k \in D_X^\pm} \# \text{Surj}(\text{Cl}(k)_p, A)}{\sum_{k \in D_X^\pm} 1}.$$

The Cohen–Lenstra heuristics over imaginary quadratic fields are then equivalent to $\tilde{E}^-(A) = 1$ for all odd order finite abelian groups $A$. Similarly, the Cohen–Lenstra heuristics over real quadratic fields are equivalent to $\tilde{E}^+(A) = 1/\#A$ for all odd order finite abelian groups $A$. The only known case of Cohen and Lenstra’s original predictions is a consequence of Davenport–Heilbronn’s work on cubic extensions [6], which shows that $\tilde{E}^-(C_3) = 1$ and $\tilde{E}^+(C_3) = 1/3$.

There is no clear choice for a probability distribution on finite nonabelian groups that can be used to generalize the heuristic. Boston–Bush–Hajir [3]
and Boston–Wood [4] have provided evidence for a particular distribution on nonabelian $p$-groups $P$ matching the distribution of unramified $P$-extensions of real/imaginary quadratic fields for some $p$-group $P$, but it is not obvious how to generalize this distribution to arbitrary finite groups. The moments version of Cohen–Lenstra does have a clear analog to nonabelian groups via class field theory. For any finite group $G$, the expected number of unramified $G$-extensions over real/imaginary quadratic fields is given by

$$E\pm(G) := \lim_{X \to \infty} \frac{\sum_{k \in D_X^\pm} \#\{K/k \text{ unramified with Galois group } G, \text{ Galois over } \mathbb{Q}\}}{\sum_{k \in D_X^\pm} 1},$$

where the extensions are considered inside a fixed algebraic closure of $\mathbb{Q}$. This is called the Cohen–Lenstra moment of $G$. Note that this is a slight abuse of terminology, as $E\pm(A)$ and $E\pm(A)$ differ by a factor of $\#\Aut(A)$ whenever $A$ is a finite abelian group of odd order.

**Remark 1.1.** The restriction to counting extensions $K/k$ which are Galois over $\mathbb{Q}$ is mostly for convenience. Extensions which are Galois over $\mathbb{Q}$ are more easily counted with the methods in this paper. Any unramified extension $K/k$ has an unramified Galois closure $\bar{K}/k$ which is Galois over $\mathbb{Q}$, which means this field is counted in $E\pm(G)$ for $G = \text{Gal}(\bar{K}/k)$.

The Cohen–Lenstra heuristics for real/imaginary quadratic fields are true for every finite abelian $p$-group $A_p$, $p \neq 2$ if and only if the following equalities hold for the moments corresponding to each finite abelian group $A$ of odd order:

$$E^+(A) = \frac{1}{\#A \#\Aut(A)}, \quad E^-(A) = \frac{1}{\#\Aut(A)}.$$

For a nonabelian group $G$, even if the group is restricted to be of odd order, the above equalities do not necessarily hold (see [1], [3], and [4] for evidence and examples of this). In [19] Melanie Matchett Wood gives conjectural values for $E\pm(G)$ for arbitrary groups $G$, which is a generalization of the Cohen–Lenstra heuristics. Namely, she conjectures that $E\pm(G)$ should be infinite whenever there is more than one conjugacy class of elements of order two in $G \rtimes C_2$ not in $G$ (for certain semidirect products of $G$ by $C_2$ described in Section 2) and finite otherwise. The main goal of this paper is to determine $E\pm(G)$ in several nonabelian cases, confirming Wood’s conjecture in those cases.

In Section 2, we discuss necessary properties for a group $G$ to have nonzero $E\pm(G)$, namely that $G$ must have a particular extension $G \hookrightarrow G \rtimes C_2$ referred to as a GI-extension. [11] can then be used to conclude that, in a certain asymptotic sense, almost all nonabelian $p$-groups have $E\pm(G) = 0$. In Section 3, we determine the number of GI-extensions for the
group of affine linear transformations \{x \mapsto ax + b : a, b \in \mathbb{F}_q \text{ with } a^d = 1\} for each \(q\) and \(d\). Notably, infinitely many of these groups have no GI-extensions and so also have \(E^\pm(G) = 0\).

Extending work of Lemmermeyer [13], in Section 4 we consider the quaternion and the dihedral groups of order 8, \(Q_8\) and \(D_4\). For both groups, we use analytic methods to show that \(E^\pm(G) = \infty\).

Lastly, we address the case of so-called trivial GI-extensions, i.e. those groups for which the corresponding GI-extension is given by \(G \hookrightarrow G \times C_2\) with the trivial action of \(C_2\) on \(G\). We give sufficient conditions for \(E^\pm(G) = \infty\), which are in particular predicted by Malle’s conjecture.

Acknowledgments. I would like to thank my advisor Nigel Boston, as well as Melanie Matchett Wood and Simon Marshall for many helpful conversations and advice. I would especially like to thank the anonymous referees and the editor Jürgen Klüners for many helpful comments and suggestions, as well as their patience during the peer review stage.

2. GI-extensions

Given an unramified extension \(K/\mathbb{Q}(\sqrt{D})\) normal over \(\mathbb{Q}\), \(\text{Gal}(K/\mathbb{Q})\) is generated by its inertia subgroups all of which necessarily have order 1 or 2. Moreover, the nontrivial inertia groups of order 2 are not contained in \(\text{Gal}(K/\mathbb{Q}(\sqrt{D}))\). This motivated Boston to make the following definition [2]:

**Definition 2.1.** Given \(G \trianglelefteq G'\) of index 2, we say \(G \hookrightarrow G'\) is a GI-extension of \(G\) if \(G'\) is generated by involutions (elements \(g \in G'\) with \(g^2 = 1\)) not contained in \(G\).

Here the GI can be taken to stand for “Generated by Involutions”. Boston gives an equivalent formulation of this definition [2]:

**Lemma 2.2.** \(G'\) is a GI-extension of \(G\) iff \(G' \cong G \rtimes C_2\), where \(C_2\) acts on \(G\) by an automorphism \(\sigma \in \text{Aut}(G)\) such that \(G\) is generated by \(\{g \in G : g^\sigma = g^{-1}\}\).

Notice that GI can coincidentally be taken to stand for “Generator Inverting”. As such, we call any \(\sigma\) satisfying the above condition a GI-automorphism of \(G\). Boston proves a more detailed correspondence between these two perspectives [2]:

**Corollary 2.3.** There is a bijection between GI-extensions of \(G\) up to isomorphism and \(\{C \subset \text{Out}(G) : C\text{ is a conjugacy class containing the coset of a GI-automorphism } \sigma \text{ of } G\}\).

Here \(\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)\) denotes the group of automorphisms modulo conjugations and an isomorphism of GI-extensions \(G'\) and \(G''\) of \(G\) is defined to be a group isomorphism \(\phi : G' \rightarrow G''\) such that \(\phi(G) = G\).
We provide some examples in the following lemma.

**Lemma 2.4.**

1. If $A$ is an abelian group, then $A$ has a unique GI-extension given by the automorphism $\sigma(a) = -a$.
2. $G \times C_2$ is a GI-extension of $G$ iff $G$ is generated by elements of order 2.
3. $S_n$ is a GI-extension of $A_n$.

**Proof.**

(1). Suppose $A$ has a GI-extension $G' \cong A \times C_2$. Then by Lemma 2.2 $A$ is generated by elements $\{a \in A : a^\sigma = -a\}$ for $\sigma$ the nontrivial element in $C_2$. $A$ is abelian, so this implies $a^\sigma = -a$ for all $a \in A$.

(2). $G \times C_2$ is a GI-extension of $G$ iff $G$ is generated by $\{g \in G : g^\sigma = g^{-1}\}$ for $\sigma$ the nontrivial element in $C_2$ by Lemma 2.2. But $g^\sigma = g$ in $G \times C_2$, so $\{g \in G : g^\sigma = g^{-1}\} = \{g \in G : g^2 = 1\}$.

(3). $A_n$ is a normal subgroup of index 2 in $S_n$. $S_n$ is generated by transpositions, which are elements of order 2 not contained in $A_n$, making it a GI-extension. \qed

**Corollary 2.5.** There exist groups $G$ with more than one non-isomorphic GI-extension.

**Proof.** This follows from points 2 and 3 in the above lemma, as $A_n$ is generated by elements of order 2 for $n \geq 5$ and $S_n \not\cong A_n \times C_2$. \qed

In generalizing the Cohen–Lenstra heuristics to nonabelian groups, it is more useful to partition the question into cases based on the isomorphism class of the GI-extension $\text{Gal}(K/\mathbb{Q})$ of $\text{Gal}(K/\mathbb{Q}(\sqrt{D}))$ to account for the differences in the action. Consider the following generalization made by Bhargava [1]: we find the expected number of times the pair $(G, G')$ with $G \leq G'$ occurs as $(\text{Gal}(K/\mathbb{Q}(\sqrt{D})), \text{Gal}(K/\mathbb{Q}))$ where $G'$ is a GI-extension of $G$. Define

$$E^\pm(G, G') := \lim_{X \to \infty} \frac{\sum_{k \in D_X^\pm} \# \left\{ K/k \text{ unramified : Gal}(K/\mathbb{Q}(\sqrt{D})) = G, \text{Gal}(K/\mathbb{Q}) = G' \right\}}{\sum_{k \in D_X^\pm} 1}.$$ 

Note that this does not alter the Cohen–Lenstra moments for abelian groups, as all abelian groups have a unique GI-extension. When expressed in this form, Bhargava proved that for $n = 3, 4, 5$:

$$E^\pm(S_n, S_n \times C_2) = \infty, \quad E^+(A_n, S_n) = \frac{1}{n!}, \quad E^-(A_n, S_n) = \frac{1}{2(n-2)!}.$$
In general, one has $E^\pm(G) = \sum_{G'} E^\pm(G, G')$ where the sum is over possible GI-extensions of $G$, so solving for $E^\pm(G, G')$ for each GI-extension $G'$ of $G$ will give us $E^\pm(G)$. As a consequence, if $G$ does not have any GI-extensions then there cannot exist any unramified extensions $K/\mathbb{Q}(\sqrt{D})$ Galois over $\mathbb{Q}$ with $\text{Gal}(K/\mathbb{Q}(\sqrt{D})) \cong G$. In this case the numerator of $E^\pm(G)$ is identically 0 for all $X$, forcing $E^\pm(G) = 0$. An example of this phenomenon is given by the following corollary:

**Corollary 2.6.** For primes $p \neq 2$, infinitely many finite $p$-groups $G$ do not have a GI-extension. In particular, $E^\pm(G) = 0$. Moreover, this is true of “asymptotically almost all” (in the sense of [11]) finite $p$-groups.

**Proof.** Helleloid–Martin [11] show that infinitely many $p$-groups have automorphism group also a $p$-group. A GI-automorphism necessarily has order dividing 2, so for $p \neq 2$ infinitely many finite $p$-groups have at most one such automorphism, the identity. This is a GI-automorphism iff the group is generated by elements of order 2, which is not the case for $p \neq 2$.

Moreover, Helleloid and Martin [11] show that the number of $p$-groups $G$ with $\text{Aut}(G)$ also a $p$-group is “asymptotically almost all $p$-groups” when $p$-groups with a fixed lower $p$-length are ordered by the number of generators, or when $p$-groups with a fixed number of generators are ordered by the lower $p$-length. This suggests that having a GI-extension may not be typical among finite groups, see [11] for more details. \hfill \Box

In the next section we present another infinite family of groups without GI-extensions.

### 3. A family of groups without GI-extensions

**Definition 3.1.** Let $q = p^n$ be a prime power and $d \mid q - 1$. Define $G(q, d) = \{ x \mapsto ax + b : a, b \in \mathbb{F}_q \text{ with } a^d = 1 \}$.

Equivalently, $G(q, d) \cong C_p^n \rtimes C_d$ where $C_p^n$ is the additive group of $\mathbb{F}_q$, and $C_d \leq \mathbb{F}_q^\times$ acts on it by multiplication.

The goal of this section will be to determine how many GI-extensions the group $G(q, d)$ has for each choice of $q$ and $d$. Our strategy will be to realize the automorphism group of $G(q, d)$ as a matrix group, and use this to determine what form a GI-automorphism can take as a matrix acting on $G(q, d)$.

The action of $G(q, d)$ on $\mathbb{F}_q^+$ makes it a Frobenius group (see [17, p. 252] or [18]):

**Definition 3.2.** A group $G$ is a Frobenius group if there is an action of $G$ on some set $X$ such that every nonidentity element has at most one fixed point and at least one nonidentity element has a fixed point. Then
the collection of elements with no fixed points together with the identity form a normal subgroup called the Frobenius kernel $K$ and $G/K = H$ is called the Frobenius complement.

In this situation $G$ can be seen to be isomorphic to a semidirect product $K \rtimes H$ and has a trivial center $Z(G) = 1$.

$G(q,d)$ is a Frobenius group acting on $\mathbb{F}_q$ as affine linear transformations, and in this situation we get $K \cong C^n_p$ and $H \cong C_d$. We consider this viewpoint in order to take advantage of a recent result due to Wang [18, Lemma 2.3]:

**Corollary 3.3.** Let $G \cong K \rtimes \phi H$ be a Frobenius group with abelian Frobenius kernel $K$ and action $\phi : H \to \text{Aut}(K)$. Then $\text{Aut}(G) = K \rtimes A$ is an internal semidirect product between the following subgroups:

1. $K \leq G$ is the Frobenius kernel of $G$, identified with the inner automorphisms of $G$ given by conjugation by elements of $K$, and
2. $A \leq \text{Aut}(G)$ is the subgroup of automorphisms $\alpha$ satisfying $\alpha(H) = H$, which satisfies $A \cong N_{\text{Aut}(K)}(\phi(H)) \leq \text{Aut}(K)$ by the map $\alpha \mapsto \alpha|_K$ with the natural action on $K$.

This decomposition induces an embedding $\text{Aut}(G) \hookrightarrow \text{Hol}(K)$ via the map $(k, \alpha) \mapsto (k, \alpha|_K)$.

Here we take the holomorph $\text{Hol}(K)$ to denote $K \rtimes \text{Aut}(K)$ with the natural action and $N_G(H)$ is the normalizer of $H$ in $G$. Lemma 2.2 in Wang’s paper takes advantage of the fact that $G$ has trivial center, i.e. $Z(G) = 1$, so that $G$ may be identified with $\text{Inn}(G) \leq \text{Aut}(G)$ the automorphisms given by conjugation. Using this identification, Wang views $K$ as a subgroup of $\text{Aut}(G)$ and shows that all automorphisms of $G$ are determined by conjugation by an element of $K$ and another automorphism of $K$.

We then necessarily have an explicit embedding of $\text{Aut}(G(q,d))$ in $\text{Hol}(C^n_p)$. In particular we can realize these as matrix groups (that are consistent with respect to the embedding):

**Lemma 3.4.** Let $x_d \in \mathbb{F}_q^\times$ be an element of multiplicative order $d$. $x_d$ acts on the additive group $\mathbb{F}_q^+ \cong C^n_p$ by multiplication, so identify $x_d$ with the matrix $X_d \in \text{GL}_n(\mathbb{F}_p) = \text{Aut}(C^n_p)$ defined by $X_d v = x_d v$. Then

\[
\text{Hol}(C^n_p) \cong \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \in \text{GL}_{n+1}(\mathbb{F}_p) : A \in \text{GL}_n(\mathbb{F}_p), b \in \mathbb{F}_p^n \right\},
\]

\[
G(q,d) \cong \left\{ \begin{pmatrix} X_d^k & b \\ 0 & 1 \end{pmatrix} \in \text{GL}_{n+1}(\mathbb{F}_p) : 0 \leq k < d, b \in \mathbb{F}_p^n \right\}
\]

are groups of block upper triangular matrices, with an $n \times n$ and a $1 \times 1$ block on the diagonal.
Proof. Let $H$ be a subgroup of $\text{GL}_n(\mathbb{F}_p) = \text{Aut}(C^n_p)$. Then there is a semidirect product decomposition

$$\left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} : A \in H, b \in \mathbb{F}_p^n \right\} \simeq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p^n \right\} \rtimes \left\{ \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} : A \in H \right\},$$

where the action is given by conjugation. These groups are isomorphic to $\mathbb{F}_p^n$ and $H$ respectively, where conjugation induces the natural action of $H \leq \text{GL}_n(\mathbb{F}_p)$ on $\mathbb{F}_p^n$ by linear transformations. The lemma follows from taking $H = \text{GL}_n(\mathbb{F}_p)$ and $\langle X_d \rangle$ respectively.

Throughout the rest of this section, we fix a choice of isomorphisms between $\text{Aut}(C^n_p)$ and $\text{GL}_n(\mathbb{F}_p)$, as well as between $\text{Hol}(C^n_p)$ and $G(q,d)$ with the groups of upper triangular block matrices in Corollary 3.3. Under this identification, the map $\text{Aut}(G) = K \rtimes \mathcal{A} \to \text{Hol}(C^n_p)$ given by

$$(b, \alpha) \mapsto \begin{pmatrix} \alpha |_{C^n_p} & b \\ 0 & 1 \end{pmatrix}$$

gives an embedding $\text{Aut}(G(q,d)) \hookrightarrow \text{Hol}(C^n_p)$ which induces the natural embedding of $G(q,d)$ when identified with $\text{Inn}(G(q,d)) \leq \text{Aut}(G(q,d))$. We take advantage of these identifications to study the automorphisms of $G(q,d)$ as matrices.

Applying the definition of GI-automorphisms to matrix operations gives the following:

**Lemma 3.5.** Fix a matrix $\begin{pmatrix} T & a \\ 0 & 1 \end{pmatrix} \in \text{Hol}(C^n_p)$ of order 1 or 2 (i.e. such that $T^2 = 1$ and $Ta = -a$). $\begin{pmatrix} T & a \\ 0 & 1 \end{pmatrix}$ is a GI-automorphism of $G(q,d)$ iff $G(q,d)$ is generated by elements of the form $\begin{pmatrix} X^k_d & b \\ 0 & 1 \end{pmatrix}$ with $TX^k_d T = X^{-k}_d$ and $TX^k_d a + Tb + a = -X^{-k}_d b$.

**Proof.** The result follows immediately from the two matrix identities

$$\begin{pmatrix} T & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^k_d & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} T & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} TX^k_d T & TX^k_d a + Tb + a \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} X^k_d & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} X^{-k}_d & -X^{-k}_d b \\ 0 & 1 \end{pmatrix}.$$

We conclude this section with a complete classification of GI-extensions of $G(q,d)$, first separating out those without a GI-extension and then counting the number of GI-extensions for the remaining groups.

**Theorem 3.6.** $G(q,d)$ has a GI-automorphism iff there exists an integer $\ell$ such that $p^\ell \equiv -1 \text{ mod } d$, where $q = p^n$. 

Proof. If \( d = 1 \), then \( p \equiv -1 \mod 1 \) trivially. Moreover, \( G(q, 1) = C_p^m \) is abelian, which has a unique GI-automorphism sending \( x \mapsto -x \). For the rest of this proof, suppose \( d > 1 \).

\( \Rightarrow \). Let \((T^a 0 1)\) be a GI-automorphism of \( G(q, d) \). Lemma 3.5 then implies \( TX_d^{-k}T = X_d^{-k} \) for a generating set of powers of \( X_d \) in \( \langle X_d \rangle \) (and so for every power of \( X_d \)). \( T \) acts by conjugation on the matrix algebra \( \mathbb{F}_p[X_d] \subset GL_n(\mathbb{F}_p) \cup \{0\} \), so without loss of generality \( T \) acts on \( \mathbb{F}_p(x_d) \) which is isomorphic to \( \mathbb{F}_p[X_d] \) as an algebra. Conjugation of matrices is a ring automorphism, so \( T \) acts on \( \mathbb{F}_p(x_d) \) by some power of Frobenius \( \phi_p \). Thus \( x_d^{-1} = x_d^T = \phi_p^\ell(x_d) = x_d^{p\ell} \) for some \( \ell \), so that \( p\ell \equiv -1 \mod d \).

\( \Leftarrow \). Fix \( m = [\mathbb{F}_p(x_d) : \mathbb{F}_p] \). The power of Frobenius \( \phi_p^\ell \) fixes \( \mathbb{F}_p \) and maps \( x_d \mapsto x_d^{-1} \) since \( p\ell \equiv -1 \mod d \). Let \( \alpha = \phi_p^\ell \) be the involution of \( \mathbb{F}_p(x_d) \). \( \alpha \) acts on the additive group of \( \mathbb{F}_p(x_d) \), which is isomorphic to \( \mathbb{F}_p^m \) as an \( m \)-dimensional vector space. Fix a basis of \( \mathbb{F}_p(x_d) \) (such as \( 1, x_d, x_d^2, \ldots, x_d^{m-1} \)) to identify with a vector space basis of \( \mathbb{F}_p^m \) and let \( T \) be the matrix in \( GL_m(\mathbb{F}_p) \) given by the action of \( \alpha \) on \( \mathbb{F}_p^m \) through this identification. (Note: if \( d = 2 \) then \( T \) is the identity matrix, otherwise \( T \) has order 2.)

First, suppose \( \mathbb{F}_q = \mathbb{F}_p(x_d) \) i.e. \( n = m \). We will show that the matrix \((T^a 0 1)\) acting on \( G(q, d) \) by conjugation is a GI-automorphism of \( G(q, d) \). By applying Lemma 3.5 with \( a = 0 \), it suffices to show that \( G(q, d) \) is generated by elements of the form \( \left( \begin{array}{cc} X_d^k & b \\ 0 & 1 \end{array} \right) \) satisfying \( TX_d^kT = X_d^{-k} \) and \( Tb = -X_d^{-k}b \).

The first equality holds by construction, as \( Tx_d = x_d^{p\ell} = x_d^{-1} \). The second equality holds trivially for \( b = 0 \), and we can check by hand that

\[
T(x_d^k - 1) = x_d^{-k} - 1
\]

\[
= -x_d^{-k}(-1 + x_d^k)
\]

\[
= -X_d^{-k}(x_d^k - 1).
\]

It now suffices to show that the set

\[
\left\{ \left( \begin{array}{cc} X_d^k & b \\ 0 & 1 \end{array} \right) : b = x_d^k - 1 \text{ for } 0 \leq k < d \right\}
\]

is a generating set for \( G(q, d) \). Consider that

\[
\left( \begin{array}{cc} X_d^k & x_d^k - 1 \\ 0 & 1 \end{array} \right) \left( \begin{array}{cc} X_d^{-k} & 0 \\ 0 & 1 \end{array} \right) = \left( \begin{array}{cc} 1 & x_d^k - 1 \\ 0 & 1 \end{array} \right).
\]

This implies that it suffices to show that

\[
\left\{ \left( \begin{array}{cc} X_d^k & 0 \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) : b = x_d^k - 1 \text{ for } 0 \leq k < d \right\}
\]
generates $G(q, d)$. We will prove that $x_d^k - 1$ for $k = 1, 2, \ldots, d - 1$ spans $F_p(x_d) = F_q$, as this would imply that both the Frobenius kernel

$$K = C_p^m = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F_q \right\}$$

and the Frobenius complement

$$H = C_d = \left\{ \begin{pmatrix} X_k^d & 0 \\ 0 & 1 \end{pmatrix} : 0 \leq k < d \right\}$$

are generated by this set. Any set generating both $K$ and $H$ also generates $K \rtimes H \cong G(q, d)$. Notice that $\gcd(d, p) = 1$ and

$$-d = \sum_{k=1}^{d-1} (x_d^k - 1).$$

Thus

$$1 = -\frac{1}{d} \sum_{k=1}^{d-1} (x_d^k - 1)$$

is contained in the span of $x_d^k - 1$, and consequently so is $x_d^k$ for any $k$. These contain a basis of $F_p(x_d) = F_q$, concluding the proof of this case.

Now suppose $[F_q : F_p(x_d)] > 1$ and keep $T$ as above. Extend a basis $\{v_i\}$ of $F_q/F_p(x_d)$ by a basis $\{w_j\}$ of $F_p(x_d)/F_p$ to a basis $\{w_jv_i\}$ of $F_q/F_p$ ordered lexicographically. Define $\tilde{T} \in \text{GL}_n(F_p)$ to be a block diagonal matrix with $T$’s along the diagonal and consider $\left( \begin{smallmatrix} \tilde{T} & 0 \\ 0 & 1 \end{smallmatrix} \right)$. We will show that conjugation by this matrix is a GI-automorphism of $G(q, d)$. All elements of the form $\left( \begin{smallmatrix} X_k^d & bv_i \\ 0 & 1 \end{smallmatrix} \right)$ satisfy the equation in Lemma 3.5 with $a = 0$ whenever $b = x_d^k - 1$, as in the first case. This follows from the fact that $\tilde{T}w_jv_i = (Tw_j)v_i$. The first case showed that such values of $b$ span $F_p(x_d)$, so it follows that the collection of $bv_i$ span $F_q$. The same argument as in the first case then implies that the matrices $\left( \begin{smallmatrix} X_k^d & bv_i \\ 0 & 1 \end{smallmatrix} \right)$ satisfying the equations in Lemma 3.5 generate $G(q, d)$, which implies $\left( \begin{smallmatrix} \tilde{T} & 0 \\ 0 & 1 \end{smallmatrix} \right)$ is a GI-extension. \hfill $\Box$

Before counting the number of GI-extensions of $G(q, d)$ in the case that $p^\ell \equiv -1 \mod d$ for some $\ell$, we need some more information on the structure of the automorphism group. Recall the statement of Corollary 3.3 proven by Wang: $\text{Aut}(G) = K \rtimes A$, where $A \cong N_{\text{Aut}(K)}(\phi(H))$. We require more information on the structure of this normalizer in the case $G = G(q, d)$, given by the following lemma:

**Lemma 3.7.** Let $C_d \leq F_q^\times$ act on $C_p^n = F_p^n = F_q$ by multiplication. Choose a basis $\{w_jv_i\}$ of $F_q/F_p$ where $\{w_j\}$ is a basis of $F_p(x_d)/F_p$ and $\{v_i\}$ is a
basis of \( \mathbb{F}_q/\mathbb{F}_p(x_d) \). Then

\[
N_{\text{GL}_n(\mathbb{F}_p)}(C_d) = A(C_d) \times B(C_d)
\]
is an internal (left) semidirect product given by the subgroups

1. \( A(C_d) \) is the group of block diagonal powers of Frobenius, i.e.

\[
A(C_d) = \left\{ M \in \text{GL}_n(\mathbb{F}_p) : M(w_jv_i) = \phi_p^m(w_j)v_i \text{ for some } m \in \mathbb{Z} \right\}.
\]

\( A(C_d) \) is a cyclic subgroup isomorphic to \( \text{Gal}(\mathbb{F}_p(x_d)/\mathbb{F}_p) \).

2. \( B(C_d) \) is the group of \( \mathbb{F}_p[x_d] \)-linear bijections \( \mathbb{F}_q \to \mathbb{F}_q \), i.e.

\[
B(C_d) = \left\{ M \in \text{GL}_n(\mathbb{F}_p) : M(w_jv_i) = w_j\overline{M}(v_i) \text{ for some } \overline{M} \in \text{GL}(\mathbb{F}_q/\mathbb{F}_p(x_d)) \right\}.
\]

\( B(C_d) \) is a normal subgroup isomorphic to \( \text{GL}(\mathbb{F}_q/\mathbb{F}_p(x_d)) \). In general, for any \( M \in B(C_d) \) we define \( \overline{M} \in \text{GL}(\mathbb{F}_q/\mathbb{F}_p(x_d)) \) to be the image of \( M \) under this isomorphism. This is explicitly defined on the basis \( \{ v_i \} \) by \( \overline{M}v_i := Mv_i \).

Given any \( S \in N_{\text{GL}_n(\mathbb{F}_p)}(C_d) \), we define \( P_S : w_jv_i \mapsto w_jS(v_i) \). Then \( SP_S^{-1} \in A(C_d) \) and \( P_S \in B(C_d) \) is the unique decomposition of \( S \) with respect to the semidirect product factorization.

We remark that a basis-free version of this lemma exists, where the choice of section for \( A(C_d) \) is equivalent to the choice of a basis, but it will be convenient for our purposes to consider everything in terms of a fixed basis.

**Proof.** For any matrix \( S \in N_{\text{GL}_n(\mathbb{F}_p)}(C_d) \), where \( C_d = \langle X_d \rangle \) under the matrix identification, regard \( S \) as an \( \mathbb{F}_p \)-linear map \( \mathbb{F}_q \to \mathbb{F}_q \). It follows that \( S(x_dy) = SX_d(y) = SX_dS^{-1}S(y) \) for any \( y \in \mathbb{F}_q \), where \( X_d \) is the matrix given by multiplication by \( x_d \in \mathbb{F}_q \) and \( SX_dS^{-1} \in \langle X_d \rangle \) by \( S \) an element of the normalizer. Thus, \( S(x_dy) = x_d^ky \) for some integer \( k \), in particular \( S(x_d) = x_d^kS(1) \). Therefore \( SX_dS^{-1} \) is the \( \mathbb{F}_p \)-linear map given by multiplication by \( \frac{S(x_d)}{S(1)} \in \langle x_d \rangle \). This implies \( S(x_dy) = \frac{S(x_d)}{S(1)}S(y) \), and together with the fact that \( S \) is an \( \mathbb{F}_p \)-linear map we conclude that \( S(xy) = \frac{S(x)}{S(1)}S(y) \) for any \( x \in \mathbb{F}_p(x_d) \) and \( y \in \mathbb{F}_q \). In particular, \( \left( x \mapsto \frac{S(x)}{S(1)} \right) \in \text{Aut}(\mathbb{F}_p(x_d)) \) is a field automorphism i.e. is given by some power of Frobenius \( \phi_p^m \).

Define \( P_S : \mathbb{F}_q \to \mathbb{F}_q \) to be the \( \mathbb{F}_p(x_d) \)-linear map sending \( w_jv_i \mapsto w_jS(v_i) \). Then \( SP_S^{-1}(w_jv_i) = S(w_jS^{-1}(v_i)) = \frac{S(w_j)}{S(1)}v_i \) by \( w_j \in \mathbb{F}_p(x_d) \).

We also know that \( x \mapsto \frac{S(x)}{S(1)} \) acts on \( \mathbb{F}_p(x_d) \) as a power of Frobenius, so this implies \( SP_S^{-1} \in A(C_d) \). By construction, \( P_S \in B(C_d) \) so we have shown that

\[
N_{\text{GL}_n(\mathbb{F}_p)}(C_d) = A(C_d)B(C_d).
\]
It is clear from the definitions that $A(C_d) \cap B(C_d) = 1$. We show that $B(C_d)$ is a normal subgroup by showing it is closed under conjugation by elements of $A(C_d)$ (and so normal in $A(C_d)B(C_d) = N_{\text{GL}_n(F_p)}(C_d)$). Let $M \in B(C_d)$ and $S \in A(C_d)$ correspond to $\phi_p^m$. $M$ is $F_p(x_d)$-linear, so that

$$SMS^{-1}(w_jv_i) = S \left( \phi_p^{-m}(w_j)M(v_i) \right).$$

Write the coordinates of $M \in \text{GL}(F_q/F_p(x_d))$ as $M_{i,j} \in F_p(x_d)$, so that

$$SMS^{-1}(w_jv_i) = S \left( \phi_p^{-m}(w_j) \sum_k M_{i,k}v_k \right) = \sum_k S(\phi_p^{-m}(w_j)M_{i,k}v_k) = \sum_k w_j \phi_p^m(M_{i,k})v_k = w_jM^{\phi_p^m}(v_i),$$

where $M^{\phi_p^m}$ is the matrix $M$ after applying $\phi_p^m$ to each coordinate. This map, denoted $M^{\phi_p^m}$, clearly belongs to $B(C_d)$ concluding the proof. □

We will count GI-extensions by showing that each isomorphism class is represented by a GI-automorphism $(T_0 1 0 1)$ where $TP_T^{-1}$ is given by $\phi_p^\ell$ and $P_T$ is diagonal with very specific eigenvalues. We will then count the sequences of eigenvalues up to the equivalence given by Corollary 2.3 to get the following result:

**Theorem 3.8.** Suppose $p^\ell \equiv -1 \mod d$, then we have the following cases:

1. If $d \neq 2$, then $G(q,d)$ has exactly one GI-extension up to isomorphism.
2. If $d = 2$, then $G(q,d)$ has exactly $\lceil [F_q:F_p]+1 \rceil$ GI-extensions up to isomorphism.

Before proving Theorem 3.8, it may be informative to see an example of case (2): the smallest nontrivial example is $G(9,2)$, for which we can produce two GI-automorphisms as conjugation by the following matrices:

$$g_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$  

These cannot be equivalent under Corollary 2.3, as $g_1 = 1 \in G(9,2) = \text{Inn}(G(9,2))$ while $g_2 \not\in \text{Inn}(G(9,2))$, and so in $\text{Out}(G)$ $g_1$ is a representative of the trivial class while $g_2$ is not. Thus, they are not conjugate. Theorem 3.8 essentially states that this is the only property that determines the structure of GI-automorphisms, as case (2) is exactly those cases
for which \( G(q,d) \) is generated by elements of order 2 and so the identity itself is a GI-automorphism.

**Proof.** Corollary 2.3 states that there is a bijection between isomorphism classes of GI-extensions of \( G \) with conjugacy classes of elements of \( \text{Out}(G) \) which have a GI-automorphism as a representative.

Recall that Corollary 3.3 and Lemma 3.4 allow us to identify \( G(q,d) \) and \( \text{Aut}(G(q,d)) \) with subgroups \( C_p^n \rtimes C_d \) and \( C_p^n \rtimes N_{\text{Aut}(C_p^n)}(C_d) \) respectively of the upper triangular block matrix group \( \text{Hol}(C_p^n) \). Fix a basis \( \{w_jv_i\} \) for the extension \( \mathbb{F}_q/\mathbb{F}_p \) as in the previous theorem, where \( \{v_i\} \) is a basis for \( \mathbb{F}_q/\mathbb{F}_p(x_d) \) and \( \{w_j\} \) is a basis for \( \mathbb{F}_p(x_d)/\mathbb{F}_p \). Thus, automorphisms of \( G(q,d) \) are represented by matrices \((T a \atop 0 1)\) in \( \text{Hol}(C_p^n) \) with \( a \in \mathbb{F}_q \) and \( T \in N_{\text{GL}_n(\mathbb{F}_p)}(C_d) \) by the matrix representation in Lemma 3.4. We will count such matrices which satisfy the conditions in Lemma 3.5, up to equivalence in the sense of Corollary 2.3.

We first show that every GI-extension is represented by a GI-automorphism with a=0: Notice that a GI-automorphism \((0 \ 1)\) satisfies

\[
\begin{pmatrix} T & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I & T^{-1}a \\
0 & 1 \end{pmatrix}.
\]

Corollary 2.3 says that if two automorphisms belong to the same coset in \( \text{Out}(G) = \text{Aut}(G)/\text{Inn}(G) \), they then correspond to isomorphic GI-extensions. \((0 \ T^{-1}a \ 1)\) is an element of \( G(q,d) = \text{Inn}(G(q,d)), \) and so does not change the corresponding coset in \( \text{Out}(G) \). This implies that \((0 \ 0 \ 1)\) is another GI-automorphism corresponding to the same GI-extension (up to isomorphism) as \((0 \ a \ 1)\). Thus, we only need to consider matrices of the form \((0 \ 0 \ 1)\) for \( T \in N_{\text{GL}_n(\mathbb{F}_p)}(C_d) \).

Given a GI-automorphism \( \sigma = (T a \ 0 \ 1) \), the construction in Lemma 3.7 together with the work in Theorem 3.6 implies \( TP_T^{-1}(w_jv_i) = \phi_p^j(w_j)v_i \) with \( p^j \equiv -1 \mod d \). The matrix \( \begin{pmatrix} X_d^k \\ 0 \ 1 \end{pmatrix} \in \text{Aut}(G(q,d)) \) is an inner automorphism, so that

\[
\begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} TX_d^k & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X_d^k & 0 \\ 0 & 1 \end{pmatrix}
\]

belong to the same coset in \( \text{Out}(G) \), and so correspond to isomorphic GI-extensions. Conjugate automorphisms also correspond to isomorphic GI-extensions under Corollary 2.3. Note that \( SX_d^kTS^{-1} = X_d^{pm} \) for any \( S \in N_{\text{GL}_n(\mathbb{F}_p)}(C_d) \) with \( S(w_jv_i) = \phi_p^m(w_j)v_i \). This shows that the relations

\[
T \sim_1 X_d^kT \quad \text{and} \quad T \sim_2 STS^{-1}
\]

commute with each other in the sense that if there exists a \( T_1 \) such that \( T \sim_1 T_1 \sim_2 T' \) then there also exists a \( T_2 \) such that \( T \sim_2 T_2 \sim_1 T' \) (noting that \( p \) is invertible mod \( d) \), so that they define a composite relation \( \sim \) on that set of matrices \( T \) giving GI-automorphisms
Consider the set
\[ \left\{ b : \exists k \text{ s.t. } \begin{pmatrix} X^k_d & b \\ 0 & 1 \end{pmatrix} \text{ is inverted by } \sigma \right\}. \]

If \( \sigma = \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \) is a GI-automorphism then this set must contain an \( \mathbb{F}_q / \mathbb{F}_p(x_d) \) basis \( \{ u_i \} \). Let \( P \in \text{GL}(\mathbb{F}_q / \mathbb{F}_p(x_d)) \) be a change of basis matrix sending \( w_j v_i \mapsto w_j u_i \) and set \( T' = P^{-1} TP \). Then \( P_{T'} \in B(C_d) \) is given by the map \( w_j v_i \mapsto w_j P_{T'}(v_i) \) where \( P_{T'} \in \text{GL}(\mathbb{F}_q / \mathbb{F}_p(x_d)) \) is the diagonal matrix with \(-x^k_d\) along the diagonals and \( k_i \) are the exponents such that
\[ \begin{pmatrix} X^k_i & u_i \\ 0 & 1 \end{pmatrix} \text{ is inverted by } \sigma, \]
as defined in Lemma 3.7(2). Additionally, \( T'P_{T'}^{-1} \in A(C_d) \) corresponds to the power of Frobenius \( \phi_p^\ell \) where \( p^\ell \equiv -1 \mod d \). This implies that each isomorphism class of GI-extensions is represented by a GI-automorphism \( \begin{pmatrix} T & 0 \\ 0 & 1 \end{pmatrix} \) for which \( P_{T'} \in \text{GL}(\mathbb{F}_q / \mathbb{F}_p(x_d)) \) is a diagonal matrix with \(-x^k_d\) along the diagonal for some values of \( k_i \), and \( T P_{T'}^{-1}(w_j v_i) = \phi_p^\ell(w_j) v_i \). Thus, it suffices to count the number of sequences \( \{ k_i \} \) of the exponents of the eigenvalues of \( P_{T'} \) up to the equivalence laid out in Corollary 2.3. We use the equivalence relations \( \sim_1 \) and \( \sim_2 \) to produce the following equivalences between sequences \( \{ k_i \} \):

(a) If \( T \sim_1 T' \) then there exists some \( \lambda \) such that
\[ T = X^\lambda_d T' = X^\lambda_d (T' P_{T'}^{-1})(P_{T'}) = (T' P_{T'}^{-1})(X^\lambda_d P_{T'}) = (T' P_{T'}^{-1})(X^\lambda_d P_{T'}) \]
Here \( X^\lambda_d P_{T'} \) is diagonal with eigenvalues \(-x^k_d - \lambda\), which shows that the sequence of eigenvalue exponents \( \{ k_i \} \) and \( \{ k_i - \lambda \} \) correspond to isomorphic GI-extensions.

(b) Let \( S \in B(C_d) \) be such that \( S \) is a permutation matrix corresponding to some permutation \( w_j v_i \mapsto w_j v_{\beta(i)} \). Then \( S = P_S \) are permutation matrices and the coordinates of \( S \in \text{GL}_n(\mathbb{F}_p) \) are all 1 or 0 which are fixed by Frobenius. Thus
\[ T \sim_2 S T S^{-1} = P_S(T P_{T}^{-1}P_T)P_S^{-1} = (T P_{T}^{-1})(P_S^\phi P_T P_S^{-1}) = (T P_{T}^{-1})(P_T P_S). \]
Here \( P_S P_T P_S^{-1} \) is diagonal with eigenvalues \(-x_d^{k_\beta-1(i)}\), which implies that the sequence of eigenvalue exponents \{k_i\} and \{k_\beta-1(i)\} correspond to isomorphic GI-extensions for any permutation \(\beta\).

(c) Suppose \(d \neq 2\), and \(2^\nu \mid p^\ell - 1\) for some \(\nu \geq 0\). Then \(d \mid p^\ell + 1\) implies \(2^\nu d \mid p^{2\ell} - 1\). Moreover, \(d \neq 2\) implies \(\phi_p^\ell \neq \text{id}\) and \(\phi_p^{2\ell}(x_d) = x_d^{(-1)^2} = x_d \) so \(\phi_p^{2\ell} = \text{id}\), so that \([\mathbb{F}_p(x_d) : \mathbb{F}_p] = 2\ell\). As \(\mathbb{F}_p(x_d)\) is cyclic of order \(p^{2\ell} - 1\), we conclude that there exists an element of order \(2^\nu d\) in \(\mathbb{F}_p(x_d)\). We choose one such element and denote it \(x_{2^\nu d} \in \mathbb{F}_p(x_d)\). Let \(S \in B(C_d)\) be the map \(w_jv_i \mapsto w_j(x_{2^\nu m_i}v_i)\) for some sequence \(\{m_i\}\) (i.e., \(S \in \text{GL}(\mathbb{F}_q/\mathbb{F}_p(x_d))\)) is diagonal with eigenvalues \(x_{2^\nu m_i}\). Then \(S = P_S\) and

\[
T \sim_2 STS^{-1} = P_S(TP_T^{-1}P_T)P_S^{-1} = (TP_T^{-1})(P_S^{\phi_p^\ell}P_T P_S^{-1}).
\]

\(P_S^{\phi_p^\ell} P_T P_S^{-1}\) is diagonal with eigenvalues

\[
x_{2^\nu d}(x_d^{k_i})x_{2^\nu d}^{-m_i} = x_d^{k_i + \frac{p^\ell - 1}{2}m_i},
\]

which implies that the sequence of eigenvalue exponents \(\{k_i\}\) and \(\{k_i + \frac{p^\ell - 1}{2}m_i\}\) correspond to isomorphic GI-extensions for any sequence \(\{m_i\}\).

We use these relations to count the number of inequivalent sequences of eigenvalue exponents \(\{k_i\}\). (In fact, a consequence of our argument is that the relations (a), (b), and (c) completely determine the composite relation \(\sim_\).)

If \(d = 1\), then \(G(q, d)\) is abelian and necessarily has a unique GI-extension.

If \(d > 2\), let \(2^\nu \mid p^\ell - 1\). Relation (c) then implies the sequences \(\{k_i\}\) and \(\{k_i + \frac{p^\ell - 1}{2}m_i\}\) correspond to isomorphic GI-extensions for each choice of \(\{m_i\}\). Note that \(d \mid p^\ell + 1\), so \((d, p^\ell - 1) \mid 2\). By construction \(\frac{p^\ell - 1}{2^\nu}\) is odd, so that \((d, \frac{p^\ell - 1}{2^\nu}) = 1\). This implies that \(\frac{p^\ell - 1}{2^\nu}\) is invertible modulo \(d\), and thus \(\frac{p^\ell - 1}{2^\nu}m_i\) spans all sequences modulo \(d\) as \(\{m_i\}\) varies. This implies that all sequences of eigenvalue exponents correspond to isomorphic GI-extensions, and so there can only be one GI-extension up to isomorphism. This concludes the proof of case (1).

For (2), the case \(d = 2\), we note that \(\mathbb{F}_p(x_2) = \mathbb{F}_p\) is the trivial extension of size \(p^\ell = p\), which is decidedly different from case (1). In this case, \(\phi_p^\ell = \text{id}\) is the trivial map, and \(A(C_2) = \text{Gal}(\mathbb{F}_p(x_2)/\mathbb{F}_p) = 1\) is trivial. Thus \(T = P_T\).
The unordered set of eigenvalues of a diagonalizable matrix is automatically preserved under conjugation, thus \( \sim_2 \) only produces the relation (b) given above: that \( \{k_i\} \) and \( \{k_{\beta(i)}\} \) correspond to isomorphic GI-extensions for all permutations \( \beta \). As an exponent of \( x_2 \), the representatives of the eigenvalue exponents \( k_i \) modulo 2 can only be 0 or 1. There are \( [\mathbb{F}_q : \mathbb{F}_p(x_2)] = [\mathbb{F}_q : \mathbb{F}_p] \) indices \( i \), and so \( [\mathbb{F}_q : \mathbb{F}_p] + 1 \) unordered sequences \( \{k_i\} \) of exactly \( [\mathbb{F}_q : \mathbb{F}_p] \) zeros and ones.

Lastly, \( \sim_1 \) gives exactly relation (a) above, that \( \{k_i\} \) and \( \{k_i - \lambda\} \) correspond to isomorphic GI-extensions. If \( \lambda = 0 \) this is trivial, but if \( \lambda = 1 \) this switches all the zeros and ones in the sequence \( \{k_i\} \). Aside from the possible middle sequence where the number of zeros and ones are the same, this divides the number of representatives by two. If \( [\mathbb{F}_q : \mathbb{F}_p] \) is even there is a middle term and we get \( \frac{[\mathbb{F}_q : \mathbb{F}_p]}{2} + 1 \) equivalence classes of \( \{k_i\} \). If \( [\mathbb{F}_q : \mathbb{F}_p] \) is odd, then there is no middle term and we get \( \frac{[\mathbb{F}_q : \mathbb{F}_p] + 1}{2} \) equivalence classes of \( \{k_i\} \). Putting these together gives \( \left\lfloor \frac{[\mathbb{F}_q : \mathbb{F}_p] + 1}{2} \right\rfloor \) equivalence classes of \( \{k_i\} \), which correspond to precisely \( \left\lfloor \frac{[\mathbb{F}_q : \mathbb{F}_p] + 1}{2} \right\rfloor \) distinct isomorphism classes of GI-extensions. \( \square \)

4. Unramified Quaternion Extensions

The goal of this section is to take the classification of unramified \( Q_8 \) and \( D_4 \) extensions of quadratic fields given by Lemmermeyer [13] and convert it into an asymptotic expected number of such extensions as the discriminant tends toward \( \pm \infty \).

We recall Lemmermeyer’s main result for \( Q_8 \) below (paraphrased by combining the statements of Proposition 4 and Theorem 1 in [13]). Lemmermeyer references a group \( D_4 \oplus \mathbb{Z} C_4 \), which denotes the direct sum of \( D_4 \oplus C_4 \) where the center \( \mathbb{Z}(D_4) \) is identified with the unique subgroup \( C_2 \leq C_4 \). If we write \( D_4 = \langle a, b : a^4 = b^2 = bab^{-1}a = 1 \rangle \) and \( C_4 = \langle c : c^4 = 1 \rangle \), then

\[
D_4 \oplus C_4 = \langle a, b, c : a^4 = b^2 = c^4 = bab^{-1}a = acac^{-1}c^{-1} = bcb^{-1}c^{-1} = c^2a^2 = 1 \rangle.
\]

Theorem 4.1. Let \( k \) be a quadratic number field with absolute discriminant \( \epsilon d \) for some \( \epsilon \in \{\pm 1\} \) and integer \( d > 0 \). There exists an unramified extension \( M/k \) with \( \text{Gal}(M/k) \cong Q_8 \) which is normal over \( \mathbb{Q} \) if and only if

1. \( \text{Gal}(M/\mathbb{Q}) \cong D_4 \oplus \mathbb{Z} C_4 \),
2. there is a factorization \( \epsilon d = \epsilon d_1 d_2 d_3 \) called a \( Q_8 \)-factorization into three coprime quadratic discriminants \( d_1, d_2, \) and \( d_3 \), where \( d_1, d_2, d_3 > 0 \),
3. for all primes \( p_i \mid d_i \), \( \left( \frac{\epsilon d_1 d_2}{p_3} \right) = \left( \frac{\epsilon d_1 d_3}{p_2} \right) = \left( \frac{\epsilon d_2 d_3}{p_1} \right) = +1 \).

A “quadratic discriminant” is an integer which occurs as the discriminant of some quadratic extension of \( \mathbb{Q} \). In particular, an integer \( d \in \mathbb{Z} \) is a
quadratic discriminant if \( d \equiv 1 \mod 4, 0 \mod 8, \) or \(-4 \mod 16\) and \( p^2 \nmid d \) for any odd prime \( p \).

Combining Lemmermeyer’s propositions 5 and 6, we conclude that every such field \( M \) is given by \( L(\sqrt{\mu}) \) for \( L = \mathbb{Q}(\sqrt{ed_1}, \sqrt{d_2}, \sqrt{d_3}) \) and a particular \( \mu \in L \). Moreover, Lemmermeyer proves that for any other unramified \( Q_8 \)-extensions \( M'/k \) such that \( L \subset M' \) there necessarily exists some quadratic discriminant \( \delta \mid ed \) such that \( M' = L(\sqrt{\delta \mu}) \). \( L(\sqrt{\delta' \mu}) \) and \( L(\sqrt{\delta'' \mu}) \) give the same extension if and only if \( \sqrt{\delta(\delta')^{-1}} \in L = \mathbb{Q}(\sqrt{ed_1}, \sqrt{d_2}, \sqrt{d_3}) \). This induces an equivalence relation on the set of quadratic discriminants \( \delta | ed \) given by \( \delta \sim \delta' \) if and only if \( \delta \delta' \in (L^*)^2 = (\mathbb{Q}^*)^2(\mathbb{Z}^*)^2 \delta_2 d_2 \delta_3 d_3 \). The number of quadratic discriminants dividing \( ed \) is given by

\[
\begin{cases}
2^\omega(d) & \text{if } d \not\equiv 0 \mod 8 \\
2^\omega(d)+1 & \text{if } d \equiv 0 \mod 8,
\end{cases}
\]

where \( \omega(n) \) is the number of distinct prime divisors of \( n \). The quadratic discriminants dividing \( d \) form a group under multiplication modulo squares, and the equivalence relation is given by the subgroup generated by \( \mathbb{Q}_8 \)-extensions \( M/k \) with \( L \subset M \) is the size of a quotient group, which is given by

\[
\begin{cases}
2^{\omega(d_1)-1}2^{\omega(d_2)-1}2^{\omega(d_3)-1} & \text{if } d \not\equiv 0 \mod 8 \\
2^{\omega(d_1)}2^{\omega(d_2)-1}2^{\omega(d_3)-1} & \text{if } d \equiv 0 \mod 8.
\end{cases}
\]

A factorization \( ed = (ed_1)d_2 d_3 \) is a \( Q_8 \)-factorization if the following equals 1 (and it equals 0 otherwise):

\[
(4.1) \quad \frac{1}{2^\omega(d)} \prod_{p|d} \left(1 + \left(\frac{ed_1 d_2}{p}\right)\right) \left(1 + \left(\frac{ed_1 d_3}{p}\right)\right) \left(1 + \left(\frac{d_2 d_3}{p}\right)\right).
\]

Each such factorization corresponds to the field \( L = \mathbb{Q}(\sqrt{ed_1}, \sqrt{d_2}, \sqrt{d_3}) \) up to permuting the factors, so that the number of unramified \( Q_8 \)-extensions of a quadratic number field \( k \) with discriminant \( ed \) is given by

\[
(4.2) \quad \alpha_{ed} = \frac{1}{8B} \sum_{d=d_1 d_2 d_3} \prod_{p|d} \left(1 + \left(\frac{ed_1 d_2}{p}\right)\right) \left(1 + \left(\frac{ed_1 d_3}{p}\right)\right) \left(1 + \left(\frac{d_2 d_3}{p}\right)\right).
\]

Here the sum is over discriminant factorizations \( ed = (ed_1)d_2 d_3 \). \( B \) accounts for symmetry in the factorization as well as the slight difference in the case \( d \equiv 0 \mod 8 \), and is given by

\[
B = \begin{cases}
2 & \text{if } ed < 0, \ d \not\equiv 0 \mod 8, \\
1 & \text{if } ed < 0, \ d \equiv 0 \mod 8, \\
6 & \text{if } ed > 0, \ d \not\equiv 0 \mod 8, \\
3 & \text{if } ed > 0, \ d \equiv 0 \mod 8.
\end{cases}
\]
This is all a rephrasing of the conditions for a $Q_8$-factorization given in
Lemmermeyer’s paper.

The goal of this section is to show that $E^\pm(Q_8) = \infty$. Lemmermeyer’s
work tells us that $E^\epsilon(Q_8) = \lim_{X \to \infty} \frac{\sum_{d < X} \epsilon d}{\sum_{d < X} 1}$,
where the sum is over $0 < d < X$ such that $\epsilon d$ is a quadratic discriminant.
The denominator is asymptotic to a constant times $X$, so it suffices to show that
$$\lim_{X \to \infty} \frac{1}{X} \sum_{d < X} a_{\epsilon d} = \infty.$$

The big idea from this section is to analyze the Dirichlet series $\sum a_{\epsilon d} d^{-s}$
and use a Tauberian theorem to determine the asymptotic behavior of $\sum_{d < X} a_{\epsilon d}$.

In fact, in order to show $E^\pm(Q_8) = \infty$ we only need a lower bound for $\frac{1}{X} \sum_{d < X} a_{\epsilon d}$
which tends to $\infty$ as $X \to \infty$. We get this lower bound by
only summing over odd quadratic discriminants $\epsilon d$. This allows us to avoid
some technical issues at the prime 2.

For the remainder of this section let $\epsilon d$ be an odd quadratic discrimi-
nant. We partition the set of factorizations $\epsilon d = (\epsilon d_1)d_2d_3$
into families of factorizations with $d_1, d_2$ fixed and $d_3 = m$ varying over odd real quadratic
discriminants, so that we may write
$$\sum_{d < X \atop d \text{ odd}} a_{\epsilon d} = \sum_{d_1, d_2} \left( \sum_{m < \frac{X}{d_1d_2}} a_{\epsilon d_1d_2m} \right),$$
where
$$a_{\epsilon d_1d_2m} = \frac{1}{8B} \prod \left( 1 + \left( \frac{\epsilon d_1m}{p} \right) \right) \left( 1 + \left( \frac{d_2m}{p} \right) \right) \prod \left( 1 + \left( \frac{\epsilon d_1d_2}{q} \right) \right)$$
$$= \frac{1}{8B} \sum_{b|d_2} \left( \frac{\epsilon d_1m}{b} \right) \sum_{a|d_1} \left( \frac{d_2m}{a} \right) \prod \left( 1 + \left( \frac{\epsilon d_1d_2}{q} \right) \right).$$

Note that when expanding the product we would get a sum of $a \mid d_1d_2$, but
$\left( \frac{d_2m}{a} \right) = 0$ if $(a, d_2) \neq 1$, and likewise for $b$, so only the terms with $a \mid d_1$
contribute a nonzero value to the summation.

We will describe the asymptotic behavior of the inner summation by
examining the corresponding Dirichlet series, finding the location and order
of the rightmost pole, and applying a Tauberian theorem.
Lemma 4.2. Let $D_\epsilon(s,d_1,d_2) = \sum_{d_1,d_2 \mid d} a_{\epsilon d_1,d_2} d^{-s}$ where the sum is over the absolute values of imaginary (respectively real) odd quadratic discriminants where $\epsilon = -1$ (respectively $\epsilon = 1$). Then $D_\epsilon(s,d_1,d_2)$ is equal to

$$(d_1d_2)^{-s} \frac{1}{16B} \sum_{a \mid d_1} \sum_{b \mid d_2} \sum_{m \in A_{\epsilon d_1,d_2}^+} 2^{\omega(m)} \left( \frac{\epsilon d_1m}{b} \right) \left( \frac{d_2m}{a} \right) (1 + \chi_4(m)) m^{-s},$$

where $A_\kappa^+ = \{ m \in \mathbb{N} : \forall \text{ primes } q \mid m, (\frac{n}{q}) = \kappa \text{ and } m \text{ odd squarefree} \}$. Moreover $D_\epsilon(s,d_1,d_2)$ is holomorphic for $\Re(s) > 1$.

Proof. The decomposition follows immediately from setting $d = d_1d_2m$ and $d_3 = m$ in the definition of $a_{\epsilon d_1,d_2}$, noting that

$$\prod_{q \mid m} \left( 1 + \left( \frac{\epsilon d_1d_2}{q} \right) \right) = \begin{cases} 2^{\omega(m)} & m \in A_{\epsilon d_1,d_2}^+, \\ 0 & \text{else}. \end{cases}$$

We will show here that the series converges absolutely for $\Re(s) > 1$. Indeed, we have an upper bound of

$$|D_\epsilon(s,d_1,d_2)| \leq (d_1d_2)^{-\Re(s)} \sum_{a \mid d_1} \sum_{b \mid d_2} \sum_{m=1}^{\infty} 2^{\omega(m)} (2\mu(m))^2 m^{-\Re(s)} \leq 2(d_1d_2)^{-\Re(s)} \left( \sum_{a \mid d_1} \sum_{b \mid d_2} 1 \right) \zeta(\Re(s))^2,$$

where the last line follows from $2^{\omega(m)}$ being equal to the number of divisors of a squarefree number $m$. This converges absolutely for $\Re(s) > 1$ by noting that $(d_1d_2)^{-s}$ is entire and $\zeta(s)$ converges absolutely for $\Re(s) > 1$. □

The factor outside the summations, $(d_1d_2)^{-s} \frac{1}{16B}$, is holomorphic and zero-free on all of $\mathbb{C}$, and so may essentially be ignored when determining the locations and orders of poles. We will deal with each summand on the right as follows:

Definition 4.3. Given a primitive Dirichlet character $\chi$, $\epsilon \in \{ \pm 1 \}$, define

$$M_\epsilon^\kappa(s,\chi) = \sum_{m \in A_\kappa^+} 2^{\omega(m)} \chi(m)m^{-s}.$$

This is defined so that we have the following decomposition:

$$D_\epsilon(s,d_1,d_2) = (d_1d_2)^{-s} \frac{1}{16B} \sum_{a \mid d_1} \sum_{b \mid d_2} \left( \frac{\epsilon d_1}{b} \right) \left( \frac{d_2}{a} \right)$$

$$\cdot \left( M_{\epsilon d_1,d_2}^+ \left( s, \left( \frac{\cdot}{\cdot ab} \right) \right) + M_{\epsilon d_1,d_2}^+ \left( s, \chi_4 \left( \frac{\cdot}{\cdot ab} \right) \right) \right).$$
We will show that \(M_\chi^+(s, \chi)\) can be meromorphically continued to an open neighborhood of \(\{s \in \mathbb{C} : \Re(s) \geq 1\}\) with one simple pole at \(s = 1\) if \(\chi = 1\) or \((\frac{a}{b})\) and is holomorphic otherwise. This will tell us that \(D_\chi(s, d_1, d_2)\) has only one simple pole in this neighborhood at \(s = 1\) and what its residue is. From here, \(D_\chi(s, d_1, d_2) = \sum_{d|d_1d_2} a_{ed,d_1,d_2}d^{-s}\) is a Dirichlet series with positive coefficients, converges for \(\Re(s) > 1\), and can be meromorphically continued to an open neighborhood of \(\{s \in \mathbb{C} : \Re(s) \geq 1\}\) with one simple pole at \(s = 1\). A standard Tauberian theorem (such as the one in [7]) then implies

\[
\sum_{d < X : d|d_1d_2} a_{ed,d_1,d_2} \sim \text{Res}_{s=1} D_\chi(s, d_1, d_2) X.
\]

We begin with the following properties for \(M_\chi^e(s, \chi)\):

**Lemma 4.4.** \(M_\chi^e(s, \chi)\) satisfies the following properties:

- It is holomorphic for \(\Re(s) > 1\),
- \(M_\chi^e(s, \chi) = \prod (\frac{\chi(n)}{n}) = (1 + 2\chi(q)q^{-s})\),
- \(M_\chi^+(s, \chi) = M_\chi^+(s, \chi (\frac{n}{q}))\),
- \(M_\chi^+(s, \chi)M_\chi^-(s, \chi) = \prod_{q|n} (1 + 2\chi(q)q^{-s})^{-1} \prod_q (1 + 2\chi(q)q^{-s})\),
- \(\frac{M_\chi^+(s, \chi)}{M_\chi^+(s, \chi)} = \prod (\frac{\chi(n)}{n}) = -(1 - 4\chi^2(q)q^{-2s})^{-1} \prod_q (1 + 2\chi(q)q^{-s})\),
- \(\frac{M_\chi^-(s, \chi)}{M_\chi^+(s, \chi)} = \prod (\frac{\chi(n)}{n}) = (1 - 4\chi^2(q)q^{-2s})^{-1} \prod_q (1 - 2\chi(q)q^{-s})\),

where each product is restricted to \(q \neq 2\).

The proofs of these follow by computation of their Euler products. We will show that \(M_\chi^e\) is both zero- and pole-free on some domain containing \(\Re(s) \geq 1\) with a possible exception at \(s = 1\), but first we must prove the following lemma:

**Lemma 4.5.** Consider the series given by the Euler product \(\prod_{p|b}(1 + b\chi(p)p^{-s})\) for \(b\) a nonzero integer. This series is meromorphic on the zero-free region of \(L(s, \chi)\), whose only pole is \(s = 1\) of order \(b\) if \(\chi = 1\). It is holomorphic on the zero-free region of \(L(s, \chi)\) if \(\chi \neq 1\).

**Remark 4.6.** This lemma remains true if \(b < 0\), where a pole of order \(b\) is taken to mean a zero of order \(-b > 0\).

**Proof.**

\[
\prod_{p|b} (1 + b\chi(p)p^{-s}) = \prod_{p|b} \left(1 + b\chi(p)p^{-s}\right) \left(1 + \sum_{k=1}^{[b]} (-1)^k \chi(p)^k p^{-ks}\right) \left(1 - sgn(b)\chi(p)p^{-s}\right)^{|b|}.
\]
This identity is achieved by multiplying the top and bottom by 
$$(1 - \text{sgn}(b)\chi(p)p^{-s})|b|,$$
where $\text{sgn}(b)$ is the sign of $b$. In particular, the numerator has no term which is linear in $p^{-s}$. Thus a computation with natural logs shows the numerator is holomorphic on $\Re(s) > \frac{1}{2}$. Denote the numerator by $G(s)$. Then

$$\prod_{p \nmid b} \left(1 + b\chi(p)p^{-s}\right) = \begin{cases} 
G(s) \prod_{p \mid |b|} G(s) \left(\frac{L(s,\chi)}{L(2s,\chi^2)}\right)_b & b > 0, \\
G(s) \prod_{p \mid |b|} \left(1 + \chi(p)p^{-s}\right)^{-b} & b < 0.
\end{cases}$$

The result is clear from this decomposition and the fact that $L(s,\chi)$ is holomorphic on $C$ if $\chi \neq 1$ and meromorphic with a unique simple pole at $s = 1$ of order $b$ if $\chi = 1$, noting that a pole of negative order is equivalent to a zero.

We remark that even if $\chi$ is imprimitive, $L(s,\chi)$ carries the same analytic properties as that of the corresponding primitive character. Suppose $\chi \mod n$ is induced by $\chi^* \mod m$ for some $m \mid n$. Then

$$L(s,\chi) = L(s,\chi^*) \prod_{p \mid |n|} \left(1 - \chi^*(p)p^{-s}\right),$$

so that $L(s,\chi)$ equals the product of $L(s,\chi^*)$ with a holomorphic function.

**Proposition 4.7.** Let $\chi$ be a primitive Dirichlet character. Then $M_n^+\chi(s,\chi)$ is meromorphic on the intersection of the zero-free regions of $L(s,\chi)$ and $L(s,\chi\left(\frac{n}{\chi}\right))$. $M_n^+\chi(s,\chi)$ has one pole at $s = 1$ of order $\epsilon$ if $\chi = 1$ or $\chi = \left(\frac{n}{\chi}\right)$, and is holomorphic and zero-free otherwise. Moreover it follows that

$$\text{Res}_{s=1} M_n^+\chi(s,1)$$

$$= \sqrt{\prod_p (1 + 2p^{-1})(1 - p^{-1})^2 \left(1 + 2\left(\frac{n}{p}\right)p^{-1}\right) \left(1 - \left(\frac{n}{p}\right)p^{-1}\right)^2 \cdot \left(2 - \left(\frac{n}{p}\right)\right) \sqrt{\prod_{q \mid n} (1 + 2q^{-1})^{-1} \prod_{(\frac{q}{n}) = -1} (1 - 4q^{-2})^{-1}L\left(1,\left(\frac{n}{q}\right)\right)}.}$$

Each product is over odd primes $p$ or $q$.

**Remark.** Lemma 4.4 implies $\text{Res}_{s=1} M_n^+\chi(s,\left(\frac{n}{\chi}\right)) = \text{Res}_{s=1} M_n^+\chi(s,1)$.

**Proof.** Using the previous lemma, we can conclude that both $M_n^+\chi(s,\chi)$ and $M_n\chi(s,\chi)$ are meromorphic on the zero-free region of $L(s,\chi\left(\frac{n}{\chi}\right))$. Additionally, they each have only one pole lying at $s = 1$ of order 2 and -2 respectively if $\chi\left(\frac{n}{\chi}\right) = 1$, and are holomorphic otherwise. As in the previous
lemma, we let $G(s) = \prod_p (1 + 2\chi(p) \left(\frac{n}{p}\right) p^{-s})(1 - \chi(p) \left(\frac{n}{p}\right) p^{-s})^2$ which is holomorphic on $\Re(s) > \frac{1}{2}$. Moreover, because we can apply this argument to both reciprocals, we know $G(s)$ is zero-free on this region and we have

$$\frac{M_n^+(s, \chi)}{M_n^-(s, \chi)} = \frac{G(s)}{(1 - \chi(2) \left(\frac{n}{2}\right) 2^{-s})^{-2}} \prod_{q \mid n} (1 - 4\chi^2(q)q^{-2s})^{-1} L\left(s, \chi \left(\frac{n}{q}\right)\right)^2.$$

We handle the reciprocal similarly, implying all the components are holomorphic and zero-free except possibly the $L$-function.

In addition, we can also use the previous lemma to show $M_n^+(s, \chi)M_n^-(s, \chi)$ is meromorphic on the zero-free region of $L(s, \chi)$ with a pole of order 2 if $\chi = 1$, and is holomorphic otherwise. Let $F(s) = \prod_p (1 + 2\chi(p)p^{-s})(1 - \chi(p)p^{-2s})^2$ which is holomorphic for $\Re(s) > \frac{1}{2}$, showing that

$$M_n^+(s, \chi)M_n^-(s, \chi) = \frac{F(s)}{(1 - \chi(2) 2^{-s})^{-2}} \prod_{q \mid n} (1 + 2\chi(q)q^{-s})^{-1} L(s, \chi)^2,$$

where each component is holomorphic and zero-free on the region in question except possibly the $L$-function.

Multiplying these two together gives

$$M_n^+(s, \chi)^2 = \frac{G(s)F(s) \prod_{q \mid n} (1 + 2\chi(q)q^{-s})^{-1} \prod_{(\frac{q}{n}) = -1} (1 - 4\chi^2(q)q^{-2s})^{-1}}{(1 - \chi(2) \left(\frac{n}{2}\right) 2^{-s})^{-2} (1 - \chi(2) 2^{-s})^{-2} \cdot L(s, \chi)^2} \cdot L(s, \chi)^2 L\left(s, \chi \left(\frac{n}{q}\right)\right)^2.$$

This function is meromorphic on the intersection of the zero-free regions of $L(s, \chi)$ and $L\left(s, \chi \left(\frac{n}{q}\right)\right)$, and has at most one pole coming from one of the $L$-functions. In particular, since every component is zero-free on this region (save a possible pole at $s = 1$), we may take a branch cut along the negative real axis with starting point $s = 1$ and take the square root both sides of this equation. This shows that

$$M_n^+(s, \chi) = \pm \frac{G(s)F(s) \prod_{q \mid n} (1 + 2\chi(q)q^{-s})^{-1} \prod_{(\frac{q}{n}) = -1} (1 - 4\chi^2(q)q^{-2s})^{-1}}{(1 - \chi(2) \left(\frac{n}{2}\right) 2^{-s})^{-1} (1 - \chi(2) 2^{-s})^{-1} \cdot L(s, \chi)L\left(s, \chi \left(\frac{n}{q}\right)\right)}.$$

where the $\pm$ depends on the root chosen. This is meromorphic on the region in question, and its only possible pole is at $s = 1$ coming from an $L$-function. Calculation of the residues can then be done by plugging in the definitions.
of $G(s)$ and $F(s)$ and noting that
\[
\left(1 - \chi(2) \left(\frac{n}{2}\right) 2^{-1}\right) \left(1 - \chi(2) 2^{-1}\right)
= \begin{cases}
(1 - \left(\frac{n}{2}\right) 2^{-1}) (1 - 2^{-1}) & \chi = 1 \\
(1 - \left(\frac{n}{2}\right)^2 2^{-1}) (1 - \left(\frac{n}{2}\right) 2^{-1}) & \chi = \left(\frac{n}{2}\right) \\
2 - \left(\frac{n}{2}\right) \cdot 4.
\end{cases}
\]

We remark that the residue of $M_n^+(s, 1)$ must be positive by application of a Tauberian theorem. Indeed,
\[
\sum_{m \in A_n^+ \cap m < X} 2^{\omega(m)} \sim \text{Res}_{s=1} M_n^+(s, 1) X
\]
is a sum of positive terms, so the residue must be nonnegative. \qed

Going back to the series in question, we can conclude the following:

**Corollary 4.8.** $D_\epsilon(s, d_1, d_2)$ is meromorphic on a finite intersection of zero-free regions of $L$-functions, which has one simple pole at $s = 1$ of residue
\[
(d_1 d_2)^{-1} \frac{1}{8B} \left(\frac{2 - \left(\frac{ed_1 d_2}{2}\right)}{4}\right) \left| L \left(1, \left(\frac{\epsilon d_1 d_2}{p}\right)\right)\right|
\]
\[
\cdot \prod_p \left(1 + 2p^{-1}\right) (1 - p^{-1})^2 \left(1 + 2 \left(\frac{\epsilon d_1 d_2}{p}\right) p^{-1}\right) \left(1 - \left(\frac{\epsilon d_1 d_2}{p}\right) p^{-1}\right)^2
\]
\[
\cdot \prod_{q | d_1 d_2} (1 + 2q^{-1})^{-1} \prod_{\left(\frac{ed_1 d_2}{q}\right) = -1} (1 - 4q^{-2})^{-1}.
\]

Each product is over odd values of $p$ and $q$.

**Proof.** The residues only come from a few terms in the sum expressing $D_\epsilon(s, d_1, d_2)$, namely those terms coming from $a | d_1$ and $b | d_2$ for which
\[
\left(\frac{\cdot}{ab}\right) = 1, \chi_4, \left(\frac{d_1 d_2}{\cdot}\right), \text{ or } \chi_4 \left(\frac{d_1 d_2}{\cdot}\right)
\]
\[
= 1, \left(\frac{-1}{\cdot}\right), \left(\frac{d_1 d_2}{\cdot}\right), \text{ or } \left(\frac{-d_1 d_2}{\cdot}\right).\]
We get the character 1 if $a = b = 1$ trivially. The character $(\frac{-1}{ab})$ may never occur as $(\frac{-1}{ab})$. This follows from the fact that

$$
\left( \frac{\cdot}{ab} \right) \text{ is primitive modulo } \begin{cases} 
ab & \text{if } ab \equiv 1 \mod 4 \\
4ab & \text{if } ab \equiv 3 \mod 4,
\end{cases}
$$

while $(\frac{-1}{ab})$ is primitive modulo 4. $\epsilon d_1$ and $d_2$ are odd quadratic discriminants, which implies $\epsilon d_1 d_2 \equiv 1 \mod 4$. Therefore quadratic reciprocity implies

$$
\left( \frac{\cdot}{d_1 d_2} \right) = \left( \frac{\epsilon d_1 d_2}{\cdot} \right),
$$

which occurs for $a = d_1$ and $b = d_2$. The opposite character cannot occur for the same reason as $(\frac{-1}{ab})$. This implies that the only terms that contribute a pole to $D_\epsilon(s, d_1, d_2)$ are

$$(d_1 d_2)^{-s} \frac{1}{16B} \left( M^+_{\epsilon d_1 d_2}(s, 1) + \left( \frac{\epsilon d_1}{d_2} \right) \left( \frac{d_2}{d_1} \right) M^+_{\epsilon d_1 d_2} \left( s, \left( \frac{\epsilon d_1 d_2}{\cdot} \right) \right) \right).$$

As $\epsilon d_1$ and $d_2$ are both odd discriminants, $\epsilon d_1 \equiv d_2 \equiv 1 \mod 4$ and quadratic reciprocity implies that

$$
\left( \frac{\epsilon d_1}{d_2} \right) \left( \frac{d_2}{d_1} \right) = 1.
$$

Additionally, Lemma 4.4 states that $M^+_{\epsilon d_1 d_2} \left( s, \left( \frac{\epsilon d_1 d_2}{\cdot} \right) \right) = M^+ \left( s, 1 \right)$.

We know that the residue of $D_\epsilon(s, d_1, d_2)$ must be nonnegative, because the Tauberian theorem [7] implies

$$
\text{Res}_{s=1} D_\epsilon(s, d_1, d_2) = \lim_{X \to \infty} \frac{1}{X} \sum_{d<X:d_1 d_2 | d} a_{\epsilon d_1 d_2},
$$

which is a sum of positive terms. Proposition 4.7 then implies that the residue of $D_\epsilon(s, d_1, d_2)$ at $s = 1$ is given by

$$(d_1 d_2)^{-1} \frac{1}{16B} \cdot 2 \left( 2 - \frac{\epsilon d_1 d_2}{2} \right) \left| L \left( 1, \left( \frac{\epsilon d_1 d_2}{\cdot} \right) \right) \right|$$

$$
\times \prod_p \left( 1 + 2p^{-1} \right) \left( 1 - p^{-1} \right)^2 \left( 1 + 2 \left( \frac{\epsilon d_1 d_2}{p} \right) p^{-1} \right) \left( 1 - \left( \frac{\epsilon d_1 d_2}{p} \right) p^{-1} \right)^2$$

$$
\times \prod_q \left( 1 + 2q^{-1} \right)^{-1} \prod \left( 1 - 4q^{-2} \right)^{-1} \cdot \left( \frac{\epsilon d_1 d_2}{q} \right) = -1,
$$

$s = 1$ being a simple pole is a consequence of the residue being nonzero. Most of the factors are given as absolutely convergent Euler products, and
so are necessarily nonzero. The special value of the $L$-function is well-known to be nonzero. Lastly, the remaining terms

$$(d_1d_2)^{-1} \frac{1}{8B} \left( 2 - \frac{\epsilon d_1d_2}{2} \right)$$

are trivially nonzero. \qed

As stated above, the Tauberian theorem shows that

$$\sum_{d<X} a_{\epsilon d,d_1,d_2} \sim \text{Res}_{s=1} D_{\epsilon}(s,d_1,d_2) X$$

with a positive residue. We can make the following bounds:

$$\sqrt{\prod_{p} (1 + 2p^{-1})(1 - p^{-1})^2 \left( 1 + 2 \left( \frac{\epsilon d_1d_2}{p} \right) p^{-1} \right) \left( 1 - \left( \frac{\epsilon d_1d_2}{p} \right) p^{-1} \right)^2}
= \sqrt{\prod_{p} (1 + 2p^{-1})(1 - p^{-1})^2 \left( 1 - 3p^{-2} + 2 \left( \frac{\epsilon d_1d_2}{p} \right) p^{-3} \right)}
\geq \sqrt{\prod_{p} (1 + 2p^{-1})(1 - p^{-1})^2 (1 - 3p^{-2} - 2p^{-3})}.$$

This is a constant independent of $d_1,d_2$. We also get a bound

$$\sqrt{\prod_{q \mid d_1d_2} (1 - 4q^{-2})^{-1} \geq 1},$$

also a constant independent of $d_1,d_2$. We can bound

$$\sqrt{\prod_{q \mid d_1d_2} (1 + 2q^{-1})^{-1} = \prod_{q \mid d_1d_2} \sqrt{\frac{q}{q+2}}}
\geq (\sqrt{3/5})^{\omega(d_1d_2)}.$$

Lastly, we can bound

$$\left( 2 - \frac{\epsilon d_1d_2}{2} \right) \geq \frac{1}{4}.$$

We conclude:

**Lemma 4.9.** There exists a constant $c$ independent of $d_1,d_2$ such that

$$\text{Res}_{s=1} D_{\epsilon}(s,d_1,d_2) \geq c (\sqrt{3/5})^{\omega(d_1d_2)} \left| L \left( 1, \left( \frac{\epsilon d_1d_2}{d_1d_2} \right) \right) \right|.$$
The expected number of unramified $Q_8$-extensions of imaginary (respectively real) quadratic fields, $E^\pm(Q_8)$, is given by the sum of these residues over all choices of $d_1$ and $d_2$. Utilizing this lower bound, we will show that this sum is necessarily infinite.

**Corollary 4.10.** $E^\pm(G,G') = \infty$ for $G = Q_8$ and $G' = D_4 \oplus \mathbb{Z} C_4$ its unique GI-extension. In particular, $E^\pm(Q_8) = \infty$.

**Proof.** We only need a lower bound on the expected number to be infinite, so let us only consider odd discriminants $\epsilon d$ for $\epsilon \in \{\pm 1\}$ and $d > 0$. By definition, this expected number is equal to $\sum_{d<X} \sum_{d_1,d_2} a_{\epsilon d,d_1,d_2}$. Then we have the following:

$$E^\epsilon(Q_8) = \lim_{X \to \infty} \frac{1}{X} \sum_{d<X} \sum_{d_1,d_2} a_{\epsilon d,d_1,d_2} \geq \sum_{d_1,d_2<N} \lim_{X \to \infty} \frac{1}{X} \sum_{d<X} a_{\epsilon d,d_1,d_2} \geq \sum_{d_1,d_2<N} c(\sqrt{3/5})^{\omega(d_1d_2)} \frac{|L(1,(\epsilon d_1d_2))|}{d_1d_2} \sum_{n<N} (\sqrt{3/5})^{\omega(n)} \sigma_0(n) \frac{|L(1,(\epsilon n))|}{n},$$

where the sum is over $d_1, d_2$ odd such that $\epsilon d_1$ and $d_2$ are quadratic discriminants, $N > 0$ is some positive integer, and $\sigma_0(n)$ is the number of divisors of $n$. For all positive integers $n$, we have a lower bound $\sigma_0(n) \geq 2^{\omega(n)}$. We then note that $2\sqrt{3/5} \geq 1$, so that

$$E^\epsilon(Q_8) \geq c \sum_{n<N} \frac{|L(1,(\epsilon n))|}{n}.$$

A result of Goldfeld–Hoffstein ([9, Theorem 2]) states that $\sum_m L(w, \chi_m) |m|^{-s}$ has a pole at $s = 1$ for $Re(w) \geq 1/2$, which implies the sum diverges as we take $N \to \infty$. □

Lemmermeyer gives a similar classification of unramified extensions with Galois group $D_4$ [13, Theorem 2], and the proof in this section can be modified to show that:

**Theorem 4.11.** $E^\pm(G) = E^\pm(G,G') = \infty$ for $G = D_4$ and $G'$ its unique GI-extension.

**Proof.** By Lemmermeyer’s classification of unramified $D_4$-extensions of quadratic fields, $D_4$ has a unique GI-extension $D_4 \times C_2$ and there exist $\prod_{i=1}^3 2^{\omega(d_i)-1}$ unramified $D_4$-extensions of $k = \mathbb{Q}(\sqrt{\epsilon d})$ whenever there is a factorization $\epsilon d = (\epsilon d_1)d_2d_3$ into three coprime quadratic discriminants.
such that \( \left( \frac{ed}{p} \right) = \left( \frac{d}{p} \right) = 1 \) for every prime \( p_i | d_i \). We trace through the same steps in this section, defining \( a_{ed,d_1,d_2} \) to be the number of such extensions with \( ed,d_1,d_2 \) fixed and \( D_\epsilon(s,d_1,d_2) = \sum_{d_1,d_2 | d} a_{ed,d_1,d_2} d^{-s} \). In the same vein as Lemma 4.2 we find that, for some integer \( 0 < B \leq 6 \) to account for permutations,\
\[
D_\epsilon(s,d_1,d_2) = (d_1d_2)^{-s} \frac{1}{16B} \sum_{a|d_1} \sum_{b|d_2} \left( \frac{ed_1}{b} \right) \left( \frac{d_2}{a} \right) \sum_{m | \mu(m)} |(1 + \chi_4(m))m|^{-s}.
\]
This series trivially has one simple pole at \( s = 1 \) with residue\
\[
(d_1d_2)^{-1} \frac{1}{16\zeta(2)B} \sum_{a|d_1} \sum_{b|d_2} \left( \frac{ed_1}{b} \right) \left( \frac{d_2}{a} \right).
\]
Consider the pairs \( d_1,d_2 \) with \( d_1 \) a fixed odd prime and \( d_2 = 4d_1x+1 > 0 \) for any integer \( x \) which also makes \( d_2 \) prime. Thus \( \sum_{a|d_1} \sum_{b|d_2} \left( \frac{ed_1}{b} \right) \left( \frac{d_2}{a} \right) = 4 \) by quadratic reciprocity. Dirichlet’s Theorem on arithmetic progressions then implies\
\[
E_\epsilon(D_4) \geq \sum_{d_2 = d_14x+1 \atop d_2 \text{ prime}} \text{Res}_{s=1} D_\epsilon(s,d_1,d_2)
\]
\[
\geq \sum_{d_2 = d_14x+1 \atop d_2 \text{ prime}} (d_1d_2)^{-1} \frac{1}{4\zeta(2)B}
\]
\[
= \frac{1}{4\zeta(2)d_1B} \sum_{d_2 \equiv 1 \mod 4d_1 \atop d_2 \text{ prime}} (d_2)^{-1}
\]
\[
= \infty. \quad \square
\]

5. Trivial GI-extensions

In one case we can say something more about \( E_\pm(G) \), and that is when the group \( G \) is generated by elements of order 2. In this case, \( G \) has a trivial GI-extension given by \( G \times C_2 \). Any unramified extension of a quadratic field corresponding to this GI-extension is then a compositum of the quadratic field and some field \( K \) with Galois group \( G \) over \( \mathbb{Q} \) whose inertia groups are all cyclic of order 1 or 2. We call any field \( K/\mathbb{Q} \) whose inertia groups are cyclic of order 1 or 2 \textit{quadratically ramified}. How much room does this extra freedom give us?

\textbf{Lemma 5.1.} Suppose \( K/\mathbb{Q} \) is a Galois extension with Galois group \( G \) such that \( K(\sqrt{d})/\mathbb{Q}(\sqrt{d}) \) is unramified for some \( d \) a quadratic discriminant. Then\
\[
\# \{ K(\sqrt{b}) : \text{unramified over } \mathbb{Q}(\sqrt{b}) \text{ and } b < X \text{ a quadratic discriminant} \}
\]
is bounded below by
\[ (1 + o(X)) \frac{3}{2C\pi^2|d| \log \log |d|} X \]
as \( X \to \infty \) for some constant \( C > 0 \) independent of \( d \).

**Proof.** For each \( p \nmid d \), \( p \) is unramified in \( K(\sqrt{d})/\mathbb{Q}(\sqrt{d}) \) and unramified in \( \mathbb{Q}(\sqrt{d})/\mathbb{Q} \). Therefore \( p \) is unramified in \( K(\sqrt{d})/\mathbb{Q} \), and so necessarily unramified in \( K/\mathbb{Q} \). Suppose \( (a,d) = 1 \) with \( \mu^2(a) = 1 \) and \( \sqrt{ad} \notin K \), then consider \( K(\sqrt{ad})/\mathbb{Q}(\sqrt{ad}) \). If \( p \nmid d \), then \( p \) is unramified in \( K/\mathbb{Q} \) and so unramified in \( K(\sqrt{ad})/\mathbb{Q}(\sqrt{ad}) \). If \( p \mid d \), then \( K(\sqrt{d}) = \mathbb{Q}(\sqrt{d})/\mathbb{Q}(\sqrt{d}) \) unramified implies \( |I_p(K/\mathbb{Q})| \leq 2 \). Therefore the quotient map
\[ \pi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Gal}(K(\sqrt{ad})/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{ad})/\mathbb{Q}) \]
sends \( \pi(I_p) \) to subgroups of the form \( \langle (g, \sigma) \rangle \) for \( \sigma \) a generator of \( \text{Gal}(\mathbb{Q}(\sqrt{ad})/\mathbb{Q}) \) and some \( g \in \text{Gal}(K/\mathbb{Q}) \) with \( g^2 = 1 \). Therefore
\[ I_p(K(\sqrt{ad})/\mathbb{Q}(\sqrt{ad})) = \text{Gal}(K(\sqrt{ad})/\mathbb{Q}(\sqrt{ad})) \cap \pi(I_p) = 1 \]
and \( p \) is unramified.

As a consequence, given such a \( K \) and \( d \), this construction gives asymptotically
\[ \left( \sum_{|ad| < X : (a,d) = 1} \mu^2(a) \right) - \# \{ a : (a,d) = 1, \mu^2(a) = 1, \sqrt{ad} \in K \} \]
\[ \sim \text{Res}_{s=1} \left( \sum_{a: (a,d) = 1} |a|^{-s} \right) \frac{X}{|d|} \]
extensions \( M \) containing a quadratic subfield \( k \) such that \( M/k \) is unramified, \( \text{Gal}(M/k) \cong G \), and \( \text{Gal}(M/\mathbb{Q}) \cong G \times C_2 \) such that \( MC_2 = K \), by summing over quadratic discriminants \( a < X \) and applying a Tauberian theorem as in [7]. Note that only finitely many \( a \) with \( (a,d) = 1 \) and \( \mu^2(a) = 1 \) have \( \sqrt{ad} \in K \) because \( K/\mathbb{Q} \) is a finite extension, so this does not contribute to the asymptotic. By manipulating the Euler product of \( \zeta(s) \) we find that
\[ \sum_{a : (a,d) = 1} |a|^{-s} = \frac{1}{\prod_{p|d}(1 + p^{-s})} \frac{\zeta(s)}{\zeta(2s)} . \]
The residue at \( s = 1 \) is \( \prod_{p|d}(1 + p^{-1})^{-1} \frac{6}{\pi^2} \). It follows that
\[ \prod_{p|d}(1 + p^{-1})^{-1} \frac{6}{\pi^2} \begin{cases} = \frac{|d|}{\prod_{p|d}(p+1)} \frac{6}{\pi^2} & d \text{ odd}, \\ \leq \frac{|d|}{4\prod_{p|d}(p+1)} \frac{6}{\pi^2} & d \text{ even}. \end{cases} \]
This implies
\[ \#\{K(\sqrt{b}) : \text{unramified over } \mathbb{Q}(\sqrt{b}) \text{ and } b < X \text{ a quadratic discriminant}\} \]
is bounded below by
\[ (1 + o(X)) \frac{6}{4\pi^2 \prod_{p | d} (p + 1)} X. \]

To conclude the proof, we cite a theorem of Grönwall [10] which says
\[ \limsup_{n \to \infty} \sum_{m \mid n} \frac{m}{n \log \log(n)} = e^\gamma, \]
where \(0 < \gamma < 1\) is the Euler–Mascheroni constant. For \(d\) sufficiently large, we find that
\[ \prod_{p \mid d} (p + 1) \leq \sum_{m \mid d} m < e|d| \log \log|d|. \]
For \(d\) too small to use this bound, there exists some positive constant \(C\) such that
\[ \prod_{p \mid d} (p + 1) \leq Ce|d| \log \log|d|, \]
which concludes the proof. \(\square\)

Counting unramified extensions of quadratic fields with Galois group \(G\) becomes a question of counting pairs of \((K, d)\) with \(d\) minimal such that \(K\mathbb{Q}(\sqrt{d})/\mathbb{Q}(\sqrt{d})\) is unramified. Recall that a quadratic discriminant refers to a discriminant of a quadratic field over \(\mathbb{Q}\).

**Lemma 5.2.** Suppose \(K/\mathbb{Q}\) is quadratically ramified with Galois group \(G\) and discriminant \(\text{disc}(K)\). Then there exists a quadratic discriminant \(\widehat{d}\) such that \(p \mid \text{disc}(K)\) if and only if \(p \mid \widehat{d}\) and \(K(\sqrt{\widehat{d}})/\mathbb{Q}(\sqrt{\widehat{d}})\) is unramified.

**Proof.** Choose \(\widehat{d} = \prod_p d_p\) defined in the following way:
\[
d_p = \begin{cases} 
1 & p \nmid \text{disc}(K), \\
(-1)^{p-1} p & p \mid \text{disc}(K), \text{ odd}, \\
n \in \{-4, 8, -8\} & \text{odd, } p \mid \text{disc}(K), p = 2, \mathbb{Q}(\sqrt{n}) \otimes \mathbb{Q}_2 \subset K_2^{un}, 
\end{cases}
\]
where we use \(K_2\) to denote the completion of \(K\) at a prime lying above \(2\), and \(K_2^{un}\) the maximal unramified extension of \(K_2\).

There may be more than one choice for \(d_2\) if \(K\) is ramified at \(2\), in order to prove this lemma it suffices to show that there exists at least one. Choose a prime of \(K\) lying above \(2\) so that we fix a field \(K_2^{un}\). If \(K\) is quadratically ramified at \(2\), there exists at least one ramified quadratic subextension \(L\) inside \(K_2\). The local Kronecker–Weber theorem shows that
Brandon Alberts

$\mathbb{Q}_2$ has one unramified quadratic extension, and three pairs of ramified quadratic extensions of discriminants $-4, 8,$ and $-8$ respectively. We set $n = \text{disc}(L/\mathbb{Q}_2) \in \{-4, 8, -8\}$. $K^\text{un}_2$ contains both ramified quadratic extensions of discriminants $-4, 8,$ and $-8$ respectively. We set $d_2 = \text{disc}(L/\mathbb{Q}_2)$.

We remark that $\widehat{d}$ is defined as a product of fundamental discriminants, and so must be a fundamental discriminant itself as the set of fundamental discriminants are closed under multiplication.

If $p \neq 2$, then $p$ is at most tamely ramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. By assumption, $K/\mathbb{Q}$ is at most quadratically ramified, which implies the ramification index satisfies $e_p(K/\mathbb{Q}) | 2$. The definition of $\widehat{d}$ implies that either $e_p(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = e_p(K/\mathbb{Q}) = 1$ or $e_p(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = e_p(K/\mathbb{Q}) = 2$. We may then apply Abhyankar’s lemma ([16, p. 229]):

**Lemma 5.3** (Abhyankar’s Lemma). If $E/L$ and $F/L$ are field extensions for which $F/L$ is tamely ramified at $p$ and $e_p(F/L) | e_p(E/L)$, then $EF/E$ is unramified at $p$.

This implies $\mathbb{Q}(\sqrt{\widehat{d}})/\mathbb{Q}(\sqrt{d})$ is unramified at all $p \neq 2$.

We are left to consider the case $p = 2$. If $K/\mathbb{Q}$ is unramified at 2 we are done, so suppose $e_2(K/\mathbb{Q}) = 2$. By construction, $\mathbb{Q}(\sqrt{d_2}) \otimes \mathbb{Q}_2 \subset K^\text{un}_2$ and satisfies

$$\text{disc}(\mathbb{Q}(\sqrt{d_2}) \otimes \mathbb{Q}_2/\mathbb{Q}_2) = d_2.$$  

In particular, $e_2(\mathbb{Q}(\sqrt{d_2})/\mathbb{Q}) = 2$. By construction, $K_2 \mathbb{Q}(\sqrt{d_2}) \subset K^\text{un}_2$ must also satisfy $e_2(K_2 \mathbb{Q}(\sqrt{d_2})/\mathbb{Q}_2) = 2$, which implies $\mathbb{Q}(\sqrt{d_2})/\mathbb{Q}(\sqrt{d_2})$ is unramified at 2. Lastly, we remark that $\widehat{d}/d_2$ is a fundamental discriminant not divisible by 2 so that $\mathbb{Q}(\sqrt{\widehat{d}/d_2})/\mathbb{Q}$ is unramified at 2. This implies

$$2 = e_2(K/\mathbb{Q}) \leq e_2 \left( \mathbb{Q}(\sqrt{d})/\mathbb{Q} \right) \leq e_2 \left( \mathbb{Q}(\sqrt{d_2})\mathbb{Q}(\sqrt{\widehat{d}/d_2})/\mathbb{Q} \right) \leq e_2(K \mathbb{Q}(\sqrt{d_2})/\mathbb{Q})e_2 \left( \mathbb{Q}(\sqrt{\widehat{d}/d_2})/\mathbb{Q} \right) = 2.$$  

Therefore these are all equalities, and $e_2(K \mathbb{Q}(\sqrt{d})/\mathbb{Q}) = 2$ implies $K \mathbb{Q}(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ is unramified at 2. \hfill $\Box$

Thus for a quadratically ramified extension $K/\mathbb{Q}$, the minimal $d$ for which $K \mathbb{Q}(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ is unramified is the one ramified at exactly the
same primes as $K$. So it follows that counting unramified $G$-extensions of quadratic fields with Galois group $G \times C_2$ over $\mathbb{Q}$ is equivalent to counting quadratically ramified extensions $K$ with Galois group $G$ ordered by $\hat{d}_K$ together with the bounds proved in Lemma 5.1.

This falls immediately into the area of number field counting problems similar to Malle’s conjecture [14, 15]:

**Conjecture 5.4** (Malle’s Conjecture). Fix a finite group $G$. Let $N(G; X)$ be number of $G$-extensions of $\mathbb{Q}$ with discriminant $< X$. Then

$$N(G; X) \sim c(\mathbb{Q}, G) X^{1/a(G)} \log(X)^{b(\mathbb{Q}, G)}$$

for explicit nonnegative integers $a(G)$ and $b(\mathbb{Q}, G)$. The invariant $a(G)$ is defined by setting $|G|(1 - 1/\ell)$ for $\ell$ the smallest prime dividing $|G|$. See [14] or [15] for the definition of $b(\mathbb{Q}, G)$.

**Remark 5.5.** Malle originally states this conjecture for counting degree $n$ (not necessarily Galois) fields ordered by the usual discriminant with prescribed Galois group given by a transitive subgroup $G \leq S_n$. We only state the case for which $G$ is given in its regular representation with $n = |G|$.

Similar asymptotics are expected to be true if we count $G$-extensions $K/\mathbb{Q}$ with certain kinds of restricted ramification (see [8] and [19] for examples). $K/\mathbb{Q}$ being quadratically ramified is a restriction on ramification, so we can ask if Malle’s conjecture is true for counting $G$-extensions $K/\mathbb{Q}$ which are quadratically ramified and have discriminant less than $X$.

Taking the asymptotic from Malle’s conjecture and combining it with the asymptotics from Lemmas 5.1 and 5.2 we would expect that $E^\pm(G, G \times C_2) = \infty$. We will prove a stronger statement, which assumes something strictly weaker than Malle’s conjecture:

**Corollary 5.6.** Let $G$ be a group generated by elements of order 2. Suppose the number of quadratically ramified $G$-extensions $K/\mathbb{Q}$ with discriminant $< X$ is at least $X^{2/\#G} \log(X)^{-1}$ for sufficiently large $X$. Then $E^\pm(G, G \times C_2) = \infty$.

**Proof.** Let $\text{disc}(K)$ be the discriminant of $K/\mathbb{Q}$. We will translate the number of quadratically ramified extensions with $|\text{disc}(K)| < X$ into the number of quadratically ramified extensions with $|\hat{d}_K| < X$, where $\hat{d}_K$ is the quadratic discriminant constructed in Lemma 5.2 corresponding to $K$. Let $n = [K(\sqrt{\hat{d}_K}) : \mathbb{Q}(\sqrt{\hat{d}_K})]$, so that $n = \#G$ if $\sqrt{\hat{d}_K} \notin K$ and $n = \#G/2$ otherwise. Then it follows that $\text{disc}(K(\sqrt{\hat{d}_K})/\mathbb{Q}) = \hat{d}_K^n$ because $K$ is unramified over $\mathbb{Q}(\sqrt{\hat{d}_K})$. Moreover, $\text{disc}(K(\sqrt{\hat{d}_K})/\mathbb{Q}) = \text{disc}(K)^{2n/\#G}$ since $K(\sqrt{\hat{d}_K})/K$ is also unramified and $2n/\#G = [K(\sqrt{\hat{d}_K}) : K]$. Putting
these together implies \(|\text{disc}(K)| = |\hat{d}_K|^{#G/2}\). This implies that there are 
\(\geq X \log(X)^{-1}\) quadratically ramified \(G\)-extensions \(K/\mathbb{Q}\) with 
\(|\hat{d}_K| < X\) for sufficiently large \(X\). In other words, for sufficiently large \(X\),
\[
\sum_{K \text{ quad. ram.}, \atop |\hat{d}_K| < X} 1 \geq X (\log X)^{-1}.
\]

For any quadratically ramified \(K/\mathbb{Q}\), Lemma 5.1 gives us a lower bound
for the number of quadratic fields \(k\) with discriminant \(d_k < X\) such that
\(Kk/k\) is unramified and \(k \cap K = \mathbb{Q}\). The expected number then satisfies
the following bound:
\[
E^\pm (G, G \times C_2) \geq \frac{3}{2Ce\pi^2} \lim_{X \to \infty} \sum_{K \text{ quad. ram.}, \atop |\hat{d}_K| < X} \frac{1}{|\hat{d}_K| \log \log |\hat{d}_K|}.
\]

Although we do not do so here, keeping track of the sign of the discriminant
only slightly changes the value \(3/2Ce\pi^2\) to another positive constant. To
conclude the proof we only need to show that this sum diverges.

By applying Abel summation we find that
\[
\sum_{|\hat{d}_K| < X} \frac{1}{|\hat{d}_K| \log \log |\hat{d}_K|} = \frac{\sum |\hat{d}_K| < X 1}{X \log \log X} - \int_1^X \left( \sum_{|\hat{d}_K| < t} 1 \right) \frac{- \log t \log \log t - 1}{t^2 (\log t)(\log \log t)^2} \, dt
\]
\[
\geq \int_1^X \left( \sum_{|\hat{d}_K| < t} 1 \right) \frac{1}{t^2 \log \log t} \, dt.
\]

Let \(N_0 \geq 1\) be a number such that \(#\{ |\hat{d}_K| < X\} \geq X (\log X)^{-1}\) for all
\(X \geq N_0\). Applying this to the integral when \(X\) is sufficiently large shows
\[
\sum_{|\hat{d}_K| < X} \frac{1}{|\hat{d}_K| \log \log |\hat{d}_K|} \geq \int_{N_0}^X \frac{dt}{t \log t \log \log t}.
\]

It then suffices to show that this integral diverges as \(X \to \infty\), which follows
from a simple calculus exercise:
\[
\int_{N_0}^\infty \frac{1}{t \log t \log \log t} \, dt = \int_{\log \log N_0}^\infty \frac{du}{u} \quad \text{for } u = \log \log t,
\]
\[
= [\log u]_{\log \log N_0}^\infty
\]
\[
= \lim_{M \to \infty} \log(M) - \log \log \log N_0
\]
\[
= +\infty. \quad \square
\]
Remark 5.7. One could also just use the heuristic in [8] for Malle’s conjecture with restricted ramification to count $G \times C_2$ extensions, which predicts that the $G \times C_2$-extensions with discriminant $< X$ unramified over their respective quadratic subfields is asymptotic to $cX \log(X)^{b(Q,G \times C_2)}$ for sufficiently large $X$ and some positive constant $c$. From this point, knowing $b(Q,G \times C_2) > 0$ is enough to conclude an infinite expected number. It is known, however, that in certain cases the value for $b(Q,G)$ in Malle’s Conjecture and related heuristics is incorrect (a counterexample is proven by Klüners [12]). The benefit of the above proof is that it is independent of the actual value for $b(Q,G)$ and assumes a far weaker asymptotic in general.

Bhargava proves $E^\pm(S_n, S_n \times C_2) = \infty$ by proving Malle’s conjecture for $S_n$, $n \leq 5$ and then using the above method [1].

References

[1] M. Bhargava, “The geometric sieve and the density of squarefree values of invariant polynomials”, https://arxiv.org/abs/1402.0031, 2014.
[2] N. Boston, “Embedding 2-groups in groups generated by involutions”, J. Algebra 300 (2006), no. 1, p. 73-76.
[3] N. Boston, M. Bush & F. Hajir, “Heuristics for p-class towers of imaginary quadratic fields”, Math. Ann. 368 (2017), no. 1-2, p. 633-669.
[4] N. Boston & M. M. Wood, “Non-abelian Cohen–Lenstra Heuristics over Function Fields”, Compos. Math. 153 (2017), no. 7, p. 1372-1390.
[5] H. Cohen & H. W. Lenstra, Jr, “Heuristics on class groups of number fields”, in Number theory, Noordwijkerhout 1983, Lecture Notes in Mathematics, vol. 1068, Springer, 1984, p. 33-62.
[6] H. Davenport & H. Heilbronn, “On the Density of Cubic Fields. II”, Proc. R. Soc. Lond., Ser. A 322 (1971), p. 405-420.
[7] H. Delange, “Généralisation du théorème de Ikehara”, Ann. Sci. Éc. Norm. Supér. 71 (1954), p. 213-242.
[8] J. Ellenberg & A. Venkatesh, “Statistics of Number Fields and Function Fields”, in Proceedings of the international congress of mathematicians (ICM 2010), World Scientific, 2011.
[9] D. Goldfeld & J. Hoffstein, “Eisenstein series of $1/2$-integral weight and the mean value of real Dirichlet L-series”, Invent. Math. 80 (1985), p. 187-208.
[10] T. H. Grönwall, “Some asymptotic expressions in the theory of numbers”, Trans. Am. Math. Soc. 14 (1913), p. 113-122.
[11] G. T. Helleloid & U. Martin, “The automorphism group of a finite p-group is almost always a p-group”, J. Algebra 312 (2007), no. 1, p. 294-329.
[12] J. Klüners, “A counter example to Malle’s conjecture on the asymptotics of discriminants”, C. R. Math. Acad. Sci. Paris 340 (2005), no. 6, p. 411-414.
[13] F. Lemmermeyer, “Unramified quaternion extensions of quadratic number fields”, J. Théor. Nombres Bordeaux 9 (1997), no. 1, p. 51-68.
[14] G. Malle, “On the Distribution of Galois Groups”, J. Number Theory 92 (2002), no. 2, p. 315-329.
[15] ———, “On the Distribution of Galois Groups, II”, Exp. Math. 13 (2004), no. 2, p. 129-135.
[16] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd (revised and extended) ed., PWN-Polish Scientific Publishers, 1974.
[17] J. J. Rotman, An introduction to the theory of groups, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer, 1995.
[18] L. Wang, “On the Automorphism Groups of Frobenius Groups”, Commun. Algebra 48 (2020), no. 12, p. 5330-5342.

[19] M. M. Wood, “Nonabelian Cohen–Lenstra Moments”, Duke Math. J. 168 (2019), no. 3, p. 377-427.

Brandon Alberts
9500 Gilman Dr. La Jolla
CA 92093, United States
E-mail: bralberts@ucsd.edu
URL: http://www.math.ucsd.edu/~bralbert