Classifying Unramified Metabelian Extensions Using Lemmermeyer Factorizations

Brandon Alberts

September 19, 2018

Abstract

We study solutions to the Brauer embedding problem with restricted ramification. Suppose $G$ and $A$ are abelian groups, $E$ is a central extension of $G$ by $A$, and $f : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \to G$ a continuous homomorphism. We determine conditions on the discriminant of $f$ that are equivalent to the existence of an unramified lift $\tilde{f}$, i.e. a continuous homomorphism making the following diagram commute:

$$
\begin{array}{cccc}
\text{Gal}(\mathbb{Q}/\mathbb{Q}) & \downarrow{} & \ & \ & \\
1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1
\end{array}
$$

As a consequence of this result, we use conditions on the discriminant of $K$ for $K/\mathbb{Q}$ abelian to classify and count unramified nonabelian extensions $L/K$ normal over $\mathbb{Q}$ where the (nontrivial) commutator subgroup of $\text{Gal}(L/\mathbb{Q})$ is contained in its center. This generalizes a result due to Lemmermeyer, which states that a quadratic field $\mathbb{Q}(\sqrt{d})$ has an unramified extension normal over $\mathbb{Q}$ with Galois group $H_8$ the quaternion group if and only if the discriminant factors $d = d_1d_2d_3$ as a product of three coprime discriminants, at most one of which is negative, satisfying the following condition on Legendre symbols:

$$(d_i d_j) = 1$$

for $\{i, j, k\} = \{1, 2, 3\}$ and $p_i$ any prime dividing $d_i$.

1 Introduction

The question of existence of unramified abelian extensions of number fields is controlled by class field theory, with the result that the maximal unramified abelian extension of a number field $K$ has Galois group isomorphic to $\text{Cl}(K)$, the class group of $K$. Class groups are computable in individual instances and Cohen-Lenstra heuristics [4] with related modifications [7] give conjectural evidence for the distribution of isomorphism classes of class groups over certain families of number fields. Yet overall there are still many open questions with regards to how often number fields have a particular class group or the relationships between class groups in families of number fields. The most basic results for computing part of the class group in families of number fields come from genus theory. If $k$ is a quadratic field of discriminant $d$, then the 2-rank $\text{rk}_2\text{Cl}(k) = \omega(d) - 1$, where $\omega(d)$ = the number of prime divisors of $d$. This gives precisely the number of unramified quadratic extensions of a given quadratic number
field. Similarly, unramified extensions of abelian number fields $L/k$ can be found using Kronecker-Weber whenever we require $L/Q$ to be abelian.

One of the earliest results that go beyond Kronecker-Weber is due to Fueter [6], Rédei and Reichardt [21] [22] [23]. Their works prove the following classification:

**Theorem 1.1.** Let $k$ be a quadratic number field with discriminant $d$. Then there exists an unramified $C_4$-extension $K/k$ if and only if there exists a factorization $d = d_1 d_2$ into coprime discriminants such that

$$\left(\frac{d_1}{p_1}\right) = \left(\frac{d_2}{p_2}\right) = 1$$

for all primes $p_j | d_j$. Moreover, there exist $2^{\omega(d)-2}$ unramified $C_4$-extensions $K/k$ satisfying $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \subset K$ for each such nontrivial factorization.

There are other results of a similar flavor to this one classifying unramified extensions of families of number fields. For instance, there are results for the $\ell$- and $\ell^2$-torsion of the class group over cyclic degree $\ell$ fields [8] [9] [14] [15] [20] and some results for nonabelian $p$-extensions of quadratic fields or cyclic fields of prime degree $q \neq p$ due to Nomura [16] [17] [18] [19]. Closest to the direction of this paper are results due to Lemmermeyer classifying unramified $G$-extensions of quadratic fields for $G$ one of several small nonabelian 2-groups [11] [12], for example:

**Theorem 1.2.** Let $k$ be a quadratic number field of discriminant $d$ and $H_8$ the quaternion group of order 8. Then there exists an unramified $H_8$-extension $K/k$ normal over $\mathbb{Q}$ if and only if there exists a factorization $d = d_1 d_2 d_3$ into three coprime discriminants, at most one of which is negative, such that

$$\left(\frac{d_1 d_2}{p_3}\right) = \left(\frac{d_1 d_3}{p_2}\right) = \left(\frac{d_2 d_3}{p_1}\right) = 1$$

for all primes $p_j | d_j$. Moreover, there exist $2^{\omega(d)-3}$ unramified $H_8$-extensions $K/k$ normal over $\mathbb{Q}$ satisfying $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}) \subset K$ for each such nontrivial factorization.

All of these results follow the same theme: existence of an unramified extension corresponds to a vanishing condition on Dirichlet characters. As a consequence these results have been used to study the arithmetic statistics of unramified extensions in [1], [2], [5], and [10].

The purpose of this paper will be to generalize these results using class field theory and the theory of embedding problems. This approach follows the same basic idea as Nomura [16] [17] [18] [19], by using local conditions to say something about the solution to an embedding problem.

Suppose we have abelian groups $G$ and $A$, and $E$ a central extension of $G$ by $A$ whose 2-coclass in $H^2(G, A)$ is represented by $[E]$. The Brauer embedding problem for a continuous homomorphism $f : G \rightarrow \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G$ and an extension $E$ of $G$ is the question of whether or not there exits a continuous homomorphism $\tilde{f} : G \rightarrow E$ such that the following diagram commutes:

\[
\begin{array}{ccc}
\text{G}_\mathbb{Q} & \xrightarrow{\tilde{f}} & G \\
\downarrow{f} & & \downarrow{f} \\
E & \rightarrow & G \rightarrow 1
\end{array}
\]

We know that the a solution to the Brauer embedding problem for central extensions exists if and only if the solutions to the corresponding local embedding problems exist [24]. Our main theorem will give explicit conditions for when we can find an unramified (at finite places) solution ot the Brauer embedding problem, namely solutions where
ker \ f \cap I_p \leq \ker \tilde{f} \text{ with } I_p \leq G_Q \text{ the inertia group at } p \text{ defined up to conjugation. This will provide the necessary framework to classify certain unramified metabelian extensions of abelian number fields in a way directly generalizing the classification due to Lemmermeyer [11, 12].}

Before stating the main result, we introduce the following notation: for a prime \( p > 2 \) fix a representative \( \tau_p \) for the generator of inertia \( I_p \leq G_Q \) (for \( p = 2 \) we choose generators \( \tau_{2,0}, \tau_{2,1} \) such that \( [\tau_{2,0}, \tau_{2,1}] = 1 \) and \( (\tau_{2,0}, \tau_{2,1})^2 = 1 \)). We also have a bilinear map \([,]_E : G \times G \to A\) given by the comutator of the lift to \( E \times E \) and use \( \exp(A) \) to denote the exponent of the group \( A \), i.e. the smallest \( n \in \mathbb{Z} > 0 \) such that \( nA = 0 \). Let \( \text{Res}^G_H : H^2(G, A) \to H^2(H, A) \) denote the restriction map on cohomology. Then the main result is as follows:

**Theorem 1.3.** Given \( f : G_Q \to G \) let \( Y_E = \{ y \in G : \text{Res}^G_{f(I_p)}([E]) = 0 \} \) and \( \text{disc}(f) = \prod p^{r_p} \). Define \( d_y = \prod_{y \in Y_E} p^{f(y)} \). Then there exists an unramified (everywhere except possibly at the infinite place) solution to the Brauer embedding problem for \( [E] \) if and only if

1. \( \text{disc}(f) = \prod_{y \in Y_E} d_y \)

2. For every prime \( p \mid d \)

\[
\sum_{y \in Y_E} \left( \frac{p}{d_y} \right)_{\exp(A)} [y, f(\tau_p)]_E = 0
\]

where \( \left( \frac{p}{d_y} \right)_{\exp(A)} \in \mathbb{Z}/\exp(A)\mathbb{Z} \).

Here \( \left( \frac{p}{d_y} \right)_{\exp(A)} \) is a Dirichlet character, which we will describe in greater detail in the body of the paper.

The paper proceeds as follows: In section 2 we begin with a review of the Brauer embedding problem with restricted ramification, which will then be converted into group theoretic conditions. In section 3 we present the proof of the main theorem. Section 4 describes how our result can be used to classify unramified metabelian extensions \( L/K \) of abelian number fields whose Galois group over \( \mathbb{Q} \) has its commutator subgroup contained in its center, generalizing the results of Fuerter, Rédei, Reichardt, and Lemmermeyer. In section 5 we walk through an example classifying all unramified \( H(\ell^3) \)-extensions of cyclic degree \( \ell \) fields tamely ramified at exactly three primes, where \( \ell \) is an odd prime and \( H(\ell^3) \) is the nonabelian group of order \( \ell^3 \) and exponent \( \ell \) (called the Heisenberg group).

### 2 The Unramified Brauer Embedding Problem

Let \( G_Q = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) denote the absolute Galois group of \( \mathbb{Q} \) with \( D_p \) and \( I_p \) the corresponding decomposition and inertia groups at the prime \( p \) (defined as subgroups of \( G_Q \) up to conjugacy for \( p \) finite or infinite). Given an extension \( E \) of a group \( G \) by an abelian group \( A \), suppose we have a commutative diagram as follows:

\[
\begin{array}{c}
1 \longrightarrow A \longrightarrow E \overset{\pi}{\longrightarrow} G \longrightarrow 1
\end{array}
\]

Then the Brauer embedding problem asks when \( f \) lifts to a continuous homomorphism \( \tilde{f} : G_Q \to E \) that makes the diagram commute. This problem is “solved” in a certain...
sense in the case of $A$ abelian and $E$ a central extension, in that a solution exists if and only if a solution exists to the corresponding local embedding problems:

$$
1 \rightarrow A \rightarrow E \xrightarrow{\pi} G \rightarrow 1
$$

where $f_p = f|_{D_p}$ \[13\] \[24\].

We call such a lift $\tilde{f}$ unramified over $f$ if $\ker f \cap I_p \leq \ker \tilde{f}$. Let $K = \mathbb{Q}^{\text{ur}}$, $L = \mathbb{Q}^{\text{ur}} \tilde{f}$, and $K_p, L_p$ the completions at a prime above $p$. Then $\tilde{f}/f$ is unramified if and only if $L/K$ is unramified, i.e. if and only if $\tilde{f}$ factors through $\text{Gal}(K^{ur,ab}/K)$ where $K^{ur,ab}$ is the maximal unramified abelian extension of $K$, otherwise known as its Hilbert class field.

The solutions to the Brauer embedding problem are a priori independent of ramification. With a little extra work, we can determine when a solution can be found with specific ramification. Some results of this nature in more specific instances were proven in \[10\] \[17\] \[18\] by Nomura and some general results can be found in \[24\].

**Theorem 2.1.** Given $f : G_Q \rightarrow G$ a continuous homomorphism with $f(D_p)$ abelian, there exists a solution to the Brauer embedding problem $\tilde{f} : G_Q \rightarrow E$ unramified at finite places if and only if $\text{Res}_{f(D_p)}^G([E])$ is abelian and $\text{Res}_{f(I_p)}^G([E]) = 0$ for all primes (finite and infinite) $p$.

**Proof.** For the forward direction, we have that $f(I_p) \cong I_p/(\ker f \cap I_p) = I_p/(\ker \tilde{f} \cap I_p) \cong \tilde{f}(I_p)$. This implies that there is a section $\tau_p : I_p \rightarrow \pi^{-1}(I_p)$, forcing $\text{Res}_{f(I_p)}^G([E]) = 0$.

Additionally, we have $L_p/K_p$ unramified, with $\tilde{f}(D_p) = \text{Gal}(L_p/\mathbb{Q})$ and $f(D_p) = \text{Gal}(K_p/\mathbb{Q})$ abelian. Any unramified extension of an abelian local field is also abelian by a standard result, so $\tilde{f}(D_p)$ is abelian. Then $\text{Res}_{f(D_p)}^G([E])$ has an abelian subgroup which surjects onto $f(D_p)$. Since this is a central extension of $f(D_p)$ this implies that $\text{Res}_{f(D_p)}^G([E])$ must also be abelian.

For the converse, note that $\text{Res}_{f(I_p)}^G([E]) = 0$ implies the local embedding problem is solvable at all places, so there exists a possibly ramified lift $\tilde{f}$ with $\pi \tilde{f} = f$. $\text{Res}_{f(I_p)}^G([E]) = 0$ implies that $\tilde{f}(I_p)$ is a trivial extension of $f(I_p)$. $\text{Res}_{f(D_p)}^G([E])$ abelian implies that inertia factors through procyclic $\mathbb{Z}_p^\times$ with finite image for both $f$ and $\tilde{f}$. Therefore we must have $\tilde{f}(I_p) \cong C_{n_p} \times f(I_p)$ with $(n_p, |f(I_p)|) = 1$. Let $\rho_p : I_p \rightarrow A$ be $\tilde{f}|_{I_p}$ composed with projection onto the first coordinate $C_{n_p}$ and embedded into $A$. Define the map

$$
\rho = (\rho_p) : G_Q = \prod I_p^{ab} \rightarrow A
$$

Then we have a map

$$
g = f \times \rho : G_Q \rightarrow G \times A
$$

which satisfies $g(I_p) \cong \tilde{f}(I_p)$ since $(|f(I_p)|, |\rho(I_p)|) = 1$ by $|\rho(I_p)| = n_p$. Then we have a map $f \times \rho : G_Q \rightarrow E \times A$ which composed with $\pi$ gives $g$, and composed with projection onto the first coordinate gives $\tilde{f}$. We have a subgroup $A \times A \leq E \times A$ and

$$(A \times A) \cap (\tilde{f} \times \rho)(I_p) = (\rho_p \times \rho_p)(I_p)$$
is a diagonal embedding of $I_p$ into $A \times A$. This implies that $(A \times A) \cap (\tilde{f} \times \rho)(I_p) \leq \Delta$ the diagonal subgroup. Let $\pi_\Delta : E \times A \to E$ be the quotient map by $\Delta$ (in other words, we are adding the extensions $[E]$ and $[G \times A]$ together in $H^2(G, A)$, which gives back $[E]$). It then follows that $\pi_\Delta \circ (\tilde{f} \times \rho) : G_\infty \to E$ is a morphism with

$$\pi_\Delta (\tilde{f}(x), \rho(x)) = \pi(\tilde{f}(x)\rho(x)^{-1})$$

$$= f(x)$$

and

$$A \cap \pi_\Delta (\tilde{f} \times \rho)(I_p) = 0$$

which implies that if $\ker f \cap I_p \leq \ker \pi_\Delta (\tilde{f} \times \rho)$ so that it is unramified at all finite places. \hfill \Box

We can also ask that $\tilde{f}$ be unramified at the infinite place. This is trivially true if $f$ is ramified at $\infty$ or if $2 \nmid |A|$. Moreover, if $2 \mid f(I_p)$ for some finite prime $p \equiv 3 \mod 4$, then we can take $g : G_\infty \to \text{Gal}(\mathbb{Q}(\sqrt{-p})/\mathbb{Q})$ and combine it with $\tilde{f}$ ramified at infinity in the same way as in the proof of this theorem to get a new lift unramified at infinity. As for when $2 \nmid f(I_p)$ only for primes $p \equiv 1 \mod 4$, the question becomes more difficult. Lemmermeyer addressed this when he studied unramified $H_p$-extensions of quadratic fields [11], but when studying the expected number of such extensions Alberts and Klys avoid using this result by showing that it only contributes to the error term \[2\]. Although we do not address ramification at $\infty$ in this paper, we expect the methods used by Lemmermeyer to extend to the results in our paper without too much difficulty.

Define $\text{Frob}_p$ to be the lift of the Frobenius automorphism in $\text{Gal}(\overline{F}_p/F_p)$ to $G_\infty$, defined up to conjugacy and modulo $I_p$. The we have the following corollary:

**Corollary 2.2.** Given $f : G_\infty \to G$ with $f(D_p)$ abelian, and $[E] \in H^2(G, A)$ such that $\text{Res}^E_{f(I_p)}([E]) = 0$, then there exists a lift $\tilde{f} : G_\infty \to E$ unramified at finite places if and only if $[f(\text{Frob}_p), f(I_p)]_E = 0$ where $[,]_E : G \times G \to E$ is the commutator of $E$.

**Proof.** $E$ is a central extension of $G$, so the commutator factors through $G \times G$. Notice that $[a^g, b^h]_E = [a, b]^g_h$ respects conjugation, so WLOG we can fix a representative of $D_p$ and $I_p$ up to conjugation. Suppose $x, y \in D_p$ are both representatives of Frobenius $\text{Frob}_p$. Because $f(D_p) \leq G$ is abelian, we have $[f(x), f(I_p)]_E, [f(y), f(I_p)]_E \leq \ker \pi = A$. Suppose $[f(x), f(I_p)]_E = 0$. Then $[f(I_p), f(I_p)]_E = 0$ since $\text{Res}^E_{f(I_p)}([E]) = 0$ implies $\pi^{-1}(I_p)$ is a trivial extension of the abelian $f(I_p)$. Then for any $i \in \tilde{f}(I_p)$

$$[\tilde{f}(x), i] \tilde{f}(x) = \tilde{f}(x)i$$

$$= \tilde{f}(y)\tilde{f}(y^{-1}x)i$$

$$= \tilde{f}(y)i\tilde{f}(y^{-1}, x)$$

$$= [\tilde{f}(y), i] \tilde{f}(y)i\tilde{f}(y^{-1}x)$$

$$= [\tilde{f}(y), i] \tilde{f}(x)$$

noting that $\tilde{f}(y^{-1}x) \in \tilde{f}(I_p)$. Thus $[f(\text{Frob}_p), f(I_p)]_E$ is a well-defined subgroup of $A$. $\text{Res}^E_{f(I_p)}([E])$ is abelian if and only if a representative of Frobenius commutes with inertia (i.e. $f(D_p)$ abelian), and so the result follows from the previous theorem. \hfill \Box
3 Lemmermeyer Factorization

In this section we will translate the conditions in Corollary 1.1 to conditions on discriminants in the specific case that $G$ is abelian. Fix an extension $[E] \in H^2(G, A)$ and the quotient map $\pi : E \to G$. Then $[,]_E : G \times G \to A$ is a well-defined bilinear map for all elements, not just the image of Frobenius and inertia. For the remainder of this section, let unramified refer only to finite places.

The previous section tells us that a continuous homomorphism $f : G_0 \to G$ has an unramified lift $\tilde{f} : G_\mathbb{Q} \to G$ if and only if $\text{Res}^G_{f(I_p)}([E]) = 0$ and $[f(Frob_p), f(I_p)]_E = 0$ for all primes $p$ (including the infinite prime).

For convenience, for $p$ odd we will use $\tau_p$ for the generator of $I_p^{ab}$, and WLOG consider $f : G_\mathbb{Q}^{ab} \to G$. (For the prime 2, we have two generators $\tau_{2,0}$ and $\tau_{2,1}$ of order $2^\infty$, whose product $\tau_{2,0}\tau_{2,1}$ has order 2. Here, $I_\infty \mapsto (\tau_{2,0}\tau_{2,1})$ is the ramification at infinity under the quotient map $G_\mathbb{Q}^{ab} \to (\tau_{2,0}, \tau_{2,1})$.) We also use $\text{disc}(f)$ to denote the discriminant of $K = \mathbb{Q}^{ab} f$.

**Lemma 3.1.** Let $Y_E = \{g \in G : \text{Res}^G_{f(I_p)}([E]) = 0\}$. Then there is a one-to-one correspondence between maps $f : G_\mathbb{Q}^{ab} \to G$ satisfying $\text{Res}^G_{f(I_p)}([E]) = 0$ with $\text{disc}(f) = \prod p^\nu$ and factorizations $\text{disc}(f) = \prod_{y \in Y_E} (d_y)^{[f(G_\mathbb{Q}) : (y)]}$ into coprime discriminants (except for at most two allowed to be even) such that

1. $|y| \mid (p - 1)p^\infty$ for every prime dividing $d_y$ where $|y|$ is the order of $y$.
2. If $d_y, d_{y'}$ are even with $y \neq y'$ then $y y'$ has order dividing 2. If $d_y$ is a unique even factor and 4 $\mid d_y$, then $y$ has order dividing 2,
3. $\prod_{2|d_y < 0} \prod_{d_y < 0} y^{y |y|/2} \in Y_E$.

Given by $d_y = \prod_{f(\tau_p) = y} p^* f([f(G_\mathbb{Q}) : (y)]$ where $p^* = (-1)^{\frac{p-1}{2}}$ for odd primes, and $2^* = -2$.

This lemma is a consequence of Kronecker-Weber. The proof is somewhat long and cumbersome, so we will first demonstrate the content of this theorem with an example from genus theory both to motivate the result and convince any reader not interested in trudging through the proof.

**Example 3.2.** Since 

$$G_\mathbb{Q}^{ab}/2G_\mathbb{Q}^{ab} = (\tau_{2,0}, \tau_{2,1}, \tau_p | p \text{ an odd prime : } \tau_{2,0}^2 = \tau_{2,1}^2 = \tau_p^2 = 1)$$

a $C_2^2$-extension of odd discriminant $d$ corresponds to a homomorphism

$$f : (\tau_p, p | d : \tau_p^2 = 1) \to C_2^2.$$

We can produce a factorization from this map as follows: let $d_y = \prod_{f(\tau_p) = y} p^* \cdot d_0 = 1$. Then $d = \prod_{y \in C_2^2} d_y^{[f(G_\mathbb{Q}) : (y)]/2}$ because the exponent of every prime dividing $d$ must be $[\text{im} f]$ divided by the ramification degree, which is 2. The field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ for $a, b \in \mathbb{Z}$ odd and squarefree corresponds to the factorization $d = (ab)^2 = a^2 \cdot b^2 = d_{v_1} \cdot d_{v_2}$ for $v_1, v_2$ a basis of $C_2^2$. This gives a one-to-one correspondence between maps $f : G_\mathbb{Q} \to C_2^2$ of discriminant and factorizations $d = \prod_{y \in C_2^2} d_y^{[f(G_\mathbb{Q}) : (y)]/2}$, since any such factorization defines a map by sending $\tau_p \mapsto y$ if $p \mid d_y$. In this case, conditions 1 and 2 on the factorizations are trivially satisfied because $|y| = 2$ and $d$ is odd.

For this lemma, we are restricting the possible images of $f(\tau_p)$ to a specific subset of elements $Y_E \subset G$ and giving a correspondence between these maps and certain
factorizations of the discriminant. This subset is specifically chosen so that we always have $\text{Res}^G_{f,I_p}([E]) = 0$, one of the conditions that we showed in the previous section was necessary to solve the Brauer embedding problem. Condition 3 is then equivalent to forcing the generator $\tau_\infty \in I_\infty$ to satisfy $f(\tau_\infty) \in Y_E$.

**Proof of 3.1.** Define $d_y := \prod f(\tau_p) = p^{s_y(p)}$ a discriminant where $p^{s_y(p)} \mid \text{disc}(f)$ exactly divides $\text{disc}(f)$ for $y \neq 0$, and $d_0 = 1$. These are all clearly coprime. There exists a continuous homomorphism $f_y : G_{\mathbb{Q}}^{ab} = \prod I_p \to \langle y \rangle$ which equals $f$ on $I_p$ for primes with $f(\tau_p) = y$ and 0 on all other primes. Let $K_y = \mathbb{Q}^{\text{ker } f_y}$. Then $\text{disc}(K_y) = d_y$ by the higher ramification formula for discriminants and $[K_y : \mathbb{Q}] = |y|$. It follows that $\prod K_y/K$ is an unramified extension, where the power of $p$ dividing $\text{disc}(\prod K_y)$ is exactly $a_p \prod K_y : K_y = a_p(\prod |y'|)/|y| = a_p \prod |y' y'|$. Thus we have

$$\prod_{y \in Y_E} (d_y)^{\prod_{y' \neq y}|y'|} = \text{disc}(\prod K_y)$$

$$= \text{disc}(K)^{\prod K_y/K}$$

$$= \text{disc}(f)^{\prod_\mathbb{Q}|y|}$$

Raising both sides to the power $\frac{|f(G_{\mathbb{Q}})|}{\prod |y|}$ yields the result up to a sign. The conditions on $d_y$ and $y$ follow immediately from $f(\tau_{2,0})$ having order dividing 2, and $|f(\tau_p)| < (p-1)p^\infty$.

Given such a factorization, define $f(\tau_p) = y \in Y_E$ where $p \mid d_y$. For the finite primes, this gives a well-defined map $f : G_{\mathbb{Q}}^{ab} = \prod I_p \to G$ by $|y'| < (p-1)p^\infty$. The other conditions on the factorization imply that this map is well-defined on $I_2$. $f(\tau_p) \in Y_E$ implies $\text{Res}^G_{f,I_p}([E]) = 0$ at all finite places.

We have now proven the theorem up to a sign, except for part 3 and the infinite place. We will first show that part 3 is equivalent to $\text{Res}^G_{f,I_\infty}([E]) = 0$, then show that signs of the factorization also match.

Given such a factorization, the signs are not an obstruction to constructing a map as $G_{\mathbb{Q}}^{ab} = \prod I_p$, a product over finite primes and we can get a map just coming from the finite primes present in the factorization. $\text{Res}^G_{f,I_\infty}([E]) = 0$ if and only if

$$f(\tau_{2,0}) \prod_{p \equiv 3 \mod 4} f(\tau_p)^{f(\tau_p)}/2 \in Y_E$$

This is the same thing as

$$\prod_{2|d_y < 0} y \prod_{d_y < 0} y^{[y]/2} \in Y_E$$

since $d_y < 0$ for $d_y$ odd if and only if an odd number of primes $p \equiv 3 \mod 4$ divide it with odd exponent and $y$ has even order. For $d$ even, we must additionally multiply by $f(\tau_{2,0})$, a product of the at most two $y \in Y_E$ such that $d_y$ is even. Thus $d_y < 0$ for $d_y$ even if and only if $f(\tau_{2,0}) = y y' \neq 1$ and 2 $\mid \# \{p \mid d_y : p \equiv 3 \mod 4\}$ or $f(\tau_{2,0}, \tau_{2,1}) = 1$ and 2 $\mid \# \{p \mid d_y : p \equiv 3 \mod 4\}$. This is the same thing as $y y'(y^y)^{y}/2$ being the contribution to the infinite inertia. So $\prod_{2|d_y < 0} y \prod_{d_y < 0} y^{[y]/2}$ is equivalent to $\text{Res}^G_{f,I_\infty}([E]) = 0$.

As for the signs of discriminants, consider the quotient map $h : \text{Gal}(\prod K_y/\mathbb{Q}) = \prod(y) \to \text{Gal}(\prod K_y/\mathbb{Q})/2\text{Gal}(\prod K_y/\mathbb{Q})$, then

$$h \left( (y^y/2)^{d_y < 0} \right) = (h(y)^{y/2})^{d_y < 0, 2|y/2}$$

$$= (h(y)^{y/2})^{d_y < 0, 2|f(G_{\mathbb{Q}})/y|}$$
is the generator of $I_\infty$, noting that $h(y)$ is nontrivial if and only if $2 \mid \{f(G_Q) : \langle y \rangle \}$ (if $2 \mid d_y < 0$ we must use $y^{[y]/2+1}$). It suffices to show that $\{\langle y \rangle \} \subseteq \{f(G_Q) : \langle y \rangle \}$ is linearly independent in the $F_2$-vector space, because then there is a map sending all such $y \mapsto -1$ which factors through $h$, so that the sign of $\text{disc}(f)$ is $-1$ to the power of $\sum_{y:|d_y|<2|f(G_Q)\langle y \rangle|} \frac{|y|}{2}$.

First, if $\{y \in Y_E : 2 \mid f(G_Q) : \langle y \rangle \} \neq \emptyset$, then the 2-Sylow subgroup of $f(G_Q)$ is cyclic. In particular, an element $x$ is a square if and only if $\{f(G_Q) : \langle x \rangle \}$ is even.

Suppose $\prod_{i=1}^{n-1} y_i^{a_i}$ is a square (i.e., an element of $2 f(G_Q)$) with $\{f(G_Q) : \langle y_i \rangle \}$ odd for all $y_i \in \{y \in Y_E : 2 \mid f(G_Q) : \langle y \rangle \}$. Then

$$\langle \prod_{i=1}^{n-1} y_i^{a_i}, y_n^{a_n} \rangle = \langle \prod_{i=1}^{n-1} y_i^{a_i} \rangle \times \langle y_n^{a_n} \rangle / \langle \prod_{i=1}^{n} y_i^{a_i} \rangle$$

as subgroups of $f(G_Q)/2 f(G_Q)$. We induct on $n$. Clearly if $n = 1$, then $y_1^{a_1} \in 2 f(G_Q)$ if and only if $1 \mid a_1$. Suppose this is true for $n - 1$. Then if $\prod_{i=1}^{n-1} y_i^{a_i}$ is a square, it follows that if $2^k \mid f(G_Q)$ then $2^{k+1} \mid \langle \prod_{i=1}^{n-1} y_i^{a_i} \rangle$. Suppose $a_n$ is odd, then $2^{k+1} \mid \langle \prod_{i=1}^{n} y_i^{a_i} \rangle$. Being a square implies $\langle \prod_{i=1}^{n} y_i^{a_i} \rangle = \langle x^2 \rangle$, and so $2^{k+1} \mid |x^2|$. By using the above isomorphism, we must have that $2^{k+1} \mid |\langle \prod_{i=1}^{n} y_i^{a_i} \rangle|$, which implies it is a square. By induction, $a_n \equiv 0 \mod 2$ for all $i = 1, \ldots, n - 1$. Then we are back to the base case $y_i^{a_i}$.

Now, the sign of $d_y$ is 1 if it is unramified at $\infty$, and $(-1)^{[y]/2}$ if ramified. This means that the sign of $\prod_{y \in Y_E} (d_y)_{\text{disc}(f(G_Q))\langle y \rangle}$ is $-1$ to the power of $\sum_{2 \mid |f(G_Q)\langle y \rangle|} |y|/2$.

If $2 \mid f(G_Q)$ then $|y|/2 = 1 = |y||f(G_Q)|/4 \mod 2$ and we get equality. If $4 \mid f(G_Q)$, then $|y|/2 = 0 = |g||f(G_Q)|/4 \mod 2$ and we also get equality. This concludes the proof.

The field $\prod_{y \in Y_E} K_y$ with Galois group $\prod_{y \in Y_E}(y)$ over $\mathbb{Q}$ is going to be very important. Call this field $L$ with Galois group $H$ over $\mathbb{Q}$. The following lemma follows immediately from properties of the quotient map $H \to G$ sending $y \mapsto y$ for each $y \in Y_E$:

**Lemma 3.3.** $|.|_E : G \times G \to A$ lifts to a map $|.|_E : H \times H \to A$ by applying $|.|_E$ coordinatewise and adding up the results, i.e., satisfies the following commutative diagram

$$
\begin{array}{ccc}
H \times H & \xrightarrow{|.|_E} & A \\
\downarrow & & \\
G \times G & \xrightarrow{|.|_E} & A
\end{array}
$$

In particular, if $g : G_Q \to \prod_{y \in Y_E}(y)$ is defined by $\tau_p \mapsto f(\tau_p) \in Y_E$, then $[f(Frob_p), f(\tau_p)]_E = [g(Frob_p), g(\tau_p)]_E$.

Thus it suffices to check the commutator condition $[f(Frob_p), f(I_p)]_E = 0$ in $\prod_{y \in Y_E} K_y$.

**Lemma 3.4.** Let $f : G_Q \to G$ be the continuous homomorphism of discriminant $\text{disc}(f) = \prod_{p \in \mathbb{P}^*} \text{corresponding to a factorization} \text{disc}(f) = \prod_{y \in Y_E} (d_y)_{\text{disc}(f(y))}$ and let $g : G_Q^{ab} \to H$ be the map sending $\tau_p \mapsto f(\tau_p) \in Y_E$. Then

$$[g(Frob_p), g(\tau_p)]_E = \sum_{y \in Y_E} \sum_{y|d_y} \left( \frac{p}{y^{q^{d_y}}} \right)_{\exp(A)} [y, g(\tau_p)]_E$$
where \( \left( \frac{a}{q^n} \right)_n \in \mathbb{Z}/n\mathbb{Z} \) is the image of \( p \) under the quotient map

\[
\mathbb{Z}_q^\times \to \mathbb{Z}_q^\times/(\mathbb{Z}_q^\times)^{(n,q^n-1(q-1))} \hookrightarrow \mathbb{Z}/n\mathbb{Z}.
\]

and \( b_q = e_q/[f(G_Q) : \langle y \rangle] \)

**Proof.** We have that the Frobenius element \( \text{Frob}_p \in G_Q^b = \prod I_q \) is \( (p)_q \) the equivalence class of \( p \) in each coordinate. Therefore, under \( g \) we get that

\[
g(\text{Frob}_p) = g \left( \sum_{q | \text{disc}(f)} (p)_q \right)
\]

\[
= \sum_{y \in E \langle q \rangle} g \left( \sum_{q | d_y} (p)_q \right)
= \sum_{y \in E \langle q \rangle} (p)_y
\]

The equivalence class of \( p \), denoted above by \( (p) \) acts on \( \langle y \rangle \) by multiplication as an element of \( \mathbb{Z}/[q]/\mathbb{Z} \), namely \( \left( \frac{a}{q^n/f(G_Q) \langle y \rangle} \right) \). The proof then follows from the bilinearity of \([\cdot, \cdot]_E \). \( \square \)

**Definition 3.1.** We define \( \left( \frac{a}{b} \right)_n : \mathbb{Z}^\times \to \mathbb{Z}/n\mathbb{Z} \) by \( \left( \frac{a}{b} \right)_n = \sum_{q \equiv a \pmod{\langle b \rangle \langle q \rangle}} (\overline{q}^e_{\langle b \rangle \langle q \rangle})_n \) for any \( (a, b) = 1 \) where \( a \) has prime factorization \( \prod q^n_a \).

We can now prove the main theorem for generalized Lemmermeyer factorizations as an immediate consequence of the work in this section, which we restate here for convenience:

**Theorem 1.3.** Given \( f : G_Q \to G \) let \( Y_E = \{ y \in G : \text{Res}_{f(Y_p)}^G ([E]) = 0 \} \) and \( \text{disc}(f) = \prod p^e_p \). Define \( d_y = \prod f(\tau_p)_y p^{e_p}/\text{Res}_{f(Y_p)}^G ([y]) \). Then there exists an unramified (everywhere except possibly at the infinite place) solution to the Brauer embedding problem for \([E] \) if and only if

1. \( \text{disc}(f) = \prod_{y \in Y_E} d_y^{f(G_Q):\langle y \rangle} \)
2. For every prime \( p | d \)

\[
\sum_{y \in Y_E} \left( \frac{p}{d_y} \right)_{\exp(A)} [y, f(\tau_p)]_E = 0
\]

where \( \left( \frac{p}{d_y} \right)_{\exp(A)} \in \mathbb{Z}/\exp(A)\mathbb{Z} \).

**Proof.** Part 1 is equivalent to \( \text{Res}_{f(Y_p)}^G ([E]) = 0 \) by Lemma 3.1

For part 2, we have that \( q | d \) if and only if \( y' = g(\tau_p) \). So we then have

\[
\sum_{y \in Y_E} \left( \frac{p}{d_y} \right)_{\exp(A)} [y, f(\tau_p)]_E = \sum_{y \in Y_E \langle q \rangle | d_y} \left( \frac{p}{q^n_y} \right)_{\exp(A)} [y, g(\tau_p)]_E
= [g(\text{Frob}_p), g(I_p)]_E
= [f(\text{Frob}_p), f(I_p)]_E
\]

Which is 0 if and only if \( [f(\text{Frob}_p), f(I_p)]_E = 0 \). \( \square \)
4 Certain Unramified Metabelian Extensions

Lemmermeyer used factorizations of the kind found in this paper to classify unramified quaternion $H$-extensions of quadratic number fields \[11\]. In this section, we will detail how to use the results of the previous section to classify certain unramified metabelian extensions of abelian number fields in similar situations.

When discussing unramified $G$-extensions of number fields $L/K$, it is useful to consider $\text{Gal}(L/Q)$ as was done in \[11\] \[3\] \[25\].

**Definition 4.1.** Call a pair $(G, G')$ with $G \leq G'$ of finite index admissible if

1. $G \trianglelefteq G'$
2. $G'$ is generated by the set $Y_G \cap (G' - G)$

Given a $G'/G$-extension $K/Q$, we call $L/K$ a $(G, G')$-extension if $L/Q$ is normal, $\text{Gal}(L/K) = G$, and $\text{Gal}(L/Q) = G'$. By properties of Galois theory, we know that if there exists an unramified $(G, G')$-extension $L/K$, then $(G, G')$ must be admissible.

Lemmermeyer noted in \[11\] that there existed a unique admissible pair $(H_k, G')$ with $[G' : H_k] = 2$, and then classified unramified $(H_k, G')$-extensions. This classification took advantage of the following property:

**Definition 4.2.** Call a pair $(G, G')$ central if

$$[G', G'] \leq Z(G')$$

where $Z(G')$ is the center of the group $G'$.

**Proposition 4.1.** Let $(G, G')$ be a central admissible pair. Then $\text{Aut}([G', G'])$ acts transitively on $\{[E] \in H^2((G')^{ab}, [G', G']) : E \cong G'\}$ with stabilizers isomorphic to $\text{Aut}([G'])$

**Proof.** Given $[E]$ with an embedding $i : [G', G'] \hookrightarrow E$, $\alpha \in \text{Aut}([G', G'])$ acts on it by $i \mapsto i \circ \alpha$. Because $[G', G'] = [E, E]$ is the commutator subgroup, every such isomorphism $[E] \cong [E]$ must arise from this action, showing that the stabilizer is a quotient of $\text{Aut}([E])$. Moreover, every extension is completely determined by the embedding of $[G', G']$ as the commutator subgroup, because the quotient is just the abelianization map which is characteristic (i.e. invariant under any automorphism which is trivial on the abelianization). Therefore the the stabilizer is isomorphic to $\text{Aut}([G'])$ and because $\text{Aut}([G', G'])$ acts transitively on $\text{Isom}([G', G'], [E, E])$, it must act transitively on $\{[E] : E \cong G'\}$. \[\square\]

This will be sufficient to prove the following two corollaries:

**Corollary 4.2.** Let $(G, G')$ be a central admissible pair and $K/Q$ an abelian extension with $\overline{f} : G_k \to \text{Gal}(K/Q) = G'/G$. There exists an unramified $(G, G')$-extension $L/K$ if and only if their exists a factorization $\text{disc}(K)^{[G', G']} = \prod_{y \in Y_{G'}(d_y)} (d_y)^{[G']^{ab}, (y)}$ into coprime discriminants (except that at most two are allowed to be even) satisfying the following:

1. (a) $Y_{G'} = \{y \in (G')^{ab} : \text{Res}_{(g)}^{(G')^{ab}} ([G']) = 0\}$
   (b) $|y| (p-1)p^{\infty}$ for every prime dividing $d_y$.
   (c) If $d_y, d_y'$ are even with $y \neq y'$ then $yy'$ has order dividing 2. If $d_y$ is a unique even factor and $4 \parallel d_y$, then $y$ has order dividing 2.
   (d) $\prod_{d_y < y} y^{|y|/2} \in Y_{G'}$.
   (e) $p | d_y$ implies $yG = \overline{f}(\tau_p) \in G'/G$
   (f) $(G')^{ab} = \langle y : d_y \neq 1 \rangle$
(g) \( d_y = 1 \) for all \( y \in Y_G \cap G \).

2. For every prime \( p \mid d \)

\[
\sum_{y \in Y_G} \left( \frac{p}{d_y} \right) \exp([G', G']) [y, f(\tau_y)]_{G'} = 0
\]

where \( \left( \frac{p}{d_y} \right) \exp([G', G']) \in \mathbb{Z}/\exp([G', G'])\mathbb{Z} \).

**Corollary 4.3.** Let \((G, G')\) be a central admissible pair and \(K/\mathbb{Q}\) an abelian extension with \(\tilde{f} : G_{\mathbb{Q}} \to \text{Gal}(K/\mathbb{Q}) = G'/G\). Suppose there exists an unramified \((G, G')\)-extension \(L/K\) with \([\text{Gal}(L/\mathbb{Q})] = [G'] \in H^2(\text{Gal}(G')^\text{ab}, [G', G'])\) corresponding to a factorization \(\text{disc}(K)^{G,[G', G']} = \prod_{y \in Y_G} (d_y)^{([G']^\text{ab}, [y])}\) as in Corollary 4.2. Then there are exactly

\[
\prod_{y \in Y_G} \left( \frac{\#([G', G'][y])}{\#\text{Aut}([G'])\#\text{Hom}(G', [G', G'])} \right)^{\omega(d_y)}
\]

such extensions, where \([G', G'][n] = \{ g \in [G', G'] : g^n = 0 \}\) is the \(n\)-torsion subgroup.

The idea is that these corollaries generalize \[\text{I.2}\] and \[\text{I.2}\]. The first one generalizes the factorization \(d = d_1d_2d_3\) and Dirichlet conditions \(\left( \frac{d_1d_2}{p_1} \right) = \left( \frac{d_1d_3}{p_2} \right) = \left( \frac{d_2d_3}{p_1} \right) = 1\) from \[\text{I.2}\] and the second one generalizes the number \(2^{\omega(d) - 3}\) of such extension corresponding to a factorization in \[\text{I.2}\]. The conditions in these results are significantly denser in order to account for more cases. The reader may be interested in reading Section 5 before the proofs of these corollaries, where we present a worked out example of the result of this section for the Heisenberg group \(H(\ell^3)\), the unique nonabelian group of cardinality \(\ell^3\) and exponent \(\ell\).

**Proof of \[\text{I.2}\].** Fix a choice of \([G'] \in H^2(\text{Gal}(G')^\text{ab}, [G', G'])\). We will prove the theorem for this choice, and then at the end of the proof show that the result for one choice implies the result for every such choice.

Because \((G, G')\) is central and admissible, we know that \(G'\) is a central \([G', G']\)-extension of \((G')^\text{ab}\). Setting \(A = [G', G'], E = G'\) gives us the set-up of the previous sections. Lemma 3.1 shows that \(1(a)(b)(c)(d)(e)\) is equivalent to the existence of a map \(f : G_{\mathbb{Q}} \to (G')^\text{ab}\) which is a lift of the quotient map \(G_{\mathbb{Q}} \to G'/G\) defining \(K/\mathbb{Q}\). 1(f) is equivalent to this map being surjective, and so is equivalent to the existence of a \((G')^\text{ab}\)-extension \(M/\mathbb{Q}\) such that \(M/K\) is unramified. In Theorem \[\text{I.2}\] we get that there exists an unramified lift of \(f\) to \(\tilde{f} : G_{\mathbb{Q}} \to G'\) if and only if part 2 holds. Furthermore, \(d_y = 1\) implies that no ramification is sent to \(y\), so it follows that \(\tilde{f}\) is unramified over the quotient map \(G_{\mathbb{Q}} \to \text{Gal}(K/\mathbb{Q})\) if and only if \(d_y = 1\) for all \(y \in Y_E \cap G\), i.e. condition 1(\(g\)), holds.

It then suffices to check whether or not \(\tilde{f}\) is surjective, by Galois theory. We have \(f\) is surjective by construction, so suppose that \(f\) is not surjective. Then \(\tilde{f}(G_{\mathbb{Q}}) \leq G'\) is a subgroup which surjects onto \((G')^\text{ab}\). Therefore \(G' = \tilde{f}(G_{\mathbb{Q}})A\) as \(A = [G', G']\). If \(A \leq \tilde{f}(G_{\mathbb{Q}})\) then we are done. Let \(B = A \cap \tilde{f}(G_{\mathbb{Q}})\). Then we have \(G'/B \cong \tilde{f}(G_{\mathbb{Q}})/B \times A/B\) since \(\tilde{f}(G_{\mathbb{Q}})/B \cap A/B = 1\). However, \(\tilde{f}(G_{\mathbb{Q}})/B \cong \tilde{f}(G_{\mathbb{Q}})/\tilde{f}(G_{\mathbb{Q}}) \cap A \leq G'/A\) is abelian, implying that \(G'/B\) is abelian. Thus \([G', G'] = A \leq B = \text{im } f \cap A\), concluding the proof for fixed \([G']\).

Because \([G', G']\) is the commutator subgroup, the previous proposition tells us that different choices of \([G']\) only differ by embedding \([G', G']\) up to automorphism. This implies that \([\cdot, \cdot]_{G'}\) differs up to automorphism and \(\text{Res}^{(G')^\text{ab}}_{(G')}([G'])\) is fixed up to isomorphism. This implies that \(Y_{G'}\) is independent of the choice of \([G']\) and \([\cdot, \cdot]_{G'}\) is fixed.
up to automorphism of \([G', G']\), for which the equation in part 2 is invariant because automorphisms of \([G', G']\) are \(\mathbb{Z}/\exp([G', G'])\mathbb{Z}\)-linear maps.

**Proof of** \(\text{L} \Rightarrow \text{R}\) Any unramified \((G, G')\)-extension \(L/K\) corresponding to the factorization \(\mathrm{disc}(K)/[G', G']\) = \(\prod_{y \in Y_{G'}} (d_y)\) contains the field \(\bar{K}\) given by the continuous homomorphism \(f : G_0^\text{ab} \to (G')^\text{ab}\) with \(f(\tau_p) = y\) for \(p \mid d_y\) by construction. So it suffices to count unramified \([G', G']\)-extensions of \(\bar{K}\) whose corresponding extension isomorphism class is \([G']\). By assumption \([G', G']\) is abelian and central, so any such extension must come from a surjective homomorphism \(\mathrm{Cl}(\bar{K}) \to [G', G']\). Let \(H(\bar{K})\) be the Hilbert class field of \(\bar{K}\). Then the exact sequence

\[
1 \longrightarrow \mathrm{Cl}(\bar{K}) \longrightarrow \mathrm{Gal}(H(\bar{K})/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\bar{K}/\mathbb{Q}) \longrightarrow 1
\]

gives rise to the following inflation-restriction sequence with trivial action on \([G', G']\):

\[
0 \longrightarrow H^1(\mathrm{Gal}(\bar{K}/\mathbb{Q}), [G', G']) \longrightarrow H^1(\mathrm{Gal}(H(\bar{K})/\mathbb{Q}), [G', G']) \longrightarrow H^1(\mathrm{Cl}(\bar{K}), [G', G'])^{\mathrm{Gal}(\bar{K}/\mathbb{Q})} \longrightarrow H^2(\mathrm{Gal}(\bar{K}/\mathbb{Q}), [G', G'])
\]

where the last map sends \(f : \mathrm{Cl}(\bar{K}) \to [G', G']\) to \([\mathrm{Gal}(H(\bar{K})^{\mathrm{ker}\ f}/\mathbb{Q})]\). By assumption \([G']\) is in the image of this map. So it follows that there are

\[
H^1(\mathrm{Gal}(H(\bar{K})/\mathbb{Q}), [G', G'])/H^1(\mathrm{Gal}(\bar{K}/\mathbb{Q}), [G', G'])
\]

such homomorphisms \(f : \mathrm{Cl}(\bar{K}) \to [G', G']\) giving rise to \([G']\). Notice that because \([G', G']\) is abelian, any homomorphism \(\mathrm{Gal}(H(\bar{K})/\mathbb{Q}) \to [G', G']\) must factor through \(\mathrm{Gal}(\bar{K}^{\text{gen}}/\mathbb{Q})\), the Galois group of the genus field. If \(f_p : G_0^\text{ab} \to \langle y \rangle\) is the map sending \(\tau_p \mapsto y\) and \(\tau_q \mapsto 0\) for any prime \(q \neq p\) then we can describe the genus field as \(\prod_{p \mid \mathrm{disc}(K)} \mathbb{Q}(\tau_p)\) with Galois group \(\prod_{p \mid \mathrm{disc}(K)} \mathrm{Gal}(\mathbb{Q} \rangle f(\tau_p)\rangle\) over \(\mathbb{Q}\). Thus

\[
H^1(\mathrm{Gal}(H(\bar{K})/\mathbb{Q}), [G', G']) = \text{Hom}\left(\prod_{p \mid \mathrm{disc}(K)} \langle f(\tau_p) \rangle, [G', G']\right)
\]

\[
= \prod_{p \mid \mathrm{disc}(K)} \text{Hom}(\langle f(\tau_p) \rangle, [G', G'])
\]

\[
= \prod_{p \mid \mathrm{disc}(K)} [G', G'][[f(\tau_p)]]
\]

\[
= \prod_{y \in Y_{G'}} \prod_{p \mid d_y} [G', G'][[[y]]]
\]

where \(G[n]\) denotes the \(n\)-torsion of an abelian group. So it follows that

\[
\#H^1(\mathrm{Gal}(H(\bar{K})/\mathbb{Q}), [G', G']) = \prod_{y \in Y_{G'}} (\#([G', G'][[[y]])^{\omega(d_y)})
\]

Then the number of such homomorphisms \(\mathrm{Cl}(\bar{K}) \to [G', G']\) giving rise to \([G']\) is

\[
\frac{\prod_{y \in Y_{G'}} |G', G'][[[y]]|^{\omega(d_y)}}{\#H^1(\mathrm{Gal}(K/\mathbb{Q}), [G', G'])} = \frac{\prod_{y \in Y_{G'}} |G', G'][[[y]]|^{\omega(d_y)}}{\#\text{Hom}((G')^\text{ab}, [G', G'])}
\]

12
Since every homomorphism \( G' \to [G', G'] \) must factor through \((G')^{ab}\), we can replace the bottom with \( \text{Hom}(G', [G', G']) \).

Normally, there are more homomorphisms than corresponding fields, so one might expect that we need to divide by \( \text{Aut}([G', G']) \) to eliminate redundancy. However, the redundancy coming from automorphisms of \([G', G']\) in the case can produce different isomorphism classes of \([G']\). The Proposition\[\text{[11]}\] shows that the subgroup \( \text{Aut}([G']) \to \text{Aut}([G', G']) \) parametrizes all the redundancy, concluding the proof. \( \square \)

5 Heisenberg Groups

Fix an odd prime \( \ell \) and consider the Heisenberg group

\[ H(\ell^3) = \langle x, y : [x, y] = z, x^\ell = y^\ell = z^\ell = 1, [x, z] = [y, z] = 1 \rangle \]

This is the unique nonabelian group of order \( \ell^3 \) and exponent \( \ell \). We define

\[ E = H(\ell^3) \rtimes \mathbb{C}_\ell = \langle x, y, \sigma : [x, y] = [x, \sigma] = z, x^\ell = y^\ell = \sigma^\ell = 1, [x, z] = [y, z] = 1 \rangle \]

In particular, \( \langle z \rangle = [E, E] \leq Z(E) \) giving us a central exact sequence

\[ 1 \longrightarrow C_\ell \longrightarrow E \longrightarrow C_\ell^3 \longrightarrow 1 \]

This makes \( (H(\ell^3), E) \) a central admissible pair. Moreover, because every element of \( E \) has order \( \ell \), it follows that \( Y_E = E^{ab} = C_\ell^3 \). We will prove the following classification as an example of Corollary\[\text{[12]}\] and Corollary\[\text{[13]}\]

**Theorem 5.1.** Let \( K/\mathbb{Q} \) be a cyclic degree \( \ell \) extension of discriminant \( d = p^{\ell-1}q^{\ell-1}r^{\ell-1} \) coprime to \( \ell \). Fix \( g \in \text{Gal}(K/\mathbb{Q}) \) as a generator of every nontrivial inertia group. Then there exists an unramified \( (H(\ell^3), E) \) extension \( L/K \) if and only if there exists \( A, B, C \in \mathbb{Z}/\ell\mathbb{Z} \) with \( A + B + C \neq 0 \) and

\[
\begin{align*}
\left( \frac{p}{q^{\ell-1}} \right)_\ell (A + (C)_\ell B) &= 0 \\
\left( \frac{q}{p^{\ell-1}} \right)_\ell A + \left( \frac{q}{r^{\ell-1}} \right)_\ell (C) &= 0 \\
\left( \frac{r}{p^{\ell-1}} \right)_\ell (-B) + \left( \frac{r}{q^{\ell-1}} \right)_\ell C &= 0
\end{align*}
\]

Moreover, in that case there are exactly \( \ell - 1 \) such extensions for each factorization, which all have distinct extension classes \( [\text{Gal}(L/\mathbb{Q})] ] \in H^3(C_\ell^3, C_\ell) \).

**Proof.** Fix \( \pi : E^{ab} \to C_\ell \) the quotient map given above. Without loss of generality, we choose generators \( \tau_p, \tau_q, \tau_r \in G_Q^{ab} \) such that \( \overline{T} : G_Q^{ab} \to \text{Gal}(K/\mathbb{Q}) = C_\ell \) satisfies \( \overline{T}(\tau_p) = \overline{T}(\tau_q) = \overline{T}(\tau_r) = g \).

We will walk through the conditions of the corollary for this case, describing what they each correspond to. Suppose we have a factorization

\[ \text{disc}(K)^{[H(\ell^3), [E, E]]} = d^2 = \prod_{y \in Y_E} (d_y)^{[E^{ab}, (y)]} = \prod_{y \in Y_E} d_y^2 \]

in other words, \( d = \prod_{y \in Y_E} d_y \). This corresponds to a lift

\[
\begin{array}{ccc}
G_Q & \xrightarrow{f} & C_\ell \\
\downarrow \overline{T} & & \\
E^{ab} & \xrightarrow{g} & C_\ell
\end{array}
\]
as in Lemma \ref{lem:4.1} if and only if the factorization satisfies 1(a)(b)(c)(d)(e) of Corollary \ref{cor:4.2}.

We will now walk through each part of Corollary \ref{cor:4.2} describing what properties they imply and verifying them for our pair \((H(\ell^3), E)\):

1. (a) \(Y_E\) is the set of possible images of ramification in \(E^{ab}\), which is equivalent to having \(\text{Res}^{E^{ab}}_{E}([E]) = 0\) for finite primes. We see that every element of \(E\) has order \(\ell\), which implies that \(Y_E = E^{ab} = C_2\).

(b) By the existence of the field \(K\), we must have \(\ell \mid p - 1, q - 1, r - 1\). Every element of \(Y_E\) has order \(\ell\), so this part is vacuous.

(c) \(K\) cannot be ramified at 2, so none of the factors are even making this part vacuous as well.

(d) \(Y_E = E^{ab}\) makes this part vacuous, as everything belongs to \(Y_E\). This part shows that \(\text{Res}^{E^{ab}}_{E}([E]) = 0\).

(e) By assumption, \(\mathcal{T}(\tau_p) = \mathcal{T}(\tau_q) = \mathcal{T}(\tau_r) = g\), so \(d_g \neq 1\) requires \(\pi(y) = g\).

This is necessary for there to exist \(f : G_Q \to E^{ab}\) a well-defined lift of \(\mathcal{T} : G_Q \to G\) corresponding to our factorization. Call the corresponding \(y\) values \(f(\tau_p) = y_p\), \(f(\tau_q) = y_q\), and \(f(\tau_r) = y_r\) respectively.

(f) This is equivalent to the lift \( f : G_Q \to E^{ab}\) being surjective, i.e. \(E^{ab} = \langle y_p, y_q, y_r \rangle\). This is true if and only if \(\ker \pi = \langle y_p y_q^{-1}, y_r y_r^{-1} \rangle\), i.e. \(y_p y_q^{-1}, y_r y_r^{-1}\) are linearly independent by \(\dim_Q\ker \pi = 2\).

(g) This is equivalent to \(f\) being unramified over \(\mathcal{T}\). Given a choice of \(y_p, y_q, y_r\) generating \(E^{ab}\) satisfying the above conditions, this is vacuously true as \(\pi(y_\ell) = g \neq 1\), so \(y_\ell \notin H(\ell^3)\).

This implies that part 1 of Corollary \ref{cor:4.2} is satisfied if and only if the factorization is given by \(d = \prod_{\pi(y) = g} d_g\) and \(\{y_p y_q^{-1}, y_r y_r^{-1}\}\) are linearly independent. Given these, part 1 gives us a lift \(f : G_Q \to E^{ab}\) with \(\text{Res}^{E^{ab}}_{E}([E]) = 0\) for all primes.

2. This is equivalent to \([f(\text{Frob}_p), f(\text{Frob}_q)]_E = 0\), and can be distilled into three equations:

\[
\begin{align*}
\left(\frac{p}{q^\ell-1}\right)_E [y_q, y_p]_E + \left(\frac{p}{r^\ell-1}\right)_E [y_r, y_p]_E &= 0 \\
\left(\frac{q}{p^\ell-1}\right)_E [y_p, y_q]_E + \left(\frac{q}{r^\ell-1}\right)_E [y_r, y_q]_E &= 0 \\
\left(\frac{r}{p^\ell-1}\right)_E [y_p, y_r]_E + \left(\frac{r}{q^\ell-1}\right)_E [y_r, y_r]_E &= 0
\end{align*}
\]

since the factors will be trivial whenever \(d_g = 1\).

Corollary \ref{cor:4.2} tells us that there exists an unramified \((H(\ell^3), E)\)-extension \(L/K\) if and only if parts 1 and 2 hold.

Consider the presentation given in the previous section

\[E = \langle x, y, \sigma : [x, y] = [x, \sigma] = [y, \sigma] = z, x^\ell = y^\ell = z^\ell = \sigma^\ell = 1, [x, z] = [y, z] = 1 \rangle\]

and without loss of generality let \(\sigma\) be a preimage of \(g\). Then we have the bilinear map

\[\langle \cdot, \cdot \rangle_E : \langle \overline{x}, \overline{y}, \overline{\sigma} : \overline{x}^\ell = \overline{y}^\ell = \overline{\sigma}^\ell = 1 \rangle^{ab} \to \langle z \rangle = \mathbb{Z}/\ell\mathbb{Z}\]

Where we write \(\mathbb{Z}/\ell\mathbb{Z}\) additively, is defined by it’s values on the basis \(\overline{x}, \overline{y}, \overline{\sigma}\), given by being antisymmetric with \([\overline{x}, \overline{y}]_E = [\overline{x}, \overline{\sigma}]_E = [\overline{y}, \overline{\sigma}]_E = z\).
By construction, we must have $y_p = v_p\mathbf{e}$, $y_q = v_q\mathbf{e}$, and $y_r = v_r\mathbf{e}$ for $v_i \in \langle \mathbf{e}, \mathbf{f} \rangle$. We have that $[y, y_j]_E = [v_i, v_j]_E + [v_i, \mathbf{e}]_E + [\mathbf{e}, v_j]_E$ for any choice of $i, j \in \{p, q, r\}$ by a simple computation. Consider

$$[\mathbf{e}^1, y_j]_E = a_1b_2 - a_2b_1 = \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

$$[\mathbf{e}^1, \mathbf{e}]_E = a_1 + b_1$$

So it follows that

$$[\mathbf{e}^1, y_j]_E = a_1b_2 - a_2b_1 + a_1 + b_1 - a_2 - b_2$$

$$= (a_1 - 1)(b_2 + 1) - (a_2 + 1)(b_1 - 1)$$

is also a determinant. The requirement that $y_p y_q^{-1}, y_p y_r^{-1}$ are linearly independent is the same as the requirement that $v_p v_q^{-1}, v_p v_r^{-1}$ are linearly independent. A pair of vectors being linearly independent is equivalent to the matrix with those vectors as column vectors having nonzero determinant. So condition 1 is equivalent to $y_p, y_q, y_r$ mapping to $g$ under $\pi$ and satisfying

$$0 \neq [v_p v_q^{-1}, v_p v_r^{-1}]_E$$

$$= -[v_p, v_r]_E - [v_q, v_p]_E + [v_q, v_r]_E$$

$$= [v_r, v_p]_E + [v_p, v_q]_E + [v_q, v_r]_E$$

$$= [y_r, y_p]_E + [y_p, y_q]_E + [y_q, y_r]_E$$

Fix $A, B, C \in \mathbb{Z}/\ell\mathbb{Z}$ with $A + B + C \neq 0$. Suppose $y_p, y_q$ are chosen with $[y_p, y_q]_E = A$. Then we have that choosing $y_r = \mathbf{e}^p y^q y^r$ with $[y_r, y_p]_E = B$ and $[y_q, y_r]_E = C$ is equivalent to solving a system of two linear equations in two variables. Write $y_p = \mathbf{e}^p y^q y^r$ and $y_q = \mathbf{e}^p y^q y^r$, then we want a solution to

$$(a_r - 1)(b_p + 1) - (a_p + 1)(b_r - 1) = B$$

$$(a_q - 1)(b_r + 1) - (a_r + 1)(b_q - 1) = C$$

In other words

$$\begin{pmatrix} b_p + 1 & -(a_p + 1) \\ -(b_q - 1) & a_q - 1 \end{pmatrix} \begin{pmatrix} a_r \\ b_r \end{pmatrix} = \begin{pmatrix} B - b_p + a_p \\ C + a_q - b_q \end{pmatrix}$$

where the matrix has determinant

$$(b_p + 1)(a_q - 1) - (a_p + 1)(b_q - 1) = [y_q, y_p]_E = -A$$

WLOG by symmetry we may assume that $A \neq 0$ by $A + B + C \neq 0$, therefore we may find such a choice for $y_r$. This shows that any such choice of $A, B, C$ can be realized by $y_p, y_q, y_r$, so the equations on Dirichlet characters in this theorem are equivalent to condition 2 of Corollary 4.2 for some choice of $y_p, y_q, y_r$ satisfying condition 1.

As for the number of such extensions corresponding to a factorization, notice that plugging $[E, E] = C_\ell$, $|y| = \ell$, and $E^{ab} = C_3^a$ into the formula in Corollary 4.3 tells us that there are

$$\frac{\ell^{\omega(d) - 3}}{\# \text{Aut}([E])} = \frac{1}{\text{Aut}([E])}$$

such extensions for the choice of $[E]$. This implies that $\text{Aut}([E]) = 1$, which can be checked group theoretically. There are $\# \text{Aut}([E, E])/\# \text{Aut}([E]) = (\ell - 1)/1$ isomorphism classes of $[E]$ by Proposition 3.1, concluding the proof.
6 Acknowledgements

I would like to thank my advisor Nigel Boston for many helpful conversations, advice, and recommendations. I would also like to thank Yuan Liu for helpful conversations about the Brauer embedding problem. This work was done with the support of National Science Foundation grant DMS-1502553.

References

[1] B. Alberts. Cohen-Lenstra moments for some nonabelian groups, Aug 2016. Preprint available at https://arxiv.org/abs/1606.07867
[2] B. Alberts and J. Klys. The distribution of $H_2$-extensions of quadratic fields, Jun 2017. Preprint available at https://arxiv.org/abs/1611.05595
[3] M. Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials, Jan 2014. Preprint available at https://arxiv.org/abs/1402.0031?context=math
[4] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. Lecture Notes in Mathematics Number Theory Noordwijkerhout 1983, page 3362, 1984.
[5] E. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. Inventiones Mathematicae, 167(3):455513, 2006.
[6] R. Fueter. Der Klassenkörper der quadratischen Körper und die komplexe Multiplikation. Diss. Göttingen, 1903.
[7] F. Gerth. The 4-class ranks of quadratic fields. Inventiones Mathematicae, 77(3):489515, 1984.
[8] G. Gras. Sur les $\ell$-classes d’idéaux dans les extensions cycliques relatives de degré premier $\ell$. Ann. Inst. Fourier, 23.3, 23.4:1–48, 1–44, 1973.
[9] E. Inaba. Über die Struktur der $\ell$-Kassengruppe zyklischer Zahlkörper von Primzahlgrad $\ell$. J. Fac. Sci. Tokyo I, 4:61–115, 1940.
[10] J. Klys. The distribution of $p$-torsion in degree $p$ cyclic fields, Oct 2016. Preprint available at https://arxiv.org/abs/1610.00226v1
[11] F. Lemmermeyer. Unramified quaternion extensions of quadratic number fields. Journal de Théorie des Nombres de Bordeaux, 9(1):5168, 1997.
[12] F. Lemmermeyer. Class field towers, 2010. available at http://www.rzuser.uni-heidelberg.de/~hb3/publ/pcft.pdf
[13] G. Malle and B. H. Matzat. Inverse Galois theory. 1994.
[14] J. Martinet. A propos de classes d’idéaux. Séminaire Théorie des Nombres Bordeaux, 5, 1971/1972.
[15] N. Nakagoshi. A construction of unramified abelian $\ell$-extensions of regular Kummer extensions. Acta Arith., 44:47–58, 1984.
[16] A. Nomura. On the existence of unramified $p$-extensions. Osaka Journal of Mathematics, 28:55–62, 1991.
[17] A. Nomura. A note on unramified quaternion extensions over quadratic number fields. Proc. Japan Acad., 78:80–82, 2002.
[18] A. Nomura. Notes on the existence of certain unramified 2-extensions. Illinois Journal of Mathematics, 46:1279–1286, 2002.
[19] A. Nomura. Notes on the existence of unramified non-abelian \( p \)-extensions over cyclic fields. *Proc. Japan Acad.*, 90:67–70, 2014.

[20] Y. Odai. On unramified cyclic extensions of degree \( \ell \) of algebraic number fields of degree \( \ell \). *Nagoya Math. J.*, 107:135–146, 1987.

[21] L. Rédei. Die Anzahl der durch 4 teilbaren Invarianz der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *Math. Naturwiss. Anz. Ungar. Akad. d. Wiss.*, 10:338–363, 1932.

[22] L. Rédei and H. Reichardt. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. Reine Angew. Math.*, 170:69–74, 1933.

[23] H. Reichardt. Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 170:75–82, 1933.

[24] J.-P. Serre. *Topics in Galois Theory*. A K Peters, 2008.

[25] M. M. Wood. Nonabelian Cohen-Lenstra moments, Feb 2017. Preprint available at [https://arxiv.org/abs/1702.04644](https://arxiv.org/abs/1702.04644)