RAMIFICATION IN THE INVERSE GALOIS PROBLEM

Benjamin Pollak

A DISSERTATION

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2019

Supervisor of Dissertation

_____

David Harbater, Christopher H. Browne Distinguished Professor in the School of Arts and Sciences

Graduate Group Chairperson

_____

Julia Hartmann, Professor of Mathematics

Dissertation Committee:
David Harbater, Christopher H. Browne Distinguished Professor in the School of Arts and Sciences
Florian Pop, Samuel D. Schack Professor of Algebra
Mona Merling, Assistant Professor of Mathematics

Acknowledgments

I would first like to thank my advisor, David Harbater, whose support was essential in the creation of this thesis. Not only did he initially introduce me to the problems that form the bulk of this dissertation, but he also was extremely generous with his time and was always willing to meet with me to work through any roadblocks I encountered. Mostly, however, I would like to thank him for teaching me how to develop a well grounded mathematical intuition that enabled me to do research in the field; the time I spent discussing mathematics with him was an indispensable part of my growth as a mathematician.

Next I would like to extend my thanks to Florian Pop for serving on both my thesis advisory committee and my thesis defense committee, to Julia Hartmann for serving on my oral exam committee and my thesis advisory committee, to Greta Panova for serving on my oral exam committee, and to Mona Merling for serving on my thesis defense committee. I also want to express my gratitude to Reshma Tanna, Monica Pallanti, Paula Scarborough, and Robin Toney for their support and for their aid in dealing with the administrative aspects of the graduate program.

Thank you to my graduate cohort, Dominick Villano, The Gia Hoang, Marcus Michelen, Michael Gerapetritis, Zhen Zeng, and Yuhang Liu, for all the encouragement they provided me as I worked on my thesis. Finally, I want to thank all of the remaining members, both former and current, of the University of Pennsylvania's Department of Mathematics for creating such a welcoming environment in which to study mathematics.

ABSTRACT

RAMIFICATION IN THE INVERSE GALOIS PROBLEM

Benjamin Pollak

David Harbater

This thesis focuses on a refinement of the inverse Galois problem. We explore what finite groups appear as the Galois group of an extension of the rational numbers in which only a predetermined set of primes may ramify. After presenting new results regarding extensions in which only a single finite prime ramifies, we move on to studying the more complex situation in which multiple primes from a finite set of arbitrary size may ramify. We then continue by examining a conjecture of Harbater that the minimal number of generators of the Galois group of a tame, Galois extension of the rational numbers is bounded above by the sum of a constant and the logarithm of the product of the ramified primes. We prove the validity of Harbater's conjecture in a number of cases, including the situation where we restrict our attention to finite groups containing a nilpotent subgroup of index $1, 2$ or 3, and also derive consequences that are implied by the truth of this conjecture. We conclude by exploring how circumstances change when the base field of the rational numbers is replaced by an arbitrary number field.

Contents

List of Tables

Chapter 1

Introduction

1.1 The Inverse Galois Problem

The traditional inverse Galois problem asks if every finite group appears as the Galois group of some extension of the rational numbers. Although this question has remained open for centuries, many families and specific examples of finite groups have been realized as Galois groups over $\mathbb{Q}$. By the end of the 19th century, it had become evident that all finite abelian groups are Galois groups over $\mathbb{Q}$. Then, in 1937, Scholz and Reichardt showed that all finite nilpotent groups of odd order occur as Galois groups over $\mathbb{Q}$. Finally, in 1954 with a subsequent correction in 1989, Shafarevich proved that every finite solvable group can be realized as a Galois group over $\mathbb{Q}$. While an answer to whether every finite non-solvable group is a Galois group over the rational numbers continues to elude us, techniques includ-

ing Hilbert irreducibility, rigidity, modular Galois representations, and computer searches have provided a partial understanding. For example, all the finite symmetric and alternating groups, as well as 25 of the 26 sporadic simple groups, are known to be Galois groups over $\mathbb{Q}$. In [34], Zywina shows the same for $\mathrm{PSL}_2(\mathbb{F}_p)$ where $p \geq 5$ is prime.

1.2 A Refinement of the Inverse Galois Problem

Given a finite group, in addition to simply asking whether it appears as a Galois group over $\mathbb{Q}$, it is also of interest to study the finer structure of extensions that realize it as a Galois group. We will focus on how the set of ramified primes in a Galois extension of the rationals relates to properties of the Galois group. More precisely, given a finite set of primes, we will explore what finite groups may appear as Galois groups of extensions of $\mathbb{Q}$ that are unramified outside of the given set of primes.

Following the notation in [10], given a square-free $n \in \mathbb{N}$ we let U_n denote $\mathrm{Spec}\left(\mathbb{Z}\left[\frac{1}{n}\right]\right)$, an open subset of $\mathrm{Spec}(\mathbb{Z})$. $\pi_1(U_n)$ will be the étale fundamental group; it is the Galois group of the maximal extension of $\mathbb{Q}$ that is unramified at finite primes not dividing n. We then let $\pi_A(U_n)$ be the set of finite quotients of $\pi_1(U_n)$; it is the set of finite groups appearing as Galois groups of extensions of $\mathbb{Q}$ unramified at finite primes not dividing n. Finally, we denote by $\pi_A^t(U_n)$ the set of Galois groups appearing when we restrict our attention to tame extensions.

Our main goal is to provide some insight into the contents of $\pi_A(U_n)$. Since at least one finite prime ramifies in every extension of $\mathbb{Q}$, $\pi_A(U_1)$ consists of only the trivial group. Apart from this simple case, there is no other square-free n for which $\pi_A(U_n)$ is completely understood. Nevertheless, we can obtain a partial description. Given a specific square-free n, the focus of Chapter 2 is to say as much as possible about extensions of $\mathbb{Q}$ unramified at finite primes not dividing n. Chapter 3 is devoted to studying how generating sets of a Galois group relate to the ramified primes in the corresponding extension.

For a finite group G, let

$$d(G) = \min\{|S| \ | S \text{ is a generating set for } G\}.$$

In the function field case, a square-free polynomial $f \in \mathbb{F}_p[t]$ of degree d has norm p^d. Let $U \subseteq \mathbb{A}^1_{\mathbb{F}_p}$ be the complement of the vanishing set of f and $\pi_A^{\mathrm{t,reg}}(U)$ be the finite groups appearing as Galois groups of tame, regular extensions of $\mathbb{F}_p(t)$ unramified outside of primes dividing f. Then, any $G \in \pi_A^{\mathrm{t,reg}}(U)$ satisfies $d(G) \leq d = \log_p(\mathrm{Norm}(f))$. Motivated by this analogy, in the arithmetic situation we view $U_n \subseteq \mathrm{Spec}(\mathbb{Z})$ as the complement of the vanishing set of a square-free natural number n that has norm n. In [10], Harbater then proposes the following conjecture:

Conjecture 1.2.1. *There is a constant C such that for every square-free $n \in \mathbb{N}$, every $G \in \pi_A^t(U_n)$ satisfies $d(G) \leq \log(n) + C$.*

Remark 1.2.2. In the function field case, the base of the logarithm was the characteristic. Since that is not possible in the arithmetic case, we use e as the base instead. The addition of the constant is because in the function field case we may require one extra generator, the Frobenius, if we do not restrict our attention to regular extensions. Additionally, the analogous statement for curves of higher genus in the function field case would require a constant depending on the genus. If in the analogy between number fields and function fields the "genus" of $\mathbb{Q}$ is not 0, then this would be accounted for by the extra constant in the conjecture.

In Chapter 3 we will prove that if we only consider groups with a nilpotent subgroup of index $1, 2$, or 3, then Conjecture 1.2.1 is true.

1.3 Background

In this section we introduce some notation and provide some background results that will be essential in the subsequent chapters. This includes statements from class field theory, bounds on the discriminant of a number field, and the Brauer-Siegel theorem; these results are collected from [20], [30], [15], and [4].

We start by listing some key results from class field theory.

Theorem 1.3.1. *(Kronecker-Weber) A finite extension of $\mathbb{Q}$ is abelian if and only if it is a subfield of some cyclotomic field.*

For a number field K with ring of integers $\mathcal{O}_K$, we let $Cl(K)$ denote the class

group of K, the group of fractional ideals modulo principal ideals in $\mathcal{O}_K$.

Theorem 1.3.2. *The Hilbert class field of a number field K is the maximal abelian unramified extension of K. The Galois group of the Hilbert class field over K is isomorphic to $Cl(K)$.*

A modulus, $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, is a formal product of primes in $\mathcal{O}_K$; $\mathfrak{m}_0$ denotes the product of the finite places and $\mathfrak{m}_\infty$ denotes the product of the infinite places. The ray class group corresponding to $\mathfrak{m}$, $Cl_\mathfrak{m}(K)$, is the group of fractional ideals coprime to $\mathfrak{m}$ modulo the group of principal ideals generated by elements that are congruent to 1 modulo $\mathfrak{m}_0$ and positive at each place dividing $\mathfrak{m}_\infty$. $\mathfrak{m}$ admits an abelian extension of K, called the ray class field corresponding to $\mathfrak{m}$, with Galois group isomorphic to $Cl_\mathfrak{m}(K)$.

Theorem 1.3.3. *Every finite abelian extension of K is contained in a ray class field of K corresponding to some modulus.*

If E/K is abelian and E is a subfield of the ray class field of K for the modulus $\mathfrak{m}$, we say that $\mathfrak{m}$ is an admissible modulus. The greatest common divisor of two admissible moduli is also admissible. Hence, there is a least admissible modulus, called the conductor.

Theorem 1.3.4. *If E/K is abelian with conductor $\mathfrak{m}$, then the primes that ramify in E/K are those that divide $\mathfrak{m}$. Furthermore, $\mathfrak{P} \mid \mathfrak{m}$ is tamely ramified if and only if the highest power of $\mathfrak{P}$ dividing $\mathfrak{m}$ is* 1.

If $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, then we let

$$(\mathcal{O}_K/\mathfrak{m})^* = (\mathcal{O}_K/\mathfrak{m}_0)^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}.$$

Let $U(K)$ denote the unit group of K and $U_{\mathfrak{m}}(K)$ the intersection of the unit group with elements that are congruent to 1 modulo $\mathfrak{m}_0$ and positive at each place dividing $\mathfrak{m}_\infty$.

Theorem 1.3.5. *The following sequence is exact:*

$$1 \to U_{\mathfrak{m}}(K) \to U(K) \to (\mathcal{O}_K/\mathfrak{m})^* \to Cl_{\mathfrak{m}}(K) \to Cl(K) \to 1.$$

We now provide some bounds for the discriminant of a number field. The following upper bound can be found in [30].

Theorem 1.3.6. *Let K be a number field with discriminant Δ. For a prime p, let e_i and f_i denote the ramification indices and residue degrees of the primes lying over it. Then*

$$v_p(\Delta) \leq \sum_i f_i \left(e_i - 1 + e_i v_p(e_i)\right).$$

[23], [24], and [7] provide lower bounds for discriminants of number fields.

We conclude with a statement of the Brauer-Siegel theorem from [4].

Theorem 1.3.7. *Let $K_1, K_2, K_3, \ldots$ be a sequence of number fields all of a fixed degree over $\mathbb{Q}$. Let d_i, h_i, and R_i denote the discriminant, class number, and regulator*

of K_i respectively. Then

$$\frac{\log(h_i R_i)}{\log\left(|d_i|^{\frac{1}{2}}\right)} \to 1 \text{ as } i \to \infty.$$

1.4 Related Results

In [10], Harbater studies extensions in which a single prime ramifies. One of his main results is

Theorem 1.4.1. *If $p < 23$ is prime, then $\pi_1^t(U_p)$ is cyclic of order $p-1$.*

In Section 2.1.1 we obtain a similar statement for totally real extensions. Harbater also more extensively studies the prime 2 and shows

Theorem 1.4.2. *1. Let G be a solvable group in $\pi_A(U_2)$. Then either G is a 2-group of order < 16, or G has a quotient of order 16.*

2. Let $K/\mathbb{Q}$ be a Galois extension in which 2 is the only finite prime that ramifies. Then 16 divides the ramification index unless the Galois group is a 2-group of order < 16.

For a prime p and a finite group G, we let $p(G)$ denote the subgroup generated by the union of the Sylow p-subgroups. In [12], Hoelscher proves the following:

Theorem 1.4.3. *1. If $p = 3$ and G is a solvable group in $\pi_A(U_p)$, then either G is cyclic, $G/p(G) \cong \mathbb{Z}/2\mathbb{Z}$, or G has a cyclic quotient of order 27.*

2. *Suppose $K/\mathbb{Q}$ is a nontrivial Galois extension in which 3 is the only finite prime that ramifies. Let G denote the Galois group. Then 9 divides the ramification index unless $G/p(G) \cong \mathbb{Z}/2\mathbb{Z}$ or $G \cong \mathbb{Z}/3\mathbb{Z}$*

In Section 2.1.2 we provide an analogous result for the prime 5. Expanding upon Harbater's work in [10], Hoelscher also shows that small groups in $\pi_A(U_p)$ for small primes tend to be solvable.

Theorem 1.4.4. *Let $2 \leq p \leq 23$ be a prime number. If $G \in \pi_A(U_p)$ and $|G| \leq 300$, then G is solvable.*

We improve upon this result in Theorem 2.1.10.

Given a finite group G, one may also ask what is the smallest number of ramified primes necessary for an extension of $\mathbb{Q}$ to have Galois group G. Letting G^{ab} denote the abelianization of G, Boston and Markin conjecture the following in [3]:

Conjecture 1.4.5. *For every nontrivial finite group G, there is an extension of $\mathbb{Q}$ with Galois group G and $\max\left\{1, d\left(G^{ab}\right)\right\}$ many ramified primes (counting the infinite place).*

If G is abelian and nontrivial, the Kronecker-Weber theorem shows that the fewest number of ramified primes in an extension of $\mathbb{Q}$ with Galois group G is $d(G)$. Hence, for an arbitrary nontrivial finite group $G, \max\left\{1, d\left(G^{\text{ab}}\right)\right\}$ is a lower bound on the minimal number of ramified primes we can have in any extension with Galois group G; Conjecture 1.4.5 posits that this lower bound is actually achieved.

Since the finite symmetric groups and alternating groups have cyclic abelianization, Conjecture 1.4.5 suggests that they should be realizable as Galois groups over $\mathbb{Q}$ with only a single ramified prime. In [14], Jones and Roberts prove the following:

Theorem 1.4.6. *1. $p = 101$ is the smallest prime such that $S_5 \in \pi_A(U_p)$.*

2. $p = 197$ is the smallest prime such that $S_6 \in \pi_A(U_p)$.

3. $p = 163$ is the smallest prime such that $S_7 \in \pi_A(U_p)$.

4. $p = 653$ is the smallest prime such that $A_5 \in \pi_A(U_p)$.

5. $p = 1579$ is the smallest prime such that $A_6 \in \pi_A(U_p)$.

In Section 2.1.4 we show that for any natural number $n \leq 30$, there is a prime p such that $S_n \in \pi_A(U_p)$. We also provide examples of A_7, A_8, A_9, and A_{10} extensions of $\mathbb{Q}$ ramified at a single finite prime.

Chapter 2

Galois Extensions of $\mathbb{Q}$ with Specified Ramification

2.1 Extensions Ramified at a Single Prime

2.1.1 Totally Real Extensions

Harbater shows in [10] that for $p < 23$ a prime number, the cyclotomic extension $\mathbb{Q}(\zeta_p)$ is the maximal extension of $\mathbb{Q}$ that is tamely ramified only at p and ∞. We now present some analogous results in the totally real case in which the infinite place is also restricted from ramifying. For a square-free $n \in \mathbb{N}$, we let $\pi_1^{\mathrm{t,tr}}(U_n)^{\mathrm{solv}}$ denote the set of solvable groups appearing as the Galois group of tame, totally real extensions of $\mathbb{Q}$ in which only primes dividing n may ramify.

Proposition 2.1.1. *Let p be a prime number. If $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ has class number*

1, *then* $\pi_1^{\mathrm{t,tr}}(U_p)^{\mathrm{solv}}$ *is cyclic of order* $\frac{p-1}{2}$. *Hence, if* $K/\mathbb{Q}$ *is a totally real, tame, solvable extension only ramified at* p, *then* $K \leq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Proof. Let p be a prime number such that $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ has class number 1. Suppose $G \in \pi_A^{\mathrm{t,tr}}(U_p)^{\mathrm{solv}}$. Let $K/\mathbb{Q}$ be an extension providing witness to the fact that $G \in \pi_A^{\mathrm{t,tr}}(U_p)^{\mathrm{solv}}$. Let $G^{(1)} = [G, G]$ and $G^{(2)} = [G^{(1)}, G^{(1)}]$ be the first and second commutator subgroups respectively. Letting $K^{G^{(1)}}$ and $K^{G^{(2)}}$ denote the fixed fields, we obtain the following diagram:

$$\begin{array}{c} K \\ | \\ K^{G^{(2)}} \\ | \\ K^{G^{(1)}} \\ | \\ \mathbb{Q} \end{array} .$$

Since $K^{G^{(1)}}$ is an abelian extension of $\mathbb{Q}$ that is totally real and tamely ramified only at p, by the Kronecker-Weber theorem we have $K^{G^{(1)}} \leq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $K^{G^{(1)}}/\mathbb{Q}$ is totally ramified. Note now that $K^{G^{(1)}}$ must have class number 1. If not, it would have a nontrivial, unramified, abelian extension. However, taking the compositum of such an extension with $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ would then yield a nontrivial, unramified, abelian extension of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$, contradicting $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ having class

number 1. Thus, the abelian extension $K^{G^{(2)}}/K^{G^{(1)}}$ has no nontrivial, unramified subextensions, and so must be totally ramified. This implies that $K^{G^{(2)}}/\mathbb{Q}$ is totally ramified. By the tameness assumption, it must also be cyclic. Hence, $G/G^{(2)}$ is abelian, and so $G^{(1)} = G^{(2)}$. By assumption of G being solvable, we conclude that $G^{(1)}$ must be trivial and $K^{G^{(1)}} = K$. Thus, $K \leq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and G is cyclic of order dividing $\frac{p-1}{2}$. □

Corollary 2.1.2. *Suppose $p \leq 151$ is an odd prime. Then $\pi_1^{\mathrm{t,tr}}(U_p)^{\mathrm{solv}}$ is cyclic of order $\frac{p-1}{2}$; the maximal tame, totally real, solvable extension of $\mathbb{Q}$ ramified only at p is $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

Proof. By Theorem 1.1 in [19], the class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is 1 for $p \leq 151$. Now apply Proposition 2.1.1. □

Remark 2.1.3. If the class number of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ is larger than 1, then, as evidenced by the Hilbert class field of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, $\pi_1^{\mathrm{t,tr}}(U_p)^{\mathrm{solv}}$ is not cyclic.

For $p \leq 53$, we can drop the solvable assumption in Proposition 2.1.1.

Proposition 2.1.4. *Suppose $p \leq 53$ is an odd prime. Then $\pi_1^{\mathrm{t,tr}}(U_p)$ is cyclic of order $\frac{p-1}{2}$ and $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the maximal totally real, tame extension of $\mathbb{Q}$ that is ramified only at p.*

Proof. It suffices to just prove the claim that $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the maximal totally real, tame extension of $\mathbb{Q}$ that is ramified only at p. In doing so, we need only consider Galois extensions; a non-Galois counterexample would provide a Galois

counterexample by taking the Galois closure. So, suppose for contradiction that the claim is false. Let K be a Galois extension of $\mathbb{Q}$ of minimal degree that contradicts it. By Corollary 2.1.2, $G = \mathrm{Gal}\,(K/\mathbb{Q})$ is non-solvable. Let e denote the ramification index of the primes above p. Since the extension is tame and $p \leq 53$, by Theorem 1.3.6 the root discriminant of $K/\mathbb{Q}$ is at most

$$p^{1+v_p(e)-\frac{1}{e}} = p^{1+0-\frac{1}{e}} = p^{1-\frac{1}{e}} \leq 53^{1-\frac{1}{e}} < 53.$$

By [7], any totally real extension of $\mathbb{Q}$ of degree 500 or larger has root discriminant bigger than 53. Hence, $[K : \mathbb{Q}] < 500$. By the minimality of $[K : \mathbb{Q}]$, every proper quotient of G must be solvable. By Corollary 2.1.2, every proper quotient is therefore abelian. By Lemma 2.5 in [10], we conclude that $e \leq 14$. Thus, the root discriminant is at most

$$53^{1-\frac{1}{14}} < 40.$$

By [7] again, we now get $[K : \mathbb{Q}] \leq 84$. The only non-solvable group of order at most 84 is A_5. Thus, $G \cong A_5$. Once more by Lemma 2.5 in [10], $e \leq 5$ and so the root discriminant is at most

$$53^{1-\frac{1}{5}} < 24.$$

Finally, [7] tells us that the root discriminant must be at least 36 for degree 60 totally real extensions of $\mathbb{Q}$. This is a contradiction. □

2.1.2 Extensions Ramified at a Small Prime

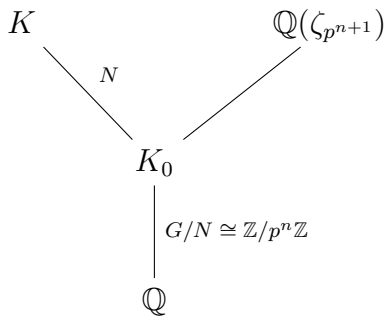
We now present some results about extensions of $\mathbb{Q}$ ramified at a single, small, integral prime. We begin by adapting a result of Hoelscher in [12] to more suitably apply to our needs.

Proposition 2.1.5. *Suppose $K/\mathbb{Q}$ is a nontrivial, solvable Galois extension ramified only at a single, odd finite prime p and possibly ∞. Let $G = \mathrm{Gal}\,(K/\mathbb{Q})$. Then, either G is a cyclic p-group, $G/p(G)$ is isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$, or G has a cyclic quotient of order p^t where $\mathbb{Q}(\zeta_{p^{t+1}})$ is the first p-power cyclotomic field with nontrivial class group.*

Proof. Let K and G satisfy the hypotheses above. Let $K_0/\mathbb{Q}$ be the maximal p-power, Galois sub-extension of $K/\mathbb{Q}$ and set $N = \mathrm{Gal}(K/K_0)$. By Theorem 2.11 in [10], N is cyclic. So,

$$\mathrm{Gal}\,(K_0/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z} \text{ for some } n.$$

Furthermore, by Kronecker-Weber, K_0 is the cyclic sub-extension of degree p^n in $\mathbb{Q}(\zeta_{p^{n+1}})$.



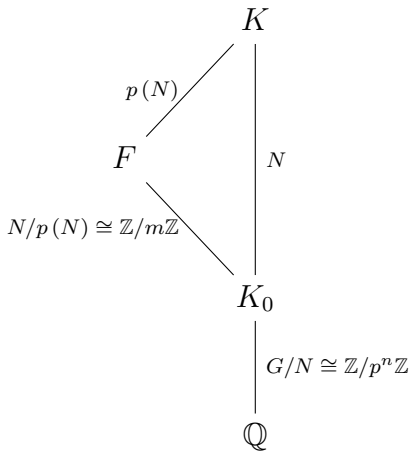
.

Suppose now that G is not a cyclic p-group and that $G/p(G)$ is not isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. We must show that $\mathbb{Q}(\zeta_{p^{n+1}})$ has nontrivial class group; this then shows that $n \geq t$, and so G has a cyclic quotient of order p^t. We first show that $N/p(N)$ is not isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$.

Suppose for contradiction that $N/p(N)$ is isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. Then,

$$N/p\,(N) \cong \mathbb{Z}/m\mathbb{Z} \text{ for some } m > 1 \text{ dividing } p-1.$$

Letting F denote the fixed field of K under $p(N)$, we obtain the following diagram:



.

Since N is normal in G and $p(N)$ is characteristic in N, $p(N)$ is also normal in G. Hence, $F/\mathbb{Q}$ is a Galois extension with

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G/p(N).$$

Because $m \mid p-1$ and $\gcd(p-1, p) = 1$, the Schur-Zassenhaus theorem tells us that

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G/p(N) \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^n\mathbb{Z}.$$

However, the automorphism group $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ has order $\phi(m)$ which is prime to p. Thus, there is no nontrivial homomorphism from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$. Hence, the above semidirect product is in fact a direct product. We conclude that

$$\mathrm{Gal}(F/\mathbb{Q}) \cong G/p(N) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}.$$

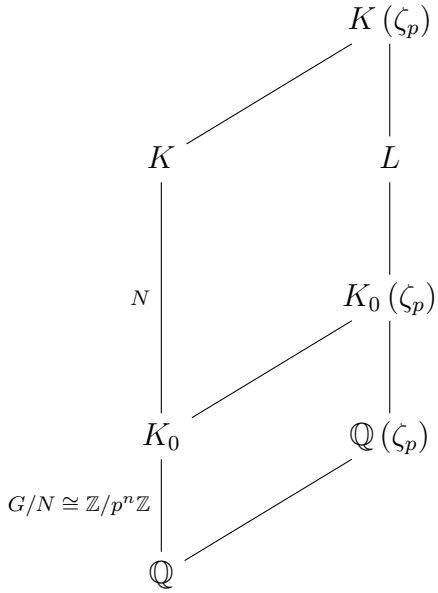
Noting that $p(G)/p(N) \cong p(G/p(N))$ and applying the third isomorphism theorem, we obtain

$$G/p(G) \cong (G/p(N))/(p(G)/p(N)) \cong (G/p(N))/p(G/p(N))$$

$$\cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z})/(\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

This contradicts our assumption that $G/p(G)$ is not isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. We conclude that $N/p(N)$ is not isomorphic to a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$.

By Theorem 1.1 and Lemma 1.4 of [12], there is a nontrivial, abelian, unramified sub-extension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p with L Galois over $\mathbb{Q}$:



.

Since $K_0 \leq \mathbb{Q}(\zeta_{p^{n+1}})$ and $[K_0 : \mathbb{Q}] = p^n$, it must be the case that $K_0(\zeta_p) = \mathbb{Q}(\zeta_{p^{n+1}})$.

Since L is a nontrivial, abelian, unramified extension of $\mathbb{Q}\left(\zeta_{p^{n+1}}\right)$, the class number of $\mathbb{Q}\left(\zeta_{p^{n+1}}\right)$ is not 1. $\square$

Corollary 2.1.6. *Let $p < 23$ be an odd prime and let $K/\mathbb{Q}$ be a nontrivial, solvable Galois extension ramified only at p and possibly ∞ with $G = \mathrm{Gal}(K/\mathbb{Q})$. One of the following holds:*

1. *$G/p(G)$ is a nontrivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$.*

2. *G has a cyclic quotient of order p.*

Proof. Apply Proposition 2.1.5 while noting that the p^{th} cyclotomic field has class number 1 for $p < 23$ a prime. $\square$

[10] obtains results about extensions in which the only finite prime that ramifies is 2, and then [12] obtains further results about extensions in which the only finite prime that ramifies is 3. For the remainder of this section, we focus on the special case in which the only finite prime that ramifies is 5.

Corollary 2.1.7. *Let G be the Galois group of a nontrivial, solvable extension ramified only at 5 and possibly ∞. One of the following holds:*

1. *G is a cyclic 5-group.*

2. *$G/p\left(G\right) \cong \mathbb{Z}/2\mathbb{Z}$.*

3. *$G/p\left(G\right) \cong \mathbb{Z}/4\mathbb{Z}$.*

4. G has a cyclic quotient of order 25.

Proof. The 125^{th} cyclotomic field is the first 5-power cyclotomic field with nontrivial class group. Apply Proposition 2.1.5. □

We conclude this section by dropping the solvable assumption and considering arbitrary extensions of $\mathbb{Q}$ in which only 5 and ∞ may ramify.

Proposition 2.1.8. *If $K/\mathbb{Q}$ is a nontrivial, Galois extension ramified only at 5 and possibly ∞ with Galois group G, then one of the following holds:*

1. $G \cong \mathbb{Z}/5\mathbb{Z}$.
2. $G/p(G) \cong \mathbb{Z}/4\mathbb{Z}$.
3. $G/p(G) \cong \mathbb{Z}/2\mathbb{Z}$.
4. $e \equiv 0 \pmod 5$ *and* $e \geq 10$ *, where e is the ramification index of the primes above 5.*

Proof. If G is solvable, then one of the conditions in Corollary 2.1.7 holds. If the second or third condition holds, then we are done. If the fourth condition holds, then, by Kronecker-Weber, the cyclic quotient of order 25 produces a totally ramified sub-extension. So, $25 \mid e$. Finally, if the first condition holds, either $G \cong \mathbb{Z}/5\mathbb{Z}$ and we are done, or $G \cong \mathbb{Z}/5^l\mathbb{Z}$ for some $l \geq 2$. Again by Kronecker-Weber, the $\mathbb{Z}/5^l\mathbb{Z}$ extension is totally ramified, and, since $25 \mid 5^l$, we get $25 \mid e$.

Suppose now that G is not solvable. Then, by the proposition in [12], $|G| > 300$. Let $n = |G|$ be the degree of the corresponding extension and let Δ be the discriminant. By [7], we know that $|\Delta|^{\frac{1}{n}} \geq 19.2$ since the degree of the extension is at least 300. But, since only 5 is ramified, we have from Theorem 1.3.6 that $|\Delta|^{\frac{1}{n}} \leq 5^{1+v_5(e)-\frac{1}{e}}$. Thus,

$$19.2 \leq 5^{1+v_5(e)-\frac{1}{e}}.$$

$v_5(e) \neq 0$ for otherwise the right hand side above is at most 5. So, $e \equiv 0 \pmod 5$. If $v_5(e) = 1$ then e still cannot be 5; if it were, the right hand side above is at most 18.12. Thus, $e \geq 10$. □

Remark 2.1.9. The fourth condition in Proposition 2.1.8 can be replaced by $25 \mid e$ if one is willing to assume the generalized Riemann hypothesis. The proof showed that in the solvable case we can unconditionally replace the fourth condition with $25 \mid e$. By Theorem 2.1.10, if G is non-solvable we actually have $|G| \geq 660$. Under assumption of the generalized Riemann hypothesis, we have from Table 1 in [22] that the Odlyzko lower bound on the root discriminant for fields of degree at least 340 is 25.09. This forces $v_5(e) \geq 2$ and so $25 \mid e$. Furthermore, for a totally real extension of degree at least 300 we get that the root discriminant is at least 50 by [7], and so we can unconditionally replace the fourth condition with $25 \mid e$ in the totally real case. Also note that by Table 2 in [22], once the extension has degree 10^7 or more, the root discriminant is at least 22.3 and so we must have that $e \geq 15$ in this scenario since the inequality $19.2 \leq 5^{1+v_5(e)-\frac{1}{e}}$ becomes $22.3 \leq 5^{1+v_5(e)-\frac{1}{e}}$.

2.1.3 Non-solvable Extensions

Harbater showed in [10] that if $G \in \pi_A(U_2)$ and $|G| \leq 300$, then G is solvable. In [12], Hoelscher strengthened this result and proved that if $2 \leq p < 23$ is prime and $G \in \pi_A(U_p)$ with $|G| \leq 300$, then G is solvable. In this section we further improve upon this result and obtain the following:

Theorem 2.1.10. *If $2 \leq p < 37$ is a prime number and $G \in \pi_A(U_p)$ with $|G| < 660$, then G is solvable.*

To prove this, we will first extend Hoelscher's result to hold for any prime $p < 37$. We will then systematically rule out the remaining non-solvable groups of order less than 660 from being elements of $\pi_A(U_p)$ for all primes $p < 37$.

Example 2.1.11. Theorem 4.1 in [14] shows that if $p < 37$, then $S_5 \notin \pi_A(U_p)$ and $A_5 \notin \pi_A(U_p)$.

We now show that $\mathrm{PSL}(2,7) \notin \pi_A(U_p)$ for $23 \leq p < 37$. Suppose for contradiction there is an extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}(2,7)$ such that $23 \leq p < 37$ is the only ramified finite prime. This group has order $168 = 2^3 \cdot 3 \cdot 7$. Hence, the ramification in $K/\mathbb{Q}$ must be tame as $p \nmid 168$. Thus, the inertia group for any prime lying over p must be cyclic. $\mathrm{PSL}(2,7)$ has cyclic subgroups of orders $1, 2, 3, 4$, and 7. Thus, the corresponding ramification indices satisfy $e \leq 7$ and the root discriminant satisfies

$$|\Delta|^{\frac{1}{168}} \leq p^{1+v_p(e)-\frac{1}{e}}.$$

By [7], we know that $|\Delta|^{\frac{1}{168}} \geq 17.95$. Thus,

$$17.95 \leq p^{1+v_p(e)-\frac{1}{e}} \leq p^{1+0-\frac{1}{7}} = p^{\frac{6}{7}}.$$

Hence,

$$p \geq 17.95^{\frac{7}{6}} > 29,$$

and so $p = 31$.

If $e \neq 7$, then $e \leq 4$. But then the root discriminant is at most $31^{1+0-\frac{1}{4}} < 17.95$ which is a contradiction. So, $e = 7$. Because the ramification is tame, the inertia group for any prime embeds into the multiplicative group of the residue field. Letting f denote the residue degree, we have $31^f \equiv 1 \pmod{e}$. Furthermore, if r is the number of primes that p splits into, we know $ref = 168$ and so $rf = \frac{168}{e} = \frac{168}{7} = 24$. From $31^f \equiv 1 \pmod{e}$ and $f \mid 24$ we conclude that $f \in \{6, 12, 24\}$. Note now that ef is equal to the order of the decomposition group which is a subgroup of $\mathrm{PSL}(2, 7)$. Since $\mathrm{PSL}(2, 7)$ has neither a subgroup of order 42 nor a subgroup of order 84, we conclude that $f = 24$ and that the decomposition group has order 168. This means that the decomposition group is all of $\mathrm{PSL}(2, 7)$. This is a contradiction because the decomposition group must be solvable, whereas $\mathrm{PSL}(2, 7)$ is not.

We can now extend Hoelscher's result to include all primes less than 37:

Proposition 2.1.12. *If $2 \leq p < 37$ is a prime number and $G \in \pi_A(U_p)$ and $|G| \leq 300$, then G is solvable.*

Proof. We already know by the proposition in [12] that the above statement holds for $2 \leq p < 23$. An analogous proof now works for $23 \leq p < 37$. That is, suppose for contradiction that $23 \leq p < 37$ and that there is a non-solvable $G \in \pi_A(U_p)$ with $|G| \leq 300$. Let G be such a group with smallest possible order. If N is any nontrivial, normal subgroup of G, then G/N is also in $\pi_A(U_p)$. Since G/N has smaller order than G, the minimality assumption on G implies that G/N is solvable. Since G itself is not solvable, N cannot be solvable. Thus, $|N| \geq 60$ and so $|G/N| \leq 5$ and G/N is abelian. By Lemma 2.5 in [10], G is isomorphic to one of S_5, A_5, or $\mathrm{PSL}(2,7)$. This is impossible by Example 2.1.11 and yields the desired contradiction. □

The following examples now examine the remaining possible non-solvable groups of order less than 660, and demonstrate that none of them appear in $\pi_A(U_p)$ for $p < 37$.

Example 2.1.13. After 300, the next non-solvable groups have order 336. There are three such groups. Two of them have a normal subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. For each of them, the quotient by this group is a non-solvable group of order 168. Since Proposition 2.1.12 says there are no non-solvable groups of order 168 in $\pi_A(U_p)$ for $p < 37$, neither of these two groups can be in $\pi_A(U_p)$ for $p < 37$.

The third group is isomorphic to $\mathrm{PGL}(2,7)$. Suppose there is a $K/\mathbb{Q}$ which realizes $\mathrm{PGL}(2,7)$ in $\pi_A(U_p)$. $\mathrm{PGL}(2,7)$ has a subgroup of order 42. The fixed field for this subgroup would yield a non-Galois, degree 8 extension of $\mathbb{Q}$. Since

the normal subgroups in $\mathrm{PGL}(2,7)$ have indices $1, 2$, and 336, the Galois closure of the degree 8 sub-extension must be all of K. Thus, the largest power of 2 dividing the Galois closure is $2^4 = 16$. By Corollary 2.3 in [13], $p \neq 2$. If p were 3, the root discriminant would be at most $3^{1+v_3(e)-\frac{1}{e}} \leq 3^{1+1-0} = 9$; but by [7], the root discriminant is at least 19.47. By Theorem 4.1 in [16], $p \neq 7$.

Primes larger than 7 do not divide 336, and so the extension must be tamely ramified. Therefore, the inertia group corresponding to any prime is cyclic. The cyclic subgroups of $\mathrm{PGL}(2,7)$ have orders $1, 2, 3, 4, 6, 7$, and 8. Thus, the ramification indices satisfy $e \leq 8$. This means the root discriminant is at most $p^{1+v_p(e)-\frac{1}{e}} \leq p^{1+0-\frac{1}{8}} = p^{\frac{7}{8}}$. Since it is also at least 19.47, we get $p \geq 19.47^{\frac{8}{7}} > 29$.

Lastly, we consider $p = 31$. If $e \leq 7$, then the root discriminant is not large enough; so, $e = 8$. The polynomial $x^6+2x^5+94x^4+126x^3+2947x^2+1736x+30691$ generates an S_3-extension of $\mathbb{Q}$ in which 31 is the only finite prime that ramifies; it is the Hilbert class field of $\mathbb{Q}(\sqrt{-31})$. Call this extension $H_{\mathbb{Q}(\sqrt{-31})}$. Since $\mathrm{PGL}(2,7)$ has no index 6 normal subgroup, $K \cap H_{\mathbb{Q}(\sqrt{-31})} \neq H_{\mathbb{Q}(\sqrt{-31})}$. Thus, $K \cap H_{\mathbb{Q}(\sqrt{-31})} = \mathbb{Q}(\sqrt{-31})$. So,

$$[KH_{\mathbb{Q}(\sqrt{-31})} : \mathbb{Q}] = \frac{336 \cdot 6}{2} = 1008.$$

$\mathrm{Gal}\left(KH_{\mathbb{Q}(\sqrt{-31})}/\mathbb{Q}\right)$ is a subgroup of $\mathrm{PGL}(2,7) \times S_3$. Suppose (g,h) is an element of this Galois group that generates an inertia group for some prime over 31. Then, under the quotient maps, g maps to an element of some inertia group in $\mathrm{PGL}(2,7)$ and h maps to an element of some inertia group in S_3. Since these inertia groups

have order 8 and 2 respectively, we get that the order of (g, h) is at most 8. Thus, the ramification indices for $KH_{\mathbb{Q}(\sqrt{-31})}/\mathbb{Q}$ are at most 8. This means that the root discriminant is at most $31^{\frac{7}{8}} < 20.2$. However, by [7], the root discriminant is at least 20.9 for degree 1008 extensions. So, $\mathrm{PGL}(2, 7) \notin \pi_A(U_{31})$.

Example 2.1.14. The next possible order of a non-solvable group is 360. There are 6 such groups. Five of them have a normal subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. In each case, the quotient group is non-solvable of order 120. But, by Proposition 2.1.12, there are no non-solvable groups of order 120 in $\pi_A(U_p)$ for $2 \leq p < 37$.

The last remaining group is A_6. By Theorem 4.2 in [14], $A_6 \notin \pi_A(U_p)$ for $2 \leq p < 37$.

Example 2.1.15. The next candidate non-solvable group has order 420. There is one non-solvable group of order 420. It has a normal subgroup isomorphic to $\mathbb{Z}/7\mathbb{Z}$. The quotient yields a non-solvable group of order 60. But, Proposition 2.1.12 tells us there is no non-solvable group of order 60 in $\pi_A(U_p)$ for $2 \leq p < 37$, and so the same is true of the non-solvable group of order 420.

Example 2.1.16. There are 26 non-solvable groups of order 480. Each of them has a normal subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In each case, the quotient group is non-solvable of order 240. Applying Proposition 2.1.12 now tells us that no such group appears in $\pi_A(U_p)$ for $2 \leq p < 37$.

Example 2.1.17. There are two non-solvable groups of order 504. One has a normal subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. The quotient group is non-solvable of order

168, and so the group cannot appear in $\pi_A(U_p)$ for $2 \leq p < 37$ by Proposition 2.1.12.

The other group is the simple group $\mathrm{PSL}(2,8)$. Suppose $K \in \pi_A(U_p)$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}(2,8)$. $\mathrm{PSL}(2,8)$ has a subgroup of order 56, and the fixed field would yield a degree 9 sub-extension of $\mathbb{Q}$. Because $\mathrm{PSL}(2,8)$ is simple, the Galois closure of this subfield is K. Corollary 4.2 in [17] now tells us that $p \geq 11$. Since 7 is the largest prime dividing 504, the ramification is tame and so the inertia groups are cyclic. The largest size of a cyclic subgroup is 9, and so the ramification indices satisfy $e \leq 9$. The root discriminant is at most $p^{1+v_p(e)-\frac{1}{e}} \leq p^{\frac{8}{9}}$. By [7], the root discriminant is at least 20.114. Thus, $p^{\frac{8}{9}} \geq 20.114$ and so $p > 29$.

We now consider $p = 31$. If $e \neq 9$, then $e \leq 7$ and the root discriminant is not large enough; thus, $e = 9$. Since ef is the order of the decomposition groups, it must also be the order of some subgroup of $\mathrm{PSL}(2,8)$. Examining the possible orders of subgroups of $\mathrm{PSL}(2,8)$, we get that $f \in \{1, 2, 56\}$. If $f = 56$, the decomposition groups are all of $\mathrm{PSL}(2,8)$, which is impossible since the decomposition groups must be solvable. Thus, $f = 2$. But, the inertia groups embed into the multiplicative groups of the residue fields, and so $31^f \equiv 1 \pmod{e}$. That is, $31 \equiv 1 \pmod{9}$ or $31^2 \equiv 1 \pmod{9}$. This is a contradiction, and so $\mathrm{PSL}(2,8) \notin \pi_A(U_{31})$.

Example 2.1.18. There are two non-solvable groups of order 540. Both have a normal subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$. The quotient in both cases is a non-solvable group of order 180. Proposition 2.1.12 now rules out either of these groups from

appearing in $\pi_A(U_p)$ for $2 \leq p < 37$.

Example 2.1.19. There are five non-solvable groups of order 600. Each has a normal subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$. The quotients are non-solvable of order 120. Proposition 2.1.12 shows that none of these groups appear in $\pi_A(U_p)$ for $2 \leq p < 37$.

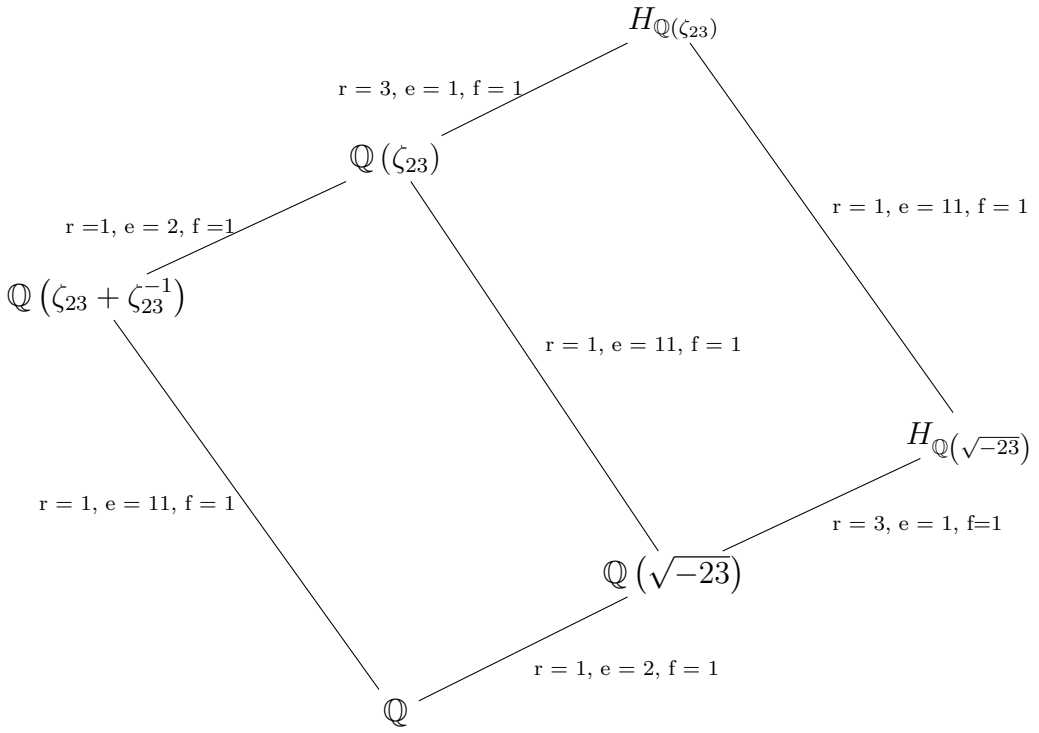
We conclude by remarking that 2.1.12, 2.1.13, 2.1.14, 2.1.15, 2.1.16, 2.1.17, 2.1.18, and 2.1.19, along with the fact that the next smallest non-solvable group has order 660, provide a proof for Theorem 2.1.10 stated at the beginning of this section.

2.1.4 Miscellaneous Examples

We now provide some more examples of certain groups that can and cannot appear in $\pi_A(U_n)$ for various choices of n.

Example 2.1.20. In Theorem 2.6 in [10], Harbater shows that for $p < 23, \pi_1^t(U_p)$ is cyclic of order $p-1$. He then shows that $\pi_1^t(U_{23})$ is not cyclic by examining the Hilbert class field of $\mathbb{Q}(\zeta_{23})$. So, 23 is the first prime number for which there exists a tame, non-cyclic Galois extension of $\mathbb{Q}$ in which that is the only finite prime that ramifies. However, there is also a smaller, tame S_3-extension of $\mathbb{Q}$ in which 23 is the only finite ramified prime. It is $H_{\mathbb{Q}(\sqrt{-23})}$, the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$. Letting $H_{\mathbb{Q}(\zeta_{23})}$ denote the Hilbert class field of $\mathbb{Q}(\zeta_{23})$, and e, f, and r denote ramification indices, residue degrees, and the number of primes a given prime splits into,

we get the following diagram:



.

A generating polynomial for $H_{\mathbb{Q}(\sqrt{-23})}/\mathbb{Q}$ is $x^6 - 3x^5 + 5x^4 - 5x^3 + 5x^2 - 3x + 1$.

The Boston-Markin conjecture suggests that each S_n and A_n should appear as the Galois group of an extension of $\mathbb{Q}$ in which only a single finite prime ramifies. We provide examples verifying the validity of this for some small n.

Example 2.1.21. The following table gives polynomials for which the splitting field is an S_n-extension of $\mathbb{Q}$ ramified at only one finite prime. Each is a polynomial of the form $x^n + ax^k + b$. The formula for the discriminant of this polynomial, not necessarily equal to the discriminant of an integral basis for the splitting field, was evaluated in Sage for various choices of n, k, a, and b with n and k coprime;

it was then examined to determine if it is divisible by only a single prime. The Galois group of the polynomial was then calculated in Magma to ensure it is the symmetric group.

Group	Polynomial	Prime Discriminant of Polynomial
S_2	x^2+x+1	-3
S_3	x^3+x+1	-31
S_4	x^4+x+1	229
S_5	x^5+x+3	253381
S_6	x^6+x+2	-1489867
S_7	x^7+x+5	-12867906031
S_8	x^8+x+8	35184371265289
S_9	x^9+5x+7	2266170022407689
S_{10}	$x^{10}+x+5$	-19531249612579511
S_{11}	$x^{11}+x+9$	-994820282519684939011
S_{12}	$x^{12}+x+3$	1579460160795535021
S_{13}	$x^{13}+3x+7$	4192195551520877139504541
S_{14}	$x^{14}+x+15$	$-216261328834767242371248934077 47$
S_{15}	$x^{15}+x+5$	$-26726922020427244030657923 91$
S_{16}	$x^{16}+x+2$	60446247191342420649371 3
S_{17}	$x^{17}+4x+15$	54336518486732469395422431439837949419 69
S_{18}	$x^{18}+7x+5$	13170703641353119003009627352771854 73
S_{19}	$x^{19}+5x+19$	$-20600759652196488327169355385743583989034909$ 4339
S_{20}	$x^{20}+9x+5$	$-24050964311140697418472492072854195764819179$
S_{21}	$x^{21}+17x+11$	72487449698637167195591949206414496100432754857 97621
S_{22}	$x^{22}+7x+8$	$-31262728669811611065470364315685876809464412$ 11243
S_{23}	$x^{23}+7x+9$	$-20571821763536694126790714014166957272330432$ 031886839
S_{24}	$x^{24}+5x+1$	$-12445728778748446499098430732220758644866423$ 90599
S_{25}	$x^{25}+7x+5$	17939251531773958204308768278139376689671443 93 557092857
S_{26}	$x^{26}+x^3+1$	$-615555580757116141717174670251161846 7$
S_{27}	$x^{27}-13x^7-1$	10298090536992665373698476272256737764641565 17 50369380850107197
S_{28}	$x^{28}-3x+10$	33145523113253364718396987685185577022071582 82 327648940441764445431 7
S_{29}	$x^{29}+3x-5$	95653765433454281336475157294578742764728557 92 5108094289378013
S_{30}	$x^{30}+13x^{23}+1$	45053348824321236991609111300883360581426126 25 28020163613845293867381 69

Table 1: S_n-extensions of $\mathbb{Q}$ Ramified at a Single Finite Prime

Example 2.1.22. The splitting fields of the following polynomials are Galois extensions of $\mathbb{Q}$ ramified at only one finite prime with Galois groups A_7, A_8, A_9, and A_{10}.

1. Group: A_7.

   Polynomial: $x^7 - 2x^6 - 5x^5 - x^4 - 3x^3 - x^2 - x - 5$.

   Discriminant of polynomial (factored): 554293^2.

2. Group: A_8.

   Polynomial: $x^8 - 4x^7 + 4x^6 + 4x^5 - 5x^4 - 4x^3 + 2x^2 + 3x + 1$.

   Discriminant of polynomial (factored): 5869^2.

3. Group: A_9.

   Polynomial: $x^9 - x^8 - 3x^7 + 3x^6 + 3x^5 - x^4 + 3x^3 + 4x^2 + x - 2$.

   Discriminant of polynomial (factored): 7089461^2.

4. Group: A_{10}.

   Polynomial: $x^{10} + 2x^9 + x^8 - 4x^7 - 2x^6 + 2x^5 - 2x^4 - 4x^3 + x^2 + 3x + 1$.

   Discriminant of polynomial (factored): 388099^2.

Remark 2.1.23. Unlike in Theorem 1.4.6, the above primes are not necessarily the smallest primes for which S_n or A_n is in $\pi_A(U_p)$.

Theorem 2.1.11 in [11] shows that if G is a length 2 solvable group and $K/\mathbb{Q}$ is a tame extension ramified only at a single finite prime p with $\mathrm{Gal}(K/\mathbb{Q}) = G$, then

K is contained in the Hilbert class field of $\mathbb{Q}(\zeta_p)$. The following example shows that this trend does not continue.

Example 2.1.24. The splitting field of $x^{24} - 6x^{22} + x^{20} + 91x^{18} + 118x^{16} - 157x^{14} - 360x^{12} + 17x^{10} + 312x^8 + 253x^6 + 95x^4 + 17x^2 + 1$ is a tame extension of $\mathbb{Q}$ in which 59 is the only finite ramified prime. Its Galois group is a length 3 solvable group. It is not in Hilbert class field tower of $\mathbb{Q}(\zeta_p)$. This is because the ramification indices are 4, which does not divide the ramification indices of $\mathbb{Q}(\zeta_p)$, which are 58.

2.2 Extensions Ramified at Arbitrary Sets of Primes

We now explore the situation in which more than a single finite prime is allowed to ramify.

Proposition 2.2.1. *Let $m \in \mathbb{N}_{>1}$ be a natural number and let $n \in \mathbb{N}_{>1}$ be a square-free natural number.*

1. *If* $\gcd\left(m, \prod_{p|n} p - 1\right) = 1$, *then no groups of order m are in $\pi_A^t(U_n)$.*
2. *If* $\gcd\left(m, \prod_{p|n} p(p-1)\right) = 1$, *then no groups of order m are in $\pi_A(U_n)$.*

Proof. Because of root discriminant bounds, there are no tame extensions of $\mathbb{Q}$ in which 2 is the only finite prime that ramifies; so, both statements above hold when $n = 2$.

Now let n have at least one odd prime factor. Suppose for contradiction that $G \in \pi_A^t(U_n)$ is a group of order m satisfying the hypothesis of 1. Because we have $\gcd\left(m, \prod_{p|n} p - 1\right) = 1$, we get that m is odd. By Feit-Thompson, G is solvable. So, G has a nontrivial, abelian quotient, A. Since $G \in \pi_A^t(U_n)$, we also have that $A \in \pi_A^t(U_n)$. By Kronecker-Weber, A is the Galois group of a sub-extension of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, and so the order of A divides $\prod_{p|n} p - 1$. Since also $|A| \mid |G| = m$, this contradicts $\gcd\left(m, \prod_{p|n} p - 1\right) = 1$.

Suppose now that $G \in \pi_A(U_n)$ is a group of order m satisfying the hypothesis of 2. Again, m must be odd and an application of Feit-Thompson yields a nontrivial, abelian quotient, A. Kronecker-Weber tells us that A is the Galois group of a sub-extension of $\mathbb{Q}(\zeta_{n^{t+1}})/\mathbb{Q}$ for some $t \in \mathbb{N}$. Thus, the order of A divides $\prod_{p|n} p^t(p-1)$. Since also $|A| \mid |G| = m$, this contradicts $\gcd\left(m, \prod_{p|n} p(p-1)\right) = 1$. □

Example 2.2.2. A Fermat prime is a prime number of the form $2^k + 1$ for some $k \in \mathbb{N}$. As a consequence of Proposition 2.2.1, no group of odd order can be the Galois group of a tame extension of $\mathbb{Q}$ in which only Fermat primes ramify.

We now show that if $n_1 \neq n_2$, then $\pi_A(U_{n_1}) \neq \pi_A(U_{n_2})$.

Proposition 2.2.3. *Let $n \in \mathbb{N}$ be square-free. Then, $\pi_A(U_n)$ determines n.*

Proof. We show that $p \mid n$ if and only if $\forall m \in \mathbb{N}, \mathbb{Z}/p^m\mathbb{Z} \in \pi_A(U_n)$. This then shows that $\pi_A(U_n)$ determines the prime factors of n, which then determines n since n is square-free.

So suppose $p \mid n$. Then, $\forall m \in \mathbb{N}, \mathbb{Q}(\zeta_{p^{m+1}})$ has a sub-extension $K_m/\mathbb{Q}$ with $\mathrm{Gal}(K_m/\mathbb{Q}) \cong \mathbb{Z}/p^m\mathbb{Z}$. Since $K_m \leq \mathbb{Q}(\zeta_{p^{m+1}})$, the only finite prime that ramifies in $K_m/\mathbb{Q}$ is p. Hence, $\mathbb{Z}/p^m\mathbb{Z} \in \pi_A(U_n)$.

Now suppose that $\forall m \in \mathbb{N}, \mathbb{Z}/p^m\mathbb{Z} \in \pi_A(U_n)$. Write the prime factorization of n as $n = q_1 \dots q_k$ where each q_i is prime. Our goal is to show that one of the q_i is really p. By Kronecker-Weber, each $\mathbb{Z}/p^m\mathbb{Z}$-extension is contained in some cyclotomic field. So, $\forall m \in \mathbb{N}, \exists t_m \in \mathbb{N}$ such that the extension providing witness to the fact that $\mathbb{Z}/p^m\mathbb{Z} \in \pi_A(U_n)$ is a sub-extension of $\mathbb{Q}(\zeta_{t_m})/\mathbb{Q}$. Furthermore, since only primes dividing n may ramify, t_m may be chosen so that its set of prime factors is contained in $\{q_1, \dots q_k\}$. That is, $t_m = q_1^{e_{m,1}} \dots q_k^{e_{m,k}}$ where each $e_{m,i}$ is a nonnegative integer. Notice now that p^m divides $\phi(t_m) = [\mathbb{Q}(\zeta_{t_m}) : \mathbb{Q}]$ since $\mathbb{Q}(\zeta_{t_m})/\mathbb{Q}$ has a sub-extension with Galois group isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$. However, $\phi(t_m) = q_1^{e_{m,1}-1}(q_1 - 1) \dots q_k^{e_{m,k}-1}(q_k - 1)$. If p were not equal to one of the q_i, the maximal power of p dividing $\phi(t_m)$ would be the maximal power of p dividing $(q_1 - 1) \dots (q_k - 1)$. This expression is independent of m, and so we may choose an $m \in \mathbb{N}$ large enough so that p^m does not divide it. Hence, p must equal one of the q_i. □

The following shows that if we only consider tame extensions, we can no longer recover n from $\pi_A^t(U_n)$.

Proposition 2.2.4. $\pi_A^t(U_6) = \pi_A^t(U_2) \cup \pi_A^t(U_3) = \pi_A^t(U_3)$ *and* $\pi_A^t(U_{10}) = \pi_A^t(U_2) \cup \pi_A^t(U_5) = \pi_A^t(U_5)$

Proof. First note that $\pi_A^t(U_2)$ consists only of the trivial group and so the final equality in both assertions holds.

Now consider $\pi_A^t(U_6)$. Any extension tamely ramified only at 2 and 3 has root discriminant at most 6. By [7], the degree of the extension is therefore at most 9. So, let $G \in \pi_A^t(U_6)$. We will show it is in $\pi_A^t(U_3)$. Suppose not. Then 2 must be ramified in the extension that realizes G. Since the extension is tame, its degree is not a power of 2. Since $\pi_A^t(U_2)$ contains only the trivial group, 3 must also be ramified. Since 3 is tamely ramified, the degree is not 3 or 9. This leaves $5, 6,$ and 7 as possibilities for the degree. Any group of order 5 or 7 is cyclic, and by Kronecker-Weber neither $\mathbb{Z}/5\mathbb{Z}$ nor $\mathbb{Z}/7\mathbb{Z}$ is in $\pi_A^t(U_6)$. Hence the degree is 6 and G is $\mathbb{Z}/6\mathbb{Z}$ or S_3. Again by Kronecker-Weber, G is not $\mathbb{Z}/6\mathbb{Z}$. Thus, G is S_3. S_3 has A_3 as an index 2 subgroup. The fixed field for A_3 would be a quadratic extension of $\mathbb{Q}$. Since it is tamely ramified only at $2, 3$ and possibly ∞, it must be $\mathbb{Q}(\sqrt{-3})$. The S_3-extension of $\mathbb{Q}$ is degree 3 over $\mathbb{Q}(\sqrt{-3})$ so is abelian over it. It is tamely ramified, so only 2 can be ramified (∞ cannot ramify as $\mathbb{Q}(\sqrt{-3})$ is totally imaginary already). So, the extension is in the ray class field for the modulus (2). But the ray class number for the modulus (2) for $\mathbb{Q}(\sqrt{-3})$ is 1, and so there is no degree 3 abelian extension ramified only at 2. This is a contradiction. Thus $\pi_A^t(U_6) = \pi_A^t(U_2) \cup \pi_A^t(U_3) = \pi_A^t(U_3)$. Note also that even the set of number fields tamely ramified only at 2 and 3 is just the set of number fields tamely ramified only at 3.

Now consider $\pi_A^t(U_{10})$. We show that any $G \in \pi_A^t(U_{10})$ is in $\pi_A^t(U_5)$. Suppose not and consider an extension realizing such a G. By [7], the degree of any extension in which 2 and 5 are the only finite primes that may ramify is at most 21. Note also that if the extension is of odd degree, it is totally real and so again by [7], the degree is at most 7. Also, as above, any such extension cannot have degree a power of 2 or 5. This leaves $3, 6, 7, 10, 12, 14, 18, 20$ as possibilities. Since groups of order 3 and 7 are cyclic, they are ruled out by Kronecker-Weber. We now consider degrees $6, 10, 12, 14, 18, 20$. As above, a degree 6 extension cannot be $\mathbb{Z}/6\mathbb{Z}$ so is S_3. As above, it would have $\mathbb{Q}(\sqrt{5})$ as a subfield. The degree 3 abelian extension would be in the ray class group for the modulus $(2)(5) = (10)$ (we do not need to worry about ∞ since that only adds powers of 2 to the order of the ray class group which is irrelevant for a degree 3 extension). But the ray class number for (10) is 1. For degree 10, it cannot be $\mathbb{Z}/10\mathbb{Z}$ by Kronecker-Weber. This leaves only D_{10}. This has the rotations as an index 2 subgroup, so has $\mathbb{Q}(\sqrt{5})$ as a subfield. The whole extension would be degree 5 over $\mathbb{Q}(\sqrt{5})$, but above we mentioned that the ray class group for (10) has order 1, so this does not happen. For degree 12, the ramification indices for primes above 2 are at most 3 and for primes above 5 are at most 12 on account of the extension being tame. The discriminant is therefore at most $2^{12-4} \cdot 5^{12-1}$, and so the root discriminant is less than 7. This is impossible by [7]. For degree 14, Kronecker-Weber prohibits $\mathbb{Z}/14\mathbb{Z}$ and the only other group is D_{14}. The same argument as for D_{10} rules out D_{14}. For degree 18, the ramification

indices for primes above 2 are at most 9 and for primes above 5 are at most 18. The discriminant is at most $2^{18-2} \cdot 5^{18-1}$, and so the root discriminant is less than 8.5. This is impossible by [7]. Finally, for degree 20, the ramification indices for primes above 2 are at most 5 and for primes above 5 are at most 20. The discriminant is at most $2^{20-4} \cdot 5^{20-1}$, and so the root discriminant is less than 8.5. This is impossible by [7]. Thus $\pi_A^t(U_{10}) = \pi_A^t(U_2) \cup \pi_A^t(U_5) = \pi_A^t(U_5)$. Note also that even the set of number field tamely ramified only at 2 and 5 is just the set of number fields tamely ramified only at 5. □

Example 2.2.5. $\pi_A^t(U_{22}) \neq \pi_A^t(U_2) \cup \pi_A^t(U_{11})$. To see this, note that $S_3 \notin \pi_A^t(U_2) \cup \pi_A^t(U_{11})$. However, the polynomial $x^6 - x^5 + 2x^4 - 3x^3 + 2x^2 - x + 1$ generates a tame S_3-extension of $\mathbb{Q}$ ramified only at 2 and 11; the ramification indices for the primes above 2 are 3 and for those above 11 are 2. Thus, $S_3 \in \pi_A^t(U_{22})$.

We now restrict out attention to tame, solvable extensions. In particular, we produce a bound on the maximal degree of a tame extension with length i solvable Galois group unramified outside of a predetermined set of primes. In what follows we will use the multichoose notation: $\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k}$.

Proposition 2.2.6. *Let n be a square-free natural number. Let $d_1 = \max\{3, \phi(n)\}$ and for $i \geq 1$,*

$$d_{i+1} = d_i \cdot \left\| \begin{array}{c} \left\lceil 6n^{\frac{d_i-1}{2}} \right\rceil \\ \\ \left\lceil \log_2(n^{\frac{d_i-1}{2}}) \right\rceil \end{array} \right\| \cdot (2n)^{d_i}.$$

If $G \in \pi_A^t(U_n)$ is a length i solvable group, then $|G| \leq n_i$.

Proof. $\pi_A^t(U_2)$ is trivial and so we will assume that $n \geq 3$. Notice also that for all i, we have $d_i \geq 3$. We proceed by induction on i. The base case of $i = 1$ corresponds to abelian extensions, and the maximal tame, abelian extension unramified outside of primes dividing n and ∞ is $\mathbb{Q}(\zeta_n)$, which has degree $d_1 = \phi(n)$.

Now, any tame extension with length $i+1$ solvable Galois group is in a ray class field for a tame extension with length i solvable Galois group. We first use Minkowski's bound to estimate the ideal class group of a tame, length i solvable extension. By the induction hypothesis, its degree is at most d_i. Since it is tame, the absolute value of the discriminant is at most n^{d_i-1}. Thus, the Minkowski bound is

$$n^{\frac{d_i-1}{2}} \cdot \left(\frac{4}{\pi}\right)^{\frac{d_i}{2}} \cdot \left(\frac{d_i!}{d_i^{d_i}}\right).$$

By [28], this is bounded above by

$$n^{\frac{d_i-1}{2}} \cdot \left(\frac{4}{\pi}\right)^{\frac{d_i}{2}} \cdot \left(\frac{1}{d_i^{d_i}}\right) \cdot \sqrt{2\pi d_i} \cdot d_i^{d_i} \cdot e^{-d_i} \cdot e^{\frac{1}{12d_i}} = n^{\frac{d_i-1}{2}} \cdot \left(\frac{4}{e\pi}\right)^{\frac{d_i}{2}} \cdot \left(\frac{1}{e^{\frac{d_i}{2}}}\right) \cdot \sqrt{2\pi d_i} \cdot e^{\frac{1}{12d_i}}.$$

Since $d_i > 1$, we have

$$\left(\frac{4}{e\pi}\right)^{\frac{d_i}{2}} \cdot \left(\frac{1}{e^{\frac{d_i}{2}}}\right) \cdot \sqrt{2\pi d_i} \cdot e^{\frac{1}{12d_i}} < 1,$$

and so the Minkowski bound is bounded above by

$$n^{\frac{d_i-1}{2}}.$$

Any prime ideal has norm at least 2. Thus, the product of $\log_2(n^{\frac{d_i-1}{2}})$ many prime ideals has norm at least $n^{\frac{d_i-1}{2}}$, and so is equivalent to an ideal of smaller norm in the ideal class group. Hence, every element in the ideal class group is expressible as a product of at most $\log_2(n^{\frac{d_i-1}{2}})$ many prime ideals, each with norm at most $n^{\frac{d_i-1}{2}}$. By [29], the prime counting function satisfies $\pi(x) < 1.3 \cdot \frac{x}{\log(x)}$, and so the number of integral primes less than $n^{\frac{d_i-1}{2}}$ is at most

$$1.3 \cdot \frac{n^{\frac{d_i-1}{2}}}{\frac{d_i-1}{2}\log(n)}.$$

Since each integral prime has at most d_i prime ideals lying above it, noting that $\frac{d_i}{(d_i-1)\log(n)} < 2$ for $n \geq 3$ and $d_i \geq 2$, this gives at most

$$1.3 \cdot \frac{n^{\frac{d_i-1}{2}}}{\frac{d_i-1}{2}\log(n)} \cdot d_i < 5.2 \cdot n^{\frac{d_i-1}{2}}$$

many prime ideals. We can count all products of at most $\log_2(n^{\frac{d_i-1}{2}})$ many prime ideals using multichoose. Since we can also choose the trivial ideal, we are actually

choosing from at most $5.2 \cdot n^{\frac{d_i-1}{2}} + 1 < 6n^{\frac{d_i-1}{2}}$ many ideals. So, the class number, h, satisfies

$$h < \left\langle\!\!\left\langle \begin{array}{c} \left\lceil 6n^{\frac{d_i-1}{2}} \right\rceil \\ \\ \left\lceil \log_2(n^{\frac{d_i-1}{2}}) \right\rceil \end{array} \right\rangle\!\!\right\rangle .$$

By V.1.7 in [20], the order of the ray class group for tame extensions ramifying at primes dividing n is $h \cdot 2^{r_0} \cdot N(n) \cdot \prod_{Q|n}(1 - \frac{1}{N(Q)}) \cdot (U : U_{n,1})^{-1}$ where r_0 is the number of real places. Since $N(n) = n^{d_i}$ and $\prod_{Q|n}(1 - \frac{1}{N(Q)}) \cdot (U : U_{n,1})^{-1} < 1$, This is at most $h \cdot (2n)^{d_i}$. By the tower law, the maximal degree over $\mathbb{Q}$ for an extension with length $i+1$ solvable Galois group is at most

$$d_i \cdot h \cdot (2n)^{d_i} < d_i \cdot \left\langle\!\!\left\langle \begin{array}{c} \left\lceil 6n^{\frac{d_i-1}{2}} \right\rceil \\ \\ \left\lceil \log_2(n^{\frac{d_i-1}{2}}) \right\rceil \end{array} \right\rangle\!\!\right\rangle \cdot (2n)^{d_i} = d_{i+1}.$$

□

Remark 2.2.7. There are only finitely many tame extensions of $\mathbb{Q}$ with length i solvable Galois group unramified outside of a fixed set of primes. Proposition 2.2.6 bounds the degree of such an extension, and hence bounds the discriminant of all such extensions. Since there are only finitely many number fields of bounded discriminant, there are only finitely many such extensions.

Remark 2.2.8. The bound in Proposition 2.2.6 is by no means sharp. It uses

Minkowski's bound to estimate the size of the class group of number fields. If one is willing to assume the generalized Riemann hypothesis, much stronger bounds are available instead.

Chapter 3

The Minimal Number of Generators of Galois Groups

Harbater originally posed Conjecture 1.2.1 in [10]. In this chapter we study how the minimal number of generators of a Galois group relates to the ramification in the corresponding extension, and prove the validity of Harbater's conjecture in some special situations.

3.1 The Nilpotent Case

We first consider nilpotent extensions of $\mathbb{Q}$.

Proposition 3.1.1. *If $G \in \pi_A^t(U_n)$ is nilpotent, then $d(G) \leq \log(n)$.*

Proof. Because G is nilpotent, $d(G) = \max\{d(P)|P \text{ is a Sylow subgroup of } G\}$.

Since each Sylow subgroup is isomorphic to some quotient of G, each Sylow subgroup is also in $\pi_A^t(U_n)$. Thus, we may restrict our attention to the case in which G is a p-group.

Since G is a p-group, by the Burnside basis theorem

$$G/\phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^{d(G)}.$$

Hence, $(\mathbb{Z}/p\mathbb{Z})^{d(G)} \in \pi_A^t(U_n)$ as well. By the Kronecker-Weber theorem, if 2 is ramified in an abelian extension, then it is wildly ramified. Again by the Kronecker-Weber theorem, each odd prime that ramifies in an abelian extension can increase the minimal size of a generating set of the Galois group by at most 1. Hence, at least $d\left((\mathbb{Z}/p\mathbb{Z})^{d(G)}\right) = d(G)$ many odd primes must ramify in the extension providing witness to the fact that $(\mathbb{Z}/p\mathbb{Z})^{d(G)} \in \pi_A^t(U_n)$. Thus, at least $d(G)$ many odd primes divide n, and so $d(G) \leq \log(n)$. □

Remark 3.1.2. In the nilpotent case, we may drop the tameness assumption in Harbater's conjecture as long as we use $C = 2$ instead of $C = 0$. That is, if $G \in \pi_A(U_n)$ is nilpotent, then $d(G) \leq \log(n) + 2$. The proof would proceed as in Proposition 3.1.1, except now 2 may ramify. If 2 ramifies, the Kronecker-Weber theorem tells us that this contributes at most 2 to the minimal size of a generating set of the Galois group. This is offset by the fact that we place the constant $C = 2$ on the right side of the inequality.

3.2 Groups with an Index 2 or Index 3 Nilpotent Subgroup

In this section we prove the validity of Harbater's conjecture if we restrict to Galois groups having an index 2 or index 3 nilpotent subgroup.

3.2.1 The Index 2 Case

We start with the index 2 case by examining nilpotent extensions of quadratic number fields.

Lemma 3.2.1. *There is a constant C such that if F is any quadratic extension of $\mathbb{Q}$ with discriminant d and class number h, then* $\log_2(h) < C + .8 \cdot \log\left(\frac{|d|}{4}\right)$.

Proof. List the quadratic number fields, $F_1, F_2, \ldots, F_i, \ldots$, ordered by increasing size of the absolute value of their discriminants, $|d_i|$. Let h_i and R_i denote the class number of F_i and the regulator of F_i respectively. By the Brauer-Siegel theorem, for all $\epsilon > 0$, there is an $N \in \mathbb{N}$ such that if $i > N$,

$$\frac{\log(h_i R_i)}{\log\left(|d_i|^{\frac{1}{2}}\right)} < (1+\epsilon).$$

Let $\epsilon = .1$. Then for $i > N$ we have

$$\log(h_i R_i) < 1.1 \cdot \log\left(|d_i|^{\frac{1}{2}}\right).$$

Since there are only finitely many number fields of bounded discriminant, we may also choose N large enough so that if $i > N$, then $|d_i| > 4$.

Let

$$C_1 = \max\{\log_2(h_i)\}_{1 \leq i \leq N} + \left|\log\left(\frac{1}{4}\right)\right|.$$

Then, for $1 \leq i \leq N$, we get

$$\log_2(h_i) < C_1 + .8 \cdot \log\left(\frac{|d_i|}{4}\right).$$

For $i > N$, we said

$$\log(h_i R_i) < 1.1 \cdot \log\left(|d_i|^{\frac{1}{2}}\right).$$

Hence,

$$h_i R_i < |d_i|^{\frac{1.1}{2}}$$

and so

$$h_i < \frac{1}{R_i} \cdot |d_i|^{\frac{1.1}{2}}.$$

Taking the base 2 logarithm of both sides of this inequality, we get

$$\begin{aligned}
\log_2(h_i) &< \log_2\left(\frac{1}{R_i}\right) + \frac{1.1}{2} \cdot \log_2\left(|d_i|\right) \\
&= \log_2\left(\frac{1}{R_i}\right) + \frac{1.1}{2\log(2)} \cdot \log\left(|d_i|\right) \\
&< \log_2\left(\frac{1}{R_i}\right) + .8 \cdot \log\left(|d_i|\right) \\
&= \log_2\left(\frac{1}{R_i}\right) + .8 \cdot \log(4) + .8 \cdot \log\left(\frac{|d_i|}{4}\right).
\end{aligned}$$

However, by [1], $R_i > .48$ for quadratic fields. Hence, there is a constant C_2 such that

$$\log_2\left(\frac{1}{R_i}\right) + .8 \cdot \log(4) < C_2.$$

Thus,

$$\log_2(h_i) < C_2 + .8 \cdot \log\left(\frac{|d_i|}{4}\right).$$

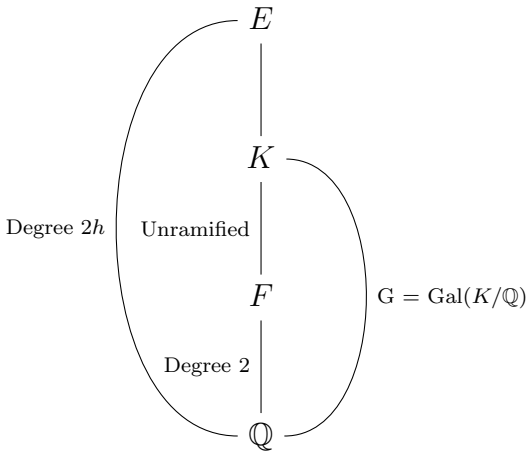
Letting $C = \max\{C_1, C_2\}$ completes the proof of the lemma. □

Remark 3.2.2. By Lemma 3.2.1, there is a constant such that that for any Galois extension $K/\mathbb{Q}$ with a quadratic sub-extension over which it is abelian and unramified, $d\left(\mathrm{Gal}\left(K/\mathbb{Q}\right)\right)$ is bounded above by the sum of the constant and the logarithm of the product of the ramified primes in $K/\mathbb{Q}$.

Any unramified, abelian extension, K, of a quadratic number field, F, is contained in, E, the Hilbert class field of F. In particular, since the Hilbert class field has degree $2h$ over $\mathbb{Q}$, where h is the class number of F, any subfield has degree at

most $2h$. So, the corresponding Galois group, G, satisfies

$$d(G) \leq \log_2(|G|) \leq \log_2(2h) = 1 + \log_2(h).$$



.

Letting C be 2 larger than the constant in Lemma 3.2.1, for any unramified, abelian extension of any quadratic number field with discriminant d, the product of the ramified primes is at least $\frac{|d|}{4}$ and

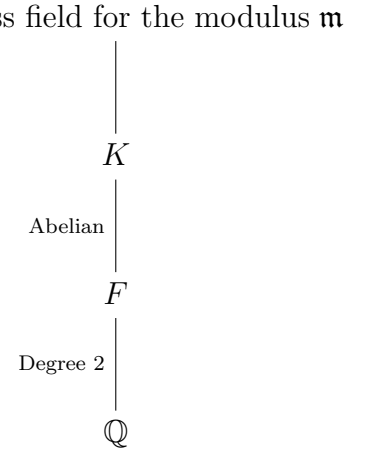
$$d(G) \leq 1 + \log_2(h) < C + \log\left(\frac{|d|}{4}\right).$$

We now consider the case where the index 2 subgroup is abelian.

Lemma 3.2.3. *There is a constant C such that if $K/\mathbb{Q}$ is any extension of $\mathbb{Q}$ with a quadratic sub-extension, F, over which K is abelian Galois and tamely ramified and if $K/\mathbb{Q}$ is unramified outside of primes dividing n and ∞, then $d\left(\mathrm{Gal}(K/F)\right)+1 \leq \log(n) + C$.*

Proof. Let K be a number field satisfying the hypotheses of the lemma. We will construct a constant, independent of K, for which the above inequality holds.

Let F be the quadratic sub-extension of $K/\mathbb{Q}$. Since K/F is abelian, K is a subfield of some ray class field of F for some modulus $\mathfrak{m}$.



Since K/F is a tame extension, we may assume that the highest power of each prime ideal dividing $\mathfrak{m}$ is 1. Furthermore, we may assume that each prime ideal $\mathfrak{P} \mid \mathfrak{m}$ ramifies in K/F, for otherwise we can replace $\mathfrak{m}$ with $\frac{\mathfrak{m}}{\mathfrak{P}}$. Let m be the square-free integer obtained by multiplying together all the integral primes lying under some prime ideal $\mathfrak{P} \mid \mathfrak{m}$. Since each prime ideal $\mathfrak{P} \mid \mathfrak{m}$ ramifies in K/F, each prime integer $p \mid m$ ramifies in $K/\mathbb{Q}$.

Let $Cl_{\mathfrak{m}}(F)$ denote the ray class group for the modulus $\mathfrak{m}$ and let $Cl(F)$ denote the ideal class group of F. By Proposition 3.2.3 in [5], $Cl(F)$ is isomorphic to $Cl_{\mathfrak{m}}(F)$ modulo some homomorphic image of $(\mathcal{O}_F/\mathfrak{m})^*$. Hence,

$$d\left(Cl_{\mathfrak{m}}(F)\right) \leq d\left((\mathcal{O}_F/\mathfrak{m})^*\right) + d\left(Cl(F)\right).$$

Letting h be the class number, we have

$$d\left(Cl(F)\right) \leq \log_2(h).$$

Write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ denotes the finite part of $\mathfrak{m}$ and $\mathfrak{m}_\infty$ denotes the infinite part of $\mathfrak{m}$. By the Chinese remainder theorem and the fact that each prime ideal $\mathfrak{P} \mid \mathfrak{m}_0$ only does so to the first power,

$$\begin{aligned}(\mathcal{O}_F/\mathfrak{m})^* &= (\mathcal{O}_F/\mathfrak{m}_0)^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|} \\ &\cong \prod_{\mathfrak{P}|\mathfrak{m}_0} (\mathcal{O}_F/\mathfrak{P})^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}.\end{aligned}$$

Since each $\mathfrak{P}$ is a prime ideal, each $(\mathcal{O}_F/\mathfrak{P})^*$ is isomorphic to the multiplicative group of some finite field and so is cyclic. Because a quadratic number field has at most two infinite places, $(\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}$ is the product of at most two cyclic groups. Moreover, each $p \mid m$ can split into at most two prime ideals in F, and so the number of prime ideals $\mathfrak{P} \mid \mathfrak{m}_0$ is at most twice the number of prime integers $p \mid m$. Letting $\omega(m)$ denote the number of prime factors of m, we obtain

$$d\left(Cl_{\mathfrak{m}}(F)\right) \leq d\left(\prod_{\mathfrak{P}|\mathfrak{m}_0} (\mathcal{O}_F/\mathfrak{P})^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}\right) + d\left(Cl(F)\right)$$

$$\leq 2 \cdot \omega(m) + 2 + \log_2(h).$$

Because K is a subfield of the ray class field, $\mathrm{Gal}(K/F)$ is a quotient of $Cl_{\mathfrak{m}}(F)$. Thus,

$$d\left(\mathrm{Gal}(K/F)\right) \leq d\left(Cl_{\mathfrak{m}}(F)\right),$$

and so

$$d\left(\mathrm{Gal}(K/F)\right) + 1 \leq 2 \cdot \omega(m) + 2 + \log_2(h) + 1.$$

Let $\pi(\cdot)$ denote the prime counting function. Note that

$$2 \cdot \omega(m) \leq 2 \cdot \pi\left(3^{20}\right) + .1 \cdot \log(m).$$

This is because each prime $p \mid m$ with $p \leq 3^{20}$ contributes 2 to the left hand side of the above inequality which is canceled out by the $2 \cdot \pi\left(3^{20}\right)$ on the right hand side. Each prime $p \mid m$ with $p > 3^{20}$ still only contributes 2 to the left hand side but contributes $.1 \cdot \log(p) > .1 \cdot \log(3^{20}) > 2$ to the right hand side. Letting

$$C_1 = 2 \cdot \pi\left(3^{20}\right) + 2,$$

we obtain that

$$2 \cdot \omega(m) + 2 \leq C_1 + .1 \cdot \log(m).$$

Denoting the discriminant of $F/\mathbb{Q}$ by d, by Lemma 3.2.1 there is a constant C_2, independent of F, such that

$$\log_2(h) + 1 < C_2 + .8 \cdot \log\left(\frac{|d|}{4}\right).$$

Hence,

$$d\left(\mathrm{Gal}(K/F)\right) + 1 < C_1 + .1 \cdot \log\left(m\right) + C_2 + .8 \cdot \log\left(\frac{|d|}{4}\right).$$

Let $C = C_1 + C_2 + 2$ and $A = \gcd\left(|d|, m\right)$. Note that C is independent of K and that

$$\begin{aligned}
&d\left(\mathrm{Gal}(K/F)\right) + 1 < (C_1 + C_2) + .1 \cdot \log\left(m\right) + .8 \cdot \log\left(\frac{|d|}{4}\right) \\
&= (C_1 + C_2) + .1 \cdot \log\left(A\right) + .1 \cdot \log\left(\frac{m}{A}\right) + .8 \cdot \log(A) + .8 \cdot \log\left(\frac{|d|}{4A}\right) \\
&< (C_1 + C_2 + 1) + .9 \cdot \log(A) + .9 \cdot \log\left(\frac{|d|}{4A}\right) + .9 \cdot \log\left(\frac{m}{A}\right) \\
&= (C_1 + C_2 + 1) + .9 \cdot \log\left(A \cdot \frac{|d|}{4A} \cdot \frac{m}{A}\right) \\
&< (C_1 + C_2 + 2) + \log\left(A \cdot \frac{|d|}{4A} \cdot \frac{m}{A}\right) \\
&= C + \log\left(\frac{\frac{|d|}{4} \cdot m}{\gcd\left(|d|, m\right)}\right).
\end{aligned}$$

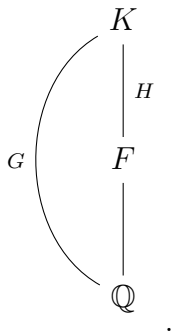
Noting that the product of the ramified primes in $K/\mathbb{Q}$ is at least $\frac{\frac{|d|}{4} \cdot m}{\gcd(|d|, m)}$ completes the proof of the lemma. □

Finally, we now allow K to be any nilpotent, tamely ramified extension over the

quadratic sub-extension.

Theorem 3.2.4. *There is a constant C such that for every positive square-free integer n, if $G \in \pi_A^t(U_n)$ has a nilpotent subgroup of index 2, then $d(G) \leq \log(n)+C$.*

Proof. Let C be the constant from Lemma 3.2.3. Let $G \in \pi_A^t(U_n)$ have a nilpotent subgroup H with $[G : H] = 2$. Let K be an extension providing witness to the fact that $G \in \pi_A^t(U_n)$. We must show that $d(G) \leq \log(n) + C$. Without loss of generality, we may assume that all primes dividing n ramify in $K/\mathbb{Q}$, since we can otherwise replace n with the product of the ramified primes in $K/\mathbb{Q}$. Let F be the quadratic number field corresponding to the fixed field for H.



Note now that

$$d(H) = \max\{d(P) \mid P \text{ is a Sylow subgroup of } H\}.$$

So, choose some Sylow subgroup $P \leq H$ such that $d(H) = d(P)$. Letting S denote

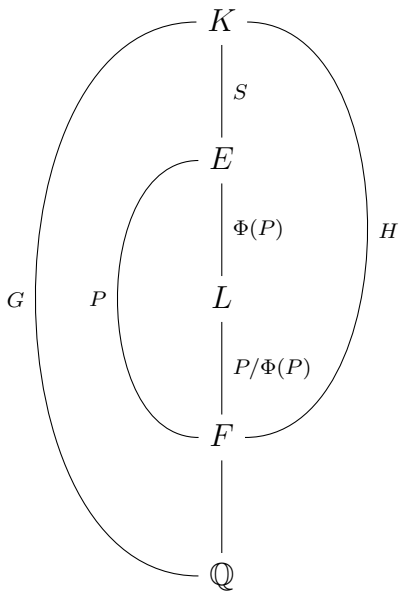
the product of the remaining Sylow subgroups, we get

$$H \cong P \times S.$$

Let E denote the fixed field under S of K/F. Hence,

$$\mathrm{Gal}(E/F) \cong P.$$

Finally, take the fixed field, L, for the Frattini subgroup of P. Hence, L/F is a sub-extension of E/F with $\mathrm{Gal}(L/F) \cong P/\Phi(P)$.



.

By the Burnside basis theorem, $P/\Phi(P)$ is abelian. By Lemma 3.2.3,

$$d\left(P/\Phi(P)\right) + 1 \leq \log(n) + C.$$

Thus,

$$\begin{aligned} d(G) &\leq d(H) + 1 \\ &= d(P) + 1 \\ &= d\left(P/\Phi(P)\right) + 1 \\ &\leq \log(n) + C. \end{aligned}$$

□

3.2.2 The Index 3 Case

We now consider the index 3 situation; the proofs are similar to the index 2 case. For an integer d, we will let $\mathrm{rad}(d) = \prod_{p|d, p \text{ prime}} p$.

Lemma 3.2.5. *There is a constant C such that if $F/\mathbb{Q}$ is any cubic extension of $\mathbb{Q}$ with discriminant d, then $d\left(Cl(F)\right) < C + .95 \cdot \log\left(\mathrm{rad}(d)\right)$.*

Proof. Let F be a number field with $[F : \mathbb{Q}] = 3$. $Cl(F)$ is abelian and so $d\left(Cl(F)\right)$ is equal to the maximal rank of the p-Sylow subgroups of $Cl(F)$. We first consider the 2-Sylow subgroup. By the remark following Theorem 1.1 in [2], there is a constant C_1, independent of F, such that the 2-rank is bounded above by

$$\log_2\left(C_1 \cdot |d|^{.2785}\right) = \log_2(C_1) + \frac{2 \cdot .2785}{\log(2)} \cdot \log\left(|d|^{\frac{1}{2}}\right).$$

Letting $C_2 = \log_2(C_1)$ and noting that $\frac{2 \cdot .2785}{\log(2)} < .85$, we get that the 2-rank is less than

$$C_2 + .85 \cdot \log\left(|d|^{\frac{1}{2}}\right).$$

For the ranks of the other Sylow subgroups we will consider the class group as a whole. An application of the Brauer-Siegel theorem, with $\epsilon = .01$, along with the fact that the regulator is at least .28 by [1], allows us to conclude that there is a C_3, independent of F, such that

$$|Cl(F)| < C_3 \cdot |d|^{\frac{1+.01}{2}}.$$

Hence, the p-rank for $p \geq 3$ is at most

$$\log_3(C_3) + 1.01 \cdot \log_3\left(|d|^{\frac{1}{2}}\right).$$

Letting $C_4 = \log_3(C_3)$ and noting that $\frac{1.01}{\log(3)} < .95$, we get that the above is at most

$$C_4 + .95 \cdot \log\left(|d|^{\frac{1}{2}}\right).$$

Finally, setting $C_5 = \max\{C_2, C_4\}$ gives

$$d\left(Cl(F)\right) < C_5 + .95 \cdot \log\left(|d|^{\frac{1}{2}}\right).$$

Note that if $p \notin \{2,3\}$, then $v_p(d) \leq 2$. By section 6 of chapter 3 in [30], $v_2(d) \leq 3$ and $v_3(d) \leq 5$. So, $|d|^{\frac{1}{2}} \leq 2 \cdot 3^3 \cdot \mathrm{rad}(d)$. Letting $C = C_5 + \log\left(2 \cdot 3^3\right)$, we conclude that

$$d\left(Cl(F)\right) < C + .95 \cdot \log\left(\mathrm{rad}(d)\right).$$

□

Remark 3.2.6. By Lemma 3.2.5, there is a constant such that if $K/\mathbb{Q}$ is Galois with a cubic sub-extension over which K is abelian and unramified, then $d\left(\mathrm{Gal}\left(K/\mathbb{Q}\right)\right)$ is bounded above by the sum of the constant and the logarithm of the product of the ramified primes in $K/\mathbb{Q}$.

If F is a cubic number field with K/F abelian and unramified and K Galois over $\mathbb{Q}$, then $d\left(\mathrm{Gal}\left(K/F\right)\right) \leq d(Cl(F))$. Since $\mathrm{Gal}(K/F)$ is of index 3 in $\mathrm{Gal}(K/\mathbb{Q}), d\left(\mathrm{Gal}\left(K/\mathbb{Q}\right)\right)$ is at most $2 + d(Cl(F))$. Note now that $\mathrm{rad}(d)$ is the product of the ramified primes in $K/\mathbb{Q}$ and so applying Lemma 3.2.5 verifies the claim at the start of the remark.

Lemma 3.2.7. *There is a constant C such that if $K/\mathbb{Q}$ is any Galois extension of $\mathbb{Q}$ with a cubic sub-extension, F, over which K is abelian and tamely ramified and if $K/\mathbb{Q}$ is unramified outside of primes dividing n and ∞, then $d\left(\mathrm{Gal}(K/F)\right) + 1 \leq \log(n) + C$.*

Proof. As in Lemma 3.2.3 we consider ray class fields. Let F be the cubic subextension and let $\mathfrak{m}$ be the smallest modulus admissible for K and m be the square-free product of integral primes lying under primes dividing $\mathfrak{m}$. We may assume that each $\mathfrak{P} \mid \mathfrak{m}$ only does so to the first power and that each such prime ideal also ramifies in K/F. An analogous argument as in Lemma 3.2.3 shows that $3 \cdot \omega(m) + 3 + d\left(Cl(F)\right)$ is an upper bound for $d\left(\mathrm{Gal}(K/F)\right)$. Letting $C_1 = 3 \cdot \pi(3^{300})$ gives $3 \cdot \omega(m) \leq C_1 + .01 \cdot \log(m)$. If $C_2 = C_1 + 3 + 1$, C_3 is the constant from Lemma 3.2.5, and d is the discriminant of F, then

$$d\left(\mathrm{Gal}(K/F)\right) + 1 < C_2 + .01 \cdot \log(m) + C_3 + .95 \cdot \log\left(\mathrm{rad}(d)\right).$$

Let $C = C_2 + C_3 + 2$ and $A = \gcd(\mathrm{rad}(d), m)$. Then,

$$\begin{aligned}
&d\left(\mathrm{Gal}(K/F)\right) + 1 \\
&< (C_2 + C_3) + .01 \cdot \log\left(\frac{m}{A}\right) + .01 \cdot \log(A) + .95 \cdot \log\left(\frac{\mathrm{rad}(d)}{A}\right) + .95 \cdot \log(A) \\
&< (C_2 + C_3 + 2) + .96 \cdot \log\left(\frac{m}{A}\right) + .96 \cdot \log\left(\frac{\mathrm{rad}(d)}{A}\right) + .96 \cdot \log(A) \\
&= C + .96 \cdot \log\left(\frac{m \cdot \mathrm{rad}(d)}{A}\right) \\
&< C + \log\left(\frac{m \cdot \mathrm{rad}(d)}{\gcd(\mathrm{rad}(d), m)}\right).
\end{aligned}$$

Note now that $\frac{m \cdot \mathrm{rad}(d)}{\gcd(\mathrm{rad}(d), m)}$ is precisely the product of the ramified primes in $K/\mathbb{Q}$, and so is at most n. This completes the proof of the lemma. $\square$

Theorem 3.2.8. *There is a constant C such that for every positive square-free integer n, if $G \in \pi_A^t(U_n)$ has a nilpotent subgroup of index 3, then $d(G) \leq \log(n)+C$.*

Proof. The proof is identical to Theorem 3.2.4 except replace Lemma 3.2.3 with Lemma 3.2.7 and let $[G : H] = 3$ instead of 2. □

3.2.3 Wild Ramification

Remark 3.2.9. Theorem 3.2.4 and Theorem 3.2.8 still hold if we expand our attention to extensions of $\mathbb{Q}$ in which primes larger than or equal to 5 are wildly ramified. Furthermore, if 3 is unramified in the quadratic or cubic sub-extension of $\mathbb{Q}$, then 3 may be wildly ramified in the nilpotent extension of the quadratic or cubic. Additionally, the above proofs still hold as written if 2 or 3 is wildly ramified in the quadratic or cubic sub-extension of $\mathbb{Q}$.

The only place that tameness was used was in bounding the number of generators of the ray class group by bounding the number of generators of

$$(\mathcal{O}_K/\mathfrak{m})^* \cong (\mathcal{O}_K/\mathfrak{m}_0)^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|} \cong \prod_{\mathfrak{P}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{P})^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}$$

in the proofs of Lemma 3.2.3 and Lemma 3.2.7. If instead we no longer consider only tame moduli for primes lying above integral primes larger than 3, or lying above 3 when 3 is unramified in the quadratic or cubic, we now get

$$(\mathcal{O}_K/\mathfrak{m})^* \cong (\mathcal{O}_K/\mathfrak{m}_0)^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|} \cong \prod_{\mathfrak{P}|\mathfrak{m}_0} \left(\mathcal{O}_K/\mathfrak{P}^{k_\mathfrak{P}}\right)^* \times (\mathbb{Z}/2\mathbb{Z})^{|\mathfrak{m}_\infty|}$$

where $k_\mathfrak{P}$ can be larger than 1 if it lies over an integral prime larger than 3 or above 3 when 3 is unramified in the quadratic or cubic. By Corollary 4.2.11 in [5], since $p \geq \min\{e+2, k_\mathfrak{P}\}$ by assumption, we get that

$$\left(\mathcal{O}_K/\mathfrak{P}^{k_\mathfrak{P}}\right)^* \cong \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times (\mathbb{Z}/p^q\mathbb{Z})^{(r+1)f} \times \left(\mathbb{Z}/p^{q-1}\mathbb{Z}\right)^{(e-r-1)f}$$

where $k_\mathfrak{P} + e - 2 = eq + r, 0 \leq r < e$. Note for a quadratic extension that $(r+1)f \leq ef \leq 2$, and$(e-r-1)f \leq (e-1)f \leq ef \leq 2$, and for a cubic extension that $(r+1)f \leq ef \leq 3$, and$(e-r-1)f \leq (e-1)f \leq ef \leq 3$. So, $\left(\mathcal{O}_K/\mathfrak{P}^{k_\mathfrak{P}}\right)^*$ is a product of at most 5 cyclic groups in the quadratic case, and 7 cyclic groups in the cubic case. If we still let m be the product of the integral primes lying under those dividing the modulus, adjusting the proof of Lemma 3.2.3 for the current situation, we now have

$$d\left(\mathrm{Gal}\left(K/F\right)\right) + 1 \leq 5 \cdot (2 \cdot \omega(m)) + 2 + \log_2(h) + 1$$

instead of

$$d\left(\mathrm{Gal}\left(K/F\right)\right) + 1 \leq 2 \cdot \omega(m) + 2 + \log_2(h) + 1.$$

If we let $C_1 = 10 \cdot \pi(3^{100}) + 2$ instead of $2 \cdot \pi(3^{20}) + 2$, we get

$$10 \cdot \omega(m) + 2 \leq C_1 + .1 \cdot \log(m)$$

and the rest of the proof is the same. Adjusting the proof of Lemma 3.2.7 for the current situation, we get that $7 \cdot (3 \cdot \omega(m)) + 3 + d\,(Cl(F)) + 1$ is an upper bound for $d\,(\mathrm{Gal}(K/F)) + 1$. Now let $C_1 = 21 \cdot \pi(3^{2100})$ instead of $3 \cdot \pi(3^{300})$ and the rest of the proof is the same. The proofs of Theorem 3.2.4 and Theorem 3.2.8 still work even in this new situation.

3.3 Modular Forms

Let $f = \sum_{n \geq 1} a_n q^n \in S_k(N, \epsilon)$ be a newform and let $K = \mathbb{Q}(\dots, a_n, \dots)$. For each nonzero prime λ in $\mathcal{O}_K$, there is a representation of the absolute Galois group of $\mathbb{Q}$ that takes values in $GL(2, \mathcal{O}_K)$. Reducing modulo λ and letting $\mathbb{F} = \mathcal{O}_K/\lambda$ and $l = \mathbb{Z} \cap \lambda$, we obtain a mod l representation

$$\overline{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}).$$

For more details, see 21.1 in [27].

Proposition 3.3.1. *If l is a regular prime and f is of level a power of l, then conjecture 2.1 in [10] holds for the field corresponding to the image of $\overline{\rho}_{f,\lambda}$ with a constant $C = 4$.*

Proof. Let $\overline{\rho}_{f,\lambda}^{proj}$ be the projectivized representation, which is the composition $\overline{\rho}_{f,\lambda}$ with the map from $\mathrm{GL}(2,\mathbb{F}) \to \mathrm{PGL}(2,\mathbb{F})$ which is just modding out by scalar matrices. Let E be the field corresponding to the image of $\overline{\rho}_{f,\lambda}^{proj}$. By Theorem 21.1.1 in [27], E is ramified only at l. By [8] and also by [32], the Galois group of $E/\mathbb{Q}$ requires at most 3 generators, or is otherwise an elementary abelian $l-$group semidirect a cyclic group of order prime to l. In the first case the conjecture is satisfied with $C = 3$, so we consider the latter where the Galois group is $G \cong (\mathbb{Z}/l\mathbb{Z})^r \rtimes \mathbb{Z}/t\mathbb{Z}$. This gives the following tower:

$$\begin{array}{c} E \\ \Big| \; (\mathbb{Z}/l\mathbb{Z})^r \\ E^{(\mathbb{Z}/l\mathbb{Z})^r} \\ \Big| \; \mathbb{Z}/t\mathbb{Z} \\ \mathbb{Q} \end{array} .$$

Since $E^{(\mathbb{Z}/l\mathbb{Z})^r}$ is an abelian extension of $\mathbb{Q}$ ramified only at l and of order prime to l, it is contained in $\mathbb{Q}(\zeta_l)$ and so is totally ramified. Since $E/E^{(\mathbb{Z}/l\mathbb{Z})^r}$ is also abelian, ramified only at primes over l, it is contained ray class field of $\mathbb{Q}(\zeta_l)$ for some modulus (l^s). Notice that there is only one prime lying over l in $E^{(\mathbb{Z}/l\mathbb{Z})^r}$ since it is totally ramified over $\mathbb{Q}$. Hence, this is the only prime that can ramify in $E/E^{(\mathbb{Z}/l\mathbb{Z})^r}$. If it is not totally ramified in this extension, then since the extension is abelian, taking the fixed field for the inertia group would give an unramified,

abelian subextension of $E/E^{(\mathbb{Z}/l\mathbb{Z})^r}$ of order dividing $[E : E^{(\mathbb{Z}/l\mathbb{Z})^r}] = l^r$. Taking the compositum of this subextension with $\mathbb{Q}(\zeta_l)$ would then give an abelian, unramified extension of $\mathbb{Q}(\zeta_l)$ of order a power of l. This would contradict l being regular, and so $E/E^{(\mathbb{Z}/l\mathbb{Z})^r}$ must be totally ramified at the prime over l. In particular, this also means that $E/\mathbb{Q}$ is totally ramified at l. Since the extension is tame, this means $r = 0$ and so G is cyclic and generated by one element.

So, the conjecture holds for the image of the projectivized representation with $C = 3$. However, the image of the projectivized representation is just the a quotient of the image of the original representation by a cyclic group, (the scalar matrices form a cyclic group isomorphic to $\mathbb{F}^*$), and so requires at most one more generator. Hence, the conjecture holds for the image of the original representation with $C = 4$. □

3.4 Consequences and Examples

Proposition 3.4.1. *If Harbater's conjecture holds, then for all $n, \pi_1^t(U_n)$ is topologically finitely generated.*

Proof. By assumption of Harbater's conjecture, every group in the inverse system whose limit is $\pi_1^t(U_n)$ is generated by at most $C + \log(n)$ elements. Now apply Lemma 2.5.3 in [26]. □

Proposition 3.4.2. *If Harbater's conjecture holds with a constant C, then for any*

tame extension $K/\mathbb{Q}$, if m is the product of the ramified primes we have that the class group of K has a generating set of size at most $1 + [K : \mathbb{Q}]\,(\log(m) + C - 1)$.

Proof. Any group G that can be generated by d elements is a quotient of the free group on d elements, F_d. So, $G \cong F_d/N$. By the correspondence theorem, any subgroup of G is of the form H/N for $N \leq H \leq F_d$. Also, $[F_d : H] = [G : H/N]$. Let this index be n. By the Nielsen-Schreier theorem, we know that H is free of rank $1 + n(d-1)$. So, H/N can be generated by $1 + n(d-1)$ elements.

Let K be a tame extension of $\mathbb{Q}$ and let m be the product of the ramified primes. Let $n = [K : \mathbb{Q}]$, H_K be the hilbert class field of K, and M be the Galois closure of H_K over $\mathbb{Q}$.

By assumption of Harbater's conjecture, we get that $\mathrm{Gal}(M/\mathbb{Q})$ has at most $\log(m) + C$ generators. Since $\mathrm{Gal}(M/K)$ is an index n subgroup, it has at most $1+n(\log(m)+C-1)$ generators. Since $\mathrm{Gal}(H_K/K)$, which is isomorphic to the class group of K, is a quotient of $\mathrm{Gal}(M/K)$, it also has at most $1+n(\log(m)+C-1) =$

$1 + [K : \mathbb{Q}](\log(m) + C - 1)$ generators. □

Example 3.4.3. As a consequence of Theorem 3.2.4 and Theorem 3.2.8, if p is a prime number and n is a square-free natural number, then there are only finitely many groups of the form $(\mathbb{Z}/p\mathbb{Z})^i \rtimes \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^i \rtimes \mathbb{Z}/3\mathbb{Z}$ in $\pi_A^t(U_n)$. If we also assume that n is coprime to 2 and 3, then the same is true for $\pi_A(U_n)$.

These groups are of interest because they are potential cases in which Harbater's conjecture could have clashed with the Boston-Markin conjecture. They include all generalized dihedral groups, of which elementary abelian p-groups semidirect $\mathbb{Z}/2\mathbb{Z}$ by inversion for $p \geq 3$ are a special case. These groups have $\mathbb{Z}/2\mathbb{Z}$ abelianization, so the Boston-Markin conjecture predicts there should exist extensions ramified at a single prime that realize each of them. The groups themselves also require as many generators as the rank of the elementary abelian p-group, so Harbater's conjecture suggests that the product of the primes in the extensions realizing them would have to be quite large.

Remark 3.4.4. The arguments of section 3.2 actually show that for the corresponding extensions, $d(G) < C + .97 \cdot \log(n)$ where n is the product of the ramified primes. This means that when n is large, $d(G) < \log(n)$ without the aid of the constant. Since each prime can only divide the discriminant a bounded number of times for quadratic and cubic extensions, this means that if the discriminant is large, then n is also large. Since there are only finitely many number fields of bounded discriminant, n is small for only finitely many such extensions and so the constant is necessary

for only finitely many such extensions. This provides evidence that the constant should be small, and perhaps even 0.

Proposition 3.4.5. *Let $K/\mathbb{Q}$ be a tame Galois extension with Galois group G. For a prime $p \in \mathbb{Z}$, let r_p be the number of primes it splits into in $K/\mathbb{Q}$. Let n be the product of the ramified primes in $K/\mathbb{Q}$. If for some prime $2 + \log_2(r_p) < \log(n)$, then $d(G) < \log(n)$.*

Proof. Since the extension is tame, the ramification group is cyclic for each prime. Also, since the quotient of the decomposition group by the ramification group is cyclic for each prime, the decomposition group can be generated by at most 2 elements for each prime. For any prime, the decomposition group, D_p, has index r_p. If D_p does not generate all of $G = Gal(K/\mathbb{Q})$, then pick some element, $g_1 \in G - D$. This generates a larger subgroup $< D, g_1 >$. Since it contains D as a subgroup, we get $|D|$ divides the order of this group and so it must have order at least $2|D|$ and hence index at most $\frac{r_p}{2}$. If $< D, g_1 > \neq G$, pick a g_2 not in its span. This then generates a subgroup at least twice as large cardinality and half as large index. Continuing in this fashion, we need only choose at most $\log_2(r_p)$ many elements until we generate a subgroup of index at most 1, and hence is all of G. So, G can be generated by the two elements generating D_p as well as $\log_2(r_p)$ many other elements. So, if $2 + \log_2(r_p) < \log(n)$, then $d(G) < \log(n)$. Note that for unramified primes, the inertia groups are trivial and so the decomposition groups are cyclic. So if the prime is unramified, we only need $1 + \log_2(r_p) < \log(n)$. □

3.5 Extensions of Other Number Fields

In this section we examine how the number of generators of the Galois group relates to the number of ramified primes in nilpotent extensions of a fixed base number field.

3.5.1 Tame Extensions

Proposition 3.5.1. *Let K be a number field with class group C. Suppose E/K is a tame, nilpotent extension in which t prime ideals in K ramify. Let $G = \mathrm{Gal}\,(E/K)$. Then, $d(G) \leq d(C) + t$. Note that in the case that K is totally real, we do not allow ramification at the infinite places.*

Proof. Noting that $d(G) = \max\{d(P) \mid P \text{ is a Sylow subgroup of } G\}$ and applying the Burnside basis theorem, it suffices to prove the proposition in the situation where E/K is abelian. Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_t$ be the primes that ramify. E is then contained in the ray class field for modulus that is the product of these primes. By Proposition 3.2.3 in [5], C is isomorphic to the ray class group modulo some homomorphic image of $(O_k/\mathfrak{P}_1 \ldots \mathfrak{P}_t)^* \cong (\mathcal{O}_K/\mathfrak{P}_1)^* \times \cdots \times (\mathcal{O}_K/\mathfrak{P}_t)^*$. Each $(\mathcal{O}_K/\mathfrak{P}_i)^*$ is cyclic, so any homorphic image of $(O_k/\mathfrak{P}_1 \ldots \mathfrak{P}_t)^*$ requires at most t generators. Thus, the ray class group can be generated using at most $d(C) + t$ elements. Since G is a quotient of the ray class group, we have $d(G) \leq d(C) + t$. □

Example 3.5.2. As a consequence of Proposition 3.5.1, if K has class number 1, then any tame, nilpotent extension ramified only at a single prime is cyclic. Suppose

instead now that K has a cyclic class group, C, of order h. Let $p \in \mathbb{Z}$ be a prime and $\mathfrak{P} \in \mathcal{O}_K$ be a prime lying over it with residue degree f. If $\gcd(h, p^f - 1) = 1$, then any tame, nilpotent extension E/K in which $\mathfrak{P}$ is the only ramified prime is cyclic. As in Proposition 3.5.1, the ray class group for $\mathfrak{P}$ modulo some homomorphic image of $(\mathcal{O}_K/\mathfrak{P})^* \cong \mathbb{Z}/(p^f - 1)\mathbb{Z}$ is isomorphic to C. Any homomorphic image is cyclic of order dividing $p^f - 1$, and so, by Schur-Zassenhaus, the ray class group is a semidirect product of a cyclic group of order dividing $p^f - 1$ and C. Since the ray class group is abelian, this is actually a direct product. Since h is coprime to $p^f - 1$ and C is cyclic, the Chinese remainder theorem tells us this direct product is a cyclic group.

3.5.2 Arbitrary Extensions

Proposition 3.5.3. *Let K be a number field with $[K : \mathbb{Q}] = n$. Let E/K be a nilpotent extension. Suppose the primes in K that are ramified in E/K do not lie over 2 or any integral prime that ramifies in $K/\mathbb{Q}$. Let C be the class group of K and a the number of primes that ramify in E/K. Then, the number of generators of the Galois group of E/K is at most $d(C) + n + a$.*

Proof. Since the number of generators required in a nilpotent group is the maximum of the number of generators of one of its Sylow subgroups, it suffices to prove this for p-groups. By the Burnside basis theorem, it then suffices to prove this for abelian p-groups. Let $\mathfrak{m}$ be the product of the primes ramifying in E/K. Any abelian

p-power extension ramified only at primes dividing $\mathfrak{m}$ is in a ray class field for $\mathfrak{m}^k$ for some k. If some prime $\mathfrak{P}$ over p divides $\mathfrak{m}$, then by Corollary 4.2.11 in [5],

$$\left(\mathcal{O}_K/\mathfrak{P}^k\right)^* \cong \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^q\mathbb{Z}\right)^{(r+1)f} \times \left(\mathbb{Z}/p^{q-1}\mathbb{Z}\right)^{(e-r-1)f}$$

where $k+e-2 = eq+r, 0 \leq r < e$. Since p is unramified by assumption,

$$\left(\mathcal{O}_K/\mathfrak{P}^k\right)^* \cong \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{k-1}\mathbb{Z}\right)^f \cong \left(\mathbb{Z}/(p^{k-1})(p^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^{k-1}\mathbb{Z}\right)^{f-1}.$$

This contributes at most $1+f-1 = f$ generators to $\left(\mathcal{O}_K/\mathfrak{m}^k\right)^*$. If g is the number of primes p splits into in K, even if all of them divide $\mathfrak{m}$, this contributes at most $gf = n$ generators to $\left(\mathcal{O}_K/\mathfrak{m}^k\right)^*$. For the primes $\mathfrak{L}$ over l that divide $\mathfrak{m}$ but do not lie over p, we have

$$\left(\mathcal{O}_K/\mathfrak{L}^k\right)^* \cong \left(\mathbb{Z}/(l^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/l^q\mathbb{Z}\right)^{(r+1)f} \times \left(\mathbb{Z}/l^{q-1}\mathbb{Z}\right)^{(e-r-1)f}.$$

This contributes to the p-part of $\left(\mathcal{O}_K/\mathfrak{m}^k\right)^*$ if and only if p divides l^f-1, in which case it contributes at most one generator since $\left(\mathbb{Z}/(l^f-1)\mathbb{Z}\right)$ is cyclic. Hence, the number of generators of the p-part of $\left(\mathcal{O}_K/\mathfrak{m}^k\right)^*$ is at most $n+a$, where a is the number of primes dividing $\mathfrak{m}$. By Proposition 3.2.3 in [5], C is isomorphic to the ray class group modulo some homomorphic image of $\left(\mathcal{O}_K/\mathfrak{m}^k\right)^*$, which implies that the p-part of the ray class group requires at most $d(C)+n+a$ generators. Note that

in the case $p = 2$, we do not allow primes lying over 2 to ramify, so we can subtract n from this bound. However, the potentially n infinite places can each contribute a $\mathbb{Z}/2\mathbb{Z}$ factor to the ray class group and so we need to add n back to the bound. $\square$

Remark 3.5.4. Proposition 3.5.3 in the case of $K = \mathbb{Q}$ says that for nilpotent extensions, the number of generators required for the Galois groups is at most 1 plus the number of ramified primes. If we allow 2 to ramify and only count finite primes, this upper bound is realized as demonstrated by the example of $\mathbb{Q}(\zeta_8)/\mathbb{Q}$, in which 2 is the only ramified finite prime, with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 3.5.5. Let K be a number field with a cyclic class group C. Let $p \geq 3$ be a prime that splits completely in $K/\mathbb{Q}$ with $\gcd(|C|, p \cdot (p-1)) = 1$. Let $\mathfrak{P}$ be any prime in $\mathcal{O}_K$ lying over p. Then, any nilpotent extension E/K ramified only at $\mathfrak{P}$ is cyclic. Note here that if K is totally real, then we do not allow any infinite place to ramify in E/K.

First consider an abelian extension E/K ramified only at $\mathfrak{P}$. Then it is in the ray class group corresponding to the modulus $\mathfrak{P}^k$ for some $k \in \mathbb{N}$. By Proposition 3.2.3 in [5], C is isomorphic to this ray class group modulo some homomorphic image of $\left(\mathcal{O}_K/\mathfrak{P}^k\right)^*$. By Corollary 4.2.11 in [5],

$$\left(\mathcal{O}_K/\mathfrak{P}^k\right)^* \cong \left(\mathbb{Z}/(p^f-1)\mathbb{Z}\right) \times \left(\mathbb{Z}/p^q\mathbb{Z}\right)^{(r+1)f} \times \left(\mathbb{Z}/p^{q-1}\mathbb{Z}\right)^{(e-r-1)f}.$$

where $k + e - 2 = eq + r, 0 \leq r < e$. By assumption, $f = e = 1$ since p splits

completely in $K/\mathbb{Q}$. So, $r = 0$ as well since $r < e$ and $q = k-1$. Hence, $(e-r-1)f = 0$, $(r+1)f = 1$, and

$$\left(\mathcal{O}_K/\mathfrak{P}^k\right)^* \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \times \left(\mathbb{Z}/p^{k-1}\mathbb{Z}\right) \cong \mathbb{Z}/\left((p-1)\cdot p^{k-1}\right)\mathbb{Z}.$$

Any homomorphic image, say N, of $\left(\mathcal{O}_K/\mathfrak{P}^k\right)^*$ is a quotient of $\left(\mathcal{O}_K/\mathfrak{P}^k\right)^*$ and so is also cyclic of order dividing $(p-1)\cdot p^{k-1}$. Thus, the ray class group modulo a cyclic group of order dividing $(p-1)\cdot p^{k-1}$, N, is isomorphic to C, a cyclic group of order prime to $(p-1)\cdot p$. By Schur-Zassenhaus, the ray class group is isomorphic to some semidirect product, $N \rtimes C$. Since the ray class group is abelian, the semidirect product must be a direct product, $N \times C$. Since N and C are both cyclic of coprime order, $N \times C$ is also cyclic.

Now suppose that E/K is a nilpotent extension ramified only at $\mathfrak{P}$. By the Burnside basis theorem, if we take the quotient of the Galois group by the Frattini subgroup, we obtain an abelian extentsion of K ramified only at $\mathfrak{P}$. By the above argument, this extension is cyclic. Hence, the original Galois group must also be cyclic.

As an application of the above, consider a quadratic extension of $\mathbb{Q}$ with class number 1. Determining whether an unramified prime $p \geq 3$ splits completely amounts to determining if it is a quadratic residue. If it is, then it splits and so the above applies to both primes above p in the quadratic field.

Bibliography

[1] Sergio Astudillo, Francisco Diaz y Diaz, and Eduardo Friedman. Sharp lower bounds for regulators of small-degree number fields. *J. Number Theory*, 167:232–258, 2016.

[2] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *ArXiv e-prints*, January 2017.

[3] Nigel Boston and Nadya Markin. The fewest primes ramified in a G-extension of $\mathbb{Q}$. *Ann. Sci. Math. Québec*, 33(2):145–154, 2009.

[4] Richard Brauer. On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947.

[5] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[6] A. Cueto-Hernández and G. D. Villa-Salvador. Nilpotent extensions of number fields with bounded ramification. *Pacific J. Math.*, 196(2):297–316, 2000.

[7] Francisco Diaz y Diaz. *Tables minorant la racine n-ième du discriminant d'un corps de degré n*, volume 6 of *Publications Mathématiques d'Orsay 80 [Mathematical Publications of Orsay 80]*. Université de Paris-Sud, Département de Mathématique, Orsay, 1980.

[8] X. Faber. Finite p-Irregular Subgroups of PGL(2,k). *ArXiv e-prints*, December 2011.

[9] Alexander Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*, volume 224 of *Lecture notes in mathematics*. Springer-Verlag, 1971.

[10] David Harbater. Galois groups with prescribed ramification. In *Arithmetic geometry (Tempe, AZ, 1993)*, volume 174 of *Contemp. Math.*, pages 35–60. Amer. Math. Soc., Providence, RI, 1994.

[11] Jing Long Hoelscher. *Galois extensions ramified at one prime*. PhD thesis, University of Pennsylvania, 2007.

[12] Jing Long Hoelscher. Galois extensions ramified only at one prime. *J. Number Theory*, 129(2):418–427, 2009.

[13] John W. Jones. Number fields unramified away from 2. *J. Number Theory*, 130(6):1282–1291, 2010.

[14] John W. Jones and David P. Roberts. Number fields ramified at one prime. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 226–239. Springer, Berlin, 2008.

[15] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[16] Sylla Lesseni. The nonexistence of nonsolvable octic number fields ramified only at one small prime. *Math. Comp.*, 75(255):1519–1526, 2006.

[17] Sylla Lesseni. Nonsolvable nonic number fields ramified only at one small prime. *J. Théor. Nombres Bordeaux*, 18(3):617–625, 2006.

[18] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[19] John C. Miller. Real cyclotomic fields of prime conductor and their class numbers. *Math. Comp.*, 84(295):2459–2469, 2015.

[20] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[21] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[22] A. M. Odlyzko. Andrew Odlyzko: Some unpublished materials. `http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`, 1976. [Online; accessed 7-November-2018].

[23] A. M. Odlyzko. On conductors and discriminants. pages 377–407, 1977.

[24] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[25] Bernat Plans. On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$. *Pacific J. Math.*, 215(2):381–391, 2004.

[26] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.

[27] Kenneth A. Ribet and William A. Stein. Lectures on modular forms and hecke operators, 2017. Available at https://wstein.org/books/ribet-stein/main.pdf.

[28] Herbert Robbins. A remark on Stirling's formula. *Amer. Math. Monthly*, 62:26–29, 1955.

[29] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[30] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[31] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[32] D. E. Taylor. Pairs of generators for matrix groups. i. *I. The Cayley Bulletin*, 3:800–0, 1987.

[33] Helmut Völklein. *Groups as Galois groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction.

[34] David Zywina. The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$. *Duke Math. J.*, 164(12):2253–2292, 2015.