Universiteit Utrecht

The inverse Galois problem with minimal ramification

Master Thesis Mathematical Sciences
July 2023

Mees Jager

Supervisor: Dr. Valentijn Karemaker
Second reader: Prof. Dr. Gunther Cornelissen

Abstract

Various authors have studied variations of the inverse Galois problem over $\mathbb{Q}$, which, in its classical form, asks for a finite group G if there exists a number field K such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. In [5, Conjecture 1.2] Boston and Markin conjecture that every group G should appear as the Galois group of a number field which ramifies at exactly d primes (counting the infinite prime), where d denotes the minimal number of generators of the abelianisation of G. They prove the validity of their conjecture for all groups up to order 32 [5, Theorem 3.1]. In Table 5.1 we provide examples of this conjecture for groups with cyclic abelianisation and we illustrate how to use these to construct examples of order larger than 32. Harbater [13, Theorem 2.23], Hoelscher [16, Corollary 2.1.6] and Pollak [27, Proposition 2.1.8] give a description of the Galois groups that can appear for number fields where a single predetermined prime is ramified. They respectively focus on the primes 2, 3 and 5. We give a similar description of the possible Galois groups that can appear for the primes $7 \leq p \leq 19$ in Proposition 3.3.3. Furthermore, Pollak proved for primes $2 \leq p < 37$ that, if G is a Galois group of a number field where only p ramifies and $|G| < 660$, then G must be solvable [27, Theorem 2.1.10]. We strengthen this result in Theorem 4.1.3 by implementing one of the approaches of Pollak in GAP [11] and obtaining an improved range of $2 \leq p < 101$ and $|G|$ being one of the orders in Table 4.1.

Acknowledgements

First and foremost I want to thank my supervisor, Valentijn, for many things. She initially introduced me to the topic, which turned out to be a really good fit. Whenever I felt I was working in too much detail or too slow she ensured me that details are not a bad thing and that breaks are necessary. The meetings we had made me feel good about the work I was doing and like I was on the right track, which was invaluable to me. I want to thank Mar for being such a good friend, the many helpful discussions we had about (mathematical) problems I was struggling with and making me truita whenever I needed it. Finally, I want to thank Mieke for helping me get through several roadblocks in the form of annoying proofs. Math is more fun together!

Contents

Conventions and notation

Throughout this thesis G will be a finite group and K a number field unless stated otherwise. If K is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ we say that K is a **G-extension** and that K **realises** G. When we speak of ramification in a number field we will be explicit about whether or not we are talking about a finite prime, i.e. a prime $p \in \mathbb{Z}$, or the infinite prime ∞ of $\mathbb{Q}$. More about this distinction can be found in Section 2.2. Following the notation of Harbater [13], Hoelscher [16] and Pollak [27], we will use $\pi_A(U_p)$ to denote the collection of finite groups G for which there exists a Galois extension $K/\mathbb{Q}$ where the only ramified finite prime is p. It is possible that such K also ramifies at the infinite prime.

Chapter 1

Introduction

1.1 What is the inverse Galois problem?

For a finite group G, the inverse Galois problem over $\mathbb{Q}$ asks if there is a Galois extension K of $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. This question remains unsolved in its full generality at this point, but some families of groups have been dealt with. The first systematic approach to solving the problem was due to Hilbert in 1892 [15]. For any $n \geq 1$, he showed that A_n and S_n can be realised as Galois groups over $\mathbb{Q}$ using his Irreducibility Theorem. We will see in Theorem 1.2.2 that all finite abelian groups are realisable as Galois groups over $\mathbb{Q}$. This result has been extended by Scholz and Reichardt [30] to all finite nilpotent groups of odd order. In 1954 Shafarevich [31] managed to extend this even further and showed that all finite solvable groups can be realised as Galois groups over $\mathbb{Q}$.

1.2 Additional restrictions on ramified primes

Any non-trivial extension $K/\mathbb{Q}$ must ramify at at least one rational prime. Hence, if we manage to realise some group G as a Galois group over $\mathbb{Q}$ we can wonder how many primes ramify in the G-extension we found. Furthermore, among all the G-extensions out there, we wonder which of them has the least amount of ramified primes (counting the infinite prime)?

Definition 1.2.1. Let G be a finite group. Let $\{K_i\}_{i\in I}$ be the collection of G-extensions K_i where I is some index set and let m_i denote the number of ramified primes in the extension K_i (counting the infinite prime). We define $\mathrm{m}(G)$ to be the minimum of the set $\{m_i\}_{i\in I}$.

Additionally, for what groups G can we obtain G-extensions which ramify at a single prime? Various authors have already provided partial answers to these questions. Boston and Markin resolve the matter for abelian groups in [5, Theorem 1.1] and we give (a more detailed version of) their proof in Section 2.4.

Theorem 1.2.2. *Let G be a non-trivial finite abelian group with a minimal generating set of d generators. Then there exists a totally real G-extension of $\mathbb{Q}$ which ramifies at exactly d finite primes. Furthermore, there is no G-extension which ramifies at fewer than d primes including ramification at the infinite prime.*

For a non-abelian group G, let d denote the minimal number of generators of the abelianisation G^{ab}. Theorem 1.2.2 tells us that we can find a G^{ab}-extension of $\mathbb{Q}$ which ramifies at exactly d primes. The Galois correspondence readily gives the following lower bound for $m(G)$.

Corollary 1.2.3. *Let G be any finite group and d the minimal number of generators of G^{ab}. Then $m(G) \geq d$.*

The proof of this follows quickly from Lemma 2.3.31 once we develop some standard results. It is conjectured in [5] that the lower bound is actually attained, i.e. we can also find a G-extension ramifying at exactly d primes.

Conjecture 1.2.4. *[5, Conjecture 1.2] Let G be a non-trivial finite group and $d \geq 1$ the minimal number of generators of the abelianisation G^{ab}. Then there exists a G-extension of $\mathbb{Q}$ which ramifies at exactly d primes (counting the infinite prime) and there is no such extension ramifying at less than d primes.*

Note that Corollary 1.2.3 proves the last sentence of Conjecture 1.2.4. In [25] the validity of this Conjecture has been checked by Nomura for 3-groups of order less than or equal to 3^5. The most general result is by Kisilevsky and Sonn [18] which states that Conjecture 1.2.4 holds for all p-groups in the class which is generated by cyclic p-groups and is closed under direct products, wreath products and rank-preserving quotients. In [5] Boston and Markin proved that Conjecture 1.2.4 holds for all groups of order less than or equal to 32.

1.3 Related results

In this thesis we have studied and adapted the results of Harbater [13], Hoelscher [16] and Pollak [27]. They studied finite extensions of $\mathbb{Q}$ where only a single predetermined finite prime p was allowed to ramify. Each of them provided results on the possible Galois groups that can occur in this setting for respectively the primes 2 [13, Theorem 2.23], 3 [16, Corollary 2.1.6] and 5 [27, Proposition 2.1.8]. In Chapter 3 we provide a similar characterisation for the primes $7 \leq p < 23$ in Proposition 3.3.3. In some instances we also give more detailed versions of the proofs of their results. Furthermore, we explain how additional assumptions on the extension K provide stronger results.

For a prime $2 \leq p < 37$ and a group $G \in \pi_A(U_p)$ with $|G| < 660$, Pollak proved that G must be solvable [27, Theorem 2.1.10]. In Chapter 4 we implement ideas of Pollak in [11, GAP] to prove that the same holds for primes $2 \leq p < 101$ and larger orders than 660. We also explain how Pollak adapted results of Harbater and Hoelscher to obtain his result.

Since the symmetric and alternating groups have cyclic abelianisations, Conjecture 1.2.4 suggests that they should be realisable as Galois groups over $\mathbb{Q}$ by some number field K with only a single ramified prime (counting the infinite prime). Jones and Roberts prove the following.

Theorem 1.3.1. *[17, Chapter 4]*

- $p = 101$ *is the smallest prime such that* $S_5 \in \pi_A(U_p)$*;*
- $p = 197$ *is the smallest prime such that* $S_6 \in \pi_A(U_p)$*;*
- $p = 163$ *is the smallest prime such that* $S_7 \in \pi_A(U_p)$*;*
- $p = 653$ *is the smallest prime such that* $A_5 \in \pi_A(U_p)$*;*
- $p = 1579$ *is the smallest prime such that* $A_6 \in \pi_A(U_p)$*.*

Extending our pool of examples for symmetric groups, Pollak gives a table which contains polynomials for all $n \leq 30$ of which the splitting fields are S_n-extensions of $\mathbb{Q}$ which ramify at a single finite prime. This proves the following result.

Theorem 1.3.2. *[27, Example 2.1.21] For all $n \in \mathbb{N}$ with $n \leq 30$ we can find a prime p such that the symmetric group S_n lies in $\pi_A(U_p)$.*

Pollak also provides examples of A_7, A_8, A_9 and A_{10} extensions of $\mathbb{Q}$ ramified at a single prime. In Chapter 5 we use the lmfdb [20] database as well as [11, GAP] to provide a list of groups G with cyclic abelianisation together with, for every group, a totally real number field K which ramifies at a single finite prime such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$. Because the extensions are totally real we know the infinite prime is not ramified and so these groups are examples of the Boston-Markin Conjecture. We proceed to illustrate a method which allows us to construct examples of the Boston-Markin Conjecture of order larger than 32.

Chapter 2

Prerequisites

In this chapter we provide the necessary background in algebraic number theory. Our results and methods heavily rely on Galois theory and the theory of number fields so a comprehensive guide to the required results of these fields is given. Many of our arguments are of a group theoretic nature so we start by providing a plethora of facts about groups. In some instances a direct proof is given, but more often a reference to a proof is provided.

2.1 Group theory

We start our prerequisites on group theory with a collection of fundamental results.

Theorem 2.1.1. *[7, Section 3.2, Theorem 8, Lagrange] Let G be a group and H any subgroup. Then the order of H divides the order of G*

Theorem 2.1.2. *[7, Sec. 3.2, Theorem 11, Cauchy] Let G be any group and p some prime dividing the order of G. Then there exists a subgroup H of G with order p.*

Theorem 2.1.3. *[7, Section 2.3, Theorem 7] Let G be a cyclic group of order n and d a divisor of n. Then G has exactly one subgroup of order d and this subgroup is again cyclic.*

Theorem 2.1.4. *[7, Section 3.3, Theorem 16, First Isomorphism Theorem] For any group morphism $\phi : G \to H$ the kernel $\ker(\phi)$ is normal in G and $G/\ker(\phi) \simeq \mathrm{im}(\phi)$.*

Theorem 2.1.5. *[7, Section 3.3, Theorem 19, Third Isomorphism Theorem] Let G be a group and H and K normal subgroups in G with $K \subset H$. Then H/K is normal in G/K and ${}^{G/K}\!/_{H/K} \simeq G/H$.*

Theorem 2.1.6. *[7, Section 3.3, Theorem 20, correspondence theorem] Let G be a group, $N \trianglelefteq G$ some normal subgroup and define $\bar{G} := G/N$. Then there is a bijection between the set of subgroups $A \subset G$ which contain N and the set of subgroups $\bar{A} \subset \bar{G}$ through the projection map $\pi : G \twoheadrightarrow G/N$. In particular every subgroup $\bar{A}$ of $\bar{G}$ is of the form A/N for some $A \subset G$ and furthermore we have that $\bar{A}$ is normal in $\bar{G}$ if and only if A is normal in G.*

Definition 2.1.7. Let G be a group. A **commutator** of G is an element of the form $ghg^{-1}h^{-1}$ for some $g, h \in G$. The **commutator subgroup** of G is the subgroup generated by all the commutators of G. We denote this subgroup by $[G, G]$. Furthermore, the **abelianisation** of G is the quotient group $G/[G, G]$ and we denote this by G^{ab}.

Proposition 2.1.8. *[7, Section 5.4, Proposition 7] Let G be a group. The abelianisation G^{ab} of G is an abelian group.*

Proposition 2.1.9. *Let G, H be finite groups. Then $(G \times H)^{\mathrm{ab}} \simeq G^{\mathrm{ab}} \times H^{\mathrm{ab}}$.*

Proof. For some element $x \in [G \times H, G \times H]$ we know that

$$\begin{aligned} x =& (g_1, h_1)(g_2, h_2)(g_1, h_1)^{-1}(g_2, h_2)^{-1} \\ =& (g_1, h_1)(g_2, h_2)(g_1^{-1}, h_1^{-1})(g_2^{-1}, h_2^{-1}) \\ =& (g_1 g_2 g_1^{-1} g_2^{-1}, h_1 h_2 h_1^{-1} h_2^{-1}). \end{aligned}$$

Here the latter is an element of $[G, G] \times [H, H]$, thus $[G \times H, G \times H] = [G, G] \times [H, H]$. Note that $(G \times H)^{\mathrm{ab}} := {}^{G \times H}\!/_{[G \times H, G \times H]}$ and $G^{\mathrm{ab}} \times H^{\mathrm{ab}} := G/[G, G] \times H/[H, H]$ and that we have the surjective morphism

$$\phi : G \times H \twoheadrightarrow G^{\mathrm{ab}} \times H^{\mathrm{ab}},$$

where ϕ maps a tuple (g, h) to $(g \pmod{[G, G]}, h \pmod{[H, H]})$. Since the kernel of ϕ is $[G, G] \times [H, H] = [G \times H, G \times H]$ we find with the First Isomorphism Theorem that

$$(G \times H)^{\mathrm{ab}} \simeq G^{\mathrm{ab}} \times H^{\mathrm{ab}}.$$

□

Proposition 2.1.10. *Let G and H be cyclic groups or respective orders n and m. Then the product of $G \times H$ is cyclic if and only if* $\gcd(n, m) = 1$.

Proof. Firstly, $|G \times H| = |G||H| = nm$, which means that $G \times H$ is cyclic if and only if it admits an element of order nm. Let g and h denote generators of G and H with orders n and m respectively. If $\gcd(n, m) = 1$ we know that g^m has order n and h^m has order n, which tells us that (g, h) has order nm in $G \times H$ proving the first implication.

Now suppose that $\gcd(n, m) > 1$ and let (g^i, h^j) be an arbitrary element of $G \times H$ for $i < n$ and $j < m$. Since

$$(g^i, h^j)^{\mathrm{lcm}(nm)} = ((g^i)^{\mathrm{lcm}(nm)}, (h^j)^{\mathrm{lcm}(nm)}) = (e, e)$$

and $\mathrm{lcm}(n, m) = \frac{nm}{\gcd(nm)} < nm$ we see that any element of $G \times H$ has an order strictly smaller than nm, which proves the other implication. □

Definition 2.1.11. Let N and H be groups and $\phi : H \to \mathrm{Aut}(N)$ be some group homomorphism. The **semi-direct product** of N and H with respect to ϕ is the group with $N \times H$ as an underlying set and the following composition. For (n_1, h_1) and (n_2, h_2) in $N \times H$ we define $(n_1, h_1) \cdot (n_2, h_2) := (n_1 \phi_{h_1}(n_2), h_1 h_2)$. We denote this group by $N \rtimes_\phi H$.

Remark 2.1.12. The direct product of two groups N and H is a special case of the semi direct product. If we consider $\phi : H \to \mathrm{Aut}(N)$ to be the trivial morphism which maps all $h \in H$ to the automorphism $\mathrm{id} : N \to N$ we see that the composition of the semi direct product is the same as the usual composition for the direct product.

Theorem 2.1.13. *[7, Section 7.4, Theorem 39, Schur-Zassenhaus] Let G be a finite group and $N \trianglelefteq G$ some normal subgroup. If the order of N is coprime to the order of G/N then $G \simeq N \rtimes G/N$.*

Theorem 2.1.14. *[12, arts. 90-91] The multiplicative group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is isomorphic to the product of the cyclic groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^{k-2})\mathbb{Z}$ of order 2^{k-1} for all $k \geq 2$.*

Lemma 2.1.15. *[14, Theorem 129] The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n is 1, 2, 4, p^k or $2p^k$ where p is an odd prime and $k > 0$. In general the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$ and so for odd primes p the group $(\mathbb{Z}/p^k\mathbb{Z})^\times$ has order*

$$\phi(p^k) = p^{k-1}(p-1) = p^k - p^{k-1}.$$

We will later see that p-groups play a big role in this thesis, so it is only right to introduce them properly.

Definition 2.1.16. A **p-group** is a group of order p^n for some $n \geq 0$.

Proposition 2.1.17. *[2, Theorem 7.2.8] Non-trivial p-groups have non-trivial centers.*

Lemma 2.1.18. *Let G be a non-trivial p-group of order p^n and let Z denote the center of G. Then G admits a normal subgroup $H \subset Z$ of order p.*

Proof. Since the center is a subgroup of G we find with the Theorem of Lagrange (2.1.1) that the order of the center divides the order of G. By Proposition 2.1.17 the center Z is a non-trivial subgroup and so its order is not 1. Since the order of G is p^n this means p divides the order of Z. By the Theorem of Cauchy (2.1.2) we know that Z admits a subgroup H of order p and since this H lies in the center of G it is normal in G. □

Theorem 2.1.19. *Let G be a p-group with order $|G| = p^n$. Then G admits a normal subgroup of order p^k for all $0 \leq k \leq n$.*

Proof. We will prove this by induction on k. Note that if $k = n$ there would be nothing to prove and so we can assume $k < n$. Firstly, for $k = 0$ we have the trivial subgroup or order p^0 which is indeed normal in G. Now, assuming that we have a normal subgroup of order p^k for some $0 \leq k < n$, we will show there is one of order p^{k+1} as well. Let $H \trianglelefteq G$ be such a normal subgroup of order p^k and consider the quotient group G/H whose order is $\frac{p^n}{p^k} = p^{n-k}$. Since $k < n$ we see that G/H is again a non-trivial p-group and so by Lemma 2.1.18 we see that G/H admits a normal subgroup, say $\overline{K}$, of order p. With the correspondence theorem (2.1.6) we know there is some normal subgroup $K \trianglelefteq G$ which is projected to $\overline{K}$ of order $p \cdot p^k = p^{k+1}$, since $\overline{K}$ was of order p and the projection map to the quotient is $p^k - \text{to} - 1$. □

Notation. Let G be some finite group and $g \in G$ some element. Then the order of g is denoted by $\text{ord}(g)$.

Definition 2.1.20. For a group G and a prime p let $p(G)$ denote the subgroup generated by all p-subgroups of G. We call $p(G)$ the **quasi-p part** of G and say that G is a **quasi p-group** if $G = p(G)$.

Lemma 2.1.21. *Let G be a group and $p(G)$ its quasi-p part. Let $G(p)$ denote the subgroup of G generated by all elements of order a power of p. Then $p(G) = G(p)$.*

Proof. First we consider a generator $x \in G(p)$ with a p-power order and we will show that $x \in p(G)$, since then all of $G(p) \subset p(G)$. The subgroup $\langle x \rangle \subset G$ has the same order as x and hence is a p-subgroup, which then contributes to generating $p(G)$ by definition. So $x \in p(G)$. Conversely, any generating element of $p(G)$ lies in some p-subgroup of G and hence has an order which divides the order of this p-subgroup, i.e. it has an order which is a power of p. So any generator of $p(G)$ is a generator of $G(p)$ which completes the proof. □

Definition 2.1.22. For a group G and subgroup H we say that H is **characteristic** in G if $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Lemma 2.1.23. *For a group G the quasi p-part of G is characteristic in G.*

Proof. We consider any p-subgroup and see that it must be mapped to any other p-subgroup of the same group under any automorphism. This means the generating set of $p(G)$ is permuted and so $p(G)$ is fixed under any $\sigma \in \mathrm{Aut}(G)$. □

Lemma 2.1.24. *Let G be a group and H some characteristic subgroup in G. Then H is normal in G.*

Proof. If a subgroup $H \subset G$ is fixed by any automorphism $\sigma \in G$ it is in particular fixed by the automorphism which, for some fixed $g \in G$, takes any $h \in G$ to ghg^{-1}. In other words, we have that $gHg^{-1} = H$ which means that H is normal in G. □

Combining Lemma's 2.1.23 and 2.1.24 gives the following corollary.

Corollary 2.1.25. *For a group G the quasi p-part of G is normal in G.*

Definition 2.1.26. Let G be a group. A **Sylow p-subgroup** H is a maximal p-subgroup, that is, there is no p-subgroup of G which strictly contains H.

Definition 2.1.27. Let G be a group and $S \subset G$ a subset. Then the **normaliser** $N_G(S)$ is defined as the following subgroup of G:

$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

Theorem 2.1.28. *[7, Section 4.5, Theorem 18, Sylow Theorems] Let G be a group and p a prime dividing $|G|$ with multiplicity n such that $|G| = p^n m$. Let n_p denote the number of Sylow p-subgroups of G.*

1. *There exists a Sylow p-subgroup of G with order p^n.*
2. *All Sylow p-subgroups are conjugate to each other.*
3. *(a) $n_p | m$*
   (b) $n_p \equiv 1 \pmod{p}$
   (c) For any Sylow p-subgroup P we have $n_p = |G : N_G(P)|$.

Corollary 2.1.29. *It follows from Item 2 of Theorem 2.1.28 that every Sylow p-subgroup has the same maximal size. Furthermore, saying that $n_p = 1$ is equivalent to saying that the Sylow p-subgroup is a normal subgroup by part c of Item 3. Finally, any p-subgroup will be contained in one of the Sylow p-subgroups due to their maximality.*

Proposition 2.1.30. *Let G be a finite group, p any prime dividing $|G|$ and $p(G)$ the quasi p-part of G. Then p does not divide the order of $G/p(G)$.*

Proof. Say the order of G is $|G| = p^k m$ for some $k \geq 0$ and $m \geq 1$ coprime to p. Then by Theorem 2.1.28 part 1 there exists a Sylow p-subgroup $H \subset G$ of order p^k. In particular this subgroup will also be a subgroup of $p(G)$ since it is part of the generating set as it is a p-group. By the Theorem of Lagrange (2.1.1) we find that the order of H divides the order of $p(G)$ and so the order of $p(G)$ contains a factor p^k, i.e. $|p(G)| = p^k l$ for some $l \geq 1$. Then we find that $|G/p(G)| = \frac{p^k m}{p^k l} = \frac{m}{l}$. Note that $\frac{m}{l} \in \mathbb{N}$, since $|p(G)|$ must divide $|G|$, again by Lagrange (2.1.1). Since m is taken to be coprime to p we have the desired result. □

Lemma 2.1.31. *Let G be a finite group. Then the order of $p(G)$ is a power of p if and only if G has exactly one Sylow p-subgroup.*

Proof. Assuming G has one Sylow p-subgroup, say H, then this H contains all p-subgroups of G and so $H = p(G)$ which means the order of $p(G)$ is a power of p and we are done. If on the other hand there are more Sylow p-subgroups, say H_i for some $1 \leq i \leq k$ with $k \geq 1$, then $p(G)$ will strictly contain all of them. Strictly, because we assume all H_i to be distinct and so whatever they generate will be strictly larger than any of them. But now the order of $p(G)$ cannot be a prime power since this would imply the existence of a p-subgroup of G which strictly contains a (or in fact all) Sylow p-subgroups. This would contradict the maximality of the H_i's. □

Lemma 2.1.32. *Let G be a finite group and N some normal subgroup. Then*

$$p(G)/p(N) \simeq p(G/p(N)).$$

Proof. We first show that $p(G)/p(N) \subset p(G/p(N))$ by showing that a generating set of $p(G)/p(N)$ is contained in $p(G/p(N))$. By Lemma 2.1.21 we know that a generating set of $p(G)$ is the collection of all elements $g \in G$ whose order is a power of p. It then follows that $p(G)/p(N)$ is generated by the classes $\bar{g} := g \pmod{p(N)}$ of these generators of $p(G)$. If the order of g is p^k then the order of $\bar{g}$ is p^l for some $l \leq k$ and so all these classes $\bar{g}$ are contained in $p(G/p(N))$ which concludes the first inclusion.

The inclusion $p(G/p(N)) \subset p(G)/p(N)$, is proved analogously by showing that a generating set of $p(G/p(N))$ is contained in $p(G)/p(N)$. Similar to above, $p(G/p(N))$ is generated by all classes $\bar{g} \in G/p(N)$ whose order is a power of p, say $\mathrm{ord}(\bar{g}) = p^k$. In order to show $\bar{g} \in p(G)/p(N)$, it is enough to find a representative of $\bar{g}$ whose order is also a power of p. Let g be some representative of $\bar{g}$. Because $\bar{g}^{p^k} = 1$ in $G/p(N)$ we know that $g^{p^k} \in p(N)$. Furthermore, the order of $\bar{g}$ divides the order of g, say $\mathrm{ord}(g) := m = p^l n$ where $\gcd(p^l, n) = 1$ and $l \geq k$. We now write $rp^l + sn = 1$ for integers r and s. Then $g^{sn} = g^{1-rp^l} = g \cdot g^{-rp^l}$ where $g^{-rp^l} \in p(N)$ because it is a power of g^{p^k} which already lies in $p(N)$. Hence g^{sn} and g differ by an element of $p(N)$ and so g^{sn} is also a representative of $\bar{g}$. Since $(g^{sn})^{p^l} = (g^{np^l})^s = 1$ we know that the order of g^{sn} must be a divisor of p^l and hence again a power of p as desired. This concludes the second inclusion. □

Lemma 2.1.33. *Let G be a group, $H \trianglelefteq G$ a normal subgroup and $K \subset H$ some characteristic subgroup in H. Then K is normal in G.*

Proof. Let $g \in G$. Because H is normal in G we already know that $gHg^{-1} = H$. But this means that the mapping $g \cdot g^{-1} : H \to H$, which maps some $h \in H$ to ghg^{-1}, is an automorphism of H, since the map $g^{-1} \cdot g : H \to H$ is its inverse. Because K is characteristic in H it is, by definition, fixed by any automorphism of H and so we find $gKg^{-1} = K$ as desired. □

Definition 2.1.34. A group G is said to admit a **subnormal series** of length n if it admits a series of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_n = G$$

such that G_i is normal in G_{i+1} for all i.

Definition 2.1.35. A group G is said to admit a **composition series** if it admits a subnormal series of finite length such that every G_i is a maximal proper normal subgroup of G_{i+1}. Equivalently we ask all quotients G_{i+1}/G_i to be simple.

Theorem 2.1.36. *[7, Section 3.4, Theorem 22, Jordan-Hölder] Any two composition series of a group have the same length and quotients up to permutation and isomorphism.*

Similar to p-groups, solvable groups will play a big role.

Definition 2.1.37. A group G is said to be **solvable** if it admits a subnormal series where all the quotients are abelian.

Lemma 2.1.38. *Let $G \neq 1$ be an abelian simple group. Then G is cyclic of prime order.*

Proof. Assume G to be infinite. Since G is simple we only have 1 and G as normal subgroups and since G is abelian we know that every subgroup will be normal. Because $G \neq 1$ there is some $1 \neq x \in G$ and by the above two comments we then know that $\langle x \rangle$ must either be trivial or all of G. We assumed $x \neq 1$ and so $G = \langle x \rangle$ is cyclic. In particular this means that x has infinite order. Again $\langle x^2 \rangle$ will be normal in G and so it will have to be 1 or all of G. Either scenario would imply that the order of x is finite even though we reasoned that the order of x must be infinite and so. We conclude that G must be finite and so that x must have a finite order. If $\text{ord}(x) = n$ for some composite n, then for any prime p which divides n we would get a proper non-trivial subgroup generated by x^p contradicting once again that there are no non-trivial subgroups. We conclude that G is cyclic and indeed of prime order. □

Lemma 2.1.39. *For a finite group G we can equivalently say that G is solvable if it admits a composition series all of whose quotients are cyclic and of prime order.*

Proof. Given a finite solvable group we know it admits a subnormal series (of finite length) where all the quotients are abelian. We can refine this subnormal series to a composition series by inserting normal subgroups. Note that the new quotients we obtain by inserting these groups stay abelian, because they are either subgroups of abelian groups or quotients of abelian groups. Now these quotients are abelian and simple and hence by Lemma 2.1.38 cyclic of prime order.

Conversely, if G admits a composition series where all quotients are cyclic (and of prime order) then they are in particular abelian and so G is solvable. □

Definition 2.1.40. Let G be any group. Then a **chief series** is a series of normal subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq .. \trianglelefteq G_n = G,$$

where $G_i \trianglelefteq G$ for all i and G_i is maximal in G_{i+1} with respect to all normal subgroups in G, i.e. there is no normal subgroup $H \trianglelefteq G$ such that $G_i \subset H \subset G_{i+1}$. We call the quotients G_{i+1}/G_i chief factors

Lemma 2.1.41. *[22, Lemma 9.1.8] Every finite group G admits a chief series.*

Lemma 2.1.42. *[22, Lemma 9.1.10] Let G be a group which admits a chief series and $N \trianglelefteq G$ some normal subgroup. Then we can find a chief series with N in it.*

Lemma 2.1.43. *[29, Page 4] Let G be any group and*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq .. \trianglelefteq G_n = G$$

a chief series for G. If a chief factor G_{i+1}/G_i is solvable it is a vector space over $\mathbb{Z}/p_i\mathbb{Z}$ for some prime p_i.

Theorem 2.1.44. *[19, Lemma, p.439] Let G be group which admits a chief series. Then the chief factors are unique up to isomorphism, independent of the particular series that they are constructed from.*

Lemma 2.1.45. *Let G be a finite solvable group and $N \trianglelefteq G$ some non-trivial normal subgroup. Then there exists a subgroup $H \subset N$ which is normal in G, such that the quotient N/H is of the form $(\mathbb{Z}/p\mathbb{Z})^n$ for some prime p and $n \geq 1$.*

Proof. Because G is finite we find it has a chief series with Lemma 2.1.41 and so, with Lemma 2.1.42, we find a chief series where N is one of the terms, say

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq .. \trianglelefteq N = G_i \trianglelefteq .. \trianglelefteq G_n = G.$$

We claim that $H := G_{i-1}$ will work and so consider the quotient N/H. Since G is solvable, we know that N is solvable and hence any quotient of N is also solvable. With Lemma 2.1.43 we then know that N/H is a $\mathbb{Z}/p\mathbb{Z}$-vector space for some prime p. Since G is finite, N and any quotient of N will also be finite, so N/H is a finite vector space over $\mathbb{Z}/p\mathbb{Z}$, which means it has to be of the form $(\mathbb{Z}/p\mathbb{Z})^n$ where n is the dimension of N/H as a vector space. Note that N/H is non-trivial, i.e. $n \geq 1$, since N is non-trivial and we take H to be a proper subgroup of N. □

Theorem 2.1.46. *[10, Feit-Thompson] Every finite group of odd order is solvable.*

Theorem 2.1.47. *[7, Section 19.2, Theorem 1, Burnside] If G is a finite group of order $p^a q^b$ for primes p and q and $a, b \geq 0$ then G is solvable.*

Theorem 2.1.48. *[28, Chapter 5] Let G and K be two groups, $H \subset G$ any subgroup and $N \trianglelefteq G$ any normal subgroup.*

- *If G is solvable H is solvable;*
- *If G solvable and there is a homomorphism $G \twoheadrightarrow K$ onto K then K is also solvable;*
- *Equivalently with the previous (due to the First Isomorphism Theorem), if G solvable then so is G/N;*
- *G is solvable if and only if N is solvable and G/N is solvable;*
- *If G and K are solvable so is $G \times K$;*

2.2 Number fields

Given a field extension L/K we can consider L as a K-vector space. Therefore, we can speak of the dimension of L as a K-vector space.

Definition 2.2.1. Let L/K be a field extension. We say that L is a **finite** extension of K if L is finite-dimensional as a K-vector space. The dimension of L over K is called the **degree** of L over K and we denote this by $[L : K]$.

Lemma 2.2.2. *[3, Corollary 6.4.3] Let L/K be a finite extension of fields. Then there exists a finite number of $\alpha_1, .., \alpha_n \in L$ such that $L = K(\alpha_1, .., \alpha_n)$. Assume the α_i's to be a minimal generating set and let d_i be the degree of α_i over K for $1 \leq i \leq n$. Then the degree is bounded as $[L : K] \leq d_1 \cdot .. \cdot d_n$. In particular, if $\gcd(d_i, d_j) = 1$ for all $i \neq j$ we have $[L : K] = d_1 \cdot .. \cdot d_n$.*

Definition 2.2.3. A **number field** K is a finite extension of $\mathbb{Q}$. We say that K is a non-trivial number field if it is not $\mathbb{Q}$ itself or, equivalently, if $[K : \mathbb{Q}] > 1$. A subring of K is called a **number ring**.

By Lemma 2.2.2 a number field is a field extension of $\mathbb{Q}$ of the form $\mathbb{Q}(\alpha_1, .., \alpha_n)$ for some $\alpha_i \in \mathbb{C}$. However, a number field can be represented in a much simpler form as Corollary 2.2.9 indicates.

Definition 2.2.4. Let K be a field. An extension L/K of fields is said to be **simple** if $L = K(x)$ for some $x \in L$.

Definition 2.2.5. Let K be a field and $f \in K[X]$ a monic polynomial of degree $n > 0$. A field extension L of K is called a **splitting field** of f over K if

- There exist $x_1, .., x_n \in L$ such that $f = \prod_{i=1}^{n}(X - x_i)$ and
- $L = K(x_1, .., x_n)$.

Definition 2.2.6. Let L/K be a finite field extension. Then an element $x \in L$ is called **separable** over K if its minimal polynomial $f \in K[X]$ has no multiple zeros in a splitting field of f. The extension L is called separable over K if every element is separable. The element x is called **inseparable** if f has x as a multiple zero.

Theorem 2.2.7. *[3, Theorem 9.4.1] Let L/K be a finite and separable field extension, say $L = K(\alpha_1, .., \alpha_r)$. Then the following hold:*

1. *There are only finitely many intermediate fields.*
2. *L is a simple extension, i.e. $L = K(\alpha)$.*

Proposition 2.2.8. *[3, Proposition 8.3.5] Let L/K be a finite field extension and $x \in L$ with f its minimal polynomial over K. Then x is inseparable over K if and only if K has positive characteristic and the derivative of f is identically zero.*

We see from Proposition 2.2.8 that every extension of $\mathbb{Q}$ is separable, since $\mathbb{Q}$ has characteristic zero. Combining Theorem 2.2.7 with the fact that number fields are finite extensions of $\mathbb{Q}$ we get the following already mentioned result.

Corollary 2.2.9. *All number fields are simple extensions of $\mathbb{Q}$.*

The integers $\mathbb{Z}$ form a subring of $\mathbb{Q}$ with many nice properties. The field of fractions of $\mathbb{Z}$ is equal to $\mathbb{Q}$ and $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. Furthermore, $\mathbb{Z}$ is a Noetherian ring, which means it satisfies the ascending chain condition on ideals and it has Krull dimension 1, which is to say that every non-zero prime ideal is a maximal ideal. Such well-behaved rings have been given the name of a **Dedekind domain** and it turns out every number field has a Dedekind domain as a subring, which is constructed out of $\mathbb{Z}$.

Definition 2.2.10. A **Dedekind domain** A is a ring which is a domain that is not a field for which one of the following equivalent conditions holds:

1. Every non-zero proper ideal $I \subset A$ factors into prime ideals $I = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$ where the $\mathfrak{p}_i \subset A$ are distinct for all i;
2. The ring A is Noetherian and the localisation at each maximal ideal is a discrete valuation ring;

3. Every non-zero fractional ideal is invertible;

4. The ring A is integrally closed in its field of fractions, Noetherian and of Krull dimension 1 (every non-zero prime is maximal);

5. For any two ideals I, J we have that $I \subset J$ if and only if J divides I as ideals, i.e. there exists an ideal H such that $I = JH$.

Definition 2.2.11. Let K be a number field. We call the integral closure of $\mathbb{Z}$ inside K the **ring of integers** of K and we will denote this by $\mathcal{O}_K$.

Proposition 2.2.12. *[33, Theorem 3.20] The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.*

Indeed, a Dedekind domain has far more characterisations and more information can be found in [1, Chapter 9]. We will primarily be interested in the ideal factorisation mentioned in Condition 1 of Definition 2.2.10. It can be shown that this factorisation is unique up to ordering of factors. In particular, we want to look at the setting where we have some number field K and a prime ideal $p\mathbb{Z} \subset \mathbb{Z}$ for some prime number p. Since $\mathbb{Z} \subset \mathcal{O}_K$ we can consider $p\mathcal{O}_K$, which is the ideal generated by p in the ring of integers $\mathcal{O}_K$. This new ideal need not be a prime ideal, but we know with Proposition 2.2.12 that it will uniquely decompose as a product of prime ideals, i.e. $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$ for distinct primes $\mathfrak{p}_i \subset \mathcal{O}_K$. We say that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ **lies over** a prime number $p \in \mathbb{Z}$ if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Lemma 2.2.13. *Let K be a number field with ring of integers $\mathcal{O}_K$ and p some rational prime. The primes $\mathfrak{p} \subset \mathcal{O}_K$ lying over p are exactly those which appear in the decomposition of $p\mathcal{O}_K$.*

Proof. Let $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$ for distinct primes $\mathfrak{p}_i \subset \mathcal{O}_K$. Then $p\mathbb{Z} \subset p\mathcal{O}_K \subset \mathfrak{p}_i$ for all i. From this we find that $p\mathbb{Z} \subset \mathfrak{p}_i \cap \mathbb{Z}$ where the latter is again an ideal from $\mathbb{Z}$ (even a prime ideal although we do not need this). Now note that $\mathbb{Z}$ is a Dedekind domain and hence all primes are maximal. Since $p\mathbb{Z}$ is prime in $\mathbb{Z}$, hence maximal, and $p\mathbb{Z} \subset \mathfrak{p}_i \cap \mathbb{Z}$, we conclude that $p\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$. Now consider some prime $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Then $p\mathcal{O}_K \subset \mathfrak{p}$ and since we have a decomposition $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$ we find that $\mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r} \subset \mathfrak{p}$. Because $\mathfrak{p}$ is a prime ideal we find that $\mathfrak{p}_i \subset \mathfrak{p}$ for some i and, again, by $\mathcal{O}_K$ being a Dedekind domain and primes being maximal we have equality. □

We introduce some terminology for the different decomposition patterns of primes which can occur in an extension of number fields. In particular, we define what it means for a prime $p \in \mathbb{Z}$ to ramify in a number field K. We also explain what we mean by the infinite primes of a number field and what it means for them to ramify.

Definition 2.2.14. Let L/K be an extension of number fields and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime in K such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$. We say the $\mathfrak{p}_i$ have **ramification degrees** e_i and **inertia degrees** $f_i := [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}]$.

We have the following fundamental identity.

Proposition 2.2.15. *[33, Theorem 3.4] Let L/K be a separable extension and $\mathfrak{p} \subset \mathcal{O}_K$ a prime in K which decomposes in $\mathcal{O}_L$ as $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$. Then*

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

Definition 2.2.16 discusses the possible ways in which a prime can decompose in an extension of number fields. In the rest of this thesis we will be working primarily with the case where the base field K is $\mathbb{Q}$ and $\mathfrak{p}$ is some prime $p \in \mathbb{Z}$.

Definition 2.2.16. Again, let L/K be an extension of number fields and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime in K such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$. The ideal $\mathfrak{p}_i$ is called **unramified** over K if $e_i = 1$ and if the residue class field extension $\mathcal{O}_L/\mathfrak{p}_i \big/ \mathcal{O}_K/\mathfrak{p}$ is separable. Note that by [24, Proposition 8.4] we never have to worry about the separability condition in the definition of $\mathfrak{p}_i$ being unramified, hence we only need to consider whether $e_i = 1$. If $e_i \neq 1$, we say $\mathfrak{p}_i$ is **ramified** and **totally ramified** if furthermore $f_i = 1$.

We say that a prime $\mathfrak{p}$ in K is unramified if all $\mathfrak{p}_i$ lying over it are unramified and it is called ramified otherwise. Furthermore, we say $\mathfrak{p}$ is totally ramified if $r = 1$ and the unique prime $\mathfrak{p}_i$ lying over $\mathfrak{p}$ is totally ramified. We see with Proposition 2.2.15 that in the case of total ramification we can equivalently say $e_i = [L : K]$. It is possible that $\mathfrak{p}$ stays prime, i.e. that $\mathfrak{p}\mathcal{O}_L$ is the unique prime above $\mathfrak{p}$ and in this case we call $\mathfrak{p}$ **inert**. Furthermore, $\mathfrak{p}$ is said to **split completely** or is **totally split** if $r = n = [L : K]$ and so $e_i = f_i = 1$ for all i. We call $\mathfrak{p}$ **nonsplit** if $r = 1$, i.e. if there is a single prime ideal lying over $\mathfrak{p}$.

The extension L/K is called unramified if all primes $\mathfrak{p}$ of K are unramified in L and it is called ramified if there is a ramified prime. Furthermore, the extension is totally ramified is there is a totally ramified prime. Finally, we say that a ramified prime $\mathfrak{p}_i$ is **tamely ramified** if e_i is not divisible by the prime p over which $\mathfrak{p}$ lies, i.e. the prime number which satisfies $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We call $\mathfrak{p}_i$ **wildy ramified** otherwise.

For a number field K we can compute a numerical invariant called the **discriminant** of K which tells us exactly which primes ramify. To define the discriminant properly we need the following proposition.

Proposition 2.2.17. *[33, Theorem 4.8] Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module and therefore admits a basis. For some $k \geq 1$ we find a basis $x_1, .., x_k \in \mathcal{O}_K$ such that any $x \in \mathcal{O}_K$ can be uniquely written as*

$$x = \sum_{i=1}^{k} n_i x_i,$$

with $n_i \in \mathbb{Z}$.

For some $x \in \mathcal{O}_K$, we consider the multiplication map $M_x : \mathcal{O}_K \to \mathcal{O}_K$ which takes any $y \in \mathcal{O}_K$ to yx. Proposition 2.2.17 tells us that $\mathcal{O}_K$ admits a $\mathbb{Z}$-basis and given such a basis we can express this map by an $n \times n$-matrix which we will also denote as M_x.

Definition 2.2.18. Let K be a number field, $\mathcal{O}_K$ its ring of integers and $x_1, .., x_k \in \mathcal{O}_K$ an integral basis for $\mathcal{O}_K$. Given some $x \in \mathcal{O}_K$ we define the **trace** of x to be $\mathrm{Tr}(x) := \mathrm{Trace}(M_x)$.

Definition 2.2.19. Let K be a number field, $\mathcal{O}_K$ its ring of integers and $x_1, .., x_k \in \mathcal{O}_K$ an integral basis for $\mathcal{O}_K$. Then the **discriminant** Δ_K of $\mathcal{O}_K$ is defined to be

$$\Delta_K := \det(\mathrm{Tr}(x_i x_j))_{i,j=1}^{n}.$$

Theorem 2.2.20. *[33, Theorem 4.14] A rational prime p ramifies in some number field K if and only if it divides the discriminant Δ_K.*

In particular this tells us that ramification is a rare occurrence:

Proposition 2.2.21. *Let K be a number field. Then there are only finitely many primes which ramify in K.*

Even though at most finitely many primes ramify we do know that there is always at least one prime which ramifies.

Theorem 2.2.22. *[24, III, Theorem 2.17, Minkowski] For a non-trivial number field K the discriminant is unequal to ± 1.*

An immediate corollary is that non-trivial number fields must have a ramifying prime, since there must be some prime number dividing the discriminant.

Corollary 2.2.23. *There are no non-trivial unramified extensions of $\mathbb{Q}$.*

A useful computational tool is that the ramification and inertia degrees are multiplicative in towers of number fields.

Lemma 2.2.24. *[35, Proposition 52] Let L/K be an extension of number fields with their respective rings of integers $\mathcal{O}_K \subset \mathcal{O}_L$ and let p be some rational prime. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal lying over $p\mathbb{Z}$ with ramification degree $e_{\mathfrak{p}/p}$ and residue degree $f_{\mathfrak{p}/p}$. Let $\mathfrak{q} \subset \mathcal{O}_L$ a prime ideal lying over $\mathfrak{p}$ with ramification degree $e_{\mathfrak{q}/\mathfrak{p}}$ and residue degree $f_{\mathfrak{q}/\mathfrak{p}}$. Then the ramification and residue degrees are multiplicative in the sense that*

$$e_{\mathfrak{q}/p} = e_{\mathfrak{q}/\mathfrak{p}} \cdot e_{\mathfrak{p}/p};$$
$$f_{\mathfrak{q}/p} = f_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{p}/p}.$$

An immediate corollary is that ramification is preserved in extensions.

Corollary 2.2.25. *Let L/K be an extension of number fields and p a rational prime which ramifies in K. Then p also ramifies in L.*

We conclude this section with two results on number fields where only a single rational prime ramifies.

Lemma 2.2.26. *Let K be a number field which ramifies at a single prime p and let K_0 be some non-trivial subextension of $\mathbb{Q}$. Then K_0 also ramifies only at p.*

Proof. Firstly, if some prime ramifies in K_0 it will also ramify in K by Corollary 2.2.25. Hence, no other prime than p can ramify. Because K_0 is non-trivial we also know that some rational prime has to ramify in K_0 by Corollary 2.2.23. We conclude that p and only p must ramify in K_0. □

Lemma 2.2.27. *Let K be a number field which is only ramified over a single rational prime p and assume additionally that it is totally ramified over p. Let K_0 be some intermediate extension and $\mathfrak{q}$ a prime lying over p in K_0. Then K_0 is also totally ramified over p and K is totally ramified over $\mathfrak{q}$.*

Proof. By Lemma 2.2.26 we know that K_0 must also ramify at the prime p and no other prime. Furthermore, p is totally ramified in K and by definition of total ramification it only has a single prime lying over it. Since $p\mathcal{O}_K = (p\mathcal{O}_{K_0})\mathcal{O}_K$ we can be sure that p only has one prime lying over it in K_0 as well. Say $p\mathcal{O}_K = \mathfrak{p}^{e_{\mathfrak{p}/p}}$ with residue degree $f_{\mathfrak{p}/p}$

and $p\mathcal{O}_{K_0} = \mathfrak{q}^{e_{\mathfrak{q}/p}}$ with residue degree $f_{\mathfrak{q}/p}$. By Proposition 2.2.15 we already know that $[K_0 : \mathbb{Q}] = e_{\mathfrak{q}/p} f_{\mathfrak{q}/p}$ and $[K : K_0] = e_{\mathfrak{p}/\mathfrak{q}} f_{\mathfrak{p}/\mathfrak{q}}$ so all we need to prove is that $f_{\mathfrak{q}/p} = 1$ and $f_{\mathfrak{p}/\mathfrak{q}}$=1 in order to conclude that K_0 and K are totally ramified. But with the multiplicativity of residue degrees as in Lemma 2.2.24 we have that $1 = f_{\mathfrak{p}/p} = f_{\mathfrak{p}/\mathfrak{q}} f_{\mathfrak{q}/p}$ and so $f_{\mathfrak{q}/p}$ and $f_{\mathfrak{p}/\mathfrak{q}}$ both have to be 1.

□

We now know what it means for a prime $p \in \mathbb{Z}$ to ramify in a number field K and also when this happens. However, there is another type of "prime" to consider.

Definition 2.2.28. Let K be a number field.

- An **archimedean place** of K is either a real embedding $\phi : K \to \mathbb{R}$ (an embedding of K in $\mathbb{C}$ whose image $\phi(K)$ lies in $\mathbb{R}$) or a pair of complex embeddings $(\psi, \bar{\psi})$ with $\psi \neq \bar{\psi}$ and $\psi : K \to \mathbb{C}$).
- A **non-archimedean place** of K is a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.

The archimedean places are also referred to as the **infinite primes** of K and the non-archimedean ones as the **finite primes** of K. We also say an archimedean place is **real** or **complex** depending on whether the image of the corresponding embedding is respectively real or complex.

Definition 2.2.29. Let L/K be an extension of number fields. Let $\phi : K \to \mathbb{C}$ be some embedding (with real or complex image) and let $\sigma : L \to \mathbb{C}$ be an embedding such that $\sigma \mid_K = \phi : K \to \mathbb{C}$. We say that σ **extends** or **lies over** ϕ.

Given an extension of number fields L/K there is also a notion of ramification for real archimedean places of K.

Definition 2.2.30. Let L/K be an extension of number fields and $\phi : K \to \mathbb{R}$ a real archimedean place. We say that ϕ **ramifies** in L if there exists a complex archimedean place $\sigma : L \to \mathbb{C}$ which extends ϕ. We say that ϕ is **unramified** if every place that lies over ϕ is real.

Proposition 2.2.31. *[8, Page 42] Let K be a number field of degree n with r real embeddings and s pairs of conjugate complex embeddings into $\mathbb{C}$. Then $n = r + 2s$.*

Proposition 2.2.31 gives us a handle on working out how many real archimedean places a number field K has. In particular, since that the degree of $\mathbb{Q}$ is 1, Proposition 2.2.31 tells us that $\mathbb{Q}$ has only one archimedean place and it is real.

Corollary 2.2.32. *There is only one infinite prime for $\mathbb{Q}$ and we refer to it as ∞.*

For a number field K we will want to determine which primes of $\mathbb{Q}$ ramify, including the prime at infinity. From now on, we will refer to ramification in K of a prime $p \in \mathbb{Z}$ as ramification of a **rational** or **finite** prime to avoid confusion with ramification of the infinite prime.

2.3 Galois theory

Definition 2.3.1. Let L/K be a field extension and $x \in L$. We say x is **algebraic** over kK if there is some monic polynomial $f \in K[X]$, such that $f(x) = 0$. The extension is said to be algebraic if all $x \in L$ are algebraic over K.

Definition 2.3.2. Let K be a field. We say K is **algebraically closed** if every non-constant polynomial in $K[X]$ has a root in K. An **algebraic closure** of K is an algebraic extension which is algebraically closed. We denote this by $\bar{K}$.

Definition 2.3.3. Let L/K be a field extension. The set of field automorphisms of L form a group, which we denote by $\mathrm{Aut}(L)$. It has a subgroup, which consists of those automorphisms $\sigma \in \mathrm{Aut}(L)$ such that $\sigma(x) = x$ for all $x \in K$. We call this subgroup the **Galois group** of the extension L/K and denote it by $\mathrm{Aut}(L/K)$.

Theorem 2.3.4. *[3, Theorem 8.3.1] Let L/K be a finite field extension. Then the order of the Galois group is bounded by the degree of the extension, i.e. $|\mathrm{Gal}(L/K)| \leq [L : K]$. Moreover, if $|\mathrm{Gal}(L/K)| = [L : K]$ then every irreducible polynomial $f \in K[X]$ with a zero in L contains precisely $\deg(f)$ distinct zeros in L.*

Definition 2.3.5. Let L/K be a finite field extension. We say that L/K is a **Galois extension** if $|\mathrm{Gal}(L/K)| = [L : K]$. In this case we denote the Galois group by $\mathrm{Gal}(L/K)$.

As we will see in Proposition 2.3.7 there are a few more ways to characterise a Galois extension.

Definition 2.3.6. Let L/K be a finite field extension. Then L is called **normal** over K if every irreducible polynomial in $K[X]$ with a zero in L has all of its zeros in L.

Proposition 2.3.7. *[3, Theorem 8.3.6] Let L/K be a finite extension. Then the following three conditions are equivalent.*

1. $|\mathrm{Gal}(L/K)| = [L : K]$;
2. *L/K is a normal and separable extension;*
3. *L is a splitting field over K of a polynomial $f \in K[X]$ with distinct zeros.*

Definition 2.3.8. Let K be a field and $f \in K[X]$ a polynomial of degree n. Let $x_1, .., x_n$ denote the n roots of f in some algebraic closure $\overline{K}$ of K. We define the Galois group of f to be the Galois group of the extension $K(x_1, .., x_n)/K$. The extension is Galois and we denote it by $\mathrm{Gal}(f)$.

Given a Galois extension, we find a correspondence between intermediate fields of the extension and subgroups of the Galois group as described in Theorem 2.3.10.

Definition 2.3.9. Let L/K be a field extension and $H \subset \mathrm{Gal}(L/K)$ a subgroup of the corresponding Galois group. Then the **fixed field** of L under H is the intermediate field of the extension given by the set

$$\{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}.$$

We denote this by L^H.

Theorem 2.3.10. *[3, Theorem 9.2.1, Galois Correspondence] Let L/K be a Galois extension with Galois group $G := \mathrm{Gal}(L/K)$. Then there is a map from the set of intermediate fields of the extension to the set of subgroups of G. This map, which sends an intermediate field M to the Galois group $\mathrm{Gal}(L/M)$, is an inclusion reversing bijection with the inverse mapping some subgroup $H \subset G$ to the fixed field L^H of L under H.*

Let L/K be a Galois extension and M an intermediate field $K \subset M \subset L$. Note that L is the splitting field over K of some polynomial $f \in K[X]$ with distinct zeros. Since $K \subset M$, we can also view f as a polynomial in $M[X]$ and just as well say that L is a splitting field of f over M. This allows us to conclude that L/M is also a Galois extension, but in general M need not be Galois over K as well.

Theorem 2.3.11. *[3, Theorem 9.2.2] Let L/K be a finite Galois extension. Then an intermediate extension M with $K \subset M \subset L$ is normal over K if and only if $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. Moreover, we can compute the corresponding Galois group as*

$$\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

If L/K is a Galois extension it is in particular separable by condition 2 of Proposition 2.3.7. By definition this means every element in L is separable over K, but then also every element in M is separable over K, so M/K is also separable. We conclude that the criterion of Theorem 2.3.11 that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$ is enough to say that M/K is a Galois extension.

Definition 2.3.12. Let L and M be fields. We define the **compositum** of L and M to be the smallest field which contains both L and M and denote it by LM.

Proposition 2.3.13. *[7, Section 14.4, Proposition 19] Let L/K be a Galois extension and K'/K any extension. Then the compositum LK' of L and K' is Galois over K' with Galois group $\mathrm{Gal}(LK'/K') \simeq \mathrm{Gal}(L/L \cap K')$.*

Corollary 2.3.14. *[7, Section 14.4, Corollary 20] Let L/K be a Galois extension and K'/K any finite extension. Then*

$$[LK' : K] = \frac{[L : K][K' : K]}{[L \cap K' : K]}.$$

Proposition 2.3.15. *[7, Section 14.4, Proposition 21] Let L_1 and L_2 be Galois extensions of a field K Then:*

1. *The intersection $L_1 \cap L_2$ is Galois over K;*
2. *The compositum L_1L_2 is Galois over K. The Galois group $\mathrm{Gal}(L_1L_2/K)$ is isomorphic to the subgroup*

$$H = \{(\sigma, \tau) \mid \sigma_{L_1 \cap L_2} = \tau_{L_1 \cap L_2}\}$$

of the direct product $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Corollary 2.3.16. *[7, Section 14.4, Corollary 22] Let L_1 and L_2 be Galois extensions of a field K such that $L_1 \cap L_2 = K$. Then*

$$\mathrm{Gal}(L_1L_2/K) \simeq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

Conversely, if L/K is a Galois extension whose Galois group G is the direct product of two subgroups of G, say $G = \mathrm{Gal}(L/K) \simeq G_1 \times G_2$, then L is the compositum of two Galois extensions L_1/K and L_2/K with $L_1 \cap L_2 = K$.

Definition 2.3.17. Let $n \geq 1$. The complex roots of the polynomial $x^n - 1$ are called the $\mathbf{n^{th}}$ **roots of unity**.

The n^{th} roots of unity are of the form $e^{\frac{2\pi ik}{n}}$ for all $1 \leq k < n$ and they form a cyclic group under multiplication.

Definition 2.3.18. Let $n \geq 1$. A generator of the cyclic group of n^{th} roots of unity is called a **primitive root of unity** and we will denote such a generator by ζ_n.

All primitive n^{th} roots of unity can be obtained by taking powers of a primitive n^{th} root of unity ζ_n^k for all $1 \leq k < n$ with $\gcd(k, n) = 1$.

Definition 2.3.19. We define the n^{th} **cyclotomic polynomial** to be

$$\Phi_n = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} (x - \zeta_n^k).$$

It can be shown that Φ_n is irreducible over $\mathbb{Q}$ and hence the minimal polynomial of ζ_n over $\mathbb{Q}$. Its roots are exactly the primitive n^{th} roots of unity and its degree is $\phi(n)$, i.e. Euler's totient function which counts the positive integers up to n which are coprime to n. Therefore we also have that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$.

Definition 2.3.20. We define $\mathbb{Q}(\zeta_n)$ to be the n^{th} **cyclotomic field**.

Note that ζ_n generates all the n^{th} roots of unity and that all these roots are distinct. Therefore, we see that $\mathbb{Q}(\zeta_n)$ is the splitting field of $f = x^n - 1$, which means it is a Galois extension over $\mathbb{Q}$.

Proposition 2.3.21. *[7, Section 14.5, Theorem 26] The Galois group* $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to* $(\mathbb{Z}/n\mathbb{Z})^\times$.

The set $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of those $1 \leq k < n$ for which $\gcd(k, n) = 1$. Any automorphism in $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is defined on the generator ζ_n by mapping it to some power ζ_n^k for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism of Proposition 2.3.21 takes any such automorphism and maps it to k.

Proposition 2.3.22. *[36, Proposition 2.7] For* $n > 2$ *the discriminant of* $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *is*

$$(-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}},$$

which implies that all the finite primes not dividing n *are unramified in this extension. If* n *is a power of a prime* p *then* p *is totally ramified in this extension.*

Proposition 2.3.23. *Let* $n = p_1^{a_1} \cdot .. \cdot p_k^{a_k}$ *The group* $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to*

$$\text{Gal}(K_1/\mathbb{Q}) \times .. \times \text{Gal}(K_k/\mathbb{Q}),$$

where K_i *denotes* $\mathbb{Q}(\zeta_{p_i^{a_i}})$.

Proof. Let

$$n_i := \prod_{\substack{i \neq j \\ 1 \leq j \leq k}} p_j^{a_j}.$$

Then for each $1 \leq i \leq k$ we have that $\zeta_n^{n_i}$ is a primitive $p_i^{a_i}$-th root of unity and so

$$K_i := \mathbb{Q}(\zeta_{p_i^{a_i}}) \subset \mathbb{Q}(\zeta_n).$$

Furthermore, any field L which contains K_i for all i also contains $\zeta_{p_1^{a_1}} \cdot .. \cdot \zeta_{p_k^{a_k}}$ which is a primitive n^{th} root of unity and so L also contains $\mathbb{Q}(\zeta_n)$. Hence, $\mathbb{Q}(\zeta_n)$ is the smallest field containing all K_i which means the compositum of all K_i is $\mathbb{Q}(\zeta_n)$. It only remains to show that $\cap_i K_i = \mathbb{Q}$, for which we argue using degrees. For each i we have $[K_i : \mathbb{Q}] = \phi(p_i^{a_i})$ and since $\phi(n) = \phi(p_1^{a_1}) \cdot .. \cdot \phi(p_k^{a_k})$ we see that the degree of the composite field over $\mathbb{Q}$ is exactly the product of the individual degrees of each K_i over $\mathbb{Q}$. Using Corollary 2.3.14 and an inductive argument gives us that

$$[\prod_i K_i : \mathbb{Q}] = \frac{\prod_i [K_i : \mathbb{Q}]}{[\cap_i K_i : \mathbb{Q}]} = \frac{\phi(p_1)^{a_1} \cdot .. \cdot \phi(p_k)^{a_k}}{[\cap_i K_i : \mathbb{Q}]}.$$

We know that the left hand side is the same as $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = \phi(p_1)^{a_1} \cdot .. \cdot \phi(p_k)^{a_k}$ and so we can conclude that $[\cap_i K_i : \mathbb{Q}] = 1$ which means that $\cap_i K_i = \mathbb{Q}$. Using Corollary 2.3.16 we now have the desired isomorphism. □

Lemma 2.3.24. *Let $n > 2$. The subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$ and real with $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. We call this subfield the* ***maximal real subfield*** *of $\mathbb{Q}(\zeta_n)$.*

Proof. Since $n > 2$ we know that $\mathbb{Q}(\zeta_n)$ is not real. Furthermore, Since ζ_n lies on the complex unit circle, we know that ζ_n^{-1} is the same as the conjugate of ζ_n. This means that $\zeta_n + \zeta_n^{-1}$ is real and so $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is a real subfield. Because $\mathbb{Q}(\zeta_n)$ itself is not real, this tells us that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \geq 2$. To show it is exactly 2 we determine the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. We consider the polynomial

$$f = x^2 - (\zeta_n + \zeta_n^{-1})x + 1,$$

which splits as $(x - \zeta_n)(x - \zeta_n^{-1})$ over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$. We see that ζ_n is a root of f and since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \geq 2$, we know that f is the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Hence we know $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. To see $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is Galois over $\mathbb{Q}$ we note that

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})) \subset \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

The latter group is abelian which implies that every subgroup is normal and so Theorem 2.3.11 tells us that $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is Galois over $\mathbb{Q}$.

□

Definition 2.3.25. A Galois extension of $\mathbb{Q}$ is said to be **abelian** if the corresponding Galois group is abelian.

Example 2.3.26. Cyclotomic extensions $\mathbb{Q}(\zeta_n)$ are abelian since Proposition 2.3.21 tells us they have Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Given multiple abelian extensions $K_1, .., K_k$ we can also say that their compositum is again an abelian extension. This is because, by Proposition 2.3.15, the Galois group of the composite will be a subgroup of the direct product of the respective Galois groups, which are all abelian and so the direct product and any subgroup of it will also be.

We already saw in the proof of Lemma 2.3.24 that any intermediate field M of an abelian extension $K/\mathbb{Q}$ is again Galois over $\mathbb{Q}$. In fact, we can say that M is again an abelian extension, since Theorem 2.3.11 tells us that $\text{Gal}(M/\mathbb{Q}) \simeq G/H$ which is the quotient of an abelian group. In particular, any intermediate field of a cyclotomic extension is again an abelian extension of $\mathbb{Q}$. The Theorem of Kronecker-Weber tells us that any abelian extension is of this form.

Theorem 2.3.27 (Kronecker-Weber)**.** *Every abelian extension K of $\mathbb{Q}$ is a subfield of some cyclotomic field $K \subset \mathbb{Q}(\zeta_n)$ for some $n \geq 1$.*

Remark 2.3.28. It is shown in [24, Theorem 1.10] that the n in Theorem 2.3.27 is a composite $n = \prod p^{e_p}$ for $e_p \geq 1$ of exactly all the rational primes p which ramify in K.

In practice we will be working with number fields K that are also Galois over $\mathbb{Q}$. This additional assumption has some simplifying implications for the decomposition of rational primes in K.

Proposition 2.3.29. *[24, Proposition 9.1] Let L/K be a Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. Furthermore, let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal and $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot .. \cdot \mathfrak{p}_r^{e_r}$ its factorisation with ramification degrees e_i and inertia degrees given by $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/p]$. Then G acts transitively on the primes $\mathfrak{p}_i$, by which we mean that for all $1 \leq i, j \leq r$ there is some $\sigma \in G$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.*

Remark 2.3.30. From the transitivity of the Galois group and the uniqueness of the factorisation we have that $e = e_1 = .. = e_r$ and $f = f_1 = .. = f_r$ for all i. The decomposition then becomes $p\mathcal{O}_L = (\prod \mathfrak{p}_i)^e$ and the identity $[L : K] = \sum_{i=1}^{r} e_i f_i$ becomes $[L : K] = efr$. This gives us an explicit expression for the number of primes $r = \frac{[L:K]}{ef}$ lying over p. Note that if a prime p ramifies at some $\mathfrak{p}_i$ it does so at all r primes which appear in the decomposition of p.

Recall that $\pi_A(U_p)$ is the collection of finite groups for which there exists a Galois number field K which is only ramified at the prime p such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$.

Lemma 2.3.31. *Let p be some prime number and $G \in \pi_A(U_p)$. Then for any normal subgroup $N \trianglelefteq G$ the quotient G/N also lies in $\pi_A(U_p)$.*

Proof. Let $K/\mathbb{Q}$ be a number field where only p ramifies with G as its Galois group. We know with the Galois correspondence that G/N corresponds to a subextension K_0 of K. Then Lemma 2.2.26 tells us that p is the only prime which ramifies in K_0 and hence $G/N \in \pi_A(U_p)$. □

Because any group G has the commutator subgroup $[G, G] \trianglelefteq G$ as a normal subgroup with quotient group G^{ab} we now also understand Corollary 1.2.3. Furthermore, we find a criterion for groups to lie in $\pi_A(U_p)$.

Corollary 2.3.32. *Let $G \in \pi_A(U_p)$ for some prime p. Then the abelianisation of G is cyclic.*

Proof. The proof follows from Corollary 1.2.3. □

To check whether the infinite prime ∞ ramifies in a number field K we need to consider all the extensions of ∞ to K. If K is a Galois extension the situation becomes a lot simpler.

Definition 2.3.33. Let K be a number field. We say that K is respectively **totally real** or **totally complex** if K has either only real or only complex embeddings into $\mathbb{C}$.

Proposition 2.3.34. *Let K be a number field that is Galois over $\mathbb{Q}$. Then K is either totally real or totally complex.*

Proof. Let $[K : \mathbb{Q}] = n$. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and embedding $\phi : K \to \mathbb{C}$ we can compose them to find some other embedding $\phi \circ \sigma : K \to \mathbb{C}$. Note that the image of ϕ and $\phi \circ \sigma$ are the same because σ is an automorphism. Since K is Galois we have n distinct automorphisms σ to compose with and since ϕ is injective we find n distinct embeddings in this way. However, by Proposition 2.2.31 we also know these are all the possible embeddings of K into $\mathbb{C}$. This means that if K admits a real embedding, all embeddings are real and similarly if K admits a complex embedding. □

Corollary 2.3.35. *Let K be a number field that is Galois over $\mathbb{Q}$. Then the prime at infinity of $\mathbb{Q}$ ramifies in K if and only if K is totally complex.*

2.4 Proof of Theorem 1.2.2

Proof of Theorem 1.2.2. Let $g_1, .., g_d$ be a minimal generating set of G with respective orders $n_1, .., n_d$. We start by writing

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times .. \times \mathbb{Z}/n_d\mathbb{Z}$$

by considering for each g_i the cyclic subgroup it generates. Since every element of G is a finite product of generators to some powers and G is abelian we see that G is indeed isomorphic to the above direct product of cyclic groups. Dirichlet's Unit Theorem states that, for any positive integers a and n such that $\gcd(a, n) = 1$, there are infinitely many primes congruent to a mod n. Hence we can choose, for every n_i, infinitely many primes p_i such that $p_i \equiv 1 \pmod{2n_i}$. In particular we can choose a p_i for every n_i such that the p_i's are all distinct. Since $\mathbb{Z}/(\frac{p_i-1}{2})\mathbb{Z}$ is cyclic and $n_i | \frac{p_i-1}{2}$ we know with Theorem 2.1.3 that $\mathbb{Z}/(\frac{p_i-1}{2})\mathbb{Z}$ contains a cyclic subgroup H_i of order $\frac{p_i-1}{2n_i}$ and that their quotient is

$$\mathbb{Z}/(\frac{p_i - 1}{2})\mathbb{Z}/H_i \simeq \mathbb{Z}/n_i\mathbb{Z}.$$

For each p_i we consider the cyclotomic extension $\mathbb{Q}(\zeta_{p_i})$ and its corresponding maximal real subfield $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$. By Lemma 2.3.24 we know that $[\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})] = 2$ and since $[\mathbb{Q}(\zeta_{p_i}) : \mathbb{Q}] = p_i - 1$ we find that $[\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) : \mathbb{Q}] = \frac{p_i-1}{2}$ as indicated in Figure 2.1.

$$\begin{array}{c} \mathbb{Q}(\zeta_{p_i}) \\ | \\ 2 \\ | \\ \mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) \\ | \\ \frac{p_i-1}{2} \\ | \\ \mathbb{Q} \end{array}$$

Figure 2.1: Degree of maximal real subfield of $\mathbb{Q}(\zeta_{p_i})$.

Since $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$ is Galois over $\mathbb{Q}$ its Galois group must correspond to a quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}) = \mathbb{Z}/(p_i - 1)/\mathbb{Z}$ by a subgroup of order 2. Hence, we can say that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})/\mathbb{Q}) \simeq \mathbb{Z}/(p_i - 1)\mathbb{Z}\big/\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/(\frac{p_i - 1}{2})\mathbb{Z}.$$

Furthermore, let C denote the compositum of the maximal real subfields $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$ for $1 \leq i \leq d$. Recall from the proof of Proposition 2.3.23 that $X := \mathbb{Q}(\zeta_{p_i}) \cap \mathbb{Q}(\zeta_{p_j}) = \mathbb{Q}$

for $i \neq j$. With this we can also conclude that $Y := \mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) \cap \mathbb{Q}(\zeta_{p_j} + \zeta_{p_j}^{-1}) = \mathbb{Q}$. This is because $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) \subset \mathbb{Q}(\zeta_{p_i})$, and the same for j, and so anything that lies in Y will also lie in X. From Corollary 2.3.16 it then follows that

$$\mathrm{Gal}(C/\mathbb{Q}) \simeq \mathbb{Z}/(\frac{p_1 - 1}{2})\mathbb{Z} \times .. \times \mathbb{Z}/(\frac{p_d - 1}{2})\mathbb{Z}.$$

Hence we see that G is a quotient of $\mathrm{Gal}(C/\mathbb{Q})$ by the subgroup $H_1 \times .. \times H_d \subset \mathrm{Gal}(C/\mathbb{Q})$. Therefore it corresponds to the Galois group of a subfield $K = C^{H_1 \times .. \times H_d}$ of C and we will show that K ramifies at exactly d primes. Let $n := p_1 \cdot .. \cdot p_d$. Then we start by noting that $C \subset \prod \mathbb{Q}(\zeta_{p_i}) = \mathbb{Q}(\zeta_n)$ where the latter equality comes from the proof of Proposition 2.3.23. Furthermore, $\zeta_n^{\frac{n}{p_i}}$ is a primitive p_i^{th} root of unity, thus we have $\mathbb{Q}(\zeta_{p_i}) \subset \mathbb{Q}(\zeta_n)$. Finally we have $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1}) \subset C$ for all i which allows us to consider the fixed field of $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$ under $H_1 \times .. \times H_d$. We summarise the setting in Figure 2.2.

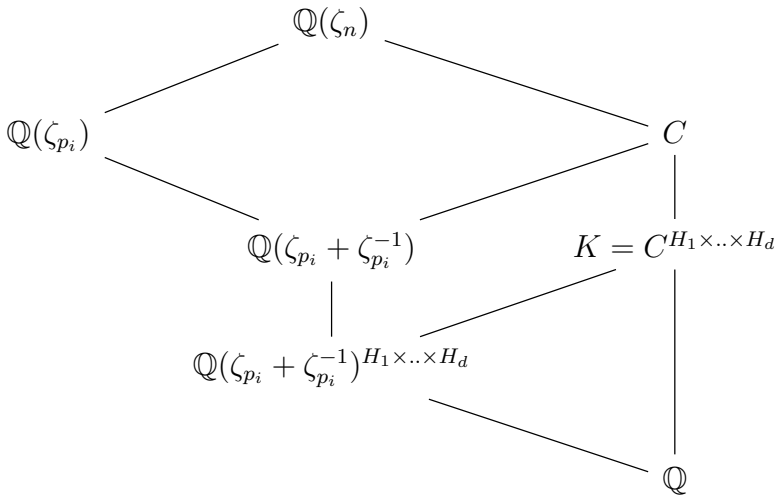


Figure 2.2: K ramifies at d primes.

Note that, by definition, any $x \in \mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})^{H_1 \times .. \times H_d}$ is an element of $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})$, and therefore also of C, which is fixed by all of $H_1 \times .. \times H_d$ and so

$$\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})^{H_1 \times .. \times H_d} \subset C^{H_1 \times .. \times H_d}.$$

As discussed in Proposition 2.3.22 the extension $\mathbb{Q}(\zeta_{p_i})$ is only ramified at p_i which, by Lemma 2.2.26, implies that any non-trivial intermediate field also only ramifies at p_i. Since G is a non-trivial quotient we see that $H_1 \times .. \times H_d$ is not the whole group and so $\mathbb{Q}(\zeta_{p_i} + \zeta_{p_i}^{-1})^{H_1 . \times .. \times H_d}$ is a non-trivial extension which therefore ramifies at p_i. It then follows with Corollary 2.2.25 that K also ramifies at p_i for all i as desired. If K would ramify at some prime $q \neq p_i$ for all i, then Corollary 2.2.25 tells us that $\mathbb{Q}(\zeta_n)$ would also ramify at q, but as discussed in Proposition 2.3.22 this is not possible. Furthermore, since K is totally real we can be sure that the infinite prime does not ramify. Hence we conclude that K ramifies at exactly d finite primes as desired.

We will now show there is no G-extension which ramifies at fewer than d primes including the infinite prime. Assume that $K/\mathbb{Q}$ is some extension with G as its Galois group and that K is ramified at the finite primes $p_1, .., p_k$ for some $k \geq 1$. By Theorem 2.3.27 we find K as a subfield of some cyclotomic field $L = \mathbb{Q}(\zeta_n)$ and with the Galois correspondence (2.3.10) we see that G is a quotient of $\mathrm{Gal}(L/\mathbb{Q})$. Since we know exactly

what primes ramify in K, and so with Corollary 2.2.25 that these primes also ramify in L, we can argue with Proposition 2.3.22 that the primes $p_1, .., p_k$ must appear in the prime factorisation of n. Furthermore, if any other prime p would appear in this factorisation of n, then p would ramify in L and we can argue in the same way as in the first part of this proof that K would also ramify at p. Hence $n = p_1^{a_1} \cdot .. \cdot p_k^{a_k}$ for some positive integers a_i. By the Chinese Remainder Theorem G is a quotient of

$$\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/(p_1^{a_1})\mathbb{Z})^\times \times .. \times (\mathbb{Z}/(p_k^{a_k})\mathbb{Z})^\times,$$

where every term $(\mathbb{Z}/(p_i^{a_i})\mathbb{Z})^\times$ is a cyclic group of order $p_i^{a_i} - p_i^{a_i-1}$ if p_i is odd. If $p_i = 2$ we know that $(\mathbb{Z}/(p_i^{a_i})\mathbb{Z})^\times$ has at most two generators and so we conclude that G has at most $k+1$ generators, i.e. $k \geq d-1$. Since G is Galois we know that K is either totally real or totally complex. If K is totally complex we know that the prime at infinity ramifies, hence the total number of ramified primes is one more and so it is at least d in this case. If however K is totally real we know that the prime at infinity does not ramify. Though, K must be contained in the maximal real subfield L^+ of L, which implies G is a quotient of $\mathrm{Gal}(L^+/\mathbb{Q})$. As previously argued in this proof, we can use Lemma 2.3.24 to show that

$$\mathrm{Gal}(L^+/\mathbb{Q}) \simeq {}^{\mathrm{Gal}(L/\mathbb{Q})}\!\diagup_{\mathbb{Z}/2\mathbb{Z}}.$$

If $p_i = 2$ then $(\mathbb{Z}/(p_i^{a_i})\mathbb{Z})^\times$ is either isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^{a_i-2})\mathbb{Z}$ dependent on a_i. In both cases we see that $\mathbb{Z}/2\mathbb{Z}$ appears as a factor which means we kill a generator of $\mathrm{Gal}(L^+/\mathbb{Q})$ by quotienting out $\mathbb{Z}/2\mathbb{Z}$ from $\mathrm{Gal}(L/\mathbb{Q})$. In particular this means that G has at most k generators in the case that K is totally real and so $k \geq d$. We conclude that the number of ramified primes is at least the number of generators. □

Chapter 3

A description of groups in $\pi_A(U_p)$ for small primes

This chapter contains results which give a description of the Galois groups of number fields which ramify at a single predetermined finite prime (and possibly ∞). We explain how Harbater [13], Hoelscher [16] and Pollak [27] built on each other's work to obtain results on the structure of groups $G \in \pi_A(U_p)$ for respectively the primes $2, 3$ and 5. We start by focusing on the techniques that were used to obtain a description of groups in $\pi_A(U_2)$ by Harbater. We then see how Hoelscher and Pollak generalised these techniques to obtain Proposition 3.2.4 which gives a description of groups in $\pi_A(U_p)$ for arbitrary odd primes p. After this we show how these techniques were used to actually obtain results for the primes 3 and 5. Using Proposition 3.2.4 we provide a result on the structure of arbitrary groups $G \in \pi_A(U_p)$ for $7 \leq p \leq 19$ in Proposition 3.3.3. Furthermore, we explain how we can strengthen our results by assuming the Generalised Riemann Hypothesis or assuming the extension to be totally real.

3.1 Groups in $\pi_A(U_2)$

We look at the techniques that Harbater used for the prime 2 where we begin with the following observation.

Proposition 3.1.1. *[13, Page 19] Let G be a group with $G \in \pi_A(U_2)$. Then G is a quasi 2-group.*

Proof. By Proposition 2.1.30 we see that the order of $G/2(G)$ is odd and hence by Theorem 2.1.46 we find that $G/2(G)$ is solvable. Therefore it admits a subnormal series

$$0 \trianglelefteq H_0/2(G) \trianglelefteq H_1/2(G) \trianglelefteq .. \trianglelefteq H_k/2(G) = G/2(G),$$

where all H_i are normal in G and all quotients are abelian. If we assume $G/2(G)$ to be non-trivial we can show that G admits a non-trivial abelian odd quotient. Firstly, If $H_{k-1}/2(G)$ is trivial we have that ${}^{G/2(G)}\!/_{1} = G/2(G)$ is non-trivial abelian and of odd order. If $H_{k-1}/2(G)$ is non-trivial we see that the quotient ${}^{G/2(G)}\!/_{H_{k-1}/2(G)} = G/H_{k-1}$ is non-trivial, abelian and of odd order as well, since $|G/2(G)|$ is odd and the order of every subgroup $H_i/2(G)$ must divide the order of $G/2(G)$. Say that $\mathbb{Q} \subset K$ is a G-extension which ramifies only at 2. Then G/H_{k-1} corresponds to a subfield $\mathbb{Q} \subset K' \subset K$ where by Lemma 2.2.26 we can say that K' must also ramify at 2. Such an abelian extension must lie in some cyclotomic field by Theorem 2.3.27 and by Remark 2.3.28 we can even say

that this field must be of the form $\mathbb{Q}(\zeta_{2^r})$ for some $r \geq 1$. However, we then have that

$$[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{2^r}) : K'][K' : \mathbb{Q}],$$

where $[K' : \mathbb{Q}]$ is odd. Since the extension is Galois we have $[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})|$ and by Proposition 2.3.21 we know that $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^r}/\mathbb{Q}) = (\mathbb{Z}/2^r\mathbb{Z})^\times$. The order of the latter group is 2^{r-1} by Theorem 2.1.14 which gives a contradiction with $[K' : \mathbb{Q}]$ being odd. We can thus conclude that $G/2(G)$ must be trivial and hence say that G is in fact a quasi 2-group. □

Harbater strengthened this result with the following proposition.

Proposition 3.1.2. *[13, Proposition 2.17] Let K be a Galois extension of $\mathbb{Q}$ ramified only at 2 and $\mathbb{Q} \subset K_0$ be an intermediate Galois extension whose degree is a power of 2 over $\mathbb{Q}$. Then either*

1. *$N := \mathrm{Gal}(K/K_0)$ is a quasi $2-$group;*
2. *There exists a non-trivial abelian unramified intermediate extension $K_0 \subset L \subset K$ of odd degree over K_0 which is Galois over $\mathbb{Q}$.*

Indeed, if $K_0 = \mathbb{Q}$ we note that there are no non-trivial unramified extensions of $\mathbb{Q}$ by Corollary 2.2.23 and so $\mathrm{Gal}(K/K_0) = G$ must be a quasi-2 group. In the case that K_0 is maximal and G is solvable this gives the following result.

Lemma 3.1.3. *[13, Lemma 2.19] Under the hypothesis of Proposition 3.1.2, let $G := \mathrm{Gal}(K/\mathbb{Q})$ be solvable and assume K_0 to be a maximal 2-power subextension of K. Then we may replace item 1 of Proposition 3.1.2 by the condition that $K = K_0$, which means G is a 2-group.*

Proof. The proof is analogous to that of Lemma 3.2.2 which we will provide below. □

Harbater could combine Proposition 3.1.2 with Lemma 3.1.3 to give a description of solvable groups in $\pi_A(U_2)$ by first determining all 2-groups in $\pi_A(U_2)$ of order less than or equal to 8.

Proposition 3.1.4. *[13, Proposition 2.15] The 2-groups of order ≤ 8 in $\pi_A(U_2)$ are precisely the groups*

- *1;*
- $\mathbb{Z}/2\mathbb{Z}$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- $\mathbb{Z}/4\mathbb{Z}$;
- $\mathbb{Z}/8\mathbb{Z}$;
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- D_4.

Moreover, all of the corresponding field extensions of $\mathbb{Q}$ have class number 1.

We can now give a structure description of all solvable groups in $\pi_A(U_2)$.

Theorem 3.1.5. *[13, Theorem 2.20] Let G be the Galois group of a non-trivial, solvable extension ramified only at 2 and possibly ∞. Then one of the following holds:*

1. *The order of G is 2, 4 or 8;*
2. *G has a quotient of order 16.*

Proof. If G is a 2-group with order $2^k \geq 16$ we know it admits a normal 2-subgroup of order 2^l for all $l \leq k$ by Theorem 2.1.19. In particular we can find a normal subgroup H of order 2^{k-4} since $k \geq 4$ and so we see that G has a quotient of order $\frac{|G|}{|H|} = \frac{2^k}{2^{k-4}} = 2^4 = 16$. So we can assume that G is not a 2-group. Let K be a G-Galois extension which is only ramified at 2 and let K_0 as in Lemma 3.1.3, i.e. an intermediate extension whose degree is a power of 2 over $\mathbb{Q}$ and maximal with respect to this. If we let $N := \mathrm{Gal}(K/K_0)$, we can say that $\mathrm{Gal}(K_0/\mathbb{Q}) = G/N$ is a 2-group, since the order of G/N is the degree of K_0 over $\mathbb{Q}$. Hence, $N \neq 1$, or equivalently $K \neq K_0$, since otherwise G would be a 2-group. By Lemma 3.1.3 we can then conclude that Item 1 does not hold and so there must be some non-trivial abelian unramified Galois sub-extension $K_0 \subset L \subset K$ of odd degree over K_0. Because this L is abelian and unramified it is contained in the Hilbert class field E of K_0, i.e. $K_0 \subset L \subset E$. We find the following expression for the class number h_{K_0} of K_0

$$h_{K_0} = [E : K_0] = [E : L][L : K_0].$$

Since L is non-trivial we must have $[L : K_0] > 1$ and so $h_{K_0} > 1$ as well. Furthermore, since K only ramifies at 2 we find by Lemma 2.2.26 that K_0 also ramifies only at 2 and so G/N lies in $\pi_A(U_2)$. Since G/N is a 2-group as well we find by Proposition 3.1.4 that $|G/N| \geq 16$, say that $|G/N| = 2^r$ with $r \geq 4$. Then, again with Theorem 2.1.19, we can say that G/N admits a normal 2-subgroup of order 2^l for all $l \leq r$. Thus we create some normal subgroup $M/N \trianglelefteq G/N$ with order 2^{r-4}, where M is a normal subgroup in G. This means that

$$|G/M| = |{}^{G/N}\!/_{M/N}| = \frac{|G/N|}{|M/N|} = \frac{2^r}{2^{r-4}} = 2^4 = 16,$$

proving that G indeed has a quotient of order 16 which completes the proof. □

Now that we know what solvable groups in $\pi_A(U_2)$ look like we can wonder how big of a restriction solvability is. Harbater proves that the "small" groups are solvable.

Lemma 3.1.6. *[13, Lemma 2.22] If $G \in \pi_A(U_2)$ and $|G| \leq 300$ then G is solvable.*

Proof. The proof is analogous to that of Proposition 4.2.3. □

With Lemma 3.1.6 Harbater can drop the solvability condition on G and still give a similar description of $G \in \pi_A(U_2)$ as in Theorem 3.1.5. This description is given in Theorem 3.1.9 and for the proof we also need the discriminant bounds of [26] and the following Lemma and Proposition.

Lemma 3.1.7. *[13, Page 12] Let $K/\mathbb{Q}$ be a finite Galois extension which is ramified only over a single prime p. Let e be the ramification index, $n = [K : \mathbb{Q}]$ and Δ the discriminant of K. Then we have the following inequality:*

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

Proposition 3.1.8. *[13, Proposition 2.8] Let p and q be (possibly equal) prime numbers, let G be a p-group, and let $\mathbb{Q} \subset K$ be a G-Galois extension ramified only at q. Then*

1. *The extension $\mathbb{Q} \subset K$ is totally ramified over q.*

2. *The class number of K is prime to p.*

We now have all the tools to drop the solvability condition in Theorem 3.1.5 and prove the following.

Theorem 3.1.9. *[13, Theorem 2.23] Let G be the Galois group of a non-trivial, solvable extension ramified only at 2 and possibly ∞. Let e denote the ramification index. Then*

1. *The order of G is 2, 4 or 8;*

2. $16|e$.

Proof. By Proposition 3.1.8 we can say that G is totally ramified if G is a 2-group. If G is not a 2-group of order < 16 and G is solvable, we know with Theorem 3.1.5 that G admits a quotient G/H of order 16. In this case the intermediate field of K which corresponds to H is totally ramified, again, by Proposition 3.1.8 and the fact that G/H lies in $\pi_A(U_2)$. Hence we have $16 = [K_0 : \mathbb{Q}] = e_{K_0/\mathbb{Q}}$, where $e_{K_0/\mathbb{Q}}$ is the ramification index of 2 in K_0. We know that $e_{K_0/\mathbb{Q}}$ divides e by Lemma 2.2.24 and so 16 divides e. It remains to consider the case where G is not a 2-group of order < 16 and G is non-solvable.

By Lemma 3.1.6 we know that $|G| > 300$. Now for a Galois extension $K/\mathbb{Q}$ of degree $n \geq 300$ we know that $|\Delta|^{\frac{1}{n}} \geq 19.26$ from [26], where Δ is the discriminant of K. Combining this with Lemma 3.1.7 and the fact that $e > 1$, we have that

$$19.26 \leq |\Delta|^{\frac{1}{n}} \leq 2^{1+\nu_2(e)-\frac{1}{e}} < 2^{1+\nu_2(e)},$$

and so $\nu_2(e) > 3$. Since $\nu_2(e)$ is an integer, it is at least 4, which means that 16 divides e. □

3.2 Groups in $\pi_A(U_3)$ and $\pi_A(U_5)$

Now that we understand how Harbater obtained a description of groups in $\pi_A(U_2)$ we will focus on adapting these techniques to obtain similar results for odd primes. The following two results are by Hoelscher and they are generalisations of Proposition 3.1.2 and Lemma 3.1.3 respectively.

Theorem 3.2.1. *[16, Theorem 2.1.1] Let K be a finite Galois extension of $\mathbb{Q}$ where the only ramified finite prime is p with p odd. Let G denote its Galois group and assume it to be solvable. Let $K_0/\mathbb{Q}$ be an intermediate abelian extension $\mathbb{Q} \subset K_0 \subset K$ and define $N := \mathrm{Gal}(K/K_0)$. Then either*

1. *$N/p(N) \subset \mathbb{Z}/(p-1)\mathbb{Z})$; or*

2. *There is a non-trivial abelian unramified subextension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p with L Galois over $\mathbb{Q}$.*

Lemma 3.2.2. *[16, Lemma 2.1.4] Under the hypothesis of Theorem 3.2.1, if K_0 is a maximal p-power subextension of $K/\mathbb{Q}$, then the Condition 1 of Theorem 3.2.1 can be replaced by the condition that either G is a cyclic p-group or $N/p(N)$ is a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$.*

Proof. Say that $[K_0 : \mathbb{Q}] = |G/N| = p^n$. We want to prove that $N/p(N) \subset \mathbb{Z}/(p-1)\mathbb{Z}$ implies that either $N/p(N)$ is non-trivial in $\mathbb{Z}/(p-1)\mathbb{Z}$ or G is a cyclic p-group. Thus it is enough to assume that $N/p(N) = 1$ and then show that G must be a cyclic p-group. Assume to the contrary that G is not a cyclic p-group. Note that N is normal since K_0 is assumed to be abelian and hence Galois over $\mathbb{Q}$. Since K_0 is maximal we know N is a minimal normal subgroup of G with index a power of p, since if there is some normal subgroup $M \subset N$ with $|G/M| = p^m$ we can say that M corresponds to a Galois subextension $K_0 \subset K' \subset K$ where $\mathrm{Gal}(K/K') = M$ and $\mathrm{Gal}(K'/\mathbb{Q}) = G/M$. But then K' would also have a p-power degree over $\mathbb{Q}$ which contradicts the maximality of K_0. We can say that N is non-trivial since otherwise $G/N \simeq G/1 \simeq G$ would be a p-group contrary to what we assumed. So G is a non-trivial solvable group which means that, by Lemma 2.1.45, G admits a normal subgroup $N_1 \subset N$, such that N/N_1 is of the form $(\mathbb{Z}/q\mathbb{Z})^l$ for some prime q and $l \geq 1$. By minimality of N we know that $|G : N_1|$ is not a power of p. We have the following expression

$$p^n = |G/N| = |{}^{G/N_1}\!/_{N/N_1}| = \frac{|G/N_1|}{|N/N_1|} = \frac{|G/N_1|}{q^l},$$

which, combined with the index of N_1 in G not being a power of p, tells us that $q \neq p$. Now, let J be any p-subgroup in N with order p^s. We want to show that J must be strictly contained in N_1. To this end let $j \in J$ and assume that $j \notin N_1$. The order of j must divide the order of J so $|j| = p^r$ for some $1 \leq r \leq s$. Since $j \notin N_1$ we find that the class $\bar{j}$ of j in N/N_1 is not 0 so it has an order which divides the order of j, i.e. $|\bar{j}| = p^k$ for some $k \leq l$. But at the same time the size of N/N_1 is q^l and the order of $\bar{j}$ should also divide this. This gives a contradiction and proves that J must be strictly contained in N_1. This means that N is not a quasi p-group, as desired. □

Pollak combined Theorem 3.2.1 and Lemma 3.2.2 to obtain Proposition 3.2.4 which is effectively a case description of solvable groups in $\pi_A(U_p)$ for odd primes. For this he also used the following theorem by Harbater.

Theorem 3.2.3. *[13, Theorem 2.11] If p is an odd prime then a finite p-group G lies in $\pi_A(U_p)$ if and only if G is cyclic.*

We now have all the tools to prove Proposition 3.2.4.

Proposition 3.2.4. *[27, Proposition 2.1.5] Suppose $K/\mathbb{Q}$ is a non-trivial, solvable Galois extension ramified only at a single, odd finite prime p and possibly ∞. We denote the Galois group as $G := \mathrm{Gal}(K/\mathbb{Q})$. Then one of the following holds:*

1. *G is a cyclic p-group;*
2. *$G/p(G)$ is isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$;*
3. *G has a cyclic quotient of order p^t, where t is the smallest number such that $\mathbb{Q}(\zeta_{p^{t+1}})$ has a non-trivial class group.*

Proof. Let K_0 be the maximal Galois subextension of K whose degree over $\mathbb{Q}$ is a power of p, say p^n for some $n \geq 0$. We set $\mathrm{Gal}(K/K_0) := N$ so that $G/N = \mathrm{Gal}(K_0/\mathbb{Q})$. Since K_0 is Galois we have that $|G/N| = p^n$, so G/N is a p-group which additionally lies in $\pi_A(U_p)$ due to Lemma 2.2.26. Then by Theorem 3.2.3 we know that G/N is cyclic so it is of the form $\mathbb{Z}/p^n\mathbb{Z}$, which means that K_0 is an abelian extension. As remarked in 2.3.28 Kronecker-Weber tells us it lies in some $\mathbb{Q}(\zeta_{p^{n_0}})$ for some n_0. We can show that

$n_0 \geq n+1$ by noting that $[\mathbb{Q}(\zeta_{p^{n_0}}) : \mathbb{Q}] = \phi(p^{n_0}) = p^{n_0-1}(p-1)$ and since $K_0 \subset \mathbb{Q}(\zeta_{p^{n_0}})$ we have that

$$[\mathbb{Q}(\zeta_{p^{n_0}}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^{n_0}}) : K_0][K_0 : \mathbb{Q}],$$

where $[K_0 : \mathbb{Q}] = p^n$. So p^n should divide $p^{n_0-1}(p-1)$. If $n_0 \leq n$ then $p^{n_0-1}(p-1) \leq p^n$ so p^n cannot divide $p^{n_0-1}(p-1)$. Hence $n_0 \geq n+1$. In fact we claim that $K_0 \subset \mathbb{Q}(\zeta_{p^{n+1}})$ and move the proof of this to Claim 3.2.5.

Now suppose that G is not a cyclic p-group and that $G/p(G)$ is not isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. We claim it is enough to show that $\mathbb{Q}(\zeta_{p^{n+1}})$ has a non-trivial class group, since this would then imply that $n \geq t$ so with Theorem 2.1.19 the group G/N, with order p^n, would admit a normal subgroup, say H/N, of order p^{n-t}, because $p^{n-t}|p^n$. Then $|G/H| = |{}^{G/N}\!/_{H/N}| = \frac{p^n}{p^{n-t}} = p^t$ which gives the desired quotient of G. Note that this quotient is cyclic, because it is in particular a quotient of G/N which we noted to be a cyclic group.

In order to show that $\mathbb{Q}(\zeta_{p^{n+1}})$ has a non-trivial class group we first prove that $N/p(N)$ is not isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. Assume to the contrary that $N/p(N) \simeq \mathbb{Z}/m\mathbb{Z}$ for some $m > 1$ which divides $p-1$. Note that $p(N)$ is characteristic in N by Lemma 2.1.23, which itself is normal in G so $p(N)$ is also normal in G by Lemma 2.1.33. This means we can form the quotient $G/p(N)$ and since N is normal in G and contains $p(N)$ we also have $N/p(N) \trianglelefteq G/p(N)$. With the third isomorphism Theorem we also have

$$G/N \simeq {}^{G/p(N)}\!/_{N/p(N)}.$$

Now recall that $N/p(N) \simeq \mathbb{Z}/m\mathbb{Z}$ and $G/N \simeq \mathbb{Z}/p^n\mathbb{Z}$. Since $\gcd(p-1, p) = 1$ and m divides $p-1$ we have that $\gcd(m, p^n) = 1$ so the Schur-Zassenhaus Theorem (2.1.13) tells us that

$$G/p(N) \simeq N/p(N) \rtimes G/N \simeq \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^n\mathbb{Z}.$$

Now, the automorphism group of $\mathbb{Z}/m\mathbb{Z}$ has order $\phi(m)$ and since m divides $p-1$ we know that $\phi(m)$ is strictly smaller than p. Hence $\phi(m)$ is coprime to p and therefore also to any power of p. Now consider some morphism $\psi : \mathbb{Z}/p^n\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$. Then for any non-trivial $x \in \mathbb{Z}/p^n\mathbb{Z}$ the order of $\psi(x)$ would have to be a divisor of the order of x, which itself needs to be a divisor of p^n, i.e. p^k for some $1 \leq k \leq n$. Note that the order of $\psi(x)$ also has to divide the order of $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ and since we just noted $\phi(m)$ is coprime to any power of p, we can say that the order of $\psi(x)$ has to be 1. This implies ψ must be the trivial morphism and we find, as remarked in 2.1.12, that the semidirect product is in fact a direct product,

$$G/p(N) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}.$$

Since any p-subgroup in N is also a p-subgroup of G we find that $p(N) \subset p(G)$. In fact, since we showed that $p(N)$ is normal in G we know it is normal in any subgroup of G which contains $p(N)$. Thus $p(N) \trianglelefteq p(G)$ and forming the quotient $p(G)/p(N)$ makes sense. With the Third Isomorphism Theorem 2.1.5 and Lemma 2.1.32 we now have that

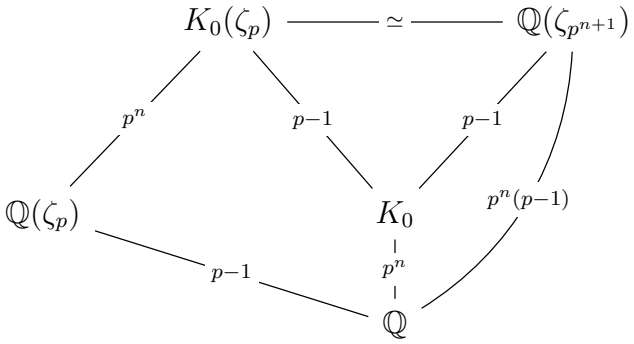
$$G/p(G) \simeq {}^{G/p(N)}\!/_{p(G)/p(N)} \simeq {}^{G/p(N)}\!/_{p(G/p(N))}.$$

Now we can compute $p(G/p(N)) \simeq \mathbb{Z}/p^n\mathbb{Z}$, since any p-subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ will lie in $\mathbb{Z}/p^n\mathbb{Z}$ so we have

$$G/p(G) \simeq {}^{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}}\!/_{\mathbb{Z}/p^n\mathbb{Z}} \simeq \mathbb{Z}/m\mathbb{Z}.$$

This contradicts the assumption that $G/p(G)$ was not a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ so we can conclude that $N/p(N)$ is not a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ either.

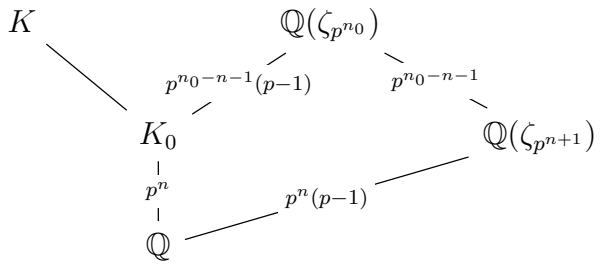
Now we are in the setting of Theorem 3.2.1 and can also use Lemma 3.2.2 to replace Condition 1 of said theorem with the condition that either G is a cyclic p-group or $N/p(N)$ is a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$. We assumed that the former does not hold and just showed the latter also does not hold. Hence item 2 of Theorem 3.2.1 must hold and we know there is some non-trivial abelian unramified subextension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ where the degree of L over $K_0(\zeta_p)$ is coprime to p. So the class number of $K_0(\zeta_p)$ is non-trivial and we now claim that $K_0(\zeta_p) \simeq \mathbb{Q}(\zeta_{p^{n+1}})$. We have the following picture to describe the situation:



Recall, $[\mathbb{Q}(\zeta_{p^{n+1}}) : \mathbb{Q}] = p^n(p-1)$ and $[K_0 : \mathbb{Q}] = p^n$, which, combined with the tower relations, gives that $[\mathbb{Q}(\zeta_{p^{n+1}}) : K_0] = p-1$. We know that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ and therefore $\mathbb{Q}(\zeta_p) \not\subset K_0$; otherwise $p-1$ would have to divide p^n by the tower relations. Note that $K_0 \simeq \mathbb{Q}(\alpha)$ for some $\alpha \in K_0$ by Corollary 2.2.9 and since $p-1$ and p^n are coprime we find with Lemma 2.2.2 that $[K_0(\zeta_p) : \mathbb{Q}] = p^n(p-1)$, which explains the final degrees in the left hand side of the picture. Also note that $(\zeta_{p^{n+1}})^{p^n} = \zeta_p$ so $\zeta_p \in \mathbb{Q}(\zeta_{p^{n+1}})$ which means $K_0(\zeta_p) \subset \mathbb{Q}(\zeta_{p^{n+1}})$. But $K_0(\zeta_p)$ and $\mathbb{Q}(\zeta_{p^{n+1}})$ have the same degree over $\mathbb{Q}$ and one lies in the other which means they are isomorphic as we wanted to show. □

Claim 3.2.5. We claim $K_0 \subset \mathbb{Q}(\zeta_{p^{n+1}})$ in the setting of Proposition 3.2.4.

Proof of claim. This is clearly the case if $n_0 = n+1$ so assume that $n_0 > n+1$. Since $(\zeta_{p^{n_0}})^{p^{n_0-n-1}}$ is a primitive p^{n+1} root of unity we find that $\mathbb{Q}(\zeta_{p^{n+1}}) \subset \mathbb{Q}(\zeta_{p^{n_0}})$. The situation of these extensions with the corresponding degrees is depicted below.



Recall that $\mathbb{Q}(\zeta_{p^{n_0}})$ is Galois over $\mathbb{Q}$ with Galois group $\bar{G} := (\mathbb{Z}/p^{n_0}\mathbb{Z})^\times$ and that Lemma 2.1.15 tells us that this group is cyclic. Since K_0 and $\mathbb{Q}(\zeta_{p^{n+1}})$ are both Galois over $\mathbb{Q}$ we know that their Galois groups are respectively of the form $\bar{G}/\bar{N}$ and $\bar{G}/\bar{M}$ where the subgroups have orders $|\bar{N}| = p^{n_0-n-1}(p-1)$ and $|\bar{M}| = p^{n_0-n-1}$. Since the order of $\bar{M}$ divides the order of $\bar{N}$ and $\bar{M}$ and $\bar{N}$ are both subgroups of a cyclic group, and hence are cyclic themselves, we can say that $\bar{M} \subset \bar{N}$ by Theorem 2.1.3. With the Galois correspondence we find that the corresponding subfields of $\mathbb{Q}(\zeta_{p^{n_0}})$ are also contained in each other, i.e. $K_0 \subset \mathbb{Q}(\zeta_{p^{n+1}})$. □

It is clear from Item 3 of Proposition 3.2.4 that we need to know more about class numbers of the cyclotomic fields $\mathbb{Q}(\zeta_{p^t})$ in order to apply this Proposition to a specific prime p. For this we have the following result.

Theorem 3.2.6. *[23, Main Theorem] There are precisely* 29 *distinct cyclotomic fields with class number* 1. *They are given by* $\mathbb{Q}(\zeta_n)$ *with*

$n =$ 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.

Remark 3.2.7. There are 15 additional values of m for which the class number of $\mathbb{Q}(\zeta_m)$ is 1. However, each of these additional values are of the form $2n$ for some n in the list of Theorem 3.2.6 and since $\mathbb{Q}(\zeta_n) \simeq \mathbb{Q}(\zeta_{2n})$ these values do not give new cyclotomic fields.

Corollary 3.2.8. *For a prime number p the class number of $\mathbb{Q}(\zeta_p)$ is 1 if and only if $p \leq 19$. Furthermore, 3 and 5 are the only primes p for which there exists a $k > 1$ such that $\mathbb{Q}(\zeta_{p^k})$ has class number 1.*

Applying Proposition 3.2.4 to the primes 3 and 5 gives the following descriptions as corollaries.

Corollary 3.2.9. *[16, Corollary 2.1.5] Let G be the Galois group of a non-trivial, solvable extension ramified only at 3 and possibly ∞. Then one of the following holds:*

1. *G is a cyclic 3-group;*
2. *$G/3(G) \simeq \mathbb{Z}/2\mathbb{Z}$;*
3. *G has a cyclic quotient of order 27;*

Proof. We apply Proposition 3.2.4 and we see from Theorem 3.2.6 that the 49^{th} cyclotomic field is the first 3-power cyclotomic field with a non-trivial class group. □

Corollary 3.2.10. *[27, Corollary 2.1.7] Let G be the Galois group of a non-trivial, solvable extension ramified only at 5 and possibly ∞. Then one of the following holds:*

1. *G is a cyclic 5-group;*
2. *$G/5(G) \simeq \mathbb{Z}/2\mathbb{Z}$;*
3. *$G/5(G) \simeq \mathbb{Z}/4\mathbb{Z}$;*
4. *G has a cyclic quotient of order 25.*

Proof. We apply Proposition 3.2.4 and we see from Theorem 3.2.6 that the 125^{th} cyclotomic field is the first 5-power cyclotomic field with a non-trivial class group. □

Hoelscher and Pollak also gave a characterisation of arbitrary groups in $\pi_A(U_3)$ and $\pi_A(U_5)$ respectively by using similar techniques as Harbater. The proofs are therefore quite similar and we will only give the proof of the case $p = 5$ in Proposition 3.2.12 to avoid repetition.

Corollary 3.2.11. *[16, Corollary 2.1.6] Suppose $K/\mathbb{Q}$ is a Galois extension with non-trivial group G, ramified only at the prime 3 and possibly ∞, with ramification index e. Then one of the following holds:*

1. *$G \simeq \mathbb{Z}/3\mathbb{Z}$;*

2. $G/3(G) \simeq \mathbb{Z}/2\mathbb{Z}$;

3. $9|e$.

Proposition 3.2.12. *[27, Proposition 2.1.8] Suppose $K/\mathbb{Q}$ is a Galois extension with non-trivial group G, ramified only at the prime 5 and possibly ∞, with ramification index e. Then one of the following holds:*

1. $G \simeq \mathbb{Z}/5\mathbb{Z}$;

2. $G/5(G) \simeq \mathbb{Z}/2\mathbb{Z}$;

3. $G/5(G) \simeq \mathbb{Z}/4\mathbb{Z}$;

4. $5|e$ *and* $e \geq 10$.

Proof. Firstly, if G is solvable we can apply Corollary 3.2.10 and we are done if the second or third condition of Corollary 3.2.10 hold. If the fourth condition of Corollary 3.2.10 holds we know that G some cyclic quotient G/N of order 25. We see from the proof of Corollary 3.2.10 that G/N corresponds to a Galois extension K_0 which ramifies only at 5. Then Proposition 3.1.8 tells us that K_0 is totally ramified over 5 which means that $|G/N| = [K_0 : \mathbb{Q}] = 25 = e$ so in particular $5|e$ and $e \geq 10$. Finally, if the first condition holds either $G \simeq \mathbb{Z}/5\mathbb{Z}$, and we are done, or $G \simeq \mathbb{Z}/5^l\mathbb{Z}$ with $l \geq 2$. In the latter case we have that K is totally ramified by Proposition 3.1.8 so $e = 5^l$. Since $l \geq 2$ we have $5|e$ and $e \geq 10$.

Suppose now that G is not solvable. Then $|G| \geq 300$ by Proposition 4.1.1. Let $n = |G|$ and let Δ be the discriminant of K. By [6, Appendix, p.1] we know that $|\Delta|^{\frac{1}{n}} \geq 19.26$ since the degree of the extension is at least 300. But since the only ramified prime is 5, we have from Lemma 3.1.7 that $|\Delta|^{\frac{1}{n}} \leq 5^{1+\nu_5(e)-\frac{1}{e}}$. Thus we find

$$19.26 \leq 5^{1+\nu_5(e)-\frac{1}{e}}. \quad (\star)$$

Because $e > 1$, and thus $5^{1-\frac{1}{e}} < 5$, we can not have $\nu_5(e) = 0$. So $\nu_5(e) \geq 1$, which already gives $5|e$ as desired. Furthermore, if $\nu_5(e) = 1$ the smallest value e can have is 5, but then the right hand side of $(\star)$ would be 18.12. This tells us that e must have some other divisor than 5 so $e \geq 10$. For $e = 10$ the right hand side of $(\star)$ is 21.28, which means we cannot say more than $e \geq 10$ with this exact approach. □

Event though the proofs of Corollary 3.2.11 and Proposition 3.2.12 are very similar there is a small remark to make.

Remark 3.2.13. In proving Corollary 3.2.11, Hoelscher also uses discriminant bounds, like Harbater and Pollak do for proving respectively Theorem 3.1.9 and Corollary 3.2.12. However, where Harbater and Pollak leverage the fact that non-solvable groups in $\pi_A(U_p)$ need to have order at least 300, Hoelscher uses the weaker statement that, in general, non-solvable groups have order at least 60. One might wonder if applying the stronger bound of 300 to the same argument of Hoelscher would give us some stronger lower bound on e, but it turns out to not make a difference. We will later see in Theorem 4.1.2 that we can even say that $|G| \geq 660$, but this will also not give better results for $p = 3$. In particular, if $|G| = n \geq 660$ we have with [6] that $|\Delta|^{\frac{1}{n}} \geq 20.47$. Using the approach of Proposition 3.2.12, if $\nu_3(e) < 2$ then $3^{1+\nu_3(e)-\frac{1}{e}} < 20.47$ so $\nu_3(e) \geq 2$. However, when $\nu_3(e) = 2$ we know e is at least 9 and this gives $3^{1+\nu_3(e)-\frac{1}{e}} = 3^{3-\frac{1}{9}} = 23.89$ which means that we cannot improve on $9|e$ or say that $e \geq 2 \cdot 9$ using the stronger bounds of $|G| \geq 660$.

We end this section by noting that additional assumptions result in improved discriminant bounds and hence improved versions of Corollary 3.2.11. Here we also use the fact that $|G| \geq 660$ if G is non-solvable, as we will see in Theorem 4.1.2.

Lemma 3.2.14. *Assuming the Generalised Riemann Hypothesis we can replace the third condition in Corollary 3.2.11 by* $27|e$.

Proof. Note that the proof of Proposition 3.2.11 (or really the analogous proof given for Proposition 3.2.12) already indicates that $27|e$ in the solvable case, because of the cyclic quotient of order 27. If G is non-solvable we know, under the assumption of the Generalised Riemann Hypothesis, that $27.33 \leq |\Delta|^{\frac{1}{n}}$ from [26, Table 1] for extensions of degree at least 600. If $\nu_3(e) \leq 2$ we would have that $3^{1+\nu_3(e)-\frac{1}{e}} < 27 < 27.33$ which would give a contradiction. So we can say that $27|e$ in the non-solvable case as well. □

Lemma 3.2.15. *Under the assumptions of Corollary 3.2.11, if we additionally assume that K is a totally real extension we can replace the third condition with* $27|e$.

Proof. If K is a totally real extension we know from [6, Appendix, Table 2, p.4] that $54.57 \leq |\Delta|^{\frac{1}{n}}$, which gives $54.57 \leq 3^{1+\nu_3(e)-\frac{1}{e}}$. If $\nu_3(e) \leq 2$ then $3^{1+\nu_3(e)-\frac{1}{e}} < 27 < 54.57$. Hence $\nu_3(e) \geq 3$ and we can replace the third condition with $27|e$. □

In a similar fashion Pollak notes that we get improved versions of Proposition 3.2.12 by additional assumptions on the corresponding extensions.

Lemma 3.2.16. *[27, Remark 2.1.9] Under the assumptions of Proposition 3.2.12, if one is willing to assume the Generalised Riemann Hypothesis we can replace the fourth condition in 3.2.12 by* $25|e$.

Proof. The proof is analogous to that of Lemma 3.2.14.

□

Lemma 3.2.17. *[27, Remark 2.1.9] Under the assumptions of Proposition 3.2.12, if K is additionally a totally real extension we can replace the fourth condition with* $25|e$.

Proof. The proof is analogous to that of Lemma 3.2.15. □

Lemma 3.2.18. *[27, Remark 2.1.9] Under the assumptions of Proposition 3.2.12, if additionally K has a degree of 2400 or more over $\mathbb{Q}$ we can say that $e \geq 15$.*

Proof. From [26, Table 2] we see that, if K has degree 2400 or more, the discriminant bound becomes $21.54 \leq |\Delta|^{\frac{1}{n}}$. If $\nu_5(e) = 1$ then e is at least 5, but then Lemma 3.1.7 tells us that $21.54 \leq 5^{1+1-\frac{1}{5}} = 18.12$ which is a contradiction. So for $\nu_5(e) = 1$ we need e to have another divisor than 5. If $e = 2 \cdot 5 = 10$ the inequality becomes $21.54 \leq 5^{1+1-\frac{1}{10}} = 21.28$, so we need $e \geq 15$. Note that the largest degree in [26, Table 2] is 10^7 which results in a bound of $22.35 \leq |\Delta|^{\frac{1}{n}}$. If $\nu_5(e) = 1$ and $e = 15$ we find that $5^{1+\nu_5(e)-\frac{1}{e}} = 22.46$ so the current bounds do not suffice to conclude $e > 15$. □

3.3 Applications to primes $7 \leq p \leq 19$

We have seen the applications of Proposition 3.2.4 to the primes 3 and 5. In this section we will explore what we can say for other primes. Pollak readily proves the following for all odd primes $p < 23$.

Corollary 3.3.1. *[27, Corollary 2.1.6] Let $p < 23$ be an odd prime and let $K/\mathbb{Q}$ be a non-trivial, solvable Galois extension ramified only at p and possibly ∞ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Then one of the following holds:*

1. *$G/p(G)$ is isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$;*

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

Proof. We apply Proposition 3.2.4. If G is a cyclic p-group of order p^k for some $k \geq 1$, it will have a quotient of order p^l for all $l \leq k$ by Theorem 2.1.19. In particular it will have a quotient of order p and since it is a cyclic group all quotients will be cyclic. If $G/p(G)$ is isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ we are done. If we find ourselves in the final case of Proposition 3.2.4, we note that for all $p < 23$ the class group of $\mathbb{Q}(\zeta_p)$ is trivial by Corollary 3.2.8, so $t \geq 1$. If $t = 1$ we get that G has a cyclic quotient of order p. If $t > 1$ we still have that $|G/H| = p^t$ for some normal subgroup $H \trianglelefteq G$. Again, the quotient G/H is a p-group and so Theorem 2.1.19 tells us it admits a normal subgroup N/H of order p^{t-1} where $N \trianglelefteq G$. This gives ${}^{G/H}\!/_{N/H} \simeq G/N$ which means the order of G/N is $\frac{p^t}{p^{t-1}} = p$ as desired. □

Remark 3.3.2. Indeed, Corollary 3.3.1 does not claim existence of a cyclic quotient with size p^k for $k > 1$. The reason we could do this for the primes 3 and 5, and not for any other primes, is that they are the only primes for which there exists a $k > 1$ such that $\mathbb{Q}(\zeta_{p^k})$ has a nontrivial class number by Corollary 3.2.8.

We already discussed how we can drop this solvability assumption for the primes up to 5. It turns out that we can do the same for the primes $7 \leq p \leq 19$ and give similar characterisations as Hoelscher and Pollak do in Corollary 3.2.11 and Proposition 3.2.12 respectively.

Proposition 3.3.3. *Suppose $K/\mathbb{Q}$ is a Galois extension with non-trivial group G, ramified only at a prime $7 \leq p \leq 19$ and possibly ∞, with ramification index e. Then one of the following holds:*

1. *$G/p(G)$ is isomorphic to a non-trivial subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$;*

2. *$p|e$.*

Proof. Firstly, if G is solvable we can apply Corollary 3.3.1 and we are done if the first condition holds. If the second condition holds we have some cyclic quotient G/N of order p. We see from the proof of Proposition 3.2.4 that G/N corresponds to a Galois extension K_0 which ramifies only at p. Then Proposition 3.1.8 tells us that K_0 is totally ramified over p which means that $|G/N| = [K_0 : \mathbb{Q}] = p = e$ so in particular $p|e$.

Suppose now that G is not solvable. We will prove that $p|e$. Then $|G| \geq 660$ by Theorem 4.1.2. Let $n = |G|$ and let Δ be the discriminant of K. By [6, Appendix, p.1] we know that $|\Delta|^{\frac{1}{n}} \geq 20.47$. But since the only ramified prime is p, we have from Lemma 3.1.7 that $|\Delta|^{\frac{1}{n}} \leq p^{1+\nu_p(e)-\frac{1}{e}}$. Thus we find

$$20.47 \leq p^{1+\nu_p(e)-\frac{1}{e}}. \quad (\star\star)$$

Because $e > 1$, and thus $p^{1-\frac{1}{e}} < p$, we cannot have $\nu_p(e) = 0$. So $\nu_p(e) \geq 1$, which already gives $p|e$ as desired. □

Remark 3.3.4. The proof of Proposition 3.3.3 is analogous to the proof of Proposition 3.2.12. However, in 3.2.12 an extra assertion is made, namely that $e \geq 10$. In a similar fashion, we would like to say for $7 \leq p < 23$ that $e \geq 2 \cdot p$, but if $\nu_p(e) = 1$ then we only have $e \geq p$. This gives $p^{2-\frac{1}{p}} \geq 37.11$ for $p \geq 7$, which does not contradict the inequality $(\star\star)$. So we cannot make a similar statement for any of the primes $7 \leq p < 23$ if we wanted to use the same argument. We see from the proof of Lemma 3.2.16 that assuming GRH would give $27.33 \leq |\Delta^{\frac{1}{n}}|$ which is again not enough to say $e \geq 2 \cdot p$ or $\nu_p(e) > 1$ for $7 \leq p < 23$.

We see from Remark 3.3.4 that we would need better discriminant bounds to say more about the size of e for a given prime. These required bounds are made explicit in Lemma 3.3.5.

Lemma 3.3.5. *Under the assumptions of Proposition 3.3.3, let Δ again denote the discriminant of K and let $B_p = p^{2-\frac{1}{p}}$ as in Table 3.1. If there is an n such that $B_p < |\Delta|^{\frac{1}{n}}$ and $[K : \mathbb{Q}] = n$ then $e \geq 2 \cdot p$.*

Primes p	required B_p
7	37.11
11	97.30
13	138.74
17	244.63
19	309.18

Table 3.1: Required discriminant bounds to find $e \geq 2 \cdot p$.

We conclude by considering what else we can say for a totally real extension where only the prime 7 is ramified.

Lemma 3.3.6. *Under the assumptions of Proposition 3.3.3, if $p = 7$ and K is a totally real extension we can replace the third condition with $49|e$.*

Proof. If K is a totally real extension we know from [6] that $54.57 \leq |\Delta|^{\frac{1}{n}}$, which, combined with Lemma 3.1.7, gives

$$54.57 \leq 7^{1+\nu_7(e)-\frac{1}{e}}.$$

If $\nu_7(e) \leq 1$, then $7^{1+\nu_7(e)-\frac{1}{e}} < 7^2 = 49$, which would give a contradiction with $(\star\star)$. So we can unconditionally replace the third condition of Proposition 3.3.3 for $p = 7$ with $49|e$ in the totally real case. □

Chapter 4

Non-solvable extensions

4.1 The result in context

In [13, Lemma 2.22], Harbater showed for a group $G \in \pi_A(U_2)$ with $|G| \leq 300$ that G is solvable. Hoelscher generalised this result to hold for more primes:

Theorem 4.1.1. *[27, Proposition 2.2.4] Let $2 \leq p < 29$ be a prime number and G a group in $\pi_A(U_p)$ with $|G| \leq 300$. Then G is solvable.*

This was improved once more by Pollak:

Theorem 4.1.2. *[27, Theorem 2.1.10] Let $2 \leq p < 37$ be a prime number and G a group in $\pi_A(U_p)$ with $|G| \leq 600$ then G is solvable.*

We improved on Theorem 4.1.1 by generalising it to hold for more primes and a lot more orders, although not all for all orders less than 660.

Theorem 4.1.3. *Let $2 \leq p < 101$ be a prime number and G a group in $\pi_A(U_p)$. If the order of G is in Table 4.1 then G is solvable.*

60, 120, 168, 180, 240, 300, 360, 420, 480, 540, 600, 780, 840, 900, 960, 1020, 1080, 1140, 1176, 1200, 1260, 1380, 1500, 1560, 1620, 1740, 1800, 1848, 1860, 1920, 2100, 2220, 2340, 2460, 2580, 2820, 2940, 3060, 3180, 3540, 3660, 3900, 4020, 4140, 4260, 4380, 4740, 4980, 5100, 5220, 5340, 5580, 5700, 5820, 6060, 6180, 6300, 6420, 6540, 6660, 6780, 6900, 7140, 7380, 7620, 7740, 7860, 7980, 8220, 8340, 8460, 8700, 8820, 8940, 9060, 9300, 9420, 9540, 9660, 9780, 10020, 10140, 10380, 10620, 10740, 10860, 10980, 11100, 11460, 11580, 11700, 11820, 11940, 12060, 12300, 12660, 12780, 12900, 13020, 13140, 13260, 13380, 13620, 13740, 13980, 14100, 14220, 14340, 14460, 14700, 14820, 14940, 15060, 15300, 15420, 15540, 15780, 15900, 16020, 16140, 16260, 16620, 16860, 16980, 17220, 17340, 17460, 17580, 17700, 17940, 18060, 18180, 18300, 18420, 18540, 18660, 18780, 19020, 19260, 19380, 19620, 19740, 19860, 20100, 20220, 20340, 20700, 20820, 20940, 21180, 21300, 21420, 21540, 21660, 21900, 22020, 22260, 22380, 22620, 22740, 22860, 22980, 23340, 23460, 23580, 23700, 23820, 24060, 24180, 24540, 24660, 24780, 24900, 25020, 25140, 25260, 25620, 25860, 25980, 26100, 26220, 26340, 26580, 26700, 26820, 26940, 27180, 27420, 27660, 27780, 27900, 28020, 28140, 28260, 28740, 28860, 28980, 29100, 29220, 29340, 29460, 29580, 29820, 29940, 30060, 30180, 30300, 30420, 30540, 30660, 30900, 31140, 31260, 31380, 31620, 31740, 31980, 32100, 32220, 32460, 32580, 32700, 32820, 33060, 33180, 33300, 33420, 33540, 33780, 33900, 34140, 34260, 34380, 34620, 34740, 34860, 35220, 35340, 35460, 35580, 35700, 35820, 35940, 36060, 36420, 36660, 36780, 36900, 37020, 37140, 37380, 37740, 37860, 37980, 38100, 38460, 38580, 38700, 38820, 39060, 39180, 39300, 39540, 39660, 39780, 39900, 40020, 40140, 40380, 40620, 40740, 40860, 40980, 41100, 41220, 41340, 41460, 41700, 41820, 41940, 42060, 42180, 42300, 42420, 42540, 42780, 43020, 43140, 43260, 43380, 43620, 43860, 43980, 44100, 44340, 44580, 44700, 44940, 45060, 45180, 45300, 45420, 45660, 45780, 46020, 46140, 46260, 46380, 46620, 46740, 47100, 47220, 47340, 47460, 47580, 47700, 47820, 47940, 48300, 48420, 48540, 48660, 48780, 48900, 49020, 49260, 49380, 49620, 49740, 49860, 49980.

Table 4.1: Orders for which $G \in \pi_A(U_p)$ is solvable with $2 \leq p < 101$.

4.2 Extending Hoelscher's result to more primes

To prove Theorem 4.1.3 we start by extending Theorem 4.1.1 to hold for any prime p in the range $2 \leq p < 101$ in Proposition 4.2.3. Before we can do this we need to determine the smallest primes such that A_5, S_5 and $PSL(2,7)$ lie in $\pi_A(U_p)$. For this we have the following theorem and the well-known fact that $GL(3,2) \simeq PSL(2,7)$ as for example proven in [7, Theorem 15].

Theorem 4.2.1. *[17, Theorem 4.1 and 4.3]*

- *The smallest prime p such that $S_5 \in \pi_A(U_p)$ is 101;*
- *The smallest prime p such that $A_5 \in \pi_A(U_p)$ is 653;*
- *The smallest prime p such that $GL(3,2) \in \pi_A(U_p)$ is 227.*

We will also need the following Lemma by Harbater to prove Proposition 4.2.3.

Lemma 4.2.2. *[13, Lemma 2.5] Let G be a non-solvable group of order ≤ 500, such that every proper quotient of G is abelian. Let $g \in G$ and n its order. Then one of the following holds:*

1. *$G \simeq A_5$, $n \leq 5$;*
2. *$G \simeq S_5$, $n \leq 6$;*
3. *$G \simeq PSL(2,7)$, $n \leq 7$;*
4. *$1 \to PSL(2,7) \xrightarrow{\phi} G \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \to 1$ is exact, $n \leq 14$;*
5. *$G \simeq A_6$, $n \leq 5$.*

We are now ready to extend Theorem 4.1.1 by Hoelscher to hold for all primes less than 101.

Proposition 4.2.3. *Let $2 \leq p < 101$ be a prime number and G a group in $\pi_A(U_p)$ with $|G| \leq 300$. Then G is solvable.*

Proof. The proof is analogous to that of [27, Proposition 2.1.12]. By this proposition we already know that the statement holds for all primes $2 \leq p < 37$ and we will now show this argument also works for the primes $37 \leq p < 101$. Suppose for a prime $37 \leq p < 101$ that there exists a non-solvable group $G \in \pi_A(U_p)$ and let G be of minimal order. For any non-trivial normal subgroup N we know that $G/N \in \pi_A(U_p)$ by Lemma 2.3.31. Since G was of minimal order and N is non-trivial we know that G/N must be solvable. By Theorem 2.1.48 we know that N must be non-solvable and thus $|N| \geq 60$ by [32]. Together with the bound on $|G|$ this means $|G/N| = \frac{|G|}{|N|} \leq 5$ and so G/N is abelian by [9]. We see that G satisfies the hypothesis of Lemma 4.2.2. Note that $|A_6| = 720$ and since $|G| \leq 300$ we know that Item 5 of Lemma 4.2.2 does not hold. Furthermore, Item 4 of Lemma 4.2.2 says that

$$1 \to \mathrm{PSL}(2,7) \xrightarrow{\phi} G \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \to 1$$

is exact. Combining this with the First Isomorphism Theorem we find that

$$\mathrm{PSL}(2,7) \simeq \mathrm{PSL}(2,7)/1 \simeq \mathrm{PSL}(2,7)/\ker(\phi) \simeq \mathrm{im}(\phi) = \ker(\psi),$$

and so that

$$G/\mathrm{PSL}(2,7) \simeq G/\ker(\psi) \simeq \mathrm{im}(\psi) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Since the order of $\mathrm{PSL}(2,7)$ is 168, the latter implies that the order of G is $2 \cdot 168 > 300$, and so this sequence cannot be exact. We conclude that G must be isomorphic either to A_5, S_5 or $\mathrm{PSL}(2,7)$. However, Theorem 4.2.1 indicates this is not possible either. We have a contradiction and can conclude that G is in fact solvable. □

4.3 Programming Pollak's approach

We are now ready to explain which argument of Pollak we implemented in [11, GAP] and how this rules out the existence of any remaining non-solvable groups in $\pi_A(U_p)$ of orders in Table 4.1 for $2 \leq p < 101$.

Proof of Theorem 4.1.3. Let $2 \leq p < 101$ be a prime number and $G \in \pi_A(U_p)$ whose order is some value in Table 4.1. We know that the statement holds if $|G| \leq 300$ by Proposition 4.2.3. We will proceed inductively to prove the statement for the orders greater than 300 in Table 4.1 in the following way. Let n be the smallest order from Table 4.1 for which the statement has not yet been checked. Let X_n denote the collection of all non-solvable groups of order n. Our goal is to show for all $H \in X_n$ that $H \notin \pi_A(U_p)$. By the same argument as in the proof of Proposition 4.2.3 it is enough to find a normal subgroup $1 \neq N \trianglelefteq H$ such that H/N is non-solvable and the order $|H/N|$ is in Table 4.1. We have written a program which implements the above idea in GAP in order to obtain the data in Table 4.1. A more legible pseudo version of the program can be found in Listing 4.1 and the GAP code can be found in the Appendix (7). Theorem 4.3.1 explains how this program works and with that concludes the proof of Theorem 4.1.3.

□

Listing 4.1: Gap implementation

```
AllNonSolvableOrders:= [60, 120, 168, 180, 240,...];
#Defining a list of all orders up to 50064 for which non-solvable groups
#exist.

BadOrders:= [];
#Defining a list which will store the orders for which there is at least
#one group which does not admit a non-solvable quotient.

BadGroups:= [];
#Defining a list which will store the groups which do not admit a
#non-solvable quotient.

NotCubeFree:= [];
#Defining a list of orders for which GAP does not contain
#the groups because their orders are above 2000 and are divisible
#by a cube.
#See Remark 4.3.2.

GoodOrders := [60, 120, 168, 180, 240, 300, 336, 360, 420, 480, 504,
540, 600];
#Defining a list of orders for which Theorem 4.1.3 was already proven by
#Hoelscher and Pollak.

AddnToList:= true;
#Defining a boolean to indicate whether or not the current order n should
#be added to the list of good orders.


#Initiating a function which determines if a group G has a non-solvable
```

```
#quotient.
NonSolvQuotientFinder := function (G)
Defining local variables: NormalSubs, H, GroupHasNonSolvQuotient, F;

NormalSubs(G) := [A function which generates a list containing the normal
    subgroups of G];

GroupHasNonSolvQuotient := false;
#Defining a boolean telling us if G admits a non-solvable quotient.

for H in NormalSubs do
        F := G/H;
        if |H| = 1 then
                stop;
        else if |H| = |G| then
                stop;
        else if F is not solvable then
                if |F| is in GoodOrders then
                    Print(G, H, |F|);
                    GroupHasNonSolvQuotient:= true;
                    return;




if GroupHasNonSolvQuotient = false then
        AddnToList := false;
        Print(G does not admit a non-solvable quotient);
        Add G to BadGroups;

end function;

#Initiating a function which checks for all non-solvable groups G
#of order n whether or not they admit a non-solvable quotient.
AllGroupsOfOrder := function(n)
Defining local variables G, NonSolvGroupsOfOrdern;

NonSolvGroupsOfOrdern(n) := [A function which generates a list of all
                            non-solvable groups of order n];

for G in NonSolvGroupsOfOrdern do
        NonSolvQuotientFinder(G);


if n>300 and AddnToList = true then
        Add n to GoodOrders;

else AddnToList = false then
        Add n to BadOrders;
```

```
end function;

#Initiating a function which checks if an order n is cubefree.
CubeFree := function(n)
Defining local variables Prime, Divisors, Cube, nIsCubeFree ;

Divisors(n) := [A function which generates a list of the distinct
                prime divisors of n];
nIsCubeFree := true;

for Prime in Divisors do
        Cube := Prime*Prime*Prime;

        if Gcd(Cube,n) = Cube then
                nIsCubeFree := false;


return nIsCubeFree;
end function;

#Initiating a function which executes AllGroupsOfORder(n) for
#all non-solvable orders n less than B.
#The function takes into account that n is between 600 and 2016 or
#that n is cubefree in order to be able to use the available groups in
#the GAP library. See Remark 4.3.2.
CheckUpToOrder:= function(B)
Defining local variable j;

for j in AllNonSolvableOrders do
        if j>600 then
                AddnToList := true;
                if j<B then
                if j = 360 then
                    stop;
                        else j<2016 then
                                AllGroupsOfOrder(j);
                        else if CubeFree(j) = true then
                                AllGroupsOfOrder(j);
                        else if CubeFree(j) = false then
                                Add j to NotCubeFree;




Print(We cannot check these orders: NotCubeFree);
Print(This does not work for these orders: BadOrders);
Print(These are the groups for which it does not work: BadGroups);
Print(The Theorem holds for these orders: GoodOrders);
end function;
```

Theorem 4.3.1. *The program described in Listing 4.1 works.*

Proof. As starting data the program already has a list "AllNonSolvableOrders" which contains all orders for which non-solvable groups exist [32]. Furthermore, it has a list "GoodOrders" which stores the orders of non-solvable groups for which the statement of Theorem 4.1.3 has already been checked and which will make up Table 4.1 once the program is done. Upon calling the program for the first time this list contains all orders up to and including 300, since this is what we proved in Proposition 4.2.3. It will also contain the order 360. As Pollak points out in [27, Example 2.1.14] there are 6 non-solvable groups of this order. Five of them admit a non-solvable quotient, and so by the argument in the proof of Theorem 4.1.3 these groups cannot lie in $\pi_A(U_p)$ for the primes $2 \leq p < 101$. The final group of order 360 is A_6 and it was proven in [17, Theorem 4.2] that $p = 1579$ is the smallest prime such that $A_6 \in \pi_A(U_p)$. Hence all groups of order 360 in $\pi_A(U_p)$ for $2 \leq p < 101$ are solvable. When running the above code in GAP we call the function "CheckUpToOrder(B)" for some positive integer bound B. For every order $300 < n < B$ in "AllNonSolvableOrders", apart from the exceptions, which are discussed in Remark 4.3.2, the program will compute all groups G of order n and call the function "NonSolvQuotientFinder(G)" for every such group G. This function computes all non-trivial normal subgroups N of G and checks for every such subgroup if the quotient is non-solvable. If this is the case the program tells us this, together with the group G, the subgroup H and the size of the quotient, before moving on to the next group. If there is no normal subgroup N such that G/N is non-solvable the program tells us this, together with the group G. If all non-solvable groups G of order n admit a non-solvable quotient we can add n to the list "GoodOrders" as is explained in the proof of Theorem 4.1.3. If there is at least one group of order n for which this is not the case we add n to the list "BadOrders". Furthermore, we keep track of each of these groups which do not admit a non-solvable quotient in the list "BadGroups". We elaborate on why we do this in Example 4.4.1. After doing this for all $n < B$ we find that the list of "GoodOrders" is exactly the values in Table 4.1. □

Remark 4.3.2. The library of GAP [11] contains a large, but limited amount of groups for us to check:

1. Those of order at most 2000;
2. Those of cubefree order of at most 50000;
3. Those of order p^7 for the primes $p = 3, 5, 7, 11$;
4. Those of order p^n for $n \leq 6$ and all primes p;
5. Those of order $q^n \cdot p$ for q^n dividing $2^8, 3^6, 5^5$ or 7^4 and all primes p with $p \neq q$;
6. All groups of squarefree order;
7. Those whose order factorises in at most three primes.

However, we do not need to check all these groups. It turns out we are only interested, and will check, all non-solvable orders up to 2000 and after this the program checks the non-solvable groups whose order is cubefree and less than 50000. We explain below why we do not need to check the other families which GAP stores.

We are not interested in the groups in Item 3, since we are only checking non-solvable groups which a priori can only have an even order by Theorem 2.1.46. Item 4 is ruled

our for the same reason paired with the fact that there are no non-solvable groups of order 2^n for any $n \leq 6$ [32]. By Theorem 2.1.47 and group of order $q^n \cdot p$ will be solvable and so Item 5 will not give us any new non-solvable groups to check. Since the order of every non-solvable group is divisible by 4 [32] none of them will be square-free so Item 6 does not apply either. Finally we know that any order of a non-solvable group will be divisible by 4 and either 3 or 5 [32], which already gives a minimum of three primes in its factorisation. Hence a non-solvable group whose order factorises into at most three primes would contain either 12 or 20 elements and we know there are no non-solvable groups of these orders. We can conclude that Item 7 also does not give us any new non-solvable groups to check. If the library of GAP expands we would be able to check more orders.

4.4 Obstructing groups

Note that Theorem 4.1.3 does not imply Pollak's Theorem 4.1.2. This is because there are non-solvable groups of order less than or equal to 600 which do not admit a non-solvable quotient. For every order n that our program checks it keeps track of the groups that obstruct it from going into Table 4.1 by collecting these groups in the appropriately named list "BadGroups". We give the first few of these orders in Table 4.2 together with one of the obstructing groups for each order.

Order n	Number of non-solvable groups of order n	Number of obstructing groups	Example of obstructing group
336	3	1	$PGL(2,7)$
504	2	1	$PSL(2,8)$
660	2	1	$PSL(2,11)$
672	8	4	$PSL(3,2) \rtimes \mathbb{Z}/4\mathbb{Z}$
720	23	3	S_6

Table 4.2: "BadGroups" - Non-solvable groups which do not have a non-solvable quotient.

Similar to Pollak [27, Example 2.1.13, 2.1.14, 2.1.18] we can try to use other arguments to show that the groups in "BadGroups" cannot lie in $\pi_A(U_p)$ for $2 \leq p < 101$ in the hopes of adding more orders to Table 4.1. We will sketch the various methods Pollak used for this. Assume that there is some field K which is ramified only at p and which realises G. Then we start by reasoning that all the primes which divide $|G|$ do not work. One way of doing this is to use the subgroups of G and their corresponding subfields of K and for small primes we can use the discriminant bounds of [6] and [26] together with Lemma 3.1.7. If we manage this we know that the ramification must be tame. This means the inertia group must be a cyclic subgroup of G which leaves only so many options. Using various facts about the decomposition and intertia group, Pollak manages to show that the remaining primes we want to rule out also do not allow for $G \in \pi_A(U_p)$. The exact nature of each step depends on the group we are dealing with. We tried using the various approaches Pollak describes in [27, Example 2.1.13, 2.1.14, 2.1.18] for all of the obstructing groups of all the orders in Table 4.2, but for each of them some part of the above process did not work. We do however have the following.

Example 4.4.1. There are three non-solvable groups of order 720 which do not admit a non-solvable quotient. One of them is S_6 which does not lie in $\pi_A(U_p)$ for $2 \leq p < 101$ as proven by Jones and Roberts in [17, Theorem 4.2]. Hence, we only need to show that two more groups do not lie in $\pi_A(U_p)$ in order to conclude 720 should be in Table 4.1.

Chapter 5

Examples of the Boston-Markin Conjecture

5.1 A totally real S_3-extension

Recall from the introduction that the Boston-Markin Conjecture [5, Conjecture 1.2] says that a group G for which the abelianisation has a minimal generating set of d elements, should appear as the Galois group of a number field which ramifies at exactly d primes (including the prime at infinity). For a group with cyclic abelianisation this would mean finding a totally real number field which ramifies at one finite prime. We require it to be totally real, because any totally complex number field will ramify at the prime at infinity as well as a finite prime by Corollary 2.2.23, making for a total of two ramified primes which is more than the Conjecture suggests. In particular, the symmetric and alternating groups have an abelianisation which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Example 5.1.1. In lmfdb we can look for S_3 extensions and filter out those which are not totally real. We do this by specifying the signature of any extension we get to be $[6, 0]$ which simply means there are 6 real embeddings of the extension. This ensures us to find a totally real Galois extension since the order of S_3 (and hence the degree of the extension and the number of embeddings) is 6. In the end we sort our results on ramified prime count to find a totally real S_3-Galois extension as the splitting field of $x^6 - 2x^5 - 14x^4 + 14x^2 - 2x - 1$ ([20, 6.6.12008989.1]) which ramifies only at the prime 229.

For every n with $2 \leq n \leq 30$, Pollak [27, Example 2.1.21] provides a polynomial of degree n whose splitting field is an S_n-extension of $\mathbb{Q}$ which ramifies at a single finite prime. He used Sage to compute the discriminant of these polynomials and then determined whether these are divisible by a single prime. Magma was used in each case to verify that the corresponding Galois group is indeed the symmetric group. Using Magma [4] we compute that each of these polynomials admits at least one complex root. Since any embedding of such a splitting field into $\mathbb{C}$ has to map non-real complex numbers to non-real complex numbers we see that each of these splitting fields only admit complex embeddings. As discussed, this means that the infinite prime does ramify in these instances giving a total of two primes ramifying in these extensions. It would be interesting to see if we could find totally real S_n extensions which ramify at a single finite prime like in Example 5.1.1 for more n.

Remark 5.1.2. In search of totally real S_n-extensions we might hope to find totally real subfields of the given extensions by Pollak in [27, Example 2.1.21]. Indeed, any subfield of such an S_n-extension would also ramify at a single finite prime by Lemma 2.2.26.

However, we claim that there are no interesting subextensions of these S_n-extensions. Firstly, we would only be interested in subfields which are also Galois over $\mathbb{Q}$ and so any such subfield would correspond to a normal subgroup of S_n by Theorem 2.3.11. Since S_n is simple for $n \geq 5$ there is no hope for any (non-trivial) subfields in this case. If $n = 2$ there are no non-trivial subfields since a Galois S_2-extension has degree 2 over $\mathbb{Q}$. If $n = 3$ there is one normal subgroup $A_3 \trianglelefteq S_3$. However, the Galois group of the corresponding extension is $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$, which is abelian and we already know the Conjecture holds for all abelian groups by Theorem 1.2.2. If $n = 4$ we have A_4 and the Klein group V_4 as normal subgroups of S_4. Similar to A_3, we know that A_4 does not tell us anything interesting and for V_4 we know the quotient is $S_4/V_4 \simeq S_3$. However, the S_4-extension which Pollak gives in [27, Example 2.1.21] ramifies at the prime 229 and we already have a totally real S_3-extension which ramifies at the prime 229 in Example 5.1.1.

5.2 Constructing examples using direct products

Unfortunately lmfdb does not contain totally real S_n extensions for $n > 3$. However, we can still investigate other groups with a cyclic abelianisation with the hopes of finding more examples of the Boston-Markin conjecture.

Example 5.2.1. Similar to the symmetric and alternating groups the dihedral groups D_{2n} of order $2n$ for n odd have an abelianisation isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We used GAP[11] to check for all non-abelian groups up to order 47 if they have a cyclic abelianisation. If so, we checked with lmfdb [20] if such a group is realised by a number field where a single prime ramifies. Table 5.1 contains the groups that GAP gave us for which lmfdb had such a number field. We included the GAP group ID in the case of a semidirect product in order to have no confusion about which semidirect product we mean.

Group G	abelianisation G^{ab}	Discriminant Δ_K	Totally real extension K in lmfdb
D_6	$\mathbb{Z}/2\mathbb{Z}$	229^3	[20, 6.6.12008989.1]
D_6	$\mathbb{Z}/2\mathbb{Z}$	257^3	[20, 6.6.16974593.1]
D_{10}	$\mathbb{Z}/2\mathbb{Z}$	1093^5	[20, 10.10.1559914552888693.1]
D_{10}	$\mathbb{Z}/2\mathbb{Z}$	1429^5	[20, 10.10.5958832035878149.1]
D_{14}	$\mathbb{Z}/2\mathbb{Z}$	577^7	[20, 14.14.21292697885552828353.1]
D_{14}	$\mathbb{Z}/2\mathbb{Z}$	1009^7	[20, 14.14.1064726745878753869969.1]
D_{18}	$\mathbb{Z}/2\mathbb{Z}$	1129^9	[20, 18.18.298020045939340081313832976 9.1]
D_{18}	$\mathbb{Z}/2\mathbb{Z}$	3137^9	[20, 18.18.2941918709901560330077723287 0977.1]
D_{22}	$\mathbb{Z}/2\mathbb{Z}$	1197^{11}	[20, 22.22.17471883970840462300304775614373553.1]
$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ([12, 1])	$\mathbb{Z}/4\mathbb{Z}$	761^9	[20, 12.12.85597663644117187118144441.1]
$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ([12, 1])	$\mathbb{Z}/4\mathbb{Z}$	2713^9	[20, 12.12.7962476138101219604907410499673.1]
$S_3 \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	4597^{15}	[20, 18.18.865202082819353469829834423700878491063874665024911209 3.1]
$S_3 \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	7057^{15}	[20, 18.18.536169075309126110397762728710839837600934204262090225 4193.1]
$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ([20, 1])	$\mathbb{Z}/4\mathbb{Z}$	401^{15}	[20, 20.20.11147194766737332313252352656931368060 01.1]
$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ([20, 3])	$\mathbb{Z}/4\mathbb{Z}$	457^{15}	[20, 20.20.79203249707529807211386221683293252031 93.1]
$\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ ([21, 1])	$\mathbb{Z}/3\mathbb{Z}$	313^{14}	[20, 21.21.866205078521369863138032297285518 89.1]
$\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ ([21, 1])	$\mathbb{Z}/3\mathbb{Z}$	877^{14}	[20, 21.21.159218785599036824660651669785398798634009.1]

Table 5.1: Totally real G-extensions which ramify at a single finite prime (and not at the prime at infinity).

It is already proven by Boston and Markin that their Conjecture holds for all groups of order less than or equal to 32 [5, Theorem 3.1]. Hence, Examples 5.1.1 and 5.2.1 are not surprising. However, we will use them to illustrate a method of constructing some new examples of the Boston-Markin Conjecture out of existing ones.

Proposition 5.2.2. *Let $p_1, .., p_n$ be distinct primes and $G_1, .., G_n$ be finite groups. Let $K_1, .., K_n$ be totally real Galois extensions of $\mathbb{Q}$ where each K_i is ramified only at p_i and has Galois group G_i. Then the compositum $C := K_1 \cdot .. \cdot K_n$ is a totally real $G_1 \times .. \times G_n$-Galois extension which only ramifies at the primes $p_1, .., p_n$.*

Proof. Proposition 2.3.15 tells us that C is again Galois over $\mathbb{Q}$ and that $\mathrm{Gal}(C/\mathbb{Q})$ is contained in $G_1 \times .. \times G_n$. We claim that the intersection of all the fields in the compositum is trivial, i.e. $I := \cap_i K_i \simeq \mathbb{Q}$ from which it follows by Corollary 2.3.16 that $\mathrm{Gal}(C/\mathbb{Q}) \simeq G_1 \times .. \times G_n$. To see this intersection is trivial we firstly note that I cannot ramify at any p_i. Assume that I does ramify at some p_i and note that $I \subset K_j$ for all $j \neq i$. Then Corollary 2.2.25 would imply that K_j also ramifies at p_i. Similarly C can also not ramify at any other prime than some p_i because all K_i are unramified outside respectively p_i. Hence C is an unramified extension of $\mathbb{Q}$, which must be trivial by Corollary 2.2.23. Furthermore, the compositum of any finite number of totally real extensions is again totally real. We argue this for two totally real extensions, say K and L. To see this, first note that any embedding σ of KL can be restricted to an embedding of K or L. Since both only admit real embeddings we know that these restrictions σ_K and σ_L must have a real image. Since K and L are number fields we can see KL as $K(L)$ where we adjoin the generators of L to K. Hence, the image of any embedding of KL is determined by the image of K and the images of the generators of L, both of which we just saw have to be real. It is clear that we can repeat this argument to conclude that C is also totally real. By [21, Theorem 31, page 76] we know that C is unramified outside of the primes p_i for all i. With Corollary 2.2.25 we also know that C does ramify at p_i for all i which concludes the proof. □

We will now illustrate how to put Proposition 5.2.2 into action with the groups in Example 5.2.1.

Proposition 5.2.3. *Let $G_1, .., G_n$ be a collection of groups chosen from Table 5.1 such that their abelianisations are the same and the corresponding extensions pairwise ramify at distinct primes. Then the product $G_1 \times .. \times G_n$ is an example of the Boston-Markin conjecture for n primes.*

Proof. Let K_i denote the corresponding Galois extension for G_i from Table 5.1 and p_i the corresponding prime which is ramified. By Proposition 5.2.2 we know that $G_1 \times .. \times G_n$ is realised by the compositum of all K_i which is a totally real Galois extension that ramifies only at the primes p_i. Because the compositum is totally real we know that there the prime at infinity does not ramify. To show this is an example of the Boston-Markin conjecture we need to prove that a minimal generating set of $(G_1 \times .. \times G_n)^{\mathrm{ab}}$ has n elements. Using Proposition 2.1.9 repeatedly we see that $(G_1 \times .. \times G_n)^{\mathrm{ab}} \simeq G_1^{\mathrm{ab}} \times .. \times G_n^{\mathrm{ab}}$. We chose all the groups in Table 5.1 to have cyclic abelianisation, hence a generating set could consist of the n tuples where we have a generator of G_i on position i and identities on every other position. We are left to show that there cannot be a generating set with less elements, so assume there is a generating set with k elements where $k < n$. Any generator must be of the form $(g_1, .., g_n)$ where $g_i \in G_i^{\mathrm{ab}}$. The order of such a generator is the least common multiple of the orders of all g_i. We assumed all the abelianisations G_i^{ab} to be the same, hence we know that the order of a generator $(g_1, .., g_n)$ is at most the order of G_i^{ab}. Furthermore, $|(G_1 \times .. \times G_n)^{\mathrm{ab}}| = |G_1^{\mathrm{ab}} \times .. \times G_n^{\mathrm{ab}}| = |G_1^{\mathrm{ab}}| \cdot .. \cdot |G_n^{\mathrm{ab}}| = n \cdot |G_i^{\mathrm{ab}}|$, which means that this generating set has to generate $n \cdot |G_i^{\mathrm{ab}}|$ elements. However, every generator has an order of at most $|G_i^{\mathrm{ab}}|$ and so together they generate at most $k \cdot |G_i^{\mathrm{ab}}|$ elements which is not enough by our assumption that $k < n$. We conclude there cannot be less than n generators and that a minimal generating set consists of n elements. □

Proposition 5.2.3 allows us to make many combinations of groups in Table 5.1 but still restricts us to take groups which have the same abelianisation. The reason for this restriction stems from the fact that we do not know the minimal generating set of arbitrary

products of the abelianisations if the groups we take in the product are distinct. We can say a bit more if we restrict the product to have two components.

Proposition 5.2.4. *Let G and H be groups realised by numberfields K and L respectively. Assume that K only ramifies at p and that L only ramifies at q where p and q are distinct primes. Assume* $\gcd(|G^{\mathrm{ab}}|, |H^{\mathrm{ab}}|) \neq 1$. *Then $G \times H$ is an example of the Boston-Markin conjecture for two primes.*

Proof. Since G and H are realised by numberfields which ramify at a single prime we know their abelianisations must be cyclic by Corollary 2.3.32. By Proposition 2.1.9 we know that $(G \times H)^{\mathrm{ab}} \simeq G^{\mathrm{ab}} \times H^{\mathrm{ab}}$ and since $|G^{\mathrm{ab}}|$ and $|H^{\mathrm{ab}}|$ are not coprime we see with Proposition 2.1.10 that the direct product is not cyclic. Hence the abelianisation of $G \times H$ has a minimal generating set of two elements. The rest of the argument is identical to the proof of Proposition 5.2.3. □

The upshot of this discussion is that Propositions 5.2.3 and 5.2.4 allow us to create groups of order larger than 32 which are examples of the Boston-Markin conjecture as illustrated in Example **??** In Table 5.1 we purposely gave several extensions for a fixed group, provided lmfdb had multiple options, to indicate that we do not need to take the product of two distinct groups. We do however want to make sure the ramifying primes in the corresponding extensions are distinct, which we did in Table 5.1.

Example 5.2.5. There exists a $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} \times S_3 \times \mathbb{Z}/3\mathbb{Z}$-extension which only ramifies at the primes 4597 and 313 by Proposition 5.2.4 and there exists a $D_6 \times D_6 \times D_{10} \times D_{14} \times D_{18} \times D_{22}$-extension which only ramifies at the primes 229, 257, 1093, 577, 1129 and 1197 by Proposition 5.2.3. Both of these groups are examples of the Boston-Markin Conjecture and we can of course take a lot more combinations from Table 5.1.

Chapter 6

Further Research

1. Our program in Chapter 4 keeps track of all the groups which do not admit a non-solvable quotient in the list "BadGroups". As noted at the end of Section 4, Pollak has other arguments (see [27, Example 2.1.13, 2.1.14 and 2.1.18]) to show that a specific group cannot lie in $\pi_A(U_p)$ for primes p in some range. We would want to show that the groups in "BadGroups" cannot lie in $\pi_A(U_p)$ for primes $p < 101$. We pointed out that we tried to apply these arguments to the first few groups in "BadGroups" and that at first glance there seems to be some problem for each group. It would be interesting to spend more time on this and try to adapt the arguments of Pollak to work for the groups we are dealing with.

2. In [27, Example 2.1.21] Pollak computes various examples of S_n extensions which ramify at a single finite prime. His approach is to compute discriminants of polynomials of the form $x^n + ax^k + b$ for various choices of n, k, a and b where n and k are coprime. If these discriminants only have a single prime dividing it, he computes the splitting field and checks what the Galois group is. Whatever the Galois group G might be, this approach gives examples of G-extensions which only ramify at a single finite prime and it would be interesting to try this for various other polynomials and see what groups occur. In particular, this then tells us that we can solve the inverse Galois problem for the groups G that we find in this process.

3. As noted in Chapter 5, the above-mentioned examples of Pollak are not totally real extensions and hence also ramify at the infinite prime. In particular this means that they do not serve as examples of the Boston-Markin conjecture. It would therefore be interesting to try and find more totally real S_n extensions which ramify at a single finite prime like in Example 5.1.1. We used lmfdb to create this example and tried to find others but, at the moment, the database does not allow for S_n or A_n examples for $n > 3$.

4. In Chapter 5 we explained how we can use two extensions which ramify at a single prime to create an extension which ramifies at two primes. We also gave the corresponding Galois group as the direct product of the respective groups. In [34, Page 243] Stoll gives several values for $a \in \mathbb{Z}$ such that for all $n \geq 1$ we have

$$\mathrm{Gal}(f^n/\mathbb{Q}) \simeq [\mathbb{Z}/2\mathbb{Z}]^n,$$

where $f = x^2 + a$, $\mathrm{Gal}(f^n/\mathbb{Q})$ denotes the Galois group of the splitting field of the n^{th} iterate of f over $\mathbb{Q}$ and $[\mathbb{Z}/2\mathbb{Z}]^n$ denotes the n^{th} wreath product. In light of this result, it is worth investigating if the wreath product can also be used to construct more examples of the Boston-Markin Conjecture.

Chapter 7

Appendix

This **link** redirects to a text document which contains the GAP code for the program described in Theorem 4.3.1. To run the code you need version 4 of [11, GAP]. In GAP you can paste the code and then press enter. After this you can type the command "CheckUpToOrder(50065);" and press enter again.

Bibliography

[1] Michael Atiyah, Introduction to commutative algebra, CRC Press, 2018.

[2] John A. Beachy and William D. Blair, Abstract algebra, Waveland Press, 2019.

[3] Frits Beukers, Course notes rings and galois theory, `https://webspace.science.uu.nl/~beuke106/ringengalois/dic.pdf`, 2016.

[4] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3-4, pp. 235–265.

[5] Nigel Boston and Nadya Markin, The fewest primes ramified in a g-extension of Q, Ann. Sci. Math. **33** (2009), no. 2, pp. 145–154.

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

[7] David S. Dummit and Richard M. Foote, Abstract algebra, third ed., Wiley, 2004.

[8] Jan-Hendrik Evertse, Course notes diophantine approximation, `https://www.math.leidenuniv.nl/~evertse/dio17-3.pdf`, 2023.

[9] Ahmed Fares, Orders of non-abelian groups, `https://oeis.org/A060689`, Accessed: 26-06-2023.

[10] Walter Feit and John G. Thompson, Solvability of groups of odd order, Pacific J. Math. **13** (1963), no. 3, pp. 775–1029.

[11] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.12.2, 2022.

[12] Carl F. Gauss, Disquisitiones arithmeticae (english translation, second, corrected edition translated by arthur a clarke), Springer Verlag, 1986.

[13] David Harbater, Galois groups with prescribed ramification, Contemporary Mathematics **174** (1994), pp. 35–60.

[14] Godfrey H. Hardy, Edward M. Wright, et al., An introduction to the theory of numbers, Oxford university press, 1979.

[15] David Hilbert, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten., J. Reine Angew. Math. **110** (1892), pp. 104–129.

[16] Jing Long Hoelscher, Galois extensions ramified at one prime, University of Pennsylvania, 2007.

[17] John W. Jones and David P. Roberts, Number fields ramified at one prime, International Algorithmic Number Theory Symposium, Springer, 2008, pp. pp. 226–239.

[18] Hershy Kisilevsky and Jack Sonn, On the minimal ramification problem for -groups, Compositio Mathematica **146** (2010), no. 3, pp. 599–606.

[19] Julio P. Lafuente, Homomorphs and formations of given derived class, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. 3, pp. 437–441.

[20] The LMFDB Collaboration, The L-functions and modular forms database, `https://www.lmfdb.org`, 2023, [Online; accessed 22 June 2023].

[21] Daniel A. Marcus and Emanuele Sacco, Number fields, vol. 1995, Springer, 1977.

[22] Nina E. Menezes, Random generation and chief length of finite groups, `https://research-repository.st-andrews.ac.uk/handle/10023/3578`, 2013.

[23] Hough L. Montgomery and John M. Masley, Cyclotomic fields with unique factorization., Journal für die reine und angewandte Mathematik **0286/0287** (1976), pp. 248–256.

[24] Jürgen Neukirch, Algebraic number theory, vol. 322, Springer Science & Business Media, 2013.

[25] Akito Nomura, Notes on the minimal number of ramified primes in some l-extensions of q, Archiv der Mathematik **90** (2008), no. 6, pp. 501–510.

[26] Andrew Odlyzko, Some unpublished materials, `https://www-users.cse.umn.edu/~odlyzko/unpublished/index.html`, 1976, Accessed: 28-04-2023.

[27] Benjamin Pollak, Ramification in the inverse galois problem, Journal of Number Theory **220** (2021), pp. 34–60.

[28] Joseph J. Rotman, An introduction to the theory of groups, vol. 148, Springer Science & Business Media, 2012.

[29] Jack Schmidt, Course notes chief factors, `https://www.ms.uky.edu/~jack/2008-03-05-ChiefFactors.pdf`, 2008.

[30] Jean-Pierre Serre, Topics in galois theory, CRC Press, 2016.

[31] Igor R. Shafarevich, Construction of fields of algebraic numbers with given solvable galois group, Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya **18** (1954), no. 6, 525–578.

[32] Neil J. A. Sloane, Orders of non-solvable groups, `https://oeis.org/A056866`, Accessed: 29-05-2023.

[33] Peter Stevenhagen, Course notes number rings, 2017.

[34] Michael Stoll, Galois groups over of some iterated polynomials, Archiv der Mathematik **59** (1992), no. 3, pp.239–244.

[35] Josh Swanson, Algebraic number theory lecture notes, 2016.

[36] Lawrence C. Washington, Introduction to cyclotomic fields, vol. 83, Springer Science & Business Media, 1997.