THE INVERSE GALOIS PROBLEM FOR NILPOTENT GROUPS OF ODD ORDER

ADAM MASSEY

Abstract. Consider any nilpotent group G of finite odd order. We ask if we can always find a galois extension K of $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong$ G. This is the famous Inverse Galois Problem applied to nilpotent groups of finite odd order. By solving the Group Extension Problem and the Embedding Problem, two problems that are related to the Inverse Galois Problem, we show that such a K always exists. A major result of Shafarevich tells us that such a K exists for all solvable groups G, but the proof is far too difficult to be presented here. Nevertheless, we present Shafarevich's results and a sketch of the main idea. We then show that for the group S_n, one can use elementary techniques in Galois Theory to solve the Embedding Problem, constructing a solution to the Inverse Galois Problem for this group as well.

Contents

1. Introduction 1
2. Cohomology and the Group Extension Problem 3
2.1. Group Rings and the Augmentation Ideal 3
2.2. Homology and Cohomology Theory of Groups 6
2.3. The Group Extension Problem and the Embedding Problem 9
3. Abelian Groups and Nilpotent Groups of Odd Order 13
3.1. Abelian Groups 14
3.2. Algebraic Number Theory I: Ramification 16
3.3. Algebraic Number Theory II: Local Fields 20
3.4. Nilpotent Groups of Odd Order 22
3.5. The Split Extension Case 24
3.6. The Non-split Extension Case 29
4. An Exploration of more General Groups 40
4.1. Shafarevich's Theorem for General Solvable Groups 40
4.2. A Number Field Extension with Galois Group S_n 42
4.3. A Second Approach To Solving The Inverse Galois Problem for S_n 44
Acknowledgements 45
References 45

1. Introduction

Galois Theory began in the early 1800's when mathematicians were exploring the solvability of general polynomials by radicals. It had been known since the days of the Babylonians that a quadratic equation existed, and the cubic and quartic formulas were known by the mid-1500's, but it was unknown whether or not a general polynomial of degree n was solvable by radicals (that is, if all of its roots could be expressed by radicals).

Date: May 22, 2006.

Key words and phrases. Inverse Galois Problem, Cohomology of Groups, Group Extension Problem, Embedding Problem, Nilpotent Group.

It was the idea of the young mathematician Evariste Galois to associate a new mathematical object (which modern mathematicians now know as a group) to a given field extension L/K (usually $K = \mathbb{Q}$) and then to use the information gained from this new perspective to discuss the general solvability of polynomials by radicals. This association is often given by the following theorem:

Theorem 1.1 (Fundamental Theorem of Galois Theory)**.** *Suppose you have a field F and a Galois extension $L \supset F$ with $Gal(L/F) = G$. Let α be the map from the set of all intermediate fields K (so $F \subset K \subset L$) to the set of subgroups H of G given by $\alpha(K) = Gal(L/K)$, and let β be the map from the above set of subgroups to the above set of intermediate fields given by $\beta(H) = L^H$. Then:*

1.) α and β are inclusion-reversing. If $K_1 \subset K_2$, then $\alpha(K_1) \supset \alpha(K_2)$, and if $H_1 \subset H_2$, then $\beta(H_1) \supset \beta(H_2)$.

2.) $\beta(\alpha(K)) = K$ and $\alpha(\beta(H)) = H$; hence α and β are bijections between all subgroups of G and all intermediate fields $F \subset K \subset L$.

3.) If $K = \beta(H)$, then $[L : K] = |H|$.

Proof. For a good proof of this theorem, see [DF] or [Rot]. □

With this theorem and a little work, Galois was able to prove that a polynomial $f(x) \in F[x]$ is solvable by radicals if and only if the the field extension of it's splitting field L over the ground field F has $Gal(L/F)$ solvable. This led to the beginning of both Group Theory and Galois Theory in modern algebra. Given the origins of groups as Galois Groups, mathematicians naturally asked if one could always realize a given group G as some Galois Group (for this paper, unless otherwise specified, we will confine ourselves to finite groups). Consider a group G of order n, the field $L = \mathbb{C}(x_1, ..., x_n)$ of rational functions in n independent variables over the complex numbers, and the group S_n, the symmetric group on n letters. One can show that $L^{S_n} = \mathbb{C}(s_1, ..., s_n)$, where s_i is the i^{th} symmetric polynomial, and $Gal(L/L^{S_n}) \cong S_n$. Then we invoke Cayley's Theorem that any group G injects into the permutations of G, and since $Perm(G) \cong S_n$, we may realize G as a subgroup of S_n. By the Fundamental Theorem of Galois Theory, we may then find L^G such that $L^{S_n} \subset L^G \subset L$, and $Gal(L/L^G) \cong G$. So we can, indeed, always realize a given group G as some Galois Group.

In the above work, we assume we can freely move the bottom field to find our desired extension. Looking at this, Emmy Noether asked the natural question: Can we realize G as the Galois Group over a fixed ground field? In particular, if we fix the ground field to be $\mathbb{Q}$, can we find an extension $L/\mathbb{Q}$ such that $Gal(L/\mathbb{Q}) \cong G$? To date this is a famous open problem in mathematics, which we will explore several aspects of in this paper.

We begin in §2 with an introduction to the elements of homological algebra relating to the Inverse Galois Problem. In particular, we go through the trouble of developing a good theory of homology and cohomology for groups in §2.1 and §2.2. It's a lot of work, but the reward is an array of tools that can be used to look at the Inverse Galois Problem via two related problems: The Group Extension Problem and the Embedding Problem, which are both explored in §2.3.

In §3 we begin to solve the Inverse Galois Problem for special classes of groups. We begin in §3.1 by solving the Inverse Galois Problem for abelian groups. While this particular proof doesn't make use of the techniques of §2, it does provide us a good starting point for the Group Extension problem in more difficult cases. With this result in place, we begin to develop the basic ideas of algebraic number theory in §3.2 and §3.3, with particular emphasis on the theory of ramification in both the global and local field settings. Using the results of §2 along with those from §3.2 and §3.3, we show that the Inverse Galois Problem is solvable for every nilpotent group

of odd order in §3.4. Doing so requires that we show that, for every p-group (for $p \neq 2$), the Inverse Galois Problem is solvable, which we work out in two separate cases in §3.5 and §3.6.

In §4 we explore the Inverse Galois Problem for more general groups. In §4.1, we discuss the major result of Shafarevich that for any finite solvable group G, the Inverse Galois Problem has a solution. This is one of the biggest breakthroughs in modern algebraic number theory, so we present the results here. In §4.2, we use techniques of basic galois theory to show that for S_n, the Inverse Galois Problem has a solution. In general this method is not efficient, but for certain groups (like S_n), it turns out to be particularly effective. This shows that even certain non-solvable groups still have a solution to the Inverse Galois Problem, and solutions can be found using relatively elementary techniques. We complete our work in §4.3, where we discuss Hilbert's Theorem and show how it immediately gives the result that the Inverse Galois Problem for S_n is solvable.

2. Cohomology and the Group Extension Problem

We begin by presenting the basic results of Group Cohomology that are used in exploring this problem. We will then show how these results allow us to explore groups and the number of "extensions" of a given group. Indeed, one may construct an entire theory of homology and cohomology of groups. We provide the essentials here to establish results we'll use later, but do not provide the proofs; for a more extensive treatment and proofs of these results, see [AW] or [Nor]. We assume that the reader already is familiar with the basics of module theory, category/functor theory, the derived functors Ext and Tor, and the concept of exact sequences.

The main focus of this section is to build the necessary techniques of homological algebra to present two problems, the solutions to which we focus on in the remaining sections of the paper. The first of these problems is the Group Extension Problem, and the second is the Embedding Problem. Each of these will be stated and explored in §2.3. The solvability of each of these problems is central to any attempt to solve the Inverse Galois Problem, and will thus be one of the main focuses of our work.

2.1. Group Rings and the Augmentation Ideal.

We begin our work by constructing a theory of homology and cohomology for groups. Unless otherwise specified, every R-module is a *left* R-module.

Definition 2.1. *Let G be a group and let $\mathbb{Z}[G]$ be the free $\mathbb{Z}$-module generated by the elements in G. Then we call $\mathbb{Z}[G]$ the group-ring of G with coefficients in $\mathbb{Z}$, with identity element 1_G. More generally, if Λ is any commutative ring with any identity, then $\Lambda[G]$ is the group-ring of G with coefficients in Λ.*

The elements of $\Lambda[G]$ are of the form $\sum_{\sigma\in G} n_\sigma \sigma$, where $n_\sigma \in \Lambda$. Consider two elements $\lambda, \lambda' \in \Lambda[G]$, where

$$\begin{aligned} \lambda &= \sum_{\sigma\in G} n_\sigma \sigma \\ \lambda' &= \sum_{\tau\in G} m_\tau \tau. \end{aligned} \tag{2.1}$$

Then one may define an element $\lambda + \lambda'$ in the obvious way. Defining the product of λ and λ' to be

$$\lambda\lambda' = \sum_{\sigma,\ \tau\in G} n_\sigma m_\tau (\sigma\tau) \tag{2.2}$$

gives $\Lambda[G]$ its ring structure.

As mentioned, the elements of $\mathbb{Z}[G]$ are of the form $\sum_{\sigma \in G} n_\sigma \sigma$. Therefore, one may define the mapping:

$$\sum_{\sigma \in G} n_\sigma \sigma \longrightarrow \sum_{\sigma \in G} n_\sigma \tag{2.3}$$

which gives us a surjective ring homomorphism

$$\epsilon : \ \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \tag{2.4}$$

which we define to be the *augmentation mapping* of $\mathbb{Z}[G]$. If $I = ker(\epsilon)$, then I is a two-sided ideal of $\mathbb{Z}[G]$ (called the augmentation ideal) and the sequence

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{2.5}$$

is exact.

Now consider a left G-module A. We define two very important functors A^G and A_G.

Definition 2.2. *Let G be a group, and let A be a left G-module. Then we define A^G to be the set of all fixed elements of A; that is, the set of all elements in A such that*

$$\sigma a = a \tag{2.6}$$

for all $\sigma \in G$.

From the definition, one immediately sees that A^G is a $\mathbb{Z}$-module. Also, if $\psi : \ A \longrightarrow B$ is a map of G-modules, then for $a \in A^G$, $\psi(a) \in B^G$ (recall that any homomorphism $f : A \longrightarrow B$, for G-modules A and B, must both be a homomorphism and satisfy $f(\sigma a) = \sigma f(a)$ for all $a \in A$ and $\sigma \in G$). Therefore A^G acts as an additive covariant functor from the category of G-modules to the category of abelian groups. Using simple techniques of elementary algebra, one may establish the following:

Proposition 2.3. *There is a $\mathbb{Z}$-isomorphism*

$$A^G \cong Hom_G(\mathbb{Z}, A) \tag{2.7}$$

where $a \in A^G$ corresponds to the homomorphism $f \in Hom_G(\mathbb{Z}, A)$ such that

$$f(1) = a. \tag{2.8}$$

Now we construct another functor (called A_G) which will compliment the functor A^G. Recall that I is the augmentation ideal. Let IA be the set of all finite sums

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n \tag{2.9}$$

where $\alpha_i \in I$ and $a_i \in A$. Then IA is a submodule of A.

Definition 2.4. *Let G be a group and A a left G-module. Let IA be as above. Then we define the functor A_G to be*

$$A_G = A/IA. \tag{2.10}$$

Furthermore, A_G is a covariant functor of A. Observe that G acts trivially on A/IA since $\sigma - e \in I$, $e \in G$ the identity element, for all $\sigma \in G$ (in fact, $\{\sigma - e\}_{\sigma \in G, \ \sigma \neq e}$ forms a $\mathbb{Z}$-base for I).

As with A^G, we may express this functor in a new form via the following:

Proposition 2.5. *Let G be a group, and A a left G-module. Using $\bar{a}$ to denote the natural image of $a \in A$ in $A/IA = A_G$, the map*

$$n \otimes a \longrightarrow n\bar{a} \tag{2.11}$$

defines an isomorphism

$$\mathbb{Z} \otimes_G A \cong A_G. \tag{2.12}$$

Proof. The proof of this proposition is not nearly so trivial as the proof of Proposition 2.3. For a good proof of this proposition, see [Nor].

□

These two new functors will allow us to develop a theory of homology and cohomology for groups, which will be crucial in setting up, as well as exploring the solutions of, the Group Extension Problem. To that end, we explore the dependence of A^G and A_G on the group G.

Proposition 2.6. *Let G, G' be groups, and let $\phi : G' \longrightarrow G$ be a group homomorphism. Then ϕ induces the injective homomorphism*

$$A^G \longrightarrow A^{G'} \tag{2.13}$$

and the surjective homomorphism

$$A_{G'} \longrightarrow A_G. \tag{2.14}$$

Proof. For a proof of this result, see [Nor].

□

We conclude this section with a quick reminder of G-projective and G-injective modules, which come up in the definition of homology and cohomology of groups.

Definition 2.7. *Let G be a group, and A, B, and C be G-modules. We say that A is* G-projective *if, whenever we have a diagram*

$$\begin{array}{ccccc} & & A & & \\ & & \downarrow & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array} \tag{2.15}$$

in which the row is exact and all the maps are G-homomorphisms, there always exists a G-homomorphism $A \longrightarrow B$ such that the map $A \longrightarrow C$ is the combined mapping $A \longrightarrow B \longrightarrow C$.

Definition 2.8. *Let G be a group, and A, B, and C be G-modules. We say that A is* G-injective *if, whenever we have a diagram*

$$\begin{array}{ccccc} 0 & \longrightarrow & B & \longrightarrow & C \\ & & \downarrow & & \\ & & A & & \end{array} \tag{2.16}$$

in which the row is exact and all the maps are G-homomorphisms, there always exists a G-homomorphism $C \longrightarrow A$ such that the mapping $B \longrightarrow A$ is the combined mapping $B \longrightarrow C \longrightarrow A$.

2.2. **Homology and Cohomology Theory of Groups.** In §2.1 we constructed the functors A^G and A_G. These will allow us to construct the homology and cohomology theories that we'll need in the formulation of the Group Extension Problem.

We first will establish a well-defined homology theory for groups, and present the axioms for the theory. Then we will do the same for cohomology.

Before we begin, we introduce the concept of a connected sequence.

Definition 2.9. *Consider an exact sequence*

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \tag{2.17}$$

of G-modules. Consider a sequence of covariant functors $[T^n]_{n\geq 0}$. We call such a sequence a connected right sequence if the sequence

$$\begin{aligned} T^0(A') \longrightarrow T^0(A) \longrightarrow T^0(A'') \longrightarrow T^1(A') \longrightarrow \cdots \\ \longrightarrow T^n(A') \longrightarrow T^n(A) \longrightarrow T^n(A'') \longrightarrow T^{n+1}(A') \longrightarrow \cdots \end{aligned} \tag{2.18}$$

is a 0-sequence; that is, every triplet in the sequence above forms a three term complex. If we modify the definition slightly, we can also construct the notion of a connected right sequence of contravariant functors. If the sequence happens to be exact, we call $[T^n]_{n\geq 0}$ an exact, connected right sequence.

Definition 2.10. *Consider an exact sequence*

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \tag{2.19}$$

of G-modules. Consider a sequence of covariant functors $[T_n]_{n\geq 0}$. We call such a sequence a connected left sequence if the sequence

$$\begin{aligned} \cdots \longrightarrow T_n(A') \longrightarrow T_n(A) \longrightarrow T_n(A'') \longrightarrow T_{n-1}(A') \longrightarrow \cdots \\ \longrightarrow T_1(A'') \longrightarrow T_0(A') \longrightarrow T_0(A) \longrightarrow T_0(A'') \end{aligned} \tag{2.20}$$

is a 0-sequence. If we modify the definition slightly, we can also construct the notion of a connected left sequence of contravariant functors. If the sequence happens to be exact, we call $[T_n]_{n\geq 0}$ an exact, connected left sequence.

We are now ready to construct a homology theory and a cohomology theory for groups.

Definition 2.11. *Let G be a group, and A a left G-module. By a homology theory for G, we mean the construction of an exact, connected left sequence*

$$..., H_2(G, A), H_1(G, A), H_0(G, A) \tag{2.21}$$

of covariant functors of A along with the following properties:

1.) $H_0(G, A) = A_G$

2.) whenever A is G-projective, $H_p(G, A) = 0$ for $p > 0$.

So because our connected sequence is exact, that means that for an exact sequence

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \tag{2.22}$$

of G-modules, the associated sequence

$$\cdots \longrightarrow H_n(G,A') \longrightarrow H_n(G,A) \longrightarrow H_n(G,A'') \longrightarrow H_{n-1}(G,A') \longrightarrow \cdots$$
$$\longrightarrow H_1(G,A'') \longrightarrow H_0(G,A') \longrightarrow H_0(G,A) \longrightarrow H_0(G,A'') \quad (2.23)$$

is also an exact sequence. Now suppose we have a group homomorphism $\phi : G' \longrightarrow G$. Taking $\sigma' a = \phi(\sigma')a$, where $\sigma' \in G'$ and $a \in A$, we see that (with such a ϕ) a G-module may instead be regarded as a G'-module, and so if we can define a homology theory for G', then the homology groups will also form an exact, connected left sequence.

We now establish a very important theorem, which allows us to see the effect of group homomorphisms on the homology theory of groups.

Theorem 2.12 (Uniqueness Theorem for Homology Theories)**.** *Let G, G' be groups with a group homomorphism $G' \longrightarrow G$ and homology theories $H_n(G', A')$ and $H_n(G, A)$. Then for A varying through the category of left G-modules, there exists a unique homomorphism of the connected sequence*

$$H_2(G', A), H_1(G', A), H_0(G', A) \quad (2.24)$$

into the connected sequence

$$H_2(G, A), H_1(G, A), H_0(G, A) \quad (2.25)$$

extending the natural homomorphism $A_{G'} \longrightarrow A_G$ from Proposition 2.6.

Proof. For a proof of this theorem, see [Nor].

□

Corollary 2.13. *If $G' \longrightarrow G$ is a group isomorphism, then the natural isomorphism $A_{G'} \cong A_G$ extends uniquely to an isomorphism of the homology theories of G and G'.*

Proof. This follows immediately by applying Theorem 2.12 to the homomorphism $G' \longrightarrow G$ and the inverse homomorphism $G \longrightarrow G'$.

□

Corollary 2.14. *For a given group G, any two homology theories are isomorphic under the unique isomorphism which extends the identity transformation of the homology group A_G.*

Proof. This follows by applying Corollary 2.13 to the identity mapping on G.

□

These results allow us to establish the existence of a homology theory for G in terms of the Tor functors.

Theorem 2.15. *Let G be a group. One obtains a homology theory for G by setting, for each left G-module A,*

$$H_n(G, A) = Tor_n^G(\mathbb{Z}, A) \quad (n \geq 0). \quad (2.26)$$

If A were instead a right G-module, then we would have

$$H_n(G, A) = Tor_n^G(A, \mathbb{Z}) \quad (n \geq 0). \quad (2.27)$$

Here we regard $\mathbb{Z}$ as a right G-module with trivial operators, and notice that, by Proposition 2.5, $Tor_0^G(\mathbb{Z}, A) = H_0(\mathbb{Z} \otimes_G A) = \mathbb{Z} \otimes_G A \cong A_G$.

Proof. It's clear that this definition of $H_n(G, A)$ satisfies all the required properties, and so by the isomorphism imposed by Corollary 2.14, our theorem is proven. □

So we have established a useful homology theory for groups. We now establish similar results to establish a useful cohomology theory for groups. As we will see in §2.3, the cohomology theory, and in particular our theory for $H^2(G, A)$, will be extremely important in the Group Extension Problem.

Definition 2.16. *Let G be a group, and A a left G-module. By a cohomology theory for G, we mean the construction of an exact, connected right sequence*

$$H^0(G, A), H^1(G, A), H^2(G, A), ... \tag{2.28}$$

of covariant functors of A along with the following properties:
1.) $H^0(G, A) = A^G$
2.) whenever A is G-injective, $H^p(G, A) = 0$ for $p > 0$.

Analogous to before, the fact that we have an exact, connect right sequence means that for any exact sequence $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$, the associated sequence

$$\begin{aligned} H^0(G, A') \longrightarrow H^0(G, A) \longrightarrow H^0(G, A'') \longrightarrow H^1(G, A') \longrightarrow \cdots \\ \longrightarrow H^n(G, A') \longrightarrow H^n(G, A) \longrightarrow H^n(G, A'') \longrightarrow H^{n+1}(G, A') \longrightarrow \cdots \end{aligned} \tag{2.29}$$

is also an exact sequence.

As before, we are able to establish a Uniqueness Theorem for Cohomology Theories completely analogous to the homology case. For the proof, see [Nor].

Theorem 2.17 (Uniqueness Theorem for Cohomology Theories)**.** *Let G, G' be groups with a group homomorphism $G' \longrightarrow G$ and cohomology theories $H^n(G', A')$ and $H^n(G, A)$. Then for A varying through the category of left G-modules, there exists a unique homomorphism of the connected sequence*

$$H^0(G, A), H^1(G, A), H^2(G, A), ... \tag{2.30}$$

into the connected sequence

$$H^0(G', A), H^1(G', A), H^2(G', A), ... \tag{2.31}$$

which extends the transformation $A^G \longrightarrow A^{G'}$ from Proposition 2.6.

It's clear that analogs of Corollaries 2.13 and 2.14 hold for Theorem 2.17 as well. This allows us to establish a cohomology theory for G in terms of the Ext functors.

Theorem 2.18. *Let G be a group. One obtains a cohomology theory for G by setting, for each left G-module A,*

$$H^n(G, A) = Ext^n_G(\mathbb{Z}, A) \quad (n \geq 0). \tag{2.32}$$

Furthermore, because of Proposition 2.3 and the fact that the functors $Ext^0_G(\mathbb{Z}, A)$ and $Hom_G(\mathbb{Z}, A)$ are naturally equivalent (see [Nor] *for the proof), we see that $Ext^0_G(\mathbb{Z}, A) \cong Hom_G(\mathbb{Z}, A) \cong A^G$.*

Proof. It's clear that the extension functors described above satisfy the required conditions. By the Uniqueness Theorem applied to the identity mapping $G \longrightarrow G$, this theorem is proven. □

2.3. **The Group Extension Problem and the Embedding Problem.** In §2.1 and §2.2 we went through the trouble of constructing a theory of homology and cohomology for groups. We will now turn our focus mainly to the cohomology theory of groups, as this will lead to an understanding of the Group Extension Problem. To do this, we introduce the notion of the *standard non-homogeneous G-free resolution of* $\mathbb{Z}$. Here we will simply state the results and take it as definition; for a more detailed understanding, see [Nor] and [AW].

Definition 2.19. *Let G be a group and (for $n \geq 0$) let Φ_n be G-modules with G-base $[\sigma_1, ..., \sigma_n]$, where*

$$[\sigma_1, ..., \sigma_n] =< 1, \sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_3, ..., \sigma_1\sigma_2 \cdots \sigma_n > \quad (n \geq 1) \tag{2.33}$$

and where $[\ ] =< 1 >$ handles the case for $n = 0$. Here the notation $< \cdot >$ refers to the generating set for Φ_n as a free $\mathbb{Z}$-module in the construction of the standard homogeneous G-free resolution of $\mathbb{Z}$, about which we refer readers to [Nor]. *Then the sequence of G-modules*

$$\cdots \longrightarrow \Phi_n \xrightarrow{d_n} \Phi_{n-1} \longrightarrow \cdots \longrightarrow \Phi_1 \xrightarrow{d_1} \Phi_0 \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{2.34}$$

with the relation

$$\begin{aligned} d_n[\sigma_1, ..., \sigma_n] = \sigma_1[\sigma_2, ..., \sigma_n] + \sum_{r=1}^{n-1}(-1)^r[\sigma_1, ..., \sigma_r\sigma_{r+1}, ..., \sigma_n] \\ +(-1)^n[\sigma_1, ..., \sigma_{n-1}] \end{aligned} \tag{2.35}$$

is an exact sequence and is called the standard non-homogeneous G-free resolution of $\mathbb{Z}$.

Applying the $Hom(-, A)$ functor to the above sequence allows us to explore the cochains and coboundaries, which allows us to describe the elements of a typical cohomology group. Observe that because $[\sigma_1, ..., \sigma_n]$ forms a G-base for Φ_n, a typical n-cochain is found by identifying an element of A with each ordered set $\sigma_1, ..., \sigma_n$. So let f be an n-cochain and let $f(\sigma_1, ..., \sigma_n)$ represent the element in A associated to $\sigma_1, ..., \sigma_n$. Then, applying the boundary homomorphism gives us $d^n f$, where

$$\begin{aligned} (d^n f)(\sigma_1, ..., \sigma_{n+1}) = \sigma_1 f(\sigma_2, ..., \sigma_{n+1}) \\ + \sum_{r=1}^{n}(-1)^r f(\sigma_1, ..., \sigma_r\sigma_{r+1}, ..., \sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, ..., \sigma_n), \end{aligned} \tag{2.36}$$

and it's understood that, when $n = 0$, $(d^0 f)(\sigma) = \sigma a - a$, where $a \in A$ corresponds to the 0-cochain f. We will now use this understanding to construct the elements of $H^2(G, A)$.

Definition 2.20. *Consider a 2-cochain f, constructed using the standard non-homogeneous G-free resolution of $\mathbb{Z}$. We know by (2.36) that for f to be a 2-cocycle, we must have*

$$\sigma_1 f(\sigma_2, \sigma_3) - f(\sigma_1\sigma_2, \sigma_3) + f(\sigma_1, \sigma_2\sigma_3) - f(\sigma_1, \sigma_2) = 0. \tag{2.37}$$

Such a 2-cocycle is called a factor system.

Definition 2.21. *Consider a 2-cochain f, constructed using the standard non-homogeneous G-free resolution of $\mathbb{Z}$. Let f be a 2-cocycle (i.e. a factor system). Observe that f is a coboundary (i.e. $f = d\phi$ for some 1-cochain ϕ) if*

$$f(\sigma_1, \sigma_2) = \sigma_1\phi(\sigma_2) - \phi(\sigma_1\sigma_2) + \phi(\sigma_1) \tag{2.38}$$

holds identically. Such an f is called a principal factor system.

So $H^2(G, A)$ is just the additive group of factor systems taken modulo the subgroup of principal factor systems.

We are now ready to introduce one of the main problems in the study of the Inverse Galois Problem. In doing so, it will be more convenient to treat A as if it's law of composition is multiplication, as opposed to addition. As such, the conditions for A being a left G-module become

$$(a_1a_2)^\sigma = a_1^\sigma a_2^\sigma, \quad (a^\sigma)^\tau = a^{\tau\sigma}, \quad a^1 = a, \tag{2.39}$$

where $a, a_1, a_2 \in A$ and $\sigma, \tau \in G$. It will also be more convenient to describe a 2-cochain as a doubly indexed family $\{a_{\sigma,\tau}\}$ of elements in A. Doing so alters the condition for being a factor system to

$$a_{\sigma_2,\ \sigma_3}^{\sigma_1} = \frac{a_{\sigma_1\sigma_2,\ \sigma_3}\, a_{\sigma_1,\ \sigma_2}}{a_{\sigma_1,\ \sigma_2\sigma_3}} \tag{2.40}$$

and it will be a principal factor system when there is a family $\{\alpha_{\sigma_1}\}$ of elements of A such that

$$a_{\sigma_1,\ \sigma_2} = \frac{\alpha_{\sigma_2}^{\sigma_1}\alpha_{\sigma_1}}{\alpha_{\sigma_1\sigma_2}}. \tag{2.41}$$

Definition 2.22 (The Group Extension Problem)**.** *Let A be a given abelian group and G be an arbitrary group. An extension of G by A means finding a group $\widetilde{G}$ containing A as a normal subgroup along with a surjective group homomorphism $\psi : \widetilde{G} \longrightarrow G$ with kernel A. Finding such a group $\widetilde{G}$, as well has how many different $\widetilde{G}_i$'s can be found, is the Group Extension Problem.*

Two extensions $\widetilde{G}_1$ and $\widetilde{G}_2$ are said to be equivalent if there is an isomorphism between them such that

$$\begin{array}{ccccc} A & \longrightarrow & \widetilde{G}_1 & \longrightarrow & G \\ \| & & \downarrow & & \| \\ A & \longrightarrow & \widetilde{G}_2 & \longrightarrow & G \end{array} \tag{2.42}$$

is a commutative diagram. Here it's understood that the maps $A \longrightarrow \widetilde{G}_1$ and $A \longrightarrow \widetilde{G}_2$ are inclusion maps

We will now attempt to classify all the (non-isomorphic) solutions to the Group Extension Problem, by means of a very important theorem. Before doing so, however, we prove the following lemma, which will be useful in proving the theorem.

Lemma 2.23. *Let A be an abelian group, G an arbitrary group, and $\widetilde{G}$ an extension of G by A. Then A has a left G-module structure.*

Proof. Let $\sigma \in G$. By the surjectivity of ψ, we may choose an element η_σ such that $\psi(\eta_\sigma) = \sigma$. Then because A is a normal subgroup of $\widetilde{G}$, the map

$$a \longrightarrow \eta_\sigma a \eta_\sigma^{-1} \tag{2.43}$$

is an automorphism of A. Also, if η'_σ is another element of $\widetilde{G}$ mapping to σ, then $\eta'_\sigma = \alpha\eta_\sigma$ for some suitable $\alpha \in A$ (remember, A is the kernel of ψ). Therefore

$$\eta'_\sigma a \eta'^{-1}_\sigma = \alpha\eta_\sigma a \eta_\sigma^{-1}\alpha^{-1} = \eta_\sigma a \eta_\sigma^{-1} \tag{2.44}$$

because A is abelian and $\eta_\sigma a\eta_\sigma^{-1} \in A$ by normality. So if we set $a^\sigma = \eta_\sigma a\eta_\sigma^{-1}$, then a^σ is independent of our choice of η_σ. With this definition, it's easy to now verify the conditions that A is a left G-module.

□

With Lemma 2.23 in place, we will now prove one of the main theorems of the paper, which will show the importance of all our work up to now. This theorem will prove useful in §3.4, when we explore the Inverse Galois Problem for nilpotent groups of odd order.

Theorem 2.24. *Let A be an abelian group, G an arbitrary group, and suppose A has the left G-module structure discussed in Lemma 2.23. Then to each extension of G by A, there is associated a definite element of $H^2(G, A)$. Furthermore, this association produces a bijection between the classes of equivalent extensions and the elements of $H^2(G, A)$.*

As mentioned, this is one of our main theorems. It tells us that the possible number of (isomorphism classes of) extensions that we need to consider can be found by looking at the number of elements of $H^2(G, A)$. For instance, if $H^2(G, A)$ is trivial, then there is only one such class and we need only consider one extension of G by A in the Inverse Galois Problem. As this is the theorem we've been working towards, we offer the full proof below, following the method discussed in [Nor].

Proof. Let $\widetilde{G}$ be an extension of G by A, and let $\{\eta_\sigma\}$ be a set of elements in $\widetilde{G}$ whose image under ψ is simply σ. Such a set is often called a *section* of the group $\widetilde{G}$. Observe that $\psi(\eta_{\sigma_1}\eta_{\sigma_2}) = \sigma_1\sigma_2 = \psi(\eta_{\sigma_1\sigma_2})$, which means that

$$\eta_{\sigma_1}\eta_{\sigma_2} = \alpha_{\sigma_1,\,\sigma_2}\eta_{\sigma_1\sigma_2} \tag{2.45}$$

where $\alpha_{\sigma_1,\,\sigma_2} \in A$. Now, making use of the fact that $\widetilde{G}$ is associative, we observe that

$$(\eta_{\sigma_1}\eta_{\sigma_2})\eta_{\sigma_3} = \alpha_{\sigma_1,\,\sigma_2}\eta_{\sigma_1\sigma_2}\eta_{\sigma_3} = \alpha_{\sigma_1,\,\sigma_2}\alpha_{\sigma_1\sigma_2,\,\sigma_3}\eta_{\sigma_1\sigma_2\sigma_3} \tag{2.46}$$

and

$$\begin{aligned}\eta_{\sigma_1}(\eta_{\sigma_2}\eta_{\sigma_3}) = \eta_{\sigma_1}\alpha_{\sigma_2,\,\sigma_3}\eta_{\sigma_2\sigma_3} &= \eta_{\sigma_1}\alpha_{\sigma_2,\,\sigma_3}\eta_{\sigma_1}^{-1}\eta_{\sigma_1}\eta_{\sigma_2\sigma_3} \\ &= \alpha^{\sigma_1}_{\sigma_2,\,\sigma_3}\alpha_{\sigma_1,\,\sigma_2\sigma_3}\eta_{\sigma_1\sigma_2\sigma_3}\end{aligned} \tag{2.47}$$

implies that

$$\alpha_{\sigma_1,\,\sigma_2}\alpha_{\sigma_1\sigma_2,\,\sigma_3} = \alpha^{\sigma_1}_{\sigma_2,\,\sigma_3}\alpha_{\sigma_1,\,\sigma_2\sigma_3}, \tag{2.48}$$

forming a factor system.

Now consider we have two extensions $\widetilde{G}_1$ and $\widetilde{G}_2$, with factor systems $\{\alpha_{\sigma_1,\,\sigma_2}\}$ and $\{\beta_{\sigma_1,\,\sigma_2}\}$ constructed as above. If $\widetilde{G}_1$ and $\widetilde{G}_2$ are equivalent, it is possible to choose sections $\{\eta_\sigma\}_1$ and $\{\eta_\sigma\}_2$ (of $\widetilde{G}_1$ and $\widetilde{G}_2$, respectively) so that $\alpha_{\sigma_1,\,\sigma_2} = \beta_{\sigma_1,\,\sigma_2}$ for all $\sigma_1, \sigma_2 \in G$. On the other hand, if we can choose sections so that $\alpha_{\sigma_1,\,\sigma_2} = \beta_{\sigma_1,\,\sigma_2}$ for all $\sigma_1, \sigma_2 \in G$, then the two extensions are equivalent. For the details of this fact, see [Nor]. So two extensions are equivalent if and only if we can rechoose sections so that $\alpha_{\sigma_1,\,\sigma_2} = \beta_{\sigma_1,\,\sigma_2}$ for all $\sigma_1, \sigma_2 \in G$.

Now we notice that, for a given section $\{\eta_\sigma\}$ of $\widetilde{G}$, we may observe that, for appropriate $a_\sigma \in A$, we may obtain any other section $\{\eta_\sigma{}^*\}$, where $\eta^*_\sigma = a_\sigma \eta_\sigma$. Then we have

$$\eta^*_{\sigma_1}\eta^*_{\sigma_2} = a_{\sigma_1}\eta_{\sigma_1}a_{\sigma_2}\eta_{\sigma_2} = a_{\sigma_1}\eta_{\sigma_1}a_{\sigma_2}\eta^{-1}_{\sigma_1}\eta_{\sigma_1}\eta_{\sigma_2} = a_{\sigma_1}a^{\sigma_1}_{\sigma_2}\alpha_{\sigma_1,\ \sigma_2}\eta_{\sigma_1\sigma_2} \tag{2.49}$$

and at the same time we have

$$\eta^*_{\sigma_1}\eta^*_{\sigma_2} = \alpha^*_{\sigma_1,\ \sigma_2}a_{\sigma_1\sigma_2}\eta_{\sigma_1\sigma_2} \tag{2.50}$$

which gives us that

$$\alpha^*_{\sigma_1,\ \sigma_2} = \alpha_{\sigma_1,\ \sigma_2}\frac{a_{\sigma_1}a^{\sigma_1}_{\sigma_2}}{a_{\sigma_1\sigma_2}} \tag{2.51}$$

As a result, two extensions will be equivalent if and only if the original factor systems belong to the same cohomology class, and as we see above that class is independent of the choice of section; as a result, every extension is associated to a unique element of $H^2(G, A)$.

Now all that remains is to show that every element of $H^2(G, A)$, there is an associated extension. Choose such an element, and let $\{\alpha_{\sigma_1,\ \sigma_2}\}$ be the representative factor system where (after multiplying by the appropriate principal factor system) $\alpha_{e,\ e} = 1_A$ where $e \in G$ is the identity element. If, in (2.40) we take (σ, e, e) and then take (e, e, σ), we get that

$$\alpha_{\sigma,\ e} = 1_A = \alpha_{e,\ \sigma} \quad (\sigma \in G). \tag{2.52}$$

Now take $\widetilde{G}$ to be the set of all pairs (a, σ) where $a \in A$ and $\sigma \in G$, combined with the multiplication law

$$(a_1, \sigma_1)(a_2, \sigma_2) = (a_1 a_2^{\sigma_1}\alpha_{\sigma_1,\ \sigma_2}, \sigma_1\sigma_2). \tag{2.53}$$

Then by routine exercises in group theory, one can show that $\widetilde{G}$ is a group with identity $(1_A, e)$ such that the mapping $(a, \sigma) \longrightarrow \sigma$ is a surjective homomorphism onto G with kernel A. Therefore, $\widetilde{G}$ is a group extension of G by A and we complete the proof.

□

Corollary 2.25. *A group extension splits if and only if it corresponds (under the association in Theorem 2.24) to the trivial element in $H^2(G, A)$.*

Proof. Recall that we have the equality

$$\eta_{\sigma_1}\eta_{\sigma_2} = \alpha_{\sigma_1,\ \sigma_2}\eta_{\sigma_1\sigma_2}, \tag{2.54}$$

where $\alpha_{\sigma_1,\ \sigma_2}$ represents the cohomology class. This class is trivial if and only if it's a coboundary (a principal factor system), or if

$$\alpha_{\sigma_1,\ \sigma_2} = \frac{a_{\sigma_1}a^{\sigma_1}_{\sigma_2}}{a_{\sigma_1\sigma_2}}. \tag{2.55}$$

Suppose we have the following extension of G by A as before:

$$1 \longrightarrow A \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1. \tag{2.56}$$

From basic algebraic topology, one knows that such an extension splits (i.e. such an exact sequence is a *split* exact sequence) if and only if, for the map $\pi : \widetilde{G} \longrightarrow G$,

there is a map $\epsilon : G \longrightarrow \widetilde{G}$ such that $\pi \circ \epsilon$ is the identity mapping on G. Suppose $\epsilon(\sigma) = a_\sigma^{-1}\eta_\sigma$. It's clear from the definitions that $\pi \circ \epsilon$ is the identity on G. But we need ϵ to be a group homomorphism; that is, $\epsilon(\sigma_1\sigma_2) = \epsilon(\sigma_1)\epsilon(\sigma_2)$. But for ϵ to satisfy this, that implies:

$$\begin{aligned}
(a_{\sigma_1\sigma_2})^{-1}\eta_{\sigma_1\sigma_2} &= (a_{\sigma_1})^{-1}\eta_{\sigma_1}(a_{\sigma_2})^{-1}\eta_{\sigma_2} \\
(a_{\sigma_1\sigma_2})^{-1}\eta_{\sigma_1\sigma_2} &= (a_{\sigma_1})^{-1}\eta_{\sigma_1}(a_{\sigma_2})^{-1}(\eta_{\sigma_1})^{-1}\eta_{\sigma_1}\eta_{\sigma_2} \\
(a_{\sigma_1\sigma_2})^{-1}\eta_{\sigma_1\sigma_2} &= (a_{\sigma_1})^{-1}(a_{\sigma_2}^{\sigma_1})^{-1}\alpha_{\sigma_1,\,\sigma_2}\eta_{\sigma_1\sigma_2} \\
(a_{\sigma_1\sigma_2})^{-1} &= (a_{\sigma_1})^{-1}(a_{\sigma_2}^{\sigma_1})^{-1}\alpha_{\sigma_1,\,\sigma_2} \\
\alpha_{\sigma_1,\,\sigma_2} &= a_{\sigma_1}a_{\sigma_2}^{\sigma_1}(a_{\sigma_1\sigma_2})^{-1} \\
\alpha_{\sigma_1,\,\sigma_2} &= \frac{a_{\sigma_1}a_{\sigma_2}^{\sigma_1}}{a_{\sigma_1\sigma_2}} \qquad (2.57)
\end{aligned}$$

and $\alpha_{\sigma_1,\,\sigma_2}$ is a coboundary. Therefore, the cohomology element corresponding to this extension is trivial if and only if the extension is a split extension.

□

We conclude this section by introducing our other main problem, the Embedding Problem. This is closely tied to the Group Extension Problem. Suppose we have a group G, and a galois extension L/K with galois group $\mathrm{Gal}(L/K) \cong G$. The Embedding Problem for the group G, given an extension $\widetilde{G}$ of G by an abelian group A, is to find a field $M \supseteq L \supseteq K$ such that $\mathrm{Gal}(M/K) \cong \widetilde{G}$, $\mathrm{Gal}(M/L) \cong A$, and the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Gal(M/L) & \longrightarrow & Gal(M/K) & \longrightarrow & Gal(L/K) & \longrightarrow & 1
\end{array} \qquad (2.58)$$

is commutative. In general, given galois extensions L/K and M/L, it's not necessarily true that M/K is galois, so finding a solution to this problem is a nontrivial matter. The ability to solve the Embedding Problem, with $K = \mathbb{Q}$, for every possible group extension $\widetilde{G}$ of G by A (where G varies through the category of groups and A varies through the category of abelian groups) will imply the solvability of the Inverse Galois Problem.

3. Abelian Groups and Nilpotent Groups of Odd Order

In this section we seek to show that every Nilpotent Group of odd order can be realized as a Galois Group of some field extension of $\mathbb{Q}$. To do that, we first establish some important results from elementary Galois Theory and use them to show that if our group is an abelian group A, then we may find a field extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong$A. This is covered in §3.1. In §3.2 and §3.3, we introduce some of the important elements of Algebraic Number Theory, focusing mainly on ramification and local fields, which will give us the tools and techniques necessary to approach more difficult pieces of this problem. In §3.4, we use these results to prove the case where G is an odd-ordered Nilpotent Group, following the ideas of Scholz and Reichardt outlined in [Ser2]. These ideas involve solving the Embedding Problem described in §2.3 for every possible group extension

$$1 \longrightarrow Z_\ell \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1 \qquad (3.1)$$

of degree ℓ. To do this we consider when the extension $\widetilde{G}$ gives us a split exact sequence, and then consider the case when the extension does not split. The first of these cases is handled in §3.5 and the second is addressed in §3.6.

3.1. **Abelian Groups.** We begin this section by exploring the problem for cyclotomic extensions, and show that the problem is trivially solved. Using these results, as well as important results from analytic number theory and basic group theory, one is able to show that if we have an abelian group A, then there is a field extension $K/\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong$A. This will be an important stepping stone towards understanding the Inverse Galois Problem. We begin with two important results for cyclotomic extensions.

Theorem 3.1. *Let ζ_n be a primitive n-th root of unity. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler Phi Function. Furthermore, the mapping*

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \tag{3.2}$$

given by a (mod n) $\longmapsto \sigma_a$ is an isomorphism, where σ_a is the map such that $\sigma_a(\zeta_n) = \zeta_n^a$.

Proof. By construction, we know that $\psi(ab) = \sigma_{ab}$. For a given ζ_n, we have $\sigma_{ab}(\zeta_n) = \zeta_n^{ab} = (\zeta_n^b)^a = \sigma_a(\zeta_n^b) = \sigma_a\sigma_b(\zeta_n)$. Thus, $\psi(ab) = \psi(a)\psi(b)$ so ψ is a homomorphism.

Since every Galois automorphism for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is of the form σ_a for some uniquely determined a relatively prime to n, the bijection of ψ is obvious.

Since $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, the result is proven. □

Theorem 3.2. *Let $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ be the decomposition of n, for $n \in \mathbb{Z}^+$, into distinct prime powers. Then the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$, for $i = 1, 2, ..., k$ intersect only in the field $\mathbb{Q}$ and their compositum is the cyclotomic field $\mathbb{Q}(\zeta_n)$. Therefore*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times \cdots \times Gal(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}). \tag{3.3}$$

By Theorem 3.1, this is simply:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times. \tag{3.4}$$

Proof. The first part of this theorem follows from the observations that $\mathbb{Q}(\zeta_{p_i^{a_i}})$ is a subfield of $\mathbb{Q}(\zeta_n)$ for every $i = 1, 2, ..., k$, that the composite contains $\zeta_{p_1^{a_1}}\zeta_{p_2^{a_2}}\cdots\zeta_{p_k^{a_k}}$ (which is a primitive n-th root of unity), that the degree $[\mathbb{Q}(\zeta_{p_i^{a_i}}) : \mathbb{Q}] = \phi(p_i^{a_i})$ for all $i = 1, 2, ..., k$, and that $\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k})$. With these conditions it follows from a common result in Galois Theory that the intersection of all these $\mathbb{Q}(\zeta_{p_i^{a_i}})$'s is precisely $\mathbb{Q}$. With this, the rest of the theorem follows trivially (the Galois Group decomposition is a consequence of considering the compositum of a collection of fields with intersection $\mathbb{Q}$, and the second follows directly from Theorem 3.1). For a more detailed proof, see [DF].

□

So we have now classified the Galois Group of every cyclotomic field extension. We now want to show that for any finite abelian group A, we may find a field extension $K/\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong$A. To do so, recall the following important theorem about abelian groups, which we will state without proof.

Theorem 3.3 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a finitely generated abelian group. Then:*

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}, \tag{3.5}$$

for some integers $r, n_1, n_2, ..., n_k$ that satisfy:

- $r \geq 0$ *and* $n_j \geq 2$ *for all* j*, and;*
- $n_{i+1} | n_i$ *for all* $1 \leq i \leq k-1$.

Furthermore, this expression is unique. Observe that G happens to be a finite abelian group if and only if $r = 0$.

So the above theorem tells us virtually everything we need to know about finite abelian groups and their structure, which we will need to exploit. For a proof of this theorem, see [DF].

Before moving on, we need one more theorem, which we will also state without proof; for a good proof of this theorem, see [IR].

Theorem 3.4 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *Suppose* $a, m \in \mathbb{Z}$*, with* $(a, m) = 1$*. Then there exist infinitely many positive prime numbers* p *such that* $p \equiv a (mod\ m)$.

Remark 3.5. *Strictly speaking, Dirichlet actually proved something much stronger, showing that the Dirichlet density of primes in a given arithmetic progression is* $\frac{1}{\phi(m)}$*, where* m *is the modulus in our arithmetic progression. This is stronger because it gives us an idea of just how many primes satisfy* $p \equiv a (mod\ m)$ *for* $(a, m) = 1$*, relative to the set of all positive primes. From the definition of Dirichlet density, one can see that a finite set has density zero, so because these sets of primes have nonzero density, they must be infinite.*

With Theorems 3.1, 3.2, 3.3, and 3.4 in place, we now have enough to show that for a given finite abelian group A, there exists a field extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong$A. This will be our first big step towards exploring the Inverse Galois Problem.

Theorem 3.6 (Inverse Galois Problem for Abelian Groups)**.** *For any finite abelian group A, the Inverse Galois Problem is solvable; that is, we may find a Galois extension* $K/\mathbb{Q}$ *with* $Gal(K/\mathbb{Q}) \cong A$*. In fact, we can find infinitely many such K with this property.*

Proof. Consider any finite abelian group A. By Theorem 3.3, we have

$$A \cong Z_{n_1} \times \cdots \times Z_{n_k}, \tag{3.6}$$

for integers $n_1, ..., n_k$. By Theorem 3.4, we can always find primes $p_1, ..., p_k$ such that

$$\begin{aligned} p_1 &\equiv 1 (mod n_1) \\ p_2 &\equiv 1 (mod n_2) \\ &\vdots \\ p_k &\equiv 1 (mod n_k) \end{aligned} \tag{3.7}$$

and let $n = p_1 p_2 \cdots p_k$. By Theorems 3.1 and 3.2, we know that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times (\mathbb{Z}/p_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times. \tag{3.8}$$

Since we know from basic group theory that $(\mathbb{Z}/p_i\mathbb{Z})^\times \cong Z_{p_i - 1}$, where the latter is the cyclic group of order $p_i - 1$, this gives us

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong Z_{p_1 - 1} \times Z_{p_2 - 1} \times \cdots \times Z_{p_k - 1}. \tag{3.9}$$

By construction, $n_i | p_i - 1$ so $Z_{p_i - 1}$ has a subgroup H_i of order $\frac{p_i - 1}{n_i}$. This means that the group $Z_{p_i - 1}/H_i$ is a cyclic group of order n_i. Let $H = H_1 \times H_2 \times \cdots \times H_k$.

Then $(\mathbb{Z}/n\mathbb{Z})^\times/H \cong A$. Furthermore, as H is normal (it's a subgroup if an abelian group), Theorem 1.1 tells us there is a field $K = \mathbb{Q}(\zeta_n)^H$ such that $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n)$, $K/\mathbb{Q}$ is a Galois extension, and $\mathrm{Gal}(K/\mathbb{Q}) \cong A$.

The claim that there are infinitely many such $K/\mathbb{Q}$ will be proven in Theorem 3.28 in §3.2.

□

3.2. **Algebraic Number Theory I: Ramification.** In §3.1 we showed that we can solve the Inverse Galois Problem for abelian groups; that is, we showed there exists a galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong A$ for any abelian group A. However, for more general groups we do not have structures that are so amenable to basic field theory and basic galois theory. As it turns out, the concept of ramification and local fields will allow us to solve the embedding problem in cases where finding a solution isn't so clear (the situation in §3.4 is such a case, as we will soon see). To that end, we seek to present the basics of ramification as discussed in [Sam] and [IR]. We will, for the most part, only be concerned with the results, and not the proofs of these results, so we will often refer the reader to these (and other) sources for proofs and deeper treatments. We assume the reader is acquainted with the basic theory of prime ideals, as well as the concepts of norm and trace from linear algebra. We introduce the basics of local fields in §3.3.

Definition 3.7. *An algebraic number is a complex number γ that is a root of a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where each $a_i \in \mathbb{Q}$. If every $a_i \in \mathbb{Z}$, then we say that γ is an algebraic integer.*

Algebraic numbers are an important area of study in mathematics; however, for our purposes we'll be focusing mainly on algebraic integers. We begin with an important (and obvious) proposition.

Proposition 3.8. *A rational number $\gamma \in \mathbb{Q}$ is an algebraic integer if and only if $\gamma \in \mathbb{Z}$.*

Proof. If $\gamma \in \mathbb{Z}$ this is obvious. Now suppose $\gamma \in \mathbb{Q}$ is an algebraic integer. Then $\gamma = c/d$, where $(c, d) = 1$. Then we have

$$c^n + a_{n-1}c^{n-1}d + \cdots + a_1cd^{n-1} + a_0d^n = 0. \tag{3.10}$$

Therefore, $d|c^n$ and since $(c, d) = 1$, that means that $d|c$. But because $(c, d) = 1$, $d = \pm 1$ and $\gamma \in \mathbb{Z}$.

□

Proposition 3.9. *Given a field extension $K/\mathbb{Q}$, the set of algebraic numbers in K forms a field and the set of algebraic integers in K forms a ring.*

Proof. For the proof, see [IR].

□

We will be concerned with this fact later, when we discuss how the ring $\mathbb{Z}$ extends when we take a field extension of $\mathbb{Q}$. To that end, we explore the problem in complete generality and then show that the cases we need to consider follow as examples.

We are now prepared to discuss the discriminant, and then relate it to the concept of galois extensions that we've been looking at up to this point. Much of what follows may be found in greater detail in [IR] and [Sam].

Definition 3.10. *Let B be a ring, and let $A \subset B$ be a subring such that B is a free A-module of finite rank n. Take any $(x_1, ..., x_n) \in B^n$. Then we define the discriminant of $(x_1, ..., x_n)$ to be the element of A given by*

$$D(x_1, ..., x_n) = det(Tr_{B/A}(x_i x_j)). \tag{3.11}$$

Proposition 3.11. *If $(y_1, ..., y_n) \in B^n$ is another such set of elements, such that $y_i = \sum_{j=1}^{n} a_{ij} x_j$, with $a_{ij} \in A$, then*

$$D(y_1, ..., y_n) = (det(a_{ij}))^2 D(x_1, ..., x_n). \tag{3.12}$$

Proof. For a proof of this result, see [Sam].

□

Proposition 3.11 tells us that the discriminants for bases of B over A are associates in A. This allows us to make the following definition:

Definition 3.12. *Given the hypotheses of Definition 3.10, we call the principal ideal of A generated by the discriminant of any base of B over A the discriminant of B over A, denoted $D_{B/A}$.*

The concept of the discriminant will prove to be useful later on, when we apply it number fields. Now we develop the concept of ramification.

Definition 3.13. *Let A be a ring, and M an A-module. We say that M is* Noetherian *if it satisfies the following equivalent conditions (for a proof of equivalence, see* [Sam]*):*

1.) Every non-empty collection of submodules of M contains a maximal element.

2.) Every increasing of submodules of M is stationary (i.e. there is an n_0 such that $Mn = M_{n_0}$ for all $n \geq n_0$, where the relation is inclusion).

3.) Every submodule of M has a finite generating set.

We say that a ring A is Noetherian if, when considered as an A-module, the ring A is a Noetherian module.

Proposition 3.14. *Let A be a Noetherian, integrally closed ring. Let K be it's field of fractions, L any finite extension of K, and A' the integral closure of A in L. If K is of characteristic 0, then A' is an A-module with finite generating set and is a Noetherian ring.*

Proof. For the proof, see [Sam].

□

Taking $A = \mathbb{Z}$ and $K = \mathbb{Q}$, we see that the ring of algebraic integers in any finite extension of $\mathbb{Q}$ is a Noetherian ring.

Definition 3.15. *An integral domain A is called a Dedekind ring if it is Noetherian and integrally closed, and if every non-zero prime ideal of A is maximal.*

We can see immediately that the ring $\mathbb{Z}$, and in fact any principal ideal ring, is a Dedekind ring. It turns out that, via the following theorem, the ring of integers in every number field is a Dedekind ring.

Lemma 3.16. *Let B be an integral domain and $A \subset B$ be a subring such that B is integral over A. Then B is a field if and only if A is a field.*

Proof. For a proof of this well known fact, see [Sam].

□

Theorem 3.17. *Let A be a Dedekind ring, K its field of fractions, L an extension of K, and A' the integral closure of A in L. Assume K has characteristic 0. Then A' is a Dedekind ring and an A-module with a finite generating set.*

Proof. For the proof, see [Sam].

□

So taking $A = \mathbb{Z}$ and $K = \mathbb{Q}$ in Theorem 3.17, we have that the ring of integers in any number field is a Dedekind ring. We now present (without proof) a theorem which shows us that for any Dedekind ring, the ideals have unique factorization. For the proof, see [Sam].

Theorem 3.18. *Let A be a Dedekind ring and let P be the set of non-zero prime ideals of A. Then every non-zero fractional ideal ϱ may be uniquely expressed in the form $\varrho = \prod_{\wp \in P} \wp^{n_\wp(\varrho)}$, where, for any $\wp \in P$, $n_\wp \in \mathbb{Z}$ and, for almost all $\wp \in P$, $n_\wp = 0$.*

So consider the ring $\mathbb{Z}$, its field of fractions $\mathbb{Q}$, and a finite field extension $K/\mathbb{Q}$. Let $\vartheta_K \subset K$ be the set of algebraic integers in K (i.e. the integral closure in K). Let (p) be a non-zero prime ideal of $\mathbb{Z}$. Then $\vartheta_K p$ is an ideal of ϑ_K, and Theorem 3.18 says that

$$\vartheta_K p = \prod_{i=1}^{n} \wp_i^{e_i} \tag{3.13}$$

where the $\wp_i$ are all distinct prime ideals of $\vartheta_K p$, the e_i's are positive integers, and the product denotes product of ideals. The integer e_i is called the *ramification index* of the prime ideal $\wp_i$ over (p), and we say that the prime $p \in \mathbb{Z}$ ramifies in the extension $K/\mathbb{Q}$ (or equivalently in the ring extension $\vartheta_K/\mathbb{Z}$) if any $e_i > 1$.

It's clear that $\mathbb{Z}/(p)$ may be identified with a subring of $\vartheta_K/\wp_i$ for every $i \in \{1, ..., n\}$, and so by Lemma 3.16 $\vartheta_K/\wp_i$ is a field. Applying Theorem 3.17 to $A = \mathbb{Z}$ and $K = \mathbb{Q}$ gives us that ϑ_K is a $\mathbb{Z}$-module with finite generating set, and so $\vartheta_K/\wp_i$ is a finite dimensional vector space over the field $\mathbb{Z}/(p)$. Let f_i be the dimension of this vector space. Then we call f_i the *residual degree* of the prime ideal $\wp_i$ over the prime p, and one can see that $|\vartheta_K/\wp_i| = p^{f_i}$. This leads to the following very important theorem:

Theorem 3.19. *$\sum_{i=1}^{g} e_i f_i = n$, where n is the degree of the extension $K/\mathbb{Q}$. If the extension happens to be Galois, then $e_1 = \cdots = e_g = e$ and $f_1 = \cdots = f_g = f$ and $efg = n$.*

Proof. For a proof of this result, see [IR] and [Sam]. □

With this new understanding, we may now classify certain *types* of ramification, which we point out in the following definition.

Definition 3.20. *Suppose we have a galois extension $K/\mathbb{Q}$, and $efg = n$ as in Theorem 3.19. We say that a prime p splits completely in K if $e = 1$, $f = 1$, and $g = n$. We say the prime p is totally ramified if $e = n$, $f = 1$, and $g = 1$. We say that p is inert if $e = 1$, $f = n$, and $g = 1$. Finally, considering the characteristic of the field $\mathbb{Z}/p\mathbb{Z}$ (which happens to be p), we say that p is tamely ramified if $e > 1$ and $gcd(e, p) = 1$.*

We present one additional fact about the ramification index and the residual degree which will prove to be extremely useful to us.

Proposition 3.21. *Let $K \subset L \subset M$ be a tower of fields. Take a prime element $p \in \vartheta_K$, and suppose that $\wp \in \vartheta_M$ is a prime element above p. Let $\wp_L = \wp \cap L$, and one sees that $\wp_L$ is also a prime element above p. The we have the following relations:*

$$\begin{aligned} e(\wp/p) &= e(\wp/\wp_L)e(\wp_L/p) \\ f(\wp/p) &= f(\wp/\wp_L)f(\wp_L/p). \end{aligned} \tag{3.14}$$

Proof. For a proof of this proposition, see [Koc].

□

We now present a very important theorem that relates the theory of ramification to the concept of the discriminant presented earlier. For the proof of this theorem, see [Sam].

Theorem 3.22. *Recall from Definition 3.12 that, for a ring B with A a subring such that B is an A-module with finite generating set, we define the discriminant $D_{B/A}$ to be the principal ideal of A generated by the discriminant of any base of B over A. Now let L/K be a number field extension with rings of integers $A \subset K$ and $A' \subset L$. A prime ideal $\wp \subset A$ ramifies in A' if and only if it contains the ideal $D_{A'/A}$. Thus, since $D_{A'/A} \neq (0)$, there are only finitely many $\wp \subset A$ that ramify in A'.*

Therefore, taking $A = \mathbb{Z}$ and $A' = \vartheta_K$ (where $K/\mathbb{Q}$ is a finite extension), then Theorem 3.22 tells us that a prime $p \in \mathbb{Z}$ ramifies if and only if $D_{\vartheta_K/\mathbb{Z}} \subset (p)$, which is equivalent to saying that p divides the discriminant of ϑ_K over $\mathbb{Z}$.

Now suppose the field extension $L/\mathbb{Q}$ is a galois extension with galois group G. We introduce two very important subgroups of G that we will be concerned with in §3.5 and §3.6.

Definition 3.23. *Let $L/\mathbb{Q}$ be a galois extension. Let $p \in \mathbb{Q}$ be a prime, and fix a prime $\wp$ above p in L. Let $O_\wp$ be the ring of integers in L localized at $\wp$. Then we have two important subgroups of G:*

$$\begin{aligned} D_{\wp/p} &= \{\sigma \in G | \sigma\wp = \wp\} \\ I_{\wp/p} &= \{\tau \in G | \tau\omega \equiv \omega \ (mod\ \wp), \forall \omega \in O_\wp\} \end{aligned} \tag{3.15}$$

called the Decomposition Group and Inertia Group, respectively. We oftentimes will just write $D_\wp$ and $I_\wp$ when it is understood that we are considering these groups over the prime p.

Definition 3.24. *Let $L/\mathbb{Q}$ be a galois extension with galois group G, and fix a prime v in L over the prime p in $\mathbb{Q}$, with decomposition group $D_v = D$ and inertia group $I_v = I$. Since each of these are subgroups of G, Theorem 1.1 says we can find fields L^D and L^I such that*

$$\mathbb{Q} \subset L^D \subset L^I \subset L. \tag{3.16}$$

We call the field L^D the decomposition field and the field L^I the inertia field.

Remark 3.25. *The field L^D turns out to be the largest intermediate field $\mathbb{Q} \subset K \supset L$ such that $e(v/p) = f(v/p) = 1$ for a prime v in K over a prime p in $\mathbb{Q}$. Similarly, the field L^I turns out to be the largest intermediate field $\mathbb{Q} \subset K' \subset L$ for which $e(v'/p) = 1$ for a prime v' in K' over a prime p in $\mathbb{Q}$, and the smallest intermediate field that the prime p totally ramifies. All of these facts are proven in* [Bak].

Proposition 3.26. *The Decomposition Group $D_\wp$ has $|D_\wp| = e(\wp/p)f(\wp/p)$. Similarly, the Inertia Group $I_\wp$ has $|I_\wp| = e(\wp/p)$. Therefore, in the tower $\mathbb{Q} \subset L^D \subset L^I \subset L$ has $[L^D : \mathbb{Q}] = g(\wp/p)$, $[L^I : L^D] = f(\wp/p)$, and $[L : L^I] = e(\wp/p)$.*

Proof. For a proof of this fact, see [Ros].

□

We conclude this section by using this fact to prove the claim put forth in Theorem 3.6 that for an abelian group A, there are infinitely many galois extensions

$K/\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong A$. To do so, we first present, without proof, the following proposition. For a proof, see [IR].

Proposition 3.27. *Consider the field extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, and suppose $p \in \mathbb{Q}$ is a prime number. Let ϑ be the ring of integers in $\mathbb{Q}(\zeta_m)$, and let $\wp \subset \vartheta$ be a prime ideal such that $\wp \cap \mathbb{Z} = p$. If p is odd, the p ramifies in ϑ if and only if $p|m$. If $p = 2$, then p ramifies if and only if $4|m$.*

With Proposition 3.27, we can now prove the following theorem, which will complete the proof of Theorem 3.6.

Theorem 3.28 (Inverse Galois Problem for Abelian Groups Revisited)**.** *For any finite abelian group A, there are infinitely many solutions to the Inverse Galois Problem; that is, we may find infinitely many galois extensions $K/\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong A$.*

Proof. Recall that in the proof of Theorem 3.6, we used Theorem 3.4 to show that there are infinitely many primes $p_1, ..., p_k$ such that

$$\begin{aligned} p_1 &\equiv 1(mod\ n_1) \\ p_2 &\equiv 1(mod\ n_2) \\ &\vdots \\ p_k &\equiv 1(mod\ n_k) \end{aligned} \tag{3.17}$$

where the integers $n_1, ..., n_k$ are the integers coming from the expression of A using Theorem 3.3 as seen in the proof of Theorem 3.6. Then we may find infinitely many $n = p_1 p_2 \cdots p_k$ such that no two share a prime factor; that is, if $n_1 = p_1 p_2 \cdots p_k$ and $n_2 = q_1 q_2 \cdots q_k$, then $p_i \neq q_j$ for any $1 \leq i, j \leq k$. That means that, by Proposition 3.27, we may find infinitely many field extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, all having different ramified primes, that satisfy the conditions employed in the proof of Theorem 3.6. Therefore, we may construct infinitely many galois extensions $K/\mathbb{Q}$ following the methods of Theorem 3.6, and all such extensions have different ramified primes, which makes all the fields distinct.

□

3.3. **Algebraic Number Theory II: Local Fields.** In this section, we introduce many of the basics of local fields that are used in the proofs in §3.4, §3.5, and §3.6. We will primarily be interested in the p-adic numbers $\mathbb{Q}_p$ and, more generally, any completion $K_\wp$, where $K/\mathbb{Q}$ is galois and $\wp$ a prime in K over p. We will be able to show that, for local fields, we may find results similar to those we found in §3.2. The techniques developed here, as well as the tools we found in §3.2, will prove extremely useful in our work on Nilpotent Groups. We begin with the concept of a discrete valuation:

Definition 3.29. *Let K be a field, and $K^\times$ its multiplicative elements, and $\mathbb{Z}$ the ordinary integers. A mapping*

$$v : K \longrightarrow \mathbb{Z} \cup \infty \tag{3.18}$$

is called a discrete valuation of K if

1.) v defines a surjective homomorphism $K^\times \longrightarrow \mathbb{Z}$;
2.) $v(0) = \infty$;
3.) $v(x + y) \geq \inf\{v(x), v(y)\}$.

One can take a discrete valuation and construct a discrete multiplicative valuation in the following way: Let v be a discrete valuation of K and let ρ be a real number such that $0 < \rho < 1$, then $|x|_v = \rho^{v(x)}$ is a discrete, non-Archimedean

valuation. From [Cas], we see that one has the *p-adic* valuation on $\mathbb{Q}$ given by $|\frac{p^a m}{n}|_p = (\frac{1}{p})^a$. More generally, one may choose a $c > 1$ and define a valuation $|x|_\wp = c^{-ord_\wp(x)}$ where x is an element of the field of fractions K for a given Dedekind ring. For a more complete explanation, see [Cas].

Definition 3.30. *We call a field $K_\wp$ a local field if it is a field and a complete metric space with respect to a discrete valuation $|\ |_\wp$. Because of the completeness condition, local fields may sometimes be called completions.*

Proposition 3.31. *Let L/K be a galois extension of fields, and let $\wp$ in L be a prime element over the prime p in K. Then the field extension $L_\wp/K_p$ is a galois extension and $[L_\wp : K_p] = e(L/K)f(L/K)$.*

Proof. See [Fro].

□

One can also see that the decomposition group and inertia group obtained by a local extension $K_\wp/\mathbb{Q}_p$ are the same as the decomposition group and inertia group that one would obtain when looking at the extension $K/\mathbb{Q}$ for the prime $\wp$ over p. Because of this, we again can find decomposition and inertia fields via Theorem 1.1 as in the global case. For more details, see [Fro].

Next we present a series of results that will allow us to connect the concept of local field extensions to the concept of finite field extensions. It's an easy fact to show that, for a local field extension L/K and a finite field k, L/K determines an algebraic extension of k via residue class fields; if L/K is unramified, then this extension of k is separable (see [Fro]). Call this extension k_L/k. However, as it turns out, we may associate to each algebraic, separable extension of k a field extension of M/K as well, which will prove useful to us in later sections. We present these results without proofs; for the proofs, see [Fro].

Theorem 3.32. *Let $\overline{k}$ be a finite, separable, algebraic extension of k. Then there is a finite, separable, algebraic extension $L = L(\overline{k})$ of K such that*

1.) $\overline{k} = k_L$ (over k),

2.) L is unramified over K,

3.) the maps

$$Hom^K(L, L') \longrightarrow Hom^k(k_L, k_{L'}) \tag{3.19}$$

are bijective for all L'.

Properties 1 and 2 or 1 and 3 determine L up to isomorphism over K.

Theorem 3.33. *L has a subfield L_0 such that the subfields L' of L which are unramified over K are precisely the subfields of L_0. Also $k_{L_0} = k_L^s$, the separable closure of k in k_L.*

Let $\overline{K}$ be the separable closure of K. The field K^U is the union of all L (where $K \subset L \subset \overline{K}$) such that L/K is unramified. We call K^U the maximal unramified extension of K. Note that when K is a perfect field, $\overline{K}$ is simply the algebraic closure of K.

Corollary 3.34. *Every finite extension of K in K^U is unramified. The galois group $Gal(K^U/K)$ is isomorphic to the galois group $Gal((\overline{k})^s/k)$ of the separable closure $(\overline{k})^s$ of k.*

Corollary 3.34 allows us to make the following observation about $Gal(K^U/K)$. Suppose that k is a finite field of characteristic p with $q = p^m$ elements. By the classic construction, $Gal((\overline{k})^s/k) \cong \hat{\mathbb{Z}}$ ($(\overline{k})^s$ contains a subfield k_m/k of degree m whose galois group is $Gal(k_m/k) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ for all m; taking the inverse limit

will give us $Gal((\overline{k})^s/k) \cong \hat{\mathbb{Z}}$). Observe that Corollary 3.34 implies that, for every $n > 0$, there is one and (up to isomorphism) only one unramified extension L/K with $[L : K] = n$.

Corollary 3.34 also tells us that $Gal(K^U/K) \cong \hat{\mathbb{Z}}$. This also allows us to conclude that K^U is the union of fields of m-th roots of unity (in a given separable closure of K) for all m such that $(m, p) = 1$. For more details of this conclusion, see [Fro].

3.4. **Nilpotent Groups of Odd Order.** We are now ready to prove our main result. We follow the method outlined in [Ser2], which was originally presented by Scholz and Reichardt. Before doing so, we state a theorem that, much like Theorem 3.3 for the abelian group case, allows us to fully understand the structure of a nilpotent group.

Theorem 3.35. *Let G be a finite group or order n, let $p_1, p_2, ...p_k$ be the distinct primes dividing n, and let P_i be a p_i-sylow subgroup of G. Then the following are equivalent:*

1.) G is nilpotent

2.) if $H < G$, then $H < N_G(H)$. In other words, every proper subgroup of G is a proper subgroup of its normalizer in G.

3.) P_i is normal in G for all $1 \leq i \leq k$.

4.) $G \cong P_1 \times P_2 \times \cdots \times P_k$.

Proof. For a proof of this theorem, see [DF].

□

So we're able to fully classify the structure of nilpotent groups in much the same way that we were able to classify the structure of abelian groups in §3.1. The difference is that before we classified our groups in terms of cyclic groups and our knowledge of cyclotomic extensions of $\mathbb{Q}$, whereas now we classify our groups in terms of p-groups and in particular the group's p-sylow subgroups. So suppose we have a nilpotent group G. By Theorem 3.35, $G \cong P_1 \times \cdots P_k$, where each P_i is as above. So if we can find a galois extension $K_i/\mathbb{Q}$ such that $\mathrm{Gal}(K_i/\mathbb{Q}) \cong P_i$ for every $1 \leq i \leq k$, then (by basic knowledge of field theory and galois theory) the compositum $K_1K_2 \cdots K_k = K$ will be such that $K/\mathbb{Q}$ is a galois extension and

$$\begin{aligned} Gal(K/\mathbb{Q}) &\cong Gal(K_1/\mathbb{Q}) \times Gal(K_2/\mathbb{Q}) \times \cdots \times Gal(K_k/\mathbb{Q}) \\ Gal(K/\mathbb{Q}) &\cong P_1 \times P_2 \times \cdots \times P_k \\ Gal(K/\mathbb{Q}) &\cong G, \end{aligned} \tag{3.20}$$

solving the Inverse Galois Problem for nilpotent G.

So the problem immediately reduces down to proving that any p-group may be realized as the galois group of some galois extension of $\mathbb{Q}$.

Theorem 3.36 (Inverse Galois Problem for Nilpotent Groups of Odd Order)**.** *For every ℓ-group G, $\ell \neq 2$, there exists a field K such that $\mathbb{Q} \subset K$, $K/\mathbb{Q}$ is a galois extension, and $Gal(K/\mathbb{Q}) \cong G$. By the above argument, the Inverse Galois Problem is solvable for Nilpotent Groups of odd order.*

Remark 3.37. *Here we say ℓ-group instead of p-group because the proof will require us to explore ramified primes, and reserving the letter p for that use will prove to be more convenient. Observe also that this proof does not work for $\ell = 2$. This is because the primitive 2-root of unity is -1, which happens to be an element of $\mathbb{Q}$. Because of this, 2 cannot divide the order of G, imposing the odd order condition.*

By Theorem 3.35, one trivially sees that any ℓ-group is a nilpotent group, and so we may build one up from a series of central extensions by groups of order ℓ. Therefore, in order to prove Theorem 3.36, it is enough to show that we may

construct a tower of extensions of degree ℓ, each time remaining galois over $\mathbb{Q}$, so that we eventually construct our desired galois extension. Doing this in general doesn't work because the embedding problem is not always solvable. So to do this, we make additional specifications about the extensions at each stage, for which the embedding problem is solvable (this is the great idea of Sholz and Reichardt). For convenience, we adopt the notation presented in [Ser2].

Let $L/\mathbb{Q}$ be a galois extension with galois group G, where G is an ℓ-group. Choose $N \geq 1$ such that ℓ^N is a multiple of the exponent of G.

Definition 3.38 (Scholz Property)**.** *The extension $L/\mathbb{Q}$ is said to have the Scholz property for N (hereby denoted (S_N)) if every prime p which is ramified in $L/\mathbb{Q}$ satisfies:*

1.) $p \equiv 1 \ (mod\ \ell^N)$

2.) If v is a prime in L dividing p, then the inertia group I_v is equal to the decomposition group D_v. In other words, the local extension $L_v/\mathbb{Q}_p$ is totally ramified.

So we adapt the group extension problem to this situation:

$$1 \longrightarrow Z_\ell \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1, \tag{3.21}$$

an exact sequence of ℓ-groups with Z_ℓ central, cyclic of order ℓ. Here let the group $\widetilde{G}$ be the solution to the group extension problem, i.e. Z_ℓ can be realized as a normal subgroup of $\widetilde{G}$ and the group $\widetilde{G}/Z_\ell \cong G$. So $\widetilde{G}$ is an extension of G by the group Z_ℓ, and so we need to show that with $\widetilde{G}$ we can solve the embedding problem also.

To solve the embedding problem for $\widetilde{G}$, we need to construct a galois extension $\widetilde{L}$ of $\mathbb{Q}$ containing L such that we have isomorphisms $\mathrm{Gal}(\widetilde{L}/L) \cong Z_\ell$ and $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \cong \widetilde{G}$, and such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_\ell & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Gal(\widetilde{L}/L) & \longrightarrow & Gal(\widetilde{L}/\mathbb{Q}) & \longrightarrow & Gal(L/\mathbb{Q}) & \longrightarrow & 1 \end{array} \tag{3.22}$$

is commutative.

With this approach, Theorem 3.36 is proven by inductively applying the following:

Theorem 3.39. *Let $L/\mathbb{Q}$ be galois with Galois group G, and assume that L has property (S_N). Assume further that ℓ^N is a multiple of the exponent of $\widetilde{G}$. Then the embedding problem for L and $\widetilde{G}$ is solvable. Furthermore, the solution $\widetilde{L}$ can be chosen to have property (S_N) and ramified in at most one more place than L.*

Proving Theorem 3.39 will reduce the entire problem of nilpotent groups of odd order to groups of order ℓ, $\ell \neq 2$ prime, which is then solved by Theorem 3.6, since all such groups are abelian. To see that we may find such an extension satisfying property (S_N), take any prime $p \equiv 1 \ (mod\ \ell^N)$ (which we can find by Theorem 3.4), and consider the field $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$. Since $p \equiv 1 \ (mod\ \ell^N)$, we know that in particular $p \equiv 1 \ (mod\ \ell)$ and from our work in §3.1, this implies the existence of a field $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$ such that $Gal(K/\mathbb{Q}) \cong Z_\ell$. From our work in §3.2, we know that the only prime which can ramify in K is the prime p, which was constructed to satisfy $p \equiv 1 \ (mod\ \ell^N)$. Therefore, the first condition holds. Now recall that for any prime v (over p) in ϑ_K, we have that $efg = \ell$ by Theorem 3.19 since $K/\mathbb{Q}$ is galois with $[K : \mathbb{Q}] = \ell$ by construction. Since ℓ is assumed to be prime and $e > 1$, we have that $e = \ell$, $f = 1$ and $g = 1$, which means that D_v/I_v has $|D_v/I_v| = 1$. Therefore, $D_v = I_v$ and the second condition holds.

So our base case is true. Now applying Theorem 3.39 inductively proves Theorem 3.36 for all ℓ-groups, $\ell \neq 2$. The idea is that we've shown our base case (worked above) to be true, so now we need to show our inductive step is true also. So we choose a group G to be a galois group over $\mathbb{Q}$ satisfying property (S_N). The purpose of Theorem 3.39 is to show that with this hypothesis, for every central extension of G by Z_ℓ (the cyclic group of order ℓ) we may solve the embedding problem to construct a new galois group satisfying property (S_N), completing the induction. To prove Theorem 3.39, we examine two cases: first, where the extension $\widetilde{G}$ is a split extension (i.e. $\widetilde{G} \cong G \times Z_\ell$), which we handle in §3.5, and then where the extension doesn't split, which we address in §3.6.

3.5. **The Split Extension Case.** In this section we prove the first case of Theorem 3.39, the case where the extension splits, so $\widetilde{G} \cong G \times Z_\ell$. These results, combined with the results of §3.6, will prove Theorem 3.39.

Let $(p_1, ..., p_m)$ be the prime numbers that are ramified in L (where $L/\mathbb{Q}$ is a galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ as before). Select a prime q with the following properties:

1.) $q \equiv 1 \ (mod\ \ell^N)$,
2.) q splits completely in the extension $L/\mathbb{Q}$,
3.) Every prime p_i, $1 \leq i \leq m$, is an ℓ-th power in $\mathbb{F}_q$.

These three conditions are equivalent to saying that the prime q splits completely in the field $L(\zeta_{\ell^N}, \sqrt[\ell]{p_1}, ..., \sqrt[\ell]{p_m})$, where ζ_{ℓ^N} is a primitive ℓ^N-th root of unity. To see this, consider the field $\mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i})$. If we can show that q splits completely in this field, then by taking the compositum of L and $\mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i})$ for all $i = 1, ..., m$, we get the desired result. We see this through the following results:

Proposition 3.40. *Let $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ be galois extensions of $\mathbb{Q}$, and let $q \in \mathbb{Q}$ be a prime. Then q splits completely in K_1K_2 if and only if q splits completely in both K_1 and K_2.*

Proof. Suppose that q splits completely in K_1K_2, so we have that

$$q\vartheta_{K_1K_2} = \wp_1\wp_2 \cdots \wp_t \tag{3.23}$$

where $t = [K_1K_2 : \mathbb{Q}]$. Let $\wp_i' = \wp_i \cap \vartheta_{K_1}$. So by the multiplicative nature of the residual degree, we have that $f(\wp_i/q) = f(\wp_i/\wp_i')f(\wp_i'/q)$. Since we're assuming that q splits completely, we have that $f(\wp_i/q) = 1$ for all i. As a result, we have that $f(\wp_i/\wp_i') = f(\wp_i'/q) = 1$, the latter of which implies that q splits in K_1. The argument is similar for K_2.

Now suppose that q splits completely in both K_1 and K_2. Let $L = K_1K_2$. We know that $\mathbb{Q} \subset L^D \subset L$ by definition. Since q splits completely in K_1 and K_2, we have that $e(\wp_i'/q) = f(\wp_i'/q) = 1$ for all primes $\wp_i'$ in K_1 and K_2 over the prime q. By Remark 3.25, $L^D \supset K_1$ and $L^D \supset K_2$, which implies that $L^D \supset L$. Therefore $L^D = L$. Since the decomposition group has order $e(\wp_i/q)f(\wp_i/q)$, Theorem 1.1 tells us that $[L : L^D] = e(\wp_i/q)f(\wp_i/q)$. Since $L = L^D$, that means that $e(\wp_i/q)f(\wp_i/q) = 1$, which can only happen if $e(\wp_i/q) = f(\wp_i/q) = 1$. Thus q splits completely in the compositum K_1K_2 as well.

□

Now we proceed by proving that the prime q splits completely in the field $\mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i})$ for every $i = 1, ..., m$. Doing so, and then applying Proposition 3.40 inductively to the fields $L, \mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_1}), ..., \mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_m})$ will show that q splits in the field $L(\zeta_{\ell^N}, \sqrt[\ell]{p_1}, ..., \sqrt[\ell]{p_m})$. We present three propositions that give us this result; proofs for all three propositions may be found in [Bir].

Proposition 3.41. *Let ζ_m be a primitive m-th root of unity. Suppose $p \in \mathbb{Q}$ is a prime not dividing m (so p is unramified in $\mathbb{Q}(\zeta_m)$), and suppose $\wp$ is a prime above p in $\mathbb{Q}(\zeta_m)$. Then $f(\wp/p)$ is the least integer $f \geq 1$ such that $p^f \equiv 1 \pmod{m}$.*

Remark 3.42. *In our case, we have $m = \ell^N$ and we have that $q \equiv 1 \pmod{\ell^N}$ by assumption; therefore, we have that $f(\wp/q) = 1$ and the prime q splits completely in the field $\mathbb{Q}(\zeta_{\ell^N})$. Furthermore, this is if and only if, since if the prime q splits completely in the field $\mathbb{Q}(\zeta_{\ell^N})$, then $f(\wp/q) = 1$ and so $q \equiv 1 \pmod{\ell^N}$.*

In the next two propositions, we assume that K is a field of characteristic prime to n (or of characteristic 0) in which $x^n - 1$ splits.

Proposition 3.43. *Suppose p is a prime in K and $\wp$ a prime in $K(\sqrt[n]{a})$ over p. The discriminant of $K(\sqrt[n]{a})$ over K divides $n^n a^{n-1}$; p is unramified if $p \nmid na$. If a^f is the least power of a such that $x^n \equiv a^f \pmod{p}$ is solvable, then $f = f(\wp/p)$, the residual degree.*

Proposition 3.44. *If $p \mid a$, $p \nmid n$ and $p^n \nmid a$ the p is tamely ramified in $K(\sqrt[n]{a})$; if $p \mid a$ and $p^2 \nmid a$ then p is totally ramified in $K(\sqrt[n]{a})$.*

Remark 3.45. *In our case, we have $K = \mathbb{Q}(\zeta_{\ell^N})$, $n = \ell$, $a = p_i$, and we're considering the prime $\wp$ in K over the prime q in $\mathbb{Q}$. Let v be the prime in $K(\sqrt[n]{a})$ over $\wp$. Then we need to find the smallest f such that $x^\ell \equiv p_i^f \pmod{\wp}$. However, we assume that $x^\ell \equiv p_i \pmod{q}$ is solvable, and since $\wp | q$, we have that $x^\ell \equiv p_i \pmod{\wp}$ is solvable. Therefore, $f(v/\wp) = 1$. Again this statement is if and only if, since if the prime $\wp$ splits completely in this extension, then $f(v/\wp) = 1$ and $x^\ell \equiv p_i \pmod{q}$ is forced.*

Combining our observations from Remarks 3.42 and 3.45, we see that the prime q is unramified in $\mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i})$. Also, we know that $f(v/q) = f(v/\wp)f(\wp/q)$, but $f(v/\wp) = 1$ and $f(\wp/q) = 1$, so $f(v/q) = 1$ also and q splits completely in $\mathbb{Q}(\zeta_{\ell^N}, \sqrt[\ell]{p_i})$.

Therefore, in order to find a prime q satisfying our three conditions, it's enough to find a prime q that splits completely in the field $L(\zeta_{\ell^N}, \sqrt[\ell]{p_1}, ..., \sqrt[\ell]{p_m})$, a finite extension of $\mathbb{Q}$. We now seek to show that such a q exists, which we may do by proving the following lemma:

Lemma 3.46. *If $K/\mathbb{Q}$ is a finite extension of $\mathbb{Q}$, then there are infinitely many primes which split completely in K.*

Proof. The proof that follows is an adaptation of the same proof for function fields. Formally, the steps follow in the same way when we consider number fields, except that we define the norm of an ideal ϱ in a ring A to be $N\varrho = card(A/\varrho)$. The proof follows as presented in [Ros].

We proceed by showing that the Dirichlet Density of such primes is nonzero. In particular, we will show that, for a finite extension $K/\mathbb{Q}$ with $[K : \mathbb{Q}] = n$, the set of primes in $\mathbb{Q}$ which split completely in K (denoted $\{K\}$) has Dirichlet Density $d\{K\} = \frac{1}{n}$. Here the set S_K denotes the set of all primes in K.

We begin by considering the logarithm of the zeta function of K. This gives us

$$log\zeta_K(s) = \sum_{\wp \in S_K} \sum_{k=1}^{\infty} k^{-1} N\wp^{-ks} = \sum_{\wp} N\wp^{-s} + \sum_{\wp} \sum_{k=2}^{\infty} k^{-1} N\wp^{-ks}. \tag{3.24}$$

Call the second of these terms $R_K(s)$, and let $x = Re(s)$. Then we observe the following:

$$|R_K(s)| < \sum_{\wp} \sum_{k=2}^{\infty} N\wp^{-kx} = \sum_{\wp} N\wp^{-2x}(1 - N\wp^{-x})^{-1}$$
$$< 2\sum_{\wp} N\wp^{-2x} < 2\zeta_K(2x) \tag{3.25}$$

and since $\zeta_K(s)$ is analytic for all $x > 1$, we have that $\zeta_K(2s)$ is bounded in a neighborhood of $s = 1$. Therefore, the term $R_K(s)$ is bounded as $s \longrightarrow 1^+$.

For the terms that remain, we group together the terms lying over a fixed prime p in $\mathbb{Q}$ and we have

$$log\zeta_K(s) \approx \sum_{p \in S_{\mathbb{Q}}} \sum_{\wp | p} N\wp^{-s}. \tag{3.26}$$

As the set of primes that ramify is finite, we may ignore them and consider only those with ramification index $e(\wp/p) = 1$. Then for all the remaining primes we have $f(\wp/p)g(\wp/p) = n$. Using the fact that $N\wp = Np^{f(\wp/p)}$, we may rewrite the sum as

$$\sum_{p \in S_{\mathbb{Q}}} \sum_{\wp | p} N\wp^{-s} = \sum_{f|n} \frac{n}{f} \sum_{p \in S_{\mathbb{Q}},\ f(\wp/p)=f} Np^{-fs}. \tag{3.27}$$

The terms with $f > 1$ is bounded in a neighborhood of $s = 1$ and the sum of the terms with $f = 1$ is exactly $n\sum_{p \in \{K\}} Np^{-s}$. Taking this expression, dividing by $-log(s-1)$, and taking the limit as $s \longrightarrow 1^+$ gives us that $1 = n(d\{K\})$, or that $d\{K\} = \frac{1}{n}$ as claimed. Since the Dirichlet Density of our set is nonzero, the set must be infinite.

□

So we choose such a prime q. Having done so, we fix a surjective homomorphism

$$\lambda' : (\mathbb{Z}/q\mathbb{Z})^{\times} \longrightarrow Z_\ell, \tag{3.28}$$

which we may find because $q \equiv 1\ (mod\ \ell)$. Composing λ' with the isomorphism $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^{\times}$ described in Theorem 3.1, we construct a mapping

$$\lambda : Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \longrightarrow Z_\ell \tag{3.29}$$

which we see is a galois character. Let $H = ker(\lambda)$. Then Theorem 1.1 says that we may find the field $M_\lambda = \mathbb{Q}(\zeta_q)^H$ and that $Gal(M_\lambda/\mathbb{Q}) \cong Z_\ell$. Furthermore, because $\mathbb{Q} \subset M_\lambda \subset \mathbb{Q}(\zeta_q)$, we have that M_λ is ramified only at the prime q (in fact the extension $M_\lambda/\mathbb{Q}$ is totally ramified). Because q was chosen to split completely in L, we have that q is ramified in M_λ and unramified in L, which forces $L \cap M_\lambda = \mathbb{Q}$. Then by basic galois theory, the compositum field $M_\lambda L/\mathbb{Q}$ is galois with galois group $G \times Z_\ell$, which by assumption is $\widetilde{G}$.

Now all we have left to show that that this new field $M_\lambda L$ has property (S_N). All the primes that ramify in $M_\lambda L$ ramify either in L or in M_λ. By construction, we have that $q \equiv 1\ (mod\ \ell^N)$ so the first condition holds for q. Because the p_i ramify in $M_\lambda L$ and because they already were assumed to satisfy $p_i \equiv 1\ (mod\ \ell^N)$ for all $i = 1, ..., m$, we see that $M_\lambda L$ satisfies the first condition of property (S_N). For the second condition, we have two cases to consider: first, we consider the prime q and show that for every $v|q$ in $M_\lambda L$, we have that $D_v = I_v$ or, equivalently, that $f(v/q) = 1$; and second, we show the same result holds for the primes $p_1, ...p_m$.

For the prime q, we recall that q was chosen to split completely in L. So we consider the local field extensions $\mathbb{Q}_q \subset L_{\wp^{(1)}} \subset (M_\lambda L)_v$ and $\mathbb{Q}_q \subset (M_\lambda)_{\wp^{(2)}} \subset$

$(M_\lambda L)_v$ where $\wp^{(1)}, \wp^{(2)}, v$ are all primes over q in their respective fields. These fields are all the completions as described in §3.3. Since all the original extensions were galois, all the local extensions are galois, and we have that

$$[L_{\wp^{(1)}} : \mathbb{Q}_q] = e(\wp^{(1)}/q)f(\wp^{(1)}/q) \tag{3.30}$$

$$[(M_\lambda L)_v : L_{\wp^{(1)}}] = e(v/\wp^{(1)})f(v/\wp^{(1)}) \tag{3.31}$$

$$[(M_\lambda)_{\wp^{(2)}} : \mathbb{Q}_q] = e(\wp^{(2)}/q)f(\wp^{(2)}/q) \tag{3.32}$$

$$[(M_\lambda L)_v : (M_\lambda)_{\wp^{(2)}}] = e(v/\wp^{(2)})f(v/\wp^{(2)}) \tag{3.33}$$

$$\begin{aligned}[(M_\lambda L)_v : \mathbb{Q}_q] &= e(v/q)f(v/q) = e(v/\wp^{(1)})e(\wp^{(1)}/q)f(v/\wp^{(1)})f(\wp^{(1)}/q) \\ &= e(v/\wp^{(2)})e(\wp^{(2)}/q)f(v/\wp^{(2)})f(\wp^{(2)}/q).\end{aligned} \tag{3.34}$$

We want to use this information to show that $f(v/q) = 1$, as doing so will imply that $D_v = I_v$. By construction, we know that q splits completely in L so we have that $e(\wp^{(1)}/q) = f(\wp^{(1)}/q) = 1$, which also gives us that $[L_{\wp^{(1)}} : \mathbb{Q}_q] = 1$. Similarly, we know that q is totally ramified in M_λ, so $e(\wp^{(2)}/q) = \ell$ and $f(\wp^{(2)}/q) = 1$. One can show that, for these fields, $e_{(M_\lambda L)_v/L_{\wp^1}} \leq e_{(M_\lambda)_{\wp^2}/\mathbb{Q}_q}$ (see [Koc]; if L/K and M/K are galois extensions of the p-adic field K, then $e_{ML/L} \leq e_{M/K}$). Because $e(\wp^{(1)}/q) = 1$, we have that $e(v/q) \leq e(\wp^{(2)}/q)$, or that $e(v/\wp^{(2)}) \leq 1$, which forces $e(v/\wp^{(2)}) = 1$. Also, because $e(\wp^{(2)}/q) = \ell$, we have that $e(v/q) \leq \ell$ and since $\ell | e(v/q)$, we have that $e(v/q) = \ell$. This forces $e(v/\wp^{(1)}) = \ell$.

Now we recall that $(M_\lambda L)_v^I \subset (M_\lambda L)_v$ is a galois extension of degree $e(v/q) = \ell$, and that $(M_\lambda L)_v^I$ is the smallest subfield of $M_\lambda L_v$ such that the prime q is totally ramified. Since q is totally ramified in M_λ (remember that $M_\lambda/\mathbb{Q}$ is a galois extension of degree ℓ), we know that $\mathbb{Q}_q \subset (M_\lambda L)_v^I \subset (M_\lambda)_{\wp^{(2)}} \subset (M_\lambda L)_v$. Since $[(M_\lambda L)_v : (M_\lambda L)_v^I] = \ell$, we have that either $(M_\lambda)_{\wp^{(2)}} = (M_\lambda L)_v$ or $(M_\lambda)_{\wp^{(2)}} = (M_\lambda L)_v^I$. Similarly, since $[(M_\lambda)_{\wp^{(2)}} : \mathbb{Q}_q] = \ell$, we have that either $(M_\lambda L)_v^I = (M_\lambda)_{\wp^{(2)}}$ or $(M_\lambda L)_v^I = \mathbb{Q}_q$. But if $(M_\lambda L)_v^I = (M_\lambda)_{\wp^{(2)}}$, then $[(M_\lambda L)_v : \mathbb{Q}_q] = \ell^2$, a contradiction. Therefore, we have that $(M_\lambda L)_v^I = \mathbb{Q}_q$ and $(M_\lambda)_{\wp^{(2)}} = (M_\lambda L)_v$. The second of these conditions implies that $f(v/\wp^{(2)}) = 1$, so $f(v/q) = 1$ and $D_v = I_v$. So the ramified prime q satisfies property (S_N).

Now we need to show that each p_i satisfies the second condition of (S_N). By assumption, p_i satisfies (S_N) in L, so for a prime $\wp_i^{(1)}$ in L over p_i, we have that $D_{\wp_i^{(1)}} = I_{\wp_i^{(1)}}$, which implies that $f(\wp_i^{(1)}/p_i) = 1$. Since $M_\lambda L$ was was constructed as the solution to the embedding problem for L and $\widetilde{G} \cong G \times Z_\ell$, we have that $Gal(M_\lambda L/L) \cong Z_\ell$. Also, by our construction above, $Gal(M_\lambda/\mathbb{Q}) \cong Z_\ell$. It is clear that the restriction map res_{M_λ} is an explicit isomorphism between $Gal(M_\lambda L/L)$ and $Gal(M_\lambda/\mathbb{Q})$. Let $\wp_i^{(2)}$ be a prime in M_λ over p_i. We prove the following result, which may be found in [Ros]:

Proposition 3.47. *Let L/K be a galois extension of number fields and let M be any intermediate field. Let v be a prime of L, and let $\wp$ and p be the primes lying below v in M and K, respectively. Let $H = Gal(L/M)$. Then*

$$(i) \quad D_{v/\wp} = H \cap D_{v/p} \quad \text{and} \quad I_{v/\wp} = H \cap I_{v/p}. \tag{3.35}$$

Now suppose H is a normal subgroup, and that $res_M : Gal(L/K) \longrightarrow Gal(M/K)$. Then

$$(ii) \quad res_M(D_{v/p}) = D_{\wp/p} \ \ and \ \ res_M(I_{v/p}) = I_{\wp/p}. \tag{3.36}$$

Proof. Part (i) is clear from the definitions. For part (ii), we first observe that if $\sigma \in D_{v/p}$, then by definition $\sigma v = v$. We know that $\wp = v \cap M$ so we have that $\sigma\wp = \sigma(v \cap M)$, and since $v \cap M \subset v$, we have that $\sigma(v \cap M) = (\sigma v) \cap M = v \cap M = \wp$. So we see that $res_M : (D_{v/p}) \longrightarrow D_{\wp/p}$. Now we want to show this map is surjective. The kernel of this mapping turns out to be $D_{v/p} \cap H = D_{v/\wp}$, which is clear. Thus, the order of the image will be:

$$\frac{e(v/p)f(v/p)}{e(v/\wp)f(v/\wp)} = e(\wp/p)f(\wp/p) = |D_{\wp/p}| \tag{3.37}$$

which proves the map is a surjection. The inertia group case is analogous.

□

So let $res_{M_\lambda} : Gal(M_\lambda L/\mathbb{Q}) \longrightarrow Gal(M_\lambda/\mathbb{Q})$, where res_{M_λ} is as before (we're simply considering it over all of $Gal(M_\lambda L/\mathbb{Q})$ instead of $Gal(M_\lambda L/L)$). Clearly, $ker(res_{M_\lambda}) = Gal(L/\mathbb{Q})$. By Proposition 3.47, $res_{M_\lambda}(D_{v/p_i}) = D_{\wp_i^{(2)}/p_i}$. If $\sigma \in D_{\wp_i^{(1)}/p_i}$, then under res_{M_λ} (because $\wp_i^{(1)} \cap M_\lambda = p_i$), we have $res_{M_\lambda}(D_{\wp_i^{(1)}/p_i}) = (e)$, where $e \in Gal(M_\lambda/\mathbb{Q})$ is the identity. Since $ker(res_{M_\lambda}) = Gal(L/\mathbb{Q})$, restricting to D_{v/p_i} gives $D_{\wp_i^{(1)}/p_i} = ker(res_{M_\lambda})$. Thus, $D_{v/p_i}/D_{\wp_i^{(1)}/p_i} \cong D_{\wp_i^{(2)}/p_i}$ and we have that

$$\frac{e(v/p_i)f(v/p_i)}{e(\wp_i^{(1)}/p_i)f(\wp_i^{(1)}/p_i)} = e(\wp_i^{(2)}/p_i)f(\wp_i^{(2)}/p_i). \tag{3.38}$$

Remembering that $e(v/p_i) = e(v/\wp_i^{(1)})e(\wp_i^{(1)}/p_i)$ and $f(v/p_i) = f(v/\wp_i^{(1)})f(\wp_i^{(1)}/p_i)$, we have

$$e(v/\wp_i^{(1)})f(v/\wp_i^{(1)}) = e(\wp_i^{(2)}/p_i)f(\wp_i^{(2)}/p_i). \tag{3.39}$$

One may, in an analogous way, find similar results for the inertia groups, and see that $I_{v/p_i}/I_{\wp_i^{(1)}/p_i} \cong I_{\wp_i^{(2)}/p_i}$. This gives us that

$$\frac{e(v/p_i)}{e(\wp_i^{(1)}/p_i)} = e(\wp_i^{(2)}/p_i) \tag{3.40}$$

which reduces to

$$e(v/\wp_i^{(1)}) = e(\wp_i^{(2)}/p_i). \tag{3.41}$$

Combining these results, we conclude that $f(v/\wp_i^{(1)}) = f(\wp_i^{(2)}/p_i)$. Since we know that $f(\wp_i^{(1)}/p_i) = 1$, we complete the proof if we can show that $f(\wp_i^{(2)}/p_i) = 1$, since doing so will imply that $f(v/p_i) = 1$ for every p_i, which implies that $D_v = I_v$ as needed.

Recall that $Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ has a specific isomorphism, where $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ is taken to $\sigma_a \in Gal(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, where $\sigma_a(\zeta_q) = \zeta_q^a$. It turns out that, for $p \in \mathbb{Q}$ and for a prime $\alpha \in \mathbb{Q}(\zeta_q)$ above it, $f(\alpha/p) = order(\sigma_p)$. To see this, we realize that $f = order(\sigma_p)$ means that σ_p^f will be the identity mapping, so $\sigma_p^f(\zeta_q) = \zeta_q$, which means that $\zeta_q^{p^f} = \zeta_q$. So $p^f \equiv 1 \ (mod\ q)$, which gives $f(\alpha/p)$.

Let λ be the map as in 3.29, and consider again the primes $p_1, ..., p_m, q$. Again, let $\wp_i^{(2)}$ be a prime in M_λ over p_i, and let $\alpha \in \mathbb{Q}(\zeta_q)$ be a prime over p_i as well. We may view λ as the restriction map from the field $\mathbb{Q}(\zeta_q)$ to the field M_λ and so by Proposition 3.47, we have that $\lambda(D_{\alpha/p_i}) = D_{\wp_i^{(2)}}$. We know p_i is unramified in both $\mathbb{Q}(\zeta_q)$ and M_λ so we know that $|D_{\alpha/p_i}| = f(\alpha/p_i) = order(\sigma_{p_i})$ and that $|D_{\wp_i^{(2)}/p_i}| = f(\wp_i^{(2)}/p_i) = order(\tau_{p_i})$, where $\tau_{p_i} = \lambda(\sigma_{p_i})$. Therefore, the automorphisms σ_{p_i} and τ_{p_i} generate the groups D_{α/p_i} and $D_{\wp_i^{(2)}/p_i}$, respectively. These automorphisms are called the *Frobenius* automorphisms for the respective extensions.

Recall that we constructed q so that p_i was an ℓ-th power in $\mathbb{F}_q$, so the congruence

$$x^\ell \equiv p_i \ (mod\ q) \tag{3.42}$$

is solvable. Let a_i be a solution to this congruence. Then we have that

$$\sigma_{a_i^\ell} = \sigma_{p_i}, \tag{3.43}$$

which implies that

$$(\sigma_{a_i})^\ell = \sigma_{p_i}. \tag{3.44}$$

Now we apply λ to both sides to get:

$$(\tau_{a_i})^\ell = \tau_{p_i} \tag{3.45}$$

and because $Gal(M_\lambda/\mathbb{Q}) \cong Z_\ell$, we know that $(\tau_{a_i})^\ell = 1$. Therefore, $\tau_{p_i} = 1$. Therefore, τ_{p_i} has order 1, which implies that $f(\wp_i^{(2)}/p_i) = 1$, which is what we needed to show.

So this shows that whenever the extension

$$1 \longrightarrow Z_\ell \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1 \tag{3.46}$$

is a split extension, then we may find a galois extension $\widetilde{L}/\mathbb{Q}$ such that $Gal(\widetilde{L}/\mathbb{Q}) \cong \widetilde{G}$ and such that $\widetilde{L}$ satisfies property (S_N).

3.6. **The Non-split Extension Case.** In this case, our group extension $\widetilde{G}$ is not a direct product of G and Z_ℓ, so our work becomes much more difficult. We will proceed in three stages. First, we find an extension $\widetilde{L}$ that solves the embedding problem for our desired group extension $\widetilde{G}$. Then we will modify the field $\widetilde{L}$ so that it has the same ramified primes as the field L. Finally, we will modify $\widetilde{L}$ a little more so that it satisfies property (S_N), with at most one additional ramified prime. Combining these results with the results of §3.5 will complete the proof of Theorem 3.39. We use the notation $G_\mathbb{Q} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

3.6.1. *Solving the Embedding Problem.* We begin with the galois extension $L/\mathbb{Q}$ as before. We observe that the extension L induces a surjective homomorphism $\phi : G_\mathbb{Q} \longrightarrow G$. To see this, we realize that $\mathbb{Q} \subset L \subset \overline{\mathbb{Q}}$ and $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) = G_\mathbb{Q}$ by definition. Then consider the restriction res_L, the map that restricts automorphisms of $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$ to automorphisms of L fixing $\mathbb{Q}$. This mapping is clearly surjective, and $N = ker(res_L) = Gal(\overline{\mathbb{Q}}/L)$. Thus, we've shown that such a ϕ exists (from this point onward we will refer to the mapping res_L as ϕ). So we have the following situation:

$$\begin{array}{ccccc} & & G_{\mathbb{Q}} & & \\ & & \downarrow & & \\ \widetilde{G} & \longrightarrow & G & \longrightarrow & (1). \end{array} \tag{3.47}$$

Suppose we could lift to a surjective map $\widetilde{\phi} : G_{\mathbb{Q}} \longrightarrow \widetilde{G}$. Then, for $\pi : \widetilde{G} \longrightarrow G$, we have that $\phi = \pi \circ \widetilde{\phi}$. Let $H = ker(\widetilde{\phi})$. Because $\phi = \pi \circ \widetilde{\phi}$, we have that $H \subset N \subset G_{\mathbb{Q}}$. Let $\widetilde{L}$ be the fixed field for H, which we know exists by Theorem 1.1. By the first isomorphism theorem, $G_{\mathbb{Q}}/H \cong \widetilde{G}$, so by basic galois theory, we have that $Gal(\widetilde{L}/\mathbb{Q}) \cong \widetilde{G}$. Thus, our problem is to lift this map to a homomorphism $\widetilde{\phi} : G_{\mathbb{Q}} \longrightarrow \widetilde{G}$ (surjectivity is automatic because we're assuming that $\widetilde{G}$ doesn't split). If we can find such a lift, then we can find $\widetilde{L}$.

As shown in Theorem 2.24, there is a bijection between the extensions $\widetilde{G}$ of G by Z_ℓ and the elements of $H^2(G, Z_\ell)$. Let $\xi \in H^2(G, Z_\ell)$ be the element corresponding to the extension $\widetilde{G}$. The homomorphism ϕ induces a homomorphism

$$\phi^* : H^2(G, Z_\ell) \longrightarrow H^2(G_{\mathbb{Q}}, Z_\ell). \tag{3.48}$$

So we now show that the existence of a lifting $\widetilde{\phi}$ is equivalent to the element ξ vanishing under ϕ^*, as seen in [MM].

Definition 3.48 (Fibre Products over Groups)**.** *Let G be a group and let $i : X \longrightarrow G$ and $j : Y \longrightarrow G$ be surjective group homomorphisms. A fibre product of X and Y over G is a group $X \times_G Y$, together with projection mappings $p_1 : X \times_G Y \longrightarrow X$ and $p_2 : X \times_G Y \longrightarrow Y$, such that for any other group Z with homomorphisms $q_1 : Z \longrightarrow X$ and $q_2 : Z \longrightarrow Y$ such that $i \circ q_1 = j \circ q_2$, there is a unique homomorphism $(q_1, q_2) : Z \longrightarrow X \times_G Y$ making the following diagram commute:*

$$\begin{array}{ccccc} Z & \longrightarrow & X & \longrightarrow & G \\ \| & & \uparrow & & \\ Z & \longrightarrow & X \times_G Y & & \\ \| & & \downarrow & & \\ Z & \longrightarrow & Y & \longrightarrow & G. \end{array} \tag{3.49}$$

In our work, we will be concerned with $X \times_G Y = \{(x, y) \in X \times Y | i(x) = j(y)\}$. This is called the subdirect product, and is an important example of a fibre product.

Theorem 3.49. *Let $L/\mathbb{Q}$ be the finite galois extension, with galois group G and with the canonical epimorphism $\phi : G_{\mathbb{Q}} \longrightarrow G$ above. Let $\widetilde{G}$ be a group extension of G by Z_ℓ, and let $\xi \in H^2(G, Z_\ell)$ be the element corresponding to this group extension, as guaranteed by Theorem 2.24. The Embedding Problem for this extension is solvable if and only if $\phi^*(\xi) = 0$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_\ell & \longrightarrow & \widetilde{G} \times_G G_{\mathbb{Q}} & \longrightarrow & G_{\mathbb{Q}} & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Z_\ell & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1, \end{array} \tag{3.50}$$

where $p_1 : \widetilde{G} \times_G G_{\mathbb{Q}} \longrightarrow \widetilde{G}$ and $p_2 : \widetilde{G} \times_G G_{\mathbb{Q}} \longrightarrow G_{\mathbb{Q}}$ are the obvious projection maps, and $\pi : \widetilde{G} \longrightarrow G$ the surjective homomorphism guaranteed because $\widetilde{G}$ is an extension of G by Z_ℓ. For simplicity in the notation, call $\Gamma = \widetilde{G} \times_G G_{\mathbb{Q}}$. Observe that the top row of (3.50) is a group extension (because Z_ℓ is the kernel of p_2) and belongs to the cohomology class of $\phi^*(\xi)$; it splits if and only if $\phi^*(\xi) = 0$ by Corollary 2.25. Suppose the top extension splits. Then there exists a group homomorphism δ such that $p_2 \circ \delta$ is the identity mapping on $G_{\mathbb{Q}}$. Let $\widetilde{\phi} = p_1 \circ \delta$.

Then $\widetilde{\phi}$ is a homomorphism from $G_{\mathbb{Q}}$ to $\widetilde{G}$ such that $\pi \circ \widetilde{\phi} = \phi$ (because the diagram commutes). Thus, $\widetilde{\phi}$ is a lift of ϕ and is surjective because p_1 is. Thus, if $\phi^*(\xi) = 0$ we can solve the embedding problem.

Now suppose we can solve the embedding problem, so we've found a surjective lift $\widetilde{\phi}$ of ϕ. Then we construct $\epsilon : G_{\mathbb{Q}} \longrightarrow \Gamma$ such that for $\gamma \in G_{\mathbb{Q}}$, we have $\epsilon(\gamma) = (\widetilde{\phi}(\gamma), \gamma)$. This is clearly a group homomorphism, since $\epsilon(\gamma_1\gamma_2) = (\widetilde{\phi}(\gamma_1\gamma_2), \gamma_1\gamma_2) = (\widetilde{\phi}(\gamma_1)\widetilde{\phi}(\gamma_2), \gamma_1\gamma_2) = (\widetilde{\phi}(\gamma_1), \gamma_1)(\widetilde{\phi}(\gamma_2), \gamma_2) = \epsilon(\gamma_1)\epsilon(\gamma_2)$, and it splits the top extension in (3.50) (because $p_2 \circ \epsilon$ is the identity on $G_{\mathbb{Q}}$). Therefore, if the embedding problem is solvable, then $\phi^*(\xi) = 0$, completing the proof.

□

Denote $H^2(G_{\mathbb{Q}}, Z_\ell)$ by $H^2(\mathbb{Q}, Z_\ell)$, as is customary in galois cohomology. We may reduce the issue of $\phi^*(\xi) = 0$ to a local question by the following lemma:

Lemma 3.50. *The restriction map*

$$\alpha : H^2(\mathbb{Q}, Z_\ell) \longrightarrow \prod_p H^2(\mathbb{Q}_p, Z_\ell) \tag{3.51}$$

is an injection. Therefore, our embedding problem is solvable if and only if it is solvable for all primes p.

Before proving Lemma 3.50, we show that the embedding problem is solvable locally at all primes. To do that, we will first need to introduce the Frattini subgroup.

Definition 3.51. *The Frattini subgroup Φ of G is the intersection of all maximal subgroups of G.*

Definition 3.52. *Consider the embedding problem as in (3.47). We call such a problem a Frattini Embedding Problem if the kernel of the mapping $\pi : \widetilde{G} \longrightarrow G$ is contained in the Frattini subgroup of $\widetilde{G}$.*

One can very easily check that Φ is normal in G. Also, if a subgroup $G' \subset G$ satisfies $\Phi G' = G$, then $G' = G$. To see this, suppose not. Then take M to be the maximal subgroup of G containing G'. Since $\Phi \subset M$ by definition and $G' \subset M$ by assumption, it follows that $\Phi G' \subset M$, which contradicts the assumption that $\Phi \cdot G' = G$. Therefore, a subset of G generates G if and only if it generates G/Φ. It is this fact that we will need in proving the following theorem:

Theorem 3.53. *Suppose we have a galois extension $L/\mathbb{Q}$ with galois group G, and canonical surjection ϕ as before. Then for every $p \in \mathbb{Q}$, the local embedding problem*

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}_p} & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & Z_\ell & \longrightarrow & \widetilde{G}_p & \longrightarrow & G_p & \longrightarrow & 1, \end{array} \tag{3.52}$$

with induced canonical surjection $\phi_p : G_{\mathbb{Q}_p} \longrightarrow G_p = Gal(L_\wp/\mathbb{Q}_p) \cong D_{\wp/p}$ (for a prime $\wp$ in L over p, as always), is solvable.

Proof. There are two cases to consider: when the prime p ramifies in L and when it is unramified in L. Suppose that p is unramified in L. Then by Proposition 3.47, ϕ_p is trivial on I_p, so ϕ_p factors through $G_{\mathbb{Q}_p}/I_p$. Note that the decomposition groups and inertia groups, D_p and I_p, are only defined up to conjugacy in $G_{\mathbb{Q}}$, and so we implicitly assume throughout that we've fixed a prime v above p so that D_p and I_p are well-defined subgroups of $G_{\mathbb{Q}}$ (and thus of $G_{\mathbb{Q}_p}$; note that $G_{\mathbb{Q}_p} = D_p$). We recall from our work in §3.5 that $G_p \cong D_{\wp/p}$ is a cyclic group generated by the Frobenius element (since p is unramified).

From Theorem 3.33, we know that there is a field $\mathbb{Q}_p^U$ such that $\mathbb{Q}_p \subset \mathbb{Q}_p^U \subset \overline{\mathbb{Q}}_p$ and $\mathbb{Q}_p^U/\mathbb{Q}_p$ is the maximal unramified extension. From Corollary 3.34 and the observation we made following it, we see that $G_{\mathbb{Q}_p}/I_p \cong Gal(\mathbb{Q}_p^U/\mathbb{Q}_p) \cong \hat{\mathbb{Z}}$. So $\phi_p : \hat{\mathbb{Z}} \longrightarrow G_p$, and we want to find a lift $\widetilde{\phi}_p : \hat{\mathbb{Z}} \longrightarrow \widetilde{G}_p$.

By basic properties of ℓ-groups, one easily checks that Z_ℓ is contained in the Frattini subgroup Φ of $\widetilde{G}_p$ (see [DF]), so our embedding problem is actually a Frattini Embedding Problem. Since $Z_\ell \subset \Phi$, we have that $\widetilde{G}_p/Z_\ell \supset \widetilde{G}_p/\Phi$. Observe that $\widetilde{G}_p/Z_\ell \cong G_p$, so $\widetilde{G}_p/\Phi$ is a subgroup of a cyclic group. Therefore, $\widetilde{G}_p/\Phi$ has one generator, which means that $\widetilde{G}_p$ has one generator and is thus cyclic. Therefore, finding a lift $\widetilde{\phi}_p$ is easy, since we can just lift the generator of $\hat{\mathbb{Z}}$ (since it's pro-cyclic). So when the prime p is unramified, we can solve the local embedding problem.

Now suppose the prime p is ramified. We know that $G_p = Gal(L_\wp/\mathbb{Q}_p)$ is an ℓ-group, and since $p \equiv 1 \ (mod\ \ell^N)$, $p \neq \ell$ and so p is tamely ramified. We know that $G_p \cong D_{\wp/p} = I_{\wp/p}$ by the assumption that our ramified primes p satisfies both conditions of (S_N); therefore $f(\wp/p) = 1$ and we know that $\vartheta_{L_\wp}/\wp = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ and $(\vartheta_{L_\wp}/\wp)^\times = (\mathbb{Z}/p\mathbb{Z})^\times$. Let α be the element generating $\wp$ (so $\wp = (\alpha)$), and construct the homomorphism

$$\lambda : G_p \longrightarrow (\vartheta_{L_\wp}/\wp)^\times = (\mathbb{Z}/p\mathbb{Z})^\times \tag{3.53}$$

by the mapping

$$\sigma \longmapsto \overline{\left(\frac{\sigma\alpha}{\alpha}\right)}, \tag{3.54}$$

the residue of $\frac{\sigma\alpha}{\alpha}$ in $\vartheta_{L_\wp}/\wp$. The fact that λ is a homomorphism and the fact that $\frac{\sigma\alpha}{\alpha}$ is a unit are both easy exercises.

So now we want to examine the kernel of the mapping λ. Since the kernel is all elements in G_p mapping to the identity in $(\mathbb{Z}/p\mathbb{Z})^\times$, we see that $ker(\lambda)$ is a p-group (all elements must be killed by p). But G_p is an ℓ-group, where $\ell \neq p$. So $ker(\lambda) = (e)$, where $e \in G_p$ is the identity. Therefore, λ is injective, and G_p can be realized as a subgroup of a cyclic group, and is hence cyclic.

Since G_p injects into $(\mathbb{Z}/p\mathbb{Z})^\times$, we see that ϕ_p factors through the map $G_{\mathbb{Q}_p} \longrightarrow Gal(E/\mathbb{Q}_p)$, where E is the maximal, abelian, tamely ramified extension of Q_p with exponent dividing ℓ^N. The reason is that the mapping:

$$\tau : G_{\mathbb{Q}_p} \longrightarrow Gal(L_\wp/\mathbb{Q}_p) \tag{3.55}$$

has the group $Gal(\overline{\mathbb{Q}}_p/E)$ in the kernel. To see this, we observe that $Gal(\overline{\mathbb{Q}}_p/E)$ has (by assumption on the maximality of E) $gcd(e,p) > 1$. Since p is a prime, this implies that $p|e$ and so the group $Gal(\overline{\mathbb{Q}}_p/E)$ has order mp, for some number m. Therefore, the image under τ is a subgroup of order mp in $Gal(L_\wp/\mathbb{Q}_p)$. But $Gal(L_\wp/\mathbb{Q}_p)$ is an ℓ-group, so every subgroup of a power of the prime ℓ. Therefore, $\tau(Gal(\overline{\mathbb{Q}}_p/E)) = (e)$, proving the claim.

We can construct E explicitly, and therefore construct its galois group explicitly. To construct E, we first take the unique unramified extension U_{ℓ^N} of $\mathbb{Q}_p$ of degree ℓ^N, which we know we may find from our work in §3.3. Since $p \equiv 1 \ (mod\ \ell^N)$, ℓ^N-th root of unity is in $\mathbb{Q}_p$ and we may take the extension $\mathbb{Q}_p(\sqrt[\ell^N]{p})/\mathbb{Q}_p$, which we see is totally ramified and cyclic of order ℓ^N. Then $E = U_{\ell^N}\mathbb{Q}_p(\sqrt[\ell^N]{p})$, the compositum of U_{ℓ^N} and $\mathbb{Q}_p(\sqrt[\ell^N]{p})$. Since p ramifies in $\mathbb{Q}_p(\sqrt[\ell^N]{p})$ and is unramified in U_{ℓ^N}, we know that $\mathbb{Q}_p(\sqrt[\ell^N]{p}) \cap U_{\ell^N} = \mathbb{Q}_p$ and so $Gal(E/\mathbb{Q}_p) \cong (\mathbb{Z}/\ell^N\mathbb{Z}) \oplus (\mathbb{Z}/\ell^N\mathbb{Z})$. It's an easy exercise to see that $(\mathbb{Z}/\ell^N\mathbb{Z}) \oplus (\mathbb{Z}/\ell^N\mathbb{Z})$ is projective in the category of abelian groups of exponent dividing ℓ^N. Therefore, for any diagram

$$\begin{array}{ccccc} & & Gal(E/\mathbb{Q}_p) & & \\ & & \downarrow & & \\ M & \longrightarrow & N & \longrightarrow & 1 \end{array} \tag{3.56}$$

of abelian groups with exponent dividing ℓ^N, we have a lift of the map $Gal(E/\mathbb{Q}_p) \longrightarrow N$ to the map $Gal(E/\mathbb{Q}_p) \longrightarrow M$.

Now consider the inverse image of $G_p = D_{\wp/p}$ in $\widetilde{G}$ (which we've been calling $\widetilde{G}_p$). Since any central extension of a cyclic group is abelian, $\widetilde{G}_p$ is an abelian group with exponent dividing ℓ^N. Therefore, we may take $M = \widetilde{G}_p$ and $N = G_p$ in (3.56). This shows us that we may construct $\widetilde{\phi}_p : G_{\mathbb{Q}_p} \longrightarrow \widetilde{G}_p$ and the local embedding problem is solvable.

□

We will find proving Lemma 3.50 much easier after we've developed some additional results and introduced a new abelian group, called the *Brauer* group.

Definition 3.54. *Let $K/\mathbb{Q}$ be a galois extension, let $\overline{K}$ be the algebraic closure of K, and let $(\overline{K})^*$ be the multiplicative (i.e. non-zero) elements of $\overline{K}$. Then, for our purposes, we may define the Brauer group of K (denoted $Br(K)$) to be $Br(K) = H^2(G_K, (\overline{K})^*) = H^2(K, (\overline{K})^*)$.*

Remark 3.55. *It's important to note that this isn't entirely correct, as $Br(K)$ is only* isomorphic *to $H^2(K, (\overline{K})^*)$ and not equal to it, since elements of $Br(K)$ are isomorphism classes of division algebras over K and $H^2(K, (\overline{K})^*)$ is as we constructed in §2. However, in the work that follows, the distinction is not needed, so we won't bother making it.*

One particularly nice fact about the group $Br(K)$ is that it is an abelian group, which means that, by Theorem 3.3, it has torsion subgroups. We may classify these via the following proposition:

Proposition 3.56. *Let K be a field of characteristic prime to n. Then we have*

$$H^2(K, Z_n) \cong Br_n(K) \tag{3.57}$$

where $Br_n(K)$ denotes the n-torsion of $Br(K)$ and Z_n is the cyclic group of order n generated by ζ_n, the primitive n-th root of unity.

Proof. From the short exact sequence

$$1 \longrightarrow Z_n \longrightarrow (\overline{K})^* \longrightarrow (\overline{K})^* \longrightarrow 1 \tag{3.58}$$

(where the map $(\overline{K})^* \longrightarrow (\overline{K})^*$ above is multiplication by n) we have the following long exact sequence:

$$1 = H^1(K, (\overline{K})^*) \longrightarrow H^2(K, Z_n) \longrightarrow H^2(K, (\overline{K})^*) \longrightarrow H^2(K, (\overline{K})^*), \tag{3.59}$$

where $H^1(K, (\overline{K})^*) = 1$ follows from Hilbert's Theorem 90 (see [Lan]). Since we have that $Br(K) = H^2(K, (\overline{K})^*)$, exactness above implies that $H^2(K, Z_n)$ is exactly the kernel of the mapping $H^2(K, (\overline{K})^*) \longrightarrow H^2(K, (\overline{K})^*)$, which is multiplication by n because it was induced by multiplication by n. This completes the proof.

□

We present (without proof) one final result which we will use in the proof of Lemma 3.50. For the proof, see [Roq].

Theorem 3.57 (Brauer-Hasse-Noether Theorem)**.** *Let K be a field containing the ℓ-th roots of unity, and let $K_\wp$ be the completion of K at the prime $\wp$ as described in §3.3. Then the sequence*

$$0 \longrightarrow Br(K) \longrightarrow \bigoplus_{\wp} Br(K_\wp) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{3.60}$$

is an exact sequence.

Corollary 3.58. *$Br(K)$ injects into $\prod_\wp Br(K_\wp)$.*

Proof. This is clear since $\bigoplus_\wp Br(K_\wp) \subset \prod_\wp Br(K_\wp)$. □

We are now ready to prove Lemma 3.50, using the notions developed above.

Proof of Lemma 3.50. Let ζ_ℓ be a primitive ℓ-th root of unity. Let L be any field, and let $M = L(\zeta_\ell)$. Then we have that $gcd([M : L], \ell) = 1$. Therefore, $H^2(L, Z_\ell) \longrightarrow H^2(M, Z_\ell)$ is injective. The reason is that we have the long exact sequence

$$\cdots \longrightarrow H^1(M, Z_\ell) \longrightarrow H^1(M/L, Z_\ell) \longrightarrow H^2(L, Z_\ell) \longrightarrow H^2(M, Z_\ell) \longrightarrow \cdots \tag{3.61}$$

from galois cohomology. Since $Gal(M/L)$ and Z_ℓ are both finite, we have that $|Gal(M/L)|H^1(M/L, Z_\ell) = 0$ and $|Z_\ell|H^1(M/L, Z_\ell) = 0$. But $gcd(|Gal(M/L)|, |Z_\ell|) = gcd(\ell - 1, \ell) = 1$ so there are $s, t \in \mathbb{Z}$ such that $s|Gal(M/L)| + t|Z_\ell| = 1$. Therefore we have

$$\begin{aligned} H^1(M/L, Z_\ell) &= (s|Gal(M/L)| + t|Z_\ell|)H^1(M/L, Z_\ell) \\ H^1(M/L, Z_\ell) &= s|Gal(M/L)|H^1(M/L, Z_\ell) + t|Z_\ell|H^1(M/L, Z_\ell) \\ H^1(M/L, Z_\ell) &= 0. \end{aligned} \tag{3.62}$$

Therefore, by exactness, $H^2(L, Z_\ell) \longrightarrow H^2(M, Z_\ell)$ is injective.

Now consider the field $\mathbb{Q}$ and ζ_ℓ the primitive ℓ-th root of unity. Let $K = \mathbb{Q}(\zeta_\ell)$. Then $gcd([K : \mathbb{Q}], \ell) = 1$ and so by what we just showed, we know that $H^2(\mathbb{Q}, Z_\ell) \longrightarrow H^2(K, Z_\ell)$ is injective. Similarly, we may consider this technique over local fields $\mathbb{Q}_p$, where p is a prime, so we have the mapping $\prod_p H^2(\mathbb{Q}_p, Z_\ell) \longrightarrow \prod_\wp H^2(K_\wp, Z_\ell)$ is injective; see [MM] for the complete details. So we have the following commutative diagram:

$$\begin{array}{ccc} H^2(K, Z_\ell) & \longrightarrow & \prod_\wp H^2(K_\wp, Z_\ell) \\ \uparrow & & \uparrow \\ H^2(\mathbb{Q}, Z_\ell) & \longrightarrow & \prod_p H^2(\mathbb{Q}_p, Z_\ell) \end{array} \tag{3.63}$$

and the two vertical maps are injective by what we've just shown. By Proposition 3.56, $H^2(K, Z_\ell) = Br_\ell(K) \subset Br(K)$ and $H^2(K_\wp, Z_\ell) = Br_\ell(K_\wp) \subset Br(K_\wp)$. By Theorem 3.57 and Corollary 3.58, the mapping $Br(K) \longrightarrow \prod_\wp Br(K_\wp)$ is injective. Since the homomorphic image of an ℓ-torsion subgroup is an ℓ-torsion subgroup, we have that $Br_\ell(K) \longrightarrow Br_\ell(K_\wp)$ is an injection. Therefore, the top mapping in (3.63) is an injection. Since three of the four mappings are injective, it's an easy exercise to show the fourth must be also, so $H^2(\mathbb{Q}, Z_\ell) \longrightarrow \prod_p H^2(\mathbb{Q}_p, Z_\ell)$ is an injection.

To see that the global embedding problem is solvable if and only if the local embedding problems are all solvable, we recall that Theorem 3.49 tells us the embedding problem is solvable if and only if $\phi^*(\xi) = 0$. Suppose the global embedding problem is solvable. Under the mapping $H^2(\mathbb{Q}, Z_\ell) \longrightarrow \prod_p H^2(\mathbb{Q}_p, Z_\ell)$, we know

that $\phi^*(\xi) \longmapsto \prod_p(\phi^*(\xi_p))$, where $\prod_p(\phi^*(\xi_p))$ is the ordered tuple of local embedding problems $\phi^*(\xi_p)$ for every prime p. Therefore, $0 = \prod_p(\phi^*(\xi_p))$ and so $\phi^*(\xi_p) = 0$ for every prime p, implying the local embedding problem is solvable for all primes.

Now suppose the local embedding problems are solvable for all primes, so $0 = \prod_p(\phi^*(\xi_p))$. Again, we know that $\phi^*(\xi) \longmapsto \prod_p(\phi^*(\xi_p)) = 0$. Since 0 is also mapped to 0, we see that the injectivity of $H^2(\mathbb{Q}, Z_\ell) \longrightarrow \prod_p H^2(\mathbb{Q}_p, Z_\ell)$ implies that $\phi^*(\xi) = 0$ and the global embedding problem is solvable.

□

Since we showed in Theorem 3.53 that the local embedding problems are solvable for every prime, Lemma 3.50 tells us that the global embedding problem is solvable also, giving us our desired $\widetilde{L}$.

3.6.2. *Modifying our solution $\widetilde{L}$ to be ramified at the same places as L.* Our work in §3.6.1 showed that if we have a galois extension $L/\mathbb{Q}$ with galois group G (G an ℓ-group) satisfying property (S_N), then for every central group extension $\widetilde{G}$ of G by Z_ℓ, we can find a galois extension $\widetilde{L}/\mathbb{Q}$ with galois group $\widetilde{G}$. In this section we will show that we are actually able to find such an $\widetilde{L}$ with the added property that $\widetilde{L}$ is ramified at the same places as L. This will prove useful in §3.6.3, when we attempt to find an $\widetilde{L}$ with property (S_N). We begin with the following very important Lemma:

Lemma 3.59. *For every prime p, let ϵ_p be a continuous homomorphism from $G_{\mathbb{Q}_p}$ to a finite abelian group C. Suppose that almost all ϵ_p are unramified. Then there is a unique $\epsilon : G_{\mathbb{Q}} \longrightarrow C$ such that for all p, the maps ϵ and ϵ_p agree on the inertia groups I_p.*

Proof. First note that we call a map ϵ_p *unramified* if the fixed field of $ker(\epsilon_p)$ is an unramified extension of $\mathbb{Q}_p$. This is equivalent to saying that $\epsilon_p(I_p) = 1$. Also notice that if we take a cyclotomic extension of $\mathbb{Q}$ by ζ_m, the m-th root of unity, and consider a galois character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow C$, then we induce a map $\epsilon : G_{\mathbb{Q}} \longrightarrow C$ by composing χ with the restriction map $res_{\mathbb{Q}(\zeta_m)}$. We will use this fact later in the proof.

From class field theory, we have a continuous homomorphism $r_p : Q_p^* \longrightarrow G_{\mathbb{Q}_p}^{ab}$ that we call the reciprocity map. It turns out that r_p is injective and *almost* surjective (meaning $im(r_p)$ is dense). Here $\mathbb{Q}_p^*$ is the group of units in Q_p. For ease of notation, we call $G_{\mathbb{Q}_p}^{ab} = \widetilde{G}_{\mathbb{Q}_p}$, where $\widetilde{G}_{\mathbb{Q}_p} = Gal(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ and $\mathbb{Q}_p^{ab}$ the maximal abelian extension of $\mathbb{Q}_p$. Since $\hat{\mathbb{Z}}$ is abelian, $\mathbb{Q}_p \subset \mathbb{Q}_p^U \subset \mathbb{Q}_p^{ab}$ and we call $Gal(\mathbb{Q}_p^{ab}/\mathbb{Q}_p^U) = \widetilde{I}_p$. We want to see what the inverse image of $\widetilde{I}_p$ under the mapping r_p is. It turns out that r_p maps $\mathbb{Z}_p^*$ isomorphically on to $\widetilde{I}_p$ (for a proof of this fact, see [Tat]), where $\mathbb{Z}_p^*$ are the units in the p-adic integers. Now take $\alpha \in \mathbb{Q}_p^*$. This means $\alpha = p^\ell u$, where $u \in \mathbb{Z}_p^*$. So $\mathbb{Q}_p^* = \mathbb{Z}_p^* \times < p > \cong \mathbb{Z}_p^* \times \mathbb{Z}$. One nice fact about the reciprocity map is that $r_p(p)|_{\mathbb{Q}_p^U}$ is a topological generator for $\phi_p^{\hat{\mathbb{Z}}}$, where ϕ_p is the Frobenius map; therefore $r_p(p)|_{\mathbb{Q}_p^U} = \phi_p$. For a deeper discussion of the reciprocity map, see [Ser1] and [Tat].

We know from Corollary 3.34 that $\mathbb{Q}_p^U = \mathbb{Q}_p(\zeta_m,\ (p,m) = 1)$. One can also show that the field $K = \mathbb{Q}_p(\zeta_{p^n},\ n = 1, 2, 3, ...)$ is a subfield of $\mathbb{Q}_p^{ab}$, $Gal(K/\mathbb{Q}_p) \cong Gal(\mathbb{Q}_p^{ab}/\mathbb{Q}_p^U) = \widetilde{I}_p$, and $\mathbb{Q}_p^{ab} = \mathbb{Q}_p^U K$ (for proofs of all these facts, see [Ser1]). So we would like to know how the element $r_p(\alpha) \in \widetilde{G}_{\mathbb{Q}_p}$ acts on ζ_m (where $(p,m) = 1$) and on ζ_{p^n} for all n. One can show that if $\alpha = p^\ell u$, then $r_p(\alpha)(\zeta_m) = \zeta_m^{p^\ell}$ and

$r_p(\alpha)(\zeta_{p^n}) = \zeta_{p^n}^{(u^{-1})}$ (see [Ser1]). We will use all these facts from class field theory in our proof.

We may now canonically identify $\epsilon_p : G_{\mathbb{Q}_p} \longrightarrow C$ with the map $\epsilon_p' : \mathbb{Q}_p^* \longrightarrow C$, by composing with the reciprocity map:

$$\mathbb{Q}_p^* \longrightarrow \widetilde{G}_{\mathbb{Q}_p} \longrightarrow C. \tag{3.64}$$

We may construct ϵ_p' in this way because $[G_{\mathbb{Q}_p}, G_{\mathbb{Q}_p}] \subset ker(\epsilon_p)$ (target of ϵ_p is abelian) so ϵ_p factors through the map $\widetilde{G}_{\mathbb{Q}_p} \longrightarrow C$. Since ϵ_p and r_p are continuous, so is ϵ_p'. Furthermore, using the discrete topology, one sees that $\{e\} \in C$ is an open subgroup, so $ker(\epsilon_p')|_{\mathbb{Z}_p^*}$ is an open subgroup of $\mathbb{Z}_p^*$. But we also know we have a sequence of open subgroups $\mathbb{Z}_p^* \supset U_p^{(1)} \supset U_p^{(2)} \supset U_p^{(3)} \supset \cdots$, where

$$U_p^{(k)} = \{u \in \mathbb{Z}_p^* \,|u \equiv\ 1\ (mod p^k)\}, \tag{3.65}$$

as proven in [Ser1]. By definition, $U_p^{(k)} = 1 + (p\mathbb{Z}_p)^k = 1 + p^k\mathbb{Z}_p$. Let m_p be the smallest k such that $U_p^{(m_p)} \subset ker(\epsilon_p')|_{\mathbb{Z}_p^*}$; we call this m_p the *conductor* of the mapping ϵ_p'. Notice that if p is unramified, then $ker(\epsilon_p')|_{\mathbb{Z}_p^*} = \mathbb{Z}_p^*$ and $m_p = 0$. So only finitely many primes have a nonzero conductor m_p.

Construct the mapping $\epsilon' : \prod_p \mathbb{Z}_p^* \longrightarrow C$ by $\epsilon'(\prod_p u_p) = \prod_p \epsilon_p'(u_p)$. This is a finite product since $\epsilon_p'(u_p) = 1$ for all unramified primes p. Let $p_1, ..., p_N$ be the ramified primes. Then we may redefine $\epsilon' : \prod_{i=1}^N \mathbb{Z}_{p_i}^* \longrightarrow C$. By definition of the conductor m_p, we know that ϵ' vanishes on $\prod_{i=1}^N (1 + p_i^{m_i}\mathbb{Z}_{p_i}^*)$, so ϵ' factors through the map

$$\chi : \prod_{i=1}^N \mathbb{Z}_{p_i}^*/(1 + p_i^{m_i}\mathbb{Z}_{p_i}^*) \longrightarrow C. \tag{3.66}$$

Since $\mathbb{Z}_{p_i}^*/(1 + p_i^{m_i}\mathbb{Z}_{p_i}^*) \cong (\mathbb{Z}_{p_i}/p_i^{m_i}\mathbb{Z}_{p_i})^\times \cong (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times$, this gives us the map

$$\chi : \prod_{i=1}^N (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times \longrightarrow C. \tag{3.67}$$

Define $M = \prod_{i=1}^N p_i^{m_i}$. Then the Chinese Remainder Theorem tells us that $(\mathbb{Z}/M\mathbb{Z})^\times \cong \prod_{i=1}^N (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times$. Therefore, we have the mapping $\chi : (\mathbb{Z}/M\mathbb{Z})^\times \longrightarrow C$. Viewing χ as a galois character, we induce a map $\epsilon : G_{\mathbb{Q}_p} \longrightarrow C$ by the remark made at the beginning of the proof. This is what we wanted to show.

□

Using Lemma 3.59, we now prove the following proposition, which allows us to modify liftings to satisfy our desired properties. Using this proposition, and the corollary that follows it, we may modify our solution $\widetilde{L}$ to have the same ramified places as L.

Proposition 3.60. *Let $1 \longrightarrow C \longrightarrow \widetilde{\Omega} \longrightarrow \Omega \longrightarrow 1$ be a central extension of a group Ω, and let $\phi : G_{\mathbb{Q}} \longrightarrow \Omega$ be a continuous homomorphism which has a lifting $\psi : G_{\mathbb{Q}} \longrightarrow \widetilde{\Omega}$. Let $\widetilde{\phi}_p : G_{\mathbb{Q}_p} \longrightarrow \widetilde{\Omega}$ be liftings of $\phi_p = \phi|_{D_p}$ such that the $\widetilde{\phi}_p$ are unramified for almost all p. Then there is a lifting $\widetilde{\phi} : G_{\mathbb{Q}} \longrightarrow \widetilde{\Omega}$ such that, for every prime p, $\widetilde{\phi}$ is equal to $\widetilde{\phi}_p$ on the inertia group I_p.*

Proof. Let $\pi : \widetilde{\Omega} \longrightarrow \Omega$ be the surjective homomorphism associated to this embedding problem. Localizing the global embedding problem at p by restricting ϕ to D_p gives us ϕ_p. We may do the same thing to the lift ψ, and ψ is then a lift of ϕ_p. Let

$\widetilde{\phi}_p$ be another lift, unramified for almost all p. So we have two lifts of the same mapping, which means that for $s_p \in G_{\mathbb{Q}_p}$, we have $\pi(\widetilde{\phi}_p(s_p)) = \pi(\psi(s_p))$. This means $(\widetilde{\phi}_p(s_p))^{-1}\psi(s_p) \in ker(\pi) = C$. This gives us a unique mapping $\epsilon_p : G_{\mathbb{Q}_p} \longrightarrow C$ such that $\epsilon_p(s_p) = (\widetilde{\phi}_p(s_p))^{-1}\psi(s_p)$, or $\psi(s_p) = \epsilon_p(s_p)\widetilde{\phi}_p(s_p)$. Since C is abelian and both ψ and $\widetilde{\phi}_p$ are homomorphisms, that forces ϵ_p to be a homomorphism also. Then by Lemma 3.59, there exists a unique $\epsilon : G_{\mathbb{Q}} \longrightarrow C$ such that ϵ agree with ϵ_p on I_p. Now consider the homomorphism $\widetilde{\phi} = \psi\epsilon^{-1}$, where $\epsilon^{-1}(s) = (\epsilon(s))^{-1}$, the inverse of the element $\epsilon(s) \in C$. This clearly agrees with $\widetilde{\phi}_p$ on I_p since ψ agrees with itself everywhere and ϵ agrees with ϵ_p on I_p. This completes the proof.

□

Corollary 3.61. *Under the assumptions of Proposition 3.60, a lifting of ϕ can be chosen to be unramified at every prime where ϕ is unramified.*

Proof. Choose local liftings $\widetilde{\phi}_p$ of ϕ that are unramified where ϕ is. We saw in §3.6.1 that this is possible, since we simply lift the generator of $\hat{\mathbb{Z}}$. Then Proposition 3.60 tells us that we may find a lift $\widetilde{\phi}$ such that $\widetilde{\phi}$ and $\widetilde{\phi}_p$ agree on I_p. Since ϕ_p is unramified at p if and only if $\phi_p(I_p) = 1$, and $\widetilde{\phi}_p$ is a lift of ϕ_p also unramified at p, then $\widetilde{\phi}_p(I_p) = 1$, and again this is true if and only if p is unramified. But $\widetilde{\phi}(I_p) = \widetilde{\phi}_p(I_p) = 1$ if and only if p is unramified, which means $\widetilde{\phi}$ is unramified where ϕ is, completing the proof.

□

So because we showed in §3.6.1 that we can find a lift of ϕ in (3.47), we may apply Corollary 3.61 and construct a lift $\widetilde{\phi}$ unramified at the same places as ϕ, which allows us to construct an $\widetilde{L}$ that is ramified at the same places as L.

3.6.3. *Modifying our solution $\widetilde{L}$ to have property (S_N).* From our work in §3.6.1 and §3.6.2, we now have a solution $\widetilde{L}$ to the embedding problem for $\widetilde{G}$ which is ramified at the same places as L. Let p be such a ramified prime. Then we have D_p and I_p (the decomposition and inertia groups for L at p) and $\widetilde{D}_p$ and $\widetilde{I}_p$ (the decomposition and inertia groups for $\widetilde{L}$ at p). Since L has property (S_N), we know that $I_p = D_p \subset G$ is a cyclic subgroup of order ℓ^α say (we know it must be some power of ℓ since G is an ℓ-group, and we call that power α; they are cyclic because $p \neq \ell$ means p is tamely ramified). Let I'_p be the pre-image of I_p in $\widetilde{G}$. Then Proposition 3.47 tells us that $\widetilde{I}_p \subset I'_p$. Similarly, Proposition 3.47 tells us that $\widetilde{D}_p \subset D'_p$, where D'_p is the inverse image of D_p. But because $D_p = I_p$, $D'_p = I'_p$ so $\widetilde{D}_p \subset I'_p$. Since $\widetilde{I}_p \subset \widetilde{D}_p$ by general principles, we have that $\widetilde{I}_p \subset \widetilde{D}_p \subset I'_p$.

We may consider the group extension problem with I_p in the following way:

$$1 \longrightarrow Z_\ell \longrightarrow I'_p \longrightarrow I_p \longrightarrow 1. \tag{3.68}$$

Since I_p is cyclic of order ℓ^α, that means that I'_p is an abelian group (just as before, a central extension of a cyclic group is abelian) of order $\ell^{\alpha+1}$. Since the homomorphic image is cyclic of order ℓ^α, Theorem 3.3 tells us that either $I'_p = Z_{\ell^{\alpha+1}}$ or $I'_p = Z_{\ell^\alpha} \times Z_\ell$. Proposition 3.47 tells us $\widetilde{I}_p$ is a subgroup of I'_p mapping onto I_p via the homomorphism $\pi : I'_p \longrightarrow I_p$. We see this by restricting (3.68) to:

$$1 \longrightarrow Z_\ell \cap \widetilde{I}_p \longrightarrow \widetilde{I}_p \longrightarrow I_p \longrightarrow 1 \tag{3.69}$$

If $Z_\ell \cap \widetilde{I}_p = 1$, then $|\widetilde{I}_p| = \ell^\alpha$ and $\widetilde{I}_p \cong I_p$. If $Z_\ell \cap \widetilde{I}_p = Z_\ell$ (the only other possibility since ℓ is prime and $\widetilde{I}_p$ has order a power of ℓ), then $|\widetilde{I}_p| = \ell^{\alpha+1}$. If we have

$|\widetilde{I}_p| = \ell^{\alpha+1}$, then $\widetilde{I}_p = I'_p$ (forcing I'_p to not split) and since $\widetilde{I}_p \subset \widetilde{D}_p \subset I'_p$, we are forced to have $\widetilde{I}_p = \widetilde{D}_p$, and property (S_N) is satisfied at the prime p.

On the other hand, if $|\widetilde{I}_p| = \ell^{\alpha}$, then $I_p \cong \widetilde{I}_p \subset I'_p$. We want to look at $\pi(Z_\ell \times \widetilde{I}_p)$. Since $Z_\ell = ker(\pi)$ and $\widetilde{I}_p \subset I'_p$, we have that $\pi(Z_\ell \times \widetilde{I}_p) \subset I_p$. Therefore, $Z_\ell \times \widetilde{I}_p \subset I'_p$. But $|I'_p| = \ell^{\alpha+1}$ and $|Z_\ell \times \widetilde{I}_p| = \ell^{\alpha+1}$ also; therefore, $I'_p \cong Z_\ell \times \widetilde{I}_p \cong Z_\ell \times I_p$ and I'_p is a split extension of I_p by Z_ℓ.

Let S be the set of all primes ramified in $L/\mathbb{Q}$ such that I'_p is a split extension of I_p, so $I'_p \cong \widetilde{I}_p \times Z_\ell$. Since $\widetilde{D}_p \subset I'_p$, we have that $\widetilde{D}_p/\widetilde{I}_p \subset I'_p/\widetilde{I}_p \cong Z_\ell$. From our work in §3.5, we know $\widetilde{D}_p/\widetilde{I}_p$ is cyclic and generated by the Frobenius map σ_p; therefore σ_p may be identified with an element $c_p \in Z_\ell$ by the above inclusion. If $c_p = 1$, then $\widetilde{D}_p = \widetilde{I}_p$ and property (S_N) is satisfied at p. If $c_p = 1$ for all ramified primes p in $\widetilde{L}/\mathbb{Q}$, then $\widetilde{L}$ satisfies property (S_N). If not, we must modify $\widetilde{L}$. Call S the set of all primes ramified in L that have $c_p \neq 1$.

To make our modification, we first construct a galois character $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow Z_\ell$ with the following properties:

1.) $q \equiv 1 \ (mod\ \ell^N)$.

2.) For every $p \in S$, $\chi(p) = c_p$, the element identified with the frobenius element.

3.) The prime q splits completely in the extension $L/\mathbb{Q}$.

By a similar logic to the one presented in §3.5, we will show these three conditions will impose conditions on the behavior of q in the fields $\mathbb{Q}(\zeta_{\ell^N})$, $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$, and L respectively. We may rewrite $\mathbb{Q}(\zeta_{\ell^N})$ as $\mathbb{Q}(\zeta_\ell)F$, where F is cyclic of order ℓ^{N-1} and totally ramified at ℓ. The reason is that $Gal(\mathbb{Q}(\zeta_{\ell^N})/\mathbb{Q}) \cong (\mathbb{Z}/\ell^N\mathbb{Z})^\times$ is a cyclic group of order $\ell^{N-1}(\ell-1)$, so there is a subgroup of order $\ell - 1$, and by Theorem 1.1, there is such a field F. We know that $F \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$ since $[F \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = gcd([F : \mathbb{Q}], [\mathbb{Q}(\zeta_\ell) : \mathbb{Q}]) = 1$. Furthermore, ℓ is totally ramified in F since it is totally ramified in $\mathbb{Q}(\zeta_{\ell^N})$.

We will now discuss the behavior of q in each of these fields. To do that, we will need the following lemma:

Lemma 3.62. *The fields F, L, and $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$ are linearly disjoint over $\mathbb{Q}$.*

Proof. Since F and L have distinct ramification (ℓ is totally ramified in F and unramified in L), they must be linearly disjoint over $\mathbb{Q}$. Therefore, $Gal(LF/\mathbb{Q}) \cong G \times Z_{\ell^{N-1}}$. We know from the theory of Kummer Extensions (see [Bir]) that $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p})/\mathbb{Q}(\zeta_\ell)$ has galois group Z_ℓ. For $p_1 \neq p_2$ (where $p_1, p_2 \in S$), then Proposition 3.43 tells us that p_2 is unramified in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_1})$ and that p_1 is unramified in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_2})$. By Proposition 3.44, p_1 is totally ramified in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_1})$ and that p_2 is totally ramified in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_2})$. Therefore the fields $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_1})$ and $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_2})$ have distinct ramification and must be linearly disjoint over $\mathbb{Q}(\zeta_\ell)$. Then $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$ is the compositum of such fields and

$$Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q}(\zeta_\ell)) \cong Z_\ell \times Z_\ell \times \cdots \times Z_\ell \quad (|S| times), \tag{3.70}$$

which we may shorten to $Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q}(\zeta_\ell)) \cong Z_\ell^s$, where $s = |S|$, the cardinality of S. Because $\ell \neq 2$, we know that $\zeta_\ell \notin \mathbb{Q}$, and so $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ is galois with $Gal(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \cong Z_{\ell-1}$; therefore, Z_ℓ^s is normal in $Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q})$. Furthermore, $Z_\ell^s \cap Z_{\ell-1} = 1$ since the groups have different orders. Therefore, $Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q}) \cong Z_\ell^s \rtimes Z_{\ell-1}$.

We want to see how conjugation acts on Z_ℓ^s. Let $H = Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q})$. Recall that $\sigma_a \in Gal(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ is the automorphism such that $\sigma_a(\zeta_\ell) = \zeta_\ell^a$. We know that, for ℓ prime, there is always such a mapping for every a (easy exercise). Because the restriction of $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$ to $\mathbb{Q}(\zeta_\ell)$ is surjective, there is a $\sigma \in H$ such that $\sigma|_{\mathbb{Q}(\zeta_\ell)} = \sigma_a$. Take such a σ. Now recall that $Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in$

$S)/\mathbb{Q}(\sqrt[\ell]{p}, p \in S)) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \cong Z_{\ell-1}$, also a galois extension. So there is a $\rho_b \in H$ (with $b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$) such that $\rho_b(\zeta_\ell) = \zeta_\ell^b$ and $\rho_b(\sqrt[\ell]{p}) = \sqrt[\ell]{p}$ for all $p \in S$. Notice that $\sigma\rho_b^{-1} \in Z_\ell^s$, so we have $\sigma \in \rho_b Z_\ell^s$; therefore $H =< \rho_b; b \in (\mathbb{Z}/\ell\mathbb{Z})^\times > Z_\ell^s$. Now notice that $\rho_b\tau\rho_b^{-1}$ (for $\tau \in Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q}(\zeta_\ell))$) has the following action:

$$\begin{aligned} \rho_b\tau\rho_b^{-1}(\zeta_\ell^j \sqrt[\ell]{p}) &= \rho_b\tau(\zeta_\ell^{b^{-1}j} \sqrt[\ell]{p}) \\ &= \rho_b(\zeta_\ell^{b^{-1}j}\zeta_\ell' \sqrt[\ell]{p}) \\ &= (\zeta_\ell')^b(\zeta_\ell^j \sqrt[\ell]{p}) \end{aligned} \tag{3.71}$$

So $\rho_b\tau\rho_b^{-1}$ is just multiplication by b in Z_ℓ^s. Therefore, $Gal(\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q}) \cong Z_\ell^s \rtimes Z_{\ell-1}$, with multiplication law $(v,a)(v',a') = (v + av', aa')$ and inverse $(v,a)^{-1} = (-a^{-1}v, a^{-1})$.

But this group has no quotient of order ℓ. To see this, observe that because ℓ is prime, a field of degree ℓ would be an abelian extension (with galois group cyclic of order ℓ). We will show that the largest abelian subgroup of H is of order $\ell - 1$. Recall that the commutator subgroup $[H,H]$ is a normal subgroup with the property that $H/[H,H]$ is the largest abelian subgroup of H. $[H,H]$ is generated by

$$\begin{aligned} (v,a)(v',a')(v,a)^{-1}(v',a')^{-1} &= (v + av', aa')(-a^{-1}v, a^{-1})(-a'^{-1}v', a'^{-1}) \\ &= (v, a')(-a'^{-1}v', a'^{-1}) \\ &= (v - v', 1); \end{aligned} \tag{3.72}$$

therefore $[H,H] \cong Z_\ell^s \rtimes 1 \cong Z_\ell^s$. This means that $H/[H,H] \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$, which is of order $\ell - 1$.

Since LF does have a subfield of degree ℓ over $\mathbb{Q}$, and ℓ is prime, these two fields are linearly disjoint, implying that L, F, and $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$ are all linearly disjoint.

□

Before moving any further, we state a very important result from algebraic number theory that we will use momentarily; for a discussion of this theorem, see [Len].

Theorem 3.63 (The Chebotarev Density Theorem)**.** *Let $K \subset L$ by a galois extension, and let $C \subset G = Gal(L/K)$ be a conjugacy class. Then*

$$\{\wp \mid \wp \in K \text{ prime}, \wp \not| D_{L/K}, \sigma_\wp \in C\} \tag{3.73}$$

has density $\frac{|C|}{|G|}$. In particular, this number is always greater than 0, so there always exist such primes.

For convenience, we will now write $S = \{p_1, ...p_k\}$. Notice that since $c_{p_i} \neq 1$, it must be an element of order ℓ; they are all generators of Z_ℓ. So we may define integers $\nu_2, ..., \nu_k$ such that $c_{p_i} = c_{p_1}^{\nu_i}$.

Now we want to look at the behavior of q in each of these fields. By construction, q splits completely in L, which means that $\sigma_q = 1$ in L. Also, since $q \equiv 1 \ (mod\ \ell^N)$, Proposition 3.41 tells us that $f = 1$, which means that $\sigma_q = 1$ in $\mathbb{Q}(\zeta_{\ell^N})$. Since F is a subfield of $\mathbb{Q}(\zeta_{\ell^N})$ over $\mathbb{Q}$, Proposition 3.21 implies $\sigma_q = 1$ in F as well. Since $\sigma_q = 1$ in both L and F, Proposition 3.40 implies that $\sigma_q = 1$ in LF also.

Now recall that $\sigma_q(\sqrt[\ell]{p}) \equiv (\sqrt[\ell]{p})^q \ (mod\ v)$, where v is a prime over q. But $(\sqrt[\ell]{p})^q = (\sqrt[\ell]{p})^{q-1}(\sqrt[\ell]{p}) = p^{\frac{q-1}{\ell}}(\sqrt[\ell]{p})$; therefore $\sigma_q(\sqrt[\ell]{p}) \equiv p^{\frac{q-1}{\ell}}(\sqrt[\ell]{p}) \ (mod\ v)$. So $c_p \equiv p^{\frac{q-1}{\ell}} \ (mod\ v)$, the ℓ-th root of unity satisfying our congruence for $\sigma_q(\sqrt[\ell]{p})$. Since $c_{p_1} \neq 1$ by assumption, $\sigma_q(\sqrt[\ell]{p_1}) \not\equiv \sqrt[\ell]{p_1} \ (mod\ v)$ and $\sigma_q \neq 1$ in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p_1})$. However,

consider σ_q in the field $\mathbb{Q}(\zeta_\ell, \frac{\sqrt[\ell]{p_i}}{\sqrt[\ell]{p_1^{\nu_i}}})$. This gives us $\sigma_q(\frac{\sqrt[\ell]{p_i}}{\sqrt[\ell]{p_1^{\nu_i}}}) \equiv (\frac{c_{p_i}}{c_{p_1}^{\nu_i}})(\frac{\sqrt[\ell]{p_i}}{\sqrt[\ell]{p_1^{\nu_i}}})\ (mod\ v)$. But we constructed ν_i so that $c_{p_1}^{\nu_i} = c_{p_i}$, meaning $\frac{c_{p_i}}{c_{p_1}^{\nu_i}} = 1$. So $\sigma_q = 1$ in the field $\mathbb{Q}(\zeta_\ell, \frac{\sqrt[\ell]{p_i}}{\sqrt[\ell]{p_1^{\nu_i}}})$.

Using Lemma 3.62, it is enough to consider the behavior of q in the field $LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)$ over $\mathbb{Q}$. We've identified all the behavior that we'll need in our work above (in a moment we'll see why), which defines a conjugacy class in $Gal(LF\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p}, p \in S)/\mathbb{Q})$. Since q is constructed to be prime in $\mathbb{Q}$ unramified in this extension, Theorem 3.63 says that such a prime q always exists.

Now construct the galois character $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow Z_\ell$ by $\chi(a) = a^{\frac{q-1}{\ell}}$. Then $\chi(p_i) = p_i^{\frac{q-1}{\ell}} = c_{p_i}$, as needed. Let $\widetilde{\phi}$ be the solution to the embedding problem that we found in §3.6.2. Then $\widetilde{\psi} = \widetilde{\phi}\chi^{-1}$ is a solution to the embedding problem that satisfies property (S_N) for all primes that ramify in L. However, now our solution field has one additional ramified prime, namely the prime q. We must show that q satisfies property (S_N) as well. The first condition is true by construction of q. Since q was not ramified in the solution found by the lift $\widetilde{\phi}$, we know that $\widetilde{\phi}(D_q) = 1$. Therefore, $\widetilde{\psi}(D_q) \subset Z_\ell$. But because $q \equiv 1\ (mod\ \ell^N)$, the restriction forces $\widetilde{\psi}(I_q) = Z_\ell$. This forces $D_q = I_q$, and q satisfies property (S_N) as well.

This completes the proof of Theorem 3.39, which in turn completes the proof of Theorem 3.36, the main theorem of this paper.

4. An Exploration of more General Groups

We conclude this paper by discussing some additional results in the subject of Inverse Galois Theory. In §4.1, we present (with minimal proof) the great theorem of Shafarevich that the Inverse Galois Problem has a solution whenever the group in question is a solvable group. This is still one of the biggest results in Number Theory to date. Then, in §4.2, we use techniques of elementary galois theory to solve the Inverse Galois Problem for the (generally) non-solvable group S_n. Solving the Inverse Galois Problem tends to be extremely difficult for groups with very general structure, but as it turns out it's relatively easy for S_n so we present the solution here. This demonstrates a relatively easy, constructive approach to solving the inverse galois problem. Finally, in §4.3, we discuss the Theorem of Hilbert and give an alternate (albeit more difficult) method of solving the Inverse Galois Problem for the group S_n.

4.1. Shafarevich's Theorem for General Solvable Groups.

Here we present the main result of Shafarevich, showing that the Inverse Galois Problem has a solution for every solvable group. We will present much of the work in this section without proof. Many of these results can be found in [Ser2]. We recall the definition of the Frattini subgroup (Definition 3.51), and prove some important results tied to it.

Proposition 4.1. *Let G be a finite group, Φ its Frattini subgroup, and N a normal subgroup of G with $\Phi \subset N \subset G$. Assume that the quotient group N/Φ is nilpotent. Then N is nilpotent.*

Proof. Recall from §3.4 that a finite group G is nilpotent if and only if it has one Sylow p-subgroup for every p dividing the order of G. Suppose p divides the order of N, and let $P \subset N$ be the corresponding Sylow p-subgroup of N. Let $Q = \Phi P$ be the product group of Φ and P, and consider the quotient map $N \longrightarrow N/\Phi$. We are particularly interested in the image of Q under this map. One can see that the image of Q under this map will be a Sylow p-subgroup of N/Φ, which will be unique because N/Φ is assumed to be nilpotent. This means that the image of Q will be fixed by conjugation of elements in G.

Let $N_G(P)$ be the normalizer of P in G. Since $P \subset Q$, then if $g \in G$, the group gPg^{-1} is a Sylow p-subgroup of Q. Thus, by the Sylow Theorems (applied to the group Q), there is a $q \in Q$ such that $qgPg^{-1}q^{-1} = P$; therefore we have $qg \in N_G(P)$. This means that $G = QN_G(P) = \Phi N_G(P)$, or that $G = N_G(P)$, and P is normal in G. As a result, P is normal in N and since all Sylow p-subgroups are conjugate, this implies that P is the only Sylow p-subgroup in N, or that N is nilpotent.

□

Corollary 4.2. *The Frattini subgroup Φ is nilpotent.*

Proof. Apply Proposition 4.1 in the case $N = \Phi$.

□

We will now use Proposition 4.1 and Corollary 4.2 to explore solvable groups and their corresponding relevance to galois theory. This will involve us presenting (without proof) a big lemma due to Shafarevich; in fact this lemma is the major backbone in the proof that we can solve the Inverse Galois Problem whenever our given group is solvable. We begin with the following proposition:

Proposition 4.3. *Let G be a finite solvable group $\neq \{e\}$. Then G is isomorphic to a quotient of a group H which is the semi-direct product $U \rtimes S$, where U is a normal nilpotent subgroup of H and S is solvable with $|S| < |G|$.*

Proof. Let Φ be the Frattini subgroup of G. Since G is solvable and Φ is solvable, we know that G/Φ is solvable and $\neq \{e\}$. Therefore, G/Φ contains a non-trivial abelian normal subgroup (namely the last non-trivial term in the descending derived series of G/Φ). Let U be the inverse image of this group under the quotient map $G \longrightarrow G/\Phi$, so U is a subgroup of G and it satisfies $\Phi \subset U \subset G$ (since its image under the quotient map is assumed to be non-trivial). Since we're assuming that U/Φ is abelian, Proposition 4.1 tells us that U is nilpotent.

Now choose a maximal subgroup S of G (S solvable) that does not contain U. Such an S clearly exists since $\Phi \subset U$ and $U/\Phi \neq \{e\}$ implies that $\Phi \neq U$. Since (as a result of what we just showed) $U \rtimes S \neq S$ and S is maximal, we have that $G = U \rtimes S$. Therefore, if we take $H = U \rtimes S$ where S acts by conjugation on the normal subgroup U, there is a surjective map $H \longrightarrow G$. The First Isomorphism Theorem gives the desired result.

□

As a result of Proposition 4.3, Shafarevich was able to prove the following major lemma, which we present without proof (for a proof of a slightly more general version of this lemma, see [SW]).

Lemma 4.4. *Let L/K be a galois extension of number fields with galois group S, let U be a nilpotent group with S-action, and let H be the semi-direct product $U \rtimes S$. Then the embedding problem has a solution $\widetilde{L}$ such that $Gal(\widetilde{L}/K) \cong H$, $Gal(\widetilde{L}/L) \cong U$, and the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U & \longrightarrow & H & \longrightarrow & S & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Gal(\widetilde{L}/L) & \longrightarrow & Gal(\widetilde{L}/K) & \longrightarrow & Gal(L/K) & \longrightarrow & 1 \end{array} \tag{4.1}$$

is commutative.

With Lemma 4.4 in place, we can now prove that the Inverse Galois Problem has a solution whenever G is solvable.

Theorem 4.5 (Inverse Galois Problem for Solvable Groups)**.** *Given any finite, solvable group G, there exists a galois extension $K/\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong G$.*

Proof. Suppose that $G \neq \{e\}$ is a solvable group of finite order. We will proceed by induction on the order of G. By Proposition 4.3, we may write G as the quotient of $U \rtimes S$ with U nilpotent and S solvable with $|S| < |G|$. By our induction hypothesis, there is a galois extension $L/\mathbb{Q}$ such that $Gal(L/\mathbb{Q}) \cong S$. Thus, Lemma 4.4 tells us that there is a galois extension $\widetilde{L}/\mathbb{Q}$ such that $Gal(\widetilde{L}/\mathbb{Q}) \cong U \rtimes S$. Since G is the quotient of $U \rtimes S$ and the kernel of the surjective mapping $U \rtimes S \longrightarrow G$ (which must be a normal subgroup by elementary group theory), Theorem 1.1 says such a K exists and basic galois theory says that $K/\mathbb{Q}$ is galois with $Gal(K/\mathbb{Q}) \cong G$, solving the Inverse Galois Problem for G.

□

4.2. **A Number Field Extension with Galois Group S_n.** In this section we illustrate a technique that allows one to calculate the galois group for a galois extension $K/\mathbb{Q}$, where K is the splitting field of a given polynomial $f(x) \in \mathbb{Q}[x]$. Doing so allows us to construct polynomials whose splitting field over $\mathbb{Q}$ has galois group S_n, for any $n \in \mathbb{Z}^+$, exhibiting an elementary solution to the Inverse Galois Problem for the group S_n. This technique may be explored at greater lengths in [DF].

Consider $f(x) \in \mathbb{Q}[x]$. In determining the galois group of $f(x)$ (that is to say, the galois group of the galois extension $K/\mathbb{Q}$, where K is the splitting field for $f(x)$), we may assume that $f(x)$ is separable and has integer coefficients. Then we may calculate the discriminant D of $f(x)$ as described in §3.2, and in particular $D \in \mathbb{Z},\ D \neq 0$.

For any prime p, we may consider the reduction $\overline{f}(x) \in \mathbb{F}_p[x]$ of the polynomial $f(x)$ in the obvious way. If p divides D, then $\overline{f}(x)$ has discriminant $\overline{D} = 0$ in $\mathbb{F}_p$ and so the polynomial is no longer separable in the reduction. However, if p does not divide D, then $\overline{f}(x)$ is a separable polynomial over $\mathbb{F}_p$ and we may factor $\overline{f}(x)$ into distinct irreducible polynomials

$$\overline{f}(x) = \overline{f}_1(x)\overline{f}_2(x)\cdots\overline{f}_k(x) \quad \text{in } \mathbb{F}_p[x] \tag{4.2}$$

where each $\overline{f}_i(x)$ is an irreducible polynomial of degree n_i. This formulation gives us the following theorem from algebraic number theory, which we present without proof:

Theorem 4.6. *For any prime p not dividing the discriminant D of $f(x)$, the galois group of $\overline{f}(x)$ over $\mathbb{F}_p$ is a permutation group isomorphic to a subgroup of the galois group of $f(x)$ over $\mathbb{Q}$.*

The meaning of the statement is that not only is the galois group of $\overline{f}(x)$ over $\mathbb{F}_p$ isomorphic to a subgroup of the galois group of $f(x)$ over $\mathbb{Q}$, but that there is an ordering (depending on p) on the roots of the polynomials $\overline{f}(x)$ and $f(x)$ so that under the isomorphism, the action of the corresponding automorphisms as permutations of these roots are the same. That means that there are elements in the galois group of $f(x)$ over $\mathbb{Q}$ with the same cycle types as corresponding elements in the galois group of $\overline{f}(x)$ over $\mathbb{F}_p$.

Corollary 4.7. *For any prime p not dividing the discriminant of $f(x)$, the galois group of $f(x)$ over $\mathbb{Q}$ contains an element with cycle decomposition $(n_1, n_2, ..., n_k)$, where n_i is the degree of the i-th irreducible factor of $f(x)$ reduced modulo p.*

Proof. We invoke the fact that every finite extension of $\mathbb{F}_p$ is a cyclic extension to point out that the galois group of $\overline{f}(x)$ over $\mathbb{F}_p$ is a cyclic group. Observe that the roots of each irreducible factor $\overline{f}_i(x)$ are permuted amongst themselves when acted upon by the elements of the galois group (that is, the galois group acts transitively

on the roots of each irreducible factor $\overline{f}_i(x)$). Take γ to be a generator for this galois group.

Label the n roots of $\overline{f}(x)$. Viewing γ as an element of S_n, we may consider its cycle decomposition. Since it must act transitively on the roots of each irreducible factor, it must be a product of k distinct permutations. It's clear that the action of γ on $\overline{f}_i(x)$ must be a cycle of length n_i, since otherwise the powers of γ could not act transitively on the roots of $\overline{f}_i(x)$. Thus the element γ has cycle decomposition $(n_1, n_2, ..., n_k)$. By Theorem 4.6, the galois group of $f(x)$ over $\mathbb{Q}$ has such an element, completing the proof.

□

We will use the above fact to construct polynomials whose galois group over $\mathbb{Q}$ will be S_n. To do so, we prove the following lemma:

Lemma 4.8. *Suppose G is a transitive subgroup of S_n that contains a transposition and an $(n-1)$-cycle. Then $G = S_n$.*

Proof. Let $\sigma \in G$ be an $(n-1)$-cycle, and let $\tau \in G$ be a transposition. We may assume, without loss of generality, that $\tau = (1, 2)$ by simply reindexing the integers between 1 and n. Since σ must fix an integer, call that integer k. There are two cases to consider: when $k \in \{1, 2\}$ and when $k \notin \{1, 2\}$. Suppose first that $k \notin \{1, 2\}$. Since G is transitive, there is a $\beta \in G$ such that $\beta(1) = k$. Let $c = \beta(2)$. Then the element $\beta\tau\beta^{-1} = (k, c) \in G$. Consider some $i \in \{1, ..., n\}$ such that $i \neq k$. Then there is some integer $1 \leq j \leq n$ such that $\sigma^j(c) = i$. Then the element $\sigma^j\beta\tau\beta^{-1}\sigma^{-j} = (k, i) \in G$. Since the element $(i, c) = (k, i)(k, c)(k, i) \in G$, we may repeat this process to generate all transpositions. Since S_n is generated by all transpositions, this completes the proof.

Now suppose that $k \in \{1, 2\}$. Assume that $k = 1$ (the case where $k = 2$ is handled in a completely analogous way). Without loss of generality (reindexing the integers between 1 and n as necessary), we may assume that $\sigma = (2, ..., n)$. For any integer $2 \leq i \leq n$, we may find an integer j such that $\sigma^j(2) = i$. Then the element $\sigma^j\tau\sigma^{-j} = (1, i) \in G$. By the method above, we may then generate every transposition, and thus $G = S_n$.

□

We now use the results of Theorem 4.6, Corollary 4.7, and Lemma 4.8 to solve the Inverse Galois Problem for the group S_n.

Theorem 4.9 (Inverse Galois Problem for S_n)**.** *For every $n \in \mathbb{Z}^+$, there are infinitely many polynomials $f(x)$ with S_n as its galois group over $\mathbb{Q}$.*

Proof. We proceed by constructing a polynomial $f(x)$ that has a reduction yielding a transposition and a reduction yielding an $(n-1)$-cycle, where n is the degree of $f(x)$. If we can construct $f(x)$ so that the galois group is transitive on the n roots of $f(x)$, then the results of Theorem 4.6 and Corollary 4.7 tell us that the galois group of $f(x)$ over $\mathbb{Q}$ is a transitive group containing a transposition and an $(n-1)$-cycle. Then by Lemma 4.8, that galois group must be S_n. Therefore, the splitting field K for $f(x)$ will be the solution to the Inverse Galois Problem. The claim that infinitely many solutions exist will be clear from the construction of the polynomial $f(x)$.

Let $f_1(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n. Let $f_2(x) \in \mathbb{F}_3[x]$ be the product of an irreducible polynomial of degree 2 with an irreducible polynomial of odd degree (i.e. $n-2$ if n is odd and $n-3$ if n is even). Let $f_3(x) \in \mathbb{F}_5[x]$ be the product of x with an irreducible polynomial of degree $n-1$. Finally, let $f(x) \in \mathbb{Z}[x]$ be any polynomial such that

$$\begin{aligned} f(x) &\equiv f_1(x) \ (mod\ 2) \\ &\equiv f_2(x) \ (mod\ 3) \\ &\equiv f_3(x) \ (mod\ 5). \end{aligned} \tag{4.3}$$

The fact that there are infinitely many such $f(x) \in \mathbb{Z}[x]$ is clear.

The reduction of $f(x)$ modulo 2 shows that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Therefore the galois group G is transitive on the n roots of $f(x)$. The factorization of $f(x)$ modulo 3 gives an element that, when raised to the appropriate odd power, shows G contains a transposition. The factorization of $f(x)$ modulo 5 shows that G contains an $(n-1)$-cycle. Therefore $G = S_n$ as claimed.

□

4.3. **A Second Approach To Solving The Inverse Galois Problem for S_n.** In this final section, we introduce a theorem, due to Hilbert, that allows us to immediately see S_n always has a solution to the inverse galois problem. We present many of these results without proof; for the full details and the proofs, see [DF]. Throughout, we will consider an arbitrary extension of fields E/F. We begin with a couple of definitions.

Definition 4.10. *A subset $\{a_1, ..., a_n\}$ of E is called algebraically independent over F if there is no nonzero polynomial $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ such that $f(a_1, ..., a_n) = 0$. An arbitrary subset S of E is called algebraically independent over F if every finite subset of S is algebraically independent. The elements of S are called independent transcendentals over F.*

Definition 4.11. *A transcendence base for E/F is a maximal subset (with respect to inclusion) of E which is algebraically independent over F.*

It's a standard Zorn's Lemma argument to see that the extension E/F has a transcendence base (if the extension is algebraic, then $\emptyset$ is the only algebraically independent set over F, and hence the only transcendence base). One may also show that any two transcendence bases for E/F must have the same cardinality (this follows the same technique that one uses in linear algebra to prove two bases of the same vector space have the same cardinality; see [DF]).

Definition 4.12. *The cardinality of the transcendence base for E/F is called the transcendence degree of E/F. Observe that algebraic extensions are precisely the extensions E/F with a transcendence degree of zero.*

We may consider the special case when E is finitely generated over F, or $E = F(a_1, ..., a_n)$, we may construct the function field in m variables (here we reindex the above set so that the first m of $a_1, ..., a_n$ are independent transcendentals, and the remaining $m - n$ of them are algebraic over F). Consider the situation where $x_1, ..., x_n$ are n indeterminates over F. Consider $f(x) = (x - x_1) \cdots (x - x_n)$. Then the symmetric functions $s_1, ..., s_n$ form a transcendence base for $F(x_1, ..., x_n)$ over F. This is because $x_1, ..., x_n$ is a transcendence base for $F(x_1, ..., x_n)$ over F and $F(x_1, ..., x_n)/F(s_1, ..., s_n)$ is a field extension of degree n. We will use this fact later in this section.

Definition 4.13. *An extension E/F is called purely transcendental if it has a transcendence base S such that $E = F(S)$.*

In particular, the fields $F(x_1, ..., x_n)$ and $F(s_1, ..., s_n)$ are both purely transcendental over F. The concept of a purely transcendental extension plays a fundamental role in the Inverse Galois Problem. To that end, we often take $F = \mathbb{Q}$. This gives us the following major theorem, due to Hilbert:

Theorem 4.14. *Let $x_1, ..., x_n$ be independent transcendentals over $\mathbb{Q}$, let $E = \mathbb{Q}(x_1, ..., x_n)$, and let G be a finite group of automorphisms of E with fixed field K. If K is a purely transcendental extension of $\mathbb{Q}$ with transcendence basis $a_1, ..., a_n$, then there are infinitely many specializations of $a_1, ..., a_n$ in $\mathbb{Q}$ such that E specializes to a galois extension of $\mathbb{Q}$ with galois group isomorphic to G.*

Remark 4.15. *Here the term "specialize" means that we evaluate the "variables" $a_1, ..., a_n$ at any element of $\mathbb{Q}$. See* [DF] *for details. Note that the fixed field K need not always be a purely transcendental extension of $\mathbb{Q}$; consider the cyclic group of order* 47*, for instance.*

We can now use Hilbert's Theorem to again show that S_n occurs as the galois group of a number field.

Corollary 4.16. *S_n is a galois group over $\mathbb{Q}$, for all n.*

Proof. We know that the fixed field of S_n acting on $\mathbb{Q}(x_1, ..., x_n)$ is the field $\mathbb{Q}(s_1, ..., s_n)$. We know that $\mathbb{Q}(s_1, ..., s_n)$ is purely transcendental over $\mathbb{Q}$, so Hilbert's Theorem tells us that we may specialize $\mathbb{Q}(x_1, ..., x_n)$ to a galois extension of $\mathbb{Q}$ with galois group S_n, precisely what we wanted to show.

□

It is important to note that even though every finite group is a subgroup of S_n and acts on $\mathbb{Q}(x_1, ..., x_n)$, it is currently not known for even the subgroup A_n if the fixed field is a purely transcendental extension of $\mathbb{Q}$, even though we have other methods of proving that A_n has a solution to the Inverse Galois Problem. As such, there are many open problems in this area available for further research.

Acknowledgements

Special thanks go out to Professor Michael Rosen, whose hours of dedication and infinite patience in instructing me has made this entire work possible.

References

[AW] M.F. Atiyah and C.T.C. Wall, *Cohomology of Groups*, pages 94-115 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

[Bak] Matt Baker, *Algebraic Number Theory Lecture 22: Galois Theory and Prime Decomposition*, (2002), found at http://www.math.uga.edu/∼mbaker/ANTlecture22.pdf.

[Bir] B.J. Birch, *Cyclotomic Fields and Kummer Extensions*, pages 85-93 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

[Cas] J.W.S. Cassels, *Global Fields*, pages 42-84 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

[DF] David S. Dummit and Richard M. Foote, *Abstract Algebra 3rd Edition*, John Wiley and Sons (2004), 158-160, 188-192, 558-602, 640-649.

[Fro] A. Frölich, *Local Fields*, pages 1-41 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

[IR] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory 2nd Edition*, Springer (1990), 172-184, 193-199, 249-251.

[Lan] Serge Lang, *Algebra Revised 3rd Edition*, Springer (2002), 261-303.

[Len] Hendrik Lenstra, *The Chebotarev Density Theorem*, found at http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf

[MM] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer (1999), 317-360.

[Nor] D.G. Northcott, *An Introduction to Homological Algebra*, Cambridge University Press (1960), 113-115, 211-265.

[Koc] H. Koch, *Number Theory II: Algebraic Number Theory*, A.N. Parshin and I.R. Shafarevich (Eds.), Springer-Verlag (1990), 45-59.

[Roq] Peter Roquette, *The Brauer-Hasse-Noether Theorem in Historical Perspective*, (2004), found at http://www.rzuser.uni-heidelberg.de/∼ci3/brhano.pdf

[Ros] Michael Rosen, *Number Theory in Function Fields*, Springer (2002), 115-125.

[Rot] Joseph Rotman, *Galois Theory 2nd Edition*, Springer (1998), 59-70, 76-85, 95-100.

[Sam] Pierre Samuel, *Algebraic Theory of Numbers*, translated by Allan J. Silberger, Houghton Mifflin Company (1970).

[Ser1] Jean-Pierre Serre, *Local Class Field Theory*, prepared by J.V. Armitage and J. Neggers, pages 129-161 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

[Ser2] Jean-Pierre Serre, *Topics in Galois Theory*, Jones and Bartlett Publishing (1992), 1-18.

[SW] Alexander Schmidt and Kay Wingberg, *Shafarevich's Theorem on Solvable Groups as Galois Groups*, (2005), found at http://www.math.uiuc.edu/Algebraic-Number-Theory/0136/.

[Tat] J.T. Tate, *Global Class Field Theory*, pages 162-203 in *Algebraic Number Theory*, edited by J.W.S. Cassels and A. Frölich, Academic Press (1967).

E-mail address: Adam_Massey@brown.edu

Department of Mathematics, Brown University, Providence, RI 02912