

INFINITE GALOIS THEORY

Frederick Michael Butler

A THESIS

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial
Fulfillment of the Requirements for the Degree of Master of Arts

2001

Supervisor of Thesis

Graduate Group Chairperson

1 Introduction

Nowhere else in the realm of basic abstract algebra does one see such an elegant interaction of topics as in the subject of Galois theory. It brings the subject of field extensions of finite degree together with the subject of finite groups, giving a bijective correspondence between intermediate fields of a Galois extension and subgroups of the Galois group of this extension.

In this paper we will briefly discuss this correspondence in the case of a finite extension of fields before moving on to an extensive discussion of the correspondence in the infinite case. This discussion will begin with basic definitions and theorems involving projective families and projective limits. We will then move on to profinite groups, which are the projective limit of a specific kind of projective family, and see how they relate to Galois groups of infinite Galois extensions. Next we discuss the Krull topology, a topology that the Galois group of an infinite Galois extension possesses, and see its use in extending the classical fundamental theorem of Galois theory to infinite extensions. We are then finally prepared to state and prove the fundamental theorem extended to the infinite case. At this point in the paper we embark upon a brief discussion of absolute Galois groups and we state (without proof) a theorem of Artin and Schreier, which demonstrates that there are many situations in which this infinite theory applies. We finish the paper by considering many examples of infinite Galois extensions, applying all that we have discussed in the rest of the paper.

An attempt was made to be as thorough as possible in development of the theory, omitting proofs only when they are technical in nature or too long or difficult for this particular paper. This paper only covers the basic theory, however, and numerous references are given for further reading.

2 A Brief Review of Classical Galois Theory

In this section we will recall the basic definitions and theorems that comprise classical Galois theory, then observe via an example that the fundamental theorem cannot carry over to the case of infinite extensions without change. For an extensive discussion of classical Galois theory see [1] Chapters 13 and 14, or [5] Chapters V and VI. Let us begin with some definitions.

We shall say that an algebraic field extension K/F is *separable* if for every $\alpha \in K$, the minimal polynomial $m_{\alpha,F}(x)$ of α over F has no repeated roots in a splitting field of $m_{\alpha,F}(x)$. An element $\alpha \in K$ whose minimal polynomial $m_{\alpha,F}(x)$ over F has no repeated roots will also be called *separable*. The extension K/F is *normal* if every irreducible polynomial $f(x) \in F[x]$ which has one root in K splits into linear

factors over K . The following theorem provides several useful equivalent definitions of a normal extension.

Theorem 2.1. *Let K/F be an algebraic field extension, and let \bar{F} denote the algebraic closure of F (so $K \subseteq \bar{F}$). Then the following are equivalent:*

- (1) K/F is a normal extension;
- (2) K is the splitting field of a family of polynomials $\{f_i(x)\}_{i \in I}$, where I is an arbitrary index set and each $f_i(x) \in F[x]$;
- (3) Every embedding $\sigma : K \hookrightarrow \bar{F}$ which fixes F induces an automorphism of K .

A proof of Theorem 2.1 can be found in [5], Chapter V §3. Note that the theorem does not make the assumption that the extension K/F is finite, just algebraic. Thus we will be able to make use Theorem 1.1 when we are considering the case of infinite algebraic extensions as well. Now we can define a *Galois* extension K/F as one which is normal and separable. The *Galois group* of the field extension K/F is the group of automorphisms of K which fix F , and is denoted $\text{Gal}(K/F)$. If $H \leq \text{Gal}(K/F)$ for some Galois field extension K/F , we call the subfield $K \supseteq E \supseteq F$ of elements of K fixed by H the *fixed field* of H , and we denote it $\mathcal{F}(H)$. The next theorem gives several equivalent definitions of a Galois field extension.

Theorem 2.2. *Let K/F be an algebraic field extension. Then the following are equivalent:*

- (1) K/F is a Galois extension;
 - (2) $\mathcal{F}(\text{Gal}(K/F)) = F$;
- If it is also the case that K/F is a finite extension, then (1) and (2) are equivalent to the following:*
- (3) $|\text{Gal}(K/F)| = [K : F]$.

A proof of Theorem 2.2 is in [5] Chapter VI §1. Note that again we made no assumption that the extension is finite in (1) and (2) of Theorem 2.2. We state one more result which will prove useful in later sections of this paper.

Theorem 2.3. (Isomorphism Extension Theorem) *Let $\sigma : E \rightarrow E'$ be a field isomorphism, $S = \{f_i(x)\}_{i \in I}$ a set of polynomials in $E[x]$, and let $S' = \{\sigma(f_i(x))\} \subseteq E'[x]$ be the image of S under σ . Let K be the splitting field for S over E , K' the splitting field of S' over E' . Then there is an isomorphism $\tau : K \rightarrow K'$ such that $\tau|_E = \sigma$. Furthermore, if $\alpha \in K$ and β is a root of $\sigma(m_{\alpha,E}(x))$ then τ can be chosen such that $\tau(\alpha) = \beta$.*

For a proof of Theorem 2.3 see [7] Chapter 1 §3. Let us quickly note the situation in which we will use Theorem 2.3 in this paper. We will have $E = E'$ and $K = K'$, and E is a Galois extension of another field F , $\sigma \in \text{Gal}(E/F)$. Then we will have K is a Galois extension of F with $K \supseteq E \supseteq F$ (hence K/E will be Galois as well), and we will seek a $\tau \in \text{Gal}(K/F)$ which extends σ to all of K . Theorem 2.3 guarantees that such a τ exists. We are now ready to state the main result of classical finite Galois theory.

Theorem 2.4. (Fundamental Theorem of Classical Galois Theory) *Let K/F be a finite Galois extension, and let $G = \text{Gal}(K/F)$. Then there is a bijection between the set of fields $K \supseteq E \supseteq F$ and the set of groups $1 \leq H \leq G$. The maps are $E \mapsto \text{Gal}(K/E)$ and $H \mapsto \mathcal{F}(H)$. We also have the following:*

(1) *If $E_1, E_2 \subseteq K$ correspond to $H_1, H_2 \leq G$ respectively, then $E_1 \subseteq E_2$ iff $H_2 \leq H_1$;*

(2) *If $E_1, E_2 \subseteq K$ correspond to $H_1, H_2 \leq G$ respectively, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$ and $E_1 E_2$ corresponds to $H_1 \cap H_2$.*

If $E = \mathcal{F}(H)$ where $H \leq G$ then we also have:

(3) *$[K : E] = |H|$ and $[E : F] = |G : H|$;*

(4) *K/E is always Galois and $\text{Gal}(K/E) = H$;*

(5) *E is Galois over F iff $H \triangleleft G$, in which case $\text{Gal}(E/F) \simeq G/H$.*

Theorem 2.4 is proved in [1] Chapter 14 §2. One sees that Theorem 2.4 proves useful in many situations, since it allows us to find out information about the intermediate fields of a Galois extension from the subgroups of the Galois group of the extension, and vice versa. This translation of a given problem into a related one is a pervasive technique in mathematics.

Because the fundamental theorem often proves useful for just the reason stated above, we would like to extend it to the case of infinite Galois extensions. Luckily our definition of a Galois extension carries over without change from the finite case to the case of infinite algebraic extensions. Thus we will agree to say that an infinite algebraic field extension is *Galois* if it is normal and separable. Unfortunately we quickly learn that the fundamental theorem as it stands does not hold for infinite algebraic extensions. We can see this fact in the example that follows.

Example 2.5. Let $S = \{\sqrt{p} \in \mathbb{N} \mid p \text{ prime}\}$, $K = \mathbb{Q}(S)$, and consider the field extension K/\mathbb{Q} . K is the splitting field of $\{x^2 - p \mid p \in \mathbb{N}, p \text{ prime}\}$ so K/\mathbb{Q} is normal by Theorem 2.1, and each polynomial $x^2 - p$ is separable hence K/\mathbb{Q} is separable. Thus by our definition, K/\mathbb{Q} is an infinite Galois extension. Any $\sigma \in \text{Gal}(K/\mathbb{Q})$ must send \sqrt{p} to a root of its minimal polynomial over \mathbb{Q} (which is $x^2 - p$), hence to \sqrt{p} or $-\sqrt{p}$, so we see that $\text{Gal}(K/\mathbb{Q})$ is an infinite elementary abelian two group. That is, $\text{Gal}(K/\mathbb{Q}) \simeq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. However $\text{Gal}(K/\mathbb{Q})$ can also be thought of as an infinite dimensional vector space V over the finite field $F = \mathbb{Z}/2\mathbb{Z}$. We see that the

dual vector space $V^* = \{\phi : V \rightarrow F \mid \phi \text{ is a linear transformation}\}$ is uncountable, so $\{\ker \phi \mid \phi \in V^*\}$ is also uncountable. We see this second fact because for any $v \in V$ and $\phi \in V^*$, $\phi(v) = 0$ or $\phi(v) = 1$, hence $\ker \phi$ tells us what the value of ϕ is on all $v \in V$; namely, $\phi(v) = 0$ if $v \in \ker \phi$ and $\phi(v) = 1$ if $v \in V - \ker \phi$. Since for each ϕ , $V/\ker \phi \simeq \mathbb{F}_2$, we see that each $\ker \phi \leq G$ is a subgroup of index 2, and there are uncountably many such subgroups. However, there are only countably many quadratic extensions of \mathbb{Q} ($\{\mathbb{Q}(\sqrt{q}) \mid q \in \mathbb{Q}, q \text{ is not a perfect square}\}$ is a complete list), hence there is no longer a bijection between intermediate fields and subgroups of the Galois group. This paper will explain what sort of correspondence exists for infinite Galois extensions.

3 Projective Families and Limits

In this section we begin to lay the foundation of infinite Galois theory with the ideas of a projective family and a projective limit. We will then see that the Galois group of an infinite Galois extension is actually the projective limit of a specific projective family. Let us begin with a basic definition.

Definition 3.1. Let A be an index set, $\{G_a\}_{a \in A}$ a family of groups. Assume that A is partially ordered (by \leq) and that for all $a, b \in A$, there exists $c \in A$ such that $a \leq c$ and $b \leq c$. Assume for all $a, b \in A$ with $a \leq b$, we have a group homomorphism $\phi_{b,a} : G_b \rightarrow G_a$, consistent in that if $a \leq b \leq c$, then $\phi_{b,a} \circ \phi_{c,b} = \phi_{c,a}$. Also $\phi_{a,a} = 1_{G_a}$ (that is, the identity in G_a) for all $a \in A$. We say that $\{G_a, \phi_{b,a}\}$ is a *projective family of groups*.

Example 3.2. Let $A = \mathbb{N}$ where $m \leq n$ iff $m|n$, $G_n = \mathbb{Z}/n\mathbb{Z}$, and $\phi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ is the trivial map if $m \neq n$, and $\phi_{n,n} = id_{G_n}$.

Example 3.3. Again $A = \mathbb{N}$ and $m \leq n$ iff $m|n$, $G_n = \mathbb{Z}/n\mathbb{Z}$, and $\phi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ is the natural map $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$.

Example 3.4. Let G be any group, A the family of all normal subgroups of G of finite index. For $N \in A$, let $G_N = G/N$. Say $N_1 \leq N_2$ iff $N_2 \subseteq N_1$; we see that if $N_1, N_2 \in A$ then $N_1 \cap N_2 \in A$, $N_1 \cap N_2 \subseteq N_1$, $N_1 \cap N_2 \subseteq N_2$, so $N_1 \cap N_2 \geq N_1$ and $N_1 \cap N_2 \geq N_2$. Finally let $\phi_{N_2, N_1} : G_{N_2} \rightarrow G_{N_1}$ be the natural map $gN_2 \mapsto gN_1$.

Note that while Examples 3.2 and 3.3 consist of the same index set, partial order, and groups, the maps are different. Thus it is important to specify the maps as well as the other information about a projective family. Also note Example 3.4 well as it will become a central focus in our discussion of Galois theory.

One familiar with category theory (see [1] Appendix II for a brief overview) is acquainted with the idea of a universal object, which we seek to define next for a projective family.

Definition 3.5. A *projective limit* of the projective family $\{G_a, \phi_{b,a}\}$ is a group G together with a collection of homomorphisms $\phi_a : G \rightarrow G_a$ such that the following hold:

- (1) If $a \leq b$, then $\phi_{b,a} \circ \phi_b = \phi_a$;
- (2) Given any group H and a collection of homomorphisms $\rho_a : H \rightarrow G_a$ satisfying (1) above, there exists a unique group homomorphism $\chi : H \rightarrow G$ such that $\phi_a \circ \chi = \rho_a$ for all $a \in A$.

A projective limit of $\{G_a, \phi_{b,a}\}$ is denoted $\varprojlim_{a \in A} G_a$ or sometimes $\varprojlim G_a$, where the set A and the maps $\phi_{b,a}$ are understood from context. For the following examples the corresponding projective families are those in Examples 3.2, 3.3, and 3.4 respectively.

Example 3.6. Here $\varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$, where $\psi_m : \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ is just the natural projection map.

Example 3.7. In this case $\varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_{p \in \mathbb{N}, p \text{ prime}} \mathbb{Z}_p$, the direct product of the p -adic integers over all primes p . This group is often denoted $\hat{\mathbb{Z}}$; we will see much more of it later.

Example 3.8. Here since we did not specify G , we cannot really describe $\varprojlim G_N$ except to say it is called the *profinite completion* of G . We see that Example 3.7 is a specific example of a profinite completion.

One of course hopes that such objects as projective limits of groups exist, and are at least up to isomorphism unique; the following proposition establishes both of these facts.

Proposition 3.9. *For a projective family $\{G_a, \phi_{b,a}\}$ of groups, a projective limit $\{G, \phi_a\}$ exists; and if $\{H, \rho_a\}$ is another projective limit, then the map $\chi : H \rightarrow G$ as in Definition 3.5 (2) is an isomorphism.*

Proof. Define $G \leq \prod_{a \in A} G_a$ by letting $(g_a)_{a \in A} \in G$ iff for all $a \leq b$ one has $\phi_{b,a}(g_b) = g_a$. Clearly $G \neq \emptyset$; it contains $(1_a)_{a \in A}$. Let $\phi_a : G \rightarrow G_a$ be the projection (that is, the ordinary projection map $\pi_a : \prod_{a \in A} G_a \rightarrow G_a$ restricted to the set G), which is clearly a homomorphism. Then we see that $\phi_{b,a} \circ \phi_b = \phi_a$. This proves condition (1) of Definition 3.5.

Now suppose $\{H, \rho_a\}$ also satisfies for $a \leq b$, that $\phi_{b,a} \circ \rho_b = \rho_a$, where the ρ_a are also group homomorphisms. Define a map $\chi : H \rightarrow \prod_{a \in A} G_a$ by setting $\chi(h) = (\rho_a(h))_{a \in A}$. Then we clearly have $\pi_a(\chi(h)) = \pi_a((\rho_a(h))_{a \in A}) = \rho_a(h)$, so $\pi_a \circ \chi = \rho_a$ for all $a \in A$. Also χ is clearly a homomorphism since each of the ρ_a are. If $a \leq b$ then $\pi_a \circ \chi = \rho_a = \phi_{b,a} \circ \rho_b = \phi_{b,a} \circ (\pi_b \circ \chi)$, so for any $h \in H$, $\chi(h)$ satisfies $\pi_a(\chi(h)) = \phi_{b,a}(\pi_b(\chi(h)))$. This implies that $\chi(h) \in G$ by our definition of G , so $\chi : H \rightarrow G$. Since $\phi_a = \pi_a|_G$, we see also that χ satisfies $\phi_a \circ \chi = \rho_a$.

Finally, if $\chi' : H \rightarrow G$ is another homomorphism satisfying $\phi_a \circ \chi' = \rho_a$ for all $h \in H$ and $a \in A$, then the a th entry of $\chi'(h)$ must be $\rho_a(h)$ for all $h \in H$ and $a \in A$, which forces $\chi(h) = \chi'(h)$ for all $h \in H$. Hence $\chi = \chi'$, so χ is unique. This proves condition (2) of Definition 3.5, so G is a projective limit of the given projective family.

Next if $\{G, \psi_a\}$ and $\{H, \rho_a\}$ are both projective limits, we know that there exists a unique map $\chi_1 : H \rightarrow G$ such that $\psi_a \circ \chi_1 = \rho_a$, and there exists a unique map $\chi_2 : G \rightarrow H$ such that $\psi_a = \rho_a \circ \chi_2$ for all $a \in A$. Thus $\rho_a = \rho_a \circ \chi_2 \circ \chi_1$, and $\psi_a = \psi_a \circ \chi_1 \circ \chi_2$ for all $a \in A$. The universal property implies that there is only one map $\sigma : G \rightarrow G$ such that $\psi_a = \psi_a \circ \sigma$, and only one map $\tau : H \rightarrow H$ such that $\rho_a = \rho_a \circ \tau$. However, 1_G satisfies $\psi_a = \psi_a \circ 1_G$, and 1_H satisfies $\rho_a = \rho_a \circ 1_H$. Thus we have $\sigma = 1_G$ and $\tau = 1_H$, so we have $\chi_1 \circ \chi_2 = 1_G$ and $\chi_2 \circ \chi_1 = 1_H$, and $\chi_1 : H \rightarrow G$ is an isomorphism with $\chi_1^{-1} = \chi_2$. \square

Now that the notion of a projective limit has been established, the Galois group of an infinite algebraic extension can be explored. From this point on in the paper, let us fix the following notation. Let K/F be an infinite Galois extension, $G = \text{Gal}(K/F)$, $\mathcal{N} = \{H \mid H = \text{Gal}(K/E) \text{ for some } E \in \mathcal{I}\}$ where $\mathcal{I} = \{E \mid K \supseteq E \supseteq F, E/F \text{ finite Galois}\}$. If $H \leq G$, we denote the fixed field of H by $\mathcal{F}(H)$ as we do in the finite case, and for $\sigma \in G$ we will use $\mathcal{F}(\sigma)$ as an abbreviation for $\mathcal{F}(\langle \sigma \rangle)$.

Lemma 3.10. *Let K/F be an infinite Galois extension, $G = \text{Gal}(K/F)$, and let $H \in \mathcal{N}$, so $H = \text{Gal}(K/E)$ for some $E \in \mathcal{I}$. Then $H \triangleleft G$, and $\text{Gal}(E/F) \simeq G/H$.*

Proof. Since E/F is a normal extension (because it is Galois), the map $\theta : G \rightarrow \text{Gal}(E/F)$ given by $\theta(\sigma) = \sigma|_E$ is a well defined map to $\text{Gal}(E/F)$ (see Theorem 2.1, equivalence (3)). Given $\tau \in \text{Gal}(E/F)$, τ can be extended to a $\tau' \in \text{Gal}(K/F)$ (so $\tau'|_E = \tau$) by Theorem 2.3; thus θ is onto. Finally, $\ker(\theta) = \text{Gal}(K/E) = H$, so $H \triangleleft G$ and by the first isomorphism theorem for groups we have $\text{Gal}(E/F) \simeq G/H$. \square

Now let us discuss the partial ordering that can be placed on \mathcal{I} . We shall say that $E_1 \leq E_2$ for two fields $E_1, E_2 \in \mathcal{I}$ if $E_1 \subseteq E_2$. We see that $\{\text{Gal}(E/F), \phi_{E_2, E_1}\}_{E \in \mathcal{I}}$ forms a projective family with maps $\phi_{E_2, E_1} : \text{Gal}(E_2/F) \rightarrow \text{Gal}(E_1/F)$ for $E_1 \leq E_2$ defined by $\phi_{E_2, E_1}(\sigma) = \sigma|_{E_1}$. ϕ_{E_2, E_1} is a well defined homomorphism by Theorem 2.1, and clearly satisfies the compatibility condition.

In light of Lemma 3.10 we see that we can define another projective family as follows. Define a partial ordering of \mathcal{N} by declaring $H_1 \leq H_2$ if $H_2 \subseteq H_1$. In this case our projective family will be $\{G/H, \phi_{H_2, H_1}\}_{H \in \mathcal{N}}$ where $\phi_{H_2, H_1} : G/H_2 \rightarrow G/H_1$ is given by $\phi_{H_2, H_1}(\sigma H_2) = \sigma H_1$. We know that for $H \in \mathcal{N}$, $H \triangleleft G$ so G/H is a group, and if $H_1 \leq H_2$ (so $H_2 \subseteq H_1$) the map ϕ_{H_2, H_1} is a well defined homomorphism, also clearly compatible.

However, if $H \in \mathcal{N}$ then $H = \text{Gal}(K/E)$ for some $E \in \mathcal{I}$, and by Lemma 3.10 we know that then $\text{Gal}(E/F) \simeq G/H$. It is also clear that if $H_1, H_2 \in \mathcal{N}$, hence $H_1 = \text{Gal}(K/E_1)$ and $H_2 = \text{Gal}(K/E_2)$ for $E_1, E_2 \in \mathcal{I}$, then $H_1 \leq H_2$ in \mathcal{N} iff $E_1 \leq E_2$ in \mathcal{I} . Finally, in this situation we see that the maps ϕ_{H_2, H_1} and ϕ_{E_2, E_1} correspond exactly, thus the projective families $\{\text{Gal}(E/F), \phi_{E_2, E_1}\}_{E \in \mathcal{I}}$ and $\{G/H, \phi_{H_2, H_1}\}_{H \in \mathcal{N}}$ are the same. We will make use of this fact, using the description that is most convenient for our purposes.

We note here that by considering the projective family $\{G/H, \phi_{H_2, H_1}\}_{H \in \mathcal{N}}$, we clearly have a collection of homomorphisms $\phi_H : G \rightarrow G/H$ which are compatible with the maps ϕ_{H_2, H_1} . Namely, $\phi_H(\sigma) = \sigma H$. The universal property of the projective limit implies that there exists a unique homomorphism $\chi' : G \rightarrow \varprojlim_{H \in \mathcal{N}} G/H$; since $\varprojlim_{H \in \mathcal{N}} G/H \simeq \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$, we also have a homomorphism $\chi : G \rightarrow \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$. We shall see momentarily that this homomorphism is in fact an isomorphism. We need a lemma first.

Lemma 3.11. *Let $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. Then there is an $E \in \mathcal{I}$ such that $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.*

Proof. Let $K \supseteq E \supseteq F$ be the splitting field of $\{m_{\alpha_i, F}(x)\}_{i=1}^n$ over F . Clearly E is normal over F , and since $K \supseteq E$ and K/F is separable, E/F is separable, so E/F is Galois. Finally, $[E : F] \leq \prod_{i=1}^n \deg(m_{\alpha_i, F}(x))! < \infty$, so $E \in \mathcal{I}$. \square

Theorem 3.12. *Let K/F be an infinite algebraic extension, with notation the same as above. Then the homomorphism $\chi : G \rightarrow \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$ is an isomorphism.*

Proof. First note that for each $\text{Gal}(E/F)$, E/F is a finite Galois extension. Hence the uniqueness of χ implies that χ is the map $\sigma \mapsto (\sigma|_E)_{E \in \mathcal{I}}$ since this map is a compatible homomorphism. χ is injective, because $\chi(\sigma) = (1_E)_{E \in \mathcal{I}}$ implies that $\sigma|_E = 1_E$ for every finite Galois extension E/F . However, since $K = \bigcup_{E \in \mathcal{I}} E$, one has that $\sigma = 1_K$. Finally, χ is onto. Let $(\sigma_E)_{E \in \mathcal{I}} \in \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$. Define σ as follows. Let $\alpha \in K$, so there exists some $E \in \mathcal{I}$ such that $\alpha \in E$ by Lemma 3.11. Then let $\sigma(\alpha) = \sigma_E(\alpha)$ for such an E as above. In this way one defines σ on all of K , and thus obtains $\sigma \in G$. Since $E_1 \leq E_2$ iff $\text{Gal}(E_1/F) \leq \text{Gal}(E_2/F)$, if $\alpha \in E_1 \leq E_2$ then $\sigma_{E_1}(\alpha) = \sigma_{E_2}(\alpha)$, so σ is well defined. Then $\chi(\sigma) = (\sigma_E)_{E \in \mathcal{I}}$, so χ is onto and hence χ is an isomorphism. \square

We see that the Galois group of an infinite algebraic extension K/F is in a sense “pasted” together from all of the Galois groups of the Galois extensions of F contained in K in a way that agrees on the overlap. Theorem 3.12 tells us formally that a Galois group of an infinite algebraic extension is a projective limit of a projective family of finite groups. This important notion will be considered in the next section.

4 Profinite Groups

In this section we explore profinite groups. We shall see that a profinite group possesses a natural topology under which it forms a topological group (that is, multiplication and inversion are continuous maps), and we will look at the properties of such a group as a topological space.

Definition 4.1. A group G is a *profinite group* if $G = \varprojlim G_a$ for a projective family $\{G_a, \phi_{b,a}\}$, where each G_a is a finite group.

We see from Theorem 3.12 that Galois groups of infinite algebraic extensions are in fact profinite groups. They will of course provide the most important example for us.

Now let us consider the natural topology on a profinite group. Let $G = \varprojlim G_a$ be a profinite group, so G is the projective limit of the projective family $\{G_a, \phi_{b,a}\}$ of finite groups. Give each G_a the discrete topology, then give $\prod_{a \in A} G_a$ the product topology, and finally give $\varprojlim G_a \subseteq \prod_{a \in A} G_a$ the subspace topology. The next proposition provides us with some evidence that this is the “right” topology to give a profinite group.

Proposition 4.2. *Under the topology described above, a profinite group G is a topological group. That is, the operations $p : G \times G \rightarrow G$ such that $p(g, h) = gh$ and $i : G \rightarrow G$ such that $i(g) = g^{-1}$ are continuous in this topology.*

Proof. The topology we are giving to $G = \varprojlim G_a$ is none other than the product topology by definition (where each G_a has the discrete topology), which is generated by the sub-basis $\bigcup_{a \in A} \{\pi_a^{-1}(\{g_a\}) \mid g_a \in G_a\}$. Thus it suffices to check that the inverse image of one of these sub-basic open sets under the maps p and i is open, which we do now. Let $\pi_a^{-1}(\{g_a\})$ be such an open set. Then it is easy to check that $p^{-1}(\pi_a^{-1}(\{g_a\})) = \bigcup_{h \in G_a} \pi_a^{-1}(\{g_a h\}) \times \pi_a^{-1}(\{h^{-1}\})$ which is clearly open in the product topology on $G \times G$. Similarly, it is easy to see that $i^{-1}(\pi_a^{-1}(\{g_a\})) = \pi_a^{-1}(\{g_a^{-1}\})$, also clearly open in the profinite group topology on G . Thus G forms a topological group under this topology. \square

Now we need one more definition, which might look strangely familiar at first.

Definition 4.3. Let A be an index set, $\{X_a\}_{a \in A}$ a family of topological spaces. Assume that A is partially ordered (by \leq) and for all $a, b \in A$ with $a \leq b$ there exists a continuous map $\phi_{b,a} : X_b \rightarrow X_a$ consistent in that if $a \leq b \leq c$ then $\phi_{b,a} \circ \phi_{c,b} = \phi_{c,a}$, and $\phi_{a,a} = 1_{X_a}$ for all $a \in A$. We say $\{X_a, \phi_{b,a}\}$ is a *projective family of topological spaces*. A *projective limit* of such a family, denoted $\varprojlim X_a$ is

a topological space X together with a collection of continuous maps $\phi_a : X \rightarrow X_a$ such that:

- (1) If $a \leq b$ then $\phi_{b,a} \circ \phi_b = \phi_a$;
- (2) Given another topological space Y and collection of maps $\rho_a : Y \rightarrow X_a$ satisfying (1) above, there exists a unique continuous map $\chi : Y \rightarrow X$ such that $\phi_a \circ \chi = \rho_a$ for all $a \in A$.

We note that in our definition of the profinite group topology, each G_a is given the discrete topology, which makes the maps $\phi_{b,a} : G_b \rightarrow G_a$ continuous (as any map $f : X \rightarrow Y$ where X has the discrete topology is continuous). Also, the maps $\phi_a : G \rightarrow G_a$ (G and ϕ_a defined analogously as in Proposition 3.9) are simply projection maps $\pi_a : \prod_{a \in A} G_a \rightarrow G_a$ restricted to G , hence are also certainly continuous. Thus we see that we are dealing with projective families and projective limits of topological groups, which can be thought of either in the context of Definitions 3.1 and 3.5 as simply groups, or in the context of Definition 4.3. By thinking of these groups in the second sense as purely topological spaces, we shall see that a profinite group under this natural topology has some perhaps surprising characteristics. In order to prove this fact we need the following lemma. The proof is fairly technical; it can be found in [13] Chapter 1 §1.

Lemma 4.4. *Let $\{G_a, \phi_{b,a}\}_{a \in A}$ be an projective family of Hausdorff topological spaces. Then $G = \varprojlim G_a$ is closed in $\prod_{a \in A} G_a$.*

Theorem 4.5. *Let G be a profinite group, and equip G with the topology described above. Then as a topological group, G is compact, Hausdorff, and totally disconnected.*

Proof. Suppose $G = \varprojlim G_a$ for some projective family $\{G_a, \phi_{b,a}\}_{a \in A}$. Each G_a is a finite group with the discrete topology, hence each G_a is compact, Hausdorff, and totally disconnected under this topology. It is an elementary fact from topology that a product of Hausdorff spaces is Hausdorff and a product of totally disconnected spaces is totally disconnected, where the product of the spaces is given the product topology. Thus $\prod_{a \in A} G_a$ is Hausdorff and totally disconnected. It is also an elementary fact from topology that a subspace of a Hausdorff space is Hausdorff and a subspace of a totally disconnected space is totally disconnected, where the subspace is given the subspace topology. Thus $\varprojlim G_a \subset \prod_{a \in A} G_a$ is Hausdorff and totally disconnected. Finally, since each G_a is compact, the Tychanoff theorem (proven in [8] Chapter 5 §1) tells us that $\prod_{a \in A} G_a$ is compact. Then Lemma 4.4 shows that $\varprojlim G_a$ is closed in $\prod_{a \in A} G_a$, hence $\varprojlim G_a$ is compact being a closed subspace of a compact space. \square

An immediate corollary of Theorem 4.5 is the following.

Corollary 4.6. *Let $G = \text{Gal}(K/F)$, K/F an infinite Galois extension. Then with the profinite group topology G is compact, Hausdorff, and totally disconnected.*

While Theorem 4.5 may seem strange, it is not completely without intuition. The simplicity of the proof demonstrates this fact. The next theorem however, the proof of which can be found in [10] Chapter 1 §1, is more surprising.

Theorem 4.7. *Let G be a compact, Hausdorff, totally disconnected topological group. Then G is a profinite group.*

Thus we see that profinite groups and compact, Hausdorff, totally disconnected topological groups are in fact identical objects. There is one final result of this section in the following theorem, whose proof can be found in [13] Chapter 3 §3.

Theorem 4.8. *Let G be a profinite group. Then G is the Galois group of some field extension.*

Thus if we collect all the results of this section we see that Galois group, profinite group, and compact, Hausdorff, totally disconnected topological group are all equivalent concepts. There is another way to define a topology on the Galois group of Galois extension, which we will discuss at length in the next section. We shall see that this topology turns out to be useful in our quest to extend the classical fundamental theorem to the infinite case.

5 The Krull Topology

In this section we define the Krull topology on the Galois group of an infinite Galois extension, and derive some of the properties of this topology. While at first the Krull topology may seem to be a more workable definition of a topology on a Galois group, we shall see that it is really nothing more than the profinite group topology of the previous section. Consider the following lemmas, which will be useful later.

Lemma 5.1. *Let $G = \text{Gal}(K/F)$ for some Galois extension K/F , and let \mathcal{N} be as defined in the previous section. Then $\bigcap_{N \in \mathcal{N}} N = \{1\}$, and for all $\sigma \in G$ we have that $\bigcap_{N \in \mathcal{N}} \sigma N = \{\sigma\}$.*

Proof. Let $\tau \in \bigcap_{N \in \mathcal{N}} N$ and let $\alpha \in K$. Lemma 3.11 implies that there is an $E \in \mathcal{I}$ with $\alpha \in E$. Let $H = \text{Gal}(K/E) \in \mathcal{N}$. Then $\tau \in H$ because $\tau \in \bigcap_{N \in \mathcal{N}} N$, but then τ fixes E , so $\tau(\alpha) = \alpha$. Thus τ fixes every $\alpha \in K$, and therefore $\tau = 1$ so $\bigcap_{N \in \mathcal{N}} N = \{1\}$.

If $\tau \in \bigcap_{N \in \mathcal{N}} \sigma N$, then $\tau\sigma^{-1} \in \bigcap_{N \in \mathcal{N}} N$, so $\tau\sigma^{-1} = 1$, and hence $\tau = \sigma$. \square

Lemma 5.2. *If $N_1, N_2 \in \mathcal{N}$, then $N_1 \cap N_2 \in \mathcal{N}$.*

Proof. Let $N_1 = \text{Gal}(K/E_1)$ and $N_2 = \text{Gal}(K/E_2)$ for $E_1, E_2 \in \mathcal{I}$. Because E_1 and E_2 are finite Galois over F , so is E_1E_2 , so $E_1E_2 \in \mathcal{I}$. However, $\text{Gal}(K/E_1E_2) = N_1 \cap N_2$, because $\sigma \in N_1 \cap N_2$ iff $\sigma|_{E_1} = 1_{E_1}$ and $\sigma|_{E_2} = 1_{E_2}$ iff $E_1, E_2 \subseteq \mathcal{F}(\sigma)$ iff $E_1E_2 \subseteq \mathcal{F}(\sigma)$ iff $\sigma \in \text{Gal}(K/E_1E_2)$. Hence $N_1 \cap N_2 = \text{Gal}(K/E_1E_2) \in \mathcal{N}$. \square

Now we are ready to take a major step toward our original goal with the following lemma.

Lemma 5.3. *Let K/F be an infinite Galois extension, $G = \text{Gal}(K/F)$. Then $\mathcal{B} = \{\sigma H \mid \sigma \in G, H \in \mathcal{N}\}$ forms a basis for a topology on G .*

Proof. Each open set is a union of cosets σH hence an arbitrary union of open sets is also a union of such cosets, so in this topology an arbitrary union of open sets is open. G is open because $G = \text{Gal}(K/F)$, and F/F is a finite Galois extension of degree 1. The main thing to check is that open sets are closed under finite intersections. It suffices to check this for two elements of the basis, which we do now. If $\tau_1 H_1$ and $\tau_2 H_2$ are two basis elements, let $\tau \in \tau_1 H_1 \cap \tau_2 H_2$. Then $\tau H_1 = \tau_1 H_1$ and $\tau H_2 = \tau_2 H_2$, so $\tau_1 H_1 \cap \tau_2 H_2 = \tau H_1 \cap \tau H_2 = \tau(H_1 \cap H_2)$. Lemma 5.2 implies that $H_1 \cap H_2 \in \mathcal{N}$, hence $\tau(H_1 \cap H_2)$ is open. Finally for some $H \in \mathcal{N}$ with $H \neq G$, choose $\tau_1, \tau_2 \in G$ such that $\tau_1 H \neq \tau_2 H$ (which we can do, otherwise $H = G$). Then $\tau_1 H \cap \tau_2 H = \emptyset$, and \emptyset is open, so \mathcal{B} is indeed the basis for a topology on G . \square

In light of Lemma 5.3 we can define the following.

Definition 5.4. Let K/F be an infinite Galois extension, $G = \text{Gal}(K/F)$. The *Krull topology* on G is the topology with basis all cosets σH , where $\sigma \in G$, $H = \text{Gal}(K/E)$, and E/F is a finite Galois extension.

Immediately we see something very interesting about the Krull topology. If $H \in \mathcal{N}$ then $H = \text{Gal}(K/E)$ and E/F is a finite Galois extension. By Lemma 3.10 we know that $\text{Gal}(E/F) \simeq \text{Gal}(K/F)/H$, so $|G : H|$ is also finite. Thus there exists $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ such that $G = H \cup \sigma_1 H \cup \dots \cup \sigma_{n-1} H$, so $G - H$ is also a union of open sets. Therefore H is both an open set and a closed set. Thus the Krull topology has a basis of sets which are both closed and open, sometimes called *clopen sets*.

At this point we recall that a Galois group of an infinite algebraic extension is also a profinite group, hence it possesses a natural topology as such a group. We have already seen that for $G = \text{Gal}(K/F)$ where K/F is infinite Galois and \mathcal{I} as above, the map $\chi : G \rightarrow \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$ given by $\chi(\sigma) = (\sigma|_E)_{E \in \mathcal{I}}$ is a group isomorphism. In fact, more is true.

Proposition 5.5. *Keeping the notation as above, giving G the Krull topology and $\varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$ the profinite group topology, the map $\chi : G \rightarrow \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$ is a homeomorphism of topological spaces.*

Proof. We already know that χ is a group isomorphism, so χ is bijective. The open sets in G are generated by the basis $\{\sigma H \mid \sigma \in G, H \in \mathcal{N}\}$ and by the sub-basis $\bigcup_{E \in \mathcal{I}} \{\pi_E^{-1}(\{\sigma\}) \mid \sigma \in \text{Gal}(E/F)\}$ in $\varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$, where we use π_E to denote the ordinary projection map restricted to $\varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$. First let us check that χ is continuous. $\chi^{-1}(\pi_E^{-1}(\{\sigma\})) = \{\tau \in G \mid \tau|_E = \sigma\} = \{\tau \in G \mid \tau \text{ is an extension of } \sigma \text{ to } K\} = \bigcup_{\tau \in G} \tau \text{Gal}(K/E)$ where the union is taken over all such τ which extend σ , and which is clearly open in G by definition of the Krull topology.

Now let us check that χ^{-1} is continuous, which is equivalent to checking that χ is an open map. Let σH be a basic open set for the Krull topology on G , so $\sigma \in G$ and $H = \text{Gal}(K/E)$ for some $E \in \mathcal{I}$. Then $\chi(\sigma H) = \{(\sigma \tau_L)_{L \in \mathcal{I}} \mid \tau_L|_E = 1_{L \cap E}\} = \{(\tau_L)_{L \in \mathcal{I}} \mid \sigma^{-1} \tau_L|_E = 1_{L \cap E}\} = \{(\tau_L)_{L \in \mathcal{I}} \mid \tau_L|_E = \sigma|_{L \cap E}\} = \pi_E^{-1}(\{\sigma|_E\})$ which is also open in $\varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$. Thus $\chi : G \rightarrow \varprojlim_{E \in \mathcal{I}} \text{Gal}(E/F)$ is a homeomorphism. \square

Proposition 5.5 trivially yields the following corollaries.

Corollary 5.6. *Equipped with the Krull topology, the Galois group G of an infinite algebraic extension forms a topological group. That is, the maps $p : G \times G \rightarrow G$ such that $p(g, h) = gh$ and $i : G \rightarrow G$ such that $i(g) = g^{-1}$ are continuous under the Krull topology.*

Corollary 5.7. *Equipped with the Krull topology, the Galois group of an infinite algebraic extension is compact, Hausdorff, and totally disconnected.*

Now we finally have all the tools necessary to discuss what sort of fundamental theorem of Galois theory exists for the infinite algebraic case. Let us discuss it now.

6 The Fundamental Theorem

In this section we will state and prove the fundamental theorem for infinite Galois theory, and look at a familiar example to which this theorem applies. We are on the brink of proving this generalized fundamental theorem. We will require just one more lemma, which we state and prove now.

Lemma 6.1. *Let K/F be a Galois extension, $G = \text{Gal}(K/F)$, $H \leq G$ and let $H' = \text{Gal}(K/L)$ where $L = \mathcal{F}(H)$. Then $H' = \bar{H}$ where \bar{H} denotes the closure of H in the Krull topology on G .*

Proof. Since every element of H fixes L by definition of L , we have $H \leq H'$. Now take $\sigma \in G - H'$. Then there is an $\alpha \in L$ with $\sigma(\alpha) \neq \alpha$. Choose $E \in \mathcal{I}$ with $\alpha \in E$ (which we know we can do by Lemma 3.11) and let $N = \text{Gal}(K/E)$. Then for any $\tau \in N$, $\tau(\alpha) = \alpha$, so $\sigma\tau(\alpha) = \sigma(\alpha) \neq \alpha$. Hence σN is an open neighborhood of σ disjoint from H' , so $G - H'$ is open and hence H' is closed.

Finally, we want to show that $H' \subseteq \bar{H}$. Then we will have $H \subseteq H' \subseteq \bar{H}$ and H' is closed, so $H' = \bar{H}$. Let $\sigma \in H'$ and again choose any $N \in \mathcal{N}$, $N = \text{Gal}(K/E)$ with $E \in \mathcal{I}$. Let $H_0 = \{\rho|_E \mid \rho \in H\} \leq \text{Gal}(E/F)$, where $\text{Gal}(E/F)$ is finite. Since the fixed field of H_0 is $\mathcal{F}(H) \cap E$, that is, $L \cap E$, the classical fundamental theorem shows that $H_0 = \text{Gal}(E/E \cap L)$. Since $\sigma \in H'$, $\sigma|_L = 1_L$, so $\sigma|_E \in H_0$. Thus there is a $\rho \in H$ with $\rho|_E = \sigma|_E$, and thus $\sigma^{-1}\rho \in \text{Gal}(K/E) = N$ so $\rho \in \sigma N \cap H$. Thus for every $\sigma \in H'$ and every basic open neighborhood σN of σ , we have $(\sigma N \cap H') - \{\sigma\} \neq \emptyset$, so $\sigma \in \bar{H}$. Therefore we have $H' \subseteq \bar{H}$, so $H' = \bar{H}$. \square

Now, finally, we are ready to state and prove our generalized fundamental theorem, valid for infinite Galois extensions.

Theorem 6.2. (Fundamental Theorem of Infinite Galois Theory) *Let K be a Galois extension of F , and let $G = \text{Gal}(K/F)$.*

(1) *With the Krull topology on G the maps $E \mapsto \text{Gal}(K/E)$ and $H \mapsto \mathcal{F}(H)$ give an inclusion-reversing correspondence between intermediate fields $K \supseteq E \supseteq F$ and closed subgroups $H \leq G$.*

(2) *If E corresponds to H then the following are equivalent:*

(a) $|G : H| < \infty$;

(b) $[E : F] < \infty$;

(c) H is open.

(3) *If the conditions in (2) are satisfied, then $|G : H| = [E : F]$.*

(4) *For any closed subgroup $H \leq G$ where $H = \text{Gal}(K/E)$, we have $H \triangleleft G$ iff E/F is Galois. If this is the case then there exists a group isomorphism $\theta : \text{Gal}(E/F) \rightarrow G/H$.*

Proof. (1) If $K \supseteq E \supseteq F$ (not necessarily $E \in \mathcal{I}$) then K/E is normal and separable, hence Galois. Thus E is the fixed field of $\text{Gal}(K/E)$ by Theorem 2.2. If $H \leq G$, then Lemma 6.1 shows that $\text{Gal}(K/\mathcal{F}(H)) = \bar{H}$. Thus we have that $H = \text{Gal}(K/E)$ for some $K \supseteq E \supseteq F$ iff H is closed, so the maps $L \mapsto \text{Gal}(K/L)$ and $H \mapsto \mathcal{F}(H)$ give the desired correspondence between intermediate fields and closed subgroups.

(2) ($|G : H| < \infty \Rightarrow H$ is open) Let $K \supseteq E \supseteq F$, $H = \text{Gal}(K/E)$, and suppose $|G : H| < \infty$. Then $G - H$ is a finite union of closed cosets (because H is closed), so H is open.

(H is open $\Rightarrow [E : F] < \infty$) If $H = \text{Gal}(K/E)$ is open then H contains some basic open neighborhood of 1, so $N \subseteq H$ for some $N \in \mathcal{N}$. If $L = \mathcal{F}(N)$ then $E \subseteq L$; $L \in \mathcal{I}$, so $[L : F] < \infty$ and $[L : F] = [L : E][E : F] < \infty$ implies $[E : F] < \infty$.

($[E : F] < \infty \Rightarrow |G : H| < \infty$) Finally, if $[E : F] < \infty$ then choose $L \in \mathcal{I}$ with $E \subseteq L$ (which can always be done by Lemma 3.11), and let $N = \text{Gal}(K/L)$. Then $N \leq H$ since $E \subseteq L$, so $|G : H| \leq |G : N| < \infty$.

(3) If $H = \text{Gal}(K/E)$ is open, then by definition E/F is a finite Galois extension. By Lemma 3.10 we know that $\text{Gal}(E/F) \simeq G/H$, and by Theorem 2.2 equivalence (3) we know that $|\text{Gal}(E/F)| = [E : F]$. Thus $|G : H| = [E : F]$.

(4) Suppose $H \triangleleft G$ is closed in G , so $H = \text{Gal}(K/E)$. Let $\alpha \in E$, and let $f(x)$ be the minimal polynomial of α over F . If $\beta \in K$ is another root of f then there is a $\sigma \in G$ with $\sigma(\alpha) = \beta$. If $\tau \in H$ then $\tau(\beta) = \sigma^{-1}(\sigma\tau\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha) = \beta$ since $\sigma\tau\sigma^{-1} \in H$. Thus β is in the fixed field of H which is E , so f splits over E . Thus E/F is normal, E/F is separable since K/F is, so E/F is Galois.

Conversely if E/F is Galois, then the map $\theta : G \rightarrow \text{Gal}(E/F)$ such that $\theta(\sigma) = \sigma|_E$ is well defined (by Theorem 2.1 because in particular E/F is a normal extension), and $\ker \theta = \text{Gal}(K/E) = H \triangleleft G$. θ is also surjective by Theorem 2.3 so $G/H \simeq \text{Gal}(E/F)$ and we are finished. \square

So it is indeed possible to extend the fundamental theorem of classical Galois theory to infinite algebraic extensions, and the results are quite stunning in their simplicity. The alert reader will note that this new theorem does indeed extend our old theorem, as the following example illustrates.

Example 6.3. If K/F is a Galois extension and $[K : F] < \infty$, then the Krull topology on $\text{Gal}(K/F)$ is discrete. This is because K/F is a finite Galois extension, hence $\text{Gal}(K/K) = \{1\}$ is open. Thus every subgroup of $\text{Gal}(K/F)$ is closed, so we obtain our original bijective correspondence between intermediate fields and subgroups.

We will look at a number of examples of extensions which do not reduce to the finite case in a little while. First, we will convince ourselves that such examples exist and are plentiful in number, which we do in the next section.

7 Absolute Galois Groups

In this section we will explore the notions of ordered fields and real closed fields en route to stating a result concerning the existence of infinite Galois extensions. This discussion leads to the notion of an absolute Galois group, a useful type of Galois group for an infinite Galois extension.

Now that we have defined these Galois groups and established a fundamental theorem for them, an appropriate question to pose is whether this new theorem is at all useful. It could be the case that infinite Galois extensions are rarely encountered, so the study of their Galois groups would be in many ways fruitless. We will state a result due to Artin and Schreier, which tells us that infinite algebraic extensions are actually quite common. First, a few definitions.

Definition 7.1. A field F can be *ordered* if there exists a set $P \subset F$ (the set of positive elements) such that P is closed under addition and multiplication, and F is the disjoint union of the three sets P , $\{0\}$, and $-P = \{-p \mid p \in P\}$.

Of course we call such a field F ordered because we can define a linear ordering on it by declaring for $a, b \in F$ that $a < b$ iff $(b - a) \in P$. We can also deduce more about an ordered field F . It is clear that if $a < b$ (as defined above) then $a + c < b + c$ for every $c \in F$ and $ap < bp$ for every $p \in P$, so $a^2 = (-a)^2 > 0$ for every $a \in F^\times$. This implies that if $\sum_{i=1}^n a_i^2 = 0$ where $a_i \in F$, then each $a_i = 0$. In particular, if each $a_i = 1$ then we obtain that $\sum_{i=1}^n 1 \neq 0$ for all values of n . Thus we see that any ordered field must have characteristic 0. Examples of well known ordered fields are \mathbb{R} and \mathbb{Q} .

Definition 7.2. A field F is *real closed* if F is ordered (with positive element set P), every $x \in P$ has a square root in F , and every polynomial $f(x) \in F[x]$ of odd degree has a root in F .

Examples of real closed fields are \mathbb{R} and $\bar{\mathbb{Q}} \cap \mathbb{R}$. We can basically think of real closed fields as being “almost” algebraically closed. The following theorem makes this statement precise.

Theorem 7.3. A field F is real closed iff $\sqrt{-1} \notin F$ (that is, the polynomial $x^2 + 1$ has no roots in F) and $K = F(\sqrt{-1})$ is algebraically closed.

A proof of Theorem 7.3 can be found in [3] Chapter 11 §2. We now state the result by Artin and Schreier which lends some validation to the study of this infinite Galois theory.

Theorem 7.4. *Let K be an algebraically closed field, $F \subsetneq K$ a proper subfield such that $[K : F] < \infty$. Then F is real closed, and $K = F(\sqrt{-1})$.*

The proof of Theorem 7.4 can be found in [3] Chapter 11 §7. Let us discuss for a moment the importance that Theorem 7.4 has for us. If we pick F in the theorem to be any field and let $K = \bar{F}$, we see that if $[\bar{F} : F] = n < \infty$, then F is a real closed field, $\bar{F} = F(\sqrt{-1})$, and hence $n = 2$. Thus if F is not a real closed field, then it must be the case that $[\bar{F} : F] = \infty$. Of course, there are many fields which fall into the category of non real closed: \mathbb{Q} , \mathbb{F}_p , and $\mathbb{C}(x)$ to name a few. We see that this Galois theory for infinite algebraic extensions is indeed quite useful, since the majority of fields which we encounter are not real closed.

There is another wrinkle in the situation. We know from elementary field theory that every algebraic extension of either a field of characteristic 0 or a finite field is separable. Thus when our field F is in one of these categories, the field extension \bar{F}/F is separable, clearly normal since \bar{F} contains all roots of every polynomial $f(x) \in F[x]$, and hence is Galois. However, there are cases when \bar{F}/F is not a separable extension as we shall see in the following example, so \bar{F}/F cannot be Galois.

Example 7.5. Let $F = \mathbb{F}_2(t)$, where t is transcendental. Then $\sqrt{t} \in \bar{F}$ because \sqrt{t} is a root of the polynomial $x^2 - t$ over F , but $x^2 - t = (x - \sqrt{t})^2$ is not separable. Hence \bar{F}/F is not a separable extension, so it cannot be Galois.

Definition 7.6. Let K/F be a field extension. The *separable closure* of F in K , denoted F_{sep} , is $\{x \in K \mid x \text{ is separable over } F\}$. When F_{sep} is written without reference to a particular extension field K of F , we will mean the separable closure of F in \bar{F} .

Definition 7.7. Let K/F be a field extension. An element $\alpha \in K$ is *inseparable* over F if the minimal polynomial $m_{\alpha,F}(x)$ of α over F has a repeated root. We say α is *purely inseparable* over F if $m_{\alpha,F}(x)$ has only one root, namely α . The extension K/F is also called *purely inseparable* if every $\alpha \in K$ is purely inseparable as above.

Several remarks need to be made about these definitions, most of which are elementary facts from classical field and Galois theory. First of all, it is fairly routine to show that F_{sep} forms a field, so we will not prove it here. Second we note that we only encounter field extensions which are not separable when we are considering fields of characteristic $p > 0$, so of course any purely inseparable extension must be of a field of prime characteristic. It is also not hard to show that if K/F is an extension of fields of characteristic $p > 0$ and $\alpha \in K$ is inseparable over F , then there exists a minimal $n \in \mathbb{N}, n > 0$ and a polynomial $f(x) \in F[x]$ which is separable and irreducible over F such that $m_{\alpha,F}(x) = f(x^{p^n})$. For more details see [7] Chapter I §4. These remarks will be useful in proving the following propositions.

Proposition 7.8. *Let K/F be algebraic, and let F_{sep} denote the separable closure of F in K . Then the extension K/F_{sep} is purely inseparable.*

Proof. If $\alpha \in F_{\text{sep}}$, then $m_{\alpha, F_{\text{sep}}}(x) = x - \alpha$ is clearly purely inseparable. Thus let $\alpha \in K - F_{\text{sep}}$ and consider $m_{\alpha, F_{\text{sep}}}(x)$. From the above remarks there exists $n > 0$ and $f(x) \in F_{\text{sep}}[x]$ separable and irreducible such that $m_{\alpha, F_{\text{sep}}}(x) = f(x^{p^n})$. Let $a = \alpha^{p^n}$. Then $f(a) = 0$ and since f is irreducible we have $f(x) = m_{a, F_{\text{sep}}}(x)$. Also since f is separable we have $a \in F_{\text{sep}}$, so clearly $m_{\alpha, F_{\text{sep}}}(x) = x^{p^n} - a = (x - \alpha)^{p^n}$ (here we are using that the characteristic is $p > 0$) and hence α is purely inseparable over F_{sep} . \square

Proposition 7.9. *Let F be a field, \bar{F} its algebraic closure, and F_{sep} its separable closure in \bar{F} . Then F_{sep}/F is a Galois extension, and $\text{Gal}(\bar{F}/F) \simeq \text{Gal}(F_{\text{sep}}/F)$.*

Proof. Let $\alpha \in F_{\text{sep}}$. Then the minimal polynomial $m_{\alpha, F}(x)$ of α over F has no repeated roots, so if β is also a root of $m_{\alpha, F}(x)$ then $\beta \in F_{\text{sep}}$ as well. Thus $m_{\alpha, F}(x)$ splits over F_{sep} , so F_{sep}/F is a normal extension. Therefore F_{sep}/F is Galois. Now the map $\theta : \text{Gal}(\bar{F}/F) \rightarrow \text{Gal}(F_{\text{sep}}/F)$ given by $\sigma \mapsto \sigma|_{F_{\text{sep}}}$ is a well-defined group homomorphism, and $\ker \theta = \text{Gal}(\bar{F}/F_{\text{sep}})$. For any $\alpha \in \bar{F}$ and any $\tau \in \text{Gal}(\bar{F}/F_{\text{sep}})$, $\tau(\alpha)$ must be a root of $m_{\alpha, F_{\text{sep}}}(x)$. However by Proposition 7.8 we know that α is purely inseparable over F_{sep} , so $m_{\alpha, F_{\text{sep}}}(x)$ has only one root, namely α . Thus $\tau(\alpha) = \alpha$ for all $\alpha \in \bar{F}$, so $\ker \theta = \{1\}$. Finally we have $\text{Gal}(\bar{F}/F) \simeq \text{Gal}(F_{\text{sep}}/F)$. \square

Definition 7.10. The group $G = \text{Gal}(F_{\text{sep}}/F)$ is the *absolute Galois group* of the field F .

More about absolute Galois groups can be found in [7] chapter IV §18. In the next section we will look at several examples of Galois groups of infinite algebraic extensions, many of which will be absolute Galois groups of various fields.

8 Examples

In this section we are finally able to enjoy the fruits of our labors. We will consider infinite Galois extensions of many different types of fields, and compute absolute Galois groups whenever possible. In order to get warmed up, let us first look at a familiar example and apply what we have learned in this paper.

Example 8.1. Let $S = \{\sqrt{p} \mid p \in \mathbb{N} \text{ and } p \text{ is prime}\}$ and $K = \mathbb{Q}(S)$. From the introduction it is known that K/\mathbb{Q} is Galois, and $\text{Gal}(K/\mathbb{Q}) \simeq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. Let us convince ourselves that this is really the projective limit over $\text{Gal}(E/F)$, E/F finite Galois extensions. We clearly have that K is generated by the set $\bigcup_{p \text{ prime}} \mathbb{Q}(\sqrt{p})$. Any intermediate field E , $K \supseteq E \supseteq \mathbb{Q}$ can be written as $E = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ for distinct primes $p_1, \dots, p_n \in \mathbb{N}$. Thus if we order these intermediate fields by \subseteq and $E_1 \leq E_2$, then $E_1 = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$ and $E_2 = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}, \sqrt{q_1}, \dots, \sqrt{q_m})$ for distinct primes $p_1, \dots, p_n, q_1, \dots, q_m \in \mathbb{N}$. Then $\text{Gal}(E_1/\mathbb{Q})$ is a quotient of $\text{Gal}(E_2/\mathbb{Q})$, via the map $\phi : \text{Gal}(E_2/\mathbb{Q}) \rightarrow \text{Gal}(E_1/\mathbb{Q})$ given by $\phi(\sigma) = \sigma|_{E_1}$. From these facts it is easy to see that $\text{Gal}(K/\mathbb{Q}) = \varprojlim_{p \text{ prime}} \text{Gal}(\mathbb{Q}(\sqrt{p})) \simeq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ as before. Note that the fact that $\text{Gal}(K/\mathbb{Q})$ has uncountably many subgroups of index 2, while \mathbb{Q} only has countably many quadratic extensions, does not contradict the fundamental theorem, as “most” of these subgroups of index 2 are not closed in the Krull topology.

Example 8.2. Consider the absolute Galois group of \mathbb{F}_p for any prime p . It is known from classical Galois theory that any algebraic extension of \mathbb{F}_p is separable, hence in particular $\bar{\mathbb{F}}_p$ is a separable extension of \mathbb{F}_p . Thus the absolute Galois group of \mathbb{F}_p is actually $\text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. It is also known from classical Galois theory that for any $n \in \mathbb{N}$, \mathbb{F}_p has a unique Galois extension of degree n (which we call \mathbb{F}_{p^n}) with Galois group $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$, and also that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $m|n$. Thus we let $A = \mathbb{N}$, say $m \leq n$ iff $m|n$, and let $\phi_{n,m} : \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \rightarrow \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ be restriction. That is, $\phi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ sends $a \pmod n$ to $a \pmod m$, and hence $\text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod_{p \in \mathbb{N}, p \text{ is prime}} \mathbb{Z}_p$, also known as $\hat{\mathbb{Z}}$.

The next example makes use of the Kronecker-Weber Theorem, the proof of which is vastly outside the scope of this paper. A proof can be found in [6] Chapter X §3. Recall that an extension of the rational numbers of the form $\mathbb{Q}(\zeta_n)$ for some n th root of unity ζ_n is called a *cyclotomic* extension of \mathbb{Q} .

Theorem 8.3. *Let K/\mathbb{Q} be a finite extension. Then K/\mathbb{Q} is abelian iff K is contained in a cyclotomic extension of \mathbb{Q} .*

Example 8.4. Consider the extension $\mathbb{Q}_{\text{ab}}/\mathbb{Q}$, where \mathbb{Q}_{ab} denotes the maximal extension of \mathbb{Q} which is abelian. The Kronecker-Weber Theorem implies that $\mathbb{Q}_{\text{ab}} = \mathbb{Q}(\{\zeta_n \mid n \in \mathbb{N}\})$. Clearly $\mathbb{Q}(\{\zeta_n \mid n \in \mathbb{N}\})$ is the splitting field of $\{x^n - 1 \mid n \in \mathbb{N}\}$ over \mathbb{Q} , a collection of separable polynomials. Hence $\mathbb{Q}_{\text{ab}}/\mathbb{Q}$ is Galois. For any $\sigma \in G = \text{Gal}(\mathbb{Q}_{\text{ab}}/\mathbb{Q})$, once the value of $\sigma(\zeta_n)$ is known for all $n \in \mathbb{N}$ then σ will be completely determined on all of \mathbb{Q}_{ab} . We know that σ must send a particular ζ_n to a root of its minimal polynomial; that is, $\sigma(\zeta_n) = \zeta_n^k$ for some $k \in \mathbb{N}$ such that $(k, n) = 1$. For fixed $n \in \mathbb{N}$, we know from classical Galois theory that $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$,

the multiplicative group of units of $\mathbb{Z}/n\mathbb{Z}$. We also see that if $m|n$, say $n = md$, then $\zeta_m = \zeta_n^d$. Thus if $\sigma(\zeta_n) = \zeta_n^k$, then $\sigma(\zeta_m) = \sigma(\zeta_n^d) = \sigma(\zeta_n)^d = \zeta_n^{kd} = (\zeta_n^d)^k = \zeta_m^k$. Now if we think of σ as an element of $\varprojlim_{n \in \mathbb{N}} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \varprojlim_{n \in \mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^\times$ (written as $\sigma = (\sigma_n)_{n \in \mathbb{N}}$) we see by the above argument that for $m|n$ we must have $\sigma_n \equiv \sigma_m \pmod{m}$. If we let $A_j = (\mathbb{Z}/j\mathbb{Z})^\times$, partially ordered by $m \leq n$ iff $m|n$, then we have the maps $\phi_{n,m} : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, where $\phi_{n,m}(a \pmod{n}) = a \pmod{m}$. Thus $\text{Gal}(\mathbb{Q}_{\text{ab}}/\mathbb{Q}) \simeq \varprojlim_{n \in \mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^\times$, which is isomorphic to the multiplicative group of units $\hat{\mathbb{Z}}^\times$ of $\hat{\mathbb{Z}}$.

It is important to point out that while the infinite Galois extension $\mathbb{Q}_{\text{ab}}/\mathbb{Q}$ is understood completely, this is not the case for the extension $\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}}$. These are two very important extensions, since any understanding of them would facilitate understanding of the Galois extension $\bar{\mathbb{Q}}/\mathbb{Q}$. In turn, any understanding of the Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ would be indispensable in solving the following problem, which is the topic of much current research.

Inverse Problem of Galois Theory. *Given a finite group G , does there exist a finite Galois extension K of \mathbb{Q} such that $\text{Gal}(K/\mathbb{Q}) \simeq G$?*

More can be read about the Inverse Galois Problem in [12]. Note that a more generalized version of the Inverse Galois Problem can be posed with \mathbb{Q} replaced by any field K . Now let us return to the extension $\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}}$. There is currently a conjecture as to what $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}})$ is as a profinite group. To understand it, we first need the concept of a free profinite group.

Definition 8.5. Let X be a set, G the abstract free group on X . Let $\hat{G} = \varprojlim G/H$ where the projective limit is taken over all $H \triangleleft G$ such that $|G:H| < \infty$ (that is, G/H is a finite group) and H contains all but a finite number of elements in the generating set X . Then \hat{G} is called the *free profinite group* on X .

For a fairly complete basic discussion of free profinite groups, see [13] Chapter 5. We are now ready to state the conjecture mentioned earlier, which is due to Shafarevich. More can be read about it in [5] Chapter VI §14, and more extensive references are given there.

Conjecture 8.6. *Consider the Galois extension $\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}}$. Then $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}})$ is isomorphic to a free profinite group on countably many generators.*

Let us pause for a moment and reflect upon the significance of Conjecture 8.6. It is known from elementary group theory that any group which is generated by n elements is a quotient of the free group on n generators. This fact comes from the universal property of the free group; see [1] Chapter 6 §3. If we let G be the abstract free group on countably many generators, then the free profinite group \hat{G} on countably many generators is the projective limit over all finitely generated

quotients of G . Thus if $\hat{G} \simeq \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}})$ then in particular for any finite group H the projection map $\pi_H : \hat{G} \twoheadrightarrow H$ is a continuous map from $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{ab}})$ onto H (since H is one of the groups over which the projective limit is taken). Thus $\ker \pi_H = \pi_H^{-1}(\{1\})$ is open in \hat{G} , so $\ker \pi_H = \text{Gal}(\bar{\mathbb{Q}}/E)$ for some finite Galois extension E of \mathbb{Q}_{ab} . Then we obtain that $H \simeq \hat{G}/\ker \pi_H \simeq \hat{G}/\text{Gal}(\bar{\mathbb{Q}}/E) \simeq \text{Gal}(E/\mathbb{Q}_{\text{ab}})$, hence the Inverse Galois Problem would have an affirmative answer over \mathbb{Q}_{ab} .

Example 8.7. Now let us consider an example which may seem less natural at first, but which finds its quite natural motivation in the realm of algebraic geometry. Let the base field be $F = \mathbb{C}(x)$, define $S = \{\sqrt[n]{x} \mid n \in \mathbb{N}\}$, and then let $K = F(S)$. Again we have K/F is Galois because K is the splitting field of $\{y^n - x \mid n \in \mathbb{N}\}$ over F , hence normal, and an extension of fields of characteristic 0, hence separable. For each finite extension $K \supseteq E \supseteq F$ where E is of the form $E = F(\sqrt[n]{x})$, $\text{Gal}(E/F) \simeq \mathbb{Z}/n\mathbb{Z}$. This fact comes from Kummer theory of finite Galois extensions. (See [5] Chapter VI §8.) Also if $m|n$, say $n = md$, and $\sigma \in \text{Gal}(K/F)$ is such that $\sigma(\sqrt[n]{x}) = \zeta_n^k \sqrt[n]{x}$, then $\sigma(\sqrt[m]{x}) = \sigma(\sqrt[n]{x^d}) = \sigma(\sqrt[n]{x})^d = \zeta_n^{kd} \sqrt[n]{x^d} = \zeta_m^k \sqrt[m]{x}$. Thus we see that $\text{Gal}(K/F) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z}$, where the indexing set \mathbb{N} is partially ordered via $m \leq n$ iff $m|n$, and for $m \leq n$ we define $\phi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ by $\phi_{n,m}(a \bmod n) = a \bmod m$. Hence again the Galois group is isomorphic to $\hat{\mathbb{Z}}$ as in Example 8.2.

Example 8.7 also has an important geometric interpretation, which we briefly discuss now. The field $\mathbb{C}(x)$ is the function field of the complex projective line $\mathbb{P}^1(\mathbb{C})$ (from now on we will write \mathbb{P}^1 in place of $\mathbb{P}^1(\mathbb{C})$), also known as the Riemann sphere. Any algebraic extension of the field $\mathbb{C}(x)$ (for example, one of the form $\mathbb{C}(x)[\sqrt[n]{x}]$ as above) corresponds to a cover of \mathbb{P}^1 in the algebraic geometric sense; we shall refer to such coverings as *branched coverings*. Each extension of the form $\mathbb{C}(x)[\sqrt[n]{x}] \simeq \mathbb{C}(x)[y]/(y^n - x) \simeq \mathbb{C}(y)$ corresponds to an n -fold branched covering of \mathbb{P}^1 by \mathbb{P}^1 via the map $y \mapsto y^n$, branched only at 0 and ∞ . This branched covering is closely related to a covering that has no branch points, which we shall call just a *covering*. That is, the map $f_n : \mathbb{P}^1 - \{0, \infty\} \rightarrow \mathbb{P}^1 - \{0, \infty\}$ for each $n \in \mathbb{N}$ is a covering map (where $f_n(z) = z^n$ for $z \in \mathbb{P}^1 - \{0, \infty\}$), and $\mathbb{P}^1 - \{0, \infty\}$ is an n -sheeted covering space of $\mathbb{P}^1 - \{0, \infty\}$ under the map f_n . The base space of this covering is also $\mathbb{P}^1 - \{0, \infty\}$, which has as its fundamental group $\pi_1(\mathbb{P}^1 - \{0, \infty\}) = \mathbb{Z}$. See [12] Chapter 4 §1 for more on the terminology in this paragraph. Note that each of the finite Galois groups occurring in Example 8.7 is a quotient of $\pi_1(\mathbb{P}^1 - \{0, \infty\})$, and the profinite completion of $\pi_1(\mathbb{P}^1 - \{0, \infty\})$ is $\hat{\mathbb{Z}}$ as in Example 8.7. These facts are not accidental, as we shall see now.

Given a covering $f : E \rightarrow B$, it is easy to show that the set $\{g : E \rightarrow E \mid g \text{ is a homeomorphism, } f \circ g = f\}$ forms a group under composition of functions, called the group of *deck transformations* of the covering $f : E \rightarrow B$ and written $\text{Deck}(f)$. When E is a connected topological space and $\text{Deck}(f)$ acts transitively on some (and hence each) fiber $f^{-1}(b)$ for $b \in B$, we say that $f : E \rightarrow B$ is a *Galois covering*. The next proposition ties together these definitions with Example 8.7 and

the comments in the the previous paragraph. It is proven in [12] Chapter 4 §1, along with more details concerning the definitions in this paragraph.

Proposition 8.8. *Let $f : E \rightarrow B$ be a Galois covering and $G = \text{Deck}(f)$. Let $e \in E$ and $b = f(e)$. Then there is a unique surjective homomorphism $\Phi_e : \pi_1(B, b) \rightarrow G$ such that $\Phi_e([\gamma])$ maps the endpoint of the lift beginning at the point b of γ (often denoted $[\gamma]b$) to the point b .*

Thus we see from Proposition 8.8 that any group G which occurs as the Galois group of a covering $f : E \rightarrow B$ must be a quotient of the fundamental group of the base space. This geometric point of view is often used in the current research involving Galois theory. The following theorem, which is proved in [12] Chapter 4 §2, is very important in that respect.

Theorem 8.9. (Riemann Existence Theorem) *Let $\mathcal{R} = (G, P, (C_p)_{p \in P})$ be a ramification type, where G is a finite group, P is a finite set of points in \mathbb{P}^1 , for each $p \in P$, C_p is a conjugacy class of G , and $|P| = r$. Then there exists a finite Galois covering of $\mathbb{P}^1 - P$ of ramification type \mathcal{R} iff there exist generators g_1, \dots, g_r of G such that $g_1 \dots g_r = 1$ and $g_i \in C_{p_i}$ for $1 \leq i \leq r$.*

For more details on ramification type, see [12] Chapter 2 §2. An almost immediate corollary of Theorem 8.9 is the following.

Corollary 8.10. *Given any finite group G , there exists a finite Galois extension K of $\mathbb{C}(x)$ such that $G \simeq \text{Gal}(K/\mathbb{C}(x))$*

Corollary 8.10 is proven in the following way. The group generated by r elements g_1, \dots, g_r subject to only the relation that $g_1 \dots g_r = 1$ is the same as the free group on $r - 1$ generators. Thus given a finite group G , we choose r sufficiently large such that G can be generated by $r - 1$ elements, say h_1, \dots, h_{r-1} . Choose distinct points $p_1, \dots, p_r \in \mathbb{P}^1$. Now if we denote the conjugacy class in G of $g \in G$ by $C_G(g)$, then Theorem 8.9 implies that there exists a finite Galois cover of ramification type $(G, P, (C_p)_{p \in P})$ where $P = \{p_1, \dots, p_r\}$, $C_{p_i} = C_G(h_i)$ for $1 \leq i \leq r - 1$ and $C_{p_r} = C_G((h_1 \dots h_{r-1})^{-1})$. This cover corresponds to a Galois field extension $K/\mathbb{C}(x)$ with Galois group G . Thus we see from Theorem 8.10 that the Inverse Galois Problem has an affirmative answer over the field $\mathbb{C}(x)$. Now on to a new example.

Example 8.11. Again let the base field $F = \mathbb{C}(x)$, and let $K = \overline{\mathbb{C}(x)}$ be the algebraic closure of F . Then $\text{Gal}(\overline{\mathbb{C}(x)}/\mathbb{C}(x))$ is the free profinite group on the set

\mathbb{C} . In fact, this result also holds if \mathbb{C} is replaced by an arbitrary algebraically closed field K . Neither of these facts is obvious, and more can be found about them in [13] Chapter 5 §1.

Before we consider the next example, let us establish a few facts.

Definition 8.12. Let F be a field. The *ring of formal Laurent series* over F , denoted $F((x))$, is the collection of all sums of the form $\sum_{n=-m}^{\infty} a_n x^n$ for some $m \in \mathbb{N}$, where each $a_i \in F$.

Addition and multiplication are defined in the ring of formal Laurent series as natural extensions of addition and multiplication of polynomials in the field $F(x)$ of rational functions over F . The 0 in this ring is the series $0 + 0x + 0x^2 + \dots$ and the 1 is the series $1 + 0x + 0x^2 + \dots$. It is clear that under these operations, $F((x))$ forms a ring. We see that a stronger fact is actually true.

Proposition 8.13. *For any field F , $F((x))$ is also a field.*

Proposition 8.13 is proved in [3] Chapter 7 §10. Now that we know that $F((x))$ is a field, we can consider its absolute Galois group. In the case when F is an algebraically closed field of characteristic 0, the field $\overline{F((x))}$ has the following simple description.

Proposition 8.14. *Let F be an algebraically closed field of characteristic 0. Then $\overline{F((x))} = [F((x))](\{\sqrt[n]{x} \mid n \in \mathbb{N}\})$.*

Proposition 8.14 is another fact the proof of which is outside the scope of this paper. See [9] Chapter IV §2 for more details and a proof. Now, finally, we have the proper knowledge to discuss the next example.

Example 8.15. Consider the field $\mathbb{C}((x))$. Since $\mathbb{C}((x))$ has characteristic 0, we know that its absolute Galois group is really just $\text{Gal}(\overline{\mathbb{C}((x))}/\mathbb{C}((x)))$. Proposition 8.14 shows that $\overline{\mathbb{C}((x))} = [\mathbb{C}((x))](\{\sqrt[n]{x} \mid n \in \mathbb{N}\})$. Since each $\sqrt[n]{x}$ has minimal polynomial $y^n - x$ over $\mathbb{C}((x))$, and each $y^n - x$ has roots $\sqrt[n]{x}, \zeta_n \sqrt[n]{x}, \dots, \zeta_n^{n-1} \sqrt[n]{x}$, we see very similarly as in Examples 8.2 and 8.7 that $\text{Gal}(\overline{\mathbb{C}((x))}/\mathbb{C}((x))) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z}$, again also known as $\hat{\mathbb{Z}}$.

There is a theorem which is the analogue of Proposition 8.14 in the case when the field F is algebraically closed of characteristic $p > 0$. It makes use of the concept of a *generalized power series*, which is an expression of the form $\sum_{i \in \mathbb{Q}} a_i t^i$ where $a_i \in F$ and the support of the series (that is, the set of all i such that $a_i \neq 0$) is a well-ordered subset of \mathbb{Q} . The set of generalized power series over a field F ,

under the natural operations of addition and multiplication, forms a ring. The theorem analogous to Proposition 8.14 states that a particular subset of the ring of generalized power series over an algebraically closed field F of characteristic $p > 0$ is the algebraic closure of $F((x))$; see [4] for details.

The next example requires some basic knowledge of the p -adic numbers, an extensive discussion of which can be found in [2].

Example 8.16. The structure of Galois extensions of \mathbb{Q}_p is discussed in detail in [9], and all of the assertions in this example are proved there in Chapter IV §1 and §2. Such extensions are constructed as a tower of three extensions $K \supseteq L \supseteq E \supseteq \mathbb{Q}_p$ in the following manner. The (unramified) extension E/\mathbb{Q}_p has Galois group $\text{Gal}(E/\mathbb{Q}_p) \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. The (tamely ramified) extension L/E has Galois group $\text{Gal}(L/E) \simeq \mathbb{Z}/m\mathbb{Z}$ for m such that $(m, p) = 1$. Finally, the (wildly ramified) extension K/L has Galois group $\text{Gal}(K/L) \simeq P$ where P is a group of order p^k for some $k \in \mathbb{N}$. The Galois group of the extension K/E is a semi-direct product; that is, $\text{Gal}(K/E) \simeq P \rtimes \mathbb{Z}/m\mathbb{Z}$ subject to the constraints above. This characterization tells us that not every group can be realized as a Galois group over \mathbb{Q}_p . For example, the alternating group A_5 is not a Galois group over \mathbb{Q}_p for any p , reasoned as follows. If it were, then it would have to be of the form discussed above. However, the group $\text{Gal}(E/\mathbb{Q}_p)$ is cyclic, which would imply that A_5 has a normal subgroup H such that A_5/H is cyclic. But A_5 is simple, so the only subgroup with this property is $H = A_5$, which implies that $E = \mathbb{Q}_p$. Then since $\text{Gal}(K/E) = \text{Gal}(K/\mathbb{Q}_p)$, A_5 must have a normal subgroup N which is a p -group such that A_5/N is cyclic of order relatively prime to p . The only normal subgroups of A_5 are A_5 and $\{1\}$, and only $\{1\}$ is a p -group. Clearly $A_5/\{1\} \simeq A_5$ is not cyclic, so A_5 is not a Galois group over \mathbb{Q}_p . However, it is the case that every group of the form $P \rtimes \mathbb{Z}/m\mathbb{Z}$ as above occurs as a Galois group over some finite cyclic extension E of \mathbb{Q}_p . From this fact we see that many non-abelian groups occur as Galois groups over \mathbb{Q}_p . Hence \mathbb{Q}_p is an example of a field over which there are many groups that do not occur as Galois groups of extensions, but there are also many groups which do occur. The structure of the absolute Galois group of \mathbb{Q}_p is fairly complicated. In particular, many non-abelian groups are quotients of $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, while A_5 is not.

9 Conclusion

In this paper we began with the basic ideas from classical Galois theory, and built upon them to apply the ideas to infinite Galois field extensions. We saw that the classical fundamental theorem of Galois theory could not be extended without change to the case of infinite Galois extensions. In fact we had to borrow from the subject of topology in order to do so. It is my hope that the example section provided the reader with ample evidence that Infinite Galois theory has many applications.

This theory, while useful in determining information about field extensions, also turns up often in many other branches of mathematics.

References

- [1] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons Inc., New York, 1999.
- [2] Fernando Q. Gouvea. *p-adic Numbers*. Springer-Verlag, New York, 1997.
- [3] Nathan Jacobson. *Basic Algebra II*. W.H. Freeman and Co., New York, 1989.
- [4] Kiran S. Kedlaya. *The Algebraic Closure of the Power Series Field in Positive Characteristic*. on the web at http://front.math.ucdavis.edu/author/Kedlaya-K*, December 1999. manuscript, to appear in Proceedings of the AMS.
- [5] Serge Lang. *Algebra*. Addison-Wesley Publishing Co., Melino Park CA, 1984.
- [6] Serge Lang. *Algebraic Number Theory*. Springer-Verlag, New York, 1986.
- [7] Patrick Morandi. *Field and Galois Theory*. Springer-Verlag, New York, 1996.
- [8] James R. Munkres. *Topology: A First Course*. Prentice-Hall, Englewood Cliffs NJ, 1974.
- [9] Jean Pierre Serre. *Local Fields*. Springer-Verlag, New York, 1979.
- [10] Jean Pierre Serre. *Galois Cohomology*. Springer-Verlag, New York, 1997.
- [11] Stephen S. Shatz. *Profinite Groups, Arithmetic, and Geometry*. Princeton University Press, Princeton NJ, 1972.
- [12] Helmut Volklein. *Groups as Galois Groups: An Introduction*. Cambridge University Press, Cambridge UK, 1996.
- [13] John S. Wilson. *Profinite Groups*. Oxford University Press, Oxford UK, 1998.