Infinite Galois Extensions: The Fundamental Galois Correspondence Theorem

Kyle Mickelson

December 4th, 2023

Contents

1 The Fundamental Theorem for Infinite Galois Extensions

1.1 Introduction

Classical Galois Theory focuses on the bijection between the set of all subgroups of the Galois group and the set of all subfields of the extension containing the base field. A natural question which arises is what occurs in the case where the extension 'looks' and 'feels' like a Galois extension, but is in fact an infinite extension. These are of course the algebraic extensions which are normal and separable, but are not finite.

Consider for instance the subfield E of $\mathbb{R}$ which is obtained by adjoining all square roots of positive rational numbers to $\mathbb{Q}$. It is clear that any such positive rational square root may be written as some combination of square roots of prime numbers. In this way, E may be identified with the splitting field of the set of polynomials $x^2 - p$ for each prime p; i.e., we have

$$E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots) = \bigcup_{p \text{ a prime}} \mathbb{Q}(\sqrt{p})$$

The extension $E/\mathbb{Q}$ is clearly algebraic, and is also normal and separable (for instance E is the splitting field of a set of polynomials in $\mathbb{Q}$, and the minimal polynomial of every element of E over $\mathbb{Q}$ is separable).

In this way, we have constructed a truly (but not technically) 'Galois' extension, which is clearly not finite (rather, E is a countably infinite extension of $\mathbb{Q}$). If we consider, for a moment, the group of automorphisms of E fixing $\mathbb{Q}$, we can easily find that each automorphism, say $\sigma \in \text{Aut}(E/\mathbb{Q})$, is determined by its action on each $\sqrt{p}$ for p a prime. Clearly either $\sigma(\sqrt{p}) = \sqrt{p}$ or $\sigma(\sqrt{p}) = -\sqrt{p}$, so that in general σ^2 is the identity automorphism. There are an infinite number of possible $\sigma \in \text{Aut}(E/\mathbb{Q})$, and hence

$$\text{Aut}(E/\mathbb{Q}) \cong \prod_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

It is a theorem that $\text{Aut}(E/\mathbb{Q})$ has an *uncountably* infinite number of subgroups of index 2. In the spirit of classical Galois theory, one might then ask how many quadratic extensions of $\mathbb{Q}$ exist.

The answer, as it turns out, is that $\mathbb{Q}$ has a *countably* infinite number of quadratic extensions. It would seem that our hope for a nice generalization of classical Galois Theory for the case of infinite 'Galois' extensions has vanished. The issue, as illustrated above, is that the subgroups of the automorphism group of the extension do no correspond bijectively to the intermediate extensions containing the base field. There are, in a sense, 'too many' subgroups of the automorphism group compared to the number of intermediate field extensions.

Is there any hope of reconciling this discrepancy? The answer, thankfully, is a resounding yes, and in order to do so we must turn to topology. Placing the 'correct' topology on the group of automorphisms above allows us to consider a specific subgroups, and relate these specific subgroups (which turn out to be closed in the topology) to the intermediate field extensions containing the base field.

1.2 Infinite Galois Extensions

In order to generalize results from classical Galois theory, it is necessary to first extend the definition of what makes an extension of fields a Galois extension. Indeed, such extensions are commonly defined only for finite algebraic extensions which are normal and separable. In other words, a finite extension of fields K/F is called a *Galois extension*, or K is said to be *Galois* over F, if $|\text{Aut}(K/F)| = [K : F]$.

For our purposes, we relax the requirement that such extensions need be finite. In doing so, we must rework how we deal with the group of automorphisms of K over F having 'enough' elements. First, we recall several definitions and simple theorems regarding separability of field extensions.

Definition. Let K be an arbitrary algebraic extension of k. We call K *separable* over k if every finitely generated subextension of K is separable over k.

Theorem 1.1. Let F be an algebraic extension of k generated over k by a family of elements $\{\alpha_i\}_{i\in I}$. If each α_i is separable over k, then F is separable over k.

Proof. For any $\alpha \in F$, we have $\alpha \in k(\alpha_{i_1}, \ldots, \alpha_{i_n})$. Specifically, any element of F lies in some subextension of K generated by a finite number of elements of the family. Since each α_i is separable over k, by assumption, we know each element of $k(\alpha_{i_1}, \ldots, \alpha_{i_n})$ is separable over k, and so must be the subextension, proving F/k is separable by definition. ■

Now we are ready to state the more general definition of a Galois extension of fields. In the coming theorems we shall see equivalent descriptions of these extensions, and will find that they work nicely with our intuition from the classical theory.

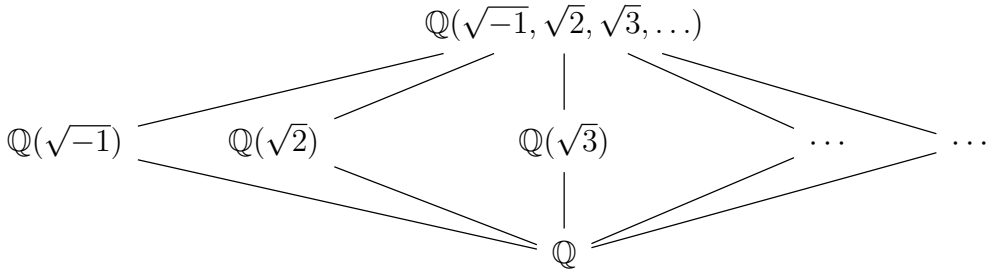
Definition. Let K/k be an algebraic extension of fields, not necessarily a finite extension. If K/k is normal and separable, then we call the extension K/k *Galois*. We may also say that K is *Galois* over k. If K/k is Galois, then we call the group of automorphisms of K fixing k the *Galois group* of K/k, and we write $\text{Aut}(K/k) = \text{Gal}(K/k)$ for this group.

Theorem 1.2. Let K/k be an algebraic extension. Then $K = \bigcup_i K_i$, where $k \subseteq K_i \subseteq K$ and K_i/k is a finite Galois extension for all i, if and only if K/k is a Galois extension.

Proof. Assume $K = \bigcup_i K_i$ with K_i/k a finite Galois extension for all i. We check that K/k is normal and separable, and thus Galois. Let $f(x)$ be an irreducible polynomial in $k[x]$ such that $\alpha \in K$ is a root of $f(x)$. Then $\alpha \in K_i$ for some i, and since K_i/k is normal, $f(x)$ splits completely in $K_i[x]$, hence in $K[x]$ since $K_i \subseteq K$. Thus K/k is normal. Let $F = k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated subextension of K. We have $\alpha_j \in K_i$ for some i. Since K_i/k is separable, α_j is separable over k. In partiular, all elements of F are separable over k, hence F is separable over k. Since F was arbitrary, K/k is separable by Theorem 1.1. ■

Remark 1.2.1. Theorem 1.2 provides a useful way to comprehend infinite Galois extensions: we may view them as the compositum of a family of subextensions which are finite and Galois over the base field.

Example 1.2.2. Consider the infinite extension $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)$ of $\mathbb{Q}$ obtained by adjoining the square root of each prime number, in addition to $i = \sqrt{-1}$. We have a tower of fields:



And it is clear to see that this extension is infinite. In fact, in light of our discussion above, this is an infinite Galois extension. Clearly $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbb{Q}$ is algebraic. Furthermore, by Theorem 1.1 it is separable, and by Theorem 1.2 it is normal. To see this, note

$$\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots) = \mathbb{Q}(\sqrt{-1}) \cup \bigcup_{p \text{ prime}} \mathbb{Q}(\sqrt{p})$$

Each $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is a finite extension which is Galois, having $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. The same holds for the finite extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$.

Now that we have seen an example of an infinite Galois extension, we may begin to wonder whether or not the Galois groups associated to such extensions are infinite, and if so how often this occurs.

In fact, the extension given in Example 1.2.2 can be seen to have an infinite Galois group. To see this, we may note that any automorphism of the form $\sqrt{p} \mapsto -\sqrt{p}$, for any choice of prime p, necessarily fixes $\mathbb{Q}$. In fact, we may string together as many of these maps as we would like, taking square roots of primes to the negative square root, and still recover an automorphism of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)$ fixing $\mathbb{Q}$

As it turns out, every infinite Galois extension has an infinite Galois group, as we shall now see.

Theorem 1.3. Let K/k be an infinite Galois extension. Then the Galois group $\mathrm{Gal}(K/k)$ is an infinite group.

Proof. Assume $|\mathrm{Gal}(K/k)| = n < \infty$. Then there are at most n distinct embeddings of K into an algebraic closure k^a of k. It then follows that for any $\alpha \in K$ the degree of the minimal polynomial for α over k has degree at most n.

Let α be an element of K having maximal degree $[k(\alpha) : k] = m \leq n$. Assume $k(\alpha) \neq K$. Then there exists some $\beta \in K$ such that $\beta \notin k(\alpha)$. Form the extension $k(\alpha, \beta)$. By the primitive element theorem, there exists an element $\gamma \in K$ such that $k(\alpha, \beta) = k(\gamma)$. Then we have the tower of field extensions $k \subseteq k(\alpha) \subseteq k(\gamma)$, and so by the formula for degrees in towers, we have

$$[k(\gamma) : k] = [k(\gamma) : k(\alpha)] \cdot [k(\alpha) : k]$$

Since $k(\alpha) \neq k(\gamma)$, we have $[k(\gamma) : k(\alpha)] > 1$.Then the above gives $[k(\gamma) : k] > m$, a contradiction to the maximality of $[k(\alpha) : k]$. Thus $k(\alpha) = K$ indeed holds, and so K/k is finite. This proves the result by contrapositive. ■

We end this section by giving one more example of an infinite Galois extension.

Example 1.3.1. Fix a prime p. Consider the p-power cyclotomic extension

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n})$$

Since $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is a finite Galois extension for each $n \in \mathbb{N}$, Theorem 1.2 asserts that $\mathbb{Q}(\zeta_{p^\infty})$ is a Galois extension of $\mathbb{Q}$.

1.3 Cosets of Galois Group and Open Sets

Our ultimate aim in reformulating the classical Galois theory to handle infinite extensions will be to place a topology on the Galois group associated to the infinite Galois extension. To this end, we need to consider the 'correct' notion of an open set in this topology.

We shall soon see that this 'correct' notion relies heavily on the fact that the lifting of intermediate extensions inside a Galois extension remains a Galois extension. We prove this fact before proceeding.

Theorem 1.4. Let K/k be an algebraic extension. If K/k is Galois, then K/L is a Galois extension for every intermediate field extension $k \subseteq L \subseteq K$.

Proof. Suppose K/k is Galois and $k \subseteq L \subseteq K$ is a tower of fields. The extension K/k is normal, and normal extensions remain normal under lifting, so that K/L is normal. Likewise, the lift of a separable extension is separable. ■

Now that we have shown the intermediate extensions of an infinite Galois extensions remain Galois under lifting, we are able to make the following definition which will allow us to construct the 'correct' notion of an open set for the topology on the infinite extension.

Definition. Let K/k be a Galois extension. A non-empty subset U of $\text{Gal}(K/k)$ is called *open* if each element of U is contained in a coset of $\text{Gal}(K/F)$ considered as a subgroup of $\text{Gal}(K/k)$, where $k \subseteq F \subseteq K$ is a finite subextension of K, with the coset being contained in U.

To be more specific, the subset U of $\text{Gal}(K/k)$ is open if for all $\sigma \in U$ there exists a finite intermediate extension F/k of K such that $\sigma\text{Gal}(K/F) \subseteq U$.

Remark 1.4.1. In a way that will become clear in view of Theorem 1.5, the open sets of $\text{Gal}(K/k)$ are those containing elements which resemble automorphisms from $\text{Gal}(K/F)$ when restricted to F on some finite subextension F of K containing k.

Theorem 1.5. Let K/k be a Galois extension, and let $\sigma \in \text{Gal}(K/k)$. Let F be a subextension of K which is a finite extension of k. Then

$$\sigma\text{Gal}(K/F) = \{\tau \in \text{Gal}(K/k) \mid \tau|_F = \sigma|_F\}$$

Proof. Let $k \subseteq F \subseteq K$ be a tower, where F/k is a finite extension. Take $\sigma \in \text{Gal}(K/k)$. Since K/k is Galois, the extension is normal, and so remains normal under lifting to K/F, so that we may consider $\text{Gal}(K/F)$. Let $\tau \in \text{Gal}(K/F)$, and take some element $\alpha \in F$. Then $\sigma(\tau(\alpha)) = \sigma(\alpha)$ since τ fixes F, so that $\sigma\tau = \sigma$ upon restriction to F. Conversely, assume $\tau \in \text{Gal}(K/k)$ such that $\tau|_F = \sigma|_F$. Define $\lambda = \sigma^{-1}\tau$. Let $\alpha \in F$, Then

$$\lambda(\alpha) = \sigma^{-1}\tau(\alpha) = \sigma^{-1}(\sigma(\alpha)) = \alpha$$

since $\tau|_F = \sigma|_F$ and $\alpha \in E$. This implies $\lambda \in \text{Gal}(K/F)$, and so we retrieve the relation $\sigma\lambda = \sigma\sigma^{-1}\tau = \tau \in \sigma\text{Gal}(K/F)$, proving the theorem. ■

Example 1.5.1. We present an example of an open set. Consider the infinite Galois extension $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)/\mathbb{Q}$. For notational convenience, we now define $E = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)$. Note that the map sending $\sqrt{p} \mapsto -\sqrt{p}$ for any prime p (or -1) is an automorphism of E which fixes $\mathbb{Q}$, and hence is contained in the Galois group of this extension. Choose one such p and note that $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is a finite subextension of E. From Theorem 1.3, we have

$$\sigma\text{Gal}(E/\mathbb{Q}(\sqrt{p})) = \{\tau \in \text{Gal}(E/\mathbb{Q}) \mid \tau|_{\mathbb{Q}(\sqrt{p})} = \sigma|_{\mathbb{Q}(\sqrt{p})}\}$$

Which is the set of automorphisms in $\text{Gal}(E/\mathbb{Q})$ that send $\sqrt{p} \mapsto -\sqrt{p}$. Since every element of this coset is, in particular, contained in this coset, this set is an open set of $\text{Gal}(E/\mathbb{Q})$.

1.4 The Krull Topology

Before we can proceed with the theory, we must first check to ensure that these appropriately chosen open sets actually do form a topology on the Galois group of an infinite extension.

Theorem 1.6. Let K/k be a Galois extension. Then the collection of open sets, including the empty set, defined in the previous section is a topology on K/k, referred to as the *Krull topology* of the extension.

Proof. Let $\mathcal{T}$ denote the collection of open sets. By construction both $\varnothing$ and $\text{Gal}(K/k)$ are contained in $\mathcal{T}$. Let $\{U_i\}_{i\in I}$ be an arbitrary collection of elements of $\mathcal{T}$. Assume $\sigma \in \bigcup_{i\in I} U_i$. Then $\sigma \in U_i$ for at least one such $i \in I$, and so there exists a finite subextension of K, say F, for which $\sigma \in \sigma\text{Gal}(K/F) \subseteq U_i$. In particular, we have $\sigma\text{Gal}(K/F) \subseteq \bigcup_{i\in I} U_i$. Since σ was arbitrary, the set $\bigcup_{i\in I} U_i$ is open by definition.

Now let $U_1, \ldots, U_m$ be open. If $\sigma \in \bigcap_{i=1}^m U_i$ then $\sigma \in U_i$ for each $i \in \{1, \ldots, m\}$, and so there exist finite subextensions of K, $F_1, \ldots, F_m$, for which $\sigma\text{Gal}(K/F_i) \subseteq U_i$ for each i. Now take F to be the compositum of the F_i. Then $\sigma\text{Gal}(K/F) \subseteq \sigma\text{Gal}(K/F_i)$ for all i. In particular, we have $\sigma\text{Gal}(K/F) \subseteq \bigcap_{i=1}^m U_i$. Since σ was arbitrary, $\bigcap_{i=1}^m U_i$ is an open set by definition.

■

1.5 The Fundamental Theorem for Infinite Galois Extensions

Now we turn our attention to constructing a generalization for infinite Galois extensions similar to the fundamental theorem for finite Galois extensions. As it turns out, we may generalize the fundamental theorem for finite extensions completely and prove a result valid for both finite and infinite extensions. This generalization is not logically independent of the finite case, however, and so is not a complete generalization in that specific sense.

Before moving on to the main theorem, we prove several facts regarding Galois groups associated to intermediate extensions of arbitrary Galois extensions.

Theorem 1.7. Let K/k be a Galois extension equipped with the Krull topology. If L is an intermediate extension of K containing k, then $\text{Gal}(K/L)$ is a closed subgroup of $\text{Gal}(K/k)$.

Proof. We know from Theorem 1.4 that the extension K/L is Galois, with Galois group $\text{Gal}(K/L) \leq \text{Gal}(K/k)$. To prove that $\text{Gal}(K/L)$ is closed, we show that its complement $\text{Gal}(K/k) \setminus \text{Gal}(K/L)$ is open. If $\text{Gal}(K/L) = \text{Gal}(K/k)$, then we are done. So assume this is not the case. Then there exists some automorphism $\sigma \in \text{Gal}(K/k) \setminus \text{Gal}(K/L)$. In particular, σ is an automorphism of K fixing k, and not fixing L. Thus there exists an element $\alpha \in L$ for which $\sigma(\alpha) \neq \alpha$.

We know there exists some finite subextension of K containing α and the base field k, for instance the simple extension $k(\alpha)/k$. Let E denote this finite subextension. From Theorem 1.3, we have:

$$\sigma\text{Gal}(K/E) = \{\tau \in \text{Gal}(K/k) \mid \tau|_E = \sigma|_E\}$$

In particular, since E/k is finite, the set $\sigma\text{Gal}(K/E)$ is open by definition, and clearly contains σ. To prove the claim, we need only show that $\text{Gal}(K/L)$ and $\sigma\text{Gal}(K/E)$ are disjoint, as this will prove that the open set is completely contained in the complement $\text{Gal}(K/k) \setminus \text{Gal}(K/L)$.

To this end, suppose τ is an automorphism contained in both sets. Since $\tau \in \text{Gal}(K/L)$, we know that τ fixes L. However, since $\tau \in \sigma\text{Gal}(K/E)$, we know $\tau|_E = \sigma|_E$, and since $\sigma(\alpha) \neq \alpha$, and $\alpha \in E$, it follows that $\tau(\alpha) \neq \alpha$. By assumption, $\alpha \in L$, and so τ does not fix L, which is a contradiction.

■

Example 1.7.1. Consider once more the extension $E = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)$ of $\mathbb{Q}$, and equip $\text{Gal}(E/\mathbb{Q})$ with the Krull topology. For any prime p, we have a tower $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq E$. In fact, $\mathbb{Q}(\sqrt{p})$ is an intermediate extension of E containing $\mathbb{Q}$, and so by Theorem 1.7, the subgroup $\text{Gal}(E/\mathbb{Q}(\sqrt{p}))$ is closed in $\text{Gal}(E/\mathbb{Q})$.

Before stating the next theorem, we quickly recall the construction of the *fixed field* corresponding to a subgroup of a Galois group. Let K/k be a Galois extension, with $\text{Gal}(K/k)$ its Galois group. If H is a subgroup of $\text{Gal}(K/k)$, then we define the set

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

It is clear that K^H is a field, and in particular contains the base field k of the extension K/k since each element of H by construction fixes k. In this way, we may view K^H as a subextension of K containing k for any subgroup H of the Galois group of K/k.

Theorem 1.8. Let K/k be a Galois extension, and equip the associated Galois group $\text{Gal}(K/k)$ with the Krull topology. If H is a subgroup of $\text{Gal}(K/k)$, then the closure of H in $\text{Gal}(K/k)$ is the subgroup $\text{Gal}(K/K^H)$.

Proof. Let $H \leq \text{Gal}(K/k)$ and let $\overline{H}$ denote its closure. First we show that $H \subseteq \text{Gal}(K/K^H)$. If $\sigma \in H$ then σ fixes all elements of K^H by construction, and so $\sigma \in$

$\text{Gal}(K/K^H)$; hence $H \subseteq \text{Gal}(K/K^H)$. By Theorem 1.7 we have that $\text{Gal}(K/K^H)$ is closed in $\text{Gal}(K/k)$, and hence contains $\overline{H}$ by elementary topology.

To prove the reverse inclusion, namely that $\text{Gal}(K/K^H) \subseteq \overline{H}$, we use the contrapositive. So assume $\sigma \in \text{Gal}(K/k) \setminus \overline{H}$. We know that $\sigma \in \overline{H}$ if and only if open sets containing σ have a non-empty intersection with H. In our case, this implies that there exists some open set of $\text{Gal}(K/k)$, say U, which contains σ and satisfies $U \cap H = \varnothing$. By definition, there exists some finite subextension of K, say F, for which $\sigma\text{Gal}(K/F) \subseteq U$, and hence $\sigma\text{Gal}(K/F) \cap H = \varnothing$. Let $E \supseteq F$ be the Galois closure of F, which is also a finite extension of k. Since $F \subseteq E$, we know $\text{Gal}(K/E) \subseteq \text{Gal}(K/F)$, and so $\sigma\text{Gal}(K/E) \cap H = \varnothing$ also.

Now we use the above information to show that $\sigma \notin \text{Gal}(K/K^H)$. Since E is the Galois closure of F, we know E/k is Galois. In particular, this means that $\text{Gal}(E/k)$ is a subgroup of $\text{Gal}(K/k)$, and hence we have a natural surjective group homomorphism

$$\Phi : \text{Gal}(K/k) \to \text{Gal}(E/k)$$

which is the restriction of the identity map on $\text{Gal}(K/k)$ to E; i.e., we have $\Phi(\varphi) = \varphi|_E$ for all $\varphi \in \text{Gal}(K/k)$. In particular, consider the image of σ and H under the map Φ. By assumption we have $\sigma\text{Gal}(K/E) \cap H = \varnothing$, and so there exists no $\tau \in H$ for which $\tau|_E = \sigma|_E$. But $\Phi(\sigma) = \sigma|_E$, and so we require $\sigma|_E \notin \Phi(H)$.

Now consider the fixed field $E^{\Phi(H)}$, which is contained in K^H. From finite Galois theory, for instance Corollary 14.11 in Dummit and Foote, every automorphism of the field E fixing $E^{\Phi(H)}$ is contained in $\Phi(H)$. In particular, the fact that $\sigma \notin \Phi(H)$ implies that σ does not fix E^H, and so does not fix some element $\alpha \in E^{\Phi(H)} \subseteq K^H$. However, this implies that σ does not fix K^H, and thus $\sigma \notin \text{Gal}(K/K^H)$.

We have shown that $\sigma \notin \overline{H}$ implies $\sigma \notin \text{Gal}(K/K^H)$, and so the contrapostiive statement gives us $\sigma \in \text{Gal}(K/K^H)$ implies $\sigma \in \overline{H}$, to which $\text{Gal}(K/K^H) \subseteq \overline{H}$. This inclusion, and the reverse shown previously, allow us to conclude that $\overline{H} = \text{Gal}(K/K^H)$, as desired.

■

Example 1.8.1. Once more consider $E = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \ldots)$ as an extension of $\mathbb{Q}$. As we saw before, the subgroup $\text{Gal}(E/\mathbb{Q}(\sqrt{p}))$ is closed in $\text{Gal}(E/\mathbb{Q})$ for any prime p. Let $H = \text{Gal}(E/\mathbb{Q}(\sqrt{p}))$. Since H is closed, it follows from Theorem 1.8 that $H = \overline{H}$, with $\overline{H} = \text{Gal}(E/E^H)$. In particular,

$$\text{Gal}(E/\mathbb{Q}(\sqrt{p})) = \text{Gal}(E/E^H)$$

The subgroup on the left consists of automorphisms of E which fix $\mathbb{Q}(\sqrt{p})$, and so in particular fix $\mathbb{Q}$ and $\sqrt{p}$. The subgroup on the right consists of automorphisms of E which fix every element of E fixed by $\text{Gal}(E/\mathbb{Q}(\sqrt{p}))$.

Equipped with the theorems above, we are now ready to state and prove the fundamental theorem for infinite Galois theory. The proof shall use many of the theorems we have proved thus far, and will attempt to illustrate key ideas and concepts clearly and explicitly where confusion may arise.

Theorem 1.9. Let K be a Galois extension of k and set $G = \text{Gal}(K/k)$. Then there is a bijection

$$\{\text{subfields } L \text{ of } K \text{ containing } k\} \longleftrightarrow \{\text{closed subgroups } H \text{ of } G\}$$

given by the correspondence

$$\begin{aligned} L &\longmapsto \text{Gal}(K/L) \\ L^H &\longmapsfrom H \end{aligned}$$

which are inverses to each other. Under this correspondence,

(1) (inclusion-reversing) If L_1, L_2 correspond to H_1, H_2, respectively, then $L_1 \subseteq L_2$ if and only if $H_2 \leq H_1$.

(2) A closed subgroup H of G is open if and only if K^H has finite degree over k. In this case, we have $[K^H : k] = [G : H]$:

$$\begin{array}{c} K \\ \Big| {\scriptstyle |H|} \\ K^H \\ \Big| {\scriptstyle [G:H]} \\ k \end{array}$$

(3) K/L is always Galois, with Galois group $\text{Gal}(K/L) = H$:

$$\begin{array}{c} K \\ \Big| {\scriptstyle H} \\ L \end{array}$$

(4) A closed subgroup H of G is normal if and only if K^H is Galois over k, in which case we have the isomorphism of groups:

$$\text{Gal}(K^H/k) \cong G/H$$

Proof. First we shall establish the correspondence. Let L be a subextension of K containing k. From Theorem 1.4 we know that K/L is Galois. In fact, the subgroup $\text{Gal}(K/L)$ is a closed subgroup of $\text{Gal}(K/k)$ by Theorem 1.7. Now we must show that sending $\text{Gal}(K/L)$ to $K^{\text{Gal}(K/L)}$ returns L. In other words, we prove that $L = K^{\text{Gal}(L/K)}$. One inclusion is clear: namely that $L \subseteq K^{\text{Gal}(K/L)}$. For the reverse containment, we use the contrapositive statement. Assume $\alpha \in K \setminus L$. Since K/L is Galois, we know from Theorem 1.2 that there exists some finite subextension of K containing L, say F, which is Galois and satisfies $\alpha \in F$.

Since $\alpha \in K \setminus L$, we have $L(\alpha) \neq L$, to which $[L(\alpha) : L] > 1$. Thus the minimal polynomial for α over L has degree greater than or equal to 2; let β be another root of this polynomial. Clearly $\beta \in F$ since F/L is Galois. In particular, we have an isomorphism $\varphi : F \to F$ taking $\alpha \mapsto \beta$, which fixes L, where $\varphi \in \text{Gal}(F/L)$. We may extend this isomorphism φ to an isomorphism $\sigma : K \to K$ which fixes L, see for instance Theorem 13.27 in Dummit and Foote. Thus we have $\sigma \in \text{Gal}(K/L)$. In particular, we have $\sigma(\alpha) \neq \alpha$, since $\sigma(\alpha) = \beta$, and we assumed $\beta \neq \alpha$ was a distinct root. This implies that $\alpha \notin K^{\text{Gal}(K/L)}$, and so by the contrapositive statement we are done.

Now we shall show the reverse direction in the correspondence. Let H be a closed subgroup of $\text{Gal}(K/k)$. The extension K/K^H is Galois, and from Theorem 1.8, we know that $\overline{H} = \text{Gal}(K/K^H)$. Since H is closed, we have $H = \overline{H}$, and hence $H = \text{Gal}(K/K^H)$ also holds. In this way, taking H to K^H returns H, and so the correspondence is proven to hold.

(1) Let H_1 and H_2 be subgroups of $\text{Gal}(K/k)$, and suppose $H_1 \subseteq H_2$. Then, under the correspondence, we have the fixed fields K^{H_1} and K^{H_2}, and clearly $K^{H_2} \subseteq K^{H_1}$. To see this, note that if $\alpha \in K^{H_2}$ then $\tau(\alpha) = \alpha$ for all $\tau \in H_2$ by construction, and since $H_1 \subseteq H_2$, we have $\alpha \in K^{H_1}$. Furthermore, if $K^{H_2} \subseteq K^{H_1}$, then we have $\text{Gal}(K/K^{H_1}) \subseteq \text{Gal}(K/K^{H_2})$, following since if $\tau \in \text{Gal}(K/K^{H_1})$ then τ fixes K^{H_1}, and so fixes the subset K^{H_2}.

(2) Let H be a closed subgroup of $\text{Gal}(K/k)$. Suppose H is open. Then there exists some finite subextension of K, say F, such that $\text{Gal}(K/F) \subseteq H$, which is an open set containing the identity automorphism. The Galois correspondence gives us that $H \mapsto K^H$, and so we may identify $H = \text{Gal}(K/K^H)$. By (1), the correspondence reverses containments, so since we have $\text{Gal}(K/F) \subseteq \text{Gal}(K/K^H)$, this gives $K^H \subseteq F$. The fact that F/k is finite implies K^H/k is finite, since we have a tower $k \subseteq K^H \subseteq F \subseteq K$. The converse statement is trivial via the correspondence ($\sigma\text{Gal}(K/K^H) \subseteq H$ for all $\sigma \in H$). Furthermore, $[K^H : k] = [G : H]$ is a consequence of (4).

(3) This condition is immediate from Theorem 1.4.

(4) Let H be a closed subgroup of $\text{Gal}(K/k)$, with corresponding subextension K^H. First, we show that $\sigma H \sigma^{-1}$ corresponds to $\sigma(K^H)$. If $\tau \in \text{Gal}(K/k)$ and $\alpha \in K$,

then $\tau(\alpha) = \alpha$ if and only if

$$\sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma(\tau(\alpha)) = \sigma(\alpha)$$

for all $\sigma \in \text{Gal}(K/k)$. In particular, we have shown that $\sigma H\sigma^{-1}$ fixes $\sigma(K^H)$ since every element of H fixes K^H by construction, and conversely any element of $\text{Gal}(K/k)$ fixing $\sigma(K^H)$ lies in $\sigma H\sigma^{-1}$. Hence $\sigma H\sigma^{-1} = \text{Gal}(K/\sigma(K^H))$.

Now if we suppose H is normal in $\text{Gal}(K/k)$, then $\sigma H\sigma^{-1} = H$, and so we have $H = \text{Gal}(K/\sigma(K^H))$; however by the bijective correspondence we have $H = \text{Gal}(K/K^H)$, and so this means that $\sigma(K^H) = K^H$. Now we aim to show that this occurs if and only if K^H/k is Galois. Clearly K^H/k is separable, as we have K/k separable. It suffices to show that K^H/k is normal. Suppose $f(x) \in k[x]$ is an irreducible polynomial with a root in K^H, say α. Since K/k is Galois, we know there are $n = \deg(f(x))$ distinct roots $\alpha_1, \ldots, \alpha_n$ in K. There is an isomorphism $\varphi : k[\alpha] \to k[\alpha_i]$ for each $i \in \{1, \ldots, n\}$, which sends $\alpha \mapsto \alpha_i$ and fixes k, and we may extend this to an isomorphism $\sigma : K \to K$ which fixes k. Since $\sigma(K^H) = K^H$ and $k \subseteq K^H$, we know that $\alpha_i \in K^H$ for each i. In particular, f splits completely in $K^H[x]$ since each root of f lies in K^H. Thus K^H/k is normal, and so Galois. In particular, we obtain:

$$\text{Gal}(K/k)/\text{Gal}(K/K^H) \cong \text{Gal}(K^H/k)$$

in a similar fashion to the fundamental theorem for finite Galois theory. ■

1.6 References

Several times throughout this paper I mentioned specific theorems from the wonderful textbook *Abstract Algebra* by Dummit and Foote (3rd Edition). I also referenced Dummit and Foote for the introduction, as they had a wonderful presentaton of the central problem with generalizing to the infinite case. I also heavily used Keith Conrad's expository paper on Infinite Galois extensions. The final reference would be J.S. Milne's notes on Field and Galois Theory; specifically his chapter on infinite Galois extensions.