An Introduction to Infinite Galois Theory

Krishna Dhulipala
Euler Circle

June 7, 2020

Abstract

The Fundamental Theorem of Classical Galois Theory shows that for finite Galois extensions E/F, there exists a one-to-one correspondence between the intermediate fields of this extension and the subgroups of the Galois group $\mathrm{Gal}(E/F)$. This theorem, however, reveals nothing about the nature of *infinite* Galois extensions. It is natural to wonder, therefore, when, if at all, the Classical Galois Correspondence holds for infinite fields. After introducing some preliminaries involving topology and category theory, this paper will examine the nature of infinite Galois extensions as inverse limits equipped with the *Krull Topology*, which enables the use of the sophisticated techniques used in Classical Galois Theory.

1 The Finite Galois Correspondence

Theorem 1.1. The Fundamental Theorem of Finite Galois Theory Suppose E/F is a finite Galois extension, and let $\mathrm{Gal}(E/F)$ be its corresponding Galois group. Then, consider the following map:

$$\begin{aligned}\Phi : \{H \leq \mathrm{Gal}(E/F)\} &\to \{K \mid F/K/E\} \\ H &\mapsto E^H,\end{aligned}$$

and the map

$$\begin{aligned}\Psi : \{K \mid F/K/E\} &\to \{H \leq \mathrm{Gal}(E/F)\} \\ K &\mapsto \mathrm{Gal}(E/K).\end{aligned}$$

Then, the following properties hold:

(i) $\Phi \circ \Psi = e$, and Φ is onto, while Ψ is one-to-one.

(ii) If the field extension E/F is *finite*, then both Φ and Ψ are bijective, from which it follows that $\Phi \circ \Psi = \Psi \circ \Phi = e$.

(iii) Suppose there exists the tower $E/K/F$ for some intermediate field K. Then the extension K/F is normal iff $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$.

Proof.

(i) Suppose that K is the intermediate field of the extension E/F. We shall show that E/K is Galois, from which it follows that $H = \mathrm{Aut}_K(E)$ is in fact a Galois group. The normality of E/F extends to the normality of E/K, so showing the separability of E/K will suffice. Consider some element $a \in E$ and the maximal set of elements $f_1, f_2, \ldots, f_n \in H$ such that each for all $i \in (1, n)$, the functions $f_i(a)$ are pairwise different to each other.[1] Let us observe the polynomial given by the factorization

$$z = \prod_{i=1}^{n} (x - f_i(a)) .$$

We know that f creates a bijective mapping from $\{f_1(a), \ldots, f_r(a)\}$ onto itself. As a consequence, the coefficients of z are fixed under H. It follows from this result that z must be a separable polynomial in the field $K(x)$, and must have the root a. Thus, all elements a from E are separable over K, proving that the extension E/K is indeed Galois.

It suffices to show that $E^H = K$. We already know that K is a subfield of E^H. To proceed, AFSOC that$K \neq E^H$. Then, there exists some $a \in E^H/K$ with some minimal polynomial with degree at least 2. Since $a \in E$ is separable over K, there must exist some $b \neq a$ and some $f \in H$ such that $f(a) = b$. However, this contradicts the fact that Φ is fixed under H. Thus, $E^H = K$, and $\Phi \circ \Psi = e$. ■

(ii) Suppose that $H \leq \mathrm{Gal}(E/F)$. Due to the fact that E/F is a *finite* extension, both $\mathrm{Gal}(E/F)$ and H are finite as well. Now, since E/K is finite and separable there exists a primitive element $a \in E$. Then, by the argument provided from the first property, it follows that

$$[E : E^H] = [E^H(a) : E^H] \leq |H|.$$

Since H fixes the elements in E^H, it is then a subgroup of $\mathrm{Gal}(E/E^H) = \mathrm{Aut}_{E^H}(E)$. However, we are aware that

$$|\,\mathrm{Gal}(E/K)| = [E : K] \leq |H|,$$

which means that $\mathrm{Gal}(E/K)$ must be equal to H, implying in turn that $\Psi \circ \Phi$ is also equal to the identity function e. ■

(iii) Suppose the extension K/F (or equivalently E^H/F) is normal. Then, consider the following map:

$$\begin{aligned} \alpha : \mathrm{Gal}(E/F) &\to \mathrm{Gal}\left(E^H/F\right) \\ f &\mapsto f|_{E^H} \end{aligned}$$

Note that this mapping is in fact a surjective group homomorphism with $\ker(\alpha) = H$. Hence, it follows that $H \lhd \mathrm{Gal}(E/F)$.

[1] Note that such a set of functions from H always exists, because the element $a \in E$ is algebraic over K.

Now let us begin by supposing that H is a normal subgroup of $\mathrm{Gal}(E/F)$. In order to prove that the extension K/F is normal, we must show that any homomorphism $f : E^H \to \bar{E}$ [2] is mapped into E^H. Since the extension E/F is normal, it follows that $f\left(E^H\right) \subseteq E$. Then, let us take some $y \in f\left(E^H\right)$ such that $f(x) = y$. Now, let us take some $h \in H$. Due to the fact that $H \lhd \mathrm{Gal}(E/F)$, there must exist some $n \in H$ such that $hf = fn$ and $h(y) = hf(x) = fn(x) = f(x) = y$. Thus, we know that $y \in E^H$, from which it follows that $f\left(E^H\right) \subseteq E^H$.

■

Lemma 1.2. *Let E/F be some field extension. Then, E/F is a Galois extension if and only if it is a union of finite Galois extensions.*

Proof. Suppose that the field E were a union of finite Galois extensions. Automatically, E is the composite field of these extensions. Since normality and separability extend to composite fields of already normal and separable fields, the extension E/F must also be Galois.

Now, suppose that the extension E/F were Galois. Then, let K be the intermediate field of this extension. Then, the extension K/F is Galois as well. Then, it is possible to rewrite the intermediate field K as $F(\theta)$ for some θ in E because of the separability of K/F. This result is accomplished by using Artin's theorem on primitive elements. Suppose that ϕ is the minimal polynomial of θ over the field F; it follows then that the splitting field of ϕ, which is in fact a finite Galois extension over F, contains K. Due to the fact that every θ from E is located within its respective intermediate field K, E is the union of each intermediate field's respective splitting field. Thus, the Galois extension E/F is a union of finite Galois extensions. ■

That we are able to describe large Galois extensions as a union of constituent Galois extensions is essential. The previous lemma inspires the notion that with the correct set of finite Galois extensions arranged in the appropriate order, one may be able to describe infinite Galois extensions. In this spirit, we can construct the infinitely long tower of fields $E/\ldots/K_3/K_2/K_1/F$[3], in which each K_i is finite Galois over the previous field. In order to describe $\mathrm{Gal}(E/F)$, we will need to take some sort of limit, which will be accomplished using the theory of inverse limits. Before we introduce these useful tools, however, we must establish some important preliminaries.

2 A Categorical Approach to Inverse Limits

Definition 2.1. (Category) A Category $\mathscr{C}$ is a collection consisting of *objects* and *morphisms*. The set of objects from $\mathscr{C}$ is denoted $\mathrm{Ob}(\mathscr{C})$, while the set of morphisms is denoted $\mathrm{Ar}(\mathscr{C})$, which stands for *arrows*. For any $\Phi, \Psi \in \mathrm{Ob}(\mathscr{C})$, there must exist a set of morphisms from Φ to Ψ denoted $\mathrm{Mor}(\Phi, \Psi)$, for which the following properties are true:

[2] Here, $\bar{E}$ represents the algebraic closure of the field E.

[3] For a nicely illustrated diagram of the homomorphisms between Galois groups generated by this tower of fields, refer to [4]

(i) For any function $z \in \mathrm{Ar}(\mathscr{C})$, there exist unique objects Φ and Ψ such that $z \in \mathrm{Mor}(\Phi, \Psi)$.

(ii) There always exists the *identity morphism*, which returns the same morphism under function composition.

(iii) Function composition is associative.

Definition 2.2. (Poset) A partially ordered set, or a *poset* for short, is some set A together with some binary relation $\leq$ on A for which the following properties hold:

(i) For all $a \in A$, a is related to itself, or $a \leq a$.

(ii) For three elements $a, b, c \in A$, the binary relation is transitive, or $a \leq b$ together with $b \leq c$ implies $a \leq c$.

(iii) If $x \leq y$ and $y \leq x$, then x must be equal to y.

Posets are often represented with the notation $\langle A, \leq \rangle$. This notation will be used for the remainder of the paper.

Definition 2.3. (Directed Set) A *directed set* is a poset $\langle X, \leq \rangle$ if for all $x, y \in X$, there exists some $z \in X$ such that $x \leq z$ and $y \leq z$. In other words, there must exist some upper bound in X for all pairs of elements in X.

Definition 2.4. (Inverse System) Let $\mathscr{C}$ be a category, and let $\langle X, \leq \rangle$ be a directed set. Then, let $\{A_x \mid x \in X\}$ be a family of objects indexed by X, and let $f_i^j : A_j \to A_i$ for $i \leq j$ be a homomorphism such that $f_i^i = \mathrm{Id}_{A_i}$, and $f_i^j \circ f_j^k = f_i^k$ for all $i \leq j \leq k$. Then, an *inverse system* of $\mathscr{C}$ consists of objects from $\{A_x \mid x \in X\}$ together with morphisms $f_i^j : A_j \to A_i$ such that $i \leq j$. From now on, we shall discuss inverse systems using $\langle X, \{A_i\}, \{f_{ji}\} \rangle$, where X is the directed set from which indices are drawn, A_i is the family of objects taking indices from X, and f_{ji} are the aforementioned morphisms.

Definition 2.5. (Compatible Family) Let $\langle A_i, fi, j \rangle$ be an inverse system of the category $\mathscr{C}$ which takes indices from X, and $O \in \mathrm{Ob}(\mathscr{C})$. Then, the family of arrows of $\mathscr{C}$ given by $\{g_x : O \longrightarrow A_x | x \in X\}$ is called a *compatible family* if the following maps are commutative together:

(i) $O \xrightarrow{g_j} A_j$

(ii) $A_j \xrightarrow{f_{ji}} A_i$

(iii) $O \xrightarrow{g_i} A_i$

Definition 2.6. (Inverse Limit)[4] Let $\mathscr{C}$ be a category and $\langle X, \{A_i\}, \{f_{ji}\} \rangle$ be an inverse system in $\mathscr{C}$. Then, the object $A \in \mathrm{Ob}(\mathscr{C})$ along with a compatible family of arrows of $\mathscr{C}$

[4]This definition of inverse limits is one of many. For a deeper look at compatible families and a visualization of the maps provided in this definition, see [3].

given by $\{f_x : A \to A_x\}$ is said to be an *inverse limit* of this system if the following property holds:

Let $O \in \mathrm{Ob}(\mathscr{C})$. Then, whenever the family of arrows of $\mathscr{C}$ given by $\{h_x : O \to A_x\}$ is compatible, there must exist a unique arrow h in the category given by $h : O \to A$ that makes the following maps commute together:

(i) $O \xrightarrow{h} A$

(ii) $A \xrightarrow{f_i} A_i$

(iii) $O \xrightarrow{h_i} A_i$

Inverse limits are also called *projective limits*, and also admit the alternative definition as a subgroup:

$$A = \varprojlim A_i = \left\{ a_o \in \prod_{A_i} \mid f_{ji}(a_j) = a_i, \ \ \forall i \leq j \right\}$$

Now that we have introduced the method of taking inverse limits, we are one step closer to approximating an infinite Galois extension $\mathrm{Gal}(E/F)$ using a union of finite Galois extensions. Before we accomplish this, however, we must first understand a few things about topological groups.

3 A Foray into Topological Groups

It is necessary during the study of Galois Groups to define a *topology* over certain groups. In the case of Galois Theory, topological groups are essential, for they provide a means of examining infinite Galois extensions. In this section, we shall define the basic objects which arise in the study of topological groups.[5]

Definition 3.1. (Topological Group) A group G is called a *Topological Group* if it is a topological space and if $G \times G$ has the *Product Topology*. This topology is characterized by the following group structure: both the multiplication map $G \times G \to G$ and the inverse map given by $G \to G : g \mapsto g^{-1}$ must be continuous.

Definition 3.2. (Krull Topology) Suppose that E/F is a Galois extension. Then, for some $\sigma \in \mathrm{Gal}(E/F)$, we shall define the *neighborhood basis* of σ as the sets $\sigma\,\mathrm{Gal}(E/K)$, where K/F runs through all finite Galois extensions of F in E. A topology is induced in the process, which is called the *Krull Topology*.

[5]For a deeper look into the interplay between projective limits and topological groups, refer to [1].

4 The Infinite Galois Correspondence

Having understood the preliminaries of inverse limits and the Krull topology, we will be able to make use of the following useful result.

Theorem 4.1. Suppose that E/F were a Galois extension, and let K_i for i in a directed set I be intermediate fields $K_i \leq E$, which are finite Galois with respect to the field F. Now, let us rename $\mathrm{Gal}(E/F)$ to G, and $\mathrm{Gal}(K_i/F)$ to G_i. Then, for all intermediate fields $K_i \leq K_j$, let us define the following morphisms:

$$f_i^j : G_j \to G_i$$
$$\tau \mapsto \tau|_{K_i}$$

Then, the Galois group $\mathrm{Gal}(E/F)$ is isomorphic to $\varprojlim G_i$, together with the projections $f_i(\tau) = \tau|_{K_i}$. [6]

Lemma 4.2. Suppose that E/F were a Galois extension, and let $H \leq \mathrm{Gal}(E/F)$. Then $\mathrm{Gal}\left(E/E^H\right) = \bar{H}$.[7]

Proof. Let us begin by noting that $H \leq \mathrm{Gal}\left(E/E^H\right)$, since, by definition, H fixes E^H. Now, suppose that (K_i) (for i in some directed set I) were the family of intermediate fields of E^H/F such that, for all $i \in I$, K_i/F were a finite Galois extension. Due to the fact that $\mathrm{Gal}\left(E/K_i\right)$ is an open subgroup of $\mathrm{Gal}(E/F)$, it is also closed. Noting this, we know that

$$\mathrm{Gal}\left(E/E^H\right) = \bigcap_{i \in I} \mathrm{Gal}\left(E/K_i\right)$$

is closed as well. We must determine, however, why H is dense in $\mathrm{Gal}\left(E/E^H\right)$. First, let us take some element p from $\mathrm{Gal}\left(E/E^H\right)$. As a consequence, all neighborhoods of p must contain some $p\,\mathrm{Gal}(E/K_i)$. Next, we shall show that there exists some $q \in H \bigcap p\,\mathrm{Gal}(E/K)$ equivalent to $q|_{K_i} = p|_{K_i}$. We begin by supposing that $H_{K_i} = \{h|_{K_i} \in \mathrm{Gal}(K_i/F) : h \in H\}$. Now, by the fundamental finite Galois theorem, we know that $H_{K_i} = \mathrm{Gal}\left(K_i/K_i^{H_{K_i}}\right)$, from which it follows that $p|_K \in H_{K_i}$. Thus, we have proven that q exists, and also that H is dense in $\mathrm{Gal}\left(E/E^H\right)$, which proves the result. [8] ■

Theorem 4.3. The Fundamental of Theorem of Infinite Galois Theory

Suppose that E/F were a Galois extension, and let us rename $\mathrm{Gal}(E/F)$ to G. Now, consider the maps given by

$$\Phi : \{H \leq G : H = \bar{H}\} \to \{K : F \leq K \leq E\}$$
$$H \mapsto E^H$$

[6] The proof of this theorem goes beyond the scope of this paper.

[7] The bar atop the field H represents the closure of the field H in the Krull topology on $\mathrm{Gal}(E/F)$.

[8] This proof relies heavily on the one provided in [2].

and

$$\Psi : \{K : F \leq K \leq E\} \to \{H \leq G : H = \bar{H}\}$$
$$K \mapsto Gal(E/K)$$

Then, Φ and Ψ are both bijective and inverse to each other, and if H is open, then E^H/F is finite, and H is also closed.

Proof. That Φ and Ψ are bijective and inverse to each other follows directly from Lemma 4.2 together with Fundamental Theorem of Finite Galois Theory. We shall begin proving the second statement by first supposing that H were a clopen[9] subgroup of G, since all open subgroups of topological groups are also closed. Let us note that an open neighborhood of the identity exists within H. This implies that there exists a field K for which Gal(E/K) is a subgroup of H, and the extension K/F is finite. Thus, $E^H \subset K$, from which it follows that the field extension E^H/F is indeed finite. If we begin instead by supposing that E^H/F is finite and H is closed, then we know that H has finite index in G, meaning that it is open, thus completing the proof. ■

References

[1] H. Liu. Infinite galois theory. 4 2016.

[2] J. Preininger. Infinite galois theory. Master's thesis, Universitat Wien, 2011.

[3] I. S. Rodríguez. Infinite galois theory. Master's thesis, Universitat de Barcelona, 2018.

[4] J. Ruiter. Infintie galois theory, 10 2019. Seminar notes.

[9] Here, "clopen" is a portmanteau of the words "closed" and "open", and means both closed and open.