Infinite Galois Theory

Haoran Liu

May 1, 2016

1 Introduction

For an finite Galois extension E/F, the fundamental theorem of Galois Theory establishes an one-to-one correspondence between the intermediate fields of E/F and the subgroups of $Gal(E/F)$, the Galois group of the extension. With this correspondence, we can examine the the finite field extension by using the well-established group theory.

Naturally, we wonder if this correspondence still holds if the Galois extension E/F is infinite. It is very tempting to assume the one-to-one correspondence still exists. Unfortunately, there is not necessary a correspondence between the intermediate fields of E/F and the subgroups of $Gal(E/F)$ when E/F is a infinite Galois extension. It will be illustrated in the following example.

Example 1.1. Let F be $\mathbb{Q}$, and E be the splitting field of a set of polynomials in the form of $x^2 - p$, where p is a prime number in $\mathbb{Z}^+$. Since each automorphism of E that fixes F is determined by the square root of a prime, thus$Aut(E/F)$ is a infinite dimensional vector space over F_2. Since the number of homomorphisms from $Aut(E/F)$ to F_2 is uncountable, which means that there are uncountably many subgroups of $Aut(E/F)$ with index 2. while the number of subfields of E that have degree 2 over F is countable, thus there is no bijection between the set of all subfields of E containing F and the set of all subgroups of $Gal(E/F)$.

Since a infinite Galois group $Gal(E/F)$normally have "too much" subgroups, there is no subfield of E containing F can correspond to most of its subgroups. Therefore, it is necessary to find a way to only look at the relevant subgroups of the infinite Galois group. Luckily, we can introduce a topology on the Galois group and the topology will serve as an device that

counts only the relevant subgroups.

2 Topological groups

Since we are going to put a topology on the infinite Galois groups. The concept of "topological groups" will naturally arise. In this chapter, we are going to define the topological groups, and look into some properties of topological groups as well.

Definition 2.1. A group G is a topological group if it is a topological space, and the multiplication $\cdot : G \times G \to G$ is continuous, where GxG is equipped with product topology, and the inverse map $G \to G$: $g \mapsto g^{-1}$ is continuous. A homomorphism between two topological groups is a continuous group homomorphism, and an isomorphism between two topological groups is a homeomorphic group isomorphism.

To understand the concept better, we should look at some examples:

Example 2.2. (1) Let G be the the group of all integers under the addition, where the topology on $\mathbb{Z}$ has discrete topology. Then $((Z), +)$ is a topological group.

(2)In fact, let G be any group, and equip it with the discrete topology, then it is a topological group. We call this kind of topological groups *discrete groups*.

(3) Consider $GL_n(\mathbb{R})$ the general linear group. Since $GL_n(\mathbb{R})$ is a subset of $\mathbb{R}^{n^2}$, let it be endowed with the subspace topology. Since both the inverse mapping and the multiplication for invertible matrices are polynomial functions at each entry. Since polynomial functions are continuous, the inverse mapping and multiplication mapping are continuous. Thus the $GL_n(\mathbb{R})$ under matrix multiplication with subspace topology is a topological group.

Now we are going to look at some of the basic properties of the topological groups.

Proposition 2.3. *(Munkres' Chapter 18 Exercise 11) Let $F : X \times Y \to Z$. We say that F is continuous in each variable separately if for each y_0 in Y, the map $h : X \to Z$ defined by $h(x) = F(x \times y_0)$ is continuous, and for each x_0 in X, the map $k : Y \to Z$ defined by $k(x) = F(x_0 \times y)$ is continuous. If F is continuous, then F is continuous in each variable seperately.*

Proof. Let V be a open set in Z. Since $F : X \times Y \to Z$ is a continuous map. $F^{-1}(V)$ is an open set in $X \times Y$, denote it as $U_1 \times U_2$. Let $X \times \{y_0\}$ be the subspace of $X \times Y$. Then $F^{-1}(V) \cap X \times \{y_0\} = U_1 \times \{y_0\}$ is an open set in $X \times \{y_0\}$. Since X is homeomorphic to $X \times \{y_0\}$ with the homeomorphism $\pi : X \times \{y_0\} \to X$ such that $(x, y_0) \mapsto x$, then U_1 is an open set in X. Moreover, $U_1 = \pi(U_1 \times \{y_0\}) = \pi(F^{-1}(V) \cap X \times \{y_0\}) = h^{-1}(V)$. Therefore, $h : X \to Z$ is continuous. Since it is symmetric for the two variables, by the same way, we will have $k : Y \to Z$ is also continuous. □

This proposition shows that the right (left) multiplication by an element is continuous in a topological group.Moreover, since the right (left) multiplication by an element in the group is an automorphism, therefore, it is a bijection. Thus, in fact, the right (left) multiplication by an element is a homeomorphism.

Since in a group, every element has an inverse. Thus an inverse map is also an bijection, therefore a homeomorphism in a topological group.

Proposition 2.4. *G is an topological group. Let $a \in G$, then For every neighborhood V of a, there exists a neighborhood of e such that $V = a \cdot U$.*

Proof. Let $U = a^{-1} \cdot V$. Since $a \in V$, $1 \in U$. Let O_1 be an open set $\subset V$. Then there exists an set $O_2 \subset U$ that is the preimage of the map of left multiplication by a^{-1}. Since the left multiplication is continuous, O_2 is an open set $\subset U$. Therefore U is a neighborhood of e. Hence the proposition. □

Definition 2.5. A subset U in a topological group is called symmetric if $U = U^{-1}$, where U^{-1} is the set of all inverses of the elements in U.

Definition 2.6. Given a topological space G, G is homogeneous if for every pair of points x, $y \in G$, there exists a homeomorphism f such that $f(x) = y$.

Proposition 2.7. *Every topological group is homogeneous.*

Proof. Let G be a topological group, and x, y be a pair of points in the topological group G. Define f: $G \to G$ as following: $g \mapsto yx^{-1}g$. Then f takes x to y. Moreover, f is a left multiplication by the element yx^{-1}, thus it is a bijection. And since G is a topological group, then the the multiplication is continuous. By the Proposition 2.4, f is continuous and so is f^{-1}. Therefore, f is a homeomorphism takes x to y. Since this is true for every pair of points in G, G is homogenous. □

Homogeneity is one of the nice properties of the topological groups. It makes us able to examine every open neighborhood in the topological groups just by looking at the neighborhood around the identity element e. We are going to use the homogeneity to prove the next proposition.

Proposition 2.8. *Let G be a topological group. Then for every neighborhood U of an element $a \in G$, there exists an open symmetric group $V \subset U$ such that $V^2 \subset U$.*

Proof. By the homogeneity and proposition 2.4, we only need to prove the proposition for the neighborhood containing the identity element e.

Consider the multiplication $\cdot : G \times G \to G$. Since U is a neighborhood of e, thus there exists an open set U' containing e. Then the preimage of U' is an open set in $G \times G$, which is of the form $V_1 \times V_2$, and V_1 and V_2 are both open sets in G. Let $V' = V_1 \cap V_2 \cap U'$. Since all three sets are open, the intersection V' is also open. Since the inverse map is continuous, thus V'^{-1} is also open. Let $V = V' \cap V'^{-1}$. Then V is an open symmetric neighborhood of e in U such that $V^2 \subset U$. □

Definition 2.9. The topological closure of a subset U in a topological group G is the smallest closed set in G containing U, denote as $\overline{U}$.

Since topological group is not only a topological space but also a group, we might as well look into the properties of the subgroups of a topological group.

Proposition 2.10. *Given a topological group G. Then every subgroup H of G is also a topological group.*

Proof. Since H is a subgroup of G, then the multiplication map and inverse map on H are just the multiplication map and inverse map on G restricted to the subgroup H. Then both the multiplication map and inverse map are continuous on H. Hence H is also a topological group. □

Proposition 2.11. *G is a topological group. If H is a subgroup of G, then $\overline{H}$ is also a subgroup of G. Moreover, if H is a normal subgroup of G, then $\overline{H}$ is also a normal subgroup of G.*

Proof. To show $\overline{H}$ is a subgroup of G, we only need to show that for every a, $b \in \overline{H}$, we have $ab^{-1} \in \overline{H}$.

Let W be a neighborhood of ab^{-1}. Since the multiplication is continuous, then there exists an open sets $UV^{-1} \subset W$, where U is an open set contains a, and V is an open set contains b. Since $a, b \in \overline{H}$, then $U \cap H \neq \emptyset$ and $V \cap H \neq \emptyset$. Therefore, $\exists x \in U \cap H$ and $y \in V \cap H$. Since H is a group, then $y^{-1} \in V^{-1} \cap H \Rightarrow xy^{-1} \in UV^{-1} \cap H \subset W \cap H$. This means the intersection of W and H is not empty. Since this is true for every neighborhood of ab^{-1}, $ab^{-1} \in \overline{H}$. □

Proposition 2.12. *If G is a topological group, and H is a subgroup of G, then they have the following properties:*

(1) if H is open (respectively, closed) in G, then its both left and right cosets are also open (respectively, closed) in G.

(2) If H is open in G, then it is closed in G.

(3)If G is compact, then every open subgroup of G has finite index.

(4)If H is closed and H has finite index, then H is open in G.

(5)If $\exists$ an open set $U \subset H$, then H is open in G.

(6)G is Hausdorff if and only if $\{e\}$ is closed in G.

Proof. (1) Since the left (right) multiplication is a homeomorphism in a topological group, the left (right) multiplication maps open(respectively closed) sets to open (respectively closed) sets. Therefore, since H is open (respectively closed) in G, thus for every $g \in G$, gH and Hg are both open (respectively closed).

(2)Let $a \in \overline{H}$. Since H is open, then since aH is a open set containing $a \Rightarrow aH$ is a neighborhood of a. Since a is in the closure of H, thus a is a limit point of H $\Rightarrow aH \cap H \neq \emptyset$. Then $\exists h_1, h_2 \in H$, such that $ah_1 = h_2 \in aH \cap H$. $\Rightarrow a = h_2 {h_1}^{-1}$. Since H is a subgroup, H is closed under multiplication and inverse mapping. Therefore, $a \in H \Rightarrow \overline{H} \subset H$. Since $H \subset \overline{H}$, we have $H = \overline{H}$. Hence, H is closed.

(3) Since the H is an open subgroup of G, the cosets of H are all open. Thus the cosets of H form a open cover of the topological group G. Moreover, since the cosets of H partition G, there is no proper subcollection of the open cover covers G. Therefore, if G is compact, H must have finite index.

(4) Since H is closed and the left multiplications are homeomorphic, then every cosets gH of H is closed in G. Since H has finite index and finite union of closed sets is also closed, then the union of all cosets of H excluding H itself $\bigcup_{g \notin H} gH$ is closed. Since H is the complement of $\bigcup_{g \notin H} gH$ in G, H is open.

(5)Since $U \subset H$, then it is obvious that $\bigcup_{h \in H} hU \subset H$. On the other hand, for every $h \in H$, hu^{-1} is also an element in H. Moreover, $h \in hu^{-1}U \Rightarrow h \in \bigcup_{h \in H} hU$. Therefore, $\bigcup_{h \in H} hU \supset H \Rightarrow \bigcup_{h \in H} hU = H$. Since U is open and left multiplication is homeomorphic, thus hU is open for every $h \in U$. Since the union of open sets is also open, $H = \bigcup_{h \in H} hU$ is open.

(6) ($\Rightarrow$) If G is Hausdorff, then every one-point set in G is closed. Hence $\{e\}$ is closed.

($\Leftarrow$) To show G is Hausdorff, we need to show that for any pair of distinct points $a, b \in G$, $\exists$ a neighborhood of a and a neighborhood of b such that they are disjoint. Since $\{e\}$ is closed, and G is a topological group, which means it is homogeneous, given $a, b \in G$, $\{a^{-1}b\}$ is also closed. Since $\{a^{-1}b\}$ is closed then its complement $G \setminus \{a^{-1}b\}$ is open. Let U be

an open subset of $G \setminus \{a^{-1}b\}$. Then since the map $f : G \times G \to G$, where $(x, y) \mapsto xy^{-1}$, is continuous, then $\exists$ open sets V, W in G such that $VW^{-1} \subset U$. Thus, $a^{-1}b \notin VW^{-1} \Rightarrow aV \cap bW = \emptyset$. Hence G is Hausdorff. $\square$

3 Projective System and Profinite Groups

After looking at the properties of the general topological groups, we should take a look at the profinite groups, which is a type of topological groups that assembled by finite groups. We will start with the definition of a *projective system* on topological spaces.

Definition 3.1. A *direct set* is a nonempty set I equipped with a partial order $\leq$, i.e $\leq$ is reflexive, antisymmetric and transitive. A *projective system* $(X_i, \phi_{ij})_I$ is consists of a collection of topological spaces $\{ X_i \mid i \in I\}$ indexed by I and a collection of continuous maps $\{\phi_{ij} : X_i \to X_j \mid i, j \in I, j \leq i\}$ where:

(1) ϕ_{ii} is the identity on X_i, $\forall\ i \in I$.

(2) $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$, $\forall\ k \leq j \leq i \in I$.

Here is an example of a projective system:

Example 3.2. Let the direct set be the natural number $\mathbb{N}$, and let $X_i := \{1, 2, ..., i\}$, and the topology on each set X_i is the discrete topology, define the map $\phi_{ij} : X_i \to X_j$ as following:

(1) $\phi_{ij}(n) = j$, if $j \leq n$.

(2) $\phi_{ij}(n) = n$, if $n \leq j$.

Then obviously, ϕ_{ii} is the identity map on X_i. Moreover, Given $k \leq j \leq i \in I$, then

(1) $\phi_{ik}(n) = \phi_{jk} \circ \phi_{ij}(n) = k$, if $k \leq n$;

and (2) $\phi_{ik}(n) = \phi_{jk} \circ \phi_{ij}(n) = n$, if $n \leq k$.

Therefore, this is a projective system.

Definition 3.3. Given a projective system $(X_i, \phi_{ij})_I$, the projective limit of the projective system is defined as following:

Let $X = \Pi_{i \in I} X_i$ with product topology, and $\pi_i : X \to X_i$ be the canonical projection. The projective limit $\varprojlim X_i = \{a \in X | \pi_j(a) = \phi_{ij} \circ \pi_j(a), \forall j \leq i\}$, and it has subspace topology.

Lemma 3.4. *Let $f, g : X \to Y$ be two continuous functions. If Y is a Hausdorff space, then the set $\{x \in X | f(x) = g(x)\}$ is a closed sets in Y.*

Proof. Since $f, g : X \to Y$ are two continuous maps, then $h = f - g : X \to Y$ is also a continuous map. Moreover, the set $\{x \in X | f(x) = g(x)\}$ is a preimage of the set $\{0\}$ in Y. Since Y is Hausdorff, then every single-point set is closed in Y. Hence, $h^{-1}(\{0\})$=$\{x \in X | f(x) = g(x)\}$ is a closed set in Y. □

Proposition 3.5. *In this proposition, we will use X to denote the product space $\Pi_{i \in I} X_i$. The projective limit $\varprojlim X_i$ has the following property:*

(1) If X_i is Hausdorff or totally disconnected for each i, then so is $\varprojlim X_i$.

(2) Moreover, If X_i is Hausdorff for each i, then $\varprojlim X_i$ is closed in $X = \Pi_{i \in I} X_i$

(3) IfX_i is compact for each i, then so is $\varprojlim X_i$.

Proof. (1) Since the product and subspace of Hausdorff spaces is always Hausdorff space, and product and subspace of totally disconnected subspaces is always totally disconnected subspaces. Hence, we have the result.

(2) By Lemma 3.4 and the fact that $\varprojlim X_i$ is a Hausdorff space, for every pair of i, j, where $j \leq i$, $\{a \in X | \pi_j(a) = \phi_{ij} \circ \pi_j(a)\}$ is a closed set. Since $\varprojlim X_i = \bigcap_{j \leq i} \{a \in X | \pi_j(a) = \phi_{ij} \circ \pi_j(a)\}$, and the fact that the intersection of closed sets is a closed set, we will have that $\varprojlim X_i$ is a closed subset of X.

(3) Since the product of compact spaces is compact, thus if X_i is compact for each i, then X is compact. Since every closed subspace of a compact space is compact, and $\varprojlim X_i$ is a closed subset of X, we have that $\varprojlim X_i$ is compact. □

If the the projective system $(X_i, \phi_{ij})_I$ is on groups, then the maps $\{\phi_{ij}\}$ will need to be group homomorphisms.

Proposition 3.6. *In this proposition, we will use X to denote the product space $\Pi_{i \in I} X_i$. If X_i is a topological groups in a projective system for each $i \in I$, then the projective limit $\varprojlim X_i$ is a topological group.*

Proof. Since if the multiplication and inverse map is continuous on X_i, for each i, then the multiplication and inverse map will be continuous on the product space X. To prove this proposition, we only need to show that the projective limit $\varprojlim X_i$ is a subgroup of X.

Since all the maps $\{\phi_{ij}\}$ are group homomorphisms, then for the identity elements e of X, $\phi_{ij}(\pi_i(e)) = \phi_{ij}(e_i) = e_j = \pi_j(e)$. Therefore the identity element e is in the projective limit $\varprojlim X_i$. And since the natural projections are homomorphisms and all the $\{\phi_{ij}\}$ are group homomorphisms, then we will have the projective limit $\varprojlim X_i$ closed under multiplication and inverse map. Therefore we have that the projective limit $\varprojlim X_i$ is a subgroup of X. Hence, the projective limit $\varprojlim X_i$ is a topological group.

□

Now we have done all the preparation, so we can define the profinite groups.

Definition 3.7. A *profinite group* G is a topological group that is isomorphic to a projective limit of a projective system $\{G_i, \phi_{ij}\}_I$, where G_i are finite discrete topological groups $\forall i \in I$.

Just by the first glimpse of the profinite group's definition, it is naturally to wonder if a Galois group $G = Gal(E/F)$ of an infinite Galois extension E/F is a profinite groups, where the finite topological groups are G/H_i, and H_i are all the normal subgroups of G with finite index. In fact, this is true. Moreover, every profinite group is isomorphic to a Galois group. We will get back to this in the further chapters.

Theorem 3.8. *Given G a profinite group, then it is totally disconnected, Hausdorff, and compact.*

Proof. Since G is a profinite group, then by the definition of the profinite group, G is isomorphic to a projective limit of a projective system $\{G_i, \phi_{ij}\}_I$, where G_i are finite discrete topological groups $\forall i \in I$. Since for each G_i, it is finite and the topology on it is the discrete topology, thus G_i is obviously Hausdorff, totally disconnected and compact for each i. By the proposition 3.5, we will have that G is a totally disconnected, Hausdorff, and compact topological group. □

Theorem 3.9. *If a topological group G is totally disconnected, Hausdorff and compact, then G is a profinite group*

With these two theorems, we have that profinite groups are equivalent to the Hausdorff, totally disconnected, and compact topological groups.

4 Finite Galois theory and The Krull topology

In this Chapter, we will review some basics of the (finite) Galois theory, and also look into some properties of the Krull topology, which is the topology we are going to put on the infinite Galois groups.

Definition 4.1. The Galois extension is a algebraic field extension that is both normal and separable.

Definition 4.2. Given an field extension E/F, the Galois group $Gal(E/F)$ is the set of all automorphisms on the field E that fixed the field F (i.e, given a $\sigma \in Gal(E/F)$, $\sigma(x) = x$, if $x \in F$) under the composition.

Definition 4.3. Let $G = Gal(E/F)$, and H is a subgroup of G, the fixing field of H is denoted as $\mathcal{F}(H)$, and is defined as following: $\mathcal{F}(H)$=$\{x \in E : \sigma(x) = x$ for every $\sigma \in H$ $\}$; and let K be a subfield of E containing F, the fixing group of K is denoted as $\mathcal{G}(K)$, and is defined as following: $\mathcal{G}(K)$=$Gal(E/K)$=$\{\sigma \in G : \sigma(x) = x$ for every $x \in K$ $\}$.

Theorem 4.4. *(Main Theorem of the Finite Galois Theory) Let E/F be an finite Galois extension. Let G be the Galois group.*

(1) If $H_1 \leq H_2$, and both of them are subgroups of G, then $\mathcal{F}(H_1) \geq \mathcal{F}(H_2)$; and If $K_1 \leq K_2$, and both of them are subfields of E, then $\mathcal{G}(K_1) \geq \mathcal{G}(K_2)$. Moreover, the map $\mathcal{F}$ is a bijection from subgroups to intermediate fields, with the inverse $\mathcal{G}$, we call this bijection the Galois Correspondence.

(2) Suppose that the subfield K of E corresponds to the subgroup H of G.Then, (i) E/F is always a normal extension, hence a Galois extension.

(ii) K/F is normal if and only if H is a normal subgroup of G, and Gal(E/F) is always isomorphic to the quotient group G/H.

(iii)[K:F]=[G:H], and [E:K]=| H |

(3) If the intermediate filed K corresponds to the subgroup H, let $\sigma \in G$, then $\sigma(K)$ corresponds to the conjugate subgroup $\sigma H \sigma^{-1}$. $\sigma(K)$ is called the conjugate subfield.

As we saw in the introduction section of this paper, the correspondence between the intermediate fields of E/F and the subgroups of $Gal(E/F)$, the Galois group of the extension, established in the theorem above, will be invalid. Therefore, we need to put the Krull topology, which is the most natural nontrivial topology for a Galois group, on the infinite Galois groups. After doing that, we will get a result, similar to the one above, that is for the infinite Galois extension.

Given an Galois extension E/F, we are going to use $\mathcal{T}$ to denote the collection of all the finite extensions K, contained in E, of the field F.

Definition 4.5. Given an Galois extension E/F, it has a Galois group G. Then the Krull topology is defined by the set of normal subgroups with finite index $\mathcal{S} = \{Gal(E/K) | K \in \mathcal{T}\}$ as the local basis of the identity element in G.

Theorem 4.6. *Let E/F be a Galois extension and let G be the Galois group $Gal(E/F)$. Then the topological group G, equipped with the Krull topology, has following properties:*

(1)Hausdorff.

(2)compact.

(3)totally disconnected.

Proof. (1) To show G is Hausdorff, we need to show that for any two distinct elements $\sigma, \tau \in G$, $\exists$ neighborhood U of σ and neighborhood V of τ such that U and V are disjoint. Since $\bigcup_{K\in\mathcal{T}} K = \bigcup_{U\in\mathcal{S}} U = E$, and every automorphism in $Gal(E/K)$ fixes K, then every element in the intersection $\bigcap_{K\in\mathcal{T}} Gal(E/K)$ fixes E.

$\Rightarrow \bigcap_{K\in\mathcal{T}} Gal(E/K) = \{e\}$.

Since σ, τ are two distinct elements in G. Thus $\sigma^{-1}\tau \neq e$. Then $\exists U' \in \mathcal{S}$, such that $\sigma^{-1}\tau \notin U'$. $\Rightarrow \tau \notin \sigma U'$.

Since U' is a subgroup of G, then the cosets of U' are all disjoint. Then by the fact that $\tau \notin \sigma U'$, we can have that $\tau U' \cap \sigma U' = \emptyset$ Since U' is an open neighborhood of e, and G is homogeneous, then $\tau U'$ is an open neighborhood of τ, and $\sigma U'$ is an open neighborhood of σ. Hence, G is Hausdorff.

(2)Define a map $h : G \to \Pi_{K\in\mathcal{T}} Gal(K/F)$, where $\sigma \mapsto \{\sigma|_K\}_{K\in\mathcal{T}}$.

Since for every $K \in \mathcal{T}$, K/F is finite $\Rightarrow$ $Gal(K/F)$ is finite $\Rightarrow$ the Krull topology on $Gal(K/F)$ is the discrete topology. Then $Gal(K/F)$ is compact for each $K \Rightarrow$ the product space $\Pi_{K\in\mathcal{T}} Gal(K/F)$ is compact.

If we show that h is a homeomorphism from G to $h(G)$, and $h(G)$ is a closed in the product space $\Pi_{K\in\mathcal{T}} Gal(K/F)$, then we will have that G is compact.

First, we need to show $h : G \to h(G)$ is a homeomorphism:

(a) Bijectivity. Since $h(G)$ is the image, h is naturally surjective. For injectivity, since $\sigma \mapsto \sigma|_K$, then if $h(\sigma) = id$, then $\sigma|_E = id$, $\forall E \in \mathcal{T}$. Since $\bigcup_{K\in\mathcal{T}} K = E$, $\sigma = id$ in $G \Rightarrow h$ is injective $\Rightarrow h$ is bijective.

(b) Continuity. Since the canonical projection $\pi_K : \Pi_{K\in\mathcal{T}} Gal(K/F) \to Gal(K/F)$ is continuous, if we show that $\pi_K \circ h : G \to Gal(K/F)$ is continuous, then h has to be continuous.

Since Gal(K/F) is finite discrete space, $\forall K \in \mathcal{T}$, and topological groups are homogeneous, then we only need to check the preimage of the open set $\{id\} \subset Gal(K/F)$. Since if $\pi_K \circ h(\sigma) = id$, then $\sigma fixes K \Rightarrow \sigma \in Gal(E/K)$. Thus the preimage of $\{id\} \subset Gal(K/F)$ is $Gal(E/K)$. Since $Gal(E/K)$ is a basis element of the Krull topology, thus it is open. Hence h is continuous.

(c) Open map. Let $Gal(E/K) \in \mathcal{S}$. Then $Gal(E/K)$ is open. Moreover, $h(Gal(E/K)=$ $h(G) \cap (\Pi_{K' \neq K} Gal(K'/F) \times \{id\})$, which is open in $h(G)$. Hence, h is open.

Therefore, $h : G \to h(G)$ is a homeomorphism. Then, we need to check $h(G)$ is closed in $\Pi_{K \in \mathcal{T}} Gal(K/F)$:

For any two intermediate fields $K_1, K_2 \in \mathcal{T}$, where $K_1 \subset K_2$, we define $M_{K1|K2} = \{\bar{\sigma} \in \Pi_{K \in \mathcal{T}} Gal(K/F) | \pi_{K_1}(\bar{\sigma}) = \pi_{K_2}(\bar{\sigma})|_{K_1}\}$.

Since $K_1 \in \mathcal{T}$, $Gal(K_1/F)$ has finitely many elements. We can write $Gal(K_1/F)$ as $\{\sigma_1 ... \sigma_r\}$, and let S_i be subset of $Gal(K_2/F)$, where it is the extension of σ_i from K_1 to K_2.

Then, $M_{K1|K2} = \bigcup_{i=1,...,r} (\Pi_{K' \neq K_1, K_2} Gal(K'/F) \times S_i \times \{\sigma_i\})$

is a closed set, since $\Pi_{K' \neq K_1, K_2} Gal(K'/F) \times S_i \times \{\sigma_i\}$ is closed, and finite union of closed sets is also closed.

Moreover, $h(G) = \bigcap_{E_1 \subset E_2} M_{K1|K2}$. Since the intersection of closed sets is always closed, we have that $h(G)$ is closed in the product space.

By everything we have above, we can conclude that G is a compact topological group.

(3) Since G is a topological group, G is homogeneous. We only need to show that the connected component H of the identity element is the one-point set $\{id\}$.

Let U be a element of the local basis of id in the Krull Topology, and use U_H to denote $U \cap H$. Since, $id \in U, and id \in H$, $id \in U_H$. Thus, U_H is not an empty set.

Let $V_H = \bigcup_{x \in H \setminus U_H} xU_H$.Since U is open, then U_H is open $\Rightarrow$ all the cosets of U_H is open $\Rightarrow$ V_H is open.

Then (U_H, V_H) form a pair of separated sets of H. Since H is connected, and U_H is not an empty set,, then V_H is an empty set. Moreover, $U_H = U \cap H = U$. Since this is true for all U in the local basis. Then $H \subset \bigcap_{U \in \mathcal{S}} U = \{id\}$. Hence the only connected component of $\{id\}$ is the single-point set $\{id\}$. Hence, G is totally disconnected.

□

By the theorem above, we have that the Galois groups with the Krull topology are Hausdorff, compact, and totally disconnected. These are actually very familiar properties. These are the properties of the profinite groups. In fact, by Theorem 3.9, we will have that the Galois groups with the Krull topology are profinite groups.

5 The Fundamental Theorem of Infinite Galois theory

This section we will look at the modified version of the main theorem of the (finite) Galois theory, that is also valid when the Galois extension is infinite. In fact, the main theorem of the infinite Galois theory is a generalization of the main theorem of the (finite) Galois theory.

Lemma 5.1. *Let E/F be a Galois extension. Let $H \leq Gal(E/F) = G$. Then $Gal(E/\mathcal{F}(H)) = \overline{H}$.*

Proof. Since H fixes $\mathcal{F}(H)$ by definition, we have $H \leq Gal(E/\mathcal{F}(H))$.

Let $\sigma \in Gal(E/F) \setminus Gal(E/\mathcal{F}(H))$. $\Rightarrow \exists \alpha \in \mathcal{F}(H)$ such that $\sigma(\alpha) \neq \alpha$.

Let K be a splitting field over F, such that $F \subset K \subset E$ and $K \in \mathcal{T}$ and $\alpha \in K$. Then $Gal(E/K)$ is an open subgroup of G.

Let $\tau \in Gal(E/K)$. Then τ fixes K. $\Rightarrow \sigma\tau(\alpha) \neq \alpha$. $\Rightarrow \sigma Gal(E/K)$ is an open neighborhood of σ that does not intersect $Gal(E/\mathcal{F}(H))$. Since this is true for every element outside $Gal(E/\mathcal{F}(H))$. $\Rightarrow Gal(E/\mathcal{F}(H))$ is closed.

Then to show $Gal(E/\mathcal{F}(H)) = \overline{H}$, we only need to show that $Gal(E/\mathcal{F}(H)) \subset \overline{H}$.

Let $\sigma \in Gal(E/\mathcal{F}(H))$ and $K \in \mathcal{T}$. Let $H_0 = \{\rho|_K : \rho \in H\}$. Since $H \leq G$, then $H_0 \subset Gal(K/F)$. Moreover, $\mathcal{F}(H_0) = (H) \cap E$. Since K/F is a finite extension, thus by the finite Galois theory, we have $H_0 = Gal(E/E \cap \mathcal{F}(H))$. Since $\sigma \in Gal(E/\mathcal{F}(H))$, then σ fixes $\mathcal{F}(H)$, therefore $\sigma|_K \in H_0$. This means that $\exists\ \rho \in H$ such that $\rho and \sigma$ agree on K. Then we have $\sigma^{-1}\rho \in Gal(E/K) \Rightarrow \rho \in \sigma Gal(E/K) \cap H$. Since This is true for all $K \in \mathcal{T}$. This means that every element in $Gal(E/\mathcal{F}(H))$ is a limit point of H. Hence $Gal(E/\mathcal{F}(H)) = \overline{H}$. □

Theorem 5.2. *(The fundamental theorem of infinite Galois theory) Let E/F be a Galois extension. Let G be the Galois group of the extension, equipped with Krull topology. Then, there is one-to-one correspondence:*

$\{H \mid H$ is closed in $G\} \longleftrightarrow \{M|F \subset M \subset E\}$. The one-to-one correspondence is given by the map $H \mapsto \mathcal{F}(H)$, and the map $M \mapsto \mathcal{G}(M)$. And there are also the following properties:

(1)Let H_1, H_2 be two closed subgroups of G, then $H_2 \subset H_1$ if and only if $\mathcal{F}(H_1) \subset \mathcal{F}(H_2)$.

(2)A closed subgroup H of G is open if and only if $\mathcal{F}(H)$ has finite degree over F.

(3) If H is a closed subgroup of G, then H is normal if and only if $\mathcal{F}(H)/F$ is a Galois extension.

Proof. Followed by the Lemma 5.1, $\mathcal{G}(\mathcal{F}(H) = \overline{H}$. Therefore, to make the bijection valid, H has to be closed.

(1) Since H_1, H_2 are closed subgroups of G, and $H_2 \subset H_1 \Rightarrow$, and $\mathcal{F}(H_1)$ is the field fixed by all the element of H_1, then $\mathcal{F}(\sigma H_1)$ is also fixed by H_2 by the fact H_2 is contained in H_1. Thus, we have $\mathcal{F}(\sigma H_1) \subset \mathcal{F}(\sigma H_2)$.

(2)For a closed subgroup H, $[\mathcal{F}(H)$:F]=$[G : H]$.

($\Rightarrow$)Since by propposition 2.12, we have that in a topological group, every closed subgroup with finite index is an open subgroup, Hence H is an open subgroup.

($\Leftarrow$) Since by the proposition 2.12, we have that in a topological group, every open subgroup is a closed subgroup. Therefore, we have this direction too.

(3) ($\Rightarrow$) If H is normal and closed in G, and $H= Gal(E/M)$, for some M intermediate fields. Let $a \in M$, and $f(x) \in F[x]$ be the minimal polynomial of a. Let b be the conjugate of a over the minimal polynomial $f(x)$.

Then $\exists \sigma \in G$ such that $\sigma(a) = b$. Let $\tau \in H$, then $\tau(b) = \tau(\sigma^{-1}(a) = \sigma^{-1}(\sigma\tau\sigma^{-1}(a))$. Since H is normal, and $\tau \in H$, then we have $\sigma\tau\sigma^{-1} \in H$.Since a is in the fixed field of H, therefore $\sigma^{-1}(\sigma\tau\sigma^{-1}(a))= \sigma^{-1}(a)$=$b$. Thus, b is also in the fixed field of H. Thus, M/F is normal. Hence, Galois.

($\Leftarrow$) If M/F is Galois, then the map $h : G \to Gal(M/F)$, where $\sigma \mapsto \sigma|_M$ is a well-defined homomorphism with the kernel = H. Hence H is normal in G.

□

References

[1] F. M. Butler, *INFINITE GALOIS THEORY*, `http://faculty.ycp.edu/~fbutler/MastersThesis.pdf`.

[2] J. Munkres, *Topology (2nd Edition)*, Pearson, 2 edition, January 2000.

[3] R. Chevalley and D. Burde, *Profinite groups and Galois cohomology.*

[4] D.S. Dummit, and R. M. Foote, *Abstract Algebra*, Englewood Cliffs, N.J.: Prentice Hall, 1991.