Profinite Groups and Infinite Galois Theory

Abhijit Mudigonda

Abstract

We discuss the applications of profinite groups to the Galois theory of infinite field extensions. We begin by defining profinite groups and characterizing their topological properties, and then show that every Galois group is a profinite group. Then, after introducing the group cohomology of profinite groups, we show how it can be coupled with Galois theory to prove the main theorem of Kummer theory.

1 Introduction

Profinite groups are groups whose structure is determined by continuous homomorphisms into finite groups. As such, they are in some sense the infinite groups which are easiest to study using the tools of finite group theory. As it turns out, many notions from finite group theory have natural generalizations in the theory of profinite groups, including the Sylow theorems, the existence of Frattini and Hall subgroups, and group cohomology. Profinite groups are also topological groups, and can be defined purely topologically.

1.1 Infinite Galois Theory

The study of profinite groups was initially motivated by Galois theory [RZ10]. In the finite case, the main theorem of Galois theory gives us a correspondence between subgroups of the Galois group of a finite Galois extension and its intermediate field extensions. However, this breaks down completely when the extension is infinite - in general, the Galois group has far more subgroups than there are intermediate field extensions. The following results, which we will prove in Section 3, demonstrate that imposing a particular topological condition on the subgroups of the Galois group lets us recover the Galois correspondence.

Theorem 1 ([RZ10] Theorem 2.11.1)**.** *Let K/F be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$, and define $\mathcal{K} := \{K_i | i \in I\}$ as the collection of finite Galois extensions K_i/F such that $F \subseteq K_i \subseteq K$. Then G endowed with the Krull topology is a profinite group and*

$$\mathrm{Gal}(K/F) = \varprojlim_{i \in I} \mathrm{Gal}(K_i/F).$$

Furthermore, the Krull topology on $\mathrm{Gal}(K/F)$ agrees with the relative subspace topology on the inverse limit, if each finite quotient is endowed with the discrete topology.

Theorem 2 ([RZ10] Theorem 2.11.3)**.** *Let K/F be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$, $\mathcal{F}(K/F)$ be the set of intermediate fields $F \subset L \subset K$, and $S(G)$ be the set of closed subgroups of G. There is an inclusion-reversing bijection between the closed subgroups of G under the Krull topology and intermediate field extensions of K/F. The bijections are as follows:*

$$\begin{array}{rcl} \phi\colon \mathcal{F}(K/F) & \to & S(G) \\ L & \mapsto & \mathrm{Gal}(K/L). \end{array}$$

Its inverse is

$$\begin{array}{rcl} \psi\colon S(G) & \to & \mathcal{F}(K/F) \\ H & \mapsto & K^H \end{array}$$

where K^H denotes the fixed subfield of K under H.

We might also ask if every profinite group can be realized as a Galois group of some Galois extension. As we will show, this is in fact true.

Theorem 3 ([RZ10] Theorem 2.11.5)**.** *If G is a profinite group, then there exists a field F and Galois extension K/F such that $\mathrm{Gal}(K/F) = G$.*

1.2 Galois Cohomology and Kummer Theory

The cohomology of Galois groups has been an extremely fruitful area of study, with applications in algebraic number theory ranging from the proof of the Mordell-Weil theorem to the Langlands program. In Section 4, we will introduce the cohomology of profinite groups and show that we can treat them almost identically to finite groups. In Section 5, we will use Galois cohomology to prove the following theorem.

Theorem 4 ([Ser97] Chapter II §1)**.** *Suppose that*

- *G is a profinite group.*
- *A is a G-module with trivial G-action.*
- *π is a surjective homomorphism of B with kernel A.*
- *B is a G-module.*
- *$H^1(G, B) = 0$.*

Then,

$$\mathrm{Hom}(G, A) \simeq B^G/\pi(B^G)$$

where $\mathrm{Hom}(G, A)$ denotes the set of continuous homomorphisms from G to A.

If we choose the groups A and G and the endomorphism π appropriately, then Theorem 4 yields the following result, the main theorem of Kummer theory, as a corollary.

Theorem 5 ([CF10] Chapter III §2)**.** *If k is a field containing n distinct roots of unity, a finite abelian extension of k of exponent dividing n can be obtained by adjoining n^{th} roots of elements of k.*

2 Preliminaries

2.1 Profinite Groups

Definition 6. A **directed poset** I is a poset satisfying the usual conditions on the partial order (reflexivity, antisymmetry, and transitivity) along with the additional condition that if $i, j \in I$, then there exists a k such that $i, j \leq k$.

Definition 7. Let I be a directed poset. An **inverse system of groups** is a collection of groups $(G_i \colon i \in I)$ indexed by I equipped with homomorphisms $\phi_{ij} \colon G_j \to G_i$ whenever $i \leq j$ and such that ϕ_{ii} is the identity and the following diagram commutes when $i \leq j \leq k$

$$\begin{tikzcd}
G_k \arrow[rr, "\phi_{ki}"] \arrow[dr, "\phi_{kj}"] & & G_i \\
& G_j \arrow[ur, "\phi_{ji}"] &
\end{tikzcd}$$

An inverse system is called **surjective** if all defined ϕ_{ij} are surjective.

Definition 8. The **inverse limit** of an inverse system of groups (G_i) is defined as

$$\left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i | g_i = \phi_{ij}(g_j) \text{ if } i \leq j \right\}.$$

In words, an element of the product group is contained in the inverse limit if it is consistent with all the group homomorphisms.

Definition 9. A **profinite group** is the inverse limit of a surjective inverse system of finite groups.

Example 10. Take the collection of groups $\{\mathbb{Z}/p^i\mathbb{Z}\}$, with homomorphisms $\phi_{ij} \colon \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ whenever $i \leq j$. This defines an inverse system. Then,

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

is one way to define the p**-adic integers**.

There is a natural topology on profinite groups. Given the inverse system corresponding to a profinite group, we can equip each finite group in the inverse system with the discrete topology[1], and consider the product topology on the product of the finite groups in the system. Then, we can take the subspace topology, viewing the inverse limit as a subset of the product. We can take this one step further, tying together the topological and inverse limit definitions of a profinite group.

Proposition 11 ([RZ10] Theorem 2.1.3)**.** *Let G be a topological group. Then, the following are equivalent:*

- *G is a profinite group.*

[1] In the discrete topology, every element is an open set.

- *G is compact, Hausdorff, totally disconnected.*
- *G is compact and there is a local base $\mathcal{U}$ of open neighborhoods U about 1 such that each U is an open normal subgroup of G and*

$$\bigcap_{U \in \mathcal{U}} U = 1.$$

- *1 admits a local base $\mathcal{U}$ of open neighborhoods U about 1 such that each U is a normal subgroup of G with finite index and*

$$G = \varprojlim_{U \in \mathcal{U}} G/U.$$

2.2 Finite Galois Theory

We will briefly state some definitions and results from finite Galois theory, and refer the reader to [Art11] for a more thorough introduction.

Definition 12. The **Galois group** of a field extension K/F, denoted $\mathrm{Gal}(K/F)$, is the group of automorphisms of K fixing F.

Definition 13. An extension is a **Galois extension** if it is algebraic, normal, and separable.

The following theorem lets us characterize finite Galois extensions using finite group theory.

Theorem 14 ([Art11] Theorem 16.7.1)**.** *Let K/F be a finite Galois extension and $G := \mathrm{Gal}(K/F)$ its Galois group. Then, there is a bijective correspondence between subgroups $H \subseteq G$ and intermediate field extensions L/F.*

Example 15. Consider the extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then, $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. The two copies of $\mathbb{Z}/2\mathbb{Z}$ correspond to the subextensions $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

Unfortunately, Theorem 14 does not work when K/F is infinite. In general, the number of subgroups can be much larger than the number of intermediate field extensions.

Example 16 ([Sut18] Problem 4)**.** The algebraic closure of $\mathbb{F}_q$, denoted $\overline{\mathbb{F}}_q$, is an infinite extension of $\mathbb{F}_q$. The set of intermediate field extensions of $\overline{\mathbb{F}}_q/\mathbb{F}_q$ has the same cardinality as $\mathbb{R}$, whereas the set of subgroups of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ has the same cardinality as $2^{\mathbb{R}}$.

3 Infinite Galois Theory

Our main goal in this section will be the proof of Theorems 1, 2, and 3.

Proposition 17 ([RZ10] §2.11)**.** *Let $G := \mathrm{Gal}(K/F)$ be the Galois group of some extension K/F, and define $\mathcal{K} := \{K_i | i \in I\}$ as the collection of finite Galois extensions K_i/F such that $F \subseteq K_i \subseteq K$. Define $U_i := \mathrm{Gal}(K/K_i)$ for $i \in I$. Then, the following hold:*

1. *For every $i \in I$, $U_i \trianglelefteq G$ and $G/U_i \simeq \mathrm{Gal}(K_i/F)$ is finite.*
2. *For every $i, j \in I$, there exists $U_k \subseteq U_i \cap U_j$.*
3. $\bigcap_{i\in I} U_i = \{1\}$.

Sketch. These mostly follow from finite Galois theory and field theory.

1. To see that U_i is normal in G, take any $u \in U_i := \mathrm{Gal}(K/K_i)$. Let $g \in G$ and consider the action of gug^{-1} on an element $\alpha \in K_i$. Let $f(x) \in K[x]$ be the minimal polynomial of α. Then, because $\sigma(f(x)) = f(\sigma(x))$ for every field automorphism fixing F, we have that g maps α to another root of f. By normality of the extension $g\alpha$ is a root of f that lies in K_i. But this means that u fixes $g\alpha$, and we have
$$gug^{-1}\alpha = gg^{-1}\alpha = \alpha$$
for every $\alpha \in K_i$, so $gug^{-1} \in U_i$ as desired.
2. Take U_k to be the Galois group of $\mathrm{Gal}(K/K_iK_j)$, where K_iK_j is the compositum of K_i and K_j. Equivalently, if K_i and K_j are the splitting fields of f_i and f_j, respectively, then we can take K_iK_j to be the splitting field of f_if_j.
3. Observe that because K is algebraic, it is the union of all the K_i's. □

Proposition 17 shows that the U_i form a local base at 1, and for a topological group, a local base defines a base for the entire group because the translation map is continuous. This means that the U_i generate a topology on the Galois group.

Definition 18. Let K/F be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$. Then, the **Krull topology** on G is the topology generated by the local base $U_i := \mathrm{Gal}(K/K_i)$ from Proposition 17

With the preliminaries out of the way, let us now prove the three main theorems of infinite Galois theory.

Theorem 1 ([RZ10] Theorem 2.11.1)**.** *Let K/F be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$, and define $\mathcal{K} := \{K_i | i \in I\}$ as the collection of finite Galois extensions K_i/F such that $F \subseteq K_i \subseteq K$. Then G endowed with the Krull topology is a profinite group and*
$$\mathrm{Gal}(K/F) = \varprojlim_{i\in I} \mathrm{Gal}(K_i/F).$$

Furthermore, the Krull topology on $\mathrm{Gal}(K/F)$ agrees with the relative subspace topology on the inverse limit, if each finite quotient is endowed with the discrete topology.

Proof. To show that G is profinite, as per Proposition 11(d), we want to show the existence of a local base of open neighborhoods about 1 such that G is homeomorphic and isomorphic as a group to an inverse limit of quotient groups
$$G_i := G/U_i \simeq \mathrm{Gal}(K_i/F).$$

Let us start by defining the inverse system. We order I by saying that $i \leq j \iff K_i \subseteq K_j \iff U_i \supseteq U_j$. Then, define the homomorphisms
$$\phi_{ji} \colon G_j = \mathrm{Gal}(K_j/F) \to G_i = \mathrm{Gal}(K_i/F)$$

by restriction. These homomorphisms are well defined because the K_i/F are Galois and hence normal. This gives us an inverse system.

We claim that

$$G \simeq \varprojlim_{i \in I} G_i.$$

We have a homomorphism from $\sigma \in G$ to the inverse limit $\sigma_1, \sigma_2, \dots \in \varprojlim_{i \in I} G_i$ by restriction. For the inverse mapping, we get a $\sigma \in G$ from a $(\sigma_1, \dots) \in \varprojlim_{i \in I} G_i$ by noting that any element $\alpha \in K/F$ must live in some finite extension K_i/F (because K/F is algebraic) and we can define $\sigma(\alpha) = \sigma_i(\alpha)$. Thus, the groups are isomorphic.

To show that this isomorphism is in fact a homeomorphism, observe that

$$\mathrm{Gal}(K/K_i) \simeq (\varprojlim_{i \in I} G_i) \cap \left(\left(\prod_{K_j \not\subseteq K_i} G_j \right) \times \left(\prod_{K_j \subseteq K_i} \{1\}_j \right) \right).$$

under the above isomorphism. Observe that the right hand side forms a local base for the identity element of the inverse limit. This means that elements generating a local base of the Galois group under the Krull topology correspond to elements generating a local base of the inverse limit, so the topologies agree. □

Example 19 (Absolute Galois Group of $\mathbb{F}_q$)**.** The finite extensions of $\mathbb{F}_q$ are $\mathbb{F}_{q^r}$ for $r \in \mathbb{Z}_{\geq 1}$. Theorem 1 tells us that

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q).$$

It can be shown that $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$, an order r group, is in fact generated by the Frobenius automorphism, $x \mapsto x^{q^r}$, and therefore that $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \simeq \mathbb{Z}/r\mathbb{Z}$. Putting this all together, we have that

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \varprojlim \mathbb{Z}/r\mathbb{Z}.$$

Theorem 2 ([RZ10] Theorem 2.11.3)**.** *Let K/F be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$, $\mathcal{F}(K/F)$ be the set of intermediate fields $F \subset L \subset K$, and $S(G)$ be the set of closed subgroups of G. There is an inclusion-reversing bijection between the closed subgroups of G under the Krull topology and intermediate field extensions of K/F. The bijections are as follows:*

$$\begin{array}{rcl} \phi\colon \mathcal{F}(K/F) & \to & S(G) \\ L & \mapsto & \mathrm{Gal}(K/L). \end{array}$$

Its inverse is

$$\begin{array}{rcl} \psi\colon S(G) & \to & \mathcal{F}(K/F) \\ H & \mapsto & K^H \end{array}$$

where K^H denotes the fixed subfield of K under H.

Remark. Every open subgroup of a topological group is also closed (it is the complement of the union of all the other cosets, each of which is open by the continuity of the translation map).

Proof. It is clear that ϕ is inclusion reversing. Denote by τ_L the Krull topology on $\mathrm{Gal}(K/L)$, generated by $\{\mathrm{Gal}(K/L_i) : L_i/L \text{ finite}\}$ (and its translates) and by τ_F the Krull topology on $\mathrm{Gal}(K/F)$. Let us start by showing that $\phi(L) = \mathrm{Gal}(K/L)$ is closed in τ_L when L/F is finite. Proposition 11 tells us that $\mathrm{Gal}(K/L)$ is compact with respect to τ_L. Because L/F is finite, the L_i are also the finite extensions of F that contain L, and thus

$$\Big\{\mathrm{Gal}(K/L_i) : L_i/L \text{ finite}\Big\} = \Big\{\mathrm{Gal}(K/F_i) \cap \mathrm{Gal}(K/L) : F_i/F \text{ finite}\Big\}.$$

Therefore, τ_L is the subspace topology of τ_F whenever L/F is finite. There can be no open cover of $\mathrm{Gal}(K/L)$ in τ_F without a finite subcover because any such open cover must restrict to an open cover without a finite subcover $\mathrm{Gal}(K/L)$ in τ_L, which is a contradiction. Thus, $\mathrm{Gal}(K/L)$ is compact in τ_F. Proposition 11 also tells us that $\mathrm{Gal}(K/F)$ is Hausdorff, and because compact subsets are closed in Hausdorff spaces, $\mathrm{Gal}(K/L)$ is closed.

When L/F is infinite, observe that $L/F = \bigcup F_i/F$ where $F \subset F_i \subset L$ and the F_i/F are finite. This implies that $\mathrm{Gal}(K/L) \simeq \bigcap \mathrm{Gal}(K/F_i)$, where each F_i/F is a finite extension. By the case above, this means that $\mathrm{Gal}(K/L)$ is the intersection of closed subgroups and hence that it is closed.

We will next show that ψ is the inverse of ϕ. First, note that $\psi\phi(L) = L$. It is clear that $L \subseteq \psi\phi(L) = \psi(\mathrm{Gal}(K/L))$. Suppose that there were some $\alpha \in K \setminus L$ that was also fixed by every element in $\mathrm{Gal}(K/L)$. Let f be the minimal polynomial of α in $L[x]$. Then, there exists an automorphism in $\mathrm{Gal}(K/L)$ that sends α to a different root of $f(x)$. However, because α is fixed by $\mathrm{Gal}(K/L)$, there must be no other roots, and f must have degree 1. Therefore, $\alpha \in L$, as desired.

For the converse, we want to show that $\phi\psi(H) = H$. It is clear that $H \subseteq \phi\psi(H) = \mathrm{Gal}(K/K^H)$. We wish to show that the inclusion is an equality. We will do so by showing that H is dense in $\mathrm{Gal}(K/K^H)$. To do this, we will show that every open neighborhood of any $\sigma \in \mathrm{Gal}(K/K^H)$ (in τ_{K^H}, the Krull topology on $\mathrm{Gal}(K/K^H)$) in fact contains some element of H. An open neighborhood around σ is a translate of an open ball around 1. In τ_{K^H}, the open neighborhoods are $\mathrm{Gal}(K/N)$ where N/K^H is finite. Thus, we want to show that

$$\tau\mathrm{Gal}(K/N) \cap H \neq \emptyset$$

for all finite extensions N/K^H and $\tau \in \mathrm{Gal}(K/K^H)$. Notice that $\{\sigma_{|N} : \sigma \in H\}$ is a group of automorphisms of N that fixes K^H. By Theorem 14, $\{\sigma_{|N}\} = \mathrm{Gal}(N/K^H)$. Thus, every $\tau_{|N}$ is equal to some $\sigma_{|N}$, and thus there exists a σ and an element $x \in \mathrm{Gal}(K/N)$ such that $\tau x = \sigma$.

□

Remark. As it turns out, normal subgroups do still in fact correspond to normal extensions, but we will not prove this here in the interest of space.

Theorem 3 ([RZ10] Theorem 2.11.5)**.** *If G is a profinite group, then there exists a field F and Galois extension K/F such that* $\mathrm{Gal}(K/F) = G$.

Proof. Intuitively, we want to pick a field K, call the field of its fixed points under G-action L, and then claim that K/L has Galois group G. the main challenge here is finding a field K that:

- Has a natural G-action.
- Is a Galois extension of the field of its fixed points under G.

Take F to be any field and let T be a set of indeterminates, one for each element in the disjoint union of G/U over all open normal subgroups $U \trianglelefteq G$. $K := F(T)$, the rational function ring of functions with coefficients in K and indeterminates from T. Then, G acts on $F[T]$ via $g \cdot (g'U) \mapsto gg'U$ and by fixing F. Define $L := K^G$ to be the set of elements of K fixed under G action. We claim that K/L is Galois.

Pick a $k \in K$. If k includes the indeterminates $\{t_i\}$, where $t_i \in G/U_j$ for $j \in \{1, \ldots, n\}$, then

$$\bigcap_{i=1}^{n} U_i \subseteq G_k$$

where G_k is the stabilizer group of $k \in K$.

We chose the U_i to be open subgroups and finite intersections of open sets are open, so $\bigcap_{i=1}^{n} U_i$ is an open subgroup of G_k. Furthermore, all its cosets in G_k are open because translation is continuous, so G_k can be written as the (possibly infinite) union of open sets and G_k is also open. Recall that in the Krull topology, open sets containing 1 are generated by subgroups of the form $\mathrm{Gal}(K_i/F)$ where K_i/F is finite. These subgroups all have finite index, and a union of subgroups, if it is also a subgroup, must have smaller (hence finite) index. Thus, the stabilizer group G_k has finite index in G and so the orbit of k is finite. Suppose that the orbit of k consists of the elements $\{k_1, k_2, \ldots, k_r\} \in K^r$. The polynomial

$$f(x) = \prod_i (x - k_i)$$

is fixed under the G-action because roots are permuted, but this means that the coefficients are fixed and thus lie in $L := K^G$. Thus, every $k \in K$ is the root of a polynomial with coefficients in L, so K/L is algebraic. Furthermore, the polynomial is separable, as the k_i are distinct, and the extension is normal because it is the union of the normal extensions $L(k_1, \ldots, k_r)/L$ - intuitively, we have all the other roots because they are all within a G-orbit. Thus, K/L is Galois.

The last thing to check is that $G = \mathrm{Gal}(K/L)$. It is clear that $G \subseteq \mathrm{Gal}(K/L)$. We will prove equality by showing that the inclusion map $G \hookrightarrow \mathrm{Gal}(K/L)$ is continuous. Consider any open subgroup $U \subseteq \mathrm{Gal}(K/L)$. Remark 3 tells us that open subgroups are closed, so K^U/L is a finite extension per Theorem 2 and the extension is isomorphic to $L(k_1, \ldots, k_r)$ for some $k_1, \ldots, k_r \in K/L$. Earlier in the proof of this theorem, we could not be sure that the stabilizer groups were of finite index because we did not *a priori* know that the extension was algebraic. Here, however, we know that K^U/L is algebraic, and therefore the groups G_{k_i} of finite index in G and are open subgroups. This tells us that $\bigcap_{i=1}^{r} G_{k_i}$ is open. However, observe that

$$\bigcap_{i=1}^{r} G_{k_i} \subseteq G \cap U$$

because an element in $\bigcap_{i=1}^{r} G_{k_i}$ fixes everything in K^U and thus must be in U by Theorem 2. The intersection of open subgroups is open, and thus $G \cap U$ contains an subgroup that is open in U. The cosets of this subgroup must also be open (by the continuity of translation), so $G \cap U$ can be written as the union of open subgroups and is an open subgroup of G. This proves continuity of the inclusion map. This tells us that G is a closed subgroup of $\mathrm{Gal}(K/L)$ (it is the inverse image of $\mathrm{Gal}(K/L)$ under a continuous map). However, two closed subgroups which fix the same field must be the same by Theorem 2 □

4 Group Cohomology

4.1 Basic Definitions

In the following, G is a profinite group and A is a discrete G-module (e.g. a discrete abelian group on which G acts). Group cohomology can be defined exactly as in the case of a finite G, except we restrict ourselves to continuous maps. All of these definitions are from [RZ10]

Definition 20. $C^n(G, A)$ is the set of *continuous maps* from G^n to A.

Definition 21. The **coboundary** of $f \in C^n(G, A)$, written df, is defined as

$$\begin{aligned} df(x_1, \ldots, x_n, x_{n+1}) :=& x_1 f(x_2, \ldots, x_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1}) + (-1)^{n+1} f(x_1, \ldots, x_n). \end{aligned}$$

Definition 22. $f \in C^n(G, A)$ is an n-**cocycle** if $df = 0$. The group of n-cocycles is denoted $Z^n(G, A) \subseteq C^n(G, A)$.

Proposition 23 (Basic Formula)**.** $d \circ d = 0$.

Definition 24. Let $B^n(G, A) = d(C^{n-1}(G, A)) \subseteq C^n(G, A)$. Then, the n^{th} **cohomology group** is defined by $H^n(G, A) := Z^n(G, A)/B^n(G, A)$.

4.2 Long Exact Sequence of Cohomology

Consider the short exact sequence

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

where A, B, C are G-modules. We have from exactness that $C \simeq B/A$. As with any objects with a group action, we are frequently interested in the fixed points of A, B, and C under G-action and the relationship between the groups of fixed points. While $B^G/A^G \subseteq C^G \simeq (B/A)^G$, the two are not in general equal. Intuitively, the cohomology group $H^1(G, A)$ measures the discrepancy between them. In fact, we can say more.

Theorem 25 ([Ser79] Chapter VII §2)**.** *Suppose that*

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

is a short exact sequence. Then, there exist ***connecting homomorphisms*** δ_i *such that we have the long exact sequence*

$$\begin{aligned} 1 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \xrightarrow{\pi} H^0(G, C) \xrightarrow{\delta_0} H^1(G, A) \\ \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \xrightarrow{\delta_1} H^2(G, A) \longrightarrow \cdots \end{aligned}$$

Sketch. We will define δ_0. The proof of exactness and the definition of δ_i for larger i is left to the reader.

For a G-module M, note that $H^0(G, M) \simeq M^G$, the fixed points of M under the G-action. Thus, δ_0 is a homomorphism from C^G to $H^1(G, A)$. Given an element $c \in C^G$, let $b \in B^G$ be a lift of c to B^G (so c is the image of b). Then, δ_0 is defined as

$$\begin{array}{rcl} \delta_0 \colon C^G & \to & H^1(G, A) \\ c & \mapsto & \left(\sigma \mapsto \frac{\sigma(b)}{b}\right). \end{array}$$

Because c is fixed under the G-action, $\frac{\sigma(b)}{b}$ is an element of A. It can be shown that the output is in fact an element of $H^1(G, A)$ that is independent of our choice of b (which lift of c we choose), so the map is well-defined. It is clear that the map is a homomorphism.

□

5 Applications to Kummer Theory and Beyond

Theorem 26 ([Art11] Theorem 15.3.3). *An extension K/F is quadratic if and only if $K = F[\sqrt{\alpha}]$ for some $\alpha \in F$ that is not a square.*

Unfortunately, while not all degree-n extensions can be obtained by adjoining an n^{th} root, the main theorem of Kummer theory tells us which degree-n extensions can be.

Theorem 5 ([CF10] Chapter III §2). *If k is a field containing n distinct roots of unity, a finite abelian extension of k of exponent dividing n can be obtained by adjoining n^{th} roots of elements of k.*

We will use all the machinery developed thus far to prove this theorem. Let us first state a lemma that will be useful in the proof. In what follows, K/F will be a Galois extension with Galois group $G := \mathrm{Gal}(K/F)$.

Lemma 27 ([Ser79] Chapter X Proposition 2). $H^1(G, K^\times) = 0$

Theorem 4 ([Ser97] Chapter II §1). *Suppose that*

- *G is a profinite group.*
- *A is a G-module with trivial G-action.*
- *π is a surjective homomorphism of B with kernel A.*
- *B is a G-module.*
- *$H^1(G, B) = 0$.*

Then,

$$\mathrm{Hom}(G, A) \simeq B^G/\pi(B^G)$$

where $\mathrm{Hom}(G, A)$ *denotes the set of continuous homomorphisms from G to A.*

Proof. The conditions imply that we have the exact sequence

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{\pi} B \longrightarrow 1$$

where i is the inclusion homomorphism. By Theorem 25, we have the exact sequence

$$A^G \longrightarrow B^G \xrightarrow{\pi} B^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B)$$

Because $H^1(G, B) = 0$, we have the isomorphism

$$B^G/\pi(B^G) \simeq H^1(G, A)$$

By the definition of cohomology groups, $f \in H^1(G, A)$ if, for every $s \in G$, f maps s to an element $a \in A$ such that $sa - a = 0$. Because we have assumed that G acts trivially on A, this is vacuously satisfied and $H^1(G, A) = \text{Hom}(G, A)$. Thus,

$$B^G/\pi(B^G) \simeq \text{Hom}(G, A)$$

as desired. □

Now, we can prove the desired result. Denote by K_{sep} the separable closure of the field K.

Proof of Theorem 5. In Theorem 4, take $B := K_{sep}^\times$, $G := \text{Gal}(K_{sep}/K)$, and π the surjective homomorphism on $K_{sep}^\times$ sending $x \mapsto x^n$. The kernel of this map, A, is the multiplicative group of the n^{th} roots of unity, which we write as μ_n, and

$$\text{Hom}(G, \mu_n) \simeq (K_{sep}^\times)^G/((K_{sep}^\times)^G)^n \simeq K^\times/(K^\times)^n.$$

Now, let us define K_{ab} to be the compositum of all abelian extensions of K and $K_{ab,n}$ to be the compositum of all abelian extensions of K which have Galois groups of exponent dividing n. We claim that $\text{Hom}(G, \mu_n) \simeq \text{Hom}(\text{Gal}(K_{ab,n}/K), \mu_n)$.

First, observe that $\text{Hom}(G, \mu_n) \simeq \text{Hom}(\text{Gal}(K_{ab}/K), \mu_n)$. Given a homomorphism π in $\text{Hom}(\text{Gal}(K_{ab}/K), \mu_n$, we can construct an element π' of $\text{Hom}(G, \mu_n)$ by defining

$$\pi'(g) = \pi(\bar{g}).$$

It is easily checked that this map is a homomorphism from $\text{Hom}(\text{Gal}(K_{ab}/K)$ into $\text{Hom}(G, \mu_n)$. To see that this map is also invertible, notice that $D(G)$ is always in the kernel of a map from G to μ_n. Therefore, $\text{Hom}(G, \mu_n) \simeq \text{Hom}(G/D(G), \mu_n)$. $\text{Gal}(K_{ab}/K)$ is the maximal abelian quotient of $G := \text{Gal}(K_{sep}/K)$ (it's the Galois group of the maximal abelian extension), and so $\text{Gal}(K_{ab}/K) \simeq G/D(G)$. Elements of exponent not dividing n necessarily map to 1 in the image, and so applying the same logic yields the isomorphism

$$K^\times/(K^\times)^n \simeq \text{Hom}(G, \mu_n) \simeq \text{Hom}(\text{Gal}(K_{ab,n}/K), \mu_n).$$

In general, for a group G' and subgroup $H' \subseteq G'$, $\text{Hom}(G'/H', \mu_n)$ can be viewed as a subgroup of $\text{Hom}(G', \mu_n)$. This is because, just as above, every element of $\text{Hom}(G'/H', \mu_n)$ extends to an element of $\text{Hom}(G', \mu_n)$ via composition with the quotient map. If L/K

is a finite abelian extension with exponent n, then $\mathrm{Gal}(L/K)$ is a finite quotient of $\mathrm{Gal}(K_{ab,n}/K)$ and we have that

$$\Delta \simeq \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$$

where Δ is a finite subgroup of $K^\times/(K^\times)^n$. To prove the theorem, it suffices to show that $L \simeq K(\Delta^{\frac{1}{n}})$, the field obtained by adjoining the n^{th} root of every element of Δ.

Let us proceed by making precise the aforementioned isomorphism. Recall from Theorem 4 the definition of the connecting homomorphism δ_0. Here, given an element $c \in \Delta$, δ_0 chooses an n^{th} root of c it calls b, and sends c to the homomorphism $\sigma \mapsto \frac{\sigma(b)}{b}$. The homomorphism σ must send b to another root of the polynomial $x^n - c$, and thus $\frac{\sigma(b)}{b} \in \mu_n$.

Now that we have specified the isomorphism, we will not detail the remainder of the proof. What follows is a sketch. The Galois group factors as a product of cyclic groups. Looking at each cyclic factor, we can use the above isomorphism to show that the corresponding cyclic extensions of K are obtained by adjoining a single n^{th} root. We can also see that these extensions intersect only at K and thus that their compositum has Galois group $\mathrm{Gal}(L/K)$. It can then be shown that L must be of the desired form.

□

References

Artin, Michael. *Algebra*. Pearson Prentice Hall, 2011. 560 pp. ISBN: 978-0-13-241377-0.

Cassels, John William Scott and Albrecht Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union*. London Mathematical Society, 2010. 366 pp. ISBN: 978-0-9502734-2-6.

Ribes, Luis and Pavel Zalesskii. *Profinite Groups*. 2nd ed. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Berlin Heidelberg: Springer-Verlag, 2010. ISBN: 978-3-642-01641-7.

Serre, Jean-Pierre. *Galois Cohomology*. Springer Monographs in Mathematics. Berlin Heidelberg: Springer-Verlag, 1997. ISBN: 978-3-540-42192-4.

— *Local Fields*. Graduate Texts in Mathematics. New York: Springer-Verlag, 1979. ISBN: 978-0-387-90424-5.

Sutherland, Drew. *Problem Set 5 - Number Theory 1*. 2018. URL: http://math.mit.edu/classes/18.785/2018fa/ProblemSet5.pdf.