Infinite Galois Theory

Arpon Basu

Last updated April 22, 2024

Contents

Acknowledgements

All this material heavily references Swayam Chube's notes [Chu23], who also taught the author this subject. Another source referred to is Keith Conrad's notes [Con20] on the same.

§1. Inverse Limits and Profinite Groups

Let $\{C_i\}_{i\in\mathcal{I}}$ is a collection of objects in a category *enriched over a set*.[1] Now consider a system of morphisms $\mu_{ij} : C_i \mapsto C_j$ satisfying $\mu_{jk} \circ \mu_{ij} = \mu_{ik}$ for all i, j, k for which the corresponding μ's exist. This is known as an *inverse system*.

We call $(E, \rho_i : E \mapsto C_i)$ as the *inverse limit* of the aforementioned inverse system if $\rho_j = \mu_{ij} \circ \rho_i$ for all relevant $i, j \in \mathcal{I}$, and the following universal property is satisfied:

If X is another object along with morphisms $\psi : X \mapsto C_i$ for all $i \in \mathcal{I}$ such that $\psi_j = \mu_{ij} \circ \psi_i$ then there exists a unique $\phi : X \mapsto E$ such that all the relevant diagrams commute.

$$\begin{tikzcd}
 & C_i \arrow[dd, bend left=70, "\mu_{ij}"] \\
X \arrow[ur, "\psi_i"] \arrow[r, "\exists!\phi"] \arrow[dr, "\psi_j"'] & E \arrow[u, "\rho_i"'] \arrow[d, "\rho_j"'] \\
 & C_j
\end{tikzcd}$$

Note that inverse limits may not always exist. However, if they do, they are unique up to unique isomorphism.

Now, we define *profinite groups*:

Definition 1.1. Profinite groups are the inverse limit of a system of finite groups.

One can give a more constructive definition of profinite groups: Suppose $\{G_i\}_{i\in\mathcal{I}}$ is a collection of finite groups, each group equipped with the discrete topology, thus making it a topological group. Also suppose that the indexing set $\mathcal{I}$ is a directed set, i.e. there exists a reflexive and transitive order $\leq$ on $\mathcal{I}$ such that for any $i, j \in \mathcal{I}$, there exists $k \in \mathcal{I}$ such that $i \leq k, j \leq k$.

Let $\{\mu_{ij} : G_i \mapsto G_j : i, j \in \mathcal{I}, j \leq i\}$ be a collection of group homomorphisms, where $\mu_{ii} = \mathrm{id}$. Then define

$$\varprojlim G_i := \left\{ (g_i)_{i\in\mathcal{I}} \in \prod_{i\in\mathcal{I}} G_i : \mu_{ij}(g_i) = g_j \text{ for all } j \leq i \right\}$$

One can verify that this satisfies the universal property of inverse limits.

The inverse limit is equipped with the product topology.

We also define the so-called *profinite completion* as follows:

Definition 1.2. Let G be any group. Then define the profinite completion of G, written $\widehat{G}$, as:

$$\widehat{G} := \varprojlim G/N$$

[1] basically, this means that all the objects in the category have an underlying set, and the collection of all morphisms between two objects of a category is a set

where N ranges over all normal subgroups of G with finite index. We also equip G/N with the discrete topology, and that turns $\widehat{G}$ into a topological group.

Profinite groups play a very important role in number theory and Galois theory. In fact, Galois groups are all, and the only, profinite groups [Wat74].
While many properties of profinite groups can be proven in a general setting, we shall not do so. We shall instead prove those properties for Galois groups, and then they will transfer over to profinite groups due to the equivalence mentioned above.

§2. Krull Topology

Let K/k be a (possibly infinite) Galois extension. We first define the so-called *Krull topology*.

Definition 2.1. Let $\mathcal{E} := \{E : K \supseteq E \supseteq k, E/k \text{ is finite Galois}\}$ be the collection of all finite Galois subextensions of K/k. We define the Krull topology as the topology generated by the basis $\mathcal{B}$, where

$$\mathcal{B} := \{\sigma \operatorname{Gal}(K/E) : \sigma \in \operatorname{Gal}(K/k), E \in \mathcal{E}\}$$

Note that we have to verify that $\mathcal{B}$ is indeed a basis: To do that, note that $\operatorname{Gal}(K/k) \in \mathcal{B}$, and thus $\mathcal{B}$ covers every point in $\operatorname{Gal}(K/k)$. Moreover, for any $\sigma \operatorname{Gal}(K/E), \sigma' \operatorname{Gal}(K/E') \in \mathcal{B}$, suppose $\tau \in \sigma \operatorname{Gal}(K/E) \cap \sigma' \operatorname{Gal}(K/E')$. Since $\sigma \operatorname{Gal}(K/E), \sigma' \operatorname{Gal}(K/E')$ are cosets containing τ, $\sigma \operatorname{Gal}(K/E) = \tau \operatorname{Gal}(K/E), \sigma' \operatorname{Gal}(K/E') = \tau \operatorname{Gal}(K/E')$. But note that $\operatorname{Gal}(K/EE') = \operatorname{Gal}(K/E) \cap \operatorname{Gal}(K/E')$, and thus $\tau \in \tau \operatorname{Gal}(K/EE') = \tau \operatorname{Gal}(K/E) \cap \tau \operatorname{Gal}(K/E') \in \mathcal{B}$, as desired.
The second order of business is to verify that the group structure and topological structure of $\operatorname{Gal}(K/k)$ are compatible.

Lemma 2.1. $\operatorname{Gal}(K/k)$ is a topological group.

Proof. Write $G := \operatorname{Gal}(K/k)$. We first verify that the map $G \ni x \mapsto x^{-1} \in G$ is continuous. Note that it is enough to verify that the pullback of the basic open sets is open. Now, the pullback of $\sigma \operatorname{Gal}(K/E)$ under the inverse map is $\operatorname{Gal}(K/E)\sigma^{-1}$. Since E/k is Galois and hence normal, $\operatorname{Gal}(K/E)$ is a normal subgroup of $\operatorname{Gal}(K/k)$. Thus, $\sigma \operatorname{Gal}(K/E)\sigma^{-1} = \operatorname{Gal}(K/E) \implies \operatorname{Gal}(K/E)\sigma^{-1} = \sigma^{-1} \operatorname{Gal}(K/E) \in \mathcal{B}$, as desired.
Now we verify that $G \times G \ni (x, y) \mapsto \varphi(x, y) := xy \in G$ is continuous. Let $U \subseteq G$ be open, and suppose $(\sigma, \tau) \in \varphi^{-1}(U)$. Then $\sigma\tau \in U \implies \sigma\tau \operatorname{Gal}(K/E) \subseteq U$ for some $E \in \mathcal{E}$, where the implication follows since U is open. We argue that $\varphi(\sigma \operatorname{Gal}(K/E) \times \tau \operatorname{Gal}(K/E)) \subseteq U \implies \sigma \operatorname{Gal}(K/E) \times \tau \operatorname{Gal}(K/E) \subseteq \varphi^{-1}(U)$, thus implying that (σ, τ) has an open neighborhood in $\varphi^{-1}(U)$, and hence is open. Indeed, let $\alpha_1, \alpha_2 \in \operatorname{Gal}(K/E)$. Then $\sigma\alpha_1\tau\alpha_2 = \sigma\tau \cdot (\tau^{-1}\alpha_1\tau\alpha_2)$. Since $\operatorname{Gal}(K/E)$ is a normal subgroup of $\operatorname{Gal}(K/k)$, $\tau^{-1}\alpha_1\tau = \alpha_1'$ for some $\alpha_1' \in \operatorname{Gal}(K/E)$, and thus $\sigma\alpha_1\tau\alpha_2 = \sigma\tau\alpha_1'\alpha_2 \in \sigma\tau \operatorname{Gal}(K/E) \subseteq U$, as desired. ■

We now characterize the topology induced by this basis.

Theorem 2.2. $\operatorname{Gal}(K/k)$ is compact, Hausdorff and totally disconnected under the Krull topology.

Remark. Recall that a topological space is called totally disconnected if it has only singletons as connected subsets. Subspaces and products of totally disconnected spaces are totally disconnected.

Proof. Consider the map:

$$\Phi : \mathrm{Gal}(K/k) \mapsto \prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$$

which maps $\mathrm{Gal}(K/k) \ni \sigma \mapsto \Phi(\sigma) := (\sigma|_E)_{E \in \mathcal{E}} \in \prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$. Note that $\sigma|_E \in \mathrm{Gal}(E/k)$ since E is normal. Furthermore, note that $\mathrm{Gal}(E/k)$ is a finite set for any $E \in \mathcal{E}$, and we equip $\mathrm{Gal}(E/k)$ with the discrete topology. Being a finite set equipped with the discrete topology, $\mathrm{Gal}(E/k)$ is compact and Hausdorff, and thus $\prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$ is also compact (by Tychonoff's theorem) and Hausdorff. Finally, the discrete topology naturally makes $\mathrm{Gal}(E/k)$ totally disconnected, and hence $\prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$ totally disconnected.
We first claim that Φ **is continuous**: For that, it is enough to show that $\pi_E \circ \Phi$ is continuous, where $\pi_E : \prod_{F \in \mathcal{E}} \mathrm{Gal}(F/k) \mapsto \mathrm{Gal}(E/k)$ is the canonical projection map. But $\pi_E \circ \Phi$ is just the restriction map $\mathrm{Gal}(K/k) \mapsto \mathrm{Gal}(E/k)$, and $(\pi_E \circ \Phi)^{-1}(\tau) = \tau \,\mathrm{Gal}(K/E) \in \mathcal{B}$ for any $\tau \in \mathrm{Gal}(E/k)$, as desired.
Secondly, we claim that Φ **is injective**: Indeed, suppose $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/k)$ are such that $\sigma_1(x) \neq \sigma_2(x)$ for some $x \in K$. Let L be the normal closure of x in K. Then note that L/k is finite Galois, and $(\sigma_1)|_L \neq (\sigma_2)|_L$, and thus $\Phi(\sigma_1) \neq \Phi(\sigma_2)$.
Thirdly, the **image of** Φ **is closed**. To prove this, we first prove a claim:

Proposition 1. Call a $(\sigma_E)_{E \in \mathcal{E}} \in \prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$ *coherent* if $\sigma_E|_{E'} = \sigma_{E'}$ for any $E, E' \in \mathcal{E}$ such that $E' \subseteq E$. Then $(\sigma_E)_{E \in \mathcal{E}}$ belongs to the image of Φ if and only if it is coherent.

Proof. Clearly, all elements in the image of Φ are coherent. Conversely, suppose $(\sigma_E)_{E \in \mathcal{E}}$ is coherent. Define a map $\sigma : K \mapsto K$ as $\sigma|_E := \sigma_E$ for all $E \in \mathcal{E}$. Note that σ maps every element $\alpha \in K$, since α is contained in its normal closure, which is contained in $\mathcal{E}$. Now, σ is not well-defined only if there exist E, E' such that $\sigma_E|_{E \cap E'} \neq \sigma_{E'}|_{E \cap E'}$. But that is not the case, since $\sigma_E|_{E \cap E'} = \sigma_{E \cap E'} = \sigma_{E'}|_{E \cap E'}$. Finally, also note that σ is in fact an automorphism, since for any $x, y \in K$, with the normal closure of x being L_x, and y being L_y, all the automorphism axioms are satisfied by $\sigma_{L_x L_y}$, and hence by σ. ■

Thus, consider $(\sigma_E)_{E \in \mathcal{E}}$ outside the image of Φ. Then there exists $F, F' \in \mathcal{E}$ with $F' \subseteq F$ such that $\sigma_F|_{F'} \neq \sigma_{F'}$. Then note that $(\sigma_E)_{E \in \mathcal{E}} \in \{\sigma_F\} \times \{\sigma_{F'}\} \times \prod_{F \in \mathcal{E} \setminus \{F, F'\}} \mathrm{Gal}(F/k) =: U$, and U is open. Furthermore, no element of U is coherent, and thus $U \cap \mathrm{im}(\Phi) = \varnothing$. Thus, every element in the complement of $\mathrm{im}(\Phi)$ has an open neighborhood outside $\mathrm{im}(\Phi)$, and thus $\mathrm{im}(\Phi)$ is closed.
Finally, Φ **is an embedding**, i.e. the map $\Phi' : \mathrm{Gal}(K/k) \mapsto \Phi(\mathrm{Gal}(K/k))$ is a homeomorphism. We already know that Φ' is a continuous bijection, so it remains to show that $(\Phi')^{-1} : \Phi(\mathrm{Gal}(K/k)) \mapsto \mathrm{Gal}(K/k)$ is continuous, which is equivalent to showing that $\Phi'(B)$ is open in $\Phi(\mathrm{Gal}(K/k))$ for any $B \in \mathcal{B}$. But note that $\Phi(\sigma \,\mathrm{Gal}(K/E))$ is the set of all coherent elements in $\{\sigma|_E\} \times \prod_{F \in \mathcal{E} \setminus E} \mathrm{Gal}(F/k)$, which is open in the subspace topology of the image of Φ.
Thus, the image of Φ is a homeomorphic copy of $\mathrm{Gal}(K/k)$. However, $\mathrm{im}(\Phi)$ is also a closed subspace of $\prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$, which itself is compact Hausdorff. Since closed subspaces of compact Hausdorff domains are compact and Hausdorff, we're done. Furthermore, since subspaces of totally disconnected spaces are totally disconnected, $\mathrm{Gal}(K/k)$ is totally disconnected. ■

As the astute reader might have already noticed, the space of 'coherent' sequences looks like an inverse limit: Indeed, consider the system $\{\mathrm{Gal}(E/k)\}_{E \in \mathcal{E}}$. Note that $(\mathcal{E}, \subseteq)$ is a directed set: The reflexivity and transitivity of $\subseteq$ is obvious, and for any $E_1, E_2 \in \mathcal{E}$, the compositum $E_1 E_2 \in \mathcal{E}$ serves as the common upper bound for E_1, E_2. Furthermore, the homomorphisms are the usual restriction maps, i.e. if $E_1, E_2 \in \mathcal{E}$ are such that $E_1 \subseteq E_2$, then we have the restriction homomorphism

$$\mathrm{res} : \mathrm{Gal}(E_2/k) \mapsto \mathrm{Gal}(E_1/k)$$

where $\mathrm{Gal}(E_2/k) \ni \sigma \mapsto \mathrm{res}(\sigma) := \sigma|_{E_1} \in \mathrm{Gal}(E_1/k)$. Then note that the inverse limit of $\{\mathrm{Gal}(E/k)\}_{E \in \mathcal{E}}$ under the aforementioned restriction maps is precisely the space of coherent sequences. But we also showed earlier that $\mathrm{Gal}(K/k)$ is isomorphic to the space of coherent sequences contained in $\prod_{E \in \mathcal{E}} \mathrm{Gal}(E/k)$. Thus, summarizing the discussion above:

Theorem 2.3.

$$\mathrm{Gal}(K/k) \cong \varprojlim \mathrm{Gal}(E/k)$$

where E ranges over all the finite Galois subextensions of K/k.

As it turns out, we can extract further unexpected mileage with the above characterization.

Lemma 2.4. Let G be an infinite compact Hausdorff topological group. Then G is uncountable.

Proof. Since G is Hausdorff, singletons are closed (for any $x \in G$, for every $y \in G$, $y \in U_y$, where U_y is an open set not containing x. Then $G \setminus \{x\} = \bigcup_{y \neq x} U_y$ is open, and thus $\{x\}$ is closed). Since G is compact, and a topological group, no singleton set is open (Since G is a topological group, if any singleton is open, all singletons have to be open. If all singletons are open, then taking their union gives an infinite open cover for G, which doesn't have any finite subcover, which can't be, if G is compact). Thus all singletons are closed sets with empty interiors. Now, by the Baire Category Theorem, compact Hausdorff spaces are Baire spaces, and thus G is a Baire space. Also, G is a union of closed sets with empty interiors. Since G doesn't have an empty interior, G has to be uncountable. ■

Corollary 2.5. Any infinite Galois group is uncountable.

§3. Galois Correspondence

Note that the usual Galois correspondence for finite extensions no longer works for infinite extensions: Indeed, consider the extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$. Note that the only finite subextensions of this extension are $\mathbb{F}_{p^n}/\mathbb{F}_p$ for all $n \in \mathbb{N}$. Now, let $\varphi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ denote the Frobenius map, i.e. $\overline{\mathbb{F}}_p \ni x \mapsto \varphi(x) := x^p \in \overline{\mathbb{F}}_p$. Recall that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi|_{\mathbb{F}_{p^n}} \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Thus, by Theorem 2.3,

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}}$$

where the restriction maps are defined as $\mu_{mn} : \mathbb{Z}/m\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z} \ni \overline{x} \mapsto \mu_{mn}(\overline{x}) := x \bmod n \in \mathbb{Z}/n\mathbb{Z}$ for all $n \mid m$.

Now, note that $\overline{\mathbb{F}}_p^{\langle\varphi\rangle} = \mathbb{F}_p$: Indeed, for any $x \in \overline{\mathbb{F}}_p \setminus \mathbb{F}_p$, we have $x \in \mathbb{F}_{p^n}$ for some n, and some power of the Frobenius automorphism moves x, since $\mathbb{F}_{p^n}^{\langle\varphi\rangle} = \mathbb{F}_{p^n}^{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)} = \mathbb{F}_p$. However, **we do not have** $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \langle\varphi\rangle$: Indeed, $\langle\varphi\rangle$ being a cyclic group is countable, while $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is uncountable.

However, we can make some 'topological' amends, and the usual Galois correspondence goes through. We first investigate some ways in which the topology of the Galois group interacts with the group structure.

Proposition 2. Let K/k be a Galois extension, and let F be any subextension, not necessarily finite. Then $\mathrm{Gal}(K/F)$ is a closed subgroup of $\mathrm{Gal}(K/k)$.

Proof. Let $\sigma \in \mathrm{Gal}(K/k) \setminus \mathrm{Gal}(K/F)$. Then there exists $\alpha \in F$ such that $\sigma(\alpha) \neq \alpha$. Let L be the normal closure of α. Then note that $\sigma\,\mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/F) = \varnothing$, because every element of $\sigma\,\mathrm{Gal}(K/L)$ moves α, while no element of $\mathrm{Gal}(K/F)$ does. But $\sigma\,\mathrm{Gal}(K/L)$ is open, and we're done. ■

Remark. Note that if F/k is a finite Galois extension, and $\sigma \in \operatorname{Gal}(K/k)$ is arbitrary, then $\sigma \operatorname{Gal}(K/F)$ is both open and closed.

Lemma 3.1. Let H be a subgroup of $G := \operatorname{Gal}(K/k)$. Then $\operatorname{Gal}(K/K^H) = \overline{H}$, i.e. $\operatorname{Gal}(K/K^H)$ equals the closure of H in G.

Proof. Clearly, $H \subseteq \operatorname{Gal}(K/K^H)$. Furthermore, by Proposition 2, $\operatorname{Gal}(K/K^H)$ is also closed, and thus $\overline{H} \subseteq \operatorname{Gal}(K/K^H)$. Now, suppose $\sigma \in \operatorname{Gal}(K/k) \setminus \overline{H}$. If we can show that $\sigma \notin \operatorname{Gal}(K/K^H) \iff \sigma$ moves something in K^H, we'll be done. Since $\operatorname{Gal}(K/k) \setminus \overline{H}$ is open, σ is contained in some basic open set, i.e. $\sigma \operatorname{Gal}(K/F) \cap \overline{H} = \varnothing$ for some $F \in \mathcal{E}$. Now AFTSOC there is no $\alpha \in K^H$ which σ also doesn't fix. Then $\sigma|_F$ fixes $F^{H|_F} \subseteq K^H$, where $H|_F := \{h|_F : h \in H\}$. But then $\sigma|_F \in \operatorname{Gal}(F/F^{H|_F}) = H|_F$, which implies there exists $h \in H$ such that $\sigma|_F = h|_F \implies \sigma \operatorname{Gal}(K/F) = h \operatorname{Gal}(K/F) \implies h \in \sigma \operatorname{Gal}(K/F) \implies \sigma \operatorname{Gal}(K/F) \cap \overline{H} \supset \{h\} \neq \varnothing$, leading to a contradiction. ■

Corollary 3.2. If H is a closed subgroup of $\operatorname{Gal}(K/k)$, then $\operatorname{Gal}(K/K^H) = H$.

Corollary 3.3. For any subgroup H of $\operatorname{Gal}(K/k)$, $K^H = K^{\overline{H}}$.

Proof. Note that $K^H = K^{\operatorname{Gal}(K/K^H)}$: Indeed, $H \subseteq \operatorname{Gal}(K/K^H)$, so $K^H \supseteq K^{\operatorname{Gal}(K/K^H)}$, and the reverse inequality is immediate too. But $K^{\operatorname{Gal}(K/K^H)} = K^{\overline{H}}$. ■

Theorem 3.4 (Galois Correspondence)**.** Let K/k be a Galois extension equipped with the Krull topology. Then for any closed subgroup H of $\operatorname{Gal}(K/k)$, $\operatorname{Gal}(K/K^H) = H$. Similarly, for *any* intermediate subfield E of K, $K^{\operatorname{Gal}(K/E)} = E$. Consequently, there is a bijection between the closed subgroups of $\operatorname{Gal}(K/k)$ and the intermediate subfields of K/k given by $E \rightsquigarrow \operatorname{Gal}(K/E)$, $H \rightsquigarrow K^H$.

References

[Chu23] Swayam Chube. Field and galois theory, 2023. URL: https://swayamchube.github.io/research-interests/galois/main.pdf.

[Con20] Keith Conrad. Infinite galois theory, 2020. URL: https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf.

[Wat74] William Waterhouse. Profinite groups are galois groups. *PROCEEDINGS of the AMERICAN MATHEMATICAL SOCIETY*, 42(2), 1974.