PROFINITE GROUPS AND INFINITE GALOIS THEORY

ZHUO ZHANG

Abstract. The purpose of this short expository paper is to give a self-contained introduction to the basics of profinite groups and a proof of the infinite Galois correspondence, assuming only knowledge of elementary Galois theory, category theory, and topology.

1. Profinite Groups

Definition 1.1. A topological group G is called *profinite* if it is isomorphic to the inverse (projective) limit of finite groups with discrete topology.

Note that the inverse limit of topological groups is a topological group under the componentwise multiplication and the subspace topology.

Example 1.2. The ring of p-adic integers, defined by

$$\mathbb{Z}_p = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})$$

is a profinite group, where the inverse system consists of the maps $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, for $m \leq n$.

Remark 1.3. Here are some simple but useful observations about topological groups that might come in handy later:

(i) Any open subgroup is closed.
(ii) Any closed subgroup of finite index is open.
(iii) In a compact group, any open subgroup must have finite index.
(iv) Any subgroup that contains an open subgroup is open.

All of the above statements can be easily proved using the fact that a group is the disjoint union of the cosets of any subgroup. For example, if G is compact and H is an open subgroup, then the cosets of H form a minimal open cover of G, and so H must have finite index. This proves (iii).

Here's one of the most important examples of profinite groups. Let L/K be a Galois extension, possibly infinite, with Galois group G. Let F_i denote some finite Galois extension of K contained in L. For every inclusion $F_1 \subset F_2$, we have a (surjective) restriction map $\mathrm{Gal}(F_2/K) \to \mathrm{Gal}(F_1/K)$, and such maps are clearly compatible with each other. The compositum F_1F_2 of the two normal extensions is again normal over K. Hence, the set $\{\mathrm{Gal}(F/K) : F\}$ forms a directed system.

Date: June 19, 2024.

Theorem 1.4. *Let L/K be Galois, possibly infinite. Then*

$$G \cong \varprojlim_F \operatorname{Gal}(F/K),$$

where F ranges over all finite Galois extensions of K contained in L. Thus, G is a profinite group with an inherited topology.

Proof. The idea is that automorphisms of L/K are determined by what they do to finite Galois extensions of K. Indeed, the projections $G \to \operatorname{Gal}(F/K)$ are compatible with the inverse system indexed by F, so there is a canonical map $\phi : G \to \varprojlim_F \operatorname{Gal}(F/K)$. The map ϕ is injective, for if $\sigma \in G$ restricts to the identity map on each F/K, then σ is the identity. The map ϕ is also surjective. Indeed, given $(\sigma_F) \in \varprojlim_F \operatorname{Gal}(F/K)$, we may find $\sigma \in G$ such that $\sigma|_F = \sigma_F$ as follows: for $x \in L$, choose any finite Galois subextension F/K of L containing x, and define $\sigma(x) = \sigma_F(x)$. The choice of such F does not matter, because (σ_F) is taken from an inverse limit and all components are compatible under restrictions. ■

By definition of the inverse limit, we may embed G into the product

$$G \subset \prod_F \operatorname{Gal}(F/K).$$

Each $\operatorname{Gal}(F/K)$ is compact, being a finite group, so the product is compact as well by Tychonoff's theorem. It can be easily checked that G is closed, so G is compact (and obviously Hausdorff).

A neighborhood basis of the product is given by the kernels of the projections onto each factor $\operatorname{Gal}(F/K)$. More explicitly, they are normal subgroups of the form

$$\{e\} \times \prod_{F \neq F_1} \operatorname{Gal}(F/K),$$

where the identity element is taken from the group $\operatorname{Gal}(F_1/K)$. The intersection of this subgroup with G are precisely those elements that fix F_1, i.e., $\operatorname{Gal}(L/F_1)$. Hence, we obtain the following

Lemma 1.5. *Let L/K be Galois. Then a neighborhood basis of G at the identity is given by open normal subgroups of the form* $\operatorname{Gal}(L/F)$*, where F ranges over all finite Galois extensions of K contained in L.*

Lemma 1.6. *Let L/K be Galois, and let E be a finite extension of K contained in L. Then* $\operatorname{Gal}(L/E)$ *is open in G.*

Proof. E is contained in some finite Galois extension F over K, and so $\operatorname{Gal}(L/F) \subset \operatorname{Gal}(L/E) \subset G$. But $\operatorname{Gal}(L/F)$ is open, and so $\operatorname{Gal}(L/E)$ is a union of cosets of $\operatorname{Gal}(L/F)$, and hence must be open. ■

This yields the following

Corollary 1.7. *Let L/K be Galois, and let M be an intermediate field. Let $H = \operatorname{Gal}(L/M) \subset G$. Then subspace topology on H inherited from G is the same as the topology on H as a Galois group.*

Proof. By lemma 1.6, a neighborhood basis of G at the identity is given by open subgroups of the form $\mathrm{Gal}(L/E)$, where E ranges over all finite extensions of K contained in L.

Fix such an E. Then $\mathrm{Gal}(L/E) \cap H = \mathrm{Gal}(L/ME) \subset H$. Since E/K is finite, so is ME/M. Conversely, given any finite extension M'/M contained in L, there is a finite extension E of K such that $M' = ME$, and so $\mathrm{Gal}(L/M') = \mathrm{Gal}(L/E) \cap H$. This shows that intersecting an identity neighborhood basis of G with H gives the same identity neighborhood basis of H as a Galois group, so the two topologies must agree. ■

2. Infinite Galois Correspondence

Recall that for a finite Galois extension L/K, there is a correspondence between intermediate subfields and subgroups of the Galois group G. For infinite extensions, it turns out that G has too many subgroups to make the correspondence hold. However, if we put an appropriate topology on G, then intermediate subfields correspond nicely to the closed subgroups. This topology, as you expect, is the one defined in Theorem 1.4.

We now prove the first half of the correspondence.

Theorem 2.1. *Let L/K be Galois. For any intermediate subfield E, we have*

$$L^{\mathrm{Gal}(L/E)} = E.$$

Furthermore, E/K is normal if and only if $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.

Proof. Clearly $E \subset L^{\mathrm{Gal}(L/E)}$. Now, let $\alpha \in L^{\mathrm{Gal}(L/E)}$ be given. Let M/E be a finite Galois subextension of L/E containing α. Any $\sigma \in \mathrm{Gal}(M/E)$ can be extended to an automorphism $\tilde{\sigma} \in \mathrm{Gal}(L/E)$, due to Zorn's lemma. Hence,

$$\sigma(\alpha) = \tilde{\sigma}(\alpha) = \alpha,$$

because $\alpha \in L^{\mathrm{Gal}(L/E)}$. Since this is true for all σ, we have $\alpha \in E^{\mathrm{Gal}(M/E)} = E$, where the last equality holds by finite Galois theory.

For the second claim, note that E/K is normal iff $gx \in E$ for all $g \in \mathrm{Gal}(L/K)$ and $x \in E$, iff $\sigma gx = gx$ for all g, x, and $\sigma \in \mathrm{Gal}(L/E)$, iff $g^{-1}\sigma gx = x$ for all g, x, σ, iff $g^{-1}\sigma g \in \mathrm{Gal}(L/E)$, iff $\mathrm{Gal}(L/E)$ is a normal subgroup. ■

The other direction of the correspondence is first proved for open subgroups. This makes sense because open subgroups are all closed (although not vice versa).

Theorem 2.2. *Let L/K be Galois, and let V be an open subgroup of G. Then $V = \mathrm{Gal}(L/L^V)$.*

Proof. It suffices to show that $V = \mathrm{Gal}(L/E)$ for some intermediate field E, since then $L^V = E$ by theorem 2.1, and so $\mathrm{Gal}(L/L^V) = \mathrm{Gal}(L/E) = V$.

Since V is open and contains the identity, lemma 1.5 implies that V contains an open normal subgroup of the form $U = \mathrm{Gal}(L/F)$, where F/K is finite Galois. In particular, $\mathrm{Gal}(F/K)$ is finite. The surjective restriction map $G = \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ has kernel $\mathrm{Gal}(L/F) = U$. The image of V is a subgroup of $\mathrm{Gal}(F/K)$, and hence by finite Galois theory, $V/U = \mathrm{Gal}(F/F') \subset \mathrm{Gal}(F/K)$ for some finite extension F'/K. The preimage of V/U under the quotient map is just V; on the other hand, since $V/U = \mathrm{Gal}(F/F')$, the preimage is the set of automorphisms of L/K fixing F', i.e., $\mathrm{Gal}(L/F')$. Thus, $V = \mathrm{Gal}(L/F')$. ■

Now we prove the full theorem.

Theorem 2.3. *Let L/K be Galois. Then the assignments*

$$\begin{tikzcd}
\{\textit{Subfields of } L/K\} & \{\textit{Closed subgroups of } G\} \\
E \arrow[r, mapsto] & \mathrm{Gal}(L/E) \\
L^H & H \arrow[l, mapsto]
\end{tikzcd}$$

are mutual inverses.

Proof. The fact that $L^{\mathrm{Gal}(L/E)} = E$ was proved in Theorem 2.1. We still need to verify that for any subfield E, $\mathrm{Gal}(L/E)$ is closed in G. Clearly E is the union of all finite extensions of K contained in E, call them $\{E_j\}$. Then $\mathrm{Gal}(L/E) = \bigcap_j \mathrm{Gal}(L/E_j)$. By lemma 1.6, each $\mathrm{Gal}(L/E_j)$ is open, hence closed, and so $\mathrm{Gal}(L/E)$ is closed as well, being an intersection of closed sets.

To prove the other direction, let S be a *closed* subgroup of G. Let $E = L^S$, and $T = \mathrm{Gal}(L/E)$. Clearly $S \subset T$. To prove that $S = T$, we argue that S is dense in T, which finishes the proof because S is closed. Note that by Corollary 1.7, we may just consider the topology on T as the Galois group of L/E.

Let V be an open normal subgroup of T, and let $M = L^V$. Then $\mathrm{Gal}(L/M) = V$ by Theorem 2.2. Therefore, $\mathrm{Gal}(M/E) = \mathrm{Gal}(L/E)/\mathrm{Gal}(L/M) = T/V$. On the other hand, $M^{SV/V}$ consists of those $\alpha \in M$ fixed by S, and $M^{SV/V} = L^S = E$. Applying finite Galois theory to T/V (which is a finite group since V has finite index in T), we see that $SV/V = T/V$, i.e., $SV = T$. Hence, each coset of V in T intersects with S. Since open sets in T are precisely unions of cosets of such V's, this shows that S is dense in T, and we are done. ■

References

[1] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory*. London Mathematical Society, 2010.

[2] D. Ramakrishnan and R.J. Valenza. *Fourier Analysis on Number Fields*. Graduate Texts in Mathematics. Springer New York, 1998.