Profinite Groups

(with infinite Galois theory at the end)

Siyan Daniel Li-Huerta

November 19, 2020

In our remaining time, we'll discuss connections to the Galois theory of extensions of number fields. We first introduce *profinite groups*.

Definition

Let G be a topological group. We say G is *profinite* if it is isomorphic to $\varprojlim_{i\in I} G_i$ as a topological group, where $\{G_i\}_{i\in I}$ is a projective system of finite discrete groups.

Proposition

Let G be a profinite group. Then G is compact and Hausdorff, and 1 has a basis of neighborhoods consisting of normal subgroups.

Proof.

Let $\{G_i\}_{i\in I}$ be a projective system of finite discrete groups such that G is isomorphic to $\varprojlim_{i\in I} G_i$. Because the G_i are compact and Hausdorff, so is their projective limit G. We see that the subsets $G \cap \prod_{i\in I} N_i$ form a basis of neighborhoods of 1, where the $N_i = \{1\}$ for cofinitely many i and $N_i = G_i$ otherwise. But these $G \cap \prod_{i\in I} N_i$ are evidently normal subgroups of G, since each N_i is normal in G_i. $\square$

The previous Proposition abstractly characterizes profinite groups.

Proposition

Let G be a topological group. Then G is profinite if and only if it is compact and Hausdorff, and 1 has a basis of neighborhoods consisting of normal subgroups.

Proof.

Let $\{M_i\}_{i \in I}$ be a basis of neighborhoods of 1 consisting of normal subgroups, and order I via declaring $i \geq j$ if and only if $M_i \subseteq M_j$. Then for any $i \geq j$ in I, we get a quotient map $G/M_i \to G/M_j$. Since G is compact and the M_i are open, we see the G/M_i are finite discrete. We have a natural continuous group homomorphism $f : G \to \varprojlim_{i \in I} G/M_i$.

I claim f is injective with dense image. As $f(G)$ must be compact and hence closed, this would imply surjectivity, and the compactness of G and Hausdorffness of $\varprojlim_{i \in I} G/M_i$ would imply f is a homeomorphism. Now, if g in G satisfies $f(g) = 1$, we see g lies in every neighborhood of 1, so 1 lies in $\overline{\{g\}} = \{g\}$. Hence $g = 1$.

Proposition

Let G be a topological group. Then G is profinite if and only if it is compact and Hausdorff, and 1 has a basis of neighborhoods consisting of normal subgroups.

Proof (continued).

For denseness, let U be a nonempty open subset of $\varprojlim_{i \in I} G/M_i$ of the form $(\varprojlim_{i \in I} G/M_i) \cap \prod_{i \in I} U_i$, where the U_i are open subsets of G/M_i such that $U_i = G/M_i$ for all i outside a finite subset $S \subseteq I$. Form the open normal subgroup $N = \bigcap_{i \in S} M_i$, and choose j in I such that $N \supseteq M_j$. For any $(u_i)_{i \in I}$ in U, consider u_j in G/M_j, and choose a representative $\widetilde{u}$ of u_j in G. Now for any i in S, the i-th component of $f(\widetilde{u})$ equals the image of u_j in G/M_i, so it lies in U_i. Therefore $f(\widetilde{u})$ lies in U, so altogether we obtain denseness. □

We can form profinite groups from arbitrary topological groups as follows.

Definition

Let G be a topological group. Its *profinite completion*, denoted by $\widehat{G}$, is the topological group $\varprojlim_{i \in I} G/O_i$, where the O_i range over all open normal finite index subgroups of G.

Examples

Suppose G is...

- profinite. Then the previous proof shows that $G \xrightarrow{\sim} \widehat{G}$.
- $\mathbb{Z}$ with the discrete topology. Then we have $\widehat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$, which by the Chinese remainder theorem is isomorphic to

$$\varprojlim_{m = p_1^{e_1} \cdots p_r^{e_r}} (\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}) = \prod_p \varprojlim_e \mathbb{Z}/p^e\mathbb{Z} = \prod_p \mathbb{Z}_p.$$

  One can show that $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} \mathbb{A}_{\mathbb{Q}}^{\infty}$, where the latter is defined to be $\mathbb{A}_{\mathbb{Q}}/\mathbb{R}$.

Examples (continued)

Suppose G is...

- $\mathbb{R}$ with the Euclidean topology. The only open subgroup of $\mathbb{R}$ is itself, so its profinite completion is trivial.
- $\prod_{i=1}^{\infty} \mathbb{F}_2$ with the product topology. As this is profinite, it's isomorphic to its profinite completion. Note that open subgroups must contain cofinitely many $\mathbb{F}_2$-factors, so there must be countably many open subgroups.
- $\prod_{i=1}^{\infty} \mathbb{F}_2$ with the discrete topology. Now $\prod_{i=1}^{\infty} \mathbb{F}_2$ is an uncountable-dimensional $\mathbb{F}_2$-vector space, so it has uncountably many finite index subgroups. With the discrete topology, they are all open! One can show its profinite completion is not isomorphic to $\prod_{i=1}^{\infty} \mathbb{F}_2$.

An important example comes from *infinite Galois theory*. Let E/F be a (not necessarily finite) Galois extension. By extending automorphisms, we see that $\mathrm{Gal}(E/F) \xrightarrow{\sim} \varprojlim_K \mathrm{Gal}(K/F)$ as groups, where K ranges over subextensions $E \supseteq K \supseteq F$ such that K/F is finite Galois.

We view the $\mathrm{Gal}(K/F)$ as finite discrete groups, and we equip $\mathrm{Gal}(E/F)$ with the resulting topological group structure. One can show then that subextensions $E \supseteq L \supseteq F$ correspond bijectively to closed subgroups of $\mathrm{Gal}(K/F)$, where L corresponds to $\mathrm{Gal}(E/L)$, and closed subgroups H of $\mathrm{Gal}(K/F)$ correspond to the fixed field E^H.

Example

Take $E = \overline{\mathbb{F}}_p$ and $F = \mathbb{F}_p$. Then $E = \bigcup_{m=1}^{\infty} \mathbb{F}_{p^m}$, and $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ is canonically isomorphic to $\mathbb{Z}/m\mathbb{Z}$ via sending 1 to the p-th power Frobenius map ϕ. Hence $\mathrm{Gal}(E/F)$ is isomorphic to the topological group $\varprojlim_m \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) = \varprojlim_m \mathbb{Z}/m\mathbb{Z} = \widehat{\mathbb{Z}}$.

To see the necessity of the closed condition in the Galois correspondence, consider the proper subgroup $\mathbb{Z} \subset \widehat{\mathbb{Z}} = \mathrm{Gal}(E/F)$. It's generated by ϕ, so its fixed field equals $E^{\phi} = \mathbb{F}_p = F$. But this is also the fixed field of all of $\mathrm{Gal}(E/F)$! So in order to obtain a bijective Galois correspondence, we must restrict to closed subgroups. For general subgroups H of $\mathrm{Gal}(E/F)$, its fixed field equals that of $\overline{H}$.

Let F be a field. The largest possible Galois extension of F would be a separable closure F^{sep} of F.

Definition

The *absolute Galois group* of F (with respect to F^{sep}), denoted by Γ_F, is the topological group $\text{Gal}(F^{\text{sep}}/F)$.

Thus studying separable extensions of F is equivalent to studying the topological group Γ_F.