Math 210B Lecture 10 Notes

Daniel Raban

January 30, 2019

1 Profinite Groups and Infinite Galois Theory

1.1 Galois groups of infinite field extensions

Example 1.1. Consider $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. It maps to each $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, so $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. This is injective because an element of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is determined by what it does to $\mathbb{F}_{p^n}$ for all n. It is surjective because we can keep lifting elements in $\mathrm{Gal}(\mathbb{F}_{p^n}.\mathbb{F}_p)$.

This example had nothing to do with $\mathbb{F}_p$. In fact, for any Galois extension K/F,

$$\mathrm{Gal}(K/F) \cong \varprojlim_{\substack{E \subseteq K \\ E/F \text{ finite, Galois}}} \mathrm{Gal}(E/F).$$

Then

$$\varprojlim_n \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

the Prüfer ring. $\mathbb{Z} < \hat{\mathbb{Z}}$ says that $\langle \varphi_p \rangle < \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbb{F}_p)$. Then $\overline{\mathbb{F}}_p^{\langle \varphi_p \rangle} = \mathbb{F}_p$. So $\mathrm{Gal}(K, K^H)$ can be bigger than H.

Suppose we have an inverse system $(G_i, \phi_{i,j})$ of groups, where I is a directed set. That is, given $i, j \in I$, there exists some k such that $k \leq i$ or $k \leq j$, and $\phi_{i,j} : G_i \to G_j$. Recall that the inverse limit $\varprojlim_i G_i \subseteq \prod_{i \in I} G_i$ is $\varprojlim_i G_i = \{(g_i)_{i \in I} : \phi_{i,j}(g_i) = g_j \,\forall i, j\}$. Then the Galois group will be $G = \varprojlim_{i \in I} G_i$. If

$$\begin{tikzcd}[column sep=small]
 & EE' \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash] & & E' \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

then $\mathrm{Gal}(EE'/F)$ surjects onto both $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(E'/F)$.

1.2 Topological and profinite groups

Definition 1.1. A **topological group** G is a group with a topology such that the multiplication map $G \times G \to G$ and inversion map $G \to G$ sending $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous.

Then $\prod_{i \in I}$ has the product topology, which is generated by the base

$$\prod_{j \in J} U_j \times \prod_{i \in I \setminus J} X_i,$$

where $U_j \subseteq X_j$ is open.

Then $G = \varprojlim_i G_i$ has the subspace topology induced from the product topology. G is a topological group with respect to this topology (exercise).

Definition 1.2. A **profinite group** is an inverse limit of finite groups $G = \varprojlim G_i$ endowed with the above topology, the **profinite topology** relative to $(G_i, \phi_{i,j})$

Example 1.2. Let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. Then $\pi_n : \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ is continuous, and $n\hat{\mathbb{Z}} = \ker(\pi_n) = \pi_n^{-1}(\{0\})$ is open. Then $n\hat{\mathbb{Z}}$ is a base of open neighborhoods of 0. Then $\{a + n\hat{\mathbb{Z}}\}$ is a basis of open neighborhoods of $a \in \mathbb{Z}$. Since $\mathbb{Z}$ surjects onto $\mathbb{Z}/n\hat{\mathbb{Z}}$, we can find $a_n \in \mathbb{Z}$ such that $a_n \mapsto a + n\hat{\mathbb{Z}}$ for all n. So $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$; that is, its closure is $\hat{\mathbb{Z}}$.

Theorem 1.1. *A topological group G is profinite if and only if it is compact, Hausdorff, and totally disconnected (every connected component is a point).*

Let's assume the following fact from topology.

Proposition 1.1. *A compact, Hausdorff space is totally disconnected if and only if it has a base of clopen neighborhoods.*

We will prove one direction of the theorem.

Proof. Assume G is profinite. Products of compact, Hausdorff spaces are compact, Hausdorff. Closed subsets of Hausdorff spaces are compact, and subsets of Hausdorff spaces are Hausdorff. To show that G is closed, note that

$$G = \bigcap_{\phi_{i,j}} \{(g_i)_{i \in I} : \phi_{i,j}(g_i) = g_j\}.$$

Now let U_j be open for all $j \in J$ with J finite. Then

$$\left(\prod_{j \in J} U_j \times \prod_{i \in I \setminus J} G_i \right)^c = \left(\bigcap_{j \in J} \left(U_j \times \prod_{i \neq j} G_i \right) \right)^c$$

$$= \bigcup_{j \in J} \left(U_j \times \prod_{i \neq j} G_i \right)^c$$
$$= \bigcup_{j \in J} U_j^c \times \prod_{i \neq j} G_i.$$

So $\prod_i G_i$ is totally disconnected. So $G = \varprojlim G_i$ is totally disconnected. $\square$

Let $\pi_I : G \to G_i$. Then $\ker(\pi_i) = (\prod_{j \neq i} G_j) \times \{1\}$. Then $\prod_{i \in I \setminus J} G_i \times \prod_{j \in J} \{1\}$ is a basis of neighborhoods of 1. Then $\bigcap \varprojlim_i G_i = \bigcap_{j \in J} \ker(\pi_j)$ is an open subgroup of $\varprojlim G_i$ with finite index.

Proposition 1.2. *In profinite groups, subgroups are open if and only if they are closed and have finite index.*

Proof. ($\Longleftarrow$): If $H \leq G$ is closed of finite index, then $\{gH : gH \neq H\} \subseteq G/H$ is a finite set. Each gH is closed, so $\bigcup_{gH \neq H} gH = H^c$. So H is open. $\square$

Definition 1.3. The **Krull topology** on $\mathrm{Gal}(K/F)$ is the profinite topology for

$$\mathrm{Gal}(K/F) = \lim_{\substack{E \subseteq K \\ E/F \text{ finite}}} \mathrm{Gal}(E/F).$$

Definition 1.4. If G is a group, the **profinite completion** is

$$\hat{G} = \varprojlim_{\substack{N \trianglelefteq G \\ \text{finite index}}} N.$$

This gives a functor from the category of groups to the category of topological groups.

1.3 The fundamental theorem of Galois theory for infinite degree extensions

Theorem 1.2 (fundamental theorem of Galois theory)**.** *Let K/F be Galois. There are inverse, inclusion reversing correspondences $\{E : K/E/F\} \to \{H : H \leq \mathrm{Gal}(K/F), H \text{ closed}\}$ sending $E \mapsto \mathrm{Gal}(K/E)$ and $H \mapsto K^H$. Respective correspondences exist for finite or normal extensions to open or normal subgroups. If E/F is normal, then $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)$, where this is a topological isomorphism.*

Example 1.3. The **absolute Galois group** of $\mathbb{Q}$ is $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example 1.4. The absolute Galois group of $\mathbb{R}$ is $G_{\mathbb{R}} \cong \mathbb{Z}/2\mathbb{Z}$.

Example 1.5. The absolute Galois group of $\mathbb{F}_p$ is $\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$,where $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Theorem 1.3 (Kronecker-Weber)**.** *Let μ_n be a primitive n-th root of unity, and let $\mathbb{Q}^{ab} = \bigcup_n \mathbb{Q}(\mu_n)$. Then $G_{\mathbb{Q}^{ab}} = \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$*