MA 252 notes - infinite Galois theory

Dan Abramovich

Brown University

March 23, 2017

Projective limits

Recall:

- Given a poset I (or more generally a small category), consider a diagram in a category C is a functor $I \to C$, namely objects $A_\alpha, \alpha \in I$ and arrows $\phi_{\alpha,\beta} : A_\alpha \to A_\beta$ whenever $\alpha \to \beta$.
- A projective limit is a system of arrows $\phi_\alpha : A \to A_\alpha$ making the diagram commutative, and we write $A = \varprojlim(A_\alpha, \phi_{\alpha,\beta})$.
- Projective limits exist in Sets - they are subsets of the product. This induces projective limits in Groups, Rings, Topological Spaces, Topological Groups.
- If the partial order is trivial get the usual product.
- Get $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{N}$ (with $I = \mathbb{N}^{op}$), $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ (Natural numbers ordered by reversed division).

Galois extensions

Definition

A finite extension K/F is Galois if $|\operatorname{Aut}(K/F)| = [K : F]$. In this case we denote $Gal(K/F) := \operatorname{Aut}(K/F)$ and call it the Galois group of K/F.

Definition

An extension K/F is Galois if it is algebraic, normal and separable.

The Fundamental Theorem of Galois Theory: finite case

(1) Given finite Galois K/F with Galois group G there is a bijection

$$\begin{array}{rcl} \{\text{intermediate fields } E\} & \leftrightarrow & \{H < G\} \\ E & \mapsto & G_E := \mathrm{Aut}(K/E) \\ K^H & \leftarrow\!\shortmid & H \end{array}$$

(2) This is order reversing: $E_1 \subset E_2 \Leftrightarrow G_{E_1} > G_{E_2}$.

(3) K/E is always Galois, with Galois group G_E.

(4) We have $[K : E] = |G_E|$ and $[E : F] = [G : G_E]$.

(5) If $E_i \leftrightarrow H_i$ then $E_1E_2 \leftrightarrow H_1 \cap H_2$.

(6) If $E_i \leftrightarrow H_i$ then $E_1 \cap E_2 \leftrightarrow \langle H_1H_2 \rangle$.

(7) For $\tau \in G$ the field $\tau(E)$ corresponds to $\tau G_E \tau^{-1}$.

(8) E/F is Galois if and only if $G_E \triangleleft G$, in which case $\mathrm{Gal}(E/F) = G/G_E$.

Infinite Galois extensions

- Let K/F be Galois, and $F \subset E \subset K$ such that E/F is finite Galois. Since every automorphism of E lifts to an automorphism of K, we have an epimorphism $\phi_E : Gal(K/F) \to G_E := Gal(E/F)$.
- If $F \subset E_1 \subset E_2 \subset K$ and $\phi_{E_2,E_1} : G_{E_2} \to G_{E_1}$ the restriction, then clearly $\phi_{E_1} = \phi_{E_1,E_2} \circ \phi_{E_2}$.
- Given an element $\sigma \in Gal(K/F)$ we obtain a compatible system $\phi(\sigma) = (\sigma_E)_{E/K \text{ Galois intermediate}}$. This is a homomorphism.
- Given a compatible system (σ_E) we define $\psi(\sigma_E) = \sigma$ with $\sigma(\alpha) = \sigma_E(\alpha)$ for a Galois extension containing α. It is a well-defined homomorphism.

Theorem

$Gal(K/F) \to \varprojlim(G_E, \phi_{E_1,E_2})$ is an isomorphism.

- Indeed the two homomorphisms are inverse to each other.

Examples

- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z}$, the system ordered by divisibility, so $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) = \varprojlim(\mathbb{Z}/n\mathbb{Z}) = \hat{\mathbb{Z}}$.
- $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, the system ordered by divisibility, so $Gal(\mathbb{Q}(\boldsymbol{\mu})/\mathbb{Q}) = \varprojlim((\mathbb{Z}/n\mathbb{Z})^\times) = \hat{\mathbb{Z}}^\times$. By Kronecker-Weber this is $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$.
- $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) = \widehat{\mathbb{Q}_p^\times} = \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times$, where $\widehat{\mathbb{Q}_p^\times}$ stands for the pro-finite completion. This is part of local class field theory, the best proof of which is in a magnificent paper of Lubin and Tate.
- Global class field theory says that, for a number field K, we have $Gal(K^{ab}/K) = \widehat{C_K}$, where C_K is the idele class group $\mathbb{A}_K^\times/K^\times$ of K.

Topologies

- The group $G = Gal(K/F)$ is a pro-finite group. Finite sets are compact Hausdorff discrete topologies. So automatically G is a compact Hausdorff topological group.
- We have a group homomorphism $ev : G \to K^K$ sending σ to the map $(\alpha \mapsto \sigma(\alpha))$. K^K has the product topology of Zariski topologies.

Lemma

ev is a homeomorphism onto the image, namely the profinite topology is the induced topology.

- Clearly $ev^{-1}F_{\alpha,\beta} = ev_\alpha^{-1}(\beta)$ is closed, since it is the inverse image of the same in $E_{\alpha,\beta}$.
- If α_i generate E then the cylinder defined by $\bar\sigma \in G_E$ is the intersection of $ev^{-1}F_{\alpha_i,\bar\sigma(\alpha_i)} = ev_{\alpha_i}^{-1}(\bar\sigma(\alpha_i))$.

Correspondence

Proposition

For any intermediate $E \subset L \subset K$ we have $Gal(K/L) \subset G$ closed. The induced topology is its profinite topology.

Indeed it is the intersection of $ev^{-1}F_{\alpha,\alpha} = ev_\alpha^{-1}(\alpha)$ over $\alpha \in L$. The induced topology is induced either way from K^K.

Proposition

$K^{Gal(K/L)} = L$.

Let $\alpha \in K^{Gal(K/L)}$ and let $L \subset E \subset K$ be intermediate Galois containing α. Then $\alpha \in E^{Gal(E/L)} = L$.

Proposition

$Gal(K/K^H) = \bar{H}$.

$L := K^H = K^{\bar{H}}$. Let E/L finite Galois intermediate. Then $\bar{H} \to Gal(E/L)$ has image $\hat{H}$, where $E^{\hat{H}} \subset K^{\bar{H}} = L$, so $\hat{H}$ is dense hence $\bar{H} = Gal(K/L)$.

Fundamental theorem: infinite case

(1) Given finite Galois K/F with Galois group G there is a bijection

$$\begin{array}{rcl} \{\text{intermediate fields } E\} & \leftrightarrow & \{H < G \text{ closed }\} \\ E & \mapsto & G_E := \mathrm{Aut}(K/E) \\ K^H & \leftarrow\!\shortmid & H \end{array}$$

(2-8) as before.

(9) E/F finite $\Leftrightarrow H < G$ open.

For (9) we use:

Lemma

An open subgroup $H < G$ in a topological group is closed. A closed subgroup in a profinite group is open if and only if it is of finite index.

If H open then each coset $Hx \subset G$ is open so $H = G \setminus \cup_{x \notin H} Hx$ is closed. In the profinite case the open covering $G = \cup_{x \in G} Hx$ has a finite covering so H is of finite index.

Examples

- The quotient $Gal(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathbb{Z}_p^\times$ corresponds to $\mathbb{Q}(\mu_{p^\infty})$.
- The quotients $Gal(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \hat{\mathbb{Z}}$ corresponds to the maximal unramified extension, whose residue field is $\bar{\mathbb{F}}_p$.
- The other quotient corresponds to purely wild extensions, related to Eisenstein polynomials, where Lubin-Tate take over.