Infinite Galois theory

Inverse limits

Easy version. Consider a sequence of surjective maps of finite sets

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \leftarrow \cdots$$

Define $$\varprojlim_n A_n := \left\{ (a_1, a_2, \cdots) \,\middle|\, \begin{array}{l} a_i \in A_i \\ f_i(a_{i+1}) = a_i \end{array} \right\}$$

This is called the inverse limit/projective limit/limit (反向极限) of the A_i's.

When each A_n has a structure of groups/rings, and f_i's are homomorphisms,

the inverse limit is a group/ring.

Example. p prime $\quad \mathbb{Z}/p\mathbb{Z} \xleftarrow{f_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{f_2} \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$

The inverse limit is $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$, the ring of **$p$-adic numbers**

$$\mathbb{Z}_p = \left\{ (x_1, x_2, \cdots) \,\middle|\, x_i \in \mathbb{Z}/p^i\mathbb{Z} \,,\ x_{i+1} \bmod p^i = x_i \right\}$$

E.g. $p=7$, 2 is invertible in $\mathbb{Z}_7$.

$$2x_1 = 1 \bmod 7 \ \Rightarrow x_1 = 4 \bmod 7$$

$$2x_2 = 1 \bmod 4 \ \Rightarrow x_2 = 25 \bmod 49 \overset{\bmod 7}{\equiv} 4 \bmod 7$$

$\cdots\cdots$

Can solve each $x_i \bmod 7^i \Rightarrow 2$ is invertible in $\mathbb{Z}_7$.

Same argument shows $\mathbb{Z}_p^\times = \left\{ (x_1, x_2, \cdots) \in \mathbb{Z}_p \,\middle|\, x_1 \neq 0 \right\}$

(In general, if $R = \varprojlim_n R_n$, then $R^\times = \varprojlim_n R_n^\times$.

Indeed, $R^\times = \left\{ \underline{a} = (a_1, a_2, \cdots) \in R \,\middle|\, \exists\, \underline{b} = (b_1, b_2, \cdots) \in R \text{ s.t. } \underline{a} \cdot \underline{b} = 1 \right\}$

$\Rightarrow$ For each $\underline{a} \in R^\times$, $a_n \in R_n^\times$ for every n.

Conversely, for each $\underline{a} \in \varprojlim_n R_n^\times$, the inverse a_n^{-1} of each a_n is unique,

so $f_n(a_{n+1}^{-1}) = a_n^{-1} \Rightarrow \underline{a}^{-1} \in \varprojlim_n R_n$.

So $R^\times = \varprojlim_n R_n^\times$.)

Note also $\mathbb{Z} \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ (this is an injection.)

$a \longmapsto (a \bmod p, a \bmod p^2, \dots)$

Example (Why call this limit?) $\mathbb{C}[[x]] := \varprojlim_n \mathbb{C}[x]/(x^n)$

Given a complex function f on $\mathbb{C}$, holomorphic at 0,

the Taylor expansion at 0 defines an element in $\mathbb{C}[[x]]$

Generalization of inverse limit.

Let I be a partially ordered set, i.e. $\forall$ two elements $i \neq j \in I$, either $i<j$ or $j>i$, or not comparable

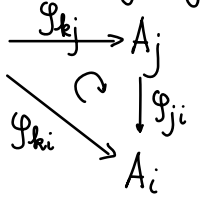
satisfying $i<j$, $j<k \Rightarrow i<k$

We say that I is filtered if $\forall i,j \in I$, $\exists k \in I$ s.t. $i<k$ and $j<k$

Suppose that for each $i \in I$, we are given a set/group/ring A_i

& if $j>i$, we have a map/homomorphism $\varphi_{ji}: A_j \to A_i$

s.t. if $k>j>i$, then

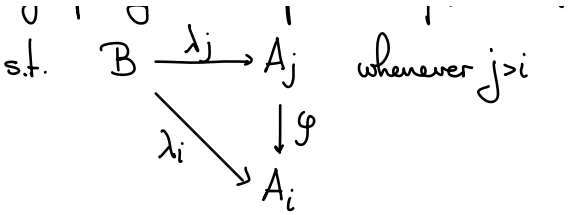


Define the inverse limit set/group/ring

$$\varprojlim_{i \in I} A_i = \left\{ (a_i)_{i \in I} \;\middle|\; \begin{array}{l} a_i \in A_i \text{ and} \\ \text{if } j>i,\ \varphi_{ji}(a_j) = a_i \end{array} \right\} \subseteq \prod_{i \in I} A_i$$

For every $i \in I$, there's a projection $\varprojlim_{i \in I} A_i \longrightarrow A_i$

- If B is a set/group/ring with maps/homomorphisms $\lambda_i : B \to A_i$



then there's a natural map/homomorphism $B \longrightarrow \varprojlim_{i\in I} A_i$

Example. $\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ inverse limit by divisibility (i.e. for $m|n$, $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$)

Fact: $\hat{\mathbb{Z}} \simeq \prod_{p \text{ prime}} \mathbb{Z}_p$

Proof: $\varphi_p : \hat{\mathbb{Z}} \longrightarrow \mathbb{Z}_p \quad \rightsquigarrow \varphi = \prod_p \varphi_p : \hat{\mathbb{Z}} \longrightarrow \prod_{p \text{ prime}} \mathbb{Z}_p.$

$(a_n)_n \longmapsto (a_{p^r})_r$

Conversely, to construct, $\prod_p \mathbb{Z}_p \longrightarrow \hat{\mathbb{Z}}$

it is enough to construct compatible family of maps $\prod_p \mathbb{Z}_p \longrightarrow \mathbb{Z}/n\mathbb{Z}$

If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\prod_p \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r} \longrightarrow \mathbb{Z}/p_1^{\alpha_1} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r} \simeq \mathbb{Z}/n$. □

More similar examples: $GL_N(\hat{\mathbb{Z}}) = \prod_{p \text{ prime}} GL_N(\mathbb{Z}_p)$

Topology of inverse limit: Assume that I is a filtered poset.

(Typically, we provide each A_i with discrete topology.)

Topology on $\varprojlim_{i\in I} A_i$: ↳ require $\varphi_{ji} : A_j \to A_i$ to be continuous.

Method 1 (A_i with discrete topology) An open subset is a union of basic opens:

for each $i \in I$ and each $a_i \rightsquigarrow \pi_i^{-1}(a_i) \subseteq A$ is a basic open.

Method 2 Embed $\varprojlim_{i\in I} A_i \subseteq \prod_{i\in I} A_i$ ← product topology

↑ closed subset

(They are equivalent because $\pi_i^{-1}(a_i) = \left(\{a_i\} \times \prod_{j\neq i} A_j\right) \cap \varprojlim_{i\in I} A_i$.)

Theorem. If each A_i is compact + Hausdorff (e.g. finite), then $\varprojlim_{i\in I} A_i$ is compact + Hausdorff.

Proof: $\prod_{i\in I} A_i$ is compact + Hausdorff by Tychonov theorem

$\Rightarrow \varprojlim_{i\in I} A_i$ is compact + Hausdorff.

E.g. $\mathbb{Z}_p$, $\hat{\mathbb{Z}}$, $\mathbb{Z}_p^\times$, $\hat{\mathbb{Z}}^\times$ are compact Hausdorff topology groups

Definition A topological group is a group G with a topology on the underlying subset such that $\iota: G \to G$ and $m: G\times G \to G$ are continuous.

$g \mapsto g^{-1}$ $\qquad$ $(g,h) \mapsto gh$

- If $U \subseteq G$ is open, then $gUh \subseteq G$ is open
- If $H \subseteq G$ is an open subgroup, then H is also closed.

(b/c $G = \coprod_{g\in G/H} gH$ is a disjoint union. But each gH is open

$\Rightarrow H = G \setminus \left(\underbrace{\coprod_{gH\neq H} gH}_{\text{open.}}\right)$ is closed.)

- If G is a compact group, then an open subgroup $H \leq G$ is of finite index

(Proof: This is because $G = \coprod_{g\in G/H} gH$ is an open disjoint cover.

compactness $\Rightarrow$ this is a finite cover, so $[G:H] < +\infty$.)

- Conversely, if $H \leq G$ is a closed subgroup of finite index $\Rightarrow H$ is open.

($G = \coprod gH \Rightarrow H = G \setminus \left(\underbrace{\bigcup_{H\neq gH} gH}_{\uparrow \text{finite union of closed subset}}\right)$ is open.)

Definition. A profinite group is an inverse limit of finite groups, with the inverse limit topology.

Lemma. If G is profinite, $G \simeq \varprojlim_{N\lhd G \text{ open}} G/N$

Remark: All such N's form a filtered system: given $N_1 \triangleleft G$, $N_2 \triangleleft G \rightsquigarrow N_1 \cap N_2 \triangleleft G$.

Proof: There's an obvious homomorphism $G \longrightarrow \varprojlim_{N \triangleleft G \text{ open}} G/N$

Conversely, if $G = \varprojlim_{i \in I} G_i$, we want to construct $\varprojlim G/N \longrightarrow G$

we need $\varprojlim_{N \triangleleft G \text{ open}} G/N \longrightarrow G_i$

But $\pi_i : G \to G_i$ the projection $\rightsquigarrow \ker \pi_i \triangleleft G$ is open

$\rightsquigarrow \varprojlim_{N \triangleleft G \text{ open}} G/N \to G/\ker \pi_i \to G_i$; easy to check compatibility with $i \in I$.

Application to Galois theory.

Recall that: a Galois extension K/F is an algebraic extension that is separable and normal.

i.e. (1) any intermediate field E/F that is finite $/F$ is separable $/F$

(2) any irreducible polynomial $f(x)$ have a root in K splits in K.

Remark: K = union of intermediate field E s.t. E/F is finite Galois.

Define $\mathrm{Gal}(K/F) = \varprojlim_{E/F \text{ finite Galois}} \mathrm{Gal}(E/F)$

The connecting map is, when $E_1 \supseteq E_2 \supseteq F$, then $\mathrm{Gal}(E_1/F) \to \mathrm{Gal}(E_2/F)$

Example. $\mathbb{Q}(\mu_{p^\infty}) := \mathbb{Q}(\zeta_{p^n} ; n \in \mathbb{N})$

$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/p^n)^\times = \mathbb{Z}_p^\times$

$\mathbb{Q}(\mu_\infty) := \mathbb{Q}(\zeta_n ; n \in \mathbb{N})$

$\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times \simeq \prod_p \mathbb{Z}_p^\times$

Claim: $\mathrm{Gal}(K/F) = \{\text{autom } \sigma : K \xrightarrow{\sim} K \mid \sigma|_F = \mathrm{id}_F\}$

Proof: $\{\text{autom } \sigma: K \xrightarrow{\sim} K \mid \sigma|_F = id_F\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{For any } E/F \text{ finite normal intermediate field} \\ \text{a compatible } \sigma_E: E \xrightarrow{\sim} E \text{ s.t. } \sigma_E|_F = id\end{array}\right\}$

$$\| \varprojlim_{E/F \text{ finite normal}} Gal(E/F)$$

Topology on $Gal(K/F)$.

If E/F is finite Galois and fix $a_E \in Gal(E/F)$

$\{\sigma: K \xrightarrow{\sim} K \text{ s.t. } \sigma|_E = a_E\}$ is a "standard" open subset of $Gal(K/F)$.

The open subsets of $Gal(K/F)$ are unions of such standard opens.

* $Gal(K/F)$ acts on K continuously: $Gal(K/F) \times K \longrightarrow K$ (K with discrete topology)

(Exercise.)

Theorem (Galois theory for infinite extensions)

Let K/F be a Galois extension. Then there's a one-to-one inclusion-reversive correspondence

$$\{\underline{\text{closed}} \text{ subgroups } H \leq Gal(K/F)\} \longleftrightarrow \{\text{intermediate fields } E \text{ of } K/F\}$$

$$H \longmapsto K^H$$

$$Gal(K/E) \longleftarrow\!\shortmid\ E$$

open subgroups $\longleftrightarrow$ those E finite $/F$

normal subgroups $\longleftrightarrow$ those E Galois $/F$

$\downarrow$

In this case $Gal(E/F) \simeq Gal(K/F)/Gal(K/E)$ as topological groups

Some preparation:

① Group side G profinite $G \simeq \varprojlim_{N \lhd G \text{ open}} G/N$. $H \leq G$ a closed subgroup

$$\begin{array}{ccc} G & - & H \\ \downarrow & & \downarrow \\ \vdots & & \vdots \end{array}$$

For each $N \lhd G$ open normal

define $H_N := \mathrm{Im}(H \to G/N)$

$$\begin{array}{ccc} G/N' & \twoheadrightarrow & \mathrm{Im}(H \to G/N') =: H_{N'} \\ \downarrow & & \downarrow \\ G/N & \twoheadrightarrow & \mathrm{Im}(H \to G/N) =: H_N \end{array}$$

Then for $N' \trianglelefteq N$, $N' \trianglelefteq G$ open, get $H_{N'} \to H_N$.

Then H as a subgroup is $H \simeq \varprojlim_{N \trianglelefteq G \text{ open}} H_N \subseteq G$.

(Note: $\varprojlim_{N \trianglelefteq G \text{ open}} H_N = G \cap \bigcap_{N \trianglelefteq G \text{ open}} \pi_N^{-1}(H_N)$, closed) So, we need H to be closed.

Proof: Suppose $H \subseteq \varprojlim_{N \trianglelefteq G \text{ open}} H_N$ is strict $\Rightarrow H^c \cap \varprojlim_{N \trianglelefteq G \text{ open}} H_N \neq \phi$ (H^c open)

$\Rightarrow \exists$ fundamental open $gN \subseteq H^c \subseteq G$

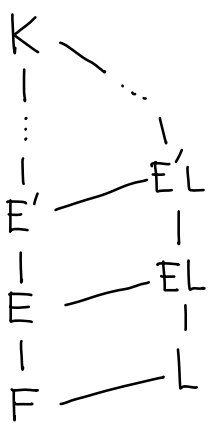
s.t. $gN \cap H \neq \phi$ but $gN \cap \varprojlim_{N' \trianglelefteq G \text{ open}} H_{N'} \neq \phi$

$\Downarrow$ $g \notin H_N$

$\Downarrow$ $g \in H_N$

Contradiction!

② Galois side



Recall $\mathrm{Gal}(K/F) = \varprojlim_{E/F \text{ fin Galois}} \mathrm{Gal}(E/F)$

For L an intermediate field

$$\mathrm{Gal}(K/L) = \varprojlim_{L'/L \text{ fin Gal}} \mathrm{Gal}(L'/L)$$

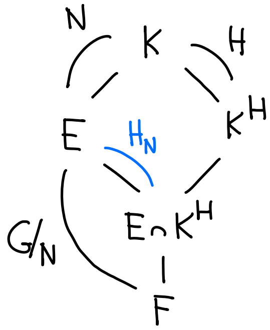
(all such L' takes the form of $L' = LE$ for E/F fin Galois)

$$= \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(EL/L) \quad (= \mathrm{Gal}(E/L \cap E) \leq \mathrm{Gal}(E/F))$$

So $\mathrm{Gal}(K/L)$ is a closed subgroup of $\mathrm{Gal}(K/F)$.

Proof of the main theorem:

(1) <u>Check</u> $\mathrm{Gal}(K/K^H) = H$.



$$\mathrm{Gal}(K/K^H) = \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/E\cap K^H)$$

<u>Note</u>: write $N := \mathrm{Gal}(K/E) \lhd G$ open

H acts on E via $\mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(E/F)$

$$\begin{array}{ccc} \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(E/F) \\ \| & & \| \\ H & \longrightarrow & G/N \end{array}$$

So $E \cap K^H = E^{H_N}$

$$\Rightarrow \mathrm{Gal}(K/K^H) = \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/E\cap K^H) = \varprojlim_{E/F \text{ fin Gal}} \mathrm{Gal}(E/E^{H_N}) = \varprojlim_{E/F \text{ fin Gal}} H_N = H.$$

(2) <u>Check</u>: $L = K^{\mathrm{Gal}(K/L)}$

For any finite Galois extension E/F, we need to check $L \cap E = K^{\mathrm{Gal}(K/L)} \cap E$

But $E \cap K^{\mathrm{Gal}(K/L)} = E^{\mathrm{im}(\mathrm{Gal}(K/L) \to \mathrm{Gal}(E/F))}$

$$\overset{②}{=} E^{\mathrm{Gal}(E/E\cap L)} = E \cap L. \checkmark$$