Lecture # 13 (18/12/2024)

Today : Infinite Galois Extensions

(Reference : J.S. Milne. Fields and Galois Theory)

Recall : A field extension L/K is

- **normal** if it is a splitting field of a collection of polynomials in $K[x]$
- **separable** if it is algebraic and $\min_K \alpha$ has no repeated roots $\forall \alpha \in L$
- **Galois** if it is both normal and separable

Notation : If L/K is Galois, we write $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$

! When L/K is not finite, not all subgroups of $\mathrm{Gal}(L/K)$ correspond to subextensions of L/K. We want to consider a topology on $\mathrm{Gal}(L/K)$ that captures those that do.

Here, is a Key observation:

Lemma A field extension L/K is Galois iff it is a union of finite Galois extensions

So, we want to consider all finite Galois subextensions in some sense.

A digression on inverse limits

Definitions

1. A directed set is a partially ordered set $(I, \leq)$ such that for all $i, j \in I$ we can find $K \in I$ s.t. $i \leq K$ and $j \leq K$.

$$\begin{cases} i \leq i \\ i \leq j \;\&\; j \leq i \Rightarrow i = j \\ i \leq j \;\&\; j \leq K \Rightarrow i \leq K \end{cases}$$

2. Given a category $\mathcal{C}$ and a directed set $(I, \leq)$ an inverse system is a collection of objects $(A_i)_{i \in I}$ together with

morphisms $\left(\varphi_i^j : A_j \to A_i\right)_{i \le j}$ s.t.

$\varphi_i^i = \mathrm{id}_{A_i}$ $\forall i$ and $\varphi_i^j \circ \varphi_j^K = \varphi_i^K$ $\forall\, i \le j \le K$.

$$\begin{tikzcd} A_K \arrow[r, "\varphi_j^K"'] \arrow[rr, bend left, "\varphi_i^K"] & A_j \arrow[r, "\varphi_i^j"'] & A_i \end{tikzcd}$$

3 Given an inverse system as in 2, an inverse limit is an object A (in $\mathcal{C}$) plus morphisms $\pi_i : A \to A_i$ satisfying

$\varphi_i^j \circ \pi_j = \pi_i$ $\forall\, i \le j$

$$\begin{tikzcd} & A \arrow[dl, "\pi_j"'] \arrow[dr, "\pi_i"] & \\ A_j \arrow[rr, "\varphi_i^j"'] & & A_i \end{tikzcd}$$

+ universal property.

$$\begin{tikzcd} & B \arrow[d, dashed, "\exists!\,\varphi"] \arrow[ddl, bend right] \arrow[ddr, bend left] & \\ & A \arrow[dl] \arrow[dr] & \\ A_j \arrow[rr] & & A_i \end{tikzcd}$$

FACT In the category of groups inverse limits always exist.

Given an inverse system of groups

$$(G_i)_{i\in I} + \left(\varphi_i^j : G_j \to G_i\right)_{i\le j}$$

$$\varprojlim G_i := \left\{ (g_i) \in \prod G_i \;;\; \varphi_i^j(g_j) = g_i \;\forall i\le j \right\}$$

this is always a subgroup of $\prod G_i$

Definition Groups which are inverse limits of finite groups are called profinite.

One can prove that every profinite group is the Galois group of some Galois extension.

FACT If we have an inverse system in the category of groups, the inverse limit is also an inverse limit in the category of topological groups <u>if</u>

- $\prod G_i$ has the product topology &
- $\varprojlim G_i$ has the subspace topology.

! Every finite group is a topological group with the discrete topology. So, every profinite group has a "natural" topology.
In fact, we obtain Hausdorff, compact and totally disconnected spaces.

only subspaces which are connected are the singletons.

Back to Galois extensions

Given L/K Galois, we can consider

- I = set of intermediate fields $K \subset F \subset L$ s.t. F/K is finite Galois.
- $\leq$ = inclusion (given $K \subset F \subset L$ and $K \subset F' \subset L$, $F, F' \subset FF'$) composite
- For each $K \subset F \subset L$, and each $F \subset F'$, we have $\varphi_F^{F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$

$$\sigma \mapsto \sigma|_F$$

Example 1

- Let $K=\mathbb{Q}$ and for each $n \in \mathbb{N}$ let $F_n = SF_{\mathbb{Q}}(x^n - 1)$.

  Consider $L = F_1 F_2 F_3 \cdots$

- $L/\mathbb{Q}$ is Galois (char $\mathbb{Q}=0$ & composite of normal extensions is normal)

- Note that $F_m \subset F_n \iff m \mid n$ and we have

$$\begin{array}{ccc} \mathrm{Gal}(F_n/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(F_m/\mathbb{Q}) \\ \cong & & \\ (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times \\ a & \longmapsto & a \bmod m \end{array}$$

- $$\mathrm{Gal}(L/\mathbb{Q}) \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \left\{ (a_n) \in \prod_{n=1}^{\infty} (\mathbb{Z}/n\mathbb{Z})^\times ; \ a_n \equiv a_m \bmod m \ \forall m \mid n \right\}$$

Example 2 (Rings & fields)

K a field, $K^{sep} = \{\alpha \in \overline{K} \text{ separable } / K\}$

- K^{sep}/K is Galois and $\overline{K}/K^{sep}$ is purely inseparable

* if char $K = 0$, then $\overline{K} = K^{sep}$

- If $K = \mathbb{F}_p$, then we have (for $\forall\, m \mid n$)

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \\ \wr\wr & & \wr\wr \\ \mathbb{Z}/n\mathbb{Z} & & \mathbb{Z}/m\mathbb{Z} \end{array}$$

$$a \mapsto a \bmod m$$

$$\begin{array}{l} \mathrm{Gal}(\mathbb{F}_p^{sep}/\mathbb{F}) = \left\{ (a_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} \,;\, a_n \equiv a_m \bmod m \;\; \forall\, m \mid n \right\} \\ \quad \Vert \\ \quad \hat{\mathbb{Z}} \end{array}$$

Proposition If L/K is a Galois extension, then

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L) \longrightarrow \varprojlim \mathrm{Gal}(F/K) \subset \prod_{\substack{F/K \\ \text{finite} \\ \text{Galois}}} \mathrm{Gal}(F/K)$$

$$\sigma \longmapsto (\sigma|_F)$$

is a group isomorphism.

Definition If L/K is Galois, then the Krull topology on $\mathrm{Gal}(L/K)$ is the unique topology on $\mathrm{Gal}(L/K)$ making the above group isomorphism a homeomorphism.

* This topology has a basis consisting of all $\mathrm{Gal}(L/F)$ such that F/K is finite and normal.

* Note that if $G = \varprojlim \mathrm{Gal}(F/K)$, then $\mathrm{Ker}\left(\pi_F : G \to \mathrm{Gal}(F/K)\right)$ are <u>open</u> normal subgroups of finite index

$\rightsquigarrow$ we get a collection of opens around 1_G.

Proposition Let L/K be a Galois extension.

(i) If $K \subset F \subset L$ is an intermediate field, then $\mathrm{Gal}(L/F)$ is closed in $\mathrm{Gal}(L/K)$, and $L^{\mathrm{Gal}(L/F)} = F$

(ii) If $H \leq \mathrm{Gal}(L/F)$ is a subgroup, then $\mathrm{Gal}(L/L^H)$ is the closure of H in $\mathrm{Gal}(L/F)$.

idea of (i)

$$\mathrm{Gal}(L/F) = \bigcap_{\substack{S \subset F \\ \text{finite}}} \underbrace{\{\sigma \in \mathrm{Gal}(L/K) ; \sigma s = s \ \forall s \in S\}}_{G(S)}$$

- Each $G(S)$ is open subgroup (of finite index).
- On a topological group, every open subgroup is also closed.

The fundamental theorem

Let L/K be Galois with Galois group G. The maps $H \longmapsto L^H$, $F \longmapsto \mathrm{Gal}(L/F)$ define inverse bijections between

$$\{\text{closed subgroups } H \leq G\} \xleftrightarrow{1:1} \{\text{intermediate } K \subset F \subset L\}$$

Moreover,

(i) the corresp. is order reversing

(ii) $H \leq G$ closed is open $\Leftrightarrow [L^H : K] < \infty$,
in which case $[L^H : K] = [G : H]$

(iii) $\sigma H \sigma^{-1} \leftrightarrow \sigma F$

(iv) $H \leq G$ closed is normal $\Leftrightarrow L^H/K$ is Galois, in which case $\mathrm{Gal}(L^H/K) \simeq G/H$

Some last remarks

(A) Not all subgroups of $\mathrm{Gal}(L/K)$ are closed.

(Krull) Any infinite Galois extension includes non-closed subgroups.

B In the Krull topology,

open + normal $\Rightarrow$ finite index

but $\exists$ normal of finite index which are <u>not</u> open

$\rightsquigarrow$ Krull topology $\subset$ profinite topology