Lecture 3: Infinite Galois theory

Recollections Let k be a field.

A field extension K/k is a (nec. injective) ring homm $k \hookrightarrow K$.

Let $x \in K$. Obtain $k[T] \xrightarrow{\alpha} K$. If α is injective,

$$\begin{aligned} k &\hookrightarrow K \\ T &\longmapsto x \end{aligned}$$

we call x transcendental $/k$.

Otherwise call x algebraic $/k$. Since $k[T]$ is a PID there is a unique monic polynomial $P_x(T) \in k[T]$ generating $\ker \alpha$. Call P_x the minimal polynomial of x.

- K/k is called algebraic if every element $x \in K$ is algebraic $/k$
- K/k is called Galois if it is algebraic and $\forall x \in K$ $$P_x(T) = \prod_{i=1}^{n} (T - x_i) \in K[T]$$ where the x_i are distinct.

  $$\left[X^p - \alpha \overset{\text{NOT:}}{=} (X - \sqrt[p]{\alpha})^p \right]$$

- K/k is called finite if $\dim_k K < \infty$.

Important observation: If $L/K/k$ are field ext^{ns} & K/k is Galois, then any endomorphism $\alpha: L \to L$ fixing k preserves K. (I.e. $\alpha(K) \subset K$)

Pf $x \in K$ $\quad P_x(x) = 0 \rightsquigarrow 0 = \alpha\, P_x(x) \underset{\uparrow \atop \alpha|_k = id}{=} P_x(\alpha x)$.

$\therefore \alpha x$ a root of $P_x(T)$

$\therefore \alpha x \in K$. $\square$

The Galois group

K/k any Galois ext^n.

$$\mathrm{Gal}(K/k) = \{\alpha : K \xrightarrow{\cong} K \mid \alpha|_k = id_k\}$$

This is a group. Give it a topology as follows:
for $k \subset k' \subset K$ s.t. k'/k finite Galois, $\mathrm{Gal}(K/k') \subset \mathrm{Gal}(K/k)$ is defined to be <u>open</u>.

I.e.: $X \subset \mathrm{Gal}(K/k)$ is open iff $\forall x \in X$ $\exists\, k \underset{\text{fin. Gal.}}{\subset} k' \subset K$ s.t. $\mathrm{Gal}(K/k')\, x \subset X$.

$\underline{\text{Th}^{m}}$ The canonical map

$$\mathrm{Gal}(K/k) \xrightarrow{\varphi} \lim_{\substack{K/k'/k \\ k'/k \text{ fin. Gal.}}} \overbrace{\mathrm{Gal}(k'/k)}^{\text{finite group (ex./std. fact)}} = \mathcal{L}$$

coming from the "important obs." is an iso of top. gps.

In particular: $\mathrm{Gal}(K/k)$ is a profinite group.

$\underset{\sim}{\text{Pf}}$ Let $g \in \mathcal{L} \subset \prod_{k'} \mathrm{Gal}(k'/k)$.

Let $x \in K$, $L \subset K$ the splitting field of $P_x(T)$ & define $(\psi g)(x) = g_L(x)$.

Obtain a map of sets $\psi g : K \longrightarrow K$.

Claim: ψg is an autom^{n} of the field K.

Suffices to check that if $k \subset k_1, k_2 \subset K$ finite Galois & $x \in \underbrace{k_1 \cap k_2}_{\text{finite Gal. ext}^{n} \text{ of } k}$, then $g_{k_1}(x) = g_{k_2}(x)$.

$\rightsquigarrow$ precisely def^{n} of $\mathcal{L} \subset \prod$.

Similarly: $\psi(g_1 \cdot g_2) = \psi(g_1) \cdot \psi(g_2)$

$\psi(e) = e$

Clear: $\psi\varphi = \mathrm{id} \qquad \varphi\psi = \mathrm{id}$

$\therefore$ inverse isom's of abstract groups.

Under this identification, the subgroup

$$\mathrm{Gal}(K/k') \subset \mathrm{Gal}(K/k)$$

corresponds to $H_{k'} \subset \ell \subset \Pi$ preimage of $\{e\}$ under proj'n to k'-factor.

Sets of this form are basis of open nbhds of 1 in product top. $\therefore \varphi, \psi$ are inverse homeom's. $\square$

<u>Lemma</u> Suppose that $K = \bigcup_{i \in I} K_i$, K_i/k finite Galois & set $\{K_i\}_i$ is directed.

Then $\mathrm{Gal}(K/k) = \varprojlim_{i \in I} \mathrm{Gal}(K_i/k)$.

<u>Proof</u> Same. $\square$

<u>Ex</u> Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n)^\times$, where $\zeta_n = e^{2\pi i/n}$ primitive nth root of unity.

Let p be an odd prime so that $(\mathbb{Z}/p^n)^\times \cong \mathbb{Z}/p^{n-1} \times \mathbb{Z}/p-1$

$$K = \bigcup_n \mathbb{Q}(\zeta_{p^n}).$$

$$\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim_n \left(\mathbb{Z}/p^{n-1} \times \mathbb{Z}/p-1\right) = \hat{\mathbb{Z}_p} \times \mathbb{Z}/p-1$$

Ex $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n = \hat{\mathbb{Z}}$

Lemma (Extension of automorphisms) Let K/k be a Galois ext^n, $k \subset K_1, K_2 \subset K$, $\gamma : K_1 \xrightarrow{\cong} K_2$ s.t. $\gamma|_k = id$.

Then $\exists \tilde{\gamma} : K \xrightarrow{\cong} K$ s.t. $\tilde{\gamma}(K_1) \subset K_2$ & $\tilde{\gamma}|_{K_1} = \gamma$

Pf WMA K is sep. closed. (I.e. if K'/K is Galois then $K \xrightarrow{\cong} K'$.)

Let $S = \left\{ (L_1, L_2, \tilde{\gamma}) \;\middle|\; \begin{array}{l} K_i \subset L_i \subset K \\ \tilde{\gamma} : L_1 \xrightarrow{\cong} L_2 \quad \tilde{\gamma}|_{K_1} = \gamma \end{array} \right\}$.

Order by inclusion & ext^n of $\tilde{\gamma}$.
Zorn's lemma $\Rightarrow$ S has max. elt $(L_1, L_2, \tilde{\gamma})$.

If $L_1 = K$ then also $L_2 = K$: else $\exists x \in L_2 \setminus K$ with min. poly. P_x over L_2. (P_x has no root in L_2).
But then $\tilde{\gamma}^{-1}(P_x)$ has no root in $L_1 = K = K^s$. ⚡

Either $L_1 = L_2 = K$, i.e. thm proved, or $L_1 \neq K$.
If so, pick $x \in K \setminus L_1$, P = min poly over L_1.

$$\begin{array}{ccc} L_1(x) & = & L_1[T]/P \\ \downarrow\cong & & \cong\downarrow \tilde{\gamma} \\ L_2(y) & = & L_2[T]/\tilde{\gamma}P \end{array}$$

Pick root of $\tilde{\gamma}P$ in K

$\therefore$ strictly bigger ext^n $\cancel{\nabla}$. $\square$

<u>Prop^n</u> K/k Galois, $k \subset M \subset K$, M/k finite (not nec. Galois). Then

$$|\mathrm{Gal}(K/k) : \mathrm{Gal}(K/M)| = [M:k] \left(= \dim_k M\right).$$

<u>Pf</u> Primitive elt thm $\rightsquigarrow$ $M \cong k[T]/P$ (i.e. $M = k(x)$)

$[M:k] = \deg P = n$ $\quad P(T) = \prod_{i=1}^{n} (T - x_i)$ $\quad x_i \in K$.

$\therefore \exists$ precisely n (distinct) field hom^{ms}
$$\begin{array}{ccc} M & \xrightarrow[\gamma_i]{T \mapsto x_i} & K \\ \uparrow & \nearrow & \\ k & & \end{array}$$

$$\gamma_i : M \xrightarrow{\cong} \gamma_i(M) \subset K$$

Obtain $\tilde{\gamma}_i : K \xrightarrow{\cong} K$ s.t. $\tilde{\gamma}_i|_M = \gamma_i$.

Suppose given $\gamma \in \mathrm{Gal}(K/k)$. Then $\gamma|_{..} = \gamma_i$ for a unique i. $\therefore \gamma_i^{-1}\gamma|_M = id$ for a unique i.

I.e.: $\gamma_1, \dots, \gamma_n$ are coset representatives for $Gal(K/M) \subset Gal(K/k)$.

$\square$

Cor $Gal(K/M) \subset Gal(K/k)$ is open.

Lemma If K/k is Galois & $k \subset M \subset K$ (not. nec. Galois or finite) then the topology on $Gal(K/M) \subset Gal(K/k)$ is the induced one.

Pf If $k \subset N \subset K$, then

$$Gal(K/M) \cap Gal(K/N) = Gal(K/M\cdot N)$$ composite subfield

$\therefore$ the induced topology on $Gal(K/M)$ has basis

$$Gal(K/k') \cap Gal(K/M) = Gal(K/k'\cdot M) \subset Gal(K/M)$$

k'/k fin. Gal. open by prev. Lemma.

Every finite Gal. $M \subset M' \subset K$ has $M' \subset M \cdot N$ for some $k \subset N \subset K$ finite Galois.

This concludes the proof. $\square$

The fundamental thm

Thm K/k Galois.

$$\{\text{subfields } k \subset M \subset K\} \underset{K^H \longleftarrow\!\shortmid H}{\overset{M \mapsto \mathrm{Gal}(K/M)}{\rightleftarrows}} \{\text{closed subgps of } \mathrm{Gal}(K/k)\}$$

are inverse bijections.

Pf $\mathrm{Gal}(K/M) \subset \mathrm{Gal}(K/k)$ is a compact subspace of a Hausdorff space $\therefore$ closed.

$\therefore$ maps are well-defined

STP: 1) If K/k is Galois, then $K^{\mathrm{Gal}(K/k)} = k$.

2) If $G \subset \mathrm{Gal}(K/k)$ is closed, then $\mathrm{Gal}(K/K^G) = G$.

Pf of 1: Let $x \in K \setminus k$. Want: $\gamma : K \xrightarrow{\cong} K$ s.t. $\gamma(x) \neq x$. $\gamma|_k = \mathrm{id}$

$P_x(T) \in k[T]$ must have another root $y \neq x$.
$\in K$

$\rightsquigarrow k(x) \xrightarrow{\cong} k(y)$

obtain γ by extension.

Pf of 2: $K^G \subset E \subset K$, E/K^G fin. Gal.

Put $G|_E$ = image of G in $\mathrm{Gal}(E/k)$.

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & \varprojlim_E G|_E \arrow[d] \\
\mathrm{Gal}(K/K^G) \arrow[r] & \varprojlim_E \mathrm{Gal}(E/K^G)
\end{tikzcd}$$

limit over finite Gal. subext^{ns} of K/K^G

$G|_E \to \mathrm{Gal}(E/K^G)$: $\cong$ by class. Gal. theory

$\cong$ $\qquad$ $\therefore \cong$

- injective
- cts
- dense image

$\Big\}$ image is closed (G cpct, lim Hausdorff) $\therefore$ bij^n (homeom^n)

$\therefore$ must be bij^n $\square$