

Lecture 24: The Fundamental Thm of Galois Theory ①

Last time:

Thm A: $G \leq \text{Aut}(K)$. Then $[K:K_G] = |G|$ and

$$\text{Aut}(K/K_G) = G.$$

Thm B: For K/F finite, the following are equivalent

① K/F is Galois, i.e. $|\text{Aut}(K/F)| = [K:F]$.

② K is the splitting field of a separable poly in $F[x]$.

③ $K_{\text{Aut}(K/F)} = F$ [Contrast: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$]

Proof: ② \Rightarrow ① is an old result.

① \Rightarrow ③: Set $G = \text{Aut}(K/F)$. Have $K \supseteq K_G \supseteq F$
and $[K:K_G] \stackrel{\uparrow}{=} |G| \stackrel{\uparrow}{=} [K:F]$; Hence $K_G = F$.
By Thm By ①

③ \Rightarrow ②: Suppose $K = F(\alpha)$ [as we saw in the proof last time].

Then $m_{\alpha, K_G}(x) = \prod (x - \alpha_i)$ where $G \cdot \alpha = \{\alpha_1, \dots, \alpha_n\}$

As $K_G = F$, get that K is the splitting field of this separable poly in $F[x]$. □

Fund. Thm of Galois Thy: K/F Galois, $G = \text{Gal}(K/F)$ (2)

$$\left\{ \begin{array}{l} \text{Subfields} \\ F \subseteq E \subseteq K \end{array} \right\} \xleftrightarrow{\text{bijection}} \left\{ \begin{array}{l} \text{Subgps} \\ H \leq G \end{array} \right\}$$

$$E \xrightarrow{\phi} G_E = \{ \sigma \in G \mid \sigma|_E = \text{id} \} = \text{Aut}(K/E)$$

$$K_H \xleftarrow{\psi} H$$

Pf: ψ is 1-1: Suppose $K_{H_1} = K_{H_2}$. By Thm A,

$$\text{Aut}(K/K_{H_i}) = H_i \text{ for each } i \Rightarrow H_1 = H_2$$

subgroups of $\text{Aut}(K)$

ψ is onto: Suppose $F \subseteq E \subseteq K$. By Thm B, K is the splitting field of a sep. poly $f(x) \in F[x]$; as $f(x)$ is also in $E[x]$ get that K/E is Galois.

Hence $[K:E] = |\text{Aut}(K/E) = G_E|$. Now

$\psi(G_E) = K_{G_E} \supseteq E$ and $[K:K_{G_E}] = |G_E|$ by

Thm A. Thus $K_{G_E} = E$ and ψ is onto. \square

Check: If $\alpha = \sigma \tau \sigma^{-1}$ with $\tau \in H$ and $e \in E$, (4)

have $\alpha(\sigma(e)) = \sigma \tau \sigma^{-1} \sigma(e) = \sigma \tau(e) = \sigma(e)$.

Conversely, if $\beta \in H'$, then $\sigma^{-1} \beta \sigma \in G_E$ since

$$\sigma^{-1} \beta \sigma(e) = \sigma^{-1} \beta(\sigma(e)) = \sigma^{-1}(\sigma(e)) = e.$$

Idea for (4): $H \triangleleft G \iff H = \sigma H \sigma^{-1}$ for all $\sigma \in G$

$$\stackrel{\text{(a)}}{\iff} \sigma(E) = E \text{ for all } \sigma \in G$$

$$\stackrel{\text{(b)}}{\iff} E/F \text{ is Galois.}$$

(a) (\Leftarrow) Above. (\Rightarrow) By above, $G_{\sigma(E)} = \sigma H \sigma^{-1} = H$.

By the FTGT, get $\sigma(E) = E$.

(b) (\Leftarrow) E is the splitting field of some $f(x) \in F[x]$

with roots α_i , and so $E = F(\alpha_1, \dots, \alpha_n)$. For any

$\sigma \in G$, have $\sigma(\alpha_i) = \alpha_j$ for all $i \Rightarrow \sigma(E) \subseteq E$

$\Rightarrow \sigma(E) = E$.

(\Leftarrow) Suppose $E = F(\alpha_1, \dots, \alpha_n)$. Now

$$m_{\alpha_i, F}(x) = \prod_j (x - \beta_{i,j}) \text{ where } G \cdot \alpha_i = \{\beta_{i,1}, \dots, \beta_{i,k}\}$$

\uparrow in $F[x]$

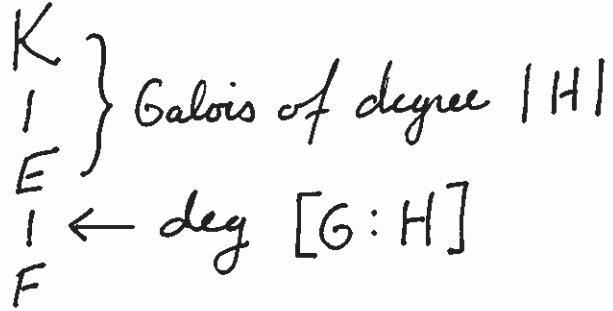
Properties:

① If E_1, E_2 correspond to H_1, H_2 then

$$E_1 \subseteq E_2 \iff H_1 \supseteq H_2$$

Pf: Clear.

② If $E \leftrightarrow H$ then



Pf:

$$\begin{array}{ccc} [K:F] & = & [K:E][E:F] \\ \parallel & & \parallel \\ |G| & & |H| \end{array}$$

③ K/E is Galois with $\text{Gal}(K/E) = H$.

④ E/F is Galois $\iff H \triangleleft G$.

In this case, $\text{Gal}(E/F) = G/H$

⑤ $E_1, E_2 \leftrightarrow H_1, H_2$. Then $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$

[Need to prove ④ and ⑤; start with ④]

Consider $F \subseteq E \subseteq K$. For $\sigma \in G$, look at $E' = \sigma(E)$.

Q: What is $H' = G_{E'}$? A: $H' = \sigma H \sigma^{-1}$

Thus E is the splitting field of the separable poly

(5)

$$f(x) = \prod m_{\alpha_i, F}(x). \quad \text{So } E/F \text{ is Galois.}$$

↑ maybe not all i

Finally, if $\sigma(E) = E$ for all $\sigma \in G$, then have

$$G = \text{Gal}(K/F) \longrightarrow \text{Gal}(E/F)$$

$$\sigma \longmapsto \sigma|_E$$

By uniqueness of splitting fields, this is onto, and moreover the kernel is exactly H . Thus

$$\text{Gal}(E/F) = G/H$$