

Lecture 25: Fundamental Thm of Galois Theory II ①

Thm: K/F Galois, $G = \text{Gal}(K/F)$. Have a bijection

$$\left\{ \begin{array}{l} \text{subfields } E \\ F \subseteq E \subseteq K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgroups} \\ H \leq G \end{array} \right\}$$

$$E \longmapsto G_E = \text{Aut}(K/E)$$

$$K_H \longleftarrow H$$

① $E_1, E_2 \leftrightarrow H_1, H_2$. Then $E_1 \subseteq E_2 \iff H_1 \geq H_2$.

② $[K:E] = |H|$, $[E:F] = [G:H]$

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

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

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

Pf of ④: Last time, saw that if $E \leftrightarrow H$

and $\sigma \in G$, then $\sigma(E) \leftrightarrow H' = \sigma H \sigma^{-1}$

Therefore, $\sigma(E) = E$ for all $\sigma \in G$

$\iff H = \sigma H \sigma^{-1}$ for all $\sigma \in G$, i.e. $H \triangleleft G$.

Claim: $\sigma(E) = E \quad \forall \sigma \in G \iff E/F$ is Galois. (2)

(\Leftarrow) E is the splitting field of a separable poly $f(x)$ in $F[x]$, with roots $\alpha_1, \dots, \alpha_n \in E$ where $n = \deg f(x)$. Any $\sigma \in G$ permutes the α_i ; as $E = F(\alpha_1, \dots, \alpha_n)$ this gives $\sigma(E) = E$.

(\Rightarrow) Suppose $E = F(\alpha_1, \dots, \alpha_n)$. For each α_i ,

have $m_{\alpha_i, F}(x) = \prod_j (x - \beta_{i,j})$ where $G \cdot \alpha_i = \underbrace{\{\beta_{i,1}, \dots, \beta_{i,k}\}}_{\text{all in } E!}$

So $m_{\alpha_i, F}(x)$ splits completely in $E[x]$,

and so E is the splitting field of

$$\prod_i m_{\alpha_i, F}(x)$$

which we can make separable by removing repeat

$m_{\alpha_i, F}(x)$. □

Related:

(3)

$K = \text{finite ext of } \mathbb{Q}$ (A number field)

Consider all embeddings $\sigma: K \rightarrow \mathbb{C}$ ("infinite place")

Thm: K/\mathbb{Q} is Galois $\Leftrightarrow \forall$ embeddings σ, τ of $K \hookrightarrow \mathbb{C}$ have $\sigma(K) = \tau(K)$.

- $K = \mathbb{Q}[x]/(x^2-2)$ has two embeddings in \mathbb{C} , namely σ with $\sigma(\bar{x}) = \sqrt{2}$ and τ with $\tau(\bar{x}) = -\sqrt{2}$

Note $\sigma(K) = \tau(K) = \mathbb{Q}(\sqrt{2})$ and K/\mathbb{Q} is Galois

- $K = \mathbb{Q}[x]/(x^3-2)$, have $\sigma(\bar{x}) = \sqrt[3]{2}$
 $\tau(\bar{x}) = \sqrt[3]{2} \zeta_3$
 $\eta(\bar{x}) = \sqrt[3]{2} \zeta_3^2$

Note $\sigma(K) \subseteq \mathbb{R}$ but $\tau(K)$ isn't.

Proof: $K = \mathbb{Q}(\alpha)$ with $f(x) = m_{\alpha, \mathbb{Q}}(x) \in \mathbb{Q}[x]$.

Get one $\sigma_i: K \rightarrow \mathbb{C}$ for each of the deg f roots of $f(x)$ in \mathbb{C} . Let $L \subseteq \mathbb{C}$

be the compositum of the $\sigma_i(K)$, which is a splitting field of $f(x)$. Thus ④

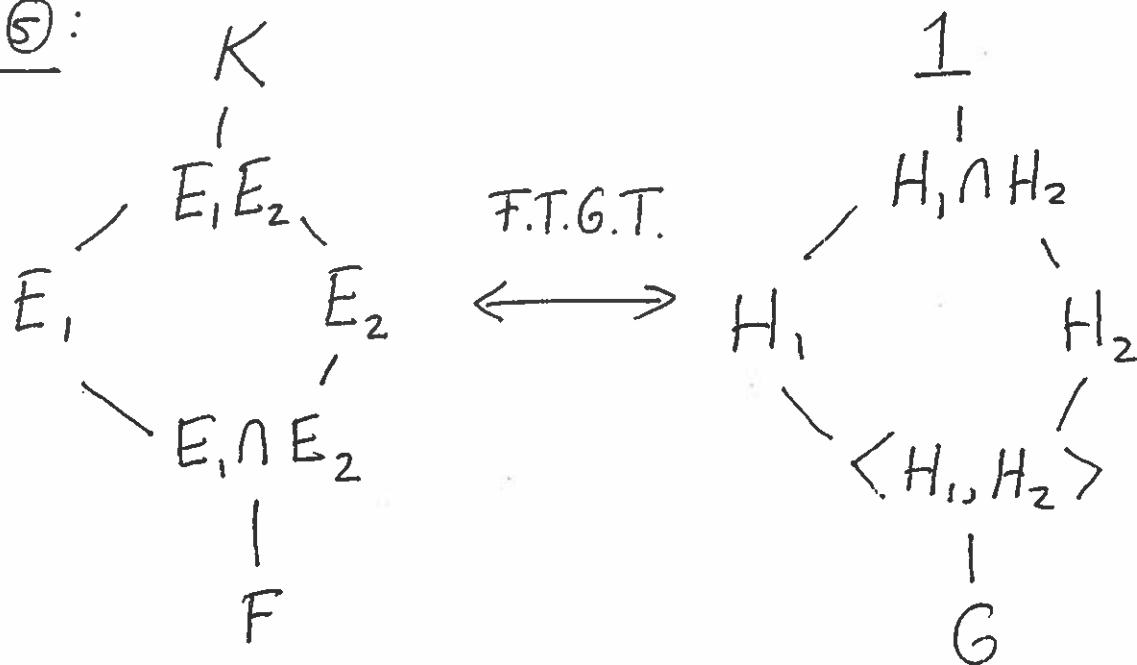
$$\sigma_i(K) = \sigma_j(K) \quad \forall i, j \iff \sigma_i(K) = L \text{ for all } i$$

$\iff f(x)$ splits completely in K .

$\iff K/\mathbb{Q}$ is Galois. □

Proof of ⑤:

Want to show



Suppose $E_1, E_2 \iff H$. By ①, $H \leq H_i$

$\implies H \leq H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$

then σ fixes E_1 and $E_2 \implies \sigma$ fixes E_1, E_2

$\implies H \geq H_1 \cap H_2$. ✓

Set $H = \langle H_1, H_2 \rangle$, will show $K_H = E_1 \cap E_2$. ⑤

As $H_i \leq H$, have $K_H \subseteq E_i \Rightarrow K_H \subseteq E_1 \cap E_2$.

Conversely, if $\alpha \in E_1 \cap E_2$ then $\sigma(\alpha) = \alpha$

for all $\alpha \in H_i \Rightarrow \sigma(\alpha) = \alpha$ for all $\alpha \in H. \Rightarrow$

$E_1 \cap E_2 \subseteq K_H \Rightarrow E_1 \cap E_2 = K_H$. ▣