Lecture 25: Fund. Thm. of Galois Theory II

Thm: K/F Galois, $G = Gal(K/F)$. Have

$$\left\{ \begin{array}{c} \text{subfields } E \\ F \subseteq E \subseteq K \end{array} \right\} \underset{\text{bijection}}{\longleftrightarrow} \left\{ \begin{array}{c} \text{subgroups} \\ H \leq G \end{array} \right\}$$

where $E = K_H$ and $H = Aut(K/E)$

① $E_1, E_2 \leftrightarrow H_1, H_2$. Then $E_1 \subseteq E_2 \Leftrightarrow H_1 \supseteq H_2$.

② $[K:E] = |H|$, $[E:K] = [G:H]$.

③ K/E is Galois with $Gal = H$.

④ E/F is Galois $\Leftrightarrow H \trianglelefteq G$.

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

Proof of ④: Last time we saw:

$$H \trianglelefteq G \Leftrightarrow \sigma(E) = E \text{ for all } \sigma \in G.$$

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

($\Leftarrow$) Then E is the splitting field of some sep. poly $f(x) \in F[x]$. So $E = F(\alpha_1, \dots, \alpha_k)$ where the α_i are all the roots of f. Let $\sigma \in G$.

Then $\sigma(\alpha_i)$ is a root of f, hence $= \alpha_j$.

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

($\Rightarrow$) Have $E = F(\alpha_1, \ldots, \alpha_k)$. For each α_i,

have $m_{\alpha_i, F}(x) = \prod (x - \beta_j)$ where

$G \cdot \alpha_i = \underbrace{\{\beta_1, \ldots, \beta_j\}}_{\text{all in } E!}$

So E is the splitting field of $\prod m_{\alpha_i, F}(x)$, which is separable if we remove any repeat factors. $\boxed{}$

<u>Related</u>: K = finite ext. of $\mathbb{Q}$. [A <u>number field</u>]

Consider all embeddings $\sigma : K \longrightarrow \mathbb{C}$ [<u>infinite places</u>]

<u>Thm</u>: $K/\mathbb{Q}$ is Galois $\Leftrightarrow \sigma(K) = \tau(K)$ for all emb. $K \to \mathbb{C}$.

<u>Ex</u>: $K = \mathbb{Q}[x]/(x^2 - 2)$ has two embeddings σ, τ into $\mathbb{C}$, with $\sigma(\bar{x}) = \sqrt{2}$ and $\tau(\bar{x}) = -\sqrt{2}$.

Note $\sigma(K) = \tau(K) = \mathbb{Q}(\sqrt{2})$

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

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

Proof: $K = \mathbb{Q}(\alpha)$ with $f(x) = \underbrace{m_{\alpha,F}(x)}_{\text{irred, sep}} \in \mathbb{Q}[x]$.

Get one $\sigma_i : K \to \mathbb{C}$ for each of the $\deg f$ roots of $f(x)$ in $\mathbb{C}$. Let $L \subseteq \mathbb{C}$ be the compositum of $\sigma_i(K)$, a splitting field of $f(x)$. Thus

$$\sigma_i(K) = \sigma_j(K)\ \forall i,j \iff \sigma_i(K) = L \text{ for all } i$$
$$\iff f(x) \text{ splits completely in } K.$$
$$\iff K/\mathbb{Q} \text{ is Galois.}$$

▨

Proof of (5):

$$\begin{tikzcd}[column sep=small]
 & K \arrow[d, dash] & \\
 & E_1E_2 \arrow[dl, dash] \arrow[dr, dash] & \\
E_1 \arrow[dr, dash] & & E_2 \arrow[dl, dash] \\
 & E_1 \cap E_2 \arrow[d, dash] & \\
 & F &
\end{tikzcd}
\quad \longleftrightarrow \quad
\begin{tikzcd}[column sep=small]
 & 1 \arrow[d, dash] & \\
 & H_1 \cap H_2 \arrow[dl, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
 & \langle H_1, H_2 \rangle \arrow[d, dash] & \\
 & G &
\end{tikzcd}$$

Suppose $E_1 E_2 \longleftrightarrow H$. By ①, $H \subseteq H_i$
$\Rightarrow H \subseteq H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$
then σ fixes E_1 and $E_2 \Rightarrow \sigma$ fixes $E_1 E_2$
$\Rightarrow H \supseteq H_1 \cap H_2$. ✓

Let $H = \langle H_1, H_2 \rangle$. As $H_i \leq H$,
$K_H \subseteq E_i \Rightarrow K_H \subseteq E_1 \cap E_2$. Conv,
if $\alpha \in E_1 \cap E_2$ then $\sigma(\alpha) = \alpha$
for all $\alpha \in H_i \Rightarrow \sigma(\alpha) = \alpha$ for all
$\sigma \in H \Rightarrow E_1 \cap E_2 \subseteq K_H$
$\Rightarrow K_H = E_1 \cap E_2$.