# Lecture 24: The Fund Thm of Galois Theory



Last time:

Thm: $G \leq Aut(K)$ finite. Then $[K:K_G] = |G|$,
and so $Aut(K/K_G) = G$.

Thm: For $K/F$ finite, T.F.A.E.

① $K/F$ is Galios, i.e. $|Aut(K/F)| = [K:F]$.

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

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

Pf: Last time ① $\Leftrightarrow$ ②. To see ① $\Leftrightarrow$ ③,
set $G = Aut(K/F)$. Then $|G| = [K:K_G] \leq [K:F]$
So $|Aut(K/F)| = [K:F] \Leftrightarrow K_G = F$. ▨

---

F.T.G.T.: Let $K/F$ be Galois, with $G = Gal(K/F)$.

$$\begin{Bmatrix} \text{Subfields } E \\ F \leq E \leq K \end{Bmatrix} \xleftrightarrow{\text{bijection}} \begin{Bmatrix} \text{Subgroups} \\ H \leq G \end{Bmatrix}$$

$$E \xrightarrow{\phi} G_E = \{\sigma \in G \mid \sigma|_E = id\}$$

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

Proof: $\psi$ is 1-1: Suppose $K_{H_1} = K_{H_2}$.

Then $Aut(K/K_{H_i}) = H_i \Rightarrow H_1 = H_2$.

$\psi$ is onto: Suppose $F \subseteq E \subseteq K$. By previous theorem, $K$ is the splitting field of a sep. poly $f(x) \in F[x]$
$\Rightarrow K$ is a splitting field $\Rightarrow K/E$ is Galois.
Now $Aut(K/E) \leq G$, in fact $Aut(K/E) = G_E$.

As $K/E$ is Gal, have $[K:E] = |G_E|$

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

$\Rightarrow K_{G_E} = E$. $\blacksquare$

Properties:

① If $E_1, E_2$ corresp to $H_1, H_2$, then
$E_1 \subseteq E_2 \Leftrightarrow H_1 \supseteq H_2$.

Pf: Clear.

(2) If $E \longleftrightarrow H$ then

$$\text{Galois}\left\{\begin{array}{l} K \\ | \leftarrow \deg = |H| \\ E \\ | \leftarrow \deg = [G:H] \\ F \end{array}\right.$$

*Pf*:

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

(3) $K/E$ is Gal. with $Gal(K/E) = H$.

(4) $E/F$ is Galois $\Longleftrightarrow H \triangleleft G$

In this case, $Gal(E/F) = G/H$.

(5) $E_1, E_2 \longleftrightarrow H_1, H_2$. Then $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$

*Proof of (4)*: Consider any subfield $E/F$.

For $\sigma \in G$, look at $\sigma(E)$.

Q: What is $H' = G_{\sigma(E)}$?

A: $H' = \sigma H \sigma^{-1}$

in H

typical elt of $\sigma(E)$.

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

$\sigma \tau \sigma^{-1} \sigma e = \sigma \tau e = \sigma e$ ✓

Conversely, if $\tau \in G_{\sigma(E)}$, then $\sigma^{-1} \tau \sigma \in G_E$ since $E = \sigma^{-1}(\sigma(E))$. So $H' = \sigma H \sigma^{-1}$.

[<u>Fancy Language</u>: $G$ acts on the set of subfields; $G_E$ is the stab. of $E$, and the stab of some other $\sigma(E)$ in the orbit of $E$ is just the conjugate $\sigma G_E \sigma^{-1}$.]

<u>Point</u>: $H$ is normal in $G$

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

$$\iff E/F \text{ is Galois}$$

Suppose $E/F$ is Galois. Then $E = F(\alpha_1, \ldots, \alpha_n)$ where the $\alpha_i$ are roots of a sep. poly $f(x) \in F[x]$. Now, for any $\sigma \in G$, have $\sigma(\alpha_i) = \alpha_j$

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

<u>Conversely</u>: Suppose $\sigma(E) = E$ for all.

Have $E = F(\alpha_1, \ldots, \alpha_n)$. Now

all in $E$!

$m_{\alpha_i, F} = \prod (x - \beta_i)$ where $G \cdot \alpha_i = \{\beta_1, \ldots, \beta_k\}$

in $F[x]$.

Thus $E$ is the splitting field of the sep poly

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

maybe not all $i$.

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

$$G = \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$$
$$\sigma \longmapsto \sigma|_E$$

By uniqueness of splitting fields, this is onto.

The kernel is exactly $H$. Thus

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

Proof of 5 next time.