Lecture 24: The Fundamental Thm of Galois Theory

Last time:

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

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

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

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

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

Proof: ② $\Rightarrow$ ① is an old result.

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

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 $G \cdot \alpha = \{\alpha_1, \ldots, \alpha_n\}$

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, $G = Gal(K/F)$

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

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

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

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

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

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 $[K:E] = |Aut(K/E) = G_E|$. 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. ∎

<u>Check</u>: If $\alpha = \sigma\tau\sigma^{-1}$ with $\tau \in H$ and $e \in E$, 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

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

<u>Idea for 4</u>:

$$\begin{aligned} H \lhd G &\iff H = \sigma H \sigma^{-1} \text{ for all } \sigma \in G \\ &\overset{a}{\iff} \sigma(E) = E \text{ for all } \sigma \in G \\ &\overset{b}{\iff} E/F \text{ is Galois.} \end{aligned}$$

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

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

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

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

Pf:

$$\underset{\substack{\| \\ |G|}}{[K:F]} = \underset{\substack{\| \\ |H|}}{[K:E]}\,[E:F]$$

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

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

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

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

[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

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

maybe not all i

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

$$G = Gal(K/F) \longrightarrow Gal(E/F)$$
$$\sigma \longmapsto \sigma|_E$$

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

$$Gal(E/F) = G/H$$

<u>Example</u>: $K = \mathbb{Q}(\alpha = \sqrt[3]{2},\ \zeta = \zeta_3 = \frac{1}{2}(1+\sqrt{3}i))$

$\quad\ \ |$

$\ F = \mathbb{Q}$ is the splitting field of $X^3 - 2 \in \mathbb{Q}[x]$.

$$X^3 - 2 = (x-\alpha)(x-\alpha\zeta)(x-\alpha\zeta^2)$$

<u>$[K:F] = 6$</u> since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ and $K = \mathbb{Q}(\alpha)\mathbb{Q}(\zeta)$

$[\mathbb{Q}(\zeta):\mathbb{Q}] = 2$

Any $\sigma \in G = Gal(K/F)$ has $\sigma(\alpha)$ in $\alpha,\ \underset{\beta}{\alpha\zeta},\ \underset{\gamma}{\alpha\zeta^2}$ (where $\beta = \alpha\zeta$, $\gamma = \alpha\zeta^2$)

and $\sigma(\zeta)$ in $\zeta,\ \zeta^2 = \bar{\zeta}$.

Since $K = \mathbb{Q}(\alpha,\zeta)$ and K/F is Galois, have

$|G| = [K:F] = 6$ so all pairs of poss. for $(\sigma(\alpha), \sigma(\zeta))$

occur.

Let $\sigma(\alpha) = \beta$ and $\sigma(\zeta) = \zeta$ $\qquad \alpha \xrightarrow{\sigma} \beta \xrightarrow{\sigma} \gamma \xrightarrow{\sigma} \alpha$

and τ be complex conj, i.e. $\tau(\alpha) = \alpha$

$\tau(\zeta) = \zeta^2$

Recall $G \cong S_3$ with $\sigma \leftrightarrow (123)$, $\tau \leftrightarrow (23)$

Note

$K_{\langle\tau\rangle} = \mathbb{Q}(\alpha)$ and $K_{\langle\sigma\rangle} = \mathbb{Q}(\zeta)$

order = 2
index in G = 3
not normal

order = 3
index = 2
normal.

$\langle \tau \rangle$ is not normal as $(\sigma \circ \tau \circ \sigma^{-1})(\alpha)$
$= \sigma \circ \tau(\gamma) = \sigma(\beta) = \gamma$ so
$\sigma \tau \sigma^{-1} \neq \tau$ and so not in $\langle \tau \rangle$.

$\langle \sigma \rangle$ is normal as index $= 2$.

$\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois as $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) = 1$.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois as is splitting field of
$x^2 + x + 1 = (x - \zeta)(x - \bar{\zeta})$.

a) Set $H = \langle \tau \rangle$. Then $H' = \sigma H \sigma^{-1} = \langle \tau' \rangle$
for $\tau' = \sigma \tau \sigma^{-1}$ is some other cyclic subgp of
order 2.

<u>Claim:</u> $K_{H'} = \sigma(K_H) = \mathbb{Q}(\beta)$

<u>Pf</u> (General!) If $\delta \in K_H$ then $\sigma(\delta)$ in $K_{H'}$
as $(\sigma \tau \sigma^{-1})(\sigma(\delta)) = \sigma \tau(\delta) = \sigma(\delta)$. So
$\sigma(K_H) \subseteq K_{H'}$. Equal since $H = \sigma^{-1} H' \sigma$
$\Rightarrow \sigma^{-1}(K_{H'}) \subseteq K_H$.

Also $H'' = \sigma^2 H \sigma^{-2}$ has $K_{H''} = \mathbb{Q}(\gamma)$.

Moral: When H is not normal, get several $K_{H'}/_F \cong K_H/_F$ inside K.

b) Set $H = \langle \sigma \rangle$, which is normal. For any $\varphi \in G$, have $\varphi H \varphi^{-1} = H$. So $\varphi(H) = H$, giving some $\bar{\varphi} \in \mathrm{Aut}(K_H/_F)$ where $K_H = \mathbb{Q}(\zeta)$.

i) $\varphi = \sigma$. Then $\sigma|_{K_H} = \mathrm{id}_H$.

ii) $\varphi = \tau$ Then $\tau|_{K_H} = \zeta \mapsto \bar{\zeta}$ is the generator of $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Moral: When H is normal, each elt of G gives an autom. of $K_H/_F$.