# Lecture 25: Fundamental Thm of Galois Theory II ①

Thm: $K/F$ finite, Galois with $G = Gal(K/F)$

$$\left\{\begin{array}{c}\text{subfields } E \\ F \leq E \leq K\end{array}\right\} \xleftrightarrow{\text{bijection}} \left\{\begin{array}{c}\text{subgps} \\ H \leq G\end{array}\right\}$$

$$E \longmapsto G_E = Aut(K/E)$$

$$K_H \longleftarrow\!\shortmid \quad H$$

① $E_1, E_2 \longleftrightarrow H_1, H_2$. Then $E_1 \subseteq E_2 \Longleftrightarrow H_1 \geq H_2$

② $[K:E] = |H|$, $[E:F] = [G:H]$

③ $K/E$ is Galois with $Gal = H$

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

$$\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}$$

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

---

[Proved except for ④ and ⑤. But let's go back to the example first.]

Ex: $K = \mathbb{Q}(\alpha = \sqrt[3]{2}, \zeta = \zeta_3)$ $\qquad \beta = \zeta\alpha$, $\gamma = \zeta^2\alpha$

$$\begin{array}{c} K \\ 6\,| \\ F = \mathbb{Q} \end{array}$$

splitting field of $x^3 - 2 = (x-\alpha)(x-\beta)(x-\gamma)$ in $\mathbb{Q}[x]$

$G = \mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ is gen by

$\sigma : \alpha \to \beta \to \gamma \to \alpha$ fixes $\zeta$ $\longleftrightarrow$ $(1\ 2\ 3)$

$\tau : \beta \longleftrightarrow \gamma$ fixes $\alpha, \zeta$ $\longleftrightarrow$ $(2\,3)$

Recall:

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

<u>Rest of $G$:</u> $\sigma^{-1} \leftrightarrow (3\ 2\ 1)$

$$\tau' = \sigma\tau\sigma^{-1} = (123)(23)(321) = (13)$$

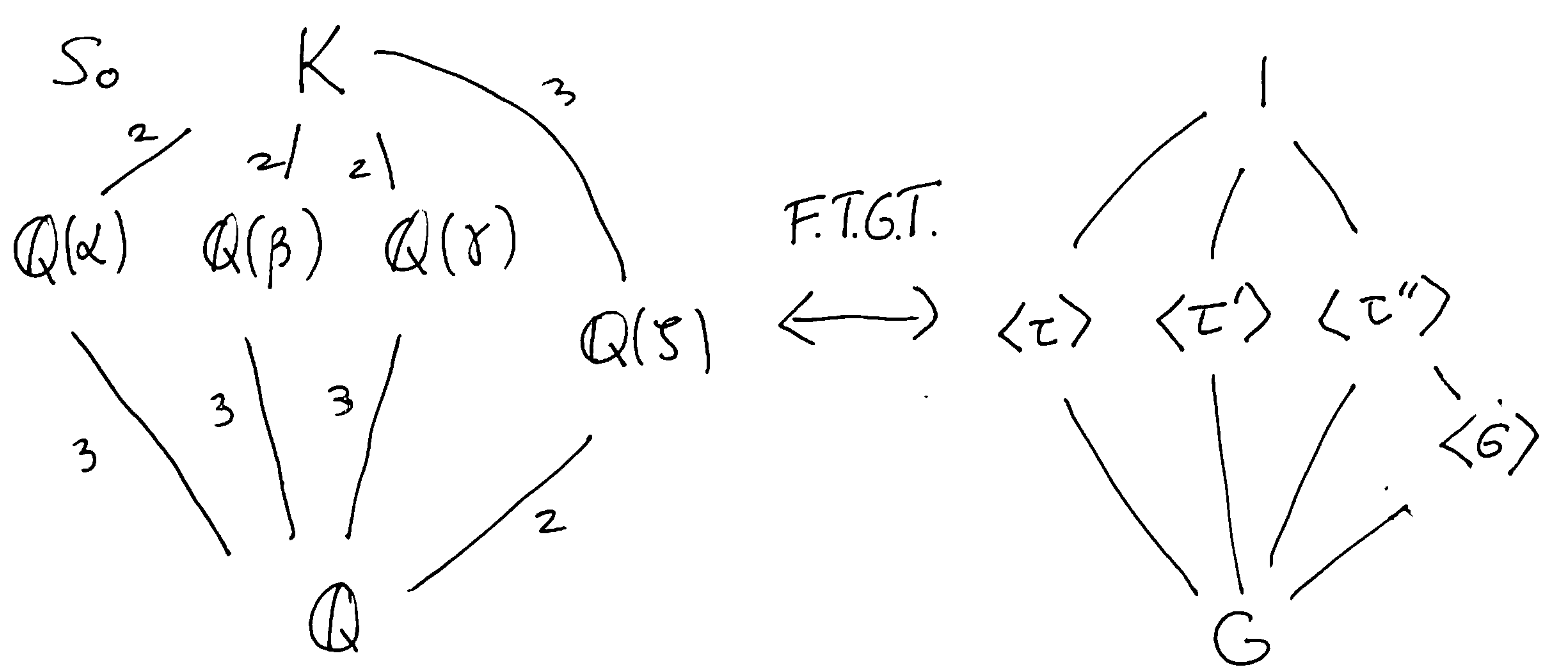
$$\tau'' = \sigma^{-1}\tau\sigma = (12)$$

Note $\zeta = \beta/\alpha$ so $\tau'(\zeta) = \beta/\gamma = 1/\zeta = \zeta^2$

$\tau''(\zeta) = \alpha/\beta = 1/\zeta = \zeta^2$

[Start here: ↴]

So



<u>Cor</u>: $K/F$ finite, then there are finitely many $E$ with $F \subseteq E \subseteq K$.

<u>Pf</u>: When $K/F$ is Galois, this follows from F.T.G.T. as $Gal(K/F)$ has finitely many subgps. <u>If</u> $K = F(\alpha)$, use spliting field $L$ of $m_{\alpha,F}(x)$ over $K$. ▨

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

$H = \langle \tau \rangle$ is not normal as $\sigma\tau\sigma^{-1} = \tau' \notin H$.

<u>Idea behind</u> 4:

Set $H' = \sigma H \sigma^{-1} = \langle \tau' \rangle$

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

This is completely 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 $H = \sigma^{-1} H' \sigma \Rightarrow \sigma^{-1}(K_{H'}) \subseteq K_H$.

Moral: If $H$ is not normal, get several subfields $E = K_H$, $E' = K_{H'}$ with $\sigma \in G$ with $\sigma(E) = E'$ $\left( \Rightarrow E/F \cong E'/F \right)$

In contrast, if $E/F$ is Galois, then $\sigma(E) = E$ for all $\sigma \in E$ since $E$ is the splitting field of some sep. poly $f \in F[x]$.

Addendum: If $H \triangleleft G$, then $Gal(E/F) \cong G/H$.

Ex: $H = \langle \sigma \rangle$ $\quad K_H = \mathbb{Q}(\zeta)$

Any $\varphi \in G$ has $\varphi H \varphi^{-1} = H$, so $\varphi(K_H) = K_H$, giving $\bar{\varphi} \in Aut(K_H/\mathbb{Q})$.

i) $\varphi = \sigma$ then $\bar{\sigma} = \sigma|_{K_H} = id_{K_H}$

ii) $\varphi = \tau$ then $\bar{\tau}$ sends $\zeta$ to $\bar{\zeta}$, which generates $Aut(\mathbb{Q}(\zeta)/\mathbb{Q})$.

[For full proofs of 4, 5 see long versions of notes for this and last lecture. Or see textbook.]

# Lecture 25: Fundamental Thm of Galois Theory II 

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

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

$$E \longmapsto G_E = Aut(K/E)$$

$$K_H \longleftarrow H$$

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 $Gal = H$.
4. $E/F$ is Galois $\iff H \lhd G$.
5. $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$ and $E_1 E_2 \longleftrightarrow H_1 \cap H_2$.

$$\begin{matrix} K \\ | \\ E \\ | \\ F \end{matrix}$$

---

**Pf of 4:** Last time, saw that if $E \longleftrightarrow H$ and $\sigma \in G$, then $\sigma(E) \longleftrightarrow H' = \sigma H \sigma^{-1}$

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

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

<u>Claim</u>: $\sigma(E) = E \ \forall \sigma \in G \iff E/F$ is Galois.

($\Leftarrow$) $E$ 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 $\alpha_i$; as $E = F(\alpha_1, \dots, \alpha_n)$ this gives $\sigma(E) = E$.

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

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

So $m_{\alpha_i, F}(x)$ splitts 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 $m_{\alpha_i, F}(x)$. $\square$

<u>Related</u>:

$K$ = finite ext of $\mathbb{Q}$ (A <u>number field</u>)

Consider <u>all</u> embeddings $\sigma : K \longrightarrow \mathbb{C}$ ("infinite place")

<u>Thm</u>: $K/\mathbb{Q}$ is Galois $\Longleftrightarrow$ $\forall$ embeddings $\sigma, \tau$ of $K \hookrightarrow \mathbb{C}$ have $\sigma(K) = \tau(K)$.

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

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

Get one $\sigma_i : K \longrightarrow \mathbb{C}$ 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

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

<u>Proof of 5</u>:

Want to show

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

Suppose $E_1E_2 \longleftrightarrow H$. By 1, $H \leq H_i$
$\Rightarrow H \subseteq H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$
then $\sigma$ fixes $E_1$ and $E_2 \Rightarrow \sigma$ fixes $E_1E_2$
$\Rightarrow H \supseteq H_1 \cap H_2$. ✓

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

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 $\alpha \in H$. $\Rightarrow$

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