Lecture 37: The Fundamental Thm of Galois Theory

§14.2 of [DF]

Previously:

Thm A: If K/F is finite then $|\mathrm{Aut}(K/F)| \leq [K:F]$.

Def: A finite K/F is Galois when $|\mathrm{Aut}(K/F)| = [K:F]$.

Thm C: Suppose $G \leqslant \mathrm{Aut}(K)$ is finite. Then K/K_G is Galois with $\mathrm{Aut}(K/K_G) = G$.

[Proved in the setting where char $K = 0$ where every finite extension is simple.]

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

1. K/F is Galois.
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 $[K:K_G] \underset{\text{by Thm C}}{=} |G| \overset{(1)}{=} [K:F]$; Hence $K_G = F$.

3 $\Rightarrow$ 2: Assume $K = F(\alpha)$ [e.g. char $K = 0$]

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 $F[x]$. $\blacksquare$

<u>Fund. Thm of Galois Theory:</u> K/F Galois, $G = Gal(K/F)$.

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

$$E \xmapsto{\quad \phi \quad} Aut(K/E) = G_E =$$

$$= \{\sigma \in G \mid \sigma|_E = id_E\}$$

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

<u>Pf:</u> ψ <u>injective</u>: Suppose $K_{H_1} = K_{H_2}$. By Thm C,

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

<u>ψ surjective</u>: Suppose $F \subseteq E \subseteq K$. By Thm B, K is a splitting field of a sep. poly $f \in F[x]$. As f is also in $E[x]$, we learn K/E is Galois.

Hence $[K:E] = |\mathrm{Aut}(K/E) = G_E|$. Now

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

Thm C. So $K_{G_E} = E$ and ψ is onto. $\blacksquare$

<u>Properties:</u>

① If E_1, E_2 correspond to H_1, H_2, then

$$E_1 \subseteq E_2 \iff H_1 \supseteq H_2.$$

② If $E \longleftrightarrow H$, then $[K:E] = |H|$
and $[E:F] = [G:H]$

③ K/E is Galois with
$\mathrm{Gal}(K/E) = H$

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

④ E/F Galois $\iff H \triangleleft G$. In this case
$\mathrm{Gal}(E/F) = G/H$.

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

<u>Easy proofs</u>: ① Clear. ③ Follows from the proof that ψ is surjective. ② Have

$$\underset{|G|}{\underset{\shortparallel}{[K:F]}} = \underset{|H|}{\underset{\shortparallel}{[K:E]}}[E:F].$$

[Will prove ④ and ⑤ later.]

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

$\quad |$

$F = \mathbb{Q}$ is the splitting field of $\underset{\underset{(x-\alpha)(x-\zeta\alpha)(x-\zeta^2\alpha)}{\|}}{x^3 - 2}$ in $\mathbb{Q}[x]$.

$[K:F] = 6$ since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ and $K = \mathbb{Q}(\alpha)\mathbb{Q}(\zeta)$
$\qquad\qquad\qquad\quad [\mathbb{Q}(\zeta):\mathbb{Q}] = 2$

Any $\sigma \in G = Gal(K/F)$ has $\sigma(\alpha)$ in $\{\alpha, \overset{\beta}{\overset{\|}{\alpha\zeta}}, \overset{\gamma}{\overset{\|}{\alpha\zeta^2}}\}$
and $\sigma(\zeta)$ in $\zeta, \zeta^2 = \bar{\zeta}$.

Since $K = \mathbb{Q}(\alpha, \zeta)$ and K/F is Galois, have $|G| = [K:F] = 6$ and so all possible pairs for $(\sigma(\alpha), \sigma(\zeta))$ must occur.

Define τ to be complex conj, i.e. $\tau(\alpha) = \alpha$
$\tau(\zeta) = \zeta^2$

and σ to satisfy $\sigma(\alpha) = \beta$
$\sigma(\zeta) = \zeta$.

$\alpha \xrightarrow{\sigma} \beta \xrightarrow{\sigma} \gamma \xrightarrow{\sigma} \alpha$

Recall $G \cong S_3$ with

$\sigma \longleftrightarrow (1\,2\,3)$

$\tau \longleftrightarrow (2\,3)$

Note $K_{\langle\tau\rangle} = \mathbb{Q}(\alpha)$ and $\langle\tau\rangle$ is not normal
(matches $\mathbb{Q}(\alpha)/\mathbb{Q}$ not Galois)

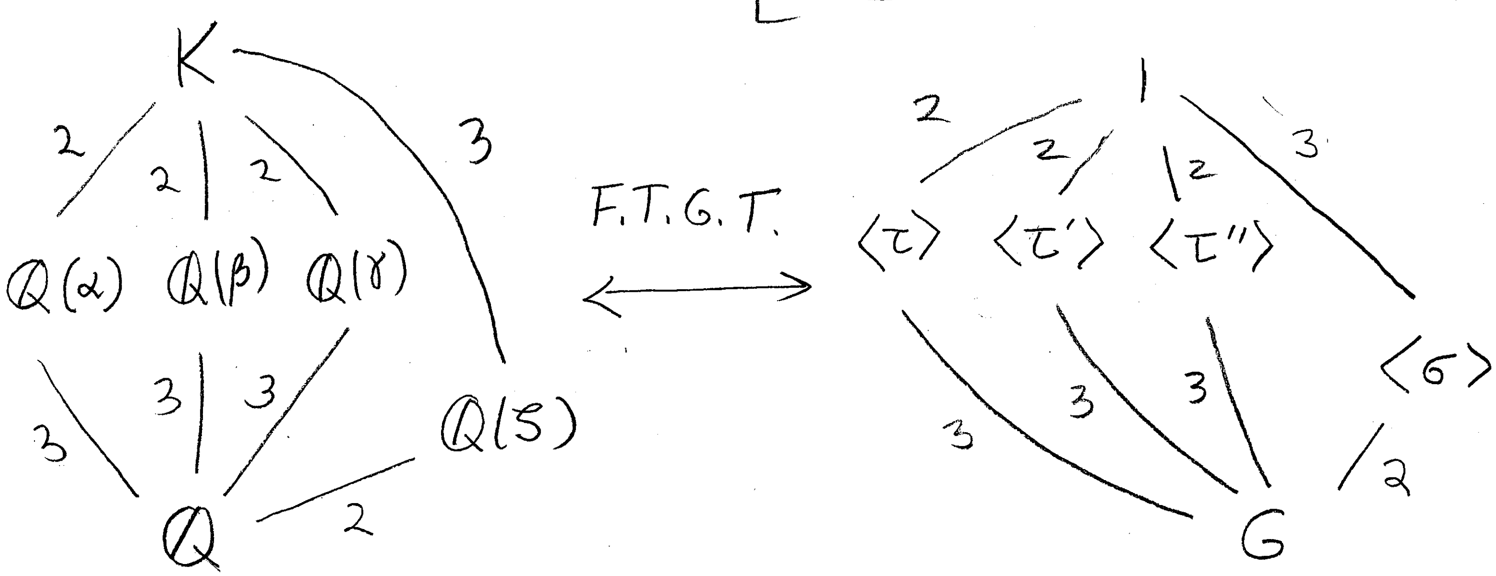
Note $K_{\langle \sigma \rangle} = \mathbb{Q}(\zeta)$ with $\langle \sigma \rangle$ normal (index 2), matching $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois.

Rest of G: $\sigma^{-1} \leftrightarrow (3\,2\,1)$ (in $\langle \sigma \rangle$)

$$\left.\begin{array}{l} \tau' \leftrightarrow (1\,3) \\ \tau'' \leftrightarrow (1\,2) \end{array}\right\} \text{ Note } \zeta = \beta/\alpha \text{ so } \tau'(\zeta) = \beta/\gamma = 1/\zeta = \zeta^2$$

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

[Start here:]



Note: None of $\langle \tau \rangle, \langle \tau' \rangle, \langle \tau'' \rangle$ are normal as e.g. $\tau' = \sigma \tau \sigma^{-1}$ and $\tau'' = \sigma^{-1} \tau \sigma$.

Cor of F.T.G.T: K/F finite, then there are finitely many E with $F \subseteq E \subseteq K$.

Pf: If K/F is Galois, this follows as the finite gp $Gal(K/F)$ has finitely many subgps.

If K is not Galois, can find $L \supseteq K$ with L/F Galois: e.g. if $K = F(\alpha)$ take L to be the splitting field of $m_{\alpha,F}(x)$ over K.

(assuming char 0 here for a shortcut.) ▨