Lecture 38: Fundamental Theorem of Galois Theory II. §14.2 of [DF]

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

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

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

$$K_H \longmapsto H$$

① $E_1 \subseteq E_2 \Leftrightarrow H_1 \supseteq H_2$ where $E_i \leftrightarrow H_i$.

② $[K:E] = |H|$, $[E:F] = [G:H]$.

③ K/E is Galois with $Gal = H$

④ E/F is Galois $\Leftrightarrow H \lhd G$; if so $Gal(E/F) \cong G/H$

⑤ $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ and $E_1E_2 \leftrightarrow H_1 \cap H_2$.

didn't mention last time.

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

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

Ex: $K = \mathbb{Q}(\alpha = \sqrt[3]{2}, \zeta = e^{2\pi i/3})$

$6 = [K:F]$, $F = \mathbb{Q}$

splitting field of $X^3 - 2 = (x-\alpha)(x-\beta)(x-\gamma)$

$\beta = \zeta\alpha$, $\gamma = \zeta^2\alpha$.

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

σ: $\alpha \to \beta \to \gamma \to \alpha$ fixes ζ $\longleftrightarrow$ (123)

τ: $\beta \longleftrightarrow \gamma$ fixes α, $\longleftrightarrow$ (23)

$\zeta \longleftrightarrow \zeta^2$

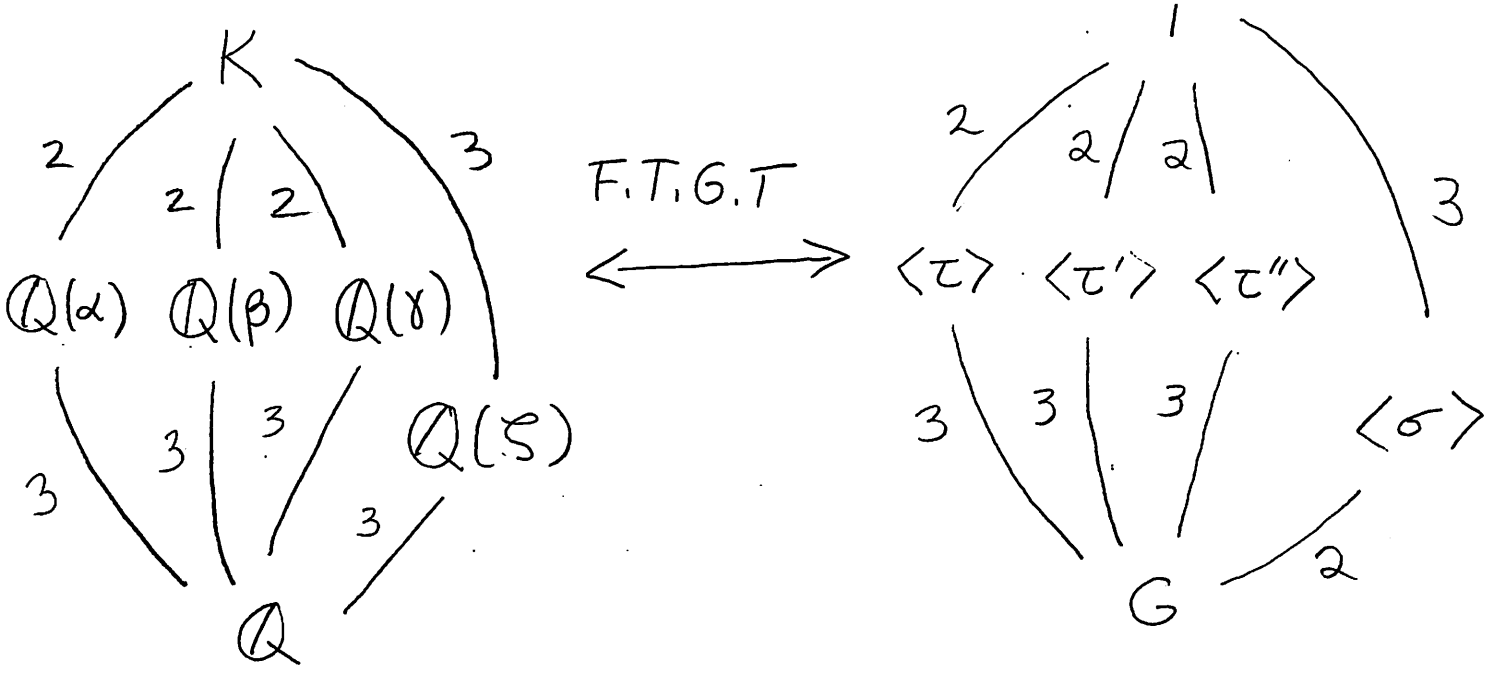
<u>Note</u>: $K_{\langle\sigma\rangle} = \mathbb{Q}(\zeta)$ since $K_{\langle\sigma\rangle} \supseteq \mathbb{Q}(\zeta)$ and $[K_{\langle\sigma\rangle} : \mathbb{Q}] = [G : \langle\sigma\rangle] = 2$.

$K_{\langle\tau\rangle} = \mathbb{Q}(\alpha)$ for same reasons.

Set $\tau' \longleftrightarrow (13)$ where $\tau'(\zeta) = \tau'(\beta/\alpha) = \beta/\gamma = 1/\zeta = \zeta^2$

$\tau'' \longleftrightarrow (12)$ $\tau''(\zeta) = \tau''(\beta/\alpha) = \alpha/\beta = 1/\zeta = \zeta^2$

[Start on right. $\longrightarrow$]



As $Aut(\mathbb{Q}(\alpha)/\mathbb{Q}) = 1$ and the same for β, γ.

whereas $\mathbb{Q}(\zeta)$ is the splitting field of x^2+x+1, the only proper subfield of $K/\mathbb{Q}$ that is Galois is $\mathbb{Q}(\zeta)$. Similarly, $\langle\sigma\rangle$ is the only normal proper subgp of G as $\sigma\tau\sigma^{-1}=\tau'$ and $\sigma^{-1}\tau\sigma=\tau''$. [Check by mult. perms!]

Proof of (4): G acts on $\{$subfields $F\subseteq E\subseteq K\}$ by $\sigma\cdot E=\sigma(E)$. G acts on $\{$subgps $H\leq G\}$ by $\sigma\cdot H=\sigma H\sigma^{-1}$!

Lemma: The bijections in the F.T.G.T. commute with these actions, i.e. $\sigma\cdot K_H = K_{\sigma\cdot H}$ and $G_{\sigma\cdot E}=\sigma\cdot G_E$.

Pf: Skip! It suffices to show $\sigma\cdot K_H\subseteq K_{\sigma\cdot H}$ as the two fields have the same degree over F.

Suppose $\alpha\in\sigma\cdot K_H$ and let η be any elt of $\sigma\cdot H$, i.e. $\alpha=\sigma(\beta)$ for $\beta\in K_H$ and $\eta=\sigma\tau\sigma^{-1}$ for $\tau\in H$.

Then $\eta(\alpha)=(\sigma\tau\sigma^{-1})(\sigma(\beta))=\sigma(\tau(\beta))$
$=\sigma(\beta)=\alpha$. Thus $\alpha\in K_{\sigma\cdot H}$
↑ as $\beta\in K_H$ as needed. ▨

Now $H \lhd G \iff \sigma \cdot H = H$ for all $\sigma \in G$

$\iff \sigma \cdot K_H = K_H$ for all $\sigma \in G$

$\overset{(\star)}{\iff} K_{H/F}$ is Galois. [Prob. skip pf of $\star$]

$(\star)$ ($\Leftarrow$) K_H is the splitting field of $f(x) \in F[x]$,
i.e. $K_H = F(\alpha_1, \ldots, \alpha_n)$ where α_i are the roots of f.
Any $\sigma \in G$ fixes $F \Rightarrow$ permutes the α_i
$\Rightarrow \sigma(K_H) = K_H$.

($\Rightarrow$) Consider the homomorphism $\pi : G \longrightarrow Aut(K_{H/F})$

$\sigma \longmapsto \sigma|_{K_H}$

Then $\ker(\pi) = Aut(K_{/K_H}) = H$, so

$|\mathrm{im}(\pi)| = |G_{/H}| \overset{(2)}{=} [K_H : F] \geq |Aut(K_{H/F})|$.

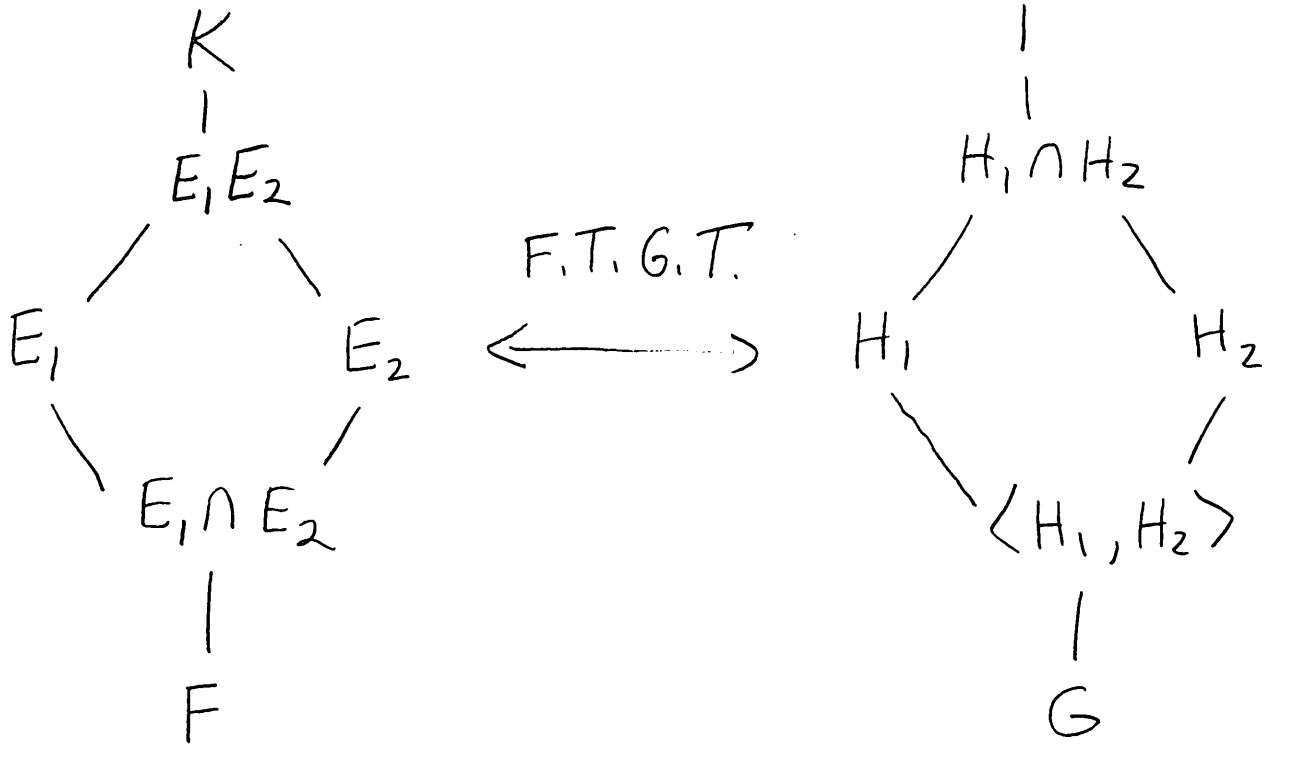
↑ Thm A from last time

Since $|\mathrm{im}(\pi)| \leq |Aut(K_{H/F})|$, we get $[K_H : F]$
$= Aut(K_{H/F})$, i.e. $K_{H/F}$ is Galois with
$Gal \cong G_{/H}$. ▨

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

Pf: When K/F is Galois, follows because $Gal(K/F)$ has finitely many subgroups. If $K = F(\alpha)$, use the splitting field of $m_{\alpha,F}(x)$ over K. ▨

Proof of (5): Want to show: [Prob. skip!]



Suppose $E_1E_2 \longleftrightarrow H$. By (1), $H \leq H_i \Rightarrow$ $H \leq H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$, then σ fixes E_1 and $E_2 \Rightarrow \sigma$ fixes E_1E_2 $\Rightarrow H \geq H_1 \cap H_2$. So $H = H_1 \cap H_2$.

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

As $H_i \leq H$, have $E_i \supseteq K_H \Rightarrow K_H \subseteq E_1 \cap E_2$.

Conversely, if $\alpha \in E_1 \cap E_2$, then $\sigma(\alpha) = \alpha$ for all $\sigma \in H_i \Rightarrow \sigma(\alpha) = \alpha$ for all $\alpha \in H \Rightarrow \alpha \in K_H$.

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