Thm: $K/F$ finite, Galois with $G = \text{Gal}(K/F)$

\[
\begin{array}{ccc}
\{ \text{Subfields } E \} & \text{bijection} & \{ \text{Subgps } H \leq G \} \\
\{ F \leq E \leq K \} & & \\
\end{array}
\]

$E_1 \rightarrow G_E = \text{Aut}(K/E)$

$K_H \leftarrow H$

1. $E_1, E_2 \leftrightarrow H_1, H_2$. Then $E_1 \leq E_2 \iff H_1 \geq H_2$

2. $[K:E] = 1 \iff 1, [E:F] = [G:H]$

3. $K/E$ is Galois with $\text{Gal} = H$

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

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

[Proved except for (4) and (5). But let’s go back]

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

Ex: $K = \mathbb{Q}(\sqrt[3]{2}, \zeta = S_3)$

$\beta = 5\alpha$, $\gamma = 5^2\alpha$

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

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

\[ \sigma : \alpha \mapsto \beta \text{ fixes } \gamma \mapsto (1\ 2\ 3) \]

\[ \tau : \beta \leftrightarrow \gamma \text{ fixes } \alpha, \gamma \leftrightarrow (2\ 3) \]

Recall:

\[ K_{\langle \tau \rangle} = \mathbb{Q}(\alpha) \] and \[ K_{\langle \sigma \rangle} = \mathbb{Q}(\gamma) \]

Rest of \( G \):

\[ \sigma^{-1} \leftrightarrow (3\ 2\ 1) \]

\[ \tau' = \sigma \tau \sigma^{-1} = (1\ 2\ 3)(2\ 3)(3\ 2\ 1) = (1\ 3) \]

\[ \tau'' = \sigma^{-1} \tau \sigma = (1\ 2) \]

Note \( \delta = \beta/\alpha \) so \( \tau'(\delta) = \beta/\gamma = 1/\delta = \delta^{-2} \)

\[ \tau''(\delta) = \alpha/\beta = 1/\delta = \delta^{-2} \]

[Start here: 1]
Cor: If $K/F$ is finite, then there are finitely many $E$ with $F \leq E \leq K$.

Pf: When $K/F$ is Galois, this follows from F.T.G.T. as $\text{Gal}(K/F)$ has finitely many subgroups. If $K = F(\alpha)$, use splitting field $L$ of $m_{\alpha,1}(x)$ over $K$. 

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

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

Idea behind (4):

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

Key: $\sigma(K_H) = \sigma(\mathbb{Q}(\alpha)) = \mathbb{Q}(\beta) = K_{H'}$.

This is completely general: If $S \in K_H$ then $\sigma(S)$ in $K_{H'}$ as $(\sigma \cdot \tau \cdot \sigma^{-1})(\sigma(S)) = \sigma(\tau(\sigma(S))) = \sigma(S)$. 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 $\sigma(E) = E'$ (\(\Rightarrow E/F \cong E'/F\)).

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 $H < G$, then $\text{Gal}(E/F) \cong G/H$.

Ex: $H = \langle \sigma \rangle$, $K_H = \mathbb{Q}(\sqrt{3})$.

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

i) $g = \sigma$ then $\bar{\sigma} = \sigma \mid_{K_H} = \text{id}_{K_H}$

ii) $g = \tau$ then $\bar{\tau}$ sends $\sqrt{3}$ to $\bar{\sqrt{3}}$, which generates $\text{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$.

[For full proofs of (4), (5) see long versions of notes for this and last lecture. Or see textbook.]
Thm: $K/F$ Galois, $G = \text{Gal}(K/F)$. Have a bijection
$$\begin{align*}
\{ \text{subfields } E \} & \longleftrightarrow \{ \text{subgroups } H \leq G \} \\
F \leq E \leq K & \quad \mapsto \quad H \leq G \\
E & \mapsto G_E = \text{Aut}(K/E) \\
K_H & \leftarrow \quad H
\end{align*}$$

1. $E_1, E_2 \leftrightarrow H_1, H_2$. Then $E_1 \subseteq E_2 \iff H_1 \supseteq H_2$.
2. $[K:E] = [H:H]$, $[E:F] = [G:H]$
3. $K/E$ is Galois with $\text{Gal} = H$.
4. $E/F$ is Galois $\iff H \triangleleft G$.
5. $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ and $E_1 E_2 \leftrightarrow H_1 \cap H_2$.

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

Therefore, $\sigma(E) = E$ for all $\sigma \in G$ $\iff H = \sigma H \sigma^{-1}$ for all $\sigma \in G$, i.e. $H \triangleleft G$. 

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

($\Leftarrow$) $E$ is the splitting field of a separable poly $f(x)$ in $F[x]$, with roots $\alpha_1, \ldots, \alpha_n \in E$ where $n = \deg f(x)$. Any $\sigma \in G$ permutes the $\alpha_i$'s; as $E = F(\alpha_1, \ldots, \alpha_n)$ this gives $\sigma(E) = E$.

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

$$m_{\alpha_i, F}(x) = \prod_{j} (x - \beta_{i,j}) \quad \text{where } G \cdot \alpha_i = \{ \beta_{i,1}, \ldots, \beta_{i,k} \} \quad \text{all in } E!$$

So $m_{\alpha_i, F}(x)$ splits 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 $m_{\alpha_i, F}(x)$. \qed
Related:

\[ K = \text{finite ext of } \mathbb{Q} \quad (\text{A number field}) \]

Consider all embeddings \( \sigma : K \to \mathbb{C} \) ("infinite place")

Thm: \( K/\mathbb{Q} \) is Galois \( \iff \forall \text{ embeddings } \sigma, \tau \text{ of } K \to \mathbb{C} \text{ have } \sigma(K) = \tau(K). \]

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

Note \( \sigma(K) = \tau(K) = \mathbb{Q}(\sqrt{2}) \) and \( K/\mathbb{Q} \) is Galois

- \( K = \mathbb{Q}[x]/(x^3 - 2) \), have \( \sigma(x) = \sqrt[3]{2} \)
  \( \tau(x) = \sqrt[3]{2} \cdot 3 \)
  \( \eta(x) = \sqrt[3]{2} \cdot \sqrt[3]{2} \)

Note \( \sigma(K) \subseteq \mathbb{R} \) but \( \tau(K) \) isn't.

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

Get one \( \sigma_i : K \to \mathbb{C} \) 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

$$\sigma_i(K) = \sigma_j(K) \quad \forall i, j \iff \sigma_i(K) = L \text{ for all } i$$

$$\iff f(x) \text{ splits completely in } K.$$ 

$$\iff K/Q \text{ is Galois.} \quad \square$$

**Proof of ⑤:**

Want to show

\[
\begin{array}{cc}
K & 1 \\
\downarrow & \downarrow \\
E_1E_2 & \text{F.T.G.T.} \\
\downarrow & \downarrow \\
E_1 \cap E_2 & \Leftrightarrow \\
\downarrow & \downarrow \\
F & H_1 \cap H_2 \\
\downarrow & \downarrow \\
< \langle H_1, H_2 \rangle & G
\end{array}
\]

Suppose $E_1E_2 \iff H$. By ①, $H \leq H_i \implies H \leq H_1 \cap H_2$. Conversely, if $\sigma \in H_1 \cap H_2$ then $\sigma$ fixes $E_1$ and $E_2 \implies \sigma$ fixes $E_1E_2 \implies H \geq H_1 \cap H_2$. √
Set $H = \langle H_1, H_2 \rangle$, will show $K_H = E_1 \cap E_2$.

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

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

$E_1 \cap E_2 \leq K_H \Rightarrow E_1 \cap E_2 = K_H$. \qed