Galois Theory:

Recall Last time : Thm. If $K/\mathbb{Q}$ is Galois, then

$$[K:\mathbb{Q}] = |\mathrm{Aut}(K/\mathbb{Q})|.$$

Converse Thm: If $[K:\mathbb{Q}] = |\mathrm{Aut}(K/\mathbb{Q})|$, then $K/\mathbb{Q}$ is Galois.

Pf: Given $\alpha \in K$, with $f(x) \in \mathbb{Q}[x]$ is the minimal degree polynomial s.t. $f(\alpha)=0$. We want to show that all roots of $f(x)$ are in K.

Construct another polynomial $\tilde{f}(x) := \prod_{\sigma \in \mathrm{Aut}(K/\mathbb{Q})} (x - \sigma(\alpha))$

<u>Claim</u>: $\tilde{f}(x) \in \mathbb{Q}[x]$.

We notice that after expanding terms of $\tilde{f}(x)$, then all the coefficients are fixed by any $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$.

eg. $\sigma_0 \left[\prod_{\sigma \in \mathrm{Aut}(K/\mathbb{Q})} -\sigma(\alpha) \right] = \prod_{\sigma \in \mathrm{Aut}(K/\mathbb{Q})} -\sigma(\alpha)$

So then all coefficients are in $\mathbb{Q}$ (An element β in K fixed by every $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ must lie in $\mathbb{Q}$, since otherwise.

$$\begin{matrix} K \\ | \\ \mathbb{Q}[\beta] \\ | \\ \mathbb{Q} \end{matrix} \qquad \underset{\substack{\| \\ [K:\mathbb{Q}]}}{|\mathrm{Aut}(K/\mathbb{Q})|} \overset{\beta \text{ fixed by } \mathrm{Aut}(K/\mathbb{Q})}{=} |\mathrm{Aut}(K/\mathbb{Q}[\beta])| \leq [K:\mathbb{Q}[\beta]].$$

Condition Given

general statement that $|\mathrm{Aut}(K/F)| \leq [K:F]$ by primitive element thm)

□

Since $f(\alpha)=0$ $\tilde{f}(\alpha)=0$

$f, \tilde{f} \in \mathbb{Q}[x]$

so $f(x) \mid \tilde{f}(x)$

since $\tilde{f}(x)$ splits in $K[x]$

So $f(x)$ splits in $K[x]$. $\square$.

Thm. $K/\mathbb{Q}$ is Galois $\Leftrightarrow$ $[K:\mathbb{Q}] = |\mathrm{Aut}(K/\mathbb{Q})|$

Assme this holds for HW. We will address this on Wednesday. → [$\Leftrightarrow$ K is a splitting field of certain $f(x) \in \mathbb{Q}[x]$] ??

Fundamental Thm of Galois Theory. $\mathrm{Aut}(K/\mathbb{Q})$ when K Galois
$\overset{!!}{}$

Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) = G$.

1) Then there is an one-to-one bijection between subfields of K and subgrps of G.

$$\begin{tikzcd}[row sep=large]
K \arrow[d, dash] & \{e\} \arrow[d, dash] \\
F \arrow[d, dash] & H \arrow[d, dash] \\
\mathbb{Q} & G
\end{tikzcd}$$

Fields		Grps
F	$\xrightarrow{\pi_1}$	$\mathrm{Aut}(K/F)$
K^H	$\xleftarrow{\pi_2}$	H

$K^H = \{a \in K \mid \forall h \in H,\ \sigma(a)=a\}$

One can easily check that K^H is a subfield.

2) K/F is always Galois and with $\mathrm{Gal}(K/F) = \mathrm{Aut}(K/F) \subseteq \mathrm{Aut}(K/\mathbb{Q})$.

3) $F/\mathbb{Q}$ is Galois $\iff$ $\mathrm{Aut}(K/F) \triangleleft \mathrm{Aut}(K/\mathbb{Q})$.

Pf: 1) $\begin{cases} \pi_1 \circ \pi_2 = id \\ \pi_2 \circ \pi_1 = id \end{cases}$ $\Rightarrow$ π_1 and π_2 are inverse of each other and gives a bijection.

So we just need to show $\pi_1 \circ \pi_2 = id$ & $\pi_2 \circ \pi_1 = id$.

This proves 2) in Thm.

<u>Claim 1</u>: For arbitrary subfield $\mathbb{Q} \subseteq F \subseteq K$. we have K/F is Galois.

· Given $\alpha \in K$. define $f_1(x) \in \mathbb{Q}[x]$ to be the minimal degree poly with $f_1(\alpha) = 0$

define $f_2(x) \in F[x]$ to be the minimal deg poly with $f_2(\alpha) = 0$.

$f_1, f_2 \in F[x]$. $f_1(\alpha) = f_2(\alpha) = 0$ so

$f_2(x) \mid f_1(x)$

But f_1 splits in K. so f_2 splits in K. $\square$.

Therefore $[K : F] = |\mathrm{Aut}(K/F)|$

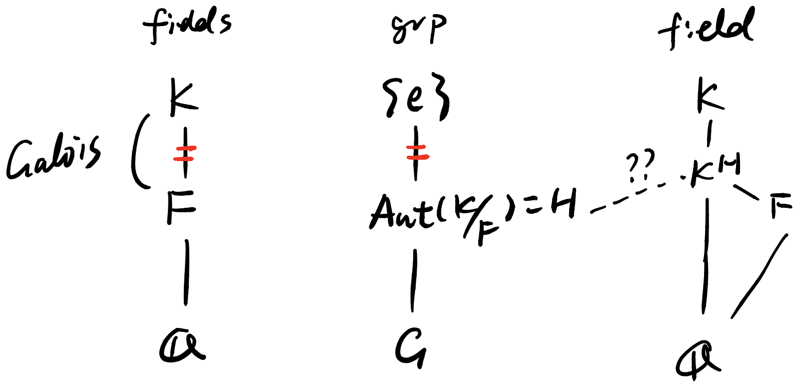
<u>Claim 2</u> $H \subseteq \mathrm{Aut}(K/K^H)$, $F \subseteq K^{\mathrm{Aut}(K/F)}$. Obvious.

$$\begin{tikzcd}
\{e\} \arrow[d, dash] & K \arrow[d, dash] \\
H \arrow[r, "\pi_2"] \arrow[d, dash] & K^H \arrow[d, dash] \\
G & \mathbb{Q}
\end{tikzcd}
\qquad
\begin{tikzcd}
K \arrow[d, dash] & \{e\} \arrow[d, dash] \\
F \arrow[r, "\pi_1"] \arrow[d, dash] & \mathrm{Aut}(K/F) \arrow[d, dash] \\
\mathbb{Q} & G
\end{tikzcd}$$

Claim 3: Given a subfield $\mathbb{Q} \subseteq F \subseteq K$. denote

$H = \mathrm{Aut}(K/F)$. and $\tilde{F} = K^H$, then. $F = \tilde{F}$.

(This is to show $\pi_2 \circ \pi_1 = id$)



Claim 1

$[K:F] \geq [K:K^H] = |\mathrm{Aut}(K/K^H)| \geq |H| = [K:F]$

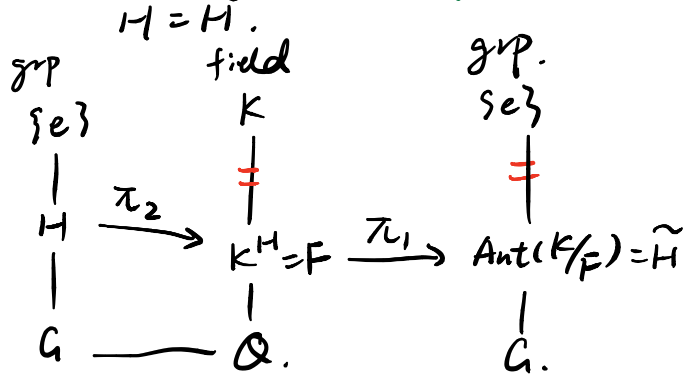
Claim 2 Claim 1 Claim 2

So $K^H = F$ □.

Claim 4: Given H denote $F = K^H$ and $\tilde{H} = \mathrm{Aut}(K/F)$. then

(This gives $\pi_1 \circ \pi_2 = id$)

$H = \tilde{H}$.



Suppose. $|H| < |\tilde{H}|$. then.

say $K = K^H[\alpha]$

then $f(x) = \prod_{\sigma \in H} (x - \sigma(\alpha))$.

so all coefficients will be fixed by H, so.

$f(x) \in F[x]$, then the degree of $f(x)$ is $|H|$.

but the deg of $[K:K^H] = |\tilde{H}| > |H|$.

So contradiction. So $|H| = |\tilde{H}|$ and $H = \tilde{H}$.

□.

3). "$\Rightarrow$" If $F/\mathbb{Q}$ is Galois, then.

define: $f: \quad \mathrm{Aut}(K/\mathbb{Q}) \longrightarrow \mathrm{Aut}(F/\mathbb{Q})$

$$\sigma: K \to K \qquad\qquad \sigma|_F : F \to F$$

$\sigma|_F : F \to F$ goes back to F since F is Galois.

then. by Fundamental Homomorphism Thm for Grps.

$$\mathrm{Aut}(K/\mathbb{Q}) / \mathrm{Aut}(K/F) \simeq . \ \mathrm{Im}(f).$$

Compare. size, $\Rightarrow$ f is surjective.

$$\left| \mathrm{Aut}(K/\mathbb{Q}) / \mathrm{Aut}(K/F) \right| = [F:\mathbb{Q}] = |\mathrm{Im}(f)| \leq \mathrm{Aut}(F/\mathbb{Q})$$

$\Rightarrow$ $\mathrm{Im}(f) = \mathrm{Aut}(F/\mathbb{Q})$,

$\mathrm{Aut}(K/F)$ is normal since it is $\ker(f)$.

"$\Leftarrow$". If $N \triangleleft \mathrm{Aut}(K/\mathbb{Q})$. then.

$$\begin{array}{c} K \\ | \\ K^H \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} K \\ | \\ \sigma(K^H) = K^{\sigma H \sigma^{-1}} \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{l} H' = \sigma H \sigma^{-1} \\ \text{then } K^{H'} = \sigma(K^H) \end{array}$$

$\swarrow$ For general sub grp.

So if N is normal. $\sigma(K^N) = K^N$ $\swarrow$ This guarantees that $\sigma: K^N \to K^N$

so there again we can construct

$f: \quad \mathrm{Aut}(K/\mathbb{Q}) \longrightarrow \mathrm{Aut}(F/\mathbb{Q}) \quad F := K^N$

$\ker(f) = \mathrm{Aut}(K/F)$

So by FHT for grp

$$\mathrm{Aut}(K/\mathbb{Q}) \big/ \mathrm{Aut}(K/F) \simeq \mathrm{Im}(f)$$

Compae size we get $\mathrm{Im}\, f = \mathrm{Aut}(F/\mathbb{Q})$.

$|\mathrm{Aut}(F/\mathbb{Q})| = [F:\mathbb{Q}] \Rightarrow F$ is Galois.

D.