May 19

<u>Fund thm of Galois theory</u> Let $K \subset L$ Galois field ext.

There is a bijective correspondence

$$\left\{ \begin{array}{c} \text{intermediate field ext} \\ K \subset E \subset L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ H < \mathrm{Gal}(L/K) \end{array} \right\}$$

$$E \longmapsto \mathrm{Gal}(L/E)$$

$$L^H \longleftarrow H$$

fixed field $L^H = \{ \alpha \in L \mid \forall \sigma \in H \ \sigma(\alpha) = \alpha \}$

Recall Last time

Prop 1 Let $K \subset L$ be a finite field extension. Let $H \subset \mathrm{Gal}(L/K)$

Then (a) $L^H \subset L$ Galois

(b) $\mathrm{Gal}(L/L^H) = H$

(c) $|H| = |L : L^H|$

Cor: Get one of the directions

$$H \longmapsto L^H \longmapsto \mathrm{Gal}(L/L^H) = H$$

Prop 2 Let $K \subset L$ Galois field ext.

Given $K \subset E \subset L$,

$$E = L^{\mathrm{Gal}(L/E)}$$

Pf: $E \subset L^{\mathrm{Gal}(L/E)}$ by defns

To show, $L^{\mathrm{Gal}(L/E)} \subset E$, we will show $\alpha \notin E \Rightarrow \alpha \notin L^{\mathrm{Gal}(L/E)}$

We have $\alpha \in L$ algebraic $/E$

Let $p(x) \in E[x]$ min poly of α/E.

Since $\alpha \notin E$, $\deg p \geq 2$

Also, L Galois $/E$

$\Rightarrow$ $p(x)$ is separable & all other roots are also in L.

$\Rightarrow$ $\exists\, \alpha' \in L$ another root $(\alpha \neq \alpha')$

We've shown that

$\Rightarrow$ $\exists\, \sigma : L \to L$ aut $/E$ such that $\sigma(\alpha) = \alpha'$

$\Rightarrow$ $\alpha \in L$ not fixed by σ

$\Rightarrow$ $\alpha \notin L^{\mathrm{Gal}(L/E)}$

Cor Let $K \subset L$ finite field ext

$K \subset L$ Galois $\overset{①}{\Longleftrightarrow}$ $K = L^{Gal(L/K)}$

$\overset{②}{\Longleftrightarrow}$ $|L:K| = |Gal(L/K)|$

Pf:

For ①, $\Rightarrow$ follows from Prop 2 applied w/ $E = K$

$\Leftarrow$ follows from Prop 1

(indeed, Prop 1 says $K = L^{Gal(L/K)} \subset L$ Galois)

For ②,

$$K \subset L^{Gal(L/K)} \subset L$$

$$|L:K| = |L : L^{Gal(L/K)}|\,|L^{Gal(L/K)} : K|$$

In particular

$$|L:K| = |L : L^{Gal(L/K)}| \Longleftrightarrow L^{Gal(L/K)} = K$$

$$K = L^{Gal(L/K)} \Longleftrightarrow |L:K| = |L : L^{Gal(L/K)}| \overset{\text{Prop 1}}{=} |Gal(L/K)|$$

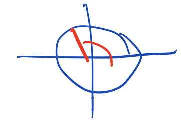
Ex: $f(x) = x^3 - 5$

$\mathbb{Q} \subset L$ splitting field.

Roots of $f(x)$ are ① $\sqrt[3]{5}$, ② $\sqrt[3]{5}\,\omega$, ③ $\sqrt[3]{5}\,\omega^2$ where

$$\boxed{\omega = e^{2\pi i/3} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2} i}$$

$$\sqrt{-3} \mapsto -\sqrt{-3}$$



$\rightsquigarrow L = \mathbb{Q}(\sqrt[3]{5}, \omega)$

$\rightsquigarrow |L : \mathbb{Q}| = 6$

Know: B/c $\mathbb{Q} \subset L$ Galois

$\Longrightarrow |Gal(L/\mathbb{Q})| = |L:\mathbb{Q}| = 6$

Know $Gal(L/\mathbb{Q}) \subseteq S_3$

$\Longrightarrow Gal(L/\mathbb{Q}) = S_3$

Correspondence

$$\{\mathbb{Q} \subset E \subset \underbrace{\mathbb{Q}(\sqrt[3]{5}, \omega)}_{=L}\} \longleftarrow \{\text{subgroups } H \subset S_3\}$$

$$L^H \longleftarrow H$$
$$L \longleftarrow 1$$
$$\mathbb{Q} \longleftarrow S_3$$

$$\begin{tikzcd}
 & & \mathbb{Q}(\sqrt[3]{5}, \omega) \arrow[dll, dash, "2"'] \arrow[dl, dash, "2"] \arrow[d, dash, "2"] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\sqrt[3]{5}\,\omega^2) \arrow[drr, dash, "3"'] & \mathbb{Q}(\sqrt[3]{5}\,\omega) \arrow[dr, dash, "3"] & \mathbb{Q}(\sqrt[3]{5}) \arrow[d, dash, "3"] & \mathbb{Q}(\omega) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & 1 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & 1 \\
\langle (1\,2) \rangle \arrow[drr, dash] & \langle (1\,3) \rangle \arrow[dr, dash] & \langle (2\,3) \rangle \arrow[d, dash] & & 2 \\
 & & & \langle (1\,2\,3) \rangle \arrow[dl, dash] & 3 \\
 & & S_3 & & 6
\end{tikzcd}$$

element $\sigma \in Gal(L/\mathbb{Q})$

$1 \overset{\sigma}{\longleftrightarrow} 2$

$3 \overset{\sigma}{\longleftrightarrow} 3$

Ques: Which element

$\sigma \in \mathrm{Gal}(L/K)$ (corresponding to $(1\,2\,3)$)

such that

$$\sqrt[3]{5} \overset{\sigma}{\longmapsto} \sqrt[3]{5}\,\omega \overset{\sigma}{\longmapsto} \sqrt[3]{5}\,\omega^2 \overset{\sigma}{\longmapsto} \sqrt[3]{5}$$