May 21

- $\mathbb{F}_p(x^p) \subset \mathbb{F}_p(x)$ finite & normal but it is not separable
- every ext. of finite fields is separable.
- extension of finite fields $\neq$ finite extension of fields

Finite field $= \mathbb{F}_{p^n}$

$K \subset L$ finite ext. $\Leftrightarrow$ $|L:K|$ finite

Reminder: The index of a subgp $H \leq G$

is

$$|G:H| = \# G/H$$
$$= |G|/|H|$$

Recall: $H \trianglelefteq G$ normal $\Leftrightarrow$ $\forall g \in G$ and $h \in H$ $ghg^{-1} \in H$

Property: $H \trianglelefteq G$ $\Leftrightarrow$ G/H is a group w/ property $G \to G/H$ group hom

Fund Thm of Galois Theory

Let $K \subset L$ be a Galois field ext.

① There is a bijective correspondence

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

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

$$L^H \longleftarrow\!\shortmid \; H$$

② $|L:E| = \#\mathrm{Gal}(L/E)$ and $|E:K| = |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)|$

In particular, $|L:K| = \#\mathrm{Gal}(L/K)$

③ $K \subset E$ normal $\Longleftrightarrow$ $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/K)$ normal subgp.

In this case, $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K) / \mathrm{Gal}(L/E)$

$$\begin{tikzcd} K \arrow[r, "?"] \arrow[rr, bend left, "\mathrm{Gal}"] & E \arrow[r, "\mathrm{Gal}"'] & L \end{tikzcd}$$

We've shown ① and ②.

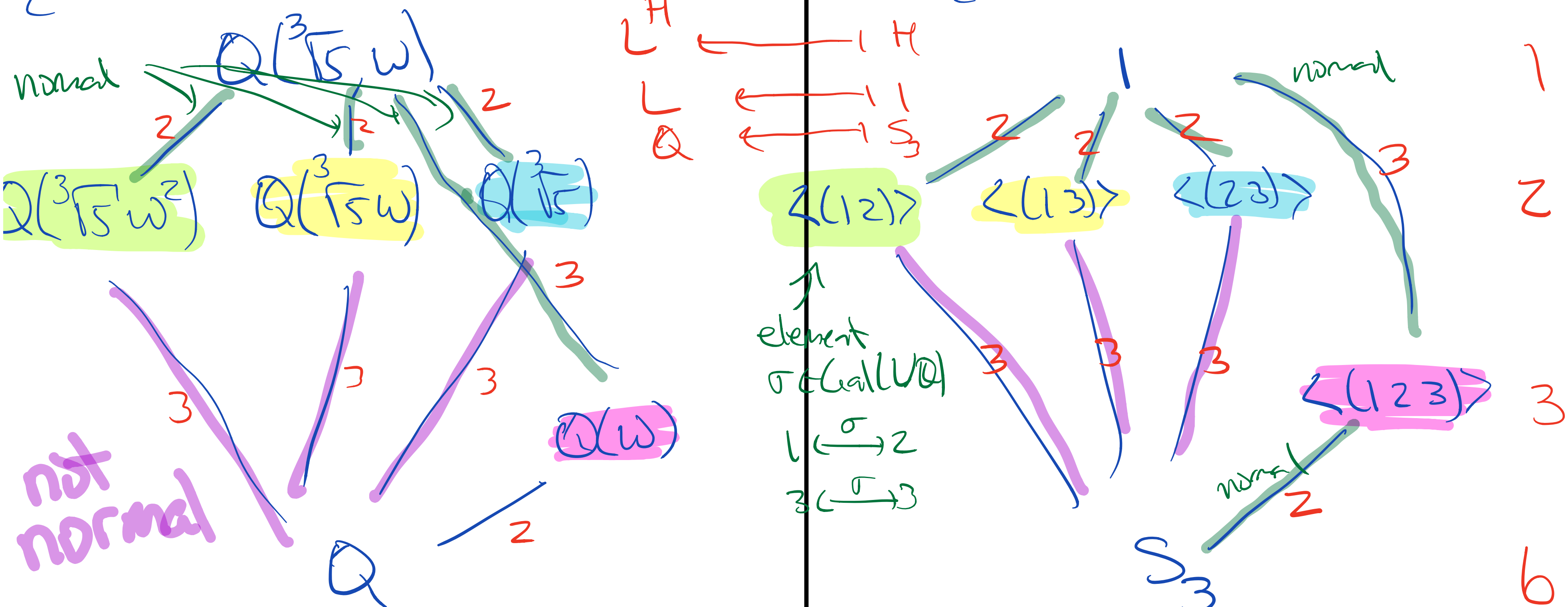
<u>Rmk</u>: Also know: $K \subset L$ Galois $\Longrightarrow$ $E \subset L$ Galois

Example from last time: L splitting of $x^3 - 5 \in \mathbb{Q}[x]$

$\omega = e^{2\pi i/3}$ $\Rightarrow$ $\mathrm{Gal}(L/\mathbb{Q}) = S_3$

Correspondence

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



Ques: For which $\mathbb{Q} \subset E \subset L$ is $\mathbb{Q} \subset E$ normal?

Ques: For which $H \subset S_3$ is $H \trianglelefteq S_3$ normal?

$$(1\,2\,3)(1\,2)(1\,2\,3)^{-1} = (2\,3)$$

Goal: Given $K \subset E \subset L$,

$K \subset E$ normal $\Leftrightarrow$ $Gal(L/E) \subseteq Gal(L/K)$ normal

---

$(\Leftarrow)$ Assume $Gal(L/E)$ normal

Let $\alpha \in E$ and $p(x) \in K[x]$ min poly

Need to show: $p(x)$ splits $/E$

Let $\beta \in L$ be another root

(Know $\beta \in L$ b/c L/K normal)

i.e. $p(x)$ splits $/L$

Need to show: $\beta \in E$

Because $E = L^{Gal(L/E)}$ it

suffices show for all $\tau \in Gal(L/E)$

that $\tau(\beta) = \beta$.

Also know b/c α, β roots of p

$\exists \sigma \in Gal(L/K)$ s.t. $\sigma(\alpha) = \beta$

$Gal(L/E)$ normal $\Rightarrow$

$\tau' = \sigma^{-1} \tau \sigma \in Gal(L/E)$

i.e. $\sigma \tau' = \tau \sigma$

Apply $\alpha \in E$

$$\underset{\shortparallel}{\tau\sigma}(\alpha) = \tau(\beta)$$

$$\sigma\tau'(\alpha) = \sigma(\alpha) = \beta$$

$\Rightarrow \forall \tau \in Gal(L/E) \quad \tau(\beta) = \beta$

$\Rightarrow \beta \in L^{Gal(L/E)} = E$

$\Rightarrow \beta \in E$ ✓

Goal: Given $K \subset E \subset L$,

$K \subset E$ normal $\Leftrightarrow$ $Gal(L/E) \subseteq Gal(L/K)$ normal

($\Rightarrow$) Assume $K \subset E$ normal

We will construct a surjective group hom

$\psi : Gal(L/K) \to Gal(E/K)$

such that $Ker(\psi) = Gal(L/E)$

In particular, this shows

- $Gal(L/E)$ normal
- $Gal(L/K)/Gal(L/E) \cong Gal(E/K)$

Let $\sigma \in Gal(L/K)$

Claim: $\sigma(E) \subseteq E$

i.e. $\forall \alpha \in E$ $\sigma(\alpha) \in E$

Pf of claim: Let $\alpha \in E$

Let $p(x) \in K[x]$ be min poly

Know $p(x)$ splits / E.

Since $\sigma(\alpha)$ is a root of p

$\Rightarrow \sigma(\alpha) \in E$

Therefore, we can restrict σ to E

$\rightsquigarrow \sigma|_E : E \to E$ auto / K

$\alpha \mapsto \sigma(\alpha)$

Define $\psi(\sigma) = \sigma|_E$

Clearly, $Ker(\psi) = Gal(L/E)$ ✓