Lecture 21: Galois groups of splitting fields

Last time:

K/F – field extension

$$\mathrm{Aut}(K/F) = \left\{ \begin{array}{l} \text{automorphisms} \\ \sigma : K \xrightarrow[\cong]{} K \text{ where } \sigma(\alpha) = \alpha \ \forall \alpha \in F \end{array} \right\}$$

Suppose $\alpha \in K$ is a root of $f(x) \in F[x]$.
Then $\forall \sigma \in \mathrm{Aut}(K/F)$, the elt $\sigma(\alpha)$ is also a root.

Thm: Suppose K is the splitting field of $f(x) \in F[x]$
Then $|\mathrm{Aut}(K/F)| \leq [K:F]$ with equality
when f is separable.

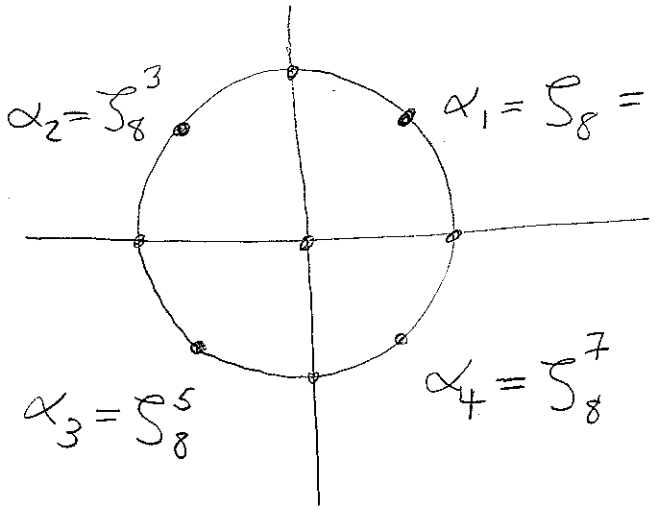
Note: Suppose f has roots $\alpha_1, \ldots, \alpha_n$.

Get a homomorphism

$$\rho : \mathrm{Aut}(K/F) \longrightarrow S_n$$
$$\sigma \longmapsto \bar{\sigma}$$

where $\bar{\sigma}(i) = j$ if
$\sigma(\alpha_i) = \alpha_j$

Ex: $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$ = splitting field of $x^4 + 1 = \Phi_8(x)$



$\sigma \in Aut(K/\mathbb{Q})$

$\sigma(\sqrt{2}) = -\sqrt{2}$

$\sigma(i) = i$

Do $\sigma(\alpha_1) = \alpha_3 \quad \sigma(\alpha_3) = \alpha_1$

$\sigma(\alpha_2) = \alpha_4 \quad \sigma(\alpha_4) = \alpha_4$

Thus

$$\rho(\sigma) = (13)(24)$$

This is where perm groups came from!

Dim. if $\tau: \begin{matrix} \sqrt{2} \to \sqrt{2} \\ i \to -i \end{matrix}$, then $\rho(\tau) = (14)(23)$

and $\rho(\tau\sigma) = \rho(\tau)\rho(\sigma) = (14)(23)(13)(24)$

$= (12)(34)$

Observation: ρ is 1-1 since $K = F(\alpha_1, \dots, \alpha_n)$

↙ du part. this is finite.

Point: Do $|Aut(K/F)| \leq |S_n| = n! \leq (\deg f)!$

which is similar to $[K:F] \leq (\deg f)!$

Proof by Example: $f(x) = x^3 - 2$ in $\mathbb{Q}[x]$.

$K = \mathbb{Q}(\sqrt[3]{2}, \underbrace{\zeta_3 \sqrt[3]{2}}_{\beta})$ $\quad (x - \sqrt[3]{2})(x - \zeta_3 \sqrt[3]{2})(x - \underbrace{\zeta_3^2 \sqrt[3]{2}}_{\gamma})$

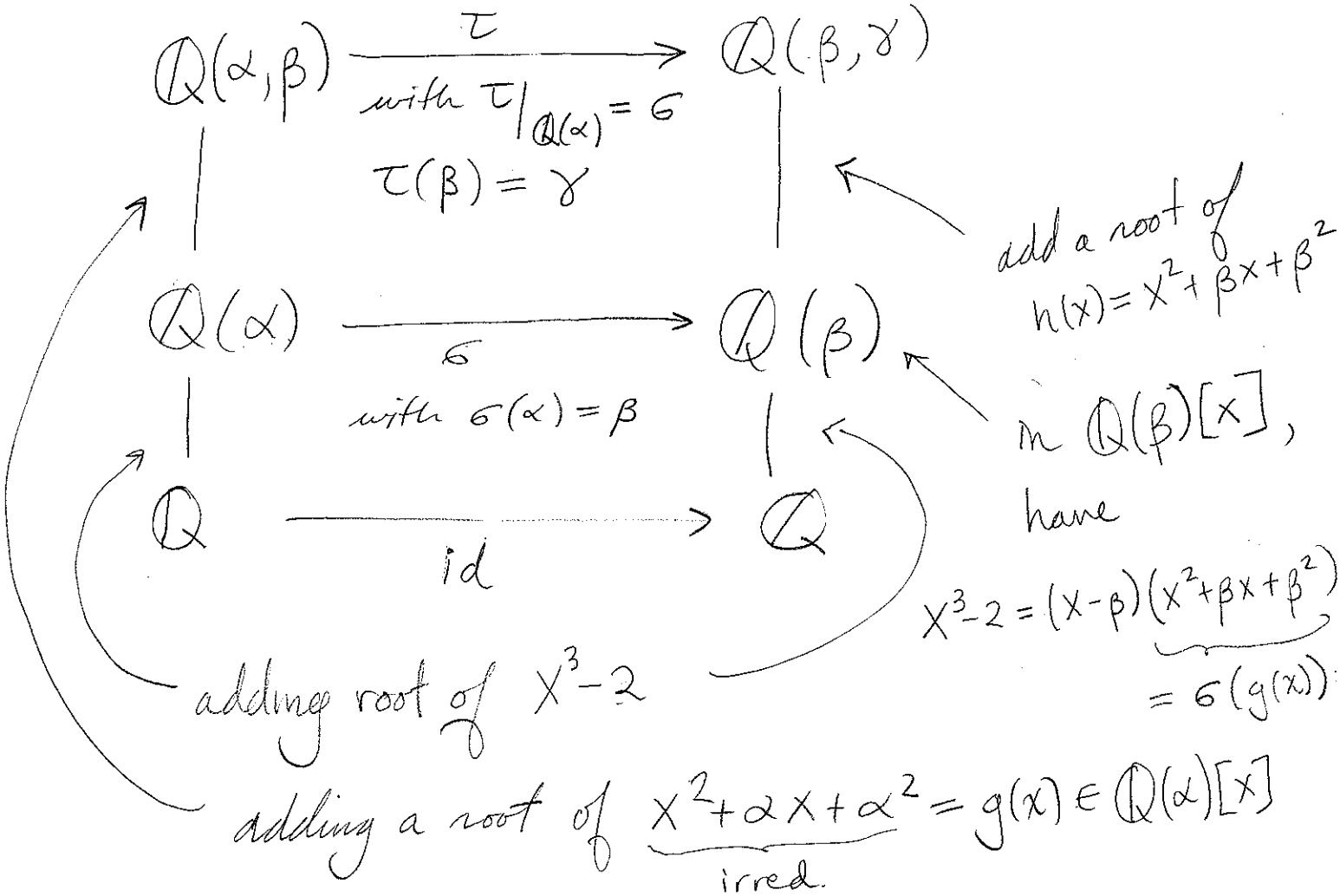
$|$

$L = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha})$ $\quad (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}\, x + (\sqrt[3]{2})^2)$

$|$

$\mathbb{Q}$ $\quad x^3 - 2$

Build $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ in two steps:



How many such τ can we construct?

(# choices at 1st stage)(# choices at 2nd stage) $= 3 \cdot 2$

$=$ (# of roots of $f(x)$)(# of roots of $g(x)$)

$=$ (deg f) (deg g) $= [\mathbb{Q}(\alpha):\mathbb{Q}][K:\mathbb{Q}(\alpha)] = [K:\mathbb{Q}]$
$= 6$

↑ as f is separable

In general, just have more stages...

See the text for a more abstract proof. ▨

<u>Def</u>: K/F a finite extension. K is <u>Galois</u> over F if $|\mathrm{Aut}(K/F)| = [K:F]$. If so, we denote $\mathrm{Aut}(K/F)$ by $\mathrm{Gal}(K/F)$ (the <u>Galois</u> group)

<u>Ex</u>: K the splitting field of a separable polynomial in $F[x]$.

Last time, talked about the connection between $H \leq Aut(K)$ and

$$K_H = \{\alpha \in K \mid h(\alpha) = \alpha \ \forall h \in H\}$$

Key: $[K : K_H] = |H|$.

Ex: $K = \mathbb{Q}(\sqrt[3]{2}, \zeta = \zeta_3)$ ① $\alpha = \sqrt[3]{2}$, ② $\beta = \zeta\alpha$, ③ $\gamma = \zeta^2\alpha$

$\sigma \in Aut(K)$ $\sigma(\alpha) = \beta$ $\sigma(\beta) = \gamma$ $\sigma(\gamma) = \alpha$

(so $\rho(\sigma) = (123)$)

$H = \langle\sigma\rangle$ has order 3. What is K_H?

A: $\mathbb{Q}(\zeta)$, and $[K : \mathbb{Q}(\zeta)] = \dfrac{[K : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} = 3$.

Why?

$K = \mathbb{Q}(\zeta)(\alpha)$ $(x-\alpha)(x-\beta)(x-\gamma)$

$(x-\zeta)(x-\zeta^2)$ $\mathbb{Q}(\zeta)$ $x^3 - 2$

$x^2 + x + 1$ $\mathbb{Q}$ $x^3 - 2$