Lecture 35: Galois groups of splitting fields

Last time: K/F field extension

$$\mathrm{Aut}(K/F) = \left\{ \begin{array}{l} \text{automorphisms } \sigma : K \to K \\ \text{with } \sigma|_F = \mathrm{id}_F \end{array} \right\}$$

If $\alpha \in K$ is a root of $f \in F[x]$, then $\sigma(\alpha)$ is also a root of f for all $\sigma \in \mathrm{Aut}(K/F)$.

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

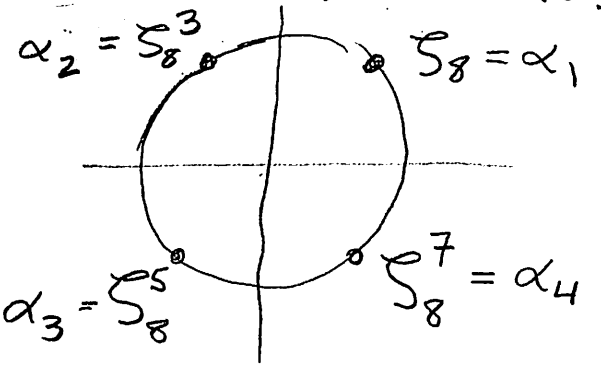
Note: Suppose f has roots $\alpha_1, \ldots, \alpha_n$ in K.

Get a homom $\rho : \mathrm{Aut}(K/F) \to S_n$ where

$\sigma \longmapsto \overline{\sigma}$

$\overline{\sigma}(i) = j \iff \sigma(\alpha_i) = \alpha_j$.

Ex: $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8 = \frac{1}{\sqrt{2}}(1+i))$ [since $\zeta_8^2 = i$ and $\zeta_8 + \zeta_8^7 = \sqrt{2}$]



$\| \; K$

K is a splitting field of $\Phi_8 = x^4 + 1$.

Take $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ with $\sigma(\sqrt{2}) = -\sqrt{2}$
$\sigma(i) = i$

So $\sigma(\alpha_1) = \alpha_3$ $\quad \sigma(\alpha_3) = \alpha_1$
$\sigma(\alpha_2) = \alpha_4$ $\quad \sigma(\alpha_4) = \alpha_2$

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

This is where permutation groups first appeared!

If τ: $\begin{matrix} \sqrt{2} \longmapsto \sqrt{2} \\ i \longmapsto -i \end{matrix}$ then $\rho(\tau) = (14)(23)$

and $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau) = (13)(24)(14)(23) = (12)(34)$

Prop: ρ is 1-1. Pf: $K = F(\alpha_1, \ldots, \alpha_n)$.

Cor: $|\mathrm{Aut}(K/F)| \leq |S_n| = n! \leq (\deg f)!$

Compare with $[K:F] \leq (\deg f)!$

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

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

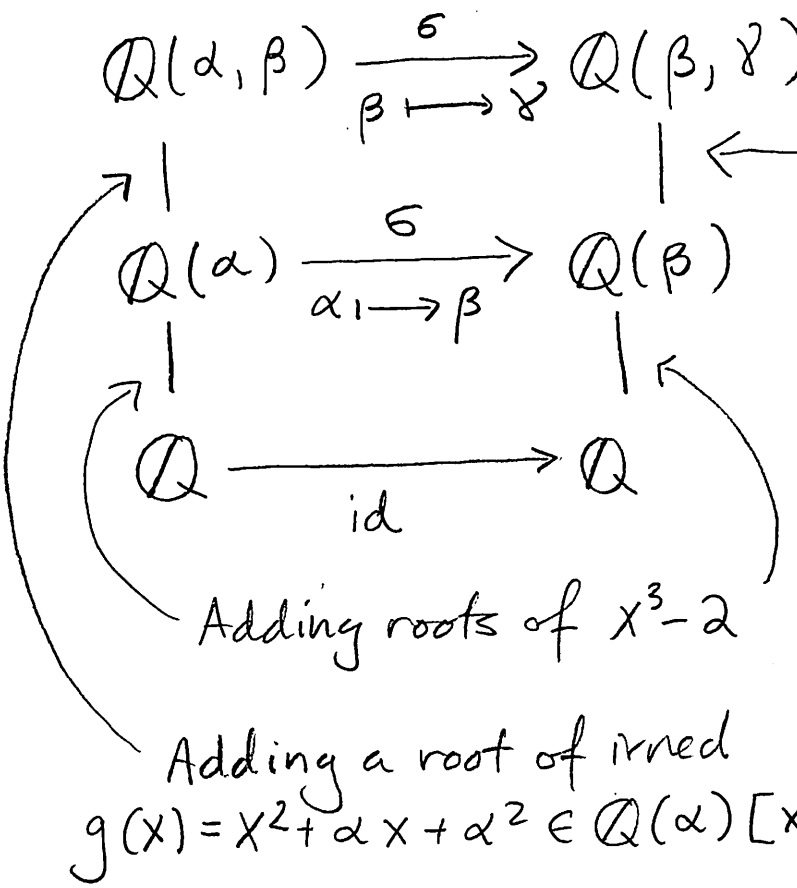
$|$

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

$|$

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

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



Adding a root of $\sigma(g(x)) = x^2+\beta x+\beta^2$ in $\mathbb{Q}(\beta)[x]$ and note $x^3-2 = (x-\beta)\sigma(g(x))$.

How many such σ can we construct?

(# of choices at 1st stage) · (# of choices at 2nd stage)

$= 3 \cdot 2 = (\#$ of roots of $f) \cdot (\#$ of roots of $g)$

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

$= [K:\mathbb{Q}] = 6.$

↑ as f is separable

In general, have more stages, but that's it.

See §14.1 of [DF] for details. ▨

Def: K/F a finite extension. Say K is **Galois** over F if $|\mathrm{Aut}(K/F)| = [K:F]$. When K/F is Galois, we denote $\mathrm{Aut}(K/F)$ by $\mathrm{Gal}(K/F)$ and call it the **Galois group**.

Ex: The splitting field of a separable poly in $F[x]$.

Non Ex: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ since $|\mathrm{Aut}| = 1$.

Recall: For $H \leq \mathrm{Aut}(K)$, set $K_H = \{\alpha \in K \mid \begin{smallmatrix} h(\alpha) = \alpha \\ \text{for all } h \in H \end{smallmatrix}\}$.

Key Thm: $[K : K_H] = |H|$. [Will prove soon.]

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

Pick $\sigma \in \mathrm{Aut}(K)$ with $\sigma(\alpha) = \beta$, $\sigma(\beta) = \gamma$ and $\sigma(\gamma) = \alpha$, so $\rho(\sigma) = (1\,2\,3)$. Then $H = \langle \sigma \rangle$ has order 3.

Q: What is K_H?

A: $\mathbb{Q}(\zeta_3)$ [Will show in a moment]

Note $[K : \mathbb{Q}(\zeta_3)] = \dfrac{[K:\mathbb{Q}]}{[\mathbb{Q}(\zeta_3):\mathbb{Q}]} = 3$, matching the thm.

Reason: $\zeta := \zeta_3 = \beta/\alpha$ and so

$$\sigma(\zeta) = \frac{\sigma(\beta)}{\sigma(\alpha)} = \frac{\gamma}{\beta} = \zeta \Rightarrow \mathbb{Q}(\zeta) \subseteq K_H.$$

To see equality, note $[K : \mathbb{Q}(\zeta)] = 3$ and so the only options for K_H are $\mathbb{Q}(\zeta)$ and K itself.

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

$$3 \;|$$

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

$$2 \;|$$

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