Lecture 20: Galois groups of splitting fields

Last time: K/F field extension

$$\mathrm{Aut}(K/F) = \left\{ \begin{array}{l} \text{automorphisms } \sigma : K \to K \\ \text{where } \sigma(\alpha) = \alpha \text{ for all } \alpha \in F \end{array} \right\}$$

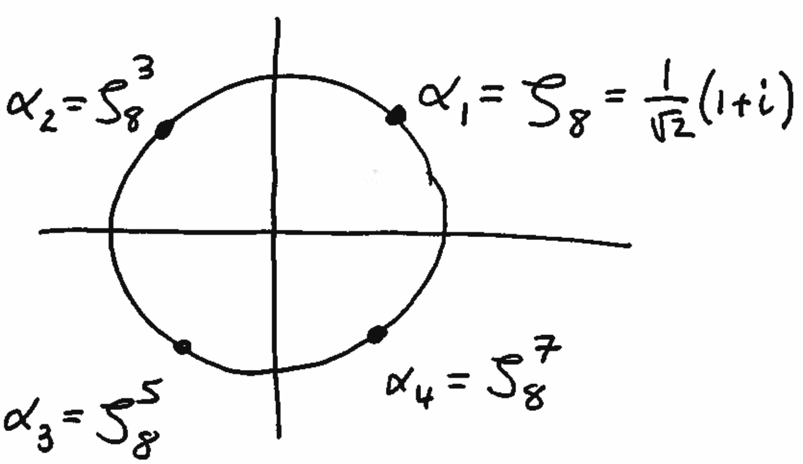
If $\alpha \in K$ is a root of $f(x) \in F[x]$, then $\sigma(\alpha)$ is also a root of f for all $\sigma \in \mathrm{Aut}(K/F)$.

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

Note: Suppose f has roots $\alpha_1, \dots, \alpha_n$ in K. Have a homomorphism

$$\rho : \mathrm{Aut}(K/F) \to S_n \qquad \text{where } \bar{\sigma}(i) = j$$
$$\sigma \longmapsto \bar{\sigma} \qquad \text{iff } \sigma(\alpha_i) = \alpha_j$$

Ex: $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8) = \text{Splitting field of } x^4+1 \,/\, \mathbb{Q} = K.$



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 $\tau : \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \end{matrix}$ then $\rho(\sigma) = (14)(23)$.

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

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

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

in particular, this is finite.

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

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

$$\begin{array}{ll}
K = \mathbb{Q}(\alpha, \underbrace{\zeta_3 \sqrt[3]{2}}_{\beta}) & (X-\alpha)(X-\beta)(X - \underbrace{\zeta_3^2 \sqrt[3]{2}}_{\gamma}) \\
\quad | & \\
L = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha}) & (X-\alpha)(X^2 + \alpha X + \alpha^2) \\
\quad | & \\
\mathbb{Q} & X^3 - 2
\end{array}$$

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

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\beta) \arrow[r, "\sigma", "\beta \mapsto \gamma"'] & \mathbb{Q}(\beta,\gamma) \\
\mathbb{Q}(\alpha) \arrow[u, dash] \arrow[r, "\sigma", "\alpha \mapsto \beta"'] & \mathbb{Q}(\beta) \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[r, "\mathrm{id}"'] & \mathbb{Q} \arrow[u, dash]
\end{tikzcd}$$

$\sigma(g(x)) = x^2 + \beta x + \beta^2$ in $\mathbb{Q}(\beta)[x]$, and note

$x^3 - 2 = (x-\beta)\,\sigma(g(x))$

Adding roots of $x^3 - 2$

Adding a root of $\underbrace{x^2 + \alpha x + \alpha^2}_{\text{irred}} = g(x) \in \mathbb{Q}(\alpha)[x]$

How many such σ can we construct?

(# of choices at 1^{st} stage)(# of choices at 2^{nd} 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, have more stages but that's it. See text for a more abstract proof. ∎

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

Key Thm (Next Lecture): $[K : K_H] = |H|$.

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

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

Q: What is K_H?

A. $\mathbb{Q}(\zeta_3)$.

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

Reason: $\zeta = \zeta_3 = \beta/\alpha$ and $\sigma(\zeta) = \dfrac{\sigma(\beta)}{\sigma(\alpha)} = \dfrac{\sigma(\gamma)}{\sigma(\beta)} = \zeta$.
so certainly $\mathbb{Q}(\zeta) \subseteq K_H$. To see equality, note $[K:\mathbb{Q}(\zeta_3)] = 3$ and so there are no options for K_H other than $\mathbb{Q}(\zeta)$ and K itself.

$$
\begin{array}{ccc}
 & \mathbb{Q}(\zeta)(\alpha) & (x-\alpha)(x-\beta)(x-\gamma) \\
 & 3 \,\big| & \\
(x-\zeta)(x-\zeta^2) & \mathbb{Q}(\zeta) & x^3-2 \\
 & 2 \,\big| & \\
x^2+x+1 & \mathbb{Q} & x^3-2
\end{array}
$$