Lecture 19: Intro to Galois Theory

An <u>automorphism</u> of a field K is a field isomorphism $\sigma: K \to K$.

Ex: $K = \mathbb{C}$, $\tau: \mathbb{C} \to \mathbb{C}$ sends $z \mapsto \bar{z}$. ($a+bi \mapsto a-bi$)

Is an auto. as is bijective and $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z} \cdot \bar{w}$.

Ex: $K = \mathbb{Q}(\sqrt{2})$ $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ for $a, b \in \mathbb{Q}$.

Can check directly that this is an isom, or appeal to $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$.

Def: $\text{Aut}(K)$ = group of automorphisms of K (op is composition)

Ex: $\text{Aut}(K = \mathbb{Q}(\sqrt{2})) = \{ \text{Id}_K, \sigma \}$

Pf. Let $\tau \in \text{Aut}(K)$

① $\tau(1) = 1 \Rightarrow \tau|_{\mathbb{Z}} = \text{id}_{\mathbb{Z}} \Rightarrow \tau|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$

$\Rightarrow \tau$ is a $\mathbb{Q}$-linear transformation

② $\tau(\sqrt{2}) = \pm\sqrt{2}$ since $(\tau(\sqrt{2}))^2 = \tau(\sqrt{2}^2) = \tau(2) = 2$

$\Rightarrow \tau(\sqrt{2})$ is a root of $x^2 - 2$.

Now use that a linear trans. is determined by what it does to the basis $\{1, \sqrt{2}\}$. $\square$

[$\mathrm{Aut}(\mathbb{C})$ is just <u>huge</u>, in particular uncountable.]

For an extension K/F, let $\mathrm{Aut}(K/F)$ is the subgp of $\sigma \in \mathrm{Aut}(K)$ which fix every $a \in F$, i.e. $\sigma(a) = a$ for all $a \in F$.

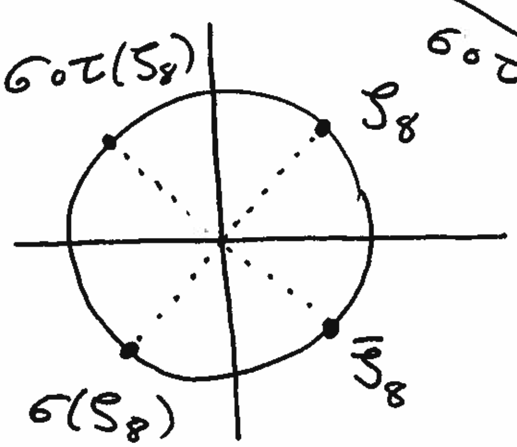
<u>Ex</u>: $K = \mathbb{Q}(\sqrt{2}, i)$ $\quad \mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q})$
$$= \{1, \sigma, \tau, \sigma \circ \tau\}$$

where $\sigma : \begin{array}{l} \sqrt{2} \to -\sqrt{2} \\ i \to i \end{array}$ and $\tau : \begin{array}{l} \sqrt{2} \to \sqrt{2} \\ i \to -i \end{array}$

$\mathrm{Aut}(K/\mathbb{Q}(\sqrt{2})) = \langle \tau \rangle \qquad \mathrm{Aut}(K/\mathbb{Q}(i)) = \langle \sigma \rangle$

$$\zeta_8 = \frac{1}{\sqrt{2}}(1+i) \xrightarrow{\sigma} -\zeta_8 = \zeta_8^5$$
$$\zeta_8 \xrightarrow{\tau} \bar{\zeta}_8 = \zeta_8^7$$
$$\zeta_8 \xrightarrow{\sigma \circ \tau} \zeta_8^3$$

These are the roots of $\Phi_8 = X^4 + 1$



<u>Thm</u>: K/F algebraic, $\sigma \in \mathrm{Aut}(K/F)$.
If $\alpha \in K$, then $\sigma(\alpha)$ is also a root of $m_{\alpha,F}(x)$.

<u>Pf</u>: Set $f(x) = m_{\alpha,F}(x) \in F[x]$. Now

$$
\begin{aligned}
f(\sigma(\alpha)) &= a_n(\sigma(\alpha))^n + \cdots + a_1(\sigma(\alpha)) + a_0 \\
&= \sigma(a_n)(\sigma(\alpha))^n + \cdots \sigma(a_1)(\sigma(\alpha)) + \sigma(a_0) \\
&= \sigma(f(\alpha)) = \sigma(0) = 0.
\end{aligned}
$$

$\square$

[So $\mathrm{Aut}(K/F)$ permutes the roots of each $f \in F[x]$.]

<u>Ex</u>: $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}\}$

<u>Reason</u>: $x^3 - 2$ has only one root in $\mathbb{Q}(\sqrt[3]{2})$,
so any automorphism σ must fix $\sqrt[3]{2}$ and hence
be the identity.

<u>Key Construction</u>: $H \leq \mathrm{Aut}(K)$ a subgp. Define

$$K_H = \{\alpha \in K \mid \text{Every elt of } H \text{ fixes } \alpha\}$$

Note K_H is a subfield since if $a, b \in K_H$

then $\forall \sigma \in H$ we have $\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$

and $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = a \cdot b$

and $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$

and so $a+b$, $a \cdot b$, and $1/a$ are in K_H.

<u>Ex</u>: $K = \mathbb{Q}(\sqrt{2}, i)$ $\quad \mathrm{Aut}(K) = \{1, \sigma, \tau, \sigma\tau\}$

$H = \langle \sigma \rangle$ has $K_H = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid b = d = 0\}$

$= \mathbb{Q}(i)$

$H = \langle \tau \rangle$ has $K_H = \mathbb{Q}(\sqrt{2})$

$H = \langle \sigma\tau \rangle$ has $K_H = \mathbb{Q}(\sqrt{-2} = \sqrt{2}i)$

Galois Theory By Example.

Subgroups | **Subfields:**

$$\begin{tikzcd}[column sep=small]
 & \mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \sigma\tau \rangle \arrow[dl, dash] \\
 & \langle 1 \rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}i) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

It's clear that these are all the subgps of $\mathrm{Aut}(K/\mathbb{Q})$. It turns out (Fund. Thm. of Galois Theory.) that these are all the subfields of $\mathbb{Q}(\sqrt{2}, i)$.

In general, the two sides correspond when $\mathrm{Aut}(K/F)$ is "large enough."