Lecture 20: Galois Theory I.

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

<u>Ex</u>: $K = \mathbb{Q}(\sqrt{2})$ $\quad \sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ for $a, b \in \mathbb{Q}$

Can see this is an isom directly, or appeal to

$$\mathbb{Q}[X]/(X^2-2) \cong \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2}).$$

<u>Def</u>: $\mathrm{Aut}(K)$ = group of aut. of K (op is composition)

<u>Ex</u>. $K = \mathbb{Q}(\sqrt{2})$. <u>Claim</u>: $\mathrm{Aut}(K) = \{1_K, \sigma\}$

<u>Pf</u>: Let $\tau \in \mathrm{Aut}(K)$.

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

$\Rightarrow \tau$ 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 $X^2 - 2 = 0$. $\blacksquare$

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

as before, if $\eta \in \mathrm{Aut}(K)$, then $\eta(i)^2 = \eta(i^2) = \eta(-1) = -1$.

<u>Ex</u>: $K = \mathbb{Q}(\sqrt{2}, i)$

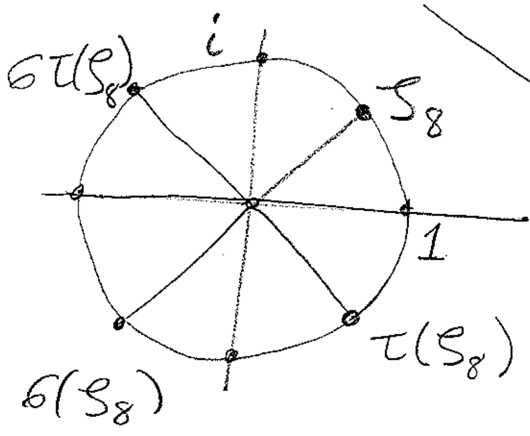
$$\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$$

where

$$\sigma: \begin{array}{l} \sqrt{2} \longrightarrow -\sqrt{2} \\ i \longrightarrow i \end{array} \qquad \tau: \begin{array}{l} \sqrt{2} \longrightarrow \sqrt{2} \\ i \longrightarrow -i \end{array}$$

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

$$\zeta_8 = \tfrac{1}{2}\sqrt{2} + \tfrac{1}{2}\sqrt{2}\, i \quad \begin{array}{l} \xrightarrow{\sigma} -\zeta_8 \\ \xrightarrow{\tau} \overline{\zeta_8} \\ \xrightarrow{\sigma\tau} \zeta_8^2 \end{array} \quad \Bigg\} \text{ These are all 4 roots of } \Phi_8 = X^4 + 1$$



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

Proof: Set $f(x) = m_{F,\alpha}(x)$. Now

$$f(\sigma(\alpha)) = a_n(\sigma(\alpha))^n + \cdots + a_1(\sigma(\alpha)) + a_0$$

$$= \sigma(a_n)(\sigma(\alpha))^n + \cdots + \sigma(a_0)$$

$$= \sigma(f(\alpha)) = \sigma(0) = 0.$$ ▨

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

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

Reason: $x^3 - 2$ has only one root in $\mathbb{Q}(\sqrt[3]{2})$, so each σ must fix $\sqrt[3]{2}$, hence is the identity.

Key const: $H \leq \mathrm{Aut}(K)$. Consider

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

Note: K_H is a subfield, since if $a, b \in K_H$, $\sigma \in H$, then $\sigma(a+b) = \sigma(a) + \sigma(b) = a+b \Rightarrow a+b \in K_H$

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1} \Rightarrow a^{-1} \in K_H.$$

Ex: $\mathrm{Aut}(\underbrace{\mathbb{Q}(\sqrt{2}, i)}_{K}) = \{1, \sigma, \tau, \sigma\tau\}$

$H = \langle \sigma \rangle \Rightarrow K_H = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid b = d = 0\}$
$= \mathbb{Q}(i)$

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

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

Galios Theory By Example:

$[K : \mathbb{Q}] = |\mathrm{Aut}(K/\mathbb{Q})| = 4$

Subgps

$$\begin{tikzcd}[column sep=small]
 & \mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \sigma\tau \rangle \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}$$

Clearly only subgps.

Subfields

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}i) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Turns out, these are the only subfields

In general, the two sides correspond when $Aut(K/F)$ is "large enought."

Splitting fields:

Suppose K is the splitting field of $f(x) \in F[x]$.

Thm: $|Aut(K/F)| \leq [K:F]$ with equality if $f(x)$ is separable.

Key example: Suppose $K = F(\theta_1)$ for θ_1 a root of $f(x)$ which is moreover irred.

$[$E.g. $f(x) = \Phi_n(x) \in \mathbb{Q}[x]$; $K = \mathbb{Q}(\zeta_n)$ $]$

Then for each root θ_i of f have $\sigma_i \in Aut(K/F)$ with $\sigma_i(\theta_1) = \theta_i$; moreover, σ_i is unique.

So

$$|Aut(K/F)| = |\#\text{ of dist. roots of } f| \leq \deg f = [K:F]$$

Equal if f is separable.