Lecture 34: Intro to Galois Theory

§14.1-2 of [DF]

Now start to apply group theory to the study of fields...

An *automorphism* of a field K is a field isomorphism $\sigma: K \to K$.

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

This is an auto. since $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z} \cdot \bar{w}$ and is a bijection ($\tau^{-1} = \tau$).

Ex: K finite with char $= p$, then the Frobenius map $\alpha \mapsto \alpha^p$ is an auto.

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

Can check directly, or appeal to

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

$$\sqrt{2} \longleftarrow x \longmapsto \sqrt{-2}$$

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

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

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

① $\tau(1) = 1 \Rightarrow \tau|_{\mathbb{Z}} = id_{\mathbb{Z}} \Rightarrow \tau|_{\mathbb{Q}} = id_{\mathbb{Q}}$.

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

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 $\{1, \sqrt{2}\}$. ▨

[For a finite field, will see that all auto. are powers of Frobenious. In contrast, $Aut(\mathbb{C})$ is just huge, in particular uncountable.]

For an extension K/F, let $Aut(K/F)$ be the subgroup of $\sigma \in Aut(K)$ with $\sigma|_F = id_F$.

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

where $\sigma: \begin{matrix}\sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i\end{matrix}$ and $\tau: \begin{matrix}\sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i\end{matrix}$ $\quad$ 112 $\quad C_2 \times C_2$

[Reason: any $\psi \in Aut(K)$ must have $\psi(\sqrt{2}) = \pm\sqrt{2}$ and $\psi(i) = \pm i$ for reason ② above. That all four poss. are realized is on HW for this week.]

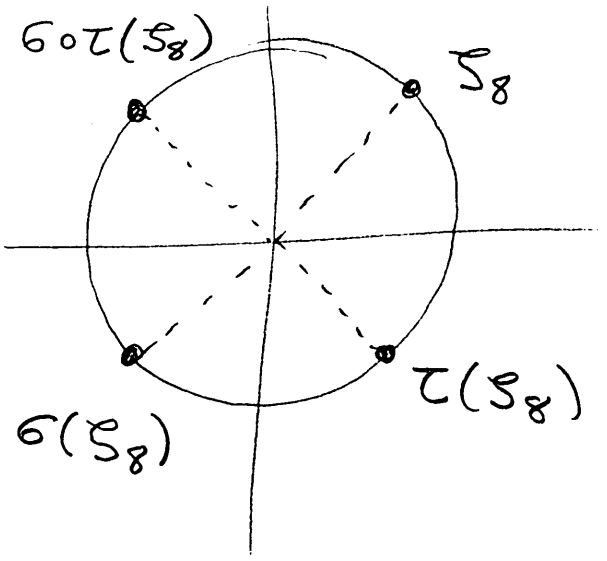
$Aut(K/\mathbb{Q}(\sqrt{2})) = \langle\tau\rangle$ $\quad Aut(K/\mathbb{Q}(i)) = \langle\sigma\rangle$

Note $\zeta_8 = \frac{1}{\sqrt{2}}(1+i) \in K$ and $\zeta_8 \xrightarrow{\sigma} -\zeta_8 = \zeta_8^5$

$\zeta_8 \xrightarrow{\tau} \overline{\zeta_8} = \zeta_8^7$

$\zeta_8 \xrightarrow{\sigma\circ\tau} \zeta_8^3$

All roots of $\Phi_8 = x^4+1$.



[Prob. skip this part of the example.]

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

Pf: $m_{\alpha,F}(\sigma(\alpha)) = \sum_{k=0}^{n} a_k (\sigma(\alpha))^k = \sum_{k=0}^{n} \sigma(a_k)\,\sigma(\alpha^k)$ (since $a_k \in F$)

$= \sigma(m_{\alpha,F}(\alpha)) = \sigma(0) = 0.$ ▨

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

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

since x^3-2 has only root in $\mathbb{Q}(\sqrt[3]{2})$, so any automorphism must fix $\sqrt[3]{2}$ and so be $id_{\mathbb{Q}(\sqrt[3]{2})}$.

Key construction: $H \leq \mathrm{Aut}(K)$ a subgroup.

Define $K_H := \{a \in K \mid \text{every elt of } H \text{ fixes } a\}$,

a subfield of K since if $a, b \in K_H$ and $\sigma \in H$

we have $\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$

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

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

$\Rightarrow a+b, ab, a^{-1}$ are all in K_H.

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

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

$= \mathbb{Q}(i)$

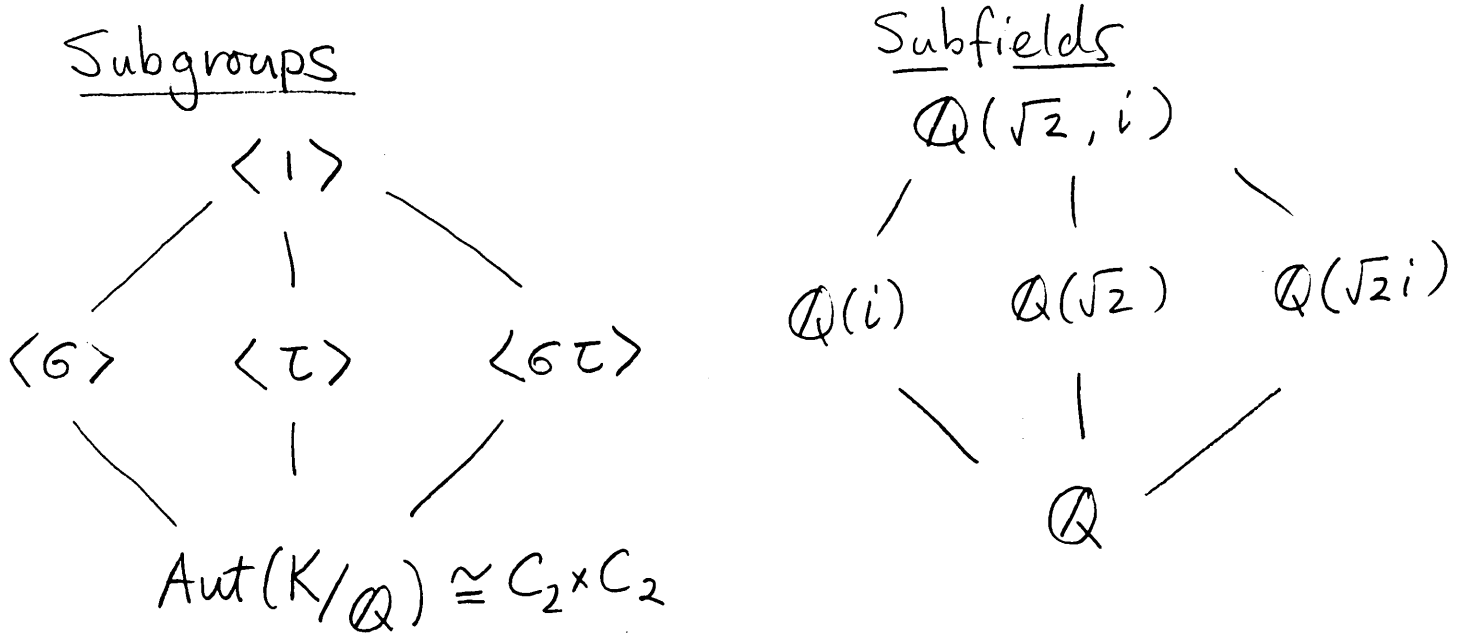
$H = \langle\tau\rangle$ has $K_{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2})$

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

$H = \mathrm{Aut}(K)$ has $K_H = \mathbb{Q}$

$H = \langle 1\rangle$ has $K_{\langle 1\rangle} = K$.

Galois Theory By Example



Know that these are all subgps of $Aut(K)$.

It turns out (Fund. Thm. of Galois Theory) that these are all subfields of $\mathbb{Q}(\sqrt{2}, i)$

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

"Secret" maps:

$$H \longmapsto K_H$$

$$Aut(K/E) \longleftarrow E \subseteq K$$