Main thm of Galois theory

Characteristic 0

$F \subset K$ finite & Galois

- $\deg(K/F) = |\mathrm{Aut}(K/F)|$

$\Updownarrow$

- K/F is a splitting field.

Set $G = \mathrm{Aut}(K/F)$

Thm: We have a bijection

$$\left\{ \begin{array}{c} \text{Fields } L \\ F \subset L \subset K \end{array} \right\} \rightleftarrows \left\{ \begin{array}{c} \text{Subgps of} \\ G \end{array} \right\}$$

given by. –

$$L \longmapsto \mathrm{Aut}(K/L) \subset G$$

$$K^H \longleftarrow H \subset G$$

$$\| $$

$$\{x \in K \mid h(x) = x \text{ for all } h \in H\}$$

Warm up:

① $L = K \longrightarrow \{id\}$ ✓

$K \longleftarrow$

② $L = F \longrightarrow G$

$K^G \longleftarrow$

$\|$ want

F

Why is $F = K^G$?

Obv : $F \subset K^G$

Have $F \subset K^G \subset K$

$$\begin{array}{ccc} \deg(K/K^G) & \text{vs} & \mathrm{Aut}(K/K^G) \\ \rotatebox{90}{$\leq$} & \geq & \| \\ \deg(K/F) & & G \\ \| & & \\ |G| & & \end{array}$$

So $\deg(K^G/F) = 1$

i.e. $F = K^G$.

First half of proof.

$$L \longrightarrow H = \mathrm{Aut}(K/L)$$

$$K^H \longleftarrow$$

Claim: $L = K^H$.

Obs: $L \subset K$ is also Galois.

Pf: Know $F \subset K$ Galois.

so $F \subset K$ is splitting field of $f(x) \in F[x]$

$L \subset K$ is the splitting field of $f(x) \in L[x]$

$\Rightarrow$ $L \subset K$ is also Galois.

Pf of Claim:

By definition, $L \subset K^H$

Want $L = K^H$.

$$L \subset K^H \subset K$$

$$\begin{array}{ccccc} \deg(K/L) & \geq & \deg(K/K^H) & \geq & |\mathrm{Aut}(K/K^H)| \\ \| & & & & \| \\ |\mathrm{Aut}(K/L)| & & & & |\mathrm{Aut}(K/L)| \\ & & & & \| \\ & & & & |H| \end{array}$$

So $L = K^H$.

$\square$

Illustration:

$F \subset K$ cubic Galois.

$K = F[x]/p(x)$ $\quad p(x)$ cubic.

In K $\quad p(x) = (x-\alpha)(x-\beta)(x-\gamma)$

$\alpha, \beta, \gamma \in K$.

$\mathrm{Aut}(K/F)$ size 3 $\subset$ Permut $\{\alpha, \beta, \gamma\}$.

must be $\quad$ id

(α, β, γ)

$(\alpha\,\gamma\,\beta)$

$$\delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\delta) \in K.$$

$\downarrow$ $\qquad (\delta^2 = \Delta)$

fixed by $\mathrm{Aut}(K/F)$.

Means : $\delta \in F$.

Other half:

$$\begin{array}{ccc} K^H & \longleftarrow & H \\ & \longrightarrow & \mathrm{Aut}(K/K^H) \\ & & \cap \\ & & \mathrm{Aut}(K/F) \end{array}$$

By def.

$$H \subset \mathrm{Aut}(K/K^H).$$

$$|H| \leq |\mathrm{Aut}(K/K^H)|$$
$$\leq \deg(K/K^H) \leq |H|$$

Claim: $\deg(K/K^H) \leq |H|$.

Say $\alpha \in K$ is primitive for K/K^H. Must get a bound on the deg of min poly of α.

Let me show a poly in

$K^H[x]$

of deg $|H|$ satisfied by α.

$$(x-\alpha)(x-h_1\alpha)(x-h_2\alpha)\cdots$$

$$f(x) = \prod_{h \in H} (x - h\alpha)$$

$f(x)$ is fixed by H.

$$f(x) = x^{|H|} + \cdots x^{|H|-1} + \cdots =$$

in K^H.

so $f(x) \in K^H[x]$

$\square$

So

$$H = \mathrm{Aut}(K/K^H)$$

What about char p = ?

There is Galois thy in char p.

Char 0 :-

less crucial' → primitive elt thm.

repeated roots.

↗

Char p careful!

Work with "separable ext"