May 16 : Fundamental Theorem of Galois Theory

Plan

- Today: Proof of Fund Thm of Galois Theory
- Wednesday: Discussion (Theory & hw 8)
- Final goal:

Thm Given $f \in \mathbb{Q}[x]$ with $\mathbb{Q} \subset L$ splitting field,

f is solvable by radicals. $\Longleftrightarrow$ $\mathrm{Gal}(L/\mathbb{Q})$ solvable

Fund thm of Galois theory

Let $K \subset L$ Galois field extension.

There is a bijective correspondence

$$\left\{\begin{matrix}\text{intermediate field ext} \\ K \subset E \subset L\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups} \\ H \subset Gal(L/K)\end{matrix}\right\}$$

The bijections are given by

$$E \longmapsto Gal(L/E)$$

$$\text{fixed field } L^H \longleftarrow H$$

$$\left(L^H = \{x \in L \mid \forall \sigma \in H \ \sigma(x) = x\} \right)$$

These two maps are inverses!

What do we need to prove?

Need to show

$$E \longmapsto Gal(L/E) \longmapsto L^{Gal(L/E)}$$

↳ Goal $\boxed{E = L^{Gal(L/E)}}$

Conversely,

$$H \longmapsto L^H \longmapsto Gal(L/L^H)$$

Goal: $\boxed{H = Gal(L/L^H)}$

Lemma: Given $H \subset Gal(L/K)$,

$L^H \subset L$ normal & separable,

that is, L is Galois over L^H.

Proof Fix $\alpha \in L$. Let's find min poly of α over L^H

⇝ Look at orbit of α under H

⇝ $\{\alpha = \alpha_1, \alpha_2, \dots, \alpha_t\}$ orbit $H\alpha$

Look at

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)$$

$$\in L^H[x]$$

Why are the coeff. in L^H?

The min poly of α divides $f(x)$.

Since the roots of f are distinct & in L,

⇝ L separable & normal $/ L^H$

Lemma: Given $H < \mathrm{Gal}(L/K)$,

$L^H \subset L$ normal & separable

that is, L is Galois over L^H.

Proof Fix $\alpha \in L$. Let's find min poly of α over L^H

$\rightsquigarrow$ Look at orbit of α under H

$\rightsquigarrow \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t\}$ orbit $H\alpha$

Look at

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t) \in L^H[x]$$

Why are the coeff. in L^H?

The min poly of α divides $f(x)$.

Since the roots of f are distinct & in L,

$\rightsquigarrow L$ separable & normal $/ L^H$

$\alpha_1 \alpha_2 \alpha_3 \cdots \alpha_t \in L^H$?

Why is $\alpha_1 \alpha_2 \cdots \alpha_t$ fixed by every $\sigma \in H$?

Ex: $\tau\left(\prod_{\sigma \in H} \sigma(\alpha)\right) = \prod_{\sigma \in H} \sigma(\alpha)$

$\tau \in H$

In general, H permutes the roots and since the coeff. are symmetric poly in $\alpha_1, \ldots, \alpha_t$, we see that each $\sigma \in H$ fixes each coeff. $\rightsquigarrow f \in L^H[x]$

Fix $K \subset L$ Galois field ext

Lemma Given $H \subset Gal(L/K)$,

$H = Gal(L/L^H)$ & $|H| = |L : L^H|$

(Consequence: $H \mapsto L^H \mapsto Gal(L/L^H)$ gives back H)

Pf We will use that every finite separable field ext is simple.

$\Rightarrow \exists\, \alpha \in L$ s.t. $L = K(\alpha)$

Observe: Have $K \subset L^H \subset L$

Also $L = L^H(\alpha)$

Given α, the H orbit

$H\alpha = \{\alpha = \alpha_1, \ldots, \alpha_t\}$

$f(x) = (x-\alpha_1) \cdots (x-\alpha_t) \in L^H[x]$

Let $p(x)$ be min poly of α / L^H

Know $p(x) \mid f(x)$.

Know

$n := [L : L^H] = \deg p(x)$

$t := \deg f(x) \geq n$

Also Know

$\# Gal(L/L^H) \leq |L : L^H|$

Also know

$H \subset Gal(L/L^H)$

$\Rightarrow \# H \leq \# Gal(L/L^H) \leq |L : L^H] = n$

Know

$\# H \geq t = \deg f \geq \deg p = n$

For any group action G acting Σ, the size of orbit $Gx \leq \# G$

Conclude $\# H = n$

Because $H \subset Gal(L/L^H)$ & have same size, $H = Gal(L/L^H)$