Lecture 26

- Recall Fund Thm of Galois Thy
- Transitivity

Let $f(x) \in F[x]$ be a separable polyn, and let K be the field of $f(x)$.

- Then K/F is Galois
- The Galois group $G = Gal(K/F) = Aut(K/F)$ is also called the Galois group of the polynomial $f(x)$

prop $f(x)$ is irred $\iff$ G acts transitively on the roots.
($\sim m_{\alpha,F}(x)$ for a root α of $f(x)$)

pf. $\Leftarrow$ We already know G can only take α to other roots of $m_{\alpha,F}(x) = f(x)$.

$\Rightarrow$ Suppose $f(x)$ is irred, and let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the roots. Then there is an isom $F(\alpha_i) \cong F(\alpha_j)$ $\forall\ i,j$.
(both are isom to $F[x]/(f(x))$)

Can extend this isom to an automorphism σ $F(\alpha_1, \alpha_2, \dots, \alpha_d) = K$, which fixes F.

Note We didn't focus on the construction of these isomorphisms. But we know how to show one step; induct.

Then $\sigma(\alpha_i) = \alpha_j$. ($\Rightarrow$ G acts trans'ly.)

//

Finite Fields

Let $\mathbb{F}$ be a finite field.

- If $\operatorname{char} \mathbb{F} = p$, then $\mathbb{F}$ is an $\mathbb{F}_p$-VS of dimension n.

  From Friday:

  - $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$
  - $\mathbb{F} \cong$ the splitting field of $\underbrace{x^{p^n} - x}_{\text{separable}}$ over $\mathbb{F}_p$.

- $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$.

  Recall Frob. Automorphism: $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\alpha \mapsto \alpha^p$

Claim $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$

Pf.

Let $G = \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

By Fund. Thm, $|G| = n$.

Note $\sigma_p \in G$. And, $(\sigma_p)^i(\alpha) = \alpha^{p^i}$.

- $\alpha^{p^n} = \alpha \implies |\sigma_p| \leq n$
- (BWOC) If $\underbrace{|\sigma_p|}_{=k} \lneq n$, then $\forall\, \alpha \in \mathbb{F}_{p^n}$,

  $\alpha^{p^k} - \alpha = 0$ ↯ since there are only $p^k < p^n$ roots of this equation!

$\implies G$ is cyclic, generated by σ_p. //

[Review Fund Thm of Galois Thy].

- By the Fund Thm of Gal Theory,

$$\{\text{subfields of } \mathbb{F} = \mathbb{F}_{p^n}\} \longleftrightarrow \{\text{subgroups of } \mathbb{Z}/n\mathbb{Z}\}$$

$\mathbb{F}_{p^d}$ where $d \mid n$.

precisely, $\mathbb{Z}/d\mathbb{Z}$ for each $d \mid n$.

No other subfields!

- $\mathbb{Z}/n\mathbb{Z}$ is Abelian $\Rightarrow$ all subgroups are normal $\Rightarrow$

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\langle \sigma_p^d \rangle$$

↖ generated by $\overline{\sigma_p}$ in here, $|\overline{\sigma_p}| = d$.

Interesting Example

Let $f(x) = x^4+1$.

- $f(x)$ is irred over $\mathbb{Z}$.

  Recall: let $x = y+1$.

  Then $(y+1)^4+1 = y^4+4y^3+6y^2+4y+2$,

  Eisenstein @ $p=2$.

- $f(x)$ over any $\mathbb{F}_p$ is reducible

  - $p=2$: $x^4+1 = (x+1)^4$.
  - p odd: $\Rightarrow$ $p \equiv 1, 3, 5, \text{or } 7 \bmod 8$.

    $\Rightarrow p^2 \equiv 1 \bmod 8$.

    $\Rightarrow 8 \mid p^2-1$

  $\Rightarrow x^8-1 \mid x^{p^2-1}-1$ (HW10 Ex3)

  $\Rightarrow x^4+1 \mid x^8-1 \mid x^{p^2-1}-1 \mid x^{p^2}-x$

  $\Rightarrow$ roots of x^4+1 are all roots of $x^{p^2}-x$, ie they are all fixed by σ_p^2. (roots are the field $\mathbb{F}_{p^2}$)

  $\Rightarrow$ If α is a root of x^4+1, then

  $$\deg_{\mathbb{F}_p}(\alpha) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \leq 2.$$

  $\Rightarrow f(x) = x^4+1$ cannot be irreducible

  (o/w, $m_{\alpha,\mathbb{F}_p}(x) = f(x) \Rightarrow \deg_{\mathbb{F}_p}(\alpha) = 4$). //