

Recall:

- 1) First MT of Galois Theory: If K/F is a splitting field, then K/F is Galois.
- 2) Splitting fields are unique up to isom

Second MT of Galois Theory Suppose K/F is Galois,
 $\text{char}(F) = 0$, $G = \text{Gal}(K/F)$.

$$\left\{ \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ H \leq G, \text{ subgr} \right\}$$

$$\begin{array}{ccc} E & \longmapsto & \text{Aut}(K/F) \\ K^H & \longleftarrow & H \end{array}$$

These are inverse bijections. In particular, $K^G = F$.

Fixed fields

• K/F fte extⁿ, suppose $\text{char}(F) = 0$. Then $K = F(\alpha)$ and we know

$$| \text{Aut}(K/F) | \leq [K:F]$$

• If $H \leq \text{Aut}(K/F)$, then

$$F \subseteq K^H \subseteq K$$

$$|H| \leq | \text{Aut}(K/K^H) | \leq [K:K^H]$$

Today: These inequalities are equalities

Thm: K field, H fte gp of automorphisms of K , $F = K^H$. Suppose $\beta_1 \in K$, and

$\{\beta_0, \dots, \beta_r\}$ the H -orbit of β_1 .

(a) The irred poly for β_1/F is $g(x) = (x - \beta_0) \cdots (x - \beta_r)$

(b) β_1 is alg $/F$, $\deg_F(\beta_1) = r$, and $r = |H|$.

Pf: (b) follows from (a) b/c orbit, divide the size of the orbit.

11. (3) ...
of the gp acting.

a): g has coeffs that are fixed by H , and thus in $K^H = F$.

Suppose $h(x) \in F[x]$ satisfies $h(\beta_1) = 0$.

Indeed $h(\beta_j) = h(\sigma(\beta_1)) = \sigma(h(\beta_1)) = 0$.

$\Rightarrow x - \beta_1, \dots, x - \beta_r \mid h(x) \text{ in } K[x]$

$\Rightarrow g(x) \mid h(x) \text{ in } K[x]$

$\Rightarrow g(x) \mid h(x) \text{ in } F[x]$

Q

Lemma: Suppose $\text{char}(F) = 0$, K/F algebraic but not fte.

Then $\exists$ elts of K whose degree $/F$ is arbitrarily large.

Pf: $F \subsetneq F_1 = F(\alpha_1) \subsetneq F_2 = F_1(\alpha_2) \subsetneq F_3 \subsetneq \dots \subseteq K$
fte

$F_n = F(\alpha_n)$, $\deg(\alpha_n) \rightarrow \infty$ as $n \rightarrow \infty$.

Q

Thm (Fixed field Thm) Suppose $\text{char}(K) = 0$, H fte gp of automorphisms of K , $F := K^H$. Then K/F is fte and $[K:F] = |H|$.

K/F is fte and $[K:F] = |H|$.

Pf: Let $n := |H|$.

• Previous Thm, K/F is algebraic, and if $\beta \in K$, $\deg_F(\beta) \mid |H|$. By lemma, K/F is fte.

• Let $K = F(\gamma)$. If $\sigma \in H$ s.t. $\sigma(\gamma) = \gamma$, then $\sigma = 1 \Rightarrow$ orbit of γ has size n .

Previous Thm $\Rightarrow \deg_F(\gamma) = n$.

$\Rightarrow [K:F] = \deg_F(\gamma) = n = |H|$. ◻

Cor: a) K/F fte, then $|Aut(K/F)| \mid [K:F]$

b) $H \leq Aut(K)$. Then K/K^H is Galois with g/H .

Pf: a) $F \subset \underbrace{K^{Aut(K/F)}}_{|Aut(K/F)|} \subset K \Rightarrow \text{claim} \checkmark$

b) $H \leq Aut(K/K^H)$. But

$$|H| \leq |Aut(K/K^H)| \leq [K:K^H] = |H|$$

... .. $\therefore H = Aut(K/K^H)$

$$|H| \leq |\text{Aut}(K/F)| = [K:F] \implies |H| = [K:F] \text{ as } K/F \text{ is Galois.}$$

Thm: K/F fte, char = 0, $G = \text{Aut}(K/F)$ TFAE

- a) K/F is Galois, i.e. $|G| = [K:F]$
- b) $F \subseteq K^G$ is an equality
- c) K is a splitting field over F .

Pf: (a) $\iff$ (b):

$$\underbrace{F \subseteq K^G}_{\text{equality}} \subseteq K \quad \underbrace{K^G \subseteq K}_{[K:K^G] = |G|}$$

Therefore $[K:F] = |G| \iff F = K^G$

(a) $\iff$ (c): Already did

(a) $\implies$ (c): Let $\alpha \in K$ be primitive over F ,
w/ irred polynomial $f(x) \in F[x]$ of degree n .

So: $[K:F] = n$.

Suppose $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$ are the distinct roots
of f in K .

... .. It is G

Thus: $|G| = r$ b/c the only elt of G that stabilizes $\gamma = \gamma_1$ is the identity.

$$r = |G| = [K:F] = n = \deg(f) \\ \Rightarrow f \text{ splits in } K$$

Cor! a) If $\text{char}(F) = 0$, K/F fte, then $\exists$
 $L \supseteq K \supseteq F$ s.t. L/F is fte and Galois.

b) If K/F is Galois, $K \supseteq L \supseteq F$, then
 K/L is Galois w gp

$$\text{Gal}(K/L) = \{ \sigma \in \text{Gal}(K/F) : \sigma|_L = \text{id} \}$$

Pf! a) K/F is contained in a splitting field
 $\Rightarrow$ claim.

b) K/F Galois $\Rightarrow K/F$ is a splitting field

$\Rightarrow K/L$ is a splitting field

$\Rightarrow K/L$ is Galois.

$$\text{Thus } \text{Gal}(K/L) = \{ \sigma \in \text{Aut}(K) : \sigma|_L = \text{id} \}$$

$$= \{ \sigma \in \text{Gal}(K/F) : \sigma|_L = \text{id} \}.$$

□

