

Thm: A finite separable extension K/F is Galois if and only if K is the splitting field of a polynomial $f \in F[x]$.

Pf: Suppose K/F is Galois. By the Prim Elem. Thm.,

$K = F(\alpha)$, for some $\alpha \in K$. Let $f = \min_F(\alpha)$. Any autom.

$\sigma \in \text{Aut}(K/F)$ is uniquely determined by $\sigma(\alpha)$, and

there are $\deg(f)$ choices for $\sigma(\alpha)$. Since

$\deg(f) = [K:F] = |\text{Aut}(K/F)|$, all of these must

\uparrow
 K/F is Galois

extend to auts. of K . This implies that all of the roots of f are in K , so K is the spl. field of f .

To prove the other direction:

Actually will prove that if K is the splitting field of $f \in F[x]$ and if $\sigma: F \rightarrow \tilde{F}$ is an isom. of fields,

with \tilde{K} a splitting field of $\tilde{f} = \sigma(f)$, then

there are $[K:F]$ ways of extending σ to an

isom. $\tilde{\sigma}: K \rightarrow \tilde{K}$.

Pf. by induction on $n = [K:F]$.

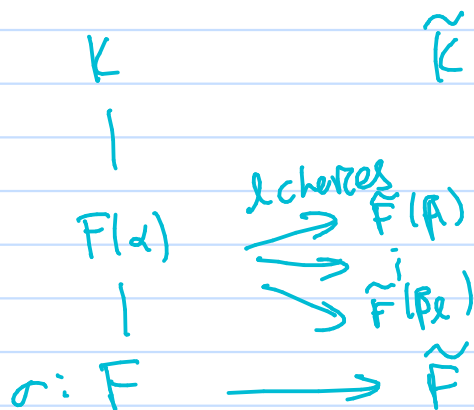
True for $n=1$. ✓

Assume true for $1 \leq m < n$. Suppose $[K:F] = n$,

and that K is the spl. field of $f \in F[x]$.

Then f has an irred. factor $p(x)$ of degree ≥ 2 . Let α be a root of p in K . Then:

i) There are $\deg p$ ways of extending σ to an isom. from $F(\alpha)$ to a subfield of \tilde{K} .



$$p(x) \longmapsto \tilde{p}(x) = (x - \beta_1) \cdots (x - \beta_e)$$

$$l = \deg p$$

ii) Since $[K:F(\alpha)] = \frac{[K:F]}{\deg p} < n$, by the Induc.

hyp. there are exactly $[K:F(\alpha)]$ ways of extending each of these l maps to an isom. $K \rightarrow \tilde{K}$.

This must account for all such auto., so the total # is

$$l \cdot [K:F(\alpha)] = n. \quad \square$$

Def: $\forall H \in \text{Aut}(K)$, the fixed field of H , denoted by K_H , is the subset of K which is fixed by everything in H .

$$K_H = \{ \alpha \in K : \forall \sigma \in H, \sigma(\alpha) = \alpha \}.$$

Lemma: (inclusion reversing)

i) If F_1, F_2 and K are fields, $F_1 \subseteq F_2 \subseteq K$, then

$$\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1).$$

\uparrow
(subgroup)

ii) If $H_1 \leq H_2 \leq \text{Aut}(K)$ then

$$K_{H_2} \subseteq K_{H_1}.$$

Fundamental Theorem of Galois Theory:

Suppose K/F is a Galois extension with $\text{Gal}(K/F) \cong G$. Then:

- i) There is a bijection between subgroups $H \leq G$ and intermediate fields of K/F , given by the map $H \mapsto K_H$. Furthermore $[K:K_H] = |H|$ (equivalently, $[K_H:F] = |G:H|$).

The lattice of intermediate fields corresponds to the "upside down" lattice of subgroups of G .

- ii) $\forall H \leq G$, the extension K/K_H is Galois, with $\text{Gal}(K/K_H) \cong H$.

- iii) $\forall H \leq G$, K_H/F is Galois $\iff H \trianglelefteq G$. (normal)

If it is Galois then $\text{Gal}(K_H/F) \cong G/H$.

Exs:

1) $K = \mathbb{Q}(\zeta_5)$, $F = \mathbb{Q}$.

$$f(x) = \min_{\mathbb{Q}}(\zeta_5) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

so $[K:\mathbb{Q}] = 4$.

Also $f(x) = \prod_{a=1}^4 (x - \zeta_5^a)$, so K is the spl. field of f .

By our thm., K/F is Galois, so $|\text{Aut}(K/F)| = 4$.

Any $\sigma \in \text{Aut}(K/F)$ is uniquely determined by $\sigma(\zeta_5)$, and there are 4 possibilities:

$$\sigma(\zeta_5) = \zeta_5^a, \quad 1 \leq a \leq 4.$$

All of these must occur, since $|\text{Aut}(K/F)| = 4$.

Let $\tau \in \text{Aut}(K/F)$ be determined by $\tau(\zeta_5) = \zeta_5^2$.

$$\text{Then } \tau^2(\zeta_5) = \tau(\zeta_5^2) = (\tau(\zeta_5))^2 = (\zeta_5^2)^2 = \zeta_5^4$$

$$\tau^3(\zeta_5) = \tau(\tau^2(\zeta_5)) = \tau(\zeta_5^4) = (\tau(\zeta_5))^4 = (\zeta_5^2)^4 = \zeta_5^3$$

$$\tau^4(\zeta_5) = \tau(\tau^3(\zeta_5)) = \tau(\zeta_5^3) = \dots \quad (\text{cont. next time})$$