

Announcements

Friday class will be in Henry Admin Bldg. 149

HW8 posted (due 4/9)

HW4/HW5/Midterm 2 regrade requests open thru. 4/9

Last time:

Thm A: If $G \subseteq \text{Aut}(K)$, then $K/\text{Fix } G$ is Galois and

$$\text{Gal}(K/\text{Fix } G) = G$$

Thm B: K/F finite extn. TFAE

a) K/F is Galois

b) K is the splitting field of a sep. poly. in $F[x]$

c) $\text{Fix}(\text{Aut}(K/F)) = F$

Today: Prove Fundamental Thm. of Galois Theory

Fundamental Thm. of Galois Theory: K/F Galois, $G := \text{Gal}(K/F)$.

There exists a bijection

$$\left\{ \begin{array}{l} \text{Intermediate} \\ \text{fields} \end{array} \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{subgps.} \\ 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

$$E \xrightarrow{\phi} \text{Aut}(K/E)$$

$$\text{Fix } H \xleftarrow{\psi} H$$

Properties: $(E \leftrightarrow H, E_1 \leftrightarrow H_1, E_2 \leftrightarrow H_2)$

$$1) E_1 \subseteq E_2 \iff H_1 \supseteq H_2$$

$$2) [K:E] = |H| \text{ and } [E:F] = \underbrace{|G:H|}_{\text{index}}$$

$$3) K/E \text{ is Galois w/ } \text{Gal}(K/E) = H$$

$$4) E/F \text{ is Galois } \iff H \trianglelefteq G$$

↖ normal subgp.

$$5) E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle \text{ and } E_1 E_2 \leftrightarrow H_1 \cap H_2$$

$$\text{In this case, } \text{Gal}(E/F) = G/H$$

Examples (cont.)

b) $K = \mathbb{Q}(\underbrace{\sqrt[3]{2}}_{\alpha}, \underbrace{\zeta_3}_{\gamma}) = \text{splitting field of } x^3 - 2 \in \mathbb{Q}[x]$
 $\beta = \zeta\alpha, \gamma = \zeta^2\alpha$

$\text{Gal}(K/\mathbb{Q}) \cong S_3$ (all permutations of α, β, γ)

$\cong \langle \sigma, \tau \rangle$ where

$\sigma: \alpha \mapsto \alpha$
 $\zeta \mapsto \zeta$

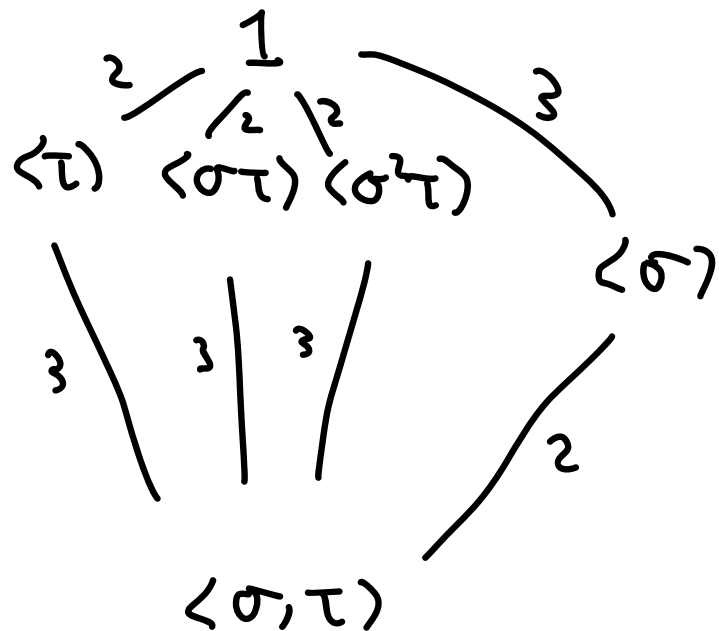
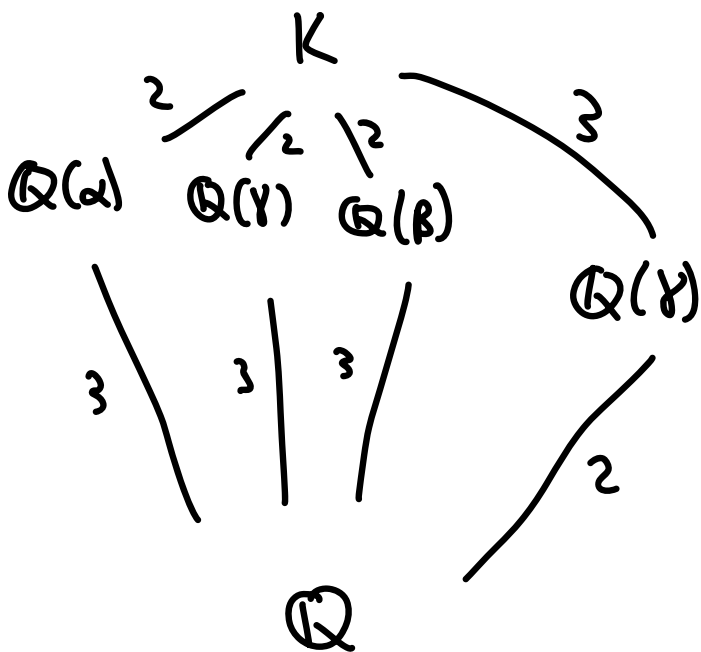
$\tau: \alpha \mapsto \alpha$
 $\zeta \mapsto \zeta^2$

$\sigma: \alpha \mapsto \zeta\alpha$
 $\zeta \mapsto \zeta$

$\sigma\tau = \tau\sigma^2: \alpha \mapsto \zeta\alpha$
 $\zeta \mapsto \zeta^2$

$\sigma^2: \alpha \mapsto \zeta^2\alpha$
 $\zeta \mapsto \zeta$

$\sigma^2\tau = \tau\sigma: \alpha \mapsto \zeta^2\alpha$
 $\zeta \mapsto \zeta^2$



PF of Fund. Thm.: Basic set theory facts: if $f \circ g$ inj, then g inj.

By Thm A, if $H \leq G$, then $\text{Aut}(K/\text{Fix } H) = H$, so ψ is inj.

By Thm B, if $F \subseteq E \subseteq K$, then K is the splitting field of a poly in $F[x]$, hence in $E[x]$, so K/E is Galois. Also by Thm. B, $\text{Fix}(\text{Aut}(K/E)) = E$, so ϕ is inj.

Therefore, ψ and ϕ are injections which compose to the identity, so they are inverse bijections.

Properties:

1) Proved in lecture 21

2) $\text{Gal}(K/E) = H$, and by the def'n of Galois ext'n, $[K:E] = |\text{Gal}(K/E)|$

By the Tower Law,

$$[E:F] = \frac{[K:F]}{[K:E]} = \frac{|G|}{|H|} = |G:H|$$

3) Follows from Thm. B

4) (sketch; see D&F pp. 575 for details)

Every $\sigma \in \text{Gal}(K/F)$ sends E to $\sigma(E) \subseteq K$, and

$\sigma(E) \cong E$. The set of embeddings of E into k fixing F is

$$\text{Emb}_k(E/F) = \{ \sigma|_E \mid \sigma \in \text{Gal}(k/F) \}$$

$$\sigma|_E = \sigma'|_E \iff \sigma H = \sigma' H,$$

$$\text{So } |\text{Emb}_k(E/F)| = |G:H| = \underset{\substack{\uparrow \\ \text{Tower Law}}}{[E:F]}$$

Now,

$$\text{Aut}(E/F) = \{ \bar{\sigma} \in \text{Emb}_k(E/F) \mid \bar{\sigma}(E) = E \} \subseteq \text{Emb}_k(E/F),$$

$$\text{So } E/F \text{ Galois} \iff \text{Aut}(E/F) = \text{Emb}_k(E/F)$$

$$\iff \sigma(E) = E \quad \forall \sigma \in G$$

$$\iff H = \text{Aut}(k/E) = \text{Aut}(k/\sigma(E)) = \sigma H \sigma^{-1} \quad \forall \sigma \in G$$

$$\iff H \trianglelefteq G.$$

$$5) e \in E_1 \cap E_2 \iff e \text{ fixed by } H_1 \cup H_2 \iff e \text{ fixed by } \langle H_1, H_2 \rangle$$

$$h \in H_1 \cap H_2 \iff h \text{ fixes } E_1 \cup E_2 \iff h \text{ fixes } E_1, E_2$$

□

(If time) Remark about finite fields:

Let $f(x) \in \mathbb{F}_p[x]$ be irred of deg n .

Then $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n} \leftarrow$ unique up to isom

So if α is a root of f , $\alpha \in \mathbb{F}_{p^n}$

So $\mathbb{F}_{p^n} = \text{Sp}_{\mathbb{F}_p} f$

In particular, $f \mid x^{p^n} - x$

Conversely, if $f \in \mathbb{F}_p[x]$ is irred. and divides $x^{p^n} - x$,
it must have degree dividing n

So over \mathbb{F}_p , $x^{p^n} - x$ is the prod. of all irred polys.
over \mathbb{F}_p of degree dividing n .