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 $G \leq \mathrm{Aut}(K)$, then $K/\mathrm{Fix}\, G$ is Galois and $\mathrm{Gal}(K/\mathrm{Fix}\, G) = G$

Thm B: K/F finite ext'n. TFAE

a) K/F is Galois

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

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

Today: Prove Fundamental Thm. of Galois Theory

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

There exists a bijection

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

$$E \xmapsto{\ \phi\ } \mathrm{Aut}(K/E)$$

$$\mathrm{Fix}\, H \xleftarrow[\ \psi\ ]{} H$$

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

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

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

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

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

normal subgp.

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

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

Examples (cont.)

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

$\beta = \zeta\alpha, \quad \gamma = \zeta^2\alpha$

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

$\quad \| $

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

$1: \alpha \mapsto \alpha, \quad \zeta \mapsto \zeta$ $\qquad\qquad$ $\tau: \alpha \mapsto \alpha, \quad \zeta \mapsto \zeta^2$

$\sigma: \alpha \mapsto \zeta\alpha, \quad \zeta \mapsto \zeta$ $\qquad\qquad$ $\sigma\tau = \tau\sigma^2: \alpha \mapsto \zeta\alpha, \quad \zeta \mapsto \zeta^2$

$\sigma^2: \alpha \mapsto \zeta^2\alpha, \quad \zeta \mapsto \zeta$ $\qquad\qquad$ $\sigma^2\tau = \tau\sigma: \alpha \mapsto \zeta^2\alpha, \quad \zeta \mapsto \zeta^2$

$$
\begin{tikzcd}
 & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, bend left, "3"] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "3"'] & \mathbb{Q}(\gamma) \arrow[d, dash, "3"] & \mathbb{Q}(\beta) \arrow[dl, dash, "3"] & \mathbb{Q}(\zeta) \arrow[dll, dash, "2"] \\
 & \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, bend left, "3"] & & \\
\langle \tau \rangle \arrow[dr, dash, "3"'] & \langle \sigma\tau \rangle \arrow[d, dash, "3"] & \langle \sigma^2\tau \rangle \arrow[dl, dash, "3"] & \langle \sigma \rangle \arrow[dll, dash, "2"] \\
 & \langle \sigma, \tau \rangle & &
\end{tikzcd}
$$

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

By Thm A, if $H \leq G$, then $\mathrm{Aut}(K/\mathrm{Fix}\,H) = H$, 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, $\mathrm{Fix}(\mathrm{Aut}(K/E)) = E$, 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) $\mathrm{Gal}(K/E) = H$, and by the def'n of Galois ext'n, $[K:E] = |\mathrm{Gal}(K/E)|$

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

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

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

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

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

Now,

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

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

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

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

$$\iff H \trianglelefteq G.$$

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

$h \in H_1 \cap H_2 \iff h$ fixes $E_1 \cup E_2 \iff h$ fixes $E_1 E_2$

$\square$

(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 $\mathbb{F}_{p^n} = Sp_{\mathbb{F}_p} f$

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.