Midterm almost graded

Rest of h/w 5 will be posted soon

Today: characterize Galois ext'ns, and fund. thm. of Galois theory

---

Thm 13: K/F Galois $\iff$ K is the splitting field of some sep. poly $/F$.

Pf: $\Leftarrow$: Prop 5.

$\Rightarrow$: Let $G = \mathrm{Gal}(K/F)$, $p(x) \in F[x]$ irred, $\alpha \in K$ root of p.

Let $\alpha_1, \dots, \alpha_r$ $(r \leq n)$ denote the Galois conjugates of α.

Since elts. of G are automorphisms, $\alpha_1, \dots, \alpha_r$ are roots of p.

Let

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r) \in K[x] \qquad (f(x) \mid p(x))$$

$f(x) \in (\mathrm{Fix}\, G)[x] \underset{\text{(Cor. 10)}}{=} F[x]$ since elts. of G permute the roots of f.

Since p irred, $f = p$, so p: sep., splits in K

Just need to find a poly. for which K is the splitting field

Let $\omega_1, \dots, \omega_n$ be a basis for K/F.

$p_i := m_{\omega_i, F}(x)$

$\prod p_i$ has splitting field K, removing duplicates gives a sep. poly. whose splitting field is K.

Cor: K/F Galois $\Rightarrow$ every irred. poly in $F[x]$ w/ a root in K is sep & splits over K

Thm 14: Fundamental Theorem of Galois Theory:

K/F: Galois ext'n, $G := \mathrm{Gal}(K/F)$. $\exists$ bijection

$$\left\{ \begin{array}{cc} \text{intermediate fields} & K \\ & | \\ F \subseteq E \subseteq K & E \\ & | \\ & F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{cc} \text{subgroups} & 1 \\ & | \\ H \leq G & H \\ & | \\ & G \end{array} \right\}$$

given by

$$E \longmapsto \mathrm{Aut}(K/E)$$

$$\mathrm{Fix}\, H \longleftarrow\!\shortmid\; H$$

"Galois correspondence".

It has the following properties ($E \leftrightarrow H$, $E_1 \leftrightarrow H_1$, $E_2 \leftrightarrow H_2$)

(1) (Inclusion reversal): $E_1 \subseteq E_2 \Leftrightarrow H_1 \geq H_2$

(2) $[K:E] = |H|$, $[E:F] = |G:H|$

$$\begin{array}{cl} K & \\ | & \big\} \; |H| \\ E & \\ | & \big\} \; |G:H| \\ F & \end{array}$$

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

(4) E/F is Galois $\Leftrightarrow H \trianglelefteq G$.

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

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

$E_1 E_2 \leftrightarrow H_1 \cap H_2$

Pf: Cor 11: $\mathrm{Aut}(K/\mathrm{Fix}\, H) = H$

Thm 13 $\Rightarrow$ K/E is Galois, so Cor 10 $\Rightarrow$ $\mathrm{Fix}\, \mathrm{Aut}(K/E) = E$

Since applying the maps in either order gives the identity, they are inverse bijections

Prop 4 $\Rightarrow$ (1)

(3) follows from above reasoning

(3) & Tower law $\Rightarrow$ (2)

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

$h \in \langle H_1, H_2 \rangle \Rightarrow h = h_1 h_2 \cdots h_n$, $h_i \in H_1$ or $h_i \in H_2$

each h_i fixes $E_1 \cap E_2$ so h fixes $E_1 \cap E_2$

$E_1 E_2 \cap H_1 \cap H_2$ similar (see D & F)

(4) Let $\mathrm{Emb}(E/F) = \{ \tau : E \underset{\text{inj.}}{\hookrightarrow} K \mid \tau(f) = f,\ f \in F \}$

We'll show that $|\mathrm{Emb}(E/F)| = [E:F] \overset{(2)}{=} [G:H]$

If $\sigma \in \mathrm{Gal}(K/F)$, $\sigma|_E \in \mathrm{Emb}(E/F)$

If $\tau \in \mathrm{Emb}(E/F)$, K is a splitting field for $\tau(E)$, so Thm 13.27:

$$\begin{array}{ccc} \sigma : K & \xrightarrow{\sim} & K \in G \\ | & & | \\ \tau : E & \xrightarrow{\sim} & \sigma(E) \end{array}$$

If $\sigma, \sigma' \in G$, then $\sigma|_E = \sigma'|_E \iff$

$\sigma^{-1}\sigma' \in H\ (= \text{Fix } E) \iff \sigma H = \sigma' H$

So $|\text{Emb}(E/F)| = [G:H] = [E:F]$.

Now, E/F Galois $\iff |\text{Aut}(E/F)| = [E:F] = |\text{Emb}(E/F)|$

$\iff E = \sigma(E)$ for all $\sigma \in G$.

$\iff H = \sigma H \sigma^{-1}$ for all $\sigma \in G$ (since $\sigma(E) \leftrightarrow \sigma H \sigma^{-1}$)

$\iff H \trianglelefteq G$

When this happens, $G/H \cong \text{Gal}(E/F)$ since G/H inherits its gp. structure from G

<u>Examples:</u>

1) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

Let $\sigma: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$ $\quad \tau: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$

Then $G = Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong K_4$

Klein 4

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\{1,\tau\} \arrow[dr, dash, "2"'] & \{1,\sigma\tau\} \arrow[d, dash, "2"] & \{1,\sigma\} \arrow[dl, dash, "2"] \\
 & K_4 &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\mathrm{Fix}\,\{1,\tau\} = \mathbb{Q}(\sqrt{2})$

$\mathrm{Fix}\,\{1,\sigma\} = \mathbb{Q}(\sqrt{3})$ $\qquad$ $\mathrm{Fix}\,\{1,\sigma\tau\} = \mathbb{Q}(\sqrt{6})$

2) $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$, $\zeta = \zeta_3$

$\sigma : \begin{cases} \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \\ \zeta \longmapsto \zeta \end{cases}$ $\qquad$ $\tau : \begin{cases} \sqrt[3]{2} \longmapsto \sqrt[3]{2} \\ \zeta \longmapsto \zeta^2 = -1-\zeta \end{cases}$

$G = \langle \sigma, \tau \rangle \cong S_3$

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "2"] & & \\
\langle\sigma\rangle \arrow[dr, dash, "2"'] & \langle\tau\rangle \arrow[d, dash, "3"] & \langle\tau\sigma\rangle \arrow[dl, dash, "3"] & \langle\tau\sigma^2\rangle \arrow[dll, dash, "3"] \\
 & S_3 & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, \zeta) \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] \arrow[drr, dash, "2"] & & \\
\mathbb{Q}(\zeta) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash, "3"] & \mathbb{Q}(\zeta, \sqrt[3]{2}) \arrow[dl, dash, "3"] & \mathbb{Q}(\zeta^2\sqrt[3]{2}) \arrow[dll, dash, "3"] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

$$\operatorname{Fix}\langle\tau\sigma\rangle = \operatorname{Fix}\left\{\begin{array}{l} \sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2} \\ \zeta \longmapsto \zeta^2 \end{array}\right. = \mathbb{Q}(\zeta\sqrt[3]{2})$$

Since $\zeta\sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2}\cdot\zeta^2 = \zeta\sqrt[3]{2}$

Which ext'ns are Galois?

$\mathbb{Q}(\sqrt[3]{2}, \zeta)/E$ for any E above

$\mathbb{Q}(\zeta)/\mathbb{Q}$ since $\langle\sigma\rangle$ is a normal subgp.
(index 2)

None of the others, since not normal subgps.

e.g. $\sigma\tau\sigma^{-1} = \tau\sigma \notin \langle\tau\rangle$