First half of HW5 posted (due Tues 2/21)

We know (Prop 5) if $F \subseteq K$ that $|\mathrm{Aut}(K/F)| \leq [K:F]$

Want to know when we have equality (i.e. Galois ext'n)

Thm 9: Let $G \leq \mathrm{Aut}(K)$, and let (G is always finite

$F = \mathrm{Fix}(G)$. Then $m := [K:F] = |G| =: n$

$n > m$: done (showed impossible)

If $n < m$, the system

$$\sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_m)x_m = 0$$

$$\vdots$$

$$\sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_m)x_m = 0$$

n eqns.
m unknowns

has a nontriv. sol'n $x_1 = \gamma_1, \ldots, x_m = \gamma_m$ in K

(but <u>not</u> in F, since $\omega_1, \ldots, \omega_m$ linearly indep. $/F$)

Reordering/scaling if necessary, assume $\gamma_1 \notin F$,

$\gamma_r = 1$, $\gamma_{r+1} = \cdots = \gamma_m = 0$

Then,

$$\begin{aligned}
\sigma_1(\omega_1)\gamma_1 + \cdots + \sigma_1(\omega_{r-1})\gamma_{r-1} + \sigma_1(\omega_r) &= 0 \\
&\vdots \qquad\qquad (*) \\
\sigma_n(\omega_1)\gamma_1 + \cdots + \sigma_n(\omega_{r-1})\gamma_{r-1} + \sigma_n(\omega_r) &= 0
\end{aligned}$$

Since $\gamma_1 \notin F = \text{Fix}\, G$, choose $k \in \{1, .., n\}$ s.t. $\sigma_k(\gamma_1) \neq \gamma_1$.
Since G is a gp., $\sigma_k\sigma_1, \sigma_k\sigma_2, \ldots, \sigma_k\sigma_n$ is a permutation of $\sigma_1, \ldots, \sigma_n$, so applying σ_k to $(*)$ gives

$$\begin{aligned}
\sigma_1(\omega_1)\sigma_k(\gamma_1) + \cdots + \sigma_1(\omega_1)\sigma_k(\gamma_{r-1}) + \sigma_1(\omega_r) &= 0 \\
&\vdots \qquad\qquad (**) \\
\sigma_n(\omega_1)\sigma_k(\gamma_1) + \cdots + \sigma_n(\omega_1)\sigma_k(\gamma_{r-1}) + \sigma_n(\omega_r) &= 0
\end{aligned}$$

Subtracting $(**)$ from $(*)$ gives a smaller nontriv. set of eqns. Contradiction! $\square$

Cor 10: K/F finite extn:

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

w/ equality iff $F = \text{Fix}(\text{Aut}(K/F))$
i.e. K/F Galois $\iff$ $F = \text{Fix}(\text{Aut}(K/F))$

Pf: Let $E = \mathrm{Fix}(\mathrm{Aut}(K/F))$. Then $F \subseteq E \subseteq K$, and by Thm 9, $|\mathrm{Aut}(K/F)| = [K:E]$.

By the Tower Law $[K:F] = |\mathrm{Aut}(K/F)|\,[E:F]$ $\square$

Sort of converse to the last result:

Cor 11: $G \leq \mathrm{Aut}(K)$, $F = \mathrm{Fix}(G)$. Then, $\mathrm{Aut}(K/F) = G$

Pf: By def'n, $G \leq \mathrm{Aut}(K/F)$. By Thm 9, $[K:F] = |G|$, and by Cor. 10, $|\mathrm{Aut}(K/F)| \leq [K:F]$, so

$$[K:F] = |G| \leq |\mathrm{Aut}(K/F)| \leq [K:F]$$

must be equal

$\square$

Cor 12: If $G, H \leq \mathrm{Aut}(K)$, $G \neq H$, then $\mathrm{Fix}\, G \neq \mathrm{Fix}\, H$.

Pf: If $\mathrm{Fix}\, G = \mathrm{Fix}\, H$, then by Cor. 11,

$$G = \mathrm{Aut}(K/\mathrm{Fix}\, G) = \mathrm{Aut}(K/\mathrm{Fix}\, H) = H$$

$\square$

Def: K/F Galois. The <u>Galois conjugates</u> of $\alpha \in K$ are $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(K/F)\}$.

Thm 13: K/F Galois $\Leftrightarrow$ 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

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

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

Since p irred, $f = p$, so p: sep., splits in $K \Rightarrow b)$

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

$$\left\{ \begin{array}{l} \text{intermediate} \\ \text{fields} \\ F \subseteq E \subseteq K \end{array} \quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgroups} \\ H \leq G \end{array} \quad \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

given by

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

$$\mathrm{Fix}\, H \longleftarrow H$$

"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) $[K:E] = |H|$, $[E:F] = |G:H|$ $\quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \begin{array}{l} \}\ |H| \\ \\ \}\ |G:H| \end{array}$

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

$E_1 E_2 \leftrightarrow H_1 \cap H_2$

Next time: pf and examples