Galois theory: Pull up the last part for weeks 11-12.

Recall If \( L/K \) and \( f(x) \in K[x] \)
then \( \text{Aut}(L/K) \) is isomorphic to the \( f \) \( a \in L \)
\[
\text{g}(a) \text{ is a root of } f \text{ if } a \text{ is.}
\]
Field automorphisms of \( L \) such that \( a \) is the identity in \( K \).
If \( \sum a_n \alpha^n = 0 \), \( a_n \in K \)
\[
\sum \text{g}(a_n) \text{g}(\alpha)^n = 0
\]
\[
\sum a_n \text{g}(\alpha)^n = 0.
\]

Observation: If \( L = K(\alpha_1, \ldots, \alpha_n) \)
\( \sigma \in \text{Aut}(L/K) \) is determined
by \( \sigma(\alpha_1), \ldots, \sigma(\alpha_n) \).
\( \sigma(\alpha_i) \) is the minimal polynomial of \( \alpha_i \)
over \( K \).
\( \sigma(\alpha_i) \leq \text{Roots of } \text{m}_{\alpha_i} \text{ in } L. \)
\( \Rightarrow \text{Aut}(L/K) \) is finite
if \( [L:K] \) is finite.

Lemma: If \( L/K \) is the splitting field of
an irreducible polynomial \( f \) then
\[ \text{Aut}(L/K) \leq [L:K] \]
Idea: Let $x_1, \ldots, x_n$ denote the roots.

$L = K(x_1, \ldots, x_n)$

$G \in \text{Aut}(L/K)$ is determined by how it permutes the roots.

\[ \text{Aut}(L/K) \leftrightarrow \text{Aut}(\text{roots of } F \text{ in } L) \]

To build $\sigma$: First, what does $G$ do to $x_i$?

$K(x_1) \rightarrow L \leftarrow$ which are the possible maps?

$\sigma_1 \in S_n$ (Act fix $K$).

So, I get $\sigma_1: K(x_1) \rightarrow L$ s.t. $\sigma_1(x_i) = i$.

$\sigma_2: K(x_1, x_2) = K(x_1)(x_2) \rightarrow L$

Where can I send $x_2$?

(excluding $\sigma_1$)

$m(x)$ is min polynomial of $x_2$ over $K(x_1)$

$K(x_1)(x_2) \cong K(x_1)C(x_2)/m(x)$

Can send $x$ to any root of
\[ \sigma_M(x) \in L \text{ if } x \in M \]

There are \( d \) choices

\[ m(x) \mid f(x), \quad \sigma_M(x) = f(x), \quad \text{all roots in } L \]

Choose \( m = [x, \alpha (x)] = \text{Hom}(\bar{K}, \bar{L}) \)

Repeat:

1. Deduce that \( |\text{Aut}(L/M)| = [L:K]\).
2. \( \text{if } f \text{ is separable} \)
   \[ \frac{f_0(x)}{f_0(y)}, \quad \text{Aut}(L(x,y)/K(x,y)) = \{1\} \text{ otherwise} \]

**Definition/Thm:** \( L/K \) finite is Galois if any of the following equivalent conditions hold:

1. \( [L:K] = |\text{Aut}(L/K)| \).
2. \( K = L \text{ Aut}(L/K) (:= \{ \sigma \in L \mid \sigma(l) = l \quad \forall l \in L \}) \)
3. \( L/K \) separable and normal if \( \alpha \in L \)
   \[ \text{then } m_\alpha(x) \text{ has distinct roots in } L \]
4. \( L/K \) is a splitting field of a separable polynomial.

(4) \( \Rightarrow \) (1) we basically just did

(2) \( \Rightarrow \) (3) easy.

Proof if \( \alpha \in L \).
$f(x) = T (x - \beta) \in \text{Ann}(L/M)$.

Point: To see this, let coefficient in $K$.

$g(f) = T (x - \sigma(x))$ for $\sigma \in \text{Aut}(L/K)$

$= T (x - \beta)$

So all the coefficients are preserved by $\text{Aut}(L/K)$ implies they are in $K$.

(3) easy. (Take product of minimal polynomials of a id of ground).

Lemma: If $L$ is a field $G \leq \text{Aut}(L)$ a finite subgroup.

Then $[L: L^G] = |G|$

Proof: Use independence of characters descend.

$k \leq \text{Aut}(L/K)$

So

$[L: k] = [L: L^\text{Aut}(L/K)] [L^\text{Aut}(L/K): k]$

If there are equal then $[L^\text{Aut}(L/K): k] = 1$

So $L^\text{Aut}(L/K) = k$.

Since congruence shows $|\text{Aut}(L/K)| \leq [L: K]$. 
Lemma shows $L/L^6$ is Galois with group $G$.
$\text{Aut}(L/L^6) = G$. 

**Note:** If $L/K$ is Galois then the roots of minimal polynomial of $\alpha \in L$ are in the Galois orbit of $\alpha$.

In particular, if $f(x) \in K[x]$ is a separable polynomial and $L/K$ is a splitting field then the irreducible factors of $f$ in $K[x]$ are in bijection with the orbits of $\text{Gal}(L/K)$ acting on $\text{Aut}(L/K)$, the roots of $f$.

**Fundamental Theorem $L/K$ Galois**

Intermediate fields $\leftrightarrow$ Subgroups of $\text{Aut}(L/M)$

$H \rightarrow F(L,H)

L^H \subseteq H$

$L(x, y) \theta x^2 + 7x + 3x, x^2$. 