Lecture 23:

Previously on Math 418:

Thm: \( K \) the splitting field of \( f(x) \in F[x] \).
Then \( |\text{Aut}(K/F)| \leq [K:F] \) with equality if \( f \) is separable.

Thm: \( K/F \) a finite extension, where \( \text{char}(F) = 0 \).
Then \( K = F(\gamma) \) for some \( \gamma \in K \) and so
\( |\text{Aut}(K/F)| \leq [K:F] \)

Constr: \( G \) a finite subgroup of \( \text{Aut}(K) \), \( F = K_G \) the
fixed field. Then given \( \alpha \in K \), the min poly
\[ m_{\alpha,F}(x) = \prod (x - \alpha_i) \text{ where } G \cdot \alpha = \{ \alpha, \ldots, \alpha_n \} \]
In particular \( \alpha \) is alg over \( F \) of deg \( \leq |G| \).

Today:

Thm: \( G \leq \text{Aut}(K) \) finite. Then \([K:K_G] = |G| \).
Hence \( K/K_G \) is Galois with \( \text{Aut}(K/K_G) = G \).

Focus: \( K \) has char 0 or \( K \) is finite
Finite Fields:

\[ K = \mathbb{F}_p^n = \text{splitting field of } x^{p^n} - x \text{ over } \mathbb{F}_p. \]

Key: \( K^x = (K \setminus \{0\}, \cdot) \) cyclic.

Pf: By the fund. theorem of finite abelian gps

\[ K^x = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \text{ with } n_1 | n_2 | \ldots | n_k \]

[Q: How many have seen this?]

If \( k > 1 \), then have at least \( n_1 + \frac{n_2}{n_1} \) els with \( x^{n_1} = 1 \). But then \( x^{n_1} - 1 \) has more than \( n_1 \) roots, a contradiction.

Cor: Any extension of finite field \( K/F \) is simple, i.e. \( K = F(\alpha) \).

Pf: Let \( F_p \) be the char field of \( K \). \( \alpha \) gen \( K^x \), then \( K = F_p(\alpha) \).

Cor: \( K = \mathbb{F}_{p^n} \). Then \( \text{Aut}(K) = \text{Aut}(K/F_p) \cong \mathbb{Z}/n\mathbb{Z} \)

is generated by Frobenius \( \sigma : K \to K \)

\[ \alpha \to \alpha^p, \]
Proof: Since $K$ is the splitting field of the separable poly $X^{p^n} - x$, have

$$|\text{Aut}(K/F_p)| = [K:F_p] = n.$$ Let $\sigma$ gen $K^*$. If $\sigma^k = 1$, then $\sigma^k(\alpha) = \alpha^{p^k} = \alpha^{p^{k-1}}$.

First, $\Rightarrow \alpha^{p^{k-1}} = 1 \Rightarrow k > n$. So $|\sigma| = n$.

$\Rightarrow$ Aut$(K/F_p) = \langle \sigma \rangle$.

Then: $G \leq \text{Aut}(K)$ finite. Then $[K:K_G] = |G|$.

Proof: Assume $\text{char}(K) = 0$ or $K$ is finite. Let $F = K_G$.

Know every $\alpha \in K$ is alg/F of deg $\leq |G|$. Let $\alpha \in K$ have max. deg/F = $n$.

Claim: $K = F(\alpha)$.

Suppose $\beta \in K$. Then $[F(\alpha, \beta):F] \leq n^2$.

and so $\exists \gamma$ with $F(\gamma) = F(\alpha, \beta)$. Thus

$[F(\gamma):F] \leq n \Rightarrow F(\gamma) = F(\alpha)$. 

Now, $K = F(x)$ is the splitting field of the separable poly $m_x, F(x)$. So

$$|G| = |\text{Aut}(K/F)| = [K:F] = n. \leq 161.$$ 

Thus $[K:F] = 161$ and $G = \text{Aut}(K/F)$.

**Thm:** A finite extension $K/F$ is Galois iff it is the splitting field of a separable poly $f(x) \in F[x]$.

**Pf:** ($\Leftarrow$) Have $|\text{Aut}(K/F)| = [K:F]$, as needed.

($\Rightarrow$) By assumption $|\text{Aut}(K/F)| = [K:F]$.

By last Thm, $K_{\text{Aut}(K/F)} = F$. By the proof of said Thm, $K = F(x)$ and is the splitting field of $m_x, F(x)$, for any $x \in K$ with $[F(x): F]$ maximal.
Cor: If \( G_1 \neq G_2 \) are finite subgroups of \( \text{Aut}(K) \), then \( K_{G_1} \neq K_{G_2} \).

Pf: Suppose \( K_{G_1} = K_{G_2} \). As noted, we have \( \text{Aut}(K/K_{G_1}) = G_i \Rightarrow G_1 = G_2 \).

Next time: Let \( K/F \) be Galois, set \( G = \text{Gal}(K/F) \). There is a bijection

\[
\left\{ \text{subfields } \frac{K}{E} \right\} \leftrightarrow \left\{ \text{subgroups } H \leq G \right\}
\]

Given by

\[
\begin{align*}
K_H & \leftrightarrow H \\
E & \leftrightarrow \text{Elements of } G \text{ fixing } E.
\end{align*}
\]