Lecture 23:

Previously on Math 418:

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

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

Const: G a finite subgp of $\mathrm{Aut}(K)$, $F = K_G$ the fixed field. Then given $\alpha \in K$, the min poly

$$m_{\alpha,F}(x) = \prod (x - \alpha_i) \quad \text{where } G \cdot \alpha = \{\alpha_1, \dots, \alpha_n\}$$

In particular α is alg over F of deg $\leq |G|$.

Today:

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

Focus: K has char 0 or K is finite

Finite Fields:

$K = \mathbb{F}_{p^n}$ = splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. (separable)

Key: $K^\times = (K \setminus \{0\}, \times)$ cyclic.

Pf: By the fund. thm. of finite abelian gps

$$K^\times \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \quad \text{with } n_1 \mid n_2 \mid \cdots \mid n_k$$

[Q: How many have seen this?]

If $k > 1$, then have at least $n_1 + \frac{n_2}{n_1}$ elts with $\alpha^{n_1} = 1$. But then $X^{n_1} - 1$ has more than n_1 roots, a contradiction. ▨

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

Pf: Let $\mathbb{F}_p$ be the char field of K. If γ gen $K^\times$, then $K = \mathbb{F}_p(\gamma)$.

Cor: $K = \mathbb{F}_{p^n}$. Then $\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ is generated by Frobenius $\sigma: K \to K$, $\alpha \mapsto \alpha^p$.

Pf: Since K is the splitting field of the separable poly $X^{p^n} - X$, have $|\mathrm{Aut}(K/\mathbb{F}_p)| = |K : \mathbb{F}_p| = n$. Let α gen $K^\times$.

If $\sigma^k = 1$, then $\sigma^k(\alpha) = \alpha^{p^k} = \alpha$

Frob. $\Rightarrow \alpha^{p^k - 1} = 1 \Rightarrow k \geq n$. So $|\sigma| = n$

$\Rightarrow \mathrm{Aut}(K/\mathbb{F}_p) = \langle \sigma \rangle$. ▨

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

Pf: Assume $\mathrm{char}(K) = 0$ 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, $K = F(\alpha)$ is the splitting field/F of the separable poly $m_{\alpha,F}(x)$. So

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

Thus $[K:F] = |G|$ and $G = \mathrm{Aut}(K/F)$. ▨

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 $|\mathrm{Aut}(K/F)| = [K:F]$, as needed.

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

By last Thm, $K_{\mathrm{Aut}(K/F)} = F$. By the proof of said Thm, $K = F(\alpha)$ and is the splitting field of $m_{\alpha,F}(x)$, for any $\alpha \in K$ with $[F(\alpha):F]$ maximal. ▨

Cor: If $G_1 \neq G_2$ are finite subgroups of $\mathrm{Aut}(K)$, then $K_{G_1} \neq K_{G_2}$.

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

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

$$\left\{ \begin{array}{c} \text{subfields:} \\ E \end{array} \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ H \leq G \end{array} \right\}$$

Given by

$$K_H \longleftarrow H$$

$$E \longrightarrow \text{Elements of } G \text{ fixing } E.$$