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 when f is separable.

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

Construction: G a finite subgroup of $\mathrm{Aut}(K)$, $F = K_G$ the fixed field. Then the min poly for $\alpha \in K$ is

$$m_{\alpha,F}(x) = \prod (x - \alpha_i) \quad \text{where } G\cdot\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

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

Today:

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

Focus: K has char 0 or K is finite.

Finite Fields: $K = \mathbb{F}_{p^n}$ = splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.

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

Pf: By the fundamental thm of finite abelian groups:

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

[How many have seen this?]

If $k > 1$, then have at least $n_1 + \frac{n_2}{n_1}$ elements with $\alpha^{n_1} = 1$. [Namely all of $\mathbb{Z}/n_1$ and the subgp of $\mathbb{Z}/n_2$ generated by $\frac{n_2}{n_1}$] But then $X^{n_1} - 1$ has more than n_1 roots in K, a contradiction. $\square$

Cor: Any extension K/F with K finite is simple.

Pf: Let γ be a generator of $K^\times$. Then $K = F(\gamma)$. $\square$

Cor: $K = \mathbb{F}_{p^n}$. Then $\mathrm{Aut}(K) = \mathrm{Aut}(K/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ with a generator being the Frobenius map $\sigma : K \to K$ where $\sigma(\alpha) = \alpha^p$.

<u>Pf</u>: 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 γ generate $K^\times$. If $\underset{\uparrow \text{Frobenius}}{\sigma^k} = 1$, then $\sigma^k(\gamma) = \gamma^{p^k} = \gamma \Rightarrow \gamma^{p^k - 1} = 1 \Rightarrow k \geq n$. So $|\sigma| = n$

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

<u>Thm</u>: G a finite subgp of $\mathrm{Aut}(K)$. Then $[K : K_G] = |G|$.

<u>Pf</u>: Assume $\mathrm{char}(K) = 0$ or K is finite. Set $F = K_G$.

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

<u>Claim</u>: $K = F(\alpha)$.

Suppose $\beta \in K$. Then $[F(\alpha, \beta) : F] \leq n^2 < \infty$ and so $\exists \gamma$ with $F(\gamma) = F(\alpha, \beta)$. Thus $[F(\gamma) : F] \leq n$ $\Rightarrow F(\gamma) = F(\alpha)$. Thus $\beta \in F(\alpha)$, proving the claim.

Now $K = F(\alpha)$ is the splitting field$/F$ of

$$m_{\alpha,F}(x) = \prod (x-\alpha_i) \quad \text{where} \quad G\cdot\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$$

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

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

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

<u>Pf</u>: ($\Leftarrow$) Have $|\mathrm{Aut}(K/F)| = [K:F]$, as needed.

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

By last thm, $[K : K_{\mathrm{Aut}(K/F)}] = |\mathrm{Aut}(K/F)|$

and so must have $K_{\mathrm{Aut}(K/F)} = F$. By the proof of said thm, K is the splitting field of a separable poly over $K_{\mathrm{Aut}(K/F)}$, as needed. $\square$

<u>Cor</u>: If $G_1 \neq G_2$ are finite subgps of $\mathrm{Aut}(K)$, then $K_{G_1} \neq K_{G_2}$.

<u>Pf</u>: As noted, we have $\mathrm{Aut}(K/K_{G_i}) = G_i$ where note both sides are subgps of $\mathrm{Aut}(K)$. $\square$

<u>Next time</u>: Let K/F be Galois, set $G = \mathrm{Gal}(K/F)$.

There is a bijection

$$\left\{ \text{Subfields } E \quad \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgps} \\ H \leq G \end{array} \right\}$$

Given by

$$K_H \longleftarrow\!\!\shortmid \; H$$

$$E \;\shortmid\!\!\longrightarrow \; \begin{array}{l} \text{Elements } \sigma \in G \\ \text{which fix } E. \end{array}$$