Lecture 22:

Last time:

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

[Will take a diff. path through the proof of the Fund. Thm. of Galois Theory, focusing on when char = 0]

Thm: K/F a finite extension where $\mathrm{char}(F) = 0$.
Then $\exists\, \gamma \in K$ with $K = F(\gamma)$. [Go to cor]

Pf: Have $K = F(\alpha_1, \dots, \alpha_n)$. Conducting on the number of α_n, see it suffices to consider $K = F(\alpha, \beta)$.

Let $f(x) = m_{\alpha,F}$, $g(x) = m_{\beta,F}(x)$. Let $S \supseteq K$ be the splitting field of $f(x) \cdot g(x)$. Let $\alpha_1, \dots, \alpha_m \in S$ be the roots of f, and $\beta_1, \dots, \beta_n \in S$ the roots of g. Let $\gamma = c\alpha + \beta$ for $c \in F$.

Claim: For most c, have $K = F(\gamma)$.

Let $L = F(\gamma)$.

Need: $\alpha \in L \Rightarrow \beta \in L \Rightarrow K = F(\alpha, \beta) = F(\gamma)$.

Will show this by calc $m_{\alpha, L}(x)$. Start with noting that f and $h(x) = g(\gamma - cx) \in L[x]$ have α as a root. So $m_{\alpha, L}(x)$ divides both f and h in $L[x]$. If $m_{\alpha, L}(x) \neq x - \alpha$, then $m_{\alpha, L}(x)$ has a second root $\delta \neq \alpha$ (as char $= 0$). Then $f(\delta) = h(\delta) = 0$. The roots of h are

$$\delta_i = \frac{\gamma - \beta_i}{c} = \frac{c\alpha + \beta - \beta_i}{c} = \alpha + \frac{\beta - \beta_i}{c}$$

So, if $\delta_i = \alpha_j \neq \alpha$, then $c = \dfrac{\alpha_j - \alpha}{\beta - \beta_i}$

Thus if we avoid these finitely many pos,

then $m_{\alpha, L}(x) = x - \alpha \Rightarrow \alpha \in L$

$\Rightarrow K = F(\gamma)$.

Cor: K/F a finite ext. of char 0 fields

Then $|\mathrm{Aut}(K/F)| \leq [K:F]$. (true for any char)

Pf: Let $K = F(\gamma)$, and let $f(x) = m_{F,\gamma}(x)$.

Consider the roots $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_k$ of f in K.

Any σ in $\mathrm{Aut}(K/F)$ takes γ to some γ_i,

and if $\sigma(\gamma) = \tau(\gamma)$ then $\sigma = \tau$. So

$$|\mathrm{Aut}(K/F)| = |\#\gamma_K| \leq \deg f = [K:F]. \qquad \blacksquare$$

Goal: $G \leq \mathrm{Aut}(K)$ a finite subgroup.

$$K_G = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$$

Thm: $[K:K_G] = |G|$. Thus $G = \mathrm{Aut}(K/K_G)$

and K/K_G is Galois.

To prove the Thm, we first explore finding min polys

Setup: K with $G \leq \mathrm{Aut}(K)$ (G finite), Let $F = K_G$.

Given $\alpha \in K$, what is $m_{\alpha,F}(x) \in F[x]$?

Now

$$G\alpha = \{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

($\alpha_1 = \alpha$; the α_i are distinct)

consists of roots of $m_{\alpha,F}(x)$. So set

$$f(x) = \prod_i (x - \alpha_i)$$

If $f(x) \in F[x]$, then $m_{\alpha,F}(x) \mid f(x)$. As each α_i is also a root of $m_{\alpha,F}(x)$, must have $m_{\alpha,F}(x) = f(x)$ since the α_i are distinct.

If $\tau \in G$, then $\tau(\alpha_i) = \tau(\sigma(\alpha)) = (\tau\sigma)(\alpha) = \alpha_j$

So τ just permutes the α_i.

cf $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_i \in K$,

then

$$\tau(f(x)) = \tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0)$$

$$= \tau\left(\prod (x - \alpha_i)\right) = \prod (x - \tau(\alpha_i))$$

$$= \prod (x - \alpha_i) = f(x) = a_n x^n + \cdots + a_0$$

Thus: $\tau(a_i) = a_i$ for <u>each</u> τ. Thus

$a_i \in F = K_6$. So $f(x) = F[x]$ and is $m_{\alpha, F}(x)$.

7