Lecture 36: Foundations of Galois Theory §14.2-3 of [DF].

Previously... $H \leq \mathrm{Aut}(K)$ $K_H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$.

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

Def: A finite K/F is Galois when $|\mathrm{Aut}(K/F)| = [K:F]$.

Ex: splitting field of a separable poly.

Key facts: [Will not show all of these today.]

Thm A: For finite K/F, have $|\mathrm{Aut}(K/F)| \leq [K:F]$.

Thm B: For K/F finite, the following are equivalent:

① K/F is Galois, i.e. $|\mathrm{Aut}(K/F)| = [K:F]$.

② K is the splitting field of a separable $f \in F[x]$.

[③ $K_{\mathrm{Aut}(K/F)} = F$.

Skip!

Contrast for ③: $K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$
so $\mathrm{Aut}(K/F) = \{id\}$ and $K_{\{id\}} = K$, not F.]

[We don't have time to prove these (or some other parts of the Fund. Thm of Galois Theory) completely. Will focus on when char $= 0$.]

Lemma: Suppose K/F is finite with char $K = 0$. Then $K = F(\alpha)$ for some α.

Pf: Suppose $K = F(\alpha_1, \ldots, \alpha_n)$. Inducting on n, suffices to consider $K = F(\alpha, \beta)$. Set $f = m_{\alpha,F}(x)$ and $g = m_{\beta,F}(x)$. Let $S \supseteq K$ be the splitting field for $f \cdot g$. Let $\alpha_i \in S$ be the roots of f and $\beta_j \in S$ the roots of g. [Skip proof of claim]

Claim: For most $c \neq 0$ in F, have $F(\underbrace{c\alpha + \beta}_{\gamma}) = K$

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

Will do by calculating $m_{\alpha,L}(x)$. Start by noting that $f(x)$ and $h(x) := g(\gamma - cx) \in L[x]$ both have α as 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 $\delta \neq \alpha$ in S, as char $= 0$ implies all irred. polys are separable.

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 $c = \dfrac{\beta - \beta_i}{\alpha_j - \alpha}$. Thus if we avoid finitely many possible c, then $m_{\alpha, L} = X - \alpha \Rightarrow \alpha \in L \Rightarrow K = F(\gamma)$. ▨

<u>Pf of Thm A when K is simple</u> (e.g. char $K = 0$).

Have $K = F(\gamma)$ and set $f = m_{\gamma, F}(x) \in F[X]$.

Any $\sigma \in \mathrm{Aut}(K/F)$ is determined by $\sigma(\gamma)$, where $\sigma(\gamma)$ must be a root of f. So

$$|\mathrm{Aut}(K/F)| \leq |\text{roots of } f| \leq \deg f = [K:F].$$ ▨

<u>Thm C</u>: Suppose $G \leq \mathrm{Aut}(K)$ is finite. Then $[K : K_G] = |G|$ and $G = \mathrm{Aut}(K/K_G)$ and K/K_G is Galois.

[<u>Note</u>: The other claims follow from $[K:K_G] = |G|$ since $G \leq \mathrm{Aut}(K/K_G)$ and $|\mathrm{Aut}(K/K_G)| \leq [K:K_G] = |G|$ by Thm A.

SKIP!]

<u>Tool</u>: In setting of thm, set $F = K_G$.

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

distinct.

Now $G\cdot\alpha = \{\sigma(\alpha) \mid \sigma \in G\} = \{\overset{\alpha}{\overset{\shortparallel}{\alpha_1}}, \dots, \alpha_n\}$

are roots of $m_{\alpha,F}$. So set

$$f(x) = \prod_i (x - \alpha_i) \in K[x]$$

<u>Claim</u>: $f \in F[x]$. This gives $m_{\alpha,F} \mid f$ as $f(\alpha) = 0$

$\Rightarrow m_{\alpha,F} = f$ as each α_i is a root of $m_{\alpha,F}$ and the α_i are distinct.

Each $\tau \in G$ gives an auto of $K[x]$ by acting on the coeffs. Note

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

Since τ just permutes the elts of the orbit $G\cdot\alpha$. Hence $\tau(a_i) = a_i$ for each coeff of $f \Rightarrow f \in F[x]$.

Pf of Thm C when char = 0: Set $F = K_G$.

Know every $\alpha \in K$ is alg$/_F$ of deg $\leq |G|$.

Choose $\alpha \in K$ to have maximal deg$/_F = n$.

Claim: $K = F(\alpha)$

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 of

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

$$\text{So } |G| \leq |\mathrm{Aut}(K/_F)| \underset{\substack{\uparrow \\ \text{as splitting field}}}{=} [K:F] = n \leq |G|.$$

Thus $[K:F] = |G|$ and $G = \mathrm{Aut}(K/_F)$, and so $K/_F$ is Galois. $\blacksquare$