Lecture 22: Primitive extensions and minimal polys.

Previously: 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.

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

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

Ex: $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$; $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Cor: K/F finite with $\mathrm{char}(F) = 0$. Then $|\mathrm{Aut}(K/F)| \leq [K:F]$. (True for any char.)

Pf of Cor: Let $K = F(\gamma)$ and set $f = m_{\gamma,F}(x)$. Let $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_k$ be the roots 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

$$|\mathrm{Aut}(K/F)| = |\{\gamma_i\}| \leq \deg f = [K:F]. \quad \square$$

Pf of Thm: Suppose $K = F(\alpha_1, \dots, \alpha_n)$. Inducting on n, it suffices to consider $K = F(\alpha, \beta)$.

Set $f = m_{\alpha, F}(x)$, $g = m_{\beta, F}(x)$. 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 $\beta_1, \dots, \beta_n \in S$ be the roots of g.

Set $\gamma = c\alpha + \beta$ for $c \in F$ with $c \neq 0$.

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

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

Will do 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 $m_{\alpha, L}$ divides both f and h in $L[x]$. If $m_{\alpha, L} \neq x - \alpha$, then $m_{\alpha, L}$ 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 $c = \dfrac{\beta - \beta_i}{\alpha_j - \alpha}$. Thus if we avoid these finitely many pos. for c, then $m_{\alpha, L} = X - \alpha \Rightarrow \alpha \in L \Rightarrow K = F(\gamma)$. ▨

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

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

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

As an aide to proving this, we first explore finding min polys.

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

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

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 $m_{\alpha, F}$. So set:

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

If $f \in F[x]$, then $m_{\alpha,F} \mid f$ in $F[x]$.

As each α_i is also a root of $m_{\alpha,F}$, must have $m_{\alpha,F} = f$ as 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_j.

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

$$\begin{aligned}\tau(f(x)) &= \tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0) \\ &= \tau\left(\prod(x-\alpha_i)\right) = \prod\left(x - \tau(\alpha_i)\right) \\ &= \prod(x-\alpha_i) = f = a_n x^n + \cdots + a_0.\end{aligned}$$

So: $\tau(a_i) = a_i$ for all $\tau \in G$. Thus $a_i \in F = K_G$.

So $f \in F[x]$ and hence is $m_{\alpha,F}(x)$. ▨

Ex: $\mathbb{Q}(\sqrt{2}, i)$ has $G = \mathrm{Aut}\left(\mathbb{Q}(\sqrt{2}, i)/_2\right) = \{1, \sigma, \tau, \sigma\tau\}$

where $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(i) = i$ and $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(i) = i$

Then if $\alpha = i + \sqrt{2}$, then $G \cdot \alpha = \{\underset{\alpha_1}{\sqrt{2}+i}, \underset{\alpha_2}{-\sqrt{2}+i}, \underset{\alpha_3}{\sqrt{2}-i}, \underset{\alpha_4}{-\sqrt{2}-i}\}$

So $m_{\alpha,\mathbb{Q}}(x) = \prod(x-\alpha_i) = x^4 - 2x^2 + 9$.