Lecture 11: Galois closure

Aim Lecture: Show separable ext^{n} can be embedded in Galois ext^{n} & so studied via Galois corresp.

Galois Closure

Let K/F = finite sep. ext^{n} say gen. by sep. elts $\alpha_1, \ldots, \alpha_n / F$. Let $p_1, \ldots, p_n \in F[x]$ be their min. poly.

Def^{n}: A **Galois closure** for K/F is any splitting field L for $p(x) = p_1(x)p_2(x)\ldots p_n(x) / K$ (for some choice of sep. gen. $\alpha_1, \ldots, \alpha_n$).

Prop^{n} 1: Let L = Galois closure of K/F.

(a) L/F is finite Galois.

(b) Let $\tilde{K}/K$ be a field ext^{n} with $\tilde{K}/F$ Galois. Then there's a field hom$_F$ $\varphi: L \to \tilde{K}$.

(c) In particular, Galois closures are unique up to isom. $/F$.

Proof: (a) Note L is also splitting field of $p(x)/F$.

(b) Let L = splitting field of $p(x)$ above. Now Lect. 2 Thm $\Rightarrow$ $p(x)$ factorises into linears $/\tilde{K}$ so $\tilde{K}$ contains a splitting field $L \subseteq \tilde{K}$ for $p(x)/F$.

Uniqueness of splitting fields

Lect. 4 Thm $\Rightarrow \exists$ isom $\varphi: L \xrightarrow{\sim} \tilde{L}$ over F.

ⓒ Let $\tilde{L}$ be another Galois closure. Now ⓑ $\Rightarrow$ there's a field hom / F $\varphi: L \to \tilde{L}$. As φ inj. suffice show surj. by proving $[L:F] \overset{(*)}{\geq} [\tilde{L}:F]$. But ⓑ $\Rightarrow$ there's also a field hom. $\psi: \tilde{L} \to L$ over F so $(*)$ holds

□

E.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is finite separable but not Galois $\because |\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 \neq [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$.

It's Galois closure is the splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega = e^{2\pi i/3})$ of $x^3 - 1 / \mathbb{Q}$.

Galois Closures of Radical Ext^{n}s

Observation: Let K/F = field ext^n, $\sigma \in \mathrm{Aut}K$ & $\alpha \in K$ be s.t. $\alpha^m \in F$ for some positive $m \in \mathbb{Z}$. Then $\sigma(\alpha)$ is an m-th root of an elt of $\sigma(F)$.

Prop^{n} 2: The Galois closure L of a radical ext^{n} K/F is radical $/F$.

Proof: Consider a radical tower

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \ldots \subseteq F(\alpha_1, \ldots, \alpha_n) = K$$

with $\alpha_i^{m_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$.

Let $Gal(L/F) = \{1, \sigma_1, \ldots, \sigma_m\}$.

Observation $\Rightarrow$ we get following radical tower for L

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \sigma_1(\alpha_1)) \subseteq \ldots \subseteq F(\alpha_1, \sigma_1(\alpha_1), \ldots, \sigma_m(\alpha_1))$$

$$\subseteq F(\alpha_1, \sigma_1(\alpha_1), \ldots, \sigma_m(\alpha_1), \alpha_2)$$

$$\subseteq F(\alpha_1, \sigma_1(\alpha_1), \ldots, \sigma_m(\alpha_1), \alpha_2, \sigma_1(\alpha_2))$$

$$\vdots$$

$$\subseteq F(\alpha_1, \sigma_1(\alpha_1), \ldots, \alpha_n, \ldots, \sigma_m(\alpha_n)) = L$$

□

Primitive Element Thm

Thm-Def^{n}: Let K/F = finite sep. ext^{n}. Then $K = F(\alpha)$ for some $\alpha \in K$. We call α a primitive element for K/F.

Proof: If F finite, so is K & K^* is cyclic by Lect. 8 Thm. We can

pick α to be a gen. for K^*.

Suppose F infinite. Pick $\alpha \in K$ with $[F(\alpha):F]$ max. We argue by contradiction & assume $K \neq F(\alpha)$ so $\exists\ \beta \in K - F(\alpha)$.

Now K/F has finitely many interm. fields $\therefore$ same is true for Galois closure L/F by Galois corresp.

$\therefore |F| = \infty$ & pigeon-hole principle $\Rightarrow$ $\exists$ distinct $c_1, c_2 \in F$ with $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$

$$F(\alpha + c_1\beta) \ni \frac{(\alpha + c_1\beta) - (\alpha + c_2\beta)}{c_1 - c_2} = \beta$$

$$\Rightarrow F(\alpha + c_1\beta) \ni \alpha$$

$\therefore F(\alpha + c_1\beta) \supsetneq F(\alpha)$ contradicting max. of $[F(\alpha):F]$.

□

Eg. $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ Galois with Galois group $G = \langle (12), (34) \rangle$

$\sqrt{2} \leftrightarrow -\sqrt{2}$ $\sqrt{3} \leftrightarrow -\sqrt{3}$

Interm. fields

$\mathbb{Q}(\sqrt{2},\sqrt{3})$

$\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(\sqrt{3})$ $\mathbb{Q}(\sqrt{6})$

$\mathbb{Q}$

$\therefore$ Any elt not in $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}) \cup \mathbb{Q}(\sqrt{6})$ is a primitive elt.