Lecture 9: Constructing Splitting Fields & their Automorphisms

Aim Lecture Construct autom. of K/F to calculate $G = Gal(K/F)$ & ensure G big enough to extract info.

Symbolic Adjunction of Roots

Rem: Let $\sigma: F \to F'$ be a field hom. Then $\ker \sigma \lhd F$ trivial. Now $\sigma(1) = 1 \Rightarrow \ker \sigma = 0$ ie. σ is inj.
1st isom. thm $\Rightarrow F \simeq \sigma(F) \subset F'$ so identifying $F \& \sigma(F)$, we can view F' as a field ext^n of F.

Prop^n 1: Let F = field, $p(x) \in F[x]$ irred.
(a) $K = F[x]/\langle p(x) \rangle$ is a field so rem. $\Rightarrow$ composite ring hom $F \to F[x] \to K$ makes K a field ext^n of F.
(b) $K = F(\alpha)$ where $\alpha = x + \langle p(x) \rangle$ is a root of $p(x)$. ie. we "symbolically" adjoined a root of $p(x)$ to F.

Proof: (a) $p(x)$ irred $\Rightarrow \langle p(x) \rangle \lhd F[x]$ max $\Rightarrow$ $F[x]/\langle p(x) \rangle$ a field.
(b) Let $f(x) = \sum a_i x^i$.

Then $f(\alpha) = \sum a_i \alpha^i = \sum a_i x^i + \langle p(x) \rangle = f(x) + \langle p(x) \rangle$

Hence $p(\alpha) = p(x) + \langle p(x) \rangle = 0_K$ & $K = F(\alpha)$

Constructing Automorphisms

Prop^n 2: Let $\sigma : F \to F'$ be a field isom. Let $p(x) \in F[x]$ be irred & α (resp α') be a root of $p(x)$ (resp. $(\sigma p)(x)$) in appropriate field ext^n's

Then there's a unique field isom.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\tilde{\sigma}} & F'(\alpha') \\ \uparrow & \curvearrowright & \uparrow \\ F & \xrightarrow{\sigma} & F' \end{array} \quad \text{s.t.}$$

(a) $\tilde{\sigma}$ extends σ ie. $\tilde{\sigma}(\beta) = \sigma(\beta)$ $\forall \beta \in F$.

(b) $\tilde{\sigma}(\alpha) = \alpha'$.

Proof: $\tilde{\sigma}$ is just composite of field isom,

$$F(\alpha) \xrightarrow[\text{Thm}]{\text{Ld.1}} \frac{F[x]}{\langle p(x) \rangle} \xrightarrow{\sigma[x]} \frac{F'[x]}{\langle (\sigma p)(x) \rangle} \xrightarrow{\sim} F'(\alpha')$$

$$\alpha \longmapsto x + \langle p(x) \rangle \longmapsto x + \langle (\sigma p)(x) \rangle \longmapsto \alpha'$$

$$F \ni \beta \longmapsto \beta + \langle p(x) \rangle \longmapsto \sigma(\beta) + \langle (\sigma p)(x) \rangle \longmapsto \sigma(\beta)$$

□

Eg. Let $\omega = e^{2\pi i/3}$ so

$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$

is a splitting field for $x^3 - 2 / \mathbb{Q}$.

Lect. 3 cor. $\Rightarrow$ $G = Gal(K/\mathbb{Q}) \xrightarrow{\cong} S_3$

Note τ = conjug^n swaps $\sqrt[3]{2}\omega \leftrightarrow \sqrt[3]{2}\omega^2$

so (23) is "in" G.

Prop^{n} 2 $\Rightarrow$ $\exists$ isom. /F $\sigma: \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega)$
which maps $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$

Prop^{n} 2 again $\Rightarrow$ $\exists$ isom. / $\mathbb{Q}$
$\tilde{\sigma}: K = [\mathbb{Q}(\sqrt[3]{2})](\omega) \longrightarrow [\mathbb{Q}(\sqrt[3]{2}\omega)](\omega)$
which extends σ & maps $\omega \mapsto \omega$.
$\therefore$ $\tilde{\sigma}: \sqrt[3]{2} \longmapsto \sqrt[3]{2}\omega$ corresponds to (1 2 3).
$\sqrt[3]{2}\omega^2$

Identifying G with subgroup $\tau(G) \leq S_3$
see $G \geq \langle (23), (123) \rangle = S_3$ i.e.
$Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \simeq S_3$.

Existence & Uniqueness of Splitting Fields

Thm: Let F = field, $f(x) \in F[x]$ of degree $n > 0$,
(a) There exists a splitting field K for $f(x)$ /F.
(b) Any two are isomorphic /F.

Proof: (a) by induction on n. When $n = 1$, $K = F$.
Let $g(x) \in F[x]$ be an irred. factor of $f(x)$. Prop^{n} 1 $\Rightarrow$ $\exists$ simple field ext^{n} $F(\alpha)/F$ with α a root of $g(x)$.

Factor thm $\Rightarrow f(x) = (x-\alpha) f_1(x)$,
where $f_1(x) \in F(\alpha)[x]$.
Inductive hypothesis $\Rightarrow \exists$ splitting field $F(\alpha, \alpha_1, \ldots, \alpha_{n-1})$ for $f_1(x)/F(\alpha)$.
It is a splitting field for $f(x)/F$.

(b) ex. Hint: Use induction on $[K:F]$ & Prop^{n} 2 to prove
Any field isom. $\sigma: F \to F'$ can be extended to a field isom
$\tilde{\sigma}: K \to K'$ where K, K' are splitting fields of $f(x)$ & $(\sigma f)(x)$.