Lecture 3: Galois Group

Aim Lecture: Intro. Galois group which is optimal group of field autom. to study field ext^{n} K/F.

Field Homomorphisms / F

Let K, K' = field ext^{n}s of F

Prop^{n}-Def^{n} 1: A field hom $\sigma: K \to K'$ fixes F or is a field hom. over F if $\sigma(\alpha) = \alpha$ for all $\alpha \in F$. Such an hom. is linear / F.

If $K = K'$ & σ an isom., we say σ is an automorphism of K/F.

Proof: Note σ additive & for $\alpha \in F$ $\gamma \in K$, $\sigma(\alpha\gamma) = \sigma(\alpha)\sigma(\gamma) = \alpha\sigma(\gamma)$ ∴

Eg. 1. $\sigma: \mathbb{C} \to \mathbb{C} : z \mapsto \bar{z}$ is an autom. of $\mathbb{C}/\mathbb{R}$ ∵ $x \in \mathbb{R} \Rightarrow \bar{x} = x$.

Prop^{n}-Def^{n} 2: Let K/F = field ext^{n} & $Gal(K/F)$ = set of autom. of K/F.

(a) Then $G = Gal(K/F) < Aut\ K$ called the Galois group of K/F

(b) $F \subseteq K^{G}$.

Proof: ⓐ Check closure axioms e.g.

$\alpha \in F \Rightarrow (\sigma_1 \sigma_2)(\alpha) = \sigma_1(\sigma_2(\alpha)) = \sigma_1(\alpha) = \alpha$

$\sigma_1, \sigma_2 \in G$ (each fixes F pointwise)

$\Rightarrow \sigma_1 \sigma_2 \in G$

ⓑ by def^n.

Field Automorphisms as Permutations of Roots

Let F = field.

Lemma 1: Let $\sigma: K \to K'$ be a field hom. / F. Let $\alpha \in K$ be a root of $f(x) \in F[x]$. Then $\sigma(\alpha)$ is a root of $f(x)$.

Proof: Let $f(x) = \sum a_i x^i$.

$$f(\sigma(\alpha)) = \sum a_i \sigma(\alpha)^i = \sum \sigma(a_i)\sigma(\alpha)^i$$

$$= \sigma\left(\sum a_i \alpha^i\right)$$

$$= \sigma(f(\alpha)) = \sigma(0) = 0.$$

Eg. 2. $G := Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$

Why? Let $\sigma \in G$, $\sqrt[3]{2}$ is only root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.

We can write $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ as

$$\alpha = \alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_1 \sqrt[3]{2^2}$$

$$\sigma(\alpha) = \sigma(\alpha_0) + \sigma(\alpha_1)\,\sigma(\sqrt[3]{2}) + \sigma(\alpha_2)\,\sigma(\sqrt[3]{2})^2$$

$$= \alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_2 (\sqrt[3]{2})^2$$

$= \alpha \implies \sigma = 1$

This argument shows

Scholium: Any field hom $\sigma : F(\alpha_1, \ldots, \alpha_n) \to K$ over F is determined completely by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

Why? Every elt. of $F(\alpha_1, \ldots, \alpha_n)$ can be expressed as a rational fn of $\alpha_1, \ldots, \alpha_n$.

Galois groups of splitting fields

Rem: $\mathrm{Gal}(K/F)$ only useful if it's big enough. Lemma 1 $\implies$ better include all roots of a poly.

Def^n: Let $f(x) \in F[x]$. A field ext^n K of F is a splitting field for $f(x)/F$ if (a) $f(x)$ factorises into linears $/K$ & (b) $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in K

i.e. K is gen. by "all" roots of $f(x)$.

Eg. 3. $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{-2\pi i/3})$ is splitting field of $x^3 - 2 / \mathbb{Q}$.

Corollary: With above notn, any $\sigma \in Gal(K/F)$ permutes the roots $\alpha_1, \ldots, \alpha_n$ by lemma 1 so scholium $\Rightarrow$ we have an injective grouphom

$$Gal(K/F) \hookrightarrow Perm\{\alpha_1, \ldots, \alpha_n\} \simeq S_n.$$

Eg. 1 again $\mathbb{C}$ = splitting field of $x^2+1/\mathbb{R}$

$\therefore Gal(\mathbb{C}/\mathbb{R}) \hookrightarrow Perm\{i, -i\} \simeq S_2$

$$id \longmapsto id$$
$$conj \longmapsto \text{swap } i \leftrightarrow -i$$

$\Rightarrow Gal(\mathbb{C}/\mathbb{R}) \simeq S_2 \simeq \mathbb{Z}/2.$

Eg. 4. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ = splitting field of $(x^2-2)(x^2-3)$ over $\mathbb{Q}$.

$\sigma \in Gal(K/\mathbb{Q})$ permutes roots of x^2-2 & x^2-3 i.e.

$\sigma: \sqrt{2} \longmapsto \pm\sqrt{2}$, $\sqrt{3} \longmapsto \pm\sqrt{3}$.

$-\sqrt{2} \longmapsto \mp\sqrt{2}$, $-\sqrt{3} \longmapsto \mp\sqrt{3}$

Labelling roots $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ as S_4 1, 2, 3, 4 see

$$Gal(K/\mathbb{Q}) \hookrightarrow \{1, (12), (34), (12)(34)\} \simeq \mathbb{Z}/2 \times \mathbb{Z}/2.$$

We saw in lect. 2 that all 4 permutations on right come from autom. of $K/\mathbb{Q}$