The Galois Group

II: How are elements in $\mathrm{Gal}(E/F)$ created?

Last time

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(f) = f \ \ \forall f \in F\}$$

ie, $\sigma \in \mathrm{Gal}(E/F)$ iff $\sigma|_F = \mathrm{id}_F$

Lemma If $\sigma \in \mathrm{Gal}(E/F)$ and $f(x) \in F[x]$ has $f(\alpha) = 0$ for $\alpha \in E$, Then $f(\sigma(\alpha)) = 0$ too.

ie, automorphisms permute roots of F-polynomials

Cor If $f(x) \in F[x]$ has n distinct roots and E is its splitting field, then $Gal(E/F) \leq S_n$.

Building on groundwork from Gabby & Rachel

Cor (Order of Galois group for splitting field) If E is a splitting field of $f(x) \in F[x]$, Then

$$|Gal(E/F)| = [E:F].$$

seperable

This is Theorem 51 applied $id_F : F \to F$


NEW
STUFF

NEW

STUFF

Lemma If $E = F(\alpha_1, \dots, \alpha_n)$ for algebraic elements $\alpha_1, \dots, \alpha_n$, Then an element $\sigma \in Gal(E/F)$ is determined by its action on $\alpha_1, \dots, \alpha_n$.

Ie, if we know the values $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$, Then we know how σ acts on any $e \in E$.

Pf An F-basis for E is given by

$$\left\{ \alpha_1^{e_1} \cdots \alpha_n^{e_n} : 0 \le e_i < \partial\left(\operatorname{irr}_{F(\alpha_1, \dots, \alpha_{i-1})}^{(\alpha_i)} \right) \right\}$$

(This is an extension of the ideas that Gabby gave us in the proof of the degree formula.)

This means that every element $e \in E$ can be expressed uniquely as an F-combination of this basis:

$$e = \sum_{\text{all exponents}} f_{e_1,\dots,e_n} \alpha_1^{e_1} \cdots \alpha_n^{e_n}.$$ Hence

So we get $\sigma(e) = \sigma\left(\sum_{\text{all exponents}} f_{e_1,\dots,e_n}\, \alpha_1^{e_1} \cdots \alpha_n^{e_n}\right)$

$$= \sum_{\text{all exponents}} \sigma\left(f_{e_1 \cdots e_n}\, \alpha_1^{e_1} \cdots \alpha_n^{e_n}\right)$$

$$= \sum_{\text{all exponents}} \sigma(f_{e_1 \cdots e_n})\, \sigma(\alpha_1)^{e_1} \cdots \sigma(\alpha_n)^{e_n}$$

$$= \sum f_{e_1 \cdots e_n}\, \sigma(\alpha_1)^{e_1} \cdots \sigma(\alpha_n)^{e_n}.$$

Ex What is $Gal(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ where

$\alpha_1 = \sqrt[3]{2}$?

Notation: $\text{irr}_{\mathbb{Q}}(\alpha_1) = x^3 - 2$ (you saw this on HW6)

other roots: $\alpha_2 = \omega\sqrt[3]{2}$ and $\alpha_3 = \omega^2\sqrt[3]{2}$

where $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ and $\omega^2 = \frac{-1-\sqrt{-3}}{2} = \overline{\omega}$

Note: ω is a "3rd root of unity" since $\omega^3 = 1$.

On homework 6 you show that $\alpha_2, \alpha_3 \notin \mathbb{Q}(\alpha_1)$.

Note $\sigma \in Gal(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ has $\sigma(\alpha_1) \in \{\alpha_1, \alpha_2, \alpha_3\}$.

On the other hand, we know $\sigma \in Aut(\mathbb{Q}(\alpha_1))$

and hence $\sigma(\alpha_1) \in \mathbb{Q}(\alpha_1)$.

Hence $\sigma(\alpha_1) = \alpha_1$.

Note a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha_1)$ is $\{1, \alpha_1, \alpha_1^2\}$

and by our last result we know that a given $\sigma \in Gal(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ is determined by its action on α_1.

Here any $\sigma \in Gal(\mathbb{Q}(\alpha_1)/\mathbb{Q})$ must be $id_{\mathbb{Q}(\alpha_1)}$

$$\begin{aligned}\sigma(e) &= \sigma(q_1 \cdot 1 + q_2 \cdot \alpha_1 + q_3 \cdot \alpha_1^2) \\ &= \sigma(q_1)\sigma(1) + \sigma(q_2)\sigma(\alpha_1) + \sigma(q_3)\sigma(\alpha_1)^2 \\ &= q_1 \cdot 1 + q_2 \cdot \alpha_1 + q_3 \cdot \alpha_1^2 = e.\end{aligned}$$

So: $\mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q}) = \{id_{\mathbb{Q}(\alpha_1)}\}$.

Note: This doesn't contradict our result that $|\mathrm{Gal}(E/F)| = [E:F]$ because this result applies only to splitting fields.

We actually find that $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ is <u>not</u> a splitting field.