Abstract Algebra
: Lecture 19

Leo

2024.12.05

E ↖ roots.
| f(x) ∈ F[x].
F.

Definition 1. *Let E/F be a finite extension. Let $f(x) \in F[x]$. The smallest subfield of E which contains all of the roots of f is called the splitting field of f over F, or a splitting extension of F.*

Example 2. *Let $F = \mathbb{Q}$, and $f(x) = x^3 - 2 \in F[x]$. Then $\alpha = \sqrt[3]{2}$ is a root of f. Let $K = F(\alpha)$. Is K the splitting field of f over F?* → at most 3 roots.

No, since K does not contain the other roots of f. Let $\beta = \alpha e^{2\pi i/3}$, $\gamma = \alpha e^{4\pi i/3}$ then β, γ are also roots of f. Let $\omega = e^{2\pi i/3}$, the splitiing field of f over F should be $F(\alpha, \omega) = F(\alpha + c\omega)$ for some $c \in \mathbb{Q} - \{0\}$.

Definition 3. *For E/F an automorphism σ of E which fixes F pointwise is called an F-automorphism of E. All automorphism of E which fix F pointwise form a group, called the Galois group of E/F, denoted by $\boxed{Gal(E/F)}$ or $Gal(E : F)$. If E is the splitting field of some $f(x) \in F[x]$, then $Gal(E/F)$ is called the Galois group of f over F, denoted by $Gal(f)$.*

Proposition 4. *Let $F < K \leqslant E$, K is the splitting field of some $f(x) \in F[x]$ over F.*
(1). K is unique; ✓.
(2). Each F-automorphism of E induces an F-automorphism of K. ✓. *Which is due to the fact that σ fixes $f(x)$ and permutes the roots of $f(x)$.*

Example 5. *Let $F = \mathbb{R}$ and $E = \mathbb{C}$. Then E is a splitting field of F and $Gal(E/F)$ is isomorphic to $Z_2 =< \sigma >$ where $\sigma : a + bi \mapsto a - bi$, $a, b \in \mathbb{R}$. Actually, $E \simeq F[x]/(x^2 + 1)$.* $\longrightarrow Gal(\mathbb{C}/\mathbb{R}) \cong <\sigma>$
$\sigma : x \mapsto \bar{x}$.

Example 6. *Let $E = \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$. Then what is the Galois group of $E/\mathbb{Q}$?*
$Z_2 =< \sigma >$. Where $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$, $a, b \in \mathbb{Q}$ since σ fixes x^2-2 $\longrightarrow Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong <\sigma>$
$\sigma : a+b\sqrt{2} \mapsto a-b\sqrt{2}$.

Example 7. *Let $x^3 - 2 \in \mathbb{Q}[x]$. Then the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $E = \mathbb{Q}(\alpha, \omega)$. Then root of $x^3 - 2$ are $\alpha, \omega\alpha, \omega^2\alpha$.* → σ needs to permute them. *Let $\rho : \alpha \mapsto \omega\alpha \mapsto \omega^2\alpha$, $\sigma : \alpha \mapsto \alpha$, $(\omega\alpha, \omega^2\alpha) \mapsto (\omega^2\alpha, \omega\alpha)$. Then $Gal(E/\mathbb{Q}) =< \rho, \sigma >\simeq S_3$.*
$\alpha \mapsto \omega\alpha$, $\omega\alpha \mapsto \omega^2\alpha$. $\omega\alpha \mapsto \omega^2\alpha$, $\omega^2\alpha \mapsto \omega\alpha$.

Example 8. *$E = \mathbb{Q}(\alpha)$* ($\sqrt[3]{2}$) *is not the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let $F = \mathbb{Q}(\omega)$.* ($e^{\frac{2\pi}{3}i}$) *Is $K = F(\alpha)$ the splitting field of $x^3 - 2$ over F? Yes.* ✓.
$Gal(E/\mathbb{Q}) =$? Suppose $\sigma \in Gal(E/\mathbb{Q})$ then let $(2^{1/3})^\sigma = \beta$, we have $2 = 2^\sigma$ (in $\mathbb{Q}$) *$= ((2^{1/3})^3)^\sigma = \beta^3$ i.e. $\beta = 2^{1/3}$ i.e. $\sigma = 1$. Hence $Gal(E/\mathbb{Q}) = 1$.* ✓.
$\alpha \mapsto \alpha$.

$Aut(\mathbb{Q}) = \{Id\}$.
→ Recall: $Aut(\mathbb{R}) = \{id\}$ as field automorphism.

$\mathbb{Q}(w,\alpha)/\mathbb{Q}(\alpha)$.

$\alpha \mapsto \alpha$.

① id.

② $w\alpha \mapsto w^2\alpha \mapsto \alpha$.

③ $w\alpha \mapsto \alpha$

$w^2\alpha \mapsto w\alpha$.

$\underbrace{(\mathbb{Q}(w))(\alpha)}_{}^{\mathbb{Q}(w,\alpha)} / (\mathbb{Q}(w))$. $\alpha \mapsto ?$

① id.

② $\alpha \mapsto w\alpha \mapsto w^2\alpha \mapsto \alpha$.

③ $\alpha \mapsto w^2\alpha \mapsto w\alpha \mapsto \alpha$.

①②③ forms Z_3.

Exercise 9. *What is $Gal(K/F)$? It's Z_3.*

σ need to fix $\mathbb{Q}(w)$ pointwise.

σ is impossible.

Example 10. *Let $L = \mathbb{Q}(\alpha)$, $Gal(E/L) = ?$ It's Z_2.*

$\mathbb{Q}(w\alpha)/\mathbb{Q}(\alpha)$.

Theorem 11. *Let L be a splitting field of $g(x) \in K[x]$. Then for any irreducible polynomial $f(x)$, whenever $f(x)$ has a root in L, then $f(x)$ splits in L.*

L / K. $g(x) \in K[x]$.

$f(x)$'s all roots all lie in L.

证明. Let $L = K(\alpha_1, \ldots, \alpha_n)$, let $f(x) \in K[x]$ be irreducible. Let α, β be two roots of $f(x)$ in L s.t. $\alpha \in L$. We aim to prove $\beta \in L$. $\forall$. ✓. $\Longleftrightarrow [L(\beta) : L] = 1$.

$L(\alpha) = K(\alpha_1, \ldots, \alpha_n)(\alpha) = K(\alpha)(\alpha_1, \ldots, \alpha_n)$, $L(\beta) = K(\alpha_1, \ldots, \alpha_n)(\beta) = K(\beta)(\alpha_1, \ldots, \alpha_n)$. $L(\beta)$ is the splitting field of g on $K(\beta)$ and $L(\alpha)$ is the splitting field of g on $K(\alpha)$. Notice that $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$ and $[K(\alpha) : K] = [K(\beta) : K]$, as α, β are two roots of the irreducible polynomial $f(x) \in K[x]$. $[L(\beta) : L][L : K] = [L(\beta) : K] = [L(\beta) : K(\beta)][K(\beta) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = [L(\alpha) : K] = [L(\alpha) : L][L : K] = [L : K]$. i.e. $[L(\beta) : L] = 1$. ✓. □

E / L / F.

Theorem 12. *Let $F < L < E$. Then L is splititng extension of F iff $Gal(E/L) \lhd Gal(E/F)$.*

证明. next time □

Definition 13. *A splitting extension is callled a normal extension.*

spiliting extension $\Leftrightarrow$ normal extension.

roots.

Example 14. *Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, $g(x) = (x^2 - 2)(x^2 - 3)$, $f(x) = x^4 - 10x^2 + 1$.*

root

(1). Different polynomials may have the same splitiing field. ✓.

(2). $Gal(g) = <\sigma> \times <\tau> \simeq Z_2 \times Z_2$, where $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ and $\tau : \sqrt{3} \mapsto -\sqrt{3}$. $Gal(f) = Z_2 \times Z_2$, they are equal. i.e. Different polynomials may have the same Galois group. But this group acts on the roots of g is not transitive, and acts on the roots of f is transitive, since f is irreducible.

permutes $\sqrt{2}, -\sqrt{2}$.

permutes $\sqrt{3}, -\sqrt{3}$.