Abstract Algebra
: Lecture 20

Leo

2024.12.12

We always assume that our fields is of char=0.

Theorem 1. *Let L be a splitting feild extension of K. Then for any irreducible polynomial $f \in K[x]$, L contains one root of $f(x)$ if and only if L contains all roots of $f(x)$.*

证明. Assume L is a splitting field of an irreducible polynomial $g(x) \in K[x]$, then $L = K(\alpha_1, \ldots, \alpha_m)$, where $\alpha_1, \ldots, \alpha_m$ are roots of $g(x)$.
Let $f(x) \in K[x]$ be irreducible, and α, β two roots of $f(x)$. Then $L = K(\alpha_1, \ldots, \alpha_m)$, $L(\alpha) = K(\alpha_1, \ldots, \alpha_m)(\alpha) = K(\alpha)(\alpha_1, \ldots, \alpha_m)$, $L(\beta) = K(\alpha_1, \ldots, \alpha_m)(\beta) = K(\beta)(\alpha_1, \ldots, \alpha_m)$.
Since $K(\alpha) \simeq K[x]/(f) \simeq K(\beta)$, we have $K(\alpha)(\alpha_1) \simeq K(\alpha)[x]/(g) \simeq K(\beta)[x]/(g^\sigma) \simeq K(\beta)(\alpha_1^\sigma)$, and $[K(\alpha)(\alpha_1) : K(\alpha)] = [K(\beta)(\alpha_1^\sigma) : K(\beta)]$. Inductively, $K(\alpha)(\alpha_1, \ldots, \alpha_m) \simeq K(\beta)(\alpha_1^\sigma, \ldots, \alpha_m^\sigma) = K(\beta)(\alpha_1, \ldots, \alpha_m)$.
In particular, $L(\alpha) \simeq L(\beta)$ and $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$.
So $[L(\beta) : L][L : K] = [L(\beta) : K] = [L(\beta) : K(\beta)][K(\beta) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = [L(\alpha) : K] = [L(\alpha) : L][L : K]$. Thus $[L(\beta) : L] = [L(\alpha) : L]$ $\square$

Definition 2. *An algebraic extension E/F is called normal if, for each irreducible polynomial $f(x) \in F[x]$, whenever E contains one root of $f(x)$, E contains all roots of $f(x)$.*

Corollary 3. *An algebraic extension is normal if and only if it is a splitting field of some polynomial over F.*

Let E/F be finite extension, $\mathrm{Gal}(E/F) = G$, G acts on E has orbits. For $F \subset L \subset E$ and $\sigma \in G$, $F = F^\sigma \subset L^\sigma \subset E^\sigma = E$, we want to know $L^\sigma \overset{?}{=} L$.

Lemma 4. *Let L be a field with $F \subset L \subset E$, then L is a field fixed by $\mathrm{Gal}(E/F)$ if and only if $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$.*

证明. Suppose L is fixed by $\mathrm{Gal}(E/F)$, then each element of $\mathrm{Gal}(E/F)$ induces an automorphism of L and hence E/F acts on L naturally. The kernel of this action is $\mathrm{Gal}(E/L)$. So $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$.
Conversely, suppose $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$. Let $\alpha \in L$ and $g \in \mathrm{Gal}(E/F)$. Claim: $\alpha^g \in L$.
Let $\beta = \alpha^g$. Then for $h \in \mathrm{Gal}(E/L)$, $\beta^{hg^{-1}} = \alpha^{ghg^{-1}} = \alpha$ as $ghg^{-1} \in \mathrm{Gal}(E/L)$. Hence $\beta = \alpha^{gh^{-1}} = \beta^{h^{-1}}$, i.e. $\beta^h = \beta$ i.e. $\beta = \alpha^g \in L$. And L is fixed by $\mathrm{Gal}(E/F)$. $\square$

Theorem 5. *Let $F \subset L \subset E$. Then $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$ if and only if L is a splitting extension of F (L is a normal extension of F).*

证明. Assume $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$.
Let $f \in F[x]$ be irreducible, and β be a root of f s.t. $\beta \in L$. We aim to prove all roots of f in L.
Let β' be another root of f. Since f is irreducible. There exists $\sigma \in \mathrm{Gal}(E/F)$ s.t. $\beta' = \beta^{\sigma}$. For any $h \in \mathrm{Gal}(E/L)$, $\beta'^{h} = \beta^{\sigma h} = \beta^{\sigma h \sigma^{-1} \sigma} = \beta^{\sigma} = \beta'$. So $\beta' \in L$. Hence L is a splitting field of f.
Conversely, Let L be a splitting field extension of F. Then for any $\alpha \in L$, and $\sigma \in \mathrm{Gal}(E/F)$, $\alpha^{\sigma} \in L$.
By the Lemma $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/F)$. □

Example 6. *Let $\omega = \frac{-1+\sqrt{3}i}{2}$ be the 3rd primitive root of unity. Let $F = \mathbb{Q} \subset L = \mathbb{Q}(\omega) \subset E = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Then $\mathbb{Q}(\omega)$ is a splitting field of $x^2 + x + 1$, $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field of $x^3 - 2$.
$\mathrm{Gal}(L/F) = Z_2$, $\mathrm{Gal}(E/L) = Z_3$ and $\mathrm{Gal}(E/F) = S_3$.*

Example 7. *Let $f(x) = x^5 - 7$. $\mathrm{Gal}(f)_{\mathbb{Q}} = \mathrm{Gal}(E/\mathbb{Q})$ where E is the splitting field of $f(x)$ over $\mathbb{Q}$, find $\mathrm{Gal}(f)_{\mathbb{Q}}$.*