Abstract Algebra
: Lecture 18

Leo

2024.12.03

Theorem 1. *If* $\operatorname{char} F = 0$*, then each finite extension of* F *is a simple extention.*

Lemma 2. *Let* $\operatorname{char} F = 0$*, and* $E = F(\alpha, \beta)$*. Then there exists* $\gamma \in E$ *such that* $E = F(\gamma)$*.*

证明. Let $f(x) = \operatorname{Irr}(\alpha, F)$ and $g(x) = \operatorname{Irr}(\beta, F)$. Let $\gamma = \alpha + c\beta$ where $c \in F$. And let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$. Then $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$. So β is a common root of $h(x)$ and $g(x)$. Assume β is the only coomon root of $h(x)$ and $g(x)$. Then $x - \beta = \gcd(h(x), g(x))$ as irreducible polynomial over char $= 0$ field is separable. Hence there exists $s(x)$ and $t(x)$ s.t. $x - \beta = s(x)h(x) + t(x)g(x) \in F(\gamma)[x]$. So $\beta \in F(\gamma)$ and $\alpha = \gamma - c\beta \in F(\gamma)$, i.e. $F(\alpha, \beta) \subseteq F(\gamma)$. Conversely, $\gamma \in F(\alpha, \beta)$, so $F(\alpha, \beta) = F(\gamma)$. Suppose β' is another common root of $h(x)$ and $g(x)$. Then $0 = h(\beta') = f(\gamma - c\beta') = f(\alpha + c\beta - c\beta')$ hence $\alpha' := \alpha + c\beta - c\beta'$ is a root of $f(x)$. Thus $c = \frac{\alpha' - \alpha}{\beta - \beta'} \in F$. Take $c \in F$ which is not of the form $\frac{\alpha' - \alpha}{\beta - \beta'}$ (this is due to $|F|$ is infinity). Suppose $\deg f = m$, $\deg g = n$ then $\#\alpha' = m$, $\#\beta' = n$, $\Rightarrow \#c = \frac{\alpha' - \alpha}{\beta - \beta'} < \infty$. ☐

证明. Let E be a finite extension of F. Then $E = F(\gamma_1, \ldots, \gamma_n)$. Then $E = F(\gamma_1, \ldots, \gamma_n) = F(\gamma_1)(\gamma_2, \ldots, \gamma_n) = E(\gamma_2, \ldots, \gamma_n) = E(\beta) = F(\gamma_1, \beta) = F(\alpha)$ is a simple extension of F for some $\alpha \in E$. ☐

Example 3. $\mathbb{Q}(\sqrt[3]{2}, \omega)$*, where* $\omega = \frac{-1+\sqrt{-3}}{2}$*.* $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$*.* $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2} + \omega)$*.*

Proposition 4. *If* F *is a finite field, then each finite extension is a simple extension.*

证明. Let E be a finite field exteniton of $F = \mathbb{F}_{p^d}$ with p prime. Then $E = \mathbb{F}_{p^n}$ with $d \mid n$, and $E^* =< \alpha >$. So $E = F(\alpha)$. ☐

Example 5. *Let* $R = \mathbb{F}_p[t]$ *and let* F *be the fraction field of* R *denoted by* $\mathbb{F}_p(t)$*. Then* $\operatorname{char} F = p$ *and* $|F| = \infty$*. Let* $f(x) = x^p - t \in F[x]$*. Suppose* α *is a root of* $f(x)$*. Then* $f(x) = (x - \alpha)^p$*.*
Claim: $f(x)$ *is irreducible in* $F[x]$*.*
Suppose $f(x) = g(x)h(x)$*,* $1 \leqslant \deg g < \deg f$*. Then* $g(x) \mid f(x) = (x - \alpha)^p$*, and* $g(x) = (x - \aleph)^m = Ax - \alpha^m$*. Thus* $\alpha^m \in F$*. Since* $F = \mathbb{F}_p(t)$*. Now* $t = \alpha^p$ *since* $\gcd(p, m) = 1$ *we have* $\alpha \in F$*. Contradiction.*

Definition 6. *If all roots of f lies in E and E is the smallest extension of F, then its called the splitting field of f.*

Let $f(x)$ be irreducible in $F[x]$, $\operatorname{char} F = 0$. Let α, β be two roots of $f(x)$. Then $F(\alpha)$, $F(\beta)$ are isomorphic field. $\alpha, \dots, \alpha_n$ are all roots of $f(x)$.
Let E be the splitting field then $E = F(\alpha, \dots, \alpha_n)$. And $F(\alpha_i) \simeq F(\alpha_j)$.
We consider $\operatorname{Aut}_F(E)$ is transitive on $\{\alpha, \dots, \alpha_n\}$.