Intro to Algebra W6-2

fat

March 29, 2024

Definition 1. $[E_s : F]$ = **separable degree** of E over F. $[E : E_s]$ = **inseparable degree** of E over F.

Corollary 1. We have

$$\left|\mathrm{Emb}(^{E}/_{F})\right| = \{E : F\} = [E_s : F]$$

Proof. $\{E : F\} = \{E : E_s\}\{E_s : F\} = 1 \cdot [E_s : F]$. $\square$

Theorem 1 (Primitive Element Theorem)**.** If E/F is a finite separable extension, then E/F is a simple extension. i.e. $E = F(\alpha)$ for some $\alpha \in E$.

Definition 2. The element α in the theorem is called a **primitive element** in the field extension.

Proof.

If F is a finite field, then so is E by Prop 18 of Chap 9. $E^{\times} = \langle \alpha \rangle$ for some $\alpha \in E$. Then $E = F(\alpha)$ is a simple extension. Now assume that $|F| = \infty$. It suffices to show that if $\alpha, \beta \in E$, then $\exists \gamma \in F$ such that $F(\gamma) = F(\alpha, \beta)$. (Say $E = F(\alpha_1, ..., \alpha_n)$. Then $F(\alpha_1, \alpha_2) = F(\beta_1) \Rightarrow F(\beta_1, \alpha_3) = F(\beta_2), ...$)
Let $f(x) = m_{\alpha,F}(x), g(x) = m_{\beta,F}(x)$. Let $\alpha_1, ..., \alpha_n$ be the roots of $f(x)$, and $\beta_1, ..., \beta_n$ be the roots of $g(x)$. Since $|F| = \infty$, $\exists a \in F$ such that $a \neq (\alpha_i - \alpha)/(\beta - \beta_j)$ for any i, j. Let $\gamma = \alpha - a\beta$. Consider the polynomial

$$h(x) = f(\gamma - ax) \in F(\gamma)$$

We have

$$h(\beta) = f(\gamma - a\beta) = f(\alpha) = 0$$

$$\Rightarrow m_{\beta,F(\gamma)}(x) | h(x) \cdots (*)$$

Also,

$$m_{\beta,F(\gamma)}(x) | g(x)$$

by the definition of $g(x)$. $\Rightarrow$ {the roots of $m_{\beta,F(\gamma)}(x)$} $\subseteq \{\beta_1, ..., \beta_n\} \cdots (**)$.

Claim. If $\beta_i \neq \beta$, then $h(\beta_i) \neq 0$.

Assume that the claim is true. Then for any $\beta_i \neq \beta$, we have $m_{\beta,F(\gamma}(\beta_i) \neq 0 \cdots (***)$. (Since $m_{\beta_i,F(\gamma)}(x) | h(x)$.) Combining $(**)$ and $(* * *)$, we see that β is the only root of $m_{\beta,F(\gamma)}(x)$. Since E/F is a separable extension, we must have $m_{\beta,F(\gamma}(x) = x - \beta$. $\Rightarrow \beta \in F(\gamma)$. $\Rightarrow \alpha = \gamma - a\beta \in F(\gamma)$. $\Rightarrow F(\alpha, \beta) \subseteq F(\gamma)$. The converse is trivial. $\Rightarrow F(\gamma) = F(\alpha, \beta)$.

Proof of the Claim.

Assume $\beta_i \neq \beta$. We have $h(\beta_i) = f(\gamma - a\beta_i)$. Recall that the roots of f are $\alpha_1, ..., \alpha_m$. So it suffices to show that $\gamma - a\beta_i \neq \alpha_j$ for any j. However, this follows from our choice of a. (To see this,

$$a \neq \frac{\alpha_j - \alpha}{\beta - \beta_j} \quad \forall i, j \text{ such that } \beta_i \neq \beta$$

$$\Rightarrow a(\beta - \beta_i) \neq \alpha_j - \alpha \quad \forall i, j \text{ such that } \beta_i \neq \beta$$

$$\Rightarrow \gamma - a\beta_i \neq \alpha_j \forall i, j \text{ such that } \beta_i \neq \beta$$

which gives our claim.) □

□

Note that in general isomorphisms ϕ in $\mathrm{Emb}(E/F)$ may not be composited with since $\phi(E)$ may not be E. (For example, $E = \mathbb{Q}(\sqrt[3]{2}), F = \mathbb{Q}$. We have $\phi_{\sqrt[3]{2}, \sqrt[3]{2}\zeta} : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\zeta), \zeta = e^{2\pi i}3$ where $\phi_{\sqrt[3]{2}, \sqrt[3]{2}\zeta} \in \mathrm{Emb}(E/F)$ is defined by $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mapsto a_0 + a_1\sqrt[3]{2}\zeta + a_2(\sqrt[3]{2}\zeta)^2$.) In order for elements of $\mathrm{Emb}(E/F)$ to composite with each other, we need $\phi(E) = E \quad \forall \phi \in \mathrm{Emb}(E/F)$. Now

$$\phi(E) = E \quad \forall \phi$$

$$\Leftrightarrow \forall \alpha \in E, \forall \phi, \phi(\alpha) \in E$$

(Recall that $\phi(\alpha)$ are conjugates of α over F.) $\Leftrightarrow \forall \alpha \in E$, all the conjugates of α over F are in E. $\Leftrightarrow E/F$ is a normal extension. (We say E/F is a normal extension if $\forall \alpha \in E$ all the conjugates of α over F are in E.) $\Leftrightarrow \forall \alpha \in E, m_{\alpha,F}(x)$ splits completely over E.