Sec 30 Vector Space

Date: Mar 13 Made by Eric

In this note, $\mathbb{E}$ is always a field

Theorems

Theorem 1. *Let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\alpha \in \mathbb{E}$ be an algebraic element over $\mathbb{F}$. Let β be an element of $\mathbb{F}(\alpha)$*

$$\beta \text{ is algebraic, and } deg(\beta, \mathbb{F}) \leq deg(\alpha, \mathbb{F})$$

Proof. We first prove that $\mathbb{F}(\alpha)$ over $\mathbb{F}$ with structure $* : \mathbb{F} \times \mathbb{F}(\alpha) \to \mathbb{F}(\alpha)$ defined by $(\gamma, v) = \gamma v$ constitute a vector space

Let δ, γ be elements of $\mathbb{F}$ and let v, w be elements of $\mathbb{F}(\alpha)$

Let $\deg(\alpha, \mathbb{F}) = n$

Express v in the form of $c_{n-1}\alpha^{n-1} + \cdots + c_0 1$

$\delta v = (\delta c_{n-1})\alpha^{n-1} + \cdots + (\delta c_0)1 \in \mathbb{F}(\alpha)$

$\delta(\gamma v) = \delta\gamma v = (\delta\gamma)v = (\delta\gamma)v$ **(Notice that the v after the second equator is in $\mathbb{F}$ and the v after third equator is in $\mathbb{F}(\alpha)$)**

$\delta(v + w) = \delta(v + w) = \delta v + \delta w$

$(\delta + \gamma)(v) = (\delta + \gamma)v = \gamma v + \delta v$

$1v = v$ (done)

We now prove $\{\alpha^{n-1}, \ldots, \alpha, 1\}$ is a basis for $\mathbb{F}(\alpha)$

Because $\deg(\alpha, \mathbb{F}) = n$, we know there exists a polynomial f in $\mathbb{F}[x]$ of degree n such that $f(\alpha) = 0$

For each element v in $\mathbb{F}(\alpha)$, we express v in the form of $g(\alpha)$ where $g \in \mathbb{F}[x]$

Do division algorithm on g with f. We have

$$g = qf + r$$

Where $\deg(r) < \deg(f)$

Because $f(\alpha) = 0$, then we see $g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$

Because $\deg(r) < n$, we know $r(\alpha) \in \text{span}(\{\alpha^{n-1}, \ldots, \alpha, 1\})$

Assume $\{\alpha^{n-1}, \ldots, \alpha, 1\}$ is linearly dependent; that is, there exists a polynomial h of degree smaller than n and greater than 0 such that $h(\alpha) = 0$

This CaC to that $deg(\alpha, \mathbb{F}) = n$ (done)

Immediately, we see $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is linearly dependent, for that $\dim(\mathbb{F}(\alpha)) = n < n + 1$. Then we can construct a polynomial $l \in \mathbb{F}[x]$ of degree less than or equal to n such that $l(\beta) = 0$

$\blacksquare$