MATH 407

4/27/18



⊛ F field, $x$ indeterminate

* $F[x] = \{p : p \text{ polynomial over } F\}$

$$p(x) = a_0 + a_1 x^1 + \dots + a_n x^n$$
$$= \sum_{i=0}^{\infty} a_i x^i, \quad a_n \text{ ultimately } 0$$

* $p(x) = \sum_i a_i x^i = q(x) = \sum_i b_i x^i$ iff $a_i = b_i, \forall i$

* $0 = \sum_i 0 \cdot x^i$

* Addition: $p(x) + q(x) = \sum_i a_i x^i + \sum_i b_i x^i$
$$= \sum_i (a_i + b_i) x^i$$

* Scalar multiplication: $\lambda \in F, p \in F[x]$
$$\Rightarrow (\lambda p)(x) = \sum_i (\lambda a_i) x^i$$

* <u>Thm</u>: $F[x]$ is a vector space over $F$ w/ basis
$$\{x^i : i \in \mathbb{Z}^+\} = \{1, x, x^2, \dots\}$$

* $\lambda(p+q) = \sum_i \lambda(a_i + b_i) x^i = \sum (\lambda a_i + \lambda b_i) x^i$
$$= \sum_i (\lambda a_i) x^i + \sum_i (\lambda b_i) x^i$$
$$= \lambda p(x) + \lambda q(x)$$

* $1 \cdot p = p, \quad 0 \cdot p = 0$

* $F[x] = \text{Span}\{1, x, x^2, \dots, x^n, \dots\}$

(*) Polynomial functions:

* If $p \in F[x]$, $c \in F$, define $p|_{x=c} = \hat{p}(c) = p(c)$

$$\hat{p}(x=c) = \sum_i a_i c^i$$

* $T: F[x] \to F^F$

$$p \to \hat{p} \quad \text{(linear transformation)}$$

Ex. $F = \mathbb{Z}_2$, $p(x) = x^2 + x$

$\Rightarrow \hat{p}(0) = 0^2 + 0 = 0$

$\hat{p}(1) = 1^2 + 1 = 1 + 1 = 0$

$\hat{p} = \hat{0}$

$\therefore$ $T$ is not one-to-one.

* If $F$ is infinite, $T$ is one-to-one.

(*) Degree of polynomial:

$\deg: F[x] \to \mathbb{Z}^+ \cup \{-\infty\}$

$\deg(0) = -\infty$,

else $p \neq 0$:

$\deg(p) = n$ where $n = \max_k(\{a_k \neq 0\})$

* $a_n$ is the leading / high order coefficient

* $\deg(p) = 0 \Rightarrow p = a_0$ (constant polynomial)

* <u>Thm</u> $\deg(p+q) \leq \max(\{\deg(p), \deg(q)\}) = k$

Pf. If $m > k$ then $a_m = 0$ and $b_m = 0$, so $a_m + b_m = 0$
Then, $\max_m(\{a_m + b_m \neq 0\}) \leq k$

* Multiplication of polynomials:

$p \cdot q$, $p = \sum_i a_i x^i$, $q = \sum_i b_i x^i$

| | $b_0$ | $b_1$ | $b_2$ | $\dots$ | $b_n \dots$ |
|---|---|---|---|---|---|
| $a_0$ | $a_0b_0$ | $a_0b_1$ | $a_0b_2$ | $\dots$ | $a_0b_n$ |
| $a_1$ | $a_1b_0$ | $a_1b_1$ | $a_1b_2$ | $\dots$ | $a_1b_n$ |
| $a_2$ | $\vdots$ | $\vdots$ | $\vdots$ | $\dots$ | $a_2b_n$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\dots$ | $\vdots$ |
| $a_n$ | $a_nb_0$ | $a_nb_1$ | $a_nb_2$ | $\dots$ | $a_nb_n$ |
| $\vdots$ | | | | | |

$\Rightarrow a_i \cdot b_j = a_i b_j x^{i+j}$

$(\rightarrow)$

④

*If $k = i + j$,

$$p \cdot q = a_k b_0 x^k + a_k b_1 x^k + \dots + a_i b_{k-1} x^k + \dots + a_0 b_k x^{k-1}$$

$$= \left( \sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

$$\parallel$$

$$c_k = \left( \sum_{i=0}^{k} a_{k-i} b_i \right) x^k$$

$$\left( \sum_i a_i x^i \right) \left( \sum_j b_j x^j \right)$$

$$= \sum_k \left( \sum_i a_i b_{k-i} \right) x^k$$

* $p = 0$ or $q = 0 \Rightarrow p \cdot q = 0$

* $\deg(pq) = \deg(p) + \deg(q)$

* Thm. $p \cdot q = 0$ iff $p = 0$ or $q = 0$

* Cor 4.16 If $f, g, h \in F[x]$ and $f \neq 0$
then $fg = fh \Rightarrow g = h$

$\hookrightarrow f(g-h) = 0$

$\Rightarrow g - h = 0$

$\Rightarrow g = h$

* Thm. If $f \in F[x]$ has a multiplicative inverse

$(\longrightarrow)$

$f^{-1}$, then $f$ is non-zero constant.

$f \cdot f^{-1} = 1$

$\deg(f) + \deg(f^{-1}) = 0$

$\Rightarrow \deg(f) = 0,\ \deg(f^{-1}) = 0$

$\Rightarrow f = a_0,\ f^{-1} = 1/a_0$