1 16-04-2018

1.1 Definitions and basic properties of polynomial

$\mathbb{N}$ = set of natural number

$\mathbb{N}_0 = \mathbb{N} union\{0\}$

for $n \in \mathbb{N}$, $\mathbb{N}_0^n = \{\alpha = (\alpha_1, \ldots, \alpha_n) | \alpha_1, \ldots, \alpha_n \in \mathbb{N}_0\}$ is semi-module because closed over addition (?)

$\nvDash = (0, \ldots, 0)$ and $x_1, \ldots, x_n$; variables

for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$

a mononomial, or direct product of variables $x^\alpha = \begin{cases} 1, (if \alpha = 0) \\ x_1^{\alpha_1} \ x_2^{\alpha_2} \ \ldots x_n^{\alpha_n}, (otherwise) \end{cases}$

K is field. [Field : is a set on which addition, subtraction, multiplication, and division are defined, and behave as when they are applied to rational and real numbers.]

Definition 1. *Let $A \subset \mathbb{N}_0^n$:finite*

$$f = \sum_{\alpha \in A} c_\alpha x^\alpha \ (c_\alpha \in K)$$

*is called **a polynomial** of $x_1, \ldots, x_n$ with K-coefficients.*

$$K[\mathbf{x}] = K[x_1, \ldots, x_n] = \{f | f is a polynomial of x_1, \ldots, x_n \ with \ K\text{-}coefficients \}$$
$$M_n = \{x^\alpha | \alpha \in \mathbb{N}_0^n\} \subset K[x]$$

Example 1. *$n = 2$ then we have $A = \{(0,0), (1,1), (0,3), (2,0), (2,1)\}$.*

$$f = x_1^2 x_2 + 5x_2^3 - 2x_1 x_2 + 10$$

$C_{(2,1)} = 1, C_{(2,0)} = 0, C_{(0,3)} = 5, C_{(1,1)} = -2, C_{(0,0)} = 10.$

Definition 2. *Support*. *$f = \sum_{\alpha \in A} c_\alpha x^\alpha \neq 0$ then*

$$supp(f) = \{\alpha \in A | C_\alpha \neq 0\}$$

Example 2. *$supp(f) = \{(0,0), (1,1), (0,3), (2,1)\}$*

Definition 3. *Total degree*. *$|\alpha| = \alpha_1 + \cdots + \alpha_n (\alpha \in (N)_0^n)$. If $supp(f) \neq \emptyset$*

$$tdeg(f) = max\{|\alpha| | \alpha \in supp(f)\}$$

Example 3. *$tdeg(f) = max\{0, 2, 3, 3\} = 3$*

$f, g \in K[x]$

$f \ g$ or associated $\Leftrightarrow \exists C \in K \ \{0\}$ such that $f = c \cdot g$.

For example : $f = x_1^2 x_2 + 1; g = 3x_1^2 x_2 + 3; h = 3x_1^2 x_2 + 2$. Then $f \ g, f not \ h$

$f | g$ or f devides $g \Leftrightarrow \exists h \in K[x]$ such that $f \cdot h = g$

Properties 1. *$f | g \Rightarrow tdeg(f) \leq tdeg(g)$*

Definition 4. *Let $f \in K[x] \ K$. f is **irreducible** if $\left(h | f \Rightarrow (h \in K or h \ f) \right)$. If $tdeg(f) > 0$ and f is not irreducible, then f is called **reducible**.*

Theorem 1. *Let $f \in K[x] \ K$. Then f can be **factorized** as*

1. $f = c \ g_1^{\beta_1} \ g_2^{\beta_2} \ldots g_n^{\beta_m}$ where $c \in K \ \{0\}$, $\beta_1, \beta_2, \ldots, \beta_m \in \mathbb{N}$, and $g_1, \ldots, g_m$: irreducible, $g_i not \ g_j \ (i \neq j)$

2. if $f = c \ g_1^{\beta_1} \ g_2^{\beta_2} \ldots g_m^{\beta_m} = d \ h_1^{\gamma_1} \ h_2^{\gamma_2} \ldots h_l^{\gamma_l}$ (factorization). Then (a) $m = l$, (b) by change of index, $g_1 \ h_1, \ldots, g_m \ h_m$.

We can define $GCD(f, g)$ for $f, g \in K[x], \left((f, g) \neq (0, 0) \right)$

Definition 5. *Let $I \in K[x], I \neq \emptyset$. I is **an ideal** if*

1. $f, g \in I \Rightarrow f + g \in I$

2. $f \in I, r \in K[x] \Rightarrow r \cdot f \in I$

Definition 6. *An ideal generated by* $f_1, \ldots, f_m$. *Let $f_1, \ldots, f_m \in K[x] \ \{0\}$*

$$< f_1, \ldots, f_m >= \{r_1 f_1 + r_2 f_2 + \cdots + r_m f_m | r_1, r_2, \ldots, r_m \in K[x]\}$$

Properties 2. *$< f_1, \ldots, f_m >$ is an ideal.*

Properties 3. *$0 \in I$ (an ideal)*

Problem : Ideal membership problem. Given $I =< f_1, \ldots, f_m >$ and a polynomial h. Determine $h \in I$ or not !

1.2 Single Variable

Take $n = 1, x = x_1, K[x] = K[x_1]$. For $f \in K[x]$ we define **degree of** f as

$$deg(f) = \begin{cases} tdeg(f), (f \neq 0) \\ -\infty, (f = 0) \end{cases}$$

We define this such that properties below is satisfied.

Properties 4. *Let* $f, g \in K[x]$.

1. $deg(f + g) \leq max\{deg(f), deg(g)\}$

2. $deg)(fg) = deg(f) + deg(g)$

Example 4.   1. $f = 2x^2 + 1, g = x + 1$

2. $f = x + 1, g = -x$

3. $f = x + 1, g = 0$

Theorem 2. *Division Principle.* *Let* $f, g \in K[x]$ *and* $g \neq 0$. *Then there exist unique polynomials* q, r *such that*

$$f = q \cdot g + r$$

and $deg(r) < deg(g)$ *where* q *is* *quotient* *and* r *is* *remainder*.

Example 5. $f = x^3 + x - 1, g = 2x^2 - 1$. *Then* $f = x^3 + x - 1 = \frac{1}{2}x(2x^2 - 1) + \frac{3}{2}x - 1$ *with* $deg(g) = 2, deg(r) = 1$