Polynomial Rings

R - ring

Definition

Ring of polynomials in x with coefficients in R

A polynomial in "variable" x with coefficients in R

$$R[x] := \{ a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \mid n \in \mathbb{N} \cup \{0\},\ a_i \in R \}$$

coefficients of polynomial

For $i > n$ we decree $a_i = 0_R$

$$f(x) = a_0 + a_1 x + \dots + a_n x^n,\quad g(x) = b_0 + b_1 x + \dots + b_m x^m$$

$$f(x) = g(x) \iff a_i = b_i \quad \forall\ i \geq 0$$ (By definition)

For example, $1 + 1 \cdot x + 2 \cdot x^2 = 1 + 1 \cdot x + 2x^2 + 0x^3 \in \mathbb{Z}[x]$

Notation Conventions :

- $1_R\, x^k = x^k$
- If $a_i = 0_R$ we omit $a_i x^i$ from notation.

Facts : $R[x]$ is a ring under the following $+$ and $\times$:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1) x + \dots + (a_k + b_k) x^k$$ ($\max\{n, m\}$)

$$f(x) g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots + \left(\sum_{j=0}^{d} a_j b_{d-j} \right) x^d + (a_n b_m) x^{(n+m)}$$

$$0_{R[x]} = 0_R \longleftarrow a_i = 0_R \quad \forall\ i \geq 0$$

$$1_{R[x]} = 1_R \longleftarrow a_0 = 1_R,\ a_i = 0_R \quad \forall\ i > 0$$

Definition Given $f(x) \in R[x]$, $f(x) \neq 0_{R[x]}$

$$\deg(f(x)) := \min i \text{ such that } a_i \neq 0_R$$ (called the leading coefficient)

For example, $\deg(1 + x) = 1$, $\deg(3) = 0$ ($a_0 = 3$, $a_i = 0$ $i > 0$)

There is a natural injective homomorphism

$$\phi : R \longrightarrow R[x]$$
$$a \longrightarrow \text{Polynomial such that } a_0 = a,\ a_i = 0\ \forall\ i > 0$$

$\mathrm{Im}(\phi) :=$ Constant Polynomials ← Polynomials of degree zero

Definition (Inductive Definition)

$R[x_1, x_2] := R[x_1][x_2]$

$\vdots$

$R[x_1, x_2, \dots, x_n] := R[x_1, \dots, x_{n-1}][x_n]$

Polynomial ring in n variables.

General term is a formal finite sum of monomials, i.e. $a x_1^{m_1} \dots x_n^{m_n}$, $a \in R$

By definition of ring structure on $R[x_1, \dots, x_n]$

Fact: Given $(a_1, a_2, \dots, a_n) \in R^n$ there is an evaluation homomorphism:

$$\psi : R[x_1, \dots, x_n] \longrightarrow R$$
$$f(x_1, \dots, x_n) \longrightarrow f(a_1, \dots, a_n)$$

The element of R given by replacing x_i with a_i and composing in R

For example, $\psi : \mathbb{Z}[x_1, x_2] \longrightarrow \mathbb{Z}$

$$f(x_1, x_2) \longmapsto f(1, 1)$$
$$1 + 2x_1x_2 \longmapsto 1 + 2 \cdot 1 \cdot 1 = 3$$

Hence $f \in R[x_1, \dots, x_n]$ gives rise to a map of sets

$$\phi_f : R^n \longrightarrow R$$
$$(a_1, \dots, a_n) \longmapsto f(a_1, \dots, a_n)$$

The function given by a polynomial does not determine it in general.

Warning: $\phi_f = \phi_g \not\Rightarrow f = g$

Example $R = \mathbb{Z}/p\mathbb{Z}$ (p prime), $f(x) = x^p - x$, $g(x) = 0$

$R^* = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$ ← finite group of order $p-1$ under $\times$

$[a] \in R^* \Rightarrow f([a]) = [a]^p - [a] = [a]([a]^{p-1} - [1]) = [a][0] = [0]$

$[a] \notin R^* \Rightarrow [a] = [0] \Rightarrow f([a]) = f([0]) = [0]^p - [0] = [0]$

Important Properties of Polynomial Rings

1/ Given $f(x), g(x) \in R[x] \setminus \{0_{R[x]}\}$

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

← can only be strict if $\deg(f(x)) = \deg(g(x))$

Example: $\deg((1+x+x^2)+(2+2x-x^2)) = \deg(3+3x) = 1$

(degree 2) (degree 2)

2/ Given $f(x), g(x) \in R[x] \setminus \{0_{R[x]}\}$, if $f(x)g(x) \neq 0_{R[x]}$, then

$$\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x))$$

← Can be strict only if $a_n b_m = 0_R$, a_n, b_m leading coefficients

Example: $R = \mathbb{Z}/15\mathbb{Z}$, $f(x) = [1] + [3]x$, $g(x) = [2] + [5]x$

$\Rightarrow f(x)g(x) = [2] + [11]x + [15]x^2 = [2] + [11]x$

$\Rightarrow \deg(f(x)g(x)) = 1 < 1 + 1 = \deg(f(x)) + \deg(g(x))$

3/ R commutative $\Rightarrow R[x_1, \ldots, x_n]$ commutative

4/ R an integral domain $\Rightarrow R[x_1, \ldots, x_n]$ an integral domain.

and $f(x), g(x) \neq 0_{R[x]} \Rightarrow \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

($a_n \neq 0_R, b_m \neq 0_R \Rightarrow a_n b_m \neq 0_R$)