Polynomial Rings

Definition: Polynomial Ring

Let R be a commutative ring with $1 \neq 0$. The *ring of polynomials*, denoted $R[x]$, is given by:

$$R[x] = \left\{ \sum_{k=0}^{n} a_k x^k \mid n \in \mathbb{N}_0 \text{ and } a_k \in R \right\}$$

In other words, $R[x]$ consists of polynomials with coefficients from R.

a_0 is called the *constant* coefficient/term.

$a_n x^n$ for largest n such that $a_n \neq 0$ is called the *leading* term and a_n is called the *leading* coefficient.

Theorem

Let R be a ring. $R[x]$ is a ring under the standard definitions of polynomial addition and multiplication:

$$\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k = \sum_{k=0}^{n} (a_k + b_l) x^k$$

$$\left(\sum_{k=0}^{n} a_k x^k \right) \left(\sum_{k=0}^{n} b_k x^k \right) = \sum_{k=0}^{n} c_k x^k, \quad c_k = \sum_{j=0}^{k} a_k b_{k-j}$$

Addition is component-wise and multiplication is based on the distributive property.

Proof

Addition is component-wise and is thus based on the additive properties of R. Thus, $R[x]$ is an additive abelian group. Likewise, multiplication is based on the associative and distributive properties of R. Therefore, $R[x]$ is a ring.

Definition: Degree

Let $R[x]$ be a polynomial ring over a ring R. The *degree* function:

$$\deg : R[x] \to \mathbb{N}_0 \cup \{-\infty\}$$

is defined by:

$$\deg(f(x)) = \begin{cases} -\infty & f(x) \equiv 0 \\ n & a_n x^n \text{ is the leading term of } f(x) \end{cases}$$

Definition: Equality

Let R be a ring and $f(x), g(x) \in R[x]$ where:

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

$$g(x) = \sum_{k=0}^{m} b_k x^k$$

To say that $f(x) = g(x)$ means $m = n$ and $a_k = b_k$ for all $0 \leq k \leq n$.

Properties: Polynomial Rings

Assume R is an integral domain:

1). $R[x]$ is an integral domain.

2). $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$

3). $R[x]^\times = R^\times$

Theorem: Division Algorithm

Let R be an integral domain and $f(x), g(x) \in R[x]$ such that $g(x) \neq 0$. There exists $k \in \mathbb{N}_0$ and $q(x), r(x) \in R[x]$ such that:

1). $b^k f(x) = q(x)g(x) + r(x)$

2). $deg(r(x)) < \deg(g(x))$

3). b is the leading coefficient of $g(x)$

Note that if b is a unit then we can take $k = 0$.

It is OK to select the minimum k that works.

For a fixed k, $q(x)$ and $r(x)$ are unique.

Example

Let $R = \mathbb{Z}$ and:

$$\begin{aligned} f(x) &= 2x^2 + 1 \\ g(x) &= 3x - 1 \end{aligned}$$

$3^k(2x^2 + 1) = (ax + b)(3x - 1) + c$
$3^k \cdot 2x^2 + 3^k = 3ax^2 + (3b - a)x + (c - b)$

$3a = 2 \cdot 3^k$
$3b - a = 0$
$c - b = 3^k$

$a = 2 \cdot 3^{k-1}$, so $k \neq 0$
$b = 2 \cdot 3^{k-2}$, so $k \neq 1$
$c = 3^k + 2 \cdot 3^{k-2}$, so $k \geq 2$

For $k = 2 : a = 6, b = 2, c = 11$:

$3^2(2x^2 + 1) = (6x + 2)(3x - 1) + 11$

Note that $\deg(3x - 1) = 1$ and $\deg(11) = 0$, and indeed: $0 \leq 0 < 1$.

<u>Proof</u>

Let $\deg(f(x)) = m$ and $\deg(g(x)) = n$

If $m < n$ then we can take $k = 0, q(x) \equiv 0$, and $r(x) = f(x)$:

$$b^0 f(x) = 0 \cdot g(x) + f(x)$$

So, AWLOG: $m \geq n \geq 0$

Let a be the leading coefficient for $f(x)$

Proof by induction on m for a given n

Base: $m = 0$

Since $m \geq n$ it must be the case that $n = 0$
$f(x) = a$ and $g(x) = b$
$bf(x) = ba = ab + 0 = ag(x) + 0$ and $-\infty < 0$

Assume the statement is true for $\deg(f(x)) < m$.

Consider $\deg(f(x)) = m$

ax^m is the leading term of $f(x)$
bx^n is the leading term of $g(x)$
Let $f_1(x) = bf(x) - a^{m-n} g(x)$
Consider the leading term of $f_1(x) : bax^m - abx^m = 0$
So $\deg(f_1(x)) < m$ and thus by the inductive assumption, there exists $k_1 \in N_0$ and $q_1(x), r_1(x) \in R[x]$ such that:

$$b^{k_1} f_1(x) = q_1(x)g(x) + r_1(x)$$

where $\deg(r_1(x)) < \deg(g(x)) = n$. Now:

$$\begin{aligned}
b^{k_1} f_1(x) &= b^{k_1+1} f(x) - b^{k_1} a^{m-n} g(x) \\
b^{k_1+1} f(x) &= b^{k_1} f_1(x) + b^{k_1} a^{m-n} g(x) \\
&= q_1(x)g(x) + r_1(x) + b^{k_1} a^{m-n} g(x) \\
&= [q_1(x) + b^{k_1} a^{m-n}]g(x) + r_1(x)
\end{aligned}$$

Let $k = k_1 + 1$, $q(x) = q_1(x) + b^{k_1} a^{m-n}$, and $r_1(x) = r(x)$:

$$b^k f(x) = q(x)g(x) + r(x) \quad \deg(r(x)) < \deg(g(x))$$

Note that if b is a unit then:

$$f(x) = [b^{-k}q(x)]g(x) + b^{-k}r(x)$$

which does not affect the various degrees.

Corollary: Remainder Theorem

Let $R[x]$ be a ring of polynomials over a ring R, $f(x), g(x) \in R[x]$, and $g(x) = x - a$. The remainder upon division of $f(x)$ by $g(x)$ is the constant $f(a)$.

Proof

$f(x) = q(x)(x - a) + r$

$f(a) = q(a)(a - a) + r = 0 + r = r$

We can also consider rings of multiple, independent, commuting variables:

$$R[x, y] = (R[x])[y]$$