MTHSC 412 Section 4.1 – Polynomial Arithmetic and the Division Algorithm

Kevin James

Definition

Suppose that $(R, \oplus, \otimes)$ is a ring then we define the ring $R[x]$ of polynomials in the variable x with coefficients in R as follows.

1. $R[x] = \left\{ \sum_{n\geq 0} a_n x^n \;\middle|\; \begin{array}{l} \text{for all } n,\ a_n \in R \text{ and for all but} \\ \text{finitely many } n,\ a_n = 0 \end{array} \right\}.$
2. $\left(\sum_{n\geq 0} a_n x^n\right) = \left(\sum_{n\geq 0} b_n x^n\right)$ if and only if $a_n = b_n$ for all n.
3. $\left(\sum_{n\geq 0} a_n x^n\right) + \left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0}(a_n \oplus b_n)x^n.$
4. $\left(\sum_{n\geq 0} a_n x^n\right) \cdot \left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0} \left(\sum_{j=0}^{n} a_j \otimes b_{n-j}\right) x^n$

Exercise

Prove that $R[x]$ is a ring if R is.

Note

1. We can think of $R \subset R[x]$.
2. $R[x]$ is commutative if and only if R is.
3. If R has an identity 1_R then $R[x]$ also has an identity, namely $1_{R[x]} = 1_R \cdot x^0$ (which we usually write as 1).

Definition

Suppose that $f(x) = \sum_{n \geq 0} a_n x^n \in R[x]$ and take

$$m = \max\{n \geq 0 \mid a_n \neq 0\}.$$

Then we say that a_m is the leading coefficient of f and that the degree of f is m and we write $\deg(f) = m$.

Note

1. The degree of 0 is undefined.
2. If $f = \sum_{n \geq 0} f_n x^n \in R[x]$ and $\deg(f) = d$, then we may write $f = \sum_{n=0}^{d} f_n x^n$.

Theorem

If R is an integral domain and $0_R \neq f, g \in R[x]$, then

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

Proof.

Suppose that R is an integral domain and $0_R \neq f, g \in R[x]$.
Write $f = \sum f_n x^n$ and $g = \sum g_n x^n$ and let d_f and d_g denote the degrees of f and g.
Then $fg = \sum_{n \geq 0} \left(\sum_{j=0}^{n} f_j g_{n-j} \right) x^n$.
First, note that if $n > d_f + d_g$, either $j > d_f$ or $(n-j) > d_g$ (otherwise $n = j + (n-j) \leq d_f + d_g$).
So, $f_j g_{n-j} = 0$ for all $n > d_f + d_g$.
Now, note that the coefficient of $x^{d_f + d_g}$ is $\sum_{k=0}^{d_f+d_g} f_k g_{d_f+d_g-k}$, and $k < d_f \Rightarrow d_f + d_g > k + d_g \Rightarrow d_f + d_g - k > d_g \Rightarrow g_{d_f+d_g-k} = 0$.
Also, $k > d_f \Rightarrow f_k = 0$.
Thus, $f_k g_{d_f+d_g-k} = 0$ except possibly when $k = d_f$.
So, the coefficient of $x^{d_f+d_g}$ is $f_{d_f} g_{d_g}$.
Since, R is an integral domain and since $f_{d_f} \neq 0$ and $g_{d_g} \neq 0$, it follows that $f_{d_f} g_{d_g} \neq 0$.
Thus $\deg(fg) = d_f + d_g$. $\square$

Corollary

If R is an integral domain, then so is $R[x]$.

Proof.

Suppose that $f \neq 0$ and $g \neq 0$ are elements in $R[x]$. Then f and g have some nonzero coefficients. Following the argument of the last proof, we see that fg will also have a nonzero coefficient (namely the coefficient of $x^{d_f+d_g}$), and is thus nonzero. So, $R[x]$ is an integral domain. $\square$

Note

By a the first part of the proof of our theorem, we have seen that if R is any ring and if $f, g \in R[x]$ are nonzero, then $\deg(fg) \leq \deg(f) + \deg(g)$.

Example

In $\mathbb{Z}_6[x]$ we have,

$$(3x + 1)(2x + 1) = 5x + 1.$$

Theorem

Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Then there exist polynomials $q, r \in F[x]$ satisfying the following.

1. $f = gq + r$.
2. *Either* $r = 0$ *or* $\deg(r) < \deg(g)$.