Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 5 : Polynomial Rings

Module 1 : Introduction to polynomials

e-Pathshala पाठशाला
A Gateway to All Post Graduate Courses

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

E-mail: anjankbhuniya@gmail.com

Introduction to polynomials

Learning Outcomes:

1. Formal definition of polynomials.
2. Degree of a nonzero polynomial.
3. Algebra of polynomials over a commutative ring with unity.
4. Units in the polynomial ring.

Let R be a commutative ring with unity 1. A polynomial over R is defined as an infinite sequence $(a_0, a_1, a_2, \cdots)$ such that all but finitely many a_i are 0, i.e. there is a nonnegative integer n (depending on the sequence $(a_0, a_1, a_2, \cdots)$ under consideration) such that $a_i = 0$ for all $i \geq n$; and the set of all polynomials on R is denoted by $R[x]$. Thus

$$R[x] = \{(a_0, a_1, a_2, \cdots) \mid a_i \in R \text{ and } a_i = 0 \text{ for all but finitely many } i\}$$

We now define addition and multiplication on $R[x]$ as follows:

$$\begin{aligned}
&(a_0, a_1, a_2, \cdots) + (b_0, b_1, b_2, \cdots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots) \\
\text{and } &(a_0, a_1, a_2, \cdots).(b_0, b_1, b_2, \cdots) = (c_0, c_1, c_2, \cdots), \\
&\qquad\qquad \text{where } c_i = \sum_{r=0}^{i} a_r b_{i-r} \text{ for } i = 0, 1, 2, \cdots .
\end{aligned}$$

We leave it to the reader to verify that $(R[x], +, .)$ is a commutative ring with unity $(1, 0, 0, \cdots)$. Also $(0, 0, \cdots)$ is the zero element of $R[x]$ and the additive inverse of $(a_0, a_1, \cdots)$ is $(-a_0, -a_1, \cdots)$.

The mapping

$$a \longrightarrow (a, 0, 0, \cdots)$$

is a monomorphism of the ring R into $R[x]$. Thus, R can be considered as a subring of $R[x]$ and we no longer distinguish between a and $(a, 0, 0, \cdots)$.

The particular element $(0, 1, 0, 0, 0, \cdots)$ is called the indeterminate over R and is usually denoted by x. Then according to the definitions of addition and multiplication in $R[x]$, we have

$$\begin{aligned}
x^2 &= (0, 1, 0, 0, \cdots)(0, 1, 0, 0, \cdots) = (0, 0, 1, 0, \cdots) \\
x^3 &= (0, 1, 0, 0, \cdots)(0, 1, 0, 0, \cdots) = (0, 0, 0, 1, 0, \cdots) \\
&\vdots
\end{aligned}$$

epathshala पाठशाला A Gateway to All Post Graduate Courses

and then

$$\begin{aligned} a_1x &= (a_1, 0, 0, \cdots)(0, 1, 0, \cdots) = (0, a_1, 0, 0, 0, \cdots) \\ a_2x^2 &= (a_2, 0, 0, \cdots)(0, 0, 1, 0, \cdots) = (0, 0, a_2, 0, 0, \cdots) \\ &\vdots. \end{aligned}$$

Thus we have

$$\begin{aligned} (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) &= (a_0, 0, 0 \cdots) + (0, a_1, 0, 0, \cdots) + \cdots + (0, \cdots, 0, a_n, 0, \cdots) \\ &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n. \end{aligned}$$

The elements $a_0, a_1, \cdots, a_n$ are called the coefficients of the polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. If $a_n \neq 0$, then a_n is called the leading coefficient and if the leading coefficient $a_n = 1$ then $p(x)$ is called a monic polynomial.

We define the zero element $(0, 0, 0, \cdots)$ of the ring $R[x]$ as the zero polynomial, and it will be denoted by 0. Thus a polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is zero if and only if $a_0 = a_1 = a_2 = \cdots = a_n = 0$.

Example 0.1. *Consider the polynomial ring $\mathbb{Z}_6[x]$. Then $f(x) = [2]x^3$ and $g(x) = [3]x^2$ are two nonzero elements of $\mathbb{Z}_6[x]$ but $f(x)g(x) = [0]$. This shows that $\mathbb{Z}_6[x]$ is not an integral domain.*

Now we characterize the rings R for which the associated polynomial ring $R[x]$ is an integral domain.

epathshala पाठशाला A Gateway to All Post Graduate Courses

Theorem 0.2. *Let R be a commutative ring with unity 1. Then $R[x]$ is an integral domain if and only if R is an integral domain.*

Proof. First assume that R is an integral domain. Then $R[x]$ is a commutative ring with 1. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$ be two nonzero polynomials in $R[x]$. Then, we may consider $a_n \neq 0$ and $b_m \neq 0$; and so $a_nb_m \neq 0$, since R is an integral domain. Then the polynomial $f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ is such that $c_{m+n} = a_nb_m \neq 0$. This implies that $f(x)g(x) \neq 0$. Thus, $R[x]$ is an integral domain.

The converse follows directly. □

In fact, even if R is a field then also $R[x]$ is not a field, for x has no multiplicative inverse.

Definition 0.3. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a nonzero polynomial in $R[x]$. If $a_n \neq 0$ then a_n is called the leading coefficient of $p(x)$; and n is called the degree of $p(x)$. It is denoted by* $\deg f(x)$. *In this case, a_n is called the leading coefficient of $f(x)$. If the leading coefficient is 1, then $f(x)$ is called a monic polynomial.*

We do not define degree of the zero polynomial.

During our school days we have seen that for two nonzero polynomials $f(x)$ and $g(x)$, $\deg f(x)g(x)$ is equal to the sum $\deg f(x) + \deg g(x)$. Recall that there we actually considered polynomials over the field of all real numbers where there is no zero divisors. Now we show that this result may not hold over an arbitrary ring. For example consider:

Example 0.4. *Consider the polynomial ring $\mathbb{Z}_6[x]$. Then $f(x) = [2]x^3+x+[1]$ and $g(x) = [3]x^2+[2]$ are two nonzero polynomials of degree 3 and 2, respectively. Now $f(x)g(x) = x^3 + [3]x^2 + [2]x + [2]$ shows that $\deg f(x)g(x) < \deg f(x) + \deg g(x)$.*

In general, we have the following inequality.

Theorem 0.5. *Let R be a commutative ring with unity and $f(x), g(x)$ be two nonzero polynomials in $R[x]$.*

1. *If $f(x)g(x) \neq 0$, then $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$. Equality holds if R is an integral domain.*

2. *If $f(x) + g(x) \neq 0$, then $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.*

Pathshala पाठशाला A Gateway to All Post Graduate Courses

Proof. (i) If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, then $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$. If $f(x)g(x) \neq 0$, then at least one of the coefficients of $f(x)g(x)$ is nonzero. Suppose $a_nb_m \neq 0$, then $\deg(f(x)g(x)) = n + m = \deg f(x) + \deg g(x)$. If $a_nb_m = 0$ (which can hold if R has zero divisors), then $\deg(f(x)g(x)) < n+m = \deg f(x)+\deg g(x)$.

(ii) If $\deg f(x) > \deg g(x)$, then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + \cdots + a_nx^n$ shows that the leading coefficient of $f(x)+g(x)$ is $a_n \neq 0$ and so $\deg(f(x)+g(x)) = n = \max\{\deg f(x), \deg g(x)\}$. If $\deg f(x) = \deg g(x)$, then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$ shows that either $f(x) + g(x) = 0$ or $\deg(f(x) + g(x)) \leq n = \max\{\deg f(x), \deg g(x)\}$ ($=$ or $<$ accordingly $a_n + b_n \neq$ or $= 0$). □

Now we characterize the units in a polynomial ring $R[x]$.

Theorem 0.6. *Let R be a commutative ring with 1. Then $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ is a unit if and only if a_0 is a unit and a_i is nilpotent in R for all $i = 1, 2, \cdots, n$.*

Proof. First assume that a_0 is a unit and $a_1, a_2, \cdots, a_n$ are nilpotents in R. Then $a_1x, a_2x^2, \cdots, a_nx^n$ are nilpotents and so $a_1x + a_2x^2 + \cdots + a_nx^n$ is a nilpotent in $R[x]$. Since a_0 is a unit, so it follows that $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a unit.

We prove the converse by induction on the $\deg f(x)$. If $\deg f(x) = 0$, then the result follows directly. Let us make our induction hypothesis that the result holds for every nonzero polynomial of degree less than n. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a unit in $R[x]$. Then there is a polynomial $b_0 + b_1x + \cdots + b_mx^m \in R[x]$ such that

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) = 1.$$

This implies that

$$a_0b_0 = 1 \tag{0.1}$$

$$a_0b_1 + a_1b_0 = 0 \tag{0.2}$$

$$a_0b_2 + a_1b_1a_2b_0 = 0 \tag{0.3}$$

$$\vdots$$

$$a_{n-2}b_m + a_{n-1}b_{m-1} + a_nb_{m-2} = 0 \tag{0.4}$$

$$a_{n-1}b_m + a_nb_{m-1} = 0 \tag{0.5}$$

$$a_nb_m = 0 \tag{0.6}$$

We multiply a_n to both sides of (0.5) and get

$$a_n^2b_{m-1} = 0.$$

Again multiplying a_n^2 to both sides of (0.4), we get

$$a_n^3b_{m-2} = 0.$$

Proceeding similarly we get $a_n^{m+1}b_0 = 0$. Since, by (0.1), b_0 is a unit, so $a_n^{m+1} = 0$. Thus a_n is a nilpotent and so is a_nx^n. Then it follows that $g(x) = f(x) - a_nx^n = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ is a unit, since $f(x)$ is a unit. Since $\deg g(x) < n$, so a_0 is a unit and $a_1, a_2, \cdots, a_{n-1}$ are nilpotents in R, by the induction hypothesis. Thus the result follows. □

1 Summary

- A polynomial over a commutative ring R with 1 is defined as an infinite sequence $(a_0, a_1, a_2, \cdots)$ such that al but finitely many a_i are 0.
- The set $R[x]$ of all polynomials is a commutative ring with unity, where
  - the zero element is $(0, 0, 0, \cdots)$;
  - the unity is $(1, 0, 0, \cdots)$;

epathshala पाठशाला A Gateway to All Post Graduate Courses

  - $-(a_0, a_1, \cdots) = (-a_0, -a_1, \cdots)$

- The particular element $(0, 1, 0, 0, 0, \cdots)$ is called the indeterminate over R and is usually denoted by x.

- A ring R is not an integral domain if and only if so is $R[x]$.

- For no commutative ring R with 1, the polynomial ring $R[x]$ is a field.

- If $p(x) \in R[x]$ is a nonzero polynomial then the largest integer n such that the coefficient of x^n is nonzero, is called the degree of $p(x)$.

- Let $f(x), g(x) \in R[x]$ be two nonzero polynomials. If F is an integral domain, then $f(x)g(x) \neq 0$ and $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

- A nonzero polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ over a commutative ring with 1 is a unit if and only if a_0 is a unit and a_i is nilpotent in R for all $i = 1, 2, \cdots, n$.

epathshala
पाठशाला
A Gateway to All Post Graduate Courses