

POLYNOMIAL RINGS

SUBJECT NAME: ABSTRACT ALGEBRA

Dr. S. VALARMATHI

ASSISTANT PROFESSOR

DEPARTMENT OF MATHEMATICS

G. VENKATASWAMY NAIDU COLLEGE

KOVILPATTI

POLYNOMIAL RINGS

Definition 0.0.1. A polynomial is of the form $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, which have coefficients form a ring R . The collection of all such polynomials form a ring called **polynomial ring**.

Let R be any ring. Let x be a symbol which is not an element of R . The symbol x is usually called an **indeterminate**.

Definition 0.0.2. Let R be a ring. A polynomial $f(x)$ with coefficients in R is defined to be an expression of the form $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, where n is a positive integer and $a_0, a_1, \dots, a_n \in R$, a_r is called the **coefficient of x^r** and a_rx^r is called a **term of the polynomial**. The set of all polynomials with coefficients in R is denoted by $R[x]$.

Note 0.0.3. $x, x^2, x^3, \dots, x^n$ are merely symbols.

Definition 0.0.4. $0 \in R[x]$ is called the zero polynomial.

Definition 0.0.5. Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $a_n \neq 0$ be an non-zero polynomial in $R[x]$. Then the degree of $f(x)$, written as $\deg f(x)$ is n and a_n is called the **leading coefficient of $f(x)$** . We do not define the degree of the zero polynomial. A polynomial in which the leading coefficient is 1 is called a **monic polynomial**. An element of R is called a **constant polynomial**. Clearly the degree of a non-zero constant polynomial is zero.

Example 0.0.6. $2x^3 + x^5$ is a monic polynomial.

Definition 0.0.7. Let $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ and $q(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$ be two polynomials in $R[x]$. $p(x)$ and $q(x)$ are said to be **equal** if $n = m$ and $a_i = b_i$ for all i .

Theorem 0.0.8. *Let R be any ring. Prove that $R[x]$ is a ring under the usual addition and multiplication of polynomials.*

Proof. [First we recall definition of a ring: A nonempty set R together with two binary operations denoted by " $+$ " and " $\cdot$ " are called addition and multiplication which satisfy the following axioms is called a ring.

(i) $(R, +)$ is an abelian group.

(ii) " $\cdot$ " is an associative binary operation on R (i.e. $a.(b.c) = (a.b).c$ for all $a, b, c \in R$).

(iii) $a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$ for all $a, b, c \in R$.]

Let R be any ring.

To prove that $R[x]$ is a ring

Now we define addition and multiplication in $R[x]$.

Let $f(x), g(x) \in R[x]$.

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ and

$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$.

We define $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots$ and

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1x + a_2x^2 + \dots + a_nx^n)(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) \\ &= c_0 + c_1x + \dots + c_{m+n}x^{m+n} \end{aligned}$$

where $c_0 = a_0b_0$

$$c_1 = a_0b_1 + a_1b_0$$

.....

$$c_r = a_0b_r + a_1b_{r-1} + \dots + a_rb_0$$

.....

$$c_{m+n} = a_nb_m.$$

(i) Let $f(x), g(x) \in R[x]$.

Clearly $f(x) + g(x)$ and $f(x)g(x) \in R[x]$.

The zero element of $R[x]$ is the zero polynomial ($0 + f(x) = f(x) + 0 = f(x)$).

If $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

then $-f(x) = -a_0 - a_1x - a_2x^2 - \dots - a_nx^n$ is the additive inverse of $f(x)$.

Also $f(x) + g(x) = g(x) + f(x)$.

Therefore $(R[x], +)$ is an abelian group.

(ii) $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$ and

$f(x).(g(x) + h(x)) = f(x).g(x) + f(x).h(x)$ for all $f(x), g(x), h(x) \in R[x]$ are straightforward. Hence $R[x]$ is a ring $\square$

Note 0.0.9. 1. $R[x]$ is called the **ring of polynomials** with coefficients in R .

2. If R is commutative, so also is $R[x]$.

3. If R is a ring with identity, so also is $R[x]$.

4. The set of all constant polynomials in $R[x]$ is a subring of $R[x]$ and is isomorphic to R .

Theorem 0.0.10. *Prove that $R[x]$ is an integral domain iff R is an integral domain.*

Proof. [First we recall definition of integral domain: A non commutative ring with identity having no zero-divisors is called an integral domain.

Thus in an integral domain $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.]

Let R be an integral domain.

To prove that $R[x]$ is an integral domain.

It is enough if we prove that the product of two non-zero polynomials is again a non-zero polynomial.

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, where $a_n \neq 0$

and $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$, where $b_m \neq 0$.

Now, $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_nb_mx^{n+m}$.

Since R is an integral domain, $a_n \neq 0$ and $b_m \neq 0 \Rightarrow a_nb_m \neq 0$.

Hence the coefficient of x^{m+n} in $f(x)g(x) \neq 0$.

$\therefore f(x)g(x) \neq 0$.

Thus $R[x]$ is an integral domain.

Conversely, let $R[x]$ be an integral domain.

Since R is a subring of $R[x]$ and $1 \in R$, hence R is an integral domain.

□

Note 0.0.11. In particular if R is an integral domain and $R[x]$ is an integral domain.

Corollary 0.0.12. If R is an integral domain and $f(x), g(x) \in R[x]$, then

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

For, we have proved that the coefficient of x^{n+m} in $f(x)g(x) = a_nb_m \neq 0$.

$$\therefore \deg f(x)g(x) = m + n = \deg f(x) + \deg g(x).$$

Note 0.0.13. If R is not an integral domain, then the above result is not true.

For example, consider $\mathbf{Z}_6[x]$ (since $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is not an integral domain).

$f(x) = x + 2x^2$ is a polynomial of degree 2 and

$g(x) = 2 + x + 3x^2$ is a polynomial of degree 2.

$$\begin{aligned}\text{But } f(x)g(x) &= (x + 2x^2)(2 + x + 3x^2) \\ &= 2x + x^2 + 3x^3 + 4x^2 + 2x^3 + 6x^4 \\ &= 2x + 5x^2 + 5x^3 + 6x^4 \\ &\equiv 2x + 5x^2 + 5x^3 + 0x^4 \pmod{6} \\ &= \text{is a polynomial of degree 3.}\end{aligned}$$

In general,

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

Note 0.0.14. *R is a field does not imply $R[x]$ is a field.*

Proof. Let R be a field.

Consider $f(x) = x \in R[x]$. To prove that $R[x]$ is not a field.

It is enough if we prove that the polynomial $f(x)$ does not have an inverse.

Suppose that $g(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ is the inverse of $f(x)$.

Then $(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)x = 1$.

$$\therefore a_0x + a_1x^2 + a_2x^3 + \dots + a_nx^{n+1} = 1.$$

$$\therefore 0 + a_0x + a_1x^2 + a_2x^3 + \dots + a_nx^{n+1} = 1 + 0x + 0x^2 + \dots + 0x^{n+1}.$$

$\therefore 0 = 1$ which is a contradiction.

Therefore the polynomial $f(x)$ does not have an inverse.

Hence $R[x]$ is not a field. □

Remark 0.0.15. Any polynomial ring over a field is a U.F.D.

Theorem 0.0.16. (*Division algorithm*) Let F be a field. Let $f(x)$ and $g(x)$ be two polynomials in $F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof.

$$\text{Let } f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, a_n \neq 0 \quad \text{and} \\ g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m, b_m \neq 0.$$

Consider the set $S = \{f(x) - g(x)s(x)/s(x) \in F[x]\}$.

Let $r(x)$ be an element of minimal degree in S .

Clearly $r(x) = f(x) - g(x)q(x)$ for some $q(x) \in F[x]$. Hence $f(x) = g(x)q(x) + r(x)$.

We claim that either $r(x) = 0$ or $\deg r(x) < m$.

Let $r(x) = c_0 + c_1x + c_2x^2 + \dots + c_tx^t, c_t \neq 0$ and $t \geq m$.

Now, consider the polynomial,

$$\begin{aligned} r_1(x) &= r(x) - c_tb_m^{-1}x^{t-m}g(x) \\ &= r(x) - c_tb_m^{-1}x^{t-m}(b_0 + b_1x + b_2x^2 + \dots + b_mx^m) \\ &= r(x) - (c_tb_m^{-1}x^{t-m} + \dots + c_tx^t). \\ &= \text{a polynomial of degree less than } t. \end{aligned}$$

$\therefore \deg r_1(x) < \deg r(x)$.

$$\begin{aligned}
\text{Also, } r_1(x) &= r(x) - c_t b_m^{-1} x^{t-m} g(x) \\
&= f(x) - g(x)q(x) - c_t b_m^{-1} x^{t-m} g(x) \\
&= f(x) - g(x)[q(x) + c_t b_m^{-1} x^{t-m}] \in S.
\end{aligned}$$

$\therefore r_1(x) \in S$ and $\deg r_1(x) < \deg r(x)$ which is a contradiction, since $r(x)$ is an element of minimal degree in S .

$\therefore \deg r(x) < m$.

Thus $f(x) = g(x)q(x) + r(x)$ where either

$$r(x) = 0 \quad \text{or } \deg r(x) < \deg g(x). \quad (1)$$

Now, we prove the uniqueness.

Suppose $f(x) = g(x)q_1(x) + r_1(x)$ where

$$r_1(x) = 0 \quad \text{or } \deg r_1(x) < \deg g(x) \quad (2)$$

$$\therefore 0 = g(x)[q(x) - q_1(x)] + [r(x) - r_1(x)] \quad (\text{by (1) and (2)})$$

$$\therefore g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

Since $\deg[r_1(x) - r(x)] < \deg g(x)$, the above equation holds good only if $q(x) - q_1(x) = 0$.

$$\therefore q(x) = q_1(x) \text{ and hence } r(x) = r_1(x). \quad \square$$