STUDY MATERIALS

(RING THEORY-II)

TOPIC: POLYNOMIAL RINGS

Mathematics Honours
Semester – 6

Paper – C14T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

Polynomial Rings :-

Let R be a ring and x be an indeterminate or a variable over R. The set of all polynomials in x over R is denoted by $R[x]$ and is defined by

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \mid a_i \in R, n \in \mathbb{Z}^+ \cup \{0\}\}.$$

Here a_i's are called the coefficients of polynomial. $R[x]$ is called the ring of polynomials over R in the indeterminate x.

Definitions :-

① If for some $n > 0$, $a_n \neq 0$ and $a_i = 0 \ \forall i > n$, then a_n is called the leading coefficient of the polynomial. And n is called the degree of the polynomial.

② If no such n exists, then the polynomial is of the form $a_0 + 0.x + 0.x^2 + \cdots + 0.x^n$, which is said to be a constant polynomial of degree 0.

③ If $a_i = 0 \ \forall i = 0, 1, 2, \cdots, n$, then the polynomial is said to be the zero polynomial of no degree assigned to it.

④ Equality in $R[x]$:-
Two polynomials $f(x) = a_0 + a_1x + a_2x^2 + \cdots$, and $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ in $R[x]$ are said to be equal, i.e., $f(x) = g(x)$ if $a_i = b_i, \forall i$. Two equal polynomials in $R[x]$ have the same degree.

⑤ Addition in $R[x]$:—

$f(x) + g(x) = c_0 + c_1 x + c_2 x^2 + \cdots$; $c_i = a_i + b_i \in R$.

$f(x), g(x) \in R[x] \Rightarrow f(x) + g(x) \in R[x]$

⑥ Multiplication on $R[x]$:—

$f(x) \cdot g(x) = d_0 + d_1 x + d_2 x^2 + \cdots$; $d_j = \sum_{i=0}^{j} a_i b_{j-i}$, $j = 0, 1, 2, \cdots$

i.e. $d_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0$.

⑦ It can be verified that —

(i) $(R[x], +)$ is a commutative group,

(ii) $(R[x], \cdot)$ is a semigroup,

(iii) Distributive laws hold in $R[x]$.

Therefore, $(R[x], +, \cdot)$ forms a ring and is said to be the polynomial ring over the ring R.

⑧ If R be a ring with unity 1, then $(R[x], +, \cdot)$ is also a ring with unity 1, which is the constant polynomial in $R[x]$.

⑨ If R be a commutative ring, then $(R[x], +, \cdot)$ is also a commutative ring.

Theorem : If R be an Integral domain, then show that $(R[x], +, \cdot)$ is so.

Proof :- Let $f(x), g(x) \in R[x]$ be non-zero s.t.

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$, with $a_m \neq 0$,

and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$, with $b_n \neq 0$.

Now $f(x) \cdot g(x) = d_0 + d_1 x + \cdots + d_{m+n-1} x^{m+n-1} + d_{m+n} x^{m+n}$;

where $d_{m+n} = a_m b_n \neq 0$, since $a_m \neq 0$, $b_n \neq 0$, and R contains no divisor of zero.

$\Rightarrow$ $f(x) \cdot g(x)$ is a non-zero polynomial in $R[x]$.

$\Rightarrow$ The ring $(R[x], +, \cdot)$ contains no divisor of zero.

Also $(R[x], +, \cdot)$ is a commutative ring with unity 1 $(a_0 = 1)$, as the ring R is an I.D.

$\therefore (R[x], +, \cdot)$ is an I.D.

Corollary:- If F be a field then the polynomial ring $(F[x], +, \cdot)$ is an I.D.

Since every field is a commutative ring with unity and contains no divisor of zero,

$\therefore$ Field F is an I.D.

$\Rightarrow$ The polynomial ring $(F[x], +, \cdot)$ is an I.D.

Theorem:- If R be a ring and $f(x)$, $g(x)$ be polynomials in $R[x]$, then $\deg(f(x) \cdot g(x)) \leq \deg f(x) + \deg g(x)$.

Equality sign holds if R be an I.D.

Let $f(x) = \sum_{i=0}^{m} a_i x^i$ with $a_m \neq 0$; and

$$g(x) = \sum_{i=0}^{n} b_i x^i \text{ with } b_n \neq 0.$$

Then $\deg f(x) = m$, $\deg g(x) = n$.

$f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_m b_n x^{m+n}$.

If R is not an I.D., and $a_m \cdot b_n = 0$,

then $\deg(f(x) \cdot g(x)) < m+n$

If R is an I.D., then $a_m \neq 0$, $b_n \neq 0 \Rightarrow a_m \cdot b_n \neq 0$,

So, $\deg(f(x) \cdot g(x)) = m+n$.

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

Corollary:- If $f(x) + g(x) \neq 0$ then

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

Definition: Let R be a ring. If $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, is a polynomial in $R[x]$, then n is called the degree of $f(x)$, denoted as $\deg f(x) = n$.

The constant polynomials in $R[x]$ are those elements from $R-\{0\}$. eg. $f(x)=a_0 \in R$.
Degree of a constant polynomial is 0.
However, zero polynomial, $0 \in R[x]$ has no degree.

Theorem:- Let R be an Integral domain, then the units in R are the only units of the ring $(R[x], +, \cdot)$

Let $f(x)$ be a unit in $R[x]$. Then $f(x) \neq 0$ and $\exists$ some $g(x) \in R[x]$, $g(x) \neq 0$ s.t.
$f(x) \cdot g(x) = g(x) \cdot f(x) = 1$, 1 being the unity in $R[x]$.

$\therefore \deg(f(x) \cdot g(x)) = \deg(1) = 0$

$\Rightarrow \deg f(x) + \deg g(x) = 0 \xrightarrow{\text{(since R is an I.D.)}} \deg f(x) = 0 = \deg g(x)$.

[$\because \deg f(x) \geq 0$, $\deg g(x) \geq 0$].

$\therefore$ $f(x)$, $g(x)$ are non-zero constant polynomials in $R[x]$, which are the elements of $R-\{0\}$.

$\therefore$ A non-zero $a \in R$ is a unit in $R[x]$ if there exists a non-zero $b \in R$ s.t. $a.b = b.a = 1$, i.e., if a be a unit in R.

$\therefore$ The units in R are the only units in $R[x]$.

~~**Cor.1.** If D be an I.D. then the units of D are the only units in the domain $D[x]$.~~

Cor. If F be a field, then the non-zero elements of F are the only units in the domain $F[x]$.

NOTE:- The polynomial ring $F[x]$ over a field F is not a field.

Because, if $p(x)$ be a non-constant polynomial in $F[x]$, then there does not exist any $q(x) \in F[x]$ s.t. $p(x) \cdot q(x) = 1$ (unity in $F[x]$), a constant polynomial in $F[x]$.

For example, let $p(x) = x \in F[x]$. $\nexists$ any $q(x) \in F[x]$ s.t. $x \cdot q(x) = 1$. $\therefore F[x]$ is not a field.

[$\deg(p(x) \cdot q(x)) = \deg 1 = 0$, which is not possible.]

Division Algorithm for polynomials :-

Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$f(x) = g(x) \cdot q(x) + r(x)$, where either $r(x) = 0$, or $\deg r(x) < \deg g(x)$.

Proof :- Existence of $q(x)$ & $r(x)$ in $F[x]$:-

If $f(x) = 0$, then $0 = g(x).0 + 0$; so that both $q(x)$ and $r(x)$ must be the zero polynomial.

If $f(x) \neq 0$ and let $\deg f(x) = n$, and $\deg g(x) = m$.

Case 1. $m > n$. Then let $q(x) = 0$ and $r(x) = f(x)$.

Case 2. $m \leq n$. We use here the 2nd principle of induction on n.

Let us assume that the theorem holds for all polynomials $f(x)$ of degree $< n$ and all $g(x) \neq 0$ s.t. $m \leq n$.

Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n$; $[a_n \neq 0]$,

and $g(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + b_m x^m$; $[b_m \neq 0]$.

Consider the polynomial $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$.

$\Rightarrow \deg f_1(x) < n$, or, $f_1(x) = 0$ in $F[x]$.

By induction hypothesis, there exist polynomials $q_1(x), r(x) \in F[x]$ s.t.

$f_1(x) = q_1(x) \cdot g(x) + r(x)$; either $r(x) = 0$, or $\deg r(x) < \deg g(x)$.

$\Rightarrow f(x) - a_n b_m^{-1} x^{n-m} g(x) = q_1(x) \cdot g(x) + r(x)$.

$\Rightarrow f(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)] \cdot g(x) + r(x) = q(x) \cdot g(x) + r(x)$

where $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x) \in F[x]$.

$\Rightarrow$ the theorem holds for all polynomials $f(x)$ of degree n and all polynomials $g(x) \neq 0$ s.t. $\deg g(x) \leq \deg f(x)$. So by the principle of induction, it holds for all polynomials $f(x), g(x) \in F[x]$ with $g(x) \neq 0$.

Uniqueness of $q(x)$ and $r(x)$:-

Suppose that there exist polynomials $q'(x), r'(x), q''(x), r''(x)$ in $F[x]$ s.t.

$f(x) = g(x)\cdot q'(x) + r'(x)$ with either $r'(x) = 0$, or $\deg r'(x) < \deg g(x)$

& $f(x) = g(x)\cdot q''(x) + r''(x)$ with either $r''(x) = 0$, or $\deg r''(x) < \deg g(x)$.

So that $f(x) = g(x)\cdot q'(x) + r'(x) = g(x)\cdot q''(x) + r''(x)$

$\Rightarrow g(x)\cdot[q'(x) - q''(x)] = r''(x) - r'(x)$.

If $q'(x) - q''(x) \neq 0$, then

$\deg(g(x)[q'(x) - q''(x)]) = \deg(r''(x) - r'(x)) \geq \deg g(x)$.

However, $\deg r''(x) < \deg g(x)$, $\deg r'(x) < \deg g(x)$.

$\therefore$ $r''(x) - r'(x)$ must be a zero polynomial.

$\Rightarrow$ $r''(x) = r'(x)$ and $\Rightarrow$ $q''(x) = q'(x)$.

Cor. 1. Remainders Theorem :-

Let F be a field and $a \in F$. If $f(x) \in F[x]$, then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

By Division algorithm, $\exists$ unique $q(x), r(x) \in F[x]$ s.t. $f(x) = (x-a)\cdot q(x) + r(x)$; $\begin{cases} r(x) = 0, \text{ or} \\ \deg r(x) < \deg(x-a) \\ \Rightarrow \deg r(x) = 0. \end{cases}$

Now let us put $x = a \in F$, then

$f(a) = (a-a)\cdot q(a) + r(a)$

$\Rightarrow$ $r(a) = f(a)$.

Cor. 2. Factor Theorem :-

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $(x-a)$ is a factor of $f(x)$.

By D. A., $\exists$ unique $q(x)$, $r(x)$ in $F[x]$, s.t. $f(x) = (x-a)\cdot q(x) + r(x)$. Let a be a zero of $f(x)$.

Then $0 = f(a) = 0 + r(a) \Rightarrow r(a) = 0$

$\Rightarrow f(x) = (x-a)\cdot q(x) \Rightarrow (x-a)$ is a factor of $f(x)$.

Conversely, if $(x-a)$ is a factor of $f(x)$, then we have $f(x) = (x-a)\cdot q_1(x)$; for some $q_1(x) \in F[x]$.
Now $f(a) = (a-a)\cdot q_1(a) = 0 \Rightarrow a$ is a zero of $f(x)$.

Cor. 3. Polynomial of degree n over a field has at most n zeros, counting multiplicity.

We do by induction on n.
A polynomial of degree 0 over a field has no zeros.
Let us suppose that $f(x)$ is a polynomial of degree n over a field F and a is a zero of $f(x)$ of multiplicity k.
Then $f(x) = (x-a)^k \cdot q(x)$ and $q(a) \neq 0$.
Now $\deg f(x) = \deg\{(x-a)^k \cdot q(x)\} = \deg(x-a)^k + \deg q(x)$
$\Rightarrow \quad n = k + \deg q(x). \Rightarrow k \leq n.$
If $f(x)$ has no zero other than a, then we are done.
If $b \neq a$ and b is a zero of $f(x)$, then
$0 = f(b) = (b-a)^k \cdot q(b) \Rightarrow q(b) = 0$
$\Rightarrow$ b is also a zero of $q(x)$ with same multiplicity as it has for $f(x)$.
By the 2nd principle of induction,
$q(x)$ has at most $n-k (= \deg q(x))$ zeros.
Thus, $f(x)$ has at most $k + n - k = n$ zeros.

Remark: Cor. 3. is NOT true for arbitrary polynomial rings.
For example, the polynomial x^2+5x+6 has FOUR zeros in Z_6.
$x^2+5x+6 \equiv 0 \pmod 6$
$\Rightarrow (x+2)(x+3) \equiv 0 \pmod 6$
$\Rightarrow x+2 \equiv 0 \pmod 6$ and $x+3 \equiv 0 \pmod 6$
$\Rightarrow x = 4$ $\Rightarrow x = 3$.

Also, when $x=0$, $0+5.0+6 \equiv 0 \pmod 6$
And when $x=1$, $1+5.1+6 \equiv 0 \pmod 6$
$\therefore$ The eqn has FOUR zeros: 0, 1, 3, 4.

Definitions:

1. Let R be a commutative ring with unity. An element $a \in R$ is said to be a zero or a root of a polynomial $f(x) \in R[x]$ if $f(a) = 0$ in R.

Example: Let us consider the polynomial
$f(x) = x^2 + 3x + 2 = (x+1)(x+2)$
$f(x)$ has only two zeros $-1, -2$ in the ring $(\mathbb{Z}, +, \cdot)$.
However, $f(x)$ has four zeros $\bar{1}, \bar{2}, \bar{4}, \bar{5}$ in the ring $(\mathbb{Z}_6, \oplus, \odot)$.
Because, $(x+\bar{1})(x+\bar{2}) \equiv \bar{0} \pmod 6$
$\Rightarrow x+\bar{1} \equiv 0 \pmod 6$ and $x+\bar{2} \equiv 0 \pmod 6$
$\Rightarrow x = \bar{5}$ and $\Rightarrow x = \bar{4}$.
Also when $x = \bar{1}$, $\bar{1}^2 + 3.\bar{1} + \bar{2} \equiv \bar{0} \pmod 6$.
and $x = \bar{2}$, $\bar{2}^2 + 3.\bar{2} + \bar{2} \equiv \bar{0} \pmod 6$.

2. Let R be a commutative ring with unity. If $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, then $a_n (\neq 0)$ is the leading coefficient, $\deg f(x) = n$. When $a_n = 1$, $f(x)$ is called a monic polynomial.
e.g. $x^2 + 3x + 2$ is a monic polynomial in $\mathbb{Z}[x]$.

Some Examples on Degree of polynomials:-

(1). Consider the polynomial ring $\mathbb{Z}_{12}[x]$.
Let $f(x) = \bar{4}x^2 + \bar{3}$ and $g(x) = \bar{5}x + \bar{8}$.
Then $f(x) \odot g(x) = (\bar{4}x^2 + \bar{3}) \odot (\bar{5}x + \bar{8})$
$= \bar{20}x^3 + \bar{32}x^2 + \bar{15}x + \bar{24} \equiv \bar{8}x^3 + \bar{8}x^2 + \bar{3}x + \bar{0}$
Hence $\deg(f(x) \odot g(x)) = 3 = \deg f(x) + \deg g(x)$
Let $h(x) = \bar{8}x^2 + \bar{9}$. Then $f(x) \oplus h(x) = \bar{12}x^2 + \bar{12}$
$= \bar{0}$
$\therefore \deg(f(x) + h(x))$ is not defined.

(2) Let $f(x) = \bar{4}x^2 + \bar{3}$ and $g(x) = \bar{3}x + \bar{4}$, then
$f(x) \odot g(x) = \bar{12}x^3 + \bar{16}x^2 + \bar{9}x + \bar{12} \equiv \bar{0}.x^3 + \bar{4}x^2 + \bar{9}x + \bar{0}$
$\therefore \deg(f(x) \odot g(x)) = 2 < 3 = \deg f(x) + \deg g(x)$.

Some Examples :-

1. Let R be a ring with unity. Show that $R[x]/\langle x\rangle \simeq R$.

Define $f : R[x] \longrightarrow R$ by $f(a_0+a_1x+\cdots+a_nx^n) = a_0$, $\forall\ a_0+a_1x+\cdots+a_nx^n \in R[x]$.

To show that f is well-defined and one-one, let us take $\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i$. $\Leftrightarrow a_0 = b_0 \Leftrightarrow f\left(\sum_{i=0}^{n} a_i x^i\right) = f\left(\sum_{i=0}^{m} b_i x^i\right)$.

f is onto, since for $a_0 \in R$, $\exists \sum_{i=0}^{n} a_i x^i \in R[x]$ s.t. $f\left(\sum_{i=0}^{n} a_i x^i\right) = a_0$.

$\therefore$ f is well-defined, one-one and onto.

To find $\ker f$. Let us consider

$f(a_0+a_1x+\cdots+a_nx^n) = 0$

$\Leftrightarrow a_0 = 0 \Leftrightarrow a_0+a_1x+\cdots+a_nx^n \in \langle x\rangle$

$\therefore \ker f = \langle x\rangle$.

To show f is a homomorphism, let us take $\sum_{i=0}^{n} a_i x^i \in R[x]$ and $\sum_{i=0}^{m} b_i x^i \in R[x]$.

$\therefore f\left(\sum_{0}^{n} a_i x^i\right) + f\left(\sum_{0}^{m} b_i x^i\right) = a_0 + b_0 = f\left(\sum_{0}^{n} a_i x^i + \sum_{0}^{m} b_i x^i\right)$

Also, $f\left(\sum_{0}^{n} a_i x^i\right) \cdot f\left(\sum_{0}^{m} b_i x^i\right) = a_0 \cdot b_0 = f\left[\left(\sum_{0}^{n} a_i x^i\right) \cdot \left(\sum_{0}^{m} b_i x^i\right)\right]$.

$\therefore$ f is an isomorphism with $\ker f = \langle x\rangle$.

Thus, by the first law of isomorphism of rings,

$R[x]/\langle x\rangle \simeq R$. (proved).