E-Learning Materials for Sem-6 (1):

Unit - 1, CC - 14

Topic - Ring theory & Linear Algebra-II

Date - 29.03.2020.

Prepaired by - Dr. Alauddin Dafadar

Scanned with CamScanner

Polynomial Rings :⇒ P(196) SK Mapa

Let R be a ring and x an indeterminate. By a polynomial in x over R we mean an expression $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where n is a non-negative integer and $a_0, a_1, \ldots$, an (called coefficient of the polynomial) all belong to R.

A polynomial in x is generally denoted by P(x), q(x), g(x) etc. The set of all polynomials over R is denoted by R[x].

i) Two polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$,

$g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$

are said to be equal if $a_0 = b_0$, $a_1 = b_1$, $\ldots$, $a_n = b_n$

ii) Addition of two polynomial f(x) and g(x)

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$,

$g(x) = b_0 + b_1x + b_2x_2 + \cdots + b_mx^m \in R[x]$

is defined by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots a_nx^n, \text{ if } m < n$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m, \text{ if } n < m$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \text{ if } n = m.$$

iii) Multiplication of two polynomials

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$

$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in R[x]$ is defined by

$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$, where

$c_j = a_0b_j + a_1b_{j-1} + \cdots + a_jb_0$ taking

$a_{n+1} = a_{n+2} = \cdots = a_{m+n} = 0$, $b_{m+1} = b_{m+2} = \cdots = b_{m+n} = 0$

Then $(R[x], +, \cdot)$ is a ring. It is called polynomial ring over R.

* If R be a ring with unity then the ring $(R[x], +, \cdot)$ is also a ring with unity.

** The identity element of the ring $(R[x], +, \cdot)$ is the constant polynomial 1, 1 being the unity in the ring R. Here $a_0 = 1$, $a_i = 0$, for $i \geq 1$.

*** The zero element of the ring is the zero polynomial 0 ($a_i = 0$ for all i).

Ex: ⇒ We consider the ring S

$$S = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z},\ n \geq 0\}$$

Then S forms a commutative ring with unity under addition and multiplication of polynomials.

This ring is denoted by $\mathbb{Z}[x]$.

Divisibility in an integral domain: ⇒ P-253

Let D be an integral domain and $a, b \in D$ with $a \neq 0$. If there exists an element c in D such that $b = ac$ then a is said to be divide b and it is expressed by the symbol $a|b$.

[*** Integral Domain: ⇒ A non trivial commutative ring R with unity contains no divisor of zero]

Every non zero element a in D divides 0 since $0 = a \cdot 0$

* Properties :⇒

Let D be an integral domain. Then

i) $a \mid a$ for every non-zero element a in D;

ii) $a \mid b$ and $b \mid c \Rightarrow a \mid c$ $(a \neq 0, b \neq 0)$.

iii) $a \mid b \Rightarrow a \mid bd$ for all $d \in D$.

● units and associates :⇒ A non zero element a in an integral domain D is said to be a unit in D if $a \mid 1$, 1 being the identity element in D. i.e.; a has a multiplicative inverse in D.

** Two non zero element a ~~and~~ and b in an integral domain D are said to be associates in D if $a = bu$ for some unit u in D.

$a = bu \Rightarrow b = au^{-1} = av$, where $v (= u^{-1})$ is a unit.

Ex 1 Find the units in the integral domain $\mathbb{Z}[i]$

⇒ The identity element in the domain is $1 (= 1 + 0i)$

Let $a + bi$ be a unit. Then $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ and there exists an element $c + id$ in the domain such that

$(a + ib)(c + id) = 1 + 0i$

This gives $(ac - bd) = 1$, $(ad + bc) = 0$.

$\therefore (a^2 + b^2)(c^2 + d^2) = 1$

Since a, b, c, d are integers, we have $a^2 + b^2 = 1$ and therefore either $a^2 = 1$, $b^2 = 0$ or, $a^2 = 0$, $b^2 = 1$ giving $a = \pm 1$, $b = 0$ or, $a = 0, b = \pm 1$

Hence the units in the domain are $1, -1, i, -i$.

Ex.2 Find the units in the integral domain $Z[x]$

⇒ The identity element in the domain is the constant polynomial 1.

Let $f(x)$ be a unit. Then $f(x)$ be a non zero polynomial in $Z[x]$.

And there exist a non-zero polynomial $g(x)$ in $Z[x]$ such that $f(x)g(x) = 1$

Let the degree of $f(x)$ and $g(x)$ be m and n respectively. Then $m \geq 0$, $n \geq 0$ and the degree of $f(x)g(x)$ is $m+n$.

Since $f(x)g(x) = 1$,

∴ The degree of $f(x)g(x)$ is 0.

∴ $m = 0$, $n = 0$ i.e; degree of $f(x) = 0$, degree of $g(x) = 0$

Consequently $f(x)$ and $g(x)$ are constant polynomials.

That is the units are the units in the ring Z.

Hence the units are 1 and -1.

Ex.3 Find the divisors of $1+i$ in the integral domain $Z[i]$

⇒ In the integral domain $Z[i]$ the units are $1, -1, i, -i$.

The improper divisor of $1+i$, $-(1+i)$, $1+i$, $i(1+i)$, $-i(1+i)$

To examine if $1+i$ has a proper divisor in the domain, let us assume $1+i = (a+ib)(c+id)$, where a, b, c, d are integers ——— (1)

Then $(ac - bd) = 1$, $ad + bc = 1$ and therefore

$(a^2+b^2)(c^2+d^2) = 2$ since a, b, c, d are integers

∴ $a^2+b^2 = 1$, $c^2+d^2 = 2$ or $a^2+b^2 = 2$, $c^2+d^2 = 1$

$a^2+b^2 = 1 \Rightarrow (a+ib)(a-ib) = 1 \Rightarrow a+bi$ is a unit

$c^2+d^2 = 1 \Rightarrow (c+di)(c-di) = 1 \Rightarrow c+di$ is a unit

By (1) $1+i$ has no proper divisor in the domain.

The only divisors of $1+i$ are the improper divisors of $1+i$.)

Multiplicative norm function on an integral domain :- 5

Let D be an integral domain. A norm function N on D is a mapping from D into the set Z satisfying the following conditions ——

1) $N(a) \geq 0$ for all $a \in D$
2) $N(a) = 0$ if and only if $a = 0$
3) $N(ab) = N(a)\,N(b)$ for all $a, b \in D$

Let D be an integral domain with a multiplicative Norm N. Then $N(u) = 1$ for every unit u in D.

Ex.1 Finds the units in the integral domain $\mathbb{Z}[i]$

⇒ On the domain $\mathbb{Z}[i]$, for $a \in \mathbb{Z}[i]$ we defined $N(a) = a \cdot \bar{a}$, i.e; $N(a+bi) = a^2+b^2$ Then

1) $N(a) \geq 0$ for all $a \in \mathbb{Z}[i]$
2) $N(a) = 0$ if and only if $a = 0$.
3) $N(ab) = N(a)\,N(b)$ for $a, b \in \mathbb{Z}[i]$

∴ N is a norm function on the domain.

Let $a \in \mathbb{Z}[i]$ be a unit. Then $N(a) = 1$,

Again $N(a) = 1 \Rightarrow a \cdot \bar{a} = 1$.

$\Rightarrow a$ is a unit, since $\bar{a} \in \mathbb{Z}[i]$

∴ a is a unit if and only if $N(a) = 1$

Let $a = a+bi$ be a unit

Then $N(a+bi)$ gives $a^2+b^2 = 1$ for integers a, b

This is possible if $a = \pm 1$, $b = 0$ or, $b \pm 1$ with $a = 0$

Therefore the units are $1, -1, i$ and $-i$

Ex.5 Find the units in the integral domain $\mathbb{Z}[\sqrt{-5}]$.

⇒ On the domain $\mathbb{Z}[\sqrt{-5}]$, for $\alpha \in \mathbb{Z}[\sqrt{-5}]$ we define $N(\alpha) = \alpha.\bar{\alpha} = a^2 + 5b^2$. Then

i) $N(\alpha) \geq 0$ for all $\alpha \in \mathbb{Z}[\sqrt{-5}]$

ii) $N(\alpha) = 0$ if and only if $\alpha = 0$

iii) $N(\alpha.\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$

∴ N is a norm function on the domain.

Let $\alpha \in \mathbb{Z}[\sqrt{-5}]$ be a unit. Then $N(\alpha) = 1$,

Again $N(\alpha) = 1$.

⇒ $\alpha.\bar{\alpha} = 1$

⇒ α is unit, since $\bar{\alpha} \in \mathbb{Z}[\sqrt{-5}]$

∴ α is a unit if and only if $N(\alpha) = 1$

Let $\alpha = a + b\sqrt{-5}$ be a unit

$N(\alpha) = 1$ gives $a^2 + 5b^2 = 1$ for some integers a, b

This is possible if $a = \pm 1$, $b = 0$.

Hence the unit in the domain are $1, -1$.

(Page- 257)

Irreducible element : ⇒ A non zero element a in an integral domain D is said to be a irreducible element in D if

i) a is not a unit in D, and

ii) The only divisors of a are unit in D and the associates of a.

** In other words, if a be an irreducible in D and $a = bc$, then, either b is a unit in D and c is an associate of a or c is a unit in D and b is an associate of a

References :- Higher Algebra - (8)
S.K. Mapa.