P.R. GOVT COLLEGE (A)
KAKINADA

GUNNAM PRASADA RAO

LECTURER IN MATHEMATICS

RING THEORY-SEM-IV

INTRODUCTION TO RINGS, SUBRINGS, IDEALS, HOMOMORPHISM, POLYNOMIAL RINGS

UNIT-3: PRINCIPAL IDEALS AND QUOTIENT RINGS

Principal ideal (Def): An ideal I of a ring R is said to be principal ideal of R if there exists $a \in I$ such that for any other ideal J of $R, a \in J$ *then* $I \subseteq J$.

If I is a principal ideal generated by an element $a \in R$ if (i) $a \in I$ (ii) $I$is an ideal of R

And (iii) for any ideal $J\ of\ R \ni a \in J \Longrightarrow I \subseteq J$

$\therefore I\ is\ the\ principal\ ideal\ generated\ by\ a\ and\ it\ is\ denoted\ by\ I =< a > or\ (a)$

Principal ideal ring (Def): A ring R is said to be principal ideal ring if every ideal of R is a principal ideal.

Theorem: The ring of integers $(\mathbb{Z};\ +,\cdot)$ is a principal ideal ring. (OR) Every ideal of $(\mathbb{Z};\ +,\cdot)$ is a principal ideal.

Proof: Let $(\mathbb{Z};\ +,\cdot)$ be the ring of integers and I be an ideal of $\mathbb{Z}, and\ I = \{0\}$

Then $I = (0), the\ ideal\ generated\ by\ zero\ element\ of\ \mathbb{Z}\ is\ a\ principal\ ideal.$

Let and I be an ideal of $\mathbb{Z}, and\ I \neq \{0\}$ $\quad \therefore \exists\ an\ element\ a \in I\ and\ a \neq 0$

$a \in I, \qquad I\ is\ an\ ideal\ \Longrightarrow -a \in I$

Since $I \subseteq \mathbb{Z} \Longrightarrow one\ of\ a, -a\ is\ a\ positive\ integer.$

Let $I^+ be\ the\ set\ of\ all\ positive\ integers\ then\ I^+ \neq \phi$

By well ordering principal I^+ has a least element say $'b'$

Now we show that $I =< b >, the\ ideal\ generated\ by\ 'b'$

Let $x \in I$

Since $x, b \in \mathbb{Z}\ and\ b \neq 0$ $\quad so\ by\ division\ algorithem\ for\ integer \exists\ q, r \in \mathbb{Z}\ such\ that$

$x = bq + r\ \ where\ 0 \leq r < b$

$b \in I, q \in \mathbb{Z}\ and\ I\ is\ an\ ideal \Longrightarrow bq \in I$

$x \in I, bq \in I \Longrightarrow x - bq \in I \Longrightarrow x - bq = r \in I$

But $0 \leq r < b\ and\ r \in I, b\ is\ the\ least\ positive\ integer\ of\ I^+\ in\ I \Longrightarrow r = 0$

$x = bq + r\ \Longrightarrow x = bq\ \ where\ q \in \mathbb{Z}$

Hence $x \in I \Longrightarrow x = bq\ \ where\ q \in \mathbb{Z}\ \Longrightarrow I = \{bq/q \in \mathbb{Z}\} \Longrightarrow I =< b >$

$\therefore I$ *is the principal ideal generated by* $'b'$ *hence* $\mathbb{Z}$ *is a principal ideal ring.*

Theorem : Every field is principal ideal ring

Proof: *We know that the ideal of* F *are* $\{0\}$*and* F *itself.*

$I = (0)$ *is the ideal generated by* 0.

$F = (1)$ *is the ideal generated by* 1.

$\therefore$ *Every ideal is a principal ideal.*

$\therefore$ *Every field is principal ideal ring*

Theorem: ***Every quotient ring of commutative ring also a commutative ring***

Proof: *Given that the set* $\frac{R}{I} = \{x + I / x \in R\}$

To Prove that the set $\frac{R}{I} = \{x + I / x \in R\}$ *is commutative ring.*

I. $\left(\frac{R}{I}, +\right)$ ***is a commutative group***:

(i) Closure property: *Let* $x + I, y + I \in \frac{R}{I}$ *where* $x, y \in R$

Now $(x + I) + (y + I) = (x + y) + I \in \frac{R}{I}$ *since* $x + y \in R$

(ii) Associative property: *Let* $x + I, y + I, z + I \in \frac{R}{I}$ *where* $x, y, z \in R$

$Now[(x + I) + (y + I)] + z + I = [(x + y) + z] + I$

$= [x + (y + z)] + I = (x + I) + [(y + I) + (z + I]$

(iii) Identity property: *Let* $x + I$ *be any element of* $\frac{R}{I}$

We have $0 + I \in \frac{R}{I}$ *since* $0 \in R$

Now $(x + I) + (0 + I) = (x + 0) + I = x + I$

$Also(0 + I) + (x + I) = (0 + x) + I = x + I$

$\therefore 0 + I = I$ *is the zero element of* $\frac{R}{I}$

(*iv*) *Inverse Property*: *Let* $x + I \in \frac{R}{I}$ *then* $x \in R \Longrightarrow -x \in R \Longrightarrow -x + I \in \frac{R}{I}$

Now $(x + I) + (-x + I) = (x - x) + I = 0 + I$

Also $(-x + I) + (x + I) = (-x + x) + I = 0 + I$

$\therefore -x + I$ *is the additive inverse of* $x + I$

(*v*) *Commutative property*: *Let* $x + I, y + I \in \frac{R}{I}$

Now $(x + I) + (y + I) = (x + y) + I$

$= (y + x) + I \quad (\because + \text{is a commutative})$

$= (y + I) + (x + I)$

$\therefore \left(\frac{R}{I}, +\right)$ *is a commutative group.*

***II*) $\left(\frac{R}{I}, \cdot\right)$ *is a semi group*.**

(*i*) *Closure property*: *Let* $x + I, y + I \in \frac{R}{I}$ *where* $x, y \in R$

Now $(x + I) \cdot (y + I) = (x \cdot y) + I \in \frac{R}{I}$ *since* $xy \in R$

(*ii*) *Associative property*: *Let* $x + I, y + I, z + I \in \frac{R}{I}$ *where* $x, y, z \in R$

Now $[(x + I) \cdot (y + I)] \cdot (z + I) = [(x \cdot y) \cdot z] + I$

$= [x \cdot (y \cdot z)] + I = (x + I) \cdot [(y + I) \cdot (z + I]$

***III*) $\cdot$ *is distributive under addition*:**

$(x + I) \cdot [(y + I) + (z + I)] = (x + I) \cdot [(y + z) + I)] = x(y + z) + I$

$= (xy + xz) + I = (xy + I) + (xz + I) = (x + I)(y + I) + (x + I)(z + I)$

similarly we can prove that

$[(y + I)(z + I)] \cdot (x + I) = (y + I)(x + I) + (z + I)(x + I)$

$\therefore \left(\frac{R}{I}, +, \cdot\right)$ *is a ring*

IV) Commutative property: *Let* $x + I, y + I \in \frac{R}{I}$ *where* $x, y \in R$

Now $(x + I) \cdot (y + I) = (x \cdot y) + I$

$= yx + I \quad since \ \cdot \ is \ a \ commutative \ in \ R$

$= (y + I)(x + I)$

$\therefore \left(\frac{R}{I}, +, \cdot\right)$ *is a commutative ring*

Quotient ring (Def): Let R be a ring and I be an ideal of R. Then the set $\frac{R}{I} = \{x + I / x \in R\}$ is a ring under the co-set addition and multiplication. This ring is called as quotient ring.

Here $0 + I$ *is the zero element of* $\frac{R}{I}$ *and* $1 + I$ *is the unity element of* $\frac{R}{I}$

Theorem1: ***The quotient ring*** $\frac{\mathbb{Z}}{p\mathbb{Z}}$ ***is a field where p is any prime number***

Proof: *Let p be a given prime number. Since* $\mathbb{Z}$ *is a commutative ring with unity*

so $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *is also commutative ring with unity . To prove that* $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *is a field. For this we have*

to show that every non − zero element in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *has multiplicative inverse.*

Let $a + p\mathbb{Z} \neq 0 + p\mathbb{Z}$ *be a non − zero element of* $\frac{\mathbb{Z}}{p\mathbb{Z}}$

$\Longrightarrow a - 0 \notin p\mathbb{Z} \Longrightarrow a \notin p\mathbb{Z}$ *and hence* $p \nmid a$

Since p isa prime and $p \nmid a$ *so* $(a, p) = 1 \Longrightarrow \exists\, s, t \in \mathbb{Z}$ *such that* $as + pt = 1$

$\Longrightarrow 1 - as = pt \in p\mathbb{Z} \Longrightarrow 1 - as \in p\mathbb{Z} \Longrightarrow 1 + p\mathbb{Z} = as + p\mathbb{Z}$

$\Longrightarrow 1 + p\mathbb{Z} = (a + p\mathbb{Z})(s + p\mathbb{Z})$

Theorem2: ***Let R be ring of characteristic*** $n > 0$. ***For any ideal I of R, then the characteristic of factor ring*** $\frac{R}{I}$ ***is a positive divisor of n.***

Proof: *Let I be an ideal of R and chr. of R is n.*

By definition so there exist a least positive integer n such that $na = 0 \ \forall a \in R$.

Let $a + I \in \frac{R}{I}$

Now $n(a+I) = (a+i) + (a+I) + \cdots + (a+I)$

$$= (a + a + a + \cdots + a) + I = na + I = 0 + I$$

$\therefore n(a+I) = 0 + I \quad \forall\, a + I \in \frac{R}{I}$

$\therefore$ *The characteristic of factor ring* $\frac{R}{I}$ *is a positive divisor of* n

Problems

1. *Determine all the ideals of the ring $\mathbb{Z}$ of integers.*

Sol: *For any non $-$ negative integer n, the set* $n\mathbb{Z} = \{na / a \in \mathbb{Z}\}$

We shall prove that every ideal must be of the form $n\mathbb{Z}$ *forsome non $-$ negative integer n. Let I be any ideal of $\mathbb{Z}$*

If $I = 0$ *then* $I = 0\mathbb{Z}$

If $I \neq 0 \therefore \exists$ *an element* $a \in I$ *and* $a \neq 0$

$a \in I$, $\quad I$ *is an ideal* $\implies -a \in I$

Since $I \subseteq \mathbb{Z} \implies$ *one of* $a, -a$ *is a positive integer.*

Let n be a least positive integer in I. We shall prove that $I = n\mathbb{Z}$

Since $n \in I, I$ *is an ideal, we get* $n\mathbb{Z} \subseteq I \rightarrow (1)$.

On the other hand, $\quad$ *Let b be any element in I.*

Since $b, n \in I$ *and* $b \neq 0$ *so by division algorithem for integer* $\exists\, q, r \in \mathbb{Z}$ *such that*

$b = nq + r$ *where* $0 \leq r < n$

$n \in I, q \in \mathbb{Z}$ *and I is an ideal* $\implies nq \in I$

$b \in I, nq \in I \implies b - nq \in I \implies b - nq = r \in I$

But $0 \leq r < n$ *and* $r \in I, n$ *is the least positive integer of* $I \Longrightarrow r = 0$

$b = nq + r \Longrightarrow b = nq$ *where* $q \in \mathbb{Z}$

Hence $b \in I \Longrightarrow b = nq \in n\mathbb{Z} \Longrightarrow I \subseteq n\mathbb{Z} \longrightarrow (2)$

From (1)& (2); *Thus* $I = n\mathbb{Z}$

2. *Determine all ideals of the ring* $\mathbb{Z}_n$ *of integers modulo n, where n is any positive integer.*

Sol: *Let n be a fixed positive integer. Then* $\mathbb{Z}_n = \{0,1,2,3 \ldots (n-1)\}$ *is ring under* $+_n, \cdot_n$

If $n = 1$ *then* $\mathbb{Z}_n = \{0\}$ *in which* $\{0\}$ *is the only ideal*

If $n > 1$, *For any positive divisor m of n for which* $m < n$.

Let $m\mathbb{Z}_n = \{m \cdot_n x / x \in \mathbb{Z}_n\}$ *Then clearly* $m\mathbb{Z}_n$ *is an ideal of* $\mathbb{Z}_n$.

On the other hand , let I be any non $-$ *zero ideal of* $\mathbb{Z}_n$.

Let m be a least positive integer in I. We shall prove that $I = m\mathbb{Z}_n$

Since $m \in I, I$ *is an ideal of* $\mathbb{Z}_n$ *we get* $m\mathbb{Z}_n \subseteq I \rightarrow (1)$.

Let a be any element in Isuch that $a \neq 0$

Since $a, m \in I$ *and* $a \neq 0$ *so by division algorithem for integer* $\exists\, q, r \in \mathbb{Z}$ *such that*

$a = mq + r$ *where* $0 \leq r < m$

$m \in I, q \in \mathbb{Z}$ *and I is an ideal* $\Longrightarrow mq \in I$

$a \in I, mq \in I \Longrightarrow a - mq \in I \Longrightarrow a +_n (m \cdot_n (-q)) = r \in I$

But $0 \leq r < m$ *and* $r \in I, m$ *is the least positive integer of* $I \Longrightarrow r = 0$

$a = mq + r \Longrightarrow a = mq$ *where* $q \in \mathbb{Z}$

Hence $a \in I \Longrightarrow a = mq \in m\mathbb{Z}_n \Longrightarrow I \subseteq m\mathbb{Z}_n \longrightarrow (2)$

From (1)& (2); *Thus* $I = m\mathbb{Z}_n$

Hence the ideals of $\mathbb{Z}_n$ *are precisely of the form* $\{0\}$ *and* $m\mathbb{Z}_n$

where m is proper positive divisor of n

3. *List all the ideals of* $\mathbb{Z}_{24}$

Sol: *The proper positive divisor of* 24 *are* 1,2,3,4,6,8, *and* 12.

$\therefore$ *The ideals of* $\mathbb{Z}_{24}$ *are* $I_0 = \{0\}, I_1 = 1 \cdot \mathbb{Z}_{24} = \mathbb{Z}_{24}$

$I_2 = 2 \cdot \mathbb{Z}_{24} = \{0,2,4,6,8,10,12,14,16,18,20,22\}$

$I_3 = 3 \cdot \mathbb{Z}_{24} = \{0,3,6,9,12,15,18,21\}$

$I_4 = 4 \cdot \mathbb{Z}_{24} = \{0,4,8,12,16,20\}$

$I_5 = 6 \cdot \mathbb{Z}_{24} = \{0,6,12,18\}$

$I_6 = 8 \cdot \mathbb{Z}_{24} = \{0,8,16\}$

$I_7 = 12 \cdot \mathbb{Z}_{24} = \{0,12\}$