COURES 1-RINGS

The Ideals

LECTURE 1

Def: Let $(S , + , .)$ be a subring of $(R , + , .)$ We say that S an ideal of R if.

1. $a - b \in S \, \forall s, b \in S$
2. $a. r \in S \;\; \forall a \in S , r \in R$

Ex: $(Z_{12} , +_{12} , ._{12})$. let $S = \{0,3,6,9\}$. show that S is in Z_{12}

a.r	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	3	6	9	0	3	6	9	0	3	6	9
6	0	6	0	6	0	6	0	6	0	6	0	6
9	0	9	6	3	0	9	6	3	0	9	6	3

a-b	0	3	6	9
0	0	3	6	9
3	9	0	3	6
6	6	9	0	3
9	3	6	9	0

Remark: The zero of the ring R belong to ideal I of R. because if $x \in I \longrightarrow 0. x = 0 \in I$

Ex: $I_1 = \{0,2,4\}$ is an ideal of Z

Ex: $I_1 = \{0,3\}$ is an ideal of Z_6

Ex: Prove that $A = \{nr, r \in Z\} = nZ$ is a ideal of Z Solution:

Let $a = nr , b = kr : a, b \in A$

$a - b = nr - kr = (n - k)r \Rightarrow (n - k)r \in A \Longrightarrow a - b \in A$

$a. b = (nr). (kr) = (nk)r \in A \Rightarrow a. b \in A$ A is a ideal of Z

Def: We say that for any ideal deference R is proper ideal.

Def: We say that the ring which no proper ideal not zero is simple ring.

Solution: Q // In (Z , + .) find (4) ∩ (6)

$(4) = \{\ldots . , -8 ,-4 , 0 , 4 ,8\ 12 ,\ldots \}$

$(6) = \{ \ldots\ldots . . , -12 , -6 , 0 , 6 ,12 \;, \ldots . \}$

$(4) \cap (6) = \{ \ldots , -24 ,-12 ,0 ,12 ,24 ,\ldots . \} = (12)$

Find (4) ∩ (6) ∩ (10)

Ex: Let Z_6 be a ring find tow ideals of Z_6 Solution:

$I_1 = \{0,2,4\}$, $I_2 = \{0,3\}$

LECTURE 2

Def: Let R be a ring and I an ideal of R if I subgroup of commutative group (+), then R/I . Is called quotient group of R.

Def: Let R be a ring and I an ideal of R. then $\frac{R}{I}$ is called quotient ring of R.

$$\therefore \frac{R}{I} = \{ a + I : a \in R \} \ni a + I = a + c \, ; i \in I$$

Remark:

1. (a + I) + (b + I) = (a + b) + I
   (a + I)(b + I) = ab + I
2. The identity with (+) is 0 + I
3. The inverse with (+) is -a + I

Not: (a + I) + (-a + I) = (a + (-a)) + I = 0 + I

Ex: $\frac{Z}{Zn} = 0 + nZ \, , 1 + nZ \, , 2 + nZ \, , \ldots \ldots (n-1) + nZ$

Such that nZ is an ideal

Theorem: Prove that $(\frac{R}{I}, +, .)$ Is a ring.

Proof: T.P $(\frac{R}{I}, +)$ is commutive group:

$\mp$

$$\forall x, y \in \frac{R}{I} \rightarrow x = a + I \;\; and \;\; y = b + I$$

Now: $x + y = (a + I) + (b + I) = (a + b) + I \in \frac{R}{I}$,Then is closed

$$\forall x, y, z \in \frac{R}{I} \rightarrow x = a + I \;\; , y = b + I \;\;\; and \;\; z = c + I$$

$$x + (y + z) = (a + I) + [(b + I) + (c + I)]$$
$$= (a + I) + [(b + c) + I]$$

$= [(a + (b + c)) + I\ ]$

$= [((a + b) + c) + I] = [(a + b) + I] + (c + I)$

$= [(a + I) + (b + I)] + (c + I)$

$= (x + y) + z$

∴ associative

$e = 0 + I \in \frac{R}{I}$ because

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

∴ e = 0 + I is identity

$(a + I) + (-a + I) = (a + (-a) + I) = (a - a) + I = 0 + I$

$-a + I$ is invers

∴ group

$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$ ∴ commutive group

T.P $(\frac{R}{+}, .)$ is semi group

$\forall\ x, y \in \frac{R}{I} \rightarrow x = a.I\ \ and\ \ y = b.I$

Now: $x.y = (a.I) + (b.I) = (a.b) + I \in \frac{R}{I}$,Then is closed

$\forall\ x, y, z \in \frac{R}{I} \rightarrow x = a.I\ \ , y = b.I\ \ \ and\ \ z = c.I$

$x.(y.z) = (a.I).[(b.I).(c.I)]$

$= (a.I).[(b.c).I]$

$= [(a.(b.c)).I\ ]$

$= [((a.b).c).I] = [(a.b).I].(c.I)$

$= [(a.I).(b.I)].(c.I)$

$= (x.y).z$

∴ semi group

$\forall\ x, y, z \in \frac{R}{I} \rightarrow$

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

$= x(y + z) + I$

$= (xy + xz) + I$

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

∴ Distributive ∴ $(R, +, .$

$)$ Is Ring

I

LECTURE 3

Ex: consider $(\frac{Z}{(3)}, +, .)$

$$\frac{Z}{(3)} = \{0 + (3), 1 + (3), 3 + (3)\}$$

$$= \{ \{\dots -6, -3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, 7, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\} \}$$

$$= \{ [0]_{mod\ 3}, [1]_{mod\ 3}, [2]_{mod\ 3} \} = Z_3$$

In general:

$(\frac{Z}{n}) = Z_n ;\ n \in \{1,2,3,\dots\}$

Def: Let R, S be two rings. A function $f: R \to S$ is called ring homomorphism if.

1. $f(a + b) = f(a) + f(b) \quad \forall a, b \in R$
2. $f(a.b) = f(a).f(b)$

Q: R ring. R commutative ⇔ $(a + b)^2 = a^2 + 2ab + b^2 \ \ \forall a, b \in R$ Solution:

Let R be a comm.

T.P : $(a + b)^2 = a^2 + 2ab + b^2 \ \ \forall a, b \in R$

$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ab + b^2$

$a^2 + 2ab + b^2$

Let: $(a + b)^2 = a^2 + 2ab + b^2$

We get $ab + ba = 2ab = ab + ab$

∴ $ab + ba = ab + ab$

∴ $ba = ab$

∴ comm

Theorem: let R be an integral domain. If

1. $a^2 = 1 \to a \in \{+1, -1\}$
2. $(P(X), \Delta, \cap)$ is a ring. Show that it is contains divisors of zero.

Proof:

1. $a^2 = 1 \to a^2 - 1 = 0 \ (a - 1)(a + 1) = 0$

   $a = 1 \ \ OR \ a = -1$

2. $\emptyset \neq A \subset X, \forall A \in P(X)$
$A \, \Delta \, A = (A \cup A) - (A \cap A)$
$= A - A = \emptyset$

LECTURE 4

$\therefore \exists$ zero divisors.

Ex: $(Z_{12}, +_{12}, ._{12})$. prove that there exist an ideal of $(Z_{12}, +_{12}, ._{12})$ has zero divisors (H.W) We know conditional of ideal are both $a - b \in S \text{ and } a.r \in S \; \forall a \in S, r \in R$ s.t S is subring

a.r	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	3	6	9	0	3	6	9	0	3	6	9
6	0	6	0	6	0	6	0	6	0	6	0	6
9	0	9	6	3	0	9	6	3	0	9	6	3

a-b	0	3	6	9
0	0	3	6	9
3	9	0	3	6
6	6	9	0	3
9	3	6	9	0

We can say that $S = \{0,3,6,9\}$ is IDEAL And has
zero divisors: $(6 \times 8) mod\ 12 = 0$

Remark: Let S be a subring of R. If S has 1 of the mother R, Then S an integral domain.

Ex: $h: Z \rightarrow Z_n \ni h(m) = [m]_{mod\ n}$ show that h is homeomorphism.

Solution:

Clearly h is a function. Why??

1. $h(m_1 + m_2) = [m_1 + m_2]_{\ mod\ n}$

   $= [m_1]_{mod\ n} +_{mod\ n} [\ m]_{mod\ n} \; \forall m_1, m_2 \in Z$

2. $h(m_1 . m_2) = [m_1 . m_2]_{\ mod\ n}$

   $= [m_1]_{mod\ n} ._{mod\ n} [\ m]_{mod\ n} \; \forall m_1, m_2 \in Z \;\; h(m_1). h(m_2)$

$\therefore$ h is a homomorphism.

Def: Let $h: R \rightarrow S$ be a ring **homomorphism.** If h is onto and one-one then h is called **isomorphism**.

Ex: let R be a ring and $h: R \rightarrow R$ defined as: $h(r) = r \; \forall r \in R$ (i.e: h is identity mapping). Then h is isomorphism Solution:

We must prove that:

1. h homomorphism
2. h on to
3. one – one

1. $h(r_1 + r_2) = r_1 + r_2 = h(r_1) + h(r_2)$ $h(r_1 . r_2) = r_1 . r_2 = h(r_1).h(r_2)$

   ∴ h homomorphism

2. $\forall\, x \in R, \exists y \in R \ni h(y) = x$ (Def: Onto)

   $\forall\, x \in R, \exists y \in R \ni h(y) = x$

   ∴ h onto

3. $Let\ h(x) = h(y) \rightarrow x = y$

∴ h one – one

∴ h isomorphism

Remarks:

1. Let R be an integral domain with 1. If S is a subring of R with 1, then S is an integral domain
2. Let $h: R \rightarrow S$ be a homomorphism. (ring homo). Then :
   - $h(O_R) = O_s$
   - $h(-a) = -h(a)$
   - $h(1_R) = 1_S$
   - $h(a^{-1}) = (h(a))^{-1}$

LECTURE 5

Kernal of homomorphism

Def: Let $h: R \to S$ be a ring homo. Then kernal of h is defined as:

$Ker(h) = \{x \in R : h(x) = 0\}$

Q: prove that $Ker(h)$ is an ideal in R.

Solution:

$h(0) = 0 \to 0 \in Ker(h)$

$\therefore Ker(h) \neq \emptyset$.

-

1- $\forall\, x, y \in Ker(h) \to x - y \in Ker(h)$

$h(x - y) = h(x) + h(-y)$ hom

$= h(x) + (-h(y))$

$= h(x) - h(y)$

$\in Ker(h)$ $\in Ker(h)$

$\therefore x - y \in \ker(h)$ why??

2- $\forall\, x \in Ker(h), y \in R \to x.y \in Ker(h)$ *and* $y.x \in Ker(h)$

والدليل على ذلك: $h(x.y) = h(x).h(y)$

$= 0 . h(y)$

$= 0 \in Ker(h)$

Def: Let R,S be two rings. We say that R embed in S if :

$R \cong S' \ni S'\ subring\ of\ S$

Not: $\cong$ means $\exists\ h: R \to S \ni h$ is $1-1$ and homomorphism.

Theorem: Any ring can be embedded in a ring with 1.

Proof:

Let R be any ring.

Let $R \times Z = \{(r, n) ; r \in R , n \in Z\}$ Let $(R \times Z, +, .)$ Be a ring with $1 = (0,1)$ $h: R \to R \times Z \ni$

$h(r) = (r, 0)\ \forall r \in R$

$h(r_1 + r_2) = (r_1 + r_2, 0)$

$= (r_1, 0) + (r_2,0) \to h(r_1) + h(r_2)$

الان $_2 h(r_1 . r_2) = (r_1 . r_2, 0) = (r_1, 0).(r_2, 0) = h(r_1).h(r)$

$h(r_1) = h(r_2) \to (r_1, 0) = (r_2,0) \to r_1 = r_2$

$\therefore h \ is \ 1 - 1$

1-1 + hom

LECTURE 6

Natural homomorphism

Def: Let R be a ring and I be an ideal in R. Then natural homo. Is defined $Nat_I: R \to {}^{R}/_{I}$

$Nat_I(x) = x + I \ \forall x \in R$

1- $Nat_I(x + y) = (x + y) + I$

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

$= Nat_I(x) + Nat_I(y)$

2- $Nat_I(x . y) = (x . y) + I$

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

$= Nat_I(x).Nat_I(y)$

Remark: Nat_I is onto homo.

$$\forall \ x + I \ \in \frac{R}{I} \ ; \ \exists \ x \in R : \ Nat_I(x) = x + I$$

∴ onto

Theorem: Let $h: R \to S$. Be a ring homo. Then h is 1-1 ⇔ Ker(h) = {0}

Proof: ⇒

Suppose that h is 1-1

T.P Ker(h) = { 0 }

Let $x \in Ker(h) \to h(x) = 0$

$\therefore x = 0 \Rightarrow Ker(h) = 0$ ⇐

Let $Ker(h) = 0$

Suppose h(x) = h(y) $\forall x, y \in R$

$h(x) - h(y) = 0$

$Ker(h)$

$\Longrightarrow h(x-y)=0 \Longrightarrow x-y \in$

$\therefore x-y=0 \Longrightarrow x=y$

$\therefore$ h is 1-1

Theorem: Let $h: R \to S$ be a ring homo and onto. then $\frac{R}{Ker(h)} \cong S$

Proof:

We must prove that homo & 1-1 & onto??? Homo: $f(x+Ker(h)+yKer(h))$

$= f((x+y)+Ker(h))$

$= (f(x+y))+Ker(h)$

$= f(x+Ker(h))+f(y+Ker(h))$

Also, $f\ ((xKer(h)).(y+Ker(h)))$

$= f(x.y)+Ker(h)$

$= f(x.Ker(h)).f(y.Ker(h))$

$\therefore$ Homom Onto: $\forall y \in S\ ;\ \exists x+Ker(h) \in \frac{R}{K}$

$\therefore y = f(x+Ker(h))$

$\therefore$ onto

$1-1$: Let $f(x+Ker(h)) = f(y+Ker(h))$

$f(x)=f(y)$

$f(x)-f(y)=0$

$f(x-y)=0$

$x-y=0$

$\therefore x=y$

LECTURE 7

Q: Let $f: z \to z$ be a homo. Then $f=0\ or\ f=I_z$ Proof:

Suppose that $f \neq 0 \therefore$ T.P

$f = I_z$??

$f(n) = f(\underbrace{1+1+\cdots+1}_{\text{n - times}})$

$= \underbrace{f(1)+f(1)+\cdots+f(1)}_{\text{n - times}}$

Also:

$$f(-n) = f(\underbrace{-1-1-1-\cdots-1}_{n\text{ - times}})$$

$= n\,f(-1) = -nf(1)$. There

$f(n) = nf(1)$ ______________________(1)

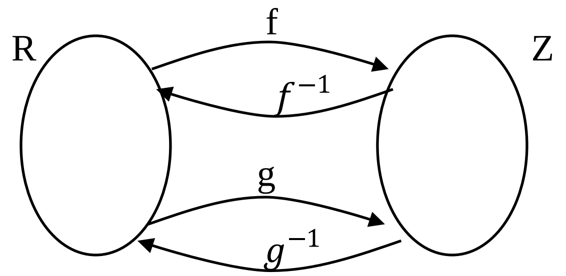
$f(n) = f(n.1) = f(n)\,.f(1)$ _________(2)

$\therefore n\,f(1) = f(n)\,f(1) \Longrightarrow f(n) = n \Longrightarrow f = I_Z$ Q: Let R be a ring. Then there exists at most one isomorphism $h: R \to Z$ Proof:

$fog^{-1}: Z \to Z$

$\therefore fog^{-1} = i_Z$

$\therefore f = g$ Whey



Theorem: Let R be a ring. Then any onto homo. from R to Z can be determine by its kernel

Proof:

Suppose that $R \underset{g}{\overset{f}{\rightarrow}} Z$

Suppose that f, g are two onto homos.

$\frac{R}{Ker(f)} \cong Z$

$\frac{R}{Ker(g)} \cong Z$

$\frac{R}{Ker(f)} \cong \frac{R}{Ker(g)}$

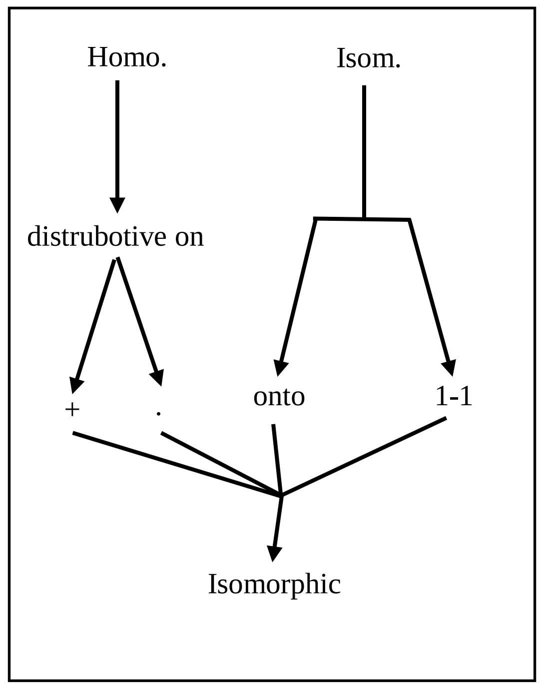
$\therefore Ker(f) = Ker(g)$

$h_1: \frac{R}{Ker(f)} \to Z$ isomorphism

$h_2: \frac{R}{Ker(f)} \to Z$ isomorphism

$\because h_1 = h_2$ Whey ??

$\therefore Ker(f) = Ker(g)$



LECTURE 8

Fields

Def: Let $(R, +, .)$ be a commutative ring with identity, So $R^{-1} = R - \{0\}$

Any non-Zero element in R has an inverse. Then we say that $(R, + , .)$ Is filed

Remark: Every field is a ring

Theorem: Every field is a integral domain. But the converse is not true.

Proof:

Let $(F, + , .)$ Be a field. We need to prove that F has non-Zero divisors??

$a . b = 0$ for some $a, b \in F$ $a \neq 0$

$a^{-1}(a. b) = 0 \rightarrow a^{-1}(a. b = 0)$

$\rightarrow (a^{-1}. a). b = 0$

$e. b = 0$

$b = 0$

∴ F has non-zero divisors ∴ F integral domain.

Ex: $(Z, + , .)$ Is integral domain because has nonzero divisors but $(Z, + , .)$ not filed

$2 \in Z^{-1} \rightarrow$

Ex: $(R^{*}, + , .)$ Is a field why?

Ex: $(Q , + , .)$ Is a field why?

Ex: $(Z , + , .)$ Is not a field why?

Remark: If $F = \{a + b\sqrt{3} : a, b \in Q \}$ then

$I_{+} = 0 + 0\sqrt{3}$

$I_{.} = 1 + 0\sqrt{3}$

Q: prove that if $(F, + , .)$ Is a filed and $a. b = 0$ $\forall a, b \in F$, then $a = 0$ *or* $b = 0$ Proof:

Let $a. b = 0$ $\forall a, b \in F$

Let $a \neq 0 \rightarrow \exists$ $a^{-1} \in F$ why??

∴ $a. a^{-1} = a^{-1}. a = 1$

$a^{-1} \dashv$ $a. b = 0$

$a^{-1}(a. b) = a^{-1}. 0$

$(a^{-1}. a). b = 0$

$e. b = 0$

$b = 0$

Theorem: any finite integral domain $(R , + , .)$ Is a field.

Proof:

Suppose that $R = \{a_1, a_2, \dots, a_n\}$ $\forall a \in R \ni a \neq 0 \to a.a_1, a.a_2, \dots, a.a_n$

$\exists a_i, a_j \in R \ni a.a_i = a.a_j$

$\Rightarrow a_i = a_j$

$\because 1 \in R \to a.a_i = 1 \quad \to a^{-1} =$
a_i why?

$\therefore R$ field.

LECTURE 9

Theorem: Let R be a commutative ring with 1. Then R is field ⇔ R has no non trivial ideal.

Proof:

$\Longrightarrow$ Let R be a field and I ideal of $R \ni I \neq 0$ and $I \neq R$

$\therefore 0 \subset I \subset R$

$\exists x \neq 0 \ni x \in I \subset R$

$\therefore \in x\ R$. But R field $\Rightarrow x_{-1}$ exists

$\therefore 1 = x^{-1}.\ x \in I \Rightarrow I = R \to$ C!

$\therefore I = 0$ and $I = R$.

$\Longleftarrow$ Let R has no non trivial ideals

Let $x \in R - \{0\} \Rightarrow x \in R^{-1}$

Consider the ideal (x)

$(x) \neq 0 \Rightarrow (x) = R$

$1 \in (x) = \{rx : r \in R\}$

$1 = r'x \Rightarrow r' = x^{-1} \ni r' \in R$

∴ R field

Theorem: Let $f: F_1 \to F_2$ be a field home. (onto). Then either $f = 0$ or $F_1 \cong F_2$

Proof:

Consider $Ker(f) \subseteq F_1$ ideal

$\Longrightarrow Ker(f) = 0$ or $Ker(f) = F_1$

$\therefore f$ one – one

$\therefore f$ isomorphism (why?)

$\therefore F_1 \cong F_2$

Def: Let F be a field and $\emptyset \neq K \subseteq F$ and $(K, +, \ .)$ is also field. We say K is subfield of F Or: F is an extension field of K

Ex: Q is subfield of R

Ex: C is an extension field of both R and Q

Remark: Let $(K\ , +\ \ , .)$ be a subfield of $(F, +, .) \Leftrightarrow$

1. $(K, +)$ subgroup of $(F, +)$
   $\forall \quad \in a, bK \to a - b \in K.$
2. $(K - \{0\}, .)$ Subgroup of $(F - \{0\}, .)$
   $\equiv \forall \quad \in \quad a, b \quad K\ ; b$

$\neq 0 \to a. b^{-1} \in K$

Theorem: Let R be an integral domain and it is a subring of the field F. Then $F' = \{a. b^{-1}: a, b \ \in R\}$ is a subfield of F and F' is the smallest one containing R $(R \subset F')$

Proof:

1. $\forall x, y \in F' \to x - y \in F'$
   Let $x \in F' \to x = a_1 . b_1^{-1}$ and $y \in F' \to y = a_2 . b_2^{-1}$
   Now: $x - y = a_1 . b_1^{-1} - a_2 . b_2^{-1} = (a_1 b_2 - a_2 b_1) . (b_1 b_2)^{-1} \in F'$
2. $\forall x, y \in F' \to x. y^{-1} \in F'$
   Now: $x . y^{-1} = (a_1\ b_1^{-1}) .\ (a_2 b_2^{-1})^{-1} = (a_1 . b_1^{-1})\ . (b_2 a_2^{-1})$

$= (a_1 . b_2) . (b_1 . a_2)^{-1} \in F'$

Let F'' subfield of F'

$\therefore a . b^{-1} , \in F''$

$\therefore F' \subseteq F''$

We have three types of ideals:

LECTURE 10

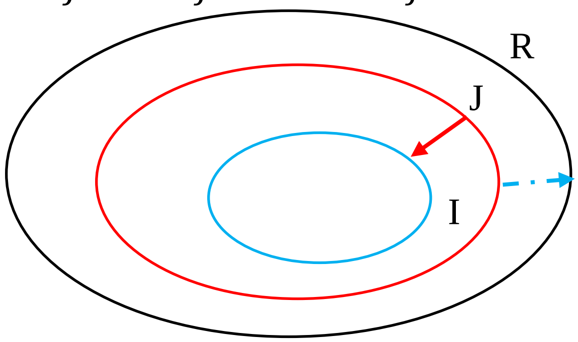
Minimum ideal

Def: Let R be a ring and I an ideal of R then I is minimum ideal if

1. $1 - I \neq 0$
2. $\exists J$ ideal of R $\ni 0 \subseteq J \subseteq I \Longrightarrow 0 = J \ or\ I = J$

Maximal ideal

Def: Let R be a ring and I be an ideal of R we say I is maximal ideal of R if there exists J is a proper ideal of R such that $I \subset J \subseteq R \Rightarrow J = R \;\; or \;\; I = J$



Remark: The ring may contain more than one Maximal ideal.

(i.e.) is Maximal of R if $I \neq R$ and if $\exists$ an ideal

$(M, +, .)$ in a ring R, s.t $J \subset M \subseteq R$ then $M = R$ **Example**: Determine

the Maximal ideals in the ring $(Z_{12}, +_{12}, ._{12})$

Solution:

$$12 = 2(6) = 4(3)$$

1. $I_1 = (\bar{2}) = (\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}, +_{12}, ._{12})$
2. $I_2 = (3) = (\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}, +_{12}, ._{12})$
3. $I_3 = (\bar{4}) = (\{\bar{0}, \bar{4}, \bar{8}\}, +_{12}, ._{12})$
4. $I_4 = (\underline{6}) = (\{\underline{0}, \underline{6}\}, +_{12}, ._{12})$

$\Longrightarrow I_1 = (2)$ *and* $I_2 = (\bar{3})$ are Maximal ideal in ring Z_{12} , Since $\nexists$ proper ideal of

ring Z_{12} containing $I_1 = (2)$ *and* $I_2 = (\bar{3})$. But $I_3 = (4)$ and $I_4 = (6)$ is not maximal ideal in ring Z_{12}. Since $(\bar{4}) \subset (\bar{2})$ and $(\bar{6}) \subset (\bar{3})$

H.W: Determine the Maximal ideals in the ring $(Z_{20}, +_{20}, ._{20})$ Solution: