The Ring

Definition 1: Let R be a non empty set, let $*,\circ$ be tow binary operation on R, then $(R,*,\circ)$ is called a ring iff :-

1- $(R,*)$ is comm. group.

2- $(R,\circ)$ is semi- group.

3- $\circ$ $is\ distribution\ over\ *$

$i.e$ $$(x*y)\circ z=(x\circ z)*(y\circ z)$$

$$z\circ(x*y)=(z\circ x)*(z\circ y) \quad \forall x,y\in R$$

Ex 1: $(R,+,\cdot)$, $(Z,+,\cdot)$, $(Q,+,\cdot)$, $(Z_n,+_n,\cdot_n)$ are Rings.

Ex 2: Is $(Z,*,\circ)$ a ring such that

$$a*b=a+b-1$$

$$a\circ b=a+b-2 \qquad \forall\ a,b\in Z$$

Ex 3: $R=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix},a,b,c,d\ \in R\right\}$ $then$ $(R,+,\cdot)$ is a ring.

Ex 4: Let $R=\{\ a+b\sqrt{3}\ |\ a,b\ \in Z\}$ $then$ $(R,+,\cdot\ )$ is a ring.

Remark: let $(R,+,\cdot)$ is a ring where

$+$ is called addition

$\cdot$ is called multiplication

Definition 2: A ring R is called commutative ring (com. ring) only if

$$a\cdot b=b\cdot a \qquad \forall\ a,b\in R$$

Ex 1: $(R,+,\cdot)$ is com. ring where R is real number.

<u>Definition 3:</u> A ring R with multiplication identity 1 such that $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$ then R is called **a ring <u>with unity</u>.**

<u>Ex 1:</u> $(R, +, \cdot)$, $(Z, +, \cdot)$ is a ring with unity =1.

<u>Ex 2:</u> $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, +, \cdot \right\}$ is a ring with unity = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

<u>Ex 3:</u> $(Z_e, +, \cdot)$ is a ring with out unity

Because $1 \notin Z$

<u>Definition 4:</u> An element (a) in a ring R is called unit if

$$\exists\, a^{-1} \in R \;\; s.t \;\; a \cdot a^{-1} = a^{-1} \cdot a = 1$$

<u>Ex 1:</u> $(R, +, \cdot)$ Every non zero element in R is unit.

<u>Ex 2:</u> The unit elements in $(Z, +, \cdot)$ are only (1) and (-1)

$$1 \cdot 1 = 1 \quad and \quad (-1) \cdot (-1) = 1$$

بعد خواص الحلقات Some properties of ring

Theorem 1: Let $(R, +, \cdot)$ is a ring with additive identity=0 then:

1- $\boldsymbol{a \cdot 0 = 0 \cdot a = 0}$.

Proof:

$a \cdot 0 = a \cdot (0 + 0)$

$\Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0$

$[a \cdot 0 + (-a \cdot 0)] = a \cdot 0 + [a \cdot 0 + (-a \cdot 0)]$ $\{R\ is\ a\ ring$
$\forall a \in R \exists -a \in R\}$

$0 = a \cdot 0 + 0$ $\{a + (-a) = I.e$

$0 = a \cdot 0$ $a + (-a) = 0$

2- $\boldsymbol{a(b) = -(ab) = (-a)b}$

Pf:

$a(-b) + (ab)$ $R\ is\ a\ ring\ have\ N.e$ $\{(ab)$ بأضافة$\}$

$= a(-b + b)$ $\{-b$ بأضافة$\}$

$= a \cdot 0$ $\{R\ is\ a\ ring\ have\ I.e\}$

$= 0$ $\{by\ (1)\ a \cdot 0 = 0 \cdot a = 0$

$-(ab) + (ab) = 0$ $\{R\ is\ a\ ring - a + a = 0\}$

$(-a)b + (ab)$

$= (-a + a)b$ $\{R\ is\ a\ ring\ have\ N.e\}$

$= 0 \cdot b$ $\{R\ is\ a\ ring\ have\ I.e\ (a + \ -a = 0)$

$= 0$ $\{by\ (1)\ \ a \cdot 0 = 0 \cdot a = 0\}$

$\therefore a(-b) = -(ab) = (-a)b$

3- $a + b = a + c \ \rightarrow b = c$

Pf:

$-a+(a+b)=-a+(a+c) \quad \{R \text{ is a ring have } N.e\}$

$\Rightarrow (-a+a)+b=(-a+a)+c \quad \{is\ ass\}$

$\Rightarrow 0+b=0+c \quad \{R \text{ is a ring have } I.e\ (a \pm a=0)$

$\Rightarrow b=c$

4- $-(-a)=a$

Pf:

$-a \text{ is inverse } (a) \quad \leftrightarrow \quad -a+a=0$

$-(-a) \text{is inverse } (-a) \ \leftrightarrow \ -(-a)+\ -a=0$

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

$\Rightarrow -(-a)+\ -a+a=0+a$

$\Rightarrow -(-a)+0=a$

$\Rightarrow -(-a)=a$

5- $(-a)\cdot(-b)=ab$

$=-(a\cdot(-b)$

$=-\big(-(ab)\big) \quad \{R \text{ is a ring } -(-a)=a\}$

$=ab$

6- $-(a+b) = (-a) + (-b)$

$-(a+b) + (a+b) = (-a) + (-b) + (a+b)$ $\{(a+b)$بأضافة

$0 = -a + (-b + a) + b$ $\{R\ is\ a\ ring\ is\ ass\ \&a \in R\ \exists - a \in R\}$

$= -a + (a + -b) + b$ $\{+\ is\ com\}$

$= (-a + a) + (-b + b)$ $\{\ is\ ass\}$

$= 0 + 0$ $\{0\ is\ I.e\ \ (a + -a = 0)$

$= 0$

$\therefore -(a+b) = (-a) + (-b)$

Example1: let $R = \{(a,b): a, b \in R\}$ we defined "+" , "·"

$$(a,b) + (c,d) = (a+c, b+d)$$

$$(a,b) \cdot (c,d) = (ac, bd)$$

$(R, +)$ is com group prove that $(R, +, \cdot)$ is com ring?

Sol:

1- $(a,b) \cdot (c,d) \in R$ $\quad is\ clouser$

2- Ass.

$[\,(a,b) \cdot (c,d)] \cdot (e,f) = (a,b) \cdot [(c,d) \cdot (e,f)]$

$(ac, bd) \cdot (e,f) = (a,b) \cdot (ce, df)$

$(ace, bdf) = (ace, bdf)$

$\therefore (R, \cdot) is\ semi - group$

3- $(a,b)\cdot[(c,d)+(e,f)] = (a,b)\cdot(c,d)+(a,b)\cdot(e,f)$

$$(a,b)\cdot(c+e,d+f) = (ac,bd)+(ae,bf)$$

$$(ac+ae,bd,bf) = (ac+ae,bd+bf)$$

4- $[(c,d)+(e,f)]\cdot(a,b) = (c,d)\cdot(a,b)+(e,f)\cdot(a,b)$

$\therefore$ $(R,+,\cdot)$ is a ring

5- $(a,b)\cdot(c,d) = (c,d)\cdot(a,b)$

$$(ac,bd) = (ca,db)$$

$$(ac,bd) = (ac,bd) \qquad \{\cdot \ \ is\ com\}$$

$\therefore$ $(R,+,\cdot)$ is com ring

If we want ring with unity

$$(a,b)\cdot(c,d) = (a,b)$$

$$(ac,bd) = (a,b)$$

$$ac = a \ \ldots\ldots(1)$$

$$bd = b\ \ldots\ldots(2)$$

From (1) $\frac{1}{a}\cdot ac = \frac{1}{a}\cdot a$ $\quad$ ($\frac{1}{a}$ بالضرب

$$c = 1$$

From (2) $\frac{1}{b}\cdot bd = \frac{1}{b}\cdot b$

$$d = 1$$

$\therefore$ $I.e = (1,1)$

If we want ring with unit

$(a,b)\cdot(a^{-1},b^{-1})=(1,1)$

$(aa^{-1},bb^{-1})=(1,1)$

$aa^{-1}=1 \ldots\ldots\ldots (1)$

$bb^{-1}=1 \ldots\ldots\ldots (2)$

From (1) $\frac{1}{a}\cdot aa^{-1}=\frac{1}{a}\cdot 1$ {a هو النظير الضربي لـ $\frac{1}{a}$

$$a^{-1}=\frac{1}{a}$$

From (2) $\frac{1}{b}\cdot bb^{-1}=\frac{1}{b}\cdot 1$

$b^{-1}=\frac{1}{b}$

$\therefore\ unit=\left(\frac{1}{a},\frac{1}{b}\right)$

$\therefore (R,+,\cdot)$ is com ring with unit

Ex: Let $(Z,+,\cdot)$ is comring with unity is$(2Z,+,\cdot)$ ring with unity and $(2Z,+)$ is com. group?

1-clouser

$2a\cdot 2b=4(ab)=2(2ab)\in 2Z$

2- Ass.

$(2a\cdot 2b)\cdot 2c=2a\cdot(2b\cdot 2c)$

3- $2a\cdot(2b+2c)=(2a\cdot 2b)+(2a\cdot 2c)$

$\therefore\ (2Z,+,\cdot)$ is a ring

But $(2Z,+,\cdot)$ is a ring with out unity — ليست حلقة مع العنصر المحايد

Since $1\notin 2Z$ — $2Z$ غير موجود في 1لان المحايد

Ex: Is $R = \{(R \times 0, +, \cdot)\}$ have unity ?

We know that

$R \times R = (a, b)$

$R \times 0 = (a, 0)$

$R = \{ (a, 0), a \in R\}$

$a \cdot 1 = a \quad let \quad I = (b, 0)$

$(a, O) \cdot (b, 0) = (a, o)$

$(ab, 0 \cdot 0) = (a, 0)$

$(ab, 0) = (a, 0)$

$ab = a \Rightarrow \frac{1}{a} \cdot ab = \frac{1}{a} \cdot a \Rightarrow b = 1$

$\therefore$ I.e $= (1, 0)$ $\quad [1 \in R]$

$\therefore$ $(R \times 0, +, \cdot)$ have unity

Ex: Let $R = R \times R = \{ (x, y): x, y \in R\}$ we definitiond "+" , " $\cdot$"

As following $(a, b) + (c, d) = (a + c, b + d)$

$(a, b) \cdot (c, d) = (ac, bc + d)$

Is R com.ring with unity

Sol:

$$(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$$

$$(ac, bc + d) \neq (ca, da + b)$$

$\therefore R$ is not com. ring

$$(a, b) \cdot (c, d) = (a, b)$$

$$(ac, bc + d) = (a, b)$$

$ac = a \Rightarrow \frac{1}{a} \cdot ac = \frac{1}{a} \cdot a \Rightarrow c = 1$

$bc + d = b \Rightarrow d = b - bc$

$\Rightarrow when\ c = 1 \Rightarrow d = b - b(1) \Rightarrow d = 0$

$\therefore\ I.e = (1, 0)$

$\therefore$ R is a ring with unity

Ex: Let $(A_{2\times 2}, +, \cdot)$ is a ring is are com. ring with untiy

We know that $(A_{2\times 2}, +, \cdot)$ have unity $= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

But is are not com.ring since

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} \neq \begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

سوف نترك للطالب اثبات ذلك (*H.w*)

Ex: Is $(Z, +, \cdot)$ has unit ?

Sol:

$1, -1$ $has\ unit\ only$ فقط الواحد والسالب واحد يمتلك نظير

$$1^{-1} = \frac{1}{1} = 1$$

$$-1^{-1} = -1$$

Th: Let R be a ring with unity, then can not divided by zero.

Pf:

We get $x \in R$ (نأخذ عنصر في R وليكن x)

Suppose ; $\frac{x}{0} \in R$, so we can take $x = 1$

(يمكن ان نأخذ $x = 1$ لان 1 احد عناصر R)

There for $\frac{1}{0}$ is inverse element of 0

(نظير الضربي لأي عدد هو مقلوب العدد نظير العدد 9 هو $\frac{1}{9}$ نظير العدد 0 هو $\frac{1}{0}$)

$\Rightarrow \left(\frac{1}{0}\right) \cdot (0) = 1$

ان اي عنصر في نظيره يساوي العنصر المحايد = *1*

But $(a \cdot 0 = 0)$

$\therefore \left(\frac{1}{0}\right) \cdot (0) = 0$

$\Rightarrow 1 = 0$ CL

$\therefore$ We can not divided by zero.

Subring

Definition: Let $(Z, +,\cdot)$ be a ring and let $\emptyset \neq S \subseteq R$ then S is subring of R $\leftrightarrow$ $(S, +,\cdot)$ is a ring itself.

Ex: $(R, +,\cdot)$ is a ring $\emptyset \neq Z \subseteq R$ then

$(Z, +,\cdot)$ is subring of R.

Ex: Let $(Z_6, +_6, \cdot_6)$ is a ring and let $H = \{\bar{0}, \bar{2}, \bar{4}\}$

. Is $(H, +_6, \cdot_6)$ subring of Z_6

$+_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

$\cdot_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

1- is closure

$\bar{a} +_6 \bar{b} \in H$

2- is ass

$(\bar{a} +_6 \bar{b}) +_6 \bar{c} = \bar{a} +_6 (\bar{b} +_6 \bar{c})$

3- $I.e = 0$

4- $N.e$ $\bar{0} = \bar{0}$

$\bar{2} = \bar{4}$

$\bar{4} = \bar{2}$

5- is com $\bar{a} +_6 \bar{b} = \bar{b} +_6 \bar{a}$

6- is closure

$\bar{a} \cdot_6 \bar{b} \in H$

7- is ass

$(\bar{a} \cdot_6 \bar{b}) \cdot_6 \bar{c} = \bar{a} \cdot_6 (\bar{b} \cdot_6 \bar{c})$

8- $\bar{a} \cdot_6 (\bar{b} +_6 \bar{c}) = (\bar{a} \cdot_6 \bar{b}) +_6 (\bar{a} \cdot_6 \bar{c})$

$\therefore (H, +_6, \cdot_6)$ is subring of Z_6

Th: Let $(R, +, \cdot)$ is a ring $\emptyset \neq S \subseteq R$ then S is subring $\Leftrightarrow$ iff

1. $a - b \in S$
2. $a \cdot b \in S$

Pf: $\Rightarrow (S, +, \cdot)$ subring

1- subring $\Rightarrow \forall\, b \in S\ \exists -b \in S,\ a \in S$

$a + (-b) \in S$ $\quad (+\ is\ clousre)$

$a-b \in S$

2- $a \cdot b \ \in S$ [Is subring $\rightarrow \cdot$ is closure]

$\Leftarrow$ 1- $a, b \ \in S \ \ \ni a, -a \ \in S$

$a-a \ \in S$

$0 \ \in S$ $(I.e \ \ +)$

2- $a-b \in S \ \Rightarrow 0-b \in S \ \Rightarrow -b \in S \quad [\,N.e \ +\,]$

3- $a-(-b) \in S \ \Rightarrow a+b \in S \quad [\,is\ closure\,]$

4- S is ass $[\,S \subseteq R, R\ is\ a\ ring \quad \therefore R\ is\ ass \ \Rightarrow S\ is\ ass]$

R تجميعية و S جزئية من R أذن S *تحمل الصفة التجميعية*

5- S is com $[a, b \in R\ , R\ is\ a\ ring \ \Rightarrow R\ is\ com \ \Rightarrow S\ is\ com]$

$\therefore$ $(S, +, \cdot)$ is com group

6- $a \cdot b \in S$, $is\ closure$

7- $\cdot$ is ass $[\,S \subseteq R, R\ is\ a\ ring \quad \therefore R\ is\ ass \ \Rightarrow S\ is\ ass]$

8-

$\therefore$ $(S, +, \cdot)$ is a subring of R

Ex: Let $(Z_6, +_6, \cdot_6)$ is a ring and let $H = \{\bar{0}, \bar{2}, \bar{4}\}$

. Is $(H, +_6, \cdot_6)$ subring of Z_6

نفس المثال السابق سوف نطبق عليه المبرهنة اعلاه

Sol:

1- $a-b = a+(-b) \in H$

$+_6$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$

$\cdot_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

$\bar{0}^{-1} = \bar{0}$

$\bar{2}^{-1} = \bar{4}$

$\bar{4}^{-1} = \bar{2}$

2- $a \cdot b \in H$

$\therefore$ $(H, +_6, \cdot_6)$ is a subring of Z_6

Th: If R is a ring with unity, then this unity 1 is the only multiplication identity.

كل حلقة يكون العنصر المحايد الضربي وحيد

Pf: let 1, 1′ are tow multiplication identities

$1' \cdot 1 = 1 \cdot 1' = 1'$ [1 هو عنصر محايد, 1′ هو عنصر عادي]

$1 \cdot 1' = 1' \cdot 1 = 1$ [1′ هو عنصر محايد, 1 هو عنصر عادي]

$1' = 1$ CL

$\therefore$ Ring you have only multiplication identity.

Th: If $(R, +, \cdot)$ be a ring with unity then $1 \neq 0$

(identity of addition ≠ identity of multiplication)

Pf:

Suppose $1 = 0$

العنصر المحايد الجمعي = العنصر المحايد الضربي

$$x \in R \quad , \quad x \neq 0$$

$$x \cdot 1 = x \cdot 0 \qquad (1 = 0)$$

$$x = 0 \qquad CL$$

$$1 \neq 0$$

العنصر المحايد الجمعي $\neq$ العنصر المحايد الضربي

In general $1 \neq 0$

الا في حالة كان $R = \{0\}$

فان $0 \cdot 0 = 0 \cdot 1$

$$0 = 0$$

$$1 = 0$$

Remark: Let $(R, +, \cdot)$ be a ring, $(S, +, \cdot)$ be a subring then:

1-If R has unity, and then it's not necessary that S has unity.

Sol: ex: $(Z, +, \cdot)$ $ring\ with\ unity = 1$

$2Z = \{0, \mp 2, \mp 4, \mp 6, \ldots.\}$

$(2Z, +, \cdot)$ $is\ a\ subring\ of\ Z$

But is a subring with out unity

2- If R, S have unity, then it is not necessary that

identity of R = identity of S

Ex: let $(Z, +, \cdot)$ ring with unity

Then $(Z + 1, +, \cdot)$ subring with out unity

Ex2: $(Z_6, +, \cdot)$ ring with unity=1

$$S = \{\bar{0}, \bar{2}, \bar{4}\}$$

$\cdot_6$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

S subring with unity =4

3- If ring without unity then subring with unity.

Ex: It may be that S has identity but R has no identity

Let $(Z \times 2Z, +, \cdot) = \{(a, 2a), +, \ \cdot\} \ s.t \ \ a \in Z \ \ ring \ \subseteq Z \times Z$

1-clouser $\quad (a, 2a) + (b, 2b) = \big(a + b, 2(a + b)\big) \in (Z \times 2Z)$

2- ass

3- com

4- $(a, 2a) + (0, 0) = (a, 2a)$

5- $(a, 2a) + (-a, -2b) = (0, 0)$

6- ass $[(a, 2a) \cdot (b, 2b)] \cdot (c, 2c) = (a, 2a) \cdot [(b, 2b) \cdot (c, 2c)$

7- closure $(a, 2a) \cdot (b, 2b) = \big(ab, 2(2ab)\big)$

8- لان الجزء ينطبق على الكل أذن شرط التوزيع متحقق

$\therefore \ (Z \times 2Z, +, \cdot)$ is ring with out unity

Let $\exists \ (c, d) \in Z \times 2Z \ \ s.t$

$(a, 2b) \ \cdot (c, d) = (a, 2b)$

$(ac, 2bd) = (a, 2b)$

$ac = a \ \Rightarrow c = 1 \in Z$

$2bd = 2b \ \Rightarrow d = 1 \notin 2Z$

$(1,1) \quad \notin Z \times 2Z$

$(Z \times \{0\}), +, \cdot)$ is subring with unity

$(a, 0) \ s.t \ a \in Z$

$(a, 0) \cdot (c, d) = (a, 0)$

$(ac, 0) = (a, 0)$

$ac = a \Rightarrow c = 1$

$I.e = (1,0) \in Z \times \{0\}$

4- If R is com. ring, then $(S, +, \cdot)$ is com. subring

Sol: let $a, b \in S \quad T.P \quad a \cdot b = b \cdot a$

$a \cdot b = b \cdot a \quad (a, b \in R , R \ is \ a \ ring)$

$\therefore \ S \ is \ com.ring$

5- If S is com. ring, then it is not necessary that R is com. ring?

Sol: **<u>Ex:</u>** Let $(A_{2\times2}, +, \cdot)$ ring but not com. ring

$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, +, \cdot \right\}$ is subring

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$$

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S$$

$\therefore \ (S, +, \cdot)$ is subring

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix}$$

Is com. ring

Th: Let $(R,+,\cdot)$ be any S,T tow subring of $(R,+,\cdot)$ then $S \cap T$ subring of R.

Pf: Let $a,b \in S \cap T$

$\rightarrow a,b \in S \quad \wedge \quad a,b \in S$

[since S,T subring] 1. $a-b \in S \quad \wedge \quad a-b \in T$

$\Rightarrow a-b \in S \cap T$

2- $a \cdot b \in S \quad \wedge \quad a \cdot b \in T$ [since S,T subring]

$\Rightarrow a \cdot b \in S \cap T$

$\therefore$ 1. $a-b \in S \cap T$

2. $a \cdot b \in S \cap T$

$\therefore$ $S \cap T$ is subring by R [by th:]

Remark: The union of tow subring is not necessary subring.

Ex: consider the ring $(Z,+,\cdot)$

$(2Z,+,\cdot)$ be subring of $(Z,+,\cdot)$

$(3Z,+,\cdot)$ be subring of $(Z,+,\cdot)$

$2Z = \{0, \mp 2, \mp 4, \ldots\}$

$3Z = \{0, \mp 3, \mp 6, \ldots\}$

But $(2Z \cup 3Z,+,\cdot)$ is not subring of $(Z,+,\cdot)$

$2Z \cup 3Z = \{0, \mp 2, \mp 3, \mp 4, \mp 6, \ldots\}$

$3,2 \in 2Z \cup 3Z$ but $3-2=1 \notin 2Z \cup 3Z$

$\therefore$ $2Z \cup 3Z$ is not subring

Ex: Let $(R,+,\cdot)$ is a ring

And let $(Q,+,\cdot)$ is a subring of R

& $(Z,+,\cdot)$ is a subring of R

$\therefore Q \cap Z = Z$ is subring

Th: Let S, T be tow subring of $(R,+,\cdot)$ then $(S \cup T)$ is subring iff $S \subseteq T$ or $T \subseteq S$.

Pf: H.W

Cancellation law

$4 \cdot x = 0 \Rightarrow x = 0$ why ?

$\frac{1}{4} \cdot 4x = \frac{1}{4} \cdot 0$ $[x \in R, R\ is\ a\ ring\ \frac{1}{4}\ is\ unit\ 0f\ 4]]$

$1 \cdot x = 0$ $[1\ is\ unity]$

$x = 0$ $[a \cdot 0 = 0]$

Ex: solve the equation:

$5x = 0 \rightarrow x = 0$; $x \in Z_6$

$5x = 0$ [we must find inverse of 5 in Z_6

يجب ايجاد النظير الضربي لمعامل x وهو 5 في Z_6

$5 \cdot 5x = 5 \cdot 0$ $[5\ inverse\ 5\ since\ 25 - 24 = 1\ in\ Z_6]$

$25x = 0$ $[25 - 24 = 1\ unity]$

$1 \cdot x = 0$ $[1\ is\ unity\ a \cdot 1 = a]$

$\therefore x = 0$

Ex3: solve the equation:

$$2x = 4 \quad ; \quad x \in Z_6$$

Cannot find inverse of 2 in Z_6 $[\ 2 \cdot m = 1]$

لا يوجد نظير ضربي لمعامل x وهو 2 في Z_6

$\therefore$ not find solution in equation in Z_6

لا يوجد حل للمعادلة في Z_6 (ربما يوجد حل للمعادلة في Z_n)

Ex: solve the equation:

$$2x = 4 \quad ; \quad x \in Z_7$$

$4 \cdot 2x = 4 \cdot 4$ $[4\ inverse\ 2\ in\ Z_7\ since\ 4 \cdot 2 = 8 - 7 = 1]$

$1 \cdot x = 2$ [1 is unity $a \cdot 1 = a$]

$x = 2$

Zero diviser

Defi: Let $(R, +, \cdot)$ be a ring, $a \neq 0$ and $b \neq 0$ are two elements of R such that $a \cdot b = 0$ then a and b is called $diviser\ of\ zero$.

Ex1: $(Z, +, \cdot)$, $(R, +, \cdot)$, $(Q, +, \cdot)$, $(C, +, \cdot)$ has no $zero\ diviser$.

Ex2: $(Z_{12}, +_{12}, \cdot_{12})$ is a ring

$\bar{2} \cdot \bar{6} = \bar{0}$ $(\bar{2} \neq \bar{0}, \bar{6} \neq \bar{0})$

$\bar{3} \cdot \bar{4} = \bar{0}$

$\bar{4} \cdot \bar{8} = \bar{0}$

Then $(\bar{2}, \bar{6}, \bar{3}, \bar{4}, \bar{8})$ are $Zero\ diviser$ 0f Z_{12}.

Th1 : The cancellation law hold in a ring R iff R has no $Zero\ diviser$.

Th2: $(Z_n, +_n, \cdot_n)$ has no $Zero\ diviser$ iff n is prime number.

Ex: $(Z_5, +_5, \cdot_5)$ has no $Zero\ diviser$.

Remark:- If a is $Zero\ diviser$ of Z_n

$\rightarrow g.c.d\ (a, n) \neq 1$

If a is not $Zero\ diviser$ of Z_n

$\rightarrow g.c.d\ (a, n) = 1$

Ex: $(Z_4, +_4, \cdot_4)$ is a ring

$2\ is\ Zero\ diviser\ \ since\ \ 2 \cdot 2 = 0$

$g.c.d(2, 4) \neq 1$

$3\ is\ not\ Zero\ diviser\ \ since\ 3 \cdot a \neq 0, a \neq 0$

$g.c.d\ (3, 4) = 1$

Q1/ Find the $diviser\ 0f\ Zero$ in

1- Z_{12} 2- Z_{11}

Sol:

1- $Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}, \overline{11}\}$

Since 12 is not prime then Z_{12} has $divisers\ of\ Zero$, which is the element are not relatively prime to 12.

لان 12 عدد غير اولي فأن Z_{12} يملك قواسم للصفر وان قواسم الصفر في Z_{12} هي العناصر التي لها عامل مشترك مع العدد 12 .

$\bar{2} \cdot_{12} \bar{6} = \bar{0} \Rightarrow \bar{2}, \bar{6}\ are\ diviser\ of\ Zero.$

$\bar{3} \cdot_{12} \bar{4} = 0 \Rightarrow \bar{3}, \bar{4}\ are\ diviser\ of\ Zero.$

$\bar{3} \cdot_{12} \ \bar{8} = 0 \Rightarrow \ \bar{3}, \bar{8}$ $are\ diviser\ of\ Zero.$

$\bar{4} \cdot_{12} \ \bar{6} = 0 \ \Rightarrow \ \bar{4}, \bar{6}$ $are\ diviser\ of\ Zero.$

$\bar{4} \cdot_{12} \ \bar{9} = 0 \ \Rightarrow \ \bar{4}, \bar{9}$ $are\ diviser\ of\ Zero.$

$\bar{6} \cdot_{12} \ \bar{8} = 0 \ \Rightarrow \ \bar{6}, \bar{8}$ $are\ diviser\ of\ Zero.$

$\bar{6} \cdot_{12} \ \overline{10} = 0 \ \Rightarrow \ \bar{6}, \overline{10}$ $are\ diviser\ of\ Zero.$

$\bar{8} \cdot_{12} \ \bar{9} = 0 \ \Rightarrow \ \bar{8}, \bar{9}$ $are\ diviser\ of\ Zero.$

$\therefore The\ diviser\ of\ Zero\ in\ Z_{12}\ are\ \{\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \overline{10}\}$

2- $Z_{11} = \{ \bar{0}, \bar{1}, \ \bar{2}, \ \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \overline{10}\}$

Since 11 is prime, then Z_{11} has no $diviser\ of\ Zero$

لان (11) عدد غير أولي فأن Z_{11} لا يملك قواسم للصفر.

Integral domain الحلقة التامة

Def.: Let $(R,+,\cdot)$ be a com.ring with unity then $(R,+,\cdot)$ is called an integral domain iff $\underline{R\ has\ no\ Zero\ diviser}$.

i.e: $(R,+,\cdot)$ is integral domain if

1- Is com.

2- With unity

3- Has no $Zero\ diviser$

Ex: $(\mathcal{R},+,\cdot)$ is an integral domain

Because $\mathcal{R}$ is com.ring with unity and has no $Zero\ diviser$

Ex: $(A_{n\times n},+,\cdot)$ is not an integral domain because $(A_{n\times n},+,\cdot)$ is not com.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \neq \begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Note: $(Z_n,+_n,\cdot_n)$

If n is prime number → Z_n is an integral domain

If n is not prime number → Z_n is not an integral domain, since Z_n has $Zero\ diviser$

H.w: Is $A_{2\times 2},+,\cdot$) have $Zero\ diviser$

Th: Let $(R,+,\cdot\ )$ be a ring with unity then R is an integral domain $a\cdot b = ac\ ,\ a \neq 0\ \ then\ \ b = c$.

Sol:

$$\Rightarrow R\ is\ I.D\ (\text{حلقة تامة})$$

- com
- $unity$
- $No\ Zero\ diviser$

$a \cdot b = ac\ \ ,a \neq 0$

$ab + (-ac) = ac + (-ac) \qquad [R\ is\ a\ ring]$

$ab + (-ac) = 0 \qquad [R\ is\ a\ ring\ a + (-a) = 0\ (I.e)]$

$a\big(b + (-c)\big) = 0$

$\therefore (no\ Zero\ diviser),\ \ a \neq 0$

أذن يجب ان يكون احد العددين يساوي صفر

$b + (-c) = 0$

$b + (-c) + c = 0 + c$ [نظائر جمعية لانها حلقة]

$b + 0 = c$

$\therefore b = c$

$\Leftarrow \quad a \neq 0$

$com + unity +$

$a \cdot b = 0 \quad ,\ \ b \in R$

$a \neq 0 \Rightarrow b = 0$

$\because R\ has\ no\ Zero\ diviser \quad \therefore (R, +, \cdot)\ is\ I.D$

Ex: prove or dis prove :

*Every subring of a ring with unity has unity?

Sol: ex: $(Z, +, \cdot)\ have\ unity = 1$

$(2Z, +, \cdot)\ with\ out\ unity$

Ideal (المثالي)

Defi: Let $(R, +, \cdot)$ be a ring , $\emptyset \neq I \subseteq R$ then I is an ideal iff

1- I is subring → $a - b \in I$ $\quad [\forall\, a, b \in R]$
↘ $a \cdot b \in I$

2- $a \cdot r \in I$, $r \cdot a \in I$ $\forall a \in I, r \in R$

Ex:- Let $(Z_{12}, +_{12}, \cdot_{12})$ be a ring and let $I = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

Is I is an ideal.

Sol:1- $a - b \in I$, $\forall a, b \in I$

$a + (-b)$

$+_{12}$	$\bar{0}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{9}$	$\bar{6}$
$\bar{6}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{9}$
$\bar{9}$	$\bar{9}$	$\bar{6}$	$\bar{3}$	$\bar{0}$

$\cdot_{12}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{0}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{0}$	$\bar{6}$
$\bar{9}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$

2- $a \cdot b \in I$

$\therefore I$ is a subring

3- $a \cdot r \in I$, $r \cdot a \in I$ $\quad \forall a \in I, r \in R$

$\cdot_{12}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{0}$	$\bar{3}$										
$\bar{6}$	$\bar{0}$	$\bar{6}$										
$\bar{9}$	$\bar{0}$	$\bar{9}$										

وهكذا نلاحظ ان جميع العناصر الموجودة في

$\therefore I \text{ is an ideal}$

Ex: Let $R = \{(a, b), +, \cdot : a, b \in Z\}$

$$I = \{(a, 0), +, \cdot : a \in Z\}$$

Is I an ideal

1- $(a, 0) - (b, 0) = (a - b, 0 - 0) = (a - b, 0) \in I$

$(a, 0) \cdot (b, 0) = (ab, o) \in I$

2- $a \cdot r \in I , a \in I \quad r \in R$

$(a, 0) \cdot (x, y) = (ax, 0 \cdot y) = (ax, 0) \in I$

$\therefore I \; is \; an \; ideal$

Ex: Let $(R, +, \cdot)$ is a ring and let $(Z, +, \cdot)$ is a subring

Is Z an ideal of R? Why?

Sol:

$(Z, +, \cdot)$ is not ideal since $a \cdot r \in Z$

$$\frac{1}{2} \in R \quad , 1 \in Z$$

$$\frac{1}{2} \cdot 1 = \frac{1}{2} \notin Z$$

Remark:

1- I is called left ideal if $r \cdot a \in I \quad \forall\, a \in I, r \in R$

2- I is called right ideal if $a \cdot r \in I \quad \forall\, a \in I, r \in R$

Simple Ring (حلقة بسيطة)

Defi: Let R and $\{0\}$ are only ideals in a ring , then R is called Simple Ring.

Ex: Is $(R, +, \cdot)$ of real number Simple Ring?

Sol: yes, since he have only ideals itself and $\{0\}$

Ex: Is $(Z_p, +_p, \cdot_p)$ $if \; p \; is \; prime \; number$ Simple Ring ?

Sol: yes, p *is prime number*

By th: $(Z_p, +_p, \cdot_p)$ has no subring only $(Z_p, +_p, \cdot_p)$& $(\{0\}, +, \cdot)$

Theorem: Let $(R, +, \cdot)$ be a ring with unity =1, let I be an ideal of R, if $a^{-1} \in I$ $s.t$ a^{-1} is inverse element (unit) ,then $I = R$.

Proof: $I = R$ → $I \subseteq R$

→ $R \subseteq I$

1- $I \subseteq R$ always
2- Let $r \in R$
$r \cdot 1 \in R$ $[R \text{ is } \in \text{ring with unity}]$
$r \cdot (a \cdot a^{-1}) \in R$
$(r \cdot a) \cdot a^{-1} \in$ R [R is a ring]
$\in R$ $\in I$
$\therefore R \subseteq I$
$\therefore$ *from* 1 &2 $R = I$

Remark: Let I be an ideal is a ring R if $1 \in I$ *then* $I = R$

اذا كان المحايد الضربي موجود في المثالي = حلقة الرتبة

Th: if I and J are tow ideals ⇒ $I \cap J$ is ideal.

Proof:

1- $I \cap J$ is subring [by th: I, J subring → $I \cap J$ is subring]
2- $r, a \in I \cap J$ $s.t$ $r \in R; a \in I \cap J$
$r, a \in I \wedge r, a \in J$
$r \cdot a \in I \wedge r \cdot a \in J$
$\therefore r \cdot a \in I \cap J$
$\therefore I \cap J$ is ideal

Ex: Is $I \cup J$ is ideal?

Sol: No, since

$(3Z, +, \cdot)$ is ideal

$(2Z, +, \cdot)$ is ideal

But $2Z \cup 3Z$ is not ideal. Why?

Definition: Let $(R, +, \cdot)$ be a ring with unity=1 let $a \in R$,

let $Ra = \{r \cdot a : r \in R\}$, then Ra is an ideal.

Ex: let $(R, +, \cdot)$ com. Ring with unity and let

$Ra = R2 = \{r \cdot 2 : r \in R\}$ is ideal?

1- $a - b \in R2$

$$r_1 \cdot 2 - r_2 \cdot 2 = (r_1 - r_2) \cdot 2 \in R2 \quad , \quad \forall r_1, r_2 \in R$$

2- $a \cdot b \in R2$

$$(r_1 \cdot 2)(r_1 \cdot 2) = ((r_1 \cdot r_2) \cdot 2) \cdot 2 \in R2 \quad \forall r_1, r_2 \in R$$

3- Let $r \in R, \ a \in R2$

$$r \cdot a = r \cdot (r_1 \cdot 2) = (r \cdot r_1) \cdot 2 \in R2$$

$\therefore R2$ is an ideal.

<u>Maximal ideal المثالى الاكبر</u>

Definition: Let $(R, +, \cdot)$ be a ring and I, J are two ideals then I is called maximal ideal if $I \subseteq J \subseteq R \Rightarrow I = R$

Or $I \subseteq J = R$

Ex: Let $(Z_8, +_8, \cdot_8)$ be a ring and let

$I = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

1- $a - b \in I \quad , \forall a, b \in I$

$+_8$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$
$\bar{6}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$

2- $a \cdot b \in I$,

$\cdot_8$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$

3- $r \cdot a = a \cdot r \in I \quad ; r \in R , a \in I$

$\therefore$ I is an ideal

Let $J = \{\bar{0}, \bar{4}\}$

1- $a - b \in J$

2- $a \cdot b \in J$

$\cdot_8$	$\bar{0}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{4}$	$\bar{0}$	$\bar{0}$

$+_8$	$\bar{0}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{4}$	$\bar{0}$

3- $r \cdot a = a \cdot r \in J$

$\therefore J$ is an ideal

We see that

$J \subseteq I \subseteq Z_8$

$\therefore I$ is maximal ideal

Ex: Let $(Z_6, +_6, \cdot_6)$ be a ring and let

$I = \{\bar{0}, \bar{2}, \bar{4}\}$ be an ideal

$J = \{\bar{0}, \bar{3}\}$ be an ideal

We see $I \nsubseteq J$ but $I \subseteq Z_6$, $J \subseteq Z_6$

So $I \quad is\ maximal\ ideal\ of\ Z_6$

$J \quad is\ maximal\ ideal\ of\ Z_6$

Ex: let $(Z, +, \cdot)$ be a com.ring with unity =1

And let $4Z = \{0, \mp 4, \mp 8, \dots\}$

$$a = r \cdot 4 \quad r \in Z$$

$$= (r \cdot 2) \cdot 2$$

1- $a - b \in 4Z$

$r_1 \cdot 4 - r_2 \cdot 4 = (r_1 - r_2) \cdot 4 \in 4Z$

2- $a \cdot b \in 4Z$

$(r_1 \cdot 4) \cdot (r_2 \cdot 4) = \big((r_1 \cdot r_2) \cdot 4\big) \cdot 4 \in 4Z$

$\therefore 4Z$ is an ideal 0f Z

$let\ 2Z = \{0, \mp 2, \mp 4, \dots.\} is\ an\ ideal\ of\ Z$

We see $4Z \subseteq 2Z \subseteq Z$

So $2Z\ is\ maximal\ ideal\ of\ Z$

Prime ideal المثالي الاولي

Definition: Let R be com. Ring with unity=1, I be a proper ideal at R, I is called ***prime ideal*** .

If $\quad a \cdot b \in I \rightarrow a \in I\ or\ b \in I\ , \quad \forall\, a, b \in R$

Ex: Let $(Z, +, \cdot)$ is com. Ring with unity = 1 and let

$I = (4) = 4Z = \{0, \mp 4, \mp 8, \mp 12, \dots\}$ is an ideal of Z

Is $I\ prime\ ideal\ of\ Z$

Sol: $4 \in 4Z$

$2 \cdot 2 \in 4Z$ but $2 \notin 4Z$

$\therefore\ I\ is\ not\ prime\ ideal$

حاصل ضرب اي عددين من الحلقة يجب ان ينتمي الى المثالي فيجب ان يكون احد العددين ينتميان الى المثالي

Ex: Let $(Z,+,\cdot)$ be a com. Ring with unity = 1

$(3) = 3Z = \{0, \mp 3, \mp 6, \mp 9, \dots\}$

Is $3Z$ $prime\ ideal$

Sol: $3 \cdot 1 \rightarrow 3 \in 3Z$, $1 \notin 3Z$

يجب احد العددين ينتمي الى المثالي وهو ٣

$3 \cdot 2 \in 3Z \rightarrow 3 \in 3Z$, $2 \notin 3Z$

$\therefore$ $3Z$ $is\ prime\ ideal$

Ex: Let $(Z,+,\cdot)$ be a com. Ring with unity=1

$I = 2Z = \{0, \mp 2, \mp 4, \mp 6, \dots\}$ Is I prime ideal.

Sol: H.w

Ex: prove or dis prove : (H.w)

1- $2Z$ is an ideal in Z.
2- Any subring is an ideal of a ring.
3- $3Z$ is a prime ideal in Z.

Th: let R be a com. Ring with unity, m be a proper ideal of R then m is maximal ideal of R $\Leftrightarrow$

$$R = m + \langle a \rangle \quad \forall a \in R \quad , \qquad a \notin m$$

Proof:

$\Rightarrow$ m $(maximal\ ideal)$ $T.P$ $R = m + \langle a \rangle$, $a \notin m$

$m \subseteq m + \langle a \rangle \subseteq R$

$m + \langle a \rangle = R$ $\quad [be\ define\ of\ m.I]$

$\Leftarrow$ $m + \langle a \rangle = R$ $T.P$ m is $m.I$

Suppose J is an ideal of R

And $m \subsetneq J$

Let $a \in I$ $\quad (a \notin m)$

$m \subseteq m + \langle a \rangle \subseteq J \subseteq R$

$\therefore \ m \ is \ maximal \ ideal$

Local ring حلقة محلية

Definition: Let R be a com. Ring with unity , R is called ***Local ring*** if R has exactly one maximal ideal.

Local →
- Com
- have unity
- Have exactly one $m.I$

Ex: Let $(Z_8, +_8, \cdot_8)$ be a com. Ring with unity

$I = <2>$, $J = <4>$

$<4> \subseteq <2> \subseteq Z_8$

$\therefore <2>$ is only maximal ideal

$\therefore \ Z_8 \ \ is \ maximal \ ideal$

Ex: $(Z, +, \cdot)$ be a com. Ring with unity

$2Z$ is an ideal [$is \ maximal \ ideal$]

$3Z$ is an ideal [$is \ maximal \ ideal$]

$\therefore \ (Z, +, \cdot)$ is not Local ring.

Ex: Let $R \times R = \{(a, b), +, \cdot \ : \ a, b \in R\}$ be a comring with unity

And Let $I = \{(a, 0), +, \cdot\}$ be an ideal in $R \times R$

$J = \{(0, b), +, \cdot\}$ be an ideal in $R \times R$

$\therefore R \times R$ is not Local ring

حلقة القسمة Quotient ring

Definition: Let $(R,+,\cdot)$ be a ring, $(I,+,\cdot)$ be an ideal of R, let

$$R/I = \{\, a+I:\ a\in R\}$$

Definition: $\oplus,\ \odot\ \ on\, R/I$

$$(a+I)\oplus(b+I) = (a+b)+I \qquad ,\ \forall\, a,b\in R$$

$$(a+I)\odot(b+I) = (ab)+I \qquad ,\ \forall\, a,b\in R$$

R/I is called Quotient ring

Th: prove $(R/I, \oplus, \odot)$ is a ring?

Proof:

1- $\oplus$ is closure

$$(a+I)\oplus(b+I) = (a+b)+I \ \in R/I$$

Is closure

2- $[(a+I)\oplus(b+I)]\oplus(c+I)$
$[(a+b)+I]\oplus(c+I) = (a+b+c)+I$
$= (a+I)\oplus[(b+c)+I] = (a+I)\oplus[(b+I)\oplus(c+I)]$
is ass.

3- $(a+I)\oplus(b+I) = (a+I)$
$(a+b)+I = (a+I)$
$a+b = a \Rightarrow b = 0$
$e = 0+I = I$

4- $(a+I)\oplus(b+I) = 0+I$
$(a+b) = 0 \ \Rightarrow a = -b$

5- $(a+I)\oplus(b+I)$
$(a+b)+I = (b+a)+I$
$= (b+I)\oplus(a+I)$

$(R/I, \oplus)$ is com. Ring

6- $(a+I)\odot(b+I) = (ab) + I \in R/I$

$\odot$ is closure

7- $[(a+I)\odot(b+I)]\odot(c+I) \quad H.W$

8- $(a+I)\odot[(b+I)\oplus(c+I)]$

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

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

$[(ab)+I]\oplus[(ac)+I] = (ab+ac)+I$

$\therefore R/I$ is a ring

Remark:

$a+I = b+I \leftrightarrow a-b \in I$

$a+I = I \leftrightarrow a \in I$

Ex: Let $(Z_6, +_6, \cdot_6)$ let $I = \{\bar{0}, \bar{3}\}$ is an ideal.

$Z_6/I = \{a+I, a \in R\}$

$\bar{3} + I = \bar{0} + I = I \rightarrow \bar{3} \in I$

$\bar{4} + I = (\bar{1} + \bar{3}) + I = \bar{1} + (\bar{3} + I) = \bar{1} + I$

$\bar{5} + I = (\bar{2} + \bar{3}) + I = \bar{2} + (\bar{3} + I) = \bar{2} + I$

$Z_6/I = \{I, \bar{1} + I, \bar{2} + I\}$

$+_6$	I	$\bar{1}+I$	$\bar{2}+I$
I	I	$\bar{1}+I$	$\bar{2}+I$
$\bar{1}+I$	$\bar{1}+I$	$\bar{2}+I$	I
$\bar{2}+I$	$\bar{2}+I$	I	$\bar{1}+I$

$I.e = I$

$\cdot_6$	I	$\bar{1}+I$	$\bar{2}+I$
I	I	I	I
$\bar{1}+I$	I	$\bar{1}+I$	$\bar{2}+I$
$\bar{2}+I$	I	$\bar{2}+I$	$\bar{1}+I$

$unity = \bar{1}+I$

${}^{R}/_{I}$ is com. Ring with unity

Th: Let I is prime ideal $\leftrightarrow$ ${}^{R}/_{I}$ is integral domain.

Proof: $\rightarrow$ I is prime ideal (T.P ${}^{R}/_{I}$ is integral domain)

$\therefore R$ is $c.r.w.1$ [com.ring with unity] $\Rightarrow$ ${}^{R}/_{I}$ $c.r.w.1$

Suppose ${}^{R}/_{I}$ have $Zero\ diviser$

$(a+I)\odot(b+I) = I$; $a+I \neq I,\quad b+I \neq I$

ملاحظة: حيث I يمثل 0 في ${}^{R}/_{I}$ حلقة القسمة

$(ab)+I = I \Rightarrow ab \in I$

$\therefore I\ is\ prime \Rightarrow a \in I\ or\ b \in I$

$a+I = I\quad or\quad b+I = I\quad C!$ تناقض

$\therefore {}^{R}/_{I}\ has\ no\ Zero\ diviser$

$\therefore {}^{R}/_{I}$ is integral domain

$\leftarrow\ let\ {}^{R}/_{I}\ is\ I.D \rightarrow T.P\quad I\ is\ prime\ ideal$

Suppose I is not prime ideal

$a\cdot b \in I \rightarrow a \notin I\quad or\quad b \notin I$

$ab+I = I\qquad a+I \neq I,\quad b+I \neq I$

$(a+I)\odot(b+I) = I$

$a + I = I \quad or \quad b + I = I \qquad C!$

$\therefore \quad I$ is prime ideal

م. ايمان فاضل

م.م. سيف زهير