نظرية الحلقات

المحاضرة الأولى

العام الدراسي 2024-2025

Rings Theory :-

أول اختلاف بين الزمرة والحلقة هي ان الزمرة تحوي عملية ثنائية واحدة بينما الحلقة فتحوي عمليتين ثنائيتين .

Definiton :- Let R be a non-empty set and Let $(+,\cdot)$ be two binary operation defin on R, then $(R,+,\cdot)$ is a ring if it is satisfying the following conditions.

$-R \neq \emptyset$ & $(+,\cdot)$ Two binary op. defin on R

R is Called Ring if :

1 - $(R,+)$ is abelian group. (الإبدالية)

2 - $(\cdot)$ is asscíative on R. (تجميعية) (i.e)

$\forall a,b,c \in R$, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

3 - $(\cdot)$ is distributive on $(+)$ (موزعة)

(i.e) $\forall a,b,c \in R$, $a\cdot(b+c) = a\cdot b + a\cdot c$

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

$\mathbb{R}$ الأعداد الحقيقية , R ring - حلقة -

<u>Notation</u>:- ① $(+)$ is denote the first operation.
$(\cdot)$ is " " second " .

تشير (+) للعملية الأولى مو شرط تكون جمع بينما تشير (.) الى العملية الثانية وايضاً مو شرط تكون ضرب.

$\boxed{2}$. We write R instead of $(R, +, \cdot)$
- " " $a-b$ " " " $a+(-b)$
- " " ab " " " $a \cdot b$

اختصارات.

$\boxed{3}$ (0) is dented to the identity w.r.t $(+)$
(1) " " " " " " $(\cdot)$
(if exist)

- في الحلقة تكون جميع العمليات كالمحايد والنظير في العملية الثانية في حالة ان وجد مو شرط يكون النظير او المحايد متوفر حتى تصبح حلقة.

Example:- $(Z, +, \cdot)$ is ring?

1- $(Z, +)$ is abelian group.

2- $(\cdot)$ is asso. i.e $\forall a,b,c \in Z \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$

3- $(\cdot)$ is distributive on $(+)$

since (2 & 3) By prop. of integers.

Equation: is $(N, +, \cdot)$ is ring?

Sol:- $(N, +)$ it is not group (check).

i- $(N, +)$ is closed since $a,b \in N \Rightarrow a+b \in N$

ii- $a,b,c \in N$, $a+(b+c) = (a+b)+c$. is asso.

iii- $\exists\, 0 \in N$ s.t $a+0 = 0+a = a \ \forall a \in N$.

iv- $\nexists$ id $\in N$ s.t $N = \{1, \ldots\ldots, 0\}$

لأن الأعداد الطبيعية تشمل الصفر والأعداد الموجبة فقط فأن

لا يوجد نظير لهذه الأعداد بحيث يجعل $a+(-a) = -a+a = 0$

$\therefore (N, +, \cdot)$ not group

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

Example:- the set of all integer number modulo n; (Z_n) is a ring with ($+_n$) and ($\cdot_n$) i.e ($Z_n, +_n, \cdot_n$) is a ring for example ($Z_6, +_6, \cdot_6$) is a ring

Proof:- $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

i- ($Z_6, +_6$) is abelian group.

ii- ($\cdot$) is asso. since: $\forall a,b,c \in Z_6$,

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

iii -($\cdot$) dis. (+) since:- $\forall a,b,c \in Z_6$ then

$a\cdot(b+c) = ab + ac$.

Proof that ($Z_4, +_4, \cdot_4$) is a ring ?

$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

i- ($Z_4, +_4$) is abelian group.

ii- ($\cdot$) is asso. $\forall a,b, \in Z_4$ then

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

iii -($\cdot$) is dis. (+) since

$a\cdot(b+c) = ab + ac$.

ابدالية

Definitions: ① A ring R is called commutative if the $(\cdot)$ is commutative.

- R is comm. if $\forall a,b \in R$, $ab = ba$.

② A ring R is called with identity if there exists $1 \in R \ni a \cdot 1 = 1 \cdot a = a \ \forall a \in R$. $\forall a \in R, \exists 1 \in R \ni a \cdot 1 = 1 \cdot a = a$

- ذات عنصر محايد ضربي بالنسبة للعملية الثانية $(\cdot)$.
- هو شرط ضربي حسب العملية الثانية.
- (1) رمز للمحايد هو شرط يكون واحد بس نرمز له ~~...~~ بأي رمز.

③ An element $a \in R$ is called invertible (unit) if $\exists \bar{a}^{1} \in R \ni a \cdot \bar{a}^{1} = \bar{a}^{1} \cdot a = 1$ $\quad \exists b \in R \ni ba = ab = 1$

- بعبارة اخرى في نظرية الحلقات فانه ليس كل حلقة يكون لها عنصر محايد وكذلك ليس كل عنصر في R له نظير مثال حلقة

ليس لكل عنصر فيها نظير حيث $2 \in Z$ ولا يوجد $2 \cdot a = a \cdot 2 = 1$ $\quad (Z, +, \cdot)$

* في Z كل العناصر ليس لها نظير عدا عنصرين $(1, -1)$

- وبعض الحلقات لا تحوي عنصر محايد مثال الحلقة $(2Z, +, \cdot)$

~~$2Z = \{0, \mp 2, \mp 4, \dots\}$~~ $\quad 2Z = \{0, \mp 2, \mp 4 \dots\}$

$a \cdot 1 = 1 \cdot a = a$

$4 \in 2Z$ but $\nexists$ $4 \cdot 1 = 1 \cdot 4 = 4$ ~~...~~

Example:- $(\mathbb{Z}, +, \cdot)$, $2 \in \mathbb{Z}$ is inv.?

Sol. No:- since $\nexists\, a \in \mathbb{Z} \ni a \cdot 2 = 2 \cdot a = 1$

فلا $a \cdot a^{-1} = a^{-1} \cdot a = 1$ def inv.

$2 \cdot (-2) = (-2) \cdot 2 = (-4) \neq 1$

$\therefore$ not inv. لأن تحقق شرط المعكوس (النظير).

Theorem:- Let R be a ring and let $a, b, c \in R$

Then:-

1. $a \cdot 0 = 0 \cdot a = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = +(ab)$
4. $(b-c)a = ba - ca$.
5. $a(b-c) = ab - ac$.

Remark:- $(\{0\}, +, \cdot)$ is Commutiting ring with 1

it is called trivial ring.

~~Note. $1 \neq 0$ [illegible]~~

اذا كانت الحلقة غير تافهة فأن $1 \neq 0$

المحايد الجمعي $\neq$ المحايد الضربي.

اذا كانت الحلقة تافهة فأن المحايد الجمعي = المحايد الضربي $1 = 0$

if not trivial ring the Multiplication identity $\neq$ ~~add~~ identity i.e $1 \neq 0$

Rem. Let R be a ring with 1 if $R \neq \{0\}$ then

$1 \neq 0$

Proof:-

$\because R \neq 0 \Rightarrow \exists a \neq 0 \in R$

if $1 = 0$ by Multiplying Two side by (a)

$$a \cdot 1 = a \cdot 0$$

$$a \qquad 0$$

So. $a = 0$ C!

$\therefore 1 \neq 0$

example. $(2\mathbb{Z}, +, \cdot)$ is ring

i- $(2\mathbb{Z}, +)$ is abelian.

ii- $(\cdot)$ asso.

iii- $(\cdot)$ dis. on $(+)$

is ring but it has no id.

.W :-

① $(M_{22}, +, \cdot)$ is ring.

② $(P(X), \Delta, \cup)$ is ring.

③ $(Z_8, +_8, \cdot_8)$ is ring.

Sol. $\boxed{1}$

i- $(M_{22}, +)$ is abelian group.

ii- $(\cdot)$ is asso. since $\left(\begin{bmatrix}a & b\\ c & d\end{bmatrix}\cdot\begin{bmatrix}e & f\\ g & h\end{bmatrix}\right)\cdot\begin{bmatrix}k & l\\ m & n\end{bmatrix}$

$$= \begin{bmatrix}a & b\\ c & d\end{bmatrix}\cdot\left(\begin{bmatrix}e & f\\ g & h\end{bmatrix}\cdot\begin{bmatrix}k & l\\ m & n\end{bmatrix}\right).$$

iii- $(\cdot)$ is dist. on $(+)$

since $\forall \begin{bmatrix}a & b\\ c & d\end{bmatrix}, \begin{bmatrix}e & f\\ g & h\end{bmatrix}, \begin{bmatrix}k & l\\ m & n\end{bmatrix} \in M_{22}$ then

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\cdot\left(\begin{bmatrix}e & f\\ g & h\end{bmatrix}+\begin{bmatrix}k & l\\ m & n\end{bmatrix}\right) \in M_{22}$$

توزيع المصفوفة الأولى على المصفوفتين.

$\boxed{3}$ $(\mathbb{Z}_8, +_8, \cdot_8)$ is ring $\quad \mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

i- $(\mathbb{Z}_8, +_8)$ is abeliangroup

ii - $\cdot_8$ is asso. $\quad a\cdot(b\cdot c) = (a\cdot b)\cdot c$

$$\bar{1}\cdot(\bar{2}\cdot\bar{4}) = (\bar{1}\cdot\bar{2})\cdot\bar{4}$$

$$\bar{1}\cdot\bar{8} = \bar{2}\cdot 4$$

$$\bar{8} = \bar{8}$$

iii - $\cdot_8$ is dis. on $+_8$

$\forall a, b, c \in \mathbb{Z} \Rightarrow a\cdot(b+c) = ab + ac$

if $a = \bar{3}$, $b = \bar{5}$, $c = \bar{4}$

$$a\cdot(b+c) = ab + ac$$

$$\bar{3}\cdot(\bar{5}+\bar{4}) = \bar{3}\cdot\bar{5} + \bar{3}\cdot\bar{4}$$

$$\bar{3}\cdot(\bar{9}) = \overline{15} + \overline{12}$$

$$\overline{27} = \overline{27}$$

$\boxed{3}$ $(\mathbb{P}(X), \triangle, \cup)$ is ring :-

i- $(\mathbb{P}(X), \triangle)$ is abelian group.

ii- $A \triangle \emptyset = (A-\emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

ii- $A \triangle A = (A-A) \cup (A-A)$, $\forall A \in \mathbb{P}(X)$

$= \emptyset \cup \emptyset = \emptyset$

$(\mathbb{P}(X), \cup)$ is ring.

i- $(\mathbb{P}(X), \cup)$

$\mathbb{P}(X) \neq \emptyset$. $\cup$ is binary operation on $P(X)$ since:

$\forall, A, B \in P(X)$ Then $A \cup B \in \mathbb{P}(X)$.

ii- $\cup$ is asso. since: $(A \cup B) \cup C = A \cup (B \cup C)$

iii- $(\mathbb{P}(X), \cup)$ is not ring since: is not identity element and inverse element.

"Zero divisor element"

Def. Let R be a ring. An element $a \neq 0 \in R$ is called zero divisor element if $\exists\, b \neq 0 \in R$ s.t $ab = 0$ or $ba = 0$; otherwise a is called (غير) non zero divisor element, i.e. $\forall\, b \in R$ with $ab = 0$ or $ba = 0$ implies that $b = 0$.

- $a \neq 0$

$$\begin{cases} \text{① Zero divisor element if } \exists\, 0 \neq b \in R \ni ab = 0 \text{ or } ba = 0 \\ \text{② } \forall\, b \in R \text{ s.t } ab = 0 \text{ or } ba = 0 \Rightarrow b = 0 \end{cases}$$

i.e. $\forall\, b \neq 0 \in R \rightarrow ab \neq 0$ and $ba \neq 0$.

Examples: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is zero divisor element.

Let $\bar{4} \in \mathbb{Z}_6$ s.t $\exists\, a \in \mathbb{Z}_6 \ni a \cdot \bar{4} = \bar{4} \cdot a = 0$, $a = \bar{3}$

$\exists\, \bar{3} \in \mathbb{Z}_6 \ni \bar{4} \cdot \bar{3} = \bar{3} \cdot \bar{4} = 0$

$\therefore \bar{4}$ is zero divior element.

- $\bar{1} \in \mathbb{Z}_6$ s.t $\exists\, a \in \mathbb{Z}_6 \ni a \cdot \bar{1} = \bar{1} \cdot a = 0$

$\nexists\, a \in \mathbb{Z}_6 \ni a \cdot \bar{1} = \bar{1} \cdot a = 0$

$\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ $\cdot (\mathbb{Z}_6, \cdot)$

$\therefore \bar{2}$ is zero divisor element.

since $\exists\, \bar{3} \neq 0 \in \mathbb{Z}_6$ s.t $\bar{2} \cdot \bar{3} = \bar{0}$

Also for the same reason $\bar{3}$ is zero divisor element $\exists\, \bar{2} \in \mathbb{Z}_6$ s.t $\bar{3} \cdot \bar{2} = \bar{0}$

* الصفر 0 لا هو قاسم الصفر ولا هو غير قاسم الصفر (مستثنى من التعريف).

* Z_{17} ... Z_2 , Z_3 , Z_5 , Z_7 , Z_{11} , Z_{13} (غير قاسمات الصفر).

Examplie: $(Z, +, \cdot)$ is $6 \in Z$ is Zero divisor element?

$\nexists\ ? \in Z \ni 6 \cdot ? = 0$ or $? \cdot 6 = 0$

$\therefore$ 6 is non Zero divisor element of Z is non Zero divisore

- Similarity For $(Q, +, \cdot)$ & $(\mathbb{R}, +, \cdot)$ & $(Z_p, +_p, \cdot_p)$

$\forall$ Prime no. p

- كلهن غير قاسمات الصفر.

Examplie: $Z_4 = \{\bar0, \bar1, \bar2, \bar3\}$

$\bar2$ is Zero divisor element but $\bar3$ is not Zero divisor element

Let $a = \bar2 \neq 0$ & $b = \bar3 \neq 0 \in Z_4$

$\bar2 \cdot \bar3 = \bar6 = 2$

$\bar2 \cdot \bar2 = \bar4 = \underline{0}$

$\bar2 \cdot \bar1 = \bar2$

$\therefore$ $\bar2$ is Zero divisor element.

$\bar3 \cdot \bar1 = \bar3 \neq 0$

$\bar3 \cdot \bar2 = 6 \neq 0$

$\bar3 \cdot \bar2 = \bar6 = \bar2 \neq 0$

$\bar3 \cdot \bar3 = \bar9 = \bar5 = \bar1 \neq 0$

$\therefore$ $\bar3$ is not Zero divisor element.

Examples:- $(M_{22}, +, \cdot)$ is the ring of all matricies 2×2 with real enteries has Zero divisor element.

~~let~~ $M_{22} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $a, b, c, d \in \mathbb{R}$.

Let $A \neq 0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_{22}$ $\exists B \neq 0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ s.t

$AB = 0 \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $\therefore M_{22}$ is Zero divisor element.

ضرب مصفوفات صف X عمود
عمود X صف.

هنا المصفوفة الصفرية هي الصفر.

Theorem:- let R be a ring with 1 Then:-

تملك عنصر محايد

1- 1 is non Zero divisor element.

Proof:- T.P 1 is non Zero divisor element.

Suppose The convers, i.e 1 is Zero divisor element.

$\Rightarrow \exists\, b \neq 0 \in R$ s.t $1b = 0$ or $b1 = 0$

Now. $1 \cdot b = 0 \Rightarrow 1 \cdot b = b \cdot 0$ (since $b \in R$ & R is Ring with 1)

$$\underset{b}{\overset{\shortparallel}{1 \cdot b}} = \underset{0}{\overset{\shortparallel}{b \cdot 0}}$$

$b = 0$ C!

1 is non Zero divisor element.

$\boxed{2}$ if a is unit element Then a is non-Zero divisor element.

Proof:- T.P a is nonZero divisor element.

Suppose The Converse. i.e a is Zero divisor element.

$\Rightarrow \exists\, b \neq 0 \in R$ s.t $a \cdot b = 0$ or $b \cdot a = 0$

Now. $ab = 0 \quad \cdots (1)$

Since a is unit element $\Rightarrow \exists\, a^{-1} \in R$ s.t $a a^{-1} = a^{-1} a = 1$

Multiplying Two side of eq(1) by (a^{-1}) we get:-

$$a^{-1}(ab) = 0\, a^{-1}$$

$\Downarrow$ asso. $\quad \overset{\shortparallel}{0}$ by Prop. of ring.

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

$\Downarrow$ by def id.

1

$1b = 0 \Rightarrow b = 0$ (by def id.).

$b = 0$ C!

$\therefore$ a is non Zero divisor element.

Theorem:- A ring R has no Zero divisor elemant $\Longleftrightarrow$ R satisfies The Concelation Law.

- البرهنة إذاً تعطي تشخيصاً آخر لمعرفة متى تكون الحلقة R خالية من العناصر القاسمة للصفر.

Proof:- R has no Zero divisor elemant $\Longleftrightarrow$ R Satisfies Concelation Law.

$\Longrightarrow$ We have R has no Zero divisor elemant T.P R satsfies Contelation Law.

Let $a, b, c \in R \ni ab = ac \rightsquigarrow b = c$ Multiply Two side $(-ac)$.

$$ab - (ac) = ac(-ac)$$
$$ab - ac = 0$$
$$a(b - c) = 0 \quad (a \neq 0) \text{ since R has no Zero divisor elemant.}$$
$$b - c = 0$$
$$b = c$$

$\Longleftarrow$ We have R satisfies the Coneclation Law T.P R has no Zero divisor elemant.

Let $a \neq 0 \in R$ and Let $b \in R \ni ab = 0$ Then $b = 0$ or $a = 0$

$$ab = 0 \Rightarrow ab = a \cdot 0$$
$$b = 0$$

Def: Let $(R, +, \cdot)$ be a ring is called Integral Domain حلقة تامة/ساحة if R is Commutative ①, with 1 ② and has no Zero divisor element ③.

$\therefore$ R is I.D
- ① Commutative.
- ② with 1
- ③ has no Zero divisor element.

$(Z_p, +_p, \cdot_p)$ is I.D. لأن تحقق الشروط الثلاثة اعلاه -
P, is Prime no. $P = (2, 3, 5, 7, 11, 13, 17)$

Examples: ① $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ are integral domain مهمة

② $(M_{2\times2}, +, \cdot)$ is not I.D (since not Commutative and has Zero divisor element).

③ $(Z_6, +, \cdot)$ is not I.D (since: has Zero divisor element).

Supgroup :-
$H \leq G$ if $\forall a, b \in H$
$\Rightarrow a * b^{-1} \in H$

<u>Def.</u> Let $(R, +, \cdot)$ be a ring and

Let $S \neq \phi$, $S \subseteq R$, S is called <u>subring</u> of R if S is ring itself. (تحت نفس العملية)

- هنالك شرطان إذا تحققت يقال عن $S \subseteq R$

$S \neq \phi$, $S \subseteq R$ ① $a \cdot b \in S$ $\forall a, b \in S$
② $a - b \in S$ $\forall a, b \in S$

* في كل حلقة توجد حلقتان جزئيتان تافهتان هما الصفر و R نفسها .

<u>Example :-</u> ① $\mathbb{R} \subseteq \mathbb{C}$, ② $\mathbb{Z} \subseteq \mathbb{R}$

③ $S = \{\bar{0}, \bar{3}\}$ is subgroup of Z_6?

① $\bar{3} - \bar{3} = \bar{0} \in S$
② $\bar{3} \cdot \bar{3} = \bar{9} = \bar{3} \in S$
$\therefore \{\bar{0}, \bar{3}\} \leq Z_6$.

④ $S = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq Z_6$
① $\bar{4} - \bar{4} = \bar{0} \in S$
$\bar{4} - \bar{0} = \bar{4} \in S$
$\bar{4} - \bar{2} = \bar{2} \in S$
② $\bar{4} \cdot \bar{4} = \overline{16} = \bar{4} \in S$
$\bar{4} \cdot \bar{0} = \bar{0} \in S$
$\bar{4} \cdot \bar{2} = \bar{8} = \bar{2} \in S$
$\therefore S = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq Z_6$.

⑤ $S = \{\bar{0}, \bar{2}\} \subseteq Z_4$
① $\bar{0} \cdot \bar{2} = \bar{0} \in S$
② $\bar{2} - \bar{0} = \bar{2} \in S$
$\therefore S = \{\bar{0}, \bar{2}\} \subseteq Z_4$

⑥ $S=\{\bar{0},\bar{2}\} \subseteq \mathbb{Z}_6$?

① $\bar{2}\cdot\bar{2}=\bar{4} \notin S\{\bar{0},\bar{2}\}$

② $\bar{2}-\bar{2}=0 \in \mathbb{Z}_6$.

$\therefore \{\bar{0},\bar{2}\} \nsubseteq \mathbb{Z}_6$.

⑦ $S=\{0,5\}$

① $\bar{5}-\bar{5}=\bar{0} \in S$, $\bar{0}-\bar{5}=0+(-5)=5 \in S$

② $a\cdot b \in S \quad \forall a,b \in S$.

$\bar{5}\cdot\bar{0}=0 \in S$

$\bar{5}\cdot\bar{5}=\overline{25}=\bar{5} \in S \qquad \therefore S \subseteq \mathbb{Z}_{10}$

<u>H.W</u> $S \subseteq R$.

① R تحوي عنصر محايد و S لا تحوي. (كلاهما لا يحتويان). <u>Example</u> $R \equiv \mathbb{Q}$, $S \equiv \mathbb{Z}$
where The id. (1).

② R لا تحوي عنصر محايد و S لا تحوي. <u>ex.</u> $R=2\mathbb{Z}\times 2\mathbb{Z}$
$S=2\mathbb{Z}\times\{0\}$

③ R لا تحوي عنصر محايد و S تحوي. <u>ex.</u> $R=\mathbb{Z}\times 2\mathbb{Z}$
$S=\mathbb{Z}\times\{0\}$

④ R تحوي عنصر محايد و S لا تحوي <u>ex.</u> $R=\mathbb{Z}$
$S=2\mathbb{Z}$

⑤ كلاهما يحتويان ولكن مختلفان <u>ex.</u> $R=\mathbb{Z}_6$
$S=\{\bar{0},\bar{2},\bar{4}\}$