المرحله الثالثه/قسم الرياضيات

الماده الحلقات

الفصل الثاني

Chapter Two

Chapter two - Subrings (الحلقات الجزئية)

Definition

let R be a ring. let $\emptyset \neq S \subseteq R$. Then S is Called a subring of R $\Leftrightarrow$ $(S,+,\cdot)$ is a ring.

Examples

1. $(\mathbb{Z},+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$
2. $(\mathbb{Z},+,\cdot)$ is a subring of $(\mathbb{Q},+,\cdot)$
3. $(\mathbb{Z}_e,+,\cdot)$ is a subring of $(\mathbb{Z},+,\cdot)$
4. $(\mathbb{Z}[\sqrt{3}],+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$
5. $(A,+,\cdot)$ is a subring of $(\mathbb{Z},+,\cdot)$, where $A=\{nK, K\in\mathbb{Z}\}$, n is a fixed positive integer.

Theorem

let $(R,+,\cdot)$ be a ring and let $\emptyset \neq S \subseteq R$. Then $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ iff

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

Proof :

$\Rightarrow$) It is clear that if $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$, the the two Conditions hold

(Since, $(S,+,\cdot)$ is subring of R $\Leftrightarrow$ $(S,+,\cdot)$ is a ring)

$\Leftarrow$) To prove S is a ring of R, we must prove that R holds all ring's Conditions.

Since $S \neq \emptyset$, then $\exists x \in S$

$\underset{\text{zero ele.}}{0} = x - x \in S \Longrightarrow 0 \in S$ by Condition ①

$\forall a \in S$, $0 - a \in S$ by Condition ①

$\Rightarrow -a \in S$

Now, $\forall a, b \in S$, $a + b = \underbrace{a}_{\in S} - \underbrace{(-b)}_{\in S} \in S$

$+$ on S is Comm. (since, $S \subseteq R$ and $+$ is Comm. on R)

$+$ on S is associative (since $S \subseteq R$ and $+$ asso. on R.)

$\cdot$ is closed on S (is given Condition ②)

$\cdot$ is asso. on S ($S \subseteq R$ and $\cdot$ asso. on R)

$\cdot$ distr. over $+$ on S ($S \subseteq R$, $\cdot$ dist. over $+$ on R.)

Thus $(S, +, \cdot)$ is a ring.

Example

Consider $(\mathbb{Z}_6, +_6, \cdot_6)$ ring.

Then all subrings of $(\mathbb{Z}_6, +_6, \cdot_6)$ are:

$(\mathbb{Z}_6, +_6, \cdot_6)$ is a subring of $(\mathbb{Z}_6, +_6, \cdot_6)$

(2) $(\{\bar{0}\}, +_6, \cdot_6)$ is a subring of $(Z_6, +_6, \cdot_6)$

(3) $A = \{\bar{0}, \bar{2}, \bar{4}\}$

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

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

$+_6$ closed on A

$\cdot_6$ closed on A

$+_6$ is Comm., associative on A

$-\bar{2} = \bar{4} \in A$

$-\bar{4} = \bar{2} \in A$

$\cdot_6$ associative on A

$\cdot_6$ dis. over $+_6$ on A

Then A is a subring of Z_6

④ $B = \{\bar{0}, \bar{3}\}$. To prove $(B, +_6, \cdot_6)$ of $(Z_6, +_6, \cdot_6)$

$+_6$	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{0}$

$+_6$ closed on B

$+_6$ Comm.

$\bar{0} \in B$, $-\bar{3} = \bar{3} \in B$

$\cdot_6$ closed on B,

$\cdot_6$ associative

$\cdot_6$ dis. over $+_6$ on B

Then B is a subring of Z_6.

Remark

Let $(R,+,\cdot)$ be a ring. Then R has at least two subring $\{0\}$, R.

Examples:

Consider the direct sum of $(Z,+,\cdot)$ with $(Z,+,\cdot)$

1. let $A=\{(a,0) : a\in Z\}$. Is A subring of direct sum.

solution

let $(a_1,0),(a_2,0)\in A$

1. $(a_1,0)-(a_2,0)=(\underbrace{a_1-a_2}_{\in Z},0)\in A$

2. $(a_1,0)\cdot(a_2,0)=(\underbrace{a_1a_2}_{\in Z},0)\in A$

$\therefore$ A is a subring of direct sum $(Z\times Z,\oplus,\odot)$

2. let $A=\{(a,1) : a\in Z\}$. Is A subring of direct sum.

Solution:

let $(a_1,1),(a_2,1)\in A$

1. $(a_1,1)-(a_2,1)=(a_1-a_2,0)\notin A$

Therefore A is not subring of $(Z,+,\cdot)$

Examples

Find all subrings of $(\mathbb{Z}_{24}, +_{24}, \cdot_{24})$ and $(\mathbb{Z}_{30}, +_{30}, \cdot_{30})$

① $(\mathbb{Z}_{24}, +_{24}, \cdot_{24})$

1. $\mathbb{Z}_{24}$ 2. $\{\bar{0}\}$ 3. $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \dots, \overline{22}\}$

4. $\{\bar{0}, \bar{4}, \bar{8}, \dots, \overline{20}\}$ 5. $\{\bar{0}, \bar{3}, \bar{6}, \dots, \overline{21}\}$

6. $\{\bar{0}, \bar{6}, \overline{12}, \dots, \overline{18}\}$ 7. $\{\bar{0}, \bar{8}, \overline{16}\}$ 8. $\{\bar{0}, \overline{12}\}$

$(\mathbb{Z}_{30}, +_{30}, \cdot_{30})$ (H.W.)

Example:

Consider the ring $(\mathbb{Z}[\sqrt{3}], +, \cdot)$.
let $A = \{a + b\sqrt{3} : a, b \in \mathbb{Z}_e\}$. Is A subring of $\mathbb{Z}[\sqrt{3}]$? (H.W.)

Solution

$0 = 0 + 0\sqrt{3} \in A$, $\therefore A \neq \emptyset$
let $a_1 + b_1\sqrt{3}$ and $a_2 + b_2\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

Now, $(a_1 + b_1\sqrt{3}) - (a_2 + b_2\sqrt{3}) = \underbrace{(a_1 - a_2)}_{\in \mathbb{Z}_e} + \underbrace{(b_1 - b_2)}_{\in \mathbb{Z}_e}\sqrt{3} \in A$

$(a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3}) = a_1a_2 + a_1b_2\sqrt{3} + b_1a_2\sqrt{3} + 3b_1b_2$

$= (a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{3} \in A$

Therefore A is a subring of $\mathbb{Z}[\sqrt{3}]$.

Remarks

Let R be a ring and S be a subring of R.

1. If R is Comm., then S is Comm.
2. If S is Comm., then it is not necessary that R is Comm. For example:
   $(M_2(\mathbb{R}), +, \cdot)$ is not Comm. ring

   let $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{R} \right\}$. Then A is Comm. subring of $(M_2(\mathbb{R}), +, \cdot)$.

3. If R has unity, then it is not necessary that S has unity. For example: $(\mathbb{Z}, +, \cdot)$ has unity 1, but the subring $(\mathbb{Z}_e, +, \cdot)$ of $(\mathbb{Z}, +, \cdot)$ has no unity.

4. It may that R, S have the same unity. For example: $(\mathbb{R}, +, \cdot)$ has unity 1 and $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$ has unity 1.

5. It may be that R, S have distinct a unites. For example: The ring $(\mathbb{Z}_6, +_6, \cdot_6)$ has unity $\bar{1}$, but the subring $(\{\bar{0}, \bar{2}, \bar{4}\}, +_6, \cdot_6)$ of $(\mathbb{Z}_6, +_6, \cdot_6)$ has unity $\bar{4}$ (since $\bar{4} \cdot_6 \bar{0} = \bar{0}$, $\bar{4} \cdot_6 \bar{2} = \bar{2}$, $\bar{4} \cdot_6 \bar{4} = \bar{4}$).

6. It may be that S has unity, but R has no unity.

H.W.

7. If R is an integral domain. Is S an integral domain? ✓

8. If S is an integral domain. Is R an integral domain? ✗

(8). $\mathbb{Z}_6$ is not integral domain since [illegible] $\neq 0$ but $S = \{0, 2, 4\}$ has no zero divisor $\longrightarrow$ integ