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 $R \iff (S,+,\cdot)$ 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. $a-b \in S \quad \forall a,b \in S$
2. $a\cdot b \in S \quad \forall a,b \in S$

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 $R \iff (S,+,\cdot)$ 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

$\Longrightarrow -a \in S$

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

$+$ 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.

<u>Example</u>

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

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

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

$+_6$ is Comm., associative on A.

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

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

$\cdot_6$ closed on 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? ✓ ok
8. If S is an integral domain. Is R an integral domain? ✗

(8). $\mathbb{Z}_6$ is not integral domain since $\bar{2} \cdot_6 \bar{3} \neq 0$ but $S = \{0, 2, 4\}$ has no zero divisor $\Rightarrow$ integ

Theorem

let $(R,+,\cdot)$ be a ring and let $(A,+,\cdot)$, $(B,+,\cdot)$ be two subrings of $(R,+,\cdot)$. Then $(A\cap B,+,\cdot)$ is a subring.

Proof

$0\in A$ and $0\in B$ (since A, B are subrings of R)

$\Rightarrow 0\in A\cap B$, implies that $A\cap B \neq \emptyset$.
let $a,b\in A\cap B$, implies $a,b\in A$ and $a,b\in B$
Thus $a\in A$ and $b\in A \Rightarrow a-b\in A$ and $a.b\in A$
(since A is subring of R) $\longrightarrow$ (1)

or $a,b\in B \Longrightarrow a-b\in B$ and $a.b\in B$ (since B is a subring of R) $\longrightarrow$ (2)

From (1) and (2), we get $a-b\in A\cap B$ and $a.b\in A\cap B$
Thus $A\cap B$ is a subring of $(R,+,\cdot)$

- As a generalization of above theorem, we have

The intersection of any family $\{A_i\}_{i\in\Lambda}$, Λ is any index set of subring of a ring $(R,+,\cdot)$ is a subring of $(R,+,\cdot)$.

Remark

The union of two subrings of a ring $(R,+,\cdot)$ need not be subring of R.

For example: Consider the ring $(\mathbb{Z},+,\cdot)$ and the subrings $A=\{0,\mp 2,\mp 4,\ldots\}$, $B=\{0,\mp 3,\mp 6,\mp 9\ldots\}$
$A\cup B=\{0,\mp 2,\mp 3,\mp 4,\mp 6,\ldots\}$

Since $2 \in A \cup B$, $3 \in A \cup B$ but $3-2=1 \notin A \cup B$.
Thus $A \cup B$ is not subring.

Definition

let $(R,+,\cdot)$ be a ring, the set $\{x : x \in R \wedge x \cdot y = y \cdot x \quad \forall y \in R\}$ is Called the center of R and denoted by $Cent(R)$

Remarks :

(1) If R is Comm. ring, then $Cent(R) = R$.

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

Proof :

let $x_1, x_2 \in Cent(R)$

1. $x_1 \cdot y = y \cdot x_1 \qquad \forall y \in R \longrightarrow ①$
2. $x_2 \cdot y = y \cdot x_2 \qquad \forall y \in R \longrightarrow ②$

Now, $\forall y \in R$ by ① and ② we get

$(x_1 - x_2) \cdot y = x_1 y - x_2 y = y \cdot x_1 - y \cdot x_2 = y \cdot (x_1 - x_2)$

$\therefore x_1 - x_2 \in Cent(R)$

Similarly $x_1, x_2 \in Cent(R)$

$(x_1 \cdot x_2) \cdot y = x_1 \cdot (x_2 y) = x_1 \cdot (y x_2) = (x_1 y) \cdot x_2$

$= (y \cdot x_1) \cdot x_2 = y \cdot (x_1 x_2)$

$\therefore x_1 x_2 \in Cent(R)$

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

Definition :

Let $(R,+,\cdot)$ be a ring and let $a \in R$, $n \in Z_+$.

Then :-

1. $na = a + a + \cdots + a$ (n-times)
2. $(-n)a = (-a) + (-a) + \cdots + (-a)$ (n-times)
3. $a^n = a \cdot a \cdot \cdots \cdot a$ (n-times)
4. If R has unity and a has multiplicative inverse a^{-1}, then $a^{-n} = a^{-1} \cdot a^{-1}, \cdots, a^{-1}$

Example :

Consider the ring $(Z_8, +_8, \cdot_8)$

Fined $(2)\cdot\bar{3}$, $(-2)\cdot\bar{3}$, $\bar{7}^{-2}$

Solution :

1. $(2)\bar{3} = \bar{3} +_8 \bar{3} = \bar{6}$

2. $(-2)\cdot\bar{3} = (-\bar{3}) + (-\bar{3}) = \bar{5} + \bar{5} = \bar{2}$

3. $\bar{7}^{-2} = (\bar{7}^{-1})^2 = (\bar{7})^2 = \bar{7} \cdot_8 \bar{7} = \bar{1}$

Theorem :

Let $(R,+,\cdot)$ be a ring. Then for $a, b \in R$ and arbitary integers m and n, the following hold

1. $(n+m)a = na + ma$
2. $(nm)a = n(ma)$
3. $n(a+b) = na + nb$
4. $n(a \cdot b) = (na)\cdot b = a \cdot (nb)$
5. $(na)\cdot(mb) = (nm)(a \cdot b)$

Proof :- (1)

Case (i) $n \in Z_+$, $m \in Z_+$

$$na + ma = (\underbrace{a + a + \cdots + a}_{n\text{-times}}) + (\underbrace{a + a + \cdots + a}_{m\text{-times}})$$

$$= \underbrace{a + a + a + \cdots + a + \cdots + a}_{(n+m)\text{-times}}$$

$$= (n+m)a$$

Case(ii) : $n \in \mathbb{Z}$, $m = 0$

$$na + ma = na + 0.a = na = (n+0)a = (n+m)a$$

Case(iii) : $n \in \mathbb{Z}_-$, $m \in \mathbb{Z}_-$ H.W.

Case(IV) : $n \in \mathbb{Z}_+$, $m \in \mathbb{Z}_-$ H.W.

Definition : مطلوب

let $(R, +, \cdot)$ be a ring, if there exists apositive n s.t. $na = 0$ $\forall a \in R$, then the least positive integer with this property is Called characteristic of R (Simply $ch(R)$).

If no such positive integer exists, implies $ch(R) = 0$

Examples :

1. Consider $(\mathbb{Z}, +, \cdot)$

$\forall a \in \mathbb{Z}$, only $na = \overset{\text{محايد}}{0}$, then $n = \overset{\text{محايد}}{0}$

$\therefore ch(\mathbb{Z}) = 0$

2. Each ring $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_e, +, \cdot)$ has chara. Zero.

3. Consider $(M_2(\mathbb{R}), +, \cdot)$

let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$

$\forall n \in \mathbb{Z}_+ \; ; \; nA = \begin{pmatrix} na & nb \\ nc & nd \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

if $A \neq O_{2\times 2}$, then $ch(M_2(\mathbb{R})) = 0$

(4) Consider $(\mathbb{Z}_3, +_3, \cdot_3)$

$(3)\bar{1} = \bar{1} +_3 \bar{1} +_3 \bar{1} = \bar{0}$

$(3)\bar{2} = \bar{2} +_3 \bar{2} +_3 \bar{2} = \bar{0}$

$\therefore ch(\mathbb{Z}_3) = 3$

(4) let $X \neq \emptyset$, Consider $(\mathbb{P}(X), \Delta, \cap)$
Zero element of this ring is $\emptyset$
let $A \in \mathbb{P}(X)$
$(1) A = A \Delta A = \emptyset$
since $A \Delta A = (A/A) \cup (A/A) = \emptyset \cup \emptyset = \emptyset =$ Zero element

$\therefore ch(\mathbb{P}(X), \Delta, \cap) = 2$

⊛ problem: Prove or disprove
let R be a ring and let S be a subring of R.
Then:
1. $ch(R) = ch(S)$
2. $ch(R) \neq ch(S)$

$ch(\mathbb{Z}_6) = 6$
but $A = \{\bar{0}, \bar{2}, \bar{4}\}$
The identity element of A is $\bar{4}$
Then $ch(A) = 3$
Since, $\bar{4} +_6 \bar{4} +_6 \bar{4} = \bar{0}$

Theorem:

let $(R, +, \cdot)$ be a ring with unity 1. Then $ch(R) = n$, $n \in \mathbb{Z}_+ \Leftrightarrow n$ is the least positive integer s.t. $n1 = 0 \rightarrow$ Zero element

Proof:-

$\Rightarrow$) If $ch(R) = n$, $n \in \mathbb{Z}_+$

① $\leftarrow \therefore n$ is the least positive integer s.t. $na = 0 \ \forall a \in R$

$1 \in R \Rightarrow n1 = 0$ by ①

suppose $\exists m \in \mathbb{Z}_+$ and $m < n$ and $m1 = 0$ البرهنة ان

أصغر عدد صحيح موجب

$\forall a \in R$, $ma = m(1 \cdot a) = (m \cdot 1) \cdot a = 0 \cdot a = a$

Since, $ma = 0 \ \forall a \in R$ and $m < n$ which Contradict the state ① تناقض العبارة

Thus n is the least positive s.t. $n1 = 0$

$\Leftarrow$) let $a \in R$, $na = n(1 \cdot a) = (n \cdot 1) a = 0 \cdot a = 0$

$\therefore ch(R) \leq n$, we must prove that n is the least positive integer

حتى تصبح $ch(R) = n$

suppose $ch(R) = m$ and $m < n$

$\Rightarrow m \cdot 1 = 0$ Cl. Therefore $ch(R) = n$.

Corollary:-

$ch(\mathbb{Z}_n, +_n, \cdot_n) = n$, $n > 1$

تطبيق مباشر على النظرية اعلاه

where $n\bar{1} = \bar{1} +_n \bar{1} +_n \bar{1} +_n \cdots +_n \bar{1} = \bar{0}$

Theorem :-

let $(R,+,.)$ be an integral domain. Then $Ch(R)$ is either Zero or prime number.

Proof :-

suppose $ch(R)=n$, $(n \in Z_+)$ and n is not prime. Thus $n=mk$ for some $m, k \in Z_+$
$1<m<n$, $1<k<n$

$ch(R)=n$ (since n is the least positive integer) ⊛
s.t. $n1=0$

$n1=0=$ Zero element

$(m.k)(1.1)=0 \Rightarrow (m.1)(k.1)=0$

$\Rightarrow m1=0$ or $k1=0$ (since R is an integral domain. i.e R has no Zero divisor)

Case ① $m1=0$, but $m<n \Rightarrow$ C! with ⊛

Case ② if $k1=0$ C! with ⊛ (since $k<n$)

∴ our assumption is false $\Rightarrow ch(R)=0$ or prime number.

كلية التربيه للعلوم الصرفه /ابن الهيثم
قسم الرياضيات/المرحله الثالثه
المادة /حلقات

الفصل الثالث

chapter three

Chapter Three *(IDEAL)* المثاليات ideals

Definition :-

let $(R,+,.)$ be a ring and S a subring of R.

1. S is Called a right ideal of $R \Leftrightarrow a.r \in S$
2. S is Called a left ideal of $R \Leftrightarrow r.a \in S$

$\forall a \in S, \forall r \in R$

3. S is Called left and right ideal of R (or two sided ideal) $\Leftrightarrow a.r \in S$ and $r.a \in S$ $\forall a \in S, r \in R$.

Remark :

In Comm. ring every left ideal is right ideal and Conversely.

Example :

The subring $(Ze,+,.)$ is an ideal of $(Z,+,.)$.

Since. If $a = 2n \in Ze$ and $r \in Z$, then

$r.a = a.r = (2n).r = 2(n.r) \in Ze$

Theorem :-

let $(R,+,.)$ be a ring, and let $\phi \neq S \subseteq R$. Then S is an ideal of $R \Leftrightarrow$

1. $a - b \in S$ $\quad \forall a,b \in S$
2. $a.r \in S$ and $r.a \in S$ $\quad \forall a \in S, r \in R$

Examples :

هذا المثال يوضح انه ليس كل subring يكون ideal

1. Consider $(\mathbb{R}, +, \cdot)$, $\emptyset \neq Z \subseteq \mathbb{R}$

$5 \in Z$, $\frac{1}{3} \in \mathbb{R}$, but $5 \cdot \frac{1}{3} = \frac{5}{3} \notin Z$

ideal $\Rightarrow$ subring
$\nLeftarrow$

$\therefore Z$ is not an ideal of $\mathbb{R}$.

2. $\emptyset \neq Q \subseteq \mathbb{R}$, $\frac{1}{2} \in Q$, $\sqrt{3} \in \mathbb{R}$, but $\frac{\sqrt{3}}{2} \notin Q$. Then Q is not ideal in $\mathbb{R}$.

3. Find all ideals of $(Z_6, +_6, \cdot_6)$

a. $(\bar{1}) = Z_6$ b. $\{\bar{0}\}$ c. $\{\bar{0}, \bar{2}, \bar{4}\}$ d. $\{\bar{0}, \bar{3}\}$

تعميم :

جميع الحلقات الجزئية من الحلقة $(Z_n, +_n, \cdot_n)$ هي مثاليات اي بمعنى ليس كل subring هو ideal فقط في $(Z_n, +_n, \cdot_n)$.

Remark : let $(R, +, \cdot)$ be a ring and $R \neq \{0\}$. Then R has at least two subrings which are $\{0\}$, R.

Example : Consider the ring $(M_2(Z), +, \cdot)$.

let

1. $S_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in Z \right\}$

$S_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in Z \right\}$

$S_3 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in Z \right\}$

① Is S_1 left (right) ideal of $M_2(Z)$?

② Is S_2 left (right) ideal of $M_2(Z)$?

③ Is S_3 left (right) ideal of $M_2(Z)$?

Solution :-

① $\emptyset \neq S_1 \subseteq M_2(Z)$

let

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix}, \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in S_1 \qquad a_1, a_2, b_1, b_2 \in Z$$

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{pmatrix} \in S_1$$

let $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(Z)$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \cdot \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} = \begin{pmatrix} xa_1 & yb_1 \\ za_1 & wb_1 \end{pmatrix} \notin S_1$$

$\therefore$ S_1 is not left ideal.

To prove (right)

$$\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a_1 x & a_1 y \\ b_1 z & b_1 w \end{pmatrix} \notin S_1$$

$\therefore$ S_1 is not right ideal.

Example :

let $R = (Z \times Z, \oplus, \odot)$.

let :

$S_1 = \{(a,0) ; a \in Z\}$

$S_2 = \{(a,b) ; a \in Z , b \in Z\}$

$S_3 = \{(a,b) ; a \in Z , b \in Z_e\}$

$S_4 = \{(a,b) ; a \in Z_e \wedge b \in Z_e\}$

IS S_1, S_2, S_3, S_4 an ideal of R ?

Solution : 3

$\emptyset \neq S_2 \subseteq R$

let $(a_1,b_1), (a_2,b_2) \in S_2$ s.t. $a_1,a_2 \in Z$
$b_1,b_2 \in Z_e$

$(a_1,b_1) - (a_2,b_2) = (a_1 - a_2 , b_1 - b_2) \in S_2$

Since $a_1,a_2 \in Z \Longrightarrow a_1 - a_2 \in Z$
$b_1, b_2 \in Z \Longrightarrow b_1 - b_2 \in Z_e$

let $(x,y) \in R = Z \times Z$

$(x,y) \odot (a_1,b_1) = (xa_1 , yb_1) \in S_2$.

Since $x \in Z , a_1 \in Z \Longrightarrow xa_1 \in Z$

$y \in Z , b_1 \in Z_e \longrightarrow yb_1 \in Z_e$ and $\odot$ is Comm.

we have S_2 is an ideal of $R = Z \times Z$

Remarks :

1. let $(R,+,\cdot)$ be a ring with unity 1, I be an

ideal of R. If $1 \in I$, then $I = R$

Proof:

$I \subseteq R$ (by def. of ideal)

$\forall r \in R \Rightarrow r = r.1$ (1 is the identity of R)

but $r \in R$, $1 \in I \Rightarrow r.1 \in I$ (I is an ideal)

$\therefore r \in I$

$\therefore R \subseteq I$. Thus $R = I$

② let R be a ring with unity 1 and I is an ideal of R, $a \in R$. If a is an invertible element and $a \in I$, then $I = R$.

Proof:

let $a \in I$ and a is an invertible element. Then $\exists\, a^{-1} \in R$ s.t $a a^{-1} = 1$

Therefore $1 = \underset{\in I}{a} . \underset{\in R}{a^{-1}} \in I$ (I is an ideal of R)

$\therefore 1 \in I$ (by previous remark)

③ Any field $(F, +, .)$ has only two ideals namely F and $\{0\}$.

Proof: let I be an ideal of R s.t. $I \neq \{0\}$

$\therefore \exists a \in I \wedge a \neq 0$

$\therefore$ a is an invertible element (since F is field)

Thus $I = F$ by previous remark.

Theorem :

let $(R,+,\cdot)$ be a ring and let I, J be two ideals of R. Then $(I\cap J,+,\cdot)$ is an ideal of R.

Proof :- $\emptyset \neq I\cap J \subseteq R$ (since $0\in I$, $0\in J \Rightarrow 0\in I\cap J$)

let $a,b \in I\cap J$, $r\in R$.

$a,b\in I\cap J \Rightarrow a\in I \wedge a\in J$, $b\in I \wedge b\in J$

$\therefore a-b\in I \wedge a-b\in J$

$r.a\in I \wedge a.r\in I$ (since I is an ideal of R)

$r.a\in J \wedge r.a\in J$ (since J is an ideal of R)

Thus $a-b\in I\cap J$ and $r.a\in I\cap J$, $ar\in I\cap J$

$\therefore I\cap J$ is an ideal of R.

Remark :-

The union of two ideals of ring R is not necessary an ideal of R, for example:

$(Z_6,+_6,\cdot_6)$, $(\bar{2})$ and $(\bar{3})$ are ideals of Z_6

But $(\bar{2})\cup(\bar{3}) = \{\bar{0},\bar{2},\bar{3},\bar{4}\}$.

since $4-3=1 \notin (\bar{2})\cup(\bar{3})$

Definition :-

let R be a Comm ring with unity and $a\in R$. let $I=\{r.a : r\in R\}$. Then I is an ideal of R and this ideal is called a principle ideal generated by a and denoted by (a), $id(a)$, $\langle a\rangle$.

proof: $I \neq \emptyset$ since, $0 = 0.a \in I$

let $x_1, x_2 \in I$; $c \in R$

$x_1 = r_1 a$, $x_2 = r_2 a$ for some $r_1, r_2 \in R$

$x_1 - x_2 = r_1 a - r_2 a = (r_1 - r_2) a \in I$

$c x_1 = c \cdot (r_1 a) = (c r_1) \cdot a \in I$

$\therefore I$ is an ideal of R.

Example:

① Consider the ring $(\mathbb{Z}, +, \cdot)$

$id(2) = \{r.2 : r \in \mathbb{Z}\} = \{0, \mp 2, \mp 4, \ldots\}$

$id(-2) = \{r.(-2) ; r \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \ldots\}$

$id(a) = id(-a)$ بصورة عامة

النظير الجمعي لـ a

$id(1) = \mathbb{Z}$, $id(0) = \{0\}$

② Consider the ring $(\mathbb{Z}_6, +_6, \cdot_6)$

$id(\bar{1}) = \{\bar{r} \cdot_6 \bar{1} ; \bar{r} \in \mathbb{Z}_6\} = \mathbb{Z}_6$

$id(\bar{0}) = \{\bar{0}\}$

$id(\bar{2}) = \{\bar{r} \cdot_6 \bar{2} : \bar{r} \in \mathbb{Z}_6\}$

$= \{\bar{0} \cdot_6 \bar{2}, \bar{1} \cdot_6 \bar{2}, \bar{2} \cdot_6 \bar{2}, \bar{3} \cdot_6 \bar{2}, \bar{4} \cdot_6 \bar{2}, \bar{5} \cdot_6 \bar{2}\}$

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

$id(\bar{3}) = \{\bar{0}, \bar{3}\}$

$id(\bar{4}) = \{\bar{0}, \bar{4}, \bar{2}\}$ نلاحظ $id(\bar{4}) = id(\bar{2})$
(لأنه واحد نظير الآخر)

$id(\bar{5}) = \{\bar{0}, \bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}\} = Z_6$
لأنه

$\bar{5} \cdot_6 \bar{5} = \bar{1} \in id(\bar{5})$

$\therefore id(\bar{5}) = Z_6$

Theorem :-
let R be a Comm. ring with unity 1.
Then :-
1. $id(1) = R$ and $id(0) = \{0\}$
2. $a \in id(a)$
3. $id(a) = id(-a)$
4. $id(a) = R$ if a is an invertible.

problems :-

1. Find all P.I. in $(Z_5, +_5, \cdot_5)$
2. Find all P.I. in $(Z_{12}, +_{12}, \cdot_{12})$

Definition : let R be a Comm. ring with unity 1, and let $a, b \in R$
$I = \{r_1 a + r_2 b : r_1, r_2 \in R\}$. Then I is an ideal of R and this ideal is called the ideal generated by a and b, denoted by $id(a,b)$, $\langle a,b \rangle$, (a,b).

let R be a comm. ring with unity 1 تعميم
let $a_1, a_2, a_3, \dots, a_n \in R$

let $I = \{\sum_{i=1}^{n} x_i a_i : x_i \in R\}$. Then I is an ideal of R.

Example:
Consider the ring $(\mathbb{Z}, +, \cdot)$.
Find $id(2,3)$, $id(2,4,6)$, $id(3,5)$

$id(3,5) = \{x_1 \cdot 3 + x_2 \cdot 5 : x_1, x_2 \in \mathbb{Z}\}$

$1 = 2 \cdot 3 + (-1) 5 \in id(3,5) = \mathbb{Z} = id(1)$

$\therefore id(n,m) = id(d)$

حيث d = القاسم المشترك
وهذه في حالة $\mathbb{Z}$ فقط
وذلك حسب خوارزمية الاقليدية والتي تنص

let $a, b \in \mathbb{Z}$, $d = gcd(a,b)$
$\Rightarrow d = r_1 a + r_2 b$ for some $r_1, r_2 \in \mathbb{Z}$

Example:
let R be the direct sum of $(\mathbb{Z}, +, \cdot)$ with $(\mathbb{Z}, +, \cdot)$. Then Find:

1. $id(1,0) = \{(r, k) \odot (1,0) : (r,k) \in R\}$

$= \{(r, 0) : r \in \mathbb{Z}\}$

2. $id((1,1), (1,1)) = R$

3. $id\left((1,0),(0,1)\right) = \{((r_1,k_1),(r_2,k_2)) \odot ((1,0),(0,1))$

$; (r_1,k_1),(r_2,k_2) \in R \}$

$= \{(r_1,0),(0,k_2) \; ; r_1,k_2 \in Z\}$.

$Z\times\{0\} \cup \{0\}\times Z$

Definition :-

let R be a Comm. ring with unity 1. R is Called a principle ideal ring (P.I.R.) iff every ideal of R is a p.I.

Example :- $(Z_8, +_8, \cdot_8)$ is a P.I.R.

Theorem :- $(Z, +, \cdot)$ is a P.I.R.

Proof :- let I be any ideal of Z

If $I=\{0\}$, then $I = id(0)$ is a P.I

If $I \neq \{0\}$, then $\exists m \in I \wedge m \neq 0$

Since $m \in I \Rightarrow -m \in I$

So, I Contians positive integers

لتكن S هي مجموعة كل الأعداد الصحيحة الموجبة الموجودة في I

$\therefore S \subseteq Z_+$. But Z_+ is a w.o.s

مجموعة مرتبة تماماً

$\therefore$ S has a least element say n.

$\therefore$ n is the least positive integer of I.

we claim that $I = id(n)$

let $x \in id(n)$

$x = r.n$ where $r \in \mathbb{Z}$

but $n \in I \Rightarrow x = rn \in I$

$\therefore id(n) \subseteq I \longrightarrow ①$

Now, let $x \in I$

$\because x, n \in \mathbb{Z} \Rightarrow \exists\, q, r \in \mathbb{Z}$ s.t.

$x = qn + r \qquad 0 \leq r < n$ (حسب خوارزمية القسمة)

if $0 < r < n$, $\quad r = \underbrace{x}_{\in I} - \underbrace{qn}_{\in I} \in I$

$\therefore x$ is a positive integer in I and $r < n$ C!

كون n أصغر عدد صحيح موجب في I

Thus $r = 0$ and so $x = qn \in id(n)$

$\therefore I \subseteq id(n) \longrightarrow ②$

From ① and ②, we get $I = id(n)$.

Theorem:

Every field is a P.I.R.

Proof: let $(F, +, .)$ be any field and F has only two ideals which are $F, \{0\}$. But $F = id(1)$, $\{0\} = id(0)$

$\therefore F$ is P.I.R

Some operations on ideals

بعض العمليات على المثاليات

Definition :

let $(R,+,\cdot)$ be a ring and I, J be two ideals of R.
Define $I+J = \{x+y : x \in I \wedge y \in J\}$. Then $I+J$ is said to be the sum of I and J.

Remark : $I+J$ is an ideal of a ring $(R,+,\cdot)$, where I, J are ideals of R.

Proof :-

Since $I+J \subseteq R$ (by Def. of ideal)

and $I+J \neq \emptyset$, since $0 = \underset{\in I}{0} + \underset{\in J}{0} \in I+J$

Now, let x_1+y_1 and $x_2+y_2 \in I+J$

s.t. $x_1, x_2 \in I$ and $y_1, y_2 \in J$

$(x_1+y_1) - (x_2+y_2) = (x_1-x_2) + (y_1-y_2) \in I+J$

Since, $x_1, x_2 \in I \Longrightarrow (x_1-x_2) \in I$
$y_1, y_2 \in J \Longrightarrow (y_1-y_2) \in J$ (since, I, J, are ideals of R

let $r \in R$, $r\cdot(x_1+y_1) = rx_1 + ry_1$

$x_1 \in I \longrightarrow rx_1 \in I$
$y_1 \in I \longrightarrow ry_1 \in I$ (Since $I \wedge J$ are ideals of R.)

Similarly : $(x_1+y_1)r \in I+J$.

Thus $I+J$ is an ideal of R.

Class

Remark :

let $(R,+,\cdot)$ be a Comm. ring and $a,b \in R$.
Then $id(a,b) = id(a) + id(b)$

Examples :

1. In $(\mathbb{Z},+,\cdot)$

⊛ $id(3) + id(4) = id(3,4) = id(1) = \mathbb{Z}$

⊛ $id(2) + id(4) = id(2,4) = id(2) = \mathbb{Z}_e$

2. Consider $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ ring.

let $I = id(\bar{2})$, $J = id(\bar{3})$, $K = id(\bar{4})$,
$L = id(\bar{6})$

⊛ $K + L = id(\bar{4}) + id(\bar{6}) = \{\bar{0},\bar{4},\bar{8}\} + \{\bar{0},\bar{6}\}$

$= \{\bar{0} +_{12} \bar{0} , \bar{0} +_{12} \bar{6} , \bar{4} +_{12} \bar{0} , \bar{4} +_{12} \bar{6} , \bar{8} +_{12} \bar{0} , \bar{8} +_{12} \bar{6}\}$

$= \{\bar{0}, \bar{6}, \bar{4}, \overline{10}, \bar{8}, \bar{2}\} = id(\bar{2})$

⊛ $L + L = id(\bar{6}) + id(\bar{6}) = \{\bar{0},\bar{6}\} + \{\bar{0},\bar{6}\}$

$= \{\bar{0},\bar{6}\}$

عند جمع المثالي مع نفسه
يكون الناتج المثالي نفسه

Now, Find $J + L$, $J + K$, $I + L$ (H.W)

Remark: Let R be a ring, I be an ideal of R. Then $I+I=I$.

Proof:
it's clearly $I \subseteq I+I$ ..

To prove $I+I \overset{?}{\subseteq} I$

For all $x+y \in I+I$, $x \in I \wedge y \in I$

$\therefore x+y \in I$ (I is an ideal of R).

Thus $I+I \subseteq I$ and hence $I+I=I$.

Definition:

let $(R,+,\cdot)$ be a ring, I, J be two ideals of R.
let $I \cdot J = \{\sum_{\text{finite sum}} a_i b_i : a_i \in I, b_i \in J\}$. Then

$I.J$ is called the product of I and J.

Remark:
$IJ \subseteq I$ and $IJ \subseteq J$

Proof:
T.P. $IJ \overset{?}{\subseteq} I$

let $x \in IJ \Longrightarrow x = \sum_{\text{finite sum}} a_i b_i$, $a_i \in I$, $b_i \in J$ $\forall i$

$x = a_1 b_1 + a_2 b_2 + \text{———} + a_n b_n$ for some $n \in \mathbb{Z}_+$

but $a_i \in I$ $\forall i = 1, 2, \ldots, n \Longrightarrow a_i b_i \in I$ $\forall i$

$\therefore x \in I$ (since $+$ is closed on I) $\Rightarrow IJ \subseteq I$

Similarly, $IJ \subseteq J$.

Example:

Consider $(\mathbb{Z}_6, +_6, \cdot_6)$. let $I = \{\bar{0}, \bar{2}, \bar{4}\}$
$J = \{\bar{0}, \bar{3}\}$

Thus $a_i \cdot b_i = 0 \quad \forall a_i \in I,\ b_i \in J$

$\therefore I \cdot J = \{\bar{0}\}$

Remark:

It is not necessary that $I \cdot I = I$.

For example:

Consider $(\mathbb{Z}, +, \cdot)$

let $I = id(2)$, $J = id(3)$

$$I \cdot J = \{\underset{\text{finite sum}}{\sum} a_i b_i : a_i \in id(2),\ b_i \in id(3)\}$$

$\therefore a_i = 2m_i \quad m_i \in \mathbb{Z}$
$\quad\ b_i = 3n_i \quad n_i \in \mathbb{Z}$

$a_i \cdot b_i = (2m_i) \cdot (3n_i) = 6(m_i n_i) = 6c_i$ where $c_i = m_i n_i$

$\therefore \underset{\text{finite sum}}{\sum} a_i b_i =$ multiple of 6.

$\therefore IJ = id(6)$
$\quad I \cdot I = id(4) \subsetneq I$

كلية التربيه للعلوم الصرفه/ابن الهيثم

قسم الرياضيات/المرحله الثالثه

الماده /الحلقات

الفصل الرابع والخامس

Chapter Four And Five

Chapter Four (Factor Rings) الحلقات الكسرية

(Quotient Rings)

مر

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

let $(R,+)$ is a Comm. group.
$(I,+)$ is a subgroup of $(R,+)$

$I \Delta R$, since every subgp. of Comm. gp is normal.

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

Define $\oplus$ on $R\backslash I$ by :

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

and define $\odot$ on $R\backslash I$ by :

$(a+I) \odot (b+I) = a\cdot b + I \quad \forall a+I, b+I \in R/I$

Then $(R/I, \oplus, \odot)$ is a ring.

Since $\oplus, \odot$ are closed on R/I (by Def. of $\oplus$ and $\odot$)

To prove $\oplus$ is well-define

let $a+I = a_1+I$ means $a+(-a_1) \in I \Rightarrow a-a_1 \in I$
$b+I = b_1+I$ means $b+(-b_1) \in I \Rightarrow b-b_1 \in I$

We must $(a+I) \oplus (b+I) = (a_1+I) \oplus (b_1+I)$
that is, $(a+b)-(a_1+b_1) \in I$