Chapter Seven

Subrings and Ideals

<u>Defintion:</u> (7.1) (Subring)

Anon-empty set S of a ring R is called a subring if itself is a ring.

<u>Defintion:</u> (7.2) (Subring)

A non-empty subset $S \subseteq R$ of a ring R is called a subring if

(i) $\forall\, a, b \in S, \quad a - b \in S$
(ii) $\forall\, a, b \in S, \quad a.b \in S$

Example: (7.3)

$(\mathbb{Z}, +, .)$ is a subring of $(\mathbb{R}, +, .)$.

Example: (7.4)

Show that $(\mathbb{Z}_e, +, .)$ is a subring of $(\mathbb{Z}, +, .)$.

Solution:

(1) Let $a, b \in \mathbb{Z}_e$

We show that $a - b \in \mathbb{Z}_e$

Let $a = 2k_1$ *and* $b = 2k_2$ where $k_1, k_2 \in \mathbb{Z}$.

Now, $a - b = 2k_1 - 2k_2 = 2(k_1 - k_2)$

Let $k_3 = k_1 - k_2$, then $2k_3 \in \mathbb{Z}_e$

$\therefore a - b \in \mathbb{Z}_e$.

(2) Let $a, b \in \mathbb{Z}_e$. We show that $a.b \in \mathbb{Z}_e$

Let $a = 2k_1$ *and* $b = 2k_2$ where $k_1, k_2 \in \mathbb{Z}$.

Now, $a.b = 2k_1 . 2k_2 = 2(2k_1 . k_2)$

Let $k_3 = 2k_1 . k_2$, then $2k_3 \in \mathbb{Z}_e$

$\Rightarrow a.b \in \mathbb{Z}_e$

Hence $\mathbb{Z}_e$ is a subring of $\mathbb{Z}$.

<u>Remark:</u> (7.5)

There exist two trivial subrings of any rings, which are $(R, +, .)$ and $(\{0\}, +, .)$.

Example: (7.6)

Let $(\mathbb{Z}, +, .)$ be the ring of integers.

$S = \{3n : n \in \mathbb{Z}\} = \langle 3 \rangle = (3)$.

$(\langle 3 \rangle, +, .)$ is a subring of $(\mathbb{Z}, +, .)$.

Remark: (7.7)

For each $n \in \mathbb{Z}$.

$(\langle n \rangle, +, .)$ is a subring of $(\mathbb{Z}, +, .)$.

Defintion: (7.8) Ideals

A non – empty subset I of a ring R is said to be a right (resp. left) ideal of R if for each $a, b \in I$ *and* $r \in R$, *then* $a - b \in I$ *and* $a.r \in I$ (*resp.* $r.a \in I$).

Defintion: (7.9)

A non – empty subset I of a ring R is said to be two - sided ideal (or ideal) if for each $a, b \in I$ *and* $r \in R$, then

(1) $a - b \in I$
(2) $a . r \in I$ *and* $r.a \in I$.

Remark: (7.10)

If R is commutative, then right ideal = left ideal = deal.

Question: (7.11) H.W.

Let $P = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_2 \right\}$. Find all right ideals and left ideals of P.

Question: (7.12) H.W.

Give an example of a ring it has right ideal, but it has no left ideal.

Question: (7.13)

Let R be a ring and a ∈ R, then show that $P = \{r \in R: ar = 0\}$ is a right ideal of R.

Sol:

(1) Let $a, b \in P$,we must to prove $a - b \in P$

Since $a \in P$, then $ar = 0$

And $b \in P$, then $br = 0$

Is $(a - b)\, r = 0$?

Now, $(a - b)\, r = ar - br = 0 - 0 = 0,$

$so, a - b \in P.$

(2) let a ∈ P and K ∈ R.

We show that ak ∈ P,

i. e, we show that $(ak). r = 0$.

$But, (ak).r = a.(k.r) = a.t = 0, where\ t = k.r$.

$\therefore a.k \in P$

$\therefore$ P is a right ideal of R

<u>Theorem:</u> (7.14)

If $(I_1, +, .)$ and $(I_2, +, .)$ are two ideals of a ring $(R, +, .)$. Then $(I_1 \cap I_2, +, .)$ also is an ideal.

<u>Proof</u>: We have,

$\emptyset \neq I_1 \subseteq R$ and $\emptyset \neq I_2 \subseteq R, then\ I_1 \cap I_2 \supseteq \{0\}$.

$\Rightarrow \emptyset \neq I_1 \cap I_2 \subseteq R$.

(1) Let $a, b \in I_1 \cap I_2$.

$\Rightarrow a, b \in I_1$ and $a, b \in I_2$.

$\Rightarrow a - b \in I_1$ and $a - b \in I_2$ $(since\ I_1\ and\ I_2 are\ ideals)$

$\Rightarrow a - b \in I_1 \cap I_2$.

(2) $Let\ a \in I_1 \cap I_2\ and\ r \in R$

$\Rightarrow a \in I_1$ and $a \in I_2$.

$\Rightarrow ar \in I_1$ $and\ ar \in I_2$ $(since\ I_1\ and\ I_2\ are\ ideals)$

$\Rightarrow ar \in I_1 \cap I_2$.

<u>Also</u> $ra \in I_1$ $and\ ra \in I_2$.

$ra \in I_1 \cap I_2$.

$\therefore (I_1 \cap I_2, +, .)$ is also an ideal of $(R, +, .)$.

Question: (7.15)

Is the union of two ideals an ideal? Explain.

Ans: No, for example

$I_1 = \{0, 3, 6, 9\}$ and $I_2 = \{0, 2, 4, 6, 8, 10\}$ are ideals of $(\mathbb{Z}_{12}, +_{12}, ._{12})$

Now, $I_1 \cup I_2 = \{0, 2, 3, 4, 6, 8, 9, 10\}$ is not ideal since $2, 3 \in I_1 \cup I_2$,

$but\ 3 - 2 = 1 \notin I_1 \cup I_2$

<u>Theorem:</u> (7.16)

Let $(R, +, .)$ be a ring with unity and I an ideal of R containing a unity. Then $I = R$.

<u>Proof:</u>

Since I ⊆ R ___________ (1)

Let r ∈ R and 1 ∈ I (since I containing the unity)

⇒ r.1 ∈ I and 1. r ∈ I (since I is an ideal)

⇒ r ∈ I

$\therefore\ R \subseteq I$ __________(2)

From (1) and (2) we get I = R.

Defintion: (7.17) (The sum of two ideals)

Let I_1 and I_2 be two ideals of a ring R, then
$I_1 + I_2 = \{a + b : a \in I_1 , b \in I_2 \}$ is said to be the sum of two ideals.

Theorem: (7.18)

For any two ideals I_1 and I_2 of a ring R, then $I_1 + I_2$ is an ideal of R.

Proof:

(1) Let $x, y \in I_1 + I_2$.

We show that $x - y \in I_1 + I_2$

Since $x \in I_1 + I_2 \Rightarrow x = a_1 + b_1$, $where\ a_1 \in I_1 , b_1 \in I_2$

and $y \in I_1 + I_2 \Rightarrow y = a_2 + b_2$, $where\ a_2 \in I_1 , b_2 \in I_2$. Then,

$x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

[$(a_1 - a_2) \in I_1$ and I_1 is an ideal] and

[$(b_1 - b_2) \in I_2$ and I_2 is an ideal]

$So, (x - y) \in I_1 + I_2$.

(2) Let $x \in I_1 + I_2\ and\ r \in R$.

We want to show that $xr \in I_1 + I_2\ and\ rx \in I_1 + I_2$.

Since $x \in I_1 + I_2 \Rightarrow x = a + b$, where $a \in I_1\ and\ b \in I_2$.

$xr = (a + b)\, r$

$= ar + br$ ($ar \in I_1$ since I_1 is an ideal of R and $br \in I_2$ since I_2 is an ideal of R)

So, $xr \in I_1 + I_2$

Also, $rx = r(a + b)$

$= ra + rb$ ($ra \in I_1$ since $I_1$is an ideal of R and $r\,b \in I_2$ since I_2 is an ideal of R)

So, $rx \in I_1 + I_2$

$\therefore I_1 + I_2\ is\ an\ ideal\ of\ R.$

Defintion: (7.18′) (The multiplication of two ideals)

Let I_1 and I_2 be two ideals, then

$I_1 I_2 = \{\sum_{i=1}^{n} a_i b_i : a_i \in I_1 \ , b_i \in I_2\}$

<u>Question:</u> (7.18″) (H.W.)

Show that I_1 I_2 is an ideal of R.

<u>Defintion:</u> (7.19) (Ideal generated by a subset)

Let S be a non-empty subset of the ring R and let $G = \{A_\alpha\}_{\alpha \in J}$ be the family of ideals.

Then, $\bigcap_{\alpha \in J} A_\alpha$ is an ideal such that $S \subseteq \bigcap_{\alpha \in J} A_\alpha$, then $\bigcap_{\alpha \in J} A_\alpha$ is an ideal generated by S and dented by $< S > = \bigcap_{\alpha \in J} A_\alpha$.

<u>Defintion:</u> (7.20) (Principal Ideal)

If R is a ring and a ∈ R, then the ideal generated by a is said to be principal ideal and it is denoted by $(< a > \ , + \ , .)$ or $((a) \ , + \ , .)$, i.e,

an ideal generated by a single ring element, say a is called a principal ideal.

<u>Remark:</u> (7.20′)

Also, we use the symbol aR (resp. Ra) for right (resp. left) principal ideal of R.

<u>Ex 7.21</u>:

Let $(\mathbb{Z} , + \ , .)$ be the ring of integers.

(2) , (3) , (5) , … are principal ideals, where

$(2) = 2\mathbb{Z}$

$(3) = 3\mathbb{Z}$

$(5) = 5\mathbb{Z}$, …

<u>Theorem:</u> (7.22)

Let I_1 and I_2 be two ideals of a ring R, then $I_1 + I_2 = < I_1 \cup I_2 >$.

Proof: (H.W.)

<u>Defintion :</u> (7.23)

A ring R is called principal ideal ring if every ideal of R is principal.

<u>Theorem:</u> (7.24)

The ring $\mathbb{Z}$ of integers is principal ideal ring; **in fact** if I is an ideal of $\mathbb{Z}$, then $I = (n)$ for some non-negative integer n.

Proof: (H.W.)

<u>Defintion:</u> (7.25) (Simple ring)

A ring R is to be simple if it has no proper ideals.

<u>Example</u>: (7.26)

(ℝ , + , .) is the simple ring, where ℝ is the set of all real numbers.

Lemma: (7.27)

Every division ring is a simple ring.

Proof:

Let R be a division ring and let I be an ideal of R.

Suppose $I \neq \{0\}$. Then $\exists\ 0 \neq a \in I$.

Since R is a division ring, then a has multiplicative inverse.

Therefor, $\exists\ b \in R$ such that $a.\ b = 1 \in I$.

Therefor, by Theorem 7.16, I = R.

∴ R is a simple ring.

Idempotent and Nilpotent elements of a ring

Defintion: (7.28) (Nilpotent element)

An element a of a ring R is said to be nilpotent if there exists a positive integer n such that $a^n = 0$.

Defintion: (7.29) (Idempotent element)

An element a of a ring R is said to be idempotent if $a^2 = a$.

Example: (7.30)

The nilpotent elements in $\mathbb{Z}_8$ are 2, 4 since $\exists\ n = 3 \in \mathbb{N}$ such that $2^3 = 0 \Rightarrow 2^3 = 8 = 0$ and $\exists\ m = 2 \in \mathbb{N}$ such that $4^2 = 0$.

Example: (7.31)

3 and 4 are idempotent elements in $\mathbb{Z}_6$ since $3^2 = 3$ and $4^2 = 4$.

Question: (7.32) (H. W.)

Find all nilpotent and idempotent elements in Z_{12} and Z_{24}.

Theorem: (7.33)

If R is a ring with identity and R has no zero divisor, then the only idempotent element is either zero or 1.

Proof: Let a be an idempotent element, then $a^2 = a$.

Since $a.\ (a - 1) = a.\ (a + (-1))$

$= a.a + a.(-1)$

$= a^2 - (a.1)$ [**Th.** $a.(-1) = -(a.1)$]

$= a - a = 0$

So, $a.(a - 1) = 0$.

Since R has no zero divisor, then either $a = 0$ or $a = 1$.

<u>Defintion:</u> (7.34) (Boolean ring)

A ring R is said be a Boolean ring if every element of R is idempotent,

i.e., $a^2 = a, \forall a \in R$.

Example: (7.35)

$(\mathbb{Z}_2, +_2, ._2)$ is the standard example of Boolean ring.

<u>Theorem:</u> (7.36)

If R is a Boolean ring, then R is (1) a commutative ring of (2) characteristic 2.

Proof:

(1) Let $a \in R$. Then

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

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

$\Rightarrow a^2 + a^2 + a^2 + a^2 = a + a$

Since R is Boolean ring, then $a^2 = a$

$\Rightarrow a + a + a + a = a + a$

$\Rightarrow a + a = 0$ (by cancellation law)

$\Rightarrow 2a = 0$

$\therefore$ R is of characteristic 2.

(2) To prove that R is commutative.

Let $(R, +, .)$ be a Boolean ring, then $a^2 = a, \forall a \in R$.

$\forall a, b \in R$, $(a + b)^2 = a + b$

$\Rightarrow a^2 + 2(a.b) + b^2 = a + b$

Since R is Boolean, then $a + a.b + a.b + b = a + b$.

$\therefore a.b + a.b = 0$ ________(1) (by cancellation law)

Also,

$(a + b)^2 = a + b \Rightarrow (a + b)(a + b) = a + b.$

$\Rightarrow \ (a + b).a + (a + b).b = a + b$

$\Rightarrow \ a^2 + b.a + a.b + b^2 = a + b.$

Since R is Boolean, then

$a + b.a + a.b + b = a + b$

$\Rightarrow \ b.a + a.b = 0$ ______(2) (by cancellation law)

From (1) & (2) we get

$a.b + a.b = b.a + a.b$

$\Rightarrow \ a.b = b.a$ (by cancellation law)

$\therefore R$ is commutative.

Defintion: (7.37) (Centre of a ring)

Let (R, +, .) be a ring, then $C(R) = \{x \in R: \ x.y = y.x, \quad \forall y \in R\}$ is said to be centre of a ring.

Theorem: (7.38)

The centre of a ring is subring of R.

Proof:

$0 \in R \Rightarrow 0.x = x.0, \forall x \in R \Rightarrow C(R) \neq \emptyset.$

Let $a, b \in C(R)$.

We prove that $a - b \in C(R)$, i.e.,

we prove that

$(a - b).x = x.(a - b)$ ___(1)

Since $a \in C(R) \Rightarrow a.x = x.a, \forall x \in R$ and

$b \in C(R) \Rightarrow b.x = x.b, \forall x \in R$

L.H.S of (1) = $(a - b).x$

$= a.x - b.x \quad (Distributive\ law)$

$= x.a - x.b \quad (since\ a \in C(R)\ and\ b \in C(R).$

$= x.(a - b) \quad (Distributive\ law)$

$So, (a - b).x = x.(a - b).$

Also, we show that

$(a.b).x = x.(a.b)$

$Now,$

$(a.b).x =$

$a.(b.x) \ (Associative\ law)$

$= a.(x.b) \quad (b \in C(R)).$

$= (a.x).b \quad (Associative\ law)$

$= (x.a).b \quad (a \in C(R))$

$= x.(a.b) \quad (Associative\ law)$

∴ C(R) is a subring of R.

<u>Defintion:</u> (7.38) (Radical Ideal)

Let I be an ideal of a commutative ring R. Then the radical of I is defined by

$\sqrt{I}$ = {$a \in$ R: $a^n \in$ I, for some positive integer n}

<u>Question:</u> (7.39)

Show that $\sqrt{I}$ is an ideal of a commutative ring of R.

Solution: H.W.

<u>Theorem:</u> (7.40)

If I and J are ideals of a commutative ring of R, then

1) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
2) $\sqrt{I \cap J} \supseteq (\sqrt{I} + \sqrt{J})$ (Equality does not hold in general, give an example)

Proof:

(1) Let $a \in \sqrt{I \cap J}$ then $\exists\ n \in \mathbb{N}$ such that

$a^n \in I \cap J$ ⇒ $a^n \in$ I and $a^n \in$ J.

$\Rightarrow\ a \in \sqrt{I} \quad and \quad a \in \sqrt{J} \quad \Rightarrow\ a \in (\sqrt{I} \cap \sqrt{J})$

∴ $\sqrt{I \cap J} \subseteq (\sqrt{I} \cap \sqrt{J})$______(1)

Let $a \in (\sqrt{I} \cap \sqrt{J})$

$\Rightarrow\ a \in \sqrt{I} \quad and \quad a \in \sqrt{J}$

⇒ ∃ positive integers n , m such

that $a^n \in$ I and $a^m \in$ J.

⇒ $a^{n+m} = a^n a^m \in I \cap J$; let $k = n + m\ (positive\ integer)$, then $a^k \in I \cap J \Rightarrow\ a \in \sqrt{I \cap J}$

$(\sqrt{I} \cap \sqrt{J}) \subseteq \sqrt{I \cap J}$______(2)

From (1) & (2) we get

$(\sqrt{I} \cap \sqrt{J}) = \sqrt{I \cap J}.$

(2) H.W. (equality does not hold, give an example).

Question: (4.40′) (H.W.)

State and prove some other (five) properties for $\sqrt{I}$.