The Rings (1)

Third Class

By

Dr. Nuhad Salim

Definition:

A ring is an ordered triple $(R,+,\cdot)$, where R is a nonempty set and $+,\cdot$ are binary operation on R such that

1) $(R,+)$is an abelian group.

Mean:(a) $(a+b)+c=a+(b+c)$, $\forall a,b,c \in R.$

(b) $\exists\, 0 \in R$ such that $a+0=0+a=a.$

(c) $\forall a \in R\ \exists(-a) \in R$ such that $a+(-a)=(-a)+a=0$.

(d) $a+b=b+a \quad \forall a,b \in R.$

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

3) a $\cdot\ (b+c)=a\cdot b+a\cdot c$, and $(a+b).c=a\cdot c+b\cdot c \quad \forall a,b,c \in R.$

Example:(1) $(Z,+,\cdot)$

1) $(Z,+)$ is abelian group.
2) $(a.b).c=a.(b.c)$.
3) $a\cdot(b+c)=a\cdot c+a\cdot c$And $(a+b)\cdot c=a\cdot c+b\cdot c.$

$\therefore (Z,+,\cdot)$ Is a ring.

Example:(2)

$(Q,+,\cdot)$ is a ring.

Example:(3)

$(Z_n,+_n,\cdot_n)$ is a ring.

$Z_n=\{\bar{0},\bar{1},\bar{2},\cdots,\bar{n}\}$

$(Z_n,+_n)$ is abelian group.

Definition:

Let $(R,+,\cdot)$ be a ring, then R commutative if $a\cdot b=b\cdot a \quad \forall a,b\in R$.

Definition:

Let $(R,+,\cdot)$ be a ring, then R is said to have identity if there exists $1\in R$ such that $1\cdot a=a\cdot 1=a, \forall a\in R$ and a is invertible (unit) if there exists $b\in R$ such that $a\cdot b=b\cdot a=1$.

Examples:

(1) $(Z,+,\cdot)$ is a ring with identity, commutative, $1,-1$ are only invertible element.

(2) $(Q,+,\cdot)$ is a ring with identity commutative, and every element in Q has inverse except 0.

(3) $(3Z,+,\cdot)$ .is a commutative with no identity.

(4) $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix},+,\cdot\right)$ is a ring not comm. with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Example: $(p(X),\Delta,\cap)$ .is a ring?

1) $(p(X),\cap)$ .is an abelian group, commutative. $A\cap A=A$ (identity) no inverse.
2) $(A\cap B)\cap C=A\cap(B\cap C) \qquad \forall A,B,C\in X$
3) $\forall A,B,C\in X \quad A\cap(B\Delta C)=(A\cap B)\Delta(A\cap C)$?

$A\cap(B\Delta C)=A\cap[(B-C)\cup(C-B)]$

$$= A \cap (B - C) \cup A \cap (C - B))$$

$$= [(A \cap B) - (A \cap C)] \cup [(A \cap C) - (A \cap B)]$$

$$= (A \cap B)\Delta(A \cap C)$$

Remark:

Let R be a ring such that $R \neq \{0\}$ is a ring with identity 1, then $1 \neq 0$.

Proof: Suppose that $1 = 0$, let $a \neq 0 \in R$, $a = a \cdot 1 = a \cdot 0 = 0$ C!

$\therefore 1 \neq 0$.

Definition:

Let R be commutative ring. An element $a \in R$ is called *zero divisor* if $a \neq 0$ and there exists $b \in R$, $b \neq 0$ with $a \cdot b = 0$.

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

Solution: $\bar{2}.\bar{3} = \bar{0}$, $\bar{3}.\bar{4} = \bar{0}$ $\bar{2}, \bar{3}, \bar{4}$ are zero divisors of Z_6

Example: $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ has no zero divisor.

Example: $(Z, +, \cdot), (\boldsymbol{C}, +, \cdot), (\boldsymbol{R}, +, \cdot), (Q, +, \cdot)$ has no zero divisor.

H.W: $(p(x), \Delta, \cap)$ has zero divisor or not?

Lemma: Let R be a ring, then

(1) $a \cdot 0 = 0 \cdot a = 0$.

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

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

(4) $a(b-c) = ab - ac \quad \forall a, b, c \in R$.

Proof(1): $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0$

Proof(2): $0 = 0 \cdot b = \big(a + (-a)\big)b = ab + (-a)b \Rightarrow (-a)b = -(ab)$

Proof(3): $(-a)(-b) = -\big(a \cdot (-b)\big) = -\big(-(a \cdot b)\big) = a \cdot b$

Proof(4): $a \cdot (b - c) = a \cdot [b + (-c)]$

$$= a.b + a \cdot (-c) \quad = a \cdot b - a \cdot c.$$

Definition:

A commutative ring with identity is called *integral domain* if it has no zero divisors.

Example:

$(Z,+,\cdot), (Q,+,\cdot), (\boldsymbol{R},+,\cdot), \big(Z_p, +_p, \cdot_p\big)$ where p is prime are integral domains.

Lemma:

Let R be commutative ring with identity, R is integral domain if and only if $a \cdot b = a \cdot c$; $a \neq o$, then $b = c$, $b.a = c.a$; $a \neq o$, then $b = c$

Proof: $\Rightarrow$) suppose $a \cdot b = a \cdot c$; $a \neq 0$

$(a \cdot b) - (a \cdot c) = 0$ [associative]

$a \cdot (b - c) = 0$ [R is integral domain]

$\because$ R has no zero divisor and $a \neq 0$

$\therefore$ $b - c = 0 \Rightarrow b = c$.

$\Leftarrow$) Let $a \in R$, $a \neq 0$

$a \cdot b = 0$, and we have $0 \cdot a = a \cdot 0 = 0$, $a \cdot b = a \cdot 0$

$\therefore$ $b = 0$.

Definition:

Let $(R, +, \cdot)$ be a ring, and $\emptyset = S \subseteq R$, then $(S, +, \cdot)$ is called ***subring*** if $(S, +, \cdot)$ is a ring itself.

Example:

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

Definition:

Let $(R, +, \cdot)$ be a ring $\emptyset \neq S \subseteq R$, then $(S, +, \cdot)$ is subring if:

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

(2) $a.b \in S \quad \forall a, b \in S$.

Example:

Z is a subring of $(Q, +, .)$.

Q is a subring of $(R,+,.)$.

R is a subring of $(C,+,.)$.

$(\{\bar{0},\bar{2},\bar{4}\},+,\cdot)$is a subring of Z_6

$(\{\bar{0},\bar{3}\},+,\cdot)$ is a subring of Z_6.

Example:

Let $(R,+,.)$ be a ring $R\times R=\{(a,b): a,b\in R)\}$

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

$$(a,b).(c,d)=(ac,bd)$$

Proof: (1) $(R\times R,+)$ is abelian group

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

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

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

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

(3)Identity $=(1,1)$; $(a,b)\cdot(1,1)=(a\cdot 1,\ b\cdot 1)=(a,b)$

$\therefore$ $(R\times R,+,.)$is a ring with identity .

(4) $S=R\times\{e\}=\{(a,0): a\in R\}$. S is a subring of $R\times R$.

Proof: $S\neq\varnothing$ since $(0,0)\in S$

$$(a,0)-(b,0)=(a-b,0)\in S$$

$$(a,0).(b,0)=(a.b,0)\in S$$

Identity $=(1,0)$

Definition:

Let R be a ring the center of a ring R is denoted by $Cent\, R$ is the set $Cent\, R = \{x \in R : x \cdot r = r \cdot x \quad \forall r \in R\}$.

Lemma:

$Cent\, R$ is a subring of R.

Proof: $Cent\, R \neq \emptyset$ $[0 \in Cent\, R,\ 0.a = a.0 = 0]$, let $a, b \in Cent\, R$

$\Rightarrow a \cdot x = x \cdot a \quad , b \cdot x = x \cdot b \quad \forall x \in R$

$x \cdot (a - b) = x \cdot a - x \cdot b = a \cdot x - b \cdot x = (a - b) \cdot x$ [Since $a, b \in Cent\, R$]

$$x \cdot (a \cdot b) = x \cdot ab = ax.b = a.bx$$

$\therefore Cent\, R$ is subring.

Remark:

(1) Let R be a ring, n positive integer,

$$na = \underbrace{a + a + \cdots + a}_{n\ times}, \quad a^n = \underbrace{a.a \ldots a}_{n\ times}$$

(2) If R is a ring with 1 and a is invertible

$$a^{-n} = \underbrace{a^{-1}.a^{-1} \ldots a^{-1}}_{n\ times}\ a^0 = 1.$$

Remark:

Let R be a ring and $n, m \in Z$

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

(2) $n(a - b) = na - nb$.

(3) $(nm)a = n(ma) = m(na)$.

Proof :(1): $(n+m)a = \underbrace{a+a+\cdots+a}_{(n+m)\ times} = \underbrace{a+a+\cdots+a}_{n\ times} + \underbrace{a+a+\cdots+a}_{m\ times}$

$$= na + ma$$

Proof: (2): $n(a-b) = \underbrace{(a-b)+(a-b)+\cdots+(a-b)}_{n\ times}$

$$= \underbrace{a+a+\cdots+a}_{n\ times} - \underbrace{b-b-\cdots-b}_{n\ times}$$

$$= na - nb$$

Definition:

Let $(R,+,\cdot)$ be a ring, if there exists a positive integer n such that $na = 0$, $\forall a \in R$, then the smallest positive integer with this property is called the *characteristic* of R. If no such positive integer exists we say R has characteristic zero, we denote the characteristic of R by $Char\ R$.

Example:

$Char\ Z = 0$, $Char\ Q = 0$, $Char\ Z_6 = 6$, $Char\ Z_4 = 4$, $Char\ Z_n = n$.

$$(p(x), \Delta, \cap)\ , Char\ p(x) = 2$$

$$2A = A\ \Delta\ A = (A - A) \cup (A - A) = \emptyset$$

Theorem: **(1)**

Let R be a ring with identity, then $Char\ R = n > 0$ if and only if n is the smallest positive integer such that $n.1 = 0$.

Proof: $\Rightarrow$) $Char\ R = n > 0$, then $n.a = 0$, then $n.1 = 0$ suppose $\exists$ positive integer m such that $m < n$, $m.1 = 0$ and let $a \in R$

$$m\,a = \underbrace{a + a + \cdots + a}_{\text{m times}} = \underbrace{a.1 + a.1 + \cdots + a.1}_{\text{m times}} = m(1.a)$$

$=(m.1).a = 0.a = 0$ C!

Since n is Char R.

$\Leftarrow$) Let $a \in R$, $na = n.(1.a) = (n.1).a = 0.a = 0$

$\therefore Char\ R = n$ since n is the smallest positive integer; $n.1 = 0$.

Corollary:

Let R be an integral domain, then $Char\ R$ is either zero or prime integer.

Proof: Suppose $Char\ R > 0$, suppose $n = n_1.n_2$, $1 < n_1 \leq n_2 < n$.

$0 = n.1 = (n_1 \cdot n_2) \cdot 1$

$(n_1.n_2).1 = (n_1.1).(n_2.1)$ [R integral domain]

But R is integral domain, then either $n_1.1 = 0$ or $n_2.1 = 0$ C! by theorem(1) since $n_1, n_2 < n$ and n is the smallest integer such that $n.1 = 0$.

$\therefore$ n is a prime integer.

Definition:

Let R and R' be rings $f: R \to R'$, then f is a ring homomorphism if

(1) $f(a + b) = f(a) + f(b)$.

(2) $f(a.b) = f(a).f(b)$.

Example:

(1)Let $\emptyset: R \longrightarrow R'$; $\emptyset(r)=0$ $\forall r \in R$ is a ring homomorphism is called zero homo.

(2) $I : R \longrightarrow R$; $I(r)=r$ $\forall r \in R$ the identity homomorphism.

(3) $h : Z \longrightarrow Z_n$; $h(n) = \bar{n}$ $\forall n \in Z$.

Definition:

Let $f : R \longrightarrow R'$ be a ring homomorphism.

1) If f is one to one, then f is monomorphism.

2) If f is onto, then f is epimorphism.

3) If f is $(1-1)$ and onto, then f is isomorphism.

Definition:

If $f : R \longrightarrow R'$ and f is isomorphism, then we say that R is isomorphic to R', $R \simeq R'$.

Remark:

If $f : R \longrightarrow R'$ is homomorphism, then:

1) $f(0_R) = 0_{R'}$.

2) $f(-a) = -f(a)$ $\forall a \in R$.

3) $f(1_R) = 1_{R'}$ when R and R' are rings with identity.

Theorem:

Any ring can be *imbedded* in a ring with identity.

Proof: Let $R \times Z = \{(r,n): r \in R , n \in Z\}$

Define $+$ and $.$ on $R \times Z$ as follows

$$(r,n)+(t,m)=(r+t,n+m).$$

$$(r,n).(t,m)=(rt+nt+mr,nm).$$

Then $R\times Z$ is a ring with identity $(0,1)$.

$$(r,n).(0,1)=(r,n).$$

$$R\times\{0\}\subseteq R\times Z.$$

Now we must show that $R\times\{0\}$ is subring of $R\times Z$

$$(a,0)\{\in R\times\{0\}\}-(b,0)\{\in R\times\{0\}f=(a-b,0)\in R\times\{0\}$$

$$(a,0).(b,0)=(ab,0)\in R\times\{0\}$$

Now we define a map $\emptyset: R\to R\times\{0\}$; $\emptyset(r)=(r,0)\quad\forall r\in R$

(1) Let $\emptyset(r_1)=\emptyset(r_2)$

$$(r_1,0)=(r_2,0)\Rightarrow r_1=r_2$$

$\therefore\emptyset$ is $(1-1)$

(2) Let $(w,0)\in R\times\{0\}$.

$\emptyset(w)=(w,0)$.

$\therefore\emptyset$ is onto, $\emptyset$ is homo.

(3) $\emptyset(r_1+r_2)=(r_1+r_2,0)=(r_1,0)+(r_2,0)=\emptyset(r_1)+\emptyset(r_2)$.

$$\emptyset(r_1.r_2)=(r_1r_2,0).$$

$$\emptyset(r_1).\emptyset(r_2)=(r_1,0).(r_2,0)=(r_1r_2,0).$$

$\therefore\emptyset$ is homomorphism.

$\therefore R\simeq R\times\{0\}$.

$\therefore R$ is imbedded in a ring $R\times Z$.

Definition:

Let R be a ring an element $a \in R$ is said to be *idempotent* element if $a^2 = a$.

Definition:

An element $a \in R$ is called *nilpotent* if there exists an integer n such that $a^n = 0$.

Examples:

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

Solution: $\bar{0}, \bar{1}, \bar{3}, \bar{4}$ are idempotent. $\bar{0}$ is nilpotent only.

(2) $Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

Solution: $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ are nilpotent elements.

(3) Z_5: the idempotent element are $\bar{0}, \bar{1}$ and nilpotent is $\bar{0}$.

(4) $(p(x), \Delta, \cap)$

Solution: $A \cap A = A$, $\forall A$ is idempotent $A \cap \ldots \cap A = \emptyset$, just when $A = \emptyset$.

Definition:

Let R be a ring such that every element of R is idempotent, then R is ***Boolean ring***.

Example :

In $Z_2 = \{0, 1\}$, $(\bar{0})^2 = 0$, $(\bar{1})^2 = 1$.

$\therefore$ Z_2 is Boolean ring.

Theorem:

Let R be a ring such that every element in R is idempotent (R is Boolean ring), then R is commutative.

Proof: $(a + b) = (a + b)^2 = (a + b)\,(a + b) = a.a + a.b + b.a + b.b$

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

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

$$0 = ab + ba \Rightarrow ab = -ba$$

$$ab = (-ba) = (-ba)^2 = b^2 a^2 = ba$$

$\therefore R$ is commutative.

Remark:

Let R be a ring if there exists an element $a \in R$, such that:

(1) a is idempotent.

(2) a is not zero divisor. Then a must be the identity of the ring.

Proof: (2) Let $b \in R$

$$a.b = a^2 b \quad \Rightarrow \quad (a^2.b) - a.b = 0.$$

$a(ab - b) = 0$ [a is not zero divisor]

$\therefore\ ab - b = 0 \quad \Rightarrow \quad ab = b$.

$\therefore\ a$ is identity.

Example:

Consider the ring $(p(x), \Delta, \cap)$; $p(x) = \{A : A \subseteq X\}$, for a fixed subset $S \subseteq X$, $S \in p(x)$, define $f : p(x) \longrightarrow p(x)$ by

$f(A) = A \cap S.$

(1) $A = B \Rightarrow A \cap S = B \cap S$.

$f(A) = f(B)$

$\therefore f$ is well defined.

(2) $f(A \varDelta B) = f(A) \varDelta f(B)$?

$f(A \varDelta B) = (A \varDelta B) \cap S$

$= [(A - B) \cup (B - A)] \cap S$

$= [(A - B) \cap S] \cup [(B - A) \cup S]$

$= (A \cap S - B \cap S) \cup (B \cap S - A \cap S)$

$= (A \cap S) \varDelta (B \ S) = f(A) \varDelta f(B)$

(2) $f(A \cap B) = (A \cap B) \cap S = (A \cap S) \cap (B \cap S) = f(A) \cap f(B)$

$\therefore f$ is homomorphism.

(3) $ker\ f = \{A \subseteq p(x) : f(A) = \emptyset\} = \{A \subseteq p(x) : A \cap S = \emptyset\} = S^c \neq$ identity.

(4) $\forall A \subseteq X \Rightarrow X \cap A = A$, identity $= X$

$\therefore f$ is not $(1 - 1)$.

Problems:

1) Let R be a ring and $a \in R$, If $C(a)$ the set of all elemente with a , $C(a) = \{ r \in R : ra = ar \}$ show that $C(a)$ is subring of R. and $Cent\ R = \cap_{a \in R} C(a)$.

2) Let $(G,+)$ be abelian group, R set of all groups homomorphism of G in to itself $(f + g)(x) = f(x) + g(x), f \circ g(x) = f\big(g(x)\big)$, show that $(R,+,\circ)$form a ring, determine the invertible elements of R.

3) Given that f is homomorphism. from the ring R in to the ring R',prove that

A. $f(Cent\,(R)) \subseteq Cent\,(f(R))$

B. If $a \in R$ is nilpotent, then $f(a)$ is nilpotent in R'**.**

C. If R has positive characteristic,then $Char\, f(R) \leq Char\, R$.

4) Let R be a ring without zero divisors:

i. $a.b = 1$ iff $b.a = 1$

ii. If $a^2 = 1$ then either $a = 1$ or $a = -1$.

Sol(***i*** **):**

If $a.b = 1$, then $b \neq 0$

[If $b = 0 \Longrightarrow a.0 = 0 \neq 1$]

$\therefore a.b = 1 \Longrightarrow b.a.b = b$

$b.a.b - b = 0 \Longrightarrow (ba - 1)b = 0 \quad ,b \neq 0$

$\therefore ba = 1$

Sol (***i i*** **):**

$a^2 = 1 \;,\; a.a = 1 - a + a$

$a.a + a - a - 1 = 0$

$a.(a + 1) - (a + 1) = 0$

$(a + 1).(a - 1) = 0$

Either $a = 1$ or $a = -1$.

Definition:

Let I be a nonempty subset of ring R, then I is ***ideal*** of R if

(1) $a - b \in I \ \forall a, b \in I$.

(2) $ar \in I$, $(ra \in I)$ $\forall a \in I , r \in R$.

(3) $I \neq \emptyset$.

Remark:

Every ideal is subring.

Proof: Let I be an ideal, to show that I is subring

(1) $I \neq \emptyset$.

(2)Let $a, b \in I \Rightarrow a.b \in I$, $a - b \in I$

$\therefore I$ is subring

But the converse is not true for example:

$(Q, +, .)$ is a ring, $Z \subseteq Q$; Z is subring

$3 \in Z$, $\frac{1}{2} \in Q$, $3.\frac{1}{2} = \frac{3}{2} \notin Z$.

$\therefore Z$ is not ideal

Example: In the ring Z

(1) $2Z$ is subring and ideal.

(2) $5Z$, $3Z$ are ideals.

In general nZ is an ideal $\forall n$.

Remark(1):

Let I be an ideal of a ring with 1. If $1 \in I$, then $I = R$.

Proof: $I \subseteq R$, let $r \in R$, $1 \in I$ but I is ideal

$\therefore 1.r \in I \Rightarrow r \in I \Rightarrow R \subseteq I$.

Thus $I = R$

Remark(2):

Let I be an ideal of a ring with 1 and I contains an invertible element, then $I = R$.

Proof: $a \in I$ but a is invertible then $\exists\ b \in R$ such that $a.b \in I \Rightarrow 1 \in I$

$\therefore I = R$, by remark (1).

Definition: An ideal I of a ring R is called a proper ideal if $I \neq R$ and I is called nontrivial ideal if $I \neq \{0\}$ and $I \neq R$.

Theorem: Let $\{I_\alpha : \alpha \in \Lambda\}$ be a family of ideals of a ring R, then $\bigcap_{\alpha\in\Lambda} I_\alpha$ is an ideal in R.

Proof: $\bigcap_{\alpha\in\Lambda} I_\alpha \neq \emptyset$ $[0 \in I_\alpha \ \forall \alpha \in \Lambda]$

Let $a, b \in \bigcap_{\alpha\in\Lambda} I_\alpha \Rightarrow a \in I_\alpha \ \forall \alpha\in\Lambda$ and $b \in I_\alpha \ \forall \alpha \in \Lambda$

$\therefore a - b \in I_\alpha \ \forall \alpha \in \Lambda$ [ideal def.] $\therefore a - b \in \bigcap_{\alpha\in\Lambda} I_\alpha$

Let $a \in \bigcap_{\alpha\in\Lambda} I_\alpha$, $r \in R$

$\therefore a \in I_\alpha \quad \forall \alpha \in \Lambda \quad \Rightarrow \quad ra \in I_\alpha \quad \forall \alpha$

$ra \in \bigcap_{\alpha \in \Lambda} I_\alpha$

$\therefore \bigcap_{\alpha \in \Lambda} I_\alpha$ is ideal.

But the union is not ideal for example:

$2Z$ is ideal, $3Z$ is ideal, $2 \in 2Z$, $3 \in 3Z$

If $2Z \cup 3Z$ is ideal

$\therefore \quad 2,3 \in 2Z \cup 3Z \therefore 3-2 \in 2Z \cup 3Z \; C! \quad 1 \notin 2Z \cup 3Z$

$\therefore \quad 2Z \cup 3Z$ is not ideal.

Definition:

Let S be a nonempty subset of a ring R the set $< S >$, where:

$$< S > = \cap \{I : I \text{ is an ideal of } R \text{ containing } S\}$$

is called the ideal generated by S.

Remark:

1. $< S >$is smallest ideal containing S.
2. $< S > = S$ if and only if S is an ideal.
3. If $S = \{a\}$, $< S > = < a >$ is called principle ideal.

Remark:

If R is commutative ring with identity and $x \in R$, then

$$< x > = \{rx : r \in R\} = Rx$$

For example:$< 2 > = 2Z$, $< 3 > = 3Z$

Definition:

A ring R is called principle ideal ring if every ideal in R is principle ideal.

Theorem:

$(Z,+,.)$ is P. I. R.

Proof: Suppose I be an ideal in Z if $I = \{0\}$, then $I =< 0 >$ if $I \neq \{0\}$, then $\exists$ an integer $0 \neq m \in I$, if it is negative then $-m \in I$, then I contains a positive integer, let n be the least positive integer such that $n \in I$, we claim that $I =< n >$.

It's clear that $< n > \subseteq I$ since $n \in I$.

Now, let $m \in I$ by division algorithm theorem $\exists\ q, r \in Z$, such that:

$$m = nq + r \quad , \quad 0 \leq r < n \quad , \qquad r = m(\in I) - nq(\in I)$$

$\therefore r \in I$ C! since n is the least positive integer $n \in I$ and $r < n$.

$\therefore r = 0 \Rightarrow m = nq$

$\therefore m \in < n >$

$\therefore I =< n >$

The union is not ideal for example:

$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\},\ I_1 = \{\bar{0}, \bar{2}, \bar{4}\},\ I_2 = \{\bar{0}, \bar{3}\}$

$\cup I_i = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$

$3 - 2 = 1 \notin \cup I_i,\ i = 1, 2$.

Definition:

Let I and J be ideals of a ring R, then the sum of I and J denoted by:

$$I + J = \{a + b : a \in I , b \in J\}.$$

Remark:

If I and J ideals in R then $I + J$ is also ideal in R.

Proof: $I + J \neq \emptyset$ $[0 \in I , 0 \in J \therefore 0 \in I + J]$

Let $w_1, w_2 \in I + J \Rightarrow w_1 = a_1 + b_1 , a_1 \in I , b_1 \in J, w_2 = a_2 + b_2 , a_2 \in I, b_2 \in J$

$$w_1 - w_2 = a_1 + b_1 - a_2 - b_2 = (a_1 - a_2)(\in I) + (b_1 - b_2)(\in J)$$

$\therefore w_1 - w_2 \in I + J.$

Let $w \in I + J , r \in R , w = a + b ; a \in I , b \in J$

$$rw = r(a + b) = ra(\in I) + rb(\in J) \in I + J$$

$\therefore I - J$ is an ideal.

Example: $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} , I = \{\bar{0}, \bar{3}\} , J = \{\bar{0}, \bar{2}, \bar{4}\}$

$I + J = \{\bar{0}, \bar{2}, \bar{4}, \bar{3}, \bar{5}, \bar{1}\} = Z_6$

$I + J$ is an ideal

Example:

In $(Z, +, .)$

$2Z + 3Z =$ ideal.

Definition:

Let I and J be ideals in a ring R we say that R is internal direct sum of I and J if:

(1) $R = I + J$

(2) $I \cap J = \{\emptyset\}$

We denote that by: $R = I \oplus J$.

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

$I = \{\bar{0}, \bar{3}\}$, $J = \{\bar{0}, \bar{2}, \bar{4}\}$

$\therefore\ Z_6 = I \oplus J \quad or \quad Z_6 = Z_6 \oplus \{0\}$

Theorem:

Let I and J be ideal in R, then $R = I \oplus J$ if and only if every element in R can be written in only one way.

Proof: $\Rightarrow$) Let $R = I \oplus J \quad \Rightarrow \quad R = I + J\ ,\ I \cap J = \{0\}$ let $r \in R$

$\therefore \exists\ a \in I\ ,\ b \in J$ such that $r = a + b$ if not $r = a1 + b1\ ,\ a1 \in I\ ,\ b1 \in J$

$$a_1 + b_1 = a + b \ \Rightarrow a_1 - a = b - b_1 \in I \cap J = \{0\}$$

$\therefore a_1 - a = 0 \ \Rightarrow\ a = a_1\ ,\ b - b_1 = 0 \ \Rightarrow\ b = b_1$

$\Leftarrow$) $I + J \subseteq R\ ,\ let\ w \in R\ ,\ w = w + 0 \in I + J$

$\therefore R \subseteq I + J \quad \therefore\ R = I + J$

Let $w \in I \cap J \ \Rightarrow\ w \in I$ and $w \in J,\ w = w + 0 = 0 + w\ C!$

$\therefore w = 0$

Definition:

Let R_1, R_2 be rings consider the set $R_1 \times R_2 = \{(x,y): x \in R_1,\ y \in R_2\}$, define $+, \cdot$ on $R_1 \times R_2$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2)$$

$$(x_1, y_1).(x_2, y_2) = (x_1.x_2\ ,\ y_1.y_2)$$

Then we can show that $R_1 \times R_2$ is a ring? Is called the external direct sum of R_1 and R_2

$$R_1 \simeq R_1 \times \{0\} \quad , \quad R_2 \simeq \{0\} \times R_2$$

Theorem:

Let $f : R \longrightarrow R'$ be ring homomorphism.

(1) If K is an ideal in R', then $f^{-1}(K)$ is an ideal in R.

(2) If J is an ideal in R and f is onto then $f(J)$ is ideal in R'

Proof: $f^{-1}(K) = \{r \in R: f(r) \in K\} \neq \emptyset$ since $[0 \in f^{-1}(K), f(0) = \bar{0} \in K]$

Let $x, y \in f^{-1}(K) \Rightarrow f(x) \in K\ ,\ f(y) \in K$

K is ideal $\Rightarrow f(x) - f(y) \in K$, f is ring homomorphism $\Rightarrow f(x-y) \in K$

$\therefore\ x - y \in f^{-1}(K)$

Let $w \in f^{-1}(K)$, $r \in R$, $f(w) \in K$, $f(r) \in R'$ and K is ideal

$\therefore f(w).f(r) \in K$ [f isring homomorphism] $f(w.r) \in K \Rightarrow w.r \in f^{-1}(K)$

$\therefore f^{-1}(K)$ is ideal.

(2) $f(J) \neq \emptyset$ since [$0_{R'} = f(0_R)$ $\therefore 0_{R'} \in f(J)$]

Let $x, y \in f(J) \Rightarrow x = f(w_1)$, $w_1 \in J$, $y = f(w_2)$, $w_2 \in J$

$w_1 - w_2 \in J$ [Since J is an ideal], $f(w_1 - w_2) \in f(J)$ [f is homomorphism]

$$f(w_1) - f(w_2) \in f(J) \ , \qquad x - y \in f(J)$$

Let $a \in f(J)$, $r' \in R'$, $a = f(w)$, $w \in J$

$r' \in R'$ since f is onto then $\exists\, r \in R$ such that $f(r) = r'$

$\therefore\ rw \in J$ [$J$is ideal]

$f(rw) \in f(J), f(r)f(w) \in f(J)$ [f is homomorphism], $r'a \in f(J)$

$\therefore\ f(J)$ is an ideal.

Corollary:

Let $f: R \rightarrow R'$be a ring homomorphism, then $ker f$ is ideal in R.

Proof: $\ker f = \{r \in R : f(r) = 0\} = f^{-1}(O_{\acute{R}}), O_{\acute{R}}$ is ideal by theorem $f^{-1}(O_{\acute{R}})$is ideal

$\therefore\ ker\, f$ is ideal.

The quotient ring, let I be an ideal in a ring R , $\frac{R}{I} = \{x + I : x \in R\}$. Define +, · as:

$$(x + I) + (y + I) = (x + y) + I \in \frac{R}{I}$$

$$(x + I).(y + I) = (x.y) + I \in \frac{R}{I}$$

To show that +,· is well define (1) is well defined, by (1)

$$x + I = x_1 + I \ \Leftrightarrow\ x - x_1 \in I$$

$$y + I = y_1 + I \ \Leftrightarrow\ y - y_1 \in I$$

$$(x + I).(y + I) = (x_1 + I).(y_1 + I)$$

$$xy + I = x_1 y_1 + I \ \Leftrightarrow\ xy - x_1 y_1 \in I$$

$$xy - x_1y_1 = xy - xy_1 + xy_1 - x_1y_1$$

$= x(y - y_1) + (x - x_1)y_1 \in I$ (I is ideal)

Then $xy - x_1y_1 \in I \Rightarrow$ is well defined.

Theorem:

Let I be an ideal of a ring R, then $\left(\frac{R}{I}, +, \cdot\right)$ is a ring which is called the quotient ring of R by I.

Proof: (1) well defined

$$a + I = a_1 + I \Leftrightarrow a - a_1 \in I, \qquad b + I = b_1 + I \Leftrightarrow b - b_1 \in I$$

$$(a + I) + (b + I) =? (a_1 + I) + (b_1 + I)$$

$$(a + b) + I = (a_1 + b_1) + I \Leftrightarrow a + b - (a_1 + b_1) \in I$$

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

$\therefore +$ is well define· is well define.

(2) Associative

$$r + I + [(r_1 + I) + (r_2 + I)] =? [(r + I) + (r_1 + I)] + (r_2 + I)$$

$$(r + I) + (r_1 + r_2 + I) = (r + r_1 + I) + (r_2 + I)$$

$$\therefore (r + r_1 + r_2) + I = (r + r_1 + r_2) + I$$

(3)The identity

$$(r + I) + (0 + I) = (r + 0) + I = r + I$$

$\therefore 0 + I = I$ is the identity.

(4) $(r + I) + [(-r) + I] = (r - r) + I = 0 + I = I$

$\therefore (-r) + I$ is the inverse

(5) $(r + I) + (r_1 + I) = (r_1 + I) + (r + I)$

$$(r + r_1) + I = (r_1 + r) + I$$

$(r + r_1) + I = (r + r_1) + I$, since $r + r_1 \in R$ and R is a ring $r + r_1 = r_1 + r$ [abelian group]

$\therefore$ $(R/I, +)$is abelian group.

(6) $[(a + I).(b + I))].(c + I) = (a.b + I).(c + I) = a.b.c + I$

$$(a + I).[(b + I).(c + I)] = (a + I).(b.c + I) = a.b.c + I$$

(7)$(a + I).[(b + I) + (c + I)] = (a + I)(b + c + I)$

$$= a.(b + c) + I$$

$$= a.b + a.c + I$$

$$= (ab + I) + (a.c + I)$$

$$= (a + I)(b + I) + (a + I)(c + I).$$

$\therefore \cdot$ Is associative $\therefore$ $\left(\frac{R}{I}, +, \cdot\right)$ is a ring.

Note: If R with identity 1, then $\frac{R}{I}$ with identity $1 + I$.

Example: Let Z be a ring,

(1) $\frac{Z}{3Z} = \{3Z, 1 + 3Z, 2 + 3Z, \cdots\}$.

(2) $\frac{Z}{4Z} = \{4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z, \cdots\}$.

(3) $\frac{Z}{2Z}=\{2Z\ ,\ 1\ +\ 2Z\ ,\cdots\}$.

Remark:

Let I be an ideal of R, the function $\pi : R \longrightarrow R/I$ defined by $\pi(r) = r + I$, for all $r \in R$, is a ring epimorphism , it is called the natural epemorphism.

$\pi\ (r_1 + r_2) =?\ \pi\ (r_1) + \pi\ (r_2)$

$(r_1 + r_2) + \mathrm{I} = (r_1 + I) + (r_2 + \mathrm{I})$

$\pi\ (r_1 . r_2) =?\ \pi\ (r_1) . \pi\ (r_2)$

$(r_1 . r_2) . I = (r_1 + I) . (r_2 + I)$.

Remark: (Fundamental Homomorphism Theorem of rings)

Let $f : R \longrightarrow R'$ be a ring homomorphism, which is onto, then $R/ker\, f \simeq R'$.

Proof: Define $g: \frac{R}{ker\, f} \longrightarrow R'$ by $g(r + K) = f(r)$ where $ker\, f = K$

(1) $r + K = r_1 + K \Leftrightarrow r - r_1 \in K$

$\Rightarrow f(r - r_1) = 0\ ,\ f(r) - f(r_1) = 0 \Rightarrow f(r) = f(r_1)$

$\therefore\ g(r + K) = g(r_1 + K)$

$\therefore$ Well defined

(2) g is homomorphism

$g\big((r + K) + (r_1 + K)\big) = g(r + K) + g(r_1 + K)$

$g(r + r_1 + K) = f(r) + f(r_1)$

$\therefore f(r + r_1) = f(r + r_1)(since\ f\ is\ homo.)$

$g\big((r+K)\cdot(r_1+K)\big) =?\ g(r+K)\cdot g(r_1+K)$

$\therefore g$ is homo.

(3) $g(r+K)=g(r_1+K) \Rightarrow f(r)=f(r_1) \Rightarrow f(r)=f(r_1)=0$ [Since f is homomorphism]

$f(r-r_1)=0 \Rightarrow r-r_1 \in ker\ f = K \Leftrightarrow r+K = r_1+K \Rightarrow g\ is\ (1-1)$

(4) Let $w \in R'$ since f is onto $\exists x \in R$, such that $f(x)=w$

$g(x+K)=f(x)=w \Rightarrow g$ is onto.

Example: Show that $\frac{Z}{nZ} \simeq Z_n$

Solution: $f : Z \longrightarrow Z_n$, $f(x) = \bar{x}$ $\forall x \in Z$

$$f(x+y) = \overline{x+y} = \bar{x} + \bar{y} = f(x) + f(y)$$

$$f(xy) = \overline{xy} = \bar{x}.\bar{y} = f(x).f(y)$$

$\therefore f$ is homo.

Let $\bar{w} \in Z_n \Rightarrow \exists\ w \in Z$ such that $f(w)=\bar{w}$

$\therefore f$ is onto

by F. H. Th. $\frac{Z}{\ker f} \simeq Z_n$

$$ker\ f = \{x \in Z : f(x) = \bar{0}\} = \{x \in Z : \bar{x} = \bar{0}\} = nZ$$

$\therefore \frac{Z}{nZ} \simeq Z_n$.

Remark:

The only nontrivial homomorphism from Z to Z is the identity.

Proof: $f : Z \longrightarrow Z$; $0 \neq n \in Z$,

$$f(n) = f\underbrace{(1+1+\cdots+1)}_{n\ times} = \underbrace{f(1)+f(1)+\cdots+f(1)}_{n\ times}$$

[Since f is homomorphism]

$f(n) = nf(1)$ ....(*)

$f(n) = f(n.1)$

$f(n).1 = f(n).f(1) \Rightarrow f(1) = 1$ [by(*)]

$\therefore\ f(n) = n$

$\therefore f$ is identity.

Corollary (1):

Let R be a ring and suppose that f, g a ring isomorphism, then

$f = g : R \longrightarrow Z.$

Proof: $f : R \longrightarrow Z$, $g: R \to Z$; $R \simeq Z$

$g^{-1}: Z \longrightarrow R$ is a ring isomorphism

$f \circ g^{-1} : Z \longrightarrow Z$, $\left(Z \xrightarrow{g^{-1}} R \xrightarrow{f} Z\right) \Rightarrow f \circ g^{-1} : Z \longrightarrow Z$

$\therefore\ f \circ g^{-1} = I$ [by Remark]

$\therefore g = f$

Corollary (2):

Let R be a ring and $f, g: R \to Z$ be an epimorphism, then if

$ker\ f = ker\ g$, then $f = g$.

Proof: by $F.H.Th.$ $R/ker\,f \simeq Z$ and $\frac{R}{ker\,g} \simeq Z$, by coro.(1) $f^* = g^*$;

$f^*: R/ker\,f \rightarrow Z$ and $g^*: R/ker\,g \rightarrow Z$. To prove that $f = g$

Let $r \in R$, $f(r) = f^*(r + ker\,f) = g^*(r + Ker g) = g(r)$;

$\therefore f = g$.

Theorem:

$Z_n \oplus Z_m \simeq Z_{nm}$ if and only if $g.c.d(n,m) = 1$.

Proof: We only have to show that $\frac{Z}{nZ} \oplus \frac{Z}{mZ} \simeq \frac{Z}{nmZ}$ since by F. H. Th. $\frac{Z}{nZ} \simeq Zn$ and $Z_{nm} \simeq \frac{Z}{nmZ}$

Define $\emptyset: Z \longrightarrow \frac{Z}{nZ} \oplus \frac{Z}{mZ}$

By $\emptyset(x) = (x + nZ\,,\ x + mZ)$ $\forall x \in Z$

$\emptyset$ is a ring homomorphism?

$\ker \emptyset = \{x \in Z : \emptyset(x) = (nZ\,, mZ)\}$

$= \{x \in Z : (x + nZ\,, x + mZ) = (nZ, mZ)\}$

$= \{x \in Z : (x \in nZ, x \in mZ)\} = \{x \in Z : x \in nZ \cap mZ\} = nmZ$

since $g.c.d(n,m) = 1$

$\emptyset$ is onto: Let $(a + nZ\,,\ b + mZ) \in \frac{Z}{nZ} \oplus \frac{Z}{mZ}$

$g.c.d(n,m) = 1 \Rightarrow \exists\, s,t \in Z$

$\Rightarrow sn + tm = 1$ ....(**) ,since $sn - 1 \in mZ$ and $tm - 1 \in nZ$

Let $x = a\,tm + bsn$ ....(*)

$$\emptyset(x) = (x + nZ\,,\ x + mZ)$$

$= (atm + nZ, bsn + mZ)$

$= (a + nZ, b + mZ)$

$a + nZ = atm + nZ \Leftrightarrow a - atm \in nZ \Leftrightarrow a(1 - tm) \in nZ \Leftrightarrow a \in nZ$

Similarly $bsn + mZ = b + mZ \Leftrightarrow (b - bsn) \in mZ \Leftrightarrow b(1 - sn) \in mZ \Leftrightarrow btm \in mZ$

$\therefore \emptyset$ is onto.

Definition:

A proper ideal M of a ring R is called *maximal ideal* if where ever I is an ideal of R with $M \subset I$, then $I = R$.

Example: In $Z_6$the ideals are:

$\{0\}$, Z_6 , $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$

$\{\bar{0}, \bar{3}\}$ is the maximal in Z_6

$\{\bar{0}, \bar{2}, \bar{4}\}$ is the maximal in Z_6.

Definition:

A proper ideal P of a ring R is called a *prime* ideal if for all a , b in R with $a.b \in P$ either $a \in P$ *or* $b \in P$.

Example:

1)$4Z$ is an ideal in Z, but not a prime ideal in Z.

2)$\{0\}$ is a prime ideal in Z.but not maximal.

3)$\{0\}$ is not a prime ideal in Z_6 .

Definition:

A commutative ring with identity is called an *integral domain* if it has no zero divisor.

Definition:

A ring $(R,+,\cdot)$ is said to be *field* if $(R-\{0\},\cdot)$ forms a commutative ring (with identity 1).

Or

The field is commutative ring with identity in which each nonzero element has inverse under multiplication.

Remark:

Every field is an integral domain.

Proof: Let R be a field and let $a, b \in R$such that $a.b=0$

If $a \neq 0 \Rightarrow a$ has inverse say a^{-1} [since $a \in$ field] $\Rightarrow a^{-1}.a.b=0 \Rightarrow b=0$

i.e., R is integral domain.

Remark:

Let R be a commutative ring with identity, then R is a field if and only if $\{0\}$ and R are the only ideals of R.

Proof:$\Rightarrow$ let $I \neq 0$ be an ideal in R let $a \neq 0$, $a \in I$, but R is a field $\Rightarrow \exists\ a^{-1}$ and $a.a^{-1} = 1 \in I$ [I ideal $a \in I$, $r \in R \Rightarrow ar \in I$] $\Rightarrow I = R$ [by remark]

$\Leftarrow$) Let $a \neq 0$, $a \in R$,$< a >$ is an ideal in R but $< a > \neq \{0\} \Rightarrow < a > = R$

$\therefore 1 \in R \Rightarrow 1 \in < a > \Rightarrow 1 = r.a$

Example:Q have ideals $\{0\}, Q$.

R have ideals $\{0\}$, R.

C have ideals $\{0\}$, C

Z_3, Z_5, Z_7 are fields.

Remark:

Every finite integral domain is field.

Proof: Let $R = \{a_1, a_2, \dots, a_n\}$ be an integral domain and $0 \neq a_j \in R$ consider the set $S = \{a_1 a_j, a_2 a_j, \dots, a_n a_j\}$ all elements of S are distinct since if $a_l a_j = a_k a_j \Rightarrow a_l = a_k$ C!

Clearly $S \subseteq R$ and $R \subseteq S \Rightarrow S = R \Rightarrow 1 \in S$

$\Rightarrow 1 \in a_n a_j \Rightarrow a_j$ has inverse $\Rightarrow R$ is field.

Remark:

Let R be an integral domain with only finite number of ideals in R, then R is a field.

Proof: Let $a \neq 0$, $a \in R$, $< a >$, $< a^2 >$, $< a^3 >$, ... be ideals in R but R has only finite number of ideals $\Rightarrow \exists\ k, \ell$ such that $k < \ell$ positive integers such that $< a^k > = < a^\ell >$.

$\Rightarrow a^k \in < a^k > = < a^\ell > \Rightarrow a^k = ra^\ell$ for some $r \in R \Rightarrow a^k = ra^\ell = ra^{\ell-k}a^k$

$\because R$ is integral domain $\Rightarrow$ cancelation law is valid. $\Rightarrow 1 = ra^{\ell-k} \Rightarrow$

$1 = \left(ra^{\ell-k-1}\right).a$ and $\because 1 = a^{-1}a$

$\therefore a^{-1} = ra^{\ell-k-1} \Rightarrow a^{-1} \in R$

$\therefore R$ is a field.

Remark:

If R is a field, then either $f : R \to R'$ is 1-1 or $f : R \to R'$ is the zero homomorphism.

Proof:

$Ker\ f$ is an ideal in R.

$Ker\ f = \{0\}$ or $ker\ f = R$.

$\therefore f$ is 1 -1 or f is the zero.

Remark:

Let R be a commutative ring with 1, let N be the set of nilpotent elements of R, then N is an ideal in $R$and $\frac{R}{N}$ has no nonzero nilpotent element.

[a is a nilpotent $a^n = 0$ for some positive integer n]

Proof: $N \neq \emptyset$ [$0 \in N$, $(0)^n = 0$, $\forall\, n$] let $a \in N$ and $r \in R$

$\because\, a \in N \Rightarrow \exists$ a positive integer k such that $a^k = 0$

$$(ar)^k = a^k r^k = 0\,.\,r^k = 0 \ , \ r \in R$$

$\therefore ar \in N$

Let $a, b \in N \Rightarrow \exists\, n, m$ positive integers such that $a^n = 0, b^m = 0$

$$(a-b)^{n+m} = a^{n+m} - (\ )a^{n+m-1}\mathrm{b} + (\ )a^{n+m-2}b^2 - (\ )a^{n+m-3}b^3 + \dots + (\ )a^n b^m + \cdots + b^{n+m} = 0.$$

$\Rightarrow (a-b)$ is nilpotent $\Rightarrow a - b \in N \Rightarrow N$ is an ideal.

Now, let $r + N$ be nilpotent element in $\frac{R}{N}$, $\exists\ k \in Z^+$ such that $(r+N)^k = N$

$$r^k + N = N \Leftrightarrow r^k \in N$$

$\Rightarrow \exists\, s \in Z^+$ such that $(r^k)^s = 0 \Rightarrow r^{ks}$(nilpotent) $= 0$

$\Rightarrow r \in N \Rightarrow r + N = N$.

<u>Remark:</u>

Let R be commutative ring with identity and let a be an idempotent element in R, then $R = \langle a \rangle \oplus \langle 1-a \rangle$

Proof: $a \in \langle a \rangle$, $a \in R$, $\langle a \rangle \subseteq R$, $\langle a \rangle + \langle 1-a \rangle \subseteq R, 1 \in R$

$$1 = a + 1 - a \Rightarrow 1 \in \langle a \rangle + \langle 1-a \rangle \Rightarrow R \subseteq \langle a \rangle + \langle 1-a \rangle$$

$$\Rightarrow R = \langle a \rangle + \langle 1-a \rangle$$

Let $w \in < a > \cap < 1 - a > \Rightarrow w = ra$; $r \in R$

$$w = t.(1 - a) \ ; \ t \in R \ \Rightarrow \ ra = t.(1 - a)$$

$\because a$ is idempotent $\Rightarrow a^2 = a$ Now,

$$w.a = r\ a^2 = ra = t(1 - a)$$

$$w = t(1 - a)a$$

$$w = t(a - a^2) = t(a - a)$$

$$w = 0 \Rightarrow < a > \cap < 1 - a > = 0$$

$\Rightarrow R = < a > \oplus < 1 - a >$.

Example: In Z_6

$\bar{3}$ is idempotent in Z_6

$(\bar{3})^2 = \bar{3} \Rightarrow Z_6 = < \bar{3} > \oplus < 1 - \bar{3} > = \{\bar{0}, \bar{3}\} \oplus \{\bar{0}, \bar{2}, \bar{4}\}$

Example:

$(p(X), \Delta, \cap)$ is a commutative ring with identity ,

Let $A \in p(X)$, then $A^2 = A \cap A = A$; A is idempotent.

$p(X) = < A > \oplus < \bar{X} - A >$.

Remark:

Let $f: R \to R'$ be an eipemorphism, if R is P I R, then so is R'.

Proof:

Let K be an ideal in R', $f^{-1}(K)$ is an ideal in R [theorem] but R is principle ideal ring, then $f^{-1}(K) = \langle x \rangle$; $x \in R$

$x \in f^{-1}(K)$, $f(x) \in K \Rightarrow \langle f(x) \rangle \subseteq K$ we claim that $K = \langle f(x) \rangle$

Let $y \in K$, f is an eipemorphism.

$\therefore \exists\, r \in f^{-1}(K)$ such that $y = f(r) \in K$ but $f^{-1}(K) = \langle x \rangle$

$\therefore r = w.x$

$$f(r) = f(w.x) = f(w).f(x) \quad \therefore y = f(w).f(x)$$

$$y \in \langle f(x) \rangle \quad \Rightarrow K = \langle f(x) \rangle$$

$\therefore R'$ is P. I. R.

Definition:

Let I and J be ideals in R, then $I.J = \{\sum_{i=1}^{n} a_i b_i : a_i \in I \ , \ b_i \in J\}$ is called the product of I and J .

Theorem:

Let $f: R \to R'$ be an epimorphism and let I, J be ideals in R, then

1) $f(I \cap J) \subseteq f(I) \cap f(J)$ and if $ker\, f \subseteq I$ or $ker\, f \subseteq J$,then

2) $f(I + J) = f(I) + f(J)$

3) $f(I.J) = f(I).f(J)$

Remark:

Let I, J, K be ideals in R , then

1) $I(J + K) = IJ + IK$.

2) If $J \subseteq I$, then $I \cap (J + K) = J + (I \cap K)$

Proof(1): Let $w \in I(J + K)$

$w = a_1 b_1 + a_2 b_2 + \dots + a_n b_n$

$a_i \in I \; , b_i \in J + K \quad b_i = c_i + d_i \quad ; c_i \in J, \; d_i \in K$

$w = a_1(c_1 + d_1) + \dots + a_n(c_n + d_n)$

$= a_1 c_1 + a_1 d_1 + \dots + a_n c_n + a_n b_n$

$= a_1 c_1 + a_2 c_2 + \dots + a_n c_n + a_1 d_1 + \dots + a_n d_n \in IJ + IK$

$\Leftarrow$) Let $x \in IJ + IK \Rightarrow a = a + b \quad ; \quad a \in IJ, b \in IK$

$a = c_1 d_1 + \dots + c_n d_n \quad , c_i \in I \; , d_i \in J$

$b = c_1 e_1 + \dots + c_n e_n \quad ; \quad c_i \in I \quad , \; e_i \in K$

$x = a + b = c_1 d_1 + \dots + c_n d_n + c_1 e_1 + \dots + c_n e_n =$

$c_1(d_1 + e_1) + \dots + c_n(d_n + e_n) \in I(J + K)$

Proof(2):

Let $w \in I \cap (J + K)$; $w \in I$ and $w \in J + K$

$w = a_1 + b_1 \; ; \; a_1 \in J \; , \; b_1 \in K$

$w = a_1 + (w - a_1); \quad w - a_1 \in I \; , \; w - a_1 = b_1 \in K$

$a_1 + w - a_1 = w$

$\therefore w \in J + (I \cap K)$

$\Leftarrow$) $y \in J + (I \cap K)$

$y = a + b \; ; \quad a \in J \; , b \in I \; , \; b \in K$

$a \in J \subseteq I \ , a \in I \ , \ b \in I$

$\therefore \ a + b = y \in J + K \ \therefore y \in I \cap (J + K)$.

Definition:

Let R be a commutative ring with identity. An ideal M of a ring R is called maximal ideal if

1) $M \neq R$.

2) Whenever J is an ideal with $J \supseteq M$, then $J = R$.

Example: In the ring Z_6 , $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$ are maximal ideals

$2Z \subset Z$ ideal, $4Z \subset Z$ is not maximal ideal, since $< 4 > \subset < 2 >$

Example: Q , R , C , Z_p ; p is prime are fields so $\{0\}$ is the only ideal

$\therefore \{0\}$ is the only maximal ideal

Theorem:

Let M be a proper ideal of a ring R, then M is maximal ideal if and only if the ideal $< M, a > = R, \ \forall \ a \in R \ , a \notin M$.

Proof:$\Rightarrow$) Let $w \in < M, a > = M + < a > = m + ra$

$M \subsetneq < M, a >$ [since $a \notin M$]

$\therefore < M, a > = R$

$\Leftarrow$) let J be an ideal in R such that $J \supsetneq M$

$\therefore \exists x \in J$ and $x \notin M$, since $< M, x > = R$

$$J \supseteq < M, x > = R$$

$\therefore J = R$, so M is maximal ideal.

Definition:

Let $\{A_\alpha\}_{\alpha\in\lambda}$ be a family of ideals of a ring R, $\{A_\alpha\}_{\alpha\in\lambda}$ is called a chain if $\forall\gamma, \beta\in\lambda$ either $A_\beta \subseteq A_\gamma$ or $A_\gamma \subseteq A_\beta$.

Zorn's Lemma:

Let F be a family of subsets of fixed nonempty set X. If for each chain $\{A_\alpha\}_{\alpha\in\lambda}$ in F the $\bigcup_{\alpha\in\lambda} A_\alpha$ is a member of F, then F contains a maximal element M in the sense that M is not contained properly in any member of F.

Theorem:

Let I be a proper ideal of a commutative ring with 1. Then there exists a maximal ideal M containing I.

Proof: Let I be a proper ideal of R, let $F = \{J: J \text{ is an ideal with } J \supseteq I, J \neq R\}$

$F \neq \emptyset$ [since I ideal proper]

Let $\{C_\alpha\}_{\alpha\in\lambda}$ be a chain in F. Then $\bigcup_{\alpha\in\lambda} C_\alpha$

(1) $\bigcup_{\alpha\in\lambda} C_\alpha$ is an ideal, $\bigcup_{\alpha\in\lambda} C_\alpha \neq \emptyset$ since $F \neq \emptyset$

Let $x, y \in \bigcup_{\alpha\in\lambda} C_\alpha$, , then $x \in C_\beta$, $y \in C_\gamma$, $\gamma, \beta \in \lambda$

But $\{C_\alpha\}$ is a chain then either $C_\beta \subseteq C_\gamma$ or $C_\gamma \subseteq C_\beta$.

If $C_\beta \subseteq C_\gamma$, then $x, y \in C_\gamma$ C_γ is ideal so $x - y \in C_\gamma$.

Or $C_\gamma \subseteq C_\beta$, then $x, y \in C_\beta$,then $x - y \in C_\beta \Rightarrow x - y \in \bigcup_{\alpha\in\lambda} C_\alpha$

Let $w \in \bigcup_{\alpha\in\lambda} C_\alpha$; $r \in R$

$\therefore w \in C_\beta$, $\beta \in \lambda \Rightarrow rw \in C_\beta$ so $rw \in \bigcup_{\alpha\in\lambda} C_\alpha$, then $\bigcup_{\alpha\in\lambda} C_\alpha$ is an ideal.

(2) $I \subseteq \bigcup_{\alpha\in\lambda} C_\alpha$ since $I \subseteq C_\alpha$, $\forall \alpha \in \lambda$

(3) $\bigcup_{\alpha\in\lambda} C_\alpha \neq R$, $I \in \bigcup_{\alpha\in\lambda} C_\alpha \Rightarrow I \in C_\alpha$ for some $\alpha \in \lambda$ $C!$ $(J \neq R)$ $\forall J \in F$

$\therefore$ By Zorn's Lemma F has maximal element say M.

We claim that M is maximal ideal if K ideal of Rsuch that $K \supsetneq M$, then $K \notin F$ (since M is maximal element in F)

$\therefore K = R$ so M is maximal ideal.

Corollary:

Every commutative ring with identity has at least one maximal ideal.

Theorem:

let R be a commutative ring with identity, an element $x \in R$ is invertible if and only if it belongs to no maximal ideal.

Proof:

$\Longrightarrow$) Let x be an invertible element of R.

Suppose $x \in M$ and M is a maximal ideal

Since x invertible, then $\exists\, y \in R$ such that $x \cdot y = 1$.

$x \in M$, then $x.y \in M, 1 \in M,$ then $M = R$ C!

$\Leftarrow$) let $x \epsilon R$ and x dose not belong to any maximal ideal

Now, $< x >$ is an ideal in R.

If $< x > = R \Rightarrow 1 \in < x > \Longrightarrow 1 = r.x \Rightarrow x$ invertible

If $< x > \neq R$, by the previous theorem there exist a maximal ideal M

$M \ni < x > \subseteq M \Rightarrow x \epsilon M$ C!.

Remark:

Let R be a ring with only one maximal ideal, then the only idempotent of R are zero and one.

Proof: let x be an idempotent element $x \neq 0$ and

$x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0$ so $x, x-1$ are zero divisors. Hence x and $x - 1$ are not invertible?

But R has only one maximal ideal M so $x, x-1 \in M$, then $x + (x-1) \in M$. Thus $1 \in M$ C!

Theorem:

Let R be a commutative ring with 1, let M be a proper ideal of R, then M is maximal if and only if $\frac{R}{M}$ is a field.

Proof:

⇒) R is commutative with 1, then $\frac{R}{M}$ is commutative with 1, let $x + M \in \frac{R}{M}$ and $x + M \neq M \Rightarrow x \notin M$,

∵ M is maximal, then $< M, x > = R$, then $1 = m + rx \Rightarrow 1 - rx = m \in M$, then $1 - rx \in M$ $[aH = bH \Leftrightarrow a - b \in H]$, then $1 + M = rx + M$. Hence $1 + M = (r + M).(x + M)$

Thus $x + M$ is invertible and $\frac{R}{M}$ is a field.

⇐) Let J be ideal

Suppose that $J \supsetneq M$, then $\exists x \in J, x \notin M$, then $x + M \neq M$.

But $\frac{R}{M}$ is a field $\Rightarrow \exists\, y + M \in \frac{R}{M}$ Such that $(x + M)(y + M) = 1 + M$

$xy + M = 1 + M$. Then $1 - xy \in M \subset J$

$(1 - xy) + xy \in J \Rightarrow 1 \in J = R$

∴ M is maximal.

Definition:

The intersection of all maximal ideal in a ring R is called the Jacoson radical of a ring R it is denoted by $rad(R)$.

Example: (1) In $Z, (2Z) \cap (3Z) \cap (7Z) \cap \ldots = \{0\}$, $rad(Z) = 0$

(2) In Z_6, $\{\bar{0}, \bar{2}, \} \cap \{\bar{0}, \bar{3}\} = \{0\}$, $rad(Z_6) = 0$

(3)In Z_4 , $M = \{0, 2\}$

$\therefore rad(Z_4) = \{0, 2\}$

Definition:

An ideal P of a ring R is called prime ideal if $P \neq R$ and for every $a.b \in P$ either $a \in P$ or $b \in P$ $\forall\, a, b \in R$.

Example: (1) In the ring Z_6 ,let $P = \{\bar{0}, \bar{2}, \bar{4}\}$, $\bar{2}.\bar{4} = \bar{2} \in P$

(2) $P \neq Z_6$, $6 \in P$

$6 = 2.3$, $2 \in P$,

$6 = 6.1$, $6 \in P$.

$\therefore$ P is a prime ideal.

Remark:

$\{0\}$ is a prime ideal if and only if R is an integral domain.

Proof:$\Rightarrow$) Let $a \neq 0$, $b \in R$ such that $a.b = 0$

$\therefore a.b \in \{0\}$ but $\{0\}$ is prime and $a \neq 0 \Rightarrow b \in \{0\}$

$\therefore$ $b = 0$.

$\therefore R$ is an integral domain.

Theorem:

Let R be commutative ring with 1 and P be a proper ideal of R, $P$is a prime ideal if and only if $\frac{R}{p}$ is integral domain.

Proof:$\Rightarrow$) Since R is commutative ring with 1 so is $\frac{R}{p}$

Let $b+P$, $a+P \in \frac{R}{p}$, then

$(a + P).(b + P) = P$, then $a \cdot b + P = P \Leftrightarrow ab \in P$

P is prime $\Rightarrow a \in P$ or $b \in P$ if $a \in P$, then $a + P = P$

Or $b \in P \Rightarrow b + P = P$.

$\Leftarrow$) $\frac{R}{p}$ is an integral domain, let $a.b \in P$

Then $ab + P = P$,

$(a + P)(b + P) = P$.

Since $\frac{R}{p}$ is an integral domain, then either $a + P = P \Leftrightarrow a \in P$ or $b + P = P \Leftrightarrow b \in P$. Thus P is prime.

Corollary:

Let R be a commutative ring with 1, then every maximal ideal is prime ideal.

Proof: M maximal ideal $\Rightarrow \frac{R}{M}$ is a field $\Rightarrow \frac{R}{M}$ is integral domain [Every field is integral domain]

Thus M is prime.

Example: In $Z, 2Z, 3Z$

(1) $2Z$ is a ring without 1 , $4Z$ is not maximal ideal and is not prime since $4 \in 4Z$ for example $4 = 2.2$, $2 \notin 4Z$

Q: $I \subseteq rad(R) \Leftrightarrow \forall\ a \in 1 + I$, a is invertible.

Proof:$\Rightarrow$) Let $I \subseteq rad(R)$ and assume that $\exists\, a \in I$such that$1 + a$ has no inverse $\exists$ maximal ideal$M$such that $1 + a \in M$,$a \in I \subseteq rad(R) \subseteq M$,$a \in M$, $1 + a - a \in M \Rightarrow 1 \in M$

Hence $M = R$ C! .Thus $1 + I$ has inverse.

$\Leftarrow$) Suppose that each member of $1 + I$ has inverse, but $I \nsubseteq rad(R) = \cap M$; M is maximal ideal, then $I \nsubseteq M$.

Now, if $a \in I$, then $a \notin M$. Since M is maximal, then $< M, a > = R$ [Theorem], hence $1 \in R \Rightarrow 1 = m + ra$; $r \in R$,$m \in M \Rightarrow m = 1 - ra$, but $1 - ra \in 1 + I$, then $m \in 1 + I$, then m has inverse.

Thus M has inverse C! [since $M = R$]

Q: a is invertible in $R \Leftrightarrow a + rad(R)$ invertible in $\frac{R}{rad(R)}$

Proof:$\Rightarrow$) a is invertible, $\exists\, b \in R$ such that $a.b = 1$

$\big(a + rad(R)\big)\big(b + rad(R)\big) = ab + rad(R) = 1 + rad(R)$

So $a + rad(R)$ is invertible in $\frac{R}{rad(R)}$

$\Leftarrow$) $(a + radR)(b + radR) = 1 + rad(R)$

$\Rightarrow ab\, rad(R) = 1 + rad(R)$

$\Leftarrow$) $ab - 1 \in rad(R)$

Then $1 + ab - 1$ is invertible, ab invertible.

Hence $\exists\, x \in R$ such that $(ab)x = 1$, $a(bx) = 1$

Thus a is invertible.

Q: $a \in rad(R) \Leftrightarrow 1 + ra$ has inverse $\forall\ r \in R$

Proof: $\Rightarrow$) Let $a \in rad(R)$, $\Rightarrow < a > \subseteq rad(R)$,

$< a >= \{ra : r \in R\}$, $1 + < a >$ has inverse

Then $1 + ra$ has inverse $\forall\, r \in R$.

$\Leftarrow$) Let $1 + ra$ $\forall\, r \in R$ has inverse

$1 + < a >$ has inverse $\Leftrightarrow < a > \subseteq rad(R)$,

$\Rightarrow a \in rad(R)$

Theorem:(Boolean ring)

Let R be a ring with $a^2 = a$,$\forall\ a \in R$, then every prime ideal is maximal ideal.

Proof: Let M be a prime ideal and J ideal of Rsuch that

$M \subsetneq J \subseteq R$, then $\exists\ a \in J , a \notin M$

$a^2 = a \Rightarrow a(a-1) = 0 \in M$ but M is prime, $a \notin M$

Then $a - 1 \in M \subseteq J$ and $a \in J$.

$\therefore a - 1$, $a \in J$ [J is ideal]

Thus $1 \in J \Rightarrow J = R$ [I ideal, $1 \in I \Rightarrow R = I$]

Theorem:

Let R be principle ideal domain, then every nonzero prime ideal is maximal.

Proof: Let $I \neq 0$, I is prime and $I \subsetneq J \subseteq R$, R is P. I. D

$\exists\ a, b \in R$ such that $I = < a > m\, J =< b >$, $< a > \subsetneq < b >$ ………(*)

So $a = rb$, $r \in R$, $rb \in < a >$, $< a >$ is prime

Then either $r \in < a >$ or $b \in < a >$ if $b \in < a > \Rightarrow < a > = < b >$ C!

Thus $r \in < a >$ and $r = sa$

$a.1 = a = rb = sab = a.s.b$ [R comm.] [R integral domain]

$$1 = s.b, 1 \in < b > = J$$

$\therefore$ J = R .

Definition:

The intersection of all prime ideals in a ring R is called the prime radical of R it is denoted by $Rad\ R$

$$rad\ R \supseteq Rad\ R$$

$$rad\ Z = Rad\ Z$$

Theorem:

Let R be a commutative ring with 1, then every maximal ideal is prime ideal.

Proof: Let M be a maximal ideal of a ring R suppose that $a.b \in M$ and $a \notin M$, M is maximal, then $< M, a > = R$, then $1 = m + ra$; $m \in M$, $r \in R$,

Hence $b = mb + rab \in M$.

Q: Is the converse true?

Example: In the ring $Z \times Z$,$\{0\} \times Z$ is a prime ideal in $Z \times Z$.

$2Z \times Z$is an ideal in $Z \times Z$ which is maximal. $\{0\} \times Z \subsetneq 2Z \times Z \subsetneq Z \times Z$.

Definition:

Let I be an ideal of a ring R. Then the nil radical of I denoted by $\sqrt{I}$ is the set:

$$\sqrt{I} = \{r \in R : \exists\, n \in Z^+ \ni r^n \in I\}$$

Remark:

1. $\sqrt{I} \supseteq I$.
2. $\sqrt{I}$is an ideal of R.

Proof: Let $x, y \in \sqrt{I},\ x \in \sqrt{I} \ni\ n \in Z^+ \ni x^n \in I$,

$$y \in \sqrt{I} \ni m \in Z^+ \ni y^m \in I.$$

$(x-y)^{n+m} = x^{n+m} + (\quad)x^{n+m-1}y + \cdots + (\quad)x^n y^m + (\quad)x^{n-1}y^{m+1} + \cdots$ $+ y^{n+m}$.

Hence $(x-y) \in \sqrt{I}$

Let $r \in R, w \in \sqrt{I}, w^n \in \sqrt{I}$; $n \in Z^+$.

$(rw)^n = r^n w^n \in I$, then $\in \sqrt{I}$.

Example:If $\sqrt{I} = \sqrt{J} \nRightarrow I = J$.

$$\sqrt{2Z} = 4Z$$

$$\sqrt{8Z} = 2Z$$

Remark:

1. $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$.
2. $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. $\sqrt{I+J} \supseteq \sqrt{I} + \sqrt{J}$.

Proof:1.Let $w \in \sqrt{I \cap J}$, then $\exists\ n \in Z^+ \ni w^n \in I \cap J$, then $w^n \in I$ and $w^n \in J$, hence $w \in \sqrt{I}$ and $w \in \sqrt{J}$. Thus $w \in \sqrt{I} \cap \sqrt{J}$.

Let $y \in \sqrt{I} \cap \sqrt{J}$, then $y \in \sqrt{I}$ and $y \in \sqrt{J}$, hence $y^n \in I$ and $y^n \in J$.

$y^{n+m}=y^n \cdot y^m \in IJ$, then $y \in \sqrt{IJ}$.

$y^{n+m}=y^n \cdot y^m \in I \cap J$, then $y \in \sqrt{I \cap J}$. Thus $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

2. Let $w \in \sqrt{\sqrt{I}} \supseteq \sqrt{I}$.

Let $x \in \sqrt{\sqrt{I}}$ $\exists\ n \in Z^+ \ni x^n \in \sqrt{I}$, and then $\exists\ m \in Z^+ \ni (x^n)^m \in I$, hence $x^n \in I$, which implies that $x \in \sqrt{I}$.

3.Let $w \in \sqrt{I} + \sqrt{J}$, then $w = x + y$; $x \in \sqrt{I}$ and $y \in \sqrt{J}$, then $\exists\ n \in Z^+ \ni$ $x^n \in I$ and $\exists\ m \in Z^+ \ni y^m \in J$.

$(x+y)^{n+m} = x^{n+m} + (\quad)x^{n+m-1}y + \cdots + (\quad)x^n y^m + (\quad)x^{n-1}y^{m+1} + \cdots + y^{n+m}$.

Thus $x + y \in \sqrt{x+y}$.

Theorem:

Let $f : R \longrightarrow R'$ be a ring epimorphism.

1. If M isa maximal (prime) with $ker\, f \subseteq M$ in R, then $f(M)$ is maximal (prime) ideal in R'.
2. If M' is a maximal (prime) in R', then $f^{-1}(M')$ is maximal (prime) in R .

Proof :1. Let M be a maximal ideal clearly $f(M)$ is an ideal in R

If $f(M) = R'$, then $1' \in f(M) \rightarrow 1' = f(m)$; $m \in M$

But $f(1) = 1' \rightarrow f(m) = f(1) \rightarrow f(m-1) = 0$

$\rightarrow m - 1 \in \ker f \subseteq M \rightarrow m - (m-1) \in M \rightarrow 1 \in M$ contradiction.

Let $J \supsetneq f\,(M)$, $\ni y \in J$ and $y \notin f(M)$

But f is $onto$ $\rightarrow \exists x \in R \ni f\,(x) = y \rightarrow x \notin M$

Then $< M, x > = R \rightarrow 1 = m + tx$; $m \in M$, $t \in R$

$1' = f(1) = f(m) + f(t).f(x)$

$1' = f(m) + f(t)y \in J \rightarrow J = R$

2. Let M' be a prime ideal of R , then clearly $f^{-1}(M)$ is an ideal in R.

If $f^{-1}(M') = R \rightarrow 1 \in f^{-1}(M') \rightarrow f(1) \in M'$

Let $x.y \in f^{-1}(M)$ and $x \notin f^{-1}(M)$

$f(x).f(y) = f(x.y) \in M'$ and $f(x) \notin M.$

$\therefore f(y) \in M' \rightarrow y \in f^{-1}(M).$