9 RINGS

HR-10
30783

9.1. RING

(P.T.U. B.Tech. Dec. 2009, May 2008, 2007, Dec. 2006, May 2005)

Let R be a non-empty set with two binary compositions, addition (+) and multiplication (.). Then R is called a ring iff it satisfies the following :

I. R is an abelian group under + *i.e.*,

(*i*) For $a, b \in R \Rightarrow a + b \in R$ *i.e.*, R is closed under addition

(*ii*) For $a, b, c \in R$, $a + (b + c) = (a + b) + c$ *i.e.*, Associativity under addition holds in R.

(*iii*) For each $a \in R$, $\exists\ 0 \in R$ such that $a + 0 = a = 0 + a$ *i.e.*, R has additive identity.

(*iv*) For each $a \in R$, $\exists\ -a \in R$ such that $a + (-a) = 0$ *i.e.*, R has an additive inverse.

(*v*) For each $a, b \in R$, $a + b = b + a$ *i.e.*, R is additive.

II. For each $a, b \in R$, $a.\ b \in R$ *i.e.*, R is closed under multiplication.

III. For $a, b, c \in R$, $a.\ (b\ .\ c) = (a.\ b)\ .\ c$ *i.e.*, Associativity under multiplication holds in R.

IV. For $a, b, c \in R$,

(*i*) $a\ .\ (b + c) = a.\ b + a.\ c$ (Left distributive law)

(*ii*) $(a + b)\ .\ c = a.\ c + b\ .\ c.$ (Right distributive law)

Remark : The additive identity 0 of R is unique. We call it 'zero' of the ring. The additive inverse is also unique.

9.2. COMMUTATIVE RING

A ring R is called a commutative ring if $a\ .\ b = b\ .\ a \quad \forall\ a, b \in R$.

9.3. RING WITH UNITY

(P.T.U. B.Tech. Dec. 2005)

A ring R is called ring with unity if for each $x \in R$, $\exists\ 1 \in R$ such that $1\ .\ x = x = x\ .\ 1$. The element '1' is called multiplicative identity of R.

9.4. FINITE AND INFINITE RING

A ring R with finite number of elements, is known as finite ring, otherwise it is known as infinite ring.

9.5. (a) RING WITH ZERO DIVISORS

Let R be a ring and $0 \neq a, b \in R$. Then R is called *ring with zero divisors* if $a.\ b = 0$. *i.e.,*

If product of two non-zero elements in a ring R is zero, then R is called ring with zero divisors. Also we say that the element a is a zero divisor of b or b is a zero divisor of a.

9.5. (b) RING WITHOUT ZERO DIVISORS

A ring R is called ring without zero divisors if whenever

$$a \,.\, b = 0 \Rightarrow a = 0 \text{ or } b = 0 \; \forall\, a, b \in R.$$

ILLUSTRATIVE EXAMPLES

Example 1. *Let Z be the set of integers, then (Z, +, .) is a ring. Also Z is a commutative ring with unity.*

Sol. We know that Z is an additive group under +. (See Chapter on 'Groups').

Also for $a, b \in Z \Rightarrow a.\ b \in Z \quad \forall\, a, b \in Z$ *i.e.,*

Z is closed under multiplication.

For $a, b, c \in Z$, $a \,.\, (b \,.\, c) = (a.\ b) \,.\, c \qquad \forall\, a, b, c \in Z$ *i.e.,*

Associativity under multiplication holds in Z.

For $a, b, c \in Z$, $a \,.\, (b + c) = a.\ b + a \,.\, c$

$$(a + b) \,.\, c = a \,.\, c + b \,.\, c \;\forall\, a, b, c \in Z$$

Hence we can say that Z is a ring.

Further, for $a, b \in Z$, $\quad a \,.\, b = b \,.\, a \qquad \forall\, a, b \in Z$

$\therefore$ Z is commutative also.

Also for $a \in Z$, $\exists\, 1 \in Z$ such that

$$1 \,.\, a = a = a \,.\, 1 \qquad \forall\, a \in Z.$$

$\therefore$ Z is a ring with unity (multiplicative identity).

Example 2. *Show that E, the set of even integers is a commutative ring without unity.*

Sol. Consider $\quad E = \{..., -4, -2, 0, 2, 4, 6, ...\}$

For $a, b \in E$, $a + b \in E \quad \forall\, a, b \in E.$ *i.e.;*

E is closed under addition.

For $a, b, c \in E$, $a + (b + c) = (a + b) + c \;\forall\, a, b, c \in E$. *i.e.,*

E is closed under association.

For $a \in E$, there exists $0 \in E$ such that

$$a + 0 = a = 0 + a \quad \forall\, a \in E.$$ *i.e.,*

0 is the additive identity of E.

For $a \in E$, there exists $-a \in E$ such that $a + (-a) = 0 = (-a) + a \qquad \forall\, a \in E$. *i.e.,*

E has additive inverse.

Also, for $a, b \in E \Rightarrow a + b = b + a \quad \forall a, b \in E$.

Hence E is an additive group.

Further, for $a, b \in E$, $a \cdot b \in E \quad \forall a, b \in E$. *i.e.*,

E is closed under multiplication.

For $a, b, c \in E$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in E$. *i.e.*,

E is closed under association w.r.t. multiplication.

Also for $a, b, c \in E$, $a \cdot (b + c) = a \cdot b + a \cdot c$

$(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in E$.

Also for $a, b \in E$, $a \cdot b = b \cdot a \; \forall a, b \in R$

$\therefore$ E is a commutative ring.

But for $a \in E$, there exists no $1 \in E$ such that $a \cdot 1 = a = 1 \cdot a$

$\therefore$ E is a commutative ring without unity (multiplicative identity).

Example 3. *Show that the set M of 2 × 2 matrices over integers form a non-commutative ring with unity under matrix addition and multiplication.*

Sol. Let $M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in Z\right\}$. We show M is a ring under matrix addition and multiplication.

Let $A, B \in M \Rightarrow A + B \in M \; \forall A, B \in M$.

Since sum of two matrices of the same order is again a matrix. Therefore M is closed under matrix addition.

For A, B, C ∈ M, $A + (B + C) = (A + B) + C \quad \forall A, B, C \in M$.

i.e., matrix addition is associative.

For A ∈ M, there exists O ∈ M such that

$A + O = A = O + A$

The element O is called additive identity of M.

For A ∈ M, there exists – A ∈ M such that

$A + (-A) = O \; \forall A \in M$.

The element – A is called additive inverse of A.

For A, B ∈ M, $A + B = B + A \quad \forall A, B \in M$ *i.e.*, matrix addition is commutative.

$\therefore$ M is an additive group.

We know that matrix multiplication is associative. *i.e.*,

$A + (B + C) = (A + B) + C \; \forall A, B, C \in M$

Also $A \cdot (B + C) = A \cdot B + A \cdot C$

$(A + B) \cdot C = A \cdot C + B \cdot C \; \forall A, B, C \in M$

i.e., left distributive law and right distributive law also hold.

Hence M is a ring under matrix addition and multiplication.

But matrix multiplication in general, is not commutative. *i.e.*, we can have A, B ∈ M for which AB ≠ BA.

Hence M is non-commutative ring.

Lastly, For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$, there exists $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ such that

$A \cdot I = A = I \cdot A$ *i.e.*,

I is the multiplicative identity of M.

Hence M is a non-commutative ring with unity.

Example 4. *Consider the set* $X = \{0, 1, 2, 3, 4, 5; +_6, \times_6\}$. *then X is a commutative ring with unity under addition and multiplication modulo 6.*

Sol. Consider the addition modulo table shown in Table. I

Table I

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

From Table I, we observe that each element inside the Table I is also in X. It means X is closed under addition modulo 6. Also addition modulo 6 is associative. *i.e.*,

$$a +_6 (b +_6 c) = (a +_6 b) +_6 c \qquad \forall\ a, b, c \in X.$$

The first row inside the table coincides with the top most row of the Table I. It means 0 is the additive identity of X.

From Table I, we observe that each element of X has an additive inverse. For *e.g.*,

Inverse of 1 is 5 (the element which is at the intersection of 1 and 5 is 0).

Similarly, Inverse of 2 is 4 etc. $(2 +_6 4 = 0)$

Also Table I is symmetrical w.r.t. $+_6$ It means $a +_6 b = b +_6 a \quad \forall\ a, b \in X.$

$\therefore$ X is an additive group under addition modulo 6 $(+_6)$.

Consider the multiplication modulo table as shown in Table II.

Table II

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From Table II, we observe that each element inside the table is also in X. It means that X is closed under multiplication modulo 6 (X_6)

i.e., for $a, b \in X, \qquad a \times_6 b \in X \qquad \forall\ a, b \in X.$

Also multiplication modulo 6 is associative *i.e.*,

for $a, b, c \in X,\ a \times_6 (b \times_6 c) = (a \times_6 b) \times_6 c\ \forall\ a, b, c \in X$

Further, $a \times_6 (b +_6 c) = a \times_6 b + a \times_6 c$

$$(a +_6 b) \times_6 c = a \times_6 c + b \times_6 c\ \forall\ a, b, c \in X$$

i.e., left distributive law and right distributive law also hold.

Hence X is a ring under addition modulo 6 and multiplication modulo 6. Also Table II is symmetrical w.r.t. $\times_6$. It means that X is a commutative ring. The second row inside Table II coincides with the top most row of Table II. It means 1 is the multiplicative identity of X.

Example 5. *Consider the set Z together with binary compositions $\oplus$ and $\odot$ defined by*

$$a \oplus b = a + b - 1$$

$$a \odot b = a + b - ab.$$ (P.T.U. B. Tech. Dec. 2010)

Show that $(Z, \oplus, \odot)$ *is a ring.*

Sol. We first show that Z is an additive group under $\oplus$. Let $a, b \in Z$. Since Z is a group under +, we have $a + b - 1 \in Z \quad \forall\, a, b \in Z$

$\Rightarrow$ $a \oplus b \in Z \ \forall\, a, b \in Z$, *i.e.*,

Z is closed under $\oplus$.

Let $a, b, c \in Z$ and consider

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 1 - 1$$
$$= a + b + c - 2 \quad ...(1)$$

Also $$(a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b - 1 + c - 1$$
$$= a + b + c - 2 \quad ...(2)$$

Hence from (1) and (2), $a \oplus (b \oplus c) = (a \oplus b) \oplus c \forall\, a, b, c \in Z$

$\therefore$ Z is closed w.r.t. association under $\oplus$.

For $a \in Z$, consider $a \oplus 1 = a + 1 - 1 = a$

$$1 \oplus a = 1 + a - 1 = a$$

$\Rightarrow$ $$a \oplus 1 = a = 1 \oplus a$$

i.e. 1 is the additive identity.

Also for $a, b \in Z$, consider $a \oplus b = 1$

$\Rightarrow$ $$a + b - 1 = 1$$

$\Rightarrow$ $$b = 2 - a$$

i.e., for $a \in Z$, $2 - a$ is the additive inverse of a. Since,

$$a \oplus 2 - a = a + 2 - a - 1 = 1$$

$$2 - a \oplus a = 2 - a + a - 1 = 1$$

$\Rightarrow$ $a \oplus 2 - a = 1 = 2 - a \oplus a.$

Further for each $a, b \in Z$, we have

$$a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$$

$\therefore$ Z is an additive group under $\oplus$.

Let $a, b \in Z \Rightarrow a \,.\, b = a + b - ab \in Z \ \forall\, a, b \in Z$

$\Rightarrow a \,.\, b \in Z$ *i.e.*, Z is closed under $\odot$

Also $$a \odot (b \odot c) = a \odot (b + c - bc) = a + b + c - bc - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc$$

$$(a \odot b) \odot c = (a + b - ab) \odot c = a + b - ab + c - (a + b - ab)c$$
$$= a + b + c - ab - bc - ac + abc$$
$$= a \odot (b \odot c)$$

i.e., Z is closed w.r.t. association under $\odot$.

Finally, For $a, b, c \in Z$, consider

$$a \odot (b \oplus c) = a \odot (b + c - 1) = a + b + c - 1 - a(b + c - 1)$$
$$= a + b + c - 1 - ab - ac + a = 2a + b + c - ab - ac - 1 \quad ...(3)$$

Also $a \odot b = a + b - ab$

$a \odot c = a + c - ab$

$\therefore \quad a \odot b \oplus a \odot c = a + b - ab \oplus a + c - ac = a + b - ab + a + c - ac - 1$

$= 2a + b + c - ab - ac - 1 \quad ...(4)$

From (3) and (4), we get $a \odot (b \oplus c) = a \odot b \oplus a \odot c$

Similarly, $(a \oplus b) \odot c = a \odot c \oplus b \odot c$

i.e., left distributive law and right distributive law also hold.

$\therefore$ Z is a ring under the binary composition $\oplus$ and $\odot$.

9.6. BOOLEAN RING

A ring R is called a Boolean ring if $x^2 = x \ \forall \ x \in R$

For example: The ring {0, 1} under addition and multiplication modulo 2 is a Boolean ring.

Example 6. *If R is a ring such that $a^2 = a \ \forall \ a \in R$. Show that*

(i) $a + a = 0 \ \forall \ a \in R$

(ii) $a + b = 0 \Rightarrow a = b$

(iii) R is commutative. (P.T.U. B.Tech., May 2009)

Sol. *(i)* Given $a^2 = a \ \forall \ a \in R$

$\Rightarrow \quad (a + a)^2 = a + a$

$\Rightarrow \quad (a + a)(a + a) = a + a$ | Distributive law

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

$\Rightarrow \quad a \cdot a + a \cdot a + a \cdot a + a \cdot a = a + a$ | $a^2 = a \Rightarrow a \cdot a = a$

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

$\Rightarrow \quad (a + a) + (a + a) = (a + a) + 0$ | Left cancellation law

$\Rightarrow \quad a + a = 0 \ \forall \ a \in R$

(ii) Let $a + b = 0 = a + a$ | By part (a)

$\Rightarrow \quad b = a$ | Left cancellation law

(iii) Given $a^2 = a \ \forall \ a \in R$

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

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

$\Rightarrow \quad (a + b) \cdot a + (a + b) \cdot b = a + b$

$\Rightarrow \quad a \cdot a + b \cdot a + a \cdot b + b \cdot b = a + b$

$\Rightarrow \quad a^2 + b \cdot a + a \cdot b + b^2 = a + b$ | $a^2 = a \ \forall \ a \in R$

$\Rightarrow \quad a + b \cdot a + a \cdot b + b = a + b$ | Left cancellation law

$\Rightarrow \quad b \cdot a + a \cdot b + b = b$ | Right cancellation law

$\Rightarrow \quad b \cdot a + a \cdot b = 0$ | From part (b), $a + b = 0 \Rightarrow a = b$

$\Rightarrow \quad b \cdot a = a \cdot b$

Hence R is commutative.

9.7. DIRECT PRODUCT OF RINGS

Let $R_1, R_2, \ldots R_n$ be n rings under the operations $+_1, +_2, \ldots, +_n$ and $\cdot_1, \cdot_2, \ldots \cdot_n$ respectively. The direct products of these n rings is defined by P, where

$$P = \prod_{i=1}^{n} R_i = R_1 \times R_2 \times R_3 \times \ldots \times R_n.$$

Theorem I. *If $R_1, R_2, \ldots R_n$ be n rings under the operation of $+_1, +_2, \ldots +_n$ and $\cdot_1, \cdot_2, \ldots \cdot_n$, respectively. Then the direct product of $R_1, R_2, \ldots R_n$ is also a ring under the operation of componentwise addition.*

Proof. Let $P = \prod_{i=1}^{n} R_i$ be the direct product of $R_1, R_2, \ldots R_n$.

Let $a, b \in P$, then $a = (a_1, a_2, \ldots a_n), a_i \in R, 1 \le i \le n$

$b = (b_1, b_2, \ldots b_n), b_i \in R, 1 \le i \le n$

We first show P is an additive group under the operation of componentwise addition defined by

$$a + b = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots a_n +_n b_n)$$

As R_i $(1 \le i \le n)$ is a ring, it must be closed under $+_i$. *i.e.*, if $a_i, b_i \in R_i \Rightarrow a_i +_i b_i \in R_i \; \forall i$

$\Rightarrow$ $(a_1 +_1 b_1, a_2 +_2 b_2, \ldots a_n +_n b_n) \in R_1 \times R_2 \times \ldots \times R_n$

$\Rightarrow$ $a + b \in P$

Hence P is closed under the operation of componentwise addition.

If $a, b, c \in P$, then $a = (a_1, a_2, \ldots a_n), b = (b_1, b_2, \ldots b_n), c = (c_1, c_2, \ldots c_n)$

Consider $a + (b + c) = (a_1 +_1 (b_1 +_1 c_1), a_2 +_2 (b_2 +_2 c_2), \ldots a_n +_n (b_n +_n c_n)$

$= ((a_1 +_1 b_1) +_1 c_1, (a_2 +_2 b_2) +_2 c_2, \ldots (a_n +_n b_n) +_n c_n)$

$= (a + b) + c$

| Each R_i is a ring. Therefore associativity holds in R_i

Hence associativity holds in P.

For $a \in P$, consider

$a + 0 = (a_1, a_2, \ldots a_n) + (0_1, 0_2, \ldots 0_n) = (a_1 +_1 0_1, a_2 +_2 0_2, \ldots a_n +_n 0_n)$

$= (a_1, a_2, \ldots a_n) = a$

Similarly, $0 + a = a$

Hence $a + 0 = a = 0 + a$

i.e., $0 = (0_1, 0_2, \ldots 0_n)$ is the additive identity of P

Further for $a \in P$, consider

$a + (-a) = (a_1, a_2, \ldots a_n) + (-a_1, -a_2, \ldots -a_n) = (a_1 +_1 (-a_1), a_2 +_2 (-a_2), \ldots a_n +_n (-a_n))$

$= (0_1, 0_2, \ldots 0_n) = 0$

Similarly, $(-a) + a = 0$

$\therefore$ P has an additive inverse.

Lastly, For $a, b \in P$, we have

$a + b = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots a_n +_n b_n) = (b_1 +_1 a_1, b_2 +_2 a_2, \ldots, b_n +_n a_n)$

$= b + a$

| Each R_i is additive group

Hence P is an additive group under the operation of componentwise addition.

We next show that associative law under multiplication holds in P.

Define $a \cdot b = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \ldots a_n \cdot_n b_n)$

For $a, b, c \in P$, consider

$$a \,.\, (b \,.\, c) = (a_1 \cdot_1 (b_1 \cdot_1 c_1), a_2 \cdot_2 (b_2 \cdot_2 c_2), \ldots a_n \cdot_n (b_n \cdot_n c_n))$$
$$= ((a_1 \cdot_1 b_1) \cdot_1 c_1, (a_2 \cdot_2 b_2) \cdot_2 c_2, \ldots (a_n \cdot_n b_n) \cdot_n c_n)$$
$$= (a \,.\, b) \,.\, c \qquad \text{| Each } R_i \text{ is associative under } \cdot$$

Thus associativity under multiplication also holds in P.

We now show that left distributive law and right distributive law also holds in P.

Consider $a \,.\, (b + c) = (a_1 \cdot_1 (b_1 +_1 c_1), a_2 \cdot_2 (b_2 +_2 c_2), \ldots a_n \cdot_n (b_n +_n c_n))$

$$= (a_1 \cdot_1 b_1 +_1 a_1 \cdot_1 c_1, a_2 \cdot_2 b_2 +_2 a_2 \cdot_2 c_2, \ldots a_n \cdot_n b_n +_n a_n \cdot_n c_n) \quad \ldots(1)$$

Also $a \,.\, b + a \,.\, c = (a_1 \cdot_1 b_1 +_1 a_1 \cdot_1 c_1, a_2 \cdot_2 b_2 +_2 a_2 \cdot_2 c_2, \ldots a_n \cdot_n b_n +_n a_n \cdot_n c_n) \quad \ldots(2)$

From (1) and (2), we get

$$a \,.\, (b + c) = a \,.\, b + a \,.\, c \quad \forall\, a, b, c \in P$$

Similarly, $(a + b) \,.\, c = a \,.\, c + b \,.\, c \quad \forall\, a, b, c \in P$

Hence P is a ring under the operation of addition and multiplication defined by

$$a + b = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots a_n +_n b_n)$$
$$a \,.\, b = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \ldots a_n \cdot_n b_n).$$

Cor. If $R_1, R_2, \ldots R_n$ are commutative rings with unity, then P is also commutative ring with unity $(1, 1, 1, \ldots 1)$.

Example 7. *If $\{Z_4, +_4, \times_4\}$ and $\{Z_3, +_3, \times_3\}$ are rings, then $Z_4 \times Z_3$ is also a ring. Find the unity, if it exists in $Z_4 \times Z_3$.*

Sol. We know that if R_1, R_2, are rings under the operation of componentwise addition and multiplication then $R_1 \times R_2$ is also a ring.

Here $Z_4 = \{0, 1, 2, 3, \cdot +_4, \times_4\}$

$Z_3 = \{0, 1, 2, +_3, \times_3\}$ are rings under the addition modulo 4 and multiplication modulo 3.

$\therefore$ $Z_4 \times Z_3$ is also a ring under the componentwise addition and multiplication.

| See Theorem I. Direct Product of rings

To find the unity: Let $(x, y) \in Z_4 \times Z_3$ and consider $(x, y)\,(m, n) = (x, y) = (m, n)\,(x, y)$

$$\Rightarrow \quad (x \times_4 m, y \times_3 n) = (x, y) = (m \times_4 x, n \times_3 y)$$

$$\Rightarrow \quad x \times_4 m = x = m \times_4 x \quad \ldots(1)$$

and $\quad y \times_3 n = y = n \times_3 y \quad \ldots(2)$

The only elements m in Z_4 and n in Z_3 which satisfies (1) and (2) are $m = 1$, $n = 1$

Hence the unity of $Z_4 \times Z_3$ is $(1, 1)$.

9.8. MORPHISM OF RINGS

The word 'morphism' is a combination of various terms like ring homomorphism, ring isomorphism etc.

9.8.1. Ring Isomorphism

Let $(R, +, \cdot)$ and $[R', +', \cdot']$ be two rings. The ring R is isomorphic to the ring R′ iff there exists a mapping $f : R \to R'$ such that

(*i*) f is one-one and onto

(*ii*) $f(a + b) = f(a) +' f(b) \quad \forall\, a, b \in R$

(*iii*) $f(a \,.\, b) = f(a) \cdot' f(b) \quad \forall\, a, b \in R.$

The mapping $f : R \to R'$ satisfying the conditions (*i*), (*ii*) and (*iii*) is called ring isomorphism.

Remarks : To check whether the two *rings are isomorphic*, we should check the following :

(*a*) Both rings should have same cardinality.

(*b*) Both rings should be commutative.

(*c*) Both rings should have unity.

(*d*) If there exists an equation which is solvable in one ring, but not solvable in another ring, then two rings cannot be isomorphic.

Example 8. *Consider the rings* $[Z, +, \cdot]$ *and* $[2Z, +, \cdot]$ *and define* $f : Z \to 2Z$ *by* $f(n) = 2n \ \forall \ n \in Z$ (P.T.U. B. Tech. Dec. 2010)

Is f a group homomorphism ? Is f a ring isomorphism ?

Sol. Z and 2Z are groups under addition.

Consider $f : Z \to 2Z$ defined by $f(n) = 2n \ \forall \ n \in Z$

For $m, n \in Z$, consider

$$f(m + n) = 2(m + n)$$
$$= 2m + 2n = f(m) + f(n) \ \forall \ m, n \in Z$$

Hence $f : Z \to 2Z$ is a group homomorphism.

To check whether f is a ring homomorphism.

For $m, n \in Z$, consider $f(mn) = 2mn$

and $f(m) f(n) = 2m \cdot 2n = 4mn.$

$\therefore$ $f(mn) \neq f(m) f(n) \ \forall \ m, n \in Z$

$\therefore$ $f : Z \to 2Z$ cannot be a ring isomorphism.

Example 9. *Examine whether [2Z, +, .) and [3Z, +, .] are isomorphic rings ?*

Sol. Consider the equation $x + x = x \cdot x$ ...(1).

This equation makes sense in both rings.

For $x = 2$, (1) gives $2 + 2 = 2 \cdot 2 \Rightarrow 4 = 4$, which is true.

Thus equation (1) has a solution $x = 2 \in 2Z$.

For $x = 3$, (1) gives $3 + 3 \neq 3 \cdot 3$. This means $x = 3$ is not a solution of (1).

Hence we conclude that equation (1) has a solution in 2Z, but does not have a solution in 3Z. Therefore 2Z and 3Z cannot be isomorphic rings. (See Remark (*d*) above example 8)

Example 10. *Show that following rings are not isomorphic.*

(*i*) $[Z, +, \cdot]$ *and* $[M_{2\times2}(R), +, \cdot]$ (*ii*) $[3Z, +, \cdot]$ *and* $[4Z, +, \cdot]$

(*iii*) $[R, +, \cdot]$ *and* $[Q, +, \cdot]$ (*iv*) $[Z_2 \times Z_2, +, .]$ *and* $[Z_4, +, .]$.

Sol. (*i*) We know that Z is a commutative ring and $M_{2\times2}$ (R) is a non-commutative ring. (since for A, B $\in M_{2\times2}$ (R), AB = BA is not true)

$\therefore$ The rings $[Z, +, \cdot]$ and $[M_{2\times2}(R), +, .]$ cannot be isomorphic rings. (Remark (*a*) above example 8)

(*ii*) Consider the equation $x + x + x = x \cdot x$ ...(1)

This equation maks sense in both rings 3Z and 4Z.

For $x = 3$, (1) gives $3 + 3 + 3 = 3.3 \Rightarrow 9 = 9$, which is true.

Hence equation (1) has a solution $x = 3$ in 3Z.

For $x = 4$, (1) gives $4 + 4 + 4 \neq 4 \cdot 4$

$\Rightarrow$ $12 \neq 16$,

Hence equation (1) has does not have a solution in 4Z

Therefore, 3Z and 4Z cannot be isomorphic rings. (Remark (*d*) above example 8)

(*iii*) We know that the set of real numbers R is uncountable and the set of rationals Q is countable (see chapter on 'sets').

Hence R and Q cannot have same cardinality and therefore cannot be isomorphic.

(*iv*) By definition, $Z_2 = [0, 1, +_2, \times_2]$

$\therefore$ $Z_2 \times Z_2 = [(0, 0), (0, 1), (1, 0), (1, 1)]$

For $(m, n) \in Z_2 \times Z_2$, consider $(m, n) \,.\, (1, 1) = (m, n) = (1, 1) \,.\, (m, n)$

i.e., $(1, 1)$ is the unity (multiplicative identity) of $Z_2 \times Z_2$.

Now $Z_4 = [0, 1, 2, 3, +_4, \times_4]$

1 is the unity of Z_4.

Thus $Z_2 \times Z_2$ and Z_4 do not have same unity. Therefore they cannot be isomorphic rings.

9.9. SUBRING

(P.T.U. Dec. 2005)

Let $[R, +, \cdot]$ be a ring and S be a subset of R. Then S is called a subring of R iff S is itself a ring under the operations of R.

Theorem II. *A non-empty subset of a ring R is a subring of R iff*

(*i*) $a, b \in S \Rightarrow a - b \in S \; \forall \; a, b \in S$

(*ii*) $a, b \in S \Rightarrow ab \in S \; \forall \; a, b \in S$.

Proof. Let S be a subring of R. We prove (*i*) and (*ii*).

As S is a subring of R, S is itself a ring under the operations of R.

Hence S is additive group under +. that is, S is closed under addition. *i.e.*,

For $a, b \in S, a + b \in S \; \forall \; a, b \in S$

Also for each $b \in S$, there exists $-b \in S$ such that $-b$ is the additive inverse of b.

Now $a \in S, -b \in S \Rightarrow a + (-b) \in S$

$\Rightarrow$ $a - b \in S$, which proves (*i*)

Further, as S is a subring of R, it must be a ring under the operations of R. Thus, S is closed under multiplication *i.e.*;

For $a, b \in S \Rightarrow a \,.\, b \in S \; \forall \; a, b \in S$, which proves (*ii*)

Converse. Let (*i*) and (*ii*) hold. We show S is a subring of R under the operations of R.

For $a, a \in S \Rightarrow a - a \in S \Rightarrow 0 \in S$ | Using (*i*)

i.e., S has additive identity.

Again $0 \in S, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S$ | Using (*i*)

i.e., S has additive inverse.

For $a \in S, b \in S \Rightarrow -b \in S$ (Proved above)

From (*i*), $a - (-b) \in S$

$\Rightarrow$ $a + b \in S \quad \forall \quad a, b \in S$

i.e., S is closed under addition.

Since $S \subseteq R$, elements of S are also in R

$\therefore$ Associativity under addition holds in S

For $a, b \in S \subseteq R \Rightarrow a, b \in R$ | R is additive group

$a + b = b + a$

$\therefore$

Hence we can say that S is an additive group.

From (*ii*), $a, b \in S \Rightarrow a \,.\, b \in S \quad \forall \quad a, b \in S$

i.e., S is closed under multiplication.

Finally, $a, b, c \in S \subseteq R \Rightarrow a, b, c \in R$

$\therefore$ $a.(b+c) = a.b + a.c$

$(a+b).c = a.c + b.c$ | Distributive laws hold in R

i.e., left distributive law and right distributive law holds in S.

Hence S is a ring under the operations of R.

Example 11. *The set of integers Z is subring of Q.*

Sol. We know that "*A non-empty subset S of a ring R is a subring of R* iff (*i*) $a, b \in S \Rightarrow a - b \in S \ \forall \ a, b \in S$

(*ii*) $a, b \in S \Rightarrow a.b \in S \ \forall \ a, b \in S$.

Since $Z \subseteq Q$ *i.e.*, Z is a subset of Q.

For $a, b \in Z \Rightarrow a - b \in Z \ \forall \ a, b \in Z$ is true.

Also for $a, b \in Z \Rightarrow a.b \in Z \ \forall \ a, b \in Z$. | Theorem II

Hence Z is a subring of Q.

Example 12. (*a*) *Show that 3Z is a subring of Z.*

(*b*) *Find all subrings of* Z_8.

Sol. (*a*) We know that "*A non-empty subset S of a ring R is a subring of R* iff (*i*) $a, b \in S \Rightarrow a - b \in S \ \forall \ a, b \in S$

(*ii*) $a, b \in S \Rightarrow a.b \in S \ \forall \ a, b \in S$

Let $x, y \in 3Z \Rightarrow x = 3m, m \in Z, \ y = 3n, n \in Z$

Consider $x - y = 3m - 3n = 3(m - n) \in 3Z$

| Since $m, n \in Z \Rightarrow m - n \in Z$ (Z is a ring)
| $\Rightarrow 3(m - n) \in 3Z$

$\Rightarrow x - y \in 3Z$

Also $x.y = 3m \,.\, 3n = 3(3mn) = 3k \in 3Z$

where $k = 3\,mn$ | since 3, $m, n \in Z$ and Z is a ring $\therefore$ $3mn \in Z$ |

Hence we can say that 3Z is a subring of Z.

(*b*) Consider the following subsets of Z_8.

$Z_2 = [0, 1, +_2, \times_2]$; $Z_3 = [0, 1, 2, +_3, \times_3]$

$Z_4 = [0, 1, 2, 3, +_4, \times_4]$; $Z_5 = [0, 1, 2, 3, 4, +_5, \times_5]$

$Z_6 = [0, 1, 2, 3, 4, 5, +_6, \times_6]$; $Z_7 = [0, 1, 2, 3, 4, 5, 6, +_7, \times_7]$

For $a, b \in Z_2$, we observe that $a - b \in Z_2 \ \forall \ a, b \in Z_2$

Also $a \,.\, b \in Z_2 \ \forall \ a, b \in Z_2$

Hence Z_2 is a subring of Z_8

For $a, b \in Z_3$, we observe that $a - b \in Z_3 \ \forall \ a, b \in Z_3$

Also $a \,.\, b \in Z_3 \ \forall \ a, b \in Z_3$

Hence Z_3 is a subring of Z_8

Similarly, we can prove that Z_4, Z_5, Z_6, Z_7 are all subrings of Z_8.

9.10. UNITS

Let (R, +, .) be a ring with unity. An element $a \in R$ is said to be a unit (or invertible) if for $0 \neq a \in R$, $\exists\, b \in R$ such that $a \,.\, b = 1 = b \,.\, a$ or

An element is *a* unit if *a* has multiplicative inverse, $a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$

Consider the rings (R, + ,.) and (Q, + ,.). Every non-zero element in R (set of reals) and Q (set of rationals) has a multiplicative inverse. For example, $\frac{4}{3} \in R$ has multiplicative inverse $\frac{3}{4} \in R$ since $\frac{4}{3} \cdot \frac{3}{4} = 1$.

The only elements in Z that have multiplicative inverses are – 1 and 1.

Theorem III. *An element a in Z_n is a unit iff a and n are relatively prime.*

Proof. By definition, $Z_n = [0, 1, 2, 3, \ldots n-1, +_n, \times_n]$

Let $a \in Z_n$ be a unit. It means there exists an element $b \in Z_n$ such that $a \times_n b = 1$ *i.e.*, when ab is divided by n, the remainder is 1. *i.e.*, $a \times_n b = 1 \Rightarrow ab = nq + 1$, where q is the quotient.

$\Rightarrow ab - nq = 1$ | For $a, b \in R$, if $\exists\, x, y \in R$ such that $ax - by = 1$, then g.c.d. $(a, b) = 1$

$\Rightarrow (a, n) = 1$

Example 13. *Determine the units (those elements which have multiplicative inverses) for each of the following rings :*

(a) $[Z, +, \cdot]$ (b) $[Q, +, \cdot]$

(c) $[C, +, \cdot]$ (d) $[M_{2\times2}(R), +, \cdot]$

(e) $[Z_2, +_2, \times_2]$ (f) $[Z_6, +_6, \times_6]$

(g) $[Z_8, +_8, \times_8]$ (h) $[Z_5, +_5, \times_5]$

(i) $[Z \times Z, +, \cdot]$ (j) $[Z_2^3, +, \cdot]$.

Sol. (a) The only units of Z are – 1 and 1. Since for each $a \in Z$, $a \cdot 1 = a = 1 \cdot a$

$a \cdot (-1) = -a = (-1) \cdot a$

(b) Every non-zero element in Q has multiplicative inverse (unit)

(c) Every non-zero complex number in C has multiplicative inverse (unit)

(d) If $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_{2\times2}(R)$, then for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times2}(R)$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Hence $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unit of $M_{2\times2}(R)$.

(e) $Z_2 = [0, 1, +_2, \times_2]$

For each $x \in Z_2$, we have $x \times_2 1 = x = 1 \times_2 x$

$\therefore$ The only unit of Z_2 is 1.

(f) $Z_6 = [0, 1, 2, 3, 4, 5, +_6, \times_6]$

The only elements in Z_6 which are relatively prime to 6 are 1 and 5.

($\because$ (1, 6) = 1, (5, 6) = 1

Hence the units of Z_6 are 1 and 5.

Also $1 \times_6 1 = 1, 5 \times_6 5 = 1$

(g) $Z_8 = [0, 1, 2, 3, 4, 5, 6, 7, +_8, \times_8]$ | Theorem III

The only units of Z_8 are those elements which are relative prime to 8.

Consider the rings (R, + ,.) and (Q, + ,.). Every non-zero element in R (set of reals) and Q (set of rationals) has a multiplicative inverse. For example, $\frac{4}{3} \in R$ has multiplicative inverse $\frac{3}{4} \in R$ since $\frac{4}{3} \cdot \frac{3}{4} = 1$.

The only elements in Z that have multiplicative inverses are – 1 and 1.

Theorem III. *An element a in Z_n is a unit iff a and n are relatively prime.*

Proof. By definition, $Z_n = [0, 1, 2, 3, \ldots n-1, +_n, \times_n]$

Let $a \in Z_n$ be a unit. It means there exists an element $b \in Z_n$ such that $a \times_n b = 1$ *i.e.,* when ab is divided by n, the remainder is 1. *i.e.,* $a \times_n b = 1 \Rightarrow ab = nq + 1$, where q is the quotient.

$\Rightarrow ab - nq = 1$ | For $a, b \in R$, if $\exists\, x, y \in R$ such that $ax - by = 1$, then g.c.d. $(a, b) = 1$

$\Rightarrow (a, n) = 1$

Example 13. *Determine the units (those elements which have multiplicative inverses) for each of the following rings :*

(a) $[Z, +, \cdot]$
(b) $[Q, +, \cdot]$
(c) $[C, +, \cdot]$
(d) $[M_{2\times2}(R), +, \cdot]$
(e) $[Z_2, +_2, \times_2]$
(f) $[Z_6, +_6, \times_6]$
(g) $[Z_8, +_8, \times_8]$
(h) $[Z_5, +_5, \times_5]$
(i) $[Z \times Z, +, \cdot]$
(j) $[Z_2^3, +, \cdot]$.

Sol. (a) The only units of Z are – 1 and 1. Since for each $a \in Z$, $a.1 = a = 1.a$

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

(b) Every non-zero element in Q has multiplicative inverse (unit)

(c) Every non-zero complex number in C has multiplicative inverse (unit)

(d) If $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_{2\times2}(R)$, then for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times2}(R)$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Hence $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unit of $M_{2\times2}(R)$.

(e) $Z_2 = [0, 1, +_2, \times_2]$

For each $x \in Z_2$, we have $x \times_2 1 = x = 1 \times_2 x$

$\therefore$ The only unit of Z_2 is 1.

(f) $Z_6 = [0, 1, 2, 3, 4, 5, +_6, \times_6]$

The only elements in Z_6 which are relatively prime to 6 are 1 and 5.

($\because$ (1, 6) = 1, (5, 6) = 1

Hence the units of Z_6 are 1 and 5.

Also $1 \times_6 1 = 1, 5 \times_6 5 = 1$ | Theorem III

(g) $Z_8 = [0, 1, 2, 3, 4, 5, 6, 7, +_8, \times_8]$

The only units of Z_8 are those elements which are relative prime to 8.

The elements relative prime to 8 are 2, 3, 5, 7.

Hence the units of Z_8 are [1, 3, 5, 7].

(*h*) $Z_5 = [0, 1, 2, 3, 4, +_5, \times_5]$

The only units of Z_5 are those elements which are relative prime to 5. The elements relative prime to 5 are 1, 2, 3, 4.

Hence the units of Z_5 are [1, 2, 3, 4].

(*i*) The units of Z are 1 and – 1. Therefore units of Z × Z are

(1, 1) (1, – 1), (– 1, 1), (– 1, – 1).

(*j*) $Z_2^3 = Z_2 \times Z_2 \times Z_2$ where $Z_2 = [0, 1, +_2, \times_2]$

The only unit of Z_2 is 1. Therefore the only unit of Z_2^3 is (1, 1, 1).

Theorem IV. *For all* $a, b \in R$,

(*i*) $a.0 = 0.a = 0$ (*ii*) $a.(-b) = (-a).b = -a.b$

(*iii*) $(-a) . (-b) = a.b$ (P.T.U. B.Tech. May 2012)

(*iv*) *If R has a unit element 1, then* $(-1) . a = -a$, $(-1) . (-1) = 1$.

Proof. (*i*) For $a \in$ R, consider

$$a . 0 = a . (0 + 0)$$ | 0 is the identity

$$= a . 0 + a . 0$$ | Left distribution law

$$\Rightarrow \quad a.0 + (-a) . 0 = a.0 + a.0 + (-a) . 0$$

$$\Rightarrow \quad (a + (-a)) . 0 = a.0 + (a + (-a)) . 0$$ | Right distributive law

$$\Rightarrow \quad 0 = a . 0 + 0$$

$$\Rightarrow \quad 0 = a. 0$$

Similarly, $0 = 0 . a$ (Try yourself)

(*ii*) Consider $a . (b + (-b)) = a.0 = 0$ | by part (*i*)

$$\Rightarrow \quad a.b + a.(-b) = 0$$ | Left distributive law

$$\Rightarrow \quad a. (-b) = -a.b$$

Similarly, $(-a) . b = -a.b$ (Try yourself)

(*iii*) $(-a) . (-b) = -(a . (-b))$

$$= -(-(a . b))$$ | by part (*ii*)

$$= a . b$$

(*iv*) If R has a unit element 1, then

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

$$= (1 + (-1)) . a$$ | Left distributive law

$$= 0 . a = 0$$ | by part (*i*)

$$\Rightarrow \quad (-1) . a = -a$$

In particular, if $a = -1$, then

$$(-1) . (-1) = -(-1) = 1.$$

9.11. INTEGRAL DOMAIN

Zero divisor

A non-zero element $a \in R$ is called a zero divisor if there exists a non-zero element $b \in R$ such that $ab = 0$

A commutative ring R is called an integral domain if for every

$$0 \neq a, b \in R, ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Thus, a commutative ring R is called an integral domain if R has no zero divisor.

Theorem V. *The element m in the ring $[Z_n, +_n, \times_n]$ is a zero divisor iff m is not relative prime to n (i.e.; g.c.d. $(m, n) \neq 1$).*

Proof. The proof of above theorem is beyond the scope of this book.

Theorem VI. *$(Z_p, +_p, \times_p]$ has no zero divisors iff p is a prime number.*

Proof. Let Z_p has no zero divisors. We show p is prime.

For if, $p = ab$, $\quad 1 < a < p, 1 < b < p$

$\Rightarrow \quad a \times_p b = 0$ where a, b are non-zero numbers

$\Rightarrow$ Z_p has a zero divisor, a contradiction, hence p is prime.

Converse. Let p is prime, we show Z_p has no zero divisor. Let $a \times_p b = 0$ for $a, b \in Z_p$

$\Rightarrow \quad ab \equiv 0 \pmod{p} \Rightarrow p/ab \Rightarrow p/a$ or p/b | p is prime

But $a, b \in Z_p \quad \therefore \quad a, b < p.$

Hence $\quad a = 0$ or $b = 0$

$\therefore$ Z_p has no zero divisor.

Example 14. *Consider $(Z_8, +_8, \times_8)$. Find the zero divisors of Z_8. Is Z_8 an integral domain ?*

Sol. $Z_8 = [0, 1, 2, 3, 4, 5, 6, 7].$

Since $4 \times_8 2 = 0 = 2 \times_8 4$

$\therefore$ 2 and 4 are zero divisors.

Also $4 \times_8 6 = 0 = 6 \times_8 4$

$\therefore$ 4 and 6 are zero divisors.

Z_8 cannot be an integral domain since $0 \neq 2, 4 \in Z_8 \Rightarrow 2 \times_8 4 = 0$ *i.e.*, Z_8 is a ring with zero divisors.

Example 15. *Show that Z, the set of integers is an integral domain.*

Sol. We know that Z is a commutative ring. Also if $a, b \in Z$ then, gives $a \cdot b = 0$

either $a = 0$ or $b = 0$

$\therefore$ Z is a commutative ring without zero divisors *i.e.*, Z is an integral domain.

Example 16. *Consider* $m = \left[\begin{pmatrix} a & b \\ c & a \end{pmatrix} a, b, c, d \in R\right]$ *as a ring under matrix addition and matrix multiplication. Show that* $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *are zero divisors.*

Sol. Given $\quad A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq 0, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$

But $$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = O$$

$\therefore$ A and B are zero divisors.

Example 17. *Show that the ring Z_{29} of integers modulo 29 is an integral domain.*

Sol. By using theorem VI, Z_p has no zero divisors iff p is prime. Here $p = 29$, which is a prime. Therefore, Z_{29} has no zero divisors. Consequently, Z_{29} is an integral domain.

Example 18. *Show that the ring Z_{105} of the integers modulo 105 is not an integral domain.*

Sol. By using theorem VI, Z_p has no zero divisors iff p is prime. Here $p = 105$, which is a composite number. Consequently, Z_{105} has zero divisors.

$\therefore$ Z_{105} cannot be an integral domain.

Theorem VII. *The cancellation laws hold in a ring $(R, +, .)$ iff R has no zero divisors.*

Or

A commutative ring R is an integral domain iff for $a, b, c \in R$ $(0 \neq a)$

$$ab = ac \Rightarrow b = c.$$

Proof. Let R be an integral domain and consider $ab = ac$ $(0 \neq a)$

$\Rightarrow$ $ab - ac = 0$

$\Rightarrow$ $a.(b - c) = 0$ | Left distribution law

$\Rightarrow$ either $a = 0$ or $b - c = 0$ | Since R is an integral domain, so it has no zero divisors

$\Rightarrow$ $b - c = 0$ | $a \neq 0$

$\Rightarrow$ $b = c.$

Converse. Let cancellation laws hold in R. We show R is an integral domain.

Let $a, b \in R$ and $0 \neq a$. Consider

$$a \,.\, b = 0$$

$\Rightarrow$ $a \,.\, b = a \,.\, 0$

$\Rightarrow$ $b = 0$ | $a \,.\, 0 = 0$

Hence R is an integral domain. | Cancellation law

Example 19. *Consider $X = [0, 2, 4, 6, 8, +_{10}, \times_{10}]$. Is X an integral domain ? Justify your answer.*

Sol. We first check whether X is a commutative ring under addition modulo 10 and multiplication modulo 10. The addition modulo 10 table is shown in Table I.

Table I

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

From Table I, we observe that every element inside the table is also in X. It means that X is closed under addition modulo 10. *i.e.*,

$$a, b \in X \Rightarrow a +_{10} b \in X \ \forall a, b \in X$$

Addition modulo 10 is associative *i.e.*,

For $a, b, c \in X$, $a +_{10} (b +_{10} c) = (a +_{10} b) +_{10} c \ \forall \ a, b, c \in X$

The first row inside the table coincides with the topmost row of the Table I. It means 0 is the additive identity of X.

Also each element of X has an additive inverse. For example

Inverse of 2 is 8 (the intersection of 2 and 8 at zero) | $2 +_{10} 8 = 0$

Inverse of 4 is 6 etc. | $4 +_{10} 6 = 0$

Table I is symmetrical w.r.t. $+_{10}$. It means $a +_{10} b = b +_{10} a \ \forall \ a, b \in X$.

Hence X is an additive group under $+_{10}$.

Now consider the multiplication modulo 10 table as shown in Table II.

Table II

$\times_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

From Table II, we observe that each element inside the table is also in X. It means that X is closed under multiplication modulo 10 *i.e.*,

For $a, b \in X$, $a \times_{10} b \in X \ \forall \ a, b \in X$

Multiplication modulo 10 is associative. Also for $a, b, c \in X$,

$a \times_{10} (b +_{10} c) = a \times_{10} b +_{10} a \times_{10} c$ | Left distributive law

$(a +_{10} b) \times_{10} c = a \times_{10} c +_{10} a \times_{10} c \ \forall \ a, b, c \in X$ | Right distributive law

Hence X is a ring under addition modulo 10 and multiplication modulo 10.

Now to check commutativity of X, from Table II, we observe that the table is symmetrical w.r.t. $\times_{10}$. It means X is a commutative ring.

Finally, X is a ring without zero divisors as it is clear from Tabe II, *i.e.*, there do not exist non-zero elements whose product is zero.

Hence $(X, +_{10}, \times_{10})$ is an integral domain.

Example 20. *Consider $X = [0, 1, 2, 3, 4, 5, +_6, \times_6]$. Is X an integral domain ? Justify your answer.*

Sol. Proceeding as in example 4, we can prove that X is a commutative ring.

Also $2, 3 \in X$ and $2 \times_6 3 = 0$ *i.e.*, product of two non-zero elements in X is a zero element. Thus, X is a commutative ring with zero divisors. So X cannot be an integral domain.

Example 21. *(i) Give an example of a finite integral domain*

(ii) Give an example of an infinite integral domain ?

(iii) Give counter example to illustrate the fact that product of two integral domain may not be an integral domain ?

Sol. (*i*) We know that Z_p is an integral domain iff p is prime. Thus $Z_2 = [0, 1, +_2, \times_2]$, $Z_3 = [0, 1, 2, +_3, \times_3]$ are finite integral domain.

(*ii*) Z, the set of integers is an example of an infinite integral domain.

(*iii*) Consider $Z_2 = [0, 1, +_2, \times_2]$; $Z_3 = [0, 1, 2, +_3, \times_3]$

Clearly, Z_2 and Z_3 are integral domains as 2 and 3 are primes.

Consider the product $Z_2 \times Z_3$. We know that Z_2 and Z_3 are commutative rings with unity so their product $Z_2 \times Z_3$ is also a commutative ring with unity.

But $(1, 0), (0, 2) \in Z_2 \times Z_3$ are two non-zero elements and $(1, 0) \cdot (0, 2) = (0, 0)$. *i.e.*, $Z_2 \times Z_3$ has zero divisors and hence cannot be an integral domain.

Example 22. *Find all zero divisors of Z_{15}, Z_6, Z_{20}.*

Sol. (*i*) $Z_{15} = [0, 1, 2, \ldots\ldots 14, +_{15}, \times_{15}]$

We know that an element m, in $[Z_n, +_n, \times_n]$ is a zero divisor iff m is not relative prime to n.

Here $n = 15$. The only elements which are not relative prime to 15 are 3, 5, 6, 9, 10, 12.

Hence 3, 5, 6, 9, 10, 12, are zero divisors.

Also $3 \times_{15} 5 = 0$, $9 \times_{15} 10 = 0$, $5 \times_{15} 6 = 0$ $10 \times_{15} 12 = 0$ etc.

(*ii*) $Z_6 = [0, 1, 2, 3, 4, 5, +_6, \times_6]$

The only elements which are not relative prime to 6 are 2, 3, 4

$\therefore$ The zero divisors of Z_6 are 2, 3, 4

Also $2 \times_6 3 = 0$, $3 \times_6 4 = 0$ etc.

(*iii*) $Z_{20} = [0, 1, 2, 3, \ldots\ldots 19, +_{20}, \times_{20}]$

The only elements which are not relative prime to 20 are 2, 4, 5, 6, 8, 10, 12, 14, 16, 18.

Hence the zero divisors of Z_{20} are 2, 4, 5, 6, 8, 10, 12, 14, 16, 18.

Example 23. *Consider the ring $Z_{10} = \{0, 1, 2, 3, \ldots\ldots, 9\}$ of integers modulo 10.*

(*a*) *Find the unit of Z_{10}*

(*b*) *Find $-3, -8, 3^{-1}$*

(*c*) *Let $f(x) = 2x^2 + 4x + 4$. Find the roots of $f(x)$ over Z_{10}. By finding roots of $f(x)$, Conclude that can a polynomial of degree n have more than n roots ?*

Sol. (*a*) The units of Z_{10} are those integers which are relatively prime to 10. Clearly, the units of Z_{10} are 1, 3, 7, 9.

(*b*) By $-a$ in a ring, we mean that element such that $a + (-a) = 0 = (-a) + a$. Therefore,

$-3 = 7$ (Since $3 + 7 = 0 = 7 + 3$)

Also, $-8 = 2$ (Since $8 + 2 = 0 = 2 + 8$)

By a^{-1} in a ring, we mean that element such that $a \cdot a^{-1} = 1 = a^{-1} a$

Therefore, $3^{-1} = 7$ (Since $3.7 = 1 = 7.3$)

(*c*) The roots of $f(x)$ will be those elements from 0 to 9 which will yield 0.

Put, $x = 0$, $f(0) = 4$,

$x = 1$, $f(1) = 2 + 4 + 4 = 10$

$x = 2$, $f(2) = 8 + 8 + 4 = 20 = 0$

$x = 3$, $f(3) = 4$,

$x = 4$, $f(4) = 2$, $f(5) = 4$, $f(6) = 0$, $f(7) = 0$, $f(8) = 4$, $f(9) = 2$

Thus, $f(1) = 0$, $f(2) = 0$, $f(6) = 0$, $f(7) = 0$

Hence, the roots of $f(x)$ are 1, 2, 6, 7.

Conclusion. This example shows that a polynomial of degree n can have more than n roots over an arbitrary ring. But this cannot happen if the ring is a field.

TEST YOUR KNOWLEDGE 9.1

1. Consider the following sets. The operations involved are the usual operations defined on the sets.
   (a) $[Z, +, \cdot]$ (b) $[Q, +, \cdot]$ (c) $[C, +, \cdot]$
   (d) $[M_{2\times2}(R), +, \cdot]$ (e) $[Z_2, +_2, \times_2]$ (f) $[Z_6, +_6, \times_6]$
   (g) $[Z_8, +_8, \times_8]$ (h) $[Z_5, +_5, \times_5]$ (i) $[Z \times Z, +, \cdot]$
   (j) $[Z_2^3, +, \cdot]$
   (i) Which of the above sets are rings ?
   (ii) Which of the above rings are commutative ? Are they rings with unity? Determine the unity of the above rings.
2. Perform the indicated operations on the $[Z_8; +_8, \times_8]$:
   (i) $2 \times_8 (-4)$ (ii) $(-3) \times_8 5$
   (iii) $(-2) \times_8 (-4)$ (iv) $(-3) \times_8 5 +_8 (-3) \times_8 (-5)$
3. (a) Determine all solutions of the equation $x^2 - 5x + 6 = 0$ in Z_{12}. Find all elements of Z_{12} which satisfy this equation.
   (b) Find all solutions of the equation $x^2 - 5x + 6 = 0$ in Z. Can there be any more than two solutions to this equations in Z ?
4. Solve the equation $x^2 - 4x + 4 = 0$
   (a) in Z_{12} (b) in Z
   (c) in $M_{2\times2}(R)$ (d) in Z_3.
5. For any ring $[R; +, \cdot]$, simplify
   (i) $(a + b)(c + d)$ for $a, b, c, d \in R$
   (ii) If R is commutative, show that $(a + b)^2 = a^2 + 2ab + b^2 \ \forall\ a, b \in R$
   (iii) Simplify $(a + b)^5$ in Z_5.
6. Consider the ring $Z_{10} = [0, 1, 2, 3, \ldots\ldots 9]$ of integers modulo 10.
   (a) Find the units of Z_{10} *(P.T.U. B.Tech. May 2008)*
   (b) Find $-3, -8$ and 3^{-1}
   (c) Let $f(x) = 2x^2 + 4x + 4$. Find the roots of $f(x)$ over Z_{10} *(P.T.U. B.Tech. May 2008)*
7. Consider $Z_{30} = [0, 1, 2, \ldots\ldots 29, +_{30}, \times_{30}]$
   (a) Find $-2, -7$ and -11 (b) Find 7^{-1}, 11^{-1} and 26^{-1}.
8. Suppose $a^2 = a$ for every $a \in R$ (such a ring is called a *Boolean ring*.) Prove that R is commutative given that $x + y = 0 \Rightarrow x = y$ for all $x, y \in R$. *(P.T.U. B.Tech. May 2009)*
9. Let G be any additive group. Define a multiplication in G by $a.b = 0$ for every $a, b \in G$. Show that this makes G into a ring.
10. Let R be a ring with a unity element. Show that R*, the set of units in R is a group under multiplication.
11. Prove that if $x^2 = 1$ in an integral domain D, then $x = 0$ or $x = 1$.
12. If R is a ring with unity, then this unity is unique.
13. Prove that the ring $Z_2 \times Z_3$ is commutative and has unity.

Answers

1. (*i*) All are rings
(*ii*) except (*d*), all rings are commutative. The unity for (*a*), (*b*), (*c*), (*e*), (*f*), (*g*), (*h*) is 1.
The unity for (*d*) is $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The unity for (*i*) is (1, 1). The unity for (*j*) is (1, 1, 1).

2. (*i*) 0 (*ii*) 1 (*iii*) 0 (*iv*) 0.

3. (*a*) $x = 2, 3$, $x = 2, 3, 6, 11$ (*b*) $x = 2, 3$, No

4. (*a*) $x = 4, 10$ (*b*) $x = -2$ (*c*) Any 2×2 matrix satisfying $(X + 2I)^2 = 0$
(*d*) $x = 1$ 5. (*c*) $(a + b)^5 = a^5 + b^5$ 6. (*a*) 1, 3, 7, 9
(*b*) $-3 = 7, -8 = 2, 3^{-1} = 7$ (*c*) 1, 2, 6, 7.

7. (*a*) $-2 = 28, -7 = 23, -11 = 19$
(*b*) $7^{-1} = 13$, $11^{-1} = 11$, 26^{-1} does not exist since 26 is not a unit.

Hints

2. By $-a$ in a ring R, we mean that element, say, a, such that $a + (-a) = 0 = (-a) + a$
$\therefore \quad -4 = 4, -3 = 5$ etc.

3. (*b*) $Z_{12} = [0, 1, 2, 3, \ldots\ldots 11, +_{12}, \times_{12}]$
If $x = 6$, then $x^2 - 5x + 6 = 36 - 30 + 6 = 12 = 0$
If $x = 11$, then $x^2 - 5x + 6 = 121 - 55 + 6 = 72 = 0$

4. (*a*) $x^2 + 4x + 4 = 0 \Rightarrow (x + 2)(x + 2) \Rightarrow x = -2, -2$. But $-2 = 10$
Also if $x = 4$, then $x^2 + 4x + 4 = 16 + 16 + 4 = 36 = 0$
(*d*) $-2 = 1 \quad \therefore \quad x = 1$ is the only solution.

5. (*i*) $(a + b)(c + d) = a.(c + d) + b.(c + d) = a.c + a.d + b.c + b.d$ | Left distributive law

(*ii*) $(a + b)^2 = (a + b)(a + b) = a.(a + b) + b(a + b)$
$= a.a + a.b + b.a + b.b = a^2 + a.b + b.a + b^2$
$= a^2 + a.b + a.b + b^2\ a^2 + 2a.b + b^2$ | R is commutative
$= a^2 + 2a.b + b^2$

(*iii*) $(a + b)^5 = 5c_0\ a^5 + 5c_1\ a^4b + 5c_2\ a^3b^2 + 5c_3\ a^2b^3 + 5c_4\ ab^4 + 5c_5b^5$
$= a^5 + 5a^4b + 10a^3b^2 + 5ab^4 + b^5$
$= a^5 + b^5$ | In Z_5, $5 = 0$, $10 = 0$ etc.

8. Given $a^2 = a$ for all $a \in R$ ...(1)
Let $a, b \in R$. Since R is a ring, it is closed under addition. $\therefore \quad a + b \in R$
Using (1), $(a + b)^2 = a + b$
$\Rightarrow \quad (a + b)(a + b) = a + b$
$\Rightarrow \quad (a + b).a + (a + b).b = a + b$ | Right distributive law
$\Rightarrow \quad a.a + b.a + a.b + b.b = a + b$
$\Rightarrow \quad a + b.a + a.b + b = a + b$ | $a.a = a^2 = a$
$\Rightarrow \quad b.a + a.b + b = b$ | Left cancellation law
$\Rightarrow \quad b.a + a.b = 0$ | Right cancellation law
$\Rightarrow \quad a.b = b.a$ | $\because$ If $x + y = 0 \Rightarrow x = y$

9. Given (G, +) is an additive group. Also $a.b = 0 \in G\ \forall\ a, b \in G \therefore$ G is closed under multiplication.
For $a, b, c \in G$, $a.(b.c) = a.0 = 0$ ...(1)

Also $(a.b) \,.\, c = 0.c = 0$ ...(2)

From (1) and (2), $a.(b.c) = (a.b) \,.\, c \;\forall\; a, b, c \in G$ $\quad | \; b, c \in G \Rightarrow b.c = 0$

$\therefore$ Associativity holds in G.

Also $a.(b + c) = a.b + a.c = 0 + 0 = 0$

$\Rightarrow$ $a.b + a.c = 0 + 0 = 0$ $\quad | \; a, c \in G \Rightarrow a.c = 0$

$\therefore$ $a.(b + c) = a.b + a.c$

Similarly, $(a + b) \,.\, c = a.c + b.c$

$\therefore$ (G, +,.) is a ring.

10. Let R* be the set of units in R. We show R* is a group under multiplication. Let $a, b \in R^*$ *i.e.*, a and b are units in R $\Rightarrow$ there exist a^{-1}, $b^{-1} \in$ R such that $aa^{-1} = 1 = a^{-1}a$ and $bb^{-1} = 1 = b^{-1}b$

Consider $(ab)\,(b^{-1}a^{-1}) = a(bb^{-1})\,a^{-1} = a \,.\, 1 \,.\, a^{-1} = aa^{-1} = 1$

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

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

Hence ab is also a unit in R. Consequently $ab \in R^*$ *i.e.*, R* is closed under multiplication.

Since R is associative and elements of R* are from R

$\therefore$ R* is associative under multiplication. Finally, if a is a unit in R, then a^{-1} is also a unit in R. Consequently $a^{-1} \in R^*$. Hence R* is a group under multiplication.

9.12. FIELD

(P.T.U. B.Tech. Dec. 2009)

A commutative ring F with unity such that each non-zero element has a multiplicative inversy is called a field. It is denoted by F. Alternatively, F is a field if its non-zero elements form a group under multiplication.

ILLUSTRATIVE EXAMPLES

Example 1. *Show that the following sets are fields.*

(i) $[Q; +, \cdot]$ *(ii)* $[R; +, \cdot]$ *(iii)* $[C; +, \cdot]$.

Sol. *(i), (ii), (iii).* We know that the sets Q, R and C and commutative ring with unity (see prob. 1. Exercise 9.1). Also each non-zero element in Q, R and C has multiplicatve inverse. Hence they form fields.

Example 2. *Consider the set M of all 2 × 2 matrices of the type* $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ *where* $\bar{a}$, $\bar{b}$ *are the conjugates of a and b. Is M a field ? Justify your answer.*

Sol. Consider A, B $\in$ M where $A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

Then $$AB = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 1 & 5 \end{pmatrix}$$

Also $$BA = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 1 & -1 \end{pmatrix} \neq AB$$

Hence M is not commutative and therefore cannot be field.

Example 3. *Consider* $Z_7 = [0, 1, 2, 3, \ldots\ldots 6, +_7, \times_7]$. *Show that* Z_7 *is a field.*

Sol. Consider the addition modulo 7 table as shown in Table I.

Table I

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

We first show that Z_7 is a ring under addition modulo 7 and multiplication modulo 7.

From Table I, we observe that each element inside the table is also in Z_7. It means that Z is closed under $+_7$.

Addition modulo is always associative

The first row inside the table coincides with the top most row of Table I. It means 0 is the additive identity.

Each element of Z_7 has additive inverse.

For example, Inverse of 1 is 6. Inverse of 2 is 5 etc. $\quad 1 +_7 6 = 7 = 0$

$2 +_7 5 = 7 = 0$

Also Table I is symmetrical w.r.t. $+_7$. It means Z_7 is additive w.r.t. $+_7$ *i.e.*,

For $\quad a, b \in Z_7,\ a +_7 b = b +_7 a \ \forall\ a, b \in Z_7$.

$\therefore$ Z_7 is an additive group w.r.t $+_7$.

Now consider the multiplication modulo 7 table as shown in Table II.

Table II

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

From Table II, we observe that each element inside the table is also in Z_7. It means Z_7 is closed w.r.t. $\times_7$. *i.e.*, for $a, b \in Z_7 \implies a \times_7 b \in Z_7\ \forall\ a, b \in Z_7$

Finally, For $a, b, c \in Z_7$,

$a \times_7 (b +_7 c) = a \times_7 b +_7 a \times_7 c$

$(a +_7 b) \times_7 c = a \times_7 c +_7 6 \times_7 c$ is true for all $a, b, c \in Z_7$.

Hence Z_7 is a ring w.r.t. addition modulo 7 and multiplication modulo 7.

Also the Table II is symmetrical w.r.t. $\times_7$. It means that Z_7 is commutative *i.e.*,

$$a \times_7 b = b \times_7 a \ \forall\ a, b \in Z_7$$

Further, the second row inside the table coincides with the topmost row of Table II. It means 1 is the multiplicative identity of Z_7.

Hence, we have shown that Z_7 is a commutative ring with unity. To show Z_7 is a field, we show each non-zero element of Z_7 has multiplicative inverse.

The units of Z_7 are those elements which are relative primes to 7. (See Topic on 'units')

The elements which are prime to 7 are 1, 2, 3, 4, 5, 6. Hence the units of Z_7 are 1, 2, 3, 4, 5, 6. We can also check the elements which are units as below :

$$1 \times_7 1 = 1;\ 2 \times_7 4 = 1;\ 3 \times_7 5 = 1;$$
$$4 \times_7 2 = 1;\ 5 \times_7 3 = 1;\ 6 \times_7 6 = 1.$$

Hence, each non-zero element of Z_7 has multiplicative inverse. Therefore Z_7 is a field.

9.13. GAUSSIAN INTEGERS

Any number of the form $a + ib$, $a, b \in Z$ is called a Gaussian integer.

Example 4. *Show that the set J[i] of Gaussian integers form a ring under addition and multiplication. Is it an integral domain ? Is it field ?*

Sol. Let $X = [a + ib, a, b \in Z]$ be the set of Gaussian integers. Then X is a ring.

We check X for integral domain.

Let $a + ib, c + id \in X$ such that a, b, c, d are non-zero integers.

Consider $(a + ib)(c + id) = 0$

$$\Rightarrow \quad ac - bd + i(ad + bc) = 0 = 0 + 0i$$
$$\Rightarrow \quad ac - bd = 0, \quad ad + bc = 0,$$

which is possible if either $a = 0 = b$ or $c = 0 = d$ *i.e.*, if either $a + ib = 0$ or $c + id = 0$

Hence X is without zero divisor. Therefore, X is an integral domain.

Further, if $0 \neq a + ib \in X$ be any non-zero element of X where $a, b \in Z$, then the multiplicative inverse of $a + ib$ is

$$\frac{1}{a+ib} = \frac{1}{a+ib} \times \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - i\,\frac{b}{a^2+b^2} \notin J[i]$$

Since $\dfrac{a}{a^2+b^2}$ is not necessary an integer.

$\therefore$ X cannot be a field.

Example 5. *The set of numbers of the form $[a + b\sqrt{2}, a, b \in Q]$ is a field.*

Sol. Let $X = [a + b\sqrt{2}; a, b \in Q]$. We show X is a ring.

Let $x, y \in X \Rightarrow x = a_1 + b_1\sqrt{2}, a_1, b_1 \in Q$

$$y = a_2 + b_2\sqrt{2}, a_2, b_2 \in Q$$

$$\Rightarrow \quad x + y = a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = a_1 + a_2 + (b_1 + b_2)\sqrt{2} \in X$$

$$\because \ a_1, a_2 \in Q \Rightarrow a_1 + a_2 \in Q$$

i.e., X is closed under addition.

Addition of rationals is associative.

(c)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition Table

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication Table

a	a^{-1}
1	4
2	3
3	2
4	1

Inverse (additive) Table

2. (a) $x = 1$ (b) $x = 1$ (c) $x = 1$ (d) None.
3. (a) 0 (over Z_2), 1 (over Z_3), 3(over Z_5) (b) 2(over Z_3), 3(over Z_5) (c) 2(over Z_5)
4.

$+_2$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

$\times_2$	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)
(1, 0)	(0, 0)	(0, 0)	(1, 0)	(1, 0)
(1, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)

Z_2^2 is a ring.

Z_2^2 is not an integral domain. Since (1, 0), (0, 1) $\in Z_2^2$ be any two non-zero elements and $\therefore$ (1, 0) . (0, 1) = (0, 0) *i.e.*, Z_2^2 is a ring with zero divisors.

Z_2^2 can not be a field. For if, Z_2^2 is a field, it must be an integral domain, which is not so.

9.14. IDEALS

Left Ideal. A non-empty subset I of a ring R is called a left ideal of R if

(*i*) For $a, b \in I \Rightarrow a - b \in I \; \forall \; a, b \in I$

(*ii*) For $a \in I, r \in R \Rightarrow ra \in I$

Right Ideal. A non-empty subset J of a ring R is called a right ideal of R if

(*i*) For $a, b \in J \Rightarrow a - b \in J \; \forall \; a, b \in J$

(*ii*) For $a \in J, r \in R \Rightarrow ar \in J$.

Ideal. A non-empty set K of a ring R is called an ideal (or two sided ideal) of R iff K is both left ideal and right ideal of R *i.e.*,

(*i*) For $a, b \in K \Rightarrow a - b \in K \; \forall a, b \in K$

(*ii*) For $a \in K, r \in R \Rightarrow ra \in K, ar \in K$.

Proper and Improper Ideals. *(P.T.U. B.Tech. Dec. 2007)*

Every ideal other than <0> and R are known as proper ideals. The ideals <0> and R are improper ideals of R.

ILLUSTRATIVE EXAMPLES

Example 1. *Show that {0} is an ideal in any ring R.* (P.T.U. B.Tech May 2010)

Sol. Let $0 \in \{0\}$ and consider $0 - 0 = 0 \in \{0\}$

For $r \in R$, $r \cdot 0 = 0 \in \{0\}$

$0 \cdot r = 0 \in \{0\}$

$\therefore$ {0} is an ideal of R.

Example 2. *Let M be the ring of real 2 × 2 matrices. Give an example of a left ideal, which is not a right ideal and an example of a right ideal, which is not a left ideal.*

Sol. Consider $L = \left\{\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in R\right\}$

Let A, B ∈ L such that $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, $B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix}$, where $a, b, c, d \in R$

Consider $A - B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a-c \\ 0 & b-d \end{pmatrix} \in L \quad \forall \; a, b, c, d \in R$

Let R ∈ M be any matrix over reals such that

$$R = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \alpha, \beta, \gamma, \delta \in R$$

Consider $RA = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & \alpha a + \beta b \\ 0 & \gamma a + \delta b \end{pmatrix} \in L$

But $AR = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\gamma & a\delta \\ b\gamma & b\delta \end{pmatrix} \in L$

Hence L is a left ideal, but not a right ideal of M

If we take $K = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in R\right\}$, then we can show that K is a right ideal, but not a left ideal of M.

Example 3. *The set of even integers is an ideal of Z.*

Sol. Consider E, the set of even integers given by $E = [2m : m \in Z]$

Let $a, b \in E \Rightarrow a = 2m, m \in Z, b = 2n, n \in Z$

$\therefore$ $a - b = 2m - 2n = 2(m - n) \in E$ $\quad | \because \; m, n \in Z \Rightarrow m - n \in Z$

For $r \in Z$, consider

$ra = r(2m) = 2(rm) \in E$

$ar = (2m)\, r = 2(mr) \in E$

$| \; m \in Z, r \in Z \Rightarrow rm \in Z$

Similarly, $mr \in Z$

Hence E is an ideal of Z.

Example 4. *Let M be a ring of 2 × 2 matrices over integers. Consider the set* $L = \left[\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in Z\right]$. *Show that L is a left ideal of M. Is L right ideal of M?* (P.T.U. B. Tech. Dec. 2010)

Sol. Since $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in L \Rightarrow L \neq \phi$ *i.e.*, L is non-empty set of M.

Let $A, B \in L \Rightarrow A = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}; a, b \in Z; B = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}; c, d \in Z$

$$A - B = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in L$$

$a, c \in Z \Rightarrow a - c \in Z$

$b, d \in Z \Rightarrow b - d \in Z$

For $\alpha, \beta, \gamma, \delta \in Z$, Let $R = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M$ and consider

$$RA = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b & 0 \\ \gamma a + \delta b & 0 \end{pmatrix} \in L$$

$\because \alpha, \beta, a, b \in Z \Rightarrow \alpha a + \beta b \in Z$

$\gamma, \delta, a, b \in Z \Rightarrow \gamma a + \delta b \in Z$

Hence L is a left ideal of M. Also

$$AR = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta \\ b\alpha & b\beta \end{pmatrix} \notin L$$

$\therefore$ L is not a right ideal of M.

Example 5. *Every ideal of a ring R is a subring of R. But the converse is not true.*

Sol. Let K be an ideal of R, then we have

For $a, b \in K \Rightarrow a - b \in K \; \forall \; a, b \in K$

For $r \in R$, $ra \in K$, $ar \in K$ ...(1)

We show K is a subring of R. *i.e.*, ...(2)

We show (*i*) for $a, b \in K \Rightarrow a - b \in K \; \forall \; a, b \in K$

(*ii*) for $a, b \in K \Rightarrow a \,.\, b \in K \; \forall \; a, b \in K$ ...(3)

Now (3) is trivial by using (1). To show (4), ...(4)

Let $b \in K \subseteq R \Rightarrow b \in R$. Since K is an ideal of R and $a \in K$, we have

$ab \in K$

Hence K is a subring of R. | Using (2))

Consider Z, the set of integers and Q, the set of rationals. We know that Z is a subring of Q. We show Z is not an ideal of Q.

Take $3 \in Z, \frac{1}{2} \in Q$, then $3 \,.\, \frac{1}{2} = \frac{3}{2} \notin Z$ *i.e.*, Z cannot be an ideal of Q.

Example 6. *If K is an ideal of R and 1 ∈ K, then K = R*

Sol. Given K is an ideal of R, so K is a subset of R *i.e.*, $K \subseteq R$. Also $r \in R$ and $1 \in K$

$\Rightarrow$ $r.1 \in K$ | K is an ideal of R

$\Rightarrow$ $r \in K \Rightarrow R \subseteq K$

$\Rightarrow$ $K = R$

Example 7. *If F is a field, then F has no proper ideals.*

Or

If F is a field, then the only ideals of F are <0> and F itself.

Sol. Let, if possible. S is any proper ideal of F and $0 \neq a \in S$. As $S \subseteq F \Rightarrow 0 \neq a \in F$. But F is a field and $0 \neq a \in F$. There exists $a^{-1} \in F$ (Every non-zero element of F has a multiplicative inverse).

Now $a \in S, a^{-1} \in F$ and since S is an ideal of F, then $aa^{-1} \in S \Rightarrow 1 \in S$

Hence S = F.

Hence the only ideals of F are 0 and F itself. | see example 6

Theorem X. *Intersection of two ideals of a ring R is an ideal of R.*

Proof. Let A and B are two ideals of R, then, $\phi \neq A \subseteq R, \phi \neq B \subseteq R \Rightarrow \phi \neq A \cap B \subseteq R$ i.e., $A \cap B$ is a non-empty subset of R. We show $A \cap B$ is an ideal of R.

Let $x, y \in A \cap B \Rightarrow x, y \in A$ and $x, y \in B$. As A and B are ideals of R

$\therefore$ $x - y \in A, x - y \in B \Rightarrow x - y \in A \cap B$

For $r \in R, x \in A \Rightarrow rx \in A$ and $xr \in A$ | A is an ideal of R.

Also for $r \in R$, $x \in B \Rightarrow rx \in B$ and $xr \in B$ | B is an ideal of R

Hence $rx \in A$, $rx \in B \Rightarrow rx \in A \cap B$

Also $xr \in A$, $xr \in B \Rightarrow xr \in A \cap B$

Hence the theorem.

9.15. SUM OF IDEALS

Let A and B be two ideals of a ring R, then the sum of the ideals A and B, denoted by A + B, is defined by $A + B = \{a + b : a \in A, b \in B\}$

Theorem XI. *If A and B are two ideals of R, then A + B is an ideal of R.*

Proof. $0 = 0 + 0 \in A + B \Rightarrow A + B \neq \phi$ i.e., A + B is non-empty subset of R.

Let $x, y \in A + B \Rightarrow x = a_1 + b_1, a_1 \in A, b_1 \in B$

$\Rightarrow$ $y = a_2 + b_2, a_2 \in A, b_2 \in B$

$\therefore$ $x - y = a_1 + b_1 - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2 \in A + B$

$\because a_1, a_2 \in A$ and A is an ideal of R

$\therefore a_1 - a_2 \in A$. Similarly $b_1 - b_2 \in B$

Further, for $r \in R, x \in A + B$, consider $rx = r(a_1 + b_1) = ra_1 + rb_1 \in A + B$

$\because r \in R, a_1 \in A$ and A is an ideal of R. $\therefore ra_1 \in A$ Similarly, $rb_1 \in B$

Also $xr = (a_1 + b_1)\, r = a_1 r + b_1 r \in A + B$

$\because r \in R, a_1 \in A$ and A is an ideal of R $\therefore a_1 r \in A$. Similarly $b_1 r \in B$

Hence A + B is an ideal of R.

9.16. QUOTIENT RING (P.T.U. B.Tech. May 2010, Dec. 2007, 2006, May 2005)

Let R be a ring and I be an ideal of R. Define R/I, by

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