(f) Normal Subgroup (M.U. 2002, 05, 07, 10, 13)

Definition : A subgroup H of G is said to be normal if for every $a \in G$ we have $aH = H$.

A subgroup of an Abelian group is normal.

Example 1 : Prove that "congruence modulo H" is an equivalence relation.

Sol. : By definition of "Congruence modulo H" $a\,R\,b$ means $a * b^{-1} \in H$.

(i) R is reflexive

$\because \quad a * a^{-1} = e$ and $e \in H \qquad \therefore \quad R$ is reflexive.

(ii) R is symmetric

$\because \quad a\,R\,b \qquad \therefore \quad a * b^{-1} = \in H$

Since, $(a * b^{-1}) \in H$, $(a * b^{-1})^{-1} \in H$

$\therefore \quad b * a^{-1} \in H \qquad \therefore \quad R$ is symmetric.

(iii) R is transitive

If $a\,R\,b$ then $a * b^{-1} \in H$

If $b\,R\,c$ then $b * c^{-1} \in H$

$\therefore \quad (a * b^{-1}) * (b * c^{-1}) \in H$

$\therefore \quad a * (b^{-1} * b) * c^{-1} \in H$

$\therefore \quad a * e \times c^{-1} \in H$

$\therefore \quad a * c^{-1} \in H \qquad \therefore \quad a\,R\,c \quad \therefore \quad R$ is transitive.

Hence, R is an equivalence relation.

Example 2 : Find all cosets of the sub-group $H = 3 \cdot Z$ of the group $(Z, +)$.

Sol. : We have $Z = \{ \ldots\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots \}$

and $H = 3 \cdot Z = \{-7, -6, -3, 0, 3, 6, \ldots\ldots \}$

Now, $H + 0 = \{ \ldots\ldots, -6, -3, 0, 3, 6, \ldots\ldots \} = H$

$H + 1 = \{ \ldots\ldots, -5, -2, 1, 4, 7, \ldots\ldots \} = H_1$

$H + 2 = \{ \ldots\ldots, -4, -1, 2, 5, 8, \ldots\ldots \} = H_2$

$H + 3 = \{ \ldots\ldots, -3, 0, 3, 6, 9, \ldots\ldots \}$

But $H + 3 = H + 0$.

Hence, H, $H + 1$, $H + 2$ are the only three distinct right cosets of H in Z.

Further all these cosets partition the set Z into three disjoint subsets such that

$H \cup H_1 \cup H_2 = Z$

Further, since G is abelian, H is abelian and $ah = ha$. Hence, every right coset is equal to the left coset.

$\therefore \quad H + 1 = 1 + H, \qquad H + 2 = 2 + H.$

Example 3 : Find all the cosets of the sub-group $H = 2 \cdot Z$ of the sub-group $(Z, +)$ in Z.

Sol. : Left to you.

Example 4 : Let $G = Z_6$. Find the left and right cosets of $H = \{[0], [3]\}$.

Is H a normal subgroup of the group Z_6.

The table of Z_6 (Here + stands for $+_6$)

$+_6$	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

The group Z_6 is abelian because $a + b = b + a$ for $a, b \in Z_6$

e.g., $1 + 2 = 3$ and $2 + 1 = 3$.

Now, left coset of $H = \{[0], [3]\}$ with respect to a in the set Z_6 is

$aH = \{ a * b \mid h \in H \}$

$\therefore$ $0H = \{0 + 0, 0 + 3\} = \{0, 3\}$, $1H = \{1 + 0, 1 + 3\} = \{1, 4\}$,

$2H = \{2 + 0, 2 + 3\} = \{2, 5\}$, $3H = \{3 + 0, 3 + 3\} = \{3, 0\}$,

$4H = \{4 + 0, 4 + 3\} = \{4, 1\}$, $5H = \{5 + 0, 5 + 3\} = \{5, 2\}$.

Now, the right coset of $H = \{ [0]_6, [3]_6 \}$ with respect to a in the set is

$Ha = \{ h * a \mid h \in H \}$

$\therefore$ $H0 = \{0 + 0, 3 + 0\} = \{0, 3\}$, $H1 = \{0 + 1, 3 + 1\} = \{1, 4\}$,

$H2 = \{0 + 2, 3 + 2\} = \{2, 5\}$, $H3 = \{0 + 3, 3 + 3\} = \{3, 0\}$,

$H4 = \{0 + 4, 3 + 4\} = \{4, 1\}$, $H5 = \{0 + 5, 3 + 5\} = \{5, 2\}$.

Clearly, we have

$0H = H0$, $1H = H1$, $2H = H2$, $3H = H3$, $4H = H4$, $5H = H5$.

$\therefore$ H is a normal subgroup of Z_6.

Example 5 : Let $G = Z_8$. Determine the left cosets of $H = \{[0], [4]\}$ in G. **(M.U. 2005)**

Sol. : The table of Z_8 (Here + stands for $+_8$)

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Now, left coset of $H = \{[0], [4]\}$ with respect to a in the Z_8 is

$aH = \{ a * h \mid h \in H \}$

$\therefore$ $0H = \{0 + 0, 0 + 4\} = \{0, 4\}$, $1H = \{1 + 0, 1 + 4\} = \{1, 5\}$,

$2H = \{2 + 0, 2 + 4\} = \{2, 6\}$, $3H = \{3 + 0, 3 + 4\} = \{3, 7\}$,

$4H = \{4 + 0, 4 + 4\} = \{4, 0\}$, $5H = \{5 + 0, 5 + 4\} = \{5, 1\}$,

$6H = \{6 + 0, 6 + 4\} = \{6, 2\}$, $7H = \{7 + 0, 7 + 4\} = \{7, 3\}$.

Example 6 : Let $G = Z_8$. Determine all right cosets of $H = \{[0], [4]\}$ in G.

Sol. : Left to you.

(g) Product Group

Definition : If G_1 and G_2 are groups and $G = G_1 \times G_2$ then G is called a product group under the operation defined by

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$$

Example : Let $G_1 = G_2 = Z_2$. If $\bar{0}$ denotes the equivalence class [0], and $\bar{1}$ denotes the equivalence class [1], then the multiplication table for the product group $G_1 \times G_2$ is given by

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

(h) Quotient **(M.U. 2000)**

We know that an equivalence relation R defined on a set A induces a partition of A denoted by A / R. In the same way the equivalence relation R, mod m induces a partition of the set S of the semi-group $(S, *)$ which we denote by S / R. S / R is called **quotient.**

Example : If A is the set of natural numbers and R is the relation defined by $a \, R \, b$ if $a \equiv b \pmod 5$, then prove that $(A / R, \oplus)$ is a group where A / R denotes the quotient group induced on A by R and $\oplus$ the addition on residue classes *i.e.* $[a] \oplus [b] = [a + b]$.

Sol. : The partition induced on A by the relation $a \equiv b \pmod 5$ is given by

$$[0] = \{ \ldots, -10, -5, 0, 5, 10, \ldots \} = [5] = [10] = \ldots$$
$$[1] = \{ \ldots, -9, -4, 1, 6, 11, \ldots \} = [1] = [6] = \ldots$$
$$[2] = \{ \ldots, -8, -3, 2, 7, 12, \ldots \} = [2] = [7] = \ldots$$
$$[3] = \{ \ldots, -7, -2, 3, 8, 13, \ldots \} = [3] = [8] = \ldots$$
$$[4] = \{ \ldots, -6, -1, 4, 9, 14, \ldots \} = [4] = [9] = \ldots$$

Thus, we have $A / R = \{ [0], [1], [2], [3], [4] \}$

and $[a] \oplus [b] = [a + b]$.

e.g., $[2] \oplus [3] = [2 + 3] = [5]$

With this understanding we can prepare the following table for $\oplus$ on A / R.

$\oplus$	[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]

From this table it is clear that $\oplus$ is a binary operation.

G1 : Associativity

$[a] \oplus ([b] \oplus [c]) = [a] \oplus [$
$= [a + (b$

Similarly, $([a] \oplus [b]) \oplus [c] = a +$

This proves associativity.

G2 : From the first row (column) w

G3 : Since in each row and column

$[0]^{-1} = [0]$, $[1]^{-}$

ecause $[0] \oplus [0] = [0]$, $[1] \oplus$

Hence, $(A / R, \oplus)$ is a group.

Definition : If R is a congruence

nd if $(S / R, \circledast)$ or $(G / R, \circledast)$ is the co

hen the function $f_R : S \to S / R$ or $f_R : G$

atural **homomorphism.**

Example 1 : Find the natural ho

nd the relation R defined by $a \, R \, b$ is

ol. : From the table given the previo

$0 \to [0]$, $1 \to [1]$, $2 \to$

Example 2 : Consider the follo

y the operation $*$ given by the adjo

Show that $R = \{(a, a), (b, b), ($

n equivalence relation.

Find the quotient semi-group

Find the operation table for $($

Sol. : It is easy to prove that R is a

The partition S / R induced b

o the elements in the same block

We denote this as congruen

Now, by definition $[a] \circledast [b$

From the given table, we fin

$[a] \circledast [a] = [a * a]$

$[c] \circledast [a] = [c * a]$

Hence, we get the table.

*	[a]	[c]
[a]	[a]	[c]
[c]	[c]	[a]

The natural hom

$(a) \to$

G 1 : Associativity

$$[a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c]$$
$$= [a + (b + c)] = (a + b + c) \quad \text{[By associativity in } A\text{]}$$

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

This proves associativity.

G 2 : From the first row (column) we see that [0] is the identity for $\oplus$.

G 3 : Since in each row and column we find the identity element, every element has its inverse.

$[0]^{-1} = [0]$, $[1]^{-1} = [4]$, $[2]^{-1} = [3]$

$[0] \oplus [0] = [0]$, $[1] \oplus [4] = [0]$, $[2] \oplus [3] = [0]$.

Hence, $(A / R, \oplus)$ is a group.

Definition : If R is a congruence relation defined on a semi-group $(S, *)$ or on a group $(G, *)$ and if $(S / R, \circledast)$ or $(G / R, \circledast)$ is the corresponding quotient semi-group or group defined as above, then the function $f_R : S \to S / R$ or $f_R : G \to G / R$ defined by $f_R(a) = [a]$ is an **homomorphism** called **natural homomorphism.**

Example 1 : Find the natural homomorphism $f_R : G \to G / R$ for the set A of natural numbers and the relation R defined by $a \, R \, b$ is $a \equiv b \pmod 5$.

Sol. : From the table given the previous page, it is clear that the natural homomorphism is given by

$$0 \to [0], \; 1 \to [1], \; 2 \to [2], \; 3 \to [3], \; 4 \to [4].$$

Example 2 : Consider the following semigroup defined on $S = \{a, b, c, d\}$ by the operation $*$ given by the adjoining table.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Show that $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (c, d), (d, c)\}$ is an equivalence relation.

Find the quotient semi-group $(S / R, \circledast)$ induced by R.

Find the operation table for $(S / R, \circledast)$. Find the natural homomorphism $f_R : S \to S / R$.

(M.U. 2006)

Sol. : It is easy to prove that R is an equivalence relation and is left to you as an exercise.

The partition S / R induced by R is $\begin{array}{|c|c|}\hline a & c \\ \hline b & d \\ \hline \end{array}$ because every element in the block is related to the elements in the same block.

We denote this as congruence classes. $[a] = \{a, b\}$, $[c] = \{c, d\}$

Now, by definition $[a] \oplus [b] = [a * b]$

From the given table, we find that

$[a] \circledast [a] = [a * a] = [a]$, $[a] \circledast [c] = [a * c] = [c]$,

$[c] \circledast [a] = [c * a] = [c]$, $[c] \circledast [c] = [c * c] = [a]$.

Hence, we get the table.

*	[a]	[c]
[a]	[a]	[c]
[c]	[c]	[a]

The natural homomorphism (from partion table).

$$(a) \to [a], \; (b) \to [a], \; (c) \to [c], \; (d) \to [c].$$

Example 3 : Consider the monoid $S = \{a, b, c, d\}$ with the operation $*$ defined by the adjoining table.

$*$	a	b	c	d
a	d	b	c	a
b	c	b	c	b
c	b	b	c	c
d	a	b	c	d

Consider the congruence relation

$$R = \{(d, d), (d, a), (a, d), (a, a), (b, b), (b, c), (c, b), (c, c)\}$$

(i) Write operation table of the quotient monoid S / R.

(ii) Find the natural homomorphism $f_R : S \to S / R$.

Sol. : You can easily prove that R is an equivalence relation.

a	b
d	c

The partition S / R is given by $[d] = \{a, d\}$, $[b] = \{b, c\}$. Further d is the identity element of $*$. From the given table, we find that,

$$[a] \circledast [a] = [a * a] = [d] = [a]$$

$$[a] \circledast [b] = [a * b] = [b]$$

$$[b] \circledast [a] = [b * a] = [c] = [b]$$

$$[b] \circledast [b] = [b * b] = [b]$$

Hence, we get the table.

$*$	$[a]$	$[b]$
$[a]$	$[a]$	$[b]$
$[b]$	$[b]$	$[b]$

The natural homomorphism is (from partion table)

$$(a) \to [a], \ (d) \to [a], \ (b) \to [b], \ (c) \to [b].$$

8. Generators and Evaluation of Powers

Let $(A, *)$ be an algebraic system in which A is a set of angles in degrees and binary operation $*$ gives the angle that the combination of 2 angles yields a new angle. We want to know all the possible combinations of angles.

Consider the group $(\{0°, 15°, 45°, 60°, 75°, 90°, 105°, 120°\}, *)$ that describes the rotation of straight line in the plane. If we can rotated straight line only by 60° each time. Successive rotations by 60° will gives the angles of rotation {0, 60°, 120°}. If we can rotate the straight line only 15° each time, successive rotations by 15° will yield all the rotations of straight line in {0°, 15°, 45°, 60°, 75°, 90°, 105°, 120°}.

A subset of a group is called **generating set**, if it can be expressed using the elements of a subset by means of the group multiplication and inversion and there is a surjective map from a free group on that many generators to given generators of the free group to the elements of this free group.

The elements of the generating set are termed as **generators**.

In general, let $(G, *)$ be an algebraic system where $*$ is a closed operation and $A = \{a, a_2, ...\}$ be a subset of G. Let A_1 be the subset of A which contains A as well as elements $a_i * a_j$ for a_i, a_j in A. A_1 is called the set generated by A, similarly, let A_2 denoted set generated by A_1, ... and A_{i+1} denoted the set generated by A_i. Let B denote the union of A, A_1, A_2, ..., A_i. The algebraic system $(B, *)$ is system generated by A and an element is said to be generated by A, if it is in B. Thus, for a group $(G, *)$, if B is finite, then $(B, *)$ is subgroup. If $B = G$, B is called a generating set or a set of generators of algebraic system $(G, *)$. In the example on rotation of straight line {15°} is a generating set.

eration *

*	a	b	c	d
a	d	b	c	d
b	c	b	c	a
c	b	b	c	b
d	a	b	c	c
	a	b	c	d

c)}

r d is the

a	b
d	c

degrees and binary operation
le. We want to know all the

hat describes the rotation of
h time. Successive rotations
e straight line only 15° each
ne in {0°, 15°, 45°, 60°, 75°,

sed using the elements of a
a surjective map from a free
to the elements of this free

peration and $A = \{a, a_2, ...\}$
lements $a_i * a_j$ for a_i, a_j in A.
rated by A_1, ... and A_{i+1}
.., A_i. The algebraic system
by A, if it is in B. Thus, for a
a generating set or a set of
ght line {15°} is a generating

Alternatively, A subset B of group A is called a generating set if it satisfies following equivalent conditions.

1. For any element $b \in A$, we can write $b = a_1, a_2, ..., a_n$ for each a_i either $a_i \in B$ or $a_i^{-1} \in B$. B is a symmetric subset *i.e.*, $a_i \in B$ implies $a_i^{-1} \in S$.
2. If C is a proper subgroup of A, then C can't contain B.
3. Consider map from free group on as many generators as elements of B to the group A, which maps the freely generating set to the elements of S, this gives surjective homomorphism from free group to G.

For example, the set of all elements of a group is a generating set for the group.

If S is a subset of a group G s.t. every element of G is a power of some elements of S, the S is a generating set. If S is empty set, then (S) is the trivial group $\{e\}$. Since we consider empty product to be the identity. The set of all non-identity elements of a group is a generating set for the group *e.g.*, the 5^{th} roots of unity in the complex plane form a group under multiplication. Each non-identity element generates the group.

Definition : An element a of a group G generates G and is a generator for G if $\langle a \rangle = G$. A group G is cyclic if there is some element a in G that generators G. A cyclic group is a group that is generated by a single element.

For example, the group Z under addition is a cyclic group, both 1 and – 1 are generators for the group.

Finding generators of a cyclic group depends upon order of group. If the order of group is 8, then the total number of generators of group G are equal to positive integers less than 8 and coprime to 8 *i.e.*, 1, 3, 5, 7 less than 8 and coprime to 8. Therefore, if a is generator of G, then a^3, a^5, a^7 are also generators of G. Hence, there are 4 generators of G.

9. Cosets and Lagrange's Theorem

(a) Coset

(M.U. 2001)

Definition : Let $(G, *)$ be group and H be a subgroup of G. If a, b are two elements of G and if $a * b^{-1} \in H$, then we say that "a is congruent to b modulo H". It is written as "$a \equiv b \bmod H$".

It can be easily verified that this congruence relation is an equivalence relation (See Ex. 1 page 16-33). Since this congruence relation is an equivalence relation on G it partitions G into **equivalent classes** called cosets.

Definition : Let $(G, *)$ be group and H be a subgroup of G.

If a is an element of G then the set $Ha = \{ h * a \mid h \in H \}$ is called the **right coset** of H.

If a is an element of G, then the set $aH = \{ a * h \mid h \in H \}$ is called the **left coset** of H.

a is called the representative element of the coset aH or Ha.

For example, consider binary operation +, group $(\mathbb{Z}_6, +)$ elements of this group are

$$\{0, 1, 2, 3, 4, 5\}.$$

Let $H = \{0, 2, 4\}$ is a subgroup of $\mathbb{Z}_6$.

The left coset of H w.r.t. 0, *i.e.*, $0 + H = \{0 + 0, 0 + 2, 0 + 4\} = \{0, 2, 4\}$

The left coset of H w.r.t. 1, *i.e.*, $1 + H = \{1 + 0, 1 + 2, 1 + 4\} = \{1, 3, 5\}$

The left coset of H w.r.t. 2, *i.e.*, $2 + H = \{2 + 0, 2 + 2, 2 + 4\} = \{2, 4, 0\}$

Note that, 0 is the identity element.

(b) Lagrange's Theorem

If H is a subgroup of finite group G ($H \subseteq G$), then the order of H divides the order of G.

For example, order of G = No. of elements = $|G|$.

Lagrange's Theorem : $H \subseteq G \Rightarrow |H|$ divides $|G|$.

Let G be a finite group with $|G| = 323 = 17 \times 19$. Divisors of 323 are 1, 17, 19, 323.

Possible subgroups orders : 1, 17, 19, 323.

Standard subgroup : G, $\{e\}$ $\quad |G| = 323, \ |\{e\}| = 1$

Any other subgroups has order 17 or 19.

10. Permutation Groups and Burnside's Theorem

(a) Permutation Groups

A permutation of a set X is a function $6 : X \to X$, *i.e.*, one-to-one and onto. Alternatively, a permutation of a set A is a function from A into B, *i.e.*, both one-to-one and onto symbolically $\phi : A \to B$.

For example, suppose $A = \{1, 2, 3, 4, 5\}$ and σ is the permutation given by as shown in the Fig. 16.7, then σ can be written in a standard notation as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

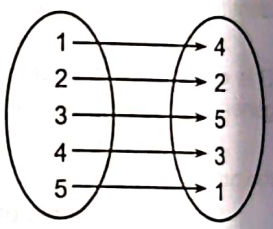

Fig. 16.7

Example 1 : Consider a set X containing 3 objects say triangle ($\triangle$), a circle ($\bigcirc$) and a rectangle ($\square$). A permutation of $X = \{\triangle, \bigcirc, \square\}$ is a function $\sigma : X \to S$ defined as $\sigma(\triangle) = \triangle$, $\sigma(\bigcirc) = \square$, $\sigma(\square) = \bigcirc$, *i.e.*, $\triangle \to \triangle$, $\bigcirc \to \square$, $\square \to \bigcirc$ respectively.

Since, what matters for a permutation is how many objects we have and not the nature of the objects. The permutation of above example can be rewritten as $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$, such that

$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$ or $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

If A is a finite set $\{1, 2, ..., n\}$ then the group of all permutations of A is the symmetric group on n letters, denoted by S_n and has $n!$ elements where $n! = n(n-1)(n-2) ..... 2 \cdot 1$.

Every permutation has an inverse, the inverse permutation (A permutation is a bijection).

Example 2 : If $n = 1$, S_1 contains only one element, the permutation identity.

Example 3 : If $n = 2$, then $X = \{1, 2\}$ and we have only two permutations

$\sigma_1 : 1 \to 1, \ 2 \to 2$ and $\sigma_2 : 1 \to 2, \ 2 \to 1$ and $S_2 = \{\sigma_1, \sigma_2\}$.

The Cayley Table of S_2 is as like as adjoining table.

	σ_1	σ_2
σ_1	σ_1	σ_2
σ_2	σ_2	σ_1

Consider $(G, 0)$ be a permutation group of a set $H = \{1, 2, 3\}$. A binary relation on H, is called binary relation induced by $(G, 0)$, is defined to be s.t. element 1 is related to element 2 iff their is a permutation in G that map 1 into 2. For example, consider

$$G = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \right\}$$

32. Let $(G_1, *_1)$ and $(G_2, *_2)$ be two groups. Prove that $(S, \odot)$ is a group where $S = G_1 \times G_2$ and $(a_1, a_2) \odot (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$.

33. Prove that $G = \{ x \mid x^4 = 1 \}$ is a group under multiplication.

34. Let Z_n denote the set of integers $\{0, 1, 2, ..., (n-1)\}$. Let $\odot$ be the binary operation on Z_n such that $a \odot b$ = the remainder of ab divided by n. **(M.U. 2001)**

(i) construct the table for the operation $\odot$ for $n = 4$.

(ii) Is Z_n a group for any n ?

[**Ans. : (ii)** $G = \{1, 2, 3, 4\}$ is an Abelian group under multiplication modulo 5. But $G = \{1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6. See Ex. 7, 8, page 16-43 and Ex. 14 page 16-44.]

35. Let S_3 be the set of bijective functions that can defined on the set $A = \{1, 2, 3\}$. And $*$ be the operation of composition of functions of the form $f \circ g$. Prove that $(S_3, *)$ is a group. Is it Abelian ? (See Ex. 21, page 16-23) **(M.U. 2006)** [**Ans. :** No]

12. Isomorphism and Homomorphism

(a) Isomorphism of groups

Definition : If $(G_1, *_1)$ and $(G_2, *_2)$ are groups, then $f : G_1 \to G_2$ is an **isomorphism** from G_1 to G_2 if (i) f is **a bijection** (*i.e.* one-to-one and onto) and (ii) $f(a *_1 b) = f(a) *_2 f(b)$. **(M.U. 1998, 99)**

If such a function exists, then G_1 is said to be **isomorphic** to G_2.

(b) Homomorphism of groups

Definition : If $(G_1, *_1)$ and $(G_2, *_2)$ are groups then $f : G_1 \to G_2$ is an **homomorphism** from G_1 to G_2 if for any $a, b \in G_1$

$$f(a *_1 b) = f(a) *_2 f(b)$$

Example 1 : Let G be the group of integers under addition and G' be the group of even integers under addition. Show that the function $f : G \to G'$ defined by $f(a) = 2a$ is an isomorphism. **(M.U. 2003, 06, 10, 12)**

Sol. : Suppose $f(a_1) = f(a_2)$ $\therefore$ $2a_1 = 2a_2$ $\therefore$ $a_1 = a_2$.

Hence, f is one-to-one.

Suppose b is an even integer *i.e.* $b \in G'$.

Then $2a = b$ $\therefore$ $a = (b/2) \in G_1$ and $f(a) = f(b/2) = 2(b/2) = b$.

$\therefore$ f is onto.

Here, $*_1$ and $*_2$ both are addition operations.

$$\therefore \quad f(a *_1 b) = f(a + b) = 2(a + b) = 2a + 2b = f(a) *_2 f(b)$$

Hence, f is a isomorphism.

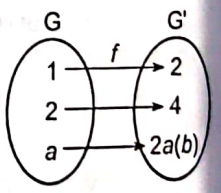

Fig. 16.9

Example 2 : Let G be the group of real numbers under addition and G' be the group of positive real under multiplication. Let $f : G \to G'$ be defined by $f(x) = e^x$. **(M.U. 1999, 2003)**

Show that f is an isomorphism.

Sol. : Suppose $f(a_1) = f(a_2)$ $\therefore$ $e^{a_1} = e^{a_2}$ $\therefore$ $a_1 = a_2$.

Hence, f is one-to-one.

roup where $S = G_1 \times G_2$ and

(M.U. 2001)

dulo 5. But

sm from G_1

he group of even
is an isomorphism.
(M.U. 2003, 06, 10, 12)

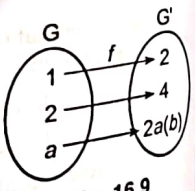

Fig. 16.9

n and G' be the group of
x. (M.U. 1999, 2003)

Suppose b is a positive real number *i.e.* $b \to G'$.

Then $b = e^a$ $\quad\therefore\quad a = \log b$.

and $f(a) = f(\log b) = e^{\log b} = b$. $\quad\therefore$ f is onto.

Now, $f(a *_1 b) = f(a + b) = e^{a+b}$

$= e^a \cdot e^b = f(a) *_2 f(b)$

$\therefore$ f is an isomorphism.

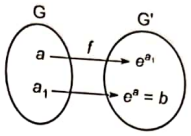

Fig. 16.10

Example 3 : Let R^+ be the set of all positive real numbers. Show that the function $f: R^+ \to R$ defined by $f(x) = \ln x$ is a an isomorphism of the semi-group $(R^+, \times)$ to the semi-group $(R^+, +)$ where $\times$ and $+$ are ordinary multiplication and addition respectively. (M.U. 2004, 05)

Sol. : **(i)** Since $f(x) = \ln x = \log_e x$ if $f(a) = f(b)$ *i.e.*, $\log a = \log b$, then $a = b$.

$\therefore$ f is one-to-one.

(ii) If $c \in R$, then $e^c \in R$ and $f(e^c) = \log e^c = c \log e = c \in R^+$

$\therefore$ f is onto.

ii) Now, $f(a \times b) = \log(a \times b) = \log a + \log b = f(a) + f(b)$

$\therefore$ f is an isomorphism.

Example 4 : Show that the additive group Z_4 is isomorphic to multiplicative group of non-zero elements of Z_5. (M.U. 2006)

Sol. : We have the following tables for the additive group G of Z_4 and multiplicative group of G' of (non-zero) Z_5,

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Now, we write the table of × taking the second column last and second row last.

×	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

Clearly, now we can see that $G \to G'$ where the mapping is $0 \to 1$, $1 \to 3$, $2 \to 4$, $3 \to 2$ is a isomorphism.

Example 5 : If ω denotes the cube root of unity, show that $G = \{1, \omega, \omega^2\}$ is isomorphic to $(Z_3, +_3)$.

Sol. : We have the following tables for × and +.

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω^2

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Clearly, $G \to G'$ where the mapping is $1 \to 0$, $w \to 1$ and $\omega^2 \to 2$ is an isomorphism.

Example 6 : Show that $(G, \times)$ where $G = \{1, -1, i, -i\}$ and $(Z_4, +_4)$ are isomorphic.

Sol. : We first prepare the following tables for × and +.

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Clearly $G \to G'$ where the mapping is $1 \to 0, -1 \to 2, i \to 1$ and $-i \to 3$ is a isomorphism.

Example 7 : If a function f is an isomorphism from a semi-group $(S, *)$ to another semi-group $(T, *')$, show that f^{-1} is also an isomorphism from $(T, *')$ to $(S, *)$. **(M.U. 2002, 15)**

Sol. : Since $f: S \to T$ is an isomorphism, f is one-to-one from S to T.

i.e., $f(a * b) = f(a) *' f(b)$ for all a, b in S. ..... (1)

$\therefore$ f^{-1} exists and is also one to one from T to S.

Now, suppose a', b' are elements of T.

Since f is onto we can always find elements a, b in S, such that

$f(a) = a', \ f(b) = b'$

Hence, $a = f^{-1}(a')$ and $b = f^{-1}(b')$

Now, $f'(a' *' b') = f^{-1}[f(a) *' f(b)]$

$= f^{-1}[f(a * b)]$ [By (1)]

$= a * b$

$= f^{-1}(a') * f^{-1}(b')$

$\therefore$ Hence, f^{-1} is an isomorphism.

Example 8 : Show that if a function f is an isomorphism from a group $(G, *)$ to another group $(G', *')$ then show that f^{-1} is also an isomorphism from $(G, *')$ to $(G, *)$. **(M.U. 2006)**

Sol. : Left to you.

Example 9 : If f is homomorphism from a commutative semigroup $(S, *)$ onto a semigroup $(T, *')$ then prove that $(T, *')$ is also commutative. **(M.U. 2002, 08, 13)**

Sol. : Let t_1 and t_2 be any two elements of T.

Since f is homomorphic there exist s_1 and s_2 in S, such that $t_1 = f(s_1)$ and $t_2 = f(s_2)$.

Hence, $t_1 *' t_2 = f(s_1) *' f(s_2)$

$= f(s_1 * s_2)$

$= f(s_2 * s_1)$ [$\because$ s is a commutative group]

$\therefore$ $t_1 *' t_2 = f(s_2) *' f(s_1) = t_2 *' t_1$

$\therefore$ $(T, *')$ is also commutative.

13. Ring

So far we have studied structures of a set under one operation. We shall now study a set with two operations + and · on its elements. This gives rise to two important algebraic structures viz. rings and fields. Rings have structures similar to natural numbers and fields have structures similar to real numbers with respect to the operations of addition and multiplication.

1	2	3
2	3	0
3	0	1
0	1	2

1 and $-i \rightarrow 3$ is a isomorphism.

group $(S, *)$ to another semi-group
*). **(M.U. 2002, 15)**
to T.

..... (1)

h that

]

m a group $(G, *)$ to another group
$(G, *)$. **(M.U. 2006)**

emigroup $(S, *)$ onto a semigroup
(M.U. 2002, 08, 13)

t $t_1 = f(s_1)$ and $t_2 = f(s_2)$.

mmutative group]

on. We shall now study a set with
nportant algebraic structures viz.
and fields have structures similar
ltiplication.

(Ring) Definition : A ring is an ordered triple $(R, +, \cdot)$ where R is a non-empty set and $+$ and $\cdot$ are two binary operations on R satisfying the following axioms.

R 1 : $(R, +)$ is a commutative group.

R 2 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$ ($\cdot$ is associative)

R 3 : $a \cdot (b + c) = a \cdot b + a \cdot c$
and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$ ($\cdot$ distributes over $+$)

(a) Examples of Rings

1. The set of all integers is a ring (with unity) for $+$ and $\times$.
2. The set of all real numbers of the form $a + \sqrt{2}\, b$ is a ring for $+$ and $\times$.
3. The set of all matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a ring for $+$ and $\times$.
4. The set of complex numbers with usual addition and multiplication is a ring.

Remark ....

The binary operation $+$ and $\cdot$ referred to above are called addition and multiplication. In the same spirit, the identity of $(R, +)$ is denoted by 0 and is called zero, a^{-1} is denoted by $-a$ and is called minus a and $a + (-b)$ is denoted by $a - b$. Addition is commutative but multiplication in general is not.

(Commutative Ring) Definition : A ring $(R, +, \cdot)$ is called **a commutative ring** if $a \cdot b = b \cdot a$ for all $a, b \in R$.

(a) Ring with Unity

Definition : A ring $(R, +, \cdot)$ is called **a ring with unity** or identity if there exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

(b) Ring with Zero Divisors

A ring $(R, +, \cdot)$ is called a **ring with zero divisor** if for $a, b \in R$, we have $a \cdot b = 0$ but $a \neq 0$, $b \neq 0$. In this case a and b are called proper zero divisors.

For example, we know that, we can find two matrices A, B such that $A \cdot B = 0$ but $A \neq 0$, $B \neq 0$.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Definition : A ring $(R, +, \cdot)$ is called a **ring without zero divisor** if for all $a, b \in R$ if $ab = 0$ then either $a = 0$ or $b = 0$ or both $a \neq 0$, $b \neq 0$.

This means in a ring without zero divisors, the left cancellation law and right cancellation laws hold.

i.e. If $ab = ac$, then $b = c$ and if $ba = ca$ then $b = c$.

Examples of Commutative Rings

Example 1 : Let R be the set of integers, positive, negative, and 0; $+$ is the usual addition and $\cdot$ the usual multiplication. Then $(R, +, \cdot)$ is a commutative ring with unity.

Example 2 : Let R be the set of even integers with usual operations of addition and multiplication. Then $(R, +, \cdot)$ is a commutative ring without unity.

Example 3 : Let R be the set of rational numbers with usual operations of addition and multiplication. Then R is a commutative ring with unity. (It is also a field). (See § 15)

Example 4 : Let $R = \{0, 1, 2, 3, 4, 5, 6\}$ and $\odot$ and $\oplus$ be two operations multiplication modulo 7 and addition modulo 7. Then, $(R, \odot, \oplus)$ is a commutative ring with unity. (It is also a field). (See § 15) **(M.U. 2005)**

The set $Z_m = \{0, 1, 2, \ldots, (m-1)\}$ under the operations of addition and multiplication modulo m is a ring. It is called **a ring of integers modulo m.** If m is a prime the Z_m is **a field**. (See § 15)

Example 5 : Let $R = \{0, 1, 2, 3, 4, 5\}$ and $\odot$ and $\oplus$ be two operations multiplication modulo 6 and addition modulo 6. Then $(R, \odot, \oplus)$ is a ring. (But it is not a field). It is a ring with zero divisors.

Example 6 : Prove that Z_4 is a ring under addition and multiplication modulo 4. **(M.U. 2004)**

Sol. : The addition and multiplication table for Z_4 modulo 4 are given below.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

***R* 1 :** $(R, +)$ is a commutative group.

***R* 2 :** $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$. X is associative.

***R* 3 :** $a \times (b + c) = a \times b + a \times c$.

e.g. $2 \times (3 + 1) = 2 \cdot 0 = 0$ and $2 \times 3 + 2 \times 1 = 2 + 2 = 0$

and $(b + c) \times a = b \times a + c \times a$ for all $a, b, c \in R$.

$\therefore$ $\times$ distributes over $+$. Hence, $(Z_4, +, \times)$ is a ring.

Example 7 : Prove that Z_5 is a ring under addition and multiplication modulo 5. **(M.U. 2005)**

Sol. : The addition and multiplication tables for Z_5 modulo 5 are given below.

+	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

×	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

Verification that $(R, +, \times)$ is a ring is left to you.

Example 8 : Prove that $R = \{0, 2, 4, 6, 8\}$ is a commutative ring under addition and multiplication modulo 10. **(M.U. 2002, 05)**

Sol. : The addition and multiplication tables are given below.

+	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

×	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	8
6	0	2	4	6	8
8	0	6	2	8	4

Verification that $(R, +, \times)$ is a ring is left to you.

Example 9 : Let $A = \{a, b, c, d\}$ an

+	a	b	c
a	a	b	c
b	b	c	d
c	c	d	a
d	d	a	b

(a) Is it a commutative ring ?

(c) Find the additive inverse of each

Sol. : (a) Commutative Ring

(i) It is easy to see that A is closed

(ii) Because, $(a + b) + c = b + c =$

and $a + (b + c) = a + c =$

$+$ is associative.

(iii) From the first row and the first c

(iv) Since $a + b = b$ and $b + a = b$ is

(v) since for every element additive i

(vi) From the second table we see th

$(a \cdot b) \cdot c = a \cdot c = a$ and

$\therefore$ $\cdot$ is associative.

(vii) You can establish distributivity. H

(b) As seen above a is the additive identit

(c) From the table we see that the inverse inverse of d is b.

Example 10 : If $x, y \in Z$ and the operati

$x \oplus y = x + y - 1$ and

Prove that $(Z, \oplus, \otimes)$ is a ring.

Sol. : See Ex. 3 of § 15.

Example 11 : Show that the set $R = \{x | x =$ addition and multiplication.

Sol. : See Ex. 2 of § 15.

(c) Basic Properties

If R is a ring with identity 0 and unit element

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot a$

(iv) unit element is unique.

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

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

Example 9 : Let $A = \{a, b, c, d\}$ and let the operations + and • be defined by the following tables.

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

•	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	a

(a) Is it a commutative ring ? (b) Does it have an identity ?

(c) Find the additive inverse of each element of A. **(M.U. 2007)**

Sol. : (a) Commutative Ring

(i) It is easy to see that A is closed under + and also under •.

(ii) Because, $(a + b) + c = b + c = c$

and $a + (b + c) = a + c = c$

+ is associative.

(iii) From the first row and the first column we see that a is the additive identity.

(iv) Since $a + b = b$ and $b + a = b$ is true for all elements and

(v) since for every element additive inverse exists $(R, +)$ is a commutative group.

(vi) From the second table we see that

$(a \cdot b) \cdot c = a \cdot c = a$ and $a \cdot (b \cdot c) = a \cdot a = a$

$\therefore$ · is associative.

(vii) You can establish distributivity. Hence, $(R, +, \cdot)$ is a ring.

(b) As seen above a is the additive identity.

(c) From the table we see that the inverse of a is a, the inverse of b is d, the inverse of c is c, the inverse of d is b.

Example 10 : If $x, y \in Z$ and the operations $\oplus$, $\otimes$ are defined by

$$x \oplus y = x + y - 1 \quad \text{and} \quad x \otimes y = x + y - xy$$

Prove that $(Z, \oplus, \otimes)$ is a ring. **(M.U. 2003, 04, 05)**

Sol. : See Ex. 3 of § 15.

Example 11 : Show that the set $R = \{x \mid x = a + b\sqrt{2}, a, b \text{ are integers}\}$ is a ring under usual addition and multiplication. **(M.U. 2003, 06)**

Sol. : See Ex. 2 of § 15.

(c) Basic Properties

If R is a ring with identity 0 and unit element 1 then for all elements $a, b, c \in R$. **(M.U. 2005)**

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot b$ **(M.U. 2006)**

(iv) unit element is unique.

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

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

Sol. : (i) We have

$$a \cdot 0 = a \cdot (0 + 0) \quad [\because 0 + 0 = 0]$$
$$= a \cdot 0 + a \cdot 0 \quad [\because \text{left distributive law}]$$
$$\therefore \quad 0 + a \cdot 0 = a \cdot 0 + a \cdot 0 \quad [\because 0 + a \cdot 0 = a \cdot 0]$$
$$\therefore \quad 0 = a \cdot 0 \quad [\because \text{right cancellation law}]$$

Similarly, we have

$$0 \cdot a = (0 + 0) \cdot a \quad [\because 0 + 0 = 0]$$
$$= 0 \cdot a + 0 \cdot a \quad [\because \text{right distributive law}]$$
$$\therefore \quad 0 + 0 \cdot a = 0 \cdot a + 0 \cdot a \quad [\because 0 + 0 \cdot a = 0 \cdot a]$$
$$\therefore \quad 0 = 0 \cdot a \quad [\because \text{right cancellation law}]$$

Hence, $a \cdot 0 = 0 \cdot a = a$

(ii) Consider

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) \quad [\because \text{left distributive law}]$$
$$= a \cdot 0 = 0$$

Hence, $a \cdot b$ is the inverse of $a \cdot (-b)$ which is unique.

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

Similarly, we can prove that,

$$(-a) \cdot b = -(a \cdot b)$$
$$\therefore \quad a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

(iii) We have

$$(-a) \cdot (-b) = -[(-a) \cdot b] \quad [\because a \cdot (-b) = -(a \cdot b)]$$
$$= -[-(a \cdot b)] \quad [\because (-a) \cdot b = -(a \cdot b)]$$
$$= a \cdot b \quad [\because -(-a) = a]$$

(iv) If possible, suppose there is another unit element 1' with the same properties as 1.

$$\therefore \quad 1 \cdot 1' = 1' \cdot 1 = 1' \quad [\because 1 \text{ is unit element}]$$
But $1 \cdot 1' = 1$ $[\because 1' \text{ is unit element}]$
$$\therefore \quad 1' = 1$$

$\therefore$ The unit element is unique.

(v) $(-1) \cdot a = -(1 \cdot a) \quad [\because (-a) \cdot b = -(a \cdot b)]$
$= -a \quad [\because 1 \text{ is unity}]$

(vi) Replacing a and b by 1 in (iii) we get (vi).

(d) Subring

Analogous to the subgroup we have a subring.

Definition : *A* subset $R \subseteq S$ is a ring where $(S, +, \cdot)$ is a ring is called a **subring** of S.

In other words if $(S, +, \cdot)$ is a ring then a subset R of S is called a subring if R has all the properties of a ring.

Examples : (i) The ring of even integers is a subring of the ring of integers.

In general for any positive integer n, the set $nZ = \{ nm \mid m \in Z \}$ is a subring of Z.

(ii) The ring of rationals is a subring of the ring of reals.

= 0]
stributive law]
· 0 = a · 0]
ancellation law]

= 0]
istributive law]
a = 0 · a]

a subring of S.
a subring if R has all the

g of integers.
} is a subring of Z.

(e) Homomorphism, Automorphism and Isomorphism

We have learnt what we mean by homomorphism, automorphism and isomorphism. We shall now define these concepts with reference to rings.

Homomorphism of ring : Let $(R, +, \cdot)$ and $(S, +', \cdot')$ be two rings.

A mapping $\Phi : R \to S$ is called a **ring homomorphism** if for $a, b \in R$.

(i) $\Phi (a + b) = \Phi (a) +' \Phi (b)$

and (ii) $\Phi (a \cdot b) = \Phi (a) \cdot' \Phi (b)$

Isomorphism of ring : Let $(R, +, \cdot)$ and $(S, +', \cdot')$ be two rings.

A mapping $\Phi : R \to S$ is called a **ring isomorphism** if for $a, b \in R$.

(i) $\Phi (a + b) = \Phi (a) +' \Phi (b)$

(ii) $\Phi (a \cdot b) = \Phi (a) \cdot' \Phi (b)$

and (iii) Φ is one-to-one.

Automorphism of ring : If Φ is an isomorphism from R on to itself then Φ is called an morphism.

Example : If $\Phi : (R, +, \cdot) \to (S, +', \cdot')$ is a ring homomorphism then prove that $\Phi (- a) = - \Phi (a)$ for all $a \in R$. **(M.U. 2004)**

Sol : Since $\Phi : R \to S$ is a homomorphism by definition for $a, b \in R$.

$$\Phi (a + b) = \Phi (a) +' \Phi (b)$$

and $$\Phi (a \cdot b) = \Phi (a) \cdot' \Phi (b)$$

Now put $a = -1$ and $b = a$,

$$\therefore \quad \Phi (-1 \cdot a) = \Phi (-1) \cdot' \Phi (a)$$

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

$$\therefore \quad \Phi (- a) = - \Phi (a).$$

EXERCISE - III

1. Show that the set $R = \{x \mid x = a + b \cdot \sqrt{2}, a, b \text{ integers}\}$ is a ring with ordinary addition and multiplication.
2. Show that the set $R = \{0, 1, 2, 3, 4\}$ is a ring with respect to addition and multiplication modulo 5. **(M.U. 2008)**
3. Show that the set of all $n \times n$ matrices is a ring with respect to addition and multiplication of matrices.
4. If R is the set of all continuous functions defined on $[0, 1]$ then prove that R is a ring with respect to addition and multiplication of functions defined by $(f + g)\, x = f(x) + g(x)$ and $(f \cdot g)\, x = f(x) \cdot g(x)$.
5. If R is a set of all real numbers and $*_1$ and $*_2$ are two operations defined on R such that $a *_1 b = a + b - 5$ and $a *_2 b = 5$, prove that $(R, *_1, *_2)$ is a commutative ring. What is its 'zero' ? Has it zero divisors ? **(M.U. 2001, 05)**

   [Ans. : 5 is its zero. Yes, it has zero divisors]
6. If Z is a set of integers and $*_1$ and $*_2$ are two operations defined on Z such that $a *_1 b = a + b - 1$ and $a *_2 b = a + b - ab$, prove that $(Z, *_1, *_2)$ is a commutative ring. What is its 'zero' ? Is it a ring with unity ? **[Ans. :** Zero. Yes]

7. If $R = \{a, b, c, d\}$ and + and × are defined on S by the following tables, prove that $(R, +, \times)$ is a ring.

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

×	a	b	c	d
a	a	a	a	a
b	a	a	b	a
c	a	b	c	d
d	a	a	d	a

8. Prove that $(M, +, \cdot)$ where M is the set of all non-singular square matrices of order n is a ring under usual addition and multiplication of matrices.

9. Prove that $(M, +, \cdot)$ where M is the set of all matrices of the form $\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ and $a, b, c, d \in R$ and $i^2 = -1$ is a ring under usual addition and multiplication of matrices.

10. Prove that $(R, +, \cdot)$ where $R = \{0, 1, 2, 3, 4\}$ is a ring under addition modulo 5 and multiplication modulo 5.

11. Let Z be the set of integers and $a \oplus b = a + b + 1$, $a \odot b = a + b + ab$ for all $a, b \in Z$. Show that $(Z, \oplus, \odot)$ is a ring. Is it a commutative ring ? What is the zero of the ring ? Is it a ring with unity ?

[**Ans. :** It is commutative ring. Zero of the ring is – 1 and 0 is its unity.]

12. Show that the set of all matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ is a non-commutative ring with respect to addition and multiplication of matrices for every $a, b \in Q$. **(M.U. 2002)**

13. Show that the set of all 2×2 matrices of the type $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $a, b, c, d \in Z$ under usual matrix multiplication and addition is a ring. Is it commutative ? What is the zero of the ring ? What is the unity of the ring ?

[**Ans. :** **(i)** Non-commutative, **(ii)** $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero of the ring, **(iii)** $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unity of the ring.]

14. Let Z be the set of integers. Let $\oplus$ and $\odot$ be defined as $a \oplus b = a + b$ and $a \odot b = 0$ for all $a, b \in Z$. Is $(Z, \oplus, \odot)$ a ring ? Is it commutative ? Does it have a unity ?

[**Ans. : (i)** Yes, **(ii)** Yes, **(iii)** No]

14. Integral Domain

Definition 1 : (Integral Domain) : A commutative ring with unity without zero divisors is called **an integral domain.**

An integral domain can also be defined more explicitly as :

Definition 2 : (Integral Domain) : A ring $(R, +, \cdot)$ is called an **integral domain** if the following axioms hold.

...*I1* : It is a commutative ring.
...*I2* : It is a ring with unity.
...*I3* : It is a ring without zero divisors.

...ples of Integral Domain**

1. The set $(Z, +, \cdot)$ is an integral dom...
2. The set $(Q, +, \cdot)$ is an integral do...
3. But the set of even integers inclu...
...gral domain because it does not have...

Example 1 : Let $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \right.$ ...

...plication.
Is $(M, +, \cdot)$ an integral domain ?

...: ***Closure***

Let $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, $a,$

Then $A + B = \begin{bmatrix} a+b & \\ 0 & \end{bmatrix}$

and $AB = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$...

$\therefore$ M is closed under additi...

I1 : Consider $(M, +)$

(i) Matrix addition is associat...

(ii) Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ...

(iii) Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} -a & \\ 0 & \end{bmatrix}$ ...

(iv) Matrix addition is commu...

$\therefore$ $(M, +)$ is a commutativ...

(v) For matrices $A \cdot (B +$ ...
Hence, $\cdot$ distributes over $+$.
Hence, $(M, +, \cdot)$ is a commut...

I2 : Consider $(M, +, \cdot)$

Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & \\ 0 & \end{bmatrix}$ ...

$\therefore$ Multiplicative identit...
Hence, $(M, +, \cdot)$ is a ring wit...

efined on S by the following tables, prove that

×	a	b	c	d
a	a	a	a	a
b	a	a	b	a
c	a	b	c	d
d	a	a	d	a

all non-singular square matrices of order n is a
on of matrices.

ll matrices of the form $\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ and
usual addition and multiplication of matrices.
3, 4} is a ring under addition modulo 5 and

$b+1$, $a \odot$

$\in Z$. Show
is it a ring

$= -1$ and 0 is its unity.]

$\begin{bmatrix} & b \\ & \end{bmatrix}$ is a

for e

$a \odot b = 0$ for
y ?
s, (ii) Yes, (iii) No]

without zero divisors is called

lowing

I_1 : It is a commutative ring.

I_2 : It is a ring with unity.

I_3 : It is a ring without zero divisors.

Examples of Integral Domain

1. The set $(Z, +, \cdot)$ is an integral domain.
2. The set $(Q, +, \cdot)$ is an integral domain.
3. But the set of even integers including zero with usual addition and multiplication is not an integral domain because it does not have multiplicative identity.

Example 1 : Let $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| \, a \in R \right\}$ and let + and $\cdot$ denote usual matrix addition and multiplication.

Is $(M, +, \cdot)$ an integral domain ?

Sol. : ***Closure*** **(M.U. 2001, 03)**

Let $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}$, $a, b \in R$.

Then $A + B = \begin{bmatrix} a+b & 0 \\ 0 & a+b \end{bmatrix} \in M$

and $AB = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} \in M$

$\therefore$ M is closed under addition and multiplication.

I_1 : Consider $(M, +)$

(i) Matrix addition is associative.

(ii) Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ for all $a \in R$, additive identity exists.

(iii) Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} -a & 0 \\ 0 & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, additive inverse exists.

(iv) Matrix addition is commutative.

$\therefore$ $(M, +)$ is a commutative group.

(v) For matrices $A \cdot (B + C) = A \cdot B + A \cdot C$ and $(B + C) \cdot A = B \cdot A + C \cdot A$.

Hence, $\cdot$ distributes over +.

Hence, $(M, +, \cdot)$ is a commutative ring.

I_2 : Consider $(M, +, \cdot)$

Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

$\therefore$ Multiplicative identity exists.

Hence, $(M, +, \cdot)$ is a ring with unity.

I 3 : Consider again $(M, +, \cdot)$

Since $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix}$, and $\begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & ba \end{bmatrix}$.

Hence, $(M, +, \cdot)$ is a commutative ring with unity but without zero divisors.

$\therefore$ $(M, +, \cdot)$ is an integral domain.

Example 2 : If addition and multiplication modulo 10 are defined on the set of integers $R = \{0, 2, 4, 6, 8\}$ then show that the system is an integral domain. **(M.U. 2006, 07)**

Sol. : Refer to Ex. 8 § 13. Yes. The system is an integral domain.

Example 3 : In an integral domain D. Show that if $ab = ac$ with $a \neq 0$ then $b = c$. **(M.U. 1998)**

Sol. : We have $ab = bc$

Multiply both sides by a^{-1},

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

$\therefore$ $(a^{-1}a)\, b = (a^{-1}\, a)\, c$ [associativety]

$eb = ec$ [inverse]

$\therefore$ $b = c$ [e is identity]

15. Field

Definition 1 (Field) : A commutative ring with unity and multiplicative inverse for each non-zero element is called a **field.**

A field can be defined in a more explicit way as follows.

Definition 2 (Field) : A field is an ordered triplet $(F, +, \cdot)$ where F is a non-empty set and + and $\cdot$ are two binary operations on F satisfying the following axioms.

***F* 1 :** $(F, +)$ is a commutative group.

***F* 2 :** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in F$ ($\cdot$ is commutative.)

***F* 3 :** $a \cdot (b + c) = a \cdot b + a \cdot c$

and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in F$ ($\cdot$ distributes over +).

***F* 4 :** $(F \sim 0, \cdot)$ is a commutative group.

Clearly, because of F_4, a field is a commutative ring with unity in which every non-zero element has multiplicative inverse.

Example 1 : Show that the set of integers Z is a ring under addition and multiplication. Is it a field ?

Sol. : ***Closure*** - Clearly Z is closed under + and $\cdot$.

***R* 1 :** Consider $(Z, +)$

(i) Since for all integers $a + (b + c) = (a + b) + c$, addition is associative.

(ii) Since $a + 0 = 0 + a$ for all $a \in Z$, additive identity exists.

(iii) Since we have $-a$ corresponding to every $a \in Z$ such that

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

for every element $a \in Z$, additive inverse exists.

(iv) Since $a + b = b + a$ for all $a, b,$

$\therefore$ $(Z, +)$ is a commutative gr

R 2 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a

R 3 : $a \cdot (b + c) = a \cdot b + a \cdot c$ and

Hence, $\cdot$ distributes over +.

Hence, $(Z, +, \cdot)$ is a ring.

However, no element of Z except

er a such that $2a = 1$.

$\therefore$ $(Z \sim 0, \cdot)$ is not a group.

Example 2 : Show that the set F

er addition and multiplication.

Closure - Let $x = a + b\sqrt{2}$, $y =$

Since, $x + y = (a + b\sqrt{2}) + (c +$

and $xy = (a + b\sqrt{2})(c + d\sqrt{2})$

$= (ac + 2bd) + \sqrt{2}\,(ad$

since $(a + c)$, $(b + d)$, $(ac + 2bd)$,

osed under addition + and multipli

F 1 : Consider $(F, +)$.

(i) Since for all rational numbe

$x + (y + z) = (x + y)$

(ii) Since $(a + b\sqrt{2}) + (0 + 0$

(iii) Since $(a + b\sqrt{2}) + (-\sqrt{a} -$

(iv) Since for rational numbers

$\therefore$ $(F, +)$ is a commuta

F 2 : It can be shown that $(x \cdot y$

Hence, $\cdot$ is associative.

F 3 : It can be shown that $x \cdot (y$

and $(x + y) \cdot z = x \cdot z + y \cdot z$ for

Hence, $\cdot$ distributes over +.

F 4 : Consider $(F \sim 0, \cdot)$,

(i) $\cdot$ is associative as noted i

(ii) Since $(a + b\sqrt{2}) \cdot (1 + 0$

(iii) If $x \neq 0$ i.e. if $a \neq 0$, $b \neq 0$,

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{}{a +}$$

ere $c = \dfrac{a}{a^2 - 2b}$, $d = -\dfrac{b}{a^2 - 2b}$.

Since $a + b\sqrt{2} \neq 0$, $a - b\sqrt{2} \neq$

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & ba \end{bmatrix}.$$

t without zero divisors.

ntegers
2006, 07)

th $a \neq 0$ then $b = c$. (M.U. 1998)

et and + and

very non-zero element

ddition and multiplication. Is it a

ion is associative.
xists.
such that

(iv) Since $a + b = b + a$ for all $a, b, c \in Z$, addition is commutative.

$\therefore$ $(Z, +)$ is a commutative group.

R 2 : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in Z$. Hence, $\cdot$ is associative.

R 3 : $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Hence, $\cdot$ distributes over $+$.

Hence, $(Z, +, \cdot)$ is a ring.

However, no element of Z except ± 1 has multiplicative inverse. For example, there exists no integer a such that $2a = 1$.

$\therefore$ $(Z \sim 0, \cdot)$ is not a group. $\therefore$ $(Z, +, \cdot)$ is not a field.

Example 2 : Show that the set $F = \{a + b\sqrt{2}\}$ where a and b are rational numbers is a field er addition and multiplication. **(M.U. 2002, 03, 08)**

***Closure* -** Let $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ where $a, b, c, d \in Q$.

Since, $x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$

and $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd$

$= (ac + 2bd) + \sqrt{2}(ad + bc)$

since $(a + c)$, $(b + d)$, $(ac + 2bd)$, $(ad + bc)$ are rational numbers $(x + y)$ and $xy \in F$. Hence, F osed under addition + and multiplication $\cdot$.

F 1 : Consider $(F, +)$.

(i) Since for all rational numbers addition is associative, we can show that

$x + (y + z) = (x + y) + z$. $\therefore$ Addition is associative.

(ii) Since $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2}$, $0 + 0\sqrt{2}$ *i.e.* $0 \in Q$ is additive identity.

(iii) Since $(a + b\sqrt{2}) + (-\sqrt{a} - b\sqrt{2}) = 0 + 0\sqrt{2}$, for every $a + b\sqrt{2}$, additive inverse exists.

(iv) Since for rational numbers addition is commutative, we can show that $x + y = y + x$.

$\therefore$ $(F, +)$ is a commutative group.

F 2 : It can be shown that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$.

Hence, $\cdot$ is associative.

F 3 : It can be shown that $x \cdot (y + z) = x \cdot y + x \cdot z$

and $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in F$.

Hence, $\cdot$ distributes over $+$.

F 4 : Consider $(F \sim 0, \cdot)$,

(i) $\cdot$ is associative as noted in F 2.

(ii) Since $(a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = a + b\sqrt{2}$, $1 + 0\sqrt{2}$, is the multiplicative identity.

(iii) If $x \neq 0$ *i.e.* if $a \neq 0$, $b \neq 0$, and $x = a + b\sqrt{2}$, then

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b} = c + d\sqrt{2}$$

where $c = \dfrac{a}{a^2 - 2b}$, $d = -\dfrac{b}{a^2 - 2b}$.

Since $a + b\sqrt{2} \neq 0$, $a - b\sqrt{2} \neq 0$ hence, $a^2 - 2b \neq 0$.

$\therefore\ c, d \in Q \quad \therefore\ \frac{1}{x} \in F.$

$\therefore$ For every $x \in (F \sim 0)$, there exists multiplicative inverse.

$\therefore$ $(F \sim 0, \cdot)$ is a commutative group.

Hence, $(F, +, \cdot)$ is a field.

Example 3 : Let Z be the set of integers and $a \oplus b = a + b - 1$ and $a \otimes b = a + b - ab$. Show that $(Z, \oplus, \otimes)$ is a ring ? Is it an integral domain ? Is it a field ?

(M.U. 1998, 99, 2005)

Sol. : (i) Clearly $a \oplus b = a + b - 1$ and $a \otimes b = = a + b - ab$ are binary operations in Z.

(ii) *R* 1 : $(Z, \oplus)$ is a commutative group as shown below.

***G* 1 :** For all $a, b, c \in Z$. $\quad a \oplus b = a + b - 1$

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

Now, $\quad b \oplus c = b + c - 1$

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

$\therefore\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$

$\therefore$ $\oplus$ is associative.

***G* 2 :** There exists additive identity (1).

This is so because,

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

Thus, 1 is the zero (*i.e.* additive identity)

***G* 3 :** For every element $a \in G$ there is an element $b = 2 - a$ which is its inverse.

This is so because

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

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

***G* 4 : Commutativity of $\oplus$**

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

$\therefore$ $a \oplus b$ is commutative.

$\therefore$ $(Z, \oplus)$ is a commutative group.

(iii) *R* 2 : $\otimes$ is associative. This is so because

$$a \otimes b = a + b - ab$$

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

Now, $\quad b \otimes c = b + c - bc$

$\therefore\ a \otimes (b \otimes c) = a \otimes (b + c - bc)$

$= a + b +$

$\therefore\ a \otimes (b \otimes c) = (a \otimes b)$

$\therefore$ $\otimes$ is associative.

R3 : Distributivity

Now, $\quad a \otimes (b \oplus c) = a \otimes (b$
$= a + b$
$= 2a + b$

and $\quad a \otimes b = a + b$
$a \otimes c = a + c$

$\therefore\ (a \otimes b) \oplus (a \otimes c) = (a + b$
$= a + b$
$= 2a +$

$\therefore\ a \otimes (b \oplus c) = (a \otimes$

$\therefore$ $\otimes$ distributes over $\oplus$.

Hence, $(Z, \oplus, \otimes)$ is a ring.

Commutativity of $\otimes$

$a \otimes b = a +$
$a \otimes b = b \otimes$

$\therefore\ (Z, \oplus, \otimes)$ is a comm

Unity

Now, $\quad a \otimes 0 = a +$

and $\quad 0 \otimes a = 0 +$

$\therefore$ 0 is its unity (*i.e.* mu

$\therefore\ (Z, \oplus, \otimes)$ is a comm

Zero Divisor

Now, $\quad a \otimes b = a +$

and $a \otimes b$ will be zero if a

$\therefore\ (Z, \oplus, \otimes)$ is a ring

$\therefore\ (Z, \oplus, \otimes)$ is an int

For $a, b \in Z$ consider the e

$\therefore\ b = -\frac{a}{1 - a}$.

Since $ab = 0$ for $b = -\frac{a}{1 -$

verse of a.

$\therefore\ (Z, \oplus, \otimes)$ is a fiel

Example 4 : Prove that
1, 2, 3, 4} modulo 5.

Sol. : We prepare the tables for

$= a + b + c - bc - ab - ac + abc$

$\therefore \quad a \otimes (b \otimes c) = (a \otimes b) \otimes c$

$\therefore$ $\otimes$ is associative.

(iv) **$R3$: Distributivity**

Now, $a \otimes (b \oplus c) = a \otimes (b + c - 1)$

$= a + b + c - 1 - ab - ac + a$

$= 2a + b + c - ab - ac - 1$

and $a \otimes b = a + b - ab$

$a \otimes c = a + c - ac$

$\therefore \quad (a \otimes b) \oplus (a \otimes c) = (a + b - ab) \oplus (a + c - ac)$

$= a + b - ab + a + c - ac - 1$

$= 2a + b + c - ab - ac - 1$

$\therefore \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

$\therefore$ $\otimes$ distributes over $\oplus$.

Hence, $(Z, \oplus, \otimes)$ is a ring.

(v) **Commutativity of $\otimes$**

$a \otimes b = a + b - ab$ and $b \otimes a = b + a - ba$

$a \otimes b = b \otimes a.$

$\therefore \quad (Z, \oplus, \otimes)$ is a commutative ring.

(vi) **Unity**

Now, $a \otimes 0 = a + 0 - a \cdot 0 = a$

and $0 \otimes a = 0 + a - 0 \cdot a = a$

$\therefore$ 0 is its unity (*i.e.* multiplicative identity).

$\therefore \quad (Z, \oplus, \otimes)$ is a commutative ring with unity.

(vii) **Zero Divisor**

Now, $a \otimes b = a + b - ab$

and $a \otimes b$ will be zero if $a = 0$ and $b = 0$.

$\therefore \quad (Z, \oplus, \otimes)$ is a ring without zero divisor.

$\therefore \quad (Z, \oplus, \otimes)$ is an integral domain.

(viii) For $a, b \in Z$ consider the equation $a \otimes b = 0$ *i.e.* $a + b - ab = 0$.

$\therefore \quad b = -\frac{a}{1-a}.$

Since $ab = 0$ for $b = -\frac{a}{1-a}$ where 0 is its multiplicative identity, $-\frac{a}{1-a}$ is the multiplicative inverse of a.

$\therefore \quad (Z, \oplus, \otimes)$ is a field.

Example 4 : Prove that $(Z_5, +, \cdot)$ is a field where Z_5 is a set R of residue classes of $\{0, 1, 2, 3, 4\}$ modulo 5. **(M.U. 2001, 03, 06, 08)**

Sol. : We prepare the tables for addition and multiplication of {0, 1, 2, 3, 4} modulo 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

×	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

Closure : It is clear from the table that Z_5 is closed under addition and multiplication modulo 5.

***F*1 :** Consider $(Z_5, +)$

(i) Since $a + (b + c) = (a + b) + c$, for all $a, b, c \in Z_5$, addition is associative.

(ii) Since $a + 0 = a$ for all $a \in Z_5$, $0 \in Z_5$ is the additive identity.

(iii) Since $1 + 4 = 0 = 4 + 1$, $2 + 3 = 0 = 3 + 2$, additive inverse exist.

(iv) Since $a + b = b + a$ for all $a, b \in Z_5$, addition is commutative.

$\therefore$ $(Z_5, +)$ is a commutative group.

***F*2 :** It is clear from the table that $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in Z_5$.

***F*3 :** It can be seen that

$$a \times (b + c) = a \times b + a \times c$$

and $$(b + c) \times a = b \times a + b \times c.$$

Hence, $\times$ distributes over $+$.

***F*4 :** Consider $(Z_5 \sim 0, \times)$.

(i) $\times$ is associative.

(ii) From the second row or second column of second table we see that 1 is the multiplicative identity.

(iii) Since $1 \times 1 = 1$, $2 \times 3 = 1$, $3 \times 2 = 1$, $4 \times 4 = 1$, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ and $4^{-1} = 4$.

For every $a \in (Z_5 \sim 0)$, there exists multiplicative inverse.

$\therefore$ $(Z_5 \sim 0, \times)$ is a commutative group.

Hence, $(Z_5, +, \times)$ is a field.

Example 5 : Is $(Z_6, +, \times)$ an integral domain ? Is it a field ? **(M.U. 2003)**

Sol. : We first prepare the tables for addition and multiplication modulo 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

×	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

Prove that it is not a field because $3 \times 4 = 0$ but $3 \neq 0$ and $4 \neq 0$.

Example 6 : Is $(Z_p, \oplus, \otimes)$ a field where p is a prime ? **(M.U. 2004)**

Sol. : We first note that $Z_p = \{0, 1, 2, \ldots, p-1\}$ where p is any prime number.

We prepare the tables for addition and multiplication of Z_p.

+	0	1	2	....	$p-1$
0	0	1	2	....	$p-1$
1	1	2	3	....	0
2	2	3	4	....	1
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	$p-1$	0	1	....	$p-2$

×	0	1	2	....	$p-1$
0	0	0	0	....	0
1	0	1	2	....	$p-1$
2	0	2	4	....	$p-2$
⋮	⋮	⋮	⋮	⋮	⋮
$p-1$	0	$p-1$	$p-2$	....	1

Closure : It is clear that Z_p is closed under addition and multiplication modulo p.

F 1 : Consider $(Z_p, +)$.

As in Ex. 4 page 16-59, we can prove that $(Z_p, +)$ is a commutative group.

F 2 : Consider $(Z_p - 0, \times)$.

Again as in Ex. 4 page 16-59, we can prove that $(Z_p, \times)$ is a commutative group.

Hence, $(Z_p, +, \times)$ is a field.

....✍

In the first table the sum of $p-1$ and $p-1 = 2p-2$. When this is divided by p the quotient in modulo operation is **not** 2 and the remainder is not -2 because the remainder in modulo operation is never negative. When $2p-2$ is divided by p the quotient is 1 and the remainder is $p-2$.

Example 7 : Let $S = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \middle| \; a \in R \right\}$ and $+$ and $\cdot$ be matrix addition and matrix multiplication. Is $(S, +, \cdot)$ an integral domain ? Is it a field ? **(M.U. 2002, 05)**

Sol. : Closure

Let $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$, $a, b \in R$

Then $A + B = \begin{bmatrix} a+b & a+b \\ a+b & a+b \end{bmatrix} \in S$ and $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}$.

$\therefore$ S is closed under addition and multiplication.

I 1 : Consider $(S, +)$

(i) Matrix addition is associative.

(ii) Since $\begin{bmatrix} a & a \\ a & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$ additive identity exists.

(iii) Since $\begin{bmatrix} a & a \\ a & a \end{bmatrix} + \begin{bmatrix} -a & -a \\ -a & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ additive inverse exists.

(iv) Matrix addition is commutative.

$\therefore$ $(S, +)$ is a commutative group.

(v) For matrices $A \cdot (B + C) = A \cdot C + B \cdot C$

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

Hence, · distributes over +.

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

I 2 : Consider $(S, +, \cdot)$

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2a & 2a \\ 2a & 2a \end{bmatrix} \quad \therefore \quad A \cdot I \neq A$$

∴ Multiplicative identity does not exist.

Hence, $(S, +, \cdot)$ is a ring without unity.

∴ It is not an integral domain.

Since, there is no multiplicative identity, there is no multiplicative inverse.

Hence, it is not a field.

Example 8 : Show that the set of matrices $M = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}$, $a, b \in Z$ form an integral domain. Is it a field ? **(M.U. 1996, 97, 98, 2004)**

Sol. : ***Closure***

Let $A = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ -5d & c \end{bmatrix}$, $a, b, c, d \in Z$.

Then $A + B = \begin{bmatrix} a+c & b+d \\ -5(b+d) & a+c \end{bmatrix} \in M$ and $AB = \begin{bmatrix} ac-5bd & ad+bc \\ -5(bc+ad) & ac-5bd \end{bmatrix} \in M.$

∴ M is closed under addition and multiplication.

I 1 : Consider $(M, +)$

(i) Matrix addition is associative.

(ii) Since $\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}$, $a, b \in Z$, additive identity exists.

(ii) Since $\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} -a & -b \\ 5b & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, additive inverse exists.

(iv) Matrix addition is commutative.

∴ $(M, +)$ is a commutative group.

(v) For matrices $A \cdot (B + C) = A \cdot B + A \cdot C$

and $(B + C) \cdot A = B \cdot A + C \cdot A.$

Hence, · distributes over +.

∴ $(M, +, \cdot)$ is a commutative ring.

I 2 : Consider $(M, +, \cdot)$

Since $\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -5b & a \end{bmatrix}$

Multiplicative unity exists.

Hence, $(M, +, \cdot)$ is a ring with unity.

I 3 : Consider $(M, +, \cdot)$

$$\begin{bmatrix} a & b \\ -5b & a \end{bmatrix}\begin{bmatrix} c & d \\ -5d & c \end{bmatrix} = \begin{bmatrix} ac-5bd & ad+bc \\ -5(bc+ad) & ac-5bd \end{bmatrix}$$

and $$\begin{bmatrix} c & d \\ -5d & c \end{bmatrix}\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} = \begin{bmatrix} ac-5d & ad+bc \\ -5(ad+bc) & ac-5bd \end{bmatrix}$$

Hence, $(M, +, \cdot)$ is a commutative ring with unity but without zero divisors.

I 4 : However, no element of M has multiplicative inverse.

$\therefore$ $(M \sim 0, \cdot)$ is not a group.

$\therefore$ Hence, $(M, +, \cdot)$ is not a field.

Example 9 : Let $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, a \in R \right\}$. Is $(S, +, \cdot)$ an integral domain ? **(M.U. 2001)**

Sol. : Yes. Prove it.

Example 10 : Prove that every field is an integral domain. Is the converse true ?

(M.U. 2001, 02, 04)

Sol. : We know that a field is a ring $(F, +, \cdot)$ in which $(F \sim 0, \cdot)$ is a commutative group.

We also know that an integral domain is a commutative ring with unity but without zero divisors.

Thus, to prove that every field is an integral domain, we have to show that a field does not have zero divisors.

Let $a \neq 0$ be an element of F. Then, a^{-1} exists where a^{-1} is the multiplicative inverse.

Let $b \in F$ be such that $ab = 0$ $\therefore$ $a^{-1}(ab) = 0$

$\therefore$ $(a^{-1}a)\, b = b$ $\therefore$ $1b = 0$ $\therefore$ $b = 0$.

Thus, we have if $ab = 0$ and $a \neq 0$ then $b = 0$.

$\therefore$ F has no divisors.

$\therefore$ A field is an integral domain.

But the converse is not true. Every integral domain is not a field. For example, Z is an integral domain under usual addition and multiplication. But Z is not a field, since $2^{-1} = \frac{1}{2} \in Z$.

Definitions (A Review)

1. **Semi-group :** A non-empty set S together with a (i) binary and (ii) associative operation is called a **semi-group** $(S, *)$.
2. **Monoid :** A semi-group $(S, *)$ which has identity is called a **monoid.**
3. **Group :** A non-empty set S together with a binary operation $*$ satisfying the following axioms

G 1 : For all $a, b, c \in G$

$a * (b * c) = (a * b) *$ (Associativity)

$a * e = e * a = a$ **(Identity)**

G 2 : For all $a \in G$ there exists $e \in G$ such $a * b = b * a = c$ **(Inverse)** is called a group

G 3 : For all $a \in G$ there exists $b \in G$ such that $(S, *)$.

Note that G 2 and G 3 make a semi-group into a group. Also note that G 3 makes a monoid into a group.

Definition : A semi-group with identity and inverse for each element is called a group.

Definition : A monoid with inverse for each element is called a group.

4. Ring : A ring $(R, +, *)$ where R is a non-empty set and $+$ and $\cdot$ are two binary operations satisfying the following axioms.

$R1$: $(R, +)$ is a commutative group.

$R2$: For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associativity of $\cdot$)

$R3$: For all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and $(b + c) \cdot a = b \cdot a + c \cdot a$ ($\cdot$ distributes over $+$)

Note that $R2$ and $R3$ make a commutative group into a **ring.**

Definition : A commutative group with another associative binary operation $\cdot$ which distributes over $+$ is called a ring.

5. Integral Domain : A commutative ring with unity and without zero divisors is called an **integral domain.**

6. Field : A commutative ring with unity, having multiplicative inverse for every non-zero element is called a **field.**

EXERCISE - IV

(A) **1.** Prove that the set of even integers is a commutative ring under addition and multiplication. But it is not a field.

2. Prove that $(3Z, +, \cdot)$ where $3Z = (\ldots, -6, -3, 0, 3, 6, \ldots)$ is a ring but not a field.

3. Prove that $(mZ, +, \cdot)$ where m is a fixed integer is a ring but not a field.

4. Prove that the set of even integers is a ring under addition and multiplication. But it is not a field. (**Hint :** Let $a = 2m$, $b = 2n$, $m, n \in Z$ etc.)

(B) Show that $R = \{0, 2, 4, 6, 8\}$ is a ring under addition and multiplication modulo 10. Is it an integral domain ? Is it a field ? [**Ans. :** Yes, Yes]

(C) **1.** Prove that $(M, +, \cdot)$ where M is the set of 3×3 matrices is a ring but not a field.

2. Prove that $(F, +, \cdot)$ where $F = a + b\sqrt{5}$, $a, b \in Q$ is a field.

3. Prove that $(F, +, \cdot)$ where $F = a + b\sqrt{7}$, $a, b \in Q$ is a field.

4. Let $S = \{0, 1, 2\}$. We define $\oplus$ as $a \oplus b$ = the least non-negative remainder obtained on dividing $a + b$ by 3 and $a \odot b$ = the least non-negative remainder obtained on dividing ab by 3 where $a, b \in S$.

Prove that $(S, \oplus, \odot)$ is a field.

(**Hint :** 0 and 1 are respectively additive and multiplicative identities. $1 \oplus 2$ implies that 1 and 2 are additive inverses of each other. $1 \odot 1$, $2 \odot 2$, implies that 1 and 2 are multiplicative inverses of themselves.)

5. Show that the matrices of the form $\begin{bmatrix} a & b \\ 2a & a \end{bmatrix}$ where $a, b = Z$ from a field under matrix addition and multiplication. (M.U. 1998)

6. Let $F = \{(a, b) \mid a, b \text{ are reals}\}$. Let $\oplus$ and $\odot$ be defined as $(a, b) \oplus (c, d) = (a + c, b + d)$ and $(a, b) \odot (c, d) = (ac - bd, bc + ad)$. Prove that F is a field. (M.U. 2004)

Sol. : Considering the above definition we have to prove that if $a, a', b, b' \in S$ and if $a \, R \, b$ and $a' \, R \, b'$, then $(a * a') \, R \, (b * b')$ *i.e.* we have to prove that if $a \equiv a' \pmod 3$ and $b = b' \pmod 3$ then $a + b = a' + b' \pmod 3$. Now, since $a \equiv a' \pmod 3$, $(a - a') = 3m$ say and since $b \equiv b' \pmod 3$, $(b - b') = 3n$, say, where m and n are integers.

$\therefore \quad a - a' + b - b' = 3m + 3n$

$\therefore \quad (a + b) - (a' + b') = 3 (m + n)$

$\therefore \quad (a + b) \equiv (a' + b') \pmod 3$

Hence, the result.

(d) Cyclic Group (M.U. 2000, 13)

Definition : A group $(G, *)$ is said to be a **cyclic group** if there exists an element $a \in G$ such that every element of G can be written as some power of a *viz.* a^k for some integer k where by a^k we mean $a \times a \times a \ldots\ldots a$ (k times).

Then G is said to be generated by a or a generates G.

A cyclic group is always Abelian because commutativity is observed,

$\because$ if $a^r, a^s \in G$, then $a^r \times a^s = a^s \times a^r$.

Example 1 : The cube roots of unity form a cyclic group under multiplication of complex numbers.

Sol. : In Example 2, page 16-13, we have proved that the cube roots of unity is a group under multiplication.

Now, we shall prove that it is cyclic *i.e.*, every element of the group $1, \omega, \omega^2$ can be expressed as integral power of some element $a \in G$.

We note that $\omega^0 = 1, \ \omega^1 = \omega, \ \omega^2 = \omega^2$.

Thus, the element $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω. Hence, the group is cyclic with ω as a generator.

Also, $(\omega^2)^0 = 1, \ (\omega^2)^1 = \omega^2, \ (\omega^2)^2 = \omega^4 = \omega^3 \cdot \omega = \omega$.

Thus, $1, \omega, \omega^2$ are expressed as 0^{th}, 1^{st} and 2^{nd} power of ω^2.

Hence, the group is cyclic with ω^2 as a generator.

Example 2 : Prove that the group $G = \{ 0, 1, 2, 3, 4, 5 \}$ is a finite, abelian, cyclic group under addition modulo 6.

Sol. : We have proved in Example 2, page 16-27 that G is an Abelian group.

Now, we shall prove that it is a cyclic group *i.e.*, every element of the group G can be expressed as integral power of some element $a \in G$.

We note that $1^1 = 1, \quad 1^2 = 1 +_6 1 = 2, \quad 1^3 = 1 + 1_6 \, 1^2 = 1 +_6 2 = 3,$

$1^4 = 1 +_6 1^3 = 1 +_6 3 = 4, \quad 1^5 = 1 +_6 1^4 = 1 +_6 4 = 5,$

$1^6 = 1 +_6 1^5 = 1 +_6 5 = 0.$ [See the table on page 16-27]

Hence, $G = \{ 1^6, 1^1, 1^2, 1^3, 1^4, 1^5 \}$.

$\therefore$ G is a cyclic group with 1 as a generator.

(It can be shown that 5 is another generator.)

(e) Subgroup

Definition : Let H be a

(i) the identity eleme

(ii) if a, b belong to

(iii) if $a \in H$ then a^{-1}

In short a subgroup is

Illustrations : (i) Let

real under multiplication.

Let $H = \{ a + ib \mid a^2 +$

(ii) Let G be the group

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \right.$

Example 1 : Consid

Let $H = \{\ldots\ldots, -3m, -$

Show that H is a sub

Sol. : (i) The identity of

(ii) If km and lm a

$(km + lm) =$

(iii) If km is an ele

$\therefore$ H is a subg

Example 2 : Find

Sol. : The operation ad

From the first row

element.

$\because \quad 1 \oplus 4 = 0$

$\because \quad 4 \oplus 1 = 0$

Also $2 \oplus 3 = 0$

and $3 \oplus 2 =$

Hence, we consi

Now, by definitio

(i) the identity

(ii) if a, b belo

(iii) if a belong

The above prop

subgroups.

Some Algebraic Structures

, $b' \in S$ and if $a \, R \, b$ and
) and $b = b'$ (mod 3) then
nd since $b \equiv b'$ (mod 3),

(M.U. 2000, 13)

an element $a \in G$ such
nteger k where by a^k we

ltiplication of complex

unity is a group under

, ω^2 can be expressed

. Hence, the group is

n, cyclic group under

G can be expressed

-27]

Subgroup

Definition : Let H be a subset of group G, such that (M.U. 2002, 04, 05, 10)

(i) the identity element e of G belongs to H.

(ii) if a, b belong to H then $a * b$ also belongs to H.

(iii) if $a \in H$ then $a^{-1} \in H$. Then H is called a **subgroup** of G.

In short a subgroup is a subset of G having all the properties of a group.

Illustrations : (i) Let G be the group of all non-zero complex numbers $a + ib$ where a, b are under multiplication.

Let $H = \{ a + ib \mid a^2 + b^2 = 1 \}$ then H is a subgroup of G.

(ii) Let G be the group of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc \neq 0$ under matrix multiplication.

Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; ad \neq 0 \right\}$, then H is a subgroup of G.

Example 1 : Consider the group Z of integers under addition.

Let $H = \{\ldots\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots\}$ where m is a positive integer.

Show that H is a subgroup of Z.

(i) The identity of element of G is 0 and 0 belongs to H.

(ii) If km and lm are any two elements of H, then

$(km + lm) = (k + l)\, m$ is also an element of H.

(iii) If km is an element of H, then its negative (inverse) $-km$ is also an element of H.

$\therefore$ H is a subgroup.

Example 2 : Find the subgroups of $(Z_5, \oplus)$ where $\oplus$ is the operation addition modulo 5. (M.U. 1998)

The operation addition modulo 5 is given by the adjoining table.

Addition Modulo 5

$\oplus$	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

From the first row and first column we see that 0 is the identity ent.

$\because$ $1 \oplus 4 = 0$, inverse of 1 is 4.

$\because$ $4 \oplus 1 = 0$, inverse of 4 is 1.

Also $2 \oplus 3 = 0$, inverse of 2 is 3.

and $3 \oplus 2 = 0$, inverse of 3 is 2.

Hence, we consider two subgroups of $(Z_5, \oplus)$ viz. $G_1 = \{0, 1, 4\}$ and $G_2 = \{0, 2, 3\}$.

Now, by definition of subgroup H is a subgroup if

(i) the identity element e belongs to H.

(ii) if a, b belongs to H then $a \oplus b$ belongs to H.

(iii) if a belongs to H then a^{-1} belongs to H.

The above properties are satisfied by $\{0, 1, 4\}$ and $\{0, 2, 3\}$ under $\oplus$ and hence they are roups.